
# WiNG™ 5.9.1

# Access Point, Wireless Controller and Service Platform

*CLI Reference Guide*

Published September 2017

9035205

## Legal Notices

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

## Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information about Extreme Networks trademarks, go to: www.extremenetworks.com/company/legal/trademarks/

## Support

For product support, including documentation, visit: www.extremenetworks.com/support/

# Contents

## Chapter 3, PRIVILEGED EXEC MODE COMMANDS

## Chapter 4, GLOBAL CONFIGURATION COMMANDS

## Chapter 5, COMMON COMMANDS



## Chapter 6, SHOW COMMANDS

## Chapter 7, PROFILES

## Chapter 8, AAA-POLICY



## Chapter 9, AUTO-PROVISIONING-POLICY



## Chapter 10, ASSOCIATION-ACL-POLICY



## Chapter 11, ACCESS-LIST

## Chapter 12, DHCP-SERVER-POLICY



## Chapter 13, FIREWALL-POLICY

## Chapter 17, RADIO-QOS-POLICY



## Chapter 18, ROLE-POLICY



## Chapter 19, SMART-RF-POLICY

## Chapter 20, WIPS-POLICY



## Chapter 21, WLAN-QOS-POLICY



## Chapter 22, L2TPV3-POLICY

## Chapter 27, PASSPOINT POLICY



## Chapter 28, BORDER GATEWAY PROTOCOL

## Chapter 29, CRYPTO-CMP-POLICY

## Chapter 30, ROAMING ASSIST POLICY



## Appendix A, CONTROLLER MANAGED WLAN USE CASE



## Appendix B, PUBLICLY AVAILABLE SOFTWARE

# ABOUT THIS GUIDE

This manual supports the following wireless controllers, service platformss, and access points:

- Wireless Controllers – RFS4000, RFS6000
- Service Platformss – NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000
- Access Points – AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8122, AP8132, AP8163, AP8232, AP8432, AP8533

**NOTE:** In this document AP8122, AP8132, AP8163 are collectively referred to as AP81XX.

**CAUTION:** To configure a WE access point, exclusively use the WE UI. Do not use the *command line interface* (CLI) along with it. Similarly, when using the CLI to configure the WE access point, do not use the WE UI along with it.

A simplified version of the WiNG operating system *user interface* (UI) is available on the following access point and service platforms models:

- AP6521E, AP6522E, AP6562E, AP7502E, AP7522E, AP7532E, AP7562E, AP7602, AP7612, AP7632, AP7662
- NX5500E, NX7510E, and VX9000E

This new WiNG *Express* (WE) UI, simplifies configuration and monitoring of small access point deployments by limiting monitoring, analytics, and configuration capabilities. The WE UI is designed for single-site access point deployments not exceeding more than 24 access points of the same model.

This section is organized into the following topics:

- *Document Conventions*
- *Notational Conventions*
- *End-User Software License Agreement*

## Document Conventions

The following conventions are used in this document to draw your attention to important information:

**NOTE:** Indicates tips or special requirements.

**CAUTION:** Indicates conditions that can cause equipment damage or data loss.

**WARNING!** Indicates a condition or procedure that could result in personal injury or equipment damage.

**Switch Note:** Indicates caveats unique to a RFS4000, RFS6000, NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, or NX9600 model controller.

## Notational Conventions

The following notational conventions are used in this document:

- Italics are used to highlight specific items in the general text, and to identify chapters and sections in this and related documents
- Bullets (•) indicate:
  - lists of alternatives
  - lists of required steps that are not necessarily sequential
  - action items
- Sequential lists (those describing step-by-step procedures) appear as numbered lists

**Understanding Command Syntax**

| | |
|---|---|
| <variable> | Variables are described with a short description enclosed within a '<' and a '>' pair.<br>For example, the command,<br>`nx9500-6C8809>show interface ge 1`<br>is documented as:<br>`show interface ge <1-2>`<br>where:<br>• show – is the command – displays information<br>• interface – is the keyword – represents the interface type<br>• <1-2> – is the variable – represents the ge interface index value |

| | |
|---|---|
| \| | The pipe symbol. This is used to separate the variables/keywords in a list.<br>For example, the command,<br>`nx9500-6C8809> show .....`<br>is documented as:<br>`show [adoption\|bluetooth\|bonjour\|boot\| ......`<br>where:<br>• show – is the command – displays information<br>• [adoption\|bluetooth\|bonjour\|boot\|.....] – indicates the different keywords that can be combined with the show command. However, only one of the above option can be used at a time.<br>`show adoption ...`<br>`show bluetooth ...`<br>`show bonjour ...` |
| [] | Of the different keywords and variables listed inside a '[' & ']' pair, only one can be used. Each choice in the list is separated with a '\|' (pipe) symbol.<br>For example, the command,<br>`nx9500-6C8809#clear ...`<br>is documented as:<br>`clear [arp-cache\|bonjour\|cdp\|counters\|crypto\| event-history\|firewall\|gre\|ip\|ipv6\|l2tpv3-stats\|lacp\|license\|lldp\|logging\|mac-address-table\|mint\|role\|rtls\|spanning-tree\|traffic-shape\|vrrp]`<br>where:<br>• clear – is the command<br>• [arp-cache\|cdp\|bonjour\|counters\|crypto\|event-history\|firewall\|gre\|ip\|ipv6\|l2tpv3-stats\|lacp\|license\|lldp\|logging\|mac-address-table\|mint\|role\|rtls\|spanning-tree\|traffic-shape\|vrrp] – indicates that these keywords are available for this command. However, only one can be used at a time. |

| | |
|---|---|
| { } | Any command/keyword/variable or a combination of them inside a *'{' &'}'* pair is optional. All optional commands follow the same conventions as listed above. However, they are displayed italicized.<br>For example, the command,<br>`nx9500-6C8809> show adoption ....`<br>is documented as:<br>`show adoption info {on <DEVICE-NAME>}`<br>here:<br>• show adoption info – is the command. This command can also be used as:<br>`show adoption info`<br>The command can also be extended as:<br>`show adoption info {on <DEVICE-NAME>}`<br>here:<br>• {on <DEVICE-NAME>} – is the keyword, which is optional. |
| command / keyword | The first word is always a command. Keywords are words that must be entered as is. Commands and keywords are mandatory.<br>For example, the command,<br>`nx9500-6C8809>show wireless`<br>is documented as:<br>`show wireless`<br>where:<br>• show – is the command<br>• wireless – is the keyword |
| () | Any command/keyword/variable or a combination of them inside a *'(' & ')'* pair are recursive. All recursive commands can be listed in any order and can be used once along with the rest of the commands.<br>For example, the command,<br>`crypto pki export request generate-rsa-key test autogen-subject-name ...`<br>is documented as:<br>`nx9500-6C8809#crypto pki export request generate-rsa-key test autogen-subject-name (<URL>,email <EMAIL>,fqdn <FQDN>,ip-address <IP>)`<br>here:<br>• crypto pki export request generate-rsa-key <RSA-KEYPAIR-NAME> auto-gen-subject-name – is the command<br>• <RSA-KEYPAIR-NAME> – is the RSA keypair name (in this example, the keypair name is 'test'), and is a variable<br>• *(<URL>,email <EMAIL>,fqdn <FQDN>,ip-address <IP>) – is the set of recursive parameters (separated by commas) that can be used in any order.* |

## End-User Software License Agreement

This document is an agreement ("Agreement") between You, the end user, and Extreme Networks, Inc., on behalf of itself and its Affiliates ("Extreme") that sets forth your rights and obligations with respect to the "Licensed Materials". BY INSTALLING SOFTWARE AND/OR THE LICENSE KEY FOR THE SOFTWARE ("License Key") (collectively, "Licensed Software"), IF APPLICABLE, COPYING, OR OTHERWISE USING THE LICENSED SOFTWARE AND/OR ANY OF THE LICENSED MATERIALS UNDER THIS AGREEMENT, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES THE LICENSE(S) AND THE LIMITATION(S) OF WARRANTY AND DISCLAIMER(S)/LIMITATION(S) OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, RETURN THE LICENSE KEY (IF APPLICABLE) TO EXTREME OR YOUR DEALER, IF ANY, OR DO NOT USE THE LICENSED SOFTWARE AND/OR LICENSED MATERIALS AND CONTACT EXTREME OR YOUR DEALER WITHIN TEN (10) DAYS FOLLOWING THE DATE OF RECEIPT TO ARRANGE FOR A REFUND. IF YOU HAVE ANY QUESTIONS ABOUT THIS AGREEMENT, CONTACT EXTREME, Attn: LegalTeam@extremenetworks.com.

1 DEFINITIONS. "Affiliates" means any person, partnership, corporation, limited liability company, or other form of enterprise that directly or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with the party specified. "Server Application" means the software application associated to software authorized for installation (per License Key, if applicable) on one or more of Your servers as further defined in the Ordering Documentation. "Client Application" shall refer to the application to access the Server Application. "Network Device" for purposes of this Agreement shall mean a physical computer device, appliance, appliance component, controller, wireless access point, or virtual appliance as further described within the applicable product documentation, which includes the Order Documentation. "Licensed Materials" means the Licensed Software (including the Server Application and Client Application), Network Device (if applicable), Firmware, media embodying software, and the accompanying documentation. "Concurrent User" shall refer to any of Your individual employees who You provide access to the Server Application at any one time. "Firmware" refers to any software program or code embedded in chips or other media. "Standalone" software is software licensed for use independent of any hardware purchase as identified in the Ordering Documentation. "Licensed Software" collectively refers to the software, including Standalone software, Firmware, Server Application, Client Application or other application licensed with conditional use parameters as defined in the Ordering Documentation. "Ordering Documentation" shall mean the applicable price quotation, corresponding purchase order, relevant invoice, order acknowledgement, and accompanying documentation or specifications for the products and services purchased, acquired or licensed hereunder from Extreme either directly or indirectly.

2 TERM. This Agreement is effective from the date on which You accept the terms and conditions of this Agreement via click-through, commence using the products and services or upon delivery of the License Key if applicable, and shall be effective until terminated. In the case of Licensed Materials offered on a subscription basis, the term of "licensed use" shall be as defined within Your Ordering Documentation.

3 GRANT OF LICENSE. Extreme will grant You a non-transferable, non-sublicensable, non-exclusive license to use the Licensed Materials and the accompanying documentation for Your own business purposes subject to the terms and conditions of this Agreement, applicable licensing restrictions, and any term, user server networking device, field of use, or other restrictions as set forth in Your Ordering Documentation. If the Licensed Materials are being licensed on a subscription and/or capacity basis, the applicable term and/or capacity limit of the license shall be specified in Your Ordering Documentation. You may install and use the Licensed Materials as permitted by the license type purchased as described below in License Types. The license type purchased is specified on the invoice issued to You by Extreme

or Your dealer, if any. YOU MAY NOT USE, COPY, OR MODIFY THE LICENSED MATERIALS, IN WHOLE OR IN PART, EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT.

4 LICENSE TYPES.

- *Single User, Single Network Device*. Under the terms of this license type, the license granted to You by Extreme authorizes You to use the Licensed Materials as bundled with a single Network Device as identified by a unique serial number for the applicable Term, if and as specified in Your Ordering Documentation, or any replacement for that network device for that same Term, for internal use only. A separate license, under a separate License Agreement, is required for any other network device on which You or another individual, employee or other third party intend to use the Licensed Materials. A separate license under a separate License Agreement is also required if You wish to use a Client license (as described below).
- *Single User, Multiple Network Device*. Under the terms of this license type, the license granted to You by Extreme authorizes You to use the Licensed Materials with a defined amount of Network Devices as defined in the Ordering Documentation.
- *Client*. Under the terms of the Client license, the license granted to You by Extreme will authorize You to install the License Key for the Licensed Materials on your server and allow the specific number of Concurrent Users as ordered by you and is set forth in Your Ordering Documentation. A separate license is required for each additional Concurrent User.
- *Standalone*. Software or other Licensed Materials licensed to You for use independent of any Network Device.
- *Subscription*. Licensed Materials, and inclusive Software, Network Device or related appliance updates and maintenance services, licensed to You for use during a subscription period as defined in Your applicable Ordering Documentation.
- *Capacity*. Under the terms of this license, the license granted to You by Extreme authorizes You to use the Licensed Materials up to the amount of capacity or usage as defined in the Ordering Documentation.

5 AUDIT RIGHTS. You agree that Extreme may audit Your use of the Licensed Materials for compliance with these terms and Your License Type at any time, upon reasonable notice. In the event that such audit reveals any use of the Licensed Materials by You other than in full compliance with the license granted and the terms of this Agreement, Extreme reserves the right to charge You for all reasonable expenses related to such audit in addition to any other liabilities and overages applicable as a result of such non-compliance, including but not limited to additional fees for Concurrent Users, excess capacity or usage over and above those specifically granted to You. From time to time, the Licensed Materials may upload information about the Licensed Materials and the associated usage to Extreme. This is to verify the Licensed Materials are being used in accordance with a valid license and/or entitlement. By using the Licensed Materials, you consent to the transmission of this information.

6 RESTRICTION AGAINST COPYING OR MODIFYING LICENSED MATERIALS. Except as expressly permitted in this Agreement, You may not copy or otherwise reproduce the Licensed Materials. In no event does the limited copying or reproduction permitted under this Agreement include the right to decompile, disassemble, electronically transfer, or reverse engineer the Licensed Materials, including the Licensed Software, or to translate the Licensed Materials into another computer language. The media embodying the Licensed Materials may be copied by You, in whole or in part, into printed or machine readable form, in sufficient numbers only for backup or archival purposes, or to replace a worn or defective copy. However, You agree not to have more than two (2) copies of the Licensed Software in whole or in part, including the original media, in your possession for said purposes without Extreme' prior written consent, and in no event shall You operate more copies of the Licensed Software than the specific licenses granted to You. You may not copy or reproduce the documentation. You agree to maintain appropriate records of the location of the original media and all copies of the Licensed Software, in whole or in part, made by You. Any portion of the Licensed Software included in any such modular work shall be used only on a single computer for internal purposes and shall remain subject to

all the terms and conditions of this Agreement. You agree to include any copyright or other proprietary notice set forth on the label of the media embodying the Licensed Software on any copy of the Licensed Software in any form, in whole or in part, or on any modification of the Licensed Software or any such modular work containing the Licensed Software or any part thereof.

7 TITLE AND PROPRIETARY RIGHTS

a The Licensed Materials are copyrighted works and are the sole and exclusive property of Extreme, any company or a division thereof which Extreme controls or is controlled by, or which may result from the merger or consolidation with Extreme (its "Affiliates"), and/or their suppliers. This Agreement conveys a limited right to operate the Licensed Materials and shall not be construed to convey title to the Licensed Materials to You. There are no implied rights. You shall not sell, lease, transfer, sublicense, dispose of, or otherwise make available the Licensed Materials or any portion thereof, to any other party.

b You further acknowledge that in the event of a breach of this Agreement, Extreme shall suffer severe and irreparable damages for which monetary compensation alone will be inadequate. You therefore agree that in the event of a breach of this Agreement, Extreme shall be entitled to monetary damages and its reasonable attorney's fees and costs in enforcing this Agreement, as well as injunctive relief to restrain such breach, in addition to any other remedies available to Extreme.

8 PROTECTION AND SECURITY. In the performance of this Agreement or in contemplation thereof, You and your employees and agents may have access to private or confidential information owned or controlled by Extreme relating to the Licensed Materials supplied hereunder including, but not limited to, product specifications and schematics, and such information may contain proprietary details and disclosures. All information and data so acquired by You or your employees or agents under this Agreement or in contemplation hereof shall be and shall remain Extreme' exclusive property, and You shall use all commercially reasonable efforts to keep, and have your employees and agents keep, any and all such information and data confidential, and shall not copy, publish, or disclose it to others, without Extreme' prior written approval, and shall return such information and data to Extreme at its request. Nothing herein shall limit your use or dissemination of information not actually derived from Extreme or of information which has been or subsequently is made public by Extreme, or a third party having authority to do so.

You agree not to deliver or otherwise make available the Licensed Materials or any part thereof, including without limitation the object or source code (if provided) of the Licensed Software, to any party other than Extreme or its employees, except for purposes specifically related to your use of the Licensed Materials on a single computer as expressly provided in this Agreement, without the prior written consent of Extreme. You acknowledge that the Licensed Materials contain valuable confidential information and trade secrets, and that unauthorized use, copying and/or disclosure thereof are harmful to Extreme or its Affiliates and/or its/their software suppliers.

9 MAINTENANCE AND UPDATES. Except as otherwise defined below, updates and certain maintenance and support services, if any, shall be provided to You pursuant to the terms of an Extreme Service and Maintenance Agreement, if Extreme and You enter into such an agreement. Except as specifically set forth in such agreement, Extreme shall not be under any obligation to provide updates, modifications, or enhancements, or maintenance and support services for the Licensed Materials to You. If you have purchased Licensed Materials on a subscription basis then the applicable service terms for Your Licensed Materials are as provided in Your Ordering Documentation. Extreme will perform the maintenance and updates in a timely and professional manner, during the Term of Your subscription, using qualified and experienced personnel. You will cooperate in good faith with Extreme in the performance of the support services including, but not limited to, providing Extreme with: (a) access to the Extreme Licensed Materials (and related systems); and (b) reasonably requested assistance and

information. Further information about the applicable maintenance and updates terms can be found on Extreme's website at http://www.extremenetworks.com/company/legal/terms-of-support

10 DEFAULT AND TERMINATION. In the event that You shall fail to keep, observe, or perform any obligation under this Agreement, including a failure to pay any sums due to Extreme, or in the event that you become insolvent or seek protection, voluntarily or involuntarily, under any bankruptcy law, Extreme may, in addition to any other remedies it may have under law, terminate the License and any other agreements between Extreme and You.

a Immediately after any termination of the Agreement, Your licensed subscription term, or if You have for any reason discontinued use of Licensed Materials, You shall return to Extreme the original and any copies of the Licensed Materials and remove the Licensed Materials, including an Licensed Software, from any modular works made pursuant to Section 3, and certify in writing that through your best efforts and to the best of your knowledge the original and all copies of the terminated or discontinued Licensed Materials have been returned to Extreme.

b Sections 1, 7, 8, 10, 11, 12, 13, 14 and 15 shall survive termination of this Agreement for any reason.

11 EXPORT REQUIREMENTS. You are advised that the Licensed Materials, including the Licensed Software is of United States origin and subject to United States Export Administration Regulations; diversion contrary to United States law and regulation is prohibited. You agree not to directly or indirectly export, import or transmit the Licensed Materials, including the Licensed Software to any country, end user or for any Use that is prohibited by applicable United States regulation or statute (including but not limited to those countries embargoed from time to time by the United States government); or contrary to the laws or regulations of any other governmental entity that has jurisdiction over such export, import, transmission or Use.

12 UNITED STATES GOVERNMENT RESTRICTED RIGHTS. The Licensed Materials (i) were developed solely at private expense; (ii) contain "restricted computer software" submitted with restricted rights in accordance with section 52.227-19 (a) through (d) of the Commercial Computer Software-Restricted Rights Clause and its successors, and (iii) in all respects is proprietary data belonging to Extreme and/or its suppliers. For Department of Defense units, the Licensed Materials are considered commercial computer software in accordance with DFARS section 227.7202-3 and its successors, and use, duplication, or disclosure by the U.S. Government is subject to restrictions set forth herein.

13 LIMITED WARRANTY AND LIMITATION OF LIABILITY. Extreme warrants to You that (a) the initially-shipped version of the Licensed Materials will materially conform to the Documentation; and (b) the media on which the Licensed Software is recorded will be free from material defects for a period of ninety (90) days from the date of delivery to You or such other minimum period required under applicable law. Extreme does not warrant that Your use of the Licensed Materials will be error-free or uninterrupted.

NEITHER EXTREME NOR ITS AFFILIATES MAKE ANY OTHER WARRANTY OR REPRESENTATION, EXPRESS OR IMPLIED, WITH RESPECT TO THE LICENSED MATERIALS, WHICH ARE LICENSED "AS IS". THE LIMITED WARRANTY AND REMEDY PROVIDED ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE EXPRESSLY DISCLAIMED, AND STATEMENTS OR REPRESENTATIONS MADE BY ANY OTHER PERSON OR FIRM ARE VOID. IN NO EVENT WILL EXTREME OR ANY OTHER PARTY WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION OR DELIVERY OF THE LICENSED MATERIALS BE LIABLE FOR SPECIAL, DIRECT, INDIRECT, RELIANCE, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING LOSS OF DATA OR PROFITS OR FOR INABILITY TO USE THE LICENSED MATERIALS, TO ANY PARTY EVEN IF EXTREME OR SUCH OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL

EXTREME OR SUCH OTHER PARTY'S LIABILITY FOR ANY DAMAGES OR LOSS TO YOU OR ANY OTHER PARTY EXCEED THE LICENSE FEE YOU PAID FOR THE LICENSED MATERIALS.

Some states do not allow limitations on how long an implied warranty lasts and some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation and exclusion may not apply to You. This limited warranty gives You specific legal rights, and You may also have other rights which vary from state to state.

14 JURISDICTION. The rights and obligations of the parties to this Agreement shall be governed and construed in accordance with the laws and in the State and Federal courts of the State of California, without regard to its rules with respect to choice of law. You waive any objections to the personal jurisdiction and venue of such courts. None of the 1980 United Nations Convention on the Limitation Period in the International Sale of Goods, and the Uniform Computer Information Transactions Act shall apply to this Agreement.

15 FREE AND OPEN SOURCE SOFTWARE. Portions of the Software (Open Source Software) provided to you may be subject to a license that permits you to modify these portions and redistribute the modifications (an Open Source License). Your use, modification and redistribution of the Open Source Software are governed by the terms and conditions of the applicable Open Source License. More details regarding the Open Source Software and the applicable Open Source Licenses are available at www.extremenetworks.com/services/SoftwareLicensing.aspx. Some of the Open Source software may be subject to the GNU General Public License v.x (GPL) or the Lesser General Public Library (LGPL), copies of which are provided with the Licensed Materials and are further available for review at www.extremenetworks.com/services/SoftwareLicensing.aspx, or upon request as directed herein. In accordance with the terms of the GPL and LGPL, you may request a copy of the relevant source code. See the Software Licensing web site for additional details. This offer is valid for up to three years from the date of original download of the software.

16 GENERAL.

a This Agreement is the entire agreement between Extreme and You regarding the Licensed Materials, and all prior agreements, representations, statements, and undertakings, oral or written, are hereby expressly superseded and canceled.

b This Agreement may not be changed or amended except in writing signed by both parties hereto.

c You represent that You have full right and/or authorization to enter into this Agreement.

d This Agreement shall not be assignable by You without the express written consent of Extreme. The rights of Extreme and Your obligations under this Agreement shall inure to the benefit of Extreme' assignees, licensors, and licensees.

e Section headings are for convenience only and shall not be considered in the interpretation of this Agreement

f The provisions of the Agreement are severable and if any one or more of the provisions hereof are judicially determined to be illegal or otherwise unenforceable, in whole or in part, the remaining provisions of this Agreement shall nevertheless be binding on and enforceable by and between the parties hereto

g Extreme's waiver of any right shall not constitute waiver of that right in future. This Agreement constitutes the entire understanding between the parties with respect to the subject matter hereof, and all prior agreements, representations, statements and undertakings, oral or written, are hereby expressly superseded and canceled. No purchase order shall supersede this Agreement.

h Should You have any questions regarding this Agreement, You may contact Extreme at the address set forth below. Any notice or other communication to be sent to Extreme must be mailed by certified mail to the following address:

Extreme Networks, Inc.

16480 Via Del

San Jose, CA 95119 United States

Tel: +1 408-579-2800

Toll-free: +1 888-257-3000

# 1 INTRODUCTION

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

Access the CLI by using:

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

**Configuration for connecting to a Controller using a terminal emulator**

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

| | |
|---|---|
| *Bits Per Second* | 19200<br>For AP8533, AP8432, AP7662, AP7632, AP7622, AP7612, AP7602, AP7502, AP7522, AP7532, AP7562, AP6521, AP6522, AP6532, AP6562 model access points set this value to 115200. |
| *Data Bits* | 8 |
| *Parity* | None |
| *Stop Bit* | 1 |
| *Flow Control* | None |

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

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

**User Credentials**

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

| | |
|---|---|
| *User Name* | **admin** |
| *Password* | **admin123** |

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

**Examples in this reference guide**

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

**Supported in the following platforms:**

- Wireless Controller – RFS6000

The above example indicates the command is only available for an RFS6000 model wireless controller.

This chapter is organized into the following sections:

- *CLI Overview*
- *Getting Context Sensitive Help*
- *Using the No Command*
- *Using CLI Editing Features and Shortcuts*
- *Using CLI to Create Profiles and Enable Remote Administration*

# 1.1 CLI Overview

*INTRODUCTION*

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

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

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

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

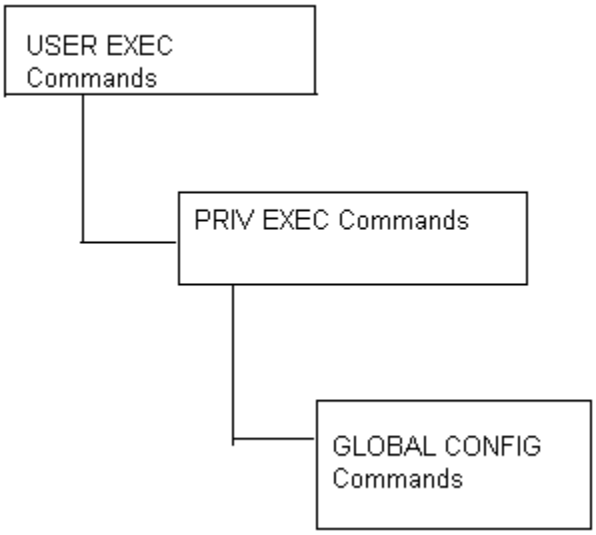


**Figure 1-1** *Hierarchy of User Modes*

**Command Modes**

A session generally begins in the USER EXEC mode (one of the two access levels of the EXEC mode). For security, only a limited subset of EXEC commands are available in the USER EXEC mode. This level is

reserved for tasks that do not change the device's (wireless controller, service platform, or AP) configuration.

```
rfs6000-6DB5D4>
```

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

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

```
rfs6000-6DB5D4>enable
rfs6000-6DB5D4#
```

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

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

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

```
rfs6000-6DB5D4#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
rfs6000-6DB5D4(config)#
```

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

```
rfs6000-6DB5D4(config)#aaa-policy test
rfs6000-6DB5D4(config-aaa-policy-test)#
```

The following table summarizes available CLI commands:

**Table 1.1** *Controller CLI Modes and Commands*

| User Exec Mode | Priv Exec Mode | Global Configuration Mode |
|---|---|---|
| captive-portal-page-upload | archive | aaa-policy |
| change-passwd | boot | aaa-tacacs-policy |
| clear | captive-portal-page-upload | alias |
| clock | cd | ap6521 |
| cluster | change-passwd | ap6522 |
| commit | clear | ap6532 |
| connect | clock | ap6562 |
| create-cluster | cluster | ap7161 |
| crypto | commit | ap7502 |
| crypto-cmp-cert-update | configure | ap7522 |
| database | connect | ap7532 |
| database-backup | copy | ap7562 |

**Table 1.1** *Controller CLI Modes and Commands*

| User Exec Mode | Priv Exec Mode | Global Configuration Mode |
|---|---|---|
| database-restore | cpe (RFS4000, RFS6000, NX9500, NX9600, VX9000) | ap7602 |
| debug | create-cluster | ap7612 |
| device-upgrade | crypto | ap7622 |
| disable | crypto-cmp-cert-update | ap7632 |
| enable | database | ap7662 |
| file-sync | database-backup | ap81xx (ap8122, ap8132, ap8163) |
| help | database-restore | ap8232 |
| join-cluster | debug | ap8432 |
| l2tpv3 | delete | ap8533 |
| logging | device-upgrade | application |
| mint | diff | application-group |
| no | dir | application-policy |
| on | disable | association-acl-policy |
| opendns | edit | auto-provisioning-policy |
| page | enable | bgp |
| ping | erase | bonjour-gw-discovery-policy |
| ping6 | ex3500 | bonjour-gw-forwarding-policy |
| revert | factory-reset | bonjour-gw-query-forwarding-policy |
| service | file-sync | captive-portal |
| show | halt | clear |
| ssh | help | client-identity |
| telnet | join-cluster | client-identity-group |
| terminal | l2tpv3 | clone |
| time-it | logging | crypto-cmp-policy |
| traceroute | mint | customize |
| traceroute6 | mkdir | database-client-policy (supported only on VX9000 |
| virtual-machine (supported only on NX9500, NX9600, and VX9000) | more | database-policy (supported only on NX9500, NX9600, and VX9000) |
| watch | no | device |
| write | on | device-categorization |
| clrscr | opendns | dhcp-server-policy |
| exit | page | dhcp6-server-policy |
| | ping | dns-whitelist |
| | ping6 | event-system-policy |

**Table 1.1** *Controller CLI Modes and Commands*

| User Exec Mode | Priv Exec Mode | Global Configuration Mode |
|---|---|---|
| | pwd | ex3500 |
| | raid (supported only on NX9500 and NX7530) | ex3500-management-policy |
| | re-elect | ex3500-qos-class-map-policy |
| | reload | ex3500-qos-policy-map |
| | remote-debug | ex3524 |
| | rename | ex3548 |
| | revert | firewall-policy |
| | rmdir | global-association-list |
| | self | guest-management |
| | service | help |
| | show | host |
| | ssh | igmp-snoop-policy (This command has been deprecated. IGMP snooping is now configurable under the profile/ device configuration mode. For more information, see *ip*. |
| | t5 (supported only on RFS4000, RFS6000, NX9500, NX9600, and VX9000) | inline-password-encryption |
| | telnet | ip |
| | terminal | ipv6 |
| | time-it | ipv6-router-advertisement-policy |
| | traceroute | l2tpv3 |
| | traceroute6 | mac |
| | upgrade | management-policy |
| | upgrade-abort | meshpoint |
| | virtual-machine (supported only on NX9500, NX9600, and VX9000) | meshpoint-qos-policy |
| | watch | mint-policy |
| | write | nac-list |
| | clrscr | no |
| | exit | nsight-policy |
| | | nx5500 (supported only on NX9500, NX9600, VX9000) |
| | | nx75xx (supported only on NX9500, NX9600, VX9000) |
| | | nx9000 (supported only on NX9500, NX9600, VX9000) |

**Table 1.1** *Controller CLI Modes and Commands*

| User Exec Mode | Priv Exec Mode | Global Configuration Mode |
|---|---|---|
| | | nx9600 (supported only on NX9600) |
| | | passpoint-policy |
| | | password-encryption |
| | | profile |
| | | radio-qos-policy |
| | | radius-group |
| | | radius-server-policy |
| | | radius-user-pool-policy |
| | | rename |
| | | replace |
| | | rf-domain |
| | | rfs4000 |
| | | rfs6000 |
| | | roaming-assist-policy |
| | | role-policy |
| | | route-map |
| | | routing-policy |
| | | rtl-server-policy |
| | | schedule-policy |
| | | self |
| | | sensor-policy |
| | | smart-rf-policy |
| | | t5 (supported only on RFS4000, RFS6000, NX9500, NX9600, VX9000) |
| | | url-filter (supported only on NX9500, NX9600, VX9000) |
| | | url-list (supported only on NX9500, NX9600, VX9000) |
| | | vx9000 (supported only on NX9500, and NX9600, VX9000) |
| | | web-filter-policy |
| | | wips-policy |
| | | wlan |
| | | wlan-qos-policy |
| | | write |
| | | clrscr |

**Table 1.1** *Controller CLI Modes and Commands*

| User Exec Mode | Priv Exec Mode | Global Configuration Mode |
|---|---|---|
| | | commit |
| | | do |
| | | end |
| | | exit |
| | | revert |
| | | service |
| | | show |

## 1.2 Getting Context Sensitive Help

*INTRODUCTION*

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

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

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

**NOTE:** The system prompt varies depending on the configuration mode.

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

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

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

```
rfs6000-6DB5D4#service?
service Service Commands
rfs6000-6DB5D4#service
```

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

```
rfs6000-6DB5D4#service ?
  block-adopter-config-update       Block configuration updates from the
  bluetooth                         Bluetooth service commands
  clear                             Clear adoption history
  cli-tables-skin                   Choose a formatting layout/skin for CLI
                                    tabular outputs (EXPERIMENTAL-Applies only
                                    to certain commands)
  cluster                           Cluster Protocol
  copy                              Copy files or directories
  delete                            Delete sessions
  delete-offline-aps                Delete Access Points that are configured
                                    but offline
  force-send-config                 Resend configuration to the device
  force-update-vm-stats             Force VM statistics to be pushed up to the
                                    NOC
  load-balancing                    Wireless load-balancing service commands
  load-ssh-authorized-keys          Load Ssh authorized keys
  locator                           Enable leds flashing on the device
  mint                              MiNT protocol
  pktcap                            Start packet capture
  pm                                Process Monitor
  radio                             Radio parameters
  radius                            Radius test
  request-full-config-from-adopter  Request full configuration from the
                                    adopter
  set                               Set global options
  show                              Show running system information
  signal                            Send a signal to a process
  smart-rf                          Smart-RF Management Commands
  snmp                              Snmp
  ssm                               Command related to ssm
  start-shell                       Provide shell access
  syslog                            Syslog service
  trace                             Trace a process for system calls and
                                    signals
  troubleshoot                      Troubleshooting
  wireless                          Wireless commands

rfs6000-6DB5D4#
```

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

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

```
rfs6000-6DB5D4>help

When using the CLI, help is provided at the command line when typing '?'. If no
help is available, the help content will be empty. Backup until entering a '?'
shows the help content.
There are two styles of help provided:
1. Full help. Available when entering a command argument (e.g. 'show ?'). This will
```

```
   describe each possible argument.

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

rfs6000-6DB5D4>
```

## 1.3 Using the No Command

*INTRODUCTION*

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

### 1.3.1 Basic Conventions

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

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

## 1.4 Using CLI Editing Features and Shortcuts

*INTRODUCTION*

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

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

## 1.4.1 Moving the Cursor on the Command Line

*Using CLI Editing Features and Shortcuts*

The following table shows the key combinations or sequences to move the command line cursor. Ctrl defines the control key, which must be pressed simultaneously with its associated letter key. Esc means the escape key (which must be pressed first), followed by its associated letter key. Keys are not case sensitive. Specific letters are used to provide an easy way of remembering their functions.

**Table 1.2** *Keystrokes Details*

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

## 1.4.2 Completing a Partial Command Name

*Using CLI Editing Features and Shortcuts*

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

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

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

```
rfs6000-6DB5D4#conf[TAB]
rfs6000-6DB5D4#configure
```

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

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

In the following example, all commands, available in the current context, starting with the characters ‘co’ are listed:

```
rfs6000-6DB5D4#co?
  commit     Commit all changes made in this session
  configure  Enter configuration mode
  connect    Open a console connection to a remote device
  copy       Copy from one file to another

rfs6000-6DB5D4#
```

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

### 1.4.3 Command Output Pagination

*Using CLI Editing Features and Shortcuts*

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

```
--More--
```

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

## 1.5 Using CLI to Create Profiles and Enable Remote Administration

*INTRODUCTION*

The following sections describe the following essential procedures:

- *Creating Profiles*
- *Changing the default profile by creating vlan 150 and mapping to ge3 Physical interface*
- *Enabling Remote Administration*

## 1.5.1 Creating Profiles

*Using CLI to Create Profiles and Enable Remote Administration*

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

- a default profile for each of the following devices:
  - RFS4000, RFS6000
- a default profile for each of the following service platforms:
  - NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000
- a default profile for each of the following access points:
  - AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533

You can modify a default profile. In the following example, an IP address is assigned to the management port on the default RFS6000 profile.

```
rfs6000-6DB5D4(config)#profile rfs6000 default-rfs6000
rfs6000-6DB5D4(config-profile-default-rfs6000)#interface me1
rfs6000-6DB5D4(config-profile-default-rfs6000-if-me1)#ip address 172.16.10.2/24
rfs6000-6DB5D4(config-profile-default-rfs6000-if-me1)#commit
rfs6000-6DB5D4(config-profile-default-rfs6000)#exit
rfs6000-6DB5D4(config)#
```

The following command displays a default AP7562 profile configuration:

```
rfs6000-6DB5D4(config-profile-default-ap7562)#
rfs6000-6DB5D4(config-profile-default-ap7562)#show context
profile ap7562 default-ap7562
 autoinstall configuration
 autoinstall firmware
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 crypto load-management
 crypto remote-vpn-client
 interface radio1
  placement outdoor
 interface radio2
  placement outdoor
 interface ge1
 interface ge2
 interface vlan1
  ip address dhcp
  ip address zeroconf secondary
  ip dhcp client request options all
--More--
rfs6000-6DB5D4(config-profile-default-ap7562)#
```

## 1.5.2 Changing the default profile by creating vlan 150 and mapping to ge3 Physical interface

*Using CLI to Create Profiles and Enable Remote Administration*

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

```
rfs6000-6DB5D4(config-profile-default-rfs6000)#interface vlan 150

rfs6000-6DB5D4(config-profile-default-rfs6000-if-vlan150)#ip address
192.168.150.20/24

rfs6000-6DB5D4(config-profile-default-rfs6000-if-vlan150)#exit

rfs6000-6DB5D4(config-profile-default-rfs6000)#interface ge 3

rfs6000-6DB5D4(config-profile-default-rfs6000-if-ge3)#switchport access vlan 150

rfs6000-6DB5D4(config-profile-default-rfs6000-if-ge3)#commit write
Please Wait .
[OK]
rfs6000-6DB5D4(config-profile-default-rfs6000-if-ge3)#

rfs6000-6DB5D4(config-profile-default-rfs6000-if-ge3)#show interface vlan 150
Interface vlan150 is UP
  Hardware-type: vlan, Mode: Layer 3, Address: 00-15-70-81-74-2D
  Index: 6, Metric: 1, MTU: 1500
  IP-Address: 192.168.150.20/24
    input packets 0, bytes 0, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 2, bytes 140, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
  IPv6 mode is disabled

rfs6000-6DB5D4(config-profile-default-rfs6000-if-ge3)#
```

### 1.5.2.1 Viewing Configured APs

To view previously configured APs, enter the following command:

```
rfs6000-6DB5D4>show wireless ap configured
-------------------------------------------------------------------------------
 IDX     NAME            MAC             PROFILE      RF-DOMAIN    ADOPTED-BY
-------------------------------------------------------------------------------
  1  ap7532-80C2AC  84-24-8D-80-C2-AC  default-ap7532  TechPubs  00-15-70-81-74-2D
  2  ap8132-74B45C  B4-C7-99-74-B4-5C  default-ap81xx  TechPubs  00-15-70-81-74-2D
  3  ap7522-8330A4  84-24-8D-83-30-A4  default-ap7522  default   00-15-70-81-74-2D
  4  ap8132-711728  B4-C7-99-71-17-28  default-ap81xx  TechPubs  00-15-70-81-74-2D
  5 ap8533-9A12DB  74-67-F7-9A-12-DB  default-ap8533  default   un-adopted
  6  ap7562-84A224  84-24-8D-84-A2-24  default-ap7562  TechPubs  00-15-70-81-74-2D
-------------------------------------------------------------------------------
rfs6000-6DB5D4>
```

## 1.5.3 Enabling Remote Administration

*Using CLI to Create Profiles and Enable Remote Administration*

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

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

This section is organized into the following sub sections:

- *Configuring Telnet for Management Access*
- *Configuring SSH for Management Access*

### 1.5.3.1 Configuring Telnet for Management Access

*Enabling Remote Administration*

To enable Telnet for management access, use the serial console to login to the device and perform the following:

1 The session, by default, opens in the USER EXEC mode (one of the two access levels of the EXEC mode). Access the PRIV EXEC mode from the USER EXEC mode.

```
rfs6000-6DB5D4>en
rfs6000-6DB5D4#
```

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

```
rfs6000-6DB5D4>en
rfs6000-6DB5D4#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
rfs6000-6DB5D4(config)#
```

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

```
rfs6000-6DB5D4(config)#management-policy ?
  MANAGEMENT  Name of the management policy to be configured (will be created
              if it does not exist)

rfs6000-6DB5D4(config)#management-policy default
rfs6000-6DB5D4(config-management-policy-default)#
```

4 Enter Telnet and the port number at the command prompt. Note, the port number is optional. If you do not specify the port, the system, by default, assigns port 23 for Telnet. Commit your changes. Telnet is enabled.

```
rfs6000-6DB5D4(config-management-policy-default)#telnet
rfs6000-6DB5D4(config-management-policy-default)#commit write
rfs6000-6DB5D4(config-management-policy-default)#end
rfs6000-6DB5D4#exit
```

5 Connect to the controller through Telnet using its configured IP address. If logging in for the first time, use the following credentials:

| | |
|---|---|
| **User Name** | admin |
| **Password** | admin123 |

At the first-time login instance, you will be prompted to change the password. Set a new password.

6 On subsequent logins, to change the password, access the default management-policy configuration mode and enter the username, new password, role, and access details.

```
rfs6000-6DB5D4(config-management-policy-default)#user testuser password test@123
 role helpdesk access all
rfs6000-6DB5D4(config-management-policy-default)#commit
rfs6000-6DB5D4(config-management-policy-default)#show context
management-policy default
 telnet
 http server
 https server
 no ftp
 ssh
 user admin password 1
fd07f19c6caf46e5b7963a802d422a708ad39a24906e04667c8642299c8462f1 role superuser
access all
 user testuser password 1
32472f01757293a181738674bdf068ffe0b777ce145524fc669278820ab582c0 role helpdesk
access all
 snmp-server community 2 uktRccdr9eLoByF5PCSuFAAAAAeB78WhgTbSKDi96msyUiW+ rw
 snmp-server community 2 Ne+R15zlwEdhybKxfbd6JwAAAAZzvrLGzU/xWXgwFtwF5JdD ro
 snmp-server user snmptrap v3 encrypted des auth md5 2 WUTBNiUi7tL4ZbU2I7Eh/
QAAAAiDhBZTln0UIu+y/W6E/0tR
 snmp-server user snmpmanager v3 encrypted des auth md5 2 9Fva4fYV1WL4ZbU2I7Eh/
QAAAAjdvbWANBNw+We/xHkH9kLi
 no https use-secure-ciphers-only
rfs6000-6DB5D4(config-management-policy-default)#
```

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

```
rfs6000 release 5.9.1.0-015D
rfs6000-6DB5D4 login: testuser
Password:
Welcome to CLI
Starting CLI...
rfs6000-6DB5D4>
```

### 1.5.3.2 Configuring SSH for Management Access

*Enabling Remote Administration*

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

To enable SSH access on a device, login through the serial console and perform the following:

1 The session, by default, opens in the USER EXEC mode (one of the two access levels of the EXEC mode). Access the PRIV EXEC mode from the USER EXEC mode.

```
rfs6000-6DB5D4>en
rfs6000-6DB5D4#
```

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

```
rfs6000-6DB5D4>en
rfs6000-6DB5D4#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
rfs6000-6DB5D4(config)#
```

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

```
rfs6000-6DB5D4(config)#management-policy ?
  MANAGEMENT  Name of the management policy to be configured (will be created
              if it does not exist)

rfs6000-6DB5D4(config)#management-policy default
rfs6000-6DB5D4(config-management-policy-default)#
```

4 Enter SSH at the command prompt.

```
rfs6000-6DB5D4(config-management-policy-default)#ssh
rfs6000-6DB5D4(config-management-policy-default)#commit write
rfs6000-6DB5D4(config-management-policy-default)#end
rfs6000-6DB5D4#exit
```

5 Connect to the controller through SSH using its configured IP address. If logging in for the first time, use the following credentials:

| | |
|---|---|
| **User Name** | admin |
| **Password** | admin123 |

At the first-time login instance, you will be prompted to change the password. Set a new password.

6 On subsequent logins, to change the password, access the default management-policy configuration mode and enter the username, new password, role, and access details.

```
rfs6000-6DB5D4(config-management-policy-default)#user testuser password test@123
 role helpdesk access all
rfs6000-6DB5D4(config-management-policy-default)#commit
rfs6000-6DB5D4(config-management-policy-default)#show context
management-policy default
 telnet
 http server
 https server
 no ftp
 ssh
 user admin password 1
fd07f19c6caf46e5b7963a802d422a708ad39a24906e04667c8642299c8462f1 role superuser
access all
 user testuser password 1
32472f01757293a181738674bdf068ffe0b777ce145524fc669278820ab582c0 role helpdesk
access all
 snmp-server community 2 uktRccdr9eLoByF5PCSuFAAAAAeB78WhgTbSKDi96msyUiW+ rw
 snmp-server community 2 Ne+R15zlwEdhybKxfbd6JwAAAAZzvrLGzU/xWXgwFtwF5JdD ro
 snmp-server user snmptrap v3 encrypted des auth md5 2 WUTBNiUi7tL4ZbU2I7Eh/
QAAAAiDhBZTln0UIu+y/W6E/0tR
 snmp-server user snmpmanager v3 encrypted des auth md5 2 9Fva4fYV1WL4ZbU2I7Eh/
QAAAAjdvbWANBNw+We/xHkH9kLi
 no https use-secure-ciphers-only
rfs6000-6DB5D4(config-management-policy-default)#
```

7 Logon to the SSH console and provide the user details configured in the previous step to access the controller.

```
rfs6000 release 5.9.1.0-015D
rfs6000-6DB5D4 login: testuser
Password:
Welcome to CLI
Starting CLI...
rfs6000-6DB5D4>
```

# 2 USER EXEC MODE COMMANDS

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

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

```
<DEVICE>>?
Command commands:
  captive-portal-page-upload  Captive portal internal and advanced page upload
  change-passwd               Change password
  clear                       Clear
  clock                       Configure software system clock
  cluster                     Cluster commands
  commit                      Commit all changes made in this session
  connect                     Open a console connection to a remote device
  create-cluster              Create a cluster
  crypto                      Encryption related commands
  crypto-cmp-cert-update      Update the cmp certs
  database                    Database
  database-backup             Backup database
  database-restore            Restore database
  debug                       Debugging functions
  device-upgrade              Device firmware upgrade
  disable                     Turn off privileged mode command
  enable                      Turn on privileged mode command
  file-sync                   File sync between controller and adoptees
  help                        Description of the interactive help system
  join-cluster                Join the cluster
  l2tpv3                      L2tpv3 protocol
  logging                     Modify message logging facilities
  mint                        MiNT protocol
  no                          Negate a command or set its defaults
  on                          On RF-Domain
  opendns                     OpenDNS configuration
  page                        Toggle paging
  ping                        Send ICMP echo messages
  ping6                       Send ICMPv6 echo messages
  revert                      Revert changes
  service                     Service Commands
  show                        Show running system information
  ssh                         Open an ssh connection
  telnet                      Open a telnet connection
  terminal                    Set terminal line parameters
  time-it                     Check how long a particular command took between
                              request and completion of response
  traceroute                  Trace route to destination
  traceroute6                 Trace route to destination(IPv6)
  virtual-machine             Virtual Machine
  watch                       Repeat the specific CLI command at a periodic
                              interval
  write                       Write running configuration to memory or
                              terminal

  clrscr                      Clears the display screen
  exit                        Exit from the CLI

<DEVICE>>
```

# 2.1 User Exec Commands

- *USER EXEC MODE COMMANDS*

The following table summarizes the User Exec Mode commands:

**Table 2.1** *User Exec Mode Commands*

| Command | Description | Reference |
|---|---|---|
| *captive-portal-page-upload* | Uploads captive portal advanced pages to adopted access points | *page 2-4* |
| *change-passwd* | Changes the password of a logged user | *page 2-8* |
| *clear* | Resets the last saved command | *page 2-9* |
| *clock* | Configures the system clock | *page 2-20* |
| *cluster* | Accesses the cluster context | *page 2-21* |
| *connect* | Establishes a console connection to a remote device | *page 2-22* |
| *create-cluster* | Creates a new cluster on a specified device | *page 2-23* |
| *crypto* | Enables encryption and configures encryption related parameters | *page 2-24* |
| *crypto-cmp-cert-update* | Triggers a CMP certificate update on a specified device or devices | *page 2-33* |
| *database* | Enables automatic repairing (vacuuming) and dropping of databases (Captive-portal and NSight) | *page 2-34* |
| *database-backup* | Backs up captive-portal and/or NSight database to a specified location and file on an FTP or SFTP server | *page 2-38* |
| *database-restore* | Restores a previously exported database [captive-portal and/or NSight]. Previously exported databases (backed up to a specified FTP or SFTP server) are restored to the original database. | *page 2-40* |
| *device-upgrade* | Configures device firmware upgrade settings | *page 2-41* |
| *disable* | Turns off (disables) the privileged mode command set | *page 2-49* |
| *enable* | Turns on (enables) the privileged mode command set | *page 2-50* |
| *file-sync* | Configures parameters enabling syncing of PKCS#12 and wireless-bridge certificate between the staging-controller and adopted access points | *page 2-51* |
| *join-cluster* | Adds a device (access point, wireless controller, or service platform) to an existing cluster of devices | *page 2-54* |
| *l2tpv3* | Establishes or brings down *Layer 2 Tunneling Protocol Version 3* (L2TPV3) tunnels | *page 2-56* |
| *logging* | Modifies message logging facilities | *page 2-58* |
| *mint* | Configures MiNT protocol | *page 2-60* |
| *no* | Negates a command or sets its default | *page 2-62* |
| *on* | Executes the following commands in the RF Domain context: clrscr, do, end, exit, help, service, and show | *page 2-64* |

**Table 2.1** *User Exec Mode Commands*

| Command | Description | Reference |
|---|---|---|
| *opendns* | Connects to the OpenDNS site using OpenDNS registered credentials (username, password) OR OpenDNS API token to fetch the OpenDNS device_id. This command is a part of the process that integrates access points, controllers, and service platforms with OpenDNS. | *page 2-65* |
| *page* | Toggles a device's (access point, wireless controller, or service platform) paging function | *page 2-67* |
| *ping* | Sends ICMP echo messages to a user-specified location | *page 2-68* |
| *ping6* | Sends ICMPv6 echo messages to a user-specified IPv6 address | *page 2-70* |
| *ssh* | Opens an SSH connection between two network devices | *page 2-71* |
| *telnet* | Opens a Telnet session | *page 2-72* |
| *terminal* | Sets the length and width of the terminal window | *page 2-73* |
| *time-it* | Verifies the time taken by a particular command between request and response | *page 2-74* |
| *traceroute* | Traces the route to its defined destination | *page 2-75* |
| *traceroute6* | Traces the route to a specified IPv6 destination | *page 2-76* |
| *virtual-machine* | Installs, configures, and monitors the status of virtual machines (VMs) installed on a WiNG controller | *page 2-77* |
| *watch* | Repeats a specific CLI command at a periodic interval | *page 2-83* |

**NOTE:** For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see *COMMON COMMANDS*.

**NOTE:** The input parameter <HOSTNAME>, if used in syntaxes across this chapter, cannot include an underscore (_) character.

## 2.1.1 captive-portal-page-upload

*User Exec Commands*

Uploads captive portal advanced pages to adopted access points. Use this command to provide access points with specific captive portal configurations, so that they can successfully provision login, welcome, and condition pages to clients attempting to access the wireless network using the captive portal.

**NOTE:** Ensure that the captive portal pages uploaded are *.tar files.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

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

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

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

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

captive-portal-page-upload delete-file <CAPTIVE-PORTAL-NAME> <FILE-NAME>

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

**Parameters**

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

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

| | |
|---|---|
| upload-time <TIME> | Optional. Schedules an AP upload time<br>• <TIME> – Specify upload time in the MM/DD/YYYY-HH:MM or HH:MM format.<br>The scheduled upload time is your local system's time. It is not the access point, controller, service platform, or virtual controller time and it is not synched with the device.<br>To view a list of uploaded captive portal files, execute the *show > captive-portal-page-upload > list-files* <CAPTIVE-PORTAL-NAME> command. |

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

| | |
|---|---|
| captive-portal-page-upload <CAPTIVE-PORTAL-NAME> | Uploads advanced pages of the captive portal identified by the <CAPTIVE-PORTAL-NAME> parameter<br>• <CAPTIVE-PORTAL-NAME> – Specify captive portal name (should be existing and configured). |
| rf-domain [<DOMAIN-NAME>\|all] | Uploads to all APs within a specified RF Domain or all RF Domains<br>• <DOMAIN-NAME> – Uploads to APs within a specified RF Domain. Specify the RF Domain name.<br>• all – Uploads to APs across all RF Domains |
| from-controller | Optional. Uploads captive-portal pages to APs via the controller to which the APs are adopted |
| upload-time <TIME> | Optional. Schedules an AP upload time<br>• <TIME> – Specify upload time in the MM/DD/YYYY-HH:MM or HH:MM format.<br>The scheduled upload time is your local system's time. It is not the access point, controller, service platform, or virtual controller time and it is not synched with the device. |

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

| | |
|---|---|
| captive-portal-page-upload cancel-upload | Cancels a scheduled AP upload |
| cancel-upload [<MAC/HOSTNAME>\|all\|on rf-domain [<DOMAIN-NAME>\|all]] | Select one of the following options:<br>• <MAC/HOSTNAME> – Cancels scheduled upload to a specified AP. Specify the AP's MAC address or hostname.<br>• all – Cancels all scheduled AP uploads<br>• on rf- domain – Cancels all scheduled uploads to APs within a specified RF Domain or all RF Domains<br>• <DOMAIN-NAME> – Cancels scheduled uploads to APs within a specified RF Domain. Specify RF Domain name.<br>• all – Cancels scheduled uploads across all RF Domains |

• `captive-portal-page-upload delete-file <CAPTIVE-PORTAL-NAME> <FILE-NAME>`

| | |
|---|---|
| captive-portal-page-upload delete-file | Deletes a specified captive portal's uploaded captive-portal Web page files |
| <CAPTIVE-PORTAL-NAME> <FILE-NAME> | Identifies the captive-portal and Web pages to delete<br>• <CAPTIVE-PORTAL-NAME> – Specify the captive portal name.<br>• <FILE-NAME> – Specify the file name. The specified internal captive portal page is deleted. |

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

| | |
|---|---|
| captive-portal-page-upload load-file | Loads captive-portal advanced pages |
| <CAPTIVE-PORTAL-NAME> <URL> | Specify the captive portal name and location. The captive portal should be existing and configured.<br>• <URL> – Specifies location of the captive-portal Web pages. Use one of the following formats to specify the location:<br>IPv4 URLs:<br>tftp://<hostname\|IP>[:port]/path/file<br>ftp://<user>:<passwd>@<hostname\|IP>[:port]/path/file<br>sftp://<user>:<passwd>@<hostname\|IP>[:port]>/path/file<br>http://<hostname\|IP>[:port]/path/file<br>cf:/path/file<br>usb<n>:/path/file<br>IPv6 URLs:<br>tftp://<hostname\|[IPv6]>[:port]/path/file<br>ftp://<user>:<passwd>@<hostname\|[IPv6]>[:port]/path/file<br>sftp://<user>:<passwd>@<hostname\|[IPv6]>[:port]>/path/file<br>http://<hostname\|[IPv6]>[:port]/path/file<br>**Note:** The captive portal pages are downloaded to the controller from the location specified here. After downloading use the *captive-portal-page-upload > <CAPTIVE-PORTAL-NAME> > <DEVICE-OR-DOMAIN-NAME>* command to upload these pages to APs. |

**Example**

```
ap6562-B1A214>captive-portal-page-upload load-file captive_portal_test tftp://
89.89.89.17/pages_new_only.tar
ap6562-B1A214>

ap6562-B1A214>show captive-portal-page-upload load-image-status
Download of captive_portal_test advanced page file is complete
ap6562-B1A214>

ap6562-B1A214>captive-portal-page-upload captive_portal_test all
--------------------------------------------------------------------------------
         CONTROLLER             STATUS                  MESSAGE
--------------------------------------------------------------------------------
  FC-0A-81-B1-A2-14         Success         Added 6 APs to upload queue
--------------------------------------------------------------------------------
ap6562-B1A214>
```

```
ap6562-B1A214>show captive-portal-page-upload status
Number of APs currently being uploaded : 1
Number of APs waiting in queue to be uploaded : 0
-------------------------------------------------------------------------------
-------
        AP           STATE     UPLOAD TIME PROGRESS RETRIES LAST UPLOAD ERROR
UPLOADED BY
-------------------------------------------------------------------------------
-------
  ap6562-B1A738   downloading   immediate   100      0       -                None
-------------------------------------------------------------------------------
-------
ap6562-B1A214>
```

## 2.1.2 change-passwd

*User Exec Commands*

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

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

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

**Parameters**

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

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

**Usage Guidelines**

A password must be from 1 - 64 characters in length.

**Example**

```
rfs6000-81742D>change-passwd
Enter old password:
Enter new password:
Password for user 'admin' changed successfully
Please write this password change to memory(write memory) to be persistent.
rfs6000-81742D#write memory
OK
rfs6000-81742D>
```

## 2.1.3 clear

*User Exec Commands*

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

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**NOTE:** When using the *clear* command, refer to the interface details provided in *interface*.

**Syntax**

```
clear [arp-cache|bonjour|cdp|counters|crypto|eguest|event-history|gre|ip|
ipv6|lacp|lldp|mac-address-table|mint|role|rtls|spanning-tree|traffic-shape|
vrrp]

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

clear bonjour cache {on <DEVICE-NAME>}

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

clear counters [ap|radio|wireless-client]

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

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

clear eguest registration statistics

clear event-history

clear gre stats {on <DEVICE-NAME>}

clear ip [bgp|dhcp|ospf]

clear ip bgp [<IP>|all|external|process]
clear ip bgp [<IP>|all|external] {in|on|out|soft}
clear ip bgp [<IP>|all|external] {in prefix-filter} {on <DEVICE-NAME>}
clear ip bgp [<IP>|all|external] {out} {(on <DEVICE-NAME>)}
clear ip bgp [<IP>|all|external] {soft {in|out}} {on <DEVICE-NAME>}
clear ip bgp process {on <DEVICE-NAME>}

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

clear ipv6 neighbor-cache {on <DEVICE-NAME>}

clear lacp [<1-4> counters|counters]
```

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

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

clear mac-address-table {interface [<IN-NAME>|ge <1-2>|port-channel <1-2>|vmif <1-8>]} {on <DEVICE-NAME>}

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

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

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

clear rtls [aeroscout|ekahau]

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

clear spanning-tree detected-protocols {interface|on}

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

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

clear traffic-shape statistics class <1-4> {(on <DEVICE-NAME>)}

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

**Parameters**

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

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

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

| | |
|---|---|
| bonjour cache | Clears all Bonjour cached statistics. Once cleared the system has to re-discover available Bonjour services. |
| on <DEVICE-NAME> | Optional. Clears all Bonjour cached statistics on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

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

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

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

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

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

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

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

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

- `clear eguest registration statistics`

| | |
|---|---|
| eguest registration statistics | Clears EGuest registration server counters. When cleared EGuest registration details are deleted, and the *show > eguest > registration > statistics* command output is null.<br>This command is applicable only on the NX9500, NX9600, and VX9000 model service platforms. |

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

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

- `clear event-history`

| | |
|---|---|
| event-history | Clears event history cache entries |

- `clear ip bgp [<IP>|all|external] {in prefix-filter} {on <DEVICE-NAME>}`

| | |
|---|---|
| ip bgp [<IP>\|all\|external] | Clears on-going BGP sessions based on the option selected<br>• <IP> – Clears BGP session with the peer identified by the <IP> keyword. Specify the BGP peer's IP address.<br>• all – Clears all BGP peer sessions<br>• external – Clears *external BGP* (eBGP) peer sessions<br>This command is applicable only to the RFS4000, RFS6000, NX9500, NX9600, and VX9000 platforms.<br>Modifications made to BGP settings (BGP access lists, weight, distance, route-maps, versions, routing policy, etc.) take effect only after on-going BGP sessions are cleared. The *clear > ip > bgp* command clears BGP sessions. To reduce lose of route updates during the process, use the 'soft' option. Soft reconfiguration stores inbound/outbound route updates to be processed later and updated to the routing table. This requires high memory usage. |
| in prefix-filter | Optional. Clears inbound route updates<br>• prefix-filter – Optional. Clears the existing *Outbound Route Filtering* (ORF) prefix-list |
| on <DEVICE-NAME> | Optional. Clears route updates on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP or service platform. |

- `clear ip bgp [<IP>|all|external] {out} {(on <DEVICE-NAME>)}`

| | |
|---|---|
| ip bgp [<IP>\|all\|external] | Clears on-going BGP sessions based on the option selected<br>• <IP> – Clears BGP session with the peer identified by the <IP> keyword. Specify the BGP peer's IP address.<br>• all – Clears all BGP peer sessions<br>• external – Clears eBGP peer sessions<br>This command is applicable only to the RFS4000, RFS6000, NX9500, NX9600, and VX9000 platforms.<br>Contd.. |

| | |
|---|---|
| | Modifications made to BGP settings (BGP access lists, weight, distance, route-maps, versions, routing policy, etc.) take effect only after on-going BGP sessions are cleared. The *clear > ip > bgp* command clears BGP sessions. To reduce lose of route updates during the process, use the 'soft' option. Soft reconfiguration stores inbound/outbound route updates to be processed later and updated to the routing table. This requires high memory usage. |
| out | Optional. Clears outbound route updates. Optionally specify the device on which to execute this command. |
| on <DEVICE-NAME> | The following keyword is recursive and optional.<br>• on <DEVICE-NAME> – Optional. Clears BGP sessions on a specified device<br>  • <DEVICE-NAME> – Specify the name of the AP or service platform. |

- `clear ip bgp [<IP>|all|external] {soft {in|out}} {on <DEVICE-NAME>}`

| | |
|---|---|
| ip bgp [<IP>\|all\|external] | Clears on-going BGP sessions based on the option selected<br>• <IP> – Clears the BGP peer session with the peer identified by the <IP> keyword. Specify the BGP peer's IP address.<br>• all – Clears all BGP peer sessions<br>• external – Clears eBGP peer sessions<br>This command is applicable only to the RFS4000, RFS6000, NX9500, NX9600, and VX9000 platforms. |
| soft {in\|out} | Optional. Initiates soft-reconfiguration of route updates for the specified IP address<br>• in – Optional. Enables soft reconfiguration of inbound route updates<br>• out – Optional. Enables soft reconfiguration of outbound route updates<br>Modifications made to BGP settings (BGP access lists, weight, distance, route-maps, versions, routing policy, etc.) take effect only after on-going BGP sessions are cleared. The *clear > ip > bgp* command clears BGP sessions. To reduce loss of route updates during the process, use the 'soft' option. Soft reconfiguration stores inbound/outbound route updates to be processed later and updated to the routing table. This requires high memory usage. |
| on <DEVICE-NAME> | Optional. Initiates soft reconfiguration inbound/outbound route updates on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP or service platform. |

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

| | |
|---|---|
| ip bgp process | Clears all BGP processes running<br>This command is applicable only to the RFS4000, RFS6000, NX9500, NX9600, and VX9000 platforms. |
| on <DEVICE-NAME> | Optional. Clears all BGP processes on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP or service platform. |

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

| | |
|---|---|
| ip | Clears a *Dynamic Host Configuration Protocol* (DHCP) server's IP address binding entries |
| dhcp bindings | Clears DHCP connections and server bindings |
| <IP> | Clears specific address binding entries. Specify the IP address to clear binding entries. |

| | |
|---|---|
| all | Clears all address binding entries |
| on <DEVICE-NAME> | Optional. Clears a specified address binding or all address bindings on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

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

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

- `clear ipv6 neighbor-cache` *{on <DEVICE-NAME>}*

| | |
|---|---|
| clear ipv6 neighbor-cache | Clears IPv6 neighbor cache entries |
| on <DEVICE-NAME> | Optional. Clears IPv6 neighbor cache entries on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `clear lacp [<1-4> counters|counters]`

| | |
|---|---|
| clear lacp [<1-4> counters\| counters] | Clears *Link Aggregation Control Protocol* (LACP) counters for a specified port-channel group or all port-channel groups configured<br>• <1-4> counters – Clears LACP counters for a specified port-channel. Specify the port-channel index number from 1 - 4. Note, LACP is supported only on the NX5500, NX7500, and NX9500 model service platforms. However, the NX9500 series service platforms support only two (2) port-channels, and the other model service platforms support four (4) port-channels.<br>• counters – Clears LACP counters for all configured port-channels on the device |

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

| | |
|---|---|
| mac-address-table | Clears MAC address forwarding table data based on the parameters passed<br>Use this command to clear the following: all or specified MAC addresses from the system, all MAC addresses on a specified interface, all MAC addresses on a specified VLAN, or the authentication state of a MAC address. |
| address <MAC> | Optional. Clears a specified MAC address from the MAC address table.<br>• <MAC> – Specify the MAC address in one of the following formats: AA-BB-CC-DD-EE-FF or AA:BB:CC;DD:EE:FF or AABB.CCDD.EEFF<br>If executed without specifying any MAC address(es), all MAC addresses from the MAC address table will be removed. |

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

• `clear mac-address-table {interface [<IF-NAME>|ge <1-X>|port-channel <1-X>]} {on <DEVICE-NAME>}`

| | |
|---|---|
| mac-address-table | Clears MAC address forwarding table data based on the parameters passed<br>Use this command to clear the following: all or specified MAC addresses from the system, all MAC addresses on a specified interface, all MAC addresses on a specified VLAN, or the authentication state of a MAC address. |
| interface | Clears all MAC addresses for the selected interface. Use the options available to specify the interface. |
| <IF-NAME> | Clears MAC address forwarding table for the specified layer 2 interface (Ethernet port)<br>• <IF-NAME> – Specify the layer 2 interface name. |
| ge <1-X> | Clears MAC address forwarding table for the specified GigabitEthernet interface<br>• <1-X> – Specify the GigabitEthernet interface index from 1 - X.<br>The number of GE interfaces supported varies for different device types. |
| port-channel <1-X> | Clears MAC address forwarding table for the specified port-channel interface<br>• <1-X> – Specify the port-channel interface index from 1 - X.<br>The number of port-channel interfaces supported varies for different device types. |
| on <DEVICE-NAME> | Optional. Clears the MAC address forwarding table, for the selected interface, on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

• `clear mac-address-table mac-auth-state address <MAC> vlan <1-4904> {on <DEVICE-NAME>}`

| | |
|---|---|
| mac-address-table mac-auth-state address <MAC> vlan <1-4904> | Clears MAC addresses learned from a particular VLAN when WLAN MAC authentication and captive-portal fall back is enabled<br>Access points/controllers provide WLAN access to clients whose MAC address has been learned and stored in their MAC address tables. Use this command to clear a specified MAC address on the MAC address table. Once cleared the client has to re-authenticate, and is provided access only on successful authentication.<br>• <MAC> – Specify the MAC address to clear.<br>• vlan <1-4904> – Specify the VLAN interface from 1 - 4094. In the AP/controller's MAC address table, the specified MAC address is cleared on the specified VLAN interface. |
| on <DEVICE-NAME> | Optional. Clears the specified MAC address on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.<br>If a device is not specified, the system clears the MAC address on all devices. |

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

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

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

| | |
|---|---|
| role ldap-stats | Clears *Lightweight Directory Access Protocol* (LDAP) server statistics |
| on <DEVICE-NAME> | Optional. Clears LDAP server statistics on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

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

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

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

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

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

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

| | |
|---|---|
| interface [<INTERFACE-NAME>\| ge <1-X>\|me1\| port-channel <1-X>\| pppoe1\|up1\| vlan <1-4094>\| wwan1] | Optional. Clears spanning tree entries on different interfaces<br>• <INTERFACE-NAME> – Clears detected spanning tree entries on a specified interface. Specify the interface name.<br>• ge <1-X> – Clears detected spanning tree entries for the selected GigabitEthernet interface. Select the GigabitEthernet interface index from 1 - X.<br>• me1 – Clears FastEthernet interface spanning tree entries<br>• port-channel <1-X> – Clears detected spanning tree entries for the selected port channel interface. Select the port channel index from 1 - X.<br>The number of port-channel interfaces supported varies for different device types.<br>• pppoe1 – Clears detected spanning tree entries for *Point-to-Point Protocol over Ethernet* (PPPoE) interface<br>• up1 – Clears detected spanning tree entries for the WAN Ethernet interface<br>• vlan <1-4094> – Clears detected spanning tree entries for the selected VLAN interface. Select a *Switch Virtual Interface* (SVI) VLAN ID from 1- 4094.<br>• wwan1 – Clears detected spanning tree entries for wireless WAN interface. |
| on <DEVICE-NAME> | Optional. Clears spanning tree entries on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `clear traffic-shape statistics class <1-4> {(on <DEVICE-NAME>)}`

| | |
|---|---|
| traffic-shape statistics | Clears traffic shaping statistics |
| class <1-4> | Clears traffic shaping statistics for a specific traffic class<br>• <1-4> – Specify the traffic class from 1 - 4.<br>**Note:** If the traffic class is not specified, the system clears all traffic shaping statistics. |
| on <DEVICE-NAME> | Optional. Clears traffic shaping statistics for the specified traffic class on a specified device<br>• <DEVICE-NAME> – Specify the name of the access point, wireless controller, or service platform.<br>**Note:** For more information on configuring traffic-shape, see *traffic-shape*. |

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

| | |
|---|---|
| vrrp | Clears a device's *Virtual Router Redundancy Protocol* (VRRP) statistics<br>VRRP allows a pool of routers to be advertized as a single virtual router. This virtual router is configured by hosts as their default gateway. VRRP elects a master router, from this pool, and assigns it a virtual IP address. The master router routes and forwards packets to hosts on the same subnet. When the master router fails, one of the backup routers is elected as the master and its IP address is mapped to the virtual IP address. |
| error-stats | Clears global error statistics |
| stats | Clears VRRP related statistics |
| on <DEVICE-NAME> | The following keywords are common to the 'error-stats' and 'stats' parameters:<br>• on <DEVICE-NAME> – Optional. Clears VRRP statistics on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

**Example**

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

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

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

rfs4000-229D58>show lldp neighbors
--------------------------
Chassis ID: 00-23-68-88-0D-A7
System Name: rfs4000-880DA7
Platform: RFS-4011-11110-US, Version 5.8.6.0-008B

Capabilities: Bridge WLAN Access Point Router
Enabled Capabilities: Bridge WLAN Access Point Router
Local Interface: ge5, Port ID (outgoing port): ge5
TTL: 176 sec
Management Addresses: 192.168.13.8,192.168.0.1,1.2.3.4
rfs4000-229D58>

rfs4000-229D58>clear lldp neighbors

rfs4000-229D58>show lldp neighbors

rfs4000-229D58>show cdp neighbors
-------------------------------------------------------------------------------
     Device ID           Platform        Local Intrfce    Port ID      Duplex
-------------------------------------------------------------------------------
 rfs4000-880DA7    RFS-4011-11110-US    ge1              ge1          full
 rfs6000-434CAA    RFS6000              ge1              ge1          full
 ap7131-139B34     AP7131N              ge1              ge1          full
-------------------------------------------------------------------------------
rfs4000-229D58>

rfs4000-229D58>clear cdp neighbors

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

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

rfs4000-229D58>

rfs4000-229D58>clear role ldap-stats

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

rfs4000-229D58>show mac-address-table
-----------------------------------------------------------
 BRIDGE VLAN PORT             MAC               STATE
-----------------------------------------------------------
 1      1    ge5              00-02-B3-28-D1-55 forward
 1      1    ge5              00-0F-8F-19-BA-4C forward
 1      1    ge5              B4-C7-99-5C-FA-8E forward
 1      1    ge5              00-23-68-0F-43-D8 forward
 1      1    ge5              00-15-70-38-06-49 forward
 1      1    ge5              00-23-68-13-9B-34 forward
 1      1    ge5              B4-C7-99-58-72-58 forward
 1      1    ge5              00-15-70-81-74-2D forward
-----------------------------------------------------------
Total number of MACs displayed: 8
rfs4000-229D58>
```

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

rfs4000-229D58>show mac-address-table
------------------------------------------------------------
 BRIDGE VLAN PORT             MAC                STATE
------------------------------------------------------------
1      1    ge5              00-0F-8F-19-BA-4C forward
1      1    ge5              B4-C7-99-5C-FA-8E forward
1      1    ge5              00-23-68-0F-43-D8 forward
1      1    ge5              00-15-70-38-06-49 forward
1      1    ge5              00-23-68-13-9B-34 forward
1      1    ge5              B4-C7-99-58-72-58 forward
1      1    ge5              00-15-70-81-74-2D forward
------------------------------------------------------------
Total number of MACs displayed: 7
rfs4000-229D58>
```

## 2.1.4 clock

*User Exec Commands*

Sets a device's system clock. By default all WiNG devices are shipped with the time zone and time format set to UTC and 24-hour clock respectively. If a device's clock is set without resetting the time zone, the time is displayed relative to the *Universal Time Coordinated* (UTC) – Greenwich Time. To display time in the local time zone format, in the device's configuration mode, use the timezone command. You can also reset the time zone at the RF Domain level. When configured as RF Domain setting, it applies to all devices within the domain. Configuring the local time zone prior to setting the clock is recommended. For more information on configuring RF Domain time zone, see *timezone*.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

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

**Parameters**

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

| | |
|---|---|
| clock set | Sets a device's software system clock |
| <HH:MM:SS> | Sets the current time (in military format hours, minutes, and seconds)<br>**Note:** By default, the WiNG software displays time in the 24-hour clock format. This setting cannot be changed. |
| <1-31> | Sets the numerical day of the month |
| <MONTH> | Sets the month of the year (Jan to Dec) |
| <1993-2035> | Sets a valid four digit year from 1993 - 2035 |
| on <DEVICE-NAME> | Optional. Sets the clock on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

**Example**

The following commands set the time zone and clock for the logged device:

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#timezone America/Los_Angeles

nx9500-6C8809>clock set 11:24:30 21 Jan 2017

nx9500-6C8809>show clock
2017-01-21 12:14:14 PDT
nx9500-6C8809>
```

Note, if the clock is set without resetting the time zone, the time displays as UTC time, as shown in the following example:

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#no timezone
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#commit

nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#show clock
2017-01-21 19:15:55 UTC

nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#
```

## 2.1.5 cluster

*User Exec Commands*

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

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

**Supported in the following platforms:**

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
cluster start-election
```

**Parameters**

- `cluster start-election`

| | |
|---|---|
| start-election | Starts a new cluster master election |

**Example**

```
nx9500-6C8809>cluster start-election
nx9500-6C8809>
```

**Related Commands**

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

## 2.1.6 connect

*User Exec Commands*

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

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

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

**Parameters**

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

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

**Example**

```
rfs6000-81742D>show mint lsp-db
9 LSPs in LSP-db of 19.6D.B5.D4:
LSP 19.6C.88.09 at level 1, hostname nx9500-6C8809", 8 adjacencies, seqnum 1294555
LSP 19.6D.B5.D4 at level 1, hostname "rfs6000-81742D", 8 adjacencies, seqnum
1915724
LSP 19.74.B4.5C at level 1, hostname "ap8132-74B45C", 8 adjacencies, seqnum 1468229
LSP 4D.80.C2.AC at level 1, hostname "ap7532-80C2AC", 8 adjacencies, seqnum 649244
LSP 4D.83.30.A4 at level 1, hostname "ap7522-8330A4", 8 adjacencies, seqnum 202821
LSP 4D.84.A2.24 at level 1, hostname "ap7562-84A224", 8 adjacencies, seqnum 380340
LSP 68.88.0D.A7 at level 1, hostname "rfs4000-880DA7", 8 adjacencies, seqnum
1494523
LSP 68.99.BB.7C at level 1, hostname "ap7131-99BB7C", 8 adjacencies, seqnum 831532
rfs6000-81742D>

rfs6000-81742D>connect mint-id 19.6C.88.09

Entering character mode
Escape character is '^]'.

NX9500 release 5.9.1.0-012D
nx9500-6C8809 login:
```

## 2.1.7 create-cluster

*User Exec Commands*

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

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

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

**Supported in the following platforms:**

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

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

**Parameters**

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

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

**Example**

```
rfs6000-81742D>create-cluster name TechPubs ip 192.168.13.23 level 1
... creating cluster
... committing the changes
... saving the changes
Please Wait .
[OK]
rfs6000-81742D>

rfs6000-81742D>show context session-config include-factory | include cluster name
TechPubs
 cluster name TechPubs
rfs6000-81742D>
```

**Related Commands**

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

## 2.1.8 crypto

*User Exec Commands*

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

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

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
crypto [key|pki]

crypto key [export|generate|import|zeroize]

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

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

crypto key generate rsa <RSA-KEYPAIR-NAME> [2048|4096] {on <DEVICE-NAME>}

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

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

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

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

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

crypto pki export [request|trustpoint]

crypto pki export request [generate-rsa-key|short|use-rsa-key] <RSA-KEYPAIR-NAME>
[autogen-subject-name|subject-name]

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

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

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

```
crypto pki generate self-signed <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key]
<RSA-KEYPAIR-NAME> [autogen-subject-name|subject-name]

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

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

crypto pki import [certificate|crl|trustpoint]

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

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

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

**Parameters**

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

| | |
|---|---|
| key | Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key. |
| export rsa <RSA-KEYPAIR-NAME> | Exports an existing RSA Keypair to a specified destination<br>• <RSA-KEYPAIR-NAME> – Specify the RSA Keypair name. |
| <EXPORT-TO-URL> | Specify the RSA Keypair destination address. Both IPv4 and IPv6 address formats are supported.<br>After specifying the destination address (where the RSA Keypair is exported), configure one of the following parameters: background or passphrase. |
| background | Optional. Performs export operation in the background. If selecting this option, you can optionally specify the device (access point or controller) to perform the export on. |
| passphrase <KEY-PASSPHRASE> background | Optional. Encrypts RSA Keypair before exporting<br>• <KEY-PASSPHRASE> – Specify a passphrase to encrypt the RSA Keypair.<br>• background – Optional. Performs export operation in the background. After specifying the passphrase, optionally specify the device (access point or controller) to perform the export on. |
| on <DEVICE-NAME> | The following parameter is recursive and common to all of the above parameters:<br>• on <DEVICE-NAME> – Optional. Performs export operation on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `crypto key generate rsa <RSA-KEYPAIR-NAME> [2048|4096] {on <DEVICE-NAME>}`

| | |
|---|---|
| key | Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key. |

| | |
|---|---|
| generate rsa <RSA-KEYPAIR-NAME> [2048\|4096] | Generates a new RSA Keypair<br>• <RSA-KEYPAIR-NAME> – Specify the RSA Keypair name.<br>• [2048\|4096] – Sets the size of the RSA key in bits. The options are 2048 bits and 4096 bits. The default size is 2048 bits.<br>After specifying the key size, optionally specify the device (access point or controller) to generate the key on. |
| on <DEVICE-NAME> | Optional. Generates the new RSA Keypair on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

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

| | |
|---|---|
| key | Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key. |
| import rsa <RSA-KEYPAIR-NAME> | Imports a RSA Keypair from a specified source<br>• <RSA-KEYPAIR-NAME> – Specify the RSA Keypair name. |
| <IMPORT-FROM-URL> | Specify the RSA Keypair source address. Both IPv4 and IPv6 address formats are supported.<br>After specifying the source address (where the RSA Keypair is imported from), configure one of the following parameters: background or passphrase. |
| background | Optional. Performs import operation in the background. If selecting this option, you can optionally specify the device (access point or controller) to perform the import on. |
| passphrase <KEY-PASSPHRASE> background | Optional. Decrypts the RSA Keypair after importing<br>• <KEY-PASSPHRASE> – Specify the passphrase to decrypt the RSA Keypair.<br>• background – Optional. Performs import operation in the background. After specifying the passphrase, optionally specify the device (access point, controller, or service platform) to perform the import on. |
| on <DEVICE-NAME> | The following parameter is recursive and common to the 'background' and 'passphrase' keywords:<br>• on <DEVICE-NAME> – Optional. Performs import operation on a specific device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

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

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

| | |
|---|---|
| on <DEVICE-NAME> | The following parameter is recursive and optional:<br>• on <DEVICE-NAME> – Optional. Deletes all certificates associated with the RSA Keypair on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

• `crypto pki authenticate <TRUSTPOINT-NAME> <URL> {background} {(on <DEVICE-NAME>)}`

| | |
|---|---|
| pki | Enables *Private Key Infrastructure* (PKI) management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated *Certificate Authority* (CA) certificates. |
| authenticate <TRUSTPOINT-NAME> | Authenticates a trustpoint and imports the corresponding CA certificate<br>• <TRUSTPOINT-NAME> – Specify the trustpoint name. |
| <URL> | Specify CA's location. Both IPv4 and IPv6 address formats are supported.<br>**Note:** The CA certificate is imported from the specified location. |
| background | Optional. Performs authentication in the background. If selecting this option, you can optionally specify the device (access point, controller, or service platform) to perform the export on. |
| on <DEVICE-NAME> | The following parameter is recursive and optional:<br>• on <DEVICE-NAME> – Optional. Performs authentication on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

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

| | |
|---|---|
| pki | Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates. |
| export request | Exports CSR to the CA for digital identity certificate. The CSR contains applicant's details and RSA Keypair's public key. |
| [generate-rsa-key\| use-rsa-key] <RSA-KEYPAIR-NAME> | Generates a new RSA Keypair or uses an existing RSA Keypair<br>• generate-rsa-key – Generates a new RSA Keypair for digital authentication<br>• use-rsa-key – Uses an existing RSA Keypair for digital authentication<br>• <RSA-KEYPAIR-NAME> – If generating a new RSA Keypair, specify a name for it. If using an existing RSA Keypair, specify its name. |
| autogen-subject-name | Auto generates subject name from configuration parameters. The subject name identifies the certificate. |
| <EXPORT-TO-URL> | Specify the CA's location. Both IPv4 and IPv6 address formats are supported.<br>**Note:** The CSR is exported to the specified location. |
| email <SEND-TO-EMAIL> | Exports CSR to a specified e-mail address<br>• <SEND-TO-EMAIL> – Specify the CA's e-mail address. |
| fqdn <FQDN> | Exports CSR to a specified *Fully Qualified Domain Name* (FQDN)<br>• <FQDN> – Specify the CA's FQDN. |
| ip-address <IP> | Exports CSR to a specified device or system<br>• <IP> – Specify the CA's IP address. |

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

| | |
|---|---|
| pki | Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates. |
| export request | Exports CSR to the CA for a digital identity certificate. The CSR contains applicant's details and RSA Keypair's public key. |
| [generate-rsa-key\| short [generate-rsa-key\|use-rsa-key]\| use-rsa-key] <RSA-KEYPAIR-NAME> | Generates a new RSA Keypair or uses an existing RSA Keypair<br>• generate-rsa-key – Generates a new RSA Keypair for digital authentication<br>• short [generate-rsa-key\|use-rsa-key] – Generates and exports a shorter version of the CSR<br>• generate-rsa-key – Generates a new RSA Keypair for digital authentication. If generating a new RSA Keypair, specify a name for it.<br>• use-rsa-key – Uses an existing RSA Keypair for digital authentication. If using an existing RSA Keypair, specify its name.<br>• use-rsa-key – Uses an existing RSA Keypair for digital authentication<br>• <RSA-KEYPAIR-NAME> – If generating a new RSA Keypair, specify a name for it. If using an existing RSA Keypair, specify its name. |
| subject-name <COMMON-NAME> | Configures a subject name, defined by the <COMMON-NAME> keyword, to identify the certificate<br>• <COMMON-NAME> – Specify the common name used with the CA certificate. The name should enable you to identify the certificate easily (2 to 64 characters in length). |
| <COUNTRY> | Sets the deployment country code (2 character ISO code) |
| <STATE> | Sets the state name (2 to 64 characters in length) |
| <CITY> | Sets the city name (2 to 64 characters in length) |
| <ORGANIZATION> | Sets the organization name (2 to 64 characters in length) |
| <ORGANIZATION-UNIT> | Sets the organization unit (2 to 64 characters in length) |
| <EXPORT-TO-URL> | Specify the CA's location. Both IPv4 and IPv6 address formats are supported.<br>The CSR is exported to the specified location. |
| email <SEND-TO-EMAIL> | Exports CSR to a specified e-mail address<br>• <SEND-TO-EMAIL> – Specify the CA's e-mail address. |
| fqdn <FQDN> | Exports CSR to a specified FQDN<br>• <FQDN> – Specify the CA's FQDN. |
| ip-address <IP> | Exports CSR to a specified device or system<br>• <IP> – Specify the CA's IP address. |

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

| | |
|---|---|
| pki | Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates. |

| | |
|---|---|
| export trustpoint <TRUSTPOINT-NAME> | Exports a trustpoint along with CA certificate, *Certificate Revocation List* (CRL), server certificate, and private key<br>• <TRUSTPOINT-NAME> – Specify the trustpoint name (should be authenticated). |
| <EXPORT-TO-URL> | Specify the destination address. Both IPv4 and IPv6 address formats are supported.<br>The trustpoint is exported to the address specified here. |
| background | Optional. Performs export operation in the background. If selecting this option, you can optionally specify the device (access point or controller) to perform the export on |
| passphrase <KEY-PASSPHRASE> background | Optional. Encrypts the key with a passphrase before exporting<br>• <KEY-PASSPHRASE> – Specify the passphrase to encrypt the trustpoint.<br>• background – Optional. Performs export operation in the background. After specifying the passphrase, optionally specify the device (access point or controller) to perform the export on. |
| on <DEVICE-NAME> | The following parameter is recursive and common to the 'background' and 'passphrase' keywords:<br>• on <DEVICE-NAME> – Optional. Performs export operation on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

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

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

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

| | |
|---|---|
| pki | Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated certificates. |
| generate self-signed <TRUSTPOINT-NAME> | Generates a self-signed certificate and a trustpoint<br>• <TRUSTPOINT-NAME> – Specify a name for the certificate and its trustpoint. |
| [generate-rsa-key\|use-rsa-key] <RSA-KEYPAIR-NAME> | Generates a new RSA Keypair, or uses an existing RSA Keypair<br>• generate-rsa-key – Generates a new RSA Keypair for digital authentication<br>• use-rsa-key – Uses an existing RSA Keypair for digital authentication<br>  • <RSA-KEYPAIR-NAME> – If generating a new RSA Keypair, specify a name for it. If using an existing RSA Keypair, specify its name. |
| subject-name <COMMON-NAME> | Configures a subject name, defined by the <COMMON-NAME> keyword, to identify the certificate<br>• <COMMON-NAME> – Specify the common name used with this certificate. The name should enable you to identify the certificate easily and should not exceed 2 to 64 characters in length. |
| <COUNTRY> | Sets the deployment country code (2 character ISO code) |
| <STATE> | Sets the state name (2 to 64 characters in length) |
| <CITY> | Sets the city name (2 to 64 characters in length) |
| <ORGANIZATION> | Sets the organization name (2 to 64 characters in length) |
| <ORGANIZATION-UNIT> | Sets the organization unit (2 to 64 characters in length) |
| email <SEND-TO-EMAIL> | Optional. Exports the self-signed certificate to a specified e-mail address<br>• <SEND-TO-EMAIL> – Specify the e-mail address. |
| fqdn <FQDN> | Optional. Exports the self-signed certificate to a specified FQDN<br>• <FQDN> – Specify the FQDN. |
| ip-address <IP> | Optional. Exports the self-signed certificate to a specified device or system<br>• <IP> – Specify the device's IP address. |

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

| | |
|---|---|
| pki | Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates. |
| import | Imports certificates, *Certificate Revocation List* (CRL), or a trustpoint to the selected device |
| [certificate\|crl] <TRUSTPOINT-NAME> | Imports a signed server certificate or CRL<br>• certificate – Imports signed server certificate<br>• crl – Imports CRL<br>  • <TRUSTPOINT-NAME> – Specify the trustpoint name (should be authenticated). |
| <IMPORT-FROM-URL> | Specify the signed server certificate or CRL source address. Both IPv4 and IPv6 address formats are supported.<br>The server certificate or the CRL (based on the parameter passed in the preceding step) is imported from the location specified here. |

| | |
|---|---|
| background | Optional. Performs import operation in the background. If selecting this option, you can optionally specify the device (access point or controller) to perform the import on. |
| on <DEVICE-NAME> | The following parameter is recursive and optional:<br>• on <DEVICE-NAME> – Optional. Performs import operation on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

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

| | |
|---|---|
| pki | Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates. |
| import | Imports certificates, CRL, or a trustpoint to the selected device |
| trustpoint <TRUSTPOINT-NAME> | Imports a trustpoint and its associated CA certificate, server certificate, and private key<br>• <TRUSTPOINT-NAME> – Specify the trustpoint name (should be authenticated). |
| <IMPORT-FROM-URL> | Specify the trustpoint source address. Both IPv4 and IPv6 address formats are supported. |
| background | Optional. Performs import operation in the background. If selecting this option, you can optionally specify the device (access point or controller) to perform the import on. |
| passphrase <KEY-PASSPHRASE> background | Optional. Decrypts trustpoint with a passphrase after importing<br>• <KEY-PASSPHRASE> – Specify the passphrase. After specifying the passphrase, optionally specify the device to perform import on.<br>• background – Optional. Performs import operation in the background. After specifying the passphrase, optionally specify the device (access point or controller) to perform the import on. |
| on <DEVICE-NAME> | The following parameter is recursive and optional:<br>• on <DEVICE-NAME> – Optional. Performs import operation on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

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

| | |
|---|---|
| pki | Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates. |
| zeroize trustpoint <TRUSTPOINT-NAME> | Deletes a trustpoint and its associated CA certificate, server certificate, and private key<br>• <TRUSTPOINT-NAME> – Specify the trustpoint name (should be authenticated). |
| del-key | Optional. Deletes the private key associated with the server certificate. Optionally specify the device to perform deletion on. |
| on <DEVICE-NAME> | The following parameter is recursive and optional:<br>• on <DEVICE-NAME> – Optional. Deletes the trustpoint on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

**Usage Guidelines**

The system supports both IPv4 and IPv6 address formats. Provide source and destination locations using any one of the following options:

- IPv4 URLs:
  tftp://<hostname|IP>[:port]/path/file
  ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file
  sftp://<user>@<hostname|IP>[:port]>/path/file
  http://<hostname|IP>[:port]/path/file
  cf:/path/file
  usb<n>:/path/file
- IPv6 URLs:
  tftp://<hostname|[IPv6]>[:port]/path/file
  ftp://<user>:<passwd>@<hostname|[IPv6]>[:port]/path/file
  sftp://<user>:<passwd>@<hostname|[IPv6]>[:port]>/path/file
  http://<hostname|[IPv6]>[:port]/path/file

**Example**

```
rfs6000-81742D>crypto key generate rsa key 1025
RSA Keypair successfully generated
rfs6000-81742D>

rfs6000-81742D>crypto key import rsa test123 url passphrase word background
RSA key import operation is started in background
rfs6000-81742D>

rfs6000-81742DE>crypto pki generate self-signed word generate-rsa-key word
autogen-subject-name fqdn word
Successfully generated self-signed certificate
rfs6000-81742D>

rfs6000-81742D>crypto pki zeroize trustpoint word del-key
Successfully removed the trustpoint and associated certificates
%Warning: Applications associated with the trustpoint will start using default-
trustpoint
rfs6000-81742D>

rfs6000-81742D>crypto pki authenticate word url background
Import of CA certificate started in background
rfs6000-81742D>

rfs6000-81742D>crypto pki import trustpoint word url passphrase word
Import operation started in background
rfs6000-81742D>
```

**Related Commands**

| | |
|---|---|
| *no* | Removes server certificates, trustpoints and their associated certificates |

## 2.1.9 crypto-cmp-cert-update

*User Exec Commands*

Triggers a *Certificate Management Protocol* (CMP) certificate update on a specified device or devices

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
crypto-cmp-cert-update <TRUSTPOINT-NAME> {on <DEVICE-NAME>}
```

**Parameters**

- `crypto-cmp-cert-update <TRUSTPOINT-NAME> {on <DEVICE-NAME>}`

| | |
|---|---|
| crypto-cmp-cert-update <TRUSTPOINT-NAME> on <DEVICE-NAME> | Triggers a CMP certificate update on a specified device or devices<br>• <TRUSTPOINT-NAME> – Specify the target trustpoint name. A trustpoint represents a CA/identity pair containing the identity of the CA, CA specific configuration parameters, and an association with an enrolled identity certificate. Use the crypto-cmp-policy context mode to configure the trustpoint.<br>• on <DEVICE-NAME> – Optional. Initiates a CMP certificate update and response on a specified device or devices. Specify the name of the AP, wireless controller, or service platform. Multiple devices can be provided as a comma separated list.<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

**Example**

```
rfs4000-229D58>crypto-cmp-cert-update test on B4-C7-99-71-17-28
CMP Cert update success
rfs4000-229D58>
```

## 2.1.10 database

*User Exec Commands*

Enables automatic repairing (vacuuming) and dropping of captive-portal and NSight databases

If enforcing authenticated access to the *database*, use this command to generate the keyfile. Every keyfile has a set of associated users having a username and password. Access to the database is allowed only if the user credentials entered during database login are valid. For more information on enabling database authentication, see *Enabling Database Authentication*.

**Supported in the following platforms:**

- Service Platforms — NX9500, NX9510, NX9600, VX9000

**Syntax**

```
database [drop|keyfile|repair]

database drop [all|captive-portal|nsight]

database repair {on <DEVICE-NAME>}

database keyfile [export|generate|import|zerzoise]
database keyfile generate
database keyfile [export|import] <URL>
database keyfile zerzoise
```

**Parameters**

- `database drop [all|captive-portal|nsight]`

| | |
|---|---|
| database drop [all\|captive-portal\| nsight] | Drops (deletes) all or a specified database. Execute the command on the database.<br>• all – Drops all databases, captive portal and NSight<br>• captive-portal – Drops the captive-portal database<br>• nsight – Drops the NSight database |

- `database repair {on <DEVICE-NAME>}`

| | |
|---|---|
| database repair on <DEVICE-NAME> | Enables automatic repairing of all databases. Repairing (vacuuming a database refers to the process of finding and reclaiming space left over from previous DELETE statements. Execute the command on the database host.<br>• on <DEVICE-NAME> – Optional. Specifies the name of the database host. When specified, databases on the specified host are periodically checked to identify and remove obsolete data documents.<br>  • <DEVICE-NAME> – Specify the name of the access point, wireless controller, or service platform.<br>**Note:** If no device is specified, the system repairs all databases. |

- `database keyfile generate`

| | |
|---|---|
| database keyfile [generate\|zerzoise] | Enables database keyfile management. This command is part of a set of configurations required to enforce database authentication. Use this command to generate database keyfiles. After generating the keyfile, create the username and password combination required to access the database. For information on creating database users see, *service*. For information on enabling database authentication, see *Enabling Database Authentication*.<br>• generate – Generates the keyfile. In case of a replica-set deployment, execute the command on the primary database host. Once generated, export the keyfile to a specified location from where it is imported on to the replica-set hosts. |

- `database keyfile [export|import] <URL>`

| | |
|---|---|
| database keyfile [export\|import] <URL> | Enables database keyfile management. This command is part of a set of configurations required to enforce database authentication. Use this command to exchange keyfiles between replica set members.<br>• export – Exports the keyfile to a specified location on an FTP/SFTP/TFTP server. Execute the command on the database host on which the keyfile has been generated.<br>• import – Imports the keyfile from a specified location. Execute the command on the replica set members.<br>The following parameter is common to both of the above keywords:<br>• <URL> – Specify the location to/from where the keyfile is to be exported/imported. Use one of the following options to specify the keyfile location:<br>ftp://<user>:<passwd>@<hostname\|IP>[:port]/path/file<br>sftp://<user>:<passwd>@<hostname\|IP>[:port]/path/file<br>tftp://<hostname\|IP>[:port]/path/file |

- `database keyfile zerzoise`

| | |
|---|---|
| database keyfile zerzoise | Enables database keyfile management. Use this command to delete keyfiles<br>• zerzoise – Deletes an existing keyfile. |

**Example**

```
nx9500-6C8809>database repair on nx9500-6C8809
nx9500-6C8809>

nx9500-6C8809>database keyfile generate
Database keyfile successfully generated
nx9500-6C8809>

nx9500-6C8809>database keyfile zeroize
Database keyfile successfully removed
nx9500-6C8809>

vx9000-1A1809>database keyfile generate
Database keyfile successfully generated
vx9000-1A1809>

vx9000-1A1809>database keyfile export ftp://1.1.1.111/db-key
Database keyfile successfully exported
vx9000-1A1809>
```

```
vx9000-D031F2>database keyfile import ftp://1.1.1.111/db-key
Database keyfile successfully imported
vx9000-D031F2>
```

**Example Enabling Database Authentication**

Follow the steps below to enable database authentication.

1 On the primary database host,

a Generate the database keyfile.

```
Primary-DB-HOST>database keyfile generate
Database keyfile successfully generated
Primary-DB-HOST>
```

b Use the *show > database > keyfile* command to view the generated keyfile.

c Export the keyfile to an external location. This is required only in case of database replica-set deployment.

```
Primary-DB-HOST>database keyfile export ftp://1.1.1.111/db-key
Database keyfile successfully exported
Primary-DB-HOST>
```

d Create the users that are allowed access to the database.

```
Primary-DB-HOST#service database authentication create-user username techpubs
password techPubs@123
Database user [techpubs] created.
Primary-DB-HOST#
```

e View the database user account created.

```
Primary-DB-HOST#show database users
--------------------------------
         DATABASE USER
--------------------------------
 techpubs
--------------------------------
Primary-DB-HOST#
```

2 On the replica set host, import the keyfile from the location specified in Step 1 c.

```
Secondary-DB-HOST#database keyfile import ftp://1.1.1.111/db-key
```

3 In the database-policy context, --- (used on the NSight/EGuest database hosts)

a Enable authentication.

```
Primary-DB-HOST(config-database-policy-techpubs)#authentication
```

b Configure the user accounts created in Step 1 d.

```
Primary-DB-HOST(config-database-policy-techpubs)#authentication username
techpubs password S540QFZz9LzSOdX1ZJEqDgAAAAy3b7GtyO4Z/Ih2ruxnOYnr
Primary-DB-HOST(config-database-policy-techpubs)#show context
database-policy techpubs
 authentication
 authentication username techpubs password 2
S540QFZz9LzSOdX1ZJEqDgAAAAy3b7GtyO4Z/Ih2ruxnOYnr
 replica-set member nx7500-A02B91 arbiter
 replica-set member vx9000-1A1809 priority 1
```

```
 replica-set member vx9000-D031F2 priority 20
Primary-DB-HOST(config-database-policy-techpubs)#
```

4 In the database-client policy context --- (used on the NSight/EGuest server host),

Note, this configuration is required only if the NSight/EGuest server and database are hosted on separate hosts.

a Configure the user credentials created in Step 1 d.

```
NOC-Controller(config-database-client-policy-techpubs)#authentication username
techpubs password S540QFZz9LzSOdX1ZJEqDgAAAAy3b7GtyO4Z/Ih2ruxnOYnr
```

b View the configuration.

```
NOC-Controller(config-database-client-policy-techpubs)#show context
database-client-policy techpubs
 authentication username techpubs password 2
S540QFZz9LzSOdX1ZJEqDgAAAAy3b7GtyO4Z/Ih2ruxnOYnr
NOC-Controller(config-database-client-policy-techpubs)#
```

**Related Commands**

| | |
|---|---|
| *database-backup* | Backs up captive-portal and/or NSight database to a specified location and file on an FTP or SFTP server |
| *database-restore* | Restores a previously exported database [captive-portal and/or NSight] |
| *database-policy* | Documents database-policy configuration commands. Use this option to enable the database. |
| *database-client-policy* | Documents database-client-policy configuration commands. Use this option to configure the database host details (IP address or hostname). If enforcing database authentication, use it to configure the users having database access. Once configured, use the policy in the NSight/EGuest server's device config context. |
| *service* | Documents the database user account configuration details |

## 2.1.11 database-backup

*User Exec Commands*

Backs up captive-portal and/or NSight database to a specified location and file on an FTP, SFTP, or TFTP server. Execute this command on the database host.

**Supported in the following platforms:**

- Service Platforms — NX9500, NX9510, NX9600, VX9000

**Syntax**

```
database-backup database [captive-portal|nsight|nsight-placement-info] <URL>

database-backup database [captive-portal|nsight] <URL>
database-backup database nsight-placement-info <URL>
```

**Parameters**

- `database-backup database [captive-portal|nsight] <URL>`

| | |
|---|---|
| database-backup database [captive-portal\| nsight] | Backs up captive portal and/or NSight database to a specified location. Select the database to backup:<br>• captive-portal – Backs up captive portal database<br>• nsight – Backs up NSight database<br>After specifying the database type, configure the destination location. |
| <URL> | Configures the destination location. The database is backed up at the specified location. Specify the location URL in one of the following formats:<br>ftp://<user>:<passwd>@<hostname\|IP>[:port]/path/file.tar.gz<br>sftp://<user>:<passwd>@<hostname\|IP>[:port]/path/file.tar.gz |

- `database-backup database nsight-placement-info <URL>`

| | |
|---|---|
| database-backup database nsight-placement-info <URL> | Backs up the NSight access point placement related details to a specified location<br>• <URL> – Specify the URL in one of the following formats:<br>ftp://<user>:<passwd>@<hostname\|IP>[:port]/path/file.tar.gz<br>sftp://<user>:<passwd>@<hostname\|IP>[:port]/path/file.tar.gz<br>tftp://<hostname\|IP>[:port]/path/file.tar.gz |

**Example**

```
NS-DB-nx9510-6C87EF>database-backup database nsight tftp://192.168.9.50/testbckup
NS-DB-nx9510-6C87EF>show database backup-status
Last Database Backup Status : In_Progress(Starting tftp transfer.)
Last Database Backup Time   : 2017-04-17 12:48:05
NS-DB-nx9510-6C87EF>show database backup-status
Last Database Backup Status : Successful
Last Database Backup Time   : Mon Apr 17 12:48:08 IST 2017
NS-DB-nx9510-6C87EF>Apr 17 12:48:17 2017: NS-DB-nx9510-6C87EF : %DATABASE-6-
OPERATION_COMPLETE: backup for database nsight successful
NS-DB-nx9510-6C87EF#
```

```
NS-DB-nx9510-6C87EF>database-backup database nsight-placement-info tftp://192.16
8.9.50/plmentinfo
NS-DB-nx9510-6C87EF>show database backup-status
Last Database Backup Status : Successful
Last Database Backup Time   : Mon Apr 17 12:48:48 IST 2017
NS-DB-nx9510-6C87EF>Apr 17 12:49:03 2017: NS-DB-nx9510-6C87EF : %DATABASE-6-
OPERATION_COMPLETE: backup for database nsight-placement-info successful

NS-DB-nx9510-6C87EF>
```

**Related Commands**

| | |
|---|---|
| *database* | Enables automatic repairing (vacuuming) and dropping of databases (captive-portal and/or NSight) |
| *database-restore* | Restores a previously exported (backed up) database (captive-portal and/or NSight)] |

## 2.1.12 database-restore

*User Exec Commands*

Restores a previously exported database [captive-portal and/or NSight]. Previously exported databases (backed up to a specified FTP or SFTP server) are restored from the backed-up location to the original database.

**Supported in the following platforms:**

- Service Platforms — NX9500, NX9510, NX9600, VX9000

**Syntax**

```
database-restore database [captive-portal|nsight] <URL>
```

**Parameters**

- `database-restore database [captive-portal|nsight] <URL>`

| | |
|---|---|
| database-restore database [captive-portal\| nsight] | Restores previously exported (backed up) captive-portal and/or NSight database. Specify the database type:<br>• captive-portal – Restores captive portal database<br>• nsight – Restores NSight database<br>After specifying the database type, configure the destination location and file name from where the files are restored. |
| <URL> | Configures the destination location. The database is restored from the specified location. Specify the location URL in one of the following formats:<br>ftp://<user>:<passwd>@<hostname\|IP>[:port]/path/file.tar.gz<br>sftp://<user>:<passwd>@<hostname\|IP>[:port]/path/file.tar.gz<br>tftp://<hostname\|IP>[:port]/path/file.tar.gz |

**Example**

```
nx9500-6C8809>database-restore database nsight ftp://
anonymous:anonymous@192.168.13.10/backups/nsight/nsight.tar.gz
```

**Related Commands**

| | |
|---|---|
| *database* | Enables automatic repairing (vacuuming) and dropping of databases (captive-portal and NSight) |
| *database-backup* | Backs up captive-portal and/or NSight database to a specified location and file on an FTP or SFTP server |

## 2.1.13 device-upgrade

*User Exec Commands*

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

In an *hierarchically managed* (HM) network, this command enables centralized device upgradation across the network. The WiNG HM network defines a three-tier structure, consisting of multiple wireless sites managed by a single *Network Operations Center* (NOC) controller. The NOC controller constitutes the first and the site controllers constitute the second tier of the hierarchy. The site controllers in turn adopt and manage access points that form the third tier of the hierarchy.

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

Use the device-upgrade command to schedule firmware upgrades across adopted devices within the network. Devices are upgraded based on their device names, MAC addresses, or RF Domain.

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

**NOTE:** A NOC controller's capacity is equal to, or higher than that of a site controller. The following devices can be deployed at NOC and sites:

- NOC controller – NX95XX (NX9500 and NX9510), NX9600, VX9000
- Site controller – RFS4000, RFS6000, NX5500, or NX95XX

**NOTE:** Standalone devices have to be manually upgraded.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
device-upgrade [<MAC/HOSTNAME>|all|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|
ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap76232|ap7662|ap81xx|ap82xx|ap8432|
ap8533|rfs4000|rfs6000|nx5500|nx75xx|nx9000|nx9600|vx9000|cancel-upgrade|load-
image|rf-domain]

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

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

device-upgrade [ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|
ap7602|ap7612|ap7622|ap76232|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|rfs6000|
nx5500|nx75xx|nx9000|nx9600|vx9000] all {force|no-reboot|reboot-time
<TIME>|upgrade-time <TIME> {no-reboot|reboot-time <TIME>}} {(staggered-reboot)}

device-upgrade cancel-upgrade [<MAC/HOSTNAME>|all|ap6521|ap6522|ap6532|ap6562|
ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap76232|ap7662|ap81xx|
ap82xx|ap8432|ap8533|rfs4000|rfs6000|nx5500|nx75xx|nx9000|nx9600|vx9000|
on rf-domain [<RF-DOMAIN-NAME>|all]]

device-upgrade load-image [ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|
ap7532|ap7562|ap7602|ap7612|ap7622|ap76232|ap7662|ap81xx|ap82xx|ap8432|ap8533|
rfs4000|rfs6000|nx5500|nx9000|nx9600|vx9000] {<IMAGE-URL>|on <DEVICE-OR-DOMAIN-
NAME>}

device-upgrade rf-domain [<RF-DOMAIN-NAME>|all|containing <WORD>|filter location
<WORD>] [all|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|
ap7602|ap7612|ap7622|ap76232|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|rfs6000|
nx5500|nx75xx|nx9000|nx9600|vx9000] {(<MAC/HOSTNAME>|force|from-controller|
no-reboot|reboot-time <TIME>|staggered-reboot|upgrade-time <TIME>)}
```

**Parameters**

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

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

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

| | |
|---|---|
| all | Upgrades firmware on all devices |
| force | Optional. Select this option to force upgrade on the selected device(s). When selected, the devices are upgraded even if they have the same firmware as the upgrading access point, wireless controller, or service platform. If forcing a device upgrade, optionally specify any one of the following options: no-reboot, reboot-time, upgrade-time, or staggered-reboot. |
| no-reboot | Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted) |
| reboot-time <TIME> | Optional. Schedules an automatic reboot after a successful upgrade<br>• <TIME> – Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format. |

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

• `device-upgrade [ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|rfs6000|nx5500|nx75xx|nx9000|nx9600|vx9000] all` *`{force|no-reboot|reboot-time <TIME>|upgrade-time <TIME> {no-reboot|reboot-time <TIME>}} {(staggered-reboot)}`*

| | |
|---|---|
| device-upgrade <DEVICE-TYPE> all | Upgrades firmware on all devices of a specific type. Select the device type. The options are: AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533, RFS4000, RFS6000, NX5500, NX75XX, NX9500, NX9600, and VX9000.<br>After selecting the device type, schedule an automatic upgrade and/or an automatic reboot. |
| force | Optional. Select this option to force upgrade on the selected device(s). When selected, the devices are upgraded even if they have the same firmware as the upgrading access point, wireless controller, or service platform. If forcing a device upgrade, optionally specify any one of the following options: no-reboot, reboot-time, upgrade-time, or staggered-reboot. |
| no-reboot | Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted) |
| reboot-time <TIME> | Optional. Schedules an automatic reboot after a successful upgrade<br>• <TIME> – Optional. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format. |
| upgrade-time <TIME> {no-reboot\| reboot-time <TIME>} | Optional. Schedules an automatic firmware upgrade on all devices, of the specified type, on a specified day and time<br>• <TIME> – Specify the upgrade time in the MM/DD/YYYY-HH:MM or HH:MM format. The following actions can be performed after a scheduled upgrade:<br>• no-reboot – Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted)<br>• reboot-time <TIME> – Optional. Schedules an automatic reboot after a successful upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format. |
| staggered-reboot | This keyword is recursive and common to all of the above.<br>• Optional. Enables staggered device reboot (one at a time) without network impact |

- `device-upgrade cancel-upgrade [<MAC/HOSTNAME>|all|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|rfs6000|nx5500|nx75xx|nx9000|nx9600|vx9000| on rf-domain [<RF-DOMAIN-NAME>|all]]`

| | |
|---|---|
| cancel-upgrade | Cancels a scheduled firmware upgrade based on the parameters passed. This command provides the following options to cancel scheduled firmware upgrades:<br>• Cancels upgrade on specific device(s). The devices are identified by their MAC addresses or hostnames.<br>• Cancels upgrade on all devices within the network<br>• Cancels upgrade on all devices of a specific type. Specify the device type.<br>• Cancels upgrade on specific device(s) or all device(s) within a specific RF Domain or all RF Domains. Specify the RF Domain name. |
| cancel-upgrade [<MAC/HOSTNAME>\| all] | Cancels a scheduled firmware upgrade on a specified device or on all devices<br>• <MAC/HOSTNAME> – Cancels a scheduled upgrade on the device identified by the <MAC/HOSTNAME> keyword. Specify the device's MAC address or hostname.<br>• all – Cancels scheduled upgrade on all devices |
| cancel-upgrade <DEVICE-TYPE> all | Cancels scheduled firmware upgrade on all devices of a specific type. Select the device type. The options are: AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533, RFS4000, RFS6000, NX5500, NX75XX, NX9500, NX9600, and VX9000. |
| cancel-upgrade on rf-domain [<RF-DOMAIN-NAME>\|all] | Cancels scheduled firmware upgrade on all devices in a specified RF Domain or all RF Domains<br>• <RF-DOMAIN-NAME> – Cancels scheduled device upgrade on all devices in a specified RF Domain. Specify the RF Domain name.<br>• all – Cancels scheduled device upgrade on all devices across all RF Domains |

- `device-upgrade load-image [ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|rfs6000|nx500|nx9000|nx9600|vx9000] {<IMAGE-URL>|on <DEVICE-OR-DOMAIN-NAME>}`

| | |
|---|---|
| load-image <DEVICE-TYPE> | Loads device firmware image from a specified location. Use this command to specify the device type and the location of the corresponding image file.<br>• <DEVICE-TYPE> – Specify the device type. The options are: AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533, RFS4000, RFS6000, NX5500, NX75XX, NX9500, NX9600, and VX9000.<br>After specifying the device type, provide the location of the required device firmware image. |
| <IMAGE-URL> | Specify the device's firmware image location in one of the following formats:<br>IPv4 URLs:<br>tftp://<hostname\|IP>[:port]/path/file<br>ftp://<user>:<passwd>@<hostname\|IP>[:port]/path/file<br>sftp://<user>:<passwd>@<hostname\|IP>[:port]>/path/file<br>http://<hostname\|IP>[:port]/path/file<br>cf:/path/file<br>usb<n>:/path/file |

| | |
|---|---|
| | IPv6 URLs:<br>tftp://<hostname\|[IPv6]>[:port]/path/file<br>ftp://<user>:<passwd>@<hostname\|[IPv6]>[:port]/path/file<br>sftp://<user>:<passwd>@<hostname\|[IPv6]>[:port]>/path/file<br>http://<hostname\|[IPv6]>[:port]/path/file |
| on <DEVICE-OR-DOMAIN-NAME> | Specify the name of the device or RF Domain. The image, of the specified device type is loaded from the device specified here. In case of an RF Domain, the image available on the RF Domain manager is loaded.<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |

- `device-upgrade rf-domain [<RF-DOMAIN-NAME>|all|containing <WORD>|filter location <WORD>] [all|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|rfs6000|nx5500|nx75xx|nx9000|nx9600|vx9000] {(<MAC/HOSTNAME>|force|from-controller|no-reboot|reboot-time <TIME>|staggered-reboot|upgrade-time <TIME>)}`

| | |
|---|---|
| rf-domain [<RF-DOMAIN-NAME>\|all\| containing <WORD>\| filter location <WORD>] | Upgrades firmware on devices in a specified RF Domain or all RF Domains. Devices within a RF Domain are upgraded through the RF Domain manager.<br>• <RF-DOMAIN-NAME> – Upgrades devices in the RF Domain identified by the <RF-DOMAIN-NAME> keyword.<br>  • <RF-DOMAIN-NAME> – Specify the RF Domain name.<br>• all – Upgrades devices across all RF Domains<br>• containing <WORD> – Filters RF Domains by their names. RF Domains with names containing the sub-string identified by the <WORD> keyword are filtered. Devices on the filtered RF Domains are upgraded.<br>• filter location <WORD> – Filters devices by their location. All devices with location matching the <WORD> keyword are upgraded. |
| <DEVICE-TYPE> | After specifying the RF Domain, select the device type. The options are: AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533, RFS4000, RFS6000, NX5500, NX75XX, NX9500, NX9600, and VX9000.<br>After specifying the RF Domain and the device type, configure any one of the following actions: force devices to upgrade, or initiate an upgrade through the adopting controller. |
| <MAC/HOSTNAME> | Optional. Use this option to identify specific devices for upgradation. Specify the device's MAC address or hostname. The device should be within the specified RF Domain and of the specified device type. After identifying the devices to upgrade, configure any one of the following actions: force devices to upgrade, or initiate an upgrade through the adopting controller.<br>**Note:** If no MAC address or hostname is specified, all devices of the type selected are upgraded. |
| force | Optional. Select this option to force upgrade for the selected device(s). When selected, the devices are upgraded even if they have the same firmware as the upgrading access point, wireless controller, or service platform. If forcing a device upgrade, optionally specify any one of the following options: no-reboot, reboot-time, upgrade-time, or reboot-time. |
| from-controller | Optional. Upgrades a device through the adopted device. If initiating an upgrade through the adopting controller, optionally specify any one of the following options: no-reboot, reboot-time, upgrade-time, or reboot-time. |

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

**Example**

```
nx9500-6C8809>show adoption status
-------------------------------------------------------------------------------
-------------------------
DEVICE-NAME      VERSION       CFG-STAT      MSGS   ADOPTED-BY    LAST-ADOPTION
UPTIME
-------------------------------------------------------------------------------
-------------------------
rfs6000-81742D 5.9.1.0-012D   configured      No   nx9500-6C8809 2 days 12:23:52
13 days 22:32:38
t5-ED7C6C         5.4.2.0-010R    configured       No   nx9500-6C8809 13 days
22:47:46    16 days 22:33:25

-------------------------------------------------------------------------------
-------------------------
Total number of devices displayed: 2
nx9500-6C8809>

nx9500-6C8809>show device-upgrade versions
-------------------------------------------------------------------------------
          CONTROLLER               DEVICE-TYPE                VERSION
-------------------------------------------------------------------------------
  nx9500-6C8809               ap621                    5.9.0.0-014D
  nx9500-6C8809               ap622                    5.9.1.0-012D
  nx9500-6C8809               ap650                    5.9.1.0-012D
  nx9500-6C8809               ap6511                   none
  nx9500-6C8809               ap6521                   5.9.0.0-014D
  nx9500-6C8809               ap6522                   5.9.1.0-012D
  nx9500-6C8809               ap6532                   5.9.1.0-012D
  nx9500-6C8809               ap6562                   5.9.1.0-012D
  nx9500-6C8809               ap71xx                   5.9.1.0-012D
  nx9500-6C8809               ap7502                   5.9.1.0-012D
  nx9500-6C8809               ap7522                   5.9.1.0-012D
  nx9500-6C8809               ap7532                   5.9.1.0-012D
  nx9500-6C8809               ap7562                   5.9.1.0-012D
  nx9500-6C8809               ap7602                   5.9.1.0-012D
  nx9500-6C8809               ap7612                   5.9.1.0-012D
  nx9500-6C8809               ap7622                   5.9.1.0-012D
  nx9500-6C8809               ap7632                   5.9.1.0-012D
  nx9500-6C8809               ap7662                   5.9.1.0-012D
  nx9500-6C8809               ap81xx                   5.9.1.0-012D
  nx9500-6C8809               ap82xx                   5.9.1.0-012D
  nx9500-6C8809               ap8432                   5.9.1.0-012D
  nx9500-6C8809               ap8533                   5.9.1.0-012D
  nx9500-6C8809               nx45xx                   none
  nx9500-6C8809               nx5500                   none
```

```
  nx9500-6C8809              nx65xx                  none
  nx9500-6C8809              nx75xx                  none
  nx9500-6C8809              nx9000                  none
  nx9500-6C8809              rfs4000                 5.9.1.0-012D
  nx9500-6C8809              rfs6000                 5.9.1.0-012D
  nx9500-6C8809              rfs7000                 5.9.0.0-010D
  nx9500-6C8809              vx9000                  none
-------------------------------------------------------------------------------
nx9500-6C8809>

nx9500-6C8809#device-upgrade load-image rfs6000 ftp://
anonymous:anonymous@192.168.13.10/LatestBuilds/W591/RFS6000-LEAN-5.9.1.0-
015D.img
-------------------------------------------------------------------------------
      CONTROLLER          STATUS                      MESSAGE
-------------------------------------------------------------------------------
  nx9500-6C8809        Success        Successfully initiated load image
-------------------------------------------------------------------------------
nx9500-6C8809#

nx9500-6C8809#show device-upgrade load-image-status
Download of rfs6000 firmware file is complete
nx9500-6C8809#

nx9500-6C8809>show device-upgrade versions
-------------------------------------------------------------------------------
          CONTROLLER              DEVICE-TYPE                VERSION
-------------------------------------------------------------------------------
  nx9500-6C8809              ap621                   5.9.0.0-014D
  nx9500-6C8809              ap622                   5.9.1.0-012D
  nx9500-6C8809              ap650                   5.9.1.0-012D
  nx9500-6C8809              ap6511                  none
  nx9500-6C8809              ap6521                  5.9.0.0-014D
  nx9500-6C8809              ap6522                  5.9.1.0-012D
  nx9500-6C8809              ap6532                  5.9.1.0-012D
  nx9500-6C8809              ap6562                  5.9.1.0-012D
  nx9500-6C8809              ap71xx                  5.9.1.0-012D
  nx9500-6C8809              ap7502                  5.9.1.0-012D
  nx9500-6C8809              ap7522                  5.9.1.0-012D
  nx9500-6C8809              ap7532                  5.9.1.0-012D
  nx9500-6C8809              ap7562                  5.9.1.0-012D
  nx9500-6C8809              ap7602                  5.9.1.0-012D
  nx9500-6C8809              ap7612                  5.9.1.0-012D
  nx9500-6C8809              ap7622                  5.9.1.0-012D
  nx9500-6C8809              ap7632                  5.9.1.0-012D
  nx9500-6C8809              ap7662                  5.9.1.0-012D
  nx9500-6C8809              ap81xx                  5.9.1.0-012D
  nx9500-6C8809              ap82xx                  5.9.1.0-012D
  nx9500-6C8809              ap8432                  5.9.1.0-012D
  nx9500-6C8809              ap8533                  5.9.1.0-012D
  nx9500-6C8809              nx45xx                  none
  nx9500-6C8809              nx5500                  none
  nx9500-6C8809              nx65xx                  none
  nx9500-6C8809              nx75xx                  none
  nx9500-6C8809              nx9000                  none
  nx9500-6C8809              rfs4000                 5.9.1.0-012D
  nx9500-6C8809              rfs6000                 5.9.1.0-015D
  nx9500-6C8809              rfs7000                 5.9.0.0-010D
  nx9500-6C8809              vx9000                  none
-------------------------------------------------------------------------------
nx9500-6C8809>
```

```
nx9500-6C8809>device-upgrade rfs6000-81742D
-------------------------------------------------------------------------------
         CONTROLLER             STATUS                    MESSAGE
-------------------------------------------------------------------------------
  B4-C7-99-6C-88-09         Success         Queued 1 devices to upgrade
-------------------------------------------------------------------------------
nx9500-6C8809>

nx9500-6C8809>show device-upgrade status
Number of devices currently being upgraded : 1
Number of devices waiting in queue to be upgraded : 0
Number of devices currently being rebooted : 0
Number of devices waiting in queue to be rebooted : 0
Number of devices failed upgrade : 0
-------------------------------------------------------------------------------
------------------------------
      DEVICE           STATE     UPGRADE TIME REBOOT TIME PROGRESS RETRIES LAST
UPDATE ERROR    UPGRADED BY
-------------------------------------------------------------------------------
------------------------------
  rfs6000-81742D downloading   immediate   immediate   17      0      -
nx9500-6C8809
-------------------------------------------------------------------------------
------------------------------
nx9500-6C8809>

nx9500-6C8809>show adoption status
-------------------------------------------------------------------------------
------------------------------
DEVICE-NAME       VERSION         CFG-STAT         MSGS ADOPTED-BY        LAST-
ADOPTION                  UPTIME
-------------------------------------------------------------------------------
------------------------------
rfs6000-81742D 5.9.1.0-015D   version-mismatch No  nx9500-6C8809 0 days 00:00:42
0 days 00:03:33
t5-ED7C6C         5.4.2.0-010R    configured       No   nx9500-6C8809 13 days
23:09:38    16 days 22:55:17
-------------------------------------------------------------------------------
------------------------------
Total number of devices displayed: 2
nx9500-6C8809>
```

## 2.1.14 disable

*User Exec Commands*

This command can be executed in the Priv Exec Mode only. When executed, the command turns off (disables) the privileged mode command set and returns to the User Executable Mode. The prompt changes from *rfs6000-81742D#* `to` *rfs6000-81742D>*.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
disable
```

**Parameters**

None

**Example**

```
rfs6000-81742D#disable
rfs6000-81742D>
```

## 2.1.15 enable

*User Exec Commands*

Turns on (enables) the privileged mode command set. The prompt changes from *rfs6000-81742D>* to *rfs6000-81742D#*. This command does not do anything in the Privilege Executable mode.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
enable
```

**Parameters**

None

**Example**

```
rfs6000-81742D>enable
rfs6000-81742D#
```

## 2.1.16 file-sync

*User Exec Commands*

Syncs trustpoint and/or EAP-TLS X.509 (PKCS#12) certificate between the staging-controller and adopted access points.

When enabling file syncing, consider the following points:

- The X.509 certificate needs synchronization only if the access point is configured to use EAP-TLS authentication.
- Execute the command on the controller adopting the access points.
- Ensure that the X.509 certificate file is installed on the controller.

Syncing of trustpoint/wireless-bridge certificate can be automated. To automate file syncing, in the controller's device/profile configuration mode, execute the following command: *file-sync [auto|count <1-20>]*. For more information, see *file-sync*.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632,AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
file-sync [cancel|load-file|trustpoint|wireless-bridge]

file-sync cancel [trustpoint|wireless-bridge]

file-sync cancel [trustpoint|wireless-bridge] [<DEVICE-NAME>|all|rf-domain
[<DOMAIN-NAME>|all]]

file-sync load-file [trustpoint|wireless-bridge]]

file-sync load-file [trustpoint <TRUSTPOINT-NAME>|wireless-bridge] <URL>

file-sync [trustpoint <TRUSTPOINT-NAME>|wireless-bridge] [<DEVICE-NAME>|all|
rf-domain [<DOMAIN-NAME>|all] {from-controller}] {reset-radio|upload-time <TIME>}
```

**Parameters**

- `file-sync cancel [trustpoint|wireless-bridge] [<DEVICE-NAME>|all|rf-domain [<DOMAIN-NAME>|all]]`

| | |
|---|---|
| file-sync cancel [trustpoint\| wireless-bridge] [<DEVICE-NAME>\| all\|rf-domain [<DOMAIN-NAME>\| all]] | Cancels scheduled file synchronization<br>• trustpoint – Cancels scheduled trustpoint synchronization on a specified AP, all APs, or APs within a specified RF Domain<br>• wireless-bridge – Cancels scheduled wireless-bridge certificate synchronization on a specified AP, all APs, or APs within a specified RF Domain<br>• <DEVICE-NAME> – Cancels scheduled trustpoint/certificate synchronization on a specified AP. Specify the AP's hostname or MAC address.<br>• all – Cancels scheduled trustpoint/certificate synchronization on all APs<br>Contd.. |

| | |
|---|---|
| | • rf-domain [<DOMAIN-NAME>\|all] – Cancels scheduled trustpoint/certificate synchronization on all APs in a specified RF Domain or in all RF Domains<br>• <DOMAIN-NAME> – Cancels scheduled trustpoint/certificate synchronization on all APs within a specified RF Domain. Specify the RF Domain's name.<br>• all – Cancels scheduled trustpoint/certificate synchronization on all RF Domains |

• `file-sync load-file [trustpoint|wireless-bridge] <URL>`

| | |
|---|---|
| file-sync load-file [trustpoint\| wireless-bridge] <URL> | Loads the following files on to the staging controller:<br>• trustpoint – Loads the trustpoint, including CA certificate, server certificate and private key<br>• wireless-bridge – Loads the wireless-bridge certificate to the staging controller<br>Use this command to load the certificate to the controller before scheduling or initiating a certificate synchronization.<br>• <URL> – Provide the trustpoint/certificate location using one of the following formats:<br>tftp://<hostname\|IP>[:port]/path/file<br>ftp://<user>:<passwd>@<hostname\|IP>[:port]/path/file<br>sftp://<user>:<passwd>@<hostname\|IP>[:port]>/path/file<br>http://<hostname\|IP>[:port]/path/file<br>cf:/path/file<br>usb<n>:/path/file<br>**Note:** Both IPv4 and IPv6 address types are supported. |

• `file-sync [trustpoint <TRUSTPOINT-NAME>|wireless-bridge] [<DEVICE-NAME>|all|rf-domain [<DOMAIN-NAME>|all] {from-controller}] {reset-radio|upload-time <TIME>}`

| | |
|---|---|
| file-sync trustpoint <TRUSTPOINT-NAME> [<DEVICE-NAME>\| all\|rf-domain [<DOMAIN-NAME> \|all] from-controller] | Configures file-syncing parameters<br>• trustpoint <TRUSTPOINT-NAME> – Syncs a specified trustpoint between controller and its adopted APs<br>• <TRUSTPOINT-NAME> – Specify the trustpoint name.<br>• wireless-bridge – Syncs wireless-bridge certificate between controller and its adopted APs<br>After specifying the file that is to be synced, configure following file-sync parameters:<br>• <DEVICE-NAME> – Syncs trustpoint/certificate with a specified AP. Specify the AP's hostname or MAC address.<br>• all – Syncs trustpoint/certificate with all APs<br>• rf-domain [<DOMAIN-NAME>\|all] – Syncs trustpoint/certificate with all APs in a specified RF Domain or in all RF Domains<br>• <DOMAIN-NAME> – Select to sync with APs within a specified RF Domain. Specify the RF Domain's name.<br>• all – Select to sync with APs across all RF Domains<br>• from-controller – Optional. Loads certificate to the APs from the adopting controller and not the RF Domain manager<br>After specifying the access points, specify the following options: reset-radio and upload-time. |

| | |
|---|---|
| reset-radio | This keyword is recursive and applicable to all of the above parameters.<br>Optional. Resets the radio after file synchronization. Reset the radio in case the certificate is renewed along with no changes made to the 'bridge EAP username' and 'bridge EAP password'. |
| upload-time <TIME> | This keyword is recursive and applicable to all of the above parameters.<br>• upload-time – Optional. Schedules certificate upload at a specified time<br>  • <TIME> – Specify the time in the MM/DD/YYYY-HH:MM or HH:MM format. If no time is configured, the process is initiated as soon as the command is executed. |

**Example**

```
rfs6000-81742D>file-sync wireless-bridge ap7131-11E6C4 upload-time 06/01/2017-
12:30
--------------------------------------------------------------------------------
          CONTROLLER               STATUS                  MESSAGE
--------------------------------------------------------------------------------
  B4-C7-99-6D-CD-4B           Success           Queued 1 APs to upload
--------------------------------------------------------------------------------
rfs6000-81742D>
```

The following command uploads certificate to all access points:

```
rfs6000-81742D>file-sync wireless-bridge all upload-time 06/01/2017-23:42
```

## 2.1.17 join-cluster

*User Exec Commands*

Adds a device (access point, wireless controller, or service platform), as a member, to an existing cluster of devices. Assign a static IP address to the device before adding to a cluster. Note, a cluster can be only formed of devices of the same model type.

**Supported in the following platforms:**

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

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

**Parameters**

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

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

**Usage Guidelines**

To add a device to an existing cluster:

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

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

**Example**

```
rfs4000-880DA7>join-cluster 192.168.13.15 user admin password superuser level 1
mode standby
... connecting to 192.168.13.15
... applying cluster configuration
... committing the changes
... saving the changes
[OK]
rfs4000-880DA7>
```

```
rfs4000-880DA7>show context
!
! Configuration of RFS4000 version 5.9.1.0-012D
!
!
version 2.5
!
!
.....................................................................................
 interface vlan1
  ip address 192.168.13.15/24
  no ipv6 enable
  no ipv6 request-dhcpv6-options
 cluster name TechPubs
 cluster mode standby
 cluster member ip 192.168.13.15
 logging on
 logging console warnings
 logging buffered warnings
!
!
end
rfs4000-880DA7>
```

**Related Commands**

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

## 2.1.18 l2tpv3

*User Exec Commands*

Establishes and/or brings down a *Layer 2 Tunnel Protocol Version 3* (L2TPV3) tunnel

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

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

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

**Parameters**

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

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

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

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

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

| | |
|---|---|
| l2tpv3 tunnel | Establishes or brings down L2TPv3 tunnels |
| all [down\|up] | Establishes or brings down all L2TPv3 tunnels<br>• down – Brings down all tunnels<br>• up – Establishes all tunnels |

| | |
|---|---|
| on <DEVICE-NAME> | Optional. Establishes or brings down all tunnels on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

**Example**

```
rfs6000-81742D>l2tpv3 tunnel Tunnel1 session Tunnel1Session1 up on rfs6000-81742D
```

**NOTE:** For more information on the L2TPv3 tunnel configuration mode and commands, see *Chapter 22, L2TPV3-POLICY*.

## 2.1.19 logging

*User Exec Commands*

Modifies message logging settings

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

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

**Parameters**

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

| | |
|---|---|
| monitor | Sets the terminal lines logging levels. The logging severity levels can be set from 0 - 7. The system uses default settings, if no logging severity level is specified.<br>• <0-7> – Optional. Specify the logging severity level from 0-7. The various levels and their implications are as follows:<br>• alerts – Optional. Immediate action needed (severity=1)<br>• critical – Optional. Critical conditions (severity=2)<br>• debugging – Optional. Debugging messages (severity=7)<br>• emergencies – Optional. System is unusable (severity=0)<br>• errors – Optional. Error conditions (severity=3)<br>• informational – Optional. Informational messages (severity=6)<br>• notifications – Optional. Normal but significant conditions (severity=5)<br>• warnings – Optional. Warning conditions (severity=4)<br>**Note:** Before configuring the message logging level, ensure logging module is enabled. To enable message logging, in the device's configuration mode, execute the *logging > on* command. Message logging can also be enabled on a profile. All devices using the profile will have message logging enabled. |

**Example**

```
rfs6000-81742D(config-device-00-15-70-81-74-2D)##logging on

rfs6000-81742D>logging monitor debugging

rfs6000-81742D>show logging

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

Log Buffer (69317 bytes):
```

```
Apr 04 11:53:02 2017: %DIAG-4-FAN_UNDERSPEED: Fan fan 1 under speed: 0 RPM is under
limit 2000 RPM
Apr 04 11:43:02 2017: %DIAG-4-FAN_UNDERSPEED: Fan fan 1 under speed: 0 RPM is under
limit 2000 RPM
--More--
rfs6000-81742D>
```

**Related Commands**

| | |
|---|---|
| *no* | Resets terminal lines logging levels |

## 2.1.20 mint

*User Exec Commands*

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

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
mint [ping|traceroute]

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

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

**Parameters**

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

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

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

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

**Example**

```
rfs6000-81742D>mint ping 19.6C.88.09
MiNT ping 19.6C.88.09 with 64 bytes of data.
 Response from 19.6C.88.09: id=1 time=0.219 ms
 Response from 19.6C.88.09: id=2 time=0.145 ms
 Response from 19.6C.88.09: id=3 time=0.127 ms

--- 19.6C.88.09 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.127/0.164/0.219 ms
rfs6000-81742D>
```

## 2.1.21 no

*User Exec Commands*

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

**NOTE:** The "no" command sub-set of commands changes with the context in which it is executed.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

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

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

**NOTE:** The *no > adoption* command resets the adoption state of a specified device (and all devices adopted to it) *or* devices within a specified RF Domain. When executed without specifying the device or RF Domain, the command resets the adoption state of the logged device and all devices, if any, adopted to it.

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

no crypto pki [server|trustpoint]

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

no logging monitor

no page

no service [block-adopter-config-update|locator|snmp|ssm|wireless]

no service snmp sysoid wing5

no service block-adopter-config-update

no service ssm trace pattern {<WORD>} {on <DEVICE-NAME>}

no service wireless [trace pattern {<WORD>} {on <DEVICE-NAME>}|unsanctioned ap air-
terminate <BSSID> {on <DOMAIN-NAME>}]

no service locator {on <DEVICE-NAME>}

no terminal [length|width]

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

no wireless client [all|<MAC>]
```

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

**Parameters**

- `no <PARAMETERS>`

| | |
|---|---|
| no <PARAMETERS> | Resets or reverts settings based on the parameters passed |

**Usage Guidelines**

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

**Example**

```
rfs4000-880DA7>no adoption
rfs4000-880DA7>no page
```

## 2.1.22 on

*User Exec Commands*

Executes the following commands in the RF Domain context: clrscr, do, end, exit, help, service, and show

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
on rf-domain [<RF-DOMAIN-NAME>|all]
```

**Parameters**

- `on rf-domain [<RF-DOMAIN-NAME>|all]`

| | |
|---|---|
| on rf-domain [<RF-DOMAIN-NAME>\|all] | Enters the RF Domain context based on the parameter specified<br>• <RF-DOMAIN-NAME> – Specify the RF Domain name. Enters the specified RF Domain context.<br>• all – Specifies all RF Domains. |

**Example**

```
nx9500-6C8809>on rf-domain TechPubs
nx9500-6C8809(TechPubs)>?
on RF-Domain Mode commands:

  clrscr   Clears the display screen
  do       Run commands from Exec mode
  end      End current mode and change to EXEC mode
  exit     End current mode and down to previous mode
  help     Description of the interactive help system
  service  Service Commands
  show     Show running system information

nx9500-6C8809(TechPubs)>

nx9500-6C8809(rf-domain-all)>?
on RF-Domain Mode commands:

  clrscr   Clears the display screen
  do       Run commands from Exec mode
  end      End current mode and change to EXEC mode
  exit     End current mode and down to previous mode
  help     Description of the interactive help system
  service  Service Commands
  show     Show running system information

nx9500-6C8809(rf-domain-all)>
```

## 2.1.23 opendns

*User Exec Commands*

Fetches the OpenDNS device_id from the OpenDNS site. Use this command to fetch the OpenDNS device_id. Once fetched, apply the device_id to WLANs that are to be OpenDNS enabled.

OpenDNS is a free DNS service that enables swift Web navigation without frequent outages. It is a reliable DNS service that provides the following services: DNS query resolution, Web-filtering, protection against virus and malware attacks, performance enhancement, etc.

This command is part of a set of configurations that are required to integrate WiNG devices with OpenDNS. When integrated, DNS queries going out of the WiNG device (access point, controller, or service platform) are re-directed to OpenDNS (208.67.220.220 or 208.67.222.222) resolvers that act as proxy DNS servers.

For more information on integrating WiNG devices with OpenDNS site, see *Enabling OpenDNS Support*.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
opendns [APIToken|username]

opendns APIToken <OPENDNS-APITOKEN>
opendns username <USERNAME> password <OPENDNS-PSWD> label <LABEL>

Note, as per the current implementation both of the above commands can be used to
fetch the device_id from the OpenDNS site.
```

**Parameters**

- `opendns APIToken <OPENDNS-APITOKEN>`

| | |
|---|---|
| opendns | Fetches the device_id from the OpenDNS site using the OpenDNS API token |
| APIToken <OPENDNS-APITOKEN> | Configures the OpenDNS APIToken. This is the token provided you by CISCO at the time of subscribing for their OpenDNS service.<br>• <OPENDNS-APITOKEN> – Provide the OpenDNS API token (should be a valid token).<br>For every valid OpenDNS API token provided a device_id is returned. Apply this device_id to WLANs that are to be OpenDNS enabled. Once applied, DNS queries originating from associating clients are appended with an additional 31 bytes of data (representing the device ID) at the end of the DNS packet. For information on configuring the device_id in the WLAN context, see *opendns*. |

- `opendns username <USERNAME> password <OPENDNS-PSWD> label <LABEL>`

| | |
|---|---|
| opendns | Fetches the device_id from the OpenDNS site using the OpenDNS credentials |
| username <USERNAME> | Configures the OpenDNS user name. This is your OpenDNS email ID provided by CISCO at the time of subscribing for their OpenDNS service.<br>• <USERNAME> – Provide the OpenDNS user name (should be a valid OpenDNS username). |

| | |
|---|---|
| password <OPENDNS-PSWD> | Configures the password associated with the user name specified in the previous step<br>• <OPENDNS-PSWD> – Provide the OpenDNS password (should be a valid OpenDNS password). |
| label <LABEL> | Configures the network label. This the label (the user friendly name) of your network, and should be the same as the label (name) configured on the OpenDNS portal.<br>• <LABEL> – Specify your network label.<br>For every set of user name, password, and label passed only one unique device_id is returned. Apply this device_id to WLANs that are to be OpenDNS enabled. Once applied, DNS queries originating from associating clients are appended with an additional 31 bytes of data (representing the device ID) at the end of the DNS packet. For information on configuring the device_id in the WLAN context, see *opendns*. |

**Usage Guidelines**

Use your OpenDNS credentials to logon to the *opendns.org* site and use the *labels*, *edit settings*, and *customize content filtering* options to configure Web filtering settings.

**Example**

```
ap7161-E6D512>opendns username bob@examplecompany.com password opendns label
company_name
Connecting to OpenDNS server...
device_id = 0014AADF8EDC6C59
ap7161-E6D512>

nx9600-7F3C7F>opendns ApiToken 9110B39543DEB2ECA1F473AE03E8899C00019073 device_id
= 001480fe36dcb245
nx9600-7F3C7F>
```

## 2.1.24 page

*User Exec Commands*

Toggles a device's paging function. When executed, this command enables the display of CLI command outputs page by page, instead of running the entire output at once.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602. AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
page
```

**Parameters**

None

**Example**

```
rfs4000-880DA7>page
rfs4000-880DA7>
```

**Related Commands**

| | |
|---|---|
| *no* | Disables device paging |

## 2.1.25 ping

*User Exec Commands*

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

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ping <IP/HOSTNAME> {count <1-10000>|dont-fragment {count|size}|size <1-64000>|
source [<IP>|pppoe|vlan <1-4094>|wwan]}
```

**Parameters**

```
• ping <IP/HOSTNAME> {count <1-10000>|dont-fragment {count|size}|size <1-64000>|
source[<IP>|pppoe|vlan <1-4094>|wwan]}
```

| | |
|---|---|
| <IP/HOSTNAME> | Specify the destination IP address or hostname. When entered without any parameters, this command prompts for an IP address or a hostname. |
| count <1-10000> | Optional. Sets the pings to the specified destination<br>• <1-10000> – Specify a value from 1 - 10000. The default is 5. |
| dont-fragment {count\|size} | Optional. Sets the don't fragment bit in the ping packet. Packets with the dont-fragment bit specified are not fragmented. When a packet, with the dont-fragment bit specified, exceeds the specified *maximum transmission unit* (MTU) value, an error message is sent from the device trying to fragment it.<br>• count <1-10000> – Optional. Sets the pings to the specified destination from 1 - 10000. The default is 5.<br>• size <1-64000> – Optional. Sets the ping payload size from 1 - 64000 bytes. The default is 100 bytes. |
| size <1-64000> | Optional. Sets the ping payload size in bytes<br>• <1-64000> – Specify the ping payload size from 1 - 64000. The default is 100 bytes. |
| source [<IP>\|pppoe\| vlan <1-4094>\| wwan] | Optional. Sets the source address or interface name. This is the source of the ICMP packet to the specified destination.<br>• <IP> – Specifies the source IP address<br>• pppoe – Selects the PPP over Ethernet interface<br>• vlan <1-4094> – Selects the VLAN interface from 1 - 4094<br>• wwan – Selects the wireless WAN interface |

**Example**

```
rfs6000-81742D>ping 192.168.13.13 count 4
PING 192.168.13.13 (192.168.13.13) 100(128) bytes of data.
108 bytes from 192.168.13.13: icmp_seq=1 ttl=64 time=0.291 ms
108 bytes from 192.168.13.13: icmp_seq=2 ttl=64 time=0.243 ms
108 bytes from 192.168.13.13: icmp_seq=3 ttl=64 time=0.239 ms
108 bytes from 192.168.13.13: icmp_seq=4 ttl=64 time=0.232 ms

--- 192.168.13.13 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 0.232/0.251/0.291/0.025 ms
rfs6000-81742D>

rfs6000-81742D>ping 10.233.89.182 source vlan 1
PING 10.233.89.182 (10.233.89.182) from 192.168.13.24 vlan1: 100(128) bytes of
data.
From 192.168.13.2 icmp_seq=1 Packet filtered
From 192.168.13.2 icmp_seq=2 Packet filtered
From 192.168.13.2 icmp_seq=3 Packet filtered
From 192.168.13.2 icmp_seq=4 Packet filtered
From 192.168.13.2 icmp_seq=5 Packet filtered

--- 10.233.89.182 ping statistics ---
5 packets transmitted, 0 received, +5 errors, 100% packet loss, time 3997ms

rfs6000-81742D>>
```

## 2.1.26 ping6

*User Exec Commands*

Sends ICMPv6 echo messages to a user-specified IPv6 address

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ping6 <IPv6/HOSTNAME> {<INTF-NAME>} {(count <1-10000>|size <1-64000>)}
```

**Parameters**

- `ping <IPv6/HOSTNAME> {<INTF-NAME>} {(count <1-10000>|size <1-64000>)}`

| | |
|---|---|
| <IPv6/HOSTNAME> | Specify the destination IPv6 address or hostname. |
| <INTF-NAME> | Specify the interface name for link local/broadcast address |
| count <1-10000> | Optional. Sets the pings to the specified IPv6 destination<br>• <1-10000> – Specify a value from 1 - 10000. The default is 5. |
| size <1-64000> | Optional. Sets the IPv6 ping payload size in bytes<br>• <1-64000> – Specify the ping payload size from 1 - 64000. The default is 100 bytes. |

**Usage Guidelines**

To configure a device's IPv6 address, in the VLAN interface configuration mode, use the *ipv6 > address <IPv6-ADDRESS> command.* After configuring the IPv6 address, use the *ipv6 > enable* command to enable IPv6. For more information, see *ipv6*.

**Example**

```
rfs4000-1B3596(config-device-00-23-68-1B-35-96-if-ge4)#show ipv6 interface brief
------------------------------------------------------------------------------
INTERFACE  IPV6 MODE  IPV6-ADDRESS/MASK              TYPE         STATUS  PROTOCOL
------------------------------------------------------------------------------
vlan1       True      fe80::223:68ff:fe88:da7/64     Link-Local       UP      up
vlan1       True      2001:10:10:10:10:10:10:1/64  Global-Permanent   UP      up
vlan2       False     UNASSIGNED                       None           UP      up
------------------------------------------------------------------------------
rfs4000-1B3596(config-device-00-23-68-1B-35-96-if-ge4)#

rfs4000-229D58>ping6 2001:10:10:10:10:10:10:1 count 6
PING 2001:10:10:10:10:10:10:1(2001:10:10:10:10:10:10:1) 100 data bytes
108 bytes from 2001:10:10:10:10:10:10:1: icmp_seq=1 ttl=64 time=0.401 ms
108 bytes from 2001:10:10:10:10:10:10:1: icmp_seq=2 ttl=64 time=0.311 ms
108 bytes from 2001:10:10:10:10:10:10:1: icmp_seq=3 ttl=64 time=0.300 ms
108 bytes from 2001:10:10:10:10:10:10:1: icmp_seq=4 ttl=64 time=0.309 ms
108 bytes from 2001:10:10:10:10:10:10:1: icmp_seq=5 ttl=64 time=0.299 ms
108 bytes from 2001:10:10:10:10:10:10:1: icmp_seq=6 ttl=64 time=0.313 ms

--- 2001:10:10:10:10:10:10:1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 6999ms
rtt min/avg/max/mdev = 0.299/0.318/0.401/0.031 ms
rfs4000-229D58>
```

## 2.1.27 ssh

*User Exec Commands*

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

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ssh <IP/HOSTNAME> <USER-NAME> {<INF-NAME/LINK-LOCAL-ADD>}
```

**Parameters**

- `ssh <IP/HOSTNAME> <USER-NAME> {<INF-NAME/LINK-LOCAL-ADD>}`

| | |
|---|---|
| <IP/HOSTNAME> | Specify the remote system's IP address or hostname. |
| <USERNAME> | Specify the name of the user requesting SSH connection with the remote system. |
| <INF-NAME/ LINK-LOCAL-ADD> | Optional. Specify the interface's name or link local address. |

**Example**

```
nx9500-6C8809>ssh 192.168.13.24 admin
admin@192.168.13.24's password:
rfs6000-81742D>
```

## 2.1.28 telnet

*User Exec Commands*

Opens a Telnet session between two network devices

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

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

**Parameters**

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

| | |
|---|---|
| <IP/HOSTNAME> | Configures the destination remote system's IP (IPv4 or IPv6) address or hostname. The Telnet session is established between the connecting system and the remote system.<br>• <IP/HOSTNAME> – Specify the remote system's IPv4 or IPv6 address or hostname. |
| <TCP-PORT> | Optional. Specify the *Transmission Control Protocol* (TCP) port number. |
| <INTF-NAME> | Optional. Specify the interface name for the link local address. |

**Example**

```
nx9500-6C8809#telnet 192.168.13.10

Entering character mode
Escape character is '^]'.

Welcome to Microsoft Telnet Service

login:
```

## 2.1.29 terminal

*User Exec Commands*

Sets the length and width of the CLI display window on a terminal

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

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

**Parameters**

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

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

**Example**

```
rfs6000-81742D>terminal length 150

rfs6000-81742D>terminal width 215

rfs6000-81742D>show terminal
Terminal Type: xterm
Length: 150     Width: 215
rfs6000-81742D>
```

**Related Commands**

| | |
|---|---|
| *no* | Resets the width or length of the terminal window |

## 2.1.30 time-it

*User Exec Commands*

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

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

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

**Parameters**

- `time-it <COMMAND>`

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

**Example**

```
rfs6000-81742D>time-it enable
That took 0.00 seconds..
rfs6000-81742D#
```

## 2.1.31 traceroute

*User Exec Commands*

Traces the route to a defined destination

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

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
traceroute <LINE>
```

**Parameters**

- `traceroute <LINE>`

| | |
|---|---|
| traceroute <LINE> | Traces the route to a destination IP address or hostname<br>• <LINE> – Specify the destination IPv6 address or hostname. |

**Example**

```
rfs6000-81742D>traceroute --help
BusyBox v1.14.4 () multi-call binary

Usage: traceroute [-FIldnrv] [-f 1st_ttl] [-m max_ttl] [-p port#] [-q nqueries]
        [-s src_addr] [-t tos] [-w wait] [-g gateway] [-i iface]
        [-z pausemsecs] HOST [data size]Options:
        -F      Set the don't fragment bit
        -I      Use ICMP ECHO instead of UDP datagrams
        -l      Display the ttl value of the returned packet
        -d      Set SO_DEBUG options to socket
        -n      Print hop addresses numerically rather than symbolically
        -r      Bypass the normal routing tables and send directly to a host
        -v      Verbose
        -m max_ttl      Max time-to-live (max number of hops)
        -p port#        Base UDP port number used in probes
                        (default is 33434)
        -q nqueries     Number of probes per 'ttl' (default 3)
        -s src_addr     IP address to use as the source address
        -t tos          Type-of-service in probe packets (default 0)
        -w wait         Time in seconds to wait for a response
                        (default 3 sec)
        -g              Loose source route gateway (8 max)

rfs6000-81742D>

rfs6000-81742D>traceroute 192.168.13.13
traceroute to 192.168.13.13 (192.168.13.13), 30 hops max, 38 byte packets
 1  192.168.13.13 (192.168.13.13)  1.150 ms  0.261 ms  0.214 ms
rfs6000-81742D>
```

## 2.1.32 traceroute6

*User Exec Commands*

Traces the route to a specified IPv6 destination

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
traceroute6 <LINE>
```

**Parameters**

- `traceroute6 <LINE>`

| | |
|---|---|
| traceroute6 <LINE> | Traces the route to a destination IPv6 address or hostname<br>• <LINE> – Specify the destination IPv6 address or hostname. |

**Example**

```
rfs6000-81742D>traceroute6 2001:10:10:10:10:10:10:1
traceroute to 2001:10:10:10:10:10:10:1 (2001:10:10:10:10:10:10:1) from
2001:10:10:10:10:10:10:2, 30 hops max, 16 byte packets
 1  2001:10:10:10:10:10:10:1 (2001:10:10:10:10:10:10:1)  6.054 ms  0.448 ms  0.555
ms
rfs6000-81742D>
```

## 2.1.33 virtual-machine

*User Exec Commands*

Installs, configures, and monitors the status of virtual machines (VMs) installed on a WiNG controller

**Supported in the following platforms:**

- Service Platforms — NX9500, NX9510, NX9600, VX9000

**Syntax**

```
virtual-machine [assign-usb-ports|export|install|restart|set|start|stop|
uninstall]

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

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

virtual-machine install [<VM-NAME>|adsp|team-urc|team-rls|team-vowlan]
{on <DEVICE-NAME>}

virtual-machine restart [<VM-NAME>|hard|team-urc|team-rls|team-vowlan]

virtual-machine set [autostart|memory|vcpus|vif-count|vif-mac|vif-to-vmif|vnc]

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

The following virtual-machine commands are supported only on the VX9000 platform:

virtual-machine volume-group [add-drive|replace-drive|resize-drive|resize-volume-
group]

virtual-machine volume-group [add-drive|replace-drive] <BLOCK-DEVICE-LABEL>

virtual-machine volume-group replace-drive <BLOCK-DEVICE-LABLE> <NEW-BLOCK-
DEVICE-LABEL>

virtual-machine volume-group resize-volume-group <BLOCK-DEVICE-LABEL>
```

**Parameters**

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

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

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

| | |
|---|---|
| virtual-machine export | Exports an existing VM image and settings. Use this command to export the VM to another <NX54XX> or <NX65XX> device in the same domain.<br>• <VM-NAME> – Specify the VM name.<br>• <FILE> – Specify the location and name of the source file (VM image). The VM image is retrieved and exported from the specified location.<br>• <URL> – Specify the destination location. This is the location to which the VM image is copied. Use one of the following formats to provide the destination path:<br>Contd.. |

| | |
|---|---|
| | tftp://<hostname\|IP>[:port]/path/file<br>ftp://<user>:<passwd>@<hostname\|IP>[:port]/path/file<br>sftp://<user>:<passwd>@<hostname\|IP>[:port]>/path/file<br>http://<hostname\|IP>[:port]/path/file<br>• on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices<br>• <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas.<br>Note: The VM should be in a stop state during the export process.<br>Note: If the destination is a device, the image is copied to a predefined location (VM archive). |

• `virtual-machine install [<VM-NAME>|adsp|team-centro|team-rls|team-vowlan] {on <DEVICE-NAME>}`

| | |
|---|---|
| virtual-machine install | Installs the VM. The install command internally creates a VM template, consisting of the specified parameters, and starts the installation process. Select one of the following options:<br>• <VM-NAME> – Installs a VM having name specified by <VM-NAME> keyword.<br>• adsp – Installs ADSP<br>• team-centro – Installs the VM TEAM-Centro image<br>• team-rls – Installs the VM TEAM-RLS image<br>• team-vowlan – Installs the VM TEAM-VoWLAN image<br>Specify the device on which to install the VM.<br>• on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices<br>• <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas. |

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

| | |
|---|---|
| virtual-machine set | Configures the VM settings<br>• autostart – Specifies whether to autostart the VM on system reboot<br>• ignore – Enables autostart on each system reboot<br>• start – Disables autostart<br>• memory – Defines the VM memory size<br>• <512-8192> – Specify the VM memory from 512 - 8192 MB. The default is 1024 MB.<br>• vcpus – Specifies the number of VCPUS for this VM<br>• <1-4> – Specify the number of VCPUS from 1- 4.<br>• vif-count – Configures or resets the VM's VIFs<br>• <0-2> – Specify the VIF number from 0 - 2.<br>• vif-mac – Configures the MAC address of the selected virtual network interface<br>• <1-2> – Select the VIF<br>• <1-8> – Specify the MAC index for the selected VIF<br>• <MAC> – Specify the customized MAC address for the selected VIF in the AA-BB-CC-DD-EE-FF format.<br>Contd.. |

| | |
|---|---|
| | Each VM has a maximum of two network interfaces (indexed 1 and 2, referred to as VIF). By default, each VIF is automatically assigned a MAC from the range allocated for that device. However, you can use the 'set' keyword to specify the MAC from within the allocated range. Each of these VIFs are mapped to a layer 2 port in the dataplane (referred to as VMIF). These VMIFs are standard l2 ports on the DP bridge, supporting all VLAN and ACL commands. The WiNG software supports up to a maximum of 8 VMIFs. By default, a VM's interface is always mapped to VMIF1. You can map a VIF to any of the 8 VMIFs. Use the vif-to-vmif command to map a VIF to a VMIF on the DP bridge.<br>• vif-to-vmif – Maps the virtual interface (1 or 2) to the selected VMIF interface. Specify the VMIF interface index from 1 - 8.<br>WiNG provides a dataplane bridge for external network connectivity for VMs. VM Interfaces define which IP address is associated with each VLAN ID the service platform is connected to and enables remote service platform administration. Each custom VM can have up to a maximum of two VM interfaces. Each VM interface can be mapped to one of the twelve ports for <NX9500> on the dataplane bridge. This mapping determines the destination for service platform routing.<br>By default, VM interfaces are internally connected to the dataplane bridge via VMIF1. VMIF1, by default, is an untagged port providing access to VLAN 1 to support the capability to connect the VM interfaces to any of the VMIF ports. This provides the flexibility to move a VM interface onto different VLANs as well as configure specific firewall and QoS rules.<br>• vnc – Disables/enables VNC port option for an existing VM. When enabled, provides remote access to VGA through the noVNC client.<br>• disable – Disables VNC port<br>• enable – Enables VNC port<br>After configuring the VM settings, identify the VM to apply the settings.<br>• <VM-NAME> – Applies these settings to the VM identified by the <VM-NAME> keyword. Specify the VM name.<br>• adsp – Applies these settings to the ADSP VM<br>• team-urc – Applies these settings to the VM TEAM-URC<br>• team-rls – Applies these settings to the VM TEAM-RLS<br>• team-vowlan – Applies these settings to the VM TEAM-VoWLAN |

`• virtual-machine start [<VM-NAME>|adsp|team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}`

| | |
|---|---|
| virtual-machine start | Starts the VM, based on the parameters passed. Select one of the following options:<br>• <VM-NAME> – Starts the VM identified by the <VM-NAME> keyword. Specify the VM name.<br>• adsp – Starts the ADSP VM<br>• team-urc – Starts the VM TEAM-URC<br>• team-rls – Starts the VM TEAM-RLS<br>• team-vowlan – Starts the VM TEAM-VoWLAN<br>The following keywords are common to all of the above parameters:<br>• on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices<br>• <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas. |

- `virtual-machine stop [<VM-NAME>|adsp|team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}`

| | |
|---|---|
| virtual-machine stop hard | Stops the VM, based on the parameters passed. Select one of the following options:<br>• <VM-NAME> – Stops the VM identified by the <VM-NAME> keyword. Specify the VM name.<br>• ADSP – Stops the ADSP VM<br>• team-urc – Stops the VM TEAM-URC<br>• team-rls – Stops the VM TEAM-RLS<br>• team-vowlan – Stops the VM TEAM-VoWLAN<br>The following keywords are common to all of the above parameters:<br>• on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices<br>• <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas.<br>Note: The option 'hard' forces the selected VM to shutdown. |

- `virtual-machine uninstall [<VM-NAME>|adsp|team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}`

| | |
|---|---|
| virtual-machine uninstall | Uninstalls the specified VM<br>• <VM-NAME> – Uninstalls the VM identified by the <VM-NAME> keyword. Specify the VM name.<br>• ADSP – Uninstalls the ADSP VM<br>• team-urc – Uninstalls the VM TEAM-URC<br>• team-rls – Uninstalls the VM TEAM-RLS<br>• team-vowlan – Uninstalls the VM TEAM-VoWLAN<br>The following keywords are common to all of the above parameters:<br>• on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices<br>• <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas.<br>Note: This command releases the VM's resources, such as memory, VCPUS, VNC port, disk space, and removes the RF Domain reference from the system. |

- `virtual-machine volume-group [add-drive|resize-drive] <BLOCK-DEVICE-LABEL>]`

| | |
|---|---|
| virtual-machine volume-group [add-drive\|resize-drive] <BLOCK-DEVICE-LABEL>] | Enables provisioning of logical volume-groups on the VX9000 platform. Logical volume-groups are created on the primary storage device, allowing the database storage to be expanded to include additional storage drives. However, volume-groups can be provisioned only on new VX9000 installation and cannot be added to existing VX9000 installation.<br>**Note:** The logical volume-group is supported only on a VX9000 running the WiNG 5.9.1 image.<br>• add-drive – Adds a new block-device to the VM. Note, currently a maximum of 3 (three) block devices can be added. To add a new drive, first halt the VM, In the Hypervisor, add a new storage disk to the VM and restart the VM. Once the VM comes up, use this command to add the new drive. To identify the new drive execute the *show > virtual-machine > volume-group > status* command. |

| | |
|---|---|
| | • resize-drive - Resizes a drive in the VM's volume group. To increase the size of a drive in the volume-group, first halt the VM. In the Hypervisor, increase the size of the existing secondary storage drive and restart the VM. Once the VM comes up, use this command to resize the drive. To identify the drive with the additional free space, execute the *show > virtual-machine > volume-group > status* command.<br>The following keyword is common to all of the above parameters:<br>• <BLOCK-DEVICE-LABEL> –Specify the block-device label to be added or resized depending on the action being performed. |

```
• virtual-machine volume-group replace-drive <BLOCK-DEVICE-LABEL> <NEW-BLOCK-
DEVICE-LABEL>]
```

| | |
|---|---|
| virtual-machine volume-group replace-drive <BLOCK-DEVICE-LABEL> <NEW-BLOCK-DEVICE-LABEL>] | Enables provisioning of VMs as logical volume-groups on the VX9000 platform. Logical volume-group VMs are created on the primary storage device, allowing the database storage to be expanded to include additional storage drives.<br>• replace-drive – Replaces an existing block-device with a new block-device in a volume-group. To replace a drive in the volume-group, first halt the VM. In the Hypervisor, add the new drive and restart the VM. Once the VM comes up, use this command to replace an existing drive with the new drive. To identify the drive with the additional free space, execute the *show > virtual-machine > volume-group > status* command<br>• <BLOCK-DEVICE-LABEL> –Specify the block-device label to be replaced.<br>• <BLOCK-DEVICE-LABEL> – Specify the replacement block-device label. |

```
• virtual-machine volume-group resize-volume-group <BLOCK-DEVICE-LABEL>]
```

| | |
|---|---|
| virtual-machine volume-group resize-volume-group <BLOCK-DEVICE-LABEL>] | Enables provisioning of VMs as logical volume-groups on the VX9000 platform. Logical volume-group VMs are created on the primary storage device, allowing the database storage to be expanded to include additional storage drives<br>• resize-volume-group – Adds drive space to an existing block-device in the volume-group<br>• <BLOCK-DEVICE-LABEL> –Specify the block-device label to which additional drive space is to be provided |

**Example**

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

Insatllation media: USB

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

Installation media: pre-installed disk image

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

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

Installation media: VM archive

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

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

**Exporting an installed VM:**

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

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

```
<exsw6>>virtual-machine install team-urc
Virtual Machine install team-urc command successfully sent.
<exsw6>>

vx9000-DE6F97>cirtual-machine add-drive sdb

vx9000-DE6F97>show virtual-machine volume-group status
----------------------------------------
Logical Volume: lv1
----------------------------------------
 STATUS           : available
 SIZE             : 81.89 GiB
 VOLUME GROUP     : vg0
 PHYSICAL VOLUMES :
     sda10        : 73.90 GiB
     sdc1         : 8.00 GiB
 AVAILABLE DISKS  :
     sdb          : size: 8590MB
----------------------------------------
* indicates a drive that must be resized
----------------------------------------
vx9000-DE6F97>
```

## 2.1.34 watch

*User Exec Commands*

Repeats the specified CLI command at periodic intervals

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

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

**Parameters**

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

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

**Example**

```
rfs6000-81742D>watch 40 ping 192.168.13.13
PING 192.168.13.13 (192.168.13.13) 100(128) bytes of data.
108 bytes from 192.168.13.13: icmp_seq=1 ttl=64 time=0.335 ms
108 bytes from 192.168.13.13: icmp_seq=2 ttl=64 time=0.217 ms
108 bytes from 192.168.13.13: icmp_seq=3 ttl=64 time=0.209 ms
108 bytes from 192.168.13.13: icmp_seq=4 ttl=64 time=0.202 ms
108 bytes from 192.168.13.13: icmp_seq=5 ttl=64 time=0.235 ms

--- 192.168.13.13 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.202/0.239/0.335/0.051 ms

rfs6000-81742D>
```

## 2.1.35 exit

*User Exec Commands*

Ends the current CLI session and closes the session window

For more information, see *exit*.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
exit
```

**Parameters**

None

**Example**

```
rfs6000-81742D>exit
```

# 3 PRIVILEGED EXEC MODE COMMANDS

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

**NOTE:** To password-protect the Privilege mode, in the Management Policy, configure the privilege-mode-password. For more information, see *privilege-mode-password*.

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

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

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

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

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

```
<DEVICE>#?
Privileged command commands:
  archive                       Manage archive files
  boot                          Boot commands
  captive-portal-page-upload    Captive portal internal and advanced page upload
  cd                            Change current directory
  change-passwd                 Change password
  clear                         Clear
  clock                         Configure software system clock
  cluster                       Cluster commands
  commit                        Commit all changes made in this session
  configure                     Enter configuration mode
  connect                       Open a console connection to a remote device
  copy                          Copy contents of one dir to another
  cpe                           T5 CPE configuration
  create-cluster                Create a cluster
  crypto                        Encryption related commands
  crypto-cmp-cert-update        Update the cmp certs
  database                      Database
  database-backup               Backup database
  database-restore              Restore database
  debug                         Debugging functions
  delete                        Deletes specified file from the system
  device-upgrade                Device firmware upgrade
  diff                          Display differences between two files
  dir                           List files on a filesystem
  disable                       Turn off privileged mode command
  edit                          Edit a text file
  enable                        Turn on privileged mode command
  erase                         Erase a filesystem
  ex3500                        EX3500 commands
  factory-reset                 Delete startup configuration on device(s),
                                reload the device(s) and remove configuration
                                entry from the controller
  file-sync                     File sync between controller and adoptees
  format                        Format file system
```

```
  halt                          Halt the system
  help                          Description of the interactive help system
  join-cluster                  Join the cluster
  l2tpv3                        L2tpv3 protocol
  logging                       Modify message logging facilities
  mint                          MiNT protocol
  mkdir                         Create a directory
  more                          Display the contents of a file
  no                            Negate a command or set its defaults
  on                            On RF-Domain
  opendns                       Opendns username/password configuration
  page                          Toggle paging
  ping                          Send ICMP echo messages
  ping6                         Send ICMPv6 echo messages
  pwd                           Display current directory
  raid                          RAID operations
  re-elect                      Perform re-election
  reload                        Halt and perform a warm reboot
  remote-debug                  Troubleshoot remote system(s)
  rename                        Rename a file
  revert                        Revert changes
  rmdir                         Delete a directory
  self                          Config context of the device currently logged
                                into
  service                       Service Commands
  show                          Show running system information
  ssh                           Open an ssh connection
  t5                            T5 commands
  telnet                        Open a telnet connection
  terminal                      Set terminal line parameters
  time-it                       Check how long a particular command took between
                                request and completion of response
  traceroute                    Trace route to destination
  traceroute6                   Trace route to destination(IPv6)
  upgrade                       Upgrade software image
  upgrade-abort                 Abort an ongoing upgrade
  virtual-machine               Virtual Machine
  watch                         Repeat the specific CLI command at a periodic
                                interval
  write                         Write running configuration to memory or
                                terminal

  clrscr                        Clears the display screen
  exit                          Exit from the CLI

<DEVICE>#
```

**NOTE:** The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (_) character.

# 3.1 Privileged Exec Mode Commands

- *PRIVILEGED EXEC MODE COMMANDS*

The following table summarizes the PRIV EXEC Mode commands:

**Table 3.1** *Privileged Exec Commands*

| Command | Description | Reference |
|---|---|---|
| *archive* | Manages file archive operations | *page 3-6* |
| *boot* | Specifies the boot partition (primary or secondary). The device uses the image stored in the specified partition to boot. | *page 3-8* |
| *captive-portal-page-upload* | Uploads captive portal advanced pages to adopted access points | *page 3-9* |
| *cd* | Changes the current directory | *page 3-13* |
| *change-passwd* | Changes the password of a logged user | *page 3-14* |
| *clear* | Clears parameters, cache entries, table entries, and other similar entries | *page 3-15* |
| *clock* | Configures the system clock | *page 3-28* |
| *cluster* | Initiates a cluster context | *page 3-29* |
| *configure* | Enters the global configuration mode | *page 3-30* |
| *connect* | Begins a console connection to a remote device | *page 3-31* |
| *copy* | Copies a file from any location to the wireless controller, service platform, or access point | *page 3-32* |
| *cpe* | Enables adopted T5 *Customer Premises Equipment* (CPE) device(s) management. Use this command to perform the following operations on the CPEs: boot, reload, upgrade. This command is specific to the RFS4000, RFS6000, and NX9500 devices. | *page 3-33* |
| *create-cluster* | Creates a new cluster on a specified device | *page 3-35* |
| *crypto* | Enables encryption | *page 3-37* |
| *crypto-cmp-cert-update* | Triggers a CMP certificate update on a specified device or devices | *page 3-46* |
| *database* | Enables automatic repairing (vacuuming) and dropping of databases (Captive-portal and NSight) | *page 3-47* |
| *database-backup* | Backs up captive-portal and/or NSight database to a specified location and file on an FTP or SFTP server | *page 3-50* |
| *database-restore* | Restores a previously exported database [captive-portal and/or NSight]. Previously exported databases (backed up to a specified FTP or SFTP server) are restored to the original database. | *page 3-52* |
| *delete* | Deletes a specified file from the system | *page 3-53* |
| *device-upgrade* | Configures device firmware upgrade parameters | *page 3-54* |
| *diff* | Displays the differences between two files | *page 3-60* |
| *dir* | Displays the list of files on a file system | *page 3-61* |
| *disable* | Disables the privileged mode command set | *page 3-62* |
| *edit* | Enables ext file editing | *page 3-63* |

**Table 3.1** *Privileged Exec Commands*

| Command | Description | Reference |
|---|---|---|
| *enable* | Turns on (enables) the privileged mode commands set | *page 3-64* |
| *erase* | Erases a file system | *page 3-65* |
| *ex3500* | Enables EX3500 switch firmware management. Use this command to perform the following operations: boot, copy, delete, and IP related configurations. | *page 3-67* |
| *factory-reset* | Erases startup configuration on a specified device or all devices within a specified RF Domain | *page 3-75* |
| *file-sync* | Configures parameters enabling syncing of PKCS#12 and wireless-bridge certificate between the staging-controller and adopted access points | *page 3-79* |
| *halt* | Halts a device (access point, wireless controller, or service platform) | *page 3-82* |
| *join-cluster* | Adds a device (access point, wireless controller, or service platform), as cluster member, to an existing cluster of devices | *page 3-83* |
| *l2tpv3* | Establishes or brings down *Layer 2 Tunneling Protocol Version* 3 (L2TPV3) tunnels | *page 3-85* |
| *logging* | Modifies message logging parameters | *page 3-87* |
| *mint* | Configures MiNT protocols | *page 3-89* |
| *mkdir* | Creates a new directory in the file system | *page 3-91* |
| *more* | Displays the contents of a file | *page 3-92* |
| *no* | Reverts a command or sets values to their default | *page 3-93* |
| *on* | Executes the following commands in the RF Domain context: clrscr, do, end, exit, help, service, show | *page 3-95* |
| *opendns* | Connects to the OpenDNS site using OpenDNS registered credentials (username, password) OR OpenDNS API token to fetch the OpenDNS device_id. This command is a part of the process integrating access points, controllers, and service platforms with OpenDNS. | *page 3-96* |
| *page* | Toggles a device's (access point, wireless controller, or service platform) paging function | *page 3-100* |
| *ping* | Sends ICMP echo messages to a user-specified location | *page 3-101* |
| *ping6* | Sends ICMPv6 echo messages to a user-specified location | *page 3-103* |
| *pwd* | Displays the current directory | *page 3-104* |
| *re-elect* | Re-elects the tunnel controller (wireless controller, service platform, or access point) | *page 3-105* |
| *reload* | Halts a device (wireless controller, service platform, or access point) and performs a warm reboot | *page 3-106* |
| *rename* | Renames a file in the existing file system | *page 3-111* |
| *rmdir* | Deletes an existing file from the file system | *page 3-112* |
| *self* | Displays the configuration context of the device | *page 3-113* |
| *ssh* | Connects to another device using a secure shell | *page 3-114* |
| *t5* | Executes the following operations on a T5 device: copy, rename, delete, and write. This command is specific to the RFS4000, RFS6000, NX9500 devices. | *page 3-115* |

**Table 3.1** *Privileged Exec Commands*

| Command | Description | Reference |
|---|---|---|
| *telnet* | Opens a Telnet session | *page 3-117* |
| *terminal* | Sets the length and width of the terminal window | *page 3-118* |
| *time-it* | Verifies the time taken by a particular command between request and response | *page 3-119* |
| *traceroute* | Traces the route to a defined destination | *page 3-120* |
| *traceroute6* | Sends ICMPv6 echo messages to a user-specified location | *page 3-121* |
| *upgrade* | Upgrades the logged device's software image | *page 3-122* |
| *upgrade-abort* | Aborts an ongoing software image upgrade | *page 3-126* |
| *virtual-machine* | Installs, configures, and monitors the status of virtual machines (VMs) installed on a WiNG controller | *page 3-127* |
| *watch* | Repeats a specified CLI command at a periodic interval | *page 3-133* |
| *raid* | Enables RAID management<br>This command is specific to the NX7530, NX9500, and NX9510 service platforms. | *page 3-135* |

**NOTE:** For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see *COMMON COMMANDS*.

**NOTE:** The input parameter <HOSTNAME>, if used in syntaxes across this chapter, cannot include an underscore (_) character.

## 3.1.1 archive

*Privileged Exec Mode Commands*

Manages file archive operations

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

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

**Parameters**

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

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

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

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

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

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

**Example**

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

```
nx9500-6C8809#dir flash:/
Directory of flash:/

 -rw-   62937      Tue Nov 24 16:00:06 2015   run-config-backup.txt
  drwx             Mon Apr  3 12:40:23 2017   crashinfo
  drwx             Wed Mar 22 13:58:28 2017   upgrade
  drwx             Mon Sep 28 09:48:33 2015   tmptpd
  drwx             Wed Apr  5 11:20:11 2017   log
  drwx             Thu Mar 30 15:07:54 2017   archived_logs
  drwx             Tue May 24 22:23:54 2016   cache
  drwx             Thu Feb 19 08:53:45 2015   floorplans
  -rw-   42018304  Tue Sep 27 10:19:24 2016   in.tar
  drwx             Tue Jan 17 10:02:01 2017   hotspot

nx9500-6C8809#

nx9500-6C8809#archive tar /create flash:/in.tar flash:/log/
log/nsightd.log.1
log/nsight_reportd.log
log/messages.1.log
log/martdb.log
log/reportd.log.2
log/adopts.log.2
log/mongod.log.2
log/dpd2.log
log/nsight_server.log
log/mart_websock_server.log
log/nuxi/
log/nuxi/beanyaml.log
log/nuxi/statsreqresp.1.log
log/nuxi/hadoop.log.2014-08-03
log/nuxi/puts.log
log/nuxi/copy2w.log
log/nuxi/obj2yaml.log
log/nuxi/infl.log

--More--

nx9500-6C8809#

nx9500-6C8809#dir flash:/
Directory of flash:/

  -rw-   62937      Tue Nov 24 16:00:06 2015   run-config-backup.txt
  drwx              Thu Sep 22 00:12:07 2016   crashinfo
  drwx              Sat Sep 17 05:14:43 2016   upgrade
  drwx              Mon Sep 28 09:48:33 2015   tmptpd
  drwx              Tue Sep 27 09:59:12 2016   log
  drwx              Mon Sep 26 09:58:54 2016   archived_logs
  drwx              Tue May 24 22:23:54 2016   cache
  drwx              Thu Feb 19 08:53:45 2015   floorplans
  -rw-   42018304   Tue Sep 27 10:19:24 2016   in.tar
  drwx              Mon Sep 15 03:40:02 2014   hotspot

nx9500-6C8809#
```

## 3.1.2 boot

*Privileged Exec Mode Commands*

Specifies the image used after reboot

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

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

**Parameters**

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

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

**Example**

```
nx9500-6C8809#show boot
------------------------------------------------------------------------------
     IMAGE            BUILD DATE              INSTALL DATE          VERSION
------------------------------------------------------------------------------
  Primary       03/26/2017 01:48:56     03/30/2017 15:02:18     5.9.0.0-012D
  Secondary     03/17/2017 13:13:38     03/22/2017 13:36:50     5.9.0.0-010D
------------------------------------------------------------------------------
Current Boot       : Primary
Next Boot          : Primary
Software Fallback  : Enabled
VM support         : Not present
nx9500-6C8809#

nx9500-6C8809#boot system secondary
Updated system boot partition
nx9500-6C8809#

nx9500-6C8809#show boot
------------------------------------------------------------------------------
     IMAGE            BUILD DATE              INSTALL DATE          VERSION
------------------------------------------------------------------------------
  Primary       03/26/2017 01:48:56     03/30/2017 15:02:18     5.9.0.0-012D
  Secondary     03/17/2017 13:13:38     03/22/2017 13:36:50     5.9.0.0-010D
------------------------------------------------------------------------------
Current Boot       : Primary
Next Boot          : Secondary
Software Fallback  : Enabled
VM support         : Not present
nx9500-6C8809#
```

## 3.1.3 captive-portal-page-upload

*Privileged Exec Mode Commands*

Uploads captive portal advanced pages to connected access points. Use this command to provide connected access points with specific captive portal configurations so they can successfully provision login, welcome, and condition pages to requesting clients attempting to access the wireless network using the captive portal.

**NOTE:** Ensure that the captive portal pages to be uploaded are *.tar files.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

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

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

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

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

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

captive-portal-page-upload delete-file <CAPTIVE-PORTAL-NAME> <FILE-NAME>

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

**Parameters**

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

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

| | |
|---|---|
| upload-time <TIME> | Optional. Schedules an upload time<br>• <TIME> – Specify upload time in the MM/DD/YYYY-HH:MM or HH:MM format.<br>The scheduled upload time is your local system's time. It is not the access point, controller, service platform, or virtual controller time and it is not synched with the device.<br>To view a list of uploaded captive portal files, execute the *show > captive-portal-page-upload > list-files* <CAPTIVE-PORTAL-NAME> command. |

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

| | |
|---|---|
| captive-portal-page-upload <CAPTIVE-PORTAL-NAME> | Uploads advanced pages specified by the <CAPTIVE-PORTAL-NAME> parameter<br>• <CAPTIVE-PORTAL-NAME> – Specify captive portal name (should be existing and configured). |
| rf-domain [<DOMAIN-NAME>\| all] | Uploads to all APs within a specified RF Domain or all RF Domains<br>• <DOMAIN-NAME> – Uploads to APs within a specified RF Domain. Specify the RF Domain name.<br>• all – Uploads to APs across all RF Domains |
| from-controller | Optional. Uploads to APs from the adopted device |
| upload-time <TIME> | Optional. Schedules an AP upload<br>• <TIME> – Specify upload time in the MM/DD/YYYY-HH:MM or HH:MM format.<br>The scheduled upload time is your local system's time. It is not the access point, controller, service platform, or virtual controller time and it is not synched with the device. |

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

| | |
|---|---|
| captive-portal-page-upload cancel-upload | Cancels a scheduled AP upload |
| cancel-upload [<MAC/ HOSTNAME>\|all\| on rf-domain [<DOMAIN-NAME>\| all]] | Select one of the following options:<br>• <MAC/HOSTNAME> – Cancels a scheduled upload to a specified AP. Specify the AP MAC address or hostname.<br>• all – Cancels all scheduled AP uploads<br>• on rf- domain – Cancels all scheduled uploads within a specified RF Domain or all RF Domains<br>• <DOMAIN-NAME> – Cancels scheduled uploads within a specified RF Domain. Specify RF Domain name.<br>• all – Cancels scheduled uploads across all RF Domains |

• `captive-portal-page-upload delete-file <CAPTIVE-PORTAL-NAME> <FILE-NAME>`

| | |
|---|---|
| captive-portal-page-upload delete-file | Deletes a specified captive portal's uploaded captive-portal internal page files |
| <CAPTIVE-PORTAL-NAME> <FILE-NAME> | Deletes a captive portal's, identified by the <CAPTIVE-PORTAL-NAME> keyword, uploaded internal page files<br>• <CAPTIVE-PORTAL-NAME> – Specify the captive portal's name.<br>• <FILE-NAME> – Specify the file name. The specified internal captive portal page is deleted. |

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

| | |
|---|---|
| captive-portal-page-upload load-file | Loads captive-portal advanced pages |
| <CAPTIVE-PORTAL-NAME> <URL> | Specify captive portal name (should be existing and configured) and location.<br>• <URL> – Specifies location of the captive-portal's advanced pages. Use one of the following formats:<br>IPv4 URLs:<br>tftp://<hostname\|IP>[:port]/path/file<br>ftp://<user>:<passwd>@<hostname\|IP>[:port]/path/file<br>sftp://<user>:<passwd>@<hostname\|IP>[:port]>/path/file<br>http://<hostname\|IP>[:port]/path/file<br>cf:/path/file<br>usb<n>:/path/file<br>IPv6 URLs:<br>tftp://<hostname\|[IPv6]>[:port]/path/file<br>ftp://<user>:<passwd>@<hostname\|[IPv6]>[:port]/path/file<br>sftp://<user>:<passwd>@<hostname\|[IPv6]>[:port]>/path/file<br>http://<hostname\|[IPv6]>[:port]/path/file<br>**Note:** The captive portal pages are downloaded to the controller from the location specified here. After downloading use the *captive-portal-page-upload> <CAPTIVE-PORTAL-NAME> > <DEVICE-OR-DOMAIN-NAME>* command to upload these pages to APs. |

**Example**

```
ap6562-B1A214#captive-portal-page-upload load-file captive_portal_test tftp://
89.89.89.17/pages_new_only.tar
ap6562-B1A214#

ap6562-B1A214#show captive-portal-page-upload load-image-status
Download of captive_portal_test advanced page file is complete
ap6562-B1A214#

ap6562-B1A214#captive-portal-page-upload captive_portal_test all
-------------------------------------------------------------------------------
         CONTROLLER             STATUS                   MESSAGE
-------------------------------------------------------------------------------
  FC-0A-81-B1-A2-14         Success         Added 6 APs to upload queue
-------------------------------------------------------------------------------
ap6562-B1A214#
```

```
ap6562-B1A214#show captive-portal-page-upload status
Number of APs currently being uploaded : 1
Number of APs waiting in queue to be uploaded : 0
-------------------------------------------------------------------------------
-------
   AP          STATE    UPLOAD TIME PROGRESS RETRIES LAST UPLOAD ERROR UPLOADED BY
-------------------------------------------------------------------------------
-------
  ap6562-B1A738   downloading   immediate   100      0       -                None
-------------------------------------------------------------------------------
-------
ap6562-B1A214#
```

The following example lists captive portal CP-BW uploaded files:

```
nx7500-7F2C13#show captive-portal-page-upload list-files CP-BW
-------------------------------------------------------------------------------
       NAME                    SIZE                LAST MODIFIED
-------------------------------------------------------------------------------
  CP-BW-1.tar.gz               6133              2017-05-16 10:38:40
  CP-BW.tar.gz                 3370              2017-05-16 10:45:44
-------------------------------------------------------------------------------
nx7500-7F2C13#
```

## 3.1.4 cd

*Privileged Exec Mode Commands*

Changes the current directory

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

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

**Parameters**

- `cd {<DIR>}`

| | |
|---|---|
| <DIR> | Optional. Changes the current directory to the directory identified by the <DIR> keyword. If a directory name is not provided, the system displays the current directory. |

**Example**

```
rfs6000-81742D#cd flash:/log/
rfs6000-81742D#pwd
flash:/log/
rfs6000-81742D#
```

## 3.1.5 change-passwd

*Privileged Exec Mode Commands*

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

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

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

**Parameters**

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

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

**Usage Guidelines**

A password must be from 1 - 64 characters in length.

**Example**

```
rfs6000-81742D#change-passwd
Enter old password:
Enter new password:
Password for user 'admin' changed successfully
Please write this password change to memory(write memory) to be persistent.
rfs6000-81742D#write memory
OK
rfs6000-81742D#
```

## 3.1.6 clear

*Privileged Exec Mode Commands*

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

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**NOTE:** When using the *clear* command, refer to the interface details provided in *interface*.

**Syntax**

```
clear [arp-cache|bonjour|cdp|counters|crypto|eguest|event-history|firewall|gre|
ip|ipv6|l2tpv3-stats|lacp|license|lldp|logging|mac-address-table|mint|role|rtls|
spanning-tree|traffic-shape|vrrp]

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

clear bonjour cache {on <DEVICE-NAME>}

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

clear counters [all|ap|bridge|interface|radio|router|thread|wireless-client]
clear counters [all|bridge|router|thread]

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

clear counters interface [<INTERFACE-NAME>|all|ge <1-X>|me1|port-channel <1-X>|
pppoe1|vlan <1-4094>|wwan1|xge <1-4>]

clear counters radio {<MAC/HOSTNAME>|on}

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

clear crypto [ike|ipsec]

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

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

clear eguest registration statistics

clear event-history

clear firewall [dhcp snoop-table|dos stats|flows [ipv4|ipv6]|neighbors snoop-
table] {on <DEVICE-NAME>}

clear gre stats {on <DEVICE-NAME>}

clear ip [bgp|dhcp|ospf]

clear ip bgp [<IP>|all|external|process]
```

```
clear ip bgp [<IP>|all|external] {in|on|out|soft}

clear ip bgp [<IP>|all|external] {in prefix-filter} {on <DEVICE-NAME>}

clear ip bgp [<IP>|all|external] {out} {(on <DEVICE-NAME>)}

clear ip bgp [<IP>|all|external] {soft {in|out}} {on <DEVICE-NAME>}

clear ip bgp process {on <DEVICE-NAME>}

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

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

clear ipv6 neighbor-cache {on <DEVICE-NAME>}

clear lacp [<1-4> counters|counters]

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

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

clear logging {on <DEVICE-NAME>}

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

clear mac-address-table mac-auth-state address <AMC> vlan <1-4094> {on <DEVICE-
NAME>}

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

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

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

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

clear rtls [aeroscout|ekahau]

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

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

clear spanning-tree detected-protocols {interface [<INTERFACE-NAME>|ge <1-x>|me1|
port-channel <1-x>|pppoe1|vlan <1-4094>|wwan1|xge <1-4>]} {on <DEVICE-NAME>}

clear traffic-shape statistics {class <1-4>} {(on <DEVICE-NAME>)}

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

The following clear command is specific to the NX95XX series service platforms:

```
clear logging analytics {on <DEVICE-NAME>}
```

**Parameters**

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

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

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

| | |
|---|---|
| bonjour cache | Clears all Bonjour cached statistics. Once cleared, the system has to re-discover available Bonjour services. |
| on <DEVICE-NAME> | Optional. Clears all Bonjour cached statistics on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

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

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

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

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

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

| | |
|---|---|
| counters [ap\|wireless-client] | Clears counters on a system<br>• ap – Clears access point wireless counters<br>• wireless-client – Clears wireless client counters |
| <MAC> | The following keyword is common to the 'ap' and 'wireless-client' parameters:<br>• <MAC> – Optional. Clears counters of the AP/wireless client identified by the <MAC> keyword. Specify the MAC address of the AP or wireless client.<br>The system clears all AP or wireless client counters, if no MAC address is specified. |

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

- `clear counters interface [<INTERFACE-NAME>|all|ge <1-X>|me1|port-channel <1-X>|pppoe1|vlan <1-4094>|wwan1|xge <1-4>]`

| | |
|---|---|
| counters interface [<INTERFACE-NAME>\|all\| ge <1-X>\|me1\| port-channel <1-X>\| pppoe1\|vlan <1-4094>\| wwan1\|xge <1-4>] | Clears interface counters for a specified interface<br>• <INTERFACE-NAME> – Clears a specified interface counters. Specify the interface name.<br>• all – Clears all interface counters<br>• ge <1-X> – Clears GigabitEthernet interface counters. Specify the GigabitEthernet interface index from 1 - X.<br>• me1 – Clears FastEthernet interface counters<br>• port-channel <1- X> – Clears port-channel interface counters. Specify the port channel interface index from 1 - X.<br>**Note:** The number of port-channel interfaces supported varies for different device types. For example, RFS4000 supports 3 port-channels.<br>• pppoe1 – Clears *Point-to-Point Protocol over Ethernet* (PPPoE) interface counters<br>• vlan <1-4094> – Clears interface counters. Specify the *Switch Virtual Interface* (SVI) VLAN ID from 1 - 4094.<br>• wwan1 – Clears wireless WAN interface counters<br>• xge <1-4> – Clears TenGigabitEthernet interface counters. Specify the GigabitEthernet interface index from 1 - 4. |

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

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

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

| | |
|---|---|
| crypto | Clears encryption module database |

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

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

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

- `clear eguest registration statistics`

| | |
|---|---|
| eguest registration statistics | Clears EGuest registration server counters. When cleared EGuest registration details are deleted, and the *show > eguest > registration > statistics* command output is null.<br>This command is applicable only on the NX95XX, NX9600, and the VX9000 model platforms. |

- `clear event-history`

| | |
|---|---|
| event-history | Clears event history cache entries |

- `clear firewall [dhcp snoop-table|dos stats|flows [ipv4|ipv6]|neighbors snoop-table]` *`{on <DEVICE-NAME>}`*

| | |
|---|---|
| firewall | Clears firewall event entries |
| dhcp snoop-table | Clears DHCP snoop table entries |
| dos stats | Clears denial of service statistics |
| flows [ipv4\|ipv6] | Clears established IPv4 or IPv6 firewall sessions |
| neighbors snoop-table | Clears IPv6 neighbors snoop-table entries |
| on <DEVICE-NAME> | The following keywords are common to the DHCP, DOS, and flows parameters:<br>• on <DEVICE-NAME> – Optional. Clears DHCP snoop table entries, denial of service statistics, or the established firewall sessions on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

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

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

- `clear ip bgp [<IP>|all|external] {in prefix-filter} {on <DEVICE-NAME>}`

| | |
|---|---|
| ip bgp [<IP>\|all\|external] | Clears BGP routing table information based on the option selected<br>• <IP> – Clears the BGP peer identified by the <IP> keyword. Specify the BGP peer's IP address.<br>• all – Clears Route Updates Received From All BGP Peers<br>• external – Clears route updates received from external BGP peers<br>This command is applicable only to the RFS4000, RFS6000, NX95XX, and NX9600 series service platforms.<br>In case of a change in routing policy it is necessary to clear BGP routing table entries in order for the new policy to take effect. |
| in prefix-filter | Optional. Clears soft-reconfiguration inbound route updates<br>• prefix-filter – Optional. Clears the existing *Outbound Route Filtering* (ORF) prefix-list. |
| on <DEVICE-NAME> | Optional. Clears soft-reconfiguration inbound route updates on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP or service platform. |

- `clear ip bgp [<IP>|all|external] {out} {(on <DEVICE-NAME>)}`

| | |
|---|---|
| ip bgp [<IP>\|all\|external] | Clears BGP routing table information based on the option selected<br>• <IP> – Clears the BGP peer identified by the <IP> keyword. Specify the BGP peer's IP address.<br>• all – Clears route updates received from all BGP peers<br>• external – Clears route updates received from external BGP peers<br>This command is applicable only to the RFS4000, RFS6000, and NX95XX series service platforms.<br>In case of a change in routing policy it is necessary to clear BGP routing table entries in order for the new policy to take effect. |
| out | Optional. Clears soft-reconfiguration outbound route updates. Optionally specify the device on which to execute this command. |
| on <DEVICE-NAME> | The following keyword is recursive and optional.<br>• on <DEVICE-NAME> – Optional. Clears BGP sessions on a specified device<br>  • <DEVICE-NAME> – Specify the name of the AP or service platform. |

- `clear ip bgp [<IP>|all|external] {soft {in|out}} {on <DEVICE-NAME>}`

| | |
|---|---|
| ip bgp [<IP>\|all\|external] | Clears BGP routing table information based on the option selected<br>• <IP> – Clears the BGP peer identified by the <IP> keyword. Specify the BGP peer's IP address.<br>• all – Clears route updates received from all BGP peers<br>• external – Clears route updates received from external BGP peers<br>This command is applicable only to the RFS4000, RFS6000, and NX95XX series service platforms.<br>In case of a change in routing policy it is necessary to clear BGP routing table entries in order for the new policy to take effect. |

| | |
|---|---|
| soft {in\|out} | Optional. Enables soft-reconfiguration of route updates for the specified IP address. This option allows routing tables to be reconfigured without clearing BGP sessions.<br>• in – Optional. Enables soft reconfiguration of inbound route updates<br>• out – Optional. Enables soft reconfiguration of outbound route updates<br>Modifications made to BGP settings (BGP access lists, weight, distance, route-maps, versions, routing policy, etc.) take effect only after on-going BGP sessions are cleared. The *clear > ip > bgp* command clears BGP sessions. To reduce loss of route updates during the process, use the 'soft' option. Soft reconfiguration stores inbound/outbound route updates to be processed later and updated to the routing table. This requires high memory usage. |
| on <DEVICE-NAME> | Optional. Clears soft-reconfiguration inbound/outbound route updates on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP or service platform. |

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

| | |
|---|---|
| ip bgp process | Clears all BGP processes running<br>This command is applicable only to the RFS4000, RFS6000, NX95XX, NX9600 platforms. |
| on <DEVICE-NAME> | Optional. Clears all BGP processes on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP or service platform. |

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

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

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

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

- `clear ipv6 neighbor-cache {on <DEVICE-NAME>}`

| | |
|---|---|
| clear ipv6 neighbor-cache | Clears IPv6 neighbor cache entries |
| on <DEVICE-NAME> | Optional. Clears IPv6 neighbor cache entries on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `clear lacp [<1-4> counters|counters]`

| | |
|---|---|
| clear lacp [<1-4> counters\| counters] | Clears *Link Aggregation Control Protocol* (LACP) counters for a specified port-channel group or all port-channel groups configured<br>• <1-4> counters – Clears LACP counters for a specified port-channel. Specify the port-channel index number from 1 - 4. Note, LACP is supported only on the NX5500, NX7500, and NX9500 model service platforms. However, the NX9500 series service platforms support only two (2) port-channels, and the other model service platforms support four (4) port-channels.<br>• counters – Clears LACP counters for all configured port-channels on the device |

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

| | |
|---|---|
| l2tpv3-stats | Clears L2TPv3 tunnel session statistics |
| tunnel <L2TPV3-TUNNEL-NAME> | Clears all sessions associated with a specified L2TPv3 tunnel<br>• <L2TPV3-TUNNEL-NAME> – Specify the L2TPv3 tunnel name. |
| session <SESSION-NAME> | Optional. Clears a specified L2TPv3 tunnel session, identified by the <SESSION-NAME> keyword<br>• <SESSION-NAME> – Specify the session name. |
| on <DEVICE-NAME> | The following parameter is recursive and optional:<br>• on <DEVICE-NAME> – Optional. Specifies the device running the L2TPv3 tunnel session<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.<br>If no optional parameters are specified, the system clears all L2TPv3 tunnel session statistics. |

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

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

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

| | |
|---|---|
| license lent | NOC controller releases or revokes all licenses loaned to a site controller |
| to <DEVICE-NAME> | Specifies the borrowing controller's name<br>• <DEVICE-NAME> – Specify the controller's name. |

| | |
|---|---|
| on <DEVICE-NAME> | Optional. Specifies the controller's name<br>• <DEVICE-NAME> – Specify the wireless controller's name.<br>If no device name is specified, the system clears all loaned licenses on the logged device. |

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

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

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

| | |
|---|---|
| mac-address-table | Clears the MAC address forwarding table |
| interface | Clears all MAC addresses for the selected interface. Use the options available to specify the interface. |
| <IF-NAME> | Clears MAC address forwarding table for the specified layer 2 interface (Ethernet port)<br>• <IF-NAME> – Specify the layer 2 interface name. |
| ge <1-X> | Clears MAC address forwarding table for the specified GigabitEthernet interface<br>• <1-X> – Specify the GigabitEthernet interface index from 1 - X. |
| port-channel <1-X> | Clears MAC address forwarding table for the specified port-channel interface<br>• <1-X> – Specify the port-channel interface index from 1 - X. |
| up <1-X> | Clears MAC address forwarding table for the WAN Ethernet interface<br>The number of WAN Ethernet interfaces supported varies for different devices. The RFS4000 and RFS6000 devices support 1 WAN Ethernet interface. |
| xge <1-4> | Clears MAC address forwarding table for the specified TenGigabitEthernet interface<br>• <1-4> – Specify the GigabitEthernet interface index from 1 - 4. |
| on <DEVICE-NAME> | Optional. Clears the MAC address forwarding table, for the selected interface, on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `clear mac-address-table mac-auth-state address <MAC> vlan <1-4904> {on <DEVICE-NAME>}`

| | |
|---|---|
| mac-address-table mac-auth-state address <MAC> vlan <1-4904> | Clears MAC addresses learned from a particular VLAN when WLAN MAC authentication and captive-portal fall back is enabled<br>Access points/controllers provide WLAN access to clients whose MAC address has been learned and stored in their MAC address tables. Use this command to clear a specified MAC address on the MAC address table. Once cleared the client has to re-authenticate, and is provided access only on successful authentication.<br>• <MAC> – Specify the MAC address to clear.<br>• vlan <1-4904> – Specify the VLAN interface from 1 - 4094. In the AP/controller's MAC address table, the specified MAC address is cleared on the specified VLAN interface. |
| on <DEVICE-NAME> | Optional. Clears the specified MAC address on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.<br>If a device is not specified, the system clears the MAC address from the MAC address table of all devices. |

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

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

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

| | |
|---|---|
| role ldap-stats | Clears role based *Lightweight Directory Access Protocol* (LDAP) server statistics |
| on <DEVICE-NAME> | Optional. Clears role based LDAP server statistics on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

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

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

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

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

- `clear spanning-tree detected-protocols {interface [<INTERFACE-NAME>|ge <1-X>|me1|port-channel <1-X>|pppoe1|vlan <1-4094>|wwan1|xge <1-4>]} {on <DEVICE-NAME>}`

| | |
|---|---|
| spanning-tree | Clears spanning tree protocols on an interface and restarts protocol migration |
| detected-protocols | Restarts protocol migration |
| interface [<INTERFACE-NAME>\| ge <1-X>\|me1\| port-channel <1-X>\| pppoe1\|vlan <1-4094>\| wwan1\|xge <1-4>] | Optional. Clears spanning tree entries on different interfaces<br>• <INTERFACE-NAME> – Clears detected spanning tree entries on a specified interface. Specify the interface name.<br>• ge <1-X> – Clears detected spanning tree entries for the selected GigabitEthernet interface. Select the GigabitEthernet interface index from 1 - X<br>• me1 – Clears FastEthernet interface spanning tree entries<br>• port-channel <1- X> – Clears detected spanning tree entries for the selected port channel interface. Select the port channel index from 1 - X.<br>The number of port-channel interfaces supported varies for different device types. For example, RFS4000 supports 3 port-channels.<br>• pppoe1 – Clears detected spanning tree entries for PPPoE interface.<br>• vlan <1-4094> – Clears detected spanning tree entries for the selected VLAN interface. Select a SVI VLAN ID from 1 - 4094.<br>• wwan1 – Clears detected spanning tree entries for wireless WAN interface<br>• xge <1-4> – Clears detected spanning tree entries for TenGigabitEthernet interfaces. Specify the GigabitEthernet interface index from 1 - 4. |
| on <DEVICE-NAME> | Optional. Clears spanning tree protocol entries on a selected device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `clear traffic-shape statistics {class <1-4>} {(on <DEVICE-NAME>)}`

| | |
|---|---|
| traffic-shape statistics | Clears traffic shaping statistics |
| class <1-4> | Optional. Clears traffic shaping statistics for a specific traffic class<br>• <1-4> – Specify the traffic class from 1 - 4.<br>**Note:** If the traffic class is not specified, the system clears all traffic shaping statistics. |
| on <DEVICE-NAME> | Optional. Clears traffic shaping statistics for the specified traffic class on a specified device<br>• <DEVICE-NAME> – Specify the name of the access point, wireless controller, or service platform.<br>**Note:** For more information on configuring traffic-shape, see *interface*. |

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

| | |
|---|---|
| vrrp | Clears *Virtual Router Redundancy Protocol* (VRRP) statistics for a device |

| | |
|---|---|
| error-stats {on <DEVICE-NAME>} | Clears global error statistics<br>• on <DEVICE-NAME> – Optional. Clears VRRP global error statistics on a selected device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |
| stats {on <DEVICE-NAME>} | Clears VRRP related statistics<br>• on <DEVICE-NAME> – Optional. Clears VRRP related statistics on a selected device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

**Example**

```
rfs4000-229D58#clear crypto ike sa all

rfs4000-229D58#show crypto ike sa
--------------------------------------------------------------------------------
-------IDX     PEER         VERSION    ENCR ALGO      HASH ALGO       DH GROUP
IKE STATE
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------Total IKE SAs: 0
rfs4000-229D58#

rfs6000-81742D#clear spanning-tree detected-protocols interface port-channel 1

rfs6000-81742D#clear ip dhcp bindings 172.16.10.9

rfs6000-81742D#clear cdp neighbors

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

rfs4000-229D58#clear lldp neighbors

rfs6000-81742D#show event-history
EVENT HISTORY REPORT
Generated on '2017-04-04 13:49:57 IST' by 'admin'

2017-04-04 13:37:31     rfs6000-81742D  SYSTEM    LOGIN              Successfully
logged in user 'admin' with privilege 'superuser' from 'ssh'
2017-04-04 13:15:19     rfs6000-81742D  SYSTEM    LOGOUT               Logged out
user 'admin' with privilege 'superuser' from '192.168.13.10'
2017-04-04 13:09:47     rfs6000-81742D  LICMGR     LIC_AP_AAP_DEPLETED  Depleted
AP/AAP license count: 1
2017-04-04 13:09:47     rfs6000-81742D  LICMGR     LIC_AP_AAP_DEPLETED  Depleted
AP/AAP license count: 1
--More--
rfs6000-81742D#

jrfs6000-81742D#clear event-history

rfs6000-81742D#show event-history
EVENT HISTORY REPORT
Generated on '2017-04-04 13:51:27 IST' by 'admin'

rfs6000-81742D#
```

```
rfs6000-81742D#show mac-address-table
------------------------------------------------------------
 BRIDGE VLAN PORT             MAC                STATE
------------------------------------------------------------
 1      1    up1              00-02-B3-28-D1-55 forward
 1      1    up1              00-0F-8F-19-BA-4C forward
 1      1    up1              84-24-8D-80-C2-AC forward
 1      1    up1              84-24-8D-80-BF-34 forward
 1      1    up1              1C-7E-E5-18-FA-67 forward
 1      1    up1              84-24-8D-83-30-A4 forward
 1      1    up1              B4-C7-99-DD-31-C8 forward
 1      1    up1              B4-C7-99-6C-88-09 forward
 1      1    up1              00-18-71-D0-1B-F3 forward
 1      1    up1              B4-C7-99-71-17-28 forward
 1      1    up1              FC-0A-81-42-93-6C forward
 1      1    up1              B4-C7-99-6D-CD-4B forward
 1      1    up1              84-24-8D-84-A2-24 forward
 1      1    up1              3C-CE-73-F4-47-83 forward
 1      1    up1              B4-C7-99-74-B4-5C forward
------------------------------------------------------------
Total number of MACs displayed: 15
rfs6000-81742D#

rfs6000-81742D>clear mac-address-table address 3C-CE-73-F4-47-83 on rfs6000-81742D

rfs6000-81742D#show mac-address-table
------------------------------------------------------------
 BRIDGE VLAN PORT             MAC                STATE
------------------------------------------------------------
 1      1    up1              00-02-B3-28-D1-55 forward
 1      1    up1              00-0F-8F-19-BA-4C forward
 1      1    up1              84-24-8D-80-C2-AC forward
 1      1    up1              84-24-8D-80-BF-34 forward
 1      1    up1              1C-7E-E5-18-FA-67 forward
 1      1    up1              84-24-8D-83-30-A4 forward
 1      1    up1              B4-C7-99-DD-31-C8 forward
 1      1    up1              B4-C7-99-6C-88-09 forward
 1      1    up1              00-18-71-D0-1B-F3 forward
 1      1    up1              B4-C7-99-71-17-28 forward
 1      1    up1              FC-0A-81-42-93-6C forward
 1      1    up1              B4-C7-99-6D-CD-4B forward
 1      1    up1              84-24-8D-84-A2-24 forward
 1      1    up1              B4-C7-99-74-B4-5C forward
------------------------------------------------------------
Total number of MACs displayed: 14
rfs6000-81742D#
```

## 3.1.7 clock

*Privileged Exec Mode Commands*

Sets a device's system clock. By default all WiNG devices are shipped with the time zone and time format set to UTC and 24-hour clock respectively. If a device's clock is set without resetting the time zone, the time is displayed relative to the *Universal Time Coordinated* (UTC) – Greenwich Time. To display time in the local time zone format, in the device's configuration mode, use the timezone command to reset the time zone. You can also reset the time zone at the RF Domain level. When configured as RF Domain setting, it applies to all devices within the domain. Configuring the local time zone prior to setting the clock is recommended. For more information on configuring RF Domain time zone, see *timezone*.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

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

**Parameters**

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

| | |
|---|---|
| clock set | Sets a device's system clock |
| <HH:MM:SS> | Sets the current time (in military format hours, minutes and seconds)<br>**Note:** By default the WiNG software displays time in the 24-hour clock format. This setting cannot be changed. |
| <1-31> | Sets the numerical day of the month |
| <MONTH> | Sets the month of the year from Jan - Dec |
| <1993-2035> | Sets a valid four digit year from 1993 - 2035 |
| on <DEVICE-NAME> | Optional. Sets the clock on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

**Example**

The following commands set the time zone and clock for the logged device:

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#timezone America/Los_Angeles

nx9500-6C8809#clock set 00:25:10 16 Jan 2017

nx9500-6C8809#show clock
2017-01-16 03:31:16 IST

nx9500-6C8809#
```

## 3.1.8 cluster

*Privileged Exec Mode Commands*

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

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

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
cluster start-election
```

**Parameters**

- `cluster start-election`

| | |
|---|---|
| start-election | Starts a new cluster master election |

**Example**

```
rfs4000-880DA7#cluster start-election
rfs4000-880DA7#
```

**Related Commands**

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

## 3.1.9 configure

*Privileged Exec Mode Commands*

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

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

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

**Parameters**

- `configure {self|terminal}`

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

**Example**

```
rfs6000-81742D#configure self
Enter configuration commands, one per line.  End with CNTL/Z.
rfs6000-81742D(config-device-00-15-70-81-74-2D)#

rfs6000-81742D#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
rfs6000-81742D(config)#
```

## 3.1.10 connect

*Privileged Exec Mode Commands*

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

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

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

**Parameters**

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

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

**Example**

```
nx9500-6C8809#show mint lsp-db
9 LSPs in LSP-db of 19.6C.88.09:
LSP 19.6C.88.09 at level 1, hostname "nx9500-6C8809", 8 adjacencies, seqnum 1294552
LSP 19.6D.B5.D4 at level 1, hostname "rfs6000-81742D", 8 adjacencies, seqnum
1915721
LSP 19.74.B4.5C at level 1, hostname "ap8132-74B45C", 8 adjacencies, seqnum 1468227
LSP 4D.80.C2.AC at level 1, hostname "ap7532-80C2AC", 8 adjacencies, seqnum 649241
LSP 4D.83.30.A4 at level 1, hostname "ap7522-8330A4", 8 adjacencies, seqnum 202818
LSP 4D.84.A2.24 at level 1, hostname "ap7562-84A224", 8 adjacencies, seqnum 380337
LSP 68.88.0D.A7 at level 1, hostname "rfs4000-880DA7", 8 adjacencies, seqnum
1494520
LSP 68.99.BB.7C at level 1, hostname "ap7131-99BB7C", 8 adjacencies, seqnum 831529
nx9500-6C8809#

nx9500-6C8809#connect mint-id ?
  MINT-ID  MiNT ID of device to connect to

nx9500-6C8809#connect mint-id 19.6D.B5.D4

Entering character mode
Escape character is '^]'.

RFS6000 release 5.9.0.0-012D
rfs6000-81742D login: admin
Password:
rfs6000-81742D>
```

## 3.1.11 copy

*Privileged Exec Mode Commands*

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

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

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

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

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

**Parameters**

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

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

**Example**

```
Transferring file snmpd.log to remote TFTP server.
rfs6000-81742D#copy flash:/log/snmpd.log
tftp://10.233.89.183:/snmpd.log
Accessing running-config file from remote TFTP server into switch running-config.
rfs6000-81742D#copy tftp://10.233.89.183:/running-config running-config
```

## 3.1.12 cpe

*Privileged Exec Mode Commands*

Enables a WiNG controller to perform certain operations on *Customer Premises Equipment* (CPEs) through an adopted T5 controller

A T5 controller uses the IPX operating system to manage its connected radio devices, as opposed to the WiNG operating system used by RFS wireless controllers and NX service platforms. However, a T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5's management within a WiNG supported subnet populated by both types of devices. The CPEs are the T5 controller managed radio devices using the IPX operating system. These CPEs use a *Digital Subscriber Line* (DSL) as their high speed Internet access mechanism using the CPE's physical wallplate connection and phone jack.

**Supported in the following platforms:**

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
cpe [boot|reload|upgrade]
cpe boot system cpe [<1-24>|all] [primary|secondary] {on <T5-DEVICE-NAME>}
cpe [reload|upgrade <IMAGE-LOCATION>] cpe [<1-24>|all] {on <T5-DEVICE-NAME>}
```

**NOTE:** These commands can also be executed on the T5 profile and device context. For more information, see *T5 Profile Config Commands*.

**Parameters**

- `cpe boot system cpe [<1-24>|all] [primary|secondary] {on <T5-DEVICE-NAME>}`

| | |
|---|---|
| cpe boot system | Changes the image used by a CPE to boot. When reloading, the CPE uses the specified image. |
| cpe [<1-24>\|all] | Identifies the CPE(s) on which this change is implemented<br>• <1-24> – Reloads only those CPEs whose IDs have been specified. Specify the ID from 1 - 24.<br>• all – Reloads all CPEs |
| [primary\|secondary] | Select the next boot image<br>• primary – Uses the primary image when reloading<br>• secondary – Uses the secondary image when reloading |
| on <T5-DEVICE-NAME> | Optional. Performs this operation on a specified T5 device<br>• <T5-DEVICE-NAME> – Specify the T5 device's hostname. |

- `cpe [reload|upgrade <IMAGE-LOCATION>] cpe [<1-24>|all] {on <T5-DEVICE-NAME>}`

| | |
|---|---|
| cpe [reload\| upgrade <IMAGE-LOCATION>] | Performs the following operations on CPEs<br>• reload – Reloads the device<br>• upgrade <IMAGE-LOCATION> – Upgrades the device<br>• <IMAGE-LOCATION> – Specify the location of the firmware image. Both IPv4 and IPv6 addresses are supported. Use one of the following options to provide the location:<br>IPv4 URLs:<br>tftp://<hostname\|IP>[:port]/path/file<br>ftp://<user>:<passwd>@<hostname\|IP>[:port]/path/file<br>sftp://<user>:<passwd>@<hostname\|IP>[:port]>/path/file<br>http://<hostname\|IP>[:port]/path/file<br>cf:/path/file<br>usb<n>:/path/file<br>IPv6 URLs:<br>tftp://<hostname\|[IPv6]>[:port]/path/file<br>ftp://<user>:<passwd>@<hostname\|[IPv6]>[:port]/path/file<br>sftp://<user>:<passwd>@<hostname\|[IPv6]>[:port]>/path/file<br>http://<hostname\|[IPv6]>[:port]/path/file<br>**Note:** After specifying the operation to perform, identify the device(s). |
| cpe [<1-24>\|all] | Identifies the CPE(s) on which the operation is performed<br>• <1-24> – Configures the CPE's ID from 1 - 24<br>• all – Configures all CPEs |
| on <T5-DEVICE-NAME> | Optional. Performs this operation on a specified T5 device<br>• <T5-DEVICE-NAME> – Specify the T5 device's hostname. |

**Example**

```
nx9500-6C8809#show t5 cpe boot on t5-ED7C6C
-------------------------------------------------------------------------------
--------------------
  DEVICE   PRIMARY VERSION   SECONDARY VERSION   NEXT BOOT   UPGRADE STATUS   UPGRADE
PROGRESS %
-------------------------------------------------------------------------------
--------------------
 cpe1      5.4.2.0-010R      5.4.2.0-006B       primary     none              0
 cpe2      5.4.2.0-010R      5.4.2.0-006B       primary     none              0
-------------------------------------------------------------------------------
--------------------
nx9500-6C8809#

nx9500-6C8809#cpe boot system cpe 1 secondary on t5-ED7C6C
Updated T5 CPE system boot partition
nx9500-6C8809#
```

## 3.1.13 create-cluster

*Privileged Exec Mode Commands*

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

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

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

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

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

**Parameters**

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

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

**Example**

```
rfs4000-229D58#create-cluster name TechPubs ip 192.168.13.8 level 2
... creating cluster
... committing the changes
... saving the changes
Please Wait .
[OK]
rfs4000-229D58#

rfs4000-229D58#show cluster configuration
```

```
Cluster Configuration Information
 Name                          : TechPubsLAN
 Configured Mode               : Active
 Master Priority               : 128
 Force configured state        : Disabled
 Force configured state delay  : 5 minutes
 Handle STP                    : Disabled
 Radius Counter DB Sync Time   : 5 minutes
rfs4000-229D58#

rfs4000-229D58#show context
!
! Configuration of RFS4000 version 5.9.1.0-012D
!
!
version 2.5
!
!
firewall-policy default
 no ip dos tcp-sequence-past-window
 alg sip
!
!
mint-policy global-default
 router packet priority 6
!
radio-qos-policy default
!
!
management-policy default
 telnet
 http server
 https server
 no ftp
--More--
rfs4000-229D58#
```

**Related Commands**

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

## 3.1.14 crypto

*Privileged Exec Mode Commands*

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

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

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
crypto [key|pki]

crypto key [export|generate|import|zeroize]

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

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

crypto key generate rsa <RSA-KEYPAIR-NAME> [2048|4096] {on <DEVICE-NAME>}

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

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

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

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

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

crypto pki export [request|trustpoint]

crypto pki export request [generate-rsa-key|short|use-rsa-key] <RSA-KEYPAIR-NAME>
[autogen-subject-name|subject-name]

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

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

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

```
crypto pki generate self-signed <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key]
<RSA-KEYPAIR-NAME> [autogen-subject-name|subject-name]

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

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

crypto pki import [certificate|crl|trustpoint]

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

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

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

**Parameters**

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

| | |
|---|---|
| key | Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key. |
| export rsa <RSA-KEYPAIR-NAME> | Exports an existing RSA Keypair to a specified destination<br>• <RSA-KEYPAIR-NAME> – Specify the RSA Keypair name. |
| <EXPORT-TO-URL> | Specify the RSA Keypair destination address. Both IPv4 and IPv6 address formats are supported.<br>After specifying the destination address (where the RSA keypair is exported), configure one of the following parameters: background or passphrase. |
| background | Optional. Performs export operation in the background. If selecting this option, you can optionally specify the device (access point or controller) to perform the export on. |
| passphrase <KEY-PASSPHRASE> background | Optional. Encrypts RSA Keypair before exporting<br>• <KEY-PASSPHRASE> – Specify a passphrase to encrypt the RSA keypair.<br>• background – Optional. Performs export operation in the background. After specifying the passphrase, optionally specify the device (access point or controller) to perform the export on. |
| on <DEVICE-NAME> | The following parameter is recursive and common to all of the above parameters:<br>• on <DEVICE-NAME> – Optional. Performs export operation on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `crypto key generate rsa <RSA-KEYPAIR-NAME> [2048|4096] {on <DEVICE-NAME>}`

| | |
|---|---|
| key | Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key. |

| | |
|---|---|
| generate rsa <RSA-KEYPAIR-NAME> [2048\|4096] | Generates a new RSA Keypair<br>• <RSA-KEYPAIR-NAME> – Specify the RSA Keypair name.<br>• [2048\|4096] – Sets the size of the RSA key in bits. The options are 2048 bits and 4096 bits. The default size is 2048 bits.<br>After specifying the key size, optionally specify the device (access point or controller) to generate the key on. |
| on <DEVICE-NAME> | Optional. Generates the new RSA Keypair on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

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

| | |
|---|---|
| key | Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key. |
| import rsa <RSA-KEYPAIR-NAME> | Imports a RSA Keypair from a specified source<br>• <RSA-KEYPAIR-NAME> – Specify the RSA Keypair name. |
| <IMPORT-FROM-URL> | Specify the RSA Keypair source address. Both IPv4 and IPv6 address formats are supported.<br>After specifying the source address (where the RSA Keypair is imported from), configure one of the following parameters: background or passphrase. |
| background | Optional. Performs import operation in the background. If selecting this option, you can optionally specify the device (access point or controller) to perform the import on. |
| passphrase <KEY-PASSPHRASE> background | Optional. Decrypts the RSA Keypair after importing<br>• <KEY-PASSPHRASE> – Specify the passphrase to decrypt the RSA keypair.<br>• background – Optional. Performs import operation in the background. After specifying the passphrase, optionally specify the device (access point or controller) to perform the import on. |
| on <DEVICE-NAME> | The following parameter is recursive and common to the 'background' and 'passphrase' keywords:<br>• on <DEVICE-NAME> – Optional. Performs import operation on a specific device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

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

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

| | |
|---|---|
| on <DEVICE-NAME> | The following parameter is recursive and optional:<br>• on <DEVICE-NAME> – Optional. Deletes all certificates associated with the RSA Keypair on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

• `crypto pki authenticate <TRUSTPOINT-NAME> <URL> {background} {(on <DEVICE-NAME>)}`

| | |
|---|---|
| pki | Enables *Private Key Infrastructure* (PKI) management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated *Certificate Authority* (CA) certificates. |
| authenticate <TRUSTPOINT-NAME> | Authenticates a trustpoint and imports the corresponding CA certificate<br>• <TRUSTPOINT-NAME> – Specify the trustpoint name. |
| <URL> | Specify CA's location. Both IPv4 and IPv6 address formats are supported.<br>**Note:** The CA certificate is imported from the specified location. |
| background | Optional. Performs authentication in the background. If selecting this option, you can optionally specify the device (access point or controller) to perform the authentication on. |
| on <DEVICE-NAME> | The following parameter is recursive and optional:<br>• on <DEVICE-NAME> – Optional. Performs authentication on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

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

| | |
|---|---|
| pki | Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates. |
| export request | Exports CSR to the CA for digital identity certificate. The CSR contains applicant's details and RSA Keypair's public key. |
| [generate-rsa-key\| use-rsa-key] <RSA-KEYPAIR-NAME> | Generates a new RSA Keypair or uses an existing RSA Keypair<br>• generate-rsa-key – Generates a new RSA Keypair for digital authentication<br>• use-rsa-key – Uses an existing RSA Keypair for digital authentication<br>• <RSA-KEYPAIR-NAME> – If generating a new RSA Keypair, specify a name for it. If using an existing RSA Keypair, specify its name. |
| autogen-subject-name | Auto generates subject name from configuration parameters. The subject name identifies the certificate. |
| <EXPORT-TO-URL> | Specify the CA's location. Both IPv4 and IPv6 address formats are supported.<br>**Note:** The CSR is exported to the specified location. |
| email <SEND-TO-EMAIL> | Exports CSR to a specified e-mail address<br>• <SEND-TO-EMAIL> – Specify the CA's e-mail address. |
| fqdn <FQDN> | Exports CSR to a specified *Fully Qualified Domain Name* (FQDN)<br>• <FQDN> – Specify the CA's FQDN. |
| ip-address <IP> | Exports CSR to a specified device or system<br>• <IP> – Specify the CA's IP address. |

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

| | |
|---|---|
| pki | Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates. |
| export request | Exports CSR to the CA for a digital identity certificate. The CSR contains applicant's details and RSA Keypair's public key. |
| [generate-rsa-key\| short [generate-rsa-key\|use-rsa-key]\| use-rsa-key] <RSA-KEYPAIR-NAME> | Generates a new RSA Keypair or uses an existing RSA Keypair<br>• generate-rsa-key – Generates a new RSA Keypair for digital authentication<br>• short [generate-rsa-key\|use-rsa-key] – Generates and exports a shorter version of the CSR<br>• generate-rsa-key – Generates a new RSA Keypair for digital authentication. If generating a new RSA Keypair, specify a name for it.<br>• use-rsa-key – Uses an existing RSA Keypair for digital authentication. If using an existing RSA Keypair, specify its name.<br>• use-rsa-key – Uses an existing RSA Keypair for digital authentication<br>• <RSA-KEYPAIR-NAME> – If generating a new RSA Keypair, specify a name for it. If using an existing RSA Keypair, specify its name. |
| subject-name <COMMON-NAME> | Configures a subject name, defined by the <COMMON-NAME> keyword, to identify the certificate<br>• <COMMON-NAME> – Specify the common name used with the CA certificate. The name should enable you to identify the certificate easily (2 to 64 characters in length). |
| <COUNTRY> | Sets the deployment country code (2 character ISO code) |
| <STATE> | Sets the state name (2 to 64 characters in length) |
| <CITY> | Sets the city name (2 to 64 characters in length) |
| <ORGANIZATION> | Sets the organization name (2 to 64 characters in length) |
| <ORGANIZATION-UNIT> | Sets the organization unit (2 to 64 characters in length) |
| <EXPORT-TO-URL> | Specify the CA's location. Both IPv4 and IPv6 address formats are supported.<br>The CSR is exported to the specified location. |
| email <SEND-TO-EMAIL> | Exports CSR to a specified e-mail address<br>• <SEND-TO-EMAIL> – Specify the CA's e-mail address. |
| fqdn <FQDN> | Exports CSR to a specified FQDN<br>• <FQDN> – Specify the CA's FQDN. |
| ip-address <IP> | Exports CSR to a specified device or system<br>• <IP> – Specify the CA's IP address. |

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

| | |
|---|---|
| pki | Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates. |

| | |
|---|---|
| export trustpoint <TRUSTPOINT-NAME> | Exports a trustpoint along with CA certificate, *Certificate Revocation List* (CRL), server certificate, and private key<br>• <TRUSTPOINT-NAME> – Specify the trustpoint name (should be authenticated). |
| <EXPORT-TO-URL> | Specify the destination address. Both IPv4 and IPv6 address formats are supported.<br>The trustpoint is exported to the address specified here. |
| background | Optional. Performs export operation in the background. If selecting this option, you can optionally specify the device (access point or controller) to perform the export on. |
| passphrase <KEY-PASSPHRASE> background | Optional. Encrypts the key with a passphrase before exporting<br>• <KEY-PASSPHRASE> – Specify the passphrase to encrypt the trustpoint.<br>• background – Optional. Performs export operation in the background. After specifying the passphrase, optionally specify the device (access point or controller) to perform the export on. |
| on <DEVICE-NAME> | The following parameter is recursive and common to the 'background' and 'passphrase' keywords:<br>• on <DEVICE-NAME> – Optional. Performs export operation on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

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

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

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

| | |
|---|---|
| pki | Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated certificates. |
| generate self-signed <TRUSTPOINT-NAME> | Generates a self-signed certificate and a trustpoint<br>• <TRUSTPOINT-NAME> – Specify a name for the certificate and its trustpoint. |
| [generate-rsa-key\|use-rsa-key] <RSA-KEYPAIR-NAME> | Generates a new RSA Keypair, or uses an existing RSA Keypair<br>• generate-rsa-key – Generates a new RSA Keypair for digital authentication<br>• use-rsa-key – Uses an existing RSA Keypair for digital authentication<br>• <RSA-KEYPAIR-NAME> – If generating a new RSA Keypair, specify a name for it. If using an existing RSA Keypair, specify its name. |
| subject-name <COMMON-NAME> | Configures a subject name, defined by the <COMMON-NAME> keyword, to identify the certificate<br>• <COMMON-NAME> – Specify the common name used with this certificate. The name should enable you to identify the certificate easily and should not exceed 2 to 64 characters in length. |
| <COUNTRY> | Sets the deployment country code (2 character ISO code) |
| <STATE> | Sets the state name (2 to 64 characters in length) |
| <CITY> | Sets the city name (2 to 64 characters in length) |
| <ORGANIZATION> | Sets the organization name (2 to 64 characters in length) |
| <ORGANIZATION-UNIT> | Sets the organization unit (2 to 64 characters in length) |
| email <SEND-TO-EMAIL> | Optional. Exports the self-signed certificate to a specified e-mail address<br>• <SEND-TO-EMAIL> – Specify the e-mail address. |
| fqdn <FQDN> | Optional. Exports the self-signed certificate to a specified FQDN<br>• <FQDN> – Specify the FQDN. |
| ip-address <IP> | Optional. Exports the self-signed certificate to a specified device or system<br>• <IP> – Specify the device's IP address. |

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

| | |
|---|---|
| pki | Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates. |
| import | Imports certificates, *Certificate Revocation List* (CRL), or a trustpoint to the selected device |
| [certificate\|crl] <TRUSTPOINT-NAME> | Imports a signed server certificate or CRL<br>• certificate – Imports signed server certificate<br>• crl – Imports CRL<br>• <TRUSTPOINT-NAME> – Specify the trustpoint name (should be authenticated). |
| <IMPORT-FROM-URL> | Specify the signed server certificate or CRL source address. Both IPv4 and IPv6 address formats are supported.<br>The server certificate or the CRL (based on the parameter passed in the preceding step) is imported from the location specified here. |

| | |
|---|---|
| background | Optional. Performs import operation in the background. If selecting this option, you can optionally specify the device (access point or controller) to perform the import on. |
| on <DEVICE-NAME> | The following parameter is recursive and optional:<br>• on <DEVICE-NAME> – Optional. Performs import operation on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

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

| | |
|---|---|
| pki | Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates. |
| import | Imports certificates, CRL, or a trustpoint to the selected device |
| trustpoint <TRUSTPOINT-NAME> | Imports a trustpoint and its associated CA certificate, server certificate, and private key<br>• <TRUSTPOINT-NAME> – Specify the trustpoint name (should be authenticated). |
| <IMPORT-FROM-URL> | Specify the trustpoint source address. Both IPv4 and IPv6 address formats are supported. |
| background | Optional. Performs import operation in the background. If selecting this option, you can optionally specify the device (access point or controller) to perform the export on. |
| passphrase <KEY-PASSPHRASE> background | Optional. Decrypts trustpoint with a passphrase after importing<br>• <KEY-PASSPHRASE> – Specify the passphrase. After specifying the passphrase, optionally specify the device to perform import on.<br>• background – Optional. Performs import operation in the background. After specifying the passphrase, optionally specify the device (access point or controller) to perform the import on. |
| on <DEVICE-NAME> | The following parameter is recursive and optional:<br>• on <DEVICE-NAME> – Optional. Performs import operation on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

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

| | |
|---|---|
| pki | Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates. |
| zeroize trustpoint <TRUSTPOINT-NAME> | Deletes a trustpoint and its associated CA certificate, server certificate, and private key<br>• <TRUSTPOINT-NAME> – Specify the trustpoint name (should be authenticated). |
| del-key | Optional. Deletes the private key associated with the server certificate. Optionally specify the device to perform deletion on. |
| on <DEVICE-NAME> | The following parameter is recursive and optional:<br>• on <DEVICE-NAME> – Optional. Deletes the trustpoint on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

**Usage Guidelines**

The system supports both IPv4 and IPv6 address formats. Provide source and destination locations using any one of the following options:

- IPv4 URLs:

tftp://<hostname|IP>[:port]/path/file

ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file

sftp://<user>@<hostname|IP>[:port]>/path/file

http://<hostname|IP>[:port]/path/file

cf:/path/file

usb<n>:/path/file

- IPv6 URLs:

tftp://<hostname|[IPv6]>[:port]/path/file

ftp://<user>:<passwd>@<hostname|[IPv6]>[:port]/path/file

sftp://<user>:<passwd>@<hostname|[IPv6]>[:port]>/path/file

http://<hostname|[IPv6]>[:port]/path/file

**Example**

```
rfs6000-81742D#crypto key generate rsa key 1025
RSA Keypair successfully generated
rfs6000-81742D#

rfs6000-81742D#crypto key import rsa test123 url passphrase word background
RSA key import operation is started in background
rfs6000-81742D#

rfs6000-81742D#crypto pki generate self-signed word generate-rsa-key word autogen-
subject-name fqdn word
Successfully generated self-signed certificate
rfs6000-81742D#

rfs6000-81742D#crypto pki zeroize trustpoint word del-key
Successfully removed the trustpoint and associated certificates
%Warning: Applications associated with the trustpoint will start using default-
trustpoint
rfs6000-81742D#

rfs6000-81742D#crypto pki authenticate word url background
Import of CA certificate started in background
rfs6000-81742D#

rfs6000-81742D#crypto pki import trustpoint word url passphrase word
Import operation started in background
rfs6000-81742D#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes server certificates, trustpoints and their associated certificates |

## 3.1.15 crypto-cmp-cert-update

*Privileged Exec Mode Commands*

Triggers a *Certificate Management Protocol* (CMP) certificate update on a specified device or devices

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
crypto-cmp-cert-update <TRUSTPOINT-NAME> {on <DEVICE-NAME>}
```

**Parameters**

- `crypto-cmp-cert-update <TRUSTPOINT-NAME> {on <DEVICE-NAME>}`

| | |
|---|---|
| crypto-cmp-cert-update <TRUSTPOINT-NAME> {on <DEVICE-NAME>} | Triggers a CMP certificate update on a specified device or devices<br>• <TRUSTPOINT-NAME> – Specify the target trustpoint name. A trustpoint represents a CA/identity pair containing the identity of the CA, CA specific configuration parameters, and an association with an enrolled identity certificate. Use the crypto-cmp-policy context to configure the trustpoint.<br>• on <DEVICE-NAME> – Optional. Triggers a CMP certificate update and response on a specified device or devices. Specify the name of the AP, wireless controller, or service platform. Multiple devices can be provided as a comma separated list.<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

**Example**

```
rfs4000-229D58#crypto-cmp-cert-update test on B4-C7-99-71-17-28
CMP Cert update success
rfs4000-229D58#
```

## 3.1.16 database

*Privileged Exec Mode Commands*

Enables automatic repairing (vacuuming) and dropping of databases (Captive-portal and NSight). Vacuuming a database refers to the process of finding and reclaiming space left over from previous DELETE statements.

If enforcing authenticated access to the database, use this command to generate the keyfile. Every keyfile has a set of associated users having a username and password. Database access is provided only if the keyfile and the user credentials entered during database longin match.

**NOTE:** For information on enabling database authentication, see *Enabling Database Authentication*.

**Supported in the following platforms:**

- Service Platforms — NX9500, NX9510, NX9600, VX9000

**Syntax**

```
database [drop|keyfile|repair]

database drop [all|captive-portal|nsight]

database repair {on <DEVICE-NAME>}

database keyfile [export|generate|import|zerzoise]
database keyfile generate
database keyfile [export|import] <URL>
database keyfile zerzoise
```

**Parameters**

- `database drop [all|captive-portal|nsight]`

| | |
|---|---|
| database drop [all\|captive-portal\|nsight] | Drops (deletes) all or a specified database. Execute the command on the database host.<br>• all – Drops all databases, captive portal and NSight.<br>• captive-portal – Drops captive-portal database only<br>• nsight – Drops NSight database only |

- `database repair {on <DEVICE-NAME>}`

| | |
|---|---|
| database repair on <DEVICE-NAME> | Enables automatic repairing of all databases. Execute the command on the database host.<br>• on <DEVICE-NAME> – Optional. Specifies the name of the access point, wireless controller, or service platform hosting the database. When specified, databases on the specified device are periodically checked through to identify and remove obsolete data documents.<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.<br>If no device is specified, the system repairs all databases. |

- `database keyfile [generate|zerzoise]`

| | |
|---|---|
| database keyfile [generate\|zerzoise] | Enables management of database keyfiles. This command is part of a series of configurations that are required to enforce authentication on the database. Use this command to generate keyfiles associated with the database. After generating the keyfile, create the users having the database access. For information on creating database users, see *service*.<br>• generate – Generates the keyfile. Execute the command on the primary database host.<br>• zerzoise – Deletes a keyfile. |

- `database keyfile [export|import] <URL>`

| | |
|---|---|
| database keyfile [export\|import] <URL> | Enables database keyfile management. This command is part of a series of configurations required to enforce database authentication. Use this command to exchange keyfiles between replica set members.<br>• export – Exports the keyfile to a specified location on an FTP/SFTP/TFTP server. Execute the command on the primary database host.<br>• import – Imports the keyfile from a specified location. Execute the command on the replica set members.<br>The following parameter is common to both of the above keywords:<br>• <URL> – Specify the location to/from where the keyfile is to be exported/imported. Use one of the following options:<br>ftp://<user>:<passwd>@<hostname\|IP>[:port]/path/file<br>sftp://<user>:<passwd>@<hostname\|IP>[:port]/path/file<br>tftp://<hostname\|IP>[:port]/path/file |

- `database keyfile zerzoise`

| | |
|---|---|
| database keyfile zerzoise | Enables the management of database keyfiles<br>• zerzoise – Deletes an existing keyfile. |

**Example**

```
nx9500-6C8809#database repair on nx9500-6C8809
nx9500-6C8809#

nx9500-6C8809#database keyfile generate
Database keyfile successfully generated
nx9500-6C8809#

nx9500-6C8809#database keyfile  zeroize
Database keyfile successfully removed
nx9500-6C8809#

vx9000-1A1809#database keyfile generate
Database keyfile successfully generated
vx9000-1A1809#

vx9000-1A1809#database keyfile export ftp://1.1.1.111/db-key
Database keyfile successfully exported
vx9000-1A1809#

vx9000-D031F2#database keyfile import ftp://1.1.1.111/db-key
Database keyfile successfully imported
vx9000-D031F2#
```

**Related Commands**

| | |
|---|---|
| *database-backup* | Backs up captive-portal and/or NSight database to a specified location and file on an FTP or SFTP server |
| *database-restore* | Restores a previously exported database [captive-portal and/or NSight] |

## 3.1.17 database-backup

*Privileged Exec Mode Commands*

Backs up captive-portal/NSight database to a specified location and file on an FTP or SFTP server

**Supported in the following platforms:**

- Service Platforms — NX9500, NX9510, NX9600, VX9000

**Syntaxf**

```
database-backup database [captive-portal|nsight|nsight-placement-info] <URL>

database-backup database [captive-portal|nsight] <URL>
database-backup database nsight-placement-info <URL>
```

**Parameters**

- `database-backup database [captive-portal|nsight] <URL>`

| | |
|---|---|
| database-backup database [captive-portal\|nsight] | Backs up captive portal and/or NSight database to a specified location. Select the database to backup:<br>• captive-portal – Backs up captive portal database<br>• nsight – Backs up NSight database<br>After specifying the database type, configure the destination location. |
| <URL> | Configures the destination location. The database is backed up at the specified location. Specify the location URL in one of the following formats:<br>ftp://<user>:<passwd>@<hostname\|IP>[:port]/path/file.tar.gz<br>sftp://<user>:<passwd>@<hostname\|IP>[:port]/path/file.tar.gz |

- `database-backup database nsight-placement-info <URL>`

| | |
|---|---|
| database-backup database nsight-placement-info <URL> | Backs up the NSight access point placement related details to a specified location<br>• <URL> – Specify the URL in one of the following formats:<br>ftp://<user>:<passwd>@<hostname\|IP>[:port]/path/file.tar.gz<br>sftp://<user>:<passwd>@<hostname\|IP>[:port]/path/file.tar.gz<br>tftp://<hostname\|IP>[:port]/path/file.tar.gz |

**Example**

```
NS-DB-nx9510-6C87EF#database-backup database nsight tftp://192.168.9.50/testbckup
NS-DB-nx9510-6C87EF#show database backup-status
Last Database Backup Status : In_Progress(Starting tftp transfer.)
Last Database Backup Time   : 2017-04-17 12:48:05
NS-DB-nx9510-6C87EF#show database backup-status
Last Database Backup Status : Successful
Last Database Backup Time   : Mon Apr 17 12:48:08 T 2017
NS-DB-nx9510-6C87EF#Apr 17 12:48:17 2017: NS-DB-nx9510-6C87EF : %DATABASE-6-
OPERATION_COMPLETE: backup for database nsight successful

NS-DB-nx9510-6C87EF#

NS-DB-nx9510-6C87EF#database-backup database nsight-placement-info tftp://192.16
8.9.50/plmentinfo
NS-DB-nx9510-6C87EF#show database backup-status
Last Database Backup Status : Successful
Last Database Backup Time   : Mon Apr 17 12:48:48 IST 2017
NS-DB-nx9510-6C87EF#Apr 17 12:49:03 2017: NS-DB-nx9510-6C87EF : %DATABASE-6-
OPERATION_COMPLETE: backup for database nsight-placement-info successful

NS-DB-nx9510-6C87EF#
```

**Related Commands**

| | |
|---|---|
| *database* | Enables automatic repairing (vacuuming) and dropping of databases (captive-portal and NSight) |
| *database-restore* | Restores a previously exported (backed up) database [captive-portal and/or NSight] |

## 3.1.18 database-restore

*Privileged Exec Mode Commands*

Restores a previously exported database [captive-portal and/or NSight]. Previously exported databases (backed up to a specified FTP or SFTP server) are restored from the backed-up location to the original database.

**Supported in the following platforms:**

- Service Platforms — NX9500, NX9510, NX9600, VX9000

**Syntax**

```
database-restore database [captive-portal|nsight] <URL>
```

**Parameters**

- `database-restore database [captive-portal|nsight] <URL>`

| | |
|---|---|
| database-restore database [captive-portal\| nsight] | Restores previously exported (backed up) captive-portal and/or NSight database. Specify the database type:<br>• captive-portal – Restores captive portal database<br>• nsight – Restores NSight database<br>After specifying the database type, configure the destination location and file name from where the files are restored. |
| <URL> | Configures the destination location. The database is restored from the specified location. Specify the location URL in one of the following formats:<br>ftp://<user>:<passwd>@<hostname\|IP>[:port]/path/file.tar.gz<br>sftp://<user>:<passwd>@<hostname\|IP>[:port]/path/file.tar.gz |

**Example**

```
nx9500-6C8809#database-restore database nsight
ftp://anonymous:anonymous@192.168.13.10/backups/nsight/nsight.tar.gz
```

**Related Commands**

| | |
|---|---|
| *database* | Enables automatic repairing (vacuuming) and dropping of databases (captive-portal and NSight) |
| *database-backup* | Backs up captive-portal and/or NSight database to a specified location and file on an FTP or SFTP server |

## 3.1.19 delete

*Privileged Exec Mode Commands*

Deletes a specified file from the device's file system

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

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

**Parameters**

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

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

**Example**

```
rfs6000-81742D#delete flash:/out.tar flash:/out.tar.gz
Delete flash:/out.tar [y/n]? y
Delete flash:/out.tar.gz [y/n]? y

rfs6000-81742D#delete /force flash:/tmp.txt
rrfs6000-81742D#

rfs6000-81742D#delete /recursive flash:/backup/
Delete flash:/backup//fileMgmt_350_180B.core

[y/n]? y
Delete

flash:/backup//fileMgmt_350_18212X.core_bk

[y/n]? n

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

[y/n]? n
rfs6000-81742D#
```

## 3.1.20 device-upgrade

*Privileged Exec Mode Commands*

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

**NOTE:** A NOC controller's capacity is equal to, or higher than that of a site controller. The following devices can be deployed at NOC and sites:

- NOC controller – NX95XX (NX9500 and NX9510), NX9600
- Site controller – RFS4000, RFS6000, NX5500, NX75XX, or NX95XX

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
device-upgrade [<MAC/HOSTNAME>|all|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|
ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|
ap8533|rfs4000|rfs6000|nx5500|nx75xx|nx9000|nx9600|vx9000|cancel-upgrade|load-
image|rf-domain]

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

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

device-upgrade [ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|
ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|rfs6000|
nx5500|nx75xx|nx9000|nx9600|vx9000] all {force|no-reboot|reboot-time <TIME>|
upgrade-time <TIME> {no-reboot|reboot-time <TIME>}} {(staggered-reboot)}

device-upgrade cancel-upgrade [<MAC/HOSTNAME>|all|ap6521|ap6522|ap6532|ap6562|
ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|
ap82xx|ap8432|ap8533|rfs4000|rfs6000|nx75xx|nx9000|nx9600|vx9000|on rf-domain
[<RF-DOMAIN-NAME>|all]]

device-upgrade load-image [ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|
ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|
rfs4000|rfs6000|nx5500|nx75xx|nx9000|nx9600|vx9000] {<IMAGE-URL>|on <DEVICE-OR-
DOMAIN-NAME>}

device-upgrade rf-domain [<RF-DOMAIN-NAME>|all|containing <WORD>|filter location
<WORD>] [all|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|
ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|rfs6000|
nx5500|nx75xx|nx9000|nx9600|vx9000] {(<MAC/HOSTNAME>|force|no-reboot|
from-controller|reboot-time <TIME>|staggered-reboot|upgrade-time <TIME>)}
```

**Parameters**

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

| | |
|---|---|
| <MAC/HOSTNAME> | Upgrades firmware on the device identified by the <MAC/HOSTNAME> keyword<br>• <MAC/HOSTNAME> – Specify the device's MAC address or hostname. |

| | |
|---|---|
| no-reboot | Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted) |
| reboot-time <TIME> | Optional. Schedules an automatic reboot after a successful upgrade<br>• <TIME> – Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format. |
| upgrade-time <TIME> {no-reboot\| reboot-time <TIME>} | Optional. Schedules an automatic device firmware upgrade on a specified day and time<br>• <TIME> – Specify the upgrade time in the MM/DD/YYYY-HH:MM or HH:MM format. The following actions can be performed after a scheduled upgrade:<br>• no-reboot – Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted)<br>• reboot-time <TIME> – Optional. Schedules an automatic reboot after a successful upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format. |

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

| | |
|---|---|
| all | Upgrades firmware on all devices |
| force | Optional. Select this option to force upgrade on the selected device(s). When selected, the devices are upgraded even if they have the same firmware as the upgrading access point, wireless controller, or service platform. If forcing a device upgrade, optionally specify any one of the following options: no-reboot, reboot-time, upgrade-time, or staggered-reboot. |
| no-reboot | Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted) |
| reboot-time <TIME> | Optional. Schedules an automatic reboot after a successful upgrade<br>• <TIME> – Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format. |
| upgrade-time <TIME> {no-reboot\| reboot-time <TIME>} | Optional. Schedules an automatic device firmware upgrade on all devices on a specified day and time<br>• <TIME> – Specify the upgrade time in the MM/DD/YYYY-HH:MM or HH:MM format. The following actions can be performed after a scheduled upgrade:<br>• no-reboot – Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted)<br>• reboot-time <TIME> – Optional. Schedules an automatic reboot after a successful upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format. |
| staggered-reboot | This keyword is recursive and common to all of the above.<br>• Optional. Enables staggered device reboot (one at a time), without network impact |

• `device-upgrade [ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|rfs6000|nx5500|nx75xx|nx9000|nx9600|vx9000] all {force|no-reboot|reboot-time <TIME>|upgrade-time <TIME> {no-reboot|reboot-time <TIME>}} {(staggered-reboot)}`

| | |
|---|---|
| device-upgrade <DEVICE-TYPE> all | Upgrades firmware on all devices of a specific type. Select the device type. The options are: AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533, RFS4000, RFS6000, NX5500, NX75XX, NX95XX, NX9600, and VX9000.<br>After selecting the device type, schedule an automatic upgrade and/or an automatic reboot. |

| | |
|---|---|
| force | Optional. Select this option to force upgrade on selected device(s). When selected, the devices are upgraded even if they have the same firmware as the upgrading access point, wireless controller, or service platform. If forcing a device upgrade, optionally specify any one of the following options: no-reboot, reboot-time, upgrade-time, or staggered-reboot. |
| no-reboot | Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted) |
| reboot-time <TIME> | Optional. Schedules an automatic reboot after a successful upgrade<br>• <TIME> – Optional. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format. |
| upgrade-time <TIME> {no-reboot\| reboot-time <TIME>} | Optional. Schedules an automatic firmware upgrade on all devices of the specified type, on a specified day and time<br>• <TIME> – Specify the upgrade time in the MM/DD/YYYY-HH:MM or HH:MM format. The following actions can be performed after a scheduled upgrade:<br>• no-reboot – Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted)<br>• reboot-time <TIME> – Optional. Schedules an automatic reboot after a successful upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format. |
| staggered-reboot | This keyword is recursive and common to all of the above.<br>• Optional. Enables staggered device reboot (one at a time), without network impact |

```
• device-upgrade cancel-upgrade [<MAC/HOSTNAME>|all|ap6521|ap6522|ap6532|
ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|
ap81xx|ap82xx|ap8432|ap8533|rfs4000|rfs6000|nx5500|nx75xx|nx9000|nx9600|vx9000|
on rf-domain [<RF-DOMAIN-NAME>|all]]
```

| | |
|---|---|
| cancel-upgrade | Cancels a scheduled firmware upgrade based on the parameters passed. This command provides the following options to cancel scheduled firmware upgrades:<br>• Cancels upgrade on specific device(s). The devices are identified by their MAC addresses or hostnames.<br>• Cancels upgrade on all devices within the network<br>• Cancels upgrade on all devices of a specific type. Specify the device type.<br>• Cancels upgrade on specific device or all device(s) within a specific RF Domain or all RF Domains. Specify the RF Domain name. |
| cancel-upgrade [<MAC/HOSTNAME>\| all] | Cancels a scheduled firmware upgrade on a specified device or on all devices<br>• <MAC/HOSTNAME> – Cancels a scheduled upgrade on the device identified by the <MAC/HOSTNAME> keyword. Specify the device's MAC address or hostname.<br>• all – Cancels scheduled upgrade on all devices |
| cancel-upgrade <DEVICE-TYPE> all | Cancels scheduled firmware upgrade on all devices of a specific type. Select the device type. The options are: AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533, RFS4000, RFS6000, NX5500, NX75XX, NX9500, NX9600, and VX9000. |
| cancel-upgrade on rf-domain [<RF-DOMAIN-NAME>\| all] | Cancels scheduled firmware upgrade on all devices in a specified RF Domain or all RF Domains<br>• <RF-DOMAIN-NAME> – Cancels scheduled device upgrade on all devices in a specified RF Domain. Specify the RF Domain name.<br>• all – Cancels scheduled device upgrade on all devices across all RF Domains |

- `device-upgrade load-image [ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|rfs6000|nx5500|nx75xx|nx9000|nx9600|vx9000] {<IMAGE-URL>|on <DEVICE-OR-DOMAIN-NAME>}`

| | |
|---|---|
| load-image <DEVICE-TYPE> | Loads device firmware image from a specified location. Select the device type and provide the location of the required device firmware image.<br>• <DEVICE-TYPE> – Specify the device type. The options are: AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533, RFS4000, RFS6000, NX5500, NX75XX, NX95XX, NX9600, and VX9000. After specifying the device type, provide the location of the required device firmware image. |
| <IMAGE-URL> | Specify the device's firmware image location in one of the following formats:<br>IPv4 URLs:<br>tftp://<hostname\|IP>[:port]/path/file<br>ftp://<user>:<passwd>@<hostname\|IP>[:port]/path/file<br>sftp://<user>:<passwd>@<hostname\|IP>[:port]>/path/file<br>http://<hostname\|IP>[:port]/path/file<br>cf:/path/file<br>usb<n>:/path/file<br>IPv6 URLs:<br>tftp://<hostname\|[IPv6]>[:port]/path/file<br>ftp://<user>:<passwd>@<hostname\|[IPv6]>[:port]/path/file<br>sftp://<user>:<passwd>@<hostname\|[IPv6]>[:port]>/path/file<br>http://<hostname\|[IPv6]>[:port]/path/file |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Specifies the name of a device or RF Domain. The image, of the specified device type is loaded from the device specified here. In case of an RF Domain, the image available on the RF Domain manager is loaded.<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |

- `device-upgrade rf-domain [<RF-DOMAIN-NAME>|all|containing <WORD>|filter location <WORD>] [all|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|rfs6000|nx5500|nx75xx|nx9000|nx9600|vx9000] {(<MAC/HOSTNAME>|force|from-controller|no-reboot|reboot-time <TIME>|staggered-reboot|upgrade-time <TIME>)}`

| | |
|---|---|
| rf-domain [<RF-DOMAIN-NAME>\|all\| containing <WORD>\| filter location <WORD>] | Upgrades firmware on devices in a specified RF Domain or all RF Domains. Devices within a RF Domain are upgraded through the RF Domain manager.<br>• <RF-DOMAIN-NAME> – Upgrades devices in the RF Domain identified by the <RF-DOMAIN-NAME> keyword.<br>  • <RF-DOMAIN-NAME> – Specify the RF Domain name.<br>• all – Upgrades devices across all RF Domains<br>• containing <WORD> – Filters RF Domains by their names. RF Domains with names containing the sub-string identified by the <WORD> keyword are filtered. Devices on the filtered RF Domains are upgraded.<br>  • filter location <WORD> – Filters devices by their location. All devices with location matching the <WORD> keyword are upgraded. |

| | |
|---|---|
| <DEVICE-TYPE> | After specifying the RF Domain, select the device type. The options are: AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533, RFS4000, RFS6000, NX5500, NX75XX, NX95XX, NX9600, and VX9000.<br>After specifying the RF Domain and the device type, configure any one of the following actions: force devices to upgrade, or initiate an upgrade through the adopting controller. |
| <MAC/HOSTNAME> | Optional. Use this option to identify specific devices for upgradation. Specify the device's MAC address or hostname. The device should be within the specified RF Domain and of the specified device type. After identifying the devices to upgrade, configure any one of the following actions: force devices to upgrade, or initiate an upgrade through the adopting controller.<br>**Note:** If no MAC address or hostname is specified, all devices of the type selected are upgraded. |
| force | Optional. Select this option to force upgrade for the selected device(s). When selected, the devices are upgraded even if they have the same firmware as the upgrading access point, wireless controller, or service platform. If forcing a device upgrade, optionally specify any one of the following options: no-reboot, reboot-time, upgrade-time, or reboot-time. |
| from-controller | Optional. Upgrades a device through the adopted device. If initiating an upgrade through the adopting controller, optionally specify any one of the following options: no-reboot, reboot-time, upgrade-time, or reboot-time. |
| no-reboot {staggered-reboot} | Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted) |
| reboot-time <TIME> {staggered-reboot} | Optional. Schedules an automatic reboot after a successful upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format. |
| staggered-reboot | This keyword is common to all of the above.<br>Optional. Enables staggered reboot (one at a time), without network impact |
| upgrade-time <TIME> {no-reboot\| reboot-time <TIME>} | Optional. Schedules an automatic firmware upgrade<br>• <TIME> – Specify the upgrade time in the MM/DD/YYYY-HH:MM or HH:MM format. After a scheduled upgrade, the following actions can be performed:<br>• no-reboot – Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted)<br>• reboot-time <TIME> – Optional. Schedules an automatic reboot after a successful upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format. |

**Example**

```
nx9500-6C8809#show device-upgrade history on TechPubs
-------------------------------------------------------------------------------
-----------------
            Device      RESULT                 TIME  RETRIES        UPGRADED-BY
LAST-UPDATE-ERROR
-------------------------------------------------------------------------------
-----------------

    rfs6000-81742D        done  2017-07-20 14:16:49        0      nx9500-6C8809 -

    rfs6000-81742D        done  2017-07-06 15:19:23        0      nx9500-6C8809 -

    rfs6000-81742D        done  2017-07-06 15:15:37        0      nx9500-6C8809 -
--More--
nx9500-6C8809#
```

```
nx9500-6C8809#device-upgrade load-image rfs6000 ftp://anonymous:anonymous@192.16
8.13.17/RFS6000-LEAN-5.9.1.0-017D.img
-------------------------------------------------------------------------------
      CONTROLLER          STATUS                      MESSAGE
-------------------------------------------------------------------------------
  nx9500-6C8809        Success        Successfully initiated load image
-------------------------------------------------------------------------------
nx9500-6C8809#

nx9500-6C8809#show device-upgrade load-image-status
Download of rfs6000 firmware file is 50 percent complete
nx9500-6C8809#

nx9500-6C8809#device-upgrade rfs6000-81742D
-------------------------------------------------------------------------------
         CONTROLLER             STATUS                   MESSAGE
-------------------------------------------------------------------------------
  B4-C7-99-6C-88-09         Success         Queued 1 devices to upgrade
-------------------------------------------------------------------------------
nx9500-6C8809#show device-upgrade status
Number of devices currently being upgraded : 0
Number of devices waiting in queue to be upgraded : 1
Number of devices currently being rebooted : 0
Number of devices waiting in queue to be rebooted : 0
Number of devices failed upgrade : 0
-------------------------------------------------------------------------------
-------------------------
      DEVICE        STATE   UPGRADE TIME REBOOT TIME PROGRESS RETRIES LAST UPDATE
ERROR   UPGRADED BY
-------------------------------------------------------------------------------
-------------------------
  rfs6000-81742D   waiting   immediate    immediate   0       0      -
nx9500-6C8809
-------------------------------------------------------------------------------
-------------------------
nx9500-6C8809#
```

## 3.1.21 diff

*Privileged Exec Mode Commands*

Displays the differences between two files on a device's file system or a particular URL

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
diff [<FILE>|<URL>] [<FILE>|<URL>]
```

**Parameters**

- `diff [<FILE>|<URL>] [<FILE>|<URL>]`

| | |
|---|---|
| <FILE> | The first <FILE> is the source file for the diff command. The second <FILE> is used for comparison. |
| <URL> | The first <URL> is the source file's URL. The second <URL> is the second file's URL. |

**Example**

```
nx9500-6C8809#diff startup-config running-config
--- startup-config
+++ running-config
@@ -1,12 +1,10 @@
+!### show running-config
 !
 ! Configuration of NX9500 version 5.9.1.0-012D
 !
 !
 version 2.5
 !
-password-encryption-version 1.0
-inline-password-encryption
-password-encryption-key secret 2
776f9d6d5bb08fac753394d779cbc5a200000020a4ca26def55d4d77952308cd5e3afc66c06581bb
1e5af6d6b033fd664c363522
 !
 client-identity-group default
  load default-fingerprints
@@ -35,13 +33,13 @@
 !
 alias string $IN-Blr-EcoSpace-Floor-4 IBEF4
 !
-alias encrypted-string $READ 2 LKSXiTieTV5hybKxfbd6JwAAAAZ/lakoqHh/ZfyHLJWzluTH
+alias encrypted-string $READ 2 1og6ZeMyEVJhybKxfbd6JwAAAAahnGq6RaJb70CEIbVpTYre
--More--
nx9500-6C8809#
```

## 3.1.22 dir

*Privileged Exec Mode Commands*

Lists files on a device's file system

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
dir {/all|/recursive|<DIR>|all-filesystems}
```

**Parameters**

- `dir {/all|/recursive|<DIR>|all-filesystems}`

| | |
|---|---|
| /all | Optional. Lists all files |
| /recursive | Optional. Lists files recursively |
| <DIR> | Optional. Lists files in the named file path |
| all-filesystems | Optional. Lists files on all file systems |

**Example**

```
nx9500-6C8809#dir flash:/
Directory of flash:/

  -rw-    62937     Tue Nov 24 16:00:06 2015   run-config-backup.txt
  drwx              Tue Nov 29 09:48:42 2016   crashinfo
  drwx              Sat Sep 17 05:14:43 2016   upgrade
  drwx              Mon Sep 28 09:48:33 2015   tmptpd
  drwx              Wed Feb 15 11:53:07 2017   log
  drwx              Wed Feb 15 11:02:55 2017   archived_logs
  drwx              Tue May 24 22:23:54 2016   cache
  drwx              Thu Feb 19 08:53:45 2015   floorplans
  -rw-    42018304  Tue Sep 27 10:19:24 2016   in.tar
  drwx              Tue Jan 17 10:02:01 2017   hotspot

nx9500-6C8809#

nx9500-6C8809#dir all-filesystems
Directory of flash:/

  -rw-    62937     Tue Nov 24 16:00:06 2015   run-config-backup.txt
  drwx              Tue Nov 29 09:48:42 2016   crashinfo
  drwx              Sat Sep 17 05:14:43 2016   upgrade
  drwx              Mon Sep 28 09:48:33 2015   tmptpd
  drwx              Wed Feb 15 11:53:07 2017   log
  drwx              Wed Feb 15 11:02:55 2017   archived_logs
  drwx              Tue May 24 22:23:54 2016   cache
  drwx              Thu Feb 19 08:53:45 2015   floorplans
  -rw-    42018304  Tue Sep 27 10:19:24 2016   in.tar
  drwx              Tue Jan 17 10:02:01 2017   hotspot

Directory of nvram:/

  lrwx    29        Tue Oct 27 16:22:21 2015   sensor_default_scan

--More--
nx9500-6C8809#
```

## 3.1.23 disable

*Privileged Exec Mode Commands*

Turns off (disables) the privileged mode command set. This command returns to the User Executable mode.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
disable
```

**Parameters**

None

**Example**

```
rfs6000-81742D#disable
rfs6000-81742D>
```

## 3.1.24 edit

*Privileged Exec Mode Commands*

Edits a text file on the device's file system

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
edit <FILE>
```

**Parameters**

```
• edit <FILE>
```

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

**Example**

```
rfs4000-880DA7#edit startup-config
  GNU nano 1.2.4               File: startup-config

!
! Configuration of RFS4000 version 5.9.1.0-015D

!
!
version 2.5
!
password-encryption-version 1.0
inline-password-encryption
no password-encryption-key
!
client-identity-group default
 load default-fingerprints
!
ip snmp-access-list default
 permit any
!
firewall-policy default
 no ip dos tcp-sequence-past-window
!
                                [ Read 400 lines ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Txt ^T To Spell
```

## 3.1.25 enable

*Privileged Exec Mode Commands*

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

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
enable
```

**Parameters**

None

**Example**

```
rfs6000-81742D#enable
rfs6000-81742D#
```

## 3.1.26 erase

*Privileged Exec Mode Commands*

Erases a device's (wireless controller, access point, and service platform) file system. Erases the content of the specified storage device. Also erases the startup configuration to restore the device to its default.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
erase [flash:|nvram:|startup-config|usb1:|usb2:|usb3:|usb4:]

erase [flash:|nvram:|usb1:|usb2:|usb3:|usb4:]

erase startup-config {<HOSTNAME/MAC>|on <DOMAIN-NAME> {containing <SUB-STRING>|
exclude-controllers|exclude-rf-domain-manager|filter <DEVICE-TYPE>}}
```

**Parameters**

- `erase [flash:|nvram:|usb1:|usb2:|usb3:|usb4:]`

| | |
|---|---|
| flash: | Erases everything in the device's flash: file |
| nvram: | Erases everything in the device's nvram: file |
| startup-config | Erases the device's startup configuration file. The startup configuration file is used to configure the device when it reboots. |
| usb1: | Erases everything in the device's usb1: file |
| usb2: | Erases everything in the device's usb2: file |
| usb3: | Erases everything in the device's usb3: file |
| usb4: | Erases everything in the device's usb4: file |

- `erase startup-config {<HOSTNAME/MAC>|on <DOMAIN-NAME> {containing <SUB-STRING>| exclude-controllers|exclude-rf-domain-manager|filter <DEVICE-TYPE>}}`

| | |
|---|---|
| startup-config: | Erases the startup configuration file on a specified device or devices in a specified RF Domain. The specified device(s) are reloaded after the startup configuration file is erased. Use the '<HOSTNAME/MAC>' or 'on <DOMAIN-NAME>' options to identify the device or RF Domain respectively. Once executed, the configuration file, for the targeted device or for all device(s) in the targeted RF Domain, is also erased from the adopting controller's configuration file. The are automatically reloaded once the startup configuration file has been erased. |
| <HOSTNAME/MAC> | Optional. Erases the startup configuration file on the device identified by the <HOSTNAME/MAC> keyword. Specify the device's hostname or MAC address. |

| | |
|---|---|
| on <DOMAIN-NAME> {containing <SUB-STRING>\| exclude-controllers\| exclude-rf-domain-manager\| filter <DEVICE-TYPE>} | Optional. Erases the startup configuration file on all devices or specified device(s) in a specified RF Domain<br>• <DOMAIN-NAME> – Specify the RF Domain name. After specifying the RF Domain, optionally use the filters provided to identify specific device(s) within the RF Domain. If none of the filters are used, the command is executed on all devices within the RF Domain. These filters are:<br>• containing <SUB-STRING> – Optional. Executes the command on all devices containing a specified sub-string in their hostname<br>• <SUB-STRING> – Specify the sub-string to match. The startup configuration file is erased on all devices whose hostname contains the sub-string specified here.<br>• exclude-controllers – Optional. Executes the command on all devices excluding controllers. The startup configuration file is erased on all devices except controllers.<br>• exclude-rf-domain-manager – Optional. Executes the command on all devices excluding RF Domain managers. The startup configuration file is erased on all devices except RF Domain managers.<br>• filter <DEVICE-TYPE> – Optional. Executes the command on all devices of a specified type<br>• <DEVICE-TYPE> – Specify the device type. The options are: AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8532, AP8432, AP8533, RFS4000, RFS6000, NX5500, NX75XX, NX95XX, NX9600, and VX9000. The startup configuration file is erased on all devices of the type specified here. For example, if AP6521 is the device-type specified, the startup configuration file on all AP6521s, within the RF Domain, is erased. |

**Example**

```
nx9500-6C8809#erase ?
  cf:             Erase everything in cf:
  flash:          Erase everything in flash:
  nvram:          Erase everything in nvram:
  startup-config  Reset configuration to factory default
  usb1:           Erase everything in usb1:
  usb2:           Erase everything in usb2:

nx9500-6C8809#
```

## 3.1.27 ex3500

*Privileged Exec Mode Commands*

Enables EX3500 switch firmware management. Use this command to perform the following operations: boot, copy, delete, and IP-related configurations.

The copy keyword provides multiple copy options. It allows you to upload or download code images or configuration files between the switch's flash memory and an FTP/TFTP server. When you save the system code or configuration settings to a file on an FTP/TFTP server, that file can later be downloaded to the switch to restore system operation. The success of the file transfer depends on the accessibility of the FTP/TFTP server and the quality of the network connection.

**Supported in the following platforms:**

- Service Platforms — NX9500, NX9510, NX9600

**Syntax**

```
ex3500 [adoptd|boot|copy|delete|ip]

ex3500 adoptd upgrade <URL> on <EX3500-DEVICE-NAME>

ex3500 boot system <1-1> (config|opcode) <FILE-NAME> on <EX3500-DEVICE-NAME>

ex3500 copy [file|ftp|running-config|startup-config|tftp|unit]

ex3500 copy [file file <SOURCE-FILE-NAME> <DEST-FILE-NAME> on <EX3500-DEVICE-NAME>

ex3500 copy [ftp|tftp] [add-to-running-config|file|https-certificate|public-key|
running-config|startup-config]

ex3500 copy [ftp|tftp] add-to-running-config <FTP/TFTP-SERVER-IP> <USER-NAME>
<PASSWORD> <SOURCE-FILE-NAME> on <EX3500-DEVICE-NAME>

ex3500 copy [ftp|tftp] file <FTP/TFTP-SERVER-IP> <USER-NAME> <PASSWORD> [1|2]
<SOURCE-FILE-NAME> <DEST-FILE-NAME> on <EX3500-DEVICE-NAME>

ex3500 copy [ftp|tftp] https-certificate <FTP/TFTP-SERVER-IP> <USER-NAME>
<PASSWORD> <SOURCE-CERT-FILE-NAME> <SOURCE-PVT-KEY-FILE-NAME> <PVT-PASS-WORD>
on <EX3500-DEVICE-NAME>

ex3500 copy [ftp|tftp] public-key <FTP/TFTP-SERVER-IP> <USER-NAME> <PASSWORD>
[1|2] <SOURCE-PUB-KEY-FILE-NAME> <USER-NAME> on <EX3500-DEVICE-NAME>

ex3500 copy [ftp|tftp] [running-config|startup-config] <FTP/TFTP-SERVER-IP> <USER-
NAME> <PASSWORD> <SOURCE-CONFIG-FILE-NAME> on <EX3500-DEVICE-NAME>

ex3500 copy running-config [file <DEST-FILE-NAME>|ftp <FTP-SERVER-IP> <USER-NAME>
<PASSWORD> <DEST-FILE-NAME>|startup-config|tftp <TFTP-SERVER-IP> <DEST-FILE-
NAME>] on <EX3500-DEVICE-NAME>

ex3500 copy startup-config [file <DEST-FILE-NAME>|ftp <FTP-SERVER-IP> <USER-NAME>
<PASSWORD> <DEST-FILE-NAME>|running-config|tftp <TFTP-SERVER-IP> <DEST-FILE-
NAME>] on <EX3500-DEVICE-NAME>

ex3500 copy unit file <1-1> [1|2] <SOURCE-FILE-NAME> <DEST-FILE-NAME> on <EX3500-
DEVICE-NAME>

ex3500 delete [file|public-key]

ex3500 delete file [name <FILE-NAME>|unit <1-1> name <FILE-NAME>] on <EX3500-
DEVICE-NAME>

ex3500 delete public-key <USER-NAME> [dsa|rsa] on <EX3500-DEVICE-NAME>
```

```
ex3500 ip ssh [crypto|save]

ex3500 ip ssh crypto host-key generates [dsa|rsa] on <EX3500-DEVICE-NAME>

ex3500 ip ssh crypto zeroize [dsa|rsa] on <EX3500-DEVICE-NAME>

ex3500 ip ssh save host-key on <EX3500-DEVICE-NAME>
```

**Parameters**

- `ex3500 adoptd upgrade <URL> on <EX3500-DEVICE-NAME>`

| | |
|---|---|
| ex3500 adoptd upgrade | Upgrades an adopted EX3500 switch<br>**Note:** After an upgrade, reboot the EX3500 switch to initiate the new image. To view an EX3500's current image version, use the *show > version > on* <EX3500-*DEVICE-NAME*> command. |
| <URL> | Specifies the location and image file name in the following format:<br>tftp://<IP>[/path]/file |
| on <EX3500-DEVICE-NAME> | Executes the command on a specified EX3500 switch<br>• <EX3500-DEVICE-NAME> – Specify the EX3500 switch's hostname. |

- `ex3500 boot system <1-1> (config|opcode) <FILE-NAME> on <EX3500-DEVICE-NAME>`

| | |
|---|---|
| ex3500 boot system | Boots a EX3500 switch using a specified configuration file |
| <1-1> | Identifies the EX3500 unit by its ID number. Specify the EX3500 ID from 1 - 1.<br>**Note:** As of now only one (1) EX3500 unit can be managed through a NOC controller. |
| (config\|opcode) <FILE-NAME> | The following keywords are recursive:<br>Specifies the image file to use for booting. The options are:<br>• config – Uses the configuration file to boot the switch<br>• opcode – Uses the *Operation Code* (opcode), which is the runtime code, to boot the switch. The opcode is like an operating system that enables the WiNG software to communicate with the EX3500 device.<br>The following parameter is common to the 'config' and opcode' keywords:<br>• <FILE-NAME> – Specify the configuration/runtime-code file name. |
| on <EX3500-DEVICE-NAME> | Reloads a specified EX3500 switch<br>• <EX3500-DEVICE-NAME> – Specify the EX3500 switch's hostname. You can also specify its MAC address. |

- `ex3500 copy file file <SOURCE-FILE-NAME> <DEST-FILE-NAME> on <EX3500-DEVICE-NAME>`

| | |
|---|---|
| ex3500 copy | Copies a configuration file to another file |
| file file <SOURCE-FILE-NAME> <DEST-FILE-NAME> | Copies a specified file (this is the source configuration file)<br>• file – Copies the specified source file to a specified file (this is the destination configuration file)<br>• <SOURCE-FILE-NAME> – Specify the source configuration file's name<br>• <DEST-FILE-NAME> – Specify the destination configuration file's name.<br>Contd.. |

| | |
|---|---|
| | When specifying the destination file name, keep in mind the following points:<br>- It should not contain slashes (\ or /),<br>- It should not exceed 32 characters for files on the switch, or 127 characters for files on the server. |
| on <EX3500-DEVICE-NAME> | Copies the file to a specified EX3500 switch<br>• <EX3500-DEVICE-NAME> – Specify the EX3500 switch's hostname. The specified source file is copied to specified destination file on the EX3500 identified here. |

• `ex3500 copy [ftp|tftp] add-to-running-config <FTP/TFTP-SERVER-IP> <USER-NAME> <PASSWORD> <SOURCE-FILE-NAME> on <EX3500-DEVICE-NAME>`

| | |
|---|---|
| ex3500 copy [ftp\|tftp] | Copies files from a FTP or TFTP server. This command allows you to copy the following types of files: HTTPS certificate, running configuration, startup configuration, public key, etc.<br>This command also allows you to add a remote system's running configuration to the current system configuration. |
| add-to-running-config | Adds a remote system's running configuration to the current system |
| <FTP/TFTP-SERVER-IP> <USER-NAME> <PASSWORD> | Configures the FTP or TFTP server details (depending on the option selected in the previous step), such as IP address and user credentials. This is the device running the FTP/TFTP server.<br>• <FTP/TFTP-SERVER-IP> – Specify the FTP or TFTP server's IP address in the A.B.C.D format.<br>• <USER-NAME> – If using a FTP server, specify the FTP server's user name (should be an authorized user)<br>• <PASSWORD> – Specify the password applicable for the above specified FTP server user name. |
| <SOURCE-FILE-NAME> | After specifying the server details, specify the name of the running configuration file.<br>• <SOURCE-FILE-NAME> – Specify the source file's name. |
| on <EX3500-DEVICE-NAME> | Copies the file to a specified EX3500 switch<br>• <EX3500-DEVICE-NAME> – Specify the EX3500 switch's hostname. The specified source file is copied to specified destination file on the EX3500 identified here. |

• `ex3500 copy [ftp|tftp] file <FTP/TFTP-SERVER-IP> <USER-NAME> <PASSWORD> [1|2] <SOURCE-FILE-NAME> <DEST-FILE-NAME> on <EX3500-DEVICE-NAME>`

| | |
|---|---|
| ex3500 copy [ftp\|tftp] | Copies files from a FTP or TFTP server. This command allows you to copy the following types of files: HTTPS certificate, running configuration, startup configuration, public key, etc. |
| file | Copies to a specified file system |
| <FTP/TFTP-SERVER-IP> <USER-NAME> <PASS-WORD> | Configures the FTP or TFTP server details (depending on the option selected in the previous step), such as IP address and user credentials. This is the device running the FTP/TFTP server.<br>• <FTP/TFTP-SERVER-IP> – Specify the FTP or TFTP server's IP address in the A.B.C.D format.<br>• <USER-NAME> – If using a FTP server, specify the FTP server's user name (should be an authorized user)<br>• <PASSWORD> – Specify the password applicable for the above specified FTP server user name. |

| | |
|---|---|
| [1\|2] <SOURCE-FILE-NAME> <DEST-FILE-NAME> | After specifying the server details, select the file type and specify the name of the source and destination file names.<br>• [1\|2] – Select the file type from 1 - 2.<br>• 1 – Copies the EX3500 configuration file.<br>• 2 – Copies the opcode, which is the runtime code. The opcode is like an operating system that enables the WiNG software to communicate with the EX3500 device.<br>• <SOURCE-FILE-NAME> – Specify the source file's name.<br>• <DEST-FILE-NAME> – Specify the destination file's name. |
| on <EX3500-DEVICE-NAME> | Copies the file to a specified EX3500 device<br>• <EX3500-DEVICE-NAME> – Specify the EX3500 device's hostname. The specified source file is copied to specified destination file on the EX3500 identified here. |

• `ex3500 copy [ftp|tftp] https-certificate <FTP/TFTP-SERVER-IP> <USER-NAME> <PASSWORD> <SOURCE-CERT-FILE-NAME> <SOURCE-PVT-KEY-FILE-NAME> <PVT-PASS-WORD> on <EX3500-DEVICE-NAME>`

| | |
|---|---|
| ex3500 copy [ftp\|tftp] | Copies files from a FTP or TFTP server. This command allows you to copy the following types of files: HTTPS certificate, running configuration, startup configuration, public key, etc. |
| https-certificate | Copies HTTPS secure site certificate from the FTP or TFTP server to the switch |
| <FTP/TFTP-SERVER-IP> <USER-NAME> <PASSWORD> | Configures the FTP or TFTP server details (depending on the option selected in the previous step), such as IP address and user credentials. This is the device running the FTP/TFTP server.<br>• <FTP/TFTP-SERVER-IP> – Specify the FTP or TFTP server's IP address in the A.B.C.D format.<br>• <USER-NAME> – If using a FTP server, specify the FTP server's user name (should be an authorized user)<br>• <PASSWORD> – Specify the password applicable for the above specified FTP server user name. |
| <SOURCE-CERT-FILE-NAME> <SOURCE-PVT-KEY-FILE-NAME> <PVT-PASS-WORD> | After identifying the FTP or TFTP server, specify the following:<br>• <SOURCE-CERT-FILE-NAME> – Specify the source HTTPS secure site certificate file name.<br>• <SOURCE-PVT-KEY-FILE-NAME> – Specify the source private-key file name.<br>• <PVT-PASS-WORD> – Specify the private password. |
| on <EX3500-DEVICE-NAME> | Copies the file to a specified EX3500 device<br>• <EX3500-DEVICE-NAME> – Specify the EX3500 device's hostname. |

• `ex3500 copy [ftp|tftp] public-key <FTP/TFTP-SERVER-IP> <USER-NAME> <PASSWORD> [1|2] <SOURCE-PUB-KEY-FILE-NAME> <USER-NAME> on <EX3500-DEVICE-NAME>`

| | |
|---|---|
| ex3500 copy [ftp\|tftp] | Copies files from a FTP or TFTP server. This command allows you to copy the following types of files: HTTPS certificate, running configuration, startup configuration, public key, etc. |
| public-key | Copies the SSH public key from the FTP or TFTP server to the switch |

| | |
|---|---|
| <FTP/TFTP-SERVER-IP> <USER-NAME> <PASSWORD> | Configures the FTP or TFTP server details (depending on the option selected in the previous step), such as IP address and user credentials. This is the device running the FTP/TFTP server.<br>• <FTP/TFTP-SERVER-IP> – Specify the FTP or TFTP server's IP address in the A.B.C.D format.<br>• <USER-NAME> – If using a FTP server, specify the FTP server's user name (should be an authorized user)<br>• <PASSWORD> – Specify the password applicable for the above specified FTP server user name. |
| [1\|2] <SOURCE-PUB-KEY-FILE-NAME> <USER-NAME> | After identifying the FTP or TFTP server, specify the following:<br>• [1\|2] – Configures the SSH public key type as RS or DSA<br>• 1 – Configures the public key type as RSA<br>• 2 – Configures the public key type as DSA<br>• <SOURCE-PUB-KEY-FILE-NAME> – Specifies the source public key file name<br>• <USER-NAME> – Specifies the public key's user name. |
| on <EX3500-DEVICE-NAME> | Copies the public key to a specified EX3500 device<br>• <EX3500-DEVICE-NAME> – Specify the EX3500 device's hostname. |

```
• ex3500 copy [ftp|tftp] [running-config|startup-config] <FTP/TFTP-SERVER-IP>
<USER-NAME> <PASSWORD> <DEST-FILE-NAME> on <EX3500-DEVICE-NAME>
```

| | |
|---|---|
| ex3500 copy [ftp\|tftp] | Copies files from a FTP or TFTP server. This command allows you to copy the following types of files: HTTPS certificate, running configuration, startup configuration, public key, etc. |
| [running-config\| startup-config] | Copies the running or startup configuration file to one of the following destinations: file system, FTP server, or TFTP server<br>The running configuration file can be copied to the startup configuration file and vice versa. |
| <FTP/TFTP-SERVER-IP> <USER-NAME> <PASSWORD> | If copying to a FTP/TFTP server, configure the following parameters:<br>• <FTP/TFTP-SERVER-IP> – Specify the FTP or TFTP server's IP address in the A.B.C.D format.<br>• <USER-NAME> – If using a FTP server, specify the FTP server's user name (should be an authorized user)<br>• <PASSWORD> – Specify the password applicable for the above specified FTP server user name. |
| <DEST-FILE-NAME> | Configures the destination file name. The running or startup configuration file is copied to the specified destination file.<br>• <DEST-FILE-NAME> – Specify the destination file name. You can also copy the running configuration file to the startup configuration file and vice versa. |
| on <EX3500-DEVICE-NAME> | Copies the running or startup configuration file on to a specified EX3500 device<br>• <EX3500-DEVICE-NAME> – Specify the EX3500 device's hostname. |

```
• ex3500 copy unit file <1-1> [1|2] <SOURCE-FILE-NAME> <DEST-FILE-NAME>
on <EX3500-DEVICE-NAME>
```

| | |
|---|---|
| ex3500 copy unit | Copies from a EX3500 switch |

| | |
|---|---|
| file <1-1> [1\|2] | Copies the file system from the EX3500 switch identified by the unit number<br>• <1-1> – Specify the unit number from 1 - 1.<br>• [1\|2] – Select the file type from 1 - 2.<br>• 1 – Copies the selected unit's configuration file.<br>• 2 – Copies the selected unit's opcode, which is the runtime code. The opcode is like an operating system that enables the WiNG software to communicate with the EX3500 device. |
| <SOURCE-FILE-NAME> | Configures the source file name<br>• <SOURCE-FILE-NAME> – Specify the source file name. You can copy the running configuration file to the startup configuration file and vice versa. |
| <DEST-FILE-NAME> | Configures the destination file name. The running or startup configuration file is copied to the specified file.<br>• <DEST-FILE-NAME> – Specify the destination file name. You can copy the running configuration file to the startup configuration file and vice versa. |
| on <EX3500-DEVICE-NAME> | Copies the running or startup configuration file on to a specified EX3500 device<br>• <EX3500-DEVICE-NAME> – Specify the EX3500 device's hostname. |

- `ex3500 delete file [name <FILE-NAME>|unit <1-1> name <FILE-NAME>] on <EX3500-DEVICE-NAME>`

| | |
|---|---|
| ex3500 delete file | Deletes a file or image on a specified EX3500 device |
| name <FILE-NAME> | Specifies the file to delete. The specified file is deleted.<br>• <FILE-NAME> – Specify the file name. |
| unit <1-1><br>name <FILE-NAME> | Identifies the unit in the stackable system on which the file is located<br>• <1-1> – Select the unit from 1 - 1.<br>• name – After identifying the unit, specify the file to delete. The specified file is deleted.<br>• <FILE-NAME> – Specify the file name. |
| on <EX3500-DEVICE-NAME> | Executes the command on a specified EX3500 device<br>• <EX3500-DEVICE-NAME> – Specify the EX3500 device's hostname. |

- `ex3500 delete public-key <USER-NAME> [dsa|rsa] on <EX3500-DEVICE-NAME>`

| | |
|---|---|
| ex3500 delete public-key <USER-NAME> [dsa\|rsa] | Deletes a specified user's public key<br>• <USER-NAME> – Specify the SSH user's name.<br>• dsa – Deletes the specified user's DSA (version 2) key<br>• rsa – Deletes the specified user's RSA (version 1) key |
| on <EX3500-DEVICE-NAME> | Executes the command on a specified EX3500 device<br>• <EX3500-DEVICE-NAME> – Specify the EX3500 device's hostname. |

- `ex3500 ip ssh crypto host-key generates [dsa|rsa] on <EX3500-DEVICE-NAME>`

| | |
|---|---|
| ex3500 ip ssh crypto host-key generates [dsa\|rsa] | Generates the host-key pair (public and private). This host key is used by the SSH server to negotiate a session key and encryption method with the client trying to connect to it.<br>• dsa – Generates DSA (version 2) key type<br>• rsa – Generates RSA (version 1) key type<br>**Note:** The RSA Version 1 is used only for SSHv1.5 clients, whereas DSA Version 2 is used only for SSHv2 clients.<br>**Note:** This generated host-key pair is stored in the volatile memory (i.e RAM). To save the host-key pair in the flash memory, use the *ex3500 > ip > ssh > save > host-key* command. |
| on <EX3500-DEVICE-NAME> | Executes the command on a specified EX3500 device<br>• <EX3500-DEVICE-NAME> – Specify the EX3500 device's hostname. |

- `ex3500 ip ssh zeroize [dsa|rsa] <EX3500-DEVICE-NAME>`

| | |
|---|---|
| ex3500 ip ssh zeroize [dsa\|rsa] | Removes the host-key (DSA and RSA) from the volatile memory (i.e. RAM) |
| on <EX3500-DEVICE-NAME> | Executes the command on a specified EX3500 device<br>• <EX3500-DEVICE-NAME> – Specify the EX3500 device's hostname. |

- `ex3500 ip ssh save host-key on <EX3500-DEVICE-NAME>`

| | |
|---|---|
| ex3500 ip ssh save host-key | Saves the host-key (DSA and RSA) to the flash memory |
| on <EX3500-DEVICE-NAME> | Executes the command on a specified EX3500 device<br>• <EX3500-DEVICE-NAME> – Specify the EX3500 device's hostname. |

**Usage Guidelines**

When using the ex3500 command and its parameters, keep in mind the following:

- Destination file names should not:
  - Contain slashes (\ or /),
  - Exceed 32 characters for files on the switch, or 127 characters for files on the server
- The FTP server's default user name is set as "anonymous".
- The Boot ROM and Loader cannot be uploaded or downloaded from the FTP/TFTP server. Follow instructions provided in the release notes for new firmware, or contact your distributor for help.
- The "Factory_Default_Config.cfg" can be used as the source to copy from, but cannot be used as the destination.
- Although the switch supports only two operation code files, the maximum number of user-defined configuration files supported is 16.

**Example**

```
nx9500-6C8809#ex3500 adopted upgrade tftp://192.168.0.99/ex3500-adopted-
5.8.5.0.img on
ex3524-ED5EAC
Flash programming started
Flash programming completed
Successful
nx9500-6C8809#


nx9500-6C8809#ex3500 copy tftp file 10.2.0.100 1 m360.bix m360.bix on ex3524-ED5EAC
\Write to FLASH Programming.
-Write to FLASH finish.
Success.
nx9500-6C8809#


nx9500-6C8809#ex3500 copy tftp startup-config 10.2.0.99 startup.01 startup on
ex3524-ED5EAC
TFTP server ip address: 10.1.0.99
Flash programming started.
Flash programming completed.
Success.
nx9500-6C8809#
```

## 3.1.28 factory-reset

*Privileged Exec Mode Commands*

Erases startup configuration on a specified device or all devices within a specified RF Domain

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
factory-reset [<HOSTNAME/MAC>|config-all|config-device-only|on <RF-DOMAIN-NAME>]

factory-reset <HOSTNAME/MAC> {<HOSTNAME/MAC>}

factory-reset on <RF-DOMAIN-NAME> {containing <SUB-STRING>|exclude-controllers|
exclude-rf-domain-manager|filter <DEVICE-TYPE>}

factory-reset [config-all|config-device-only] [<HOSTNAME/MAC> {<HOSTNAME/MAC>}|
on <RF-DOMAIN-NAME> {containing <SUB-STRING>|exclude-controllers|exclude-rf-
domain-manager|filter <DEVICE-TYPE>}]
```

**Parameters**

- `factory-reset <HOSTNAME/MAC> {<HOSTNAME/MAC>}`

| | |
|---|---|
| factory-reset | Erases startup configuration and reloads device(s) based on the parameters passed<br>For more information on the actions performed by this command, see *Actions performed by the factory-reset command.* |
| <HOSTNAME/MAC> *{<HOSTNAME/MAC>}* | Erases startup configuration and reloads the device identified by the <HOSTNAME/MAC> keyword. Specify the device's hostname or MAC address.<br>• <HOSTNAME/MAC> – Optional. You can optionally specify multiple space-separated devices. |

- `factory-reset on <RF-DOMAIN-NAME> {containing <SUB-STRING>|exclude-controllers|exclude-rf-domain-manager|filter <DEVICE-TYPE>}`

| | |
|---|---|
| factory-reset | Erases startup configuration and reloads device(s) based on the parameters passed<br>For more information on the actions performed by this command, see *Actions performed by the factory-reset command.* |
| on <RF-DOMAIN-NAME><br>{containing <SUB-STRING>\|<br>exclude-controllers\|<br>exclude-rf-domain-manager\|<br>filter <DEVICE-TYPE>]} | Erases startup configuration and reloads all devices or specified device(s) within a specified RF Domain identified by the <RF-DOMAIN-NAME> keyword<br>• <RF-DOMAIN-NAME> – Specify the RF Domain name. After specifying the RF Domain, optionally use the filters provided to identify specific device(s) within the RF Domain. If none of the filters are used, the command is executed on all devices within the RF Domain. These filters are:<br>• containing <SUB-STRING> – Optional. Executes the command on all devices containing a specified sub-string in their hostname<br>• <SUB-STRING> – Specify the sub-string to match.<br>Contd... |

| | |
|---|---|
| | • exclude-controllers – Optional. Executes the command on all devices excluding controllers. Since only a NOC controller is capable of adopting other controllers, use this option when executing the command on a NOC controller.<br>• exclude-rf-domain-manager – Optional. Executes the command on all devices excluding RF Domain managers. Use this option when executing the command on the NOC, site controller, or RF Domain manager.<br>• filter <DEVICE-TYPE> – Optional. Executes the command on all devices of a specified type<br>• <DEVICE-TYPE> – Specify the device type. The options are: AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533, RFS4000, RFS6000, NX5500, NX75XX, NX95XX, NX9600, and VX9000. The startup configuration is erased on all devices of the type specified here. For example, if AP6521 is the device-type specified, the command is executed on all AP6521s within the specified RF Domain. |

• `factory-reset [config-all|config-device-only] [<HOSTNAME/MAC> {<HOSTNAME/MAC>}|on <RF-DOMAIN-NAME> {containing <SUB-STRING>|exclude-controllers|exclude-rf-domain-manager|filter <DEVICE-TYPE>}]`

| | |
|---|---|
| factory-reset | Erases startup configuration and reloads device(s) based on the parameters passed<br>For more information on the actions performed by this command, see *Actions performed by the factory-reset command.* |
| [config-all\| config-device-only] | Erases startup configuration and reloads only controller-adopted devices or the controller as well as its adopted devices<br>• config-all – Erases startup configuration on the controller and all devices adopted by it<br>• config-device-only – Erases startup configuration only on the devices adopted by the controller |
| <HOSTNAME/MAC> {<HOSTNAME/MAC>} | This parameter is common to the 'config-all' and 'config-device-only' keywords:<br>• <HOSTNAME/MAC> – Erases startup configuration and reloads the device identified by the <HOSTNAME/MAC> keyword. Specify the device's hostname or MAC address.<br>• <HOSTNAME/MAC> – Optional. You can optionally specify multiple space-separated devices. |
| | The following parameters are common to the 'config-all' and 'config-device-only' keywords:<br>• on <RF-DOMAIN-NAME> – Erases startup configuration and reloads all devices or specified device(s) within a specified RF Domain<br>• <RF-DOMAIN-NAME> – Specify the RF Domain name. After specifying the RF Domain, optionally use the filters provided to identify specific device(s) within the RF Domain. If none of the filters are used, the command is executed on all devices within the RF Domain. These filters are:<br>• containing <SUB-STRING> – Optional. Executes the command on all devices containing a specified sub-string in their hostname<br>• <SUB-STRING> – Specify the sub-string to match.<br>• exclude-controllers – Optional. Executes the command on all devices excluding controllers. Since only a NOC controller is capable of adopting other controllers, use this option when executing the command on a NOC controller.<br>Contd... |

| | |
|---|---|
| on <RF-DOMAIN-NAME> {containing <SUB-STRING>\| exclude-controllers\| exclude-rf-domain-manager\| filter <DEVICE-TYPE>]} | • exclude-rf-domain-manager – Optional. Executes the command on all devices excluding RF Domain managers. Use this option when executing the command on the NOC, Site controller, or RF Domain manager.<br>• filter <DEVICE-TYPE> – Optional. Executes the command on all devices of a specified type<br>• <DEVICE-TYPE> – Specify the device type. The options are: AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533, RFS4000, RFS6000, NX5500, NX75XX, NX95XX, NX9600, and VX9000. The startup configuration is erased on all devices of the type specified here. For example, if AP6521 is the device-type specified, the command is executed on all AP6521s within the specified RF Domain. |

**Usage Guidelines Actions performed by the factory-reset command.**

The action taken by this command depends on the parameters passed.

- For the '*factory-reset [<DEVICE-NAME>|on <RF-DOMAIN-NAME>]*' options, the command:
  - Erases startup configuration on the target device (or) all devices in the target RF Domain.
  - Erases the device configuration entries from the controller's configuration for the target device (or) for all the devices in the target RF Domain.
  - Reloads the target device (or) all devices in the target RF Domain.
- For the '*factory-reset config-all [<DEVICE-NAME>|on <RF-DOMAIN-NAME>]*' options, the command:
  - Erases startup configuration on the target device (or) all devices in the target RF Domain.
  - Erases the device configuration entries from the controller's configuration for the target device (or) for all the devices in the target RF Domain.
- For the '*factory-reset config-device-only [<DEVICE-NAME>|on <RF-DOMAIN-NAME>]*' options, the command:
  - Erases startup configuration on the target device (or) all devices in the target RF Domain.

**Example**

```
nx7500-7F3609#factory-reset config-all ap6522-5A873C
In progress ....
Erased startup-config - success 1 fail 0
Successful device deletion - total 1
nx7500-7F3609#

rfs6000-18072B# factory-reset B4-C7-99-5A-87-3C
In progress ....
Erased startup-config and initiated reload - success 1 fail 0
Successful device deletion - total 1
rfs6000-18072B#
```

The following example displays the access points in the RF Domain 'rfd1':

```
nx7500-7F3609#show wireless ap on rfd1
-------------------------------------------------------------------------------
-------
  MODE        : radio modes - W = WLAN, S=Sensor, ' ' (Space) = radio not present
-------------------------------------------------------------------------------
-------
-------------------------------------------------------------------------------
-------
 AP-NAME     AP-LOCATION  RF-DOMAIN     AP-MAC         #RADIOS  MODE  #CLIENT
IPv4   IPv6
-------------------------------------------------------------------------------
-------
```

```
ap7131-1180FC            rfd1    00-23-68-11-80-FC   2 W-W        0     0.0.0.0
::
ap6522-551648            rfd1    B4-C7-99-55-16-48   2 W-W        0     0.0.0.0
::
ap8232-7F0DF8               rfd1     FC-0A-81-7F-0D-F8    2 W-W          0
0.0.0.0      ::
--------------------------------------------------------------------------------
-------
Total number of APs displayed: 3
nx7500-7F3609#
```

Note, the factory-reset command executed on an RF Domain with the ‘exclude-rf-domain-manager’ option erases the startup configuration on all devices other than the RF Domain manager.

```
nx7500-7F3609#factory-reset config-device-only on rfd1 exclude-rf-domain-manager

In progress ....
Erased startup-config -
ap7131-1180FC: OK
ap6522-551648: OK

nx7500-7F3609#

nx7500-7F3609# factory-reset on rfd2
In progress ....
Erased startup-config and initiated reload -
ap650-A6566C: OK,Reload scheduled in 60 seconds...
ap4532-34505C: OK,Reload scheduled in 60 seconds...
ap650-345000: OK,Reload scheduled in 60 seconds...

Successful device deletion - total 3
nx7500-7F3609#
```

## 3.1.29 file-sync

*Privileged Exec Mode Commands*

Syncs trustpoint and/or EAP-TLS X.509 (PKCS#12) certificate between the staging-controller and adopted access points.

When enabling file syncing, consider the following points:

- The X.509 certificate needs synchronization only if the access point is configured to use EAP-TLS authentication.
- Execute the command on the controller adopting the access points.
- Ensure that the X.509 certificate file is installed on the controller.

Syncing of trustpoint/wireless-bridge certificate can to be automated. To automate file syncing, in the controller's device/profile configuration mode, execute the following command: *file-sync [auto|count <1-20>]*. For more information, see *file-sync*.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
file-sync [cancel|load-file|trustpoint|wireless-bridge]

file-sync cancel [trustpoint|wireless-bridge]

file-sync cancel [trustpoint|wireless-bridge] [<DEVICE-NAME>|all|rf-domain
[<DOMAIN-NAME>|all]]

file-sync load-file [trustpoint|wireless-bridge]]

file-sync load-file [trustpoint <TRUSTPOINT-NAME>|wireless-bridge] <URL>

file-sync [trustpoint <TRUSTPOINT-NAME>|wireless-bridge] [<DEVICE-NAME>|all|
rf-domain [<DOMAIN-NAME>|all] {from-controller}] {reset-radio|upload-time <TIME>}
```

**Parameters**

```
• file-sync cancel [trustpoint|wireless-bridge] [<DEVICE-NAME>|all|rf-domain
[<DOMAIN-NAME>|all]]
```

| | |
|---|---|
| file-sync cancel [trustpoint\| wireless-bridge] [<DEVICE-NAME>\| all\|rf-domain [<DOMAIN-NAME>\| all]] | Cancels scheduled file synchronization<br>• trustpoint – Cancels scheduled trustpoint synchronization on a specified AP, all APs, or APs within a specified RF Domain<br>• wireless-bridge – Cancels scheduled wireless-bridge certificate synchronization on a specified AP, all APs, or APs within a specified RF Domain<br>• <DEVICE-NAME> – Cancels scheduled trustpoint/certificate synchronization on a specified AP. Specify the AP's hostname or MAC address.<br>Contd.. |

| | |
|---|---|
| | • all – Cancels scheduled trustpoint/certificate synchronization on all APs<br>• rf-domain [<DOMAIN-NAME>\|all] – Cancels scheduled trustpoint/certificate synchronization on all APs in a specified RF Domain or in all RF Domains<br>• <DOMAIN-NAME> – Cancels scheduled trustpoint/certificate synchronization on all APs within a specified RF Domain. Specify the RF Domain's name.<br>• all – Cancels scheduled trustpoint/certificate synchronization on all RF Domains |

• `file-sync load-file [trustpoint|wireless-bridge] <URL>`

| | |
|---|---|
| file-sync load-file [trustpoint\| wireless-bridge] <URL> | Loads the following files on to the staging controller:<br>• trustpoint – Loads the trustpoint, including CA certificate, server certificate and private key<br>• wireless-bridge – Loads the wireless-bridge certificate to the staging controller<br>Use this command to load the certificate to the controller before scheduling or initiating a certificate synchronization.<br>• <URL> – Provide the trustpoint/certificate location using one of the following formats:<br>tftp://<hostname\|IP>[:port]/path/file<br>ftp://<user>:<passwd>@<hostname\|IP>[:port]/path/file<br>sftp://<user>:<passwd>@<hostname\|IP>[:port]>/path/file<br>http://<hostname\|IP>[:port]/path/file<br>cf:/path/file<br>usb<n>:/path/file<br>**Note:** Both IPv4 and IPv6 address types are supported. |

• `file-sync [trustpoint <TRUSTPOINT-NAME>|wireless-bridge] [<DEVICE-NAME>| all|rf-domain [<DOMAIN-NAME>|all] {from-controller}] {reset-radio|upload-time <TIME>}`

| | |
|---|---|
| file-sync trustpoint <TRUSTPOINT-NAME> [<DEVICE-NAME>\| all\|rf-domain [<DOMAIN-NAME> \|all] from-controller] | Configures file-syncing parameters<br>• trustpoint <TRUSTPOINT-NAME> – Syncs a specified trustpoint between controller and its adopted APs<br>• <TRUSTPOINT-NAME> – Specify the trustpoint name.<br>• wireless-bridge – Syncs wireless-bridge certificate between controller and its adopted APs<br>After specifying the file that is to be synced, configure following file-sync parameters:<br>• <DEVICE-NAME> – Syncs trustpoint/certificate with a specified AP. Specify the AP's hostname or MAC address.<br>• all – Syncs trustpoint/certificate with all APs<br>• rf-domain [<DOMAIN-NAME>\|all] from-controller – Syncs trustpoint/certificate with all APs in a specified RF Domain or in all RF Domains<br>• <DOMAIN-NAME> – Select to sync with APs within a specified RF Domain. Specify the RF Domain's name.<br>• all – Select to sync with APs across all RF Domains<br>• from-controller – Optional. Loads certificate to the APs from the adopting controller and not the RF Domain manager<br>After specifying the access points, specify the following options: reset-radio and upload-time. |

| | |
|---|---|
| reset-radio | This keyword is recursive and applicable to all of the above parameters.<br>Optional. Resets the radio after file synchronization. Reset the radio in case the certificate is renewed along with no changes made to the 'bridge EAP username' and 'bridge EAP password'. |
| upload-time <TIME> | This keyword is recursive and applicable to all of the above parameters.<br>• upload-time – Optional. Schedules certificate upload at a specified time<br>  • <TIME> – Specify the time in the MM/DD/YYYY-HH:MM or HH:MM format. If no time is configured, the process is initiated as soon as the command is executed. |

**Example**

```
rfs6000-81742D#file-sync wireless-bridge ap7131-11E6C4 upload-time 06/01/2017-
12:30
--------------------------------------------------------------------------------
          CONTROLLER               STATUS                  MESSAGE
--------------------------------------------------------------------------------
  B4-C7-99-6D-CD-4B           Success           Queued 1 APs to upload
--------------------------------------------------------------------------------
rfs6000-81742D#
```

The following command uploads certificate to all access points:

```
rfs6000-81742D#file-sync wireless-bridge all upload-time 06/01/2017-23:42
```

## 3.1.30 halt

*Privileged Exec Mode Commands*

Stops (halts) a device (access point, wireless controller, or service platform). Once halted, the system must be restarted manually.

This command stops the device immediately. No indications or notifications are provided while the device shuts down.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
halt {force} {(on <DEVICE-NAME>)}
```

**Parameters**

- `halt {force} {(on <DEVICE-NAME>)}`

| | |
|---|---|
| halt | Halts a device |
| force | Optional. Forces a device to halt ignoring in-progress operations, such as firmware upgrades, downloads, unsaved configuration changes, etc. |
| on <DEVICE-NAME> | The following keywords are recursive and applicable to the 'force' parameter:<br>• on <DEVICE-NAME> – Optional. Specifies the name of the device to be halted<br>• <DEVICE-NAME> – Enter the name of the AP, wireless controller, or service platform.<br>If the device name is not specified, the logged device is halted. |

**Example**

```
nx9500-6C8809#halt on rfs6000-81742D
nx9500-6C8809#
```

## 3.1.31 join-cluster

*Privileged Exec Mode Commands*

Adds a device (access point, wireless controller, or service platform), as cluster member, to an existing cluster of devices. Assign a static IP address to the device before adding to a cluster. Note, a cluster can be only formed of devices of the same model type.

**Supported in the following platforms:**

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

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

**Parameters**

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

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

**Usage Guidelines**

To add a device to an existing cluster:

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

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

**Example**

```
rfs6000-81742D#join-cluster 192.168.13.16 user admin password superuser level 1
 mode standby
... connecting to 192.168.13.16
... applying cluster configuration
... committing the changes
... saving the changes
[OK]
rfs6000-81742D#
```

```
rfs6000-81742D#show context
!
! Configuration of RFS6000 version 5.9.1.0-012D

!
!
version 2.5
!
!
.....................................................................................
 interface ge1
  switchport mode access
  switchport access vlan 1
 interface vlan1
  ip address 192.168.13.16/24
  ip dhcp client request options all
  no ipv6 enable
  no ipv6 request-dhcpv6-options
 cluster name TechPubs
 cluster mode standby
 cluster member ip 192.168.13.16 level 1
 logging on
 logging console warnings
 logging buffered warnings
!
!
end
rfs6000-81742D#
```

**Related Commands**

| | |
|---|---|
| *cluster* | Initiates the cluster context. The cluster context provides centralized management to configure all cluster members from any one member. |
| *create-cluster* | Creates a new cluster on a specified device |

## 3.1.32 l2tpv3

*Privileged Exec Mode Commands*

Establishes or brings down an L2TPv3 tunnel

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
l2tpv3 tunnel [<TUNNEL-NAME>|all]

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

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

**Parameters**

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

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

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

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

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

| | |
|---|---|
| l2tpv3 tunnel | Establishes or brings down a L2TPv3 tunnel |
| all [down\|up] | Establishes or brings down all L2TPv3 tunnels<br>• down – Brings down all tunnels<br>• up – Establishes all tunnels |

| | |
|---|---|
| on <DEVICE-NAME> | Optional. Establishes or brings down all tunnels on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

**Example**

```
rfs6000-81742D#l2tpv3 tunnel Tunnel1 session Tunnel1Session1 up on rfs6000-81742D
```

**NOTE:** For more information on the L2TPv3 tunnel configuration mode and commands, see *Chapter 22, L2TPV3-POLICY*.

## 3.1.33 logging

*Privileged Exec Mode Commands*

Modifies message logging settings

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

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

**Parameters**

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

| | |
|---|---|
| monitor | Sets terminal lines logging levels. The logging severity levels can be set from 0 - 7. The system configures default settings, if no logging severity level is specified.<br>• <0-7> – Optional. Enter the logging severity level from 0 - 7. The various levels and their implications are:<br>• alerts – Optional. Immediate action needed (severity=1)<br>• critical – Optional. Critical conditions (severity=2)<br>• debugging – Optional. Debugging messages (severity=7)<br>• emergencies – Optional. System is unusable (severity=0)<br>• errors – Optional. Error conditions (severity=3)<br>• informational – Optional. Informational messages (severity=6)<br>• notifications – Optional. Normal but significant conditions (severity=5)<br>• warnings – Optional. Warning conditions (severity=4)<br>**Note:** Ensure that the logging module is enabled, before configuring the message logging level. To enable message logging, in the device's configuration mode, execute the *logging > on* command. Message logging can also be enabled on a profile. |

**Example**

```
rfs6000-81742D(config-device-00-15-70-81-74-2D)#logging on

rfs6000-81742D#logging monitor debugging

rfs6000-81742D#show logging

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

Log Buffer (70096 bytes):


Apr 04 12:43:02 2017: %DIAG-4-FAN_UNDERSPEED: Fan fan 1 under speed: 0 RPM is under
limit 2000 RPM
Apr 04 12:33:02 2017: %DIAG-4-FAN_UNDERSPEED: Fan fan 1 under speed: 0 RPM is under
limit 2000 RPM
--More--
rfs6000-81742D#
```

**Related Commands**

| | |
|---|---|
| *no* | Resets terminal lines logging levels |

## 3.1.34 mint

*Privileged Exec Mode Commands*

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

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
mint [ping|traceroute]

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

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

**Parameters**

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

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

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

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

**Example**

```
rfs4000-229D58#mint ping 68.88.0D.A7
MiNT ping 68.88.0D.A7 with 64 bytes of data.
 Response from 68.88.0D.A7: id=1 time=0.364 ms
 Response from 68.88.0D.A7: id=2 time=0.333 ms
 Response from 68.88.0D.A7: id=3 time=0.368 ms

--- 68.88.0D.A7 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.333/0.355/0.368 ms
rfs4000-229D58#
```

## 3.1.35 mkdir

*Privileged Exec Mode Commands*

Creates a new directory in the file system

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
mkdir <DIR>
```

**Parameters**

- `mkdir <DIR>`

| | |
|---|---|
| <DIR> | Specify a directory name.<br>**Note:** A directory, specified by the <DIR> parameter, is created within the file system. |

**Example**

```
rfs4000-880DA7#dir
Directory of flash:/.

  drwx             Tue Sep 27 06:25:15 2016   log
  drwx             Sat Jan  1 05:30:08 2000   configs
  drwx             Sat Jan  1 05:30:08 2000   cache
  drwx             Wed Nov  4 16:12:15 2015   crashinfo
  drwx             Mon Sep 26 10:45:03 2016   archived_logs
  drwx             Sat Jan  1 05:30:08 2000   upgrade
  drwx             Sat Jan  1 05:30:23 2000   hotspot
  drwx             Sat Jan  1 05:30:08 2000   floorplans
  drwx             Sat Jan  1 05:30:08 2000   tmptpd

rfs4000-880DA7#

rfs4000-880DA7#mkdir test

rfs4000-880DA7#dir
Directory of flash:/.

  drwx             Tue Sep 27 06:25:15 2016   log
  drwx             Tue Sep 27 15:20:01 2016   test
  drwx             Sat Jan  1 05:30:08 2000   configs
  drwx             Sat Jan  1 05:30:08 2000   cache
  drwx             Wed Nov  4 16:12:15 2015   crashinfo
  drwx             Mon Sep 26 10:45:03 2016   archived_logs
  drwx             Sat Jan  1 05:30:08 2000   upgrade
  drwx             Sat Jan  1 05:30:23 2000   hotspot
  drwx             Sat Jan  1 05:30:08 2000   floorplans
  drwx             Sat Jan  1 05:30:08 2000   tmptpd

rfs4000-880DA7#
```

## 3.1.36 more

*Privileged Exec Mode Commands*

Displays files on the device's file system. This command navigates and displays specific files in the device's file system. Provide the complete path to the file `more <file>`.

The more command also displays the startup configuration file.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
more <FILE>
```

**Parameters**

- `more <FILE>`

| | |
|---|---|
| <FILE> | Specify the file name and location. |

**Example**

```
rfs4000-880DA7#more flash:/archived_logs/startup.5.log
00-07-42-05-30-17
May 30 05:37:43 2017: %PM-6-PROCSTART: Starting process "/usr/sbin/logd"
May 30 05:37:43 2017: %PM-6-PROCSTART: Starting process "/usr/sbin/isDiag"
May 30 05:37:48 2017: %PM-6-PROCSTART: Starting process "/usr/sbin/rim"
May 30 05:37:51 2017: %DIAG-4-FAN_UNDERSPEED: Fan fan 1 under speed: 0 RPM is under
limit 2000 RPM
May 30 05:38:18 2017: %PM-6-PROCSTART: Starting process "/etc/init.d/cfgd"
May 30 05:38:19 2017: %KERN-6-INFO: up1 { no link }.
May 30 05:38:19 2017: %PM-6-PROCSTART: Starting process "/usr/sbin/nsm"
May 30 05:38:21 2017: %PM-6-PROCSTART: Starting process "/usr/sbin/mstp"
May 30 05:38:21 2017: %PM-6-PROCSTART: Starting process "/usr/sbin/hsd"
May 30 05:38:22 2017: %PM-6-PROCSTART: Starting process "/etc/init.d/dpd2.init"
May 30 05:38:22 2017: %PM-6-PROCSTART: Starting process "/usr/sbin/ssm"
--More--
rfs4000-880DA7#
```

## 3.1.37 no

*Privileged Exec Mode Commands*

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

The no commands have their own set of parameters that can be reset. These parameters depend on the context in which the command is being used.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
no [adoption|captive-portal|cpe|crypto|debug|logging|page|raid|service|
terminal|upgrade|virtual-machine|wireless]

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

**NOTE:** The *no > adoption* command resets the adoption state of a specified device (and all devices adopted to it) or devices within a specified RF Domain. When executed without specifying the device or RF Domain, the command resets the adoption state of the logged device and all devices, if any, adopted to it.

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

no crypto pki [server|trustpoint]

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

no logging monitor

no page

no service [block-adopter-config-update|locator|snmp|ssm|wireless]

no service block-adopter-config-update

no service locator {on <DEVICE-NAME>}

no service snmp sysoid wing5

no service ssm trace pattern {<WORD>} {(on <DEVICE-NAME>)}

no service wireless [trace pattern {<WORD>} {(on <DEVICE-NAME>)}|unsanctioned ap
air-terminate <BSSID> {on <DOMAIN-NAME>}]

no terminal [length|width]

no upgrade <PATCH-NAME> {on <DEVICE-NAME>}

no wireless client [all|<MAC>]
```

```
no wireless client all {filter|on}

no wireless client all {filter [wlan <WLAN-NAME>]}

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

no wireless client mac <MAC> {on <DEVICE-OR-DOMAIN-NAME>}
```

The following command is available only on the NX95XX series service platforms:

```
no cpe led cpe [<1-24>|all] {on <T5-DEVICE-NAME>}

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

no raid locate
```

**Parameters**

- no <PARAMETERS>

| | |
|---|---|
| no <PARAMETERS> | Resets or reverts settings based on the parameters passed |

**Usage Guidelines**

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

**Example**

```
rfs4000-229D58#no adoption
rfs4000-229D58#

rfs6000-81742D#no page
rfs6000-81742D#
```

## 3.1.38 on

*Privileged Exec Mode Commands*

Executes the following commands in the RF Domain context: clrscr, do, end, exit, help, service, and show

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
on rf-domain [<RF-DOMAIN-NAME>|all]
```

**Parameters**

- `on rf-domain [<RF-DOMAIN-NAME>|all]`

| | |
|---|---|
| on rf-domain [<RF-DOMAIN-NAME>\|all] | Enters the RF Domain context based on the parameter specified<br>• <RF-DOMAIN-NAME> – Specify the RF Domain name. Enters the specified RF Domain context.<br>• all – Specifies all RF Domains. |

**Example**

```
nx9500-6C8809#on rf-domain TechPubs
nx9500-6C8809(TechPubs)#

nx9500-6C8809(TechPubs)#?
on RF-Domain Mode commands:

  clrscr   Clears the display screen
  do       Run commands from Exec mode
  end      End current mode and change to EXEC mode
  exit     End current mode and down to previous mode
  help     Description of the interactive help system
  service  Service Commands
  show     Show running system information
nx9500-6C8809(TechPubs)#?

nx9500-6C8809(TechPubs)#show adoption timeline on TechPubs/ap7562-84A224
-------------------------------------------------------------------------------
-----
             AP-NAME      RF-DOMAIN   LAST-ADOPTION-TIMESTAMP        ADOPTED-SINCE
-------------------------------------------------------------------------------
-----
      nx9500-6C8809       TechPubs       2016-09-09 00:00:14     7 days 05:19:49
     rfs4000-880DA7       TechPubs       2016-09-08 23:59:57     7 days 05:20:06
     rfs6000-81742D       TechPubs       2016-09-08 05:52:04     7 days 23:27:58
-------------------------------------------------------------------------------
-----
Total number of devices displayed: 3
nx9500-6C8809(TechPubs)#
```

## 3.1.39 opendns

*Privileged Exec Mode Commands*

Fetches the OpenDNS device_id from the OpenDNS site. Use this command to fetch the OpenDNS device_id. Once fetched, apply the device_id to WLANs that are to be OpenDNS enabled.

OpenDNS is a free DNS service that enables swift Web navigation without frequent outages. It is more reliable than other available DNS services, and provides the following services: DNS query resolution, Web-filtering, protection against virus and malware attacks, performance enhancement, etc.

This command is part of a set of configurations that are required to integrate WiNG devices with OpenDNS. When integrated, DNS queries going out of the WiNG device (access point, controller, or service platform) are re-directed to OpenDNS (208.67.220.220 or 208.67.222.222) resolvers that act as proxy DNS servers. For more information on enabling OpenDNS support, see *Enabling OpenDNS Support*.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
opendns [APIToken|username]

opendns APIToken <OPENDNS-APITOKEN>
opendns username <USERNAME> password <OPENDNS-PSWD> label <LABEL>

Note, you can use either of the above commands to fetch the device_id from the
OpenDNS site.
```

**Parameters**

- `opendns APIToken <OPENDNS-APITOKEN>`

| | |
|---|---|
| opendns | Fetches the device_id from the OpenDNS site using the OpenDNS API token |
| APIToken <OPENDNS-APITOKEN> | Configures the OpenDNS APIToken. This is the token provided you by CISCO at the time of subscribing for their OpenDNS service.<br>• <OPENDNS-APITOKEN> – Provide the OpenDNS API token (should be a valid token).<br>For every valid OpenDNS API token provided a device_id is returned. Apply this device_id to WLANs that are to be OpenDNS enabled. Once applied, DNS queries originating from associating clients are appended with an additional 31 bytes of data (representing the device ID) at the end of the DNS packet. For information on configuring the device_id in the WLAN context, see *opendns*. |

- `opendns username <USERNAME> password <OPENDNS-PSWD> label <LABEL>`

| | |
|---|---|
| opendns | Fetches the device_id from the OpenDNS site using the OpenDNS credentials |
| username <USERNAME> | Configures the OpenDNS user name. This is your OpenDNS email ID provided by CISCO at the time of subscribing for their OpenDNS service.<br>• <USERNAME> – Provide the OpenDNS user name (should be a valid OpenDNS username). |

| | |
|---|---|
| password <OPENDNS-PSWD> | Configures the password associated with the user name specified in the previous step<br>• <OPENDNS-PSWD> – Provide the OpenDNS password (should be a valid OpenDNS password). |
| label <LABEL> | Configures the network label. This the label (the user friendly name) of your network, and should be the same as the label (name) configured on the OpenDNS portal.<br>• <LABEL> – Specify your network label.<br>For every set of username, password, and label passed only one unique device_id is returned. Apply this device_id to WLANs that are to be OpenDNS enabled. Once applied, DNS queries originating from associating clients are appended with an additional 31 bytes of data (representing the device ID) at the end of the DNS packet. For information on configuring the device_id in the WLAN context, see *opendns*. |

**Example**

```
ap7131-E6D512#opendns username bob@examplecompany.com password opendns label
company_name
Connecting to OpenDNS server...
device_id = 0014AADF8EDC6C59
ap7131-E6D512#

nx9600-7F3C7F#opendns ApiToken 9110B39543DEB2ECA1F473AE03E8899C00019073
device_id = 001480fe36dcb245
nx9600-7F3C7F#
```

**Example Enabling OpenDNS Support**

The following example shows how to enable OpenDNS support'

1 Fetch the OpenDNS device_id from the OpenDNS site.

a In the User/Privilege executable mode execute one of the following commands:

```
nx9500-6C874D#opendns APIToken <OPENDNS-APITOKEN>
nx9500-6C8809#opendns ApiToken 9110B39543DEB2ECA1F473AE03E8899C00019073
device_id = 001480fe36dcb245
nx9500-6C8809#
OR
nx9500-6C8809#opendns username <USERNAME> password <OPENDNS-PSWD> label
<LABEL>
```

Note, the *OpenDNS API token* and/or *user account credentials* are provided the OpenDNS service provider when subscribing for the OpenDNS service.

b Apply the device_id fetched in the step 1 to the WLAN.

```
nx9500-6C8809(config-wlan-opendns)#opendns device-id <OPENDNS-DEVICE-ID>
nx9500-6C8809(config-wlan-opendns)#opendns device-id 001480fe36dcb245
nx9500-6C8809(config-wlan-opendns)#show context
wlan opendns
 ssid opendns
 bridging-mode local
 encryption-type none
 authentication-type none
 opendns device-id 001480fe36dcb245
nx9500-6C8809(config-wlan-opendns)#
```

Once applied, DNS queries originating from wireless clients associating with the WLAN are appended with an additional 31 bytes of data (representing the device ID) at the end of the DNS packet.

2 Configure a DHCP server policy, and set the DHCP pool's DNS server configuration to point to the OpenDNS servers.

```
nx9500-6C8809(config-dhcp-policy-opendns-pool-opendnsPool)#dns-server
208.67.222.222
```

Note, you can configure any one of the following OpenDNS servers: **208.67.222.222** OR **208.67.222.220**

```
nx9500-6C8809(config-dhcp-policy-opendns-pool-opendnsPool)#show context
 dhcp-pool opendnsPool
  dns-server  208.67.222.222
nx9500-6C8809(config-dhcp-policy-opendns-pool-opendnsPool)#
```

3 Apply the DHCP server policy configured in step 2 on the access point, controller, or service platform.

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#use dhcp-server-policy
opendns
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#show context include-factory
| include use
 use profile default-nx9000
 use rf-domain TechPubs
 use database-policy default
 use nsight-policy noc
 use dhcp-server-policy opendns
 use auto-provisioning-policy TechPubs
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#
```

When configured, DNS queries are forwarded by the access point, controller, or service platform to the specified OpenDNS resolver.

4 Configure an IP Access Control List with the following permit and deny rules:

```
nx9500-6C8809(config-ip-acl-OpenDNS)#permit udp any host 208.67.222.222 eq
dns rule-precedence 1 rule-description "allow dns queries only to OpenDNS"

nx9500-6C8809(config-ip-acl-OpenDNS)#deny udp any any eq dns rule-precedence
10 rule-description "block all DNS queries"

nx9500-6C8809(config-ip-acl-OpenDNS)#permit ip any any rule-precedence 100
rule-description "allow all other ip packets"

nx9500-6C8809(config-ip-acl-OpenDNS)#show context
ip access-list OpenDNS
permit udp any host 208.67.222.222 eq dns rule-precedence 1 rule-description
"allow dns queries only to OpenDNS"
deny udp any any eq dns rule-precedence 10 rule-description "block all dns
queries"
permit ip any any rule-precedence 100 rule-description "allow all other ip
packets"
nx9500-6C8809config-ip-acl-OpenDNS)#
```

When configured and applied in the WLAN context, the IP ACL prevents wireless clients from adding their own DNS servers to bypass the Web filtering and network policies enforced by OpenDNS.

5 Apply the IP ACL configured in step 4 in the WLAN context.

```
nx9500-6C8809(config-wlan-opendns)#use ip-access-list out OpenDNS
nx9500-6C8809(config-wlan-opendns)#show context
wlan opendns
 ssid opendns
 vlan 1
 bridging-mode local
 encryption-type none
 authentication-type none
 use ip-access-list in OpenDNS
 use ip-access-list out OpenDNS
 opendns device-id 0014AADF8EDC6C59
nx9500-6C8809(config-wlan-opendns)#
```

When applied to the WLAN, only the DNS queries directed to the OpenDNS server are forwarded. All other DNS queries are dropped.

## 3.1.40 page

*Privileged Exec Mode Commands*

Toggles controller paging. Enabling this command displays the CLI command output page by page, instead of running the entire output at once.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
page
```

**Parameters**

None

**Example**

```
rfs6000-81742D#page
rfs6000-81742D#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables controller paging |

## 3.1.41 ping

*Privileged Exec Mode Commands*

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

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ping <IP/HOSTNAME> {count <1-10000>|dont-fragment {count|size}|size <1-64000>|
source [<IP>|pppoe|vlan <1-4094>|wwan]}
```

**Parameters**

```
• ping <IP/HOSTNAME> {count <1-10000>|dont-fragment {count|size}|size <1-64000>|
source [<IP>|pppoe|vlan <1-4094>|wwan]}
```

| | |
|---|---|
| <IP/HOSTNAME> | Specify the destination IP address or hostname to ping. When entered without any parameters, this command prompts for an IP address or a hostname. |
| count <1-10000> | Optional. Sets the pings to the specified destination<br>• <1-10000> – Specify a value from 1 - 10000. The default is 5. |
| dont-fragment {count\|size} | Optional. Sets the dont-fragment bit in the ping packet. Packets with the dont-fragment bit specified, are not fragmented. When a packet, with the dont-fragment bit specified, exceeds the specified *Maximum Transmission Unit* (MTU) value, an error message is sent from the device trying to fragment it.<br>• count <1-10000> – Sets the pings to the specified destination from 1 - 10000. The default is 5.<br>• size – <1-64000> – Sets the size of ping payload size from 1 - 64000 bytes. The default is 100 bytes. |
| size <1-64000> | Optional. Sets the ping packet's size in bytes<br>• <1-64000> – Specify the ping payload size from 1 - 64000 bytes. The default is 100 bytes. |
| source [<IP>\|pppoe\|vlan <1-4094>\|wwan] | Optional. Sets the source address or interface name. This is the source of the ICMP packet to the specified destination.<br>• <IP> – Specifies the source IP address<br>• pppoe – Selects the PPP over Ethernet interface<br>• vlan <1-4094> – Selects the VLAN interface from 1 - 4094<br>• wwan – Selects the wireless WAN interface |

**Example**

```
rfs6000-81742D#ping 192.168.13.13 count 4
PING 192.168.13.13 (192.168.13.13) 100(128) bytes of data.
108 bytes from 192.168.13.13: icmp_seq=1 ttl=64 time=0.356 ms
108 bytes from 192.168.13.13: icmp_seq=2 ttl=64 time=0.211 ms
108 bytes from 192.168.13.13: icmp_seq=3 ttl=64 time=0.199 ms
108 bytes from 192.168.13.13: icmp_seq=4 ttl=64 time=0.215 ms

--- 192.168.13.13 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.199/0.245/0.356/0.065 ms
rfs6000-81742D#

rfs6000-81742D#ping 10.233.89.182 source vlan 1
PING 10.233.89.182 (10.233.89.182) from 192.168.13.24 vlan1: 100(128) bytes of
data.
From 192.168.13.2 icmp_seq=1 Packet filtered
From 192.168.13.2 icmp_seq=2 Packet filtered
From 192.168.13.2 icmp_seq=3 Packet filtered
From 192.168.13.2 icmp_seq=4 Packet filtered
From 192.168.13.2 icmp_seq=5 Packet filtered

--- 10.233.89.182 ping statistics ---
5 packets transmitted, 0 received, +5 errors, 100% packet loss, time 3997ms

rfs6000-81742D#
```

## 3.1.42 ping6

*Privileged Exec Mode Commands*

Sends ICMPv6 echo messages to a user-specified IPv6 address

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ping6 <IPv6/HOSTNAME> {<INTF-NAME>|count <1-10000>|size <1-64000>}
```

**Parameters**

- `ping <IPv6/HOSTNAME> {<INTF-NAME>|count <1-10000>|size <1-64000>}`

| | |
|---|---|
| <IPv6/HOSTNAME> | Specify the destination IPv6 address or hostname. |
| <INTF-NAME> | Optional. Specify the interface name for link local/broadcast address |
| count <1-10000> | Optional. Sets the pings to the specified IPv6 destination<br>• <1-10000> – Specify a value from 1 - 10000. The default is 5. |
| size <1-64000> | Optional. Sets the IPv6 ping payload size in bytes<br>• <1-64000> – Specify the ping payload size from 1 - 64000. The default is 100 bytes. |

**Usage Guidelines**

To configure a device's IPv6 address, in the VLAN interface configuration mode, use the *ipv6 > address <IPv6-ADDRESS> command.* After configuring the IPv6 address, use the *ipv6 > enable* command to enable IPv6. For more information, see *ipv6*.

**Example**

```
rfs4000-880DA7#ping6 2001:10:10:10:10:10:10:2 count 6 size 200
PING 2001:10:10:10:10:10:10:2(2001:10:10:10:10:10:10:2) 200 data bytes
208 bytes from 2001:10:10:10:10:10:10:2: icmp_seq=1 ttl=64 time=0.509 ms
208 bytes from 2001:10:10:10:10:10:10:2: icmp_seq=2 ttl=64 time=0.323 ms
208 bytes from 2001:10:10:10:10:10:10:2: icmp_seq=3 ttl=64 time=0.318 ms
208 bytes from 2001:10:10:10:10:10:10:2: icmp_seq=4 ttl=64 time=0.317 ms
208 bytes from 2001:10:10:10:10:10:10:2: icmp_seq=5 ttl=64 time=0.314 ms
208 bytes from 2001:10:10:10:10:10:10:2: icmp_seq=6 ttl=64 time=0.318 ms

--- 2001:10:10:10:10:10:10:2 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 4999ms
rtt min/avg/max/mdev = 0.314/0.349/0.509/0.075 ms
rfs4000-880DA7#
```

## 3.1.43 pwd

*Privileged Exec Mode Commands*

Displays the full path of the present working directory, similar to the UNIX pwd command

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
pwd
```

**Parameters**

None

**Example**

```
rfs4000-229D58#pwd
flash:/
rfs4000-229D58#

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

  drwx             Mon Feb  8 17:37:21 2016   log
  drwx             Sat Jan  1 05:30:08 2000   configs
  drwx             Sat Jan  1 05:30:08 2000   cache
  drwx             Thu Nov 12 17:55:02 2015   crashinfo
  drwx             Mon Feb  8 17:34:21 2016   archived_logs
  drwx             Sat Jan  1 05:30:08 2000   upgrade
  drwx             Sat Jan  1 05:30:23 2000   hotspot
  drwx             Sat Jan  1 05:30:08 2000   floorplans
  drwx             Sat Jan  1 05:30:08 2000   tmptpd

rfs4000-229D58#
```

## 3.1.44 re-elect

*Privileged Exec Mode Commands*

Re-elects the tunnel controller (wireless controller or service platform)

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

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

**Parameters**

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

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

**Example**

```
rfs4000-880DA7#re-elect tunnel-controller
OK
rfs4000-880DA7#
```

## 3.1.45 reload

*Privileged Exec Mode Commands*

Halts a device or devices and performs a warm reboot

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
reload {<DEVICE-MAC-OR-HOSTNAME>|at|cancel|force|in|on|staggered}

reload {(<DEVICE-MAC-OR-HOSTNAME>)}

reload {at <TIME> <1-31> <MONTH> <1993-2035> {on <DEVICE-OR-DOMAIN-NAME>}}

reload {cancel} {on <DEVICE-OR-DOMAIN-NAME>}

reload {force} {(<DEVICE-MAC-OR-HOSTNAME>|on <DOMAIN-NAME>|staggered)}

reload {force} {(<DEVICE-MAC-OR-HOSTNAME>)}

reload {force} {on <DOMAIN-NAME> {staggered}|staggered {<DEVICE-MAC-OR-HOSTNAME>|
on <DOMAIN-NAME>}} {containing <WORD>|exclude-controllers|exclude-rf-domain-
manager|filter <DEVICE-TYPE>}

reload {in <1-999>} {list|on}

reload {in <1-999>} {list {<LINE>|all}|on <DEVICE-OR-DOMAIN-NAME>}

reload {in <1-999>} {on <DEVICE-OR-DOMAIN-NAME>}

reload {on <DOMAIN-NAME>} {containing <WORD>|exclude-controllers|exclude-rf-
domain-manager|filter <DEVICE-TYPE>}

reload {staggered} {(<DEVICE-MAC-OR-HOSTNAME>)|on <DOMAIN-NAME>} {containing
<WORD>|exclude-controllers|exclude-rf-domain-manager|filter <DEVICE-TYPE>}
```

**Parameters**

- `reload {(<DEVICE-MAC-OR-HOSTNAME>)}`

| | |
|---|---|
| reload <DEVICE-MAC-OR-HOSTNAME> | Initiates device(s) reload and configures associated parameters<br>The following keyword is recursive and allows you to specify multiple devices:<br>• <DEVICE-MAC-OR-HOSTNAME> – Optional. Reloads a specified device(s), identified by the <DEVICE-MAC-OR-HOSTNAME> keyword. Specify the device's hostname or MAC address.<br>If no device is specified, the system reloads the logged device. |

- `reload {at <TIME> <1-31> <MONTH> <1993-2035> {on <DEVICE-OR-DOMAIN-NAME>}}`

| | |
|---|---|
| reload at | Initiates device(s) reload and configures associated parameters<br>• at – Optional. Schedules a reload at a specified time and day. Use the following keywords to specify the time and day: <TIME>, <1-31>, <MONTH>, and <1993-2035>. |
| <TIME> | Specifies the time in the HH:MM:SS format |

| | |
|---|---|
| <1-31> | Specifies the day of the month from 1 - 31 |
| <MONTH> | Specifies the month from Jan - Dec |
| <1993-2035> | Specifies the year from 1993 - 2035. It should be a valid 4 digit year. |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Performs reload at the scheduled time, on a specified device or all devices within a specified RF Domain<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. When a RF Domain name is provided, all devices within the specified RF Domain are reloaded at the scheduled time.<br>If no device is specified, the reload is scheduled on the logged device. |

- `reload {cancel} {on <DEVICE-OR-DOMAIN-NAME>}`

| | |
|---|---|
| reload cancel on <DEVICE-OR-DOMAIN-NAME> | Cancels pending/scheduled reloads of device(s)<br>• cancel – Optional. Cancels all pending reloads<br>• on <DEVICE-OR-DOMAIN-NAME> – Optional. Cancels reloads pending on a specified device or all devices within a specified RF Domain<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.<br>If no device is specified, the system cancels reloads pending on the logged device. |

- `reload {force} {(<DEVICE-MAC-OR-HOSTNAME>)}`

| | |
|---|---|
| reload force | Initiates device(s) reload and configures associated parameters<br>• force – Optional. Forces device(s) to reload, while ignoring conditions like upgrade in progress, unsaved changes, etc. Use the options provided to force a reload on a specified device or all devices in a RF Domain. |
| <DEVICE-MAC-OR-HOSTNAME> | This keyword is recursive and allows you to specify multiple devices.<br>• <DEVICE-MAC-OR-HOSTNAME> – Optional. Forces a reload on a specified device identified by the <DEVICE-MAC-OR-HOSTNAME> keyword. Specify the device's hostname or MAC address. When executed, the specified device(s) are forced to halt and a warm reboot is performed.<br>If no device is specified, the system forcefully reloads the logged device. |

- `reload {force} {on <DOMAIN-NAME> {staggered}|staggered {<DEVICE-MAC-OR-HOSTNAME>|on <DOMAIN-NAME>}} {containing <WORD>|exclude-controllers|exclude-rf-domain-manager|filter <DEVICE-TYPE>}`

| | |
|---|---|
| reload force | Initiates device(s) reload and configures associated parameters<br>• force – Optional. Forces device(s) to reload, while ignoring conditions like upgrade in progress, unsaved changes, etc. Use the options provided to force a reload on a specified device or all devices in a RF Domain. |
| on <DOMAIN-NAME> staggered | Optional. Forces a reload on all devices in a RF Domain<br>• <DOMAIN-NAME> – Optional. Specify the name of the RF Domain. When executed, all devices within the specified RF Domain are forced to halt and a warm reboot is performed.<br>• staggered – Optional. Enables staggered reload of devices (one at a time) without network impact. Use this option when rebooting multiple devices within an RF Domain. When executed, all devices within the specified RF Domain are forced to halt and reboot in a staggered manner. |

| | |
|---|---|
| staggered {<DEVICE-MAC-OR-HOSTNAME>\| on <DOMAIN-NAME>} | Optional. Enables staggered reload of devices (one at a time) without network impact<br>• <DEVICE-MAC-OR-HOSTNAME> – Optional. Forces a reload on specified device(s) identified by the <DEVICE-MAC-OR-HOSTNAME> keyword. Specify the device's hostname or MAC address. This is a recursive keyword that allows you to specify multiple devices. When executed, the specified device(s) are forced to halt and a warm reboot is performed.<br>• on <DOMAIN-NAME> – Optional. Forces a reload on all devices in a RF Domain. Specify the name of the RF Domain. When executed, all devices within the specified RF Domain are forced to halt and a warm reboot is performed.<br>If no device or RF Domain is specified, the system forcefully reloads the logged device. |
| {containing <WORD>\| exclude-controllers\| exclude-rf-domain-manager\| filter <DEVICE-TYPE>} | When forcefully reloading devices in a RF Domain, you can use following options to filter specific devices or device types:<br>• containing <WORD> – Optional. Filters out devices containing a specified sub-string in their hostnames<br>• <WORD> – Optional. Provide the sub-string to match. All devices having host-names containing the provided sub-string are filtered and forcefully reloaded.<br>• exclude-controllers – Optional. Excludes all controllers in the specified RF Domain from the reload process<br>• exclude-rf-domain-manager – Optional. Excludes the RF Domain manager from the reload process<br>• filter <DEVICE-TYPE> – Optional. Filters devices by the device type specified. Select the type of device. All devices, of the specified type, within the specified RF Domain, are forcefully reloaded.<br>• <DEVICE-TYPE> – Select the type of device to reload. The options are: AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533, RFS4000, RFS6000, NX5500, NX75XX, NX95XX, NX9600, VX9000, t5. |

- `reload {in <1-999>} {list {<LINE>|all}|on <DEVICE-OR-DOMAIN-NAME>}`

| | |
|---|---|
| reload in <1-999> | Initiates device(s) reload and configures associated parameters<br>• in – Optional. Performs a reload after a specified time period<br>• <1-999> – Specify the time from 1 - 999 minutes |
| list {<LINE>\|all} | Optional. Reloads all adopted devices or specified devices<br>• <LINE> – Optional. Reloads listed devices. List all devices (to be reloaded) separated by a space.<br>• all – Optional. Reloads all devices adopted by this controller |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Reloads a specified device or all devices within a specified RF Domain<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |

- `reload {on <DOMAIN-NAME>} {containing <WORD>|exclude-controllers|exclude-rf-domain-manager|filter <DEVICE-TYPE>}`

| | |
|---|---|
| reload<br>on <DOMAIN-NAME> | Initiates device(s) reload and configures associated parameters<br>• on <DOMAIN-NAME> – Optional. Enables reload of all devices in a RF Domain<br>• <DOMAIN-NAME> – Specify the name of the RF Domain. When executed, all devices within the specified RF Domain are immediately halted and a warm reboot is performed.<br>If no RF Domain is specified, the system reloads the logged device. |
| {containing <WORD>\|<br>exclude-controllers\|<br>exclude-rf-domain-manager\|<br>filter <DEVICE-TYPE>} | When reloading devices in a RF Domain, you can use following options to filter specific devices or device types:<br>• containing <WORD> – Optional. Filters out devices containing a specified sub-string in their hostnames.<br>• <WORD> – Optional. Provide the sub-string to match. All devices having hostnames containing the provided sub-string are filtered and forcefully reloaded.<br>• exclude-controllers – Optional. Excludes all controllers in the specified RF Domain from the reload process<br>• exclude-rf-domain-manager – Optional. Excludes the RF Domain manager from the reload process<br>• filter <DEVICE-TYPE> – Optional. Filters devices by the device type specified. Select the type of device to reload. All devices, of the specified type, within the specified RF Domain, are forcefully reloaded.<br>• <DEVICE-TYPE> – Select the type of device to reload. The options are: AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP81XX, AP8232, AP8432, AP8533, RFS4000, RFS6000, NX5500, NX75XX, NX95XX, NX9600, VX9000, t5. All devices of the type specified are reloaded. |

- `reload {staggered} {(<DEVICE-MAC-OR-HOSTNAME>)|on <DOMAIN-NAME>} {containing <WORD>|exclude-controllers|exclude-rf-domain-manager|filter <DEVICE-TYPE>}`

| | |
|---|---|
| reload staggered | Initiates device(s) reload and configures associated parameters<br>• staggered – Optional. Enables staggered reload of devices (one at a time) without network impact |
| {<DEVICE-MAC-OR-HOSTNAME>\|<br>on <DOMAIN-NAME>} | Use one of the following options to specify a single device, multiple devices, or a RF Domain<br>• <DEVICE-MAC-OR-HOSTNAME> – Optional. Performs staggered reload on specified device(s) identified by the <DEVICE-MAC-OR-HOSTNAME> keyword. Specify the device's hostname or MAC address. This is a recursive keyword that allows you to specify multiple devices. When executed, the specified device(s) are halted and a warm reboot is performed. Multiple devices are halted and rebooted one at a time without impacting network functioning.<br>Contd.. |
| | • <DOMAIN-NAME> – Optional. Performs staggered reload of all devices in a RF Domain. Specify the name of the RF Domain. When executed, devices in the specified RF Domain are halted and rebooted one at a time without impacting network functioning. Use additional filter options to filter devices in the specified RF Domain.<br>If no device or RF Domain is specified, the system reloads the logged device. |

| | |
|---|---|
| {containing <WORD>\| exclude-controllers\| exclude-rf-domain-manager\| filter <DEVICE-TYPE>} | When reloading devices in a RF Domain, you can use following options to filter specific devices or device types:<br>• containing <WORD> – Optional. Filters out devices containing a specified sub-string in their hostnames.<br>• <WORD> – Optional. Provide the sub-string to match. All devices having host-names containing the provided sub-string are filtered and reloaded.<br>• exclude-controllers – Optional. Excludes all controllers in the specified RF Domain from the reload process<br>• exclude-rf-domain-manager – Optional. Excludes the RF Domain manager from the reload process<br>• filter <DEVICE-TYPE> – Optional. Filters devices by the device type specified. Select the type of device. All devices, of the specified type, within the specified RF Domain, are reloaded.<br>• <DEVICE-TYPE> – Select the type of device to reload. The options are: AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533, RFS4000, RFS6000, NX5500, NX75XX, NX95XX, NX9600, VX9000, t5. |

**Example**

```
rfs7000-6DCD4B#reload at 12:30:00 31 Mar 2015 on rfs6000-81742D
Reload scheduled at 2015-03-31 12:30:00 UTC ...
rfs7000-6DCD4B#

rfs7000-6DCD4B#reload cancel on rfs6000-81742D
Scheduled reload cancelled.
rfs7000-6DCD4B#
```

The following example schedules a reload on all non-controller devices in the RF Domain ‘default’:

```
rfs7000-6DCD4B#reload on default exclude-controllers
ap8132-711728: OK

rfs7000-6DCD4B#
```

## 3.1.46 rename

*Privileged Exec Mode Commands*

Renames a file in the devices' file system

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
rename <OLD-FILE-NAME> <NEW-FILE-NAME>
```

**Parameters**

- `rename <OLD-FILE-NAME> <NEW-FILE-NAME>`

| | |
|---|---|
| <OLD-FILE-NAME> | Specify the file to rename. |
| <NEW-FILE-NAME> | Specify the new file name. |

**Example**

```
rfs4000-880DA7#dir
Directory of flash:/.

  drwx             Wed Sep 14 13:54:10 2016   log
  drwx             Sat Jan  1 05:30:08 2000   configs
  drwx             Sat Jan  1 05:30:08 2000   cache
  drwx             Wed Nov  4 16:12:15 2015   crashinfo
  drwx             Fri Sep 16 05:26:37 2016   testdir
  drwx             Thu Sep  8 04:09:30 2016   archived_logs
  drwx             Sat Jan  1 05:30:08 2000   upgrade
  drwx             Sat Jan  1 05:30:23 2000   hotspot
  drwx             Sat Jan  1 05:30:08 2000   floorplans
  drwx             Sat Jan  1 05:30:08 2000   tmptpd

rfs4000-880DA7#

rfs4000-880DA7#rename flash:/testdir/ Final
rfs4000-880DA7#

rfs4000-880DA7#dir
Directory of flash:/.

  drwx             Wed Sep 14 13:54:10 2016   log
  drwx             Sat Jan  1 05:30:08 2000   configs
  drwx             Fri Sep 16 05:26:37 2016   Final
  drwx             Sat Jan  1 05:30:08 2000   cache
  drwx             Wed Nov  4 16:12:15 2015   crashinfo
  drwx             Thu Sep  8 04:09:30 2016   archived_logs
  drwx             Sat Jan  1 05:30:08 2000   upgrade
  drwx             Sat Jan  1 05:30:23 2000   hotspot
  drwx             Sat Jan  1 05:30:08 2000   floorplans
  drwx             Sat Jan  1 05:30:08 2000   tmptpd

rfs4000-880DA7#
```

## 3.1.47 rmdir

*Privileged Exec Mode Commands*

Deletes an existing directory from the file system (only empty directories can be removed)

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
rmdir <DIR>
```

**Parameters**

- `rmdir <DIR>`

| | |
|---|---|
| rmdir <DIR> | Specifies the directory name<br>**Note:** The directory, specified by the <DIR> parameter, is removed from the file system. |

**Example**

```
rfs4000-880DA7#dir
Directory of flash:/.

  drwx             Wed Sep 14 13:54:10 2016   log
  drwx             Sat Jan  1 05:30:08 2000   configs
  drwx             Fri Sep 16 05:26:37 2016   Final
  drwx             Sat Jan  1 05:30:08 2000   cache
  drwx             Wed Nov  4 16:12:15 2015   crashinfo
  drwx             Thu Sep  8 04:09:30 2016   archived_logs
  drwx             Sat Jan  1 05:30:08 2000   upgrade
  drwx             Sat Jan  1 05:30:23 2000   hotspot
  drwx             Sat Jan  1 05:30:08 2000   floorplans
  drwx             Sat Jan  1 05:30:08 2000   tmptpd

rfs4000-880DA7#

rfs4000-880DA7#rmdir Final
rfs4000-880DA7#

rfs4000-880DA7#dir
Directory of flash:/.

  drwx             Wed Sep 14 13:54:10 2016   log
  drwx             Sat Jan  1 05:30:08 2000   configs
  drwx             Sat Jan  1 05:30:08 2000   cache
  drwx             Wed Nov  4 16:12:15 2015   crashinfo
  drwx             Thu Sep  8 04:09:30 2016   archived_logs
  drwx             Sat Jan  1 05:30:08 2000   upgrade
  drwx             Sat Jan  1 05:30:23 2000   hotspot
  drwx             Sat Jan  1 05:30:08 2000   floorplans
  drwx             Sat Jan  1 05:30:08 2000   tmptpd

rfs4000-880DA7#
```

## 3.1.48 self

*Privileged Exec Mode Commands*

Enters the logged device's configuration context

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
self
```

**Parameters**

None

**Example**

```
rfs6000-81742D#self
Enter configuration commands, one per line.  End with CNTL/Z.
rfs6000-81742D(config-device-00-15-70-81-74-2D)#
```

## 3.1.49 ssh

*Privileged Exec Mode Commands*

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

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ssh <IP/HOSTNAME> <USERNAME> {<INF-NAME/LINK-LOCAL-ADD>}
```

**Parameters**

- `ssh <IP/HOSTNAME> <USERNAME> {<INF-NAME/LINK-LOCAL-ADD>}`

| | |
|---|---|
| <IP/HOSTNAME> | Specify the remote system's IP address or hostname. |
| <USERNAME> | Specify the name of the user requesting the SSH connection. |
| <INF-NAME/ LINK-LOCAL-ADD> | Optional. Specify the interface's name or link local address. |

**Usage Guidelines**

To exit the other device's context, use the command that is relevant to that device.

**Example**

```
nx9500-6C8809#ssh 192.168.13.16 admin
admin@192.168.13.16's password:
rfs6000-81742D>
```

## 3.1.50 t5

*Privileged Exec Mode Commands*

Executes following operations on a T5 device through the WiNG controller:

- copy, rename, and delete files on the T5 device's file system
- write running configuration to the T5 device's memory

The T5 switch is a means of providing cost-effective, high-speed, wall-to-wall coverage across a building. The T5 switch leverages the in-building telephone lines to extend Ethernet and Wireless LAN networks without additional expenditure on re-wiring. This setup is ideally suited for hotels, providing high-speed Wi-Fi coverage to guest rooms.

The entire setup consists of the DSL T5 switch, TW-510 Ethernet wallplates, and TW-511 wireless wallplate access points. Replace the phone jack plate in a room with the TW-511 delivers 802.11 a/b/g/n and extend wireless connectivity in that room and the neighboring rooms. These TW-511 wallplates (also referred to as the CPEs) are connected to the T5 switch over the DSL interface using a phone block.

The T5 switch is adopted and managed through a WiNG controller. The connection between the T5 and WiNG switches is over a WebSocket.

**NOTE:** For more information on other T5 CPE related commands, see *cpe*.

**Supported in the following platforms:**

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
t5 [copy <SOURCE-FILE-NAME> <DEST-FILE-NAME>|delete <FILE-NAME>|rename <SOURCE-FILE-NAME> <DEST-FILE-NAME>|write memory] {on <T5-DEVICE-NAME>}
```

**Parameters**

```
• t5 [copy <SOURCE-FILE-NAME> <DEST-FILE-NAME>|delete <FILE-NAME>|rename <SOURCE-FILE-NAME> <DEST-FILE-NAME>|write memory] {on <T5-DEVICE-NAME>}
```

| | |
|---|---|
| copy <SOURCE-FILE-NAME> <DEST-FILE-NAME> | Copies file to an external server<br>• <SOURCE-FILE-NAME> – Specify the source file name.<br>• <DEST-FILE-NAME> – Specify the destination file name.<br>The content from the source file is copied to the destination file.<br>The source or destination files can be local or remote FTP or TFTP files. The source file also can be a pre-defined keyword. At least one of the files should be a local file. Use this command to copy the startup and/or running configurations to an external server. |
| delete <FILE-NAME> | Deletes files on the T5 device's file system<br>• <FILE-NAME> – Specify the file name. The specified file is deleted. |

| | |
|---|---|
| rename <SOURCE-FILE-NAME> <DEST-FILE-NAME> | Renames a file on the T5 device's file system<br>• <SOURCE-FILE-NAME> – Specify the source file name<br>• <DEST-FILE-NAME> – Specify the new file name. The source file is renamed to the input provided here. |
| write memory | Writes running configuration to an adopted T5 device's memory<br>• memory – Writes running configuration to the T5 device's *non-volatile* (NV) memory. |
| on <T5-DEVICE-NAME> | Optional. Executes these operation on a specified T5 device<br>• <T5-DEVICE-NAME> – Specify the T5 device's hostname. |

**Example**

```
nx9500-6C8809#t5 write memory on t5-ED7C6C
Success
nx9500-6C8809#
```

## 3.1.51 telnet

*Privileged Exec Mode Commands*

Opens a Telnet session between two network devices

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

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

**Parameters**

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

| | |
|---|---|
| <IP/HOSTNAME> | Configures the remote system's IP (IPv4 or IPv6) address or hostname. The Telnet session will be established between the connecting system and the remote system.<br>• <IP> – Specify the remote system's IPv4 or IPv6 address or hostname. |
| <TCP-PORT> | Optional. Specify the *Transmission Control Protocol* (TCP) port. |
| <INTF-NAME> | Optional. Specify the interface name for the link local address. |

**Usage Guidelines**

To exit the other device's context, use the command relevant to that device.

**Example**

```
nx9500-6C8809#telnet 192.168.13.22

Entering character mode
Escape character is '^]'.


AP7131 release 5.9.0.0-012D
ap7131-11E6C4 login: admin
Password:
ap7131-11E6C4>
```

## 3.1.52 terminal

*Privileged Exec Mode Commands*

Sets the number of characters per line, and the number of lines displayed within the terminal window

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

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

**Parameters**

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

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

**Example**

```
rfs6000-81742D#terminal length 150

rfs6000-81742D#terminal width 215

rfs6000-81742D#show terminal
Terminal Type: xterm
Length: 150     Width: 215
rfs6000-81742D#
```

**Related Commands**

| | |
|---|---|
| *no* | Resets the width of the terminal window or the number of lines displayed on a terminal window |

## 3.1.53 time-it

*Privileged Exec Mode Commands*

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

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

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

**Parameters**

- `time-it <COMMAND>`

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

**Example**

```
rfs6000-81742D#time-it config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
That took 0.00 seconds..
rfs6000-81742D(config)#
```

## 3.1.54 traceroute

*Privileged Exec Mode Commands*

Traces the route to a defined destination

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

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
traceroute <WORD>
```

**Parameters**

- `traceroute <WORD>`

| | |
|---|---|
| <WORD> | Traces the route to a IP address or hostname<br>• <WORD> – Specify the IPv4 address or hostname. |

**Example**

```
nx9500-6C8809#traceroute 192.168.13.16
traceroute to 192.168.13.16 (192.168.13.16), 30 hops max, 46 byte packets
 1  192.168.13.16 (192.168.13.16)  0.479 ms  0.207 ms  0.199 ms
nx9500-6C8809#
```

## 3.1.55 traceroute6

*Privileged Exec Mode Commands*

Traces the route to a specified IPv6 destination

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
traceroute6 <WORD>
```

**Parameters**

- `traceroute6 <WORD>`

| | |
|---|---|
| traceroute6 <WORD> | Traces the route to a IPv6 address or hostname<br>• <WORD> – Specify the IPv6 address or hostname. |

**Example**

```
rfs4000-880DA7#traceroute6 2001:10:10:10:10:10:10:2
traceroute to 2001:10:10:10:10:10:10:2 (2001:10:10:10:10:10:10:2) from
2001:10:10:10:10:10:10:1, 30 hops max, 16 byte packets
 1  2001:10:10:10:10:10:10:2 (2001:10:10:10:10:10:10:2)  0.622 ms  0.497 ms  0.531
ms
rfs4000-880DA7#
```

## 3.1.56 upgrade

*Privileged Exec Mode Commands*

Upgrades a device's software image

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
upgrade [<FILE>|<URL>|dhcp-vendor-options]

upgrade [<FILE>|<URL>] {background|on <DEVICE-NAME>|on <RF-DOMAIN-NAME>}

upgrade dhcp-vendor-options {<DEVICE-NAME>|on <RF-DOMAIN-NAME>}

upgrade dhcp-vendor-options {<DEVICE-NAME>} {<DEVICE-NAME>}

upgrade dhcp-vendor-options {on <RF-DOMAIN-NAME>} {containing <SUB-
STRING>|exclude-controllers|exclude-rf-domain-managers|filter <DEVICE-TYPE>}
```

**Parameters**

- `upgrade [<FILE>|<URL>] {background|on <DEVICE-NAME>|on <RF-DOMAIN-NAME>}`

| | |
|---|---|
| <FILE> | Specify the target firmware image location in the following format:<br>cf:/path/file<br>usb1:/path/file<br>usb2:/path/file<br>usb<n>:/path/file |
| <URL> | Specify the target firmware image location. Use one of the following formats:<br>IPv4 URLs:<br>tftp://<hostname\|IP>[:port]/path/file<br>ftp://<user>:<passwd>@<hostname\|IP>[:port]/path/file<br>sftp://<user>:<passwd>@<hostname\|IP>[:port]>/path/file<br>http://<hostname\|IP>[:port]/path/file<br>cf:/path/file<br>usb<n>:/path/file<br>IPv6 URLs:<br>tftp://<hostname\|[IPv6]>[:port]/path/file<br>ftp://<user>:<passwd>@<hostname\|[IPv6]>[:port]/path/file<br>sftp://<user>:<passwd>@<hostname\|[IPv6]>[:port]>/path/file<br>http://<hostname\|[IPv6]>[:port]/path/file |
| background | Optional. Performs upgrade in the background |

| | |
|---|---|
| on <DEVICE-NAME> | Optional. Upgrades the software image on a specified remote device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |
| on <RF-DOMAIN-NAME> | Optional. Upgrades the software image on all devices within a specified RF Domain<br>• <RF-DOMAIN-NAME> – Specify the name of the RF Domain. |

- `upgrade dhcp-vendor-options {<DEVICE-NAME>} {<DEVICE-NAME>}`

| | |
|---|---|
| dhcp-vendor-options | Uses DHCP vendor options to upgrade device(s) |
| <DEVICE-NAME> {<DEVICE-NAME>} | Optional. Uses DHCP vendor options to upgrade a specified device. Specify the name of the AP, wireless controller, or service platform.<br>• <DEVICE-NAME> – Optional. You can optionally specify multiple comma-separated device names/MAC addresses to upgrade. |

- `upgrade dhcp-vendor-options {on <RF-DOMAIN-NAME>} {containing <SUB-STRING>| exclude-controllers|exclude-rf-domain-managers|filter <DEVICE-TYPE>}`

| | |
|---|---|
| dhcp-vendor-options | Uses DHCP vendor options to upgrade device(s) |
| on <RF-DOMAIN-NAME> {containing <SUB-STRING>\| exclude-controllers\| exclude-rf-domain-managers\| filter <DEVICE-TYPE>} | Optional. Uses DHCP vendor options to upgrade all devices or specified device(s) within the RF Domain identified by the <RF-DOMAIN-NAME> keyword<br>• <RF-DOMAIN-NAME> – Specify the RF Domain name. After specifying the RF Domain, optionally use the filters provided to identify specific device(s) within the RF Domain. If none of the filters are used, all devices within the RF Domain are upgraded. These filters are:<br>• containing <SUB-STRING> – Optional. Upgrades all devices, within the specified RF Domain, containing a specified sub-string in their hostname<br>• <SUB-STRING> – Specify the sub-string to match.<br>• exclude-controllers – Optional. Upgrades all devices, within the specified RF Domain, excluding controllers. Since only a NOC controller is capable of adopting other controllers, use this option when executing the command on a NOC controller.<br>• exclude-rf-domain-manager – Optional. Upgrades all devices, within the specified RF Domain, excluding RF Domain managers. Use this option when executing the command on the NOC, Site controller, or RF Domain manager.<br>• filter <DEVICE-TYPE> – Optional. Executes the command on all devices, within the specified RF Domain, of a specified type<br>• <DEVICE-TYPE> – Specify the device type. The options are: AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP81XX, AP8232, AP8432, AP8533, RFS4000, RFS6000, NX5500, NX75XX, NX95XX, NX9600, and VX9000. Upgrades all devices of the type specified here. For example, if AP6521 is the device-type specified, all AP6521s within the specified RF Domain are upgraded |

**Example**

```
nx9500-6C8809#show boot
------------------------------------------------------------------------------
     IMAGE            BUILD DATE             INSTALL DATE          VERSION
------------------------------------------------------------------------------
  Primary       02/05/2017 14:33:58     02/11/2017 12:27:53     5.9.0.0-024D
  Secondary     02/01/2017 21:36:24     02/03/2017 12:05:48     5.8.6.0-007B
------------------------------------------------------------------------------
Current Boot       : Secondary
Next Boot          : Primary
Software Fallback  : Enabled
VM support         : Not presentt
nx9500-6C8809#
```

```
nx9500-6C8809#upgrade ftp://anonymous:anonymous@192.168.13.10/LatestBuilds/W59/
NX9500.img
Running from partition /dev/sda7
Validating image file header
Removing other partition
Making file system
Extracting files (this may take some
time).....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................
Control C disabled
Version of firmware update file is 5.9.0.0-026D
Removing unneeded files from flash:/crashinfo directory
Removing unneeded files from flash:/var2/log directory
Creating LILO files
Running LILO
Successful
nx9500-6C8809#

nx9500-6C8809#show boot
------------------------------------------------------------------------------
     IMAGE            BUILD DATE              INSTALL DATE          VERSION
------------------------------------------------------------------------------
  Primary       05/01/2017 12:03:13 05/10/2017 10:12:53     5.9.0.0-026D
  Secondary     05/01/2017 19:30:21 05/02/2017 10:05:48     5.9.0.0-007B
------------------------------------------------------------------------------
Current Boot       : Secondary
Next Boot          : Primary
Software Fallback  : Enabled
VM support         : Not present
nx9500-6C8809#
```

After upgrading, the device has to be reloaded to boot using the new image.

```
nx7500-7F3609#upgrade tftp://192.168.0.50/RFS6000-5.9.0.-012D.img rfs6000-6DCBB3
------------------------------------------------------------------------------
      DEVICE                      STATUS                MESSAGE
------------------------------------------------------------------------------
  rfs6000-6DCBB3                Success                   None
------------------------------------------------------------------------------
nx7500-7F3609#show upgrade-status
Last Image Upgrade Status : Successful
Last Image Upgrade Time   : 2017-03-26 10:31:12
nx7500-7F3609#
```

The following example shows the upgrade status:

```
nx7500-7F3609#show upgrade detail
Last Image Upgrade Status : Successful
Last Image Upgrade Time   : 2017-03-26 10:31:12
-----------------------------------------------
Running from partition /dev/sda7
var2 is 2 percent full
/tmp is 2 percent full
Free Memory 15258044 kB
FWU invoked via Linux shell
Validating image file header
Removing other partition
```

```
Making file system
Extracting files (this may take some time).
Control C disabled
Version of firmware update file is 5.9.0.-012D
Creating LILO files
Running LILO
Successful

nx7500-7F3609#

nx7500-7F3609#show upgrade on rfs6000-6DCBB3
Last Image Upgrade Status :Successful
Last Image Upgrade Time   :2017-03-26 10:31:12
nx7500-7F3609#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes a patch installed on a specified device |

## 3.1.57 upgrade-abort

*Privileged Exec Mode Commands*

Aborts an ongoing software image upgrade

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
upgrade-abort {on <DEVICE-OR-DOMAIN-NAME>}
```

**Parameters**

- `upgrade-abort {on <DEVICE-OR-DOMAIN-NAME>}`

| | |
|---|---|
| upgrade-abort | Aborts an ongoing software image upgrade |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Aborts an ongoing software image upgrade on a specified device or domain<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |

**Example**

```
rfs4000-229D58#upgrade ftp://anonymous:anonymous@192.168.13.10/LatestBuilds/W59/
RFS4000-5.9.0.0-012D.img
Running from partition /dev/mtdblock6
Validating image file header
Making file system
Extracting files (this may take some time).................

rfs6000-81701D#upgrade-abort on rfs4000-229D58

rfs4000-229D58#upgrade ftp://anonymous:anonymous@192.168.13.10/LatestBuilds/W59/
RFS4000-5.9.0.0-012D.img.img
Running from partition /dev/mtdblock6
Validating image file header
Making file system
Extracting files (this may take some time).................
Update error:  Aborted
rfs4000-229D58#
```

## 3.1.58 virtual-machine

*Privileged Exec Mode Commands*

Installs, configures, and monitors the status of virtual machines (VMs) installed on a WiNG controller

**Supported in the following platforms:**

- Service Platforms — NX9500, NX9510, NX9600, VX9000

**Syntax**

```
virtual-machine [assign-usb-ports|export|install|restart|set|start|
stop|uninstall]

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

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

virtual-machine install [<VM-NAME>|adsp|team-urc|team-rls|team-vowlan]
{on <DEVICE-NAME>}

virtual-machine restart [<VM-NAME>|hard|team-urc|team-rls|team-vowlan]

virtual-machine set [autostart|memory|vcpus|vif-count|vif-mac|vif-to-vmif|vnc]

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

The following virtual-machine commands are supported only on the VX9000 platform:

virtual-machine volume-group [add-drive|replace-drive|resize-drive|resize-volume-
group]

virtual-machine volume-group [add-drive|replace-drive] <BLOCK-DEVICE-LABEL>

virtual-machine volume-group replace-drive <BLOCK-DEVICE-LABLE> <NEW-BLOCK-
DEVICE-LABEL>

virtual-machine volume-group resize-volume-group <BLOCK-DEVICE-LABEL>
```

**Parameters**

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

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

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

| | |
|---|---|
| virtual-machine export | Exports an existing VM image and settings. Use this command to export the VM to another <NX54XX> or <NX65XX> device in the same domain.<br>• <VM-NAME> – Specify the VM name.<br>• <FILE> – Specify the location and name of the source file (VM image). The VM image is retrieved and exported from the specified location.<br>• <URL> – Specify the destination location. This is the location to which the VM image is copied. Use one of the following formats to provide the destination path:<br>Contd.. |

| | |
|---|---|
| | tftp://<hostname\|IP>[:port]/path/file<br>ftp://<user>:<passwd>@<hostname\|IP>[:port]/path/file<br>sftp://<user>:<passwd>@<hostname\|IP>[:port]>/path/file<br>http://<hostname\|IP>[:port]/path/file<br>• on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices<br>• <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas.<br>Note: The VM should be in a stop state during the export process.<br>Note: If the destination is a device, the image is copied to a predefined location (VM archive). |

• `virtual-machine install [<VM-NAME>|adsp|team-centro|team-rls|team-vowlan] {on <DEVICE-NAME>}`

| | |
|---|---|
| virtual-machine install | Installs the VM. The install command internally creates a VM template, consisting of the specified parameters, and starts the installation process. Select one of the following options:<br>• <VM-NAME> – Installs a VM having name specified by <VM-NAME> keyword.<br>• adsp – Installs ADSP<br>• team-centro – Installs the VM TEAM-Centro image<br>• team-rls – Installs the VM TEAM-RLS image<br>• team-vowlan – Installs the VM TEAM-VoWLAN image<br>Specify the device on which to install the VM.<br>• on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices<br>• <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas. |

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

| | |
|---|---|
| virtual-machine set | Configures the VM settings<br>• autostart – Specifies whether to autostart the VM on system reboot<br>• ignore – Enables autostart on each system reboot<br>• start – Disables autostart<br>• memory – Defines the VM memory size<br>• <512-8192> – Specify the VM memory from 512 - 8192 MB. The default is 1024 MB.<br>• vcpus – Specifies the number of VCPUS for this VM<br>• <1-4> – Specify the number of VCPUS from 1- 4.<br>• vif-count – Configures or resets the VM's VIFs<br>• <0-2> – Specify the VIF number from 0 - 2.<br>• vif-mac – Configures the MAC address of the selected virtual network interface<br>• <1-2> – Select the VIF<br>• <1-8> – Specify the MAC index for the selected VIF<br>• <MAC> – Specify the customized MAC address for the selected VIF in the AA-BB-CC-DD-EE-FF format.<br>Contd.. |

| | |
|---|---|
| | Each VM has a maximum of two network interfaces (indexed 1 and 2, referred to as VIF). By default, each VIF is automatically assigned a MAC from the range allocated for that device. However, you can use the 'set' keyword to specify the MAC from within the allocated range. Each of these VIFs are mapped to a layer 2 port in the dataplane (referred to as VMIF). These VMIFs are standard l2 ports on the DP bridge, supporting all VLAN and ACL commands. The WiNG software supports up to a maximum of 8 VMIFs. By default, a VM's interface is always mapped to VMIF1. You can map a VIF to any of the 8 VMIFs. Use the vif-to-vmif command to map a VIF to a VMIF on the DP bridge.<br>• vif-to-vmif – Maps the virtual interface (1 or 2) to the selected VMIF interface. Specify the VMIF interface index from 1 - 8.<br>WiNG provides a dataplane bridge for external network connectivity for VMs. VM Interfaces define which IP address is associated with each VLAN ID the service platform is connected to and enables remote service platform administration. Each custom VM can have up to a maximum of two VM interfaces. Each VM interface can be mapped to one of the twelve ports for <NX9500> on the dataplane bridge. This mapping determines the destination for service platform routing.<br>By default, VM interfaces are internally connected to the dataplane bridge via VMIF1. VMIF1, by default, is an untagged port providing access to VLAN 1 to support the capability to connect the VM interfaces to any of the VMIF ports. This provides the flexibility to move a VM interface onto different VLANs as well as configure specific firewall and QoS rules.<br>• vnc – Disables/enables VNC port option for an existing VM. When enabled, provides remote access to VGA through the noVNC client.<br>  • disable – Disables VNC port<br>  • enable – Enables VNC port<br>After configuring the VM settings, identify the VM to apply the settings.<br>• <VM-NAME> – Applies these settings to the VM identified by the <VM-NAME> keyword. Specify the VM name.<br>• adsp – Applies these settings to the ADSP VM<br>• team-urc – Applies these settings to the VM TEAM-URC<br>• team-rls – Applies these settings to the VM TEAM-RLS<br>• team-vowlan – Applies these settings to the VM TEAM-VoWLAN |

• `virtual-machine start [<VM-NAME>|adsp|team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}`

| | |
|---|---|
| virtual-machine start | Starts the VM, based on the parameters passed. Select one of the following options:<br>• <VM-NAME> – Starts the VM identified by the <VM-NAME> keyword. Specify the VM name.<br>• adsp – Starts the ADSP VM<br>• team-urc – Starts the VM TEAM-URC<br>• team-rls – Starts the VM TEAM-RLS<br>• team-vowlan – Starts the VM TEAM-VoWLAN<br>The following keywords are common to all of the above parameters:<br>• on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices<br>  • <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas. |

- `virtual-machine stop [<VM-NAME>|adsp|team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}`

| | |
|---|---|
| virtual-machine stop hard | Stops the VM, based on the parameters passed. Select one of the following options:<br>• <VM-NAME> – Stops the VM identified by the <VM-NAME> keyword. Specify the VM name.<br>• ADSP – Stops the ADSP VM<br>• team-urc – Stops the VM TEAM-URC<br>• team-rls – Stops the VM TEAM-RLS<br>• team-vowlan – Stops the VM TEAM-VoWLAN<br>The following keywords are common to all of the above parameters:<br>• on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices<br>• <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas.<br>Note: The option 'hard' forces the selected VM to shutdown. |

- `virtual-machine uninstall [<VM-NAME>|adsp|team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}`

| | |
|---|---|
| virtual-machine uninstall | Uninstalls the specified VM<br>• <VM-NAME> – Uninstalls the VM identified by the <VM-NAME> keyword. Specify the VM name.<br>• ADSP – Uninstalls the ADSP VM<br>• team-urc – Uninstalls the VM TEAM-URC<br>• team-rls – Uninstalls the VM TEAM-RLS<br>• team-vowlan – Uninstalls the VM TEAM-VoWLAN<br>The following keywords are common to all of the above parameters:<br>• on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices<br>• <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas.<br>Note: This command releases the VM's resources, such as memory, VCPUS, VNC port, disk space, and removes the RF Domain reference from the system. |

- `virtual-machine volume-group [add-drive|resize-drive] <BLOCK-DEVICE-LABEL>]`

| | |
|---|---|
| virtual-machine volume-group [add-drive\|resize-drive] <BLOCK-DEVICE-LABEL>] | Enables provisioning of logical volume-groups on the VX9000 platform. Logical volume-groups are created on the primary storage device, allowing the database storage to be expanded to include additional storage drives. However, volume-groups can be provisioned only on new VX9000 installation and cannot be added to existing VX9000 installation.<br>**Note:** The logical volume-group is supported only on a VX9000 running the WiNG 5.9.1 image.<br>Contd.. |

| | |
|---|---|
| | • add-drive – Adds a new block-device to the VM. Note, currently a maximum of 3 (three) block devices can be added. To add a new drive, first halt the VM, In the Hypervisor, add a new storage disk to the VM and restart the VM. Once the VM comes up, use this command to add the new drive. To identify the new drive execute the *show > virtual-machine > volume-group > status* command.<br>• resize-drive - Resizes a drive in the VM's volume group. To increase the size of a drive in the volume-group, first halt the VM. In the Hypervisor, increase the size of the existing secondary storage drive and restart the VM. Once the VM comes up, use this command to resize the drive. To identify the drive with the additional free space, execute the show > virtual-machine > volume-group > status command.<br>The following keyword is common to all of the above parameters:<br>• <BLOCK-DEVICE-LABEL> –Specify the block-device label to be added or resized depending on the action being performed. |

• `virtual-machine volume-group replace-drive <BLOCK-DEVICE-LABEL> <NEW-BLOCK-DEVICE-LABEL>]`

| | |
|---|---|
| virtual-machine volume-group replace-drive <BLOCK-DEVICE-LABEL> <NEW-BLOCK-DEVICE-LABEL>] | Enables provisioning of VMs as logical volume-groups on the VX9000 platform. Logical volume-group VMs are created on the primary storage device, allowing the database storage to be expanded to include additional storage drives.<br>• replace-drive – Replaces an existing block-device with a new block-device in a volume-group. To replace a drive in the volume-group, first halt the VM. In the Hypervisor, add the new drive and restart the VM. Once the VM comes up, use this command to replace an existing drive with the new drive. To identify the drive with the additional free space, execute the *show > virtual-machine > volume-group > status* command<br>• <BLOCK-DEVICE-LABEL> –Specify the block-device label to be replaced.<br>• <BLOCK-DEVICE-LABEL> – Specify the replacement block-device label. |

• `virtual-machine volume-group resize-volume-group <BLOCK-DEVICE-LABEL>]`

| | |
|---|---|
| virtual-machine volume-group resize-volume-group <BLOCK-DEVICE-LABEL>] | Enables provisioning of VMs as logical volume-groups on the VX9000 platform. Logical volume-group VMs are created on the primary storage device, allowing the database storage to be expanded to include additional storage drives<br>• resize-volume-group – Adds drive space to an existing block-device in the volume-group<br>• <BLOCK-DEVICE-LABEL> –Specify the block-device label to which additional drive space is to be provided |

### Example

The following examples show the VM installation process:

**Insatllation media: USB**

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

**Installation media: pre-installed disk image**

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

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

**Installation media: VM archive**

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

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

**Exporting an installed VM:**

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

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

```
nx9500-6C8809#virtual-machine install team-urc
Virtual Machine install team-urc command successfully sent.
nx9500-6C8809#

vx9000-DE6F97>cirtual-machine add-drive sdb

vx9000-DE6F97>show virtual-machine volume-group status
----------------------------------------
Logical Volume: lv1
----------------------------------------
 STATUS           : available
 SIZE             : 81.89 GiB
 VOLUME GROUP     : vg0
 PHYSICAL VOLUMES :
     sda10        : 73.90 GiB
     sdc1         : 8.00 GiB
 AVAILABLE DISKS  :
     sdb          : size: 8590MB
----------------------------------------
* indicates a drive that must be resized
----------------------------------------
vx9000-DE6F97#
```

## 3.1.59 watch

*Privileged Exec Mode Commands*

Repeats a specified CLI command at periodic intervals

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

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

**Parameters**

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

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

**Example**

```
rfs6000-81742D#watch 1 show clock
rfs6000-81742D#
```

## 3.1.60 exit

*Privileged Exec Mode Commands*

Ends the current CLI session and closes the session window

For more information, see *exit*.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
exit
```

**Parameters**

None

**Example**

```
rfs6000-81742D#exit
```

## 3.1.61 raid

*Privileged Exec Mode Commands*

Enables *Redundant Array of Independent Disks* (RAID) management

RAID is a group of one or more independent, physical drives, referred to as an array or drive group, These physically independent drives are linked together and appear as a single storage unit or multiple virtual drives. Replacing a single, large drive system with an array, improves performance (input and output processes are faster) and increases fault tolerance within the data storage system.

In an array, the drives can be organized in different ways, resulting in different RAID types. Each RAID type is identified by a number, which determines the RAID level. The common RAID levels are 0, 00, 1, 5, 6, 50 and 60. The WiNG MegaRAID implementation supports RAID-1, which provides data mirroring, but does not support data parity. RAID-1 consists of a two-drive array, where the data is simultaneously written on both drives, ensuring total data redundancy. In case of a drive failure the information on the other drive is used to rebuild the failed drive.

An array is said to be degraded when one of its drives has failed. A degraded array continues to function and can be rebooted using the one remaining functional drive. When a drive fails, the chassis sounds an alarm (if enabled), and the CLI prompt changes to “RAID degraded”. The failed drive is automatically replaced with a hot spare (provided a spare is installed). The spare is used to re-build the array.

Use this command to:

- Verify the current array status
- Start and monitor array consistency checks
- Retrieve date and time of the last consistency check
- Shut down drives before physically removing them
- Install new drives
- Assign drives as hot spares
- Identify a degraded drive
- Deactivate an alarm (triggered when a drive is removed from the array)

**Supported in the following platforms:**

- Service Platforms — NX7530, NX9500, NX9510

**NOTE:** RAID controller drive arrays are available within NX7530 and NX95XX series service platforms (NX9500 and NX9510 models) only. However, they can be administrated on behalf of a NX9500 profile by a different model service platform or controller. The NX9500 service platform includes a single Intel MegaRAID controller, configured to provide a single virtual drive. This virtual drive is of the RAID-1 type, and has a maximum of two physical drives. In addition to these two drives, there are three hot spares, which are used in case of a primary drive failure.

**Syntax**

```
raid [check|install|locate|remove|silence|spare]

raid [check|silence]

raid [install|locate|remove|spare] drive <0-4>
```

**Parameters**

- `raid [check|silence]`

| | |
|---|---|
| check | Starts a consistency check on the RAID array. Use the *show > raid* command to view consistency check status.<br>A consistency check verifies the data stored in the array. When regularly executed, it helps protect against data corruption, and ensures data redundancy. Consistency checks also warn of potential disk failures. |
| silence | Deactivates an alarm<br>When enabled, an audible alarm is triggered when a drive in the array fails. The *silence* command deactivates the alarm (sound).<br>**Note:** To enable RAID alarm, in the device configuration mode, use the *raid > alarm > enable* command. A NX9500 profile can also have the RAID alarm feature activated. For more information on the enabling RAID alarm, see *raid*. |

- `raid [install|locate|remove|spare] drive <0-4>`

| | |
|---|---|
| install <0-4> | Installs a new drive, inserted in one of the available slots, in the array. Specify the drive number.<br>Drives 0 and 1 are the array drives. Drives 2, 3, and 4 are the hot spare drives. You can include the new drive in a degraded array, or enable it as a hot spare.<br>If the array is in a degraded state, the re-build process is triggered and the new drive is used to repair the degraded array. |
| locate <0-4> | Enables LEDs to blink on a specified drive. Specify the drive number.<br>Blinking LEDs enable you correctly locate a drive. |
| remove <0-4> | Removes (shuts downs) a disk from the array, before it is physically removed from its slot. Specify the drive number containing the disk.<br>Use this command to also remove a hot spare. |
| spare <0-4> | Converts an unused drive into a hot spare. Specify the drive number. |

**Example**

```
nx9500-6C874D#raid install drive 0
Error: Input Error: Drive 0 is already member of array, can't be added
nx9500-6C874D#
```

# 4 GLOBAL CONFIGURATION COMMANDS

This chapter summarizes the global-configuration commands in the CLI command structure.

The term global indicates characteristics or features effecting the system as a whole. Use the Global Configuration Mode to configure the system globally, or enter specific configuration modes to configure specific elements (such as interfaces or protocols). Use the configure terminal command (under PRIV EXEC) to enter the global configuration mode.

The following example describes the process of entering the global configuration mode from the PRIV EXEC mode:

```
<DEVICE>#configure terminal
<DEVICE>(config)#
```

**NOTE:** The system prompt changes to indicate you are now in the global configuration mode. The prompt consists of the device host name followed by (config) and a pound sign (#).

Commands entered in the global configuration mode update the running configuration file as soon as they are entered. However, these changes are not saved in the startup configuration file until a *commit write memory* command is issued.

```
<DEVICE>(config)#?
Global configuration commands:
aaa-policy                              Configure a
                                          authentication/accounting/authorization
                                          policy
  aaa-tacacs-policy                       Configure an
                                          authentication/accounting/authorization
                                          TACACS policy
  alias                                   Alias
  ap621                                   AP621 access point
  ap622                                   AP622 access point
  ap650                                   AP650 access point
  ap6511                                  AP6511 access point
  ap6521                                  AP6521 access point
  ap6522                                  AP6522 access point
  ap6532                                  AP6532 access point
  ap6562                                  AP6562 access point
  ap71xx                                  AP71XX access point
  ap7502                                  AP7502 access point
  ap7522                                  AP7522 access point
  ap7532                                  AP7532 access point
  ap7562                                  AP7562 access point
  ap7602                                  AP7602 access point
  ap7612                                  AP7612 access point
  ap7622                                  AP7622 access point
  ap7632                                  AP7632 access point
  ap7662                                  AP7662 access point
  ap81xx                                  AP81XX access point
  ap82xx                                  AP82XX access point
  ap8432                                  AP8432 access point
  ap8533                                  AP8533 access point
  application                             Configure an application
  application-group                       Configure an application-group
  application-policy                      Configure an application policy
  association-acl-policy                  Configure an association acl policy
  auto-provisioning-policy                Configure an auto-provisioning policy
  bgp                                     BGP Configuration
  bonjour-gw-discovery-policy             Bonjour Gateway discovery policy
  bonjour-gw-forwarding-policy            Bonjour Gateway forwarding policy
```

```
bonjour-gw-query-forwarding-policy  Bonjour Gateway Query forwarding policy
captive-portal                      Configure a captive portal
clear                               Clear
client-identity                     Client identity (DHCP Device
                                    Fingerprinting)
client-identity-group               Client identity group (DHCP Fingerprint
                                    Database)
clone                               Clone configuration object
crypto-cmp-policy                   CMP policy
customize                           Customize the output of summary cli
                                    commands
database-client-policy              Configure database client policy
database-policy                     Configure database policy
device                              Configuration on multiple devices
device-categorization               Configure a device categorization object
dhcp-server-policy                  DHCP server policy
dhcpv6-server-policy                DHCPv6 server related configuration
dns-whitelist                       Configure a whitelist
event-system-policy                 Configure a event system policy
ex3500                              Ex3500 device
ex3500-management-policy            Configure a ex3500 management policy
ex3500-qos-class-map-policy         Configure a ex3500 qos class-map policy
ex3500-qos-policy-map               Configure a ex3500 qos policy-map
ex3524                              EX3524 wireless controller
ex3548                              EX3548 wireless controller
firewall-policy                     Configure firewall policy
global-association-list             Configure a global association list
guest-management                    Configure a guest management policy
help                                Description of the interactive help
                                    system
host                                Enter the configuration context of a
                                    device by specifying its hostname
igmp-snoop-policy                   Create igmp snoop policy
inline-password-encryption          Store encryption key in the startup
                                    configuration file
ip                                  Internet Protocol (IP)
ipv6                                Internet Protocol version 6 (IPv6)
ipv6-router-advertisement-policy    IPv6 Router Advertisement related
                                    configuration
l2tpv3                              L2tpv3 tunnel protocol
mac                                 MAC configuration
management-policy                   Configure a management policy
meshpoint                           Create a new MESHPOINT or enter
                                    MESHPOINT configuration context for one
                                    or more MESHPOINTs
meshpoint-qos-policy                Configure a meshpoint quality-of-service
                                    policy
mint-policy                         Configure the global mint policy
nac-list                            Configure a network access control list
no                                  .
nsight-policy                       Configure a Nsight policy
nx45xx                              NX45XX integrated services platform
nx5500                              NX5500 wireless controller
nx65xx                              NX65XX integrated services platform
nx75xx                              NX75XX wireless controller
nx9000                              NX9000 wireless controller
passpoint-policy                    Configure a passpoint policy
password-encryption                 Encrypt passwords in configuration
profile                             Profile related commands - if no
                                    parameters are given, all profiles are
                                    selected
radio-qos-policy                    Configure a radio quality-of-service
                                    policy
radius-group                        Configure radius user group parameters
radius-server-policy                Create device onboard radius policy
radius-user-pool-policy             Configure Radius User Pool
rename                              Clone configuration object
replace                             Replace configuration object
```

```
  rf-domain                       Create a RF Domain or enter rf-domain
                                  context for one or more rf-domains
  rfs4000                         RFS4000 wireless controller
  rfs6000                         RFS6000 wireless controller
  rfs7000                         RFS7000 wireless controller
  roaming-assist-policy           Configure a roaming-assist policy
  role-policy                     Role based firewall policy
  route-map                       Dynamic routing route map Configuration
  routing-policy                  Policy Based Routing Configuration
  rtl-server-policy               Configure a rtl server policy
  schedule-policy                 Configure a schedule policy
  self                            Config context of the device currently
                                  logged into
  sensor-policy                   Configure a sensor policy
  smart-rf-policy                 Configure a Smart-RF policy
  t5                              T5 DSL switch
  url-filter                      Configure a url filter
  url-list                        Configure a URL list
  vx9000                          VX9000 wireless controller
  web-filter-policy               Configure a web filter policy
  wips-policy                     Configure a wips policy
  wlan                            Create a new WLAN or enter WLAN
                                  configuration context for one or more
                                  WLANs
  wlan-qos-policy                 Configure a wlan quality-of-service
                                  policy
  write                           Write running configuration to memory or
                                  terminal

  clrscr                          Clears the display screen
  commit                          Commit all changes made in this session
  do                              Run commands from Exec mode
  end                             End current mode and change to EXEC mode
  exit                            End current mode and down to previous
                                  mode
  revert                          Revert changes
  service                         Service Commands
  show                            Show running system information

<DEVICE>(config)#
```

# 4.1 Global Configuration Commands

- *GLOBAL CONFIGURATION COMMANDS*

The following table summarizes Global Configuration mode commands:

**Table 4.1** *Global Config Commands*

| Command | Description | Reference |
|---|---|---|
| *aaa-policy* | Creates a AAA policy and enters its configuration mode. This policy enables administrators to define access control within the network. | *page 4-9* |
| *aaa-tacacs-policy* | Creates a AAA-TACACS policy and enters its configuration mode. This policy provides access control to network devices such as routers, network access servers, and other computing devices through centralized servers. | *page 4-20* |
| *alias* | Creates various types of aliases, such as network, VLAN, network-group, network-service, encrypted-string, hashed -string, etc. | *page 4-11* |
| *ap6521* | Adds an AP6521 to the network | *page 4-22* |
| *ap6522* | Adds an AP6522 to the network | *page 4-23* |
| *ap6532* | Adds an AP6532 to the network | *page 4-24* |
| *ap6562* | Adds an AP6562 to the network | *page 4-25* |
| *ap71xx* | Adds an AP7161 to the network | *page 4-26* |
| *ap7502* | Adds an AP7502 to the network | *page 4-27* |
| *ap7522* | Adds an AP7522 to the network | *page 4-28* |
| *ap7532* | Adds an AP7532 to the network | *page 4-29* |
| *ap7562* | Adds an AP7562 to the network | *page 4-30* |
| *ap7602* | Adds an AP7602 to the network | *page 4-31* |
| *ap7612* | Adds an AP7612 to the network | *page 4-32* |
| *ap7622* | Adds an AP7622 to the network | *page 4-33* |
| *ap7632* | Adds an AP7632 to the network | *page 4-34* |
| *ap7662* | Adds an AP7662 to the network | *page 4-35* |
| *ap81xx* | Adds an AP81XX to the network | *page 4-36* |
| *ap82xx* | Adds an AP82XX to the network | *page 4-37* |
| *ap8432* | Adds an AP8432 to the network | *page 4-38* |
| *ap8533* | Adds an AP8533 to the network | *page 4-39* |
| *application* | Creates an application definition and enters its configuration mode. This command allows you to create a customized application detection definition. | *page 4-40* |
| *application-group* | Creates an application group and enters its configuration mode | *page 4-48* |
| *application-policy* | Creates an application policy and enters its configuration mode. This policy defines the actions executed on recognized HTTP (e.g. Facebook), enterprise (e.g. Webex) and peer-to-peer (e.g. gaming) applications or application-categories. | *page 4-55* |

**Table 4.1** *Global Config Commands*

| Command | Description | Reference |
|---|---|---|
| *association-acl-policy* | Creates an association ACL policy and enters its configuration mode. This policy restricts access by specifying a client MAC address or range of addresses to either include or exclude from WLAN connectivity. | *page 4-78* |
| *auto-provisioning-policy* | Creates an auto provisioning policy and enters its configuration mode. This policy defines the process by which an access point discovers controllers and associates with it. | *page 4-79* |
| *bgp* | Configures *Border Gateway Protocol* (BGP) settings | *page 4-81* |
| *bonjour-gw-discovery-policy* | Creates a Bonjour GW Discovery policy and enters its configuration mode. This policy configures the VLANs on which Bonjour services are located. | *page 4-84* |
| *bonjour-gw-forwarding-policy* | Configures a Bonjour GW Forwarding policy and enters its configuration mode. This policy enables the discovery of services on VLANs not visible to the device running the Bonjour Gateway. | *page 4-90* |
| *bonjour-gw-query-forwarding-policy* | Creates a Bonjour GW Query Forwarding policy and enters its configuration mode. This policy enables Bonjour query forwarding across multiple VLANs. | *page 4-92* |
| *captive portal* | Creates a captive portal and enters its configuration mode | *page 4-93* |
| *clear* | Clears the event history | *page 4-146* |
| *client-identity* | Creates a client identity definition and enters its configuration mode. This feature enables client identification through DHCP device fingerprinting. | *page 4-147* |
| *client-identity-group* | Creates a new client identity group and enters its configuration mode | *page 4-156* |
| *clone* | Clones a specified configuration object | *page 4-164* |
| *crypto-cmp-policy* | Creates a crypto *Certificate Management Protocol* (CMP) policy and enters its configuration mode. CMP is an Internet protocol designed to obtain and manage digital certificates in a *Public Key Infrastructure* (PKI) network. | *page 4-165* |
| *customize* | Customizes the CLI command summary output | *page 4-166* |
| *database-client-policy* | Creates a database client policy and enters its configuration mode. The database client policy configures the IP address or hostname of the VX9000 hosting the *captive-portal/NSight database*. Use this option when deploying a split NSight/EGuest deployment. | *page 4-177* |
| *database-policy* | Creates a database policy and enters its configuration mode. This policy enables the database, and also configures the database replica set. | *page 4-184* |
| *device* | Specifies configuration on multiple devices | *page 4-192* |
| *device-categorization* | Creates a device categorization list and enters its configuration mode. The list categorizes devices as sanctioned or neighboring. Categorization of devices enables quick identification and blocking of unsanctioned devices in the network. | *page 4-194* |
| *dhcp-server-policy* | Creates a DHCP server policy and enters its configuration mode. This policy allows hosts on an IP network to request and be assigned IP addresses and discover information about the network. | *page 4-200* |

**Table 4.1** *Global Config Commands*

| Command | Description | Reference |
|---|---|---|
| *dhcpv6-server-policy* | Creates a DHCPv6 server policy and enters its configuration mode. This policy configures hosts with IPv6 addresses, IP prefixes and other configuration attributes required on an IPv6 network. | *page 4-201* |
| *dns-whitelist* | Creates a DNS whitelist and enters its configuration mode. A DNS whitelist is used with a captive portal to provide access services to requesting wireless clients. | *page 4-203* |
| *event-system-policy* | Creates an Event system policy and enters its configuration mode. This policy enables administrators to create notification mechanisms using one, some, or all of the SNMP, syslog, controller forwarding, or email notification options available to the controller or service platform. | *page 4-209* |
| *ex3500* | Creates an EX3500 time range list and enters its configuration mode | *page 4-227* |
| *ex3500-management-policy* | Creates an EX3500 management policy and enters its configuration mode. This policy controls access to the EX3500 switch from management stations using SNMP. | *page 4-233* |
| *ex3500-qos-class-map-policy* | Creates an EX3500 QoS class map policy and enters its configuration mode. The QoS policy map assigns priority to mission critical EX3500 switch data traffic, prevent EX3500 switch bandwidth congestion, and prevent packet drops. | *page 4-254* |
| *ex3500-qos-policy-map* | Creates an EX3500 QoS policy map and enters its configuration mode. This policy defines rules that filter traffic exchanged between the EX3500 switch and its connected devices. | *page 4-262* |
| *ex3524* | Adds a EX3524 switch to the network | *page 4-277* |
| *ex3548* | Adds a EX3548 switch to the network | *page 4-279* |
| *firewall-policy* | Creates a firewall policy and enters its configuration mode. This policy configures safe guards against *denial of service* (DoS) attacks and packet storms. It also configures firewall parameters, such as logging, application layer gateway, TCP protocol checks, state flow checks, etc. | *page 4-280* |
| *global-association-list* | Creates a global list of client MAC addresses | *page 4-282* |
| *guest-management* | Creates a guest management policy and enters its configuration mode. This policy redirects guest users to a registration portal, upon association to a captive portal *Service Set Identifier* (SSID). | *page 4-286* |
| *host* | Sets the system's network name | *page 4-297* |
| *inline-password-encryption* | Stores the encryption key in the startup configuration file | *page 4-298* |
| *ip* | Creates a IP *access control list* (ACL) and/or a *Simple Network Management Protocol* (SNMP) ACL, and enters its configuration mode | *page 4-299* |
| *ipv6* | Creates a IPv6 ACL and enters its configuration mode | *page 4-301* |
| *ipv6-router-advertisement-policy* | Creates an IPv6 *router advertisement* (RA) policy and enters its configuration mode | *page 4-302* |
| *l2tpv3* | Creates *Layer 2 Tunneling Protocol Version 3* (L2TPV3) tunnel policy and enters its configuration mode. This policy defines control and encapsulation protocols for tunneling layer 2 frames between two IP nodes. | *page 4-320* |

**Table 4.1** *Global Config Commands*

| Command | Description | Reference |
|---|---|---|
| *mac* | Configures MAC access lists (goes to the MAC ACL mode) | *page 4-322* |
| *management-policy* | Creates a management policy and enters its configuration context. This policy configures services that run on a device, such as welcome messages, banners, etc. | *page 4-323* |
| *meshpoint* | Creates a meshpoint and enters its configuration mode | *page 4-325* |
| *meshpoint-qos-policy* | Creates a meshpoint *quality of service* (QoS) policy and enters its configuration mode | *page 4-327* |
| *mint-policy* | Creates a MiNT security policy and enters its configuration mode | *page 4-328* |
| *nac-list* | Creates a network ACL and enters its configuration mode | *page 4-329* |
| *no* | Negates a command or sets its default | *page 4-335* |
| *nsight-policy* | Creates an NSight policy and enters its configuration mode | *page 4-339* |
| *passpoint-policy* | Creates a new passpoint policy and enters its configuration mode | *page 4-350* |
| *password-encryption* | Enables password encryption | *page 4-352* |
| *profile* | Creates a device profile and enters its configuration mode | *page 4-353* |
| *radio-qos-policy* | Creates a radio qos policy and enters its configuration mode | *page 4-357* |
| *radius-group* | Creates a RADIUS group and enters its configuration mode | *page 4-358* |
| *radius-server-policy* | Creates a RADIUS server policy and enters its configuration mode | *page 4-359* |
| *radius-user-pool-policy* | Creates a RADIUS user pool policy and enters its configuration mode | *page 4-361* |
| *rename* | Renames and existing *top-level object* (TLO) | *page 4-362* |
| *replace* | Selects an existing device by its MAC address or hostname and replaces it with a new device having a different MAC address | *page 4-364* |
| *rf-domain* | Creates an RF Domain and enters its configuration mode | *page 4-366* |
| *rfs4000* | Adds an RFS4000 to the network | *page 4-404* |
| *rfs6000* | Adds an RFS6000 to the network | *page 4-403* |
| *nx5500* | Adds an NX5500 to the network | *page 4-405* |
| *nx75xx* | Adds an NX75XX to the network | *page 4-406* |
| *nx9000* | Adds a NX9500 or NX9510 to the network | *page 4-407* |
| *roaming-assist-policy* | Configures a roaming assist policy and enters its configuration mode. This policy enables access points to assist wireless clients in making roaming decisions, such as which access point to connect, etc. | *page 4-408* |
| *role-policy* | Creates a role policy and enters its configuration mode | *page 4-410* |
| *route-map* | Creates a dynamic BGP route map and enters its configuration mode | *page 4-411* |
| *routing-policy* | Creates a routing policy and enters its configuration mode | *page 4-412* |
| *rtl-server-policy* | Creates an RTL server policy and enters its configuration mode. The RTL server policy provides the exact location (URL) at which the Euclid server can be reached. | *page 4-413* |
| *schedule-policy* | Creates a schedule policy and enters its configuration mode | *page 4-419* |

**Table 4.1** *Global Config Commands*

| Command | Description | Reference |
|---|---|---|
| *self* | Displays a logged device's configuration context | *page 4-426* |
| *sensor-policy* | Creates a sensor policy and enters its configuration mode | *page 4-427* |
| *smart-rf-policy* | Creates a Smart RF policy and enters its configuration mode | *page 4-436* |
| *t5* | Configures a t5 wireless controller. This command is applicable only on the RFS4000, RFS6000, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, and VX9000 platforms. | *page 4-438* |
| *web-filter-policy* | Creates a Web Filtering policy and enters its configuration mode | *page 4-440* |
| *wips-policy* | Creates a WIPS policy and enters its configuration mode | *page 4-451* |
| *wlan* | Creates a *Wireless Local Area Network* (WLAN) and enters its configuration mode | *page 4-452* |
| *wlan-qos-policy* | Creates a WLAN QoS policy and enters its configuration mode | *page 4-549* |
| *url-filter* | Creates an URL filter and enters its configuration mode. URL filtering is a licensed feature. | *page 4-551* |
| *url-list* | Creates an URL list and enters its configuration mode. | *page 4-565* |
| *vx9000* | Configures a *Virtual WLAN Controller* (V-WLC) in a *virtual machine* (VM) environment | *page 4-571* |

**NOTE:** For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see *COMMON COMMANDS*.

**NOTE:** The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (_) character.

## 4.1.1 aaa-policy

*Global Configuration Commands*

Configures an *Authentication, Accounting, and Authorization* (AAA) policy. Network administrators can use an AAA policy to define access control within the network.

A controller, service platform, or access point can interoperate with external RADIUS and LDAP servers (AAA Servers) to provide an additional user database and authentication resource. Each WLAN can maintain its own unique AAA configuration. Up to six servers can be configured for providing AAA services.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
aaa-policy <AAA-POLICY-NAME>
```

**Parameters**

- `aaa-policy <AAA-POLICY-NAME>`

| | |
|---|---|
| <AAA-POLICY-NAME> | Specify the AAA policy name. If the policy does not exist, it is created. |

**Example**

```
rfs6000-81742D(config)#aaa-policy test
rfs6000-81742D(config-aaa-policy-test)#?
AAA Policy Mode commands:
  accounting            Configure accounting parameters
  attribute             Configure RADIUS attributes in access and accounting
                        requests
  authentication        Configure authentication parameters
  health-check          Configure server health-check parameters
  mac-address-format    Configure the format in which the MAC address must be
                        filled in the Radius-Request frames
  no                    Negate a command or set its defaults
  proxy-attribute       Configure radius attribute behavior when proxying
                        through controller or rf-domain-manager
  server-pooling-mode   Configure the method of selecting a server from the
                        pool of configured AAA servers
  use                   Set setting to use

  clrscr                Clears the display screen
  commit                Commit all changes made in this session
  do                    Run commands from Exec mode
  end                   End current mode and change to EXEC mode
  exit                  End current mode and down to previous mode
  help                  Description of the interactive help system
  revert                Revert changes
  service               Service Commands
  show                  Show running system information
  write                 Write running configuration to memory or terminal

rfs6000-81742D(config-aaa-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing AAA policy |

**NOTE:** For more information on the AAA policy commands, see *Chapter 8, AAA-POLICY*.

## 4.1.2 alias

*Global Configuration Commands*

Configures the following types of aliases: network, VLAN, host, string, network-service, etc.

Aliases are objects having a unique name and content that is determined by the alias type (network, VLAN, and network-service).

A typical large enterprize network consists of multiple sites (RF Domains) having similar configuration parameters with few elements that vary, such as networks or network ranges, hosts having different IP addresses, and VLAN IDs or URLs. These elements can be defined as aliases (object oriented wireless firewalls) and used across sites by applying overrides to the object definition. Using aliases results in a configuration that is easier to understand and maintain.

Multiple instances of an alias (same type and same name) can be defined at any of the following levels: global, RF Domain, profile, or device. An alias defined globally functions as a *top-level-object* (TLO). An alias defined on a device is applicable to that device only. An alias defined on a profile applies to every device using the profile. Similarly, aliases defined at the RF Domain level apply to all devices within that domain.

Aliases defined at any given level can be overridden at any of the next lower levels. For example, a global alias can be redefined on a selected set of RF Domains, profiles, or devices. Overrides applied at the device level take precedence.

The different aliases types supported are:

- address-range alias – Maps a user-friendly name to a range of IP addresses. An address-range alias can be utilized at different deployments. For example, if an ACL defines a pool of network addresses as 192.168.10.10 through 192.168.10.100 for an entire network, and a remote location's network range is 172.16.13.20 through 172.16.13.110, the remote location's ACL can be overridden using an alias. At the remote location, the ACL works with the 172.16.13.20-110 address range. A new ACL need not be created specifically for the remote deployment location.
- host alias – Maps a user-friendly name to a specific host (identified by its IP address. For example, 192.168.10.23). A host alias can be utilized at different deployments. For example, if a central network DNS server is set a static IP address, and a remote location's local DNS server is defined, this host can be overridden at the remote location. At the remote location, the network is functional with a local DNS server, but uses the name set at the central network. A new host need not be created at the remote location. This simplifies creating and managing hosts and allows an administrator to better manage specific local requirements.
- network alias – Maps a user-friendly name to a network. A network alias can be utilized at different deployments. For example, if a central network ACL defines a network as 192.168.10.0/24, and a remote location's network range is 172.16.10.0/24, the ACL can be overridden at the remote location to suit their local (but remote) requirement. At the remote location, the ACL functions with the 172.16.10.0/24 network. A new ACL need not be created specifically for the remote deployment. This simplifies ACL definition and allows an administrator to better manage specific local requirements.
- network-group alias – Maps a user-friendly name to a single or a range of addresses of devices, hosts, and network configurations. Network configurations are complete networks in the form 192.168.10.0/24 or IP address range in the form 192.168.10.10-192.168.10.20.

  A network-group alias can contain a maximum of eight (8) host entries, eight (8) network entries, and eight (8) IP address-range entries. A maximum of 32 network-group alias entries can be created.

A network-group alias can be used in IP firewall rules to substitute hosts, subnets, and IP address ranges.

- network-service alias – Maps a user-friendly name to service protocols and ports. Both source and destination ports are configurable. For each protocol, up to 2 source port ranges and up to 2 destination port ranges can be configured. A maximum of 4 protocol entries can be configured per network-service alias. When used with an ACL, the network-service alias defines the service-specific components of the ACL rule. Overrides can be applied to the service alias, at the device level, without modifying the ACL. Application of overrides to the service alias allows an ACL to be used across sites.

Use a network-service alias to associate more than one IP address to a network interface, providing multiple connections to a network from a single IP node.

- number alias – Maps a user-friendly name to a number
- vlan alias – Maps a user-friendly name to a VLAN ID. A VLAN alias can be used at different deployments. For example, if a named VLAN is defined as 10 for the central network, and the VLAN is set at 26 at a remote location, the VLAN can be overridden at the deployment location with an alias. At the remote deployment location, the network is functional with a VLAN ID of 26, but utilizes the name defined at the centrally managed network. A new VLAN need not be created specifically for the remote deployment.
- string alias – Maps a user-friendly name to a specific string (for example, RF Domain name). A string alias can be utilized at different deployments. For example, if the main domain at a remote location is called *loc1.domain.com* and at another deployment location it is called *loc2.domain.com*, the alias can be overridden at the remote location to suit the local (but remote) requirement. At one remote location, the alias functions with the *loc1.domain.com* domain and at the other with the *loc2.domain.com* domain.
- encrypted-string alias – Maps a user-friendly name to a string value. The string value of this alias is encrypted when "password-encryption" is enabled. Encrypted-string aliases can be used for string configuration parameters that are encrypted by the "password-encryption" feature.
- hashed-string alias – Maps a user-friendly name to a hashed-string value. Hashed-string aliases can be used for string configuration parameters that are hashed, such as passwords.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
alias [address-range|encrypted-string|hashed-string|host|network|network-group|
network-service|number|string|vlan]

alias address-range <ADDRESS-RANGE-ALIAS-NAME> <STARTING-IP> to <ENDING-IP>

alias encrypted-string <ENCRYPTED-STRING-ALIAS-NAME> [0|2] <LINE>

alias hashed-string <HASHED-STRING-ALIAS-NAME> <LINE>

alias host <HOST-ALIAS-NAME> <HOST-IP>

alias network <NETWORK-ALIAS-NAME> <NETWORK-ADDRESS/MASK>

alias network-group <NETWORK-GROUP-ALIAS-NAME> [address-range|host|network]
```

```
alias network-group <NETWORK-GROUP-ALIAS-NAME> [address-range <STARTING-IP> to
<ENDING-IP> {<STARTING-IP> to <ENDING-IP>}|host <HOST-IP> {<HOST-IP>}|network
<NETWORK-ADDRESS/MASK> {<NETWORK-ADDRESS/MASK>}]

alias network-service <NETWORK-SERVICE-ALIAS-NAME> proto [<0-254>|<WORD>|eigrp|
gre|igmp|igp|ospf|vrrp] {(<1-65535>|<WORD>|bgp|dns|ftp|ftp-data|gopher|https|
ldap|nntp|ntp|pop3|proto|sip|smtp|sourceport|ssh|telnet|tftp|www)}

alias network-service <NETWORK-SERVICE-ALIAS-NAME> proto [<0-254>|<WORD>|eigrp|
gre|igmp|igp|ospf|vrrp] {(<1-65535>|<WORD>|bgp|dns|ftp|ftp-data|gopher|https|
ldap|nntp|ntp|pop3|proto|sip|smtp|sourceport [<1-65535>|<WORD>]|ssh|telnet|
tftp|www)}

alias number <NUMBER-ALIAS-NAME> <0-4294967295>

alias string <STRING-ALIAS-NAME> <LINE>

alias vlan <VLAN-ALIAS-NAME> <1-4094>
```

**Parameters**

- `alias address-range <ADDRESS-RANGE-ALIAS-NAME> <STARTING-IP> to <ENDING-IP>`

| | |
|---|---|
| address-range <ADDRESS-RANGE-ALIAS-NAME> | Creates an address-range alias, defining a range of IP addresses<br>• <ADDRESS-RANGE-ALIAS-NAME> – Specify the address-range alias name.<br>Alias name should begin with '$'. |
| <STARTING-IP> to <ENDING-IP> | Associates a range of IP addresses with this address-range alias<br>• <STARTING-IP> – Specify the first IP address in the range.<br>• to <ENDING-IP> – Specify the last IP address in the range. |

- `alias encrypted-string <ENCRYPTED-STRING-ALIAS-NAME> [0|2] <LINE>`

| | |
|---|---|
| encrypted-string <ENCRYPTED-STRING-ALIAS-NAME> | Creates an alias for an encrypted string. Use this alias for string configuration values that are encrypted when "password-encryption" is enabled. For example, in the management-policy, use it to define the SNMP community string. For more information, see *snmp-server*.<br>• <ENCRYPTED-STRING-ALIAS-NAME> – Specify the encrypted-string alias name.<br>Alias name should begin with '$'. |
| [0\|2] <LINE> | Configures the value associated with the alias name specified in the previous step<br>• [0\|2] <LINE> – Configures the alias value<br>Note, if password-encryption is enabled, in the *show > running-config* output, this clear text is displayed as an encrypted string, as shown below:<br>`nx9500-6C8809(config)#show running-config`<br>`!.............................`<br>`alias encrypted-string $enString 2`<br>`fABMK2is7UToNiZE3MQXbgAAAAxB0ZIysdqsEJwr6AH/Da//`<br>`!`<br>`--More--`<br>`nx9500-6C8809`<br>In the above *show > running-config* output, the '2' displayed before the encrypted-string alias value indicates that the displayed text is encrypted and not a clear text.<br>Cotnd.. |

| | |
|---|---|
| | However, if password-encryption is disabled the clear text is displayed as is:<br>`nx9500-6C8809(config)#show running-config`<br>`!.............................`<br>`!`<br>`alias encrypted-string $enString 0 test11223344`<br>`!`<br>`--More--`<br>`nx9500-6C8809`<br>For more information on enabling password-encryption, see *password-encryption*. |

- `alias hashed-string <HASHED-STRING-ALIAS-NAME> <LINE>`

| | |
|---|---|
| hashed-string <HASHED-STRING-ALIAS-NAME> | Creates an alias for a hashed string. Use this alias for configuration values that are hashed strings, such as passwords. For example, in the management-policy, use it to define the privilege mode password. For more information, see .<br>• <HASHED-STRING-ALIAS-NAME> – Specify the hashed-string alias name.<br>Alias name should begin with '$'. |
| <LINE> | Configures the hashed-string value associated with this alias.<br>`nx9500-6C8809(config)#show running-config`<br>`!`<br>`alias encrypted-string $WRITE 2`<br>`sBqVCDAoxs3oByF5PCSuFAAAAAd7HT2+EiT/l/BXm9c4SBDv`<br>`!`<br>`alias hashed-string $PriMode 1`<br>`faffdde27cb49ad634ea20df4f7c8ef2685894d10ffcb1b2efba054112ec`<br>`fc75`<br>`0--More--`<br>`nx9500-6C8809`<br>In the above *show > running-config* output, the '1' displayed before the hashed-string alias value indicates that the displayed text is hashed and not a clear text. |

- `alias host <HOST-ALIAS-NAME> <HOST-IP>`

| | |
|---|---|
| host <HOST-ALIAS-NAME> | Creates a host alias, defining a single network host<br>• <HOST-ALIAS-NAME> – Specify the host alias name.<br>Alias name should begin with '$'. |
| <HOST-IP> | Associates the network host's IP address with this host alias. For example, 'alias host $HOST 1.1.1.100'. In this example, the host alias name is: *$HOST* and the host IP address it is mapped to is: *1.1.1.100*.<br>• <HOST-IP> – Specify the network host's IP address. |

- `alias network <NETWORK-ALIAS-NAME> <NETWORK-ADDRESS/MASK>`

| | |
|---|---|
| network <NETWORK-ALIAS-NAME> | Creates a network alias, defining a single network address<br>• <NETWORK-ALIAS-NAME> – Specify the network alias name.<br>Alias name should begin with '$'. |
| <NETWORK-ADDRESS/MASK> | Associates a single network with this network alias. For example, 'alias network $NET 1.1.1.0/24'. In this example, the network alias name is: *$NET* and the network it is mapped to is: *1.1.1.0/24*.<br>• <NETWORK-ADDRESS/MASK> – Specify the network's address and mask. |

```
• alias network-group <NETWORK-GROUP-ALIAS-NAME> [address-range <STARTING-IP> to
<ENDING-IP> {<STARTING-IP> to <ENDING-IP>}|host <HOST-IP> {<HOST-IP>}|
network <NETWORK-ADDRESS/MASK> {<NETWORK-ADDRESS/MASK>}]
```

| | |
|---|---|
| network <NETWORK-GROUP-ALIAS-NAME> | Creates a network-group alias<br>• <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name.<br>Alias name should begin with '$'.<br>The network-group aliases are used in ACLs, to define the network-specific components. ACLs using aliases can be used across sites by re-defining the network-group alias elements at the device or profile level.<br>After specifying the name, specify the following: a range of IP addresses, host addresses, or a range of network addresses. |
| address-range <STARTING-IP> to <ENDING-IP> {<STARTING-IP> to <ENDING-IP>} | Associates a range of IP addresses with this network-group alias<br>• <STARTING-IP> – Specify the first IP address in the range.<br>• to <ENDING-IP> – Specify the last IP address in the range.<br>• <STARTING-IP> to <ENDING-IP> – Optional. Specifies more than one range of IP addresses. A maximum of eight (8) IP address ranges can be configured. |
| host <HOST-IP> {<HOST-IP>} | Associates a single or multiple hosts with this network-group alias<br>• <HOST-IP> – Specify the hosts' IP address.<br>• <HOST-IP> – Optional. Specifies more than one host. A maximum of eight (8) hosts can be configured. |
| network <NETWORK-ADDRESS/MASK> {<NETWORK-ADDRESS/MASK>} | Associates a single or multiple networks with this network-group alias<br>• <NETWORK-ADDRESS/MASK> – Specify the network's address and mask.<br>• <NETWORK-ADDRESS/MASK> – Optional. Specifies more than one network. A maximum of eight (8) networks can be configured. |

```
• alias network-service <NETWORK-SERVICE-ALIAS-NAME> proto [<0-254>|<WORD>|
eigrp|gre|igmp|igp|ospf|vrrp] {(<1-65535>|<WORD>|bgp|dns|ftp|ftp-data|gopher|
https|ldap|nntp|ntp|pop3|proto|sip|smtp|sourceport [<1-65535>|<WORD>]|ssh|telnet|
tftp|www)}
```

| | |
|---|---|
| alias network-service <NETWORK-SERVICE-ALIAS-NAME> | Configures an alias that specifies available network services and the corresponding source and destination software ports<br>• <NETWORK-SERVICE-ALIAS-NAME> – Specify a network-service alias name.<br>Alias name should begin with '$'.<br>Network-service aliases are used in ACLs, to define the service-specific components. ACLs using aliases can be used across sites by re-defining the network-service alias elements at the device or profile level. |
| proto [<0-254>\|<WORD>\|eigrp\|gre\|igmp\|igp\|ospf\|vrrp] | Use one of the following options to associate an Internet protocol with this network-service alias:<br>• <0-254> – Identifies the protocol by its number. Specify the protocol number from 0 - 254. This is the number by which the protocol is identified in the *Protocol* field of the IPv4 header and the *Next Header* field of IPv6 header. For example, the *User Datagram Protocol's* (UDP) designated number is 17.<br>• <WORD> – Identifies the protocol by its name. Specify the protocol name.<br>• eigrp – Selects *Enhanced Interior Gateway Routing Protocol* (EIGRP). The protocol number 88.<br>Contd.. |

| | |
|---|---|
| | • gre – Selects *Generic Routing Encapsulation* (GRE). The protocol number is 47.<br>• igmp – Selects *Internet Group Management Protocol* (IGMP). The protocol number is 2.<br>• igp – Selects *Interior Gateway Protocol* (IGP). The protocol number is 9.<br>• ospf – Selects *Open Shortest Path First* (OSPF). The protocol number is 89.<br>• vrrp – Selects *Virtual Router Redundancy Protocol* (VRRP). The protocol number is 112. |
| {(<1-65535>\|<WORD>\|bgp\|dns\|ftp\|ftp-data\|gopher\|https\|ldap\|nntp\|ntp\|pop3\|proto\|sip\|smtp\|sourceport [<1-65535>\|<WORD>]\|ssh\|telnet\|tftp\|www)} | After specifying the protocol, you may configure a destination port for this service. These keywords are recursive and you can configure multiple protocols and associate multiple destination and source ports.<br>• <1-65535> – Optional. Configures a destination port number from 1 - 65535<br>• <WORD> – Optional. Identifies the destination port by the service name provided. For example, the *secure shell* (SSH) service uses TCP port 22.<br>• bgp – Optional. Configures the default *Border Gateway Protocol* (BGP) services port (179)<br>• dns – Optional. Configures the default *Domain Name System* (DNS) services port (53)<br>• ftp – Optional. Configures the default *File Transfer Protocol* (FTP) control services port (21)<br>• ftp-data – Optional. Configures the default FTP data services port (20)<br>• gopher – Optional. Configures the default gopher services port (70)<br>• https – Optional. Configures the default HTTPS services port (443)<br>• ldap – Optional. Configures the default *Lightweight Directory Access Protocol* (LDAP) services port (389)<br>• nntp – Optional. Configures the default Newsgroup (NNTP) services port (119)<br>• ntp – Optional. Configures the default *Network Time Protocol* (NTP) services port (123)<br>• POP3 – Optional. Configures the default *Post Office Protocol* (POP3) services port (110)<br>• proto – Optional. Use this option to select another Internet protocol in addition to the one selected in the previous step.<br>• sip – Optional. Configures the default *Session Initiation Protocol* (SIP) services port (5060)<br>• smtp – Optional. Configures the default *Simple Mail Transfer Protocol* (SMTP) services port (25)<br>• sourceport [<1-65535>\|<WORD>] – Optional. After specifying the destination port, you may specify a single or range of source ports.<br>  • <1-65535> – Specify the source port from 1 - 65535.<br>  • <WORD> – Specify the source port range, for example 1-10.<br>• ssh – Optional. Configures the default SSH services port (22)<br>• telnet – Optional. Configures the default Telnet services port (23)<br>• tftp – Optional. Configures the default *Trivial File Transfer Protocol* (TFTP) services port (69) |

- `alias number <NUMBER-ALIAS-NAME> <0-4294967295>`

| | |
|---|---|
| alias number <NUMBER-ALIAS-NAME> <0-4294967295> | Creates a number alias identified by the <NUMBER-ALIAS-NAME> keyword. Number aliases map a name to a numeric value. For example, 'alias number $NUMBER 100'<br>• The number alias name is: $NUMBER<br>• The value assigned is: 100<br>The value referenced by alias $NUMBER, wherever used, is 100.<br>• <NUMBER-ALIAS-NAME> – Specify the number alias name.<br>• <0-4294967295> – Specify the number, from 0 - 4294967295, assigned to the number alias created.<br>Alias name should begin with '$'. |

- `alias string <STRING-ALIAS-NAME> <LINE>`

| | |
|---|---|
| alias string <STRING-ALIAS-NAME> | Creates a string alias identified by the <STRING-ALIAS-NAME> keyword<br>• <STRING-ALIAS-NAME> – Specify the string alias name.<br>• <LINE> – Specify the string value associated with the specified <STRING-ALIAS-NAME> keyword.<br>String aliases map a name to an arbitrary string value. For example, 'alias string $DOMAIN test.example_company.com'.<br>• The string alias name is: $DOMAIN<br>• The value assigned is: test.example_company.com (a domain name)<br>The value referenced by alias $DOMAIN, wherever used, is test.example_company.com.<br>Alias name should begin with '$'.<br>You can also use a string alias to configure the Bonjour Service instance name. Once configured, use the string alias in the Bonjour Gateway Discovery Policy context to specify the Bonjour service instance name to be used as the match criteria. For more information, see *allow-service*. |

- `alias vlan <VLAN-ALIAS-NAME> <1-4094>`

| | |
|---|---|
| alias vlan <VLAN-ALIAS-NAME> | Creates a VLAN alias identified by the <VLAN-ALIAS-NAME> keyword<br>• <VLAN-ALIAS-NAME> – Specify the VLAN alias name.<br>Alias name should begin with '$'. |
| <1-4094> | Maps the VLAN alias to a VLAN ID<br>• <1-4094> – Specify the VLAN ID from 1 - 4094. |

**Example**

```
rfs4000-229D58(config)##alias address-range $AddRanAlias 192.168.13.10 to
192.168.13.13

rfs4000-229D58(config)#alias network $NetworkAlias 192.168.13.0/24

rfs4000-229D58(config)#alias host $HostAlias 192.168.13.100

rfs4000-229D58(config)#alias vlan $VlanAlias 1

rfs4000-229D58(config)#alias address-range $AddRangeAlias 192.168.13.2 to 192.16
8.13.10

rfs4000-229D58(config)#alias network-service $NetServAlias proto igmp
```

```
rfs4000-229D58(config)#show running-config | include alias
alias network-group $NetGrAlias address-range 192.168.13.7 to 192.168.13.9
192.168.13.20 to 192.168.13.25
alias network $NetworkAlias 192.168.13.0/24
alias host $HostAlias 192.168.13.10
alias address-range $AddRangeAlias 192.168.13.2 to 192.168.13.10
alias network-service $NetServAlias proto igmp
alias vlan $VlanAlias 1
rfs4000-229D58(config)#

nx9500-6C8809(config)#alias number $NUMBER 100

nx9500-6C8809(config)#show context include-factory | include alias
alias string $DOMAIN test.examplecompany.com
alias string $DOMAIN2 test.example_company.com
alias number $NUMBER 100
alias string $SN B4C7996C8809
nx9500-6C8809(config)#
```

The following examples show encrypted-string alias configuration:

```
nx9500-6C8809(config)#alias encrypted-string $WRITE 0 private
nx9500-6C8809(config)#alias encrypted-string $READ 0 public

nx9500-6C8809(config)#show context | include alias
alias vlan $BLR-01 1
alias string $IN-Blr-EcoSpace-Floor-4 IBEF4
alias encrypted-string $READ 0 public
alias encrypted-string $WRITE 0 private
nx9500-6C8809(config)#
```

The following example shows the encrypted-string aliases, configured in the previous example, used in the management-policy:

```
nx9500-6C8809(config-management-policy-default)#snmp-server community 0 $WRITE rw
nx9500-6C8809(config-management-policy-default)#snmp-server community 0 $READ ro

nx9500-6C8809(config-management-policy-default)#show context
management-policy default
 no telnet
 no http server
 https server
 rest-server
 ssh
 user admin password 1
ad4d8797f007444ccdda3788b9ee0e8b46f3facb4308e045239eb7771e127ed5 role superuser
access all
 snmp-server community 0 $WRITE rw
 snmp-server community 0 $READ ro
 snmp-server user snmptrap v3 encrypted des auth md5 2 yqr96yyVzmD4ZbU2I7Eh/
QAAAAjWNKa4KXF95pruUCSnhOiT
 snmp-server user snmpmanager v3 encrypted des auth md5 2 NOf8+2+AY2r4ZbU2I7Eh/
QAAAAgc0l8ahJYo3AjHo9wXzYGo
 t5 snmp-server community public ro 192.168.0.1
 t5 snmp-server community private rw 192.168.0.1
nx9500-6C8809(config-management-policy-default)#
```

The following example shows hashed-string alias configuration:

```
nx9500-6C8809(config)#alias hashed-string $PriMode Test12345

nx9500-6C8809(config)#show context | include alias
alias vlan $BLR-01 1
alias string $IN-Blr-EcoSpace-Floor-4 IBEF4
alias encrypted-string $READ 0 public
alias encrypted-string $WRITE 0 private
alias hashed-string $PriMode 1
faffdde27cb49ad634ea20df4f7c8ef2685894d10ffcb1b2efba054112ecfc75
nx9500-6C8809(config)#
```

The following example shows the hashed-string alias, configured in the previous example, used in the management-policy:

```
nx9500-6C8809(config-management-policy-default)#show context
management-policy default
https server
 rest-server
 ssh
 user admin password 1
ad4d8797f007444ccdda3788b9ee0e8b46f3facb4308e045239eb7771e127ed5 role superuser
access all
 snmp-server community 0 $WRITE rw
 snmp-server community 0 $READ ro
 snmp-server user snmptrap v3 encrypted des auth md5 2 yqr96yyVzmD4ZbU2I7Eh/
QAAAAjWNKa4KXF95pruUCSnhOiT
 snmp-server user snmpmanager v3 encrypted des auth md5 2 NOf8+2+AY2r4ZbU2I7Eh/
QAAAAgc0l8ahJYo3AjHo9wXzYGo
 t5 snmp-server community public ro 192.168.0.1
 t5 snmp-server community private rw 192.168.0.1
 privilege-mode-password $PriMode
nx9500-6C8809(config-management-policy-default)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing network, VLAN, service, string, etc. alias |

## 4.1.3 aaa-tacacs-policy

*Global Configuration Commands*

Configures AAA *Terminal Access Controller Access-Control System+* (TACACS) policy. TACACS+ is a protocol created by CISCO Systems which provides access control to network devices such as routers, network access servers and other networked computing devices through one or more centralized servers. TACACS provides separate authentication, authorization, and accounting services running on different servers.

TACACS controls user access to devices and network resources while providing separate accounting, authentication, and authorization services. Some of the services provided by TACACS are:

- Authorizing each command with the TACACS+ server before execution.
- Accounting each session's logon and log off events.
- Authenticating each user with the TACACS+ server before enabling access to network resources.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
aaa-tacacs-policy <AAA-TACACS-POLICY-NAME>
```

**Parameters**

- `aaa-tacacs-policy <AAA-TACACS-POLICY-NAME>`

| | |
|---|---|
| <AAA-TACACS-POLICY-NAME> | Specify the AAA-TACACS policy name. If the policy does not exist, it is created. |

**Example**

```
rfs6000-81742D(config)#aaa-tacacs-policy testpolicy
rfs6000-81742D(config-aaa-tacacs-policy-testpolicy)#?
AAA TACACS Policy Mode commands:
  accounting      Configure accounting parameters
  authentication  Configure authentication parameters
  authorization   Configure authorization parameters
  no              Negate a command or set its defaults

  clrscr          Clears the display screen
  commit          Commit all changes made in this session
  do              Run commands from Exec mode
  end             End current mode and change to EXEC mode
  exit            End current mode and down to previous mode
  help            Description of the interactive help system
  revert          Revert changes
  service         Service Commands
  show            Show running system information
  write           Write running configuration to memory or terminal

rfs6000-81742D(config-aaa-tacacs-policy-testpolicy)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing AAA TACACS policy |

**NOTE:** For more information on the AAA-TACACS policy commands, see *Chapter 25, AAA-TACACS-POLICY*.

## 4.1.4 ap6521

*Global Configuration Commands*

Adds an AP6521 to the network. If a profile for the AP is not available, a new profile is created.

**Supported in the following platforms:**

- Access Point — AP6521
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ap6521 <MAC>
```

**Parameters**

- `ap6521 <MAC>`

| | |
|---|---|
| <MAC> | Specify the AP6521's MAC address. |

**Example**

```
nx9500-6C8809(config)#ap6521 FC-0A-81-42-93-6C
nx9500-6C8809(config-device-FC-0A-81-42-93-6C)#show context
ap6521 FC-0A-81-42-93-6C
 use profile default-ap6521
 use rf-domain default
 hostname ap6521-42936C
nx9500-6C8809(config-device-FC-0A-81-42-93-6C)#

nx9500-6C8809(config)#show wireless ap configured
-------------------------------------------------------------------------------
-------
 IDX       NAME              MAC            PROFILE      RF-DOMAIN      ADOPTED-BY
-------------------------------------------------------------------------------
-------
  1   ap6521-42936C      FC-0A-81-42-93-6C   default-ap6521     default     B4-C7-
99-6C-88-09
-------------------------------------------------------------------------------
-------
nx9500-6C8809(config)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an AP6521 from the network |

## 4.1.5 ap6522

*Global Configuration Commands*

Adds an AP6522 to the network. If a profile for the AP is not available, a new profile is created.

**Supported in the following platforms:**

- Access Point — AP6522
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ap6522 <MAC>
```

**Parameters**

- `ap6522 <MAC>`

| | |
|---|---|
| <MAC> | Specify the AP6522's MAC address. |

**Example**

```
nx9500-6C8809(config)#ap6522 B4-C7-99-58-72-58
nx9500-6C8809(config-device-B4-C7-99-58-72-58)#show context
ap6522 B4-C7-99-58-72-58
 use profile default-ap6522
 use rf-domain default
 hostname ap6522-587258
nx9500-6C8809(config-device-B4-C7-99-58-72-58)#

nx9500-6C8809(config)#show wireless ap configured
-------------------------------------------------------------------------------
-------
 IDX       NAME              MAC            PROFILE      RF-DOMAIN      ADOPTED-BY
-------------------------------------------------------------------------------
-------
 1   ap6521-42936C      FC-0A-81-42-93-6C   default-ap6521     default     B4-C7-
99-6C-88-09
 2  ap6522-587258     B4-C7-99-58-72-58   default-ap6522    default   B4-C7-99-6C-
88-09
-------------------------------------------------------------------------------
-------
nx9500-6C8809(config)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an AP6522 from the network |

## 4.1.6 ap6532

*Global Configuration Commands*

Adds an AP6532 to the network. If a profile for the AP is not available, a new profile is created.

**Supported in the following platforms:**

- Access Point — AP6532
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ap6532 <MAC>
```

**Parameters**

- `ap6532 <MAC>`

| | |
|---|---|
| <MAC> | Specify the AP6532's MAC address. |

**Example**

```
nx9500-6C8809(config)#ap6532 00-23-68-31-16-59
nx9500-6C8809(config-device-B4-C7-99-58-72-58)#show context
ap6532 00-23-68-31-16-59
 use profile default-ap6532
 use rf-domain default
 hostname ap6532-311659
nx9500-6C8809(config-device-00-23-68-31-16-59)#

nx9500-6C8809(config)#show wireless ap configured
-------------------------------------------------------------------------------
-------
 IDX       NAME              MAC            PROFILE      RF-DOMAIN       ADOPTED-BY
-------------------------------------------------------------------------------
-------
  1   ap6521-42936C      FC-0A-81-42-93-6C   default-ap6521     default     B4-C7-
99-6C-88-09
2  ap6522-587258     B4-C7-99-58-72-58   default-ap6522    default   B4-C7-99-6C-
88-09
 3  ap6532-311659     00-23-68-31-16-59   default-ap6532    default   B4-C7-99-6C-
88-09
-------------------------------------------------------------------------------
-------
nx9500-6C8809(config)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an AP6532 from the network |

## 4.1.7 ap6562

*Global Configuration Commands*

Adds an AP6562 to the network. If a profile for the AP is not available, a new profile is created.

**Supported in the following platforms:**

- Access Point — AP6562
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ap6562 <MAC>
```

**Parameters**

- `ap6562 <MAC>`

| | |
|---|---|
| <MAC> | Specify the AP6562's MAC address. |

**Example**

```
nx9500-6C8809(config)#ap6562 00-23-09-0E-12-60
nx9500-6C8809(config-device-00-23-09-0E-12-60)#show context
ap6562 00-23-09-0E-12-60
 use profile default-ap6562
 use rf-domain default
 hostname ap6562-0E1260
nx9500-6C8809(config-device-00-23-09-0E-12-60)#

nx9500-6C8809(config)#show wireless ap configured
-------------------------------------------------------------------------------
-------
 IDX       NAME              MAC            PROFILE      RF-DOMAIN      ADOPTED-BY
-------------------------------------------------------------------------------
-------
  1  ap6521-42936C      FC-0A-81-42-93-6C   default-ap6521     default     B4-C7-
99-6C-88-09
2  ap6522-587258     B4-C7-99-58-72-58   default-ap6522    default   B4-C7-99-6C-
88-09
 3  ap6532-311659     00-23-68-31-16-59   default-ap6532    default   B4-C7-99-6C-
88-09
 4  ap6562-0E1260     00-23-09-0E-12-60   default-ap6562     default    B4-C7-99-
6C-88-09
-------------------------------------------------------------------------------
-------
nx9500-6C8809(config)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an AP6562 from the network |

## 4.1.8 ap71xx

*Global Configuration Commands*

Adds an AP7161 series to the network. If a profile for the AP is not available, a new profile is created.

**Supported in the following platforms:**

- Access Point — AP7161
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ap71xx <MAC>
```

**Parameters**

- `ap71xx <MAC>`

| | |
|---|---|
| <MAC> | Specify the AP7161's MAC address. |

**Example**

```
nx9500-6C8809(config)#ap71xx 00-23-68-11-E6-C4
nx9500-6C8809(config-device-00-23-68-11-E6-C4)#show context
ap71xx 00-23-68-11-E6-C4
 use profile default-ap71xx
 use rf-domain TechPubs
 hostname ap71xx-11E6C4
 no staging-config-learnt
 ip default-gateway 192.168.13.2
 interface vlan1
  ip address 192.168.13.23/24
 use auto-provisioning-policy TecPubs
 no auto-learn staging-config
 adopter-auto-provisioning-policy-lookup evaluate-always
nx9500-6C8809(config-device-00-23-68-11-E6-C4)#

nx9500-6C8809(config)#show wireless ap configured
-------------------------------------------------------------------------------
-------
 IDX      NAME              MAC             PROFILE      RF-DOMAIN       ADOPTED-BY
-------------------------------------------------------------------------------
-------
 1    ap71xx-11E6C4    00-23-68-11-E6-C4    default-ap71xx    TechPubs    un-adopted
 2    ap7532-80C2AC    84-24-8D-80-C2-AC    default-ap7532    TechPubs    B4-C7-99-
6C-88-09
 3    ap7131-9C63D4    00-23-68-9C-63-D4    default-ap71xx    default     un-adopted
 4    t5-ED7C6C        B4-C7-99-ED-7C-6C    default-t5        TechPubs    B4-C7-99-
6C-88-09
 5    rfs4000-880DA7   00-23-68-88-0D-A7    default-rfs4000   TechPubs    B4-C7-99-
6C-88-09
 6    ap7131-99BB7C    00-23-68-99-BB-7C    default-ap71xx    TechPubs    B4-C7-99-
6C-88-09
-------------------------------------------------------------------------------
-------
nx9500-6C8809(config)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an AP7161 from the network |

## 4.1.9 ap7502

*Global Configuration Commands*

Adds an AP7502 series to the network. If a profile for the AP is not available, a new profile is created.

**Supported in the following platforms:**

- Access Point — AP7502
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ap7502 <MAC>
```

**Parameters**

- `ap7502 <MAC>`

| | |
|---|---|
| <MAC> | Specify the AP7502's MAC address. |

**Example**

```
rfs6000-81742D(config)#ap7502 00-23-68-99-BF-A8
rfs6000-81742D(config-device-00-23-68-99-BF-A8)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an AP7502 from the network |

## 4.1.10 ap7522

*Global Configuration Commands*

Adds an AP7522 series to the network. If a profile for the AP is not available, a new profile is created.

**Supported in the following platforms:**

- Access Point – AP7522
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ap7522 <MAC>
```

**Parameters**

- `ap7522 <MAC>`

| | |
|---|---|
| <MAC> | Specify the AP7522's MAC address. |

**Example**

```
rfs6000-81742D(config)#ap7522 00-23-09-0E-12-63
rfs6000-81742D(config-device-00-23-09-0E-12-63)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an AP7522 from the network |

## 4.1.11 ap7532

*Global Configuration Commands*

Adds an AP7532 series to the network. If a profile for the AP is not available, a new profile is created.

**Supported in the following platforms:**

- Access Point — AP7532
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ap7532 <MAC>
```

**Parameters**

- `ap7532 <MAC>`

| | |
|---|---|
| <MAC> | Specify the AP7532's MAC address. |

**Example**

```
rfs6000-81742D(config)#ap7532 00-23-09-0E-12-71
rfs6000-81742D(config-device-00-23-09-0E-12-71)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an AP7532 from the network |

## 4.1.12 ap7562

*Global Configuration Commands*

Adds an AP7562 series to the network. If a profile for the AP is not available, a new profile is created.

**Supported in the following platforms:**

- Access Point — AP7562
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ap7562 <MAC>
```

**Parameters**

- `ap7562 <MAC>`

| | |
|---|---|
| <MAC> | Specify the AP7562's MAC address. |

**Example**

```
rfs6000-81742D(config)#ap7562 84-24-8D-80-C2-AC
rfs6000-81742D(config-device-84-24-8D-80-C2-AC)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an AP7562 from the network |

## 4.1.13 ap7602

*Global Configuration Commands*

Adds an AP7602 series to the network. If a profile for the AP is not available, a new profile is created.

**Supported in the following platforms:**

- Access Point — AP7602
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ap7602 <MAC>
```

**Parameters**

- `ap7602 <MAC>`

| | |
|---|---|
| <MAC> | Specify the AP7602's MAC address. |

**Example**

```
nx9500-6C8809(config)#ap7602 11-2C-3b-01-aa-23
nx9500-6C8809(config-device-11-2C-3B-01-AA-23)#show context
ap7602 11-2C-3B-01-AA-23
 use profile default-ap7602
 use rf-domain default
 hostname ap7602-01AA23
nx9500-6C8809(config-device-11-2C-3B-01-AA-23)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an AP7602 from the network |

## 4.1.14 ap7612

*Global Configuration Commands*

Adds an AP7612 series to the network. If a profile for the AP is not available, a new profile is created.

**Supported in the following platforms:**

- Access Point — AP7612
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ap7612 <MAC>
```

**Parameters**

- `ap7612 <MAC>`

| | |
|---|---|
| <MAC> | Specify the AP7612's MAC address. |

**Example**

```
nx9500-6C8809(config)#ap7612 10-1c-AB-11-0E-20
nx9500-6C8809(config-device-10-1c-AB-11-0E-20)#show context
ap7612 10-1C-AB-11-0E-20
 use profile default-ap7612
 use rf-domain default
 hostname ap7612-110E20
nx9500-6C8809(config-device-10-1c-AB-11-0E-20)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an AP7612 from the network |

## 4.1.15 ap7622

*Global Configuration Commands*

Adds an AP7622 series to the network. If a profile for the AP is not available, a new profile is created.

**Supported in the following platforms:**

- Access Point — AP7622
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ap7622 <MAC>
```

**Parameters**

- `ap7622 <MAC>`

| | |
|---|---|
| <MAC> | Specify the AP7622's MAC address. |

**Example**

```
nx9500-6C8809(config-device-01-11-CD-21-0B-13)#show con
ap7622 01-11-CD-21-0B-13
 use profile default-ap7622
 use rf-domain default
 hostname ap7622-210B13
nx9500-6C8809(config-device-01-11-CD-21-0B-13)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an AP7622 from the network |

## 4.1.16 ap7632

*Global Configuration Commands*

Adds an AP7632 series to the network. If a profile for the AP is not available, a new profile is created.

**Supported in the following platforms:**

- Access Point — AP7632
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ap7632 <MAC>
```

**Parameters**

- `ap7632 <MAC>`

| | |
|---|---|
| <MAC> | Specify the AP7632's MAC address. |

**Example**

```
nx9500-6C8809(config)#ap7632 23-12-A1-F0-12-02
nx9500-6C8809(config-device-23-12-A1-F0-12-02)#show context
ap7632 23-12-A1-F0-12-02
 use profile default-ap7632
 use rf-domain default
 hostname ap7632-F01202
nx9500-6C8809(config-device-23-12-A1-F0-12-02)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an AP7632 from the network |

## 4.1.17 ap7662

*Global Configuration Commands*

Adds an AP7662 series to the network. If a profile for the AP is not available, a new profile is created.

**Supported in the following platforms:**

- Access Point — AP7662
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ap7662 <MAC>
```

**Parameters**

- `ap7662 <MAC>`

| | |
|---|---|
| <MAC> | Specify the AP7662's MAC address. |

**Example**

```
nx9500-6C8809(config)#ap7662 20-12-bd-4C-31-5F
nx9500-6C8809(config-device-20-12-BD-4C-31-5F)#show context
ap7662 20-12-BD-4C-31-5F
 use profile default-ap7662
 use rf-domain default
 hostname ap7662-4C315F
nx9500-6C8809(config-device-20-12-BD-4C-31-5F)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an AP7662 from the network |

## 4.1.18 ap81xx

*Global Configuration Commands*

Adds an AP81XX series to the network. If a profile for the AP is not available, a new profile is created.

**Supported in the following platforms:**

- Access Point — AP81XX
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ap81xx <MAC>
```

**Parameters**

- `ap81xx <MAC>`

| | |
|---|---|
| <MAC> | Specify the AP81XX's MAC address. |

**Example**

```
rfs6000-81742D#ap81xx B4-C7-99-71-17-28
rfs6000-81742D(config-device-B4-C7-99-71-17-28)#show context
ap8132 B4-C7-99-71-17-28
 use profile default-ap81xx
 use rf-domain default
 hostname ap8132-711728
 license AAP DEFAULT-LICENSE
rfs6000-81742D(config-device-B4-C7-99-71-17-28)#

rfs6000-81742D(config)#show wireless ap configured
-------------------------------------------------------------------------------
-------
 IDX       NAME             MAC             PROFILE       RF-DOMAIN       ADOPTED-BY
-------------------------------------------------------------------------------
-------
  1   ap8132-711728   B4-C7-99-71-17-28   default-ap81xx   default     00-15-70-
81-74-2D
-------------------------------------------------------------------------------
-------
rfs6000-81742D(config)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an AP81XX from the network |

## 4.1.19 ap82xx

*Global Configuration Commands*

Adds an AP82XX series to the network. If a profile for the AP is not available, a new profile is created.

**Supported in the following platforms:**

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ap82xx <MAC>
```

**Parameters**

- `ap82xx <MAC>`

| | |
|---|---|
| <MAC> | Specify the AP82XX's MAC address. |

**Example**

```
rfs6000-81742D(config-device-00-23-68-14-77-48)
rfs6000-81742D(config-device-00-23-68-14-77-48)#show context
ap82xx 00-23-68-14-77-48
 use profile default-ap82xx
 use rf-domain default
 hostname ap8232-147748
rfs6000-81742D(config-device-00-23-68-14-77-48)#

rfs6000-81742D(config)#show wireless ap configured
-------------------------------------------------------------------------------
-------
IDX        NAME              MAC             PROFILE       RF-DOMAIN    ADOPTED-BY
-------------------------------------------------------------------------------
-------
1 ap6511-08456A      5C-0E-8B-08-45-6A   default-ap6511    default     un-adopted
2 ap8232-147748      00-23-68-14-77-48   default-ap82xx    default     un-adopted
-------------------------------------------------------------------------------
-------
rfs6000-81742D(config)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an AP82XX from the network |

## 4.1.20 ap8432

*Global Configuration Commands*

Adds an AP8432 series to the network. If a profile for the AP is not available, a new profile is created.

**Supported in the following platforms:**

- Access Point — AP8432
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ap8432 <MAC>
```

**Parameters**

- `ap8432 <MAC>`

| | |
|---|---|
| <MAC> | Specify the AP8432's MAC address. |

**Example**

```
nx9500-6C8809(config)#ap8432 84-24-8D-80-C2-AC
nx9500-6C8809(config-device-84-24-8D-80-C2-AC)#show context
ap8432 84-24-8D-80-C2-AC
 use profile default-ap8432
 use rf-domain default
 hostname ap8432-80C2AC
nx9500-6C8809(config-device-84-24-8D-80-C2-AC)#

nx9500-6C8809(config)#show wireless ap configured
-------------------------------------------------------------------------------
-------
IDX        NAME              MAC             PROFILE      RF-DOMAIN    ADOPTED-BY
-------------------------------------------------------------------------------
-------
 1   ap8432-80C2AC      84-24-8D-80-C2-AC   default-ap8432   default     un-adopted
-------------------------------------------------------------------------------
-------
nx9500-6C8809(config)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an AP8432 from the network |

## 4.1.21 ap8533

*Global Configuration Commands*

Adds an AP8533 series to the network. If a profile for the AP is not available, a new profile is created.

- Access Point — AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ap8533 <MAC>
```

**Parameters**

- `ap8533 <MAC>`

| | |
|---|---|
| <MAC> | Specify the AP8533's MAC address. |

**Example**

```
nx9500-6C8809(config)#ap8533 B4-C7-99-74-B4-5C)
nx9500-6C8809(config-device-B4-C7-99-74-B4-5C)#show context
ap8533 B4-C7-99-74-B4-5C
 use profile default-ap8533
 use rf-domain default
 hostname ap8533-74B45C
nx9500-6C8809(config-device-B4-C7-99-74-B4-5C)#

nx9500-6C8809(config)#show wireless ap configured
-------------------------------------------------------------------------------
-------
IDX        NAME              MAC             PROFILE       RF-DOMAIN    ADOPTED-BY
-------------------------------------------------------------------------------
-------
 1   ap8533-74B45C      B4-C7-99-74-B4-5C   default-ap8533   default     un-adopted
-------------------------------------------------------------------------------
-------
nx9500-6C8809(config)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an AP8533 from the network |

## 4.1.22 application

*Global Configuration Commands*

The following table lists the commands that enable you to enter the Application definition configuration mode:

**Table 4.2** *Application-Policy Config Command*

| Command | Description | Reference |
|---|---|---|
| *application* | Creates a new application definition and enters its configuration mode. This command allows you to create a customized application detection definition. | *page 4-41* |
| *application-config-mode commands* | Summarizes application definition configuration mode commands | *page 4-42* |

### 4.1.22.1 application

*application*

Creates a new application definition and enters its configuration mode

**Supported in the following platforms:**

- Access Points — AP7522, AP7532
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
application <APPLICATION-NAME>
```

**Parameters**

- `application <APPLICATION-NAME>`

| | |
|---|---|
| application <APPLICATION-NAME> | Creates a new application definition and enters its configuration mode<br>• <APPLICATION-NAME> – Specify a name of the new application definition. It is created if not already existing in the system. |

**Example**

```
nx9500-6C8809(config)#application Bing
nx9500-6C8809(config-application-Bing)#?
Application Mode commands:
  app-category  Set application category (default is custom)
  description   Add application description
  https         Secure HTTP
  no            Negate a command or set its defaults
  use           Set setting to use

  clrscr        Clears the display screen
  commit        Commit all changes made in this session
  do            Run commands from Exec mode
  end           End current mode and change to EXEC mode
  exit          End current mode and down to previous mode
  help          Description of the interactive help system
  revert        Revert changes
  service       Service Commands
  show          Show running system information
  write         Write running configuration to memory or terminal

nx9500-6C8809(config-application-Bing)#
```

**Related Commands**

| | |
|---|---|
| *no* | Deletes an existing application definition |

### 4.1.22.2 application-config-mode commands

- *application*

The following table summarizes Application definition configuration mode commands:

**Table 4.3** *Application- Config-Mode Commands*

| Command | Description | Reference |
|---|---|---|
| *app-category* | Configures the category for this application definition | *page 4-43* |
| *description* | Configures a description for this application definition | *page 4-44* |
| *https* | Configures the HTTPS common-name attribute value for this application category's server certificate. Applicable only to applications using HTTPS protocol. | *page 4-45* |
| *use* | Associates a network-service alias or a URL list with this application definition. Applicable for applications using protocols other than HTTPS. | *page 4-46* |
| *no* | Removes or resets this application definition's configured settings | *page 4-47* |

#### 4.1.22.2.1 app-category

*application-config-mode commands*

Configures the category for this application definition

**Supported in the following platforms:**

- Access Points — AP7522, AP7532
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
app-category <APP-CATEGORY-NAME>
```

**Parameters**

- `app-category <APP-CATEGORY-NAME>`

| | |
|---|---|
| app-category <APP-CATEGORY-NAME> | Select the category best suited for this application definition. There are twenty three categories. These are: business, conference, custom, database, filetransfer, gaming, generic, im, mail, mobile, network\ management, other, p2p, remote_control, social\ networking, standard, streaming, tunnel, video, voip, and Web.<br>The default setting is custom. Use this option to categorize your internal custom applications, so that they do not appear as unknown traffic. |

**Example**

```
nx9500-6C8809(config-application-Bing)#app-category [TAB]
business              conference           custom
database              filetransfer         gaming
generic               im                   mail
mobile                network\ management  other
p2p                   remote_control       sharehosting
social\ networking    streaming            tunnel
voip                  web

nx9500-6C8809(config-application-Bing)#

nx9500-6C8809(config-application-Bing)#app-category streaming

nx9500-6C8809(config-application-Bing)#show context
application Bing
 app-category streaming
nx9500-6C8809(config-application-Bing)#
```

**Related Commands**

| | |
|---|---|
| *no* | Resets application category to default (custom) |

### 4.1.22.2.2 description

*application-config-mode commands*

Configures a description for this application definition

**Supported in the following platforms:**

- Access Points — AP7522, AP7532
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
description <WORD>
```

**Parameters**

- `description <WORD>`

| | |
|---|---|
| description <WORD> | Configures a description for this application<br>• <WORD> – Specify a description not exceeding 80 characters in length. Enter the descriptive text within double quotes. |

**Example**

```
nx9500-6C8809(config-application-Bing)#description "Bing is Microsoft's Web search
engine"

nx9500-6C8809(config-application-Bing)#show context
application Bing
 description "Bing is Microsoft's Web search engine"
 app-category streaming
nx9500-6C8809(config-application-Bing)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes this description configured for this application |

### 4.1.22.2.3 https

*application-config-mode commands*

Configures the HTTPS parameter type, attribute type, match criteria for the HTTPS server name and 64 character maximum server name attribute used in the HTTPS server message exchange

**Supported in the following platforms:**

- Access Points — AP7522, AP7532
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
https server-cert common-name [contains|ends-with] <WORD>
```

**Parameters**

- `https server-cert common-name [contains|ends-with] <WORD>`

| | |
|---|---|
| https server-cert | Configures the HTTPS parameter type as server certificate |
| common-name [contains\|ends-with] <WORD> | Configures the HTTPS attribute match criteria as common name. This is the only option applicable when the HTTPS parameter type is set to server-cert. Use one of the following options to provide the common-name attribute value used as the match criteria:<br>• contains – Filters applications having common-name attributes containing the string specified here<br>• ends-with – Filters applications ending with the string specified here<br>  • <WORD> – Specify the string to match (should not exceed 64 characters). |

**Example**

```
nx9500-6C8809(config-application-Bing)#https server-cert common-name exact
bing.com

nx9500-6C8809(config-application-Bing)#show context
application Bing
 description "Bing is Microsoft's web search engine"
 app-category streaming
 https server-cert common-name exact bing.com
nx9500-6C8809(config-application-Bing)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the HTTPS common-name attribute value configured with this application category |

#### 4.1.22.2.4 use

*application-config-mode commands*

Associates a network-service alias or a URL list with this application definition

For applications using protocols other than HTTPS, use this command to define the protocols, ports, and/or URL host name to match.

**Supported in the following platforms:**

- Access Points — AP7522, AP7532
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
use [network-service <NETWORK-SERVICE-ALIAS-NAME>|url-list <URL-LIST-NAME>]
```

**Parameters**

- `use [network-service <NETWORK-SERVICE-ALIAS-NAME>|url-list <URL-LIST-NAME>]`

| | |
|---|---|
| use | Configures this application definition to use a network-service alias or a URL list |
| network-service <NETWORK-SERVICE-ALIAS-NAME> | Associates a network-service alias with this application definition<br>• <NETWORK-SERVICE-ALIAS-NAME> – Specify the network-service alias name (should be existing and configured). The network-service alias should specify the protocols and ports to match. |
| url-list <URL-LIST-NAME> | Associates a URL list with this application definition. URL lists are utilized for whitelisting and blacklisting Web application URLs from being launched and consuming bandwidth within the WiNG managed network.<br>• <URL-LIST-NAME> – Specify the URL list name (should be existing and configured). The URL list should specify the HTTP URL host names to match. |

**Example**

```
nx9500-6C8809(config-application-Bing)#use url-list Bing

nx9500-6C8809(config-application-Bing)#show context
application Bing
 description "Bing is Microsoft's web search engine"
 app-category streaming
 use url-list Bing
 https server-cert common-name exact bing.com
nx9500-6C8809(config-application-Bing)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the network-service alias or the URL list associated with this application definition |

#### 4.1.22.2.5 no

*application-config-mode commands*

Removes or resets this application definition's configured settings

**Supported in the following platforms:**

- Access Points — AP7522, AP7532
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
no [app-category|description|https|use]

no [app-category|description]

no https server-cert common-name [contains|ends-with] <WORD>

no use [network-service <NETWORK-SERVICE-ALIAS-NAME>|url-list <URL-LIST-NAME>]
```

**Parameters**

- no <PARAMETERS>

| | |
|---|---|
| no <PARAMETERS> | Removes or resets this application definition's configured settings based on the parameters passed |

**Example**

The following example displays the application definition 'Bing' parameters before the 'no' commands are executed:

```
nx9500-6C8809(config-application-Bing)#show context
application Bing
 description "Bing is Microsoft's web search engine"
 app-category streaming
 use url-list Bing
 https server-cert common-name exact bing.com
nx9500-6C8809config-application-Bing)#

nx9500-6C8809(config-application-Bing)#no description
nx9500-6C8809(config-application-Bing)#no https server-cert common-name exact
bing.com
```

The following example displays the application definition 'Bing' parameters after the 'no' commands are executed:

```
nx9500-6C8809(config-application-Bing)#show context
application Bing
 app-category streaming
 use url-list Bing
nx9500-6C8809(config-application-Bing)#
```

## 4.1.23 application-group

*Global Configuration Commands*

The following table lists the commands that enable you to create a new application group and enter its configuration mode:

**Table 4.4** *Application-Group Config Command*

| Command | Description | Reference |
|---|---|---|
| *application-group* | Creates a new application group and enters its configuration mode | *page 4-49* |
| *application-group-mode commands* | Summarizes application group configuration mode commands | *page 4-50* |

### 4.1.23.1 application-group

*application-group*

An application group is a collection of system-provided and/or user-defined applications. It is a subset of the total number of supported applications. There are a total of 299 system-provided applications.

**Supported in the following platforms:**

- Access Points — AP7522, AP7532
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
application-group <APPLICATION-GROUP-NAME>
```

**Parameters**

- `application-group <APPLICATION-GROUP-NAME>`

| | |
|---|---|
| application-group <APPLICATION-GROUP-NAME> | Creates an application group and enters its configuration mode<br>• <APPLICATION-GROUP-NAME – Specify the application group name. If an application group with the specified name does not exist, it is created. The name should not exceed 32 characters in length. |

**Example**

```
nx9500-6C8809(config)#application-group amazon
nx9500-6C8809(config-app-group-amazon)#?
Application Group Mode commands:
  application  Add application to group
  description  Add application-group description
  no           Negate a command or set its defaults

  clrscr       Clears the display screen
  commit       Commit all changes made in this session
  do           Run commands from Exec mode
  end          End current mode and change to EXEC mode
  exit         End current mode and down to previous mode
  help         Description of the interactive help system
  revert       Revert changes
  service      Service Commands
  show         Show running system information
  write        Write running configuration to memory or terminal

nx9500-6C8809(config-app-group-amazon)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing application group |

### 4.1.23.2 application-group-mode commands

*application-group*

The following table summarizes the application group configuration mode commands:

**Table 4.5** *Application-Group-Config-Mode Commands*

| Command | Description | Reference |
|---|---|---|
| *application* | Adds an application to this application group | *page 4-51* |
| *description* | Configures a description for this application group | *page 4-53* |
| *no* | Removes this application group's configured parameters (application and/or description) | *page 4-54* |

### 4.1.23.2.1 application

*application-group-mode commands*

Adds an application to this application group. You can add a system-provided or user-defined application.

**Supported in the following platforms:**

- Access Points — AP7522, AP7532
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
application <APPLICATION-NAME>
```

**Parameters**

- `application <APPLICATION-NAME>`

| | |
|---|---|
| application <APPLICATION-NAME> | Configures the application to be added to this application group<br>• <APPLICATION-NAME> – Provide the application name (should be available as an option in the system). A maximum of eight (8) applications can be added to a group.<br>If the desired application is not available as an option, use the *application* command to add it. |

**Example**

To view all applications available in the system, use [TAB], as shown in the following example:

```
nx9500-6C8809(config-app-group-test)#application [TAB]
Display all 299 possibilities? (y or n)
1-clickshare-com                1-upload-com
1-upload-to                     10upload-com

--More--
nx9500-6C8809(config-app-group-test)#
```

Select the desired application from the list displayed, as shown in the following examples:

```
nx9500-6C8809(config-app-group-amazon)#application amazon [TAB]
amazon-prime-music  amazon-prime-video  amazon_cloud  amazon_shop
nx9500-6C8809(config-app-group-amazon)#

nx9500-6C8809(config-app-group-amazon)#application amazon-prime-music
nx9500-6C8809(config-app-group-amazon)#application amazon-prime-video
nx9500-6C8809(config-app-group-amazon)#application amazon_cloud
nx9500-6C8809(config-app-group-amazon)#application amazon_shop

nx9500-6C8809(config-app-group-amazon)#show context
application-group amazon
 application amazon-prime-music
 application amazon-prime-video
 application amazon_cloud
 application amazon_shop
nx9500-6C8809(config-app-group-amazon)#
```

Note, the system returns an error message if the application entered is not listed, as shown in the following example:

```
nx9500-6C8809(config-app-group-test)#application bing
% Error: application 'bing' is not defined
nx9500-6C8809(config-app-group-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes a specified application from this application group |

### 4.1.23.2.2 description

*application-group-mode commands*

Configures a description for this application group

**Supported in the following platforms:**

- Access Points — AP7522, AP7532
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
description <WORD>
```

**Parameters**

- `description <WORD>`

| | |
|---|---|
| description <WORD> | Configures a description for this application group that uniquely differentiates it from other existing application groups<br>• <WORD> – Provide a description not exceeding 80 characters in length. |

**Example**

```
nx9500-6C8809(config-app-group-amazon)#description "This application-group lists
 all Amazon applications."

nx9500-6C8809(config-app-group-amazon)#show context
application-group amazon
 description "This application-group lists all Amazon applications."
 application amazon-prime-music
 application amazon-prime-video
 application amazon_cloud
 application amazon_shop
nx9500-6C8809(config-app-group-amazon)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the description configured for this application group |

#### 4.1.23.2.3 no

*application-group-mode commands*

Removes this application group's configured parameters (application and/or description)

**Supported in the following platforms:**

- Access Points — AP7522, AP7532
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
no [application <APPLICATION-NAME>|description]
```

**Parameters**

- `no [application <APPLICATION-NAME>|description]`

| | |
|---|---|
| no <PARAMETERS> | Removes an application associated with this group, and removes this group's description |

**Example**

The following example displays the application-group 'amazon' configuration before the execution of 'no' commands:

```
nx9500-6C8809(config-app-group-amazon)#show context
application-group amazon
 description "This application-group lists all Amazon applications."
 application amazon-prime-music
 application amazon-prime-video
 application amazon_cloud
 application amazon_shop
nx9500-6C8809(config-app-group-amazon)#

nx9500-6C8809(config-app-group-amazon)#no application amazon_cloud
nx9500-6C8809(config-app-group-amazon)#no description
```

The following example displays the application-group 'amazon' configuration after the execution of 'no' commands:

```
nx9500-6C8809(config-app-group-amazon)#show context
application-group amazon
 application amazon-prime-music
 application amazon-prime-video
 application amazon_shop
nx9500-6C8809(config-app-group-amazon)#
```

## 4.1.24 application-policy

*Global Configuration Commands*

The following table lists the commands that enable you to enter the Application policy configuration mode:

**Table 4.6** *Application-Policy Config Command*

| Command | Description | Reference |
|---|---|---|
| *application-policy* | Creates an application policy and enters its configuration mode | *page 4-56* |
| *application-policy-mode commands* | Summarizes the application policy configuration mode commands | *page 4-58* |

### 4.1.24.1 application-policy

*application-policy*

When an application is recognized and classified by the WiNG application recognition engine, administrator defined actions can be applied to that specific application. An application policy defines the rules or actions executed on recognized applications (for example, Facebook) or application-categories (for example, social-networking). The following are the rules/actions that can be applied in an application policy:

- *Allow* - Allow packets for a specific application or application category
- *Deny* - Deny packets for a a specific application or application category
- *Mark* - Mark packets with DSCP/8021p value for a specific application or application category
- *Rate-limit* - Rate limit packets from specific application types.

For each rule defined, a precedence is assigned to resolve conflicting rules for applications and categories. A *deny* rule is exclusive, as no other action can be combined with a deny. An *allow* rule is redundant with other actions, since the default action is allow. An allow rule is useful when wanting to deny packets for a category, but wanting to allow a few applications in the same category to proceed. In such a cases, add an allow rule for applications with a higher precedence then a deny rule for that category.

*Mark* actions mark packets for a recognized application and category with DSCP/8021p values used for QoS. *Rate-limits* create a rate-limiter applied to packets recognized for an application and category. Ingress and egress rates need to be specified for the rate-limiter, but both are not required. Mark and rate-limit are the only two actions that can be combined for an application and category. All other combinations are invalid.

Once created and configured, apply the application policy at the following levels within the network to enforce application assurance:

- RADIUS CoA usage – In the device/profile configuration mode, use the *application-policy > radius > <APPLICATION-POLICY-NAME>* command to apply the policy to every user successfully authenticated by the RADIUS server.
- User role – In the role-policy-user-role configuration mode, use the *use > application-policy <APPLICATION-POLICY-NAME>* command to apply the policy to all users assigned to the role.
- WLAN – In the WLAN configuration mode, use the *use > application-policy <APPLICATION-POLICY-NAME>* command to apply the policy to all users accessing the WLAN.
- Bridge VLAN – In the bridge VLAN configuration mode, use the *use > application-policy <APPLICATION-POLICY-NAME>* command to apply the policy for the traffic corresponding to the bridged VLAN.

**Supported in the following platforms:**

- Access Points — AP7522, AP7532
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
application-policy <APPLICATION-POLICY-NAME>
```

**Parameters**

- `application-policy <APPLICATION-POLICY-NAME>`

| | |
|---|---|
| application-policy <APPLICATION-POLICY-NAME> | Specify the application policy name. If an application policy with the specified name does not exist, it is created. The name should not exceed 32 characters in length. |

**Example**

```
nx9500-6C8809(config)#application-policy TestAppliPolicy
nx9500-6C8809(config-app-policy-TestAppliPolicy)#?
Application Policy Mode commands:
  allow              Allow packets
  deny               Deny packets
  description        Application policy description
  enforcement-time   Configure policy enforcement based on time
  logging            Application recognition logging
  mark               Mark packets
  no                 Negate a command or set its defaults
  rate-limit         Rate-limit packets

  clrscr             Clears the display screen
  commit             Commit all changes made in this session
  do                 Run commands from Exec mode
  end                End current mode and change to EXEC mode
  exit               End current mode and down to previous mode
  help               Description of the interactive help system
  revert             Revert changes
  service            Service Commands
  show               Show running system information
  write              Write running configuration to memory or terminal

nx9500-6C8809(config-app-policy-TestAppliPolicy)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing application policy |

### 4.1.24.2 application-policy-mode commands

*application-policy*

The following table summarizes Application policy configuration mode commands:

**Table 4.7** *Application- Policy-Mode Commands*

| Command | Description | Reference |
|---|---|---|
| *allow* | Creates an allow rule and configures the match criteria based on which packets are filtered and the allow access action applied | *page 4-59* |
| *deny* | Creates a deny rule and configures the match criteria based on which packets are filtered and the deny access action applied | *page 4-62* |
| *description* | Configures a brief description for this application policy that enables you to differentiate it from other application policies | *page 4-65* |
| *enforcement-time* | Configures an enforcement time period in days and hours for this application policy. The policy is enforced only during the specified time period. | *page 4-66* |
| *logging* | Enables logging of application recognition hits made by the DPI engine. It also sets the logging level. | *page 4-68* |
| *mark* | Creates a mark rule and configures the match criteria based on which packets are filtered and marked with 802.1p priority value or *Differentiated Service Code Point* (DSCP) code | *page 4-70* |
| *rate-limit* | Creates a rate-limit rule and configures the match criteria based on which incoming and outgoing packets are filtered and the configured rate limits applied | *page 4-73* |
| *no* | Removes or resets this application policy's settings | *page 4-76* |

### 4.1.24.2.1 allow

*application-policy-mode commands*

Creates an allow rule and configures the match criteria based on which packets are filtered and the allow access action applied

**Supported in the following platforms:**

- Access Points — AP7522, AP7532
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
allow [app-category [<APP-CATEGORY-NAME>|all]|application <APPLICATION-NAME>]
schedule <SCHEDULE-POLICY-NAME> (precedence <1-256>)
```

**Parameters**

```
• allow [app-category [<APP-CATEGORY-NAME>|all]|application <APPLICATION-NAME>]
schedule <SCHEDULE-POLICY-NAME> (precedence <1-256>)
```

| | |
|---|---|
| allow | Creates an allow rule and configures the match criteria. The options are app-category and application. |
| app-category [<APP-CATEGORY-NAME>\|all] | Uses application category as the match criteria<br>• <APP-CATEGORY-NAME> – Specify the application category. The options are: antivirus\ update, audio, business, conference, custom, database, file transfer, gaming, generic, im, mail, mobile, network\ management, other, p2p, remote_control, social\ networking, standard, streaming, tunnel, video, voip, and web. Each packet's app-category is matched with the value specified here. In case of a match, the system forwards the packet or else drops it.<br>• all – The system forwards all packets irrespective of the application category. |
| application <APPLICATION-NAME> | Uses application name as the match criteria<br>• <APPLICATION-NAME> – Specify the application name. Each packet's application is matched with the application name specified here. In case of a match, the system forwards the packet.<br>The WiNG database provides approximately 381 canned applications. In addition to these, the database also includes custom-made applications. These are application definitions created using the *application* command. |
| schedule <SCHEDULE-POLICY-NAME> | Schedules an enforcement time for this allow rule by associating a schedule policy with it. Use this parameter to apply rule-specific enforcement time.<br>• schedule <SCHEDULE-POLICY-NAME> – Associates a schedule policy with the rule. When associated, the rule is enforced only on the days and time configured in the schedule policy. Without the association of a schedule policy, all rules within an application policy are enforced concurrently (defined by the application-policy > enforcement-time command). If scheduling a rule, ensure that the time configured in the schedule policy is a subset of the application policy's enforcement time. In other words the application policy should be active when the rule is being enforced. For example, if the application policy is enforced on Mondays from 10:00 to 22:00 hours and the schedule policy time-rule is set for Fridays, then this rule will never be hit. When enforcing rules at different times the best practice would be to keep the application policy active at all time (i.e., retain the default enforcement-time setting as 'all').<br>Contd.. |

| | |
|---|---|
| | • <SCHEDULE-POLICY-NAME> – Specify the policy name (should be existing and configured). After applying a schedule policy, specify a precedence for the rule.<br>In case of no schedule policy being applied, the rule is enforced as per the enforcement-time configured in the application policy. For more information, see *enforcement-time*. |
| precedence <1-256> | Assigns a precedence value for this allow rule. The precedence value differentiates between rules applicable to applications and the application categories to which they belong. The allow, deny, mark, rate-limit options are mutually exclusive. In other words, in an application policy, for a specific application or application category, you can create either an allow rule, or a deny rule, or a mark and rate-limit rule.<br>Let us consider application *youtube* belonging to app-category *streaming*.<br>The action required is: Allow *youtube* packets and deny all other applications belonging to app-category *streaming*.<br>The rules can be defined as:<br>`#allow application youtube precedence 1`<br>`#deny app-category streaming precedence 2`<br>The following configuration is incorrect:<br>`#deny app-category streaming precedence 1`<br>`#allow application youtube precedence 2`<br>Once the deny app-category streaming precedence 1 rule is hit, all streaming packets, including youtube, are dropped. Consequently, there are no packets left to apply the subsequent allow rule.<br>The mark and rate-limit rules are the only two actions that can be combined for a specific application or application category type. |

**Example**

The following example shows how to view all built-in, system provided applications:

```
nx9500-6C8809(config-app-policy-test)#allow application [TAB]
Display all 366 possibilities? (y or n)
1-clickshare-com                    1-upload-com
1-upload-to                         10upload-com
123upload-pl                        139pan-com
163pan-com                          1clickshare-net
1fichier-com                        1kxun
2channel                            2gis
2shared-com                         360mobile
4fastfile-com                       4share-ws
Dota\ 2                             EA\ Origin
--More--
nx9500-6C8809(config-app-policy-test)#
```

The following examples show two *allow* rules, allowing access to all packets belonging to the *application category* 'business' and the *application* 'Bing':

```
nx9500-6C8809(config-app-policy-Bing)#allow application Bi [TAB]
Bing                        BitTorrent                  BitTorrent_encrypted
BitTorrent_plain            BitTorrent_uTP              BitTorrent_uTP_encrypted
nx9500-6C8809(config-app-policy-Bing)#
```

Note: Bing is not one of the WiNG built-in database applications. It is a customized application created using the *application* command.

```
nx9500-6C8809(config-app-policy-Bing)#allow application Bing precedence 1
```

```
nx9500-6C8809(config-app-policy-Bing)#allow app-category [TAB]
all                  antivirus\ update    audio
business             conference           custom
database             filetransfer         gaming
generic              im                   mail
mobile               network\ management   other
p2p                  remote_control       social\ networking
standard             streaming            tunnel
video                voip                 web
nx9500-6C8809(config-app-policy-Bing)#

nx9500-6C8809(config-app-policy-Bing)#allow app-category business precedence 2

nx9500-6C8809(config-app-policy-Bing)#show context
application-policy Bing
 allow application Bing precedence 1
 allow app-category business precedence 2
nx9500-6C8809(config-app-policy-Bing)#
```

The following example shows an application policy 'SocialNet' having an allow rule with an associated schedule policy named 'FaceBook':

```
nx9500-6C8809(config-app-policy-SocialNet)#allow application facebook schedule
Facebook precedence 1

nx9500-6C8809(config-app-policy-SocialNet)#show context
application-policy SocialNet
 description "This application policy relates to Social Networking sites."
 allow application facebook schedule FaceBook precedence 1
nx9500-6C8809(config-app-policy-SocialNet)#
```

The schedule policy 'FaceBook' configuration is as follows. As per this policy, the above allow rule will apply to all FaceBook packets every Friday between 13:00 and 18:00 hours.

```
nx9500-6C8809(config-schedule-policy-FaceBook)#show context
schedule-policy FaceBook
 description "Allows FaceBook traffic on Fridays."
 time-rule days friday start-time 13:00 end-time 18:00
nx9500-6C8809(config-schedule-policy-FaceBook)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes this allow rule from the application policy |

### 4.1.24.2.2 deny

*application-policy-mode commands*

Creates a deny rule and configures the match criteria based on which packets are filtered and the deny access action applied

**Supported in the following platforms:**

- Access Points — AP7522, AP7532
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
deny [app-category [<APP-CATEGORY-NAME>|all]|application <APPLICATION-NAME>]
schedule <SCHEDULE-POLICY-NAME> (precedence <1-256>)
```

**Parameters**

```
• deny [app-category [<APP-CATEGORY-NAME>|all]|application <APPLICATION-NAME>]
schedule <SCHEDULE-POLICY-NAME> (precedence <1-256>)
```

| | |
|---|---|
| deny | Creates a deny rule and configures the match criteria. The options are app-category and application. |
| app-category [<APP-CATEGORY-NAME>\|all] | Uses application category as the match criteria<br>• <APP-CATEGORY-NAME> – Specify the application category name. The options are: antivirus\ update, audio, business, conference, custom, database, file transfer, gaming, generic, im, mail, mobile, network\ management, other, p2p, remote_control, social\ networking, standard, streaming, tunnel, video, voip, and web. Each packet's app-category is matched with the value specified here. In case of a match, the system drops the packet.<br>• all – The system drops all packets irrespective of the application category. |
| application <APPLICATION-NAME> | Uses application name as the match criteria<br>• <APPLICATION-NAME> – Specify the application name. Each packet's application is matched with the application name specified here. In case of a match, the system drops the packet.<br>There are approximately some 381 canned applications in the database. In addition to these, the database displays custom-made applications also. These are application definitions created using the application command. |
| schedule <SCHEDULE-POLICY-NAME> | Schedules an enforcement time for this deny rule by associating a schedule policy with it. Use this parameter to apply rule-specific enforcement time.<br>• schedule <SCHEDULE-POLICY-NAME> – Associates a schedule policy with the rule. When associated, the rule is enforced only on the days and time configured in the schedule policy. Without the association of a schedule policy, all rules within an application policy are enforced concurrently (defined by the application-policy > enforcement-time command). If scheduling a rule, ensure that the time configured in the schedule policy is a subset of the application policy's enforcement time. In other words the application policy should be active when the rule is being enforced. For example, if the application policy is enforced on Mondays from 10:00 to 22:00 hours and the schedule policy time-rule is set for Fridays, then this rule will never be hit. When enforcing rules at different times the best practice would be to keep the application policy active at all time (i.e., retain the default enforcement-time setting as 'all').<br>Contd.. |

| | |
|---|---|
| | • <SCHEDULE-POLICY-NAME> – Specify the policy name (should be existing and configured). After applying a schedule policy, specify a precedence for the rule.<br>In case of no schedule policy being applied, the rule is enforced as per the enforcement-time configured in the application policy. For more information, see *enforcement-time*. |
| precedence <1-256> | Assigns a precedence value for this deny rule. The precedence value differentiates between rules applicable to applications and the application categories to which they belong. The allow, deny, mark, rate-limit options are mutually exclusive. In other words, in an application policy, for a specific application or application category, you can create either an allow rule, or a deny rule, or a mark and rate-limit rule.<br>Let us consider application *youtube* belonging to app-category *streaming*.<br>The action required is: Allow *youtube* packets and deny all other applications belonging to app-category *streaming*.<br>The rules can be defined as:<br>`#allow application youtube precedence 1`<br>`#deny app-category streaming precedence 2`<br>The following configuration is incorrect:<br>`#deny app-category streaming precedence 1`<br>`#allow application youtube precedence 2`<br>Once the deny app-category streaming precedence 1 rule is hit, all streaming packets, including youtube, are dropped. Consequently, there are no packets left to apply the subsequent allow rule.<br>The mark and rate-limit rules are the only two actions that can be combined for a specific application or application category type. |

**Example**

The following example shows one *deny* rule, denying access to all packets belonging to the application category 'social\ networking':

```
nx9500-6C8809(config-app-policy-Bing)#deny app-category social\ networking
precedence 3

nx9500-6C8809(config-app-policy-Bing)#show context
application-policy Bing
 allow application Bing precedence 1
 allow app-category business precedence 2
 deny app-category "social networking" precedence 3
nx9500-6C8809(config-app-policy-Bing)#
```

The following example displays the schedule policy 'DenyS-N' settings. The time-rule defined in the policy is *all weekdays from 9:30 AM to 11:30 PM*.

```
nx9500-6C8809(config-schedule-policy-DenyS-N)#show context
schedule-policy DenyS-N
 description "Denies all social Networking sites on weekdays."
 time-rule days weekdays start-time 09:30 end-time 23:30
nx9500-6C8809(config-schedule-policy-DenyS-N)#
```

The following example displays the schedule policy 'FaceBook' settings. The time-rule defined in the policy is *Friday from 1:00 PM to 6:00 PM*.

```
nx9500-6C8809(config-schedule-policy-FaceBook)#show context
schedule-policy FaceBook
 description "Allows FaceBook traffic on Fridays."
 time-rule days friday start-time 13:00 end-time 18:00
nx9500-6C8809(config-schedule-policy-FaceBook)#
```

The following example shows an application policy 'SocialNet' defining an *allow* and *deny* rule. Both rules have different enforcement time, which is defined by their respective schedule policies (DentS-N and FaceBook). As per these two schedule policy settings, this application policy:

- Denies all social\ networking sites on weekdays (barring Fridays between 1:00 PM to 6:00 PM) from 9:30 AM to 11:30 PM.

On Fridays, between 1:00 PM to 6:00 PM, it:

- Denies all social\ networking sites except Facebook.

```
nx9500-6C8809(config-app-policy-SocialNet)#show context
application-policy SocialNet
 description "This application policy relates to Social Networking sites."
 allow application facebook schedule FaceBook precedence 1
 deny app-category "social networking" schedule DenyS-N precedence 2
nx9500-6C8809(config-app-policy-SocialNet)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes this deny rule from the application policy |

### 4.1.24.2.3 description

*application-policy-mode commands*

Configures a brief description for this application policy that enables you to differentiate it from other application policies

**Supported in the following platforms:**

- Access Points — AP7522, AP7532
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
description <LINE>
```

**Parameters**

- `description <LINE>`

| | |
|---|---|
| description <LINE> | Configures this application policy's description<br>• <LINE> – Specify a brief description not exceeding 80 characters in length. |

**Example**

```
nx9500-6C8809(config-app-policy-Bing)#description "This application policy allows
Bing search engine packets"

nx9500-6C8809(config-app-policy-Bing)#show context
application-policy Bing
 description "This application policy allows Bing search engine packets"
 allow application Bing precedence 1
 allow app-category business precedence 2
 deny app-category "social networking" precedence 3
nx9500-6C8809(config-app-policy-Bing)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes this application policy's description |

### 4.1.24.2.4 enforcement-time

*application-policy-mode commands*

Configures an enforcement time period in days and hours for this application policy. The enforcement time is applicable only to those rules, within the application policy, that do not have a schedule policy associated. By default an application policy is enforced on all days.

**NOTE:** Schedule policies are a means of enforcing allow/deny/mark/rate-limit rules at different time periods. If no schedule policy is applied, all rules within an application policy are enforced at the time specified using this enforcement-time command. For more information on configuring a schedule policy, see *schedule-policy*.

**Supported in the following platforms:**

- Access Points — AP7522, AP7532
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
enforcement-time days [sunday|monday|tuesday|wednesday|thursday|friday|
saturday|all|weekends|weekdays] {start-time <HH:MM> end-time <HH:MM>}
```

**Parameters**

```
• enforcement-time days [sunday|monday|tuesday|wednesday|thursday|friday|
saturday|all|weekends|weekdays] {start-time <HH:MM> end-time <HH:MM>}
```

| | |
|---|---|
| enforcement-time days | Enforces this application policy on only on the days specified here<br>• sunday – Enforces the policy only on Sundays<br>• monday – Enforces the policy only on Mondays<br>• tuesday – Enforces the policy only on Tuesdays<br>• wednesday – Enforces the policy only on Wednesdays<br>• thursday – Enforces the policy only on Thursdays<br>• friday – Enforces the policy only on Fridays<br>• saturday – Enforces the policy only on Saturdays<br>• all – Enforces the policy on all days. This is the default setting.<br>• weekends – Enforces the policy only on weekends<br>• weekdays – Enforces the policy only on weekdays<br>In case no enforcement time is specified, the application policy is enforced on all days (i.e., always active).<br>If using schedule policies with the allow/deny/mark/rate-limit rules, the best practice would be to keep the application policy active at all time (i.e., retain the default enforcement-time setting of 'all'). |
| start-time <HH:MM> end-time <HH:MM> | Optional. Configures this application policy's enforcement period<br>• start-time – Configures the start time. This is the time at which the application policy enforcement begins.<br>• end-time – Configures the end time. This is the time at which the application policy enforcement ends.<br>  • <HH:MM> – Specify the start and end time in the HH:MM format. |

**Example**

```
nx9500-6C8809(config-app-policy-Bing)#enforcement-time days weekdays start-time
10:30 end-time 20:00

nx9500-6C8809(config-app-policy-Bing)#show context
application-policy Bing
 description "This application policy allows Bing search engine packets"
 enforcement-time days weekdays start-time 10:30 end-time 20:00
 allow application Bing precedence 1
 allow app-category business precedence 2
 deny app-category "social networking" precedence 3
nx9500-6C8809(config-app-policy-Bing)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes this application policy's enforcement period |

### 4.1.24.2.5 logging

*application-policy-mode commands*

Enables DPI application recognition logging. It also sets the logging level.

DPI is an advanced packet analysis technique, which analyzes packet and packet content headers to determine the nature of network traffic. When enabled, DPI inspects packets of all flows to identify applications (such as, Netflix, Twitter, Facebook, etc.) and extract metadata (such as, host name, server name, TCP-RTT, etc.) for further use by the WiNG firewall.

**Supported in the following platforms:**

- Access Points — AP7522, AP7532
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
logging [level|on]

logging on

logging level [<0-7>|alerts|critical|debugging|emergencies|errors|informational|
notifications|warnings]
```

**Parameters**

- `logging on`

| | |
|---|---|
| logging on | Enables logging of application recognition hits made by the DPI engine. This option is disabled by default. |

- `logging level [<0-7>|alerts|critical|debugging|emergencies|errors|informational|notifications|warnings]`

| | |
|---|---|
| logging level [<0-7>\|alerts\|critical\|debugging\|emergencies\|errors\|informational\|notifications\|warnings] | Sets the logging level for application recognition hits made by the DPI engine. This option is disabled by default.<br>• <0-7> – Sets the message logging severity level on a scale of 0 - 7<br>• emergencies – Severity level 0: System is unusable<br>• alerts – Severity level 1: Requires immediate action<br>• critical – Severity level 2: Critical conditions<br>• errors – Severity level 3: Error conditions<br>• warnings – Severity level 4: Warning conditions<br>• notifications – Severity level 5: Normal but significant conditions (this is the default setting)<br>• informational – Severity level 6: Informational messages<br>• debugging – Severity level 7: Debugging messages |

**Example**

```
nx9500-6C8809(config-app-policy-Bing)#logging level critical

nx9500-6C8809(config-app-policy-Bing)#show context
application-policy Bing
 description "This application policy allows Bing search engine packets"
 enforcement-time days weekdays start-time 12:30 end-time 20:00
 allow application Bing precedence 1
 allow app-category business precedence 2
 deny app-category "social networking" precedence 3
 logging level critical
nx9500-6C8809(config-app-policy-Bing)#
```

**Related Commands**

| | |
|---|---|
| *no* | Resets the logging level to default (notifications). And the *no > logging > on* command disables DPI logging. |

### 4.1.24.2.6 mark

*application-policy-mode commands*

Creates a mark rule and configures the match criteria based on which packets are marked

Marks packets, matching a specified set of application categories or applications/protocols, with 802.1p priority level or *Differentiated Services Code Point* (DSCP) *type of service* (ToS) code. Marking packets is a means of identifying them for specific actions, and is used to provide different levels of service to different traffic types.

**Supported in the following platforms:**

- Access Points — AP7522, AP7532
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
mark [app-category [<APP-CATEGORY-NAME>|all]|application <APPLICATION-NAME>]
[8021p <0-7>|dscp <0-63>] schedule <SCHEDULE-POLICY-NAME> (precedence <1-256>)
```

**Parameters**

```
• mark [app-category [<APP-CATEGORY-NAME>|all]|application <APPLICATION-NAME>]
[8021p <0-7>|dscp <0-63>] schedule <SCHEDULE-POLICY-NAME> (precedence <1-256>)
```

| | |
|---|---|
| mark | Creates a mark rule and configures the match criteria. When applied, the rule marks packets, matching the criteria configured here, with 802.1p priority value or DSCP code. The match criteria options are: app-category and application. |
| app-category [<APP-CATEGORY-NAME>\|all] | Uses application category as the match criteria<br>• <APP-CATEGORY-NAME> – Specify the application category. The options are: antivirus\ update, audio, business, conference, custom, database, file transfer, gaming, generic, im, mail, mobile, network\ management, other, p2p, remote_control, social\ networking, standard, streaming, tunnel, video, voip, and web. Each packet's app-category is matched with the value specified here. In case of a match, the system marks the packet.<br>• all – The system marks all packets irrespective of the application category. |
| application <APPLICATION-NAME> | Uses application name as the match criteria<br>• <APPLICATION-NAME> – Specify the application name. Each packet's application is matched with the application name specified here. In case of a match, the system marks the packet.<br>The WiNG database provides approximately 381 canned applications. In addition to these, the database includes custom-made applications. These are application definitions created using the *application* command. |
| 8021p <0-7> | Marks packets matching the specified criteria with 802.1p priority value<br>• <0-7> – Specify a value from 0 - 7.<br>The IEEE 802.1p signaling standard enables marking of layer 2 network traffic. Layer 2 network devices (such as switches), using 802.1p standards, group traffic into classes based on their 802.1p priority value, which is appended to the packet's MAC header. In case of traffic congestion, packets with higher priority get precedence over lower priority packets and are forwarded first. |

| | |
|---|---|
| dscp <0-63> | Marks packets matching the specified criteria with DSCP ToS code<br>• <0-63> – Specify a value from 0 - 63.<br>The DSCP protocol marks layer 3 network traffic. Layer 3 network devices (such as routers) using DSCP, mark each layer 3 packet with a six-bit DSCP code, which is appended to the packet's IP header. Each DSCP code is assigned a corresponding level of service, enabling packet prioritization. |
| schedule <SCHEDULE-POLICY-NAME> | Schedules an enforcement time for this mark rule by associating a schedule policy with it. Use this parameter to apply rule-specific enforcement time.<br>• schedule <SCHEDULE-POLICY-NAME> – Associates a schedule policy with the rule. When associated, the rule is enforced only on the days and time configured in the schedule policy. Without the association of a schedule policy, all rules within an application policy are enforced concurrently (defined by the application-policy > enforcement-time command). If scheduling a rule, ensure that the time configured in the schedule policy is a subset of the application policy's enforcement time. In other words the application policy should be active when the rule is being enforced. For example, if the application policy is enforced on Mondays from 10:00 to 22:00 hours and the schedule policy time-rule is set for Fridays, then this rule will never be hit. When enforcing rules at different times the best practice would be to keep the application policy active at all time (i.e., retain the default enforcement-time setting as 'all').<br>• <SCHEDULE-POLICY-NAME> – Specify the policy name (should be existing and configured). After applying a schedule policy, specify a precedence for the rule.<br>In case of no schedule policy being applied, the rule is enforced as per the enforcement-time configured in the application policy. For more information, see *enforcement-time*. |
| precedence <1-256> | Assigns a precedence value for this mark rule. The precedence value differentiates between rules applicable to applications and the application categories they belong. The allow, deny, mark, rate-limit options are mutually exclusive. In other words, in an application policy, for a specific application or application category, you can create either an allow rule, or a deny rule, or a mark and rate-limit rule.<br>Let us consider application *youtube* belonging to app-category *streaming*.<br>The action required is: Allow *youtube* packets and deny all other applications belonging to app-category *streaming*.<br>The rules can be defined as:<br>`#allow application youtube precedence 1`<br>`#deny app-category streaming precedence 2`<br>The following configuration is incorrect:<br>`#deny app-category streaming precedence 1`<br>`#allow application youtube precedence 2`<br>Once the deny app-category streaming precedence 1 rule is hit, all streaming packets, including youtube, are dropped. Consequently, there are no packets left to apply the subsequent allow rule.<br>The mark and rate-limit rules are the only two actions that can be combined for a specific application or application category type. |

**Example**

```
nx9500-6C8809(config-app-policy-Bing)#mark app-category video dscp 9 precedence 4

nx9500-6C8809(config-app-policy-Bing)#mark application facetime dscp 10 precedence
5

nx9500-6C8809(config-app-policy-Bing)#show context
application-policy Bing
 description "This application policy allows Bing search engine packets"
 enforcement-time days weekdays start-time 12:30 end-time 20:00
 allow application Bing precedence 1
 allow app-category business precedence 2
 deny app-category "social networking" precedence 3
 mark app-category video dscp 9 precedence 4
 mark application facetime dscp 10 precedence 5
 logging level critical
nx9500-6C8809(config-app-policy-Bing)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes this mark rule from the application policy |

### 4.1.24.2.7 rate-limit

*application-policy-mode commands*

Creates a rate-limit rule and configures the match criteria

**Supported in the following platforms:**

- Access Points — AP7522, AP7532
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
rate-limit [app-category [<APP-CATEGORY-NAME>|all]|application <APPLICATION-
NAME>] ([egress|ingress]) rate <50-1000000> max-burst-size <2-1024> schedule
<SCHEDULE-POLICY-NAME> (precedence <1-256>)
```

**Parameters**

```
• rate-limit [app-category [<APP-CATEGORY-NAME>|all]|application <APPLICATION-
NAME>] ([egress|ingress]) rate <50-1000000> max-burst-size <2-1024> schedule
<SCHEDULE-POLICY-NAME> (precedence <1-256>)
```

| | |
|---|---|
| rate-limit | Creates a rate-limit rule and configures the match criteria. When applied, the rule applies a rate-limit to packets that match the criteria configured here. These packets could be incoming, outgoing, or both. The match criteria options are: app-category and application. |
| app-category [<APP-CATEGORY-NAME>\|all] | Uses application category as the match criteria<br>• <APP-CATEGORY-NAME> – Specify the application category. The options are: antivirus\ update, audio, business, conference, custom, database, file transfer, gaming, generic, im, mail, mobile, network\ management, other, p2p, remote_control, social\ networking, standard, streaming, tunnel, video, voip, and web. Each packet's app-category is matched with the value specified here. In case of a match, the system rate-limits the packet.<br>• all – The system rate-limits all packets irrespective of the application category. |
| application <APPLICATION-NAME> | Uses application name as the match criteria<br>• <APPLICATION-NAME> – Specify the application name. Each packet's application is matched with the application name specified here. In case of a match, the system rate-limits the packet. |
| [egress\|ingress] | The egress and ingress parameters are recursive and can be used to rate limit either incoming, outgoing, or both incoming and outgoing traffic.<br>• egress – Selects the traffic type as outgoing<br>• ingress – Selects the traffic type as outgoing<br>After selecting the traffic type (incoming/outgoing) configure the rate and maximum burst size. |
| rate <50-1000000> | The following parameters are common to the 'egress' and 'ingress' keywords:<br>• rate – Configures the rate limit, in Kbps, for both incoming and outgoing packets<br>  • <50-1000000> – Specify the rate limit from 50 - 1000000 Kbps. |
| max-burst-size | The following parameters are common to the 'egress' and 'ingress' keywords:<br>• max-burst-size – Configures the maximum burst size, in Kbytes, for both incoming and outgoing packets<br>  • <2-1024> – Specify the maximum burst size from 2 - 1024 Kbytes. |

| | |
|---|---|
| schedule <SCHEDULE-POLICY-NAME> | Schedules an enforcement time for this rate-limit rule by associating a schedule policy with it. Use this parameter to apply rule-specific enforcement time.<br>• schedule <SCHEDULE-POLICY-NAME> – Associates a schedule policy with the rule. When associated, the rule is enforced only on the days and time configured in the schedule policy. Without the association of a schedule policy, all rules within an application policy are enforced concurrently (defined by the application-policy > enforcement-time command). If scheduling a rule, ensure that the time configured in the schedule policy is a subset of the application policy's enforcement time. In other words the application policy should be active when the rule is being enforced. For example, if the application policy is enforced on Mondays from 10:00 to 22:00 hours and the schedule policy time-rule is set for Fridays, then this rule will never be hit. When enforcing rules at different times the best practice would be to keep the application policy active at all time (i.e., retain the default enforcement-time setting as 'all').<br>• <SCHEDULE-POLICY-NAME> – Specify the policy name (should be existing and configured). After applying a schedule policy, specify a precedence for the rule.<br>In case of no schedule policy being applied, the rule is enforced as per the enforcement-time configured in the application policy. For more information, see *enforcement-time*. |
| precedence <1-256> | Assigns a precedence value for this mark rule. The precedence value differentiates between rules applicable to applications and the application categories they belong. The allow, deny, mark, rate-limit options are mutually exclusive. In other words, in an application policy, for a specific application or application category, you can create either an allow rule, or a deny rule, or a mark and rate-limit rule.<br>Let us consider application *youtube* belonging to app-category *streaming*.<br>The action required is: Allow *youtube* packets and deny all other applications belonging to app-category *streaming*.<br>The rules can be defined as:<br>`#allow application youtube precedence 1`<br>`#deny app-category streaming precedence 2`<br>The following configuration is incorrect:<br>`#deny app-category streaming precedence 1`<br>`#allow application youtube precedence 2`<br>Once the deny app-category streaming precedence 1 rule is hit, all streaming packets, including youtube, are dropped. Consequently, there are no packets left to apply the subsequent allow rule.<br>The mark and rate-limit rules are the only two actions that can be combined for a specific application or application category type. |

**Example**

```
nx9500-6C8809(config-app-policy-Bing)#rate-limit application BGP ingress rate 100
max-burst-size 25 egress rate 50 max-burst-size 25 precedence 6

nx9500-6C8809(config-app-policy-Bing)#show context
application-policy Bing
 description "This application policy allows Bing search engine packets"
 enforcement-time days weekdays start-time 12:30 end-time 20:00
 allow application Bing precedence 1
 allow app-category business precedence 2
 deny app-category "social networking" precedence 3
 mark app-category video dscp 9 precedence 4
 mark application facetime dscp 10 precedence 5
 rate-limit application BGP ingress rate 100 max-burst-size 25 egress rate 50 max-
burst-size 25 precedence 6
 logging level critical

nx9500-6C8809(config-app-policy-Bing)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes this rate-limit rule from the application policy |

### 4.1.24.2.8 no

*application-policy-mode commands*

Removes or resets this application policy's settings

**Supported in the following platforms:**

- Access Points — AP7522, AP7532
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
no [allow|deny|description|enforcement-time|logging|mark|rate-limit]

no allow [app-category [<APP-CATEGORY-NAME>|all]|application <APPLICATION-NAME>]
precedence <1-256>

no deny [app-category [<APP-CATEGORY-NAME>|all]|application <APPLICATION-NAME>]
precedence <1-256>

no description

no enforcement-time days [sunday|monday|tuesday|wednesday|thursday|friday|
saturday|all|weekends|weekdays]

no logging [level|on]

no mark [app-category [<APP-CATEGORY-NAME>|all]|application <APPLICATION-NAME>]
precedence <1-256>

no rate-limit [app-category [<APP-CATEGORY-NAME>|all]|application <APPLICATION-
NAME>] precedence <0-256>
```

**Parameters**

- no <PARAMETERS>

| | |
|---|---|
| no <PARAMETERS> | Removes or resets this application policy settings based on the parameters passed |

**Example**

The following example shows the application policy 'Bing' settings before the 'no' commands are executed:

```
nx9500-6C8809(config-app-policy-Bing)#show context
application-policy Bing
 description "This application policy allows Bing search engine packets"
 enforcement-time days weekdays start-time 12:30 end-time 20:00
 allow application Bing precedence 1
 allow app-category business precedence 2
 deny app-category "social networking" precedence 3
 mark app-category video dscp 9 precedence 4
 mark application facetime dscp 10 precedence 5
 rate-limit application BGP ingress rate 100 max-burst-size 25 egress rate 50 max-
burst-size 25 precedence 6
 logging level critical

nx9500-6C8809(config-app-policy-Bing)#

nx9500-6C8809(config-app-policy-Bing)#no allow app-category business precedence 2
nx9500-6C8809(config-app-policy-Bing)#no deny app-category social\ networking
precedence 3
```

The following example shows the application policy ‘Bing’ settings after the ‘no’ commands are executed:

```
nx9500-6C8809(config-app-policy-Bing)#show context
application-policy Bing
 description "This application policy allows Bing search engine packets"
 enforcement-time days weekdays start-time 12:30 end-time 20:00
 allow application Bing precedence 1
 mark app-category video dscp 9 precedence 4
 mark application facetime dscp 10 precedence 5
 rate-limit application BGP ingress rate 100 max-burst-size 25 egress rate 50 max-
burst-size 25 precedence 6
 logging level critical
nx9500-6C8809(config-app-policy-Bing)#
```

## 4.1.25 association-acl-policy

*Global Configuration Commands*

Configures an association ACL policy. This policy defines a list of devices allowed or denied access to the network.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
association-acl-policy <ASSOCIATION-ACL-POLICY-NAME>
```

**Parameters**

- `association-acl-policy <ASSOCIATION-ACL-POLICY-NAME>`

| | |
|---|---|
| <ASSOCIATION-ACL-POLICY-NAME> | Specify the association ACL policy name. If the policy does not exist, it is created. |

**Example**

```
rfs6000-81742D(config)#association-acl-policy test
rfs6000-81742D(config-assoc-acl-test)#?
Association ACL Mode commands:
  deny      Specify MAC addresses to be denied
  no        Negate a command or set its defaults
  permit    Specify MAC addresses to be permitted

  clrscr    Clears the display screen
  commit    Commit all changes made in this session
  do        Run commands from Exec mode
  end       End current mode and change to EXEC mode
  exit      End current mode and down to previous mode
  help      Description of the interactive help system
  revert    Revert changes
  service   Service Commands
  show      Show running system information
  write     Write running configuration to memory or terminal

rfs6000-81742D(config-assoc-acl-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Resets values or disables commands |

**NOTE:** For more information on the association-acl-policy, see *Chapter 10, ASSOCIATION-ACL-POLICY*.

## 4.1.26 auto-provisioning-policy

*Global Configuration Commands*

Configures an auto provisioning policy. This policy configures the automatic provisioning of device adoption. The policy configures how an AP is adopted based on its type.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
auto-provisioning-policy <AUTO-PROVISIONING-POLICY-NAME>
```

**Parameters**

- `auto-provisioning-policy <AUTO-PROVISIONING-POLICY-NAME>`

| | |
|---|---|
| <AUTO-PROVISIONING-POLICY-NAME> | Specify the auto provisioning policy name. If the policy does not exist, it is created. |

**Example**

```
rfs6000-81742D(config)#auto-provisioning-policy test
rfs6000-81742D(config-auto-provisioning-policy-test)#?
Auto-Provisioning Policy Mode commands:
  Auto-Provisioning Policy Mode commands:
  adopt                       Add rule for device adoption
  auto-create-rfd-template    When RF Domain specified by the matching rule
                              template does not exist create new RF Domain
                              automatically
  default-adoption            Adopt devices even when no matching rules are
                              found.  Assign default profile and default
                              rf-domain
  deny                        Add rule to deny device adoption
  evaluate-always             Set the flag to evaluate the policy everytime,
                              regardless of previous adoption status
  no                          Negate a command or set its defaults
  redirect                    Add rule to redirect device adoption
  upgrade                     Add rule for device upgrade

  clrscr                      Clears the display screen
  commit                      Commit all changes made in this session
  do                          Run commands from Exec mode
  end                         End current mode and change to EXEC mode
  exit                        End current mode and down to previous mode
  help                        Description of the interactive help system
  revert                      Revert changes
  service                     Service Commands
  show                        Show running system information
  write                       Write running configuration to memory or terminal

rfs6000-81742D(config-auto-provisioning-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing Auto Provisioning policy |

**NOTE:** For more information on the auto-provisioning-policy, see *Chapter 9, AUTO-PROVISIONING-POLICY*.

## 4.1.27 bgp

*Global Configuration Commands*

Configures *Border Gateway Protocol* (BGP) settings

BGP is an inter-ISP routing protocol which establishes routing between *Internet Service Providers* (ISPs). ISPs use BGP to exchange routing and reachability information between *Autonomous Systems* (AS) on the Internet. BGP makes routing decisions based on paths, network policies and/or rules configured by network administrators. The primary role of a BGP system is to exchange network reachability information with other BGP peers. This information includes information on AS that the reachability information traverses. This information is sufficient to create a graph of AS connectivity from which routing decisions can be created and rules enforced.

An AS is a set of routers under the same administration that use *Interior Gateway Protocol* (IGP) and common metrics to define how to route packets within the AS. AS uses inter-AS routing to route packets to other ASs. For an external AS, an AS appears to have a single coherent interior routing plan and presents a consistent picture of the destinations reachable through it.

Routing information exchanged through BGP supports only destination based forwarding (it assumes a router forwards packets based on the destination address carried in the IP header of the packet).

BGP uses TCP as its transport protocol. This eliminates the need to implement explicit update fragmentation, retransmission, acknowledgment, and sequencing. BGP listens on TCP port 179. The error notification mechanism used in BGP assumes that TCP supports a *graceful* close (all outstanding data is delivered before the connection is closed).

**Supported in the following platforms:**

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
bgp [as-path-list|community-list|extcommunity-list|ip-access-list|ip-prefix-list]
<LIST-NAME>
```

**Parameters**

```
• bgp [as-path-list|community-list|extcommunity-list|ip-access-list|ip-prefix-
list] <LIST-NAME>
```

| | |
|---|---|
| as-path-list <LIST-NAME> | Creates an AS path list and enters its configuration mode<br>• <LIST-NAME> – Provide the AS-PATH-LIST name. |
| community-list <LIST-NAME> | Creates a community list and enters its configuration mode<br>• <LIST-NAME> – Provide the COMMUNITY-LIST name. |
| extcommunity-list <LIST-NAME> | Creates an extended community list and enters its configuration mode<br>• <LIST-NAME> – Provide the EXTCOMMUNITY-LIST name. |
| ip-access-list <LIST-NAME> | Creates a BGP IP access list and enters its configuration mode<br>• <LIST-NAME> – Provide the BGP IP-ACCESS-LIST name. |
| ip-prefix-list <LIST-NAME> | Creates a BGP IP prefix list and enters its configuration mode<br>• <LIST-NAME> – Provide the BGP IP-PREFIX-LIST name. |

**Example**

```
nx9500-6C8809(config)#bgp ?
  as-path-list       BGP AS path list Configuration
  community-list     Add a community list entry
  extcommunity-list  Add a extended community list entry (EXPERIMENTAL)
  ip-access-list     Add an access list entry
  ip-prefix-list     Build a prefix list

nx9500-6C8809(config)#

nx9500-6C8809(config)#bgp as-path-list AS-TEST-PATH
nx9500-6C8809(config-bgp-as-path-list-AS-TEST-PATH)#?
BGP AS Path List Mode commands:
  deny     Specify packets to reject
  no       Negate a command or set its defaults
  permit   Specify packets to forward

  clrscr   Clears the display screen
  commit   Commit all changes made in this session
  do       Run commands from Exec mode
  end      End current mode and change to EXEC mode
  exit     End current mode and down to previous mode
  help     Description of the interactive help system
  revert   Revert changes
  service  Service Commands
  show     Show running system information
  write    Write running configuration to memory or terminal

nx9500-6C8809(config-bgp-as-path-list-AS-TEST-PATH)#
```

**Related Commands**

| | |
|---|---|
| *no* | Modifies BGP settings, based on the parameters passed |

**NOTE:** For more information on configuring BGP *Top-Level Objects* (TLOs), see *Chapter 28, BORDER GATEWAY PROTOCOL*.

## 4.1.28 bonjour-gateway-discovery-policy

*Global Configuration Commands*

The following table lists the commands that allows you to create a Bonjour Gateway Discovery Policy:

**Table 4.8** *Bonjour-Gateway-Discovery Config Commands*

| Command | Description | Reference |
|---|---|---|
| *bonjour-gw-discovery-policy* | Creates a Bonjour Gateway Discovery policy and enters its configuration mode | *page 4-84* |
| *bonjour-gateway-discovery-policy-mode commands* | Summarizes Bonjour Gateway Discovery policy configuration mode commands | *page 4-86* |

### 4.1.28.1 bonjour-gw-discovery-policy

*bonjour-gateway-discovery-policy*

Bonjour is Apple's zero-configuration networking (Zeroconf) implementation. Bonjour enables automatic IP address assignment, name to address resolution, and service discovery without having to configure a DHCP server, DNS server, and Directory server. When configured and applied on a WLAN, the Bonjour Gateway Discovery policy queries for and locates Bonjour devices (printers, computers, file-sharing servers, etc.) and services these computers provide over a local network. Bonjour works only within a single broadcast domain. However, with a special DNS configuration, it can be extended to find services across broadcast domains.

Use this command to configure a Bonjour GW Discovery policy. The policy defines a list of services clients can discover across subnets. A maximum of 8 (eight) policies can be created on access points, wireless controllers, or service platforms.

When configured and applied, this feature enables discovery of Bonjour services on local and/or tunneled VLANs.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
bonjour-gw-discovery-policy <POLICY-NAME>
```

**Parameters**

- `bonjour-gw-discovery-policy <POLICY-NAME>`

| | |
|---|---|
| <POLICY-NAME> | Specify the Bonjour GW Discovery policy name. If the policy does not exist, it is created. In the Bonjour GW Discovery policy configuration mode, use the allow-service keyword to configure the services that the Bonjour gateway is allowed to discover. A maximum of 16 (sixteen) service rules can be created. Optionally, you can restrict this facility for users on specific VLANs. To do so, specify the VLAN IDs.<br>Execute the bonjour-gw-forwarding-policy command to enable forwarding of Bonjour service responses across VLANs.<br>To associate a Bonjour GW Discovery policy with a WLAN, in the WLAN configuration mode, execute the following command: *use > bonjour-gw-discovery-policy > <POLICY-NAME>*. For more information, see *use*.<br>To associate a Bonjour GW Discovery policy with a VLAN, in the interface VLAN configuration mode, execute the following command: *use > bonjour-gw-discovery-policy > <POLICY-NAME>*. For more information, see *use*.<br>To associate a Bonjour GW Discovery policy with a user role, in the role-policy - user-role - configuration mode, execute the following command: *use > bonjour-gw-discovery-policy > <POLICY-NAME>*. For more information, see *use*. |

**Example**

```
rfs6000-81742D(config)#bonjour-gw-discovery-policy TestPolicy
rfs6000-81742D(config-bonjour-gw-discovery-policy-TestPolicy)#?
 commands:
  allow-service  Allow Bonjour Service on local or tunneled vlan,Optionally
                 VLAN IDs can be given so service will be discovered for those
                 vlan only
  no             Negate a command or set its defaults

  clrscr         Clears the display screen
  commit         Commit all changes made in this session
  do             Run commands from Exec mode
  end            End current mode and change to EXEC mode
  exit           End current mode and down to previous mode
  help           Description of the interactive help system
  revert         Revert changes
  service        Service Commands
  show           Show running system information
  write          Write running configuration to memory or terminal

rfs6000-81742D(config-bonjour-gw-discovery-policy-TestPolicy)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing Bonjour GW Discovery policy |

### 4.1.28.2 bonjour-gateway-discovery-policy-mode commands

*bonjour-gateway-discovery-policy*

The following table summarizes the Bonjour Gateway Discovery Policy configuration mode commands:

**Table 4.9** *Bonjour-Gateway-Discovery-Policy-Mode Commands*

| Command | Description | Reference |
|---|---|---|
| *allow-service* | Configures the Bonjour Services that can be discovered on Local or Tunneled VLANs. It configures the local VLANs on which these services can be found. | *page 4-87* |
| *no* | Removes or modifies the Bonjour Gateway Discovery policy settings | *page 4-89* |

### 4.1.28.2.1 allow-service

*bonjour-gateway-discovery-policy-mode commands*

Enables discovery of Bonjour devices and the services they provide on Local or Tunneled VLANs

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
allow-service <BONJOUR-SERVICE-NAME> [local|tunneled]

allow-service <BONJOUR-SERVICE-NAME> local {instance-name contains <WORD>}
({service-vlans <WORD>})

allow-service <BONJOUR-SERVICE-NAME> tunneled {instance-name contains <WORD>}
```

**Parameters**

```
• allow-service <BONJOUR-SERVICE-NAME> local {instance-name contains <WORD>}
({service-vlans <WORD>})
```

| | |
|---|---|
| allow-service <BONJOUR-SERVICE-NAME> | Configures the services that can be discovered by the Bonjour gateway. And also configures the VLANs on which the selected services can be discovered.<br>• <BONJOUR-SERVICE-NAME> – You can either select the Bonjour services from a set of system-provided, pre-defined Apple services, or use an existing alias to define a service not available in the predefined list.<br>The predefined Apple services available are: Afp, AirPlay, AirPort, AirPrint, AirTunes, AppleTimeMachine, Chromecast, Daap, HomeSharing, Printer, and Scanner.<br>Use the <WORD> keyword to define a service not included in the system-provided, pre-defined list. Ensure this device is registered with the *Multicast DNS Responder* (mDNSResponder). |
| local | Select to enable the discovery of the selected Bonjour Services on the local VLAN |
| instance-name contains <WORD> | Optional. Specifies the selected Bonjour service's instance name. When specified, the Bonjour service discovery queries contain the instance name. of the service to be discovered.<br>This option is useful especially in large distributed, enterprise networks. Use it to create different instances of a Bonjour service for the different organizations or departments (VLANS) within your network. Creating instances allows you to advertise specific service instances for a specific set of VLANs, instead of advertising top-level Bonjour Services to various allocated VLAN(s).<br>• contains <WORD> – Specify the instance name. You can either directly specify the string value to be used as a match criteria, or use a string alias (for example, $BONJOUR-STRING) to identify the string to match. If using a string alias, ensure that it is existing and configured. For information on configuring a string alias, see *alias*. |
| service-vlans <WORD> | Optional. Configures a VLAN or a list of VLANs on which the selected service is discoverable. When specified, Bonjour discovery queries are delivered to all clients on the specified VLANs. Applicable only if enabling Bonjour Services discovery on local VLANs. |

- `allow-service <BONJOUR-SERVICE-NAME> tunneled {instance-name contains <WORD>}`

| | |
|---|---|
| allow-service <BONJOUR-SERVICE-NAME> | Configures the services that can be discovered by the Bonjour gateway. And also configures the VLANs on which the selected services can be discovered.<br>• <BONJOUR-SERVICE-NAME> – You can either select the Bonjour Services from a set of system-provided, pre-defined Apple services, or use an existing alias to define a service not available in the predefined list.<br>The predefined Apple services available are: Afp, AirPlay, AirPort, AirPrint, AirTunes, AppleTimeMachine, Chromecast, Daap, HomeSharing, Printer, and Scanner.<br>Use the <WORD> keyword to define a service not included in the system-provided, predefine list. |
| tunneled | Select to enable the discovery of the selected Bonjour Services on tunneled VLANs |
| instance-name contains <WORD> | Optional. Adds a Bonjour Service instance name. If you have a large enterprise network, use this option to create different Bonjour Service instances for the different organizations or departments (VLANS) within your network. Creating instances allows you to advertise specific service instances for a specific set of VLANs, instead of advertising top-level Bonjour Services to various allocated VLAN(s).<br>• contains <WORD> – Specify the sub-string to match. You can either directly specify the string value to be used as a match criteria, or use a string alias (for example, $BONJOUR-STRING) to identify the string to match. If using a string alias, ensure that it is existing and configured. For information on configuring aliases, see *alias*. |

**Example**

```
nx9500-6C8809(config-bonjour-gw-discovery-policy-test)#allow-service Afp local

nx9500-6C8809(config-bonjour-gw-discovery-policy-test)#allow-service Printer lo
cal instance-name contains $Bonjour_Service service-vlans 1,2

nx9500-6C8809(config-bonjour-gw-discovery-policy-test)#show context
bonjour-gw-discovery-policy test
 allow-service Printer local service-vlans 1-2 instance-name contains
$Bonjour_Service
 allow-service Afp local
nx9500-6C8809(config-bonjour-gw-discovery-policy-test)#

Following example configures the string alias named $Bonjour_Service:

nx9500-6C8809(config)#alias string $Bonjour_Service admin
nx9500-6C8809(config)#commit
nx9500-6C8809(config)#show context include-factory | include alias string
alias string $Bonjour_Service admin
nx9500-6C8809(config)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes or modifies this Bonjour Gateway Discovery Policy settings |

### 4.1.28.2.2 no

*bonjour-gateway-discovery-policy-mode commands*

Removes or modifies the Bonjour Gateway Discovery policy settings

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
no allow-service <BONJOUR-SERVICE-NAME> [local|tunneled] {service-vlans <WORD>}
```

**Parameters**

- `no allow-service <BONJOUR-SERVICE-NAME> [local|tunneled] {service-vlans <WORD>}`

| | |
|---|---|
| no <parameters> | Removes allow-service rules in the selected Bonjour GW Discovery policy, based on the parameters passed |

**Example**

```
The following example shows the Bonjour GW Discovery policy 'test' settings before
the 'no' command is executed:

nx9500-6C8809(config-bonjour-gw-discovery-policy-test)#show context
bonjour-gw-discovery-policy test
 allow-service Printer local service-vlans 1-2 instance-name contains
$Bonjour_Service
 allow-service Afp local
nx9500-6C8809(config-bonjour-gw-discovery-policy-test)#

nx9500-6C8809(config-bonjour-gw-discovery-policy-test1)#no allow-service Afp
local

The following example shows the Bonjour GW Discovery policy 'test' settings after
the 'no' command was executed:

nx9500-6C8809(config-bonjour-gw-discovery-policy-test)#show context
bonjour-gw-discovery-policy test
 allow-service Printer local service-vlans 1-2 instance-name contains
$Bonjour_Service
nx9500-6C8809(config-bonjour-gw-discovery-policy-test)#
```

## 4.1.29 bonjour-gw-forwarding-policy

*Global Configuration Commands*

Configures a Bonjour GW Forwarding policy. When configured and applied on the controller, the policy defines the service VLANs (the VLANs on which Bonjour services are running) and client VLANs where clients are present. All Bonjour responses from service VLANs are forwarded to client VLANs. A maximum of 2 (two) policies can be created on a wireless controller or service platform. And only 1 (one) policy can be created on an access point.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
bonjour-gw-forwarding-policy <POLICY-NAME>
```

**Parameters**

- `bonjour-gw-forwarding-policy <POLICY-NAME>`

| | |
|---|---|
| <POLICY-NAME> | Specify the Bonjour GW Forwarding policy name. If the policy does not exist, it is created.<br>To receive Bonjour service responses from specific VLANs, specify the VLAN IDs. In the Bonjour GW Forwarding policy configuration mode, provide a list of VLAN IDs from which Bonjour responses can be received (format: 10-20, 25, 30-35). And then specify the list of client VLANs that can access Bonjour services.<br>Execute the bonjour-gw-discovery-policy command to define the Bonjour services allowed on local and tunneled VLANs.<br>To associate a Bonjour GW Forwarding policy with a device or profile, in the profile/device configuration mode, execute the *use > bonjour-gw-forwarding-policy > <POLICY-NAME>* command. For more information, see *use*. |

**Example**

```
rfs6000-81742D(config)#bonjour-gw-forwarding-policy TestPolicy
rfs6000-81742D(config-bonjour-gw-forwarding-policy-TestPolicy)#?
 commands:
  forward-bonjour-response  Forwards bonjour service response across vlans
  no                        Negate a command or set its defaults

  clrscr                    Clears the display screen
  commit                    Commit all changes made in this session
  do                        Run commands from Exec mode
  end                       End current mode and change to EXEC mode
  exit                      End current mode and down to previous mode
  help                      Description of the interactive help system
  revert                    Revert changes
  service                   Service Commands
  show                      Show running system information
  write                     Write running configuration to memory or terminal

rfs6000-81742D(config-bonjour-gw-forwarding-policy-TestPolicy)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing Bonjour GW Forwarding policy |

## 4.1.30 bonjour-gw-query-forwarding-policy

*Global Configuration Commands*

Configures a Bonjour GW Query Forwarding policy and enters its configuration mode. When created and applied, this policy enables forwarding of Bonjour queries across VLANs.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
bonjour-gw-query-forwarding-policy <POLICY-NAME>
```

**Parameters**

- `bonjour-gw-query-forwarding-policy <POLICY-NAME>`

| | |
|---|---|
| <POLICY-NAME> | Specify the Bonjour GW Query Forwarding policy name. If the policy does not exist, it is created.<br>In the Bonjour GW Query Forwarding policy configuration mode, specify the 'from' and 'to' VLAN(s). The *from-vlans* option configures the VLAN(s) that are the source of the Bonjour queries. The *to-vlans* option configures the destination VLAN(s) that can access the Bonjour queries.<br>To associate a Bonjour GW Query Forwarding policy with a device or profile, in the profile/device configuration mode, execute the *use > bonjour-gw-query-forwarding-policy > <POLICY-NAME>* command. For more information, see *use*. |

**Example**

```
rfs6000-81742D(config)#bonjour-gw-query-forwarding-policy TestPolicy
rfs6000-81742D(config-bonjour-gw-query-forwarding-policy-test)#?
(config-bonjour-gw-query-forwarding-policy) commands:
  forward-bonjour-query  Forwards bonjour query across vlans
  no                     Negate a command or set its defaults

  clrscr                 Clears the display screen
  commit                 Commit all changes made in this session
  do                     Run commands from Exec mode
  end                    End current mode and change to EXEC mode
  exit                   End current mode and down to previous mode
  help                   Description of the interactive help system
  revert                 Revert changes
  service                Service Commands
  show                   Show running system information
  write                  Write running configuration to memory or terminal

rfs6000-81742D(config-bonjour-gw-query-forwarding-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing Bonjour GW Query Forwarding policy |

## 4.1.31 captive portal

*Global Configuration Commands*

The following table lists the commands that enable you to create a new captive portal policy and enter its configuration mode:

**Table 4.10** *Captive-Portal Config Commands*

| Command | Description | Reference |
|---|---|---|
| *captive-portal* | Creates a new captive portal and enters its configuration mode | *page 4-94* |
| *captive-portal-mode commands* | Summarizes captive portal configuration commands | *page 4-96* |

### 4.1.31.1 captive-portal

*captive portal*

Configures a captive portal policy and enters its configuration mode. Once created and configured, use the captive portal policy in the WLAN context, and in the device/profile contexts of the access point or controller hosting the captive portal server.

A captive portal provides secure access using a standard Web browser. Captive portals provide authenticated access by capturing and re-directing a wireless user's Web browser session to a captive portal login page where the user must enter valid credentials to access to the wireless network. Once logged into the captive portal, additional Acknowledgment, Agreement, Welcome, No Service, and Fail pages provide the administrator options to customize the screen flow and user appearance.

Captive portals are recommended for providing guests or visitors authenticated access to network resources when 802.1X EAP is not a viable option. Captive portal authentication does not provide end-user data encryption, but it can be used with static WEP, WPA-PSK or WPA2-PSK encryption.

Authentication for captive portal access requests is performed using a username and password pair, authenticated by an integrated RADIUS server. Authentication for private network access is conducted either locally on the requesting wireless client, or centrally at a data center.

Captive portals use a Web provisioning tool to create guest user accounts directly on the controller, service platform, or access point. The connection medium defined for the Web connection is either HTTP or HTTPS. Both HTTP and HTTPS use a request and response procedure to disseminate information to and from requesting wireless clients.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
captive-portal <CAPTIVE-PORTAL-NAME>
```

**Parameters**

- `captive-portal <CAPTIVE-PORTAL-NAME>`

| | |
|---|---|
| <CAPTIVE-PORTAL-NAME> | Specify the captive portal name. If a captive portal with the specified name does not exist, it is created. |

**Example**

```
rfs6000-81742D(config)#captive-portal test
rfs6000-81742D(config-captive-portal-test)#?
Captive Portal Mode commands:
access-time                 Allowed access time for the client. Used when
                              there is no session time in radius response
  access-type               Access type of this captive portal
  accounting                Configure how accounting records are created for
                              this captive portal policy
  bypass                    Bypass captive portal
  connection-mode           Connection mode for this captive portal
  custom-auth               Custom user information
  data-limit                Enforce data limit for clients
  inactivity-timeout        Inactivity timeout in seconds. If a frame is not
                              received from client for this amount of time,
                              then current session will be removed
  ipv6                      Internet Protocol version 6 (IPv6)
  localization              Configure the FQDN address to get the
                              localization parameters for the client
  logout-fqdn               Configure the FQDN address to logout the session
                              from client
  no                        Negate a command or set its defaults
  oauth                     OAuth 2.0 authentication configuration
  php-helper                Configure the captive portal to use a server for
                              help with php
  post-authentication-vlan  Configure post authentication vlan for captive
                              portal users
  radius-vlan-assignment    Enable radius vlan assignment for captive portal
                              users
  redirection               Configure connection redirection parameters
  report-loyalty-application Report customer loyalty application presence in
                              clients
  server                    Configure captive portal server parameters
  simultaneous-users        Particular username can only be used by a
                              certain number of MAC addresses at a time
  terms-agreement           User needs to agree for terms and conditions
  use                       Set setting to use
  webpage                   Configure captive portal webpage parameters
  webpage-auto-upload       Enable automatic upload of internal and advanced
                              webpages
  webpage-location          The location of the webpages to be used for
                              authentication. These pages can either be hosted
                              on the system or on an external web server.
  welcome-back              Welcome back page settings

  clrscr                    Clears the display screen
  commit                    Commit all changes made in this session
  do                        Run commands from Exec mode
  end                       End current mode and change to EXEC mode
  exit                      End current mode and down to previous mode
  help                      Description of the interactive help system
  revert                    Revert changes
  service                   Service Commands
  show                      Show running system information
  write                     Write running configuration to memory or
                              terminal

rfs6000-81742D(config-captive-portal-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing captive portal |

### 4.1.31.2 captive-portal-mode commands

*captive portal*

The following table summarizes captive portal configuration mode commands:

**Table 4.11** *Captive-Portal-Mode Commands*

| Command | Description | Reference |
|---|---|---|
| *access-time* | Defines a client's access time. It is used when no session time is defined in the RADIUS response. | *page 4-98* |
| *access-type* | Configures a captive portal's access type | *page 4-99* |
| *accounting* | Enables a captive portal's accounting records | *page 4-100* |
| *bypass* | Enables bypassing of captive portal detection requests from wireless clients | *page 4-102* |
| *connection-mode* | Configures a captive portal's connection mode | *page 4-103* |
| *custom-auth* | Configures custom user information | *page 4-104* |
| *data-limit* | Enforces data limit on captive portal clients | *page 4-105* |
| *inactivity-timeout* | Defines an inactivity timeout in seconds | *page 4-106* |
| *ipv6* | Configures the IPv6 address of the internal captive portal server | *page 4-107* |
| *localization* | Configures an FQDN address string that enables the client to receive localization parameters. This command also allows the configuration of a response message. | *page 4-108* |
| *logout-fqdn* | Clears the logout FQDN address | *page 4-110* |
| *no* | Reverts the selected captive portal's settings to default | *page 4-111* |
| *oauth* | Enables OAuth-based authentication support on the captive portal. When enabled, OAuth allows captive-portal users to sign in to guest WLANs using their Facebook or Google credentials. | *page 4-113* |
| *php-helper* | Configures a PHP helper to serve the captive portal's PHP splash pages to guest users using social-media to login to the captive portal. | *page 4-115* |
| *post-authentication-vlan* | Assigns a post authentication RADIUS VLAN for this captive portal's users | *page 4-117* |
| *radius-vlan-assignment* | Assigns a RADIUS VLAN for this captive portal | *page 4-118* |
| *redirection* | Enables redirection of client connections to specified destination ports | *page 4-119* |
| *report-loyalty-application* | Enables detection of captive portal client's *loyalty application* presence and stores this information in the captive portal's user database | *page 4-120* |
| *server* | Configures the captive portal server settings | *page 4-121* |
| *simultaneous-users* | Specifies a username used by a MAC address pool | *page 4-123* |
| *terms-agreement* | Enforces the user to agree to terms and conditions (included in login page) for captive portal access | *page 4-124* |
| *use* | Associates a AAA policy and a DNS whitelist with a captive portal | *page 4-125* |
| *webpage* | Configures captive portal Web page settings | *page 4-127* |

**Table 4.11** *Captive-Portal-Mode Commands*

| Command | Description | Reference |
|---|---|---|
| *webpage-auto-upload* | Enables automatic upload of advanced Web pages on a captive portal | *page 4-135* |
| *webpage-location* | Specifies the location of Web pages used for captive portal authentication | *page 4-136* |
| *welcome-back* | Enables the provision of direct Internet access to once-registered, captive-portal guest users on subsequent log-ins | *page 4-137* |
| *configuring device registration with dynamic VLAN assignment* | Documents configuration details required to enable device registration with dynamic VLAN assignment in a multi-vendor environment | *page 4-139* |
| *configuring WeChat Wi-Fi hotspot support in WiNG captive portal* | Documents configuration details required to support the WeChat WiFi hotspot, so that WeChat users, on their first connect to a WiNG access point, can automatically authenticate with the WeChat server through an intermediate server | *page 4-141* |
| *configuring ExtremeGuest captive-portal* | Documents the basic configurations required to deploy an ExtremeGuest setup | *page 4-143* |

### 4.1.31.2.1 access-time

*captive-portal-mode commands*

Defines the permitted access time for a client. It is used when no session time is defined in the RADIUS response.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
access-time <10-10080>
```

**Parameters**

- `access-time <10-10080>`

| | |
|---|---|
| access-time <10-10080> | Defines the duration wireless clients are allowed access to the Internet using this captive portal policy<br>• <10-10080> – Specify a value from 10 - 10080 minutes. The default is 1440 minutes. |

**Example**

```
rfs6000-81742D(config-captive-portal-test)#access-time 35

rfs6000-81742D(config-captive-portal-test)#show context
captive-portal test
 access-time 35
rfs6000-81742D(config-captive-portal-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Reverts to the default permitted access time (1440 minutes) |

### 4.1.31.2.2 access-type

*captive-portal-mode commands*

Defines the captive portal's access type. The authentication scheme configured here is applied to wireless clients using this captive portal.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

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

**Parameters**

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

| | |
|---|---|
| custom-auth-radius | Specifies the custom user information used for authentication (RADIUS lookup of given information, such as name, e-mail address, telephone, etc.). When configured, accessing clients are required to provide a 1-32 character lookup data string used to authenticate their credentials.<br>When selecting this option, use the custom-auth command to configure the required user information. |
| logging | Provides users access without authentication. The system logs access details of users allowed access. |
| no-auth | Defines no authentication required for a guest (guest is redirected to welcome message). Provides users access to the captive portal without authentication. |
| radius | Enables RADIUS authentication for wireless clients. Provides captive portal access to successfully authenticated users only. This is the default setting. |
| registration | Enables captive portal's clients to self register in the captive portal's database. When configured, a requesting client's user credentials require authentication locally or through social media credential exchange and validation.<br>If enabled, use the *webpage > internal > registration > field* command to customize the registration page. If not customized, the default, built-in registration Web page is displayed. |

**Example**

```
rfs6000-81742D(config-captive-portal-test)#access-type logging

rfs6000-81742D(config-captive-portal-test)#show context
captive-portal test
 access-type logging
 access-time 35
rfs6000-81742D(config-captive-portal-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the captive portal access type or reverts to default (radius) |

### 4.1.31.2.3 accounting

*captive-portal-mode commands*

Enables support for accounting messages for this captive portal

When enabled, accounting for clients entering and exiting the captive portal is initiated. Accounting is the method of collecting and sending security server information for billing, auditing, and reporting user data. This data includes information, such as start and stop times, executed commands (such as PPP), number of packets and number of bytes transmitted, etc. Accounting enables tracking of captive portal services consumed by clients.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
accounting [radius|syslog]

accounting radius

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

**Parameters**

- `accounting radius`

| | |
|---|---|
| radius | Enables support for RADIUS accounting messages. When enabled, this option uses an external RADIUS resource for AAA accounting. This option is disabled by default. |

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

| | |
|---|---|
| syslog host <IP/ HOSTNAME> | Enables support for syslog accounting messages. When enabled, data relating to wireless client usage of remote access services is logged on the specified external syslog resource. This information assists in differentiating between local and remote users. Remote user information can be archived to an external location for periodic network and user administration. This option is disabled by default.<br>• host <IP/HOSTNAME> – Specifies the destination where accounting messages are sent. Specify the destination's IP address or hostname. |
| port <1-65535> | Optional. Specifies the syslog server's listener port<br>• <1-65535> – Specify the UDP port from 1- 65535. The default is 514. |
| proxy-mode [none\| through-controller\| through-rf-domain-manager] | Optional. Specifies the mode of proxying the syslog server<br>• none – Accounting messages are sent directly to the syslog server<br>• through-controller – Accounting messages are sent through the controller configuring the device<br>• through-rf-domain-manager – Accounting messages are sent through the local RF Domain manager |

**Example**

```
rfs6000-81742D(config-captive-portal-test)#accounting syslog host 172.16.10.13
port 1

rfs6000-81742D(config-captive-portal-test)#show context
captive-portal test
 access-type logging
 access-time 35
 accounting syslog host 172.16.10.13 port 1
rfs6000-81742D(config-captive-portal-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables accounting records for this captive portal |

### 4.1.31.2.4 bypass

*captive-portal-mode commands*

Enables bypassing of captive portal detection requests from wireless clients

Certain devices, such as Apple IOS devices send *Captive Network Assistant* (CNA) requests to detect existence of captive portals. When enabled, the bypass option does not allow CNA requests to be redirected to the captive portal pages.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
bypass captive-portal-detection
```

**Parameters**

- `bypass captive-portal-detection`

| | |
|---|---|
| bypass captive-portal-detection | Bypasses captive portal detection requests |

**Example**

```
rfs4000-229D58(config-captive-portal-test)#bypass captive-portal-detection

rfs4000-229D58(config-captive-portal-test)#show context
captive-portal test
 bypass captive-portal-detection
rfs4000-229D58(config-captive-portal-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables bypassing of captive portal detection requests |

### 4.1.31.2.5 connection-mode

*captive-portal-mode commands*

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

Both HTTP and HTTPS use the same *Uniform Resource Identifier* (URI), so controller and client resources can be identified. However, the use of HTTPS is recommended, as it affords controller and client transmissions some measure of data protection HTTP cannot provide.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

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

**Parameters**

- `connection-mode [http|https]`

| | |
|---|---|
| http | Sets HTTP as the default connection mode. This is the default setting. |
| https | Sets HTTPS as the default connection mode<br>HTTPS is a more secure version of HTTP, and uses encryption while sending and receiving requests. |

**Example**

```
rfs6000-81742D(config-captive-portal-test)#connection-mode https

rfs6000-81742D(config-captive-portal-test)#show context
captive-portal test
 access-type logging
 access-time 35
 connection-mode https
 accounting syslog host 172.16.10.13 port 1
rfs6000-81742D(config-captive-portal-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes this captive portal's connection mode |

### 4.1.31.2.6 custom-auth

*captive-portal-mode commands*

Configures custom user information

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
custom-auth info <LINE>
```

**Parameters**

- `custom-auth info <LINE>`

| | |
|---|---|
| info <LINE> | Configures information used for RADIUS lookup when custom-auth RADIUS access type is configured<br>• <LINE> – Guest data needs to be provided. Specify the name, e-mail address, and telephone number of the user. |

**Example**

```
rfs6000-81742D(config-captive-portal-test)#custom-auth info bob
bob@examplecompany.com

rfs6000-81742D(config-captive-portal-test)#show context
captive-portal test
 access-type logging
 access-time 35
 custom-auth info bob bob@examplecompany.com
 connection-mode https
 accounting syslog host 172.16.10.13 port 1
rfs6000-81742D(config-captive-portal-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes custom user information configured with this captive portal |

### 4.1.31.2.7 data-limit

*captive-portal-mode commands*

Enforces data transfer limits on captive portal clients. This feature enables the tracking and logging of user usage. Users exceeding the allowed bandwidth are restricted from the captive portal.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
data-limit <1-102400> {action [log-and-disconnect|log-only]}
```

**Parameters**

- `data-limit <1-102400> {action [log-and-disconnect|log-only]}`

| | |
|---|---|
| data-limit <1-102400> | Sets a captive portal client's data transfer limit in megabytes. This limit is applicable for both upstream and downstream data transfer.<br>• <1-102400> – Specify a value from 1 - 102400 MB. |
| action [log-and-disconnect\| log-only] | Optional. Specifies the action taken when a client exceeds the configured data limit. The options are:<br>• log-and-disconnect – When selected, an entry is added to the log file any time a captive portal client exceeds the data limit, and the client is disconnected.<br>• log-only – When selected, an entry is added to the log file any time a captive portal client exceeds the data limit. the client, however, remains connected to the captive portal. This is the default setting. |

**Example**

```
rfs6000-81742D(config-captive-portal-test)#data-limit 200 action log-and-
disconnect

rfs6000-81742D(config-captive-portal-test)#show context
captive-portal test
 data-limit 200 action log-and-disconnect
rfs6000-81742D(config-captive-portal-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes data limit enforcement for captive portal clients |

### 4.1.31.2.8 inactivity-timeout

*captive-portal-mode commands*

Defines the inactivity timeout in seconds. If a frame is not received from a client for the specified interval the current session is terminated.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
inactivity-timeout <60-86400>
```

**Parameters**

- `inactivity-timeout <60-86400>`

| | |
|---|---|
| <60-86400> | Defines the interval for which a captive portal session is kept alive without receiving a frame from the client. The session is automatically terminated once this interval is over.<br>• <60-86400> – Specify a value from 60 - 86400 seconds. The default is 10 minutes or 600 seconds. |

**Example**

```
rfs6000-81742D(config-captive-portal-test)#inactivity-timeout 750

rfs6000-81742D(config-captive-portal-test)#show context
captive-portal test
 access-type logging
 access-time 35
 custom-auth info bob bob@examplecompany.com
 connection-mode https
 inactivity-timeout 750
 accounting syslog host 172.16.10.13 port 1
rfs6000-81742D(config-captive-portal-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the client inactivity-timeout configured with this captive portal |

### 4.1.31.2.9 ipv6

*captive-portal-mode commands*

Configures the internal captive portal server's (running on the centralized mode) IPv6 address. If using centralized server mode, use this option to define the controller, service platform, or access point resource's (hosting the captive portal) IPv6 address. For information on configuring the server mode, see *server*.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ipv6 server host <IPv6>
```

**Parameters**

- `ipv6 server host <IPv6>`

| | |
|---|---|
| ipv6 server host <IPv6> | Configures the IPv6 address of the internal captive portal server<br>• <IPv6> – Specify the captive portal server's global IPv6 address. |

**Example**

```
rfs6000-81742D(config-captive-portal-test2)#ipv6 server host
2001:10:10:10:6d:33:fa:8b

rfs6000-81742D(config-captive-portal-test2)#show context
captive-portal test2
 access-type OAuth
 ipv6 server host 2001:10:10:10:6d:33:fa:8b
 OAuth client-id Google TechPubs.printer.google.com
rfs6000-81742D(config-captive-portal-test2)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the captive portal server's IPv6 address |

### 4.1.31.2.10 localization

*captive-portal-mode commands*

Configures an FQDN address string that enables the client to receive localization parameters. Use this option to add a URL to trigger a one-time redirect on demand. The defined URL is triggered from a mobile application to derive location information from the wireless network so an application can be localized to a particular store or region.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
localization [fqdn <WORD>|response <WORD>]
```

**Parameters**

- `localization [fqdn <WORD>|response <WORD>]`

| | |
|---|---|
| localization | Configures an FQDN address string that enables the client to receive localization parameters. This command also allows the configuration of a response message. |
| fqdn <WORD> | Configures the FQDN address string, which is used to obtain localization parameters for the captive portal's client.<br>• <WORD> – Specify the FQDN address string. For example, local.guestaccess.com |
| response <WORD> | Configures a message, which is sent back to the client in response to the client's localization HTTP requests<br>• <WORD> – Specify the response message (should not exceed 512 characters in length). The following built-in query tags can be included in the response message:<br>WING_TAG_CLIENT_IP' -Captive portal client IPv4 address<br>'WING_TAG_CLIENT_MAC' - Captive portal client MAC address<br>'WING_TAG_WLAN_SSID ' - Captive portal client WLAN ssid<br>'WING_TAG_AP_MAC' - Captive portal client AP MAC address<br>'WING_TAG_AP_NAME' - Captive portal client AP Name<br>'WING_TAG_RF_DOMAIN' - Captive portal client RF Domain<br>'WING_TAG_USERNAME' - Captive portal authentication username<br>'WING_TAG_USERTYPE' - Captive portal usertype (new/return/refresh) Example:-<br><local><site>WING_TAG_RF_DOMAIN</site><ap>WING_TAG_AP_NAME</ap></local |

**Example**

```
nx9500-6C8809(config-captive-portal-test)#localization fqdn local.guestaccess.com

nx9500-6C8809(config-captive-portal-test)#localization response
<local><site>SJExtreme</site><ap>ap8132-74B45C</ap><user>Bob</user><local>

nx9500-6C8809(config-captive-portal-TechPubsNew)#show context
captive-portal TechPubsNew
 webpage internal registration field city type text enable label "City" placeholder
"Enter City"
 webpage internal registration field street type text enable label "Address"
placeholder "123 Any Street"
 webpage internal registration field name type text enable label "Full Name"
placeholder "Enter First Name, Last Name"
 webpage internal registration field zip type number enable label "Zip" placeholder
"Zip"
 webpage internal registration field via-sms type checkbox enable title "SMS
Preferred"
 webpage internal registration field mobile type number enable label "Mobile"
placeholder "Mobile Number with Country code"
 webpage internal registration field age-range type dropdown-menu enable label "Age
Range" title "Age Range"
 webpage internal registration field email type e-address enable mandatory label
"Email" placeholder "you@domain.com"
 webpage internal registration field via-email type checkbox enable title "Email
Preferred"
 localization fqdn local.guestaccess.com
 localization response <local><site>SJExtreme</site><ap>ap8132-74B45C</
ap><user>Bob</user><local>
nx9500-6C8809(config-captive-portal-TechPubsNew)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the FQDN address string and response message configured on a captive portal for localization |

### 4.1.31.2.11 logout-fqdn

*captive-portal-mode commands*

Configures the *Fully Qualified Domain Name* (FQDN) address to logout of the session from the client

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
logout-fqdn <WORD>
```

**Parameters**

- `logout-fqdn <WORD>`

| | |
|---|---|
| logout-fqdn <WORD> | Configures the FQDN address used to logout<br>• <WORD> – Provide the FQDN address (for example, logout.guestaccess.com). |

**Example**

```
rfs6000-81742D(config-captive-portal-test)#logout-fqdn logout.testuser.com

rfs6000-81742D(config-captive-portal-test)#show context
captive-portal test
 logout-fqdn logout.testuser.com
rfs6000-81742D(config-captive-portal-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Clears the logout FQDN address |

### 4.1.31.2.12 no

*captive-portal-mode commands*

The `no` command reverts the selected captive portal's settings or resets settings to default.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
no [access-time|access-type|accounting|bypass|connection-mode|custom-auth|
data-limit|inactivity-timeout|ipv6|localization|logout-fqdn|oauth|php-helper|
post-authentication-vlan|radius-vlan-assignment|redirection|
report-loyalty-application|server|simultaneous-users|terms-agreement|use|
webpage|webpage-auto-upload|webpage-location|welcome-back]

no [access-time|access-type|connection-mode|data-limit|inactivity-timeout|
logout-fqdn|post-authentication-vlan|radius-vlan-assignment|report-loyalty-
application|simultaneous-users|terms-agreement|webpage-auto-upload|
webpage-location]

no accounting [radius|syslog]

no bypass captive-portal-detection

no custom-auth info

no ipv6 server host

no localization [fqdn|response]

no oauth {client-id}

no php-helper

no redirection ports

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

no use [aaa-policy|dns-whitelist]

no webpage external [acknowledgement|agreement|fail|login {post}|no-service|
registration|welcome]

no webpage internal [acknowledgement|agreement|fail|login|no-service|org-name|
org-signature|registration|welcome]

no webpage internal [org-name|org-signature]

no webpage internal [acknowledgment|agreement|fail|login|no-service] [body-
background-color|body-font-color|description|footer|header|main-logo|org-
background-color|org-font-color|small-logo|title]

no webpage internal registration [body-background-color|body-font-color|
description|field|footer|header|main-logo|org-background-color|org-font-
color|small-logo|title]
```

```
no webpage internal registration field [age-range|city|country|custom <FIELD-
NAME>|disclaimer|dob|email|gender|member|mobile|name|optout|street|via-email|
via-sms|zip] {enable}

no webpage internal welcome [body-background-color|body-font-color|description|
footer|header|main-logo|org-background-color|org-font-color|small-logo|title|
use-external-success-url]

no welcome-back pass-through
```

**Parameters**

- no <PARAMETERS>

| | |
|---|---|
| no <PARAMETERS> | Removes or resets this captive portal's settings, based on the parameters passed. |

**Example**

The following example shows the captive portal 'test' settings before the 'no' commands are executed:

```
rfs6000-81742D(config-captive-portal-test)#show context
captive-portal test
 access-type logging
 access-time 35
 custom-auth info bob bob@examplecompany.com
 connection-mode https
 inactivity-timeout 750
 accounting syslog host 172.16.10.13 port 1
rfs6000-81742D(config-captive-portal-test)#

rfs6000-81742D(config-captive-portal-test)#no accounting syslog
rfs6000-81742D(config-captive-portal-test)#no access-type
```

The following example shows the captive portal 'test' settings after the 'no' commands are executed:

```
rfs6000-81742D(config-captive-portal-test)#show context
captive-portal test
 access-time 35
 custom-auth info bob bob@examplecompany.com
 connection-mode https
 inactivity-timeout 750
rfs6000-81742D(config-captive-portal-test)#
```

### 4.1.31.2.13 oauth

*captive-portal-mode commands*

Enables OAuth-driven Google and/or Facebook authentication on captive portals that use internal Web pages.

To enable Google and Facebook captive-portal authentication:

- Enforce captive-portal authentication on the WLAN to which wireless-clients associate. For information, see *captive-portal-enforcement*.
- Set captive-portal Web page location to internal. For more information, see *webpage-location*.
- Register your captive-portal individually on Google/FaceBook APIs and generate a *client-id* and *client-secret*. The client-ids retrieved during registration are the IDs for the WiNG application running on the access point/controller. The WiNG application uses these client-ids to access the Google and Facebook Auth APIs, and authenticate the guest client on behalf of the user.

If enabling OAuth-driven Google and/or Facebook authentication on the captive portal, use this command to configure the Google/Facebook client-ids. Once enabled, the captive portal landing page, displayed on the client's browser, provides the Facebook and Google login buttons.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
oauth

oauth client-id [facebook|google] <WORD>
```

**Parameters**

- `oauth`

| | |
|---|---|
| oauth | Execute this command without the associated keywords to enable OAuth on this captive-portal. If enabling OAuth, ensure the captive-portal Web page location is configured as advanced or external. |

- `oauth client-id [facebook|google] <WORD>`

| | |
|---|---|
| oauth client-id [facebook\|google] <WORD> | Configures the client-ids retrieved from the Google and Facebook API manager portals during registration<br>• facebook – Configures the Facebook API client-id (is a 15 digit entity)<br>• google – Configures the Google API client-id (is a 12 digit number)<br>  • <WORD> – Provide the Facebook/Google client-id.<br>If the captive-portal Web page location is advanced or external, and you are enabling OAuth support, you need not configure the client-id. In such a scenario, the client-id is configured through the EGuest server UI and not the WiNG CLI. |

**Example**

```
nx7500-6DCD39(config-captive-portal-test2)#OAuth

nx7500-6DCD39(config-captive-portal-test2)#OAuth client-id Google
xxxxxxxxxxxx.apps.googleusercontent.com Facebook yyyyyyyyyyyyyyy

nx7500-6DCD39(config-captive-portal-test2)#show context
captive-portal test2
 server host guest.social.com
  oauth
  oauth client-id Google xxxxxxxxxxxx.apps.googleusercontent.com Facebook
yyyyyyyyyyyyyyy

nx7500-6DCD39(config-captive-portal-test)#
```

In the above example:

- xxxxxxxxxxxx - Is the 12 digit numeric part of your Google client-id.
- yyyyyyyyyyyyyyy - Is the 15 digit Facebook client-id

**Related Commands**

| | |
|---|---|
| *no* | Removes all OAuth client identities configured for this captive portal |

### 4.1.31.2.14 php-helper

*captive-portal-mode commands*

Configures a PHP helper to serve the PHP splash pages to guest users logging in to the captive portal using social-media credentials. Configure a PHP helper only if the following criteria are fulfilled:

- OAuth-based authentication is enabled on the captive portal.
- The captive-portal server mode is “self”.
- The access point, hosting the captive-portal server, has low memory space (for example, the AP6511, AP6521, AP6522, AP6532, and AP7502 model access points).
- A hotspot server, hosting the captive-portal PHP splash pages, is up and running.

The WiNG software introduces HybridAuth support on captive portals. HybridAuth is an open-source, social-sign on PHP Library. In addition to Google and Facebook, it allows a variety of third-party social authentications, such as LinkedIn, Twitter, Live, Yahoo, OpenID, etc. However, HybridAuth uses space-consuming PHP splash pages that cannot be loaded on access points with low memory space. These access points can only serve the initial landing page, where guests clicking on a social login button are redirected by the *php-helper* to a PHP page hosted on the *PHP-helper.*

To create PHP splash pages, use the splash template configuration tool available on the *ExtremeGuest* (EGuest) dashboard. Upload the generated tar to both the hotspot server and the php helper. Note, the EGuest dashboard can be launched from the WiNG controller (NX9500/NX9600/VX9000) enabled as the EGuest server.

For more information on enabling the EGuest server, see *eguest-server (VX9000 only)*.

For more information on configuring an EGuest captive portal, see *configuring ExtremeGuest captive-portal*.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
php-helper [controller|domain-manager]

php-helper controller <IP/HOSTNAME> hosting-vlan-interface <0-4096>

php-helper domain-manager <IP/HOSTNAME>
```

**Parameters**

- `php-helper controller <IP/HOSTNAME> hosting-vlan-interface <0-4094>]`

| | |
|---|---|
| php-helper | Configures the php-helper parameters |
| controller <IP/ HOSTNAME> | Configures the controller adopting the captive-portal access point as the php-helper<br>• <IP/HOSTNAME> – Specify the adopting controller’s IP address or host name. |
| hosting-vlan-interface <0-4096> | Optional. Configures the VLAN on which the php-helper is reachable<br>• <0-4096> – Specify the VLAN hosting the php-helper from 0 - 4096. |

- `php-helper domain-manager <IP/HOSTNAME>`

| | |
|---|---|
| php-helper | Configures the php-helper parameters |
| domain-manager <IP/HOSTNAME> | Configures the captive-portal access point's RF Domain manager as the php-helper<br>• <IP/HOSTNAME> – Specify the RF Domain manager's IP address or host name. |

**Example**

To enable php-helper configure the following parameters in the captive-portal context:

```
ap6532-3163A4(config-captive-portal-php-helper)#oauth

ap6532-3163A4(config-captive-portal-php-helper)#php-helper controller nx9500-
6C8809

ap6532-3163A4(config-captive-portal-php-helper)#server mode self

ap6532-3163A4(config-captive-portal-php-helper)#server host cpsocial.extreme.com
```

Note, when configuring the server, specify the server's hostname and not the IP address, because some social media do not allow IP address as a redirect URI.

```
ap6532-3163A4(config-captive-portal-php-helper)#show running-config captive-
portal php-helper
captive-portal php-helper
 server host cpsocial.extreme.com
 php-helper controller nx9500-6C8809
 oauth
 webpage internal registration field city type text enable label "City" placeholder
"Enter City"
 webpage internal registration field street type text enable label "Address"
placeholder "123 Any Street"
 webpage internal registration field name type text enable label "Full Name"
placeholder --More--
ap6532-3163A4(config-captive-portal-php-helper)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the PHP helper configuration |

### 4.1.31.2.15 post-authentication-vlan

*captive-portal-mode commands*

Configures the VLAN that is assigned to this captive portal's users upon successful authentication

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
post-authentication-vlan [<1-4096>|<VLAN-ALIAS>]
```

**Parameters**

- `post-authentication-vlan [<1-4096>|<VLAN-ALIAS>]`

| | |
|---|---|
| post-authentication-vlan [<1-4096>\| <VLAN-ALIAS>] | Configures the post authentication VLAN. The VLAN specified here is assigned to this captive portal's users after they have authenticated and logged on to the network. Provide the VLAN ID, or use an existing VLAN alias to identify the post authentication VLAN.<br>• <1-4096> – Specify the VLAN's number from 1 - 4096.<br>• <VLAN-ALIAS> – Specify the VLAN alias (should be existing and configured).<br>VLAN alias names begin with a '$'. |

**Example**

```
rfs4000-229D58(config-captive-portal-test)#post-authentication-vlan 1

rfs4000-229D58(config-captive-portal-test)#show context
captive-portal test
 post-authentication-vlan 1
rfs4000-229D58(config-captive-portal-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the post authentication RADIUS VLAN assigned to this captive portal's users |
| *radius-vlan-assignment* | Enables assignment of a RADIUS VLAN for this captive portal |

### 4.1.31.2.16 radius-vlan-assignment

*captive-portal-mode commands*

Enables assignment of a RADIUS VLAN for this captive portal

When enabled, if the RADIUS server as part of the authentication process returns a client's VLAN-ID in a RADIUS access-accept packet, all client traffic is forwarded on the post authentication VLAN. If disabled, the RADIUS server's VLAN assignment is ignored and the VLAN configuration defined within the WLAN configuration is used instead. This feature is disabled by default.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
radius-vlan-assignment
```

**Parameters**

None

**Example**

```
rfs4000-229D58(config-captive-portal-test)#radius-vlan-assignment

rfs4000-229D58(config-captive-portal-test)#show context
captive-portal test
 post-authentication-vlan 1
 radius-vlan-assignment
rfs4000-229D58(config-captive-portal-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables assignment of a RADIUS VLAN for this captive portal |
| *post-authentication-vlan* | Assigns a post authentication RADIUS VLAN for this captive portal's users |

### 4.1.31.2.17 redirection

*captive-portal-mode commands*

Configures a list of destination ports (separated by commas, or using a dash for a range) that are taken into consideration when redirecting client connections

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
redirection ports <LIST-OF-PORTS>
```

**Parameters**

- `redirection ports <LIST-OF-PORTS>`

| | |
|---|---|
| ports <LIST-OF-PORTS> | Configures destination ports considered for redirecting client connection<br>A maximum of 16 ports can be specified in a comma-separated list. Standard ports 80 and 443 are always considered for client connections regardless of what's entered by the administrator. |

**Example**

```
rfs4000-229D58(config-captive-portal-test)#redirection ports 1,2,3

rfs4000-229D58(config-captive-portal-test)#show context
captive-portal test
 redirection ports 1-3
rfs4000-229D58(config-captive-portal-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables redirection of client connection |

### 4.1.31.2.18 report-loyalty-application

*captive-portal-mode commands*

Enables detection of captive portal client's usage of a selected (preferred) loyalty application

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
report-loyalty-application {custom-app <APPLICATION-NAME>}
```

**Parameters**

- `report-loyalty-application {custom-app <APPLICATION-NAME>}`

| | |
|---|---|
| report-loyalty-application {custom-app <APPLICATION-NAME>} | Reports a captive portal client's loyalty application presence and stores this information in the captive portal's user database. The client's loyalty application detection occurs on the access point to which the client is associated. Retail administrators can use this information to assess whether patrons' loyalty application usage is as per expectation within specific retail environments. This option is disabled by default.<br>• custom-app <APPLICATION-NAME> – Optional. Uses a custom application definition as match criteria.<br>  • <APPLICATION-NAME> – Specify the custom application name (should be existing and configured). Ensure that the application specified is available and configured. If not, create an application definition. For more information, see *application*.<br>If no custom application definition is specified, the system uses localization to detect application presence. |

**Example**

```
nx9500-6C8809(config-captive-portal-test)#report-loyalty-application custom-app
AntiVirus

nx9500-6C8809(config-captive-portal-test)#show context include-factory | include
 report-loyalty-application
 report-loyalty-application custom-app AntiVirus
nx9500-6C8809(config-captive-portal-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables detection of customer-loyalty application presence |

### 4.1.31.2.19 server

*captive-portal-mode commands*

Configures captive portal server parameters, such as the hostname, IP address, and mode of operation. This is the captive-portal server hosting the captive portal Web pages.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
server [host|mode]

server host <IP/HOSTNAME>

server mode [centralized|centralized-controller {hosting-vlan-interface <0-4096>}|self]
```

**Parameters**

- `server host <IP/HOSTNAME>`

| | |
|---|---|
| host <IP/HOSTNAME> | Configures the internal captive portal server (wireless controller, access point, service platform)<br>• <IP/HOSTNAME> – Specify the IPv4/IPv6 address or hostname of the captive portal server.<br>For centralized-controller mode, the server host should be a virtual hostname and not an IP address.<br>If enabling OAuth (social-media login) on the captive portal, configure the server's hostname and not the IP address. This is because some social media do not allow IP address as redirect-uri. For more information, see *oauth* and *php-helper*. |

- `server mode [centralized|centralized-controller {hosting-vlan-interface <0-4096>}|self]`

| | |
|---|---|
| mode | Configures the captive portal server mode. This parameter identifies the device that will capture and redirect a wireless user's Web browser session to a landing page where the user has to provide login credentials in order to access the managed network. The WiNG captive portal implementation is very flexible and allows captive portal services to reside anywhere within the WiNG managed network. For example, the capture and redirection can be performed directly by the access points at the edge of the network, centrally on the controllers or service platforms managing the access points, or on dedicated wireless controller deployed within an isolated network. |
| centralized | Select this option if capture and redirection is provided by a designated wireless controller/service platform on the network defined using an IPv4/IPv6 address or hostname. This dedicated device can either be managing the dependent/independent access points or be a dedicated device deployed over the intermediate network.<br>Ensure the IPv4 address or hostname of the WiNG wireless controller performing the capture and redirection is defined in the captive portal policy. And also, that the wireless controller is reachable via MINT. |

| | |
|---|---|
| centralized-controller {hosting-vlan-interface <0-4096>} | Select this option if capture and redirection is on a cluster of wireless controller/ service platforms managing dependent/independent access points when redundancy is required. The capture and redirection is provided by one of the controllers in the cluster that is operating as the designated forwarder for the tunneled VLAN. The cluster can be configured as active/active or active/standby as required.<br>If using this option, ensure a non-resolvable virtual hostname is defined in the captive portal policy which is shared between the controllers in the cluster.<br>• hosting-vlan-interface – Optional. Configures the VLAN where the client can reach the captive-portal server. This option is available only for the centralized-controller mode.<br>• <0-4096> – Specify the VLAN number (0 implies the controller is available on the client's VLAN). |
| self | Select this option if capture and redirection is provided by the access point that is servicing the captive portal enabled Wireless LAN. This is the default setting.<br>When enabled each remote access point servicing the captive portal enabled WLAN performs the captive portal capture and redirection internally. The WLAN users are mapped to a locally bridged VLAN for which each access point has a *Switched Virtual Interface* (SVI) defined. The SVI can either have a static or dynamic (DHCP) IPv4 address assigned. The capture, redirection, and presentation of the captive portal pages are performed using the SVI on each access point the wireless device is associated to. |

**Example**

```
rfs6000-81742D(config-captive-portal-test)#server host 172.16.10.9

rfs6000-81742D(config-captive-portal-test)#show context
captive-portal test
 access-time 35
 custom-auth info bob bob@examplecompany.com
 connection-mode https
 inactivity-timeout 750
 server host 172.16.10.9
rfs6000-81742D(config-captive-portal-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Resets or disables captive portal host and mode settings |

### 4.1.31.2.20 simultaneous-users

*captive-portal-mode commands*

Specifies the number of users (client MAC addresses) that can simultaneously logon to the captive portal. This option is disabled by default.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
simultaneous-users <1-8192>
```

**Parameters**

- `simultaneous-users <1-8192>`

| | |
|---|---|
| simultaneous-users <1-8192> | Specifies the number of MAC addresses that can simultaneously access the captive portal<br>• <1-8192> – Select a number from 1 - 8192. |

**Example**

```
rfs6000-81742D(config-captive-portal-test)#simultaneous-users 5

rfs6000-81742D(config-captive-portal-test)#show context
captive-portal test
 access-time 35
 custom-auth info bob bob@examplecompany.com
 connection-mode https
 inactivity-timeout 750
 server host 172.16.10.9
 simultaneous-users 5
rfs6000-81742D(config-captive-portal-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Resets or disables captive portal commands |

### 4.1.31.2.21 terms-agreement

*captive-portal-mode commands*

Enforces the user to agree to terms and conditions (included in the login page) for captive portal access. This feature is disabled by default.

When enabled, the system enforces a previously registered user to re-confirm the terms of agreement, on successive log ins, only if the interval between the last log out and the current log in exceeds the *agreement-refresh* timeout configured in the WLAN context. For more information on configuring the agreement-refresh timeout value, see *registration*.

For example:

If the agreement-refresh timeout is set at 20 minutes, the following two possibilities can arise:

- The interval between logging out and re-logging *exceeds* 20 minutes - in which case the user is served the Terms of Agreement page on successful authentication.
- The interval between logging out and re-logging is *less than* 20 minutes - in which case the user is provided direct Internet access.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
terms-agreement
```

**Parameters**

None

**Example**

```
rfs6000-81742D(config-captive-portal-test)#terms-agreement

rfs6000-81742D(config-captive-portal-test)#show context
captive-portal test
 access-time 35
 custom-auth info bob bob@examplecompany.com
 connection-mode https
 inactivity-timeout 750
 server host 172.16.10.9
 simultaneous-users 5
 terms-agreement
rfs6000-81742D(config-captive-portal-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Resets or disables captive portal commands |

### 4.1.31.2.22 use

*captive-portal-mode commands*

Configures a AAA policy and DNS whitelist with this captive portal policy. AAA policies are used to configure authentication and accounting servers for this captive portal. DNS whitelists restrict users to a set of configurable domains on the Internet.

For more information on AAA policies, see *AAA-POLICY*.

For more information on DNS whitelists, see *dns-whitelist*.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
use [aaa-policy <AAA-POLICY-NAME>|dns-whitelist <DNS-WHITELIST-NAME>]
```

**Parameters**

- `use [aaa-policy <AAA-POLICY-NAME>|dns-whitelist <DNS-WHITELIST-NAME>]`

| | |
|---|---|
| aaa-policy <AAA-POLICY-NAME> | Associates a AAA policy with this captive portal. AAA policies validate user credentials and provide captive portal access to the network.<br>• <AAA-POLICY-NAME> – Specify the AAA policy name. |
| dns-whitelist <DNS-WHITELIST-NAME> | Associates a DNS whitelist to use with this captive portal. A DNS whitelist defines a set of allowed destination IP addresses. DNS whitelists restrict captive portal access.<br>• <DNS-WHITELIST-NAME> – Specify the DNS whitelist name.<br>To effectively host captive portal pages on an external Web server, the IP address of the destination Web server(s) should be added to the DNS whitelist. |

**Example**

```
rfs6000-81742D(config-captive-portal-test)#use aaa-policy test

rfs6000-81742D(config-captive-portal-test)#use dns-whitelist test

rfs6000-81742D(config-captive-portal-test)#show context
captive-portal test
 access-time 35
 custom-auth info bob bob@examplecompany.com
 connection-mode https
 inactivity-timeout 750
 server host 172.16.10.9
 simultaneous-users 5
 terms-agreement
 use aaa-policy test
 use dns-whitelist test
rfs6000-81742D(config-captive-portal-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes a DNS Whitelist or a AAA policy from the captive portal |
| *dns-whitelist* | Configures a DNS whitelist |
| *aaa-policy* | Configures a AAA policy |

### 4.1.31.2.23 webpage

*captive-portal-mode commands*

Use this command to define the appearance and flow of Web pages requesting clients encounter when accessing a controller, service platform, or access point managed captive portal. Define whether the Web pages are maintained locally or externally to the managing device as well as messages displayed requesting clients.

Configures Web pages displayed when interacting with a captive portal. These pages are:

- acknowledgment – This page displays details for the user to acknowledge
- agreement – This page displays “Terms and Conditions” that a user accepts before allowed access to the captive portal.
- fail – This page is displayed when the user is not authenticated.
- login – This page is displayed when the user connects to the captive portal. It fetches login credentials from the user.
- no-service – This page is displayed when a captive portal user is unable to access the captive portal due to unavailability of critical services.
- registration – This page is displayed when users are redirected to a Web page where they have to register in the captive portal’s database.
- welcome – This page is displayed to welcome an authenticated user to the captive portal.

These Web pages, which interact with captive portal users, can be located either on the controller or an external location.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
webpage [external|internal]

webpage external [acknowledgment|agreement|fail|login {post}|no-service|
registration|welcome] <URL>

webpage internal [acknowledgment|agreement|fail|login|no-service|org-name|
org-signature|registration|welcome]

webpage internal [acknowledgment|agreement|fail|login|no-service|registration|
welcome] [description|footer|header|title] <CONTENT>

webpage internal [acknowledgment|agreement|fail|login|no-service|registration|
welcome] [body-background-color|body-font-color|org-background-color|org-font-
color] <WORD>

webpage internal [acknowledgment|agreement|fail|login|no-service|registration|
welcome] [main-logo use-as-banner|small-logo] <URL>

webpage internal registration field [age-range|city|country|custom|disclaimer|
dob|email|gender|member|mobile|name|optout|street|via-email|via-sms|zip] type
[checkbox|date|dropdown-menu|e-address|number|radio-button|text] enable {label
<LINE>|mandatory|title <LINE>|placeholder <LINE>}
```

```
webpage internal welcome use-external-success-url

webpage internal [org-name|org-signature] <LINE>
```

**Parameters**

```
• webpage external [acknowledgment|agreement|fail|login {post}|no-service|
registration|welcome] <URL>
```

| | |
|---|---|
| external | Indicates Web pages being served are hosted on an external (to the captive portal) server resource |
| acknowledgment | Indicates the page is displayed for user acknowledgment of details. Users are redirected to this page to acknowledge information provided. |
| agreement | Indicates the page is displayed for “Terms & Conditions”<br>The agreement page provides conditions that must be agreed to before captive portal access is permitted. |
| fail | Indicates the page is displayed for login failure<br>The fail page asserts authentication attempt has failed, the user is not allowed to access the Internet (using this captive portal) and must provide the correct login information again to access the Internet. |
| login {post} | Indicates the page is displayed for getting user credentials. This page is displayed by default.<br>• post – Optional. Redirects users to post externally during authentication<br>The login page prompts the user for a username and password to access the captive portal and proceed to either the agreement page (if used) or the welcome page. |
| no-service | Indicates the page is displayed when certain critical services are unavailable and the user fails to access the captive portal. The no-service page asserts the captive portal service is temporarily unavailable due to technical reasons. Once the services become available, the captive portal user is automatically connected back to the services available through the captive portal. The possible scenarios are:<br>• The RADIUS server (on-board or external) is not reachable and the user cannot be authenticated<br>• The external captive portal server is not reachable<br>• The connectivity between the adopted AP and controller is lost<br>• The external DHCP server is not reachable<br>To provide this service, enable the following:<br>• External captive portal server monitoring<br>• AAA server monitoring. This enables detection of RADIUS server failure.<br>• External DHCP server monitoring<br>For more information on enabling these critical resource monitoring, see *service*. |
| registration | Indicates the page is displayed when users are redirected to a Web page where they have to register in the captive portal’s database<br>Guest users are redirected to an internally (or) externally hosted registration page (registration.html) upon association to a captive portal SSID, where previously, not-registered guest users can register. |
| welcome | Indicates the page is displayed after a user has been successfully authenticated<br>The welcome page asserts a user has logged in successfully and can access the captive portal. |

| | |
|---|---|
| <URL> | This parameter is common to all of the above mentioned Web pages, and specifies the Web page URL. The Web page is retrieved and served from the specified external location.<br>The URL can include following query tags:<br>'WING_TAG_CLIENT_IP' - Captive portal client IPv4 address<br>'WING_TAG_CLIENT_MAC' - Captive portal client MAC address<br>'WING_TAG_WLAN_SSID ' - Captive portal client WLAN ssid<br>'WING_TAG_AP_MAC' - Captive portal client AP MAC address<br>'WING_TAG_AP_NAME' - Captive portal client AP Name<br>'WING_TAG_RF_DOMAIN' - Captive portal client RF Domain<br>'WING_TAG_CP_SERVER' - Captive portal server address<br>'WING_TAG_USERNAME' - Captive portal authentication username<br>Example:<br>http://cportal.com/policy/login.html?client_ip=WING_TAG_CLIENT_IP&ap_mc=WING_TAG_AP_MAC.<br>Use '&' or '?' character to separate field-value pair.<br>Enter 'ctrl-v' followed by '?' to configure query string. |

```
• webpage internal [acknowledgment|agreement|fail|login|no-service|
registration|welcome] [description|footer|header|title] <CONTENT>
```

| | |
|---|---|
| internal | Indicates the Web pages are hosted on an internal server resource. This is the default setting. |
| acknowledgment | Indicates the Web page is displayed for users to acknowledge the information provided |
| agreement | Indicates the page is displayed for “Terms & Conditions” |
| fail | Indicates the page is displayed for login failure |
| login | Indicates the page is displayed for entering user credentials |
| no-service | Indicates the page is displayed when certain critical services are unavailable and the user fails to access the captive portal. The possible scenarios are:<br>• The RADIUS server (on-board or external) is not reachable and the user cannot be authenticated<br>• The external captive portal server is not reachable<br>• The connectivity between the adopted AP and controller is lost<br>• The external DHCP server is not reachable<br>To provide this service, enable the following:<br>• External captive portal server monitoring<br>• AAA server monitoring. This enables detection of RADIUS server failure.<br>• External DHCP server monitoring<br>• AP to controller connectivity monitoring<br>For more information on enabling these critical resource monitoring, see *service*. |

| | |
|---|---|
| registration | Indicates the page is displayed when users are redirected to a Web page where they have to register in the captive portal's database<br>Guest users are redirected to an internally (or) externally hosted registration page (registration.html) upon association to a captive portal SSID, where previously, not-registered guest users can register. |
| welcome | Indicates the page is displayed after a user has been successfully authenticated |
| description | Indicates the content is the description portion of each of the following internal Web pages: acknowledgment, agreement, fail, login, no-service, and welcome |
| footer | Indicates the content is the footer portion of each of the following internal Web pages: acknowledgment, agreement, fail, no-service, and welcome page. The footer portion contains the signature of the organization that hosts the captive portal. |
| header | Indicates the content is the header portion of each of the following internal Web pages: acknowledgment, agreement, fail, no-service, and welcome page. The header portion contains the heading information for each of these pages. |
| title | Indicates the content is the title of each of the following internal Web pages: acknowledgment, agreement, fail, no-service, and welcome page. The title for each of these pages is configured here. |
| <CONTENT> | The following keyword is common to all of the above internal Web page options:<br>• <CONTENT> – Specify the content displayed for each of the different components of the internal Web page. Enter up to 900 characters for the description and 256 characters each for header, footer, and title. |

- `webpage internal [acknowledgment|agreement|fail|login|no-service|registration|welcome] [main-logo use-as-banner|small-logo] <URL>`

| | |
|---|---|
| internal | Indicates the Web pages are hosted on an internal server resource |
| agreement | Indicates the page is displayed for "Terms & Conditions" |
| acknowledgment | Indicates the Web page is displayed for users to acknowledge the information provided |
| fail | Indicates the page is displayed for login failure |
| login | Indicates the page is displayed for user credentials |
| no-service | Indicates the page is displayed when certain critical services are unavailable and the user fails to access the captive portal. The possible scenarios are:<br>• The RADIUS server (on-board or external) is not reachable and the user cannot be authenticated<br>• The external captive portal server is not reachable<br>• The connectivity between the adopted AP and controller is lost<br>• The external DHCP server is not reachable<br>To provide this service, enable the following:<br>• External captive portal server monitoring<br>• AAA server monitoring. This enables detection of RADIUS server failure.<br>• External DHCP server monitoring<br>• AP to controller connectivity monitoring<br>For more information on enabling these critical resource monitoring, see *wlan*. |

| | |
|---|---|
| registration | Indicates the page displayed is the registration page to which users are redirected in order to register in the captive portal's database<br>Guest users are redirected to an internally (or) externally hosted registration page (registration.html) upon association to a captive portal SSID, where previously, not-registered guest users can register. |
| welcome | Indicates the page is displayed after a user has been successfully authenticated |
| main-logo<br>use-as-banner | The following keyword is common to all of the above internal Web page options:<br>• main-logo – Indicates the main logo displayed in the header of each Web page<br>• use-as-banner – Uses the image, specified here, as the Web page banner, in place of the logo and organization name |
| small-logo | The following keyword is common to all of the above internal Web page options:<br>• small-logo – Indicates the logo image displayed in the footer of each Web page, and constitutes the organization's signature |
| <URL> | This parameter is common to the 'main-logo' and 'small-logo' keywords and provides the complete URL from where the main-logo and small-logo files are loaded and subsequently cached on the system.<br>• <URL> – Specify the location and name of the main-logo and the small-logo image files. |

• `webpage internal registration field [age-range|city|country|custom|disclaimer|dob|email|gender|member|mobile|name|optout|street|via-email|via-sms|zip] type [checkbox|date|dropdown-menu|e-address|number|radio-button|text] enable` *`{label <LINE>|mandatory|title <LINE>|placeholder <LINE>}`*

| | |
|---|---|
| internal | Indicates the Web pages are hosted on an internal server resource |
| registration | Allows you to customize the user registration page. Select this option if the captive-portal's access-type is set to registration. Use the *field* and *type* options to define the input fields (for example, age-range, city, email, etc.) and the field type (for example, text, checkbox, dropdown-menu, radio-button, etc.)<br>Guest users are redirected to an internally (or) externally hosted registration page (registration.html) upon association to a captive portal SSID, where previously, not-registered guest users can register.<br>If the registration Web page is not customized, the built-in, default registration page is displayed to the client. |
| field [age-range\|<br>city\|country\|<br>custom <WORD >\|<br>disclaimer\|] | Configures the captive portal's registration page fields<br>Following are the available fields and the field type for each:<br>• age-range – Creates the age-range input field (enabled by default and included in the built-in registration page)<br>• dropdown-menu – Configures the age-range field as a drop-down menu<br>• radio-button – Configures the age-range field as a radio button menu<br>• city – Creates the *postal address: city name* input field (enabled by default and included in the built-in registration page)<br>• text – Configures the city field as only alpha-numeric and special characters input field<br>Contd.. |

| | |
|---|---|
| | • country – Creates the *postal address: country name* input field (disabled by default)<br>  • text – Configures the country field as only alpha-numeric and special characters input field<br>• custom <WORD> – Creates a customized field (as per your requirement). Use the 'custom' option to create a field not included in the built-in list.<br>  • <WORD> – Provide a name for the field. On the registration page, the field is displayed under the name specified here.<br>• disclaimer – Creates client's disclaimer-confirmation input field (disabled by default)<br>• checkbox – Configures the disclaimer field as a check box |
| field [dob\|email\|gender\|member\|mobile\|name\|optout\|street\|via-email\|via-sms\|zip] | • dob – Creates the client's *date of birth* (DoB) input field (disabled by default)<br>  • date – Configures the DoB field as only date-format input field<br>  • dropdown-menu – Configures the DoB field as a drop-down menu<br>  • text – Configures the DoB field as only alpha-numeric and special characters input field<br>• email – Creates the e-mail address input field (enabled by default and included in the built-in registration page)<br>  • e-address – Configures the e-mail field as only e-mail address format input field<br>• gender – Creates client's gender input field (disabled by default)<br>  • dropdown-menu – Configures the gender field as a drop-down menu<br>  • radio-button – Configures the gender field as a radio button menu<br>• member – Creates client's loyalty or captive-portal membership card number input field (disabled by default)<br>  • number – Configures the member field as only-numeric characters input field<br>  • text – Configures the member field as only alpha-numeric and special characters input field<br>• mobile – Creates the mobile number input field (enabled by default and included in the built-in registration page)<br>  • number – Configures the mobile field as only-numeric characters input field<br>  • text – Configures the mobile field as only alpha-numeric and special characters input field<br>• name – Creates the client name input field (enabled by default and included in the built-in registration page)<br>  • text – Configures the name field as only alpha-numeric and special characters input field<br>• optout – Creates an input field that enables clients to opt out from registering<br>  • checkbox – Configures the optout field as a check box<br>• street – Creates the *postal address: street name/number* input field (enabled by default and included in the built-in registration page)<br>  • text – Configures the street field as only alpha-numeric and special characters input field<br>• via-email – Creates the client's preferred mode of communication as e-mail input field (enabled by default and included in the built-in registration page)<br>  • checkbox – Configures the via-email field as a check box<br>• via-sms – Creates the client's preferred mode of communication as SMS input field (enabled by default and included in the built-in registration page)<br>  • checkbox – Configures the via-sms field as a check box<br>Contd.. |

| | |
|---|---|
| | • zip – Creates the *postal address: zip* input field (enabled by default and included in the built-in registration page)<br>• number – Configures the zip field as only-numeric characters input field<br>• text – Configures the zip field as only alpha-numeric and special characters input field |
| type [checkbox\|date\|dropdown-menu\|e-address\|number\|radio-button\|text] | After specifying the field, configure the field type. The options displayed depend on the field selected in the previous step. These options are: checkbox, date, dropdown-menu, e-address, number, radio-button, and text.<br>• checkbox – Configures the field as a check box<br>• date – Configures the field as only date-format input field<br>• dropdown-menu – Configures the field as a drop-down menu<br>• e-address – Configures the field as an e-mail address input field<br>• number – Configures the field as only-numeric characters input field<br>• radio-button – Configures the field as a radio button<br>• text – Configures the field as only alpha-numeric and special characters input field<br>Some of the fields can have more than one field type options. For example, the field 'zip' can either be a numerical field or a text. Select the one best suited for your captive-portal. |
| enable {label <LINE>\|mandatory\|title <LINE>\|placeholder <LINE>} | Enables the field. When enabled, the field is displayed on the registration page. After enabling the field, optionally configure the following parameters:<br>• label <LINE> – Optional. Configures the field's label<br>• mandatory – Optional. Makes the field mandatory<br>• title – Optional. Configures the comma-separated list of items to include in the drop-down menu.<br>• placeholder <LINE> – Optional. Configures a string, not exceeding 300 characters, that is displayed within the field. If not configured, the field remains blank. |

- `webpage internal welcome use-external-success-url`

| | |
|---|---|
| internal | Indicates the Web pages are hosted on an internal server resource |
| welcome | Indicates the page is displayed after a user has been successfully authenticated |
| use-external-success-url | When configured, redirects the user, on successful authentication, to an externally hosted success URL from the locally-hosted landing page.<br>Use the *webpage > external > welcome > <URL>* command to specify the location of the Welcome page. |

- `webpage internal [org-name|org-signature] <LINE>`

| | |
|---|---|
| internal | Indicates the Web pages are hosted on an internal server resource |
| org-name | Specifies the company's name, included on Web pages along with the main image |
| org-signature | Specifies the company's signature information, included in the bottom of Web pages along with a small image |
| <LINE> | Specify the company's name or signature depending on the option selected. |

**Example**

```
rfs6000-81701D(config-captive-portal-guest)#webpage external welcome http://
192.168.9.46/welcome.html

rfs6000-81701D(config-captive-portal-guest)#show context
captive-portal guest
webpage external welcome http://192.168.9.46/welcome.html
rfs6000-81701D(config-captive-portal-guest)#

nx9500-6C8809(config-captive-portal-register)#webpage internal registration field
age-range type dropdown-menu enable mandatory title 10-20,20-30,30-40,50-60,60-70

nx9500-6C8809(config-captive-portal-register)#show context include-factory |
include age-range
 webpage internal registration field age-range type dropdown-menu enable mandatory
label "Age Range" title "10-20,20-30,30-40,50-60,60-70"
nx9500-6C8809(config-captive-portal-register)#
```

In the following examples, the background and font colors have been customized for the captive portal's login page. Similar customizations can be applied to the acknowledgement, agreement, fail, welcome, no-service, and registration captive portal pages.

```
rfs6000-81701D(config-captive-portal-cap-enhanced-policy)#webpage internal login
body-background-color #E7F0EB

rfs6000-81701D(config-captive-portal-cap-enhanced-policy)#webpage internal login
body-font-color #EF68A7

rfs6000-81701D(config-captive-portal-cap-enhanced-policy)#webpage internal login
org-background-color #EFE4E9

rfs6000-81701D(config-captive-portal-cap-enhanced-policy)#webpage internal login
org-font-color #BA4A21

rfs6000-81701D(config-captive-portal-cap-enhanced-policy)#show context
captive-portal cap-enhanced-policy
 webpage internal login org-background-color #EFE4E9
 webpage internal login org-font-color #BA4A21
 webpage internal login body-background-color #E7F0EB
 webpage internal login body-font-color #EF68A7
rfs6000-81701D(config-captive-portal-ca-enhanced-policy)#
```

The following examples configure a scenario where a successfully authenticated user is redirected to an externally hosted Welcome page from the internal landing page.

```
rfs6000-81701D(config-captive-portal-cap-enhanced-policy)#webpage external
welcome http://192.168.13.10/WelcomePage.html

rfs6000-81701D(config-captive-portal-cap-enhanced-policy)#webpage internal
welcome use-external-success-url

rfs6000-81701D(config-captive-portal-cap-enhanced-policy)#show context
captive-portal cap-enhanced-policy
 webpage external welcome http://192.168.13.10/WelcomePage.html
 webpage internal acknowledgement org-background-color #33ff88
 webpage internal acknowledgement org-font-color #bb6622
 webpage internal acknowledgement body-background-color #22aa11
 webpage internal acknowledgement body-font-color #bb6622
 webpage internal welcome use-external-success-url
rfs6000-81701D(config-captive-portal-ca-enhanced-policy)#
```

**Related Commands**

| | |
|---|---|
| *no* | Resets or disables captive portal configurations |

### 4.1.31.2.24 webpage-auto-upload

*captive-portal-mode commands*

Enables automatic upload of advanced Web pages to requesting clients on association. Enable this option if the webpage-location is selected as *advanced*. For more information, see *webpage-location*.

If this feature is enabled, access points shall request for Web pages from the controller during adoption. If the controller has a different set of Web pages, than the ones existing on the access points, the controller shall distribute the Web pages uploaded on it to the access points.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
webpage-auto-upload
```

**Parameters**

None

**Example**

```
rfs6000-81742D(config-captive-portal-test)#webpage-auto-upload

rfs6000-81742D(config-captive-portal-test)#show context
captive-portal test
 webpage-auto-upload
 logout-fqdn logout.testuser.com
rfs6000-81742D(config-captive-portal-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables automatic upload of advanced Web pages on a captive portal |
| *webpage* | Configures Web pages displayed when interacting with a captive portal |
| *webpage-location* | Specifies the location of the Web pages used for authentication |

### 4.1.31.2.25 webpage-location

*captive-portal-mode commands*

Specifies the location of the Web pages used for authentication. These pages can either be hosted on the system or on an external Web server.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
webpage-location [advanced|external|internal]
```

**Parameters**

- `webpage-location [advanced|external|internal]`

| | |
|---|---|
| advanced | Uses Web pages for login, welcome, failure, and terms created and stored on the controller. Select *advanced* to use a custom-developed directory full of Web page content that can be copied in and out of the controller, service platform, or access point.<br>If selecting advanced, enable the *webpage-auto-upload* option to automatically launch the advanced pages to requesting clients upon association. For more information, see *webpage-auto-upload*. |
| external | Uses Web pages for login, welcome, failure, and terms located on an external server. Provide the URL for each of these pages. |
| internal | Uses Web pages for login, welcome, and failure that are automatically generated |

**Example**

```
rfs6000-81742D(config-captive-portal-test)#webpage-location external

rfs6000-81742D(config-captive-portal-test)#show context
captive-portal test
 access-time 35
 custom-auth info bob bob@examplecompany.com
 connection-mode https
 inactivity-timeout 750
 server host 172.16.10.9
 simultaneous-users 5
 terms-agreement
 webpage-location external
 use aaa-policy test
rfs6000-81742D(config-captive-portal-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Resets or disables captive portal Web page settings |
| *webpage* | Configures a captive portal's Web page (acknowledgment, agreement, login, welcome, fail, no-service, and terms) settings |
| *webpage-auto-upload* | Enables an automatic upload of advanced Web pages on a captive portal |

### 4.1.31.2.26 welcome-back

*captive-portal-mode commands*

Enables the provision of direct Internet access to once-registered, captive-portal guest users on subsequent log-ins. When enabled, a registered captive-portal guest user, on subsequent logins, is served the *Acknowledgement* page only if:

- The *agreement-refresh* option is enabled for device-based (device and device-OTP) registration, and
- The interval between logout and login is *lesser* than the *agreement-refresh* timeout configured in the WLAN context. If this interval *exceeds* the agreement-refresh timeout, the user is served the *Agreement* page. For more information on configuring the agreement-refresh timeout value, see *registration*.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
welcome-back pass-through
```

**Parameters**

- `welcome-back pass-through`

| | |
|---|---|
| welcome-back pass-through | Enables display of the Acknowledgement page to an already registered user on subsequent captive-portal log-ins, provided the interval between logout and login is lesser than the *agreement-refresh* timeout<br>• pass-through – Provides user direct Internet access, from the Welcome-back page, without any user action |

**Example**

```
nx9500-6C8809(config-captive-portal-test)#show context
captive-portal test
 welcome-back pass-through
 webpage internal registration field city type text enable label "City" placeholder
"Enter City"
 webpage internal registration field street type text enable label "Address"
placeholder "123 Any Street"
 webpage internal registration field name type text enable label "Full Name"
placeholder "Enter First Name, Last Name"
 webpage internal registration field zip type number enable label "Zip" placeholder
"Zip"
 webpage internal registration field via-sms type checkbox enable title "SMS
Preferred"
 webpage internal registration field mobile type number enable label "Mobile"
placeholder "Mobile Number with Country code"
 webpage internal registration field age-range type dropdown-menu enable label "Age
Range" title "Age Range"
 webpage internal registration field email type e-address enable mandatory label
"Email" placeholder "you@domain.com"
 webpage internal registration field via-email type checkbox enable title "Email
Preferred"
nx9500-6C8809(config-captive-portal-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables the provision of direct Internet access to once-registered, captive-portal guest users on subsequent log-ins |

### 4.1.31.2.27 configuring device registration with dynamic VLAN assignment

*captive-portal-mode commands*

This section provides the configurations required to enable device registration with dynamic VLAN assignment in a multi-vendor environment.

1 Create vendor-specific RADIUS user groups and assign an allowed VLAN to each group, as shown in the following examples:

```
nx9500-6C8809(config)#radius-group Apple
nx9500-6C8809(config-radius-group-Apple)#policy vlan 200
nx9500-6C8809(config)#radius-group Samsung
nx9500-6C8809(config-radius-group-Samsung)#policy vlan 100
nx9500-6C8809(config)#radius-group Devices
nx9500-6C8809(config-radius-group-Devices)#policy vlan 1

Note, if necessary, configure the session-time for each of the above configured
RADIUS group. This is the duration for which a RADIUS group client's session
remains active after successful authentication. Upon expiration, the RADIUS
session is terminated. Use the policy > session-time > <5-144000> command to
specify the session-time.
```

2 Create a RADIUS user pool, add users to the pool, and assign the users to the vendor-specific user groups: as shown in the following examples:

```
nx9500-6C8809(config)#radius-user-pool-policy Vendor-Devices
nx9500-6C8809(config-radius-user-pool-Vendor-Devices)#user Samsung password 0
samsung group Samsung
nx9500-6C8809(config-radius-user-pool-Vendor-Devices)#user test password 0
test123 group Apple
```

3 Create a RADIUS server policy, and associate the RADIUS groups and user pool created in steps 1 and 2 respectively, as shown in the following examples:

```
nx9500-6C8809(config)#radius-server-policy Guest-Radius
nx9500-6C8809(config-radius-server-policy-Guest-Radius)#use radius-user-pool-
policy Vendor-Devices
nx9500-6C8809(config-radius-server-policy-Guest-Radius)#use radius-group
Samsung
nx9500-6C8809(config-radius-server-policy-Guest-Radius)#use radius-group Sony
nx9500-6C8809(config-radius-server-policy-Guest-Radius)#use radius-group
Apple
```

4 Create an AAA Policy, on the controller, and configure the authentication server as self, as shown in the following example:

```
nx9500-6C8809(config)#aaa-policy OnBoard-NX
nx9500-6C8809(config-aaa-policy-OnBoard-NX)#authentication server 1 onboard
controller
nx9500-6C8809(config-aaa-policy-OnBoard-NX)#show context
aaa-policy OnBoard-NX
 authentication server 1 onboard self
nx9500-6C8809(config-aaa-policy-OnBoard-NX)#
```

5 Create a captive-portal, and point to the captive-portal's server, enable RADIUS VLAN assignment, and associate the AAA policy, as shown in the following examples:

```
nx9500-6C8809(config)#captive-portal DeviceRegistration
nx9500-6C8809(config-captive-portal-DeviceRegistration)#server host
captive.extremenoc.com
nx9500-6C8809(config-captive-portal-DeviceRegistration)#radius-vlan-
assignment
nx9500-6C8809(config-captive-portal-DeviceRegistration)#use aaa-policy
OnBoard-NX
nx9500-6C8809(config-captive-portal-DeviceRegistration)#access-type radius
```

6 Configure a WLAN and enable RADIUS VLAN assignment, as shown in the following examples:

```
nx9500-6C8809(config)#wlan CP-OnBoarding
nx9500-6C8809(config-wlan-CP-OnBoarding)#ssid CP-OnBoarding
nx9500-6C8809(config-wlan-CP-OnBoarding)#radius vlan-assignment
nx9500-6C8809(config-wlan-CP-OnBoarding)#use aaa-policy OnBoard-NX
nx9500-6C8809(config-wlan-CP-OnBoarding)#use captive-portal
DeviceRegistration
nx9500-6C8809(config-wlan-CP-OnBoarding)#captive-portal-enforcement fall-back
nx9500-6C8809(config-wlan-CP-OnBoarding)#registration device group-name
Devices expiry-time 4320
nx9500-6C8809(config-wlan-CP-OnBoarding)#authentication-type mac
```

7 Create an access point profile, associate the RADIUS server policy, captive-portal policy to it, and also assign the WLAN to the AP radio, as shown in the following examples:

```
nx9500-6C8809(config-profile-SITE-10)#use radius-server-policy Guest-Radius
nx9500-6C8809(config-profile-SITE-10)#use captive-portal server
DeviceRegistration
nx9500-6C8809(config-profile-SITE-10-if-radio2)#wlan CP-OnBoarding bss 1
primary
nx9500-6C8809(config-profile-SITE-10-if-ge1)#switchport mode trunk
nx9500-6C8809(config-profile-SITE-10-if-ge1)#switchport trunk native vlan 90
nx9500-6C8809(config-profile-SITE-10-if-ge1)#switchport trunk allowed vlan
1,90,1000-1002
nx9500-6C8809(config-profile-SITE-10-if-ge1)#no switchport trunk native
tagged
```

8 Use the access point profile in the access point's device context.

**Related Commands**

| | |
|---|---|
| *radius-server-policy* | Documents RADIUS server policy configuration commands |
| *radius-group* | Documents RADIUS group policy configuration commands |
| *radius-user-pool-policy* | Documents RADIUS user policy configuration commands |
| *aaa-policy* | Documents AAA policy configuration commands |
| *captive portal* | Documents captive-portal configuration commands |
| *wlan* | Documents WLAN configuration commands |
| *Profile Config Commands* | Documents profile configuration commands |
| *guest-registration* | Documents *show > guest-registration* command and outputs. Use this command to view guest registration statistics once device-registration is enabled. |

### 4.1.31.2.28 configuring WeChat Wi-Fi hotspot support in WiNG captive portal

*captive-portal-mode commands*

WeChat is a popular messaging app used in China with more than 500 million installations. WeChat's WiFi hotspot solution allows businesses to provide Internet access to their customers. The WiNG captive portal can be configured to incorporate the WeChat WiFi hotspot, so that WeChat users, on their first connect to a WiNG access point, can automatically authenticate with the WeChat server through an intermediate server.

This section provides an example that shows the configurations required to be made on the WiNG portal to enable WeChat Wi-Fi hotspot.

1 Create an AAA policy re-directing the WiNG captive portal user to WeChat's AAA server for authentication, as shown in the following example:

```
nx9500-6C8809(config)#aaa-policy cloud2
nx9500-6C8809(config-aaa-policy-cloud2)#authentication server 1 host
cloud2.synchroweb.com secret 0 firmware
nx9500-6C8809(config-aaa-policy-cloud2)#show context
aaa-policy cloud2
authentication server 1 host cloud2.synchroweb.com secret 0 firmware
nx9500-6C8809(config-aaa-policy-cloud2)#

Note, Synchroweb is an independent software vendor (ISV), whose third-party
software is being used as the intermediate server. The AAA server and RADIUS
accounting server configured in AAA policy must be as per the specification
provided by the ISV.
```

2 Create a DNS whitelist, whitelisting WeChat's server name in order to initiate RADIUS authentication. The "qq.com" domain name is where WeChat server can be reached.

```
nx9500-6C8809(config)#dns-whitelist wxWL
nx9500-6C8809(config-dns-whitelist-wxWL)#permit cloud2.synchroweb.com
nx9500-6C8809(config-dns-whitelist-wxWL)#permit qq.com suffix
nx9500-6C8809(config-dns-whitelist-wxWL)#show context
dns-whitelist wxWL
permit qq.com suffix
permit cloud2.synchroweb.com
nx9500-6C8809(config-dns-whitelist-wxWL)#
```

3 Create a captive portal and associate the AAA policy and DNS whitelist created in steps 1 & 2, as shown in the following example:

```
nx9500-6C8809(config)#captive-portal wxCP
nx9500-6C8809(config-captive-portal-wxCP)#use aaa-policy cloud2
nx9500-6C8809(config-captive-portal-wxCP)#use dns-whitelist wxWL
```

4 Configure the following captive portal parameters:

```
nx9500-6C8809(config)#captive-portal wxCP
nx9500-6C8809(config-captive-portal-wxCP)#access-time 10
nx9500-6C8809(config-captive-portal-wxCP)#server host guest.extreme.com
nx9500-6C8809(config-captive-portal-wxCP)#webpage-location external
nx9500-6C8809(config-captive-portal-wxCP)#webpage external login http://
cloud2.synchroweb.com/wechat.nx/index.phpc=WING_TAG_CLIENT_MAC
```

```
nx9500-6C8809(config-captive-portal-wxCP)#)#show context
captive-portal wxCP
access-time 10
server host guest.extreme.com
webpage-location external
webpage external login http://cloud2.synchroweb.com/wechat.nx/
index.phpc=WING_TAG_CLIENT_MAC
use aaa-policy cloud2
use dns-whitelist wxWL
--More--
nx9500-6C8809(config-captive-portal-wxCP)#
```

Note, the login URL configured here must be as per the specifications provided by the ISV.

Note, the access-type remains unchanged (i.e radius, which is the default setting). The *access-time* is set to a minimum value (10 minutes in this example) in order to avoid the default value of 24 hours being applied, in case the RADIUS response does not contain the session-timeout attribute.

5 Create a WLAN and associate the captive portal created in step 3:

```
nx9500-6C8809(config)#wlan wxOpen
nx9500-6C8809(config-wlan-wxOpen)#ssid wxOpen
nx9500-6C8809(config-wlan-wxOpen)#vlan 200
nx9500-6C8809(config-wlan-wxOpen)##use captive-portal wxCP
nx9500-6C8809(config-wlan-wxOpen)#captive-portal-enforcement
nx9500-6C8809(config-wlan-wxOpen)#show context
wlan wxOpen
ssid wxOpen
vlan 200
bridging-mode local
encryption-type none
authentication-type none
use captive-portal wxCP
captive-portal-enforcement
nx9500-6C8809(config-wlan-wxOpen)#
```

Note, the modes of authentication and encryption remain unchanged (i.e none, which is the default setting for both parameters). Ensure captive-portal-enforcement is enabled on the WLAN.

**Related Commands**

| | |
|---|---|
| *AAA-POLICY* | Documents AAA policy configuration mode commands |
| *dns-whitelist* | Documents DNS whitelist configuration mode commands |
| *captive portal* | Documents captive portal configuration mode commands |
| *wlan* | Documents WLAN configuration mode commands |

### 4.1.31.2.29 configuring ExtremeGuest captive-portal

*captive-portal-mode commands*

This section documents the basic configurations required to deploy an *ExtremeGuest* (EGuest) setup. A typical EGuest deployment consists of the EGuest server, EGuest captive-portal database, and NOC adopting the access points. The EGuest server and database can be hosted only on the VX9000 platform.

In the following example, the EGuest server and database are hosted on the same device.

1 On the EGuest server/database host,
   a enable the EGuest daemon. When enabled, the EGuset server is up and running.

```
EG-Server-DB(config-device-02-EE-1A-7E-AE-5B)#eguest-server
```

   b apply a database-policy to enable the EGuest database.

```
EG-Server-DB(config-device-02-EE-1A-7E-AE-5B)#use database-policy default
```

   c configure the NTP server. This is to ensure time synchronization across replica-set members (this is mandatory in replica-set deployments and should be configured either on the replica-set members' device or profile context).

```
EG-Server-DB(config-device-02-EE-1A-7E-AE-5B)#ntp server time.nist.govt
```

2 On the NOC,
   a create an AAA policy with the following configurations:
      - Configure the EGuest server (configured in Step 1) as the authentication and accounting RADIUS server.

```
NOC(config-aaa-policy-EguestAAA)#authentication server 1 host EG-Server secret 0 extreme123
NOC(config-aaa-policy-EguestAAA)#accounting server 1 host EG-Server secret 0 extreme123
```

      - Configure the proxy-mode as 'through-controller'. When configured, all requests to the server are proxied through the NOC.

```
NOC(config-aaa-policy-EguestAAA)#authentication server 1 proxy-mode through-controller
NOC(config-aaa-policy-EguestAAA)#accounting server 1 proxy-mode through-controller

NOC(config-aaa-policy-EguestAAA)#show context
aaa-policy EguestAAA
accounting server 1 host EG-OnBServer secret 0 extreme123
accounting server 1 proxy-mode through-controller
authentication server 1 host EG-Server secret 0 extreme123
authentication server 1 proxy-mode through-controller
NOC(config-aaa-policy-EguestAAA)#
```

   b Create a DNS whitelist. Note, DNS whitelist configuration is required only if enabling OAuth on the EGuest captive-portal. When created and used on the EGuest captive-portal, the DNS whitelist renders social plugin buttons on the client prior to successful captive portal authentication.
      - Configure the following permit rules:

```
NOC(config-dns-whitelist-EguestDNS)#permit fbstatic-a.akamaihd.net
NOC(config-dns-whitelist-EguestDNS)#permit connect facebook.net
NOC(config-dns-whitelist-EguestDNS)#permit facebook.com suffix
NOC(config-dns-whitelist-EguestDNS)#permit fbcdn.net suffix
```

```
NOC(config-dns-whitelist-EguestDNS)#permit googleapis.com suffix
NOC(config-dns-whitelist-EguestDNS)#permit google.com suffix
NOC(config-dns-whitelist-EguestDNS)#permit googleusercontent.com suffix
NOC(config-dns-whitelist-EguestDNS)#permit linkedin.com suffix
NOC(config-dns-whitelist-EguestDNS)#permit static.licdn.com
NOC(config-dns-whitelist-EguestDNS)#permit twitter.com suffix
NOC(config-dns-whitelist-EguestDNS)#permit twimg.com suffix
NOC(config-dns-whitelist-EguestDNS)#permit instagramstatic-a.akamaihd.net
NOC(config-dns-whitelist-EguestDNS)#permit instagram.com suffix
NOC(config-dns-whitelist-EguestDNS)#permit ssl.gstatic.com
NOC(config-dns-whitelist-EguestDNS)#permit extremenetworks.com suffix
NOC(config-dns-whitelist-EguestDNS)#permit local.extreme.com
```

c Create a captive-portal with the following configurations:

- Specify the captive-portal server.

```
NOC(config-captive-portal-EguestCP)#server host guest.extreme.com
```

- Use the AAA policy created in Step 2 a.

```
NOC(config-captive-portal-EguestCP)#use aaa-policy EguestAAA
```

- Enable social-media authentication. This setting is optional.

```
NOC(config-captive-portal-EguestCP)#oauth
```

- Use the DNS whitelist created in Step 2 b. Note, the DNS whitelist is required only if enabling OAuth on the captive-portal.

```
NOC(config-captive-portal-EguestCP)#use dns-whitelist EguestDNS
```

- Configure the webpage-location as advanced. Note, webpage-location should be 'advanced' if using pages created with EGuest splash templates.

```
NOC(config-captive-portal-EguestCP)#webpage-location advanced
```

d Create a WLAN policy with the following configurations:

- Enable MAC authentication.

```
NOC(config-wlan-EguestWLAN)#authentication-type mac
```

- Use the AAA policy created in Step 2 a.

```
NOC(config-wlan-EguestWLAN)#use aaa-policy EguestAAA

--When used, access points/controllers forward registration requests to the EGuest
server specified in the AAA policy. However, ensure that the registration >
external > follow-aaa option is configured on the WLAN. See below.

NOC(config-wlan-EguestWLAN)#registration external follow-aaa

--This enables the use of the Authentication and Accounting servers specified
in the AAA policy applied on the WLAN.
```

- Use the captive-portal created in Step 2 c.

```
NOC(config-wlan-EguestWLAN)#use captive-portal EguestCP
```

- Enable captive-portal enforcement with fall-back.

```
NOC(config-wlan-EguestWLAN)#captive-portal-enforcement fall-back
```

- Configure the following guest registration parameters:

```
NOC(config-wlan-EguestWLAN)#registration device group-name Eguest expiry-time
4320 agreement-refresh 1440

--This is the RADIUS group assigned to registered users post authentication.

NOC(config-wlan-EguestWLAN)#show context
wlan EguestWLAN
ssid _EXTREME-GUEST-NRF2017
vlan 1
bridging-mode local
encryption-type none
authentication-type mac
no answer-broadcast-probes
no client-client-communication
wireless-client hold-time 300
use aaa-policy EguestAAA
use captive-portal EguestCP
captive-portal-enforcement fall-back
registration device group-name Eguest expiry-time 4320 agreement-refresh 1440
registration external follow-aaa
mac-authentication cached-credentials
NOC(config-wlan-EguestWLAN)#
```

e In the NOC's self context, configure the EGuest server.

```
NOC(config-device-74-67-F7-5C-64-4A)#eguest-server host 1 EG-Server https
```

3 In the Access Point's device or profile context,

a Use the captive-portal configured in Step 2 c.

```
Eguest-AP(config-device-74-67-F7-5C-64-4A)#use captive-portal EguestCP
```

4 To view EGuest registration status and statistics, on the EGuest server, use the following commands:

```
EG-Server-DB#show eguest registration statistics
EG-Server-DB#show eguest registration status
```

5 To clear EGuest registration statistics, on the EGuest server, use the following command:

```
EG-Server-DB#clear eguest registration statistics
```

**Related Commands**

| | |
|---|---|
| *eguest-server (VX9000 only)* | Documents the eguest-server command. When used in the EGuest server's device/profile context, without the 'host' option, it enables the EGuest daemon. When used on the NOC along with the 'host' option, it points to the EGuest server. |
| *AAA-POLICY* | Documents AAA policy configuration commands |
| *dns-whitelist* | Documents DNS-whitelist configuration commands |
| *captive portal* | Documents captive-portal configuration commands |
| *wlan* | Documents WLAN configuration commands |
| *eguest* | Documents the *show > eguest* command outputs |

## 4.1.32 clear

*Global Configuration Commands*

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

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
clear event-history
```

**Parameters**

- `clear event-history`

| | |
|---|---|
| event-history | Clears the event history file |

**Example**

```
rfs4000-880DA7(config)#show event-history
EVENT HISTORY REPORT
Generated on '2017-06-09 14:23:31 IST' by 'admin'

2017-06-09 14:16:28 rfs4000-880DA7  SYSTEM     LOGIN                Successfully
logged in user 'admin' with privilege 'superuser' from 'ssh'
2017-06-09 14:06:21 rfs4000-880DA7  DEVICE     OFFLINE              Device B4-C7-
99-71-17-28(ap8132-711728) is offline, last seen:10 minutes ago on switchport
ap7522-8330A4:ge1
2017-06-09 13:46:15 rfs4000-880DA7  SYSTEM     CONFIG_REVISION      Configuration
revision updated to 10 from 9
2017-06-09 13:36:12 rfs4000-880DA7  SYSTEM     CONFIG_REVISION      Configuration
revision updated to 9 from 8
2017-06-09 13:26:09 rfs4000-880DA7  SYSTEM     CONFIG_COMMIT        Configuration
commit by user 'cfgd' (site apply config diff) from '127.0.0.1'
2017-06-09 13:16:06 rfs4000-880DA7  DEVICE     UNADOPTED           Device('ap8132-
711728'/'ap81xx'/B4-C7-99-71-17-28) at rf-domain:'TechPubs' unadopted. Radios:
Count=2, Bss: B4-C7-99-78-53-10|B4-C7-99-78-53-70|
2017-06-09 13:10:047     ap8132-711728  SYSTEM     WARM_START          System Warm
Start Reason : Upgrade done, reloading... (user: system @ rfs4000-880DA7)
Timestamp: Nov 04 11:32:27 2016
2017-06-09 13:06:03 rfs4000-880DA7  DEVICE    DEVICE_UPGRADE_REBOOT DEVICEUPGRADE:
ap81xx mac B4-C7-99-71-17-28 Device upgrade rebooting

--More--
rfs4000-880DA7(config)#

rfs4000-880DA7(config)#clear event-history

rfs4000-880DA7(config)#show event-history
EVENT HISTORY REPORT
Generated on '2017-06-09 14:27:05 IST' by 'admin'

rfs4000-880DA7(config)#
```

## 4.1.33 client-identity

*Global Configuration Commands*

With an increase in *Bring Your Own Device* (BYOD) corporate networks, there is a parallel increase in the number of possible attack scenarios within the network. BYOD devices are inherently unsafe, as the organization's security mechanisms do not extend to these personal devices deployed in the corporate wireless network. Organizations can protect their network by limiting how and what these BYODs can access on and through the corporate network.

Device fingerprinting assists administrators by controlling how BYOD devices access a corporate wireless domain.

Device fingerprinting uses DHCP options sent by the client in request or discover packets to derive a unique signature specific to device class. For example, Apple devices have a different signature from Android devices. The signature is used to classify the devices and assign permissions and restrictions on each device class.

The following table summarizes the commands available for creating and configuring a set of new client identity parameters:

**Table 4.12** *Client-Identity-Config Commands*

| Command | Description | Reference |
|---|---|---|
| *client-identity* | Creates a new client identity and enters its configuration mode | *page 4-148* |
| *client-identity-mode commands* | Invokes the client identity policy configuration mode commands | *page 4-150* |
| *client-identity-group* | Creates a new client identity group and enters its configuration mode | *page 4-156* |

### 4.1.33.1 client-identity

*client-identity*

Creates a new client identity and enters its configuration mode. Client identity is a set of unique fingerprints used to identify a class of devices. This information is used to configure permissions and access rules for the identified class of devices in the network. The client-identity feature enables device fingerprinting.

Device fingerprinting is a technique of collecting, analyzing, and identifying traffic patterns originating from remote computing devices. When enabled, device fingerprinting helps to identify a wireless client's device type. There are two methods of fingerprinting devices: Active and Passive.

Active fingerprinting is based on the fact that traffic patterns vary with varying device types. It involves the sending of requests (HTTP, etc.) to devices (clients) and analyzing their response to determine the device type. For example, an invalid request is sent to a device, and its error response is analyzed to identify the device type. Since active device fingerprinting involves sending of packets, the probability of the network getting flooded is very high, especially when many devices are being fingerprinted simultaneously.

Passive fingerprinting involves monitoring of devices to check for known traffic patterns specific to devices based on the protocol, driver implementation, etc. This method accurately classifies a client's TCP/IP configuration, OS fingerprints, wireless settings etc. No packets are sent to the device. Some of the commonly used protocols for passive device fingerprinting are, TCP, DHCP, HTTP, etc.

This feature implements DHCP device fingerprinting, which relies on specific information sent by a wireless client when acquiring IP address and other configuration information from a DHCP server. The feature uses the DHCP options sent by the wireless client in the DHCP request or discover packets to derive a unique signature specific to the class of devices. For example, Apple devices have a different signature than Android devices. This unique signature can then be used to classify the devices and assign permissions and restrictions on each device class.

The WiNG software provides a set of built-in device fingerprints that load by default and identify client device types. Use the *service > show > client-identity-defaults* command to view default client identity fingerprints.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
client-identity <CLIENT-IDENTITY-NAME>
```

**Parameters**

- `client-identity <CLIENT-IDENTITY-NAME>`

| | |
|---|---|
| client-identity <CLIENT-IDENTITY-NAME> | Creates a new client identity policy and enters its configuration mode<br>• <CLIENT-IDENTITY--NAME> – Specify a client identity policy name. If the client identity policy does not exist, it is created. |

**Usage Guidelines**

The following points should be considered when configuring the client identity (device fingerprinting) feature:

- Ensure that DHCP is enforced on the WLANs. For more information on enforcing DHCP on WLANs, see *enforce-dhcp*.
- Successful identification of different device types depends on the uniqueness of the configured fingerprints. DHCP fingerprinting identifies clients based on the patterns (fingerprints) in the DHCP discover and request messages sent by clients. If different operating systems have the same fingerprints. it will be difficult to identity the device type.
- When associating client identities with a role policy, ensure that the profile/device, under which the role policy is being used, also has an associated client identity group (containing all the client identities used by the role policy).

**Example**

```
rfs4000-229D58(config)#client-identity test
rfs4000-229D58(config-client-identity-test)#?
Client Identity Mode commands:
  dhcp                      Add a DHCP option based match criteria
  dhcp-match-message-type   Specify DHCP message type to match
  no                        Negate a command or set its defaults

  clrscr                    Clears the display screen
  commit                    Commit all changes made in this session
  do                        Run commands from Exec mode
  end                       End current mode and change to EXEC mode
  exit                      End current mode and down to previous mode
  help                      Description of the interactive help system
  revert                    Revert changes
  service                   Service Commands
  show                      Show running system information
  write                     Write running configuration to memory or terminal

rfs4000-229D58(config-client-identity-test)#
```

Use the *service > show > client-identity-defaults* command to view default, built-in, system-provided client identity fingerprints:

```
nx9500-6C8809#service show client-identity-defaults
client-identity Android-2-1
 dhcp 1 message-type request option 55 exact hexstring 0103061c21333a3b79
 dhcp 6 message-type request option 60 exact ascii dhcpcd\ 4.0.1
client-identity Android-2-2
 dhcp 1 message-type request option 55 exact hexstring 01792103061c333a3b
 dhcp 6 message-type request option 60 exact ascii dhcpcd\ 4.0.15
client-identity Android-2-3
 dhcp 3 message-type request option 55 exact hexstring 01792103061c333a3b
 dhcp 6 message-type request option 60 exact ascii dhcpcd\ 4.0.15
 dhcp 1 message-type request option-codes exact hexstring 353d32393c37
 dhcp 2 message-type request option-codes exact hexstring 353d3236393c37
 dhcp 10 message-type request option-codes exact hexstring 353d3236393c0c37
--More--
nx9500-6C8809#
```

### 4.1.33.2 client-identity-mode commands

- *client-identity*

The following table summarizes client identity configuration mode commands:

**Table 4.13** *Client-Identity-Mode Commands*

| Command | Description | Reference |
|---|---|---|
| *dhcp* | Configures the DHCP option match criteria for device fingerprinting | *page 4-151* |
| *dhcp-match-message-type* | Configures the DHCP message type for device fingerprinting | *page 4-154* |
| *no* | Removes the DHCP option (used for client identification) configurations | *page 4-155* |

### 4.1.33.2.1 dhcp

*client-identity-mode commands*

Configures the DHCP option match criteria (signature) for the discover and request message types received from wireless clients

When accessing a network, DHCP discover and request messages are passed between wireless clients and the DHCP server. These messages contain DHCP options and option values that differ from device to device and are based on the DHCP implementation in the device's *operating system* (OS). Options and option values contained in a client's messages are parsed and compared against the configured DHCP option values to identify the device. Once a device type is identified, the wireless client database is updated with the discovered device type.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
dhcp <1-16> message-type [discover|request] [option|option-codes]
dhcp <1-16> message-type [discover|request] [option <1-254>|option-codes]
[contains|exact|starts-with] [ascii|hexstring] <WORD>
```

**Parameters**

```
• dhcp <1-16> message-type [discover|request] [option <1-254>|option-codes]
[contains|exact|starts-with] [ascii|hexstring] <WORD>
```

| | |
|---|---|
| dhcp <1-16> | Adds a DHCP option match criteria signature<br>• <1-16> – Specify an index for this DHCP match criteria from 1 - 16.<br>A maximum of 16 match criteria can be configured. |
| message-type [discover\|request] | Specifies the message type to which this DHCP match criteria is applicable<br>• discover – Applies this match criteria to DHCP discover messages only. Indicates that the fingerprint is only checked with any DHCP discover messages received from any device.<br>• request – Applies this match criteria to DHCP request messages only. Indicates that the fingerprint is only checked with any DHCP request messages received from any device.<br>It is recommended to configure client-identity with request messages, because clients rarely send discover messages.<br>If the message type is not specified, the fingerprint is checked with all message types (DHCP request and DHCP discover). |
| option <1-254> | The following keywords are common to the 'discover' and 'request' message types:<br>• option – Configures a DHCP option value, which is used as the match criteria<br>  • <1-254> – Configures a code for this DHCP option from 1 - 254 (except option 53) |

| | |
|---|---|
| option-codes | The following keyword is common to the 'discover' and 'request' message types:<br>• option-codes – Matches criteria based on the DHCP option codes contained in the client's discover/request messages<br>Devices pass options in their DHCP discover/request messages as option codes, option types, and option value sets. These option codes are extracted and matched against the configured DHCP option codes and a fingerprint is derived. This derived fingerprint is used to identify the device. |
| contains | The following keyword is common to the 'discover' and 'request' message types:<br>• contains – Specifies that the DHCP options received in the client's discover/request messages contains the configured option code string |
| exact | The following keyword is common to the discover and request message types:<br>• exact – Specifies that the DHCP options received in the client's discover/request messages is an exact match with the configured option code string |
| starts-with | The following keyword is common to the 'discover' and 'request' message types:<br>• starts-with – Specifies that the DHCP options received in the client's discover/request messages starts with the configured option code string |
| ascii <WORD> | The following keywords are common to the 'contains', 'exact', and 'starts-with' parameters:<br>• ascii – Configures the DHCP option in the ASCII format<br>• <WORD> – Specify the DHCP option ASCII value to match. |
| hexstring <WORD> | The following keywords are common to the 'contains', 'exact', and 'starts-with' parameters:<br>• hexstring – Configures the DHCP option in the hexa-decimal format<br>• <WORD> – Specify the DHCP option hexstring value to match. |

**Usage Guidelines**

The following DHCP options are useful for identifying different device types:

- Option 55: Used by a DHCP client to request values for specific configuration parameters. It is a list of DHCP option codes and can be in the client's order of preference.
- Client configured list of DHCP options (all options parsed into a hex string).
- Option 60: Vendor class identifier. Used to identify the vendor and functionality of a DHCP client (some devices do not set the value of this field).

Though it is possible to use any option to configure a device fingerprint, the use of a combination of one or more of the preceding options to define a device is recommended.

**Example**

```
rfs4000-229D58(config-client-identity-test)#dhcp 1 message-type request option
60 exact ascii MSFT\5.0
rfs4000-229D58(config-client-identity-test)#dhcp 2 message-type discover option
 2 exact hexstring 012456c22c44

rfs4000-229D58(config-client-identity-test)#show context
client-identity test
 dhcp 2 message-type discover option 2 exact hexstring 012456c22c44
 dhcp 1 message-type request option 60 exact ascii MSFT5.0
rfs4000-229D58(config-client-identity-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes a DHCP option signature (match criteria) |

### 4.1.33.2.2 dhcp-match-message-type

*client-identity-mode commands*

Configures the DHCP message type to match

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
dhcp-match-message-type [all|any|discover|request]
```

**Parameters**

- `dhcp-match-message-type [all|any|discover|request]`

| | |
|---|---|
| dhcp-match-message-type [all\|any\|discover\|request] | Specifies the DHCP message type to consider for matching<br>• all – Matches all message types: discover and request. Indicates that the fingerprint is checked with both the DHCP request and the DHCP discover message.<br>• any – Matches any message type: discover or request. Indicates that the fingerprint is checked with either the DHCP request or the DHCP discover message.<br>• discover – Matches discover messages only. Client matches the client identity only if the discover message sent by the client matches. Values configured for request messages are ignored.<br>• request – Matches request messages only. Client matches the client identity only if the request message sent by the client matches. Values configured for discover messages are ignored. |

**Example**

```
rfs4000-229D58(config-client-identity-test)#dhcp-match-message-type all

rfs4000-229D58(config-client-identity-test)#show context
client-identity test
 dhcp 2 message-type discover option 2 exact hexstring 012456c22c44
 dhcp 1 message-type request option 60 exact ascii MSFT5.0
 dhcp-match-message-type all
rfs4000-229D58(config-client-identity-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the DHCP message type to match |

#### 4.1.33.2.3 no

*client-identity-mode commands*

Removes the DHCP options match criteria configurations

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
no [dhcp <1-16>|dhcp-match-message-type]
```

**Parameters**

- `no [dhcp <1-16>|dhcp-match-message-type]`

| | |
|---|---|
| dhcp <1-16> | Removes the DHCP option match criteria rule identified by the <1-16> keyword<br>• <1-16> – Specify the DHCP option match criteria rule index |
| dhcp-match-message-type | Removes the DHCP message type to match |

**Example**

The following example shows the client identity 'test' settings before the 'no' commands are executed:

```
rfs4000-229D58(config-client-identity-test)#show context
client-identity test
 dhcp 2 message-type discover option 2 exact hexstring 012456c22c44
 dhcp 1 message-type request option 60 exact ascii MSFT5.0
 dhcp-match-message-type all
rfs4000-229D58(config-client-identity-test)#
```

The following example shows the client identity 'test' settings after the 'no' commands are executed:

```
rfs4000-229D58(config-client-identity-test)#no dhcp 2

rfs4000-229D58(config-client-identity-test)#no dhcp-match-message-type

rfs4000-229D58(config-client-identity-test)#show context
client-identity test
 dhcp 1 message-type request option 60 exact ascii MSFT5.0
rfs4000-229D58(config-client-identity-test)#
```

**Related Commands**

| | |
|---|---|
| *dhcp* | Configures the DHCP option match criteria for device fingerprinting |
| *dhcp-match-message-type* | Configures the DHCP message type for device fingerprinting |

## 4.1.34 client-identity-group

*client-identity*

The following table summarizes commands available to enter the client identity group configuration mode:

**Table 4.14** *Client-Identity-Group Config Commands*

| Command | Description | Reference |
|---|---|---|
| *client-identity-group* | Creates a new client identity group and enters its configuration mode | *page 4-157* |
| *client-identity-group-mode commands* | Invokes the client identity group configuration mode commands | *page 4-158* |
| *client-identity* | Creates new client identity policy and enters its configuration mode | *page 4-147* |

### 4.1.34.1 client-identity-group

*client-identity-group*

Configures a new client identity group

A client identity group is a collection of client identities. Each client identity included in a client identity group is set a priority value that indicates the priority for that identity when device fingerprinting.

Device Fingerprinting relies on specific information sent by a wireless client when acquiring IP address and other configuration information from a DHCP server. The feature uses the DHCP options sent by the wireless client in the DHCP request or discover packets to derive a unique signature specific to the class of devices. For example, Apple devices have a different signature than Android devices. This unique signature can then be used to classify the devices and assign permissions and restrictions on each device class.

A client identity group can be attached to a profile or device, enabling device fingerprinting on them.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
client-identity-group <CLIENT-IDENTITY-GROUP-NAME>
```

**Parameters**

- `client-identity-group <CLIENT-IDENTITY-GROUP-NAME>`

| | |
|---|---|
| client-identity-group <CLIENT-IDENTITY-GROUP-NAME> | Creates a new client identity group and enters its configuration mode<br>• <CLIENT-IDENTITY-GROUP-NAME> – Specify a client identity group name. If the group does not exist, it is created. |

**Example**

```
rfs4000-229D58(config)#client-identity-group test
rfs4000-229D58(config-client-identity-group-test)#
Client Identity group Mode commands:
  client-identity  Client identity (DHCP Device Fingerprinting)
  load             Load Client identity Fingerprints
  no               Negate a command or set its defaults

  clrscr           Clears the display screen
  commit           Commit all changes made in this session
  do               Run commands from Exec mode
  end              End current mode and change to EXEC mode
  exit             End current mode and down to previous mode
  help             Description of the interactive help system
  revert           Revert changes
  service          Service Commands
  show             Show running system information
  write            Write running configuration to memory or terminal

rfs4000-229D58(config-client-identity-group-test)#
```

### 4.1.34.2 client-identity-group-mode commands

*client-identity-group*

The following table summarizes client identity group configuration mode commands:

**Table 4.15** *Client-Identity-Group-Mode Commands*

| Command | Description | Reference |
|---|---|---|
| *client-identity* | Associates an existing and configured client identity (device fingerprint) with this client identity group | *page 4-159* |
| *load* | Loads default (system-provided) client identity fingerprints | *page 4-161* |
| *no* | Removes the client identity associated with this client identity group | *page 4-155* |

#### 4.1.34.2.1 client-identity

*client-identity-group-mode commands*

Associates an existing and configured client identity (device fingerprint) with this client identity group

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
client-identity <CLIENT-IDENTITY-NAME> precedence <1-10000>
```

**Parameters**

- `client-identity <CLIENT-IDENTITY-NAME> precedence <1-10000>`

| | |
|---|---|
| client-identity <CLIENT-IDENTITY-NAME> | Associates a client identity with this group<br>• <CLIENT-IDENTITY-NAME> – Specify a client identity name (should be existing and configured) |
| precedence <1-10000> | Determines the order in which client identity is used<br>• <1-10000> – Specify this client identity precedence from <1-10000>.<br>The client identity rule is applied based on its precedence value. Lower the value, higher is the precedence. Therefore, a client identity with precedence 5 gets precedence over a client identity having precedence 20. |

**Example**

The following example shows two client identities created and configured:

```
rfs4000-229D58(config)#show context
!
! Configuration of RFS4000 version 5.9.1.0-029R
!
!
version 2.5
!
!
client-identity TestClientIdentity
 dhcp 1 message-type request option-codes exact hexstring 5e4d36780b3a7f
!
client-identity test
 dhcp 2 message-type discover option 2 exact hexstring 012456c22c44
 dhcp 1 message-type request option 60 exact ascii MSFT5.0
 dhcp-match-message-type all
!
client-identity-group ClientIdentityGroup
 client-identity TestClientIdentity precedence 1
!
client-identity-group test
!
ip access-list BROADCAST-MULTICAST-CONTROL
 permit tcp any any rule-precedence 10 rule-description "permit all TCP traffic"
 --More--
rfs4000-229D58(config)#
```

The following example associates client identity ‘test’ with the client identity group ‘test’:

```
rfs4000-229D58(config-client-identity-group-test)#client-identity test precedence
1
```

The following example shows the client identity group ‘test’ with two associated client identities having precedence 1 and 2:

```
rfs4000-229D58(config-client-identity-group-test)#client-identity
TestClientIdentity precedence 2
rfs4000-229D58(config-client-identity-group-test)#show context
client-identity-group test
 client-identity test precedence 1
 client-identity TestClientIdentity precedence 2
rfs4000-229D58(config-client-identity-group-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the client identity associated with the client identity group |

#### 4.1.34.2.2 load

*client-identity-group-mode commands*

Loads default (built-in, system-provided) client identity fingerprints. This option is enabled by default.

The WiNG software provides some built-in client identity fingerprints that are automatically loaded when the client identity group if applied to a device (either directly or through the profile).

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
load default-fingerprints
```

**Parameters**

- `load default-fingerprints`

| | |
|---|---|
| load default-fingerprints | Loads client identity default fingerprints. This option is enabled by default. |

**Example**

The auto-load default fingerprints option is enabled by default, as shown in the following example:

```
nx9500-6C8809(config-client-identity-group-test)#show context
client-identity-group test
 load default-fingerprints
nx9500-6C8809(config-client-identity-group-test)#
```

In scenarios where only customized client identities are to be applied, use the *no > load > default-fingerprints* command to disable auto-loading of default device fingerprints.

```
nx9500-6C8809(config-client-identity-group-test)#no load default-fingerprints

nx9500-6C8809(config-client-identity-group-test)#show context
client-identity-group test
 no load default-fingerprints
nx9500-6C8809(config-client-identity-group-test)#
```

Use the *service > show > client-identity-defaults* command to view default client identity fingerprints:

```
nx9500-6C8809#service show client-identity-defaults
client-identity Android-2-1
 dhcp 1 message-type request option 55 exact hexstring 0103061c21333a3b79
 dhcp 6 message-type request option 60 exact ascii dhcpcd\ 4.0.1
client-identity Android-2-2
 dhcp 1 message-type request option 55 exact hexstring 01792103061c333a3b
 dhcp 6 message-type request option 60 exact ascii dhcpcd\ 4.0.15
client-identity Android-2-3
 dhcp 3 message-type request option 55 exact hexstring 01792103061c333a3b
 dhcp 6 message-type request option 60 exact ascii dhcpcd\ 4.0.15
 dhcp 1 message-type request option-codes exact hexstring 353d32393c37
 dhcp 2 message-type request option-codes exact hexstring 353d3236393c37
 dhcp 10 message-type request option-codes exact hexstring 353d3236393c0c37
--More--
nx9500-6C8809#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables automatic loading of default client identity fingerprints |

### 4.1.34.2.3 no

*client-identity-group-mode commands*

Removes the client identity associated with the client identity group

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
no [client-identity|load]

no client-identity <CLIENT-IDENTITY-NAME> precedence <1-10000>

no load default-fingerprints
```

**Parameters**

- `no client-identity <CLIENT-IDENTITY-NAME> precedence <1-10000>`

| | |
|---|---|
| no client-identity <CLIENT-IDENTITY-NAME> precedence <1-10000> | Disassociates a specified client identity from this client identity group<br>• <CLIENT-IDENTITY-NAME> – Specify the client identity name.<br>• precedence <1-10000> – Specify the above specified client identity's precedence value from <1-10000>.<br>The client identity rule is applied based on its precedence value. Lower the value, higher is the precedence. Therefore, a client identity with precedence 5 gets precedence over a client identity having precedence 20. |

- `no load default-fingerprints`

| | |
|---|---|
| no load default-fingerprints | Disables automatic loading of built-in, system-provided client identity fingerprints |

**Example**

```
rfs4000-229D58(config-client-identity-group-test)#show context
client-identity-group test
 client-identity test precedence 1
rfs4000-229D58(config-client-identity-group-test)#

rfs4000-229D58(config-client-identity-group-test)#no client-identity test
rfs4000-229D58(config)#
```

**Related Commands**

| | |
|---|---|
| *client-identity* | Associates an existing and configured client identity (device fingerprint) with this client identity group |
| *load* | Loads default (built-in, system-provided) client identity fingerprints. This option is enabled by default. |

## 4.1.35 clone

*Global Configuration Commands*

Creates a replica of an existing object or device. The configuration of the new object or device is an exact copy of the existing object or device configuration. Use this command to copy existing configurations and then modifying only the required parameters.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
clone [TLO|device]

clone TLO <EXISTING-OBJECT-NAME> <NEW-OBJECT-NAME>

clone device <EXISTING-DEVICE-MAC/NAME> <NEW-DEVICE-MAC>
```

**Parameters**

- `clone TLO <EXISTING-OBJECT-NAME> <NEW-OBJECT-NAME>`

| | |
|---|---|
| TLO <EXISTING-OBJECT-NAME> <NEW-OBJECT-NAME> | Creates a new TLO by cloning an existing top-level object. The new object has the same configuration as the cloned object.<br>• <EXISTING-OBJECT-NAME> – Specify the existing object's (to be cloned) name<br>• <NEW-OBJECT-NAME> – Provide the new object's name.<br>Enter *clone* and press Tab to list objects available for cloning. |

- `clone device <EXISTING-DEVICE-MAC/NAME> <NEW-DEVICE-MAC>`

| | |
|---|---|
| device <EXISTING-DEVICE-MAC/NAME> <NEW-DEVICE-MAC> | Configures a new device based on an existing device configuration<br>• <EXISTING-DEVICE-MAC/NAME> – Specify the existing device's name or MAC address (the device to be cloned)<br>• <NEW-DEVICE-MAC> – Provide the new device's MAC address.<br>Enter *clone > device* and press Tab to list devices available for cloning. |

**Example**

```
nx9500-6C8809(config)#clone rf_domain TechPubs Cloned_TechPubs2
nx9500-6C8809(config)#show context
!
! Configuration of NX9500 version 5.9.1.0-008B
!
!
version 2.5
!
.....................................................................................
rf-domain TechPubs
 location SanJose
 timezone America/Los_Angeles
 country-code us
!
rf-domain Cloned_TechPubs2
 location SanJose
--More--
nx9500-6C8809(config)#
```

## 4.1.36 crypto-cmp-policy

*Global Configuration Commands*

Creates a crypto *Certificate Management Protocol* (CMP) policy and enters its configuration mode

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
crypto-cmp-policy <CRYPTO-CMP-POLICY-NAME>
```

**Parameters**

- `crypto-cmp-policy <CRYPTO-CMP-POLICY-NAME>`

| | |
|---|---|
| <CRYPTO-CMP-POLICY-NAME> | Specify the crypto CMP policy name. If the policy does not exist, it is created. |

**Example**

```
nx9500-6C8809(config)#crypto-cmp-policy CMP
nx9500-6C8809(config-cmp-policy-CMP)#?
CMP Policy Mode commands:
  ca-server              CMP CA Server configuration commands
  cert-key-size          Set key size for certificate request
  cert-renewal-timeout   Trigger a cert renewal request on timeout
  cross-cert-validate    Validate cross-cert using factory-cert
  no                     Negate a command or set its defaults
  subjectAltName         Configure subjectAltName value
  trustpoint             Trustpoint for CMP
  use                    Set setting to use

  clrscr                 Clears the display screen
  commit                 Commit all changes made in this session
  do                     Run commands from Exec mode
  end                    End current mode and change to EXEC mode
  exit                   End current mode and down to previous mode
  help                   Description of the interactive help system
  revert                 Revert changes
  service                Service Commands
  show                   Show running system information
  write                  Write running configuration to memory or terminal

nx9500-6C8809(config-cmp-policy-CMP)#
```

**Related Commands**

| | |
|---|---|
| *no* | Resets values or disables commands |

**NOTE:** For more information on the crypto CMP policy, see *Chapter 29, CRYPTO-CMP-POLICY*.

## 4.1.37 customize

*Global Configuration Commands*

Customizes the output of the summary CLI commands. Use this command to define the data displayed as a result of various show commands.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
customize [cdp-lldp-info-column-width|hostname-column-width|show-adoption-status|
show-wireless-client|show-wireless-client-stats|show-wireless-client-stats-rf|
show-wireless-meshpoint|show-wireless-meshpoint-accelerated-multicast|
show-wireless-meshpoint-neighbor-stats|show-wireless-meshpoint-neighbor-stats-rf
|show-wireless-mint-client|show-wireless-mint-client-stats|show-wireless-mint-
client-stats-rf|show-wireless-mint-portal|show-wireless-mint-portal-stats|
show-wireless-mint-portal-stats-rf|show-wireless-radio|show-wireless-radio-
stats|show-wireless-radio-stats-rf]

customize [cdp-lldp-info-column-width|hostname-column-width] <1-64>

customize show-adoption-status (adopted-by,ap-name <1-64>,cdp-lldp-info,config-
status,last-adoption,msgs,uptime,version)

customize show-wireless-client (ap-name <1-64>,auth,client-identity <1-32>,bss,
enc,hostname <1-64>,ip,last-active,location <1-64>,mac,radio-alias <3-67>,radio-
id,radio-type,role <1-32>,state,username <1-64>,vendor,vlan,wlan)

customize show-wireless-client-stats (hostname <1-64>,mac,rx-bytes,rx-errors,rx-
packets,rx-throughput,t-index,tx-bytes,tx-dropped,tx-packets,tx-throughput)

customize show-wireless-client-stats-rf (average-retry-number,error-rate,hostname
<1-64>,mac,noise,q-index,rx-rate,signal,snr,tx-rate)

customize show-wireless-meshpoint-accelerated-multicast (ap-hostname,group-addr,
mesh-name,neighbor-hostname,neighbor-ifid,radio-alias,radio-id,radio-mac,
subscriptions)

customize show-wireless-meshpoint (ap-mac,cfg-as-root,hops,hostname <1-64>,
interface-ids,is-root,mesh-name <1-64>,mpid,next-hop-hostname <1-64>,next-hop-
ifid,next-hop-use-time,path-metric,root-bound-time,root-hostname <1-64>,root-
mpid)

customize show-wireless-meshpoint-neighbor-stats (ap-hostname <1-64>,neighbor-
hostname <1-64>,neighbor-ifid,rx-bytes,rx-errors,rx-packets,rx-throughput,t-
index,tx-bytes,tx-dropped,tx-packets,tx-throughput)

customize show-wireless-meshpoint-neighbor-stats-rf (ap-hostname <1-64>,average-
retry-number,error-rate,neighbor-hostname <1-64>,neighbor-ifid,noise,q-index,rx-
rate,signal,snr,t-index,tx-rate)

customize show-wireless-mint-client (client-alias <1-64>,client-bss,portal-alias
<1-64>,portal-bss,up-time)

customize show-wireless-mint-client-stats (client-alias <1-64>,portal-alias <1-
64>,portal-bss,rx-bytes,rx-errors,rx-packets,rx-throughput,t-index,tx-bytes,tx-
dropped,tx-packets,tx-throughput)
```

```
customize show-wireless-mint-client-stats-rf (average-retry-number,client-alias
<1-64>,error-rate,noise,portal-alias <1-64>,portal-bss,q-index,rx-rate,signal,
snr,tx-rate)

customize show-wireless-mint-portal (client-alias <1-64>,client-bss,portal-alias
<1-64>,portal-bss,up-time)

customize show-wireless-mint-portal-stats (client-alias <1-64>,client-bss,portal-
alias <1-64>,rx-bytes,rx-errors,rx-packets,rx-throughput,t-index,tx-bytes,tx-
dropped,tx-packets,tx-throughput)

customize show-wireless-mint-portal-stats-rf (average-retry-number,client-alias
<1-64>,client-bss,error-rate,noise,portal-alias <1-64>,q-index,rx-rate,signal,
snr,tx-rate)

customize show-wireless-radio (adopt-to,ap-name <1-64>,channel,location <1-64>,
num-clients,power,radio-alias <3-67>,radio-id,radio-mac,rf-mode,state)

customize show-wireless-radio-stats (radio-alias <3-67>,radio-id,radio-mac,
rx-bytes,rx-errors,rx-packets,rx-throughput,tx-bytes,tx-dropped,tx-packets,
tx-throughput)

customize show-wireless-radio-stats-rf (average-retry-number,error-rate,noise,
q-index,radio-alias <3-67>,radio-id,radio-mac,rx-rate,signal,snr,t-index,tx-rate)
```

**Parameters**

- `customize [cdp-lldp-info-column-width|hostname-column-width] <1-64>`

| | |
|---|---|
| hostname-column-width <1-64> | Configures default width of the hostname column in all show command outputs<br>• <1-64> – Sets the hostname column width from 1 - 64 characters |
| cdp-lldp-info-column-width <1-64> | Configures the column width in the *show > cdp/lldp > [neighbor\|report]* command output<br>• <1-64> – Sets the column width from 1 - 64 characters |

- `customize show-adoption-status (adopted-by,ap-name <1-64>,cdp-lldp-info,config-status,last-adoption,msgs,uptime,version)`

| | |
|---|---|
| show-adoption-status | Configures the information displayed in the *show > adoption > status* command output. Select the columns (information) displayed from the following options: adopted-by, ap-name, cdp-lldp-info, config-status, last-adoption, msgs, uptime, and version. These are recursive parameters and you can select multiple options at a time.<br>The columns displayed by default are: Device-Name, Version, Config-Status, MSGS, Adopted-By, Last-Adoption, and Uptime.<br>Where ever available, you can optionally use the <1-64> parameter to set the column width. |

- `customize show-wireless-client (ap-name <1-64>,auth,client-identity <1-32>,bss,enc,hostname <1-64>,ip,last-active,location <1-64>,mac,radio-alias <3-67>,radio-id,radio-type,role <1-32>,state,username <1-64>,vendor,vlan,wlan)`

| | |
|---|---|
| show-wireless-client | Customizes the *show > wireless > client* command output<br>The columns displayed by default are: MAC, IPv4, Vendor, Radio-ID, WLAN. VLAN, and State. |
| ap-name <1-64> | Includes the ap-name column, which displays the name of the AP with which this client associates<br>• <1-64> – Sets the ap-name column width from 1 - 64 characters |
| auth | Includes the auth column, which displays the authorization protocol used by the wireless client |

| | |
|---|---|
| client-identity <1-32> | Includes the client-identity (device type) column, which displays details gathered from DHCP device fingerprinting feature (when enabled). For more information, see *client-identity*.<br>• <1-32> – Sets the client-identity column width from 1 - 32 characters |
| bss | Includes the BSS column, which displays the BSS ID the wireless client is associated with |
| enc | Includes the enc column, which displays the encryption suite used by the wireless client |
| hostname <1-64> | Includes the hostname column, which displays the wireless client's hostname<br>• <1-64> – Sets the hostname column width from 1 - 64 characters |
| ip | Includes the IP column, which displays the wireless client's current IP address |
| last-active | Includes the last-active column, which displays the time of last activity seen from the wireless client |
| location <1-64> | Includes the location column, which displays the location of the client's associated access points<br>• <1-64> – Sets the location column width from 1 - 64 characters |
| mac | Includes the MAC column, which displays the wireless client's MAC address |
| radio-alias <3-67> | Includes the radio-alias column, which displays the radio alias with the AP's hostname and radio interface number in the "HOSTNAME:RX" format<br>• <3-64> – Sets the radio-alias column width from 3 - 67 characters |
| radio-id | Includes the radio-id column, which displays the radio ID with the AP's MAC address and radio interface number in the "AA-BB-CC-DD-EE-FF:RX" format |
| radio-type | Includes the radio-type column, which displays the wireless client's radio type |
| role <1-32> | Includes the role column, which displays the client's role<br>• <1-32> – Sets the role column width from 1 - 32 characters |
| state | Includes the state column, which displays the wireless client's current availability state |
| username <1-64> | Includes the username column, which displays the wireless client's username<br>• <1-64> – Specify the username column width from 1 - 64 characters. |
| vendor | Includes the vendor column, which displays the wireless client's vendor ID |
| vlan | Includes the VLAN column, which displays the wireless client's assigned VLAN |
| wlan | Includes the WLAN column, which displays the wireless client's assigned WLAN |

```
• customize show-wireless-client-stats (hostname <1-64>,mac,rx-bytes,rx-errors,
rx-packets,rx-throughput,t-index,tx-bytes,tx-dropped,tx-packets,tx-throughput)
```

| | |
|---|---|
| show-wireless-client-stats | Customizes the *show > wireless > client > statistics* command output<br>The columns displayed by default are: MAC, Tx bytes, RX bytes, Tx pkts, Rx pkts, and Tx bps, RX bps, T-Index, and Dropped pkts. |
| hostname <1-64> | Includes the hostname column, which displays the wireless client's hostname<br>• <1-64> – Sets the hostname column width from 1 - 64 characters |
| mac | Includes the MAC column, which displays the wireless client's MAC address |
| rx-bytes | Includes the rx-bytes column, which displays the total number of bytes received by the wireless client |

| | |
|---|---|
| rx-errors | Includes the rx-error column, which displays the total number of errors received by the wireless client |
| rx-packets | Includes the rx-packets column, which displays the total number of packets received by the wireless client |
| rx-throughput | Includes the rx-throughput column, which displays the receive throughput at the wireless client |
| t-index | Includes the t-index column, which displays the traffic utilization index at the particular wireless client |
| tx-bytes | Includes the tx-bytes column, which displays the total number of bytes transmitted by the wireless client |
| tx-dropped | Includes the tx-dropped column, which displays the total number of dropped packets by the wireless client |
| tx-packets | Includes the tx-packets column, which displays the total number of packets transmitted by the wireless client |
| tx-throughput | Includes the tx-throughput column, which displays the transmission throughput at the wireless client |

- `customize show-wireless-client-stats-rf (average-retry-number,error-rate,host-name <1-64>,mac,noise,q-index,rx-rate,signal,snr,tx-rate)`

| | |
|---|---|
| show-wireless-client-stats-rf | Customizes the *show > wireless > client > statistics > rf* command output<br>The columns displayed by default are: MAC, Signal (dBm), Noise (dBm), SNR (dB), TX Rate (Mbps), Retry Avg, Errors (pps), and Q-Index (%). |
| average-retry-number | Includes the average-retry-number column, which displays the average number of retransmissions made per packet |
| error-rate | Includes the error-rate column, which displays the rate of error for the wireless client |
| hostname <1-64> | Includes the hostname column, which displays the wireless client's hostname<br>• <1-64> – Sets the hostname column width from 1 - 64 characters |
| mac | Includes the MAC column, which displays the wireless client's MAC address |
| noise | Includes the noise column, which displays the noise (in dBm) as detected by the wireless client |
| q-index | Includes the q-index column, which displays the RF quality index<br>Higher values indicate better RF quality. |
| rx-rate | Includes the rx-rate column, which displays the receive rate at the particular wireless client |
| signal | Includes the signal column, which displays the signal strength (in dBm) at the particular wireless client |
| snr | Includes the snr column, which displays the *signal to noise* (SNR) ratio (in dB) at the particular wireless client |
| tx-rate | Includes the tx-rate column, which displays the packet transmission rate at the particular wireless client |

```
• customize show-wireless-meshpoint-accelerated-multicast (ap-hostname,group-
addr,mesh-name,neighbor-hostname,neighbor-ifid,radio-alias,radio-id,radio-mac,
subscriptions)
```

| | |
|---|---|
| show-wireless-meshpoint-accelerated-multicast | Configures the information displayed in the *show > wireless > meshpoint > accelerated multicast* command output. Select the columns (information) displayed from the following options: ap-hostname, group-addr, mesh-name, neighbor-hostname, neighbor-ifid, radio-alias, radio-id, radio-mac, subscriptions. These are recursive parameters and you can select multiple options at a time.<br>The columns displayed by default are: Mesh, Radio, Neighbor-IFID, Neighbor-Hostname, Group-MAC, and Subscriptions. |

```
• customize show-wireless-meshpoint (ap-mac,cfg-as-root,hops,hostname <1-64>,
interface-ids,is-root,mesh-name <1-64>,mpid,next-hop-hostname <1-64>,next-hop-
ifid,next-hop-use-time,path-metric,root-bound-time,root-hostname <1-64>,root-
mpid)
```

| | |
|---|---|
| show-wireless-meshpoint | Customizes the *show > wireless > meshpoint* command output<br>The columns displayed by default are: Mesh, Hostname, Hops, Is-Root, Config-As-Root, Root-Hostname, Root-Bound-Time, Path-Metric, Next-Hop-Hostname, and Next-Hop-Use-Time. |
| ap-mac | Includes the ap-mac column, which displays the AP's MAC address in the AA-BB-CC-DD-EE-FF format. Applicable only in case of non-controller meshpoints |
| cfg-as-root | Includes the cfg-as-root column, which displays the configured root state of the meshpoint |
| hops | Includes the hops column, which displays the number of hops to the root for this meshpoint |
| hostname <1-64> | Includes the hostname column, which displays the AP's hostname. Applicable only in case of non-wireless controller meshpoints<br>• <1-64> – Sets the hostname column width from 1 - 64 characters |
| interface-ids | Includes the interface-ids column, which displays the interface identifiers (interfaces used by this meshpoint) |
| is-root | Includes the is-root column, which displays the current root state of the meshpoint |
| mesh-name <1-64> | Includes the mesh-name column, which displays the meshpoint's name<br>• <1-64> – Sets the mesh-name column width from 1 - 64 characters |
| mpid | Includes the mpid column, which displays the meshpoint identifier in the AA-BB-CC-DD-EE-FF format |
| next-hop-hostname <1-64> | Includes the next-hop-hostname column, which displays the next-hop AP's name (the AP next in the path to the bound root)<br>• <1-64> – Sets the next-hop-hostname column width from 1 - 64 characters |
| next-hop-ifid | Includes the next-hop-ifid column, which displays the next-hop interface identifier in the AA-BB-CC-DD-EE-FF format |
| next-hop-use-time | Includes the next-hop-use-time column, which displays the time since this meshpoint started using this next hop |
| root-bound-time | Includes the root-bound-time column, which displays the time since this meshpoint has been bound to the current root |

| | |
|---|---|
| root-hostname <1-64> | Includes the root-hostname column, which displays the root AP's hostname to which this meshpoint is bound<br>• <1-64> – Sets the root-hostname column width from 1 - 64 characters |
| root-mpid | Includes the root-mpid column, which displays the bound root meshpoint identifier in the AA-BB-CC-DD-EE-FF format |

```
• customize show-wireless-meshpoint-neighbor-stats (ap-hostname <1-64>,
neighbor-hostname <1-64>,neighbor-ifid,rx-bytes,rx-errors,rx-packets,rx-
throughput,t-index,tx-bytes,tx-dropped,tx-packets,tx-throughput)
```

| | |
|---|---|
| show-wireless-meshpoint-neighbor-stats | Customizes the *show > wireless > meshpoint > neighbor > statistics* command output<br>The columns displayed by default are: AP Hostname, Neighbor-IFID, TX bytes, RX bytes, Tx pkts, Rx pkts, Tx (bps), Rx (bps), T-Index (%), and Dropped pkts. |
| ap-name <1-64> | Includes the ap-name column, which displays name of the AP reporting a neighbor<br>• <1-64> – Sets the ap-name column width from 1 - 64 characters |
| neighbor-hostname <1-64> | Includes the neighbor-hostname column, which displays the reported neighbor's hostname<br>• <1-64> – Sets the neighbor-hostname column width from 1 - 64 characters |
| neighbor-ifid | Includes the neighbor-ifid column, which displays the neighbor's interface ID |
| rx-bytes | Includes the rx-bytes column, which displays the total bytes received |
| rx-errors | Includes the rx-error column, which displays the total bytes of error received |
| rx-packets | Includes the rx-packets column, which displays the number of packets received |
| rx-throughput | Includes the rx-throughput column, which displays neighbor's received throughput |
| t-index | Includes the t-index column, which displays the traffic utilization index at the neighbor end |
| tx-bytes | Includes the tx-bytes column, which displays the total bytes transmitted |
| tx-dropped | Includes the tx-dropped column, which displays the total bytes dropped |
| tx-packets | Includes the tx-packets column, which displays the number of packets transmitted |
| tx-throughput | Includes the tx-throughput column, which displays neighbor's transmitted throughput |

```
• customize show-wireless-meshpoint-neighbor-stats-rf (ap-hostname <1-64>,
average-retry-number,error-rate,neighbor-hostname <1-64>,neighbor-ifid,noise,
q-index,rx-rate,signal,snr,t-index,tx-rate)
```

| | |
|---|---|
| show-wireless-meshpoint-neighbor-stats-rf | Customizes the *show > wireless > meshpoint > neighbor > statistics > rf* command output<br>The columns displayed by default are: AP Hostname, Neighbor-IFID, Signal (dBm), Noise (dBm), SNR (dB), Tx-Rate (Mbps), Rx-Rate (Mbps), Retry Avg, Errors (pps), and Q-Index (%). |
| ap-name <1-64> | Includes the ap-name column, which displays name of the AP reporting a neighbor<br>• <1-64> – Sets the ap-name column width from 1 - 64 characters |
| average-retry-number | Includes the average-retry-number column, which displays the average number of retransmissions made per packet. |
| error-rate | Includes the error-rate column |
| neighbor-hostname <1-64> | Includes the neighbor-hostname, which displays reported neighbor's hostname<br>• <1-64> – Sets the neighbor-hostname column width from 1 - 64 characters |

| | |
|---|---|
| noise | Includes the noise column, which displays the noise level in dBm |
| q-index | Includes the q-index column, which displays the q-index |
| rx-rate | Includes the rx-rate column, which displays rate of receiving |
| signal | Includes the signal column, which displays the signal strength in dBm |
| snr | Includes the snr column, which displays the signal-to-noise ratio |
| t-index | Includes the t-index column, which displays t-index |
| tx-rate | Includes the tx-rate column, which displays rate of transmission |

- `customize show-wireless-mint-client (client-alias <1-64>,client-bss,portal-alias <1-64>,portal-bss,up-time)`

| | |
|---|---|
| show-wireless-mint-client | Configures the information displayed in the *show > wireless > mint > client* command output. Select the columns (information) displayed from the following options: client-alias, client-bss, portal-alias, portal-bss, and up-time. These are recursive parameters and you can select multiple options at a time.<br>The columns displayed by default are: Portal, Portal-Radio-MAC, Client, Client-Radio-MAC, and Up-Time. |

- `customize show-wireless-mint-client-stats (client-alias <1-64>,portal-alias <1-64>,portal-bss,rx-bytes,rx-errors,rx-packets,rx-throughput,t-index,tx-bytes,tx-dropped,tx-packets,tx-throughput)`

| | |
|---|---|
| show-wireless-mint-client-stats | Configures the information displayed in the *show > wireless > mint > client > statistics* command output. Select the columns (information) displayed from the following options: client-alias, portal-alias, portal-bss, rx-bytes, rx-errors, rx-packets, rx-throughput, t-index, tx-bytes, tx-dropped, tx-packets, tx-throughput. These are recursive parameters and you can select multiple options at a time.<br>The columns displayed by default are: Portal, Portal-Radio-MAC, Client, Tx bytes, Rx bytes, TX pkts, Rx pkts, TX (bps), Rx (bps), T-Index (%), and Dropped pkts.<br>Where ever available, you can optionally use the <1-64> parameter to set the column width. |

- `customize show-wireless-mint-client-stats-rf (average-retry-number,client-alias <1-64>,error-rate,noise,portal-alias <1-64>,portal-bss,q-index,rx-rate,signal,snr,tx-rate)`

| | |
|---|---|
| show-wireless-mint-client-stats-rf | Configures the information displayed in the *show > wireless > mint > client > statistics > rf* command output. Select the columns (information) displayed from the following options: average-retry-number, client-alias, error-rate, noise, portal-alias, portal-bss, q-index, rx-rate, signal, snr, and tx-rate. These are recursive parameters and you can select multiple options at a time.<br>The columns displayed by default are: MAC, Signal (dBm), Noise (dBm), SNR (dB), Tx-Rate (Mbps), Rx-rate (Mbps), Retry Avg, Errors (pps), and Q-Index (%).<br>Where ever available, you can optionally use the <1-64> parameter to set the column width. |

```
• customize show-wireless-mint-portal (client-alias <1-64>,client-bss,portal-
alias <1-64>,portal-bss,up-time)
```

| | |
|---|---|
| show-wireless-mint-portal | Configures the information displayed in the *show > wireless > mint > portal* command output. Select the columns (information) displayed from the following options: client-alias, client-bss, portal-alias, portal-bss, and up-time. These are recursive parameters and you can select multiple options at a time.<br>The columns displayed by default are: Client, Client-Radio-MAC, Portal, Portal-Radio-MAC, and Up-Time.<br>Where ever available, optionally use the <1-64> parameter to set the column width. |

```
• customize show-wireless-mint-portal-stats (client-alias <1-64>,client-bss,
portal-alias <1-64>,rx-bytes,rx-errors,rx-packets,rx-throughput,t-index,
tx-bytes,tx-dropped,tx-packets,tx-throughput)
```

| | |
|---|---|
| show-wireless-mint-portal-stats | Configures the information displayed in the *show > wireless > mint > portal > statistics* command output. Select the columns (information) displayed from the following options: client-alias, client-bss, portal-alias, rx-bytes, rx-errors, rx-packets, rx-throughput, t-index, tx-bytes, tx-dropped, tx-packets, tx-throughput. These are recursive parameters and you can select multiple options at a time.<br>The columns displayed by default are: Client, Client-Radio-MAC, Portal, Tx bytes, Rx bytes, TX pkts, Rx pkts, TX (bps), Rx (bps), T-Index (%), and Dropped pkts.<br>Where ever available, optionally use the <1-64> parameter to set the column width. |

```
• customize show-wireless-mint-portal-stats-rf (average-retry-number,client-alias
<1-64>,client-bss,error-rate,noise,portal-alias <1-64>,q-index,rx-rate,signal,
snr,tx-rate)
```

| | |
|---|---|
| show-wireless-mint-portal-stats-rf | Configures the information displayed in the *show > wireless > mint > portal > statistics > rf* command output. Select the columns (information) displayed from the following options: average-retry-number, client-alias, client-bss, error-rate, noise, portal-alias, q-index, rx-rate, signal, snr, tx-rate. These are recursive parameters and you can select multiple options at a time.<br>The columns displayed by default are: Client, Client-Radio-MAC, Portal, Signal (dBm), Noise (dBm), SNR (dB), Tx-Rate (Mbps), Rx-rate (Mbps), Retry Avg, Errors (pps), and Q-Index (%).<br>Where ever available, optionally use the <1-64> parameter to set the column width. |

```
• customize show-wireless-radio (adopt-to,ap-name <1-64>,channel,location <1-64>,
num-clients,power,radio-alias <3-67>,radio-id,radio-mac,rf-mode,state)
```

| | |
|---|---|
| show-wireless-radio | Customizes the show wireless radio command output |
| adopt-to | Includes the adopt-to column, which displays information about the wireless controller adopting this AP |
| ap-name <1-64> | Includes the ap-name column, which displays information about the AP this radio belongs<br>• <1-64> – Sets the ap-name column width from 1 - 64 characters |
| channel | Includes the channel column, which displays information about the configured and current channel for this radio |
| location <1-64> | Includes the location column, which displays the location of the AP this radio belongs<br>• <1-64> – Sets the location column width from 1 - 64 characters |
| num-clients | Includes the num-clients column, which displays the number of clients associated with this radio |

| | |
|---|---|
| power | Includes the power column, which displays the radio's configured and current transmit power |
| radio-alias <3-67> | Includes the radio-alias column, which displays the radio's alias (combination of AP's hostname and radio interface number in the "HOSTNAME:RX" formate)<br>• <3-67> – Sets the radio-alias column width from 3 - 67 characters |
| radio-id | Includes the radio-id column, which displays the radio's ID (combination of AP's MAC address and radio interface number in the "AA-BB-CC-DD-EE-FF:RX" format) |
| radio-mac | Includes the radio-mac column, which displays the radio's base MAC address |
| rf-mode | Includes the rf-mode column, which displays the radio's operating mode. The radio mode can be 2.4 GHz, 5.0 GHz, or sensor. |
| state | Includes the state column, which displays the radio's current operational state |

```
• customize show-wireless-radio-stats (radio-alias <3-67>,radio-id,radio-mac,
rx-bytes,rx-errors,rx-packets,rx-throughput,tx-bytes,tx-dropped,tx-packets,
tx-throughput)
```

| | |
|---|---|
| show-wireless-radio-stats | Customizes the show wireless radio statistics command output |
| radio-alias <3-67> | Includes the radio-alias column, which displays the radio's alias (combination of AP's hostname and radio interface number in the "HOSTNAME:RX" format)<br>• <3-67> – Sets the radio-alias column width from 3 - 67 characters |
| radio-id | Includes the radio-id column, which displays the radio's ID (combination of AP's MAC address and radio interface number in the "AA-BB-CC-DD-EE-FF:RX" format) |
| radio-mac | Includes the radio-mac column, which displays the radio's base MAC address |
| rx-bytes | Includes the rx-bytes column, which displays the total number of bytes received by the radio |
| rx-errors | Includes the rx-error column, which displays the total number of errors received by the radio |
| rx-packets | Includes the rx-packets column, which displays the total number of packets received by the radio |
| rx-throughput | Includes the rx-throughput column, which displays the receive throughput at the radio |
| tx-bytes | Includes the tx-bytes column, which displays the total number of bytes transmitted by the radio |
| tx-dropped | Includes the tx-dropped column, which displays the total number of packets dropped by the radio |
| tx-packets | Includes the tx-packets column, which displays the total number of packets transmitted by the radio |
| tx-throughput | Includes the tx-throughput column, which displays the transmission throughput at the radio |

```
• customize show-wireless-radio-stats-rf (average-retry-number,error-rate,noise,
q-index,radio-alias <3-67>,radio-id,radio-mac,rx-rate,signal,snr,t-index,tx-rate)
```

| | |
|---|---|
| show-wireless-radio-stats-rf | Customizes the show wireless radio stats RF command output |
| average-retry-number | Includes the average-retry-number column, which displays the average number of retransmissions per packet |

| | |
|---|---|
| error-rate | Includes the error-rate column, which displays the rate of error for the radio |
| noise | Includes the noise column, which displays the noise detected by the radio |
| q-index | Includes the q-index column, which displays the RF quality index<br>Higher values indicate better RF quality. |
| radio-alias <3-67> | Includes the radio-alias column, which displays the radio's alias (combination of AP's hostname and radio interface number in the "HOSTNAME:RX" format)<br>• <3-67> – Sets the radio-alias column width from 3 - 67 characters |
| radio-id | Includes the radio-id column, which displays the radio's ID (combination of AP's MAC address and radio interface number in the "AA-BB-CC-DD-EE-FF:RX" format) |
| radio-mac | Includes the radio-mac column, which displays the radio's base MAC address |
| rx-rate | Includes the rx-rate column, which displays the receive rate at the particular radio |
| signal | Includes the signal column, which displays the signal strength at the particular radio |
| snr | Includes the snr column, which displays the signal-to-noise ratio at the particular radio |
| t-index | Includes the t-index column, which displays the traffic utilization index at the particular radio |
| tx-rate | Includes the tx-rate column, which displays the packet transmission rate at the particular radio |

**Example**

The following example shows the shows the *show > adoption > status* command output before customizing the output:

```
rfs6000-81742D#show adoption status
Adopted by:
Type           : nx9000
System Name    : nx9500-6C8809
MAC address    : B4-C7-99-6C-88-09
MiNT address   : 19.6C.88.09
Time           :   4 days 22:38:32 ago

Adopted Devices:
--------------------------------------------------------------------------------
------------------------------
DEVICE-NAME       VERSION         CFG-STAT         MSGS ADOPTED-BY        LAST-
ADOPTION                  UPTIME
--------------------------------------------------------------------------------
------------------------------
ap7532-A2A56C   5.9.0.0-010D  *configured No  rfs6000-81742D    4 days 22:25:56
4 days 22:31:23
--------------------------------------------------------------------------------
------------------------------
Total number of devices displayed: 1
rfs6000-81742D#

rfs6000-81742D(config)#customize show-adoption-status adopted-by ap-name config-
status last-adoption
rfs6000-81742D(config)#commit
```

The following example shows the shows the *show > adoption > status* command output after customizing the output:

```
rfs6000-81742D#show adoption status
Adopted by:
Type           : nx9000
System Name    : nx9500-6C8809
```

```
MAC address    : B4-C7-99-6C-88-09
MiNT address   : 19.6C.88.09
Time
Adopted Devices:
-------------------------------------------------------------------------
ADOPTED-BY        DEVICE-NAME       CFG-STAT         LAST-ADOPTION
-------------------------------------------------------------------------
rfs6000-81742D ap7532-A2A56C    *configured        4 days 22:25:56
-------------------------------------------------------------------------

Total number of devices displayed: 1
rfs6000-81742D(config)#
```

Use the *no > customize > show-adoption-status* command to revert back to the default format.

```
rfs6000-81742D(config)#no customize show-adoption-status
rfs6000-81742D(config)#commit

rfs6000-81742D#show adoption status
Adopted by:
Type           : nx9000
System Name    : nx9500-6C8809
MAC address    : B4-C7-99-6C-88-09
MiNT address   : 19.6C.88.09
Time           :   4 days 22:38:32 ago

Adopted Devices:
-------------------------------------------------------------------------------
--------------------------------
DEVICE-NAME       VERSION         CFG-STAT         MSGS ADOPTED-BY        LAST-
ADOPTION                  UPTIME
-------------------------------------------------------------------------------
--------------------------------
ap7532-A2A56C   5.9.0.0-010D  *configured No  rfs6000-81742D    4 days 22:25:56
4 days 22:31:23
-------------------------------------------------------------------------------
--------------------------------
Total number of devices displayed: 1
rfs6000-81742D#
```

**Related Commands**

| | |
|---|---|
| *no* | Restores custom CLI settings to default |
| *wireless* (show commands) | Displays wireless configuration and other information |

## 4.1.38 database-client-policy

*Global Configuration Commands*

The following table summarizes the config database client policy commands:

**Table 4.16** *Database-Client-Policy Config Commands*

| Command | Description | Reference |
|---|---|---|
| *database-client-policy* | Creates a database-client policy and enters its configuration mode | *page 4-178* |
| *database-client-policy-mode commands* | Summarizes the database client policy mode commands | *page 4-180* |

### 4.1.38.1 database-client-policy

*database-client-policy*

Creates a database-client-policy and enters its configuration mode. The database-client-policy configures the IP address or hostname of the *database* host, and is used on the NSight/EGuest server's device cortext. However, the database-client-policy is required only in a split deployment, where the server and database are hosted on separate boxes. In such a scenario, the database-client-policy enables the server to identify the database host.

If enforcing database authentication, configure the user-name and password required to access the database on the database-client-policy. For more information on enabling database authentication, see *database*.

**Supported in the following platforms:**

- Service Platforms — NX9500, NX9600, VX9000

**Syntax**

```
database-client-policy <DATABASE-CLIENT-POLICY-NAME>
```

**Parameters**

- `database-client-policy <DATABASE-CLIENT-POLICY-NAME>`

| | |
|---|---|
| database-policy <DATABASE-CLIENT-POLICY-NAME> | Specify the database-client-policy name. If the policy does not exist, it is created.<br>Once created and configured, use this policy in the NSight/EGuest server's device context. |

**Example**

```
vx9000-34B78B(config)#database-client-policy DBClientPolicy
vx9000-34B78B(config-database-client-policy-DBClientPolicy)#?
Database Client Policy Mode commands:
  authentication   Database authentication
  database-server  Add database server
  no               Negate a command or set its defaults

  clrscr           Clears the display screen
  commit           Commit all changes made in this session
  do               Run commands from Exec mode
  end              End current mode and change to EXEC mode
  exit             End current mode and down to previous mode
  help             Description of the interactive help system
  revert           Revert changes
  service          Service Commands
  show             Show running system information
  write            Write running configuration to memory or terminal

vx9000-34B78B(config-database-client-policy-DBClientPolicy)#
```

To setup a database/server environment, with the database and the server hosted n separate hosts:

1 On the database host, use the database policy. This brings up the database server.

2 On the NSight/EGuest server, create the database-client-policy, and configure the database host's IP address or hostname.

```
vx9000-34B78B(config)#database-client-policy DBClientPolicy
vx9000-34B78B(config-database-client-policy-DBClientPolicy)#database-server
192.168.13.10
vx9000-34B78B(config-database-client-policy-DBClientPolicy)#show context
database-client-policy DBClientPolicy
  database-server 192.168.13.10
vx9000-34B78B(config-database-client-policy-DBClientPolicy)#
```

3 Use this database-client-policy in the NSight/EGuest server's device configuration context. Once applied, the server posts details to the database specified in the policy.

```
vx9000-34B78B(config-device-00-0C-29-34-B7-8B)#use database-client-policy
DBClientPolicy

vx9000-34B78B(config-device-00-0C-29-34-B7-8B)#show context include-factory |
include database-client-policy
 use database-client-policy DBClientPolicy
vx9000-34B78B(config-device-00-0C-29-34-B7-8B)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing database-client-policy |
| *database-policy* | Documents database policy configuration commands. If enforcing authenticated database access, use this command to enable authentication on the database and configure the username and password. |
| *nsight-policy* | Documents NSight policy configuration commands. The NSight policy is a tool, which when created and applied at the RF Domain level allows the RF Domain manager to send statistics (polled from devices within the RF Domain) to the NOC. The NOC, when enabled as the NSight server, stores this data in a locally or externally hosted database. |
| *use* (profile/device context) | Uses a database-client-policy in the VX9000's device or profile context |
| *database* | Drops or repairs a database. Also provides database keyfile management capabilities. If enforcing authenticated access to the database, use this command to generate, export, import, and zerzoise the keyfile. |

### 4.1.38.2 database-client-policy-mode commands

*database-client-policy*

The following table summarizes database-client-policy configuration mode commands:

**Table 4.17** *Database-Client-Policy-Config-Mode Commands*

| Command | Description | Reference |
|---|---|---|
| *authentication* | Configures the captive-portal/NSight database users | *page 4-181* |
| *database-server* | Configures the database host's IP address or hostname. Use this command to configure the IP address or hostname of the VM hosting the database. | *page 4-182* |
| *no* | Removes the database host's IP/hostname configuration | *page 4-183* |

### 4.1.38.2.1 authentication

*database-client-policy-mode commands*

Configures the database's username and password

**Supported in the following platforms:**

- Service Platforms — NX9500, NX9600, VX9000

**Syntax**

```
authentication username <USER-NAME> password <PASSWORD>
```

**Parameters**

- `authentication username <USER-NAME> password <PASSWORD>`

| | |
|---|---|
| authentication username <USER-NAME> password <PASSWORD> | Configures the username and password required to access the database. Note, username and password specified here should be the same as those already created on the database host. For more information on creating database users, see *service*.<br>• username <USER-NAME> – Configures the user name<br>• password <PASSWORD> – Configures the password for the username specified above.<br>However, ensure database authentication is enabled in the database-policy.<br>For more information on database-policy, see *database-policy*.<br>For more information on enabling database authentication, see *database* |

**Example**

```
vx9000-65672(config-database-client-policy-DBClientPolicy)# authentication
username extreme password 2 test@12345

vx9000-656725#show running-config database-client-policy replica-set
database-client-policy replica-set
 database-server 13.13.13.3
 database-server 14.14.14.2
 authentication username extreme password 2 q4cUyedmA4BFsn1kg/
xjCQAAAAliMbdrXKblQbsyrwMGdVzv
vx9000-656725#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing database username and password |

### 4.1.38.2.2 database-server

*database-client-policy-mode commands*

Configures the IPv4/IPv6 address or hostname of the VM hosting the database

**Supported in the following platforms:**

- Service Platforms — VX9000

**Syntax**

```
database-server [<IP>|<HOSTNAME>|<IPv6>]
```

**Parameters**

- `database-server [<IP>|<HOSTNAME>|<IPv6>]`

| | |
|---|---|
| database-server [<IP>\|<HOSTNAME>\|<IPv6>] | Identifies the database host using one of the following options:<br>• <IP> – Specifies the host's IPv4 address<br>• <HOSTNAME> – Specifies the host's hostname<br>• <IPv6> – Specifies the host's IPv6 address. |

**Example**

```
vx9000-34B78B(config-database-client-policy-DBClientPolicy)#database-server
192.168.13.10

vx9000-34B78B(config-database-client-policy-DBClientPolicy)#show context
database-client-policy DBClientPolicy
database-server 192.168.13.10
vx9000-34B78B(config-database-client-policy-DBClientPolicy)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the database server's (the VM hosting the database) IP/hostname configuration |

### 4.1.38.2.3 no

*database-client-policy-mode commands*

Removes the database host's IP/hostname configuration

**Supported in the following platforms:**

- Service Platforms — VX9000

**Syntax**

```
no [authentication|database-server]

no authentication username <USER-NAME>

no database-server [<IP>|<HOST-NAME>|<IPv6>]
```

**Parameters**

- `no [authentication|database-server]`

| | |
|---|---|
| no database-server | Removes the database VM's IPv4/Ipv6 address or hostname associated with this database client policy. Also removes database user details. |

**Example**

```
vx9000-34B78B(config-database-client-policy-DBClientPolicy)#show context
database-client-policy DBClientPolicy
database-server 192.168.13.10
vx9000-34B78B(config-database-client-policy-DBClientPolicy)#

vx9000-34B78B(config-database-client-policy-DBClientPolicy)#no database-server

vx9000-34B78B(config-database-client-policy-DBClientPolicy)#show context
database-client-policy DBClientPolicy
vx9000-34B78B(config-database-client-policy-DBClientPolicy)#
```

## 4.1.39 database-policy

*Global Configuration Commands*

The following table summarizes the config database policy commands:

**Table 4.18** *Database-Policy Config Commands*

| Command | Description | Reference |
|---|---|---|
| *database-policy* | Creates a database policy and enters its configuration mode | *page 4-185* |
| *database-policy-mode commands* | Lists database policy configuration mode commands | *page 4-186* |

### 4.1.39.1 database-policy

*database-policy*

Creates a database-policy and enters its configuration mode. After creating the database-policy, use it on the database host. This enables the database. If deploying a database replica-set, use this command to define the replica set configurations.

To enforce database authentication, enable authentication on the database-policy, and configure the username and password required to access the database. Note, this command is part of a set of configurations that are required to enable authentication. For more information on the entire set of configurations, see *database*.

**Supported in the following platforms:**

- Service Platforms — NX9500, NX9510, VX9000

**Syntax**

```
database-policy <DATABASE-POLICY-NAME>
```

**Parameters**

- `database-policy <DATABASE-POLICY-NAME>`

| | |
|---|---|
| database-policy <DATABASE-POLICY-NAME> | Specify the database policy name. If the policy does not exist, it is created. |

**Example**

```
nx9500-6C8809(config-database-policy-test)#?
Database Policy Mode commands:
  authentication  Database authentication
  no              Negate a command or set its defaults
  replica-set     Replica Set
  shutdown        Disable database server

  clrscr          Clears the display screen
  commit          Commit all changes made in this session
  do              Run commands from Exec mode
  end             End current mode and change to EXEC mode
  exit            End current mode and down to previous mode
  help            Description of the interactive help system
  revert          Revert changes
  service         Service Commands
  show            Show running system information
  write           Write running configuration to memory or terminal
nx9500-6C8809(config-database-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing database policy |

### 4.1.39.2 database-policy-mode commands

*database-policy*

The following table summarizes database-policy configuration mode commands:

**Table 4.19** *Database-Policy-Config-Mode Commands*

| Command | Description | Reference |
|---|---|---|
| *authentication* | Enables database authentication and configures the username and password required to access the database | *page 4-187* |
| *replica-set* | Adds a member to a database replica set | *page 4-188* |
| *shutdown* | Shuts down the database server | *page 4-190* |
| *no* | Removes a member from the database replica set | *page 4-191* |

### 4.1.39.2.1 authentication

*database-policy-mode commands*

Enables database authentication. When enabled and applied on the database host, this policy enforces authenticated access to the database. This command also configures the username and password required to access the database.

**Supported in the following platforms:**

- Service Platforms — NX9500, NX9600, VX9000

**Syntax**

```
authentication
authentication username <USER-NAME> password <PASSWORD>
```

**Parameters**

- `authentication`

| | |
|---|---|
| authentication | Enables database authentication on this database-policy. When executed without the associated keywords, the command enables authentication on the database host using the policy. Execute the command along with the username and password inputs to configure the user credentials required for access the database. |

- `authentication username <USER-NAME> password <PASSWORD>`

| | |
|---|---|
| authentication username <USER-NAME> password <PASSWORD> | Configures the username and password required to access the database. Note, username and password specified here should be the same as those already created on the database host. For more information, see *service*.<br>• username <USER-NAME> – Configures the database username<br>• password <PASSWORD> – Configures the password for the username specified above<br>Users using these credentials are allowed database access. In case of a split NSight/EGuest deployment, ensure that the database-client-policy running on the NSight/EGuest server has the same user details configured.<br>For information on creating database-client-policy, see *database-client-policy*<br>For more information on enabling database authentication, see *database*. |

**Example**

```
nx9500-6C8809(config-database-policy-test)#authentication
nx9500-6C8809(config-database-policy-test)#no shutdown
nx9500-6C8809(config-database-policy-test)#authentication username user1 password
uesr@123

nx9500-6C8809(config-database-policy-test)#show context
database-policy test
 authentication
 authentication username user1 password 2 f20/dTjYiMnR/tqbGFaO5gAAAAjL/
xo8clisk1TZjimo128t
nx9500-6C8809(config-database-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables database authentication, and removes the username and password configuration. |

### 4.1.39.2.2 replica-set

*database-policy-mode commands*

Adds a member to a database replica set. A replica-set is a group of devices (replica-set members) running the database instances that maintain the same data set. Replica sets provide redundancy and high availability and are the basis for all production deployments. The replica set usually consists of: an arbiter, a primary member, and one or more secondary members. The primary member and the secondary member(s) maintain replicas of the data set.

Before deploying a replica set, ensure that each of the replica-set member:

- has the DB instances installed, and
- is able to communicate with every other member in the set.

After ensuring the above,

- Create a database policy (with identical replica-set configuration) on each of the member devices, and
- Use the database policy in the member device's configuration mode.

These member devices elect a primary member, which begins accepting client-write operations. Remaining devices in the replica-set, with the exception of the arbiter, are designated as secondary members.

**Supported in the following platforms:**

- Service Platforms — NX9500, NX9600, VX9000, NX7500, NX5500

**Syntax**

```
replica-set member [<IP>|<FQDN>] {arbiter|priority <0-255>}
```

**Parameters**

- `replica-set member [<IP>|<FQDN>] {arbiter|priority <0-255>}`

| | |
|---|---|
| replica-set member [<IP>\|<FQDN>] {arbiter\|priority <0-255>} | Adds a member to the database replica set. To identify the member, use one of the following options:<br>• <IP> – Specify the member's IP address.<br>• <FQDN> – Specify the member's *Fully Qualified Domain Name* (FQDN).<br>After specifying the IP address or FQDN, specify the following:<br>• arbiter – Optional. Select to configure the member as the arbiter.<br>• priority <0-255> – Optional. Configures the priority of a non-arbiter member of the replica set<br>• <0-255> – Specify the priority from 0 - 255. This value determines the member's position within the replica set as primary or secondary. It also helps in electing the fall-back primary member in the eventuality of the current primary member being unreachable.<br>A replica set should have at least three members. The maximum number of members can go up to fifty (50). However, configuring a three-member replica set is recommended. Replica sets should have odd number of members. In case of an even-numbered replica set, add an arbiter to make the member count odd. This ensures that at least one member gets a majority vote in the primary-member election. |

**Example**

```
nx9500-6C8809(config-database-policy-test)#replica-set member 192.168.13.14
arbiter

nx9500-6C8809(config-database-policy-test)#replica-set member 192.168.13.16
priority 1

nx9500-6C8809(config-database-policy-test)#replica-set member 192.168.13.12
priority 2

nx9500-6C8809(config-database-policy-test)#show context
database-policy test
 replica-set member 192.168.13.12 priority 2
 replica-set member 192.168.13.14 arbiter
 replica-set member 192.168.13.16 priority 1
nx9500-6C8809(config-database-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes a member from the database replica set |

### 4.1.39.2.3 shutdown

*database-policy-mode commands*

Shuts down the database server. The factory default is set as *no shutdown*.

**Supported in the following platforms:**

- Service Platforms — NX9500, NX9600, VX9000, NX7500, NX5500

**Syntax**

```
shutdown
```

**Parameters**

None

**Example**

```
nx9500-6C8809(config-database-policy-test)#shutdown

nx9500-6C8809(config-database-policy-test)#show context
database-policy test
 shutdown
nx9500-6C8809(config-database-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Enables the database server |

### 4.1.39.2.4 no

*database-policy-mode commands*

Removes or reverts the database policy settings to default values

**Supported in the following platforms:**

- Service Platforms — NX9500, NX9600, VX9000, NX7500, NX5500

**Syntax**

```
no [authentication|replica-set|shutdown]

no authentication {username <USER-NAME>}

no replica-set member [<IP>|<FQDN>]

no shutdown
```

**Parameters**

- no <PARAMETERS>

| | |
|---|---|
| no <PARAMETERS> | Removes a member from the database replica set, or brings up a database server that is down. Also disables database authentication and removes user |

**Example**

The following example shows a three-member replica set:

```
nx9500-6C8809(config-database-policy-test)#show context
database-policy test
 replica-set member 192.168.13.12 priority 2
 replica-set member 192.168.13.14 arbiter
 replica-set member 192.168.13.16 priority 1
nx9500-6C8809(config-database-policy-test)#
```

In the following example the arbiter is being removed, leaving the replica set with only two members:

```
nx9500-6C8809(config-database-policy-test)#no replica-set member 192.168.13.14

nx9500-6C8809(config-database-policy-test)#show context
database-policy test
 replica-set member 192.168.13.12 priority 2
 replica-set member 192.168.13.16 priority 1
nx9500-6C8809(config-database-policy-test)#
```

Since a replica set must have at least three members, another member must be added to this replica set. This member may or may not be an arbiter.

```
nx9500-6C8809(config-database-policy-test)#replica-set member 192.168.13.8
priority 3

nx9500-6C8809(config-database-policy-test)#show context
database-policy test
 replica-set member 192.168.13.12 priority 2
 replica-set member 192.168.13.16 priority 1
 replica-set member 192.168.13.8 priority 3
nx9500-6C8809(config-database-policy-test)#
```

## 4.1.40 device

*Global Configuration Commands*

Enables simultaneous configuration of multiple devices

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
device {containing|filter}

device {containing <STRING>} {filter type [ap6521|ap6522|ap6532|ap6562|ap71xx|
ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|
ap8432|ap8533|ex3524|ex3548|rfs4000|rfs6000|nx5500|nx75xx|nx9000|nx9600|t5|
vx9000]}

device {filter type [ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|
ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|ex3524|
ex3548|rfs4000|rfs6000|nx5500|nx75xx|nx9000|nx9600|t5|vx9000]}
```

**Parameters**

```
• device {containing <STRING>} {filter type [ap6521|ap6522|ap6532|ap6562|ap71xx|
ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|
ap8432|ap8533|ex3524|ex3548|rfs4000|rfs6000|nx5500|nx75xx|nx9000|nx9600|t5|
vx9000]}
```

| | |
|---|---|
| device | Enters a device's configuration mode. Use this command to simultaneously configure devices having similar configuration. |
| containing <STRING> | Optional. Configures the string to search for in the device's hostname. All devices having hostnames containing the string specified here are filtered, and can be configured simultaneously.<br>• <STRING> – Specify the string to search for in the device's hostname. |
| filter type <DEVICE-TYPE> | Optional. Filters out a specific device type. After specifying the hostname string, select the device type. The options are: AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533, EX3524, EX3548, RFS4000, RFS6000, NX5500, NX75XX, NX95XX, NX9600, t5, and VX9000 (V-WLC).<br>The t5 option is applicable only on the NX7500, NX7510, NX7520, NX7530, NX95XX, NX9500, NX9510, and NX9600 platforms.<br>The VX9000 option is applicable only to the NX9500, NX9510, and NX9600 platforms. |

```
• device {filter type [ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|
ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|ex3524|
ex3548|rfs4000|rfs6000|nx5500|nx75xx|nx9000|nx9600|t5|vx9000]}
```

| | |
|---|---|
| device | Configures a basic device profile |

| | |
|---|---|
| filter type <DEVICE-TYPE> | Optional. Filters out a specific device type. The options are: AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533, EX3524, EX3548, RFS4000, RFS6000, NX5500, NX75XX, NX95XX, NX9600, t5, and VX9000 (V-WLC).<br>The t5 option is applicable only on the NX7500, NX7510, NX7520, NX7530, NX95XX, NX9500, NX9510, and NX9600 platforms.<br>The VX9000 option is applicable only to the NX9500, NX9510, and NX9600 platforms. |

**Example**

```
rfs6000-81742D(config)#device filter type ap7532
rfs6000-81742D(config-device-{'type': 'ap7532'})#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes multiple devices from the network |

## 4.1.41 device-categorization

*Global Configuration Commands*

Categorizes devices as sanctioned or neighboring. Categorization of devices enables quick identification and blocking of unsanctioned devices in the network.

The following table summarizes the device categorization mode commands:

**Table 4.20** *Device-Categorization Config Command*

| Command | Description | Reference |
|---|---|---|
| *device-categorization* | Creates a device categorization list and enters its configuration mode | *page 4-195* |
| *device-categorization-mode commands* | Summarizes device categorization list configuration mode commands | *page 4-196* |

### 4.1.41.1 device-categorization

*device-categorization*

Configures a device categorization list

Proper classification and categorization of devices (access points, clients, etc.) helps suppress unnecessary unauthorized access point alarms, allowing network administrators to focus on alarms on devices actually behaving in a suspicious manner. An intruder with a device erroneously authorized could potentially perform activities that harm your organization.

Authorized access points and clients are generally known to you and conform with your organization's security policies. Unauthorized devices are those detected as interoperating within the network, but are not approved. These devices should be filtered to avoid jeopardizing the data within a managed network. Use this command to apply the neighboring and sanctioned (approved) filters on peer devices operating within a wireless controller or access point's radio coverage area. Detected client MAC addresses can also be filtered based on their classification.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
device-categorization <DEVICE-CATEGORIZATION-LIST-NAME>
```

**Parameters**

- `device-categorization <DEVICE-CATEGORIZATION-LIST-NAME>`

| | |
|---|---|
| <DEVICE-CATEGORIZATION-LIST-NAME> | Specify the device categorization list name. If a list with the same name does not exist, it is created. |

**Example**

```
rfs6000-81742D(config)#device-categorization rfs6000
rfs6000-81742D(config-device-categorization-rfs6000)#?
Device Category Mode commands:
  mark-device  Add a device
  no           Negate a command or set its defaults

  clrscr       Clears the display screen
  commit       Commit all changes made in this session
  do           Run commands from Exec mode
  end          End current mode and change to EXEC mode
  exit         End current mode and down to previous mode
  help         Description of the interactive help system
  revert       Revert changes
  service      Service Commands
  show         Show running system information
  write        Write running configuration to memory or terminal

rfs6000-81742D(config-device-categorization-rfs6000)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing device categorization list |

### 4.1.41.2 device-categorization-mode commands

*device-categorization*

The following table summarizes device categorization configuration mode commands:

**Table 4.21** *Device-Categorization-Mode Commands*

| Command | Description | Reference |
|---|---|---|
| *mark-device* | Adds a device to the device categorization list | *page 4-197* |
| *no* | Removes a device from the device categorization list | *page 4-199* |

### 4.1.41.2.1 mark-device

*device-categorization-mode commands*

Adds a device to the device categorization list as sanctioned or neighboring. Devices are further classified as AP or client.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
mark-device <1-1000> [sanctioned|neighboring] [ap|client]

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

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

**Parameters**

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

| | |
|---|---|
| <1-1000> | Configures the device categorization entry index number |
| sanctioned | Marks a device as sanctioned. A sanctioned device is authorized to use network resources. |
| neighboring | Marks a device as neighboring. A neighboring device is a neighbor in the same network as this device. |
| ap {mac <MAC>\| ssid <SSID>} | Marks a specified AP as sanctioned or neighboring based on its MAC address or SSID<br>• mac <MAC> – Optional. Specify the AP's MAC address<br>• ssid <SSID> – Optional. Specify the AP's SSID. After specifying the SSID, you can optionally specify its MAC SSID.<br>All APs are marked if no specific MAC address or SSID is provided. |

- `mark-device [sanctioned|neighboring] client {mac <MAC>}`

| | |
|---|---|
| <1-1000> | Configures the device categorization entry index number |
| sanctioned | Marks the wireless client as sanctioned. A sanctioned device is authorized to use network resources. |
| neighboring | Marks the wireless client as neighboring. A neighboring device is a neighbor in the same network as this device. |
| client {mac <MAC>} | Marks a specified wireless client as sanctioned or neighboring based on its MAC address<br>• mac <MAC> – Optional. Specify the wireless client's MAC address. |

**Example**

```
rfs6000-81742D(config-device-categorization-rfs6000)#mark-device 1 sanctioned ap
 mac 11-22-33-44-55-66

rfs6000-81742D(config-device-categorization-rfs6000)#show context
device-categorization rfs6000
 mark-device 1 sanctioned ap mac 11-22-33-44-55-66
rfs6000-81742D(config-device-categorization-rfs6000)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an entry from the device categorization list |

### 4.1.41.2.2 no

*device-categorization-mode commands*

Removes a device from the device categorization list

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

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

**Parameters**

- no <PARAMETERS>

| | |
|---|---|
| no <PARAMETERS> | Removes a mark device (AP or wireless client) entry from this device categorization list |

**Example**

The following example shows the device categorization list ‘rfs6000’ settings before the ‘no’ command is executed:

```
rfs6000-81742D(config-device-categorization-rfs6000)#show context
device-categorization rfs6000
 mark-device 1 sanctioned ap mac 11-22-33-44-55-66
rfs6000-81742D(config-device-categorization-rfs6000)#

rfs6000-81742D(config-device-categorization-rfs6000)#no mark-device 1 sanctioned
ap mac 11-22-33-44-55-66
```

The following example shows the device categorization list ‘rfs6000’ settings after the ‘no’ command is executed:

```
rfs6000-81742D(config-device-categorization-rfs6000)#show context
device-categorization rfs6000
rfs6000-81742D(config-device-categorization-rfs6000)#
```

**Related Commands**

| | |
|---|---|
| *mark-device* | Adds a device to a list of sanctioned or neighboring devices |

## 4.1.42 dhcp-server-policy

*Global Configuration Commands*

Configures DHCPv4 server policy parameters, such as class, address range, and options. A new policy is created if it does not exist.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
dhcp-server-policy <DHCP-SERVER-POLICY-NAME>
```

**Parameters**

- `dhcp-server-policy <DHCP-SERVER-POLICY-NAME>`

| | |
|---|---|
| <DHCP-SERVER-POLICY-NAME> | Specify the DHCPv4 server policy name. If the policy does not exist, it is created. |

**Example**

```
rfs6000-81742D(config)#dhcp-server-policy test
rfs6000-81742D(config-dhcp-policy-test)#?
DHCP policy Mode commands:
  bootp         BOOTP specific configuration
  dhcp-class    Configure DHCP class (for address allocation using DHCP
                user-class options)
  dhcp-pool     Configure DHCP server address pool
  dhcp-server   Activating dhcp server based on criteria
  no            Negate a command or set its defaults
  option        Define DHCP server option
  ping          Specify ping parameters used by DHCP Server

  clrscr        Clears the display screen
  commit        Commit all changes made in this session
  do            Run commands from Exec mode
  end           End current mode and change to EXEC mode
  exit          End current mode and down to previous mode
  help          Description of the interactive help system
  revert        Revert changes
  service       Service Commands
  show          Show running system information
  write         Write running configuration to memory or terminal

rfs6000-81742D(config-dhcp-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing DHCP server policy |

**NOTE:** For more information on DHCP policy, see *Chapter 12, DHCP-SERVER-POLICY*.

## 4.1.43 dhcpv6-server-policy

*Global Configuration Commands*

Creates a DHCPv6 server policy and enters its configuration mode

DHCPv6 is a networking protocol for configuring IPv6 hosts with IP addresses, IP prefixes, or other configuration attributes required on an IPv6 network.

DHCPv6 servers pass IPv6 network addresses to IPv6 clients. The DHCPv6 address assignment feature manages non-duplicate addresses in the correct prefix based on the network where the host is connected. Assigned addresses can be from one or multiple pools. Additional options, such as the default domain and DNS name-server address, can be passed back to the client. Address pools can be assigned for use on a specific interface or on multiple interfaces, or the server can automatically find the appropriate pool.

When configured and applied to a device, the DHCPv6 server policy enables the device to function as a stateless DHCPv6 server.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
dhcpv6-server-policy <DHCPv6-SERVER-POLICY-NAME>
```

**Parameters**

- `dhcpv6-server-policy <DHCPv6-SERVER-POLICY-NAME>`

| | |
|---|---|
| <DHCPv6-SERVER-POLICY-NAME> | Specify the DHCPv6 server policy name. If the policy does not exist, it is created. |

**Example**

```
rfs6000-81742D(config-dhcpv6-server-policy-test)#?
DHCPv6 server policy Mode commands:
  dhcpv6-pool              Configure DHCPV6 server address pool
  no                       Negate a command or set its defaults
  option                   Define DHCPv6 server option
  restrict-vendor-options  Restrict vendor specific options to be sent in
                           server reply
  server-preference        Server preference value sent in the reply, by the
                           server to client

  clrscr                   Clears the display screen
  commit                   Commit all changes made in this session
  do                       Run commands from Exec mode
  end                      End current mode and change to EXEC mode
  exit                     End current mode and down to previous mode
  help                     Description of the interactive help system
  revert                   Revert changes
  service                  Service Commands
  show                     Show running system information
  write                    Write running configuration to memory or terminal

rfs6000-81742D(config-dhcpv6-server-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing DHCPv6 server policy |

**NOTE:** For more information on DHCP policy, see *Chapter 12, DHCP-SERVER-POLICY*.

## 4.1.44 dns-whitelist

*Global Configuration Commands*

Configures a DNS whitelist. A DNS whitelist is a list of domains allowed access to the network.

The following table lists DNS Whitelist configuration mode commands:

**Table 4.22** *DNS-Whitelist Config Commands*

| Command | Description | Reference |
|---|---|---|
| *dns-whitelist* | Creates a DNS whitelist and enters its configuration mode | *page 4-204* |
| *dns-whitelist-mode commands* | Summarizes DNS whitelist configuration mode commands | *page 4-205* |

### 4.1.44.1 dns-whitelist

*dns-whitelist*

Configures a DNS whitelist. A DNS whitelist is a list of allowed DNS destination IP addresses pre-approved to access a controller, service platform, or access point managed captive portal.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
dns-whitelist <DNS-WHITELIST-NAME>
```

**Parameters**

- `dns-whitelist <DNS-WHITELIST-NAME>`

| | |
|---|---|
| <DNS-WHITELIST-NAME> | Specify the DNS whitelist name. If the whitelist does not exist, it is created. |

**Example**

```
rfs6000-81742D(config)#dns-whitelist test
rfs6000-81742D(config-dns-whitelist-test)#?
DNS Whitelist Mode commands:
  no       Negate a command or set its defaults
  permit   Match a host

  clrscr   Clears the display screen
  commit   Commit all changes made in this session
  end      End current mode and change to EXEC mode
  exit     End current mode and down to previous mode
  help     Description of the interactive help system
  revert   Revert changes
  service  Service Commands
  show     Show running system information
  write    Write running configuration to memory or terminal

rfs6000-81742D(config-dns-whitelist-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing DNS Whitelist |

### 4.1.44.2 dns-whitelist-mode commands

*dns-whitelist*

The following table summarizes DNS Whitelist configuration mode commands:

**Table 4.23** *DNS-Whitelist-Mode Commands*

| Command | Description | Reference |
|---|---|---|
| *permit* | Permits a host, existing on a DNS whitelist, access to the network or captive portal | *page 4-206* |
| *no* | Negates a command or reverts to default | *page 4-207* |

### 4.1.44.2.1 permit

*dns-whitelist-mode commands*

A whitelist is a list of host names and IP addresses permitted access to the network or captive portal. This command adds a host or destination IP address to the DNS whitelist.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
permit <IPv4/IPv6/HOSTNAME> {suffix}
```

**Parameters**

- `permit <IPv4/IPv6/HOSTNAME> {suffix}`

| | |
|---|---|
| <IPv4/IPv6/ HOSTNAME> | Adds a device to the DNS whitelist<br>• <IPv4/IPv6/HOSTNAME> – Provide a hostname or numerical IPv4 or IPv6 address for each destination IP address or host included in the whitelist.<br>A maximum of 256 entries can be made. |
| suffix | Optional. Matches any hostname or domain name including the specified name as suffix |

**Example**

```
rfs6000-81742D(config-dns-whitelist-test)#permit example_company.com suffix

rfs6000-81742D(config-dns-whitelist-test)#show context
dns-whitelist test
permit example_company.com suffix
rfs6000-81742D(config-dns-whitelist-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes a DNS whitelist entry |

### 4.1.44.2.2 no

*dns-whitelist-mode commands*

Removes a specified host or IP address from the DNS whitelist, and prevents it from accessing network resources

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
no permit <IPv4/IPv6/HOSTNAME>
```

**Parameters**

- `no permit <IPv4/IPv6/HOSTNAME>`

| | |
|---|---|
| <IPv4/IPv6/ HOSTNAME> | Removes a device from the DNS whitelist (identifies the device by its IP address or hostname)<br>• <IPv4/IPv6/HOSTNAME> – Specify the device's IPv4/IPv6 address or hostname. |

**Example**

```
rfs6000-81742D(config-dns-whitelist-test)#show context
dns-whitelist test
permit example_company.com suffix
rfs6000-81742D(config-dns-whitelist-test)#

rfs6000-81742D(config-dns-whitelist-test)#no permit example_company.com

rfs6000-81742D(config-dns-whitelist-test)#show context
dns-whitelist test
rfs6000-81742D(config-dns-whitelist-test)#
```

**Related Commands**

| | |
|---|---|
| *permit* | Adds a device to the DNS whitelist |

## 4.1.45 end

*Global Configuration Commands*

Ends and exits the current mode and moves to the PRIV EXEC mode

The prompt changes to the PRIV EXEC mode.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
end
```

**Parameters**

None

**Example**

```
rfs4000-229D58(config)#end
rfs4000-229D58#
```

## 4.1.46 event-system-policy

*Global Configuration Commands*

The following table lists event system configuration mode commands:

**Table 4.24** *Event-System-Policy Config Command*

| Command | Description | Reference |
|---|---|---|
| *event-system-policy* | Creates an event system policy and enters its configuration mode | *page 4-210* |
| *event-system-policy-mode commands* | Summarizes event system policy configuration mode commands | *page 4-211* |

### 4.1.46.1 event-system-policy

*event-system-policy*

Configures a system wide events handling policy

Event system policies enable administrators to create notification mechanisms using one, some, or all of the SNMP, syslog, controller forwarding, or email notification options available to the controller or service platform. Each listed event can have customized notification settings defined and saved as part of an event policy. Thus, policies can be configured and administrated in respect to specific sets of client association, authentication or encryption, and performance events. Once policies are defined, they can be mapped to device profiles strategically as the likelihood of an event applies to particular devices.

To view an existing event system policy configuration details, use the *show > event-system-policy* command.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
event-system-policy <EVENT-SYSTEM-POLICY-NAME>
```

**Parameters**

- `event-system-policy <EVENT-SYSTEM-POLICY-NAME>`

| | |
|---|---|
| <EVENT-SYSTEM-POLICY-NAME> | Specify the event system policy name. If the policy does not exist, it is created. |

**Example**

```
rfs6000-81701D(config)#event-system-policy event-testpolicy
rfs6000-81701D(config-event-system-policy-event-testpolicy)#?
Event System Policy Mode commands:
  event    Configure an event
  no       Negate a command or set its defaults

  clrscr   Clears the display screen
  commit   Commit all changes made in this session
  do       Run commands from Exec mode
  end      End current mode and change to EXEC mode
  exit     End current mode and down to previous mode
  help     Description of the interactive help system
  revert   Revert changes
  service  Service Commands
  show     Show running system information
  write    Write running configuration to memory or terminal

rfs6000-81701D(config-event-system-policy-event-testpolicy)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an event system policy |

### 4.1.46.2 event-system-policy-mode commands

*event-system-policy*

The following table summarizes event system policy configuration mode commands:

**Table 4.25** *Event-System-Policy Mode Commands*

| Command | Description | Reference |
|---|---|---|
| *event* | Configures an event | *page 4-212* |
| *no* | Negates a command or reverts to default | *page 4-225* |

### 4.1.46.2.1 event

*event-system-policy-mode commands*

Configures an event and sets the action performed when the event happens

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
event <EVENT-TYPE> <EVENT-NAME> (email,forward-to-switch,snmp,syslog)
[default|on|off]
The event types are:

rfs6000-81742D(config-event-system-policy-testpolicy)#event ?
  aaa              AAA/Radius module
  adapt            Adaptivity Module
  adopt-service    Adoption Service
  adv-wips         Adv-wips module
  ap               Access Point module
  bt               Bluetooth
  captive-portal   Captive Portal
  cdp              Cisco Discovery Protocol
  certmgr          Certificate Manager (Not valid for NCAP/MCN)
  cfgd             Cfgd module
  cluster          Cluster module
  crm              Critical Resource Monitoring
  database         Database Services
  device           Device module
  dhcpsvr          DHCP Configuration Daemon
  diag             Diag module
  dot11            802.11 management module
  dot1x            802.1X Authentication
  fwu              Firmware update module
  isdn             Isdn module
  l2gre            Layer 2 GRE Tunnel
  l2tpv3           Layer 2 Tunneling Protocol Version 3
  licmgr           License module
  lldp             Link Layer Discovery Protocol
  mesh             Mesh module
  mgmt             Management Services
  nsm              Network Services Module
  pm               Process-monitor module
  radconf          Radius Configuration Daemon
  rasst            Roaming-Assist module
  radio            Radio module
  smrt             Smart-rf module
  smtpnot          Smtpnot module
  system           System module
  test             Test module
  vrrp             Virtual Router Redundancy Protocol
  webf             Webf module
  wips             Wireless IPS module

rfs6000-81742D(config-event-system-policy-testpolicy)#
```

**NOTE:** The parameter values for <EVENT-TYPE> and <EVENT-NAME> are summarized in the table under the Parameters section.

**Parameters**

```
• event <EVENT-TYPE> <EVENT-NAME> (email,forward-to-switch,snmp,syslog)
[default|on|off]
```

| <event-type> | <event-name> |
|---|---|
| aaa | Enables and configures logging of the following authentication, authorization, and accounting related events:<br>• radius-discon-msg – RADIUS disconnection<br>• radius-session-expired – RADIUS session expired<br>• radius-session-not-started – RADIUS session not started<br>• radius-vlan-update – RADIUS VLAN update |
| adapt | Enables and configures logging of the following adaptivity module related events:<br>• adaptivity-change – Event adaptivity change<br>• adaptivity-rehome – Event adaptivity rehome |
| adopt-services | Enables and configures the logging of adopted services related events |
| adv-wips | Enables and configures the logging of advanced WIPS related events |
| ap | Enables and configures logging of the following AP related events:<br>• adopted – Event AP adopted<br>• adopted-to-controller – Event AP adopted to wireless controller<br>• ap-adopted – Event access port adopted<br>• ap-autoup-done – Event AP autoup done<br>• ap-autoup-fail – Event AP autoup fail<br>• ap-autoup-needed – Event AP autoup needed<br>• ap-autoup-no-need – Event AP autoup not needed<br>• ap-autoup-reboot – Event AP autoup reboot<br>• ap-autoup-timeout – Event AP autoup timeout<br>• ap-autoup-ver – Event AP autoup version<br>• ap-reset-detected – Event access port reset detected<br>• ap-reset-request – Event access port user requested reset<br>• ap-timeout – Event access port timed out<br>• ap-unadopted – Event access port unadopted<br>• image-parse-failure – Event image parse failure message<br>• legacy-auto-update – Event legacy auto update<br>• no-image-file – Event no image file<br>• offline – Event AP detected as offline<br>• online – Event offline AP detected as online<br>Contd... |

| <event-type> | <event-name> |
|---|---|
| | • reset – Event AP reset<br>• sw-conn-lost – Event software connection with AP lost<br>• unadopted – Event AP unadopted |
| bt | Enables and configures logging of the following bluetooth related events:<br>• bt-started – Event *bluetooth* (bt) started<br>• bt-state-change – Event bt state change |
| captive-portal | Enables and configures logging of the following captive portal (hotspot) related events:<br>• allow-access – Event client allowed access<br>• auth-failed – Event client authentication failed<br>• auth-success – Event client authentication success<br>• client-disconnect – Event client disconnected<br>• client-removed – Event client removed<br>• data-limit-exceed – Event client data limit exceed<br>• flex-log-access – Event flexible log access granted to client<br>• inactivity-timeout – Event client time-out due to inactivity<br>• page-cre-failed – Event captive portal page creation failure<br>• purge-client – Event client purged<br>• session-timeout – Event client's session timeout<br>• vlan-switch – Event client switched VLAN |
| cdp | Enables and configures logging of the following *CISCO Discovery Protocol* (cdp) related event:<br>• duplex-mismatch – Event duplex mismatch detected between CDP neighbors |
| certmgr | Enables and configures logging of the following certificate manager related events (not applicable to AP6511 and AP6521 model access points):<br>• ca-cert-actions-failure – Event CA certificate actions failure<br>• ca-cert-actions-success – Event CA certificate actions success<br>• ca-key-actions-failure – Event CA key actions failure<br>• ca-key-actions-success – Event CA key actions success<br>• cert-expiry – Event certificate expiry<br>• crl-actions-failure – Event *Certificate Revocation List* (CRL) actions failure<br>• crl-actions-success – Event CRL actions success<br>• csr-export-failure – Event CSR export failure<br>• csr-export-success – Event CSR export success<br>• delete-trustpoint-action – Event delete trustpoint action<br>• export-trustpoint – Event trustpoint exported<br>• import-trustpoint – Event trustpoint imported<br>• rsa-key-actions-failure – Event RSA key actions failure<br>• rsa-key-actions-success – Event RSA key actions success<br>• svr-cert-actions-success – Event server certificate actions success<br>• svr-cert-actions-failure – Event server certificate actions failure |

| <event-type> | <event-name> |
|---|---|
| certmgr-lite | Enables and configures logging of certificate manager (lite version) related event messages (applicable only to AP6521 and AP6511 model access points) |
| cfgd | Enables and configures logging of the following configuration daemon module related events:<br>• acl-attached-altered – Event *Access List* (ACL) attached altered<br>• acl-rule-altered – Event ACL rule altered |
| cluster | Enables and configures logging of the following cluster module related events:<br>• cmaster-cfg-update-fail – Event cluster master config update failed<br>• max-exceeded – Event maximum cluster count exceeded<br>• state-change – Event cluster state change (active/inactive)<br>• state-change-active – Event cluster state change to active<br>• state-change-inactive – Event cluster state change to inactive<br>• state-retain-active – Event cluster state retained as active |
| crm | Enables and configures logging of the following *Critical Resource Monitoring* (CRM) related events:<br>• critical-resource-down – Event critical resource goes down<br>• critical-resource-up – Event critical resource comes up |
| device | Enables and configures the logging of device module related events |
| database | Enables and configures logging of the following error conditions in the captive-portal/NSIght database:<br>• database-election-fail – Event primary database node selection failure. Requires manual intervention to select primary database node.<br>• database-exception – Event database may need to be dropped and device restarted<br>• database-low-disk-space – Event database low disk space<br>• Database-new-state – Event database state change<br>• database-op-failure – Event database failure<br>• database-set-name-mismatch – Event replica-set not enabled on host<br>• database-storage-mismatch – Event database mismatch. All database files must be removed.<br>• operation-complete – Event database operation completed successfully<br>• operation-failed – Event database operation failure |
| dhcpsvr | Enables and configures logging of the following DHCP server related events:<br>• dhcp-start – Event DHCP server started<br>• dhcpsvr-stop – Event DHCP sever stopped<br>• relay-iface-no-ip – Event no IP address on DHCP relay interface<br>• relay-no-iface – Event no interface for DHCP relay<br>• relay-start – Event relay agent started<br>• relay-stop – Event DHCP relay agent stopped |

| <event-type> | <event-name> |
|---|---|
| diag | Enables and configures logging of the following diagnostics module related events:<br>• autogen-tech-sprt – Event autogen technical support<br>• buf-usage – Event buffer usage<br>• cpu-load – Event CPU load<br>• cpu-usage-too-high – Event CPU usage high<br>• cpu-usage-too-high-recover – Event recovery from high CPU usage<br>• disk-usage – Event disk usage<br>• elapsed-time – Event elapsed time<br>• fan-underspeed – Event fan underspeed<br>• fd-count – Event forward count<br>• free-flash-disk – Event free flash disk<br>• free-flash-inodes – Event free flash inodes<br>• free-nvram-disk – Event free nvram disk<br>• free-nvram-inodes – Event free nvram inodes<br>• free-ram – Event free ram<br>• free-ram-disk – Event free ram disk<br>• free-ram-inodes – Event free ram inodes<br>• head-cache-usage – Event head cache usage<br>• high-temp – Event high temp<br>• ip-dest-usage – Event ip destination usage<br>• led-identify – Event led identify<br>• low-temp – Event low temp<br>• mem-usage-too-high – Event memory usage high<br>• mem-usage-too-high-recover – Event recovery from high memory usage<br>• new-led-state – Event new led state<br>• over-temp – Event over temp<br>• over-voltage – Event over voltage<br>• poe-init-fail – Event PoE init fail<br>• poe-power-level – Event PoE power level<br>• poe-read-fail – Event PoE read fail<br>• poe-state-change – Event PoE state change<br>• poe-state-change – Event PoE state change<br>• pwrsply-fail – Event failure of power supply<br>• raid-degraded – Event *Redundant Array of Independent Disks* (RAID) degraded<br>• raid-error – Event RAID error<br>• ram-usage – Event ram usage<br>• under-voltage – Event under voltage<br>• wd-reset-sys – Event wd reset system<br>• wd-state-change – Event wd state change |

| <event-type> | <event-name> |
|---|---|
| dot11 | Enables and configures logging of the following 802.11 management module related events:<br>• client-assoc-ignored – Wireless client association ignored event<br>• client-associated – Wireless client associated event<br>• client-denied-assoc – Event client denied association<br>• client-disassociated – Wireless client disassociated<br>• country-code – Event country code applied<br>• country-code-error – Event country code error<br>• eap-cached-keys – Event *Extensible Authentication Protocol* (EAP) cached keys<br>• eap-client-timeout – Event EAP client timeout<br>• eap-failed – Event EAP failed<br>• eap-opp-cached-keys – Event EAP opp cached keys<br>• eap-preauth-client-timeout – Event EAP pre authentication client timeout<br>• eap-preauth-failed – Event EAP pre authentication failed<br>• eap-preauth-server-timeout – Event EAP pre authentication server timeout<br>• eap-preauth-success – Event EAP pre authentication success<br>• eap-server-timeout – Event EAP server timeout<br>• eap-success – Event EAP success<br>• ft-roam-success – Event client fast BSS transition<br>• gal-rx-request – Event GAL request received event<br>• gal-tx-response – Event response sent to GAL request<br>• gal-validate-failed – Event GAL validation failed<br>• gal-validate-req – Event GAL validation request<br>• gal-validate-success – Event GAL validation success<br>• kerberos-client-success – Event client Kerberos authentication success<br>• kerberos-wlan-failed – Event WLAN Kerberos authentication failed<br>• kerberos-wlan-success – Event WLAN Kerberos authentication success<br>• kerberos-wlan-timeout – Event Kerberos authentication timed out<br>• move-operation-success – Event move operation success<br>• neighbor-denied-assoc – Event neighbor denied association<br>• tkip-cntrmeas-end – Event TKIP countermeasures ended<br>• tkip-cntrmeas-start – Event TKIP countermeasures initiated<br>• tkip-mic-fail-report – Event TKIP MIC failure report<br>• tkip-mic-failure – Event TKIP MIC check failed<br>• voice-call-completed – Event voice call completed<br>• voice-call-established – Event voice call established<br>• voice-call-failed – Event voice call failed<br>• wlan-time-access-disable – Event WLAN disabled by time-based-access<br>• wlan-time-access-enable – Event WLAN re-enabled by time-based-access<br>Contd.. |

| <event-type> | <event-name> |
|---|---|
| | • wlan-time-access-disable – Event WLAN disabled by time-based-access<br>• wlan-time-access-enable – Event WLAN re-enabled by time-based-access<br>• wpa-wpa2-failed – Event WPA-WPA2 failed<br>• wpa-wpa2-key-rotn – Event WPA-WPA2 key rotn<br>• wpa-wpa2-success – Event WPA-WPA2 success |
| dot1x | Enables and configures logging of the following 802.1X authentication related events:<br>• dot1x-failed – Event EAP authentication failure<br>• dot1x-success – Event dot1x-success |
| fwu | Enables and configures logging of the following *firmware update* (fwu) related events:<br>• fwuaborted – Event fwu aborted<br>• fwubadconfig – Event fwu aborted due to bad config<br>• fwucorruptedfile – Event fwu aborted due to corrupted file<br>• fwucouldntgetfile – Event fwu aborted because the system could not get file<br>• fwudone – Event fwu done<br>• fwufileundef – Event fwu aborted due to file undefined<br>• fwunoneed – Event fwu no need<br>• fwuprodmismatch – Event fwu aborted due to product mismatch<br>• fwuserverundef – Event fwu aborted due to server undefined<br>• fwuserverunreachable – Event fwu aborted due to server unreachable<br>• fwusignmismatch – Event fwu aborted due to signature mismatch<br>• fwusyserr – Event fwu aborted due to system error<br>• fwuunsupportedhw – Event fwu aborted due to unsupported hardware<br>• fwuunsupportedmodelnum – Event fwu aborted due to unsupported FIPS model number<br>• fwuvermismatch – Event fwu aborted due to version mismatch |
| isdn | Enables and configures logging of the following file *Integrated Service Digital Network* (ISDN) module related events:<br>• isdn-alert – Event ISDN alert<br>• isdn-crit – Event ISDN critical<br>• isdn-debug – Event ISDN debug<br>• isdn-emerg – Event ISDN emergency<br>• isdn-err – Event ISDN error<br>• isdn-info – Event ISDN info<br>• isdn-notice – Event ISDN notice<br>• isdn-warning – Event ISDN warning |
| l2gre | Enables and configures logging of the following *Layer 2 GRE* (L2GRE) tunnel related events:<br>• l2gre-tunnel-down – Event L2GRE tunnel down<br>• l2gre-tunnel-failover – Event L2GRE tunnel failover<br>• l2gre-tunnel-up – Event L2GRE tunnel up |

| <event-type> | <event-name> |
|---|---|
| l2tpv3 | Enables and configures logging of the following L2TPv3 related events:<br>• l2tpv3-tunnel-down – Event L2TPv3 tunnel down<br>• l2tpv3-tunnel-up – Event L2TPv3 tunnel up |
| licmgr | Enables and configures logging of the following license manager module related events:<br>• lic-installed-count – Event total number of license installed count<br>• lic-installed-default – Event default license installation<br>• lic-installed – Event license installed<br>• lic-invalid – Event license installation failed<br>• lic-removed – Event license removed |
| lldp | Enables and configures logging of the following *Link Layer Discovery Protocol* (LLDP) related events:<br>• lldp-loop-detected – Event layer 2 switching loop<br>• lldp-loop-recovery – Event recovery from layer 2 switching loop |
| mgmt | Enables and configures logging of the following management services module related events:<br>• log-http-init – Event Web server started<br>• log-http-local-start – Event Web server started in local mode<br>• log-http-start – Event Web server started in external mode<br>• log-https-start – Event secure Web server started<br>• log-https-wait – Event waiting for Web server to start<br>• log-key-deleted – Event RSA key associated with SSH is deleted<br>• log-key-restored – Event RSA key associated with SSH is added<br>• log-trustpoint-deleted – Event trustpoint associated with HTTPS is deleted |
| mesh | Enables and configures logging of the following mesh module related events:<br>• mesh-link-down – Event mesh link down<br>• mesh-link-up – Event mesh link up<br>• meshpoint-down – Event meshpoint down<br>• meshpoint-loop-prevent-off – Event meshpoint loop prevent off<br>• meshpoint-loop-prevent-on – Event meshpoint loop prevent on<br>• meshpoint-path-change – Event meshpoint-path-change<br>• meshpoint-root-change – Event meshpoint-root-change<br>• meshpoint-up – Event meshpoint up |
| nsm | Enables and configures logging of the following *Network Service Module* (NSM) related events:<br>• dhcpc-err – Event DHCP certification error<br>• dhcpdefrt – Event DHCP defrt<br>• dhcpip – Event DHCP IP<br>• dhcpipchg – Event DHCP IP change<br>• dhcpipnoadd – Event DHCP IP overlaps static IP address<br>Contd... |

| <event-type> | <event-name> |
|---|---|
| | • dhcplsexp – Event DHCP lease expiry<br>• dhcpnak – Event DHCP server returned DHCP NAK response<br>• dhcpnodefrt – Event interface no default route<br>• if-failback – Event interface failback message<br>• if-failover – Event interface failover message<br>• ifdown – Event interface down message<br>• ifipcfg – Event interface IP config message<br>• ifup – Event interface up message<br>• nsm-ntp – Event translate host name message<br>• ntp-start – Event NTP server start message<br>• ntp-stop – Event NTP server stop message |
| pm | Enables and configures logging of the following process monitor module related events:<br>• procid – Event proc ID generated<br>• procmaxrstrt – Event proc max restart<br>• procnoresp – Event proc no response<br>• procrstrt – Event proc restart<br>• procstart – Event proc start<br>• procstop – Event proc stop<br>• procsysrstrt – Event proc system restart<br>• startupcomplete – Event startup complete |
| radconf | Enables and configures logging of the following RADIUS configuration daemon related events:<br>• could-not-stop-radius – Event could not stop RADIUS server<br>• radiusdstart – Event RADIUS server started<br>• radiusdstop – Event RADIUS server stopped |
| radio | Enables and configures logging of the following radio module related events:<br>• acs-scan-complete – Event ACS scan completed<br>• acs-scan-started – Event ACS scan started<br>• cb-associated – Event client-bridge access point associates with an infrastructure access point<br>• cb-roam – Event client-bridge access point roams from one infrastructure access point to another infrastructure access point<br>• cb-wired-client-added – Event wired client is added to the client-bridge<br>• cb-wired-client-removed – Event wired client is removed from the client-bridge<br>• channel-country-mismatch – Event channel and country of operation mismatch<br>• radar-det-info – Event radar detected radar info<br>• radar-detected – Event radar detected<br>• radar-scan-completed – Event radar scan completed<br>• radar-scan-started – Event radar scan started<br>• radio-antenna-error – Event invalid antenna type on this radio<br>Contd.. |

| <event-type> | <event-name> |
|---|---|
| | • radio-antenna-setting – Event antenna type setting on this radio<br>• radio-state-change – Event radio state change<br>• resume-home-channel – Event resume home channel |
| rasst | Enables and configures the logging of roaming assist module related events |
| smrt | Enables and configures logging of the following SMART RF module related events:<br>• calibration-done – Event calibration done<br>• calibration-started – Event calibration started<br>• channel-change – Event channel change<br>• config-cleared – Configuration cleared event<br>• cov-hole-recovery – Event coverage hole recovery<br>• cov-hole-recovery-done – Event coverage hole recovery done<br>• interference-recovery – Event interference recovery<br>• neighbor-recovery – Event neighbor recovery<br>• power-adjustment – Event power adjustment<br>• root-recovery – Event meshpoint root recovery |
| smtpnot | Enables and configures logging of the following SMTP module related events:<br>• cfg – Event cfg<br>• cfginc – Event cfg inc<br>• net – Event net<br>• proto – Event proto<br>• smtpauth – Event SMTP authentication<br>• smtperr – Event SMTP error<br>• smtpinfo – Event SMTP information |
| system | Enables and configures logging of the following system module related events:<br>• clock-reset – Event clock reset<br>• cold-start – Event cold start<br>• config-commit – Event configuration commit<br>• config-revision – Event config-revision done<br>• devup-rfd-fail – Event device-upgrade failed on rf-domain manager managed devices<br>• guest-user-exp – Event guest user purging<br>• http-err – Event Web server failed to start<br>• login – Event user successfully logged in<br>• login-fail – Event login fail. Occurs when user authentication fails.<br>• login-fail-access – Event login fail access. Occurs in case of access violation.<br>• login-fail-bad-role – Event login fail bad role. Occurs when user uses an invalid role to logon.<br>Contd.. |

| <event-type> | <event-name> |
|---|---|
| system | • login-lockout – Event user account locked out message. Occurs when a user account is locked due to exceeding of maximum number failed login attempts threshold. Configure this event notification only if the max-fail and lockout-time parameters have been configured in the management-policy context. For more information, see *passwd-entry*.<br>• login-unlocked – Event user account un-locked. Occurs when a locked user account is re-activated. Enable this event notification only if the max-fail and lockout-time parameters have been configured in the management-policy context. For more information, see *passwd-entry*.<br>• logout – Event user logout<br>• maat-light – Event action on Research in Motion (RIM) radio(s) from the Maat light module<br>• panic – Event panic<br>• periodic-heart-beat – Event periodic heart beat<br>• procstop – Event proc stop<br>• server-unreachable – Event server-unreachable<br>• system-autoup-disable – Event system autoup disable<br>• system-autoup-enable – Event system autoup enable<br>• t5-config-error – Event t5-config-error<br>• ui-user-auth-fail – Event user authentication fail<br>• ui-user-auth-success – Event user authentication success<br>• warm-start – Event warm start<br>• warm-start-recover – Event recovery from warm start |
| test | Enables and configures logging of the following test module related events:<br>• testalert – Event test alert<br>• testargs – Event test arguments<br>• testcrit – Event test critical<br>• testdebug – Event test debug<br>• testemerg – Event test emergency<br>• testerr – Event test error<br>• testinfo – Event test information<br>• testnotice – Event test notice<br>• testwarn – Event test warning |
| vrrp | Enables and configures logging of the following *Virtual Router Redundancy Protocol* (VRRP) related events:<br>• vrrp-monitor-change – Event VRRP monitor link state change<br>• vrrp-state-change – Event VRRP state transition<br>• vrrp-vip-subnet-mismatch – Event VRRP IP not overlapping with an interface addresses |

| <event-type> | <event-name> |
|---|---|
| webf | Enables and configures logging of the following *Web Filtering* (webf) module related events:<br>• malform-url-request – Event malformed URL request<br>• no-parent-engine – Event 'no session to URL classification server'<br>• srvr-connect-fail – Event URL classification server unreachable<br>• url-blocked – Event URL blocked<br>• webf-lic-acquired – Event webf license acquired<br>• webf-lic-missing – Event webf license missing<br>• webf-lic-revoked – Event webf license revoked |
| wips | Enables and configures logging of the following Wireless IPS module related events:<br>• air-termination-active – Event air termination active<br>• air-termination-ended – Event air termination ended<br>• air-termination-inactive – Event air termination inactive<br>• air-termination-initiated – Event air termination initiated<br>• rogue-ap-active – Event rogue AP active<br>• rogue-ap-inactive – Event rogue AP inactive<br>• unsanctioned-ap-active – Event unsanctioned AP active<br>• unsanctioned-ap-inactive – Event unsanctioned AP inactive<br>• unsanctioned-ap-status-change – Event unsanctioned AP changed state<br>• wips-client-blacklisted – Event WIPS client blacklisted<br>• wips-client-rem-blacklist – Event WIPS client rem blacklist<br>• wips-event – Event WIPS event triggered |
| email | Sends e-mail notifications to a pre configured e-mail ID |
| forward-to-switch | Forwards the messages to an external server |
| snmp | Logs an SNMP event |
| syslog | Logs an event to syslog |
| default | Performs the default action for the event |
| off | Switches the event off, when the event happens, and no action is performed |
| on | Switches the event on, when the event happens, and the configured action is taken |

**Example**

```
rfs4000-229D58(config-event-system-policy-event-testpolicy)#event aaa radius-
discon-msg email on forward-to-switch default snmp default syslog default
rfs4000-229D58(config-event-system-policy-event-testpolicy)#

rfs4000-229D58(config-event-system-policy-testpolicy)#show context
event-system-policy test
 event aaa radius-discon-msg email on
rfs4000-229D58(config-event-system-policy-testpolicy)#

nx9500-6C8809(config-event-system-policy-test)#event database database-exception
 syslog default snmp default forward-to-switch default email default

nx9500-6C8809(config-event-system-policy-test)#event database operation-failed
syslog default snmp default forward-to-switch default email default
```

```
nx9500-6C8809(config-event-system-policy-test)#show context include-factory |
grep operation-failed
 event database operation-failed syslog default snmp default forward-to-switch
default email default
nx9500-6C8809(config-event-system-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Resets or disables event monitoring |

### 4.1.46.2.2 no

*event-system-policy-mode commands*

Negates an event monitoring configuration

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

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

**Parameters**

- `no <PARAMETERS>`

| | |
|---|---|
| no <PARAMETERS> | Removes event monitoring and message forwarding activity based on the parameters passed<br>The system stops network monitoring for the occurrence of the specified event and no notification is sent if the event occurs. |

**Example**

```
rfs4000-229D58(config-event-system-policy-TestPolicy)#event ap adopted syslog
default

rfs4000-229D58(config-event-system-policy-TestPolicy)#no event ap adopted syslog
```

**Related Commands**

| | |
|---|---|
| *event* | Configures the action taken for each event |

## 4.1.47 ex3500

*GLOBAL CONFIGURATION COMMANDS*

The following table lists EX3500 time-range configuration mode commands. It also provides links to other EX3500 related configuration modes:

**Table 4.26** *EX3500-Time-Range-List Config Command*

| Command | Description | Reference |
|---|---|---|
| *ex3500* | Creates an EX3500 time range list and enters its configuration mode | *page 4-227* |
| *ex3500-time-range-config-mode commands* | Summarizes EX3500 time range list configuration mode commands | *page 4-228* |
| *ex3500-management-policy* | Creates an EX3500 management policy and enters its configuration mode | *page 4-233* |
| *ex3500-qos-class-map-policy* | Creates an EX3500 QoS class map policy and enters its configuration mode | *page 4-254* |
| *ex3500-qos-policy-map* | Creates an EX3500 QoS policy map and enters its configuration mode | *page 4-262* |
| *ex3524* | Adds a EX3524 switch to the network | *page 4-277* |
| *ex3548* | Adds a EX3548 switch to the network | *page 4-279* |

### 4.1.47.1 ex3500

*ex3500*

Creates an EX3500 time range list and enters its configuration mode

An EX3500 time range list consists of a set of periodic and absolute time range rules. Periodic time ranges recur periodically at specified time periods, such as daily, weekly, weekends, weekdays, and on specific week days, for example on every successive Mondays. Absolute time ranges are not periodic and do not recur. They consist of a range of days during a particular time period (the starting and ending days and time are fixed).

The EX3500 series switch is a Gigabit Ethernet layer 2 switch with either 24 or 48 10/100/1000-BASE-T ports, and four *Small Form Factor Pluggable* (SFP) transceiver slots for fiber connectivity. The EX3500 series switch can adopt to a WiNG NOC controller and be managed by it. The EX3500 time range values configured here are used in EX3500 MAC ACL firewall rules that filter an EX3500's incoming and outgoing traffic. For more information on creating EX3500 MAC ACL rules, see *ex3500* and *access-group*.

**Supported in the following platforms:**

- Service Platforms — NX7500, NX9500

**Syntax**

```
ex3500 time-range <TIME-RANGE-NAME>
```

**Parameters**

- `ex3500 time-range <TIME-RANGE-NAME>`

| | |
|---|---|
| ex3500 time-range <TIME-RANGE-NAME> | Configures EX3500 time range list and enters its configuration mode<br>• <TIME-RANGE-NAME> – Enter a name for this EX3500 time range. If the time range does not exist, it is created. |

**Example**

```
nx9500-6C8809(config)#ex3500 time-range EX3500_TimeRange_02
nx9500-6C8809(config-ex3500-time-range-EX3500_TimeRange_02)#?
EX3500 Time Range Configuration commands:
  absolute  Absolute time and date
  no        Negate a command or set its defaults
  periodic  Periodic time and date

  clrscr    Clears the display screen
  commit    Commit all changes made in this session
  do        Run commands from Exec mode
  end       End current mode and change to EXEC mode
  exit      End current mode and down to previous mode
  help      Description of the interactive help system
  revert    Revert changes
  service   Service Commands
  show      Show running system information
  write     Write running configuration to memory or terminal

nx9500-6C8809(config-ex3500-time-range-EX3500_TimeRange_02)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes this EX3500 time range list |

### 4.1.47.2 ex3500-time-range-config-mode commands

*ex3500*

The following table summarizes EX3500 time-range configuration mode commands:

**Table 4.27** *EX3500-Time-Range-Mode Commands*

| Command | Description | Reference |
|---|---|---|
| *absolute* | Configures an absolute time range rule for this EX3500 time range list | *page 4-229* |
| *periodic* | Configures a periodic time range rule for this EX3500 time range list | *page 4-230* |
| *no* | Removes this EX3500 time range list settings | *page 4-232* |

### 4.1.47.2.1 absolute

*ex3500-time-range-config-mode commands*

Configures an absolute time range rule for this EX3500 time range list

Absolute time ranges are not periodic and do not recur. They consist of a range of days during a particular time period.

**Supported in the following platforms:**

- Service Platforms — NX7500, NX9500

**Syntax**

```
absolute start <0-23> <0-59> <1-31> <MONTH> <2013-2037> {end <0-23> <0-59> <1-31> <MONTH> <2013-2037>}
```

**Parameters**

- `absolute start <0-23> <0-59> <1-31> <MONTH> <2013-2037> {end <0-23> <0-59> <1-31> <MONTH> <2013-2037>}`

| | |
|---|---|
| absolute | Configures an absolute time range rule settings |
| start <0-23> <0-59> <1-31> <MONTH> <2013-2037> | Configures the start day and time settings<br>• <0-23> – Specify the start time from 0 - 23 hours.<br>• <0-59> – Specify the start time from 0 - 59 minutes.<br>For example, if the values provided are 12 hours and 30 minutes, the start time is 12:30 A.M on the specified day.<br>• <1-31> – Specify the day of month from 1 - 31 when the time range starts.<br>• <MONTH> – Specify the month. The options are: April, August, December, February, January, July, June, March, May, November, October, September.<br>• <2013-2037> – Specify the year from 2013 - 2037. |
| end <0-23> <0-59> <1-31> <MONTH> <2013-2037> | Optional. Configures the end day and time settings<br>• <0-23> – Specify the end time from 0 - 23 hours.<br>• <0-59> – Specify the end time from 0 - 59 minutes.<br>• <1-31> – Specify the day of month from 1 - 31 when the time range ends.<br>• <MONTH> – Specify the month. The options are: April, August, December, February, January, July, June, March, May, November, October, September.<br>• <2013-2037> – Specify the year from 2013 - 2037. |

**Example**

```
nx9500-6C8809(config-ex3500-time-range-EX3500-TimeRange-01)#absolute start 1 0 1
 june 2017 end 1 0 30 june 2018

nx9500-6C8809(config-ex3500-time-range-EX3500-TimeRange-01)#show context
ex3500 time-range EX3500-TimeRange-01
 absolute start 1 0 1 june 2017 end 1 0 30 june 2018
nx9500-6C8809(config-ex3500-time-range-EX3500-TimeRange-01)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes this absolute time range rule from the EX3500 time range list |

### 4.1.47.2.2 periodic

*ex3500-time-range-config-mode commands*

Configures a periodic time range rule for this EX3500 time range list

Periodic time ranges are configured to recur based on periodicity such as daily, weekly, weekends, weekdays, and on specific week days, such as on every successive Sunday.

**Supported in the following platforms:**

- Service Platforms — NX7500, NX9500

**Syntax**

```
periodic [daily|friday|monday|saturday|sunday|thursday|tuesday|wednesday|
weekdays|weekend] <0-23> <0-59> to [<023> <0-59>|daily|friday|monday|saturday|
sunday|thursday|tuesday|wednesday|weekdays|weekend] <0-23> <0-59> rule-precedence
<1-7>
```

**Parameters**

```
• periodic [daily|friday|monday|saturday|sunday|thursday|tuesday|wednesday|
weekdays|weekend] <0-23> <0-59> to [<023> <0-59>|daily|friday|monday|saturday|
sunday|thursday|tuesday|wednesday|weekdays|weekend] <0-23> <0-59> rule-precedence
<1-7>
```

| | |
|---|---|
| periodic [daily\|friday\|monday\|saturday\|sunday\|thursday\|tuesday\|wednesday\|weekdays\|weekend] | Configures this periodic time range's start day. The options are:<br>• daily<br>• Friday<br>• Monday<br>• Saturday<br>• Sunday<br>• Thursday<br>• Tuesday<br>• Wednesday<br>• weekdays<br>• weekend |
| <0-23> <0-59> | After specifying the start day, specify the start time in hours (24 hours format) and minutes<br>• <0-23> – Specify the start time from 0 - 23 hours.<br>• <0-59> – Specify the start time from 0 - 59 minutes.<br>For example, if the values provided are 12 hours and 30 minutes, the start time is 12:30 A.M on the specified day. |
| to [<023> <0-59>\|daily\|friday\|monday\|saturday\|sunday\|thursday\|tuesday\|wednesday\|weekdays\|weekend] | Configures this periodic time range's end day. This is the day when the time range ends. The options available changes depending on the *start day* configured. The options are:<br>• <0-23> <0-59> – Select this option to end the time range on the same day as it starts. Specify the end hour from 0 - 23 hours and the minutes from 0 - 59 minutes.<br>• daily – Select this option if the time range starts and ends every day at a specified time<br>• friday – Select this option if the time range ends on Fridays<br>Contd.. |

| | |
|---|---|
| | • monday – Select this option if the time range ends on Mondays<br>• saturday – Select this option if the time range ends on Saturdays<br>• sunday – Select this option if the time range ends on Sundays<br>• thursday – Select this option if the time range ends on Thursdays<br>• tuesday – Select this option if the time range ends on Tuesdays<br>• wednesday – Select this option if the time range ends on Wednesdays<br>• weekdays – Select this option if the time range ends on Weekdays<br>• weekend – Select this option if the time range ends on Weekends<br>If the time range does not end on the same day, select the end day, and then specify the end time, or else just specify the end time. |
| <0-23> <0-59> | After specifying the end day, specify the end time in hours (in 24 hours format) and minutes<br>• <0-23> – Specify the end time from 0 - 23 hours.<br>• <0-59> – Specify the end minute from 0 - 59 minutes.<br>In case of time ranges starting and ending on the same day, ensure that the end time (hours and minutes) is not lower than the specified start time. |
| rule-precedence <1-7> | Configures a precedence value for this periodic time range rule. Rules with lower precedence have higher priority and are applied first.<br>• <1-7> – Specify a precedence value from 1 - 7. |

**Example**

```
nx9500-6C8809(config-ex3500-time-range-EX3500-TimeRange-01)#periodic daily 1 10
to daily 23 10 rule-precedence 1

nx9500-6C8809(config-ex3500-time-range-EX3500-TimeRange-01)#show context
ex3500 time-range EX3500-TimeRange-01
 periodic daily 1 10 to daily 23 10 rule-precedence 1
 absolute start 1 0 1 june 2017 end 1 0 30 june 2018
nx9500-6C8809(config-ex3500-time-range-EX3500-TimeRange-01)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes this periodic time range rule from the EX3500 time range list |

### 4.1.47.2.3 no

*ex3500-time-range-config-mode commands*

Removes this EX3500 time range list settings

**Supported in the following platforms:**

- Service Platforms — NX7500, NX9500

**Syntax**

```
no [absolute|periodic]

no absolute

no periodic [daily|friday|monday|saturday|sunday|thursday|tuesday|wednesday|
weekdays|weekend] <0-23> <0-59> to [<0-23> <0-59>|daily|friday|monday|saturday|
sunday|thursday|tuesday|wednesday|weekdays|weekend]
```

**Parameters**

- `no <PARAMETERS>`

| | |
|---|---|
| no <PARAMETERS> | Removes this EX3500 time range list settings based on the parameters passed |

**Example**

```
nx9500-6C8809(config-ex3500-time-range-EX3500-TimeRange-01)#show context
ex3500 time-range EX3500-TimeRange-01
 periodic daily 1 10 to daily 23 10 rule-precedence 1
 absolute start 1 0 1 june 2015 end 1 0 30 june 2016
nx9500-6C8809(config-ex3500-time-range-EX3500-TimeRange-01)#

nx9500-6C8809(config-ex3500-time-range-EX3500-TimeRange-01)#no periodic daily 1
10 to daily 23 10 rule-precedence 1

nx9500-6C8809(config-ex3500-time-range-EX3500-TimeRange-01)#show context
ex3500 time-range EX3500-TimeRange-01
 absolute start 1 0 1 june 2015 end 1 0 30 june 2016
nx9500-6C8809(config-ex3500-time-range-EX3500-TimeRange-01)#
```

## 4.1.48 ex3500-management-policy

*Global Configuration Commands*

The following table lists EX3500 management policy configuration mode commands:

**Table 4.28** *EX3500-Management-Policy Config Command*

| Command | Description | Reference |
|---|---|---|
| *ex3500-management-policy* | Creates an EX3500 management policy and enters its configuration mode | *page 4-234* |
| *ex3500-management-policy config commands* | Summarizes EX3500 management policy configuration mode commands | *page 4-236* |
| *ex3500* | Creates an EX3500 time range list and enters its configuration mode | *page 4-226* |
| *ex3500-qos-class-map-policy* | Creates an EX3500 QoS class map policy and enters its configuration mode | *page 4-254* |
| *ex3500-qos-policy-map* | Creates an EX3500 QoS policy map and enters its configuration mode | *page 4-262* |
| *ex3524* | Adds a EX3524 switch to the network | *page 4-277* |
| *ex3548* | Adds a EX3548 switch to the network | *page 4-279* |

### 4.1.48.1 ex3500-management-policy

*ex3500-management-policy*

Creates an EX3500 management policy and enters its configuration mode. Once configured and applied on a EX3500 switch, the management policy controls access to the switch from management stations using SNMP.

The EX3500 management policy is either applied:

- Individually on an adopted EX3500 series switch (in the device configuration mode), or
- To a EX3524 and/or EX3548 profile, which is then applied to an adopted EX3500 series switch.

EX3500 devices (EX3524 and EX3548) are layer 2 Gigabit Ethernet switches with either 24 or 48 10/100/1000-BASE-T ports, and four SFP transceiver slots for fiber connectivity. Each 10/100/1000 Mbps port supports both the IEEE 802.3af and IEEE 802.3at-2009 PoE standards. An EX3500 switch has an SNMP-based management agent that provides both in-band and out-of-band management access. The EX3500 switch utilizes an embedded HTTP Web agent and CLI, which in spite of being different from that of the WiNG operating system provides WiNG controllers PoE and port management resources.

Going forward NX9500 and NX7500 WiNG managed series service platforms and WiNG VMs can discover, adopt, and partially manage EX3500 series Ethernet switches without modifying the proprietary operating system running the EX3500 switches. The WiNG service platforms utilize standardized WiNG interfaces to push configuration files to the EX3500 switches, and maintain a translation layer, understood by the EX3500 switch, for statistics retrieval.

WiNG can partially manage an EX3500 without using DHCP option 193, provided the EX3500 is directly configured to specify the IPv4 addresses of potential WiNG adopters. To identify the potential WiNG adopter, in the EX3500's device configuration mode specify the adopter's IPv4 address using the *controller > host > <IP-ADDRESS>* command. WiNG service platforms leave the proprietary operating system running the EX3500 switches unmodified, and partially manage them utilizing standardized WiNG interfaces. WiNG service platforms use a translation layer to communicate with the EX3500.

**Supported in the following platforms:**

- Service Platforms — NX7500, NX9500

**Syntax**

```
ex3500-management-policy <POLICY-NAME>
```

**Parameters**

- `ex3500-management-policy <POLICY-NAME>`

| | |
|---|---|
| <POLICY-NAME> | Specify the EX3500 management policy name. If the policy does not exist, it is created. |

**Example**

```
nx9500-6C8809(config)#ex3500-management-policy test
nx9500-6C8809(config-ex3500-management-policy-test)#?
EX3500_Management Mode commands:
  enable        Modifies enable password parameters
  http          Hyper Text Terminal Protocol (HTTP)
  memory        Memory utilization
  no            Negate a command or set its defaults
  process-cpu   Process-cpu utilization
  snmp-server   Enable SNMP server configuration
  ssh           Secure Shell server connections
  username      Login TACACS server port

  clrscr        Clears the display screen
  commit        Commit all changes made in this session
  do            Run commands from Exec mode
  end           End current mode and change to EXEC mode
  exit          End current mode and down to previous mode
  help          Description of the interactive help system
  revert        Revert changes
  service       Service Commands
  show          Show running system information
  write         Write running configuration to memory or terminal

nx9500-6C8809(config-ex3500-management-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes this EX3500 management policy |

### 4.1.48.2 ex3500-management-policy config commands

*ex3500-management-policy*

The following table summarizes EX3500 management policy configuration mode commands:

**Table 4.29** *EX3500-Management-Policy Config Mode Commands*

| Command | Description | Reference |
|---|---|---|
| *enable* | Configures an executive password for this EX3500 management policy | *page 4-237* |
| *http* | Configures the HTTP server settings used to authenticate HTTP connection to a EX3500 switch | *page 4-239* |
| *memory* | Configures the EX3500's memory utilization rising (upper) and falling (lower) threshold values | *page 4-240* |
| *process-cpu* | Configures the EX3500's CPU (processor) utilization rising (upper) and falling (lower) threshold values | *page 4-241* |
| *snmp-server* | Configures *Simple Network Management Protocol* (SNMP) server settings. Once configured and applied on a EX3500 switch, the management policy controls access to the switch from management stations using SNMP. | *page 4-242* |
| *ssh* | Configures the SSH server settings used to authenticate Secure Shell (SSH) connection to a EX3500 switch | *page 4-249* |
| *username* | Configures a EX3500 switch user settings | *page 4-251* |
| *no* | Removes or reverts this EX3500 management policy settings | *page 4-252* |

### 4.1.48.2.1 enable

*ex3500-management-policy config commands*

Configures an executive password for this EX3500 management policy

Each EX3500 management policy can have a unique executive password with its own privilege level assigned. Utilize these passwords as specific EX3500 management sessions require priority over others.

**Supported in the following platforms:**

- Service Platforms — NX7500, NX9500

**Syntax**

```
enable password [0|7|level]

enable password [0|7] <PASSWORD>

enable password level <0-15> [0 <PASSWORD>|7 <PASSWORD>]
```

**Parameters**

- `enable password [0|7] <PASSWORD>`

| | |
|---|---|
| enable password [0\|7] <PASSWORD> | Creates a new executive password for this EX3500 management policy. The password could be in clear text or encrypted<br>• 0 – Configures a clear text password using ASCII characters (should be 1 - 32 characters long)<br>• 7 – Configures an encrypted password using HEX characters (should be 32 characters long)<br>  • <PASSWORD> – Specify the password. |

- `enable password level <0-15> [0 <PASSWORD>|7 <PASSWORD>]`

| | |
|---|---|
| enable password level <0-15> | Creates a new executive password for this EX3500 management policy and sets its privilege level<br>• <0-15> – Specify the privilege level for this executive password from 0 - 15. Lower values have higher priority, to slot and prioritize executive passwords and EX3500 management sessions. |
| [0\|7] <PASSWORD> | After setting the privilege level, configure the password, which could be in clear text or encrypted<br>• 0 – Configures a clear text password using ASCII characters (should be 1 - 32 characters long)<br>• 7 – Configures an encrypted password using HEX characters (should be 32 characters long)<br>  • <PASSWORD> – Specify the password. |

**Example**

```
nx9500-6C8809(config-ex3500-management-policy-test)#enable password level 3 7
12345678901020304050607080929291

nx9500-6C8809(config-ex3500-management-policy-test)#show context
ex3500-management-policy test
 enable password level 3 7 12345678901020304050607080929291
 snmp-server notify-filter 1 remote 127.0.0.1
nx9500-6C8809(config-ex3500-management-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes a executive password from this EX3500 management policy |

### 4.1.48.2.2 http

*ex3500-management-policy config commands*

Configures the HTTP server settings used to authenticate HTTP connection to a EX3500 switch

Management access to an EX3500 switch can be enabled/disabled as required using separate interfaces and protocols (HTTP, SSH). Disabling un-used and insecure interfaces and unused management services can dramatically reduce an attack footprint and free resources within an EX3500 management policy.

**Supported in the following platforms:**

- Service Platforms — NX7500, NX9500

**Syntax**

```
http [port <1-65535>|secure-port <1-65535>|secure-server|server]
```

**Parameters**

- `http [port <1-65535>|secure-port <1-65535>|secure-server|server]`

| | |
|---|---|
| http | Configures following HTTP settings: port, secure-port, secure-server, and server |
| port <1-65535> | Configures the HTTP port number. This is the port used to connect to the HTTP server.<br>• <1-65535> – Specify a value from 1 - 65535. The default port is 80. |
| secure-port <1-65535> | Enables secure HTTP connection over a designated secure port. Ensure that the HTTP secure server is enabled before specifying the secure-server port.<br>• <1-65535> – Specify the secure HTTP server port from 1 - 65535. The default port is 443. |
| secure-server | Enables HTTP secure server. This option is disabled by default. |
| server | Enables HTTP server. This option is enabled by default. Consequently, HTTP management access is allowed by default. |

**Example**

```
nx9500-6C8809(config-ex3500-management-policy-test)#http secure-server

nx9500-6C8809(config-ex3500-management-policy-test)#show context
ex3500-management-policy test
 http secure-server
 enable password level 3 7 12345678901020304050607080929291
 snmp-server notify-filter 1 remote 127.0.0.1
nx9500-6C8809(config-ex3500-management-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Reverts to default HTTP server settings (HTTP server enabled, HTTP port 80) |

### 4.1.48.2.3 memory

*ex3500-management-policy config commands*

Configures the EX3500's memory utilization rising (upper) and falling (lower) threshold values. Once configured, the system sends a notification when the memory utilization exceeds the specified rising limit or falls below the specified falling limit.

By customizing an EX3500's memory and CPU utilization's upper and lower thresholds, you can avoid over utilization of the EX3500's processor capacity when sharing network resources with an NX series service platform or a WiNG VM.

**Supported in the following platforms:**

- Service Platforms — NX7500, NX9500

**Syntax**

```
memory [falling-threshold|rising-threshold] <1-100>
```

**Parameters**

- `memory [falling-threshold|rising-threshold] <1-100>`

| | |
|---|---|
| memory | Configures the EX3500's memory utilization rising and falling threshold values. The system generates a notification when either of these limits is exceeded. |
| falling-threshold <1-100> | Configures the falling threshold for the EX3500 memory utilization<br>• <1-100> – Specify the falling threshold as a percentage from 1 - 100. The default is 70%. |
| rising-threshold <1-100> | Configures the rising threshold for the EX3500's memory utilization<br>• <1-100> – Specify the rising threshold as a percentage from 1 - 100. The default is 90%. |

**Example**

```
nx9500-6C8809(config-ex3500-management-policy-test)#memory falling-threshold 50

nx9500-6C8809(config-ex3500-management-policy-test)#memory rising-threshold 95

nx9500-6C8809(config-ex3500-management-policy-test)#show context
ex3500-management-policy test
 http secure-server
 enable password level 3 7 12345678901020304050607080929291
 snmp-server notify-filter 1 remote 127.0.0.1
 memory falling-threshold 50
 memory rising-threshold 95
nx9500-6C8809(config-ex3500-management-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Reverts the memory utilization's falling-threshold and/or rising threshold to 70% and 90% respectively |

### 4.1.48.2.4 process-cpu

*ex3500-management-policy config commands*

Configures the EX3500's CPU (processor) utilization rising (upper) and falling (lower) threshold values. Once configured, the system sends a notification when the CPU utilization exceeds the specified rising limit or falls below the specified falling limit.

By customizing an EX3500's memory and CPU utilization's upper and lower thresholds, you can avoid over utilization of the EX3500's processor capacity when sharing network resources with an NX series service platform or a WiNG VM.

**Supported in the following platforms:**

- Service Platforms — NX7500, NX9500

**Syntax**

```
process-cpu [falling-threshold|rising-threshold] <1-100>
```

**Parameters**

- `process-cpu [falling-threshold|rising-threshold] <1-100>`

| | |
|---|---|
| process-cpu | Configures the EX3500's CPU utilization rising and falling threshold values. The system generates a notification when either of these limits is exceeded. |
| falling-threshold <1-100> | Configures the falling threshold for the EX3500's CPU utilization<br>• <1-100> – Specify the falling threshold as a percentage from 1 - 100. The default is 70%. |
| rising-threshold <1-100> | Configures the rising threshold for the EX3500's CPU utilization<br>• <1-100> – Specify the rising threshold as a percentage from 1 - 100. The default is 90%. |

**Example**

```
nx9500-6C8809(config-ex3500-management-policy-test)#process-cpu falling-threshold
60

nx9500-6C8809(config-ex3500-management-policy-test)#process-cpu rising-threshold
80

nx9500-6C8809(config-ex3500-management-policy-test)#show context
ex3500-management-policy test
 http secure-server
 enable password level 3 7 12345678901020304050607080929291
 snmp-server notify-filter 1 remote 127.0.0.1
 memory falling-threshold 50
 memory rising-threshold 95
 process-cpu falling-threshold 60
 process-cpu rising-threshold 80
nx9500-6C8809(config-ex3500-management-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Reverts the CPU utilization's falling-threshold and/or rising threshold to 70% and 90% respectively |

### 4.1.48.2.5 snmp-server

*ex3500-management-policy config commands*

Configures *Simple Network Management Protocol* (SNMP) server settings. Once configured and applied on a EX3500 switch, the management policy controls access to the switch from management stations using SNMP.

SNMP is an application layer protocol that facilitates the exchange of management information between the management stations and a managed EX3500 switch. SNMP-enabled devices listen on port 162 (by default) for SNMP packets from the management server. SNMP uses read-only and read-write community strings as an authentication mechanism to monitor and configure supported devices. The read-only community string is used to gather statistics and configuration parameters from a supported wireless device. The read-write community string is used by a management server to set device parameters. SNMP is generally used to monitor a system's performance and other parameters.

**Supported in the following platforms:**

- Service Platforms — NX7500, NX9500

**Syntax**

```
snmp-server {community|contact|enable|engine-id|group|host|location|notify-
filter|user|view}

snmp-server {community <STRING> {ro|rw}}

snmp-server {contact <NAME>}

snmp-server {enable traps {authentication|link-up-down}}

snmp-server {engine-id [local <WORD>|remote <IP> <WORD>]}

snmp-server {group <GROUP-NAME> [v1|v2c|v3 [auth|noauth|priv]] {notify <WORD>|
read <WORD>|write <WORD>}}

snmp-server {host <IP> [<STRING>|inform]}

snmp-server {host <IP> <STRING> version [v1|v2c|v3 [auth|noauth|priv]] {udp-port
<1-65535>}}

snmp-server {host <IP> inform [retry <0-255>|timeout <0-2147483647>] <STRING>
version [v2c|v3 [auth|noauth|priv]] {udp-port <1-65535>}}

snmp-server {location <WORD>}

snmp-server {notify-filter <WORD> remote <IP>}

snmp-server {user <USER-NAME> <GROUP-NAME> [remote-host|v1|v2c|v3]}

snmp-server {user <USER-NAME> <GROUP-NAME> remote-host <IP> v3 [auth|encrypted
auth] [md5|sha] <WORD> {priv [3des|aes128|aes192|aes256|des56] <WORD>}}

snmp-server {user <USER-NAME> <GROUP-NAME> [v1|v2c|v3]}

snmp-server {view <VIEW-NAME> <OID-TREE-STRING> [excluded|included]}
```

**Parameters**

- `snmp-server {community <STRING> {ro|rw}}`

| | |
|---|---|
| snmp-server community <STRING> {ro\|rw} | Configures SNMP-server related settings<br>• community – Optional. Configures an SNMP community access string used to authorize management access by clients using SNMP v1, v2c, or v3<br>  • <STRING> – Specify the SNMP community access string (should not exceed 32 characters).<br>After specifying the string, optionally specify the access type associated with it.<br>• ro – Optional. Provides read-only access with this SNMP community string. Allows authorized clients to only retrieve *Management Information Base* (MIB) objects. This is the default setting.<br>• rw – Optional. Provides read-write access with this SNMP community string. Allows authorized clients to retrieve as well as modify MIB objects.<br>You can configure a maximum of five (5) community strings per EX3500 management policy. |

- `snmp-server {contact <NAME>}`

| | |
|---|---|
| snmp-server contact <NAME> | Configures SNMP-server related settings<br>• contact – Optional. Configures the system's contact information<br>  • <NAME> – Specify the contact person's name (should not exceed 255 characters). |

- `snmp-server {enable traps {authentication|link-up-down}}`

| | |
|---|---|
| snmp-server enable traps {authentication\| link-up-down} | Configures SNMP-server related settings<br>• enable traps – Optional. Enables the EX3500 switch to send following SNMP traps or notifications:<br>  • authentication – Optional. Enables SNMP authentication trap. This option is disabled by default.<br>  • link-up-down – Optional. Enables SNMP link up and link down traps. This option is disabled by default.<br>If the command is executed without either of the above mentioned trap options, the system enables both authentication and link-up-down traps.<br>If enabling SNMP traps, use the snmp-server > host command to specify the host(s) receiving the SNMP notifications. |

- `snmp-server {engine-id [local <WORD>|remote <IP> <WORD>]}`

| | |
|---|---|
| snmp-server engine-id [local <WORD>\| remote <IP> <WORD>] | Configures SNMP-server related settings<br>• engine-id – Optional. Configures an identification string for the SNMPv3 engine. The SNMP engine is an independent SNMP agent residing either on the logged switch or on a remote device. It prevents message replay, delay, and redirection. In SNMPv3, the engine ID in combination with user passwords generates the security keys that is used for SNMPv3 packet authentication and encryption.<br>  • local – Configures the SNMP engine on the logged switch<br>  • <WORD> – Specify the hexadecimal engine ID string identifying the SNMP engine (should be 9 - 64 characters in length).<br>Contd.. |

| | |
|---|---|
| | • remote <IP> <WORD> – Configures a remote device as the SNMP engine<br>• <IP> – Specify the remote device's IP address.<br>• <WORD> – Specify the hexadecimal engine ID string identifying the SNMP engine (should be 9 - 64 characters in length).<br>Configure the remote engine ID when using SNMPv3 informs. The remote ID configured here is used to generate the security digest for authentication and encryption of packets exchanged between the switch and the and the remote host user. SNMP passwords are localized using the engine ID of the authoritative agent. For informs, the authoritative SNMP agent is the remote agent. You therefore need to configure the remote agent's SNMP engine ID before you can send proxy requests or informs to it. |

• `snmp-server {group <GROUP-NAME> [v1|v2c|v3 [auth|noauth|priv]] {notify <WORD>| read <WORD>|write <WORD>}}`

| | |
|---|---|
| snmp-server group <GROUP-NAME> | Configures SNMP-server related settings<br>• group – Optional. Configures an SNMP user group, mapping SNMP users to SNMP views<br>• <GROUP-NAME> – Specify the SNMP group name (should not exceed 32 characters). |
| [v1\|v2c\|v3 [auth\|noauth\|priv]] | Configures the SNMP version used for authentication by this user group<br>• v1 – Configures the SNMP version as v1.<br>• v2c – Configures SNMP version as v2c<br>• v3 – Configures the SNMP version as v3. If using SNMP v3, specify the authentication and encryption levels.<br>• auth – Uses SNMP v3 with authentication and *no* privacy<br>• noauth – Uses SNMP v3 with *no* authentication and *no* privacy<br>• priv – Uses SNMP v3 with authentication and privacy |
| notify <WORD> | Optional. Configures the notification view string<br>• <WORD> – Specify the string (should not exceed 32 characters). |
| read <WORD> | Optional. Configures the read view string<br>• <WORD> – Specify the string (should not exceed 32 characters). |
| write <WORD> | Optional. Configures the write view string<br>• <WORD> – Specify the string (should not exceed 32 characters). |

• `snmp-server {host <IP> <STRING> version [v1|v2c|v3 [auth|noauth|priv]] {udp-port <1-65535>}}`

| | |
|---|---|
| snmp-server host <IP> | Configures SNMP-server related settings<br>• host – Optional. Configures the host(s) receiving the SNMP notifications. At least one SNMP server host should be configured in order to configure the switch to send notifications<br>• <IP> – Specify the SNMP host's IP address.<br>You can configure a maximum of five (5) SNMP trap recipients per EX3500 management policy.<br>Ensure that SNMP trap notification is enabled. |

| | |
|---|---|
| <STRING> | Configures the SNMP community string. You can configure the SNMP community string here, or else use the string configured using the *snmp-server > community <STRING> > {ro\|rw}* command. It is recommended that you configure the SNMP community string prior to configuring the SNMP host.<br>• <STRING> – Specify the community string. The string configured here is sent in the SNMP traps to the SNMPv1 or SNMPv2c hosts. |
| version [v1\|v2c\| v3 [auth\|noauth\| priv]] | Configures the SNMP version used<br>• v1 – Configures the SNMP version as 1. This is the default setting.<br>• v2c – Configures SNMP version as 2c<br>• v3 – Configures the SNMP version as 3. If using SNMPv3, specify the authentication and encryption levels.<br>  • auth – Uses SNMP v3 with authentication and *no* privacy<br>  • noauth – Uses SNMP v3 with *no* authentication and *no* privacy<br>  • priv – Uses SNMP v3 with authentication and privacy |
| udp-port <1-65535> | Optional. After specifying the SNMP version, optionally specify the host UDP port<br>• <1-65535> – Specify the UDP port. The default is 162. |

• *snmp-server {host <IP> inform [retry <0-255>\|timeout <0-2147483647>] <STRING> version [v2c\|v3 [auth\|noauth\|priv]] {udp-port <1-65535>}}*

| | |
|---|---|
| snmp-server host <IP> | Configures SNMP-server related settings<br>• host – Optional. Configures the host(s) receiving the SNMP notifications<br>  • <IP> – Specify the SNMP host's IP address.<br>You can configure a maximum of five (5) SNMP trap recipients per EX3500 management policy.<br>Ensure that SNMP trap notification is enabled. |
| inform [retry <0-255>\| timeout <0-2147483647>] | Enables sending of SNMP notifications as inform messages, and configures inform message settings.<br>• retry <0-255> – Configures the maximum number attempts made to re-send an inform message in case the specified SNMP host does not acknowledge receipt.<br>  • <0-255> – Specify a value from 0 - 255. The default is 3.<br>• timeout <0-2147483647> – Configures the interval, in seconds, to wait for an acknowledgment from the SNMP host before re-sending an inform message<br>  • <0-2147483647> – Specify a value from 0 - 2147483647 seconds. The default is 1500 seconds.<br>Inform messages are more reliable than trap messages since they include a request for acknowledgement of receipt. Using inform messages to communicate critical information would be good practice. However, since inform messages are retained in the memory until a response is received, they consume more memory and may also result in traffic congestion. Take into considerations these facts when configuring the notification format. |
| <STRING> | Configures the SNMP community string. You can configure the SNMP community string here, or else use the string configured using the *snmp-server > community <STRING> > {ro\|rw}* command. It is recommended that you configure the SNMP community string prior to configuring the SNMP host.<br>• <STRING> – Specify the community string. The string configured here is sent in the SNMP inform messages to the SNMPv2c or SNMPv3 hosts. |

| | |
|---|---|
| version [v2c\| v3 [auth\|noauth\| priv]] | Configures the SNMP version used<br>• v2c – Configures the SNMP version as v2c<br>• v3 – Configures the SNMP version as v3. If using SNMP v3, specify the authentication and encryption levels.<br>  • auth – Uses SNMP v3 with authentication and *no* privacy<br>  • noauth – Uses SNMP v3 with *no* authentication and *no* privacy<br>  • priv – Uses SNMP v3 with authentication and privacy<br>SNMP inform messages are not supported on SNMP v1. |
| udp-port <1-65535> | Optional. After specifying the SNMP version, optionally specify the host UDP port<br>• <1-65535> – Specify the UDP port. The default is 162. |

- `snmp-server {location <WORD>}`

| | |
|---|---|
| snmp-server location <WORD> | Configures SNMP-server related settings<br>• location – Optional. Configures the EX3500's location string<br>  • <WORD> – Specify the location (should not exceed 255 characters). |

- `snmp-server {notify-filter <WORD> remote <IP>}`

| | |
|---|---|
| snmp-server notify-filter <WORD> | Configures SNMP-server related settings<br>• notify-filter – Optional. Modifies the SNMP server's notify filter<br>  • <WORD> – Specify the SNMP notify-filter name. |
| remote <IP> | Optional. Configures the remote host's IP address<br>• <IP> – Specify the IP address in the A.B.C.D format. |

- `snmp-server {user <USER-NAME> <GROUP-NAME> remote <IP> v3 {auth|encrypted auth} [md5|sha] <WORD> {priv [3des|aes128|aes192|aes256|des56] <WORD>}}`

| | |
|---|---|
| snmp-server user <USER-NAME> <GROUP-NAME> | Configures SNMP-server related settings<br>• user – Optional. Configures the name of the SNMP user (connecting to the SNMP agent) and adds the user to an existing SNMP group. It also specifies the SNMP version type used. In case of SNMP version 3, this command also configures the remote host's IP address and the authentication type used.<br>  • <USER-NAME> – Specify the user's name (should not exceed 32 characters).<br>  • <GROUP-NAME> – Specify the SNMP group name to which this user is assigned. |
| remote <IP> v3 | Configures the remote host on which the SNMPv3 engine is running<br>• <IP> – Specify the remote host's IP address.<br>This option is available only for SNMPv3 engine.<br>After configuring the remote host, optionally configure the authentication type and the corresponding authentication password used. |
| {auth\|encrypted auth} [md5\|sha] <WORD> {priv [3des\|aes128\|aes192\|aes256\|des56] <WORD>} | Optional. Configures authentication and encryption settings<br>• auth – Specifies the authentication type used and configures the authentication password<br>• encrypted – Enables encryption. When enabled all communications between the user and the SNMP engine are encrypted. After enabling encryption, specify the authentication type and configure the authentication password.<br>Contd.. |

| | |
|---|---|
| | The following parameters are common to the 'auth' and 'encrypted' keywords:<br>• md5 – Uses MD5 to authenticate the user<br>• sha – Uses SHA to authenticate the user<br>The following parameter is common to the 'md5' and 'sha' keywords:<br>• <WORD> – Specify the authentication password.<br>If the 'encrypted' option is not being used, enter an 8 - 40 characters ASCII password. Whereas, in case of an encrypted password enter a HEX characters password of 32 characters.<br>• priv – Optional. Uses SNMPv3 with privacy. Select one of the privacy options: des, aes128, aes192, aes256, des56<br>• <WORD> – Configures the privacy password. If the 'encrypted' option is not being used, enter an 8 - 40 characters long ASCII password. Whereas, the encrypted password should be 32 HEX characters. |

- `snmp-server {user <USER-NAME> <GROUP-NAME> [v1|v2c|v3]}`

| | |
|---|---|
| snmp-server user <USER-NAME> <GROUP-NAME> [v1\|v2c\|v3] | Configures SNMP-server related settings<br>• user – Optional. Configures the name of the SNMP user (connecting to the SNMP agent) and adds the user to an existing SNMP group. It also specifies the SNMP version type used. In case of SNMPv3, this command also configures the authentication type used and the enables encryption.<br>• <USER-NAME> – Specify the user's name (should not exceed 32 characters).<br>• <GROUP-NAME> – Specify the SNMP group name to which this user is assigned.<br>• [v1\|v2c\|v3] – After specifying the group name, specify the SNMP version used. The options are SNMP version v1, SNMP version 2c, and SNMP version 3.<br>If using SNMP version 3, optionally specify the authentication type and the corresponding authentication password used. Please see previous table for SNMPv3 authentication and encryption configuration details. |

- `snmp-server {view <VIEW-NAME> <OID-TREE-STRING> [excluded|included]}`

| | |
|---|---|
| snmp-server view <VIEW-NAME> | Configures SNMP-server related settings<br>• view – Optional. Creates an SNMP view. SNMP views are used to control user access to the MIB.<br>• <VIEW-NAME> – Provide a name for this SNMP view (should not exceed 32 characters). |
| <OID-TREE-STRING> [excluded\|included] | Configures the *object identifier* (OID) of a branch within the MIB tree<br>• excluded – Specifies an excluded view<br>• included – Specifies an included view |

**Example**

```
nx9500-6C8809(config-ex3500-management-policy-test)#snmp-server enable traps

nx9500-6C8809(config-ex3500-management-policy-test)#snmp-server host
192.168.13.10 snmpteststring version 1 udp-port 170

nx9500-6C8809(config-ex3500-management-policy-test)#snmp-server host 1.2.3.4
inform retry 2 test version 3 auth udp-port 180

nx9500-6C8809(config-ex3500-management-policy-test)#snmp-server engine-id local
1234567890

nx9500-6C8809(config-ex3500-management-policy-test)#show context
ex3500-management-policy test
 http secure-server
 enable password level 3 7 12345678901020304050607080929291
 snmp-server enable traps authentication
 snmp-server notify-filter 3 remote 1.2.3.4
 snmp-server notify-filter 1 remote 127.0.0.1
 snmp-server notify-filter 2 remote 192.168.13.10
 snmp-server host 1.2.3.4 inform timeout 1500 retry 2 test version 3 auth udp-port
180
 snmp-server host 192.168.13.10 snmpteststring version 1 udp-port 170
 snmp-server engine-id local 1234567890
 memory falling-threshold 50
 memory rising-threshold 95
 process-cpu falling-threshold 60
 process-cpu rising-threshold 80
nx9500-6C8809(config-ex3500-management-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes SNMP server related settings or reverts them to default |

### 4.1.48.2.6 ssh

*ex3500-management-policy config commands*

Configures the SSH server settings used to authenticate *Secure Shell* (SSH) connection to a EX3500 switch

Management access to an EX3500 switch can be enabled/disabled as required using separate interfaces and protocols (HTTP, SSH). Disabling un-used and insecure interfaces and unused management services can dramatically reduce an attack footprint and free resources within an EX3500 management policy.

**Supported in the following platforms:**

- Service Platforms — NX7500, NX9500

**Syntax**

```
ssh [authentication-retries <1-5>|server|server-key size <512-1024>|timeout <1-120>]
```

**Parameters**

```
• ssh [authentication-retries <1-5>|server|server-key size <512-1024>|timeout <1-120>]
```

| | |
|---|---|
| ssh | Enables SSH management access to an EX3500 switch. This option is disabled by default. Use this command to configure SSH access settings. |
| authentication-retries <1-5> | Configures the maximum number of retries made to connect to the SSH server resource<br>• <1-5> – Specify a value from 1 - 5. The default setting is 3. |
| server | Enables SSH server connection |
| server-key size <512-1024> | Configures the SSH server key size<br>• <512-1024> – Specify the SSH server key from 512 - 1,024. The default length is 768. |
| timeout <1-120> | Configures the SSH server resource inactivity timeout value in seconds. When the specified time is exceeded, the SSH server resource becomes unreachable and must be re-authenticated.<br>• <1-120> – Specify a value from 1 120 seconds. The default is 120 seconds. |

**Example**

```
nx9500-6C8809(config-ex3500-management-policy-test)#ssh authentication-retries 4

nx9500-6C8809(config-ex3500-management-policy-test)#ssh timeout 90

nx9500-6C8809(config-ex3500-management-policy-test)#ssh server-key size 600

nx9500-6C8809(config-ex3500-management-policy-test)#ssh server

nx9500-6C8809(config-ex3500-management-policy-test)#show context
ex3500-management-policy test
 ssh server
 ssh authentication-retries 4
 ssh timeout 90
 ssh server-key size 600
 http secure-server
 enable password level 3 7 12345678901020304050607080929291
 snmp-server enable traps authentication
 --More--
nx9500-6C8809(config-ex3500-management-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables SSH management access to an EX3500 switch |

### 4.1.48.2.7 username

*ex3500-management-policy config commands*

Configures a EX3500 switch user settings

The EX3500 switch user details are stored in a local database on the NX9500, NX7500, or WiNG VM. You can configure multiple users, each having a unique name, access level, and password.

**Supported in the following platforms:**

- Service Platforms — NX7500, NX9500

**Syntax**

```
username <USER-NAME> [access-level <0-15>|nopassword|password [0|7] <PASSWORD>]
```

**Parameters**

- `username <USER-NAME> [access-level <0-15>|nopassword|password [0|7] <PASSWORD>]`

| | |
|---|---|
| username <USER-NAME> | Configures the TACACS server port username<br>• <USER-NAME> – Specify the user name (should not exceed 32 characters) |
| access-level <0-15> | Configures the access level for this user. This value determines the access priority of each user requesting access and interoperability with EX3500 switch.<br>• <0-15> – Specify the access level from 0 - 15. The default is 0. |
| nopassword | Allows user to login without a password |
| password [0\|7] <PASSWORD> | Configures the password for this user<br>• 0 – Configures a plain text password<br>• 7 – Configures an encrypted password (should be 32 characters in length)<br>  • <PASSWORD> – Specify the password. |

**Example**

```
nx9500-6C8809(config-ex3500-management-policy-test)#username user1 access-level 5

nx9500-6C8809(config-ex3500-management-policy-test)#username user1 password 0
user1@1234

nx9500-nx9500-6C8809(config-ex3500-management-policy-test)#show context
ex3500-management-policy test
 ssh server
 ssh authentication-retries 4
 ssh timeout 90
 ssh server-key size 600
 http secure-server
 enable password level 3 7 12345678901020304050607080929291
 username user1 access-level 5
 username user1 password 7 5c4786c1e52f913d38168ce89154a079
 snmp-server enable traps authentication
 snmp-server notify-filter 3 remote 1.2.3.4
 snmp-server notify-filter 1 remote 127.0.0.1
--More--
nx9500-6C8809(config-ex3500-management-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes this SNMP user settings |

### 4.1.48.2.8 no

*ex3500-management-policy config commands*

Removes or reverts this EX3500 management policy settings

**Supported in the following platforms:**

- Service Platforms — NX7500, NX9500

**Syntax**

```
no [enable|http|memory|process-cpu|snmp-server|ssh|username]

no enable password {level <0-15>}

no http [port|secure-port|secure-sever|server]

no memory [falling-threshold|rising-threshold]

no process-cpu [falling-threshold|rising-threshold]

no snmp-server {community|contact|enable|engine-id|group|host|location|notify-
filter|user|view}

no snmp-server {community <STRING>}

no snmp-server {contact}

no snmp-server {enable traps {authentication|link-up-down}}

no snmp-server {engine-id [local|remote <IP>]}

no snmp-server {group <GROUP-NAME> [v1|v2c|v3 [auth|noauth|priv]]}

no snmp-server {host <IP>}

no snmp-server {location}

no snmp-server {notify-filter <WORD> remote <IP>}

no snmp-server {user <USER-NAME> [v1|v2c|v3]}

no snmp-server {user <USER-NAME> <GROUP-NAME> remote-host <IP> v3}

no snmp-server {view <VIEW-NAME> {<OID-TREE-STRING>}}

no ssh [authentication-retries|server|server-key size <512-1024>|timeout]

no username
```

**Parameters**

- no <PARAMETERS>

| | |
|---|---|
| no <PARAMETERS> | Removes this EX3500 management policy settings based on the parameters passed |

**Example**

```
nx9500-6C8809(config-ex3500-management-policy-test)#show context
ex3500-management-policy test
 ssh server
 ssh authentication-retries 4
 ssh timeout 90
 ssh server-key size 600
 http secure-server
 enable password level 3 7 12345678901020304050607080929291
 username user1 access-level 5
 username user1 password 7 5c4786c1e52f913d38168ce89154a079
 snmp-server enable traps authentication
 snmp-server notify-filter 3 remote 1.2.3.4
 snmp-server notify-filter 1 remote 127.0.0.1
 snmp-server notify-filter 2 remote 192.168.13.10
 snmp-server host 1.2.3.4 inform timeout 1500 retry 2 test version 3 auth udp-port
180
 snmp-server host 192.168.13.10 snmpteststring version 1 udp-port 170
 snmp-server engine-id local 1234567890
 memory falling-threshold 50
 memory rising-threshold 95
 process-cpu falling-threshold 60
 process-cpu rising-threshold 80
nx9500-6C8809(config-ex3500-management-policy-test)#

nx9500-6C8809(config-ex3500-management-policy-test)#no http secure-server

nx9500-6C8809(config-ex3500-management-policy-test)#no memory falling-threshold

nx9500-6C8809(config-ex3500-management-policy-test)#no process-cpu rising-
threshold

nx9500-6C8809(config-ex3500-management-policy-test)#no snmp-server notify-filter
3 remote 1.2.3.4

nx9500-6C8809(config-ex3500-management-policy-test)#show context
ex3500-management-policy test
 ssh server
 ssh authentication-retries 4
 ssh timeout 90
 ssh server-key size 600
 enable password level 3 7 12345678901020304050607080929291
 username user1 access-level 5
 username user1 password 7 5c4786c1e52f913d38168ce89154a079
 snmp-server enable traps authentication
 snmp-server notify-filter 1 remote 127.0.0.1
 snmp-server notify-filter 2 remote 192.168.13.10
 snmp-server host 1.2.3.4 inform timeout 1500 retry 2 test version 3 auth udp-port
180
 snmp-server host 192.168.13.10 snmpteststring version 1 udp-port 170
 snmp-server engine-id local 1234567890
 memory rising-threshold 95
 process-cpu falling-threshold 60
nx9500-6C8809(config-ex3500-management-policy-test)#
```

## 4.1.49 ex3500-qos-class-map-policy

*Global Configuration Commands*

The following table lists EX3500 QoS class map policy configuration mode commands:

**Table 4.30** *EX3500-QoS-Class-Map Config Command*

| Command | Description | Reference |
|---|---|---|
| *ex3500-qos-class-map-policy* | Creates an EX3500 QoS class map policy and enters its configuration mode | *page 4-255* |
| *ex3500-qos-class-map-policy config commands* | Summarizes EX3500 QoS class map policy configuration mode commands | *page 4-256* |
| *ex3500-qos-policy-map* | Creates an EX3500 QoS policy map and enters its configuration mode | *page 4-262* |
| *ex3500* | Creates an EX3500 time range list and enters its configuration mode | *page 4-226* |
| *ex3500-management-policy* | Creates an EX3500 management policy and enters its configuration mode | *page 4-233* |
| *ex3524* | Adds a EX3524 switch to the network | *page 4-277* |
| *ex3548* | Adds a EX3548 switch to the network | *page 4-279* |

### 4.1.49.1 ex3500-qos-class-map-policy

*ex3500-qos-class-map-policy*

Creates a EX3500 *Quality of Service* (QoS) class map policy and enters its configuration mode

A QoS class map policy contains a set of *Differentiated Services* (DiffServ) classification criteria that are used to classify incoming traffic into different category and provide differentiated service based on this classification. Each policy defines a set match criteria rules that use objects, such as access lists, IP precedence or DSCP values, and VLANs. When configured and applied, the policy classifies traffic based on layer 2, layer 3, or layer 4 information contained in each incoming packet.

**Supported in the following platforms:**

- Service Platforms — NX7500, NX9500

**Syntax**

```
ex3500-qos-class-map-policy <POLICY-NAME>
```

**Parameters**

- `ex3500-qos-class-map-policy <POLICY-NAME>`

| | |
|---|---|
| <POLICY-NAME> | Specify the EX3500 QoS class map policy name. If the policy does not exist, it is created. |

**Example**

```
nx9500-6C8809(config)#ex3500-qos-class-map-policy dscp
nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#?
EX3500_Qos_class_map Mode commands:
  description  Class-map description
  match        Defines the match criteria to classify traffic
  no           Negate a command or set its defaults
  rename       Redefines the name of class-map

  clrscr       Clears the display screen
  commit       Commit all changes made in this session
  do           Run commands from Exec mode
  end          End current mode and change to EXEC mode
  exit         End current mode and down to previous mode
  help         Description of the interactive help system
  revert       Revert changes
  service      Service Commands
  show         Show running system information
  write        Write running configuration to memory or terminal

nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing EX3500 QoS class map policy |

### 4.1.49.2 ex3500-qos-class-map-policy config commands

*ex3500-qos-class-map-policy*

The following table summarizes EX3500 QoS class map policy configuration mode commands:

**Table 4.31** *EX3500-Management-Policy Commands*

| Command | Description | Reference |
|---|---|---|
| *description* | Configures a description for this EX3500 QoS class map policy | *page 4-257* |
| *match* | Configures match criteria rules used to classify traffic | *page 4-258* |
| *rename* | Renames an existing EX3500 QoS class map object | *page 4-260* |
| *no* | Removes this EX3500 QoS class map policy's description and match criteria | *page 4-261* |

### 4.1.49.2.1 description

*ex3500-qos-class-map-policy config commands*

Configures this EX3500 QoS class map policy's description

**Supported in the following platforms:**

- Service Platforms — NX7500, NX9500

**Syntax**

```
description <LINE>
```

**Parameters**

- `description <LINE>`

| | |
|---|---|
| description <LINE> | Configures this EX3500 QoS class map policy's description<br>• <LINE> – Enter a description that allows to you differentiate it from other policies with similar configuration (should not exceed 64 characters) |

**Example**

```
nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#description "Matches
packets marked for DSCP service 3"

nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#show context
ex3500-qos-class-map-policy dscp
 description "Matches packets marked for DSCP service 3"
nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes this EX3500 QoS class map policy's description |

### 4.1.49.2.2 match

*ex3500-qos-class-map-policy config commands*

Configures match criteria rules used to classify traffic

Access lists, IP precedence, DSCP values, or VLANs are commonly used to classify traffic. Access lists select traffic based on layer 2, layer 3, or layer 4 information contained in each packet.

**Supported in the following platforms:**

- Service Platforms — NX7500, NX9500

**Syntax**

```
match [access-list [ex3500-ext-access-list|ex3500-std-access-list|mac-acl] <ACL-NAME>|cos <0-7>|ip [dscp <0-63>|precedence <0-7>]|ipv6 dscp <0-63>|vlan <1-4094>]
```

**Parameters**

```
• match [access-list [ex3500-ext-access-list|ex3500-std-access-list|mac-acl] <ACL-NAME>|cos <0-7>|ip [dscp <0-63>|precedence <0-7>]|ipv6 dscp <0-63>|vlan <1-4094>]
```

| | |
|---|---|
| match | Configures the match criteria. The options are: access-list, cos, ip, ipv6, vlan<br>Incoming packets matching the specified criteria are included in this QoS class map. |
| access-list [ex3500-ext-access-list\| ex3500-std-access-list\| mac-acl] <ACL-NAME> | Uses access lists to provide the match criteria. You can use any one the following ACL types to classify traffic:<br>• ex3500-ext-access-list – Uses an IPv4 EX3500 extended ACL<br>• ex3500-std-access-list – Uses an IPv4 EX3500 standard ACL<br>• mac-acl – Uses a MAC EX3500 ACL<br>The following keyword is common to all of the above ACL types:<br>• <ACL-NAME> – Specify the ACL name (should be existing and configured). |
| cos <0-7> | Configures the *class of service* (CoS) value used to apply user priority. CoS is a form of QoS applicable only to layer 2 Ethernet frames. It uses 3-bits (8 values) of the 802.1Q tag to differentiate and shape network traffic.<br>• <0-7> – Specify the CoS value from 0 - 7.<br>Following are the 8 traffic classes based on the CoS value:<br>000 (0) - Routine<br>001 (1) - Priority<br>010 (2) - Immediate<br>011 (3) - Flash<br>100 (4) - Flash Override<br>101 (5) - Critical<br>110 (6) - Internetwork Control<br>111 (7) - Network Control |

| | |
|---|---|
| ip [dscp <0-63>\| precedence <0-7>] | Configures the IPv4 DSCP value to match and/or the IP precedence value to match.<br>• <0-63> – Specify the DSCP value from 0 - 63. Use this option to specify the *type of service* (ToS) field values included in the IP header. The ToS field exists between the header length and the total length fields. The DSCP constitutes the first 6 bits of the ToS field.<br>• precedence <0-7> – Configures the IP precedence to match. Following are the 8 traffic classes based on the IP precedence values:<br>000 (0) - Routine<br>001 (1) - Priority<br>010 (2) - Immediate<br>011 (3) - Flash<br>100 (4) - Flash Override<br>101 (5) - Critical<br>110 (6) - Internetwork Control<br>111 (7) - Network Control |
| ipv6 dscp <0-63> | Configures the IPv6 DSCP value to match<br>• <0-63> – Specify the DSCP value from 0 - 63. |
| vlan <1-4094> | Configures the VLAN to match<br>• <1-4094> – Specify the VLAN ID. |

**Usage Guidelines**

When configuring match entries, take into consideration the following points:

- Deny rules included in an ACL (associated with a EX3500 QoS class map policy) are ignored whenever an incoming packet matches the ACL.
- A class map policy cannot include both IP ACL or IP precedence rule and a VLAN rule.
- A class map policy containing a MAC ACL or VLAN rule cannot include either an IP ACL or a IP precedence rule.
- A class map policy can include a maximum of 16 match entries.

**Example**

```
nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#match ip dscp 3

nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#show context
ex3500-qos-class-map-policy dscp
 description "Matches packets marked for DSCP service 3"
 match ip dscp 3
nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#

nx9500-6C8809(config-ex3500-qos-class-map-policy-test2)#match ip precedence 1
```

**Related Commands**

| | |
|---|---|
| *no* | Removes match criteria rules configured for this EX3500 QoS class map policy |

### 4.1.49.2.3 rename

*ex3500-qos-class-map-policy config commands*

Renames an existing EX3500 QoS class map policy

**Supported in the following platforms:**

- Service Platforms — NX7500, NX9500

**Syntax**

```
rename <EX3500-QOS-CLASS-MAP-POLICY-NAME> <NEW-EX3500-QOS-CLASS-MAP-POLICY-NAME>
```

**Parameters**

```
• rename <EX3500-QOS-CLASS-MAP-POLICY-NAME> <NEW-EX3500-QOS-CLASS-MAP-POLICY-
NAME>
```

| | |
|---|---|
| rename <EX3500-QOS-CLASS-MAP-POLICY-NAME> <NEW-EX3500-QOS-CLASS-MAP-NAME> | Renames an existing EX3500 QoS class map<br>• <EX3500-QOS-CLASS-MAP-POLICY-NAME> – Enter the EX3500 QoS class map's current name.<br>• <NEW-EX3500-QOS-CLASS-MAP-POLICY-NAME> – Enter the new name. |

**Example**

```
nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#rename [TAB]
dscp   test   test2
nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#

nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#rename test2 IP_Precedence

nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#rename [TAB]
dscp   IP_Precedence   test
nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#
```

### 4.1.49.2.4 no

*ex3500-qos-class-map-policy config commands*

Removes this EX3500 QoS class map policy's description and match criteria

**Supported in the following platforms:**

- Service Platforms — NX7500, NX9500

**Syntax**

```
no [description|match]

no description

no match [access-list [ex3500-ext-access-list|ex3500-std-access-list|mac-acl]
<ACL-NAME>|cos <0-7>|ip [dscp <0-63>|precedence <0-7>]|ipv6 dscp <0-63>|vlan <1-
4094>]
```

**Parameters**

- `no <PARAMETERS>`

| | |
|---|---|
| no <PARAMETERS> | Removes the EX3500 QoS class map policy's settings based on the parameters passed |

**Example**

The following example shows the EX3500 QoS class map policy 'test' settings before the 'no' command are executed:

```
nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#show context
ex3500-qos-class-map-policy dscp
 description "Matches packets marked for DSCP service 3"
 match ip dscp 3
nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#

nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#no description

nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#no match ip dscp
```

The following example shows the EX3500 QoS class map policy 'test' settings after the 'no' command are executed:

```
nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#show context
ex3500-qos-class-map-policy test
nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#
```

## 4.1.50 ex3500-qos-policy-map

*Global Configuration Commands*

The following table lists EX3500 QoS policy map configuration mode commands:

**Table 4.32** *EX3500-QoS-Policy-Map Config Command*

| Command | Description | Reference |
|---|---|---|
| *ex3500-qos-policy-map* | Creates a EX3500 policy map and enters its configuration mode | *page 4-263* |
| *ex3500-qos-policy-map config commands* | Summarizes EX3500 QoS policy map configuration mode commands | *page 4-264* |

### 4.1.50.1 ex3500-qos-policy-map

*ex3500-qos-policy-map*

Creates an EX3500 policy map and enters its configuration mode

An EX3500 policy map contains one or more EX3500 QoS class maps traffic classifications (existing and configured) and can be attached to multiple interfaces. Creates an EX3500 policy map, and then use the class parameter to configure policies for traffic that matches the criteria defined in the EX3500 QoS class map policy. For more information, see *match*.

**Supported in the following platforms:**

- Service Platforms — NX7500, NX9500

**Syntax**

```
ex3500-qos-policy-map <EX3500-QOS-POLICY-MAP-NAME>
```

**Parameters**

- `ex3500-qos-policy-map <EX3500-QOS-POLICY-MAP-NAME>`

| | |
|---|---|
| <EX3500-QOS-POLICY-MAP-NAME> | Specify the EX3500 policy map's name |

**Example**

```
nx9500-6C8809(config)#ex3500-qos-policy-map testPolicyMap
nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap)#?
EX3500_Qos_policy_map Mode commands:
  class         Defines a traffic classification for the policy
  description   Policy-map description
  no            Negate a command or set its defaults

  clrscr        Clears the display screen
  commit        Commit all changes made in this session
  do            Run commands from Exec mode
  end           End current mode and change to EXEC mode
  exit          End current mode and down to previous mode
  help          Description of the interactive help system
  revert        Revert changes
  service       Service Commands
  show          Show running system information
  write         Write running configuration to memory or terminal

nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing EX3500 QoS policy map |

### 4.1.50.2 ex3500-qos-policy-map config commands

*ex3500-qos-policy-map*

The following table summarizes EX3500 QoS policy map configuration mode commands:

**Table 4.33** *EX3500-QoS-Policy-Map Commands*

| Command | Description | Reference |
|---|---|---|
| *class* | Creates a policy map class and enters its configuration mode | *page 4-265* |
| *description* | Configures this EX3500 QoS policy map's description | *page 4-275* |
| *no* | Removes this EX3500 QoS policy map's settings. Use this keyword to remove or modify the description and to remove the QoS traffic classification created. | *page 4-276* |

### 4.1.50.2.1 class

*ex3500-qos-policy-map config commands*

Creates a policy map class and enters its configuration mode. The policy map class is a traffic classification upon which a policy can act.

**Supported in the following platforms:**

- Service Platforms — NX7500, NX9500

**Syntax**

```
class <EX3500-QoS-CLASS-MAP-POLICY-NAME>
```

**Parameters**

- `class <EX3500-QoS-CLASS-MAP-POLICY-NAME>`

| | |
|---|---|
| <EX3500-QoS-CLASS-MAP-POLICY-NAME> | Specify the EX3500 QoS class map policy's name (should be existing and configured) |

**Example**

```
nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap)#class dscp
nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#?
commands:
  no        Negate a command or set its defaults
  police    Defines a policer for classified traffic
  set       Classify IP traffic

  clrscr    Clears the display screen
  commit    Commit all changes made in this session
  do        Run commands from Exec mode
  end       End current mode and change to EXEC mode
  exit      End current mode and down to previous mode
  help      Description of the interactive help system
  revert    Revert changes
  service   Service Commands
  show      Show running system information
  write     Write running configuration to memory or terminal

nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes this policy map class association |
| *ex3500-qos-policy-map* | EX3500 QoS policy map configuration mode commands |

#### 4.1.50.2.2 ex3500-qos-policy-map-class-config commands

- *class*

The following table summarizes the policy map class configuration mode commands

**Table 4.34** *EX3500-Policy-Map-Class Config Command*

| Command | Description | Reference |
|---|---|---|
| *police* | Configures an enforcer for classified traffic | *page 4-267* |
| *set* | Sets *class of service* (CoS) value, *per-hop behavior* (PHB) value, and IP DSCP value in matching packets | *page 4-272* |
| *no* | Removes this traffic classification's settings | *page 4-274* |

### 4.1.50.2.3 police

*ex3500-qos-policy-map-class-config commands*

Configures an enforcer for classified traffic

**Supported in the following platforms:**

- Service Platforms — NX7500, NX9500

**Syntax**

```
police [flow|srtcm-color-aware|srtcm-color-blind|trtcm-color-aware|trtcm-color-blind]

police flow <0-1000000> <0-16000000> conform-action transmit violate-action [<0-63>|drop]

police [srtcm-color-aware|srtcm-color-blind] <0-1000000> <0-16000000> <0-16000000> conform-action transmit exceed-action [<0-63>|drop] violate-action [<0-63>|drop]

police [trtcm-color-aware|trtcm-color-blind] <0-1000000> <0-16000000> <0-1000000> <0-16000000> conform-action transmit exceed-action [<0-63>|drop] violate-action [<0-63>|drop]
```

**Parameters**

```
• police flow <0-1000000> <0-16000000> conform-action transmit violate-action [<0-63>|drop]
```

| | |
|---|---|
| police | Configures an enforcer for classified traffic |
| flow <0-1000000> <0-16000000> | Configures an enforcer for classified traffic based on the metered flow rate<br>• <0-1000000> – Configures the *committed information rate* (CIR) from 0 -1000000 kilobits per second.<br>• <0-16000000> – Configures the *committed burst size* (BC) from 0 - 16000000 bytes.<br>Policing is based on a token bucket, where bucket depth (i.e., the maximum burst before the bucket overflows) is specified by the committed-burst field, and the average rate tokens are added to the bucket is specified by the committed-rate option. Note that the token bucket functions similar to that described in RFC 2697 and RFC 2698.<br>The behavior of the meter is specified in terms of one token bucket (C), the rate at which the tokens are incremented CIR and the maximum size of the token bucket BC.<br>The token bucket C is initially full, that is, the token count Tc(0) = BC. Thereafter, the token count Tc is updated CIR times per second as follows:<br>• If Tc is less than BC, Tc is incremented by one, else<br>• Tc is not incremented.<br>When a packet of size B bytes arrives at time t, the following happens:<br>• If Tc(t)-B > OR = 0, the packet is green and Tc is decremented by B down to the minimum value of 0, else<br>• The packet is red and Tc is not decremented. |

| | |
|---|---|
| conform-action transmit | Configures the action applied when packets fall within the specified CIR and BC limits<br>• transmit – Transmits packets falling within the specified CIR and BC limits. This is subject to there being enough tokens to service the packet, in which case the packet is set green. |
| violate-action [<0-63>\|drop] | Configures the action applied when packets violate the specified CIR and BC limits<br>• <0-63> – Applies a new DSCP value. Select the DSCP value from 0 - 63.<br>• drops – Drops packets violating the specified CIR and BC limits |

```
• police [srtcm-color-aware|srtcm-color-blind] <0-1000000> <0-16000000> <0-
16000000> conform-action transmit exceed-action [<0-63>|drop] violate-action [<0-
63>|drop]
```

| | |
|---|---|
| police | Configures an enforcer for classified traffic |
| [srtcm-color-aware\| srtcm-color-blind] <0-1000000> <0-16000000> <0-16000000> | Configures an enforcer for classified traffic based on *single rate three color meter* (srTCM) mode. The srTCM as defined in RFC 2697 meters a traffic stream and processes its packets according to three traffic parameters – *Committed Information Rate* (CIR), *Committed Burst Size* (BC), and *Excess Burst Size* (BE).<br>• srtcm-color-blind - Single rate three color meter in color-blind mode<br>• srtcm-color-aware - Single rate three color meter in color-aware mode<br>The meter operates in one of two modes. In the color-blind mode, the meter assumes that the packet stream is uncolored. In color-aware mode the meter assumes that some preceding entity has pre-colored the incoming packet stream so that each packet is either green, yellow, or red. The marker (re)colors an IP packet according to the results of the meter. The color is coded in the DS<br>field [RFC 2474] of the packet.<br>• <0-1000000> – Configures the CIR from 0 -1000000 kilobits per second.<br>• <0-16000000> – Configures the BC from 0 - 1600000 bytes.<br>• <0-16000000> – Configures the BE from 0 - 1600000 bytes.<br>The behavior of the meter is specified in terms of its mode and two token buckets, C and E, which both share the common rate CIR. The maximum size of the token bucket C is BC and the maximum size of the token bucket E is BE.<br>The token buckets C and E are initially full, that is, the token count Tc(0) = BC and the token count Te(0) = BE. Thereafter, the token counts Tc and Te are updated CIR times per second as follows:<br>• If Tc is less than BC, Tc is incremented by one, else<br>• If Te is less then BE, Te is incremented by one, else<br>• neither Tc nor Te is incremented.<br>When a packet of size B bytes arrives at time t, the following happens if srTCM is configured to operate in color-blind mode:<br>• If Tc(t)-B > OR = 0, the packet is green and Tc is decremented by B down to the minimum value of 0, else<br>• if Te(t)-B > OR = 0, the packets is yellow and Te is decremented by B down to the minimum value of 0,<br>• else the packet is red and neither Tc nor Te is decremented.<br>Contd.. |

| | |
|---|---|
| | When a packet of size B bytes arrives at time t, the following happens if srTCM is configured to operate in color-aware mode:<br>• If the packet has been pre-colored as green and Tc(t)-B ? 0, the packet is green and Tc is decremented by B down to the minimum value of 0, else<br>• If the packet has been pre-colored as yellow or green and if<br>• Te(t)-B > OR = 0, the packets is yellow and Te is decremented by B down to the minimum value of 0, else the packet is red and neither Tc nor Te is decremented.<br>The metering policy guarantees a deterministic behavior where the volume of green packets is never smaller than what has been determined by the CIR and BC, that is, tokens of a given color are always spent on packets of that color. Refer to RFC 2697 for more information on other aspects of srTCM. |
| conform-action transmit | Configures the action applied when packet rates fall within the specified CIR and BC limits<br>• transmit – Transmits packets falling within the specified CIR and BC limits |
| exceed-action [<0-63>\|drop] | Configures the action applied when packet rates exceed the specified CIR and BC limits<br>• <0-63> – Applies a new DSCP value. Select the DSCP value from 0 - 63.<br>• drops – Drops packets exceeding the specified CIR and BC limits |
| violate-action [<0-63>\|drop] | Configures the action applied when packet rates exceed the specified BE limit<br>• <0-63> – Applies a new DSCP value. Select the DSCP value from 0 - 63.<br>• drops – Drops packets exceeding the specified BE limit |

• `police [trtcm-color-aware|trtcm-color-blind] <0-1000000> <0-16000000> <0-1000000> <0-16000000> conform-action transmit exceed-action [<0-63>|drop] violate-action [<0-63>|drop]`

| | |
|---|---|
| police | Configures an enforcer for classified traffic |
| [trtcm-color-aware\| trtcm-color-blind] <0-1000000> <0-16000000> <0-1000000> <0-16000000> | Configures an enforcer for classified traffic based on a *two rate three color meter* (trTCM) mode. The trTCM as defined in RFC 2698 meters a traffic stream and processes its packets based on two rates – *Committed Information Rate* (CIR) and *Peak Information Rate* (PIR), and their associated burst sizes - *Committed Burst Size* (BC) and *Peak Burst Size* (BP).<br>• trtcm-color-blind - Two rate three color meter in color-blind mode<br>• trtcm-color-aware - Two rate three color meter in color-aware mode<br>• <0-1000000> – Configures the CIR from 0 - 1000000 kilobits per second<br>• <0-16000000> – Configures the BC from 0 - 1600000 bytes.<br>• <0-1000000> – Configures the PIR from 0 - 1000000 kilobits per second<br>• <0-16000000> – Configures the BP from 0 - 1600000 bytes<br>The meter operates in one of two modes. In the color-blind mode, the meter assumes that the packet stream is uncolored. In color-aware mode the meter assumes that some preceding entity has pre-colored the incoming packet stream so that each packet is either green, yellow, or red. The marker (re)colors an IP packet according to the results of the meter. The color is coded in the DS field [RFC 2474] of the packet.<br>Contd.. |

| | |
|---|---|
| | The behavior of the meter is specified in terms of its mode and two token buckets, P and C, which are based on the rates PIR and CIR, respectively. The maximum size of the token bucket P is BP and the maximum size of the token bucket C is BC.<br>The token buckets P and C are initially (at time 0) full, that is, the token count Tp(0) = BP and the token count Tc(0) = BC. Thereafter, the token count Tp is incremented by one PIR times per second up to BP and the token count Tc is incremented by one CIR times per second up to BC.<br>When a packet of size B bytes arrives at time t, the following happens if trTCM is configured to operate in color-blind mode:<br>• If Tp(t)-B < 0, the packet is red, else<br>• if Tc(t)-B < 0, the packet is yellow and Tp is decremented by B, else<br>• The packet is green and both Tp and Tc are decremented by B.<br>When a packet of size B bytes arrives at time t, the following happens if trTCM is configured to operate in color-aware mode:<br>• If the packet has been pre-colored as red or if Tp(t)-B < 0, the packet is red, else<br>• if the packet has been pre-colored as yellow or if Tc(t)-B < 0, the packet is yellow and Tp is decremented by B, else<br>• the packet is green and both Tp and Tc are decremented by B.<br>The trTCM can be used to mark a IP packet stream in a service, where different, decreasing levels of assurances (either absolute or relative) are given to packets which are green, yellow, or red. Refer to RFC 2698 for more information on other aspects of trTCM. |
| conform-action transmit | Configures the action applied when packet rates fall within the specified CIR and BP limits<br>• transmit – Transmits packets falling within the specified CIR and BC limits |
| exceed-action [<0-63>\|drop] | Configures the action applied when packet rates exceed the specified CIR limit, but are within the specified PIR limit<br>• <0-63> – Applies a new DSCP value. Select the DSCP value from 0 - 63.<br>• drops – Drops packets exceeding the specified CIR and BC limit |
| violate-action [<0-63>\|drop] | Configures the action applied when packet rates exceed the specified PIR limit<br>• <0-63> – Applies a new DSCP value. Select the DSCP value from 0 - 63.<br>• drops – Drops packets exceeding the specified BE limit |

**Usage Guidelines**

When configuring the traffic class enforcer parameters, take into consideration the following factors:

- You can configure up to 200 enforcers/policers (i.e., class maps) for ingress ports.
- The committed-rate cannot exceed the configured interface speed, and the committed-burst cannot exceed 16 Mbytes.

**Example**

The following example uses the police trtcm-color-blind command to limit the average bandwidth to 100,000 Kbps, the committed burst rate to 4000 bytes, the peak information rate to 1,000,000 Kbps, the peak burst size to 6000, to remark any packets exceeding the committed burst size, and to drop any packets exceeding the peak information rate.

```
nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#police
 trtcm-color-blind 100000 4000 100000 6000 conform-action transmit exceed-action
 0 violate-action drop
nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#

nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#show
context
 class dscp
  police trtcm-color-blind 100000 4000 100000 6000 conform-action transmit exceed-
action 0 violate-action drop
nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the traffic enforcer settings |

### 4.1.50.2.4 set

*ex3500-qos-policy-map-class-config commands*

Sets *class of service* (CoS) value, *per-hop behavior* (PHB) value, and IP DSCP value in matching packets

**Supported in the following platforms:**

- Service Platforms — NX7500, NX9500

**Syntax**

```
set [cos <0-7>|ip dscp <0-63>|phb <0-7>]
```

**Parameters**

- `set [cos <0-7>|ip dscp <0-63>|phb <0-7>]`

| | |
|---|---|
| set | Sets the match criteria used to identify and classify traffic into different classes. The match criteria options are: CoS, IP DSCP, and PHB values. |
| cos <0-7> | Configures the CoS value for a matching packet (as specified by the match command) in the packet's VLAN tag<br>• <0-7> – Specify a value from 0 - 7. The CoS is modified to the value specified here. |
| ip dscp <0-63> | Modifies the IP DSCP value in a matching packet (as specified by the match command)<br>• <0-63> – Specify a value from 0 - 63. The DSCP value is modified to the value specified here. |
| phb <0-7> | Configures a PHB value for a matching packets<br>• <0-7> – Specify a value from 0 -7.<br>The PHB label is composed of five bits, three bits for per-hop behavior, and two bits for the color scheme used to control queue congestion. A packet is marked green, yellow, or red as per the following:<br>• green if it does not exceed the CIR and BC limits<br>• yellow if it exceeds the CIR and BC limits, but not the BE limit, and<br>• red otherwise. |

**Example**

The following example uses the *set > phb* command to classify the service that incoming packets will receive, and then uses the *police > trtcm-color-blind* command to limit the average bandwidth to 100,000 Kbps, the committed burst rate to 4000 bytes, the peak information rate to 1,000,000 Kbps, the peak burst size to 6000 bytes, to remark any packets exceeding the committed burst size, and to drop any packets exceeding the peak information rate.

```
nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-test2)#set
phb 3

nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-
test2)#police
 trtcm-color-blind 100000 4000 1000000 6000 conform-action transmit exceed-action
0 violate-action drop

nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-test2)#show
context
 class test2
  set phb 3
  police trtcm-color-blind 100000 4000 100000 6000 conform-action transmit exceed-
action 0 violate-action drop
nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-test2)#
```

The following example uses the *set > ip dscp* command to classify the service that incoming packets will receive, and then uses the *police > flow* command to limit the average bandwidth to 100,000 Kbps, the burst rate to 4000 bytes, and configure the response to drop any violating packets:

```
nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#set ip
dscp 3

nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#police
 flow 100000 4000 conform-action transmit violate-action drop

nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#show
context
 class dscp
  set ip dscp 3
  police flow 100000 4000 conform-action transmit violate-action drop
nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes CoS value, PHB value, or IP DSCP value from this traffic class |

### 4.1.50.2.5 no

*ex3500-qos-policy-map-class-config commands*

Removes this traffic classification's settings

**Supported in the following platforms:**

- Service Platforms — NX7500, NX9500

**Syntax**

```
no [police|set]

no police [flow|srtcm-color-aware|srtcm-color-blind|trtcm-color-aware|trtcm-
color-blind]

no set [cos|ip dscp|phb]
```

**Parameters**

- no <PARAMETERS>

| | |
|---|---|
| no <PARAMETERS> | Removes this traffic class settings based on the parameters passed |

**Example**

```
nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#show
context
 class dscp
  set ip dscp 3
  police flow 100000 4000 conform-action transmit violate-action drop
nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#

nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#no set
ip dscp

nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#no
police flow

nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#show
context
 class dscp
nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#
```

### 4.1.50.2.6 description

*ex3500-qos-policy-map config commands*

Configures this EX3500 QoS policy map's description

**Supported in the following platforms:**

- Service Platforms — NX7500, NX9500

**Syntax**

```
description <LINE>
```

**Parameters**

- `description <LINE>`

| | |
|---|---|
| description <LINE> | Configures this EX3500 QoS policy map's description<br>• <LINE> – Enter a description that allows to you differentiate it from other policies with similar configuration (should not exceed 64 characters) |

**Example**

```
nx9500-6C8809(config-ex3500-qos-policy-map-test)#description "This is a test
EX3500 QoS Policy Map"

nx9500-6C8809(config-ex3500-qos-policy-map-test)#show context
ex3500-qos-policy-map test
 description "This is a test EX3500 QoS Policy Map"
 class test
nx9500-6C8809(config-ex3500-qos-policy-map-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes this EX3500 QoS policy map's description |

#### 4.1.50.2.7 no

*ex3500-qos-policy-map config commands*

Removes this EX3500 QoS policy map's settings. Use this keyword to remove the description and to remove the QoS traffic classification created.

**Supported in the following platforms:**

- Service Platforms — NX7500, NX9500

**Syntax**

```
no [class <EX3500-QoS-POLICY-MAP-NAME>|description]
```

**Parameters**

- `no <PARAMETERS>`

| | |
|---|---|
| no <PARAMETERS> | Removes this EX3500 QoS policy map's settings based on the parameters passed |

**Example**

The following example shows the EX3500 QoS policy map 'test' settings before the 'no' command are executed:

```
nx9500-6C8809(config-ex3500-qos-policy-map-test)#show context
ex3500-qos-policy-map test
 description "This is a test EX3500 QoS Policy Map"
 class test
nx9500-6C8809(config-ex3500-qos-policy-map-test)#

nx9500-6C8809(config-ex3500-qos-policy-map-test)#no description

nx9500-6C8809(config-ex3500-qos-policy-map-test)#no class test
```

The following example shows the EX3500 QoS policy map 'test' settings after the 'no' command are executed:

```
nx9500-6C8809(config-ex3500-qos-policy-map-test)#show context
ex3500-qos-policy-map test
nx9500-6C8809(config-ex3500-qos-policy-map-test)#
```

## 4.1.51 ex3524

*Global Configuration Commands*

Adds a EX3524 switch to the network

The EX3500 series switch is a Gigabit Ethernet layer 2 switch with either 24 or 48 10/100/1000-BASE-T ports, and four *Small Form Factor Pluggable* (SFP) transceiver slots for fiber connectivity.

To enable layer 3 adoption of the logged EX3524 switch to a NOC controller, navigate to the EX3524 switch's device configuration mode and execute the following command: *controller > host > <IP/HOSTANME>.*

EX3500 devices (EX3524 and EX3548) are layer 2 Gigabit Ethernet switches with either 24 or 48 10/100/1000-BASE-T ports, and four SFP transceiver slots for fiber connectivity. Each 10/100/1000 Mbps port supports both the IEEE 802.3af and IEEE 802.3at-2009 PoE standards. An EX3500 switch has an SNMP-based management agent that provides both in-band and out-of-band management access. The EX3500 switch utilizes an embedded HTTP Web agent and CLI, which in spite of being different from that of the WiNG operating system provides WiNG controllers PoE and port management resources.

Going forward NX9500 and NX7500 WiNG managed series service platforms and WiNG VMs can discover, adopt, and partially manage EX3500 series Ethernet switches without modifying the proprietary operating system running the EX3500 switches. The WiNG service platforms utilize standardized WiNG interfaces to push configuration files to the EX3500 switches, and maintain a translation layer, understood by the EX3500 switch, for statistics retrieval.

**Supported in the following platforms:**

- Service Platforms — NX7500, NX9500

**Syntax**

```
ex3524 <DEVICE-EX3524-MAC>
```

**Parameters**

- `ex3524 <DEVICE-EX3524-MAC>`

| | |
|---|---|
| <DEVICE-EX3524-MAC> | Specifies the MAC address of a EX3524 switch |

**Example**

```
nx9500-6C8809(config)#ex3524 A1-C4-33-6D-66-07

nx9500-6C8809(config-device-A1-C4-33-6D-66-07)#?
EX35xx Device Mode commands:
  hostname          Set system's network name
  interface         Select an interface to configure
  ip                Internet Protocol (IP)
  no                Negate a command or set its defaults
  power             EX3500 Power over Ethernet Command
  remove-override   Remove configuration item override from the device (so
                    profile value takes effect)
  upgrade           Configures upgrade option for ex3500 system
  use               Set setting to use

  clrscr            Clears the display screen
  commit            Commit all changes made in this session
  do                Run commands from Exec mode
  end               End current mode and change to EXEC mode
  exit              End current mode and down to previous mode
  help              Description of the interactive help system
  revert            Revert changes
```

```
  service          Service Commands
  show             Show running system information
  write            Write running configuration to memory or terminal

nx9500-6C8809(config-device-A1-C4-33-6D-66-07)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes a EX3524 switch from the network |

## 4.1.52 ex3548

*Global Configuration Commands*

Adds a EX3548 switch to the network

The EX3500 series switch is a Gigabit Ethernet layer 2 switch with either 24 or 48 10/100/1000-BASE-T ports, and four SFP transceiver slots for fiber connectivity.

**Supported in the following platforms:**

- Service Platforms — NX7500, NX9500

**Syntax**

```
ex3548 <DEVICE-EX3548-MAC>
```

**Parameters**

- `ex3548 <DEVICE-EX3548-MAC>`

| | |
|---|---|
| <DEVICE-EX3548-MAC> | Specifies the MAC address of a EX3548 switch |

**Example**

```
nx9500-6C8809(config)#ex3548 22-65-78-09-12-35
nx9500-6C8809(config-device-22-65-78-09-12-35)#?
EX35xx Device Mode commands:
  hostname          Set system's network name
  interface         Select an interface to configure
  ip                Internet Protocol (IP)
  no                Negate a command or set its defaults
  power             EX3500 Power over Ethernet Command
  remove-override   Remove configuration item override from the device (so
                    profile value takes effect)
  upgrade           Configures upgrade option for ex3500 system
  use               Set setting to use

  clrscr            Clears the display screen
  commit            Commit all changes made in this session
  do                Run commands from Exec mode
  end               End current mode and change to EXEC mode
  exit              End current mode and down to previous mode
  help              Description of the interactive help system
  revert            Revert changes
  service           Service Commands
  show              Show running system information
  write             Write running configuration to memory or terminal

nx9500-6C8809(config-device-22-65-78-09-12-35)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes a EX3548 switch from the network |

## 4.1.53 firewall-policy

*Global Configuration Commands*

Configures a firewall policy. This policy defines a set of rules for managing network traffic and prevents unauthorized access to the network behind the firewall.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
firewall-policy <FIREWALL-POLICY-NAME>
```

**Parameters**

- `firewall-policy <FIREWALL-POLICY-NAME>`

| | |
|---|---|
| <FIREWALL-POLICY-NAME> | Specify the firewall policy name. If a firewall policy does not exist, it is created. |

**Example**

```
rfs6000-81742D(config)#firewall-policy test
rfs6000-81742D(config-fw-policy-test)#?
Firewall policy Mode commands:
  acl-logging                     Log on flow creating traffic
  alg                             Enable ALG
  clamp                           Clamp value
  dhcp-offer-convert              Enable conversion of broadcast dhcp offers to
                                  unicast
  dns-snoop                       DNS Snooping
  firewall                        Wireless firewall
  flow                            Firewall flow
  ip                              Internet Protocol (IP)
  ip-mac                          Action based on ip-mac table
  ipv6                            Internet Protocol version 6 (IPv6)
  ipv6-mac                        Action based on ipv6-mac table
  logging                         Firewall enhanced logging
  no                              Negate a command or set its defaults
  proxy-arp                       Enable generation of ARP responses on behalf
                                  of another device
  proxy-nd                        Enable generation of ND responses (for IPv6)
                                  on behalf of another device
  stateful-packet-inspection-l2   Enable stateful packet inspection in layer2
                                  firewall
  storm-control                   Storm-control
  virtual-defragmentation         Enable virtual defragmentation for IPv4
                                  packets (recommended for proper functioning
                                  of firewall)

  clrscr                          Clears the display screen
  commit                          Commit all changes made in this session
  do                              Run commands from Exec mode
  end                             End current mode and change to EXEC mode
  exit                            End current mode and down to previous mode
  help                            Description of the interactive help system
  revert                          Revert changes
  service                         Service Commands
  show                            Show running system information
  write                           Write running configuration to memory or
```

```
                                        terminal

rfs6000-81742D(config-fw-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing firewall policy |

**NOTE:** For more information on Firewall policy, see *Chapter 13, FIREWALL-POLICY*.

## 4.1.54 global-association-list

*Global Configuration Commands*

Configures a global list of client MAC addresses. Based on the deny or permit rules specified, clients are either allowed or denied access to the managed network.

The global association list serves the same purpose as an *Association Access Control List* (ACL). However, the Association ACL allows a limited number of entries, a few thousand only, and does not suffice the requirements of a large deployment. This gap is filled by a global association list, which is much larger (with tens of thousands of entries). Both lists co-exist in the system. When an access request comes in, the association ACL is looked up first and if the requesting MAC address is listed in one of the deny ACLs, the association is denied. But, if the requesting client is permitted access, or if in case none of the ACLs list the client's MAC address, the global association ACL is checked. Once authenticated, the client's credentials are cached on the access point, and subsequent requests are not referenced to the controller. An entry in an APs credential cache means a pass in the global association list.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
global-association-list <GLOBAL-ASSOC-LIST-NAME>
```

**Parameters**

- `global-association-list <GLOBAL-ASSOC-LIST-NAME>`

| | |
|---|---|
| <GLOBAL-ASSOC-LIST-NAME> | Specify the global association list name. If a list with the same name does not exist, it is created.<br>Map this global association list to a device (controller) or a controller profile. Once associated, the controller applies this association list to requests received from all adopted APs. For more information, see *use*.<br>The global association list can also be mapped to a WLAN. The usage of global access lists is controlled on a per-WLAN basis. For more information, see *association-list*. |

**Example**

```
rfs4000-229D58(config)#global-association-list my-clients
rfs4000-229D58(config-global-assoc-list-my-clients)#?
Global Association List Mode commands:
  default-action  Configure the default action when the client MAC does not
                  match any rule
  deny            Specify MAC addresses to be denied
  no              Negate a command or set its defaults
  permit          Specify MAC addresses to be permitted

  clrscr          Clears the display screen
  commit          Commit all changes made in this session
  do              Run commands from Exec mode
  end             End current mode and change to EXEC mode
  exit            End current mode and down to previous mode
  help            Description of the interactive help system
  revert          Revert changes
  service         Service Commands
```

```
  show              Show running system information
  write             Write running configuration to memory or terminal

rfs4000-229D58(config-global-assoc-list-my-clients)#
```

To enable global-association-list controlled client association, execute the following commands:

1 Create a global association list, and configure it as shown in the following examples:

```
rfs4000-229D58(config)#global-association-list vtt-list

rfs4000-880DA7(config-global-assoc-list-vtt-list)#permit 01-22-33-44-55-66
description sample
rfs4000-880DA7(config-global-assoc-list-vtt-list)#permit 40-B8-9A-39-F1-27
description acer
rfs4000-880DA7(config-global-assoc-list-vtt-list)#permit 42-B8-9A-39-F1-27
description ami
rfs4000-880DA7(config-global-assoc-list-vtt-list)#permit 6C-40-08-B2-80-6C
description mac
rfs4000-880DA7(config-global-assoc-list-vtt-list)#permit E0-98-61-34-11-47
description my_mobile

rfs4000-880DA7(config-global-assoc-list-vtt-list)#show context
global-association-list vtt-list
 default-action deny
 permit 01-22-33-44-55-66 description sample
 permit 40-B8-9A-39-F1-27 description acer
 permit 42-B8-9A-39-F1-27 description ami
 permit 6C-40-08-B2-80-6C description mac
 permit E0-98-61-34-11-47 description my_mobile
rfs4000-880DA7(config-global-assoc-list-vtt-list)#
```

2 Attach this global association list to the profile or device context of the access point *or* controller, as shown in the following examples:

3 On the access point's profile context:

```
Note: Ensure that the global association list is associated with the profile
being applied on the access point.

rfs4000-880DA7(config-profile-testAP6522)#use global-association-list server
vtt-list

rfs4000-880DA7(config-profile-testAP6522)#show context include-factory |
include g
lobal-association-list
 service global-association-list blacklist-interval 60
 use global-association-list server vtt-list
rfs4000-880DA7(config-profile-testAP6522)#
```

4 On the access point's device context:

```
ap6522(config-device-B4-C7-99-EA-DF-2C)#use global-association-list server
vtt-list
ap6522 (config-device-B4-C7-99-EA-DF-2C)#show context include-factory | in
clude global-association-list
 use global-association-list server vtt-list
ap6522(config-device-B4-C7-99-EA-DF-2C)#
```

5 On the controller's device context:

```
rfs4000-880DA7(config-device-00-23-68-88-0D-A7)#use global-association-list
server vtt-list

rfs4000-880DA7(config-device-00-23-68-88-0D-A7)#show context include-factory
| in
clude global-association-list
 use global-association-list server vtt-list
ap6522(config-device-B4-C7-99-EA-DF-2C)#
```

6 Attach this global association list with the WLAN, as shown in the following example:

```
rfs4000-880DA7(config-wlan-GLAssList)#association-list global vtt-list

rfs4000-880DA7(config-wlan-GLAssList)#show context include-factory | include
association-list
 association-list global vtt-list
rfs4000-880DA7(config-wlan-GLAssList)#
```

## 4.1.55 guest-management

*Global Configuration Commands*

The following table summarizes the guest management policy configuration mode commands:

**Table 4.35** *Guest-Management Policy Config Command*

| Command | Description | Reference |
|---|---|---|
| *guest-management* | Creates a guest management policy and enters its configuration mode | *page 4-286* |
| *guest-management-mode commands* | Summarizes guest management policy configuration mode commands | *page 4-287* |

### 4.1.55.1 guest-management

*guest-management*

Configures a guest management policy that redirects guest users to a registration portal upon association to a captive portal. Guest users are redirected to an internally (or) externally hosted registration page (registration.html) where previously, not-registered guest users can register. The internally hosted captive portal registration page can be customized based on business requirements.

Use the guest management policy commands to configure parameters, such as E-mail host and SMS gateway along with the credentials required for sending pass code to guest via e-mail and SMS. You can configure up to 32 different guest management policies. Each guest management policy allows you to configure the SMS gateway, SMS message body, E-mail SMTP server, E-mail subject contents, and E-mail message body. Although, at any point-in-time, multiple guest management policies may exist, only one guest management policy can be active per device.

Guest registration is supported only on the NX95XX and NX7500 series service platforms. However, the number of user identity entries supported on each varies. It is 2 million and 1 million user-identity entries for the NX95XX and NX75XX model service platforms respectively.

**Supported in the following platforms:**

- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
guest-management <POLICY-NAME>
```

**Parameters**

- `guest-management <POLICY-NAME>`

| | |
|---|---|
| <POLICY-NAME> | Specify the guest management policy name. If the policy does not exist, it is created. |

**Example**

```
nx9500-6C8809(config)#guest-management guest
nx9500-6C8809(config-guest-management-guest)#?
Guest Management Mode commands:
  email                   Email guest-notification configuration
  guest-database-backup   Configure guest-database-backup parameters
  guest-database-export   Configure guest-database-export parameters
  no                      Negate a command or set its defaults
  sms                     SMS guest-notification configuration
  sms-over-smtp           Sms-over-smtp configuration to email sms gateway
                          address

  clrscr                  Clears the display screen
  commit                  Commit all changes made in this session
  do                      Run commands from Exec mode
  end                     End current mode and change to EXEC mode
  exit                    End current mode and down to previous mode
  help                    Description of the interactive help system
  revert                  Revert changes
  service                 Service Commands
  show                    Show running system information
  write                   Write running configuration to memory or terminal

nx9500-6C8809(config-guest-management-guest)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing guest management policy |

### 4.1.55.2 guest-management-mode commands

*guest-management*

The following table summarizes guest management policy configuration mode commands:

**Table 4.36** *Guest-Management-Policy-Config-Mode Commands*

| Command | Description | Reference |
|---|---|---|
| *email* | Configures guest user e-mail notification settings | *page 4-288* |
| *guest-database-backup* | Enables periodic backup of the captive portal's guest registration user database | *page 4-290* |
| *guest-database-export* | Schedules an export of the Guest Management User database to a specified external server | *page 4-291* |
| *sms* | Configures guest user SMS notification settings | *page 4-292* |
| *sms-over-smtp* | Configures an e-mail host server along with sender credentials and the recipient's gateway e-mail address to which the message is e-mailed. The gateway server converts the e-mail into SMS and forwards the message to the guest users's mobile device. | *page 4-294* |
| *no* | Removes this guest management policy settings | *page 4-296* |

### 4.1.55.2.1 email

*guest-management-mode commands*

Configures guest user e-mail notification settings. When configured, guest users can register themselves with their e-mail credentials as a primary key for authentication. The captive portal system provides the pass code for their registration. Guest users need to use their registered e-mail, mobile, or member ID and the received pass code for subsequent logins to the captive portal.

This option is disabled by default.

**Supported in the following platforms:**

- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
email [host|message|subject]

email host [<IP/HOSTNAME>|<HOST-ALIAS-NAME>] sender <EMAIL-ADDRESS> security
[none|ssl|starttls] username <USER-NAME> password <PASSWORD>

email message <LINE>

email subject <LINE>
```

**Parameters**

```
• email host [<IP/HOSTNAME>|<HOST-ALIAS-NAME>] sender <EMAIL-ADDRESS> security
[none|ssl|starttls] username <USER-NAME> password <PASSWORD>
```

| | |
|---|---|
| email | Configures guest user e-mail notification settings |
| host [<IP/HOSTNAME>\| <HOST-ALIAS-NAME>] | Configures the SMTP server's IP address or hostname used for guest management e-mail traffic, guest user credential validation, and pass code reception. Optionally you can use an existing host alias to identify the SMTP server host.<br>• <IP/HOSTNAME> – Specify the SMTP server's IPv4 address or hostname.<br>• <HOST-ALIAS-NAME> – Specify the host alias name (should be existing and configured). Consider providing the host as an alias. A host alias is a configuration item that maps the alias to a hostname. Once created, it can be used across different configuration modes. Where ever used the alias is replaced by the associated hostname. |
| sender <EMAIL-ADDRESS> | Configures the sender's name for the guest user receiving the passcode required for registering their guest E-mail credentials using SMTP.<br>• <EMAIL-SENDER> – Specify the sender's name (should not exceed 100 characters). |
| security [none\|ssl\|starttls] | Configures the encryption protocol used by the SMTP server when communicating the pass code<br>• none – No encryption used. Use if no additional user authentication is needed beyond the required username and password combination.<br>• SSL – Uses SSL encryption. This is the default setting.<br>• STARTTLS – Uses STARTTLS encryption |
| username <USER-NAME> | Configures a username unique to this SMS guest management configuration. After configuring the username, specify the associated password. Ensure that the password is correctly provided to receive the pass code required for registering guest user credentials with SMS.<br>• <USER-NAME> – Specify the username (should not exceed 100 characters). |

| | |
|---|---|
| password <PASSWORD> | Configures the password associated with the specified SMTP user name<br>• <PASSWORD> – Specify the password (should not exceed 63 characters). |

- `email message <LINE>`

| | |
|---|---|
| email | Configures guest user e-mail notification content |
| message <LINE> | Configures the content of the e-mail sent to the guest user notifying the pass code (should not exceed 1024 characters)<br>• <LINE> – Specify the message content. When entering the message, use the following tags:<br>GM-NAME – for the guest user's name<br>GM_PASSCODE – for the pass code<br>CR-NL – to enter a new line<br>For example: Dear *GM_NAME*, *CR-NL* your internet access pass code is *GM_PASSCODE*. *CR-NL* Use this for internet access. |

- `email subject <LINE>`

| | |
|---|---|
| email | Configures guest user e-mail notification subject line |
| subject <LINE> | Configures the subject line of the e-mail sent to the guest user notifying the pass code (should not exceed 100 characters)<br>• <LINE> – Specify the subject line content. When entering the subject line, use the following tag:<br>GM-NAME – for the guest user's name<br>For example: *GM_NAME*, your internet access code |

**Example**

```
nx9500-6C8809(config-guest-management-test)#email host 192.168.13.10 sender
bob@extremenetworks.com security ssl username guest1 password guest1@123

nx9500-6C8809(config-guest-management-test)#show context
guest-management test
 email host 192.168.13.10 sender bob@extremenetworks.com security ssl username
guest1 password guest1@123
nx9500-6C8809(config-guest-management-test)#

nx9500-6C8809(config-guest-management-test2)#email message Dear GM_Guest2, CR-NL
Your internet access passcode is GM_Guest2. CR-NL Use this for internet access.

nx9500-6C8809(config-guest-management-test2)#email subject GM_Guest2 Your
internet access code

nx9500-6C8809(config-guest-management-test2)#show context
guest-management test2
 email subject GM_Guest2 Your internet access code
 email message Dear GM_Guest2,  CR-NL  Your internet access passcode is GM_Guest2.
CR-NL  Use this for internet access.
nx9500-6C8809(config-guest-management-test2)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the e-mail settings used to send notification mails to the guest user |

### 4.1.55.2.2 guest-database-backup

*guest-management-mode commands*

Enables periodic backup of a captive portal's guest registration user database. This option is enabled by default.

**Supported in the following platforms:**

- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
guest-database-backup enable {<TIME>}
```

**Parameters**

- `guest-database-backup enable {<TIME>}`

| | |
|---|---|
| guest-database-backup enable <TIME> | Enables periodic backup of a captive portal's guest registration user database. This command also allows you to configure the time at which the system starts backing up the database. The default backup-start time is '00:00' (midnight every day).<br>• <TIME> – Optional. Resets the periodic database backup-start time to a user-defined value in the HH;MM format. When specified, the system starts periodic backup of the database, every day, at the specified time. |

**Example**

```
nx9500-6C8809(config-guest-management-test)#guest-database-backup enable 12:30

vnx9500-6C8809(config-guest-management-test)#show context
guest-management test
 guest-database-backup enable 12:30
nx9500-6C8809(config-guest-management-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables periodic backup of a captive portal's guest registration user database |

### 4.1.55.2.3 guest-database-export

*guest-management-mode commands*

Schedules an export of the Guest Management user database to a specified external server. This option is enabled by default.

**Supported in the following platforms:**

- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
guest-database-export <TIME> frequency <1-168> url-directory <URL> {(format
[csv|json]|last-visit-within <1-168>)}
```

**Parameters**

```
• guest-database-export <TIME> frequency <1-168> url-directory <URL> {(format
[csv|json]|last-visit-within <1-168>)}
```

| | |
|---|---|
| guest-database-export <TIME> | Schedules an export of the Guest Management User collection to an external server<br>• <TIME> – Configures the start time of the export operation in the HH:MM format |
| frequency <1-168> | Configures the user collection export frequency in hours<br>• <1-168> – Configures the frequency from 1 - 168 hours. If the frequency is set at 3 hours, the user database is exported once in every 3 hours. The default is 4 hours. |
| url-directory <URL> | Configures external server's URL and directory to where the collection is exported<br>• <URL> – Specify the external server's URL |
| format [csv\|json] | Optional. Configures the file format<br>• csv – Exports collection to the specified location in CSV format. This is the default setting.<br>• json – Exports collection to the specified location in JSON format |
| last-visit-within <1-168> | Configures a filters guest users who have last visited within a specified period of time<br>• <1-168> – Specify a time period from 1 - 168 hours. If for example, the last-visit-within value is set at 2 hours, then only the last two hours guest user collections will be exported. The default is 4 hours. |

**Example**

```
nx9500-6C8809(config-guest-management-gm1)#guest-database-export 10:30 frequency
 6 url-directory ftp://admin:xxxxxx@192.168.13.10/dbe_dir format json last-visit
-within 168

nx9500-6C8809(config-guest-management-test)#show context
guest-management test
 guest-database-export 12:30 frequency 20 url-directory ftp://
admin:xxxxxx@192.168.13.10/dbe_dir format json last-visit-within 168
nx9500-6C8809(config-guest-management-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Reverts the guest database export parameters to default |

### 4.1.55.2.4 sms

*guest-management-mode commands*

Configures guest user SMS notification settings

When configured, guest users can register themselves with their e-mail or mobile device ID as the primary key for authentication. The captive portal provides the pass code for registration. Guest users use their registered e-mail or mobile device ID and the received pass code for subsequent logins to the captive portal.

**NOTE:** When using SMS, ensure that the WLAN's mode of authentication is set to *none* and the mode of registration is set to *user*. In other words, captive portal authentication must always enforce guest registration.

SMS is similar to MAC address-based self registration, but in addition the captive portal sends an SMS message, containing an access code, to the user's mobile phone number provided at the time of registration. The captive portal verifies the code, returns the *Welcome* page and provides access. This allows the administrator to verify the phone number provided and can be traced back to a specific individual should the need arise.

The default gateway used with SMS is *Clickatell.* A pass code can be sent with SMS to the guest user directly using Clickatell, or the pass code can be sent via e-mail to the SMS Clickatell gateway server, and Clickatell sends the pass code SMS to the guest user.

**Supported in the following platforms:**

- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
sms [host|message]

sms host clickatell username <USER-NAME> password <PASSWORD> api-id <ID> user-agent
<PYCLICKATELL> {source-number <WORD>}

sms message <LINE>
```

**Parameters**

```
• sms host clickatell username <USER-NAME> password <PASSWORD> api-id <ID> user-
agent <PYCLICKATELL> {source-number <WORD>}
```

| | |
|---|---|
| sms | Configures guest user SMS notification settings |
| host clickatell | By default, *clickatell* is the host SMS gateway server resource. Upon receiving the pass code e-mail, the SMS gateway sends the actual notification pass code SMS to the guest user. |
| username <USER-NAME> | Configures a username unique to this SMS guest management configuration. After configuring the username, specify the associated password. Ensure that the password is correctly provided to receive the pass code required for registering guest user credentials with SMS.<br>• <USER-NAME> – Specify the username (should not exceed 32 characters). |
| password <PASSWORD> | Configures the password associated with the specified username<br>• <PASSWORD> – Specify the password (should not exceed 63 characters). |
| api-id <ID> | Set a 32 character maximum API ID<br>• <API-ID> – Specify the API ID (should not exceed 32 characters). |

| | |
|---|---|
| user-agent <PYCLICKATELL> | Since the SMS service provider by default is Clickatell, set the user agent name to *pyclickatell*. The user-agent value ensures the Clickatell SMS gateway server and its related credentials, needed for sending the pass code to guest users, are configured. |
| source-number <WORD> | Optional. Configures the long-address or the from-number associated with this Clickatell user account<br>• <WORD> – Specify the source number (should not exceed 32 characters). |

- `sms message <LINE>`

| | |
|---|---|
| SMS | Configures guest user SMS notification content |
| message <LINE> | Configures the content of the SMS sent to the guest user notifying the pass code (should not exceed 1024 characters)<br>• <LINE> – Specify the message content. When entering the message, use the following tags:<br>GM-NAME – for the guest user's name<br>GM_PASSCODE – for the pass code<br>For example: Dear *GM_NAME*, your internet access pass code is *GM_PASSCODE*. |

**Example**

```
nx9500-6C8809(config-guest-management-test)#sms host clickatell username guest1
password guest1@123 api-id test user-agent pyclickatell

nx9500-6C8809(config-guest-management-test)#sms message Dear guest1, Your passcode
for internet access is GM-guest1

nx9500-6C8809(config-guest-management-test)#show context
guest-management test
 email host 192.168.13.10 sender bob@extremenetworks.com security ssl username
guest1 password guest1@123
 sms host clickatell username guest1 password guest1@123 api-id test user-agent
pyclickatell
 sms message Dear guest1, Your passcode for internet access is GM-guest1
nx9500-6C8809(config-guest-management-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the SMS settings used to send SMS to the guest user |

### 4.1.55.2.5 sms-over-smtp

*guest-management-mode commands*

Configures an e-mail host server (for example: smtp.gmail.com) along with sender related credentials and the recipient gateway e-mail address to which the message is E-mailed. The gateway server converts the e-mail into SMS and sends the message to the guest users's mobile device.

When sending an e-mail, the e-mail client interacts with a SMTP server to handle the content transmission. The SMTP server on the host may have conversations with other SMTP servers to deliver the e-mail.

**Supported in the following platforms:**

- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
sms-over-smtp [host|message|subject]

sms-over-smtp host [<IP/HOSTNAME>|<HOST-ALIAS-NAME>] sender <EMAIL-ADDRESS>
security [none|ssl|starttls] username <USER-NAME> password <PASSWORD> recipient
<EMAIL-ADDRESS>

sms-over-smtp message <LINE>

sms-over-smtp subject <LINE>
```

**Parameters**

```
• sms-over-smtp host [<IP/HOSTNAME>|<HOST-ALIAS-NAME>] sender <EMAIL-ADDRESS>
security [none|ssl|starttls] username <USER-NAME> password <PASSWORD> recipient
<EMAIL-ADDRESS>
```

| | |
|---|---|
| sms-over-smtp | Configures guest user SMS over SMTP notification settings |
| host [<IP/HOSTNAME>\| <HOST-ALIAS-NAME>] | Configures the SMS gateway server resource's IPv4 address or hostname used for guest management SMS over SMTP traffic, guest user credential validation and pass code reception. Optionally you can use an existing host alias to identify the SMS gateway server resource.<br>• <IP/HOSTNAME> – Specify the SMTP gateway server resource's IP address or hostname.<br>• <HOST-ALIAS-NAME> – Specify the host alias name (should existing and configured). Consider providing the host as an alias. A host alias is a configuration item that maps the alias to a hostname. Once created, it can be used across different configuration modes. Where ever used the alias is replaced by the associated hostname. |
| sender <EMAIL-ADDRESS> | Configures the sender's e-mail address. The sender here is the guest user receiving the pass code. Guest users require this pass code for registering their guest e-mail credentials using SMTP.<br>• <EMAIL-ADDRESS> – Specify the e-mail address (should not exceed 64 characters). |
| security [none\|ssl\|starttls] | Configures the encryption protocol used by the SMTP server when communicating the pass code<br>• none – No encryption used. Use if no additional user authentication is needed beyond the required username and password combination.<br>• SSL – Uses SSL encryption. This is the default setting.<br>• STARTTLS – Uses STARTTLS encryption |

| | |
|---|---|
| username <USER-NAME> | Configures a username unique to this SMTP guest management configuration. After configuring the username, specify the associated password. Ensure that the correct password is provided to receive the pass code required for registering guest user credentials with SMTP.<br>• <USER-NAME> – Specify the username (should not exceed 64 characters). |
| password <PASSWORD> | Configures the password associated with the specified SMTP user name<br>• <PASSWORD> – Specify the password (should not exceed 64 characters). |
| recipient <EMAIL-ADDRESS> | Configures the e-mail recipient's e-mail address<br>• <EMAIL-ADDRESS> – Specify the recipient's e-mail address (should not exceed 64 characters in length. |

- `sms-over-smtp message <LINE>`

| | |
|---|---|
| `sms-over-smtp` | Configures guest user SMS over SMTP notification message content |
| message <LINE> | Configures the content of the SMS over SMTP sent to the guest user notifying the pass code (should not exceed 1024 characters)<br>• <LINE> – Specify the message content. When entering the message, use the following tags:<br>GM-NAME – for the guest user's name<br>GM_PASSCODE – for the pass code<br>CR-NL – to enter a new line<br>For example: Dear *GM_NAME*, *CR-NL* your internet access pass code is *GM_PASSCODE*. *CR-NL* Use this access code for internet access. |

- `sms-over-smtp subject <LINE>`

| | |
|---|---|
| `sms-over-smtp` | Configures guest user e-mail notification subject line content |
| subject <LINE> | Configures the subject line of the SMS over SMTP sent to the guest user notifying the pass code (should not exceed 100 characters)<br>• <LINE> – Specify the subject line content. When entering the subject line, use the following tag:<br>GM-NAME – for the guest user's name<br>For example: *GM_NAME*, your internet access code |

**Example**

```
nx9500-6C8809(config-guest-management-test3)#sms-over-smtp host test sender
bob@extremenetworks.com security ssl username bob password bob@123 recipient
john@extremenetworks.com

nx9500-6C8809(config-guest-management-test3)#show context
guest-management test3
 sms-over-smtp host test sender bob@extremenetworks.com security ssl username bob
password bob@123 recipient john@extremenetworks.com
nx9500-6C8809(config-guest-management-test3)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the SMS over SMTP settings used to send SMS to the guest user |

### 4.1.55.2.6 no

*guest-management-mode commands*

Removes this guest management policy settings

**Supported in the following platforms:**

- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
no [email|guest-database-backup|guest-database-export|sms|sms-over-smtp]

no email [host|message|subject]

no guest-database-backup enable

no guest-database-export

no gmd report-generation enable

no sms [host|message]

no sms-over-smtp [host|message|subject]
```

**Parameters**

- no <PARAMETERS>

| | |
|---|---|
| no <PARAMETERS> | Removes this guest management policy settings based on the parameters passed |

**Example**

```
nx9500-6C8809(config-guest-management-test3)#show context
guest-management test3
 sms-over-smtp host test sender bob@extremenetworks.com security ssl username bob
password bob@123 recipient john@extremenetworks.com
nx9500-6C8809(config-guest-management-test3)#

nx9500-6C8809(config-guest-management-test)#no sms-over-smtp host

nx9500-6C8809(config-guest-management-test3)#show context
guest-management test3
nx9500-6C8809(config-guest-management-test3)#
```

## 4.1.56 host

*Global Configuration Commands*

Enters the configuration context of a remote device using its hostname

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
host <DEVICE-NAME>
```

**Parameters**

- `host <DEVICE-NAME>`

| | |
|---|---|
| <DEVICE-NAME> | Specify the device's hostname. All discovered devices are displayed when 'Tab' is pressed to auto complete this command. |

**Example**

```
rfs4000-229D58(config)#host rfs4000-229D58
rfs4000-229D58(config-device-00-23-68-22-9D-58)#
```

## 4.1.57 inline-password-encryption

*Global Configuration Commands*

Stores the encryption key in the startup configuration file

By default, the encryption key is not stored in the startup-config file. Use the inline-password-encryption command to move the encrypted key to the startup-config file. This command uses the master key to encrypt the password, then moves it to the startup-config file.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
inline-password-encryption
```

**Parameters**

None

**Usage Guidelines**

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

**Example**

The following command uses the specified password for encryption key and stores it outside of startup-config:

```
rfs6000-81742D(config)#password-encryption secret 2 12345678

rfs6000-81742D(config)#commit write memory
```

The following command moves the same password to the startup-config and encrypts it with the master key:

```
rfs6000-81742D(config)#inline-password-encryption
```

**Related Commands**

| | |
|---|---|
| *no* | Disables storing of the encryption key in the startup configuration file |
| *password-encryption* | Enables password encryption |

## 4.1.58 ip

*Global Configuration Commands*

Creates a IP *access control list* (ACL) and/or a SNMP IP ACL

Access lists define access permissions to the network using a set of rules. Each rule specifies an action taken when a packet matches the rule. If the action is deny, the packet is dropped. If the action is permit, the packet is allowed.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ip [access-list|snmp-access-list]

ip access-list <IP-ACL-NAME>
ip snmp-access-list <IP-SNMP-ACL-NAME>
```

**Parameters**

- `ip access-list <IP-ACL-NAME>`

| | |
|---|---|
| access-list <IP-ACL-NAME> | Creates an IP ACL and enters its configuration mode<br>• <IP-ACL-NAME> – Specify the ACL name. If the access list does not exist, it is created. |

- `ip snmp-access-list <IP-SNMP-ACL-NAME>`

| | |
|---|---|
| snmp-access-list <IP-SNMP-ACL-NAME> | Creates a SNMP IP ACL and enters its configuration mode. An SNMP IP ACL is an access control mechanism that uses a combination of IP ACL and SNMP community string.<br>SNMP performs network management functions using a data structure called a *Management Information Base* (MIB). SNMP is widely implemented but not very secure, since it uses only text community strings for accessing controller or service platform configuration files.<br>Use SNMP ACLs (firewalls) to help reduce SNMP's vulnerabilities, as SNMP traffic can be easily exploited to produce a *denial of service* (DoS).<br>• <IP-SNMP-ACL-NAME> – Specify the SNMP IP ACL name. If the access list does not exist, it is created. After creating the SNMP ACL, define the deny/permit rules based on the network and/or host IP addresses. Once created and configured, link this SNMP IP ACL with a SNMP community string.<br>To link the SNMP community string with the SNMP IP ACL, in the management-policy-config-mode, use the following command: *snmp-server > community <COMMUNITY-STRING> > [ro/rw] > ip-snmp-access-list <IP-SNMP-ACL-NAME>.* |

**Example**

```
rfs6000-81742D(config)#ip access-list test
rfs6000-81742D(config-ip-acl-test)#?
ACL Configuration commands:
  deny      Specify packets to reject
  disable   Disable rule if not needed
  no        Negate a command or set its defaults
  permit    Specify packets to forward

  clrscr    Clears the display screen
  commit    Commit all changes made in this session
  end       End current mode and change to EXEC mode
  exit      End current mode and down to previous mode
  help      Description of the interactive help system
  revert    Revert changes
  service   Service Commands
  show      Show running system information
  write     Write running configuration to memory or terminal

rfs6000-81742D(config-ip-acl-test)#

rfs6000-81742D(config)#ip snmp-access-list SNMPAcl
rfs6000-81742D(config-ip-snmp-acl-SNMPAcl)#?
SNMP ACL Configuration commands:
  deny      Specify packets to reject
  no        Negate a command or set its defaults
  permit    Specify packets to forward

  clrscr    Clears the display screen
  commit    Commit all changes made in this session
  do        Run commands from Exec mode
  end       End current mode and change to EXEC mode
  exit      End current mode and down to previous mode
  help      Description of the interactive help system
  revert    Revert changes
  service   Service Commands
  show      Show running system information
  write     Write running configuration to memory or terminal

rfs6000-81742D(config-ip-snmp-acl-SNMPAcl)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an IP access control list |

**NOTE:** For more information on access control lists, see *Chapter 11, ACCESS-LIST*.

## 4.1.59 ipv6

*Global Configuration Commands*

Creates a IPv6 ACL

An IPv6 ACL defines a set of rules that filter IPv6 packets flowing through a port or interface. Each rule specifies the action taken when a packet matches the rule. If the action is deny, the packet is dropped. If the action is permit, the packet is allowed.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ipv6 access-list <IPv6-ACL-NAME>
```

**Parameters**

- `ipv6 access-list <IPv6-ACL-NAME>`

| | |
|---|---|
| access-list <IPv6-ACL-NAME> | Configures an IPv6 access list and enters its configuration mode<br>• <IPv6-ACL-NAME> – Specify the IPv6 ACL name. If the access list does not exist, it is created. |

**Example**

```
rfs4000-229D58(config)#ipv6 access-list IPv6ACLTest
rfs4000-229D58(config-ipv6-acl-IPv6ACLTest)#?
IPv6 Access Control Mode commands:
  deny      Specify packets to reject
  no        Negate a command or set its defaults
  permit    Specify packets to forward

  clrscr    Clears the display screen
  commit    Commit all changes made in this session
  do        Run commands from Exec mode
  end       End current mode and change to EXEC mode
  exit      End current mode and down to previous mode
  help      Description of the interactive help system
  revert    Revert changes
  service   Service Commands
  show      Show running system information
  write     Write running configuration to memory or terminal

rfs4000-229D58(config-ipv6-acl-IPv6ACLTest)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an IPv6 access control list |

**NOTE:** For more information on access control lists, see *Chapter 11, ACCESS-LIST*.

## 4.1.60 ipv6-router-advertisement-policy

*Global Configuration Commands*

The following table lists the IPv6 *router advertisement* (RA) policy configuration commands:

**Table 4.37** *IPv6-Router-Advertisement-Policy-Config Commands*

| Command | Description | Reference |
|---|---|---|
| *ipv6-router-advertisement-policy* | Creates a new IPv6 RA policy and enters its configuration mode | *page 4-303* |
| *ipv6-router-advertisement-policy-mode commands* | Summarizes the IPv6 RA policy configuration mode commands | *page 4-305* |

### 4.1.60.1 ipv6-router-advertisement-policy

*ipv6-router-advertisement-policy*

Creates an IPv6 RA policy and enters its configuration mode

An IPv6 router policy allows routers to advertise their presence in response to solicitation messages. After receiving a neighbor solicitation message, the destination node sends an advertisement message. which includes the link layer address of the source node. After receiving the advertisement, the destination device replies with a neighbor advertisement message on the local link. After the source receives the advertisement it can communicate with other devices.

Advertisement messages are also sent to indicate a change in link layer address for a node on the local link. With such a change, the multicast address becomes the destination address for advertisement messages.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ipv6-router-advertisement-policy <POLICY-NAME>
```

**Parameters**

- `ipv6-router-advertisement-policy <POLICY-NAME>`

| | |
|---|---|
| ipv6-router-advertisement-policy <POLICY-NAME> | Specify an IPv6 RA policy name. If the policy does not exist, it is created. |

**Example**

```
rfs4000-229D58(config)#ipv6-router-advertisement-policy test
rfs4000-229D58(config-ipv6-radv-policy-test)#?
IPv6 Router Advertisement Policy Mode commands:
  advertise                       Option to advertise in router advertisement
  assist-neighbor-discovery       Send the Source Link Layer address option
                                  in Router Advertisement to assist in
                                  neighbor discovery
  check-ra-consistency            Check if the parameters advertised by other
                                  routers on the link are in conflict with
                                  those configured on this router. Conflicts
                                  are logged.
  dns-server                      DNS Server
  domain-name                     Configure domain-name
  managed-config-flag             Set the managed-address-configuration flag
                                  in Router Advertisements. When set, it
                                  indicates that the addresses are available
                                  via DHCPv6
  nd-reachable-time               Time that a node assumes a neighbor is
                                  reachable after having received a
                                  reachability confirmation
  no                              Negate a command or set its defaults
  ns-interval                     Time between retransmitted Neighbor
                                  Solicitation messages
  other-config-flag               Set the other-configuration flag in Router
                                  Advertisements. When set, it indicates that
                                  other configuration information is
```

```
                                    available via DHCPv6.
ra                                  Router Advertisements
router-lifetime                     Lifetime associated with the default router
router-preference                   Preference of this router over other
                                    routers
unicast-solicited-advertisement     Unicast the solicited Router Advertisements

clrscr                              Clears the display screen
commit                              Commit all changes made in this session
do                                  Run commands from Exec mode
end                                 End current mode and change to EXEC mode
exit                                End current mode and down to previous mode
help                                Description of the interactive help system
revert                              Revert changes
service                             Service Commands
show                                Show running system information
write                               Write running configuration to memory or
                                    terminal

rfs4000-229D58(config-ipv6-radv-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the specified IPv6 RA policy |

### 4.1.60.2 ipv6-router-advertisement-policy-mode commands

*ipv6-router-advertisement-policy*

The following table summarizes IPv6 router advertisement policy configuration commands:

**Table 4.38** *IPv6-Router-Advertisement-Policy-Config-Mode Commands*

| Command | Description | Reference |
|---|---|---|
| *advertise* | Enables advertisement of IPv6 *maximum transmission unit* (MTU) and hop-count value in RAs | *page 4-306* |
| *assist-neighbor-discovery* | Enables advertisement of the source link layer address in RAs | *page 4-307* |
| *check-ra-consistency* | Enables checking of consistency in RA values advertised by this router with those advertised by other routers, if any, on the same link | *page 4-308* |
| *dns-server* | Configures the DNS server's IPv6 address and lifetime advertised in RAs | *page 4-309* |
| *domain-name* | Configures the Domain name search label advertised in RAs | *page 4-310* |
| *managed-config-flag* | Sets the managed address configuration flag in RAs | *page 4-311* |
| *nd-reachable-time* | Enables advertisement of neighbor reachable time in RAs | *page 4-312* |
| *no* | Removes or reverts router advertisement policy settings | *page 4-313* |
| *ns-interval* | Configures the interval between two successive retransmitted *neighbor solicitation* (NS) messages | *page 4-314* |
| *other-config-flag* | Sets the other-configuration flag in RAs | *page 4-315* |
| *ra* | Configures RA related parameters, such as the interval between two unsolicited successive RAs | *page 4-316* |
| *router-lifetime* | Configures the default router's lifetime, in seconds, advertised in RAs | *page 4-317* |
| *router-preference* | Configures the router preference field value advertised in RAs | *page 4-318* |
| *unicast-solicited-advertisement* | Enables unicasting of solicited RAs | *page 4-319* |

### 4.1.60.2.1 advertise

*ipv6-router-advertisement-policy-mode commands*

Enables advertisement of IPv6 MTU and hop-count value in RAs

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
advertise [hop-limit|mtu]
```

**Parameters**

- `advertise [hop-limit|mtu]`

| | |
|---|---|
| advertise [hop-limit\|mtu] | Enables advertisement of IPv6 MTU and hop-count value in RAs. Both these features are disabled by default. |

**Example**

```
rfs6000-81742D(config-ipv6-radv-policy-test)#advertise hop-limit

rfs6000-81742D(config-ipv6-radv-policy-test)#advertise mtu

rfs6000-81742D(config-ipv6-radv-policy-test)#show context
ipv6-router-advertisement-policy test
 advertise mtu
 advertise hop-limit
rfs6000-81742D(config-ipv6-radv-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables advertisement of IPv6 MTU and hop-count value in RAs |

#### 4.1.60.2.2 assist-neighbor-discovery

*ipv6-router-advertisement-policy-mode commands*

Enables advertisement of the source link layer address in RAs to facilitate neighbor discovery. This feature is enabled by default.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
assist-neighbor-discovery
```

**Parameters**

None

**Example**

```
rfs6000-81742D(config-ipv6-radv-policy-test)#assist-neighbor-discovery
```

**Related Commands**

| | |
|---|---|
| *no* | Disables the advertisement of the source link layer address in RAs |

### 4.1.60.2.3 check-ra-consistency

*ipv6-router-advertisement-policy-mode commands*

Enables checking of consistency in RA values advertised by this router with those advertised by other routers, if any, on the same link. If the values advertised are inconsistent, a conflict is logged.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
check-ra-consistency
```

**Parameters**

None

**Example**

```
rfs6000-81742D(config-ipv6-radv-policy-test)#check-ra-consistency

rfs6000-81742D(config-ipv6-radv-policy-test)#show context
ipv6-router-advertisement-policy test
 advertise mtu
 advertise hop-limit
 check-ra-consistency
rfs6000-81742D(config-ipv6-radv-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables comparison of interface-specific parameters advertised by other routers, within the link, with those advertised with this router |

### 4.1.60.2.4 dns-server

*ipv6-router-advertisement-policy-mode commands*

Configures the DNS server's IPv6 address and lifetime. The configured values are advertised in RAs.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
dns-server <IPv6> {lifetime [<4-3600>|expired|infinite]}
```

**Parameters**

- `dns-server <IPv6> {lifetime [<4-3600>|expired|infinite]}`

| | |
|---|---|
| dns-server <IPv6> | Configures the DNS server's IPv6 address<br>Enables the use of a DNS server to resolve host names to IPv6 addresses. When an IPv6 host is configured with the address of a DNS server, the host sends DNS name queries to the server for resolution.<br>• <IPv6> – Specify the DNS server's address. This address is advertised in RAs. A maximum of four (4) entries can be made per policy. |
| lifetime [<4-3600>\|expired\|infinite] | Optional. Configures the DNS server's (identified by the <IPv6> parameter) lifetime<br>• <4-3600> – Configures a lifetime in seconds. Specify a value form 4 - 3600 seconds. The default is 600 seconds.<br>• expired – Advertises that this DNS server's lifetime has expired and should not be used<br>• infinite – Advertises that this DNS server's lifetime is infinite |

**Example**

```
rfs6000-81742D(config-ipv6-radv-policy-test)#dns-server 2002::2 lifetime 3000

rfs6000-81742D(config-ipv6-radv-policy-test)#show context
ipv6-router-advertisement-policy test
 advertise mtu
 advertise hop-limit
 check-ra-consistency
 dns-server 2002::2 lifetime 3000
rfs6000-81742D(config-ipv6-radv-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the DNS server settings advertised in RAs. Once removed these values are not advertised in RAs. |

### 4.1.60.2.5 domain-name

*ipv6-router-advertisement-policy-mode commands*

Configures the Domain name search label advertised in RAs

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
domain-name <WORD> {lifetime [<4-3600>|expired|infinite]}
```

**Parameters**

- `domain-name <WORD> {lifetime [<4-3600>|expired|infinite]}`

| | |
|---|---|
| domain-name <WORD> | Configures the Domain name search label advertised in RAs<br>Enter a *fully qualified domain name* (FQDN), which is an unambiguous domain name available in a router advertisement resource. To distinguish an FQDN from a regular domain name, a trailing period is added. For example, somehost.example.com.<br>• <WORD> – Specify the Domain name search label. A maximum of four (4) entries can be made per policy. |
| lifetime [<4-3600>\| expired\|infinite] | Optional. Configures the Domain name search label's lifetime<br>• <4-3600> – Configures a lifetime in seconds. Specify a value form 4 - 3600 seconds. The default is 600 seconds.<br>• expired – Advertises that this Domain name search label's lifetime has expired and should not be used<br>• infinite – Advertises that this Domain name search label's lifetime is infinite |

**Example**

```
rfs6000-81742D(config-ipv6-radv-policy-test)#domain-name TechPubs lifetime
infinite

rfs6000-81742D(config-ipv6-radv-policy-test)#show context
ipv6-router-advertisement-policy test
 advertise mtu
 advertise hop-limit
 check-ra-consistency
 dns-server 2002::2 lifetime 3000
 domain-name TechPubs lifetime infinite
rfs6000-81742D(config-ipv6-radv-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the Domain name settings advertised in RAs. Once removed these values are not advertised in RAs. |

### 4.1.60.2.6 managed-config-flag

*ipv6-router-advertisement-policy-mode commands*

Sets the managed address configuration flag in RAs. When set, it indicates that IPv6 addresses are available through DHCPv6. This feature is disabled by default.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
managed-config-flag
```

**Parameters**

None

**Example**

```
rfs6000-81742D(config-ipv6-radv-policy-test)#managed-config-flag

rfs6000-81742D(config-ipv6-radv-policy-test)#show context
ipv6-router-advertisement-policy test
 managed-config-flag
 advertise mtu
 advertise hop-limit
 check-ra-consistency
 dns-server 2002::2 lifetime 3000
 domain-name TechPubs lifetime infinite
rfs6000-81742D(config-ipv6-radv-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the managed address configuration flag advertised in RAs |

### 4.1.60.2.7 nd-reachable-time

*ipv6-router-advertisement-policy-mode commands*

Enables advertisement of neighbor discovery reachable time in RAs. This feature is disabled by default.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
nd-reachable-time [<5000-3600000>|global]
```

**Parameters**

- `nd-reachable-time [<5000-3600000>|global]`

| | |
|---|---|
| nd-reachable-time [<5000-3600000>\| global] | Configures the interval, in milliseconds, that a node assumes a neighbor is reachable after receiving a reachability confirmation from the neighbor. Therefore, a neighbor is reachable, after being discovered, for a period specified here. This value is advertised in RAs. Use one of the following options:<br>• <5000-3600000> – Configures an interface-specific value. Specify a value from 5000 - 3600000 milliseconds. The default is 5000 milliseconds.<br>• global – Advertises the neighbor reachable time configured for the system. This is the value configured at the device configuration mode. For more information, see *use*. |

**Example**

```
rfs6000-81742D(config-ipv6-radv-policy-test)#nd-reachable-time 6000

rfs6000-81742D(config-ipv6-radv-policy-test)#show context
ipv6-router-advertisement-policy test
 managed-config-flag
 nd-reachable-time 6000
 advertise mtu
 advertise hop-limit
 check-ra-consistency
 dns-server 2002::2 lifetime 3000
 domain-name TechPubs lifetime infinite
rfs6000-81742D(config-ipv6-radv-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables advertisement of neighbor reachable time in RAs |

### 4.1.60.2.8 no

*ipv6-router-advertisement-policy-mode commands*

Removes or reverts router advertisement policy settings. Use the no command to remove or revert the interface-specific parameters that are advertised by link router.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
no [advertise [hop-limit|mtu]|assist-neighbor-discovery|check-ra-consistency|
dns-server <IPv6>|domain-name <WORD>|managed-config-flag|nd-reachable-time|
ns-interval|other-config-flag|ra [interval|suppress]|router-lifetime|
unicast-solicited-advertisement]
```

**Parameters**

- no <PARAMETERS>

| | |
|---|---|
| no <PARAMETERS> | Removes or reverts this IPv6 router advertisement policy's settings based on the parameters passed |

**Example**

```
rfs6000-81742D(config-ipv6-radv-policy-test)#show context
ipv6-router-advertisement-policy test
 managed-config-flag
 nd-reachable-time global
 advertise mtu
 advertise hop-limit
 check-ra-consistency
 dns-server 2002::2 lifetime 3000
 domain-name TechPubs lifetime infinite
rfs6000-81742D(config-ipv6-radv-policy-test)#

rfs6000-81742D(config-ipv6-radv-policy-test)#no managed-config-flag

rfs6000-81742D(config-ipv6-radv-policy-test)#no nd-reachable-time

rfs6000-81742D(config-ipv6-radv-policy-test)#no check-ra-consistency

rfs6000-81742D(config-ipv6-radv-policy-test)#show context
ipv6-router-advertisement-policy test
 advertise mtu
 advertise hop-limit
 dns-server 2002::2 lifetime 3000
 domain-name TechPubs lifetime infinite
rfs6000-81742D(config-ipv6-radv-policy-test)#
```

### 4.1.60.2.9 ns-interval

*ipv6-router-advertisement-policy-mode commands*

Configures the *neighbor solicitation* (NS) retransmit timer value advertised in RAs. This is the interval between two successive NS messages. When specified, it enables the sending of the specified value in RAs. This feature is disabled by default.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ns-interval [<1000-3600000>|global]
```

**Parameters**

- `ns-interval [<1000-3600000>|global]`

| | |
|---|---|
| ns-interval [<1000-3600000>\| global] | Configures the NS interval advertised in RAs. Use one of the following options:<br>• <1000-3600000> – Specify a value from 1000 - 3600000 milliseconds. The default is 1000 milliseconds.<br>• global – Advertises the NS interval configured for the system. This is configured on the device in the device configuration mode. For more information, see *ipv6*. |

**Example**

```
rfs6000-81742D(config-ipv6-radv-policy-test)#ns-interval 3000

rfs6000-81742D(config-ipv6-radv-policy-test)#show context
ipv6-router-advertisement-policy test
 managed-config-flag
 nd-reachable-time global
 ns-interval 3000
 advertise mtu
 advertise hop-limit
 check-ra-consistency
 dns-server 2002::2 lifetime 3000
 domain-name TechPubs lifetime infinite
rfs6000-81742D(config-ipv6-radv-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables advertisement of NS interval in RAs |

### 4.1.60.2.10 other-config-flag

*ipv6-router-advertisement-policy-mode commands*

Sets the other-configuration flag in RAs. When set, it indicates that other configuration details, such as DNS-related information, are available through DHCPv6. This feature is enabled by default.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
other-config-flag
```

**Parameters**

None

**Example**

```
rfs6000-81742D(config-ipv6-radv-policy-test)#other-config-flag
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the other-config-flag advertised on RAs |

### 4.1.60.2.11 ra

*ipv6-router-advertisement-policy-mode commands*

Configures RA related parameters, such as the interval between two unsolicited successive RAs. It also allows suppression of RAs.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ra [interval <3-1800>|suppress]
```

**Parameters**

- `ra [interval <3-1800>|suppress]`

| | |
|---|---|
| interval <3-1800> | Configures the interval, in seconds, between two unsolicited successive RAs<br>• <3-1800> – Specify a value from 3 - 1800 seconds. The default is 300 seconds.<br>The router-lifetime should be at least three times the specified router interval. |
| suppress | Enables the suppression of RAs. When enabled, the transmission of RAs in IPv6 packets is suppressed. This option is disabled by default.<br>The *no > ra > suppress* command enables the sending of RAs. |

**Example**

```
rfs6000-81742D(config-ipv6-radv-policy-test)#ra interval 200

rfs6000-81742D(config-ipv6-radv-policy-test)#ra suppress

rfs6000-81742D(config-ipv6-radv-policy-test)#show context
ipv6-router-advertisement-policy test
 ra suppress
 ra interval 200
 managed-config-flag
 nd-reachable-time global
 advertise mtu
 advertise hop-limit
 check-ra-consistency
 dns-server 2002::2 lifetime 3000
 domain-name TechPubs lifetime infinite
rfs6000-81742D(config-ipv6-radv-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the RA interval, and enables the sending of RAs |

### 4.1.60.2.12 router-lifetime

*ipv6-router-advertisement-policy-mode commands*

Configures the default router's lifetime, in seconds, advertised in RAs

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
router-lifetime <0-9000>
```

**Parameters**

- `router-lifetime <0-9000>`

| | |
|---|---|
| router-lifetime <0-9000> | Configures the default router's lifetime<br>• <0-9000> – Specify a value from 0 - 9000 seconds. The default value is 1500 seconds.<br>A value of "0" indicates that this router is not the default router. |

**Example**

```
rfs6000-81742D(config-ipv6-radv-policy-test)#router-lifetime 2000

rfs6000-81742D(config-ipv6-radv-policy-test)#show context
ipv6-router-advertisement-policy test
 ra suppress
 ra interval 200
 managed-config-flag
 nd-reachable-time global
 router-lifetime 2000
 advertise mtu
 advertise hop-limit
 check-ra-consistency
 dns-server 2002::2 lifetime 3000
 domain-name TechPubs lifetime infinite
rfs6000-81742D(config-ipv6-radv-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the default router's lifetime |

### 4.1.60.2.13 router-preference

*ipv6-router-advertisement-policy-mode commands*

Configures the router preference field value advertised in RAs. The options are high, medium, and low. This value is used to prioritize and select the default router when multiple routers are discovered.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
router-preference [high|medium|low]
```

**Parameters**

- `router-preference [high|medium|low]`

| | |
|---|---|
| router-preference [high\|medium\|low] | Sets this router's preference over other routers, in the link, to be the default router. The options are high, low, and medium. The default value is medium.<br>The following points should be taken into consideration when configuring router preference:<br>• For a router to be selected as a default router, the router's lifetime should not be equal to "0".<br>• To enable default router selection, using router information contained in RAs, configure default router selection on that interface. |

**Example**

```
rfs6000-81742D(config-ipv6-radv-policy-test)#router-preference high

rfs6000-81742D(config-ipv6-radv-policy-test)#show context
ipv6-router-advertisement-policy test
 ra suppress
 ra interval 200
 managed-config-flag
 nd-reachable-time global
 router-lifetime 2000
 advertise mtu
 advertise hop-limit
 router-preference high
 check-ra-consistency
 dns-server 2002::2 lifetime 3000
 domain-name TechPubs lifetime infinite
rfs6000-81742D(config-ipv6-radv-policy-test)#
```

### 4.1.60.2.14 unicast-solicited-advertisement

*ipv6-router-advertisement-policy-mode commands*

Enables unicasting of solicited RAs. This feature is disabled by default.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
unicast-solicited-advertisement
```

**Parameters**

None

**Example**

```
rfs6000-81742D(config-ipv6-radv-policy-test)#unicast-solicited-advertisement

rfs6000-81742D(config-ipv6-radv-policy-test)#show context
ipv6-router-advertisement-policy test
 ra suppress
 ra interval 200
 unicast-solicited-advertisement
 managed-config-flag
 nd-reachable-time global
 router-lifetime 2000
 advertise mtu
 advertise hop-limit
 router-preference high
 check-ra-consistency
 dns-server 2002::2 lifetime 3000
 domain-name TechPubs lifetime infinite
rfs6000-81742D(config-ipv6-radv-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables unicasting of solicited RAs |

## 4.1.61 l2tpv3

*Global Configuration Commands*

Configures a *Layer 2 Tunnel Protocol Version 3* (L2TPv3) tunnel policy, used to create one or more L2TPv3 tunnels

The L2TPv3 policy defines the control and encapsulation protocols needed for tunneling layer 2 frames between two IP nodes. This policy enables creation of L2TPv3 tunnels for transporting Ethernet frames between bridge VLANs and physical GE ports. L2TPv3 tunnels can be created between any vendor devices supporting L2TPv3 protocol.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
l2tpv3 policy <L2TPV3-POLICY-NAME>
```

**Parameters**

- `l2tpv3 policy <L2TPV3-POLICY-NAME>`

| | |
|---|---|
| l2tpv3 policy <L2TPV3-POLICY-NAME> | Configures an L2TPv3 tunnel policy<br>• <L2TPV3-POLICY-NAME> – Specify a policy name. The policy is created if it does not exist. To modify an existing L2TPv3, specify its name. |

**Example**

```
rfs6000-81742D(config)#l2tpv3 policy L2TPV3Policy1
rfs6000-81742D(config-l2tpv3-policy-L2TPV3Policy1)#?
L2tpv3 Policy Mode commands:
  cookie-size             Size of the cookie field present in each l2tpv3 data
                          message
  failover-delay          Time interval for re-establishing the tunnel after
                          the failover (RF-Domain
                          manager/VRRP-master/Cluster-master failover)
  force-l2-path-recovery  Enables force learning of servers, gateways etc.,
                          behind the l2tpv3 tunnel when the tunnel is
                          established
  hello-interval          Configure the time interval (in seconds) between
                          l2tpv3 Hello keep-alive messages exchanged in l2tpv3
                          control connection
  no                      Negate a command or set its defaults
  reconnect-attempts      Maximum number of attempts to reestablish the
                          tunnel.
  reconnect-interval      Time interval between the successive attempts to
                          reestablish the l2tpv3 tunnel
  retry-attempts          Configure the maximum number of retransmissions for
                          signaling message
  retry-interval          Time interval (in seconds) before the initiating a
                          retransmission of any l2tpv3 signaling message
  rx-window-size          Number of signaling messages that can be received
                          without sending the acknowledgement
  tx-window-size          Number of signaling messages that can be sent
                          without receiving the acknowledgement

  clrscr                  Clears the display screen
  commit                  Commit all changes made in this session
```

```
  end                          End current mode and change to EXEC mode
  exit                         End current mode and down to previous mode
  help                         Description of the interactive help system
  revert                       Revert changes
  service                      Service Commands
  show                         Show running system information
  write                        Write running configuration to memory or terminal

rfs6000-81742D(config-l2tpv3-policy-L2TPV3Policy1)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing L2TPv3 tunnel policy |
| *mint-policy* | Configures the global MiNT policy |

**NOTE:** For more information on the L2TPv3 tunnel configuration mode and commands, see *Chapter 22, L2TPV3-POLICY*.

## 4.1.62 mac

*Global Configuration Commands*

Configures a MAC ACLs

Access lists define access permissions to the network using a set of rules. Each rule specifies an action taken when a packet matches the rule. If the action is deny, the packet is dropped. If the action is permit, the packet is allowed.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
mac access-list <MAC-ACL-NAME>
```

**Parameters**

- `mac access-list <MAC-ACL-NAME>`

| | |
|---|---|
| access-list <MAC-ACL-NAME> | Configures a MAC access control list<br>• <MAC-ACL-NAME> – Specify the MAC ACL name. If the access control list does not exist, it is created. |

**Example**

```
rfs6000-81742D(config)#mac access-list test
rfs6000-81742D(config-mac-acl-test)#?
MAC Extended ACL Configuration commands:
  deny     Specify packets to reject
  disable  Disable rule if not needed
  no       Negate a command or set its defaults
  permit   Specify packets to forward

  clrscr   Clears the display screen
  commit   Commit all changes made in this session
  end      End current mode and change to EXEC mode
  exit     End current mode and down to previous mode
  help     Description of the interactive help system
  revert   Revert changes
  service  Service Commands
  show     Show running system information
  write    Write running configuration to memory or terminal

rfs6000-81742D(config-mac-acl-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes a MAC access control list |

**NOTE:** For more information on MAC access control lists, see *Chapter 11, ACCESS-LIST*.

## 4.1.63 management-policy

*Global Configuration Commands*

Configures a management policy. Management policies include services that run on a device, welcome messages, banners, etc.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
management-policy <MANAGEMENT-POLICY-NAME>
```

**Parameters**

- `management-policy <MANAGEMENT-POLICY-NAME>`

| | |
|---|---|
| <MANAGEMENT-POLICY-NAME> | Specify the management policy name. If the policy does not exist, it is created. |

**Example**

```
<DEVICE>(config)#management-policy test
<DEVICE>(config-management-policy-test)#?
Management Mode commands:
  aaa-login                 Set authentication for logins
  allowed-locations         Add allowed locations
  banner                    Define a login banner
  ftp                       Enable FTP server
  http                      Hyper Text Terminal Protocol (HTTP)
  https                     Secure HTTP
  idle-session-timeout      Configure idle timeout for a configuration session
                            (GUI or CLI)
  ipv6                      IPv6 Protocol
  no                        Negate a command or set its defaults
  passwd-retry              Lockout user if too many consecutive login failures
  privilege-mode-password   Set the password for entering CLI privilege mode
  rest-server               Enable rest server for device on-boarding
                            functionality
  restrict-access           Restrict management access to the device
  snmp-server               SNMP
  ssh                       Enable ssh
  t5                        T5 configuration
  telnet                    Enable telnet
  user                      Add a user account

  clrscr                    Clears the display screen
  commit                    Commit all changes made in this session
  do                        Run commands from Exec mode
  end                       End current mode and change to EXEC mode
  exit                      End current mode and down to previous mode
  help                      Description of the interactive help system
  revert                    Revert changes
  service                   Service Commands
  show                      Show running system information
  write                     Write running configuration to memory or terminal

<DEVICE>(config-management-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing management policy |

**NOTE:** For more information on Management policy configuration, see *Chapter 15, MANAGEMENT-POLICY*.

## 4.1.64 meshpoint

*Global Configuration Commands*

Creates a new meshpoint and enters its configuration mode. Use this command to select and configure existing meshpoints.

**Supported in the following platforms:**

- Access Points — AP6522, AP6532, AP6562, AP7161, AP7522, AP7532, AP7562, AP81XX
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

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

**Parameters**

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

| | |
|---|---|
| <MESHPOINT-NAME> | Specify the meshpoint name. If the meshpoint does not exist, it is created. |
| containing <WORD> | Selects existing meshpoints containing the sub-string <WORD> in their names |

**Example**

```
rfs6000-81742D(config)#meshpoint TestMeshpoint
rfs6000-81742D(config-meshpoint-TestMeshpoint)#?
Mesh Point Mode commands:
  allowed-vlans  Set the allowed VLANs
  beacon-format  The beacon format of this meshpoint
  control-vlan   VLAN for meshpoint control traffic
  data-rates     Specify the 802.11 rates to be supported on this meshpoint
  description    Configure a description of the usage of this meshpoint
  force          Force suboptimal paths
  meshid         Configure the Service Set Identifier for this meshpoint
  neighbor       Configure neighbor specific parameters
  no             Negate a command or set its defaults
  root           Set this meshpoint as root
  security-mode  The security mode of this meshpoint
  shutdown       Shutdown this meshpoint
  use            Set setting to use
  wpa2           Modify ccmp wpa2 related parameters

  clrscr         Clears the display screen
  commit         Commit all changes made in this session
  do             Run commands from Exec mode
  end            End current mode and change to EXEC mode
  exit           End current mode and down to previous mode
  help           Description of the interactive help system
  revert         Revert changes
  service        Service Commands
  show           Show running system information
  write          Write running configuration to memory or terminal

rfs6000-81742D(config-meshpoint-TestMeshpoint)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing meshpoint |

**NOTE:** For more information on Meshpoint configuration, see *Chapter 26, MESHPOINT*.

## 4.1.65 meshpoint-qos-policy

*Global Configuration Commands*

Configures a set of parameters that defines the meshpoint *quality of service* (QoS) policy

**Supported in the following platforms:**

- Access Points — AP6522, AP6532, AP6562, AP7161, AP7522, AP7532, AP7562, AP81XX
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
meshpoint-qos-policy <MESHPOINT-QOS-POLICY-NAME>
```

**Parameters**

- `meshpoint-qos-policy <MESHPOINT-QOS-POLICY-NAME>`

| | |
|---|---|
| <MESHPOINT-QOS-POLICY-NAME> | Specify the meshpoint QoS policy name. If the policy does not exist, it is created. |

**Example**

```
rfs6000-81742D(config)#meshpoint-qos-policy TestMeshpointQoS
rfs6000-81742D(config-meshpoint-qos-TestMeshpointQoS)#?
Mesh Point QoS Mode commands:
  accelerated-multicast  Configure accelerated multicast streams address and
                         forwarding QoS classification
  no                     Negate a command or set its defaults
  rate-limit             Configure traffic rate-limiting parameters on a
                         per-meshpoint/per-neighbor basis

  clrscr                 Clears the display screen
  commit                 Commit all changes made in this session
  do                     Run commands from Exec mode
  end                    End current mode and change to EXEC mode
  exit                   End current mode and down to previous mode
  help                   Description of the interactive help system
  revert                 Revert changes
  service                Service Commands
  show                   Show running system information
  write                  Write running configuration to memory or terminal

rfs6000-81742D(config-meshpoint-qos-TestMeshpointQoS)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing meshpoint QoS policy |

**NOTE:** For more information on Meshpoint QoS policy configuration, see *Chapter 26, MESHPOINT*.

## 4.1.66 mint-policy

*Global Configuration Commands*

Configures the global MiNT policy

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

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

**Parameters**

- `mint-policy global-default`

| | |
|---|---|
| global-default | Configures the global default MiNT policy |

**Example**

```
rfs6000-81742D(config)#mint-policy global-default
rfs6000-81742D(config-mint-policy-global-default)#?
Mint Policy Mode commands:
  level    Mint routing level
  lsp      LSP
  mtu      Configure the global Mint MTU
  no       Negate a command or set its defaults
  router   Mint router
  udp      Configure mint UDP/IP encapsulation

  clrscr   Clears the display screen
  commit   Commit all changes made in this session
  do       Run commands from Exec mode
  end      End current mode and change to EXEC mode
  exit     End current mode and down to previous mode
  help     Description of the interactive help system
  revert   Revert changes
  service  Service Commands
  show     Show running system information
  write    Write running configuration to memory or terminal

rfs6000-81742D(config-mint-policy-global-default)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing MiNT policy |

**NOTE:** For more information on MiNT policy configuration, see *Chapter 14, MINT-POLICY*.

## 4.1.67 nac-list

*Global Configuration Commands*

A *Network Access Control* (NAC) policy configures a list of devices that can access a network based on their MAC addresses.

The following table lists NAC list configuration mode commands:

**Table 4.39** *NAC-List Config Command*

| Command | Description | Reference |
|---|---|---|
| *nac-list* | Creates a NAC list and enters its configuration mode | *page 4-330* |
| *nac-list-mode commands* | Summarizes NAC list configuration mode commands | *page 4-331* |

### 4.1.67.1 nac-list

*nac-list*

Configures a NAC list that manages access to the network

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
nac-list <NAC-LIST-NAME>
```

**Parameters**

- `nac-list <NAC-LIST-NAME>`

| | |
|---|---|
| <NAC-LIST-NAME> | Specify the NAC list name. If the NAC list does not exist, it is created. |

**Example**

```
rfs6000-81742D(config)#nac-list test
rfs6000-81742D(config-nac-list-test)#?
NAC List Mode commands:
  exclude  Specify MAC addresses to be excluded from the NAC enforcement list
  include  Specify MAC addresses to be included in the NAC enforcement list
  no       Negate a command or set its defaults

  clrscr   Clears the display screen
  commit   Commit all changes made in this session
  do       Run commands from Exec mode
  end      End current mode and change to EXEC mode
  exit     End current mode and down to previous mode
  help     Description of the interactive help system
  revert   Revert changes
  service  Service Commands
  show     Show running system information
  write    Write running configuration to memory or terminal

rfs6000-81742D(config-nac-list-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes a NAC list |

### 4.1.67.2 nac-list-mode commands

*nac-list*

The following table summarizes NAC list configuration mode commands:

**Table 4.40** *NAC-List-Mode Commands*

| Command | Description | Reference |
|---|---|---|
| *exclude* | Specifies the MAC addresses excluded from the NAC enforcement list | *page 4-332* |
| *include* | Specifies the MAC addresses included in the NAC enforcement list | *page 4-333* |
| *no* | Cancels an exclude or include NAC list rule | *page 4-334* |

### 4.1.67.2.1 exclude

*nac-list-mode commands*

Specifies the MAC addresses excluded from the NAC enforcement list

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
exclude <START-MAC> [<END-MAC> precedence <1-1000>|precedence <1-1000>]
```

**Parameters**

- `exclude <START-MAC> [<END-MAC> precedence <1-1000>|precedence <1-1000>]`

| | |
|---|---|
| <START-MAC> | Specifies a range of MAC addresses or a single MAC address to exclude from the NAC enforcement list<br>• <START-MAC> – Specify the first MAC address in the range.<br>Use this parameter to specify a single MAC address. |
| <END-MAC> | Specifies the last MAC address in the range (optional if a single MAC is added to the list)<br>• <END-MAC> – Specify the last MAC address in the range. |
| precedence <1-1000> | Sets the rule precedence. Exclude entries are checked in the order of their rule precedence.<br>• <1-1000> – Specify a value from 1 - 1000. |

**Example**

```
rfs6000-81742D(config-nac-list-test)#exclude 00-40-96-B0-BA-2A precedence 1

rfs6000-81742D(config-nac-list-test)#show context
nac-list test
 exclude 00-40-96-B0-BA-2A 00-40-96-B0-BA-2A precedence 1
rfs6000-81742D(config-nac-list-test)#
```

### 4.1.67.2.2 include

*nac-list-mode commands*

Specifies the MAC addresses included in the NAC enforcement list

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
include <START-MAC> [<END-MAC> precedence <1-1000>|precedence <1-1000>]
```

**Parameters**

- `include <START-MAC> [<END-MAC> precedence <1-1000>|precedence <1-1000>]`

| | |
|---|---|
| <START-MAC> | Specifies a range of MAC addresses or a single MAC address to include in the NAC enforcement list<br>• <START-MAC> – Specify the first MAC address in the range.<br>Use this parameter to specify a single MAC address. |
| <END-MAC> | Specifies the last MAC address in the range (optional if a single MAC is added to the list)<br>• <END-MAC> – Specify the last MAC address in the range. |
| precedence <1-1000> | Sets the rule precedence. Include entries are checked in the order of their rule precedence.<br>• <1-1000> – Specify a value from 1 - 1000. |

**Example**

```
rfs6000-81742D(config-nac-list-test)#include 00-15-70-38-06-49 precedence 2

rfs6000-81742D(config-nac-list-test)#show context
nac-list test
 exclude 00-04-96-B0-BA-2A 00-04-96-B0-BA-2A precedence 1
 include 00-15-70-38-06-49 00-15-70-38-06-49 precedence 2
rfs6000-81742D(config-nac-list-test)#
```

### 4.1.67.2.3 no

*nac-list-mode commands*

Cancels an exclude or include NAC list rule

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
no [exclude|include]

no [exclude|include] <START-MAC> [<END-MAC> precedence <1-1000>|precedence <1-1000>]
```

**Parameters**

- `no <PARAMETERS>`

| | |
|---|---|
| no <PARAMETERS> | Removes or reverts this NAC list's settings based on the parameters passed |

**Example**

The following example shows the NAC list 'test' settings before the 'no' command is executed:

```
rfs6000-81742D(config-nac-list-test)#show context
nac-list test
 exclude 00-04-96-B0-BA-2A 00-04-96-B0-BA-2A precedence 1
 include 00-15-70-38-06-49 00-15-70-38-06-49 precedence 2
rfs6000-81742D(config-nac-list-test)#

rfs6000-81742D(config-nac-list-test)#no exclude 00-40-96-B0-BA-2A precedence 1
```

The following example shows the NAC list 'test' settings after the 'no' command is executed:

```
rfs6000-81742D(config-nac-list-test)#show context
nac-list test
 include 00-15-70-38-06-49 00-15-70-38-06-49 precedence 2
rfs6000-81742D(config-nac-list-test)#
```

**Related Commands**

| | |
|---|---|
| *exclude* | Specifies MAC addresses excluded from the NAC enforcement list |
| *include* | Specifies MAC addresses included in the NAC enforcement list |

## 4.1.68 no

*Global Configuration Commands*

Negates a command, or reverts configured settings to their default

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
no [aaa-policy|aaa-tacacs-policy|alias|ap6521|ap6522|ap6532|ap6562|ap71xx|
ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|
ap8432|ap8533|nx5500|nx75xx|nx9000|nx9600|application|application-group|
application-policy|association-acl-policy|auto-provisioning-policy|bgp|bonjour-
gw-discovery-policy|bonjour-gw-forwarding-policy|bonjour-gw-query-forwarding-
policy|captive-portal|client-identity|client-identity-group|crypto-cmp-policy|
customize|database-policy|device|device-categorization|dhcp-server-policy|
dhcpv6-server-policy|dns-whitelist|event-system-policy|ex3500|
ex3500-management-policy|ex3500-qos-class-map-policy|ex3500-qos-policy-map|
ex3524|ex3548|firewall-policy|global-association-list|guest-management|
igmp-snoop-policy|inline-password-encryption|ip|ipv6|ipv6-router-advertisement-
policy|l2tpv3|mac|management-policy|meshpoint|meshpoint-qos-policy|nac-list|
nsight-policy|passpoint-policy|password-encryption|profile|radio-qos-policy|
radius-group|radius-server-policy|radius-user-pool-policy|rf-domain|rfs4000|
rfs6000|roaming-assist-policy|role-policy|route-map|routing-policy|
rtl-server-policy|schedule-policy|t5|sensor-policy|smart-rf-policy|url-filter|
url-list|vx9000|web-filter-policy|wips-policy|wlan|wlan-qos-policy|service]

no alias [address-range <ADDRESS-RANGE-ALIAS-NAME>|host <HOST-ALIAS-NAME>|network
<NETWORK-ALIAS-NAME>|network-group <NETWORK-GROUP-ALIAS-NAME> [address-
range|host|network]|network-service <NETWORK-SERVICE-ALIAS-NAME>|number <NUMBER-
ALIAS-NAME>|string <STRING-ALIAS-NAME>|vlan <VLAN-ALIAS-NAME>]

no [aaa-policy|aaa-tacacs-policy|application-policy|auto-provisioning-policy|
auto-provisioning-policy|bonjour-gw-discovery-policy|bonjour-gw-forwarding-
policy|bonjour-gw-query-forwarding-policy|database-policy|captive-portal|
crypto-cmp-policy|device-categorization|dhcp-server-policy|dhcpv6-server-policy|
dns-whitelist|event-system-policy|ex3500|ex3500-management-policy|ex3500-qos-
class-map-policy|ex3500-qos-policy|firewall-policy|global-association-list|
guest-management|igmp-snoop-policy|inline-password-encryption|ip|ipv6|
ipv6-router-advertisement-policy|l2tpv3|mac|management-policy|meshpoint|
meshpoint-qos-policy|nac-list|nsight-policy|passpoint-policy|radio-qos-policy|
radius-group|radius-server-policy|radius-user-pool-policy|roaming-assist-policy|
role-policy|routing-policy|rtl-server-policy|schedule-policy|sensor-policy|
smart-rf-policy|web-filter-policy|wips-policy|wlan-qos-policy] <POLICY-NAME>

no application <APPLICATION-NAME>

no application-group <APPLICATION-GROUP-NAME>

no [ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|
ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|ex3524|ex3548|rfs4000|
rfs6000|t5|nx5500|nx75xx|nx9000|nx9600|vx9000] <MAC>

no client-identity <CLIENT-IDENTITY-NAME>

no client-identity-group <CLIENT-IDENTITY-GROUP-NAME>
```

```
no device {containing <WORD>} {(filter type [ap6521|ap6522|ap6532|ap6562|ap71xx|
ap7502|ap7522|ap7532|ap7562|ap81xx|ap82xx|ap8432|ap8533|ex3524|ex3548|rfs4000|
rfs6000|t5|nx5500|nx75xx|nx9000|nx9600|vx9000])}

no customize [hostname-column-width|show-wireless-client|show-wireless-client-
stats|show-wireless-client-stats-rf|show-wireless-meshpoint|show-wireless-
meshpoint-neighbor-stats|show-wireless-meshpoint-neighbor-stats-rf|show-
wireless-radio|show-wireless-radio-stats|show-wireless-radio-stats-rf]

no password-encryption secret 2 <OLD-PASSPHRASE>

no profile {ap6521|ap6522|ap6532|ap71xx|ap7502|ap7522|ap7532|ap7562|ap81xx|
ap82xx|ap8432|ap8533|ex3524|ex3548|containing|filter|rfs4000|rfs6000|nx5500|
nx75xx|nx9000|nx9600|t5|vx9000} <PROFILE-NAME>

no wlan [<WLAN-NAME>|all|containing <WLAN-NAME-SUBSTRING>]

no service set [command-history|reboot-history|upgrade-history] {on <DEVICE-NAME>}
```

The following ‘no’ commands are specific to the RFS4000, RFS6000, and NX95XX platforms:

```
no t5 <T5-DEVICE-MAC>
```

The following ‘no’ commands are specific to the RFS4000, RFS6000, and NX95XX platforms:

```
no bgp [as-path-list|community-list|extcommunity-list|ip-access-list|ip-prefix-
list] <LIST-NAME>
```

The following ‘no’ commands are specific to the NX95XX series service platforms:

```
no route-map <ROUTE-MAP-NAME>
```

The following ‘no’ commands are specific to the AP6522, AP6532, AP7161, AP7502, AP7522, AP7532, AP8132, RFS4000, RFS6000 platforms:

```
no url-filter <URL-FILTER-NAME>
no url-list <URL-LIST-NAME>
no web-filter-name <WEB-FILTER-NAME>
```

The following ‘no’ command is specific to the VX9000 virtual machine platform:

```
no database-client-policy <POLICY-NAME>
```

**Parameters**

- `no <PARAMETERS>`

| | |
|---|---|
| no <PARAMETERS> | Removes or resets settings, configurable in the global configuration mode, based on the parameters passed |

**Example**

```
<DEVICE>(config)#no ?
  aaa-policy                          Delete a aaa policy
  aaa-tacacs-policy                   Delete a aaa tacacs policy
  alias                               Alias
  ap650                               Delete an AP650 access point
  ap6511                              Delete an AP6511 access point
  ap6521                              Delete an AP6521 access point
  ap6522                              Delete an AP6522 access point
  ap6532                              Delete an AP6532 access point
  ap6562                              Delete an AP6562 access point
  ap71xx                              Delete an AP7161 access point
  ap7502                              Delete an AP7502 access point
  ap7522                              Delete an AP7522 access point
  ap7532                              Delete an AP7532 access point
  ap7562                              Delete an AP7562 access point
  ap7602                              Delete an AP7602 access point
  ap7612                              Delete an AP7612 access point
  ap7622                              Delete an AP7622 access point
  ap7632                              Delete an AP7632 access point
  ap7662                              Delete an AP7662 access point
  ap81xx                              Delete an AP81XX access point
```

```
ap82xx                                Delete an AP82XX access point
ap8432                                Delete an AP8432 access point
ap8533                                Delete an AP8533 access point
application                           Delete an application
application-group                     Delete an application-group
application-policy                    Delete an application policy
association-acl-policy                Delete an association-acl policy
auto-provisioning-policy              Delete an auto-provisioning policy
bgp                                   BGP Configuration
bonjour-gw-discovery-policy           Disable Bonjour Gateway discovery policy
bonjour-gw-forwarding-policy          Disable Bonjour Gateway Forwarding
                                      policy
bonjour-gw-query-forwarding-policy    Disable Bonjour Gateway Query Forwarding
                                      policy
captive-portal                        Delete a captive portal
client-identity                       Client identity (DHCP Device
                                      Fingerprinting)
client-identity-group                 Client identity group (DHCP Fingerprint
                                      Database)
crypto-cmp-policy                     CMP policy
customize                             Restore the custom cli commands to
                                      default
database-client-policy                Configure database policy
database-policy                       Configure database policy
device                                Delete multiple devices
device-categorization                 Delete  device categorization object
dhcp-server-policy                    DHCP server policy
dhcpv6-server-policy                  DHCPv6 server related configuration
dns-whitelist                         Delete a whitelist object
event-system-policy                   Delete a event system policy
ex3500                                EX3500 device
ex3500-management-policy              Delete a ex3500 management policy
ex3500-qos-class-map-policy           Delete a ex3500 qos class-map policy
ex3500-qos-policy-map                 Delete a ex3500 qos policy-map
ex3524                                Delete an EX3524 wireless controller
ex3548                                Delete an EX3548 wireless controller
firewall-policy                       Configure firewall policy
global-association-list               Delete a global association list
guest-management                      Delete a guest management policy
igmp-snoop-policy                     Remove device onboard igmp snoop policy
inline-password-encryption            Disable storing encryption key in the
                                      startup configuration file
ip                                    Internet Protocol (IP)
ipv6                                  Internet Protocol version 6 (IPv6)
ipv6-router-advertisement-policy      IPv6 Router Advertisement related
                                      configuration
l2tpv3                                Negate a command or set its defaults
mac                                   MAC configuration
management-policy                     Delete a management policy
meshpoint                             Delete a meshpoint object
meshpoint-qos-policy                  Delete a mesh point QoS configuration
                                      policy
nac-list                              Delete an network access control list
nsight-policy                         Delete a nsight policy
nx5500                                Delete an NX5500 wireless controller
nx75xx                                Delete an NX75XX wireless controller
nx9000                                Delete an NX9000 wireless controller
passpoint-policy                      Delete a passpoint configuration policy
password-encryption                   Disable password encryption in
                                      configuration
profile                               Delete a profile and all its associated
                                      configuration
radio-qos-policy                      Delete a radio QoS configuration policy
radius-group                          Local radius server group configuration
radius-server-policy                  Remove device onboard radius policy
radius-user-pool-policy               Configure Radius User Pool
rf-domain                             Delete one or more RF-domains and all
                                      their associated configurations
```

```
  rfs4000                          Delete an RFS4000 wireless controller
  rfs6000                          Delete an RFS6000 wireless controller
  roaming-assist-policy            Delete a roaming-assist policy
  role-policy                      Role based firewall policy
  route-map                        Dynamic routing route map Configuration
  routing-policy                   Policy Based Routing Configuration
  rtl-server-policy                Delete a rtl server policy
  schedule-policy                  Delete a schedule policy
  sensor-policy                    Delete a sensor policy
  smart-rf-policy                  Delete a smart-rf-policy
  t5                               Delete an T5 wireless controller
  url-filter                       Delete a url filter
  url-list                         Delete a URL list
  vx9000                           Delete an VX9000 wireless controller
  web-filter-policy                Delete a web filter policy
  wips-policy                      Delete a wips policy
  wlan                             Delete a wlan object
  wlan-qos-policy                  Delete a wireless lan QoS configuration
                                   policy

  service                          Service Commands

<DEVICE>(config)#
```

## 4.1.69 nsight-policy

*Global Configuration Commands*

The following table lists NSight policy configuration mode commands:

**Table 4.41** *NSight-Policy Config Command*

| Command | Description | Reference |
|---|---|---|
| *nsight-policy* | Creates an NSight policy and enters its configuration mode | *page 4-340* |
| *nsight-policy commands* | Summarizes NSight policy configuration mode commands | *page 4-342* |

### 4.1.69.1 nsight-policy

*nsight-policy*

Creates an NSight policy and enters its configuration mode

The NSight policy is an advance management, analytics, reporting, and troubleshooting tool, which when created and applied at the RF Domain level allows the RF Domain manager to send statistics (polled from devices within the RF Domain) to the NOC. The NOC, when enabled as the NSight server, stores this data in a locally or externally hosted database. This large, complex data is collated and presented on an NSight Dashboard that can be launched from the NSight-enabled NOC. For large networks, enabling NSight removes the inadequacies of the existing data collection, presentation, and analytics framework. It simplifies network monitoring, troubleshooting, and reporting.

**NOTE:** NSight is a licensed feature, and can be enabled only on the application of an NSight license in the NSight server's self mode.

The NSight features include:

- Network statistic and event visualization - Simplified and unified network views based on defined user roles
- Custom dashboards - Live network health information in real-time to optimally assist network administrators
- Live troubleshooting tools - Packet capture, wireless debug logs, TCP/IP ping and traceroute
- Interactive floor maps with timeline views - Visualize and identify potential issues and problems areas
- Real-time trend analysis - Simplify network growth planning
- Exceptionally responsive interface - Any information the admin needs is three, or less, clicks away

The WiNG NSight implementation consists of the following components:

- An NSight server
- A database. This database consists of AP statistics gathered by RF Domain managers.
- An NSight UI portal
- An NSight client hosted on the RF Domain manager, which periodically gathers statistics from APs and forwards to the NSight server.
- Event history – Event details for all APs adopted by the NOC. These are events received by the Cfgd every 30 seconds and sent to the MART server. Each event consists of the RF Domain name, wireless client MAC if applicable, AP MAC, event mnemonic, event timestamp, and the event string itself.

**Supported in the following platforms:**

- Service Platforms — NX7500, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
nsight-policy <NSIGHT-POLICY-NAME>
```

**Parameters**

- `nsight-policy <NSIGHT-POLICY-NAME>`

| | |
|---|---|
| <NSIGHT-POLICY-NAME> | Specify the NSight policy name. If the policy does not exist, it is created. |

**Example**

```
nx9500-6C8809(config)#nsight-policy test
nx9500-6C8809(config-nsight-policy-test)#?
Nsight Policy Mode commands:
  enable               Enable this Nsight policy
  event-history-size   Size of the event history collection
  history-ttl          Time to live for historical data
  no                   Negate a command or set its defaults
  nsight-server        Enable Nsight server functionality
  server               Configure Nsight server

  clrscr               Clears the display screen
  commit               Commit all changes made in this session
  end                  End current mode and change to EXEC mode
  exit                 End current mode and down to previous mode
  help                 Description of the interactive help system
  revert               Revert changes
  service              Service Commands
  show                 Show running system information
  write                Write running configuration to memory or terminal

nx9500-6C8809(config-nsight-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing NSight policy |

### 4.1.69.2 nsight-policy commands

*nsight-policy*

The following table summarizes NSight policy configuration mode commands:

**Table 4.42** *NSight-Policy-Config Mode Commands*

| Command | Description | Reference |
|---|---|---|
| *enable* | Enables this NSight policy | *page 4-343* |
| *event-history-size* | Converts and sizes the NSight event history collection to a capped collection | *page 4-344* |
| *history-ttl* | Configures the *time-to-live* (TTL), in days, for historical data related to clients and devices | *page 4-345* |
| *nsight-server* | Enables NSight server functionality and configures the SMTP report delivery settings | *page 4-346* |
| *server* | Configures the NSight server host. This configuration is used by the NSight client to identify the NSight server host. | *page 4-348* |
| *no* | Removes this NSight policy settings | *page 4-349* |

### 4.1.69.2.1 enable

*nsight-policy commands*

Enables this NSight policy. The default setting is enabled.

**Supported in the following platforms:**

- Service Platforms — NX9500, NX9510, NX9600, VX9000

**Syntax**

```
enable
```

**Parameters**

None

**Example**

```
nx9510-6C8A5C(config-nsight-policy-test2)#enable
```

**Related Commands**

| | |
|---|---|
| *no* | Disables this NSight policy |

### 4.1.69.2.2 event-history-size

*nsight-policy commands*

Converts and sizes the NSight event history collection to a capped collection. The conversion occurs when upgrading. Use this command to define the NSight event history collection's size and prevent its unbounded growth. Note, resizing the collection results in the collection contents being dropped.

**Supported in the following platforms:**

- Service Platforms — NX9500, NX9510, NX9600, VX9000

**Syntax**

```
event-history-size [high|low|medium]
```

**Parameters**

- `event-history-size [high|low|medium]`

| | |
|---|---|
| event-history-size [high\|low\|medium] | Defines the size of the NSight event history collection. The options are:<br>• high – Sets the size at approximately 10 M events<br>• low – Sets the size at approximately 500 K events. This is the default setting.<br>• medium – Sets the size at approximately 5 M events |

**Example**

```
nx9500-6C8809(config-nsight-policy-test)#event-history-size medium

nx9500-6C8809(config-nsight-policy-test)#show context
nsight-policy test
 event-history-size medium
nx9500-6C8809(config-nsight-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Reverts the NSight event history collection size to default (5 M) |

### 4.1.69.2.3 history-ttl

*nsight-policy commands*

Configures the *time-to-live* (TTL), in days, for historical data related to clients, devices, and guest users. This is the duration for which clients, devices, or guest user related data is retained in the NSight database.

**Supported in the following platforms:**

- Service Platforms — NX9500, NX9510, NX9600, VX9000

**Syntax**

```
history-ttl [clients|devices|guest-clients]

history-ttl [clients|devices] <1-3650>

history-ttl guest-clients <8-48>
```

**Parameters**

- `history-ttl [clients|devices] <1-3650>`

| | |
|---|---|
| history-ttl [client\|devices] <1-3650> | Configures the TTL for historical data related to clients and devices<br>• clients – Configures the TTL for wireless clients related historical data<br>• devices – Configures the TTL for devices (adopted access points or site controllers) related historical data<br>The following is common to both the 'clients' and 'devices' keywords:<br>• <1-3650> – Specify a value from 1 - 3650 days. The default for both (clients and devices) is 180 days. |

- `history-ttl guest-clients <8-48>`

| | |
|---|---|
| history-ttl guest-clients <8-48> | Configures the TTL for historical data related to clients and devices<br>• guest-clients – Configures the TTL for guest-client related historical data<br>• <8-48> – Specify a value from 8 - 48 hours. The default is 8 hours. |

**Example**

```
nx9500-6C8809(config-nsight-policy-test)#history-ttl clients 250

nx9500-6C8809(config-nsight-policy-test)#show context
nsight-policy test
 history-ttl clients 250
nx9500-6C8809(config-nsight-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Reverts the NSight clients or devices TTL duration to default (180 days) |

### 4.1.69.2.4 nsight-server

*nsight-policy commands*

Enables NSight server functionality and configures the SMTP report delivery settings.

**Supported in the following platforms:**

- Service Platforms — NX9500, NX9510, NX9600, VX9000

**Syntax**

```
nsight-server {smtp-report-delivery|standalone}

nsight-server {smtp-report-delivery host <WORD> sender <EMAIL-ADD> [port <1-65535>|security [none|ssl|starttls]|username <USER-NAME> password [0|2|<WORD>]]}

nsight-server {standalone}
```

**Parameters**

- `nsight-server {smtp-report-delivery host <WORD> sender <EMAIL-ADD> [port <1-65535>|security [none|ssl|starttls]|username <USER-NAME> password [0|2|<WORD>]]}`

| | |
|---|---|
| nsight-server | Enables NSight server functionality on the host using this NSight policy |
| smtp-report-delivery host <WORD> | Optional. Configures SMTP report delivery settings<br>• host <WORD> – Configures the SMTP server host<br>• <WORD> – Specify the SMTP server host's IP address or hostname. |
| sender <EMAIL-ADD> | Optional. Configures the SMTP sender's e-mail address<br>• <EMAIL-ADD> – Specify the sender's e-mail address. |
| port <1-65535> | Optional. Configures the SMTP server port<br>• <1-65535> – Specify the port from 1 - 65535. |
| security [none\|ssl\|starttls] | Optional. Configures the encryption protocol used by the SMTP server. The options are:<br>• none – Uses no encryption<br>• ssl – Uses SSL encryption<br>• starttls – Uses STARTTLS encryption |
| username <USER-NAME> password [0\|2\|<WORD>] | Optional. Configures the SMTP username<br>• <USER-NAME> Specify the user name<br>• password [0\|2\|<WORD>] – Configures the password associated with the above configured user<br>• 0 – Configures a clear text password<br>• 2 – Configures an encrypted password<br>• <WORD> – Enter the password. |

- `nsight-server {standalone}`

| | |
|---|---|
| nsight-server | Enables NSight server functionality on the host using this NSight policy |
| standalone | Optional. Configures NSight server as standalone. Use this option in the split NSight deployment scenario where the NSight server and database are hosted on separate hosts. |

**Example**

```
nx9510-6C8A5C(config-nsight-policy-test2)#nsight-server

nx9510-6C8A5C(config-nsight-policy-test2)#show context
nsight-policy test2
 nsight-server
nx9510-6C8A5C(config-nsight-policy-test2)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables NSight server functionality on this NSight policy |

### 4.1.69.2.5 server

*nsight-policy commands*

Configures the NSight server host. This configuration is used by the NSight client to identify the NSight server host.

**Supported in the following platforms:**

- Service Platforms — NX9500, NX9510, NX9600, VX9000

**Syntax**

```
server host [<IP>|<HOSTNAME>|<X:X::X:X>] {http|https}
```

**Parameters**

- `server host [<IP>|<HOSTNAME>|<X:X::X:X>] {http|https}`

| | |
|---|---|
| server host [<IP>\| <HOSTNAME>\| <X:X::X:X>] | Configures the NSight server host's address. Use one of the following options to identify the NSight server host:<br>• <IP> – Configures the NSight server's IPv4 address<br>• <HOSTNAME> – Configures the NSight server's hostname<br>• <X:X::X:X> – Configures the NSight server's IPv6 address |
| {http\|https} | Optional. Configures the protocol used to communicate with the NSight server<br>• http – Optional. Uses HTTP to communicate<br>• https – Optional. Uses HTTPS to communicate (this is the default setting) |

**Example**

```
nx9510-6C8A5C(config-nsight-policy-test2)#server host 172.22.0.153 http

nx9510-6C8A5C(config-nsight-policy-test2)#show context
nsight-policy test2
 server host 172.22.0.153 http
 nsight-server
nx9510-6C8A5C(config-nsight-policy-test2)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes NSight server host settings from this NSight policy |

### 4.1.69.2.6 no

*nsight-policy commands*

Removes NSight policy settings

**Supported in the following platforms:**

- Service Platforms — NX9500, NX9510, NX9600, VX9000

**Syntax**

```
no [enable|event-history-size|history-ttl [clients|devices|guest-clients]|
   nsight-server {smtp-report-delivery}|server host [<IP>|<HOSTNAME>|<X:X::X:X>]]
```

**Parameters**

- `no <PARAMETERS>`

| | |
|---|---|
| no <PARAMETERS> | Removes NSight policy settings based on the parameters passed |

**Example**

The following example shows the NSight policy 'test2' settings before the 'no' command is executed:

```
nx9510-6C8A5C(config-nsight-policy-test2)#show context
nsight-policy test2
 server host 172.22.0.153 http
 nsight-server
nx9510-6C8A5C(config-nsight-policy-test2)#

nx9510-6C8A5C(config-nsight-policy-test2)#no server host 172.22.0.153
```

The following example shows the NSight policy 'test2' settings after the 'no' command is executed:

```
nx9500-6C8809(config-nsight-policy-test2)#show context
nsight-policy test2
 nsight-server
nx9510-6C8A5C(config-nsight-policy-test2)#
```

## 4.1.70 passpoint-policy

*Global Configuration Commands*

Creates a new passpoint policy and enters its configuration mode

The passpoint policy implements the Hotspot 2.0 Wi-Fi Alliance standard, enabling interoperability between clients, infrastructure, and operators. It makes a portion of the IEEE 802.11u standard mandatory and adds Hotspot 2.0 extensions that allow clients to query a network before actually attempting to join it.

The passpoint policy allows a single or set of Hotspot 2.0 configurations to be global and referenced by the devices that use it. It is mapped to a WLAN. However, only primary WLANs on a BSSID will have their passpoint policy configuration used.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
passpoint-policy <POLICY-NAME>
```

**Parameters**

- `passpoint-policy <POLICY-NAME>`

| | |
|---|---|
| passpoint-policy <POLICY-NAME> | Specify the passpoint policy name. If a passpoint policy does not exist, it is created. |

**Example**

```
rfs4000-229D58(config)#passpoint-policy test
rfs4000-229D58(config-passpoint-policy-test)#?
Passpoint Policy Mode commands:
  3gpp                    Configure a 3gpp plmn (public land mobile network) id
  access-network-type     Set the access network type for the passpoint
  connection-capability   Configure the connection capability for the passpoint
  domain-name             Add a domain-name for the passpoint
  hessid                  Set a homogeneous ESSID value for the passpoint
  internet                Advertise the passopint having internet access
  ip-address-type         Configure the advertised ip-address-type
  nai-realm               Configure a NAI realm for the passpoint
  net-auth-type           Add a network authentication type to the passpoint
  no                      Negate a command or set its defaults
  operator                Add configuration related to the operator of the
                          passpoint
  osu                     Online signup
  roam-consortium         Add a roam consortium for the passpoint
  venue                   Set the venue parameters of the passpoint
  wan-metrics             Set the wan-metrics of the passpoint

  clrscr                  Clears the display screen
  commit                  Commit all changes made in this session
  do                      Run commands from Exec mode
  end                     End current mode and change to EXEC mode
  exit                    End current mode and down to previous mode
  help                    Description of the interactive help system
  revert                  Revert changes
  service                 Service Commands
  show                    Show running system information
```

```
  write                  Write running configuration to memory or terminal
rfs4000-229D58(config-passpoint-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing passpoint policy |

**NOTE:** For more information on passpoint policy, see *Chapter 27, PASSPOINT POLICY*.

## 4.1.71 password-encryption

*Global Configuration Commands*

Enables password encryption and configures the passphrase used to encrypt passwords. When enabled, passwords configured within the system are not displayed as clear text.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
password-encryption secret 2 <LINE>
```

**Parameters**

- `password-encryption secret 2 <LINE>`

| | |
|---|---|
| secret 2 <LINE> | Encrypts passwords with a secret phrase<br>• 2 – Specifies the encryption type as either SHA256 or AES256<br>• <LINE> – Specify the encryption passphrase. |

**Example**

```
nx9500-6C8809(config)#password-encryption secret 2 test@123
```

To confirm if password encryption is enabled, execute the following command:

```
nx9500-6C8809(config)#show password-encryption status
Password encryption is enabled
nx9500-6C8809(config)#
```

The following example shows the privilege-mode-password as encrypted text. Note, the digit '1' preceding the password implies that displayed text is the encrypted password and not clear text.

```
nx9500-6C8809(config-management-policy-test)#show context include-factory |
include privilege-mode-password
 privilege-mode-password 1
bc28e4d82bb11fa75a3c56346441d48f50f19c47184e2575a59a6a5d18e63925
nx9500-6C8809(config-management-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables password encryption |

## 4.1.72 profile

*Global Configuration Commands*

Configures profile related commands. If no parameters are given, all profiles are selected.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
profile {anyap|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|
ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|containing|filter
|rfs4000|rfs6000|nx5500|nx75xx|nx9000|nx9600|vx9000}

profile {anyap|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|
ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|rfs6000|
nx5500|nx75xx|nx9000|nx9600|vx9000} <DEVICE-PROFILE-NAME>

profile {containing <DEVICE-PROFILE-NAME>} {filter type [ap6521|ap6522|ap6532|
ap6562|ap71xx|ap7502|ap7522|ap7532|ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|
ap82xx|ap8432|ap8533|rfs4000|rfs6000|nx75xx|nx9000|vx9000]}

profile {filter type [ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|
ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|
rfs6000|nx5500|nx75xx|nx9000|nx9600|vx9000]}
```

**Parameters**

- `profile {anyap|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|rfs6000|nx5500|nx75xx|nx9000|nx9600|vx9000} <DEVICE-PROFILE-NAME>`

| | |
|---|---|
| profile <DEVICE-TYPE> <DEVICE-PROFILE-NAME> | Configures device profile commands. If no device profile is specified, the system configures all device profiles.<br>• <DEVICE-TYPE> – Optional. Select the device type. The options are: AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533, RFS4000, RFS6000, NX5500, NX75XX, NX95XX, NX9600, and VX9000. After specifying the device type, specify the profile name.<br>• <DEVICE-PROFILE-NAME> – Specify the profile name.<br>Select 'anyap' to configure a profile applicable to any access point.<br>The NX9600 profile option is only available on an NX9600 device. |

- `profile {containing <DEVICE-PROFILE-NAME>} {filter type [ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|rfs6000|nx5500|nx75xx|nx9000|nx9600|vx9000]}`

| | |
|---|---|
| profile | Configures device profile commands |
| containing <DEVICE-PROFILE-NAME> | Optional. Configures profiles that contain a specified sub-string in the hostname<br>• <DEVICE-PROFILE-NAME> – Specify a substring in the profile name to filter profiles. |

| | |
|---|---|
| filter type | Optional. An additional filter used to configure a specific type of device profile. If no device type is specified, the system configures all device profiles.<br>• type – Filters profiles by the device type. Select a device type from the following options: AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533, RFS4000, RFS6000, NX5500, NX75XX, NX95XX, NX9600, and VX9000.<br>The NX9600 profile option is only available on an NX9600 device. |

• `profile {filter type [ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|rfs6000|nx5500|nx75xx|nx9000|nx9600|vx9000]}`

| | |
|---|---|
| profile | Configures device profile commands |
| filter type | Optional. An additional filter used to configure a specific type of device profile. If no device type is specified, the system configures all device profiles.<br>• type – Filters profiles by the device type. Select a device type from the following options: AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533, RFS4000, RFS6000, NX5500, NX75XX, NX95XX, NX9600, and VX9000.<br>The NX9600 profile option is only available on an NX9600 device. |

**Example**

```
<DEVICE>(config)#profile <DEVICE-TYPE> <PROFILE-NAME>
<DEVICE>(config-profile-<PROFILE-NAME>)#?
Profile Mode commands:
  adopter-auto-provisioning-policy-lookup  Use centralized auto-provisioning
                                           policy when adopted by another
                                           controller
  adoption                                 Adoption configuration
  alias                                    Alias
  application-policy                       Application Policy configuration
  area                                     Set name of area where the system
                                           is located
  arp                                      Address Resolution Protocol (ARP)
  auto-learn                               Auto learning
  autogen-uniqueid                         Autogenerate a unique id
  autoinstall                              Autoinstall settings
  bluetooth-detection                      Detect Bluetooth devices using the
                                           Bluetooth USB module - there will
                                           be interference on 2.4 Ghz radio in
                                           wlan mode
  bridge                                   Ethernet bridge
  captive-portal                           Captive portal
  cdp                                      Cisco Discovery Protocol
  cluster                                  Cluster configuration
  configuration-persistence                Enable persistence of configuration
                                           across reloads (startup config
                                           file)
  controller                               WLAN controller configuration
  critical-resource                        Critical Resource
  crypto                                   Encryption related commands
  database                                 Database command
  device-onboard                           Device-onboarding configuration
  device-upgrade                           Device firmware upgrade
  diag                                     Diagnosis of packets
  dot1x                                    802.1X
  dpi                                      Enable Deep-Packet-Inspection
                                           (Application Assurance)
  dscp-mapping                             Configure IP DSCP to 802.1p
                                           priority mapping for untagged
```

```
                                         frames
eguest-server                            Enable EGuest Server functionality
email-notification                       Email notification configuration
enforce-version                          Check the firmware versions of
                                         devices before interoperating
environmental-sensor                     Environmental Sensors Configuration
events                                   System event messages
export                                   Export a file
file-sync                                File sync between controller and
                                         adoptees
floor                                    Set the floor within a area where
                                         the system is located
gre                                      GRE protocol
http-analyze                             Specify HTTP-Analysis configuration
interface                                Select an interface to configure
ip                                       Internet Protocol (IP)
ipv6                                     Internet Protocol version 6 (IPv6)
l2tpv3                                   L2tpv3 protocol
l3e-lite-table                           L3e lite Table
led                                      Turn LEDs on/off on the device
led-timeout                              Configure the time for the led to
                                         turn off after the last radio state
                                         change
legacy-auto-downgrade                    Enable device firmware to auto
                                         downgrade when other legacy devices
                                         are detected
legacy-auto-update                       Auto upgrade of legacy devices
lldp                                     Link Layer Discovery Protocol
load-balancing                           Configure load balancing parameter
logging                                  Modify message logging facilities
mac-address-table                        MAC Address Table
mac-auth                                 802.1X
management-server                        Configure management server address
memory-profile                           Memory profile to be used on the
                                         device
meshpoint-device                         Configure meshpoint device
                                         parameters
meshpoint-monitor-interval               Configure meshpoint monitoring
                                         interval
min-misconfiguration-recovery-time       Check controller connectivity after
                                         configuration is received
mint                                     MiNT protocol
misconfiguration-recovery-time           Check controller connectivity after
                                         configuration is received
neighbor-inactivity-timeout              Configure neighbor inactivity
                                         timeout
neighbor-info-interval                   Configure neighbor information
                                         exchange interval
no                                       Negate a command or set its
                                         defaults
noc                                      Configure the noc related setting
nsight                                   NSight
ntp                                      Ntp server WORD
offline-duration                         Set duration for which a device
                                         remains unadopted before it
                                         generates offline event
otls                                     Omnitrail Location Server
power-config                             Configure power mode
preferred-controller-group               Controller group this system will
                                         prefer for adoption
preferred-tunnel-controller              Tunnel Controller Name this system
                                         will prefer for tunneling extended
                                         vlan traffic
radius                                   Configure device-level radius
                                         authentication parameters
raid                                     RAID
remove-override                          Remove configuration item override
                                         from the device (so profile value
```

```
                                                takes effect)
  rf-domain-manager                             RF Domain Manager
  router                                        Dynamic routing
  slot                                          PCI expansion Slot
  spanning-tree                                 Spanning tree
  traffic-class-mapping                         Configure IPv6 traffic class to
                                                802.1p priority mapping for
                                                untagged frames
  traffic-shape                                 Traffic shaping
  trustpoint                                    Assign a trustpoint to a service
  tunnel-controller                             Tunnel Controller group this
                                                controller belongs to
  use                                           Set setting to use
  vrrp                                          VRRP configuration
  vrrp-state-check                              Publish interface via OSPF/BGP only
                                                if the interface VRRP state is not
                                                BACKUP
  wep-shared-key-auth                           Enable support for 802.11 WEP
                                                shared key authentication
  zone                                          Configure Zone name

  clrscr                                        Clears the display screen
  commit                                        Commit all changes made in this
                                                session
  do                                            Run commands from Exec mode
  end                                           End current mode and change to EXEC
                                                mode
  exit                                          End current mode and down to
                                                previous mode
  help                                          Description of the interactive help
                                                system
  revert                                        Revert changes
  service                                       Service Commands
  show                                          Show running system information
  write                                         Write running configuration to
                                                memory or terminal

<DEVICE>(config-profile-<PROFILE-NAME>)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes a profile and its associated configurations |

**NOTE:** For more information on profiles and how to configure profiles, see *Chapter 7, PROFILES*.

## 4.1.73 radio-qos-policy

*Global Configuration Commands*

Configures a radio *quality-of-service* (QoS) policy

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
radio-qos-policy <RADIO-QOS-POLICY-NAME>
```

**Parameters**

- `radio-qos-policy <RADIO-QOS-POLICY-NAME>`

| | |
|---|---|
| <RADIO-QOS-POLICY-NAME> | Specify the radio QoS policy name. If the policy does not exist, it is created. |

**Example**

```
rfs6000-81742D(config)#radio-qos-policy test
rfs6000-81742D(config-radio-qos-test)#?
Radio QoS Mode commands:
  accelerated-multicast  Configure multicast streams for acceleration
  admission-control      Configure admission-control on this radio for one or
                         more access categories
  no                     Negate a command or set its defaults
  smart-aggregation      Configure smart aggregation parameters
  wmm                    Configure 802.11e/Wireless MultiMedia parameters

  clrscr                 Clears the display screen
  commit                 Commit all changes made in this session
  do                     Run commands from Exec mode
  end                    End current mode and change to EXEC mode
  exit                   End current mode and down to previous mode
  help                   Description of the interactive help system
  revert                 Revert changes
  service                Service Commands
  show                   Show running system information
  write                  Write running configuration to memory or terminal

rfs6000-81742D(config-radio-qos-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing Radio QoS policy |

**NOTE:** For more information on radio qos policy, see *Chapter 17, RADIO-QOS-POLICY*.

## 4.1.74 radius-group

*Global Configuration Commands*

Configures RADIUS user group parameters

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
radius-group <RADIUS-GROUP-NAME>
```

**Parameters**

- `radius-group <RADIUS-GROUP-NAME>`

| | |
|---|---|
| <RADIUS-GROUP-NAME> | Specify a RADIUS user group name. The name should not exceed 64 characters. If the RADIUS user group does not exist, it is created. |

**Example**

```
rfs6000-81742D(config)#radius-group testgroup
rfs6000-81742D(config-radius-group-testgroup)#?
Radius user group configuration commands:
  guest       Make this group a Guest group
  no          Negate a command or set its defaults
  policy      Radius group access policy configuration
  rate-limit  Set rate limit for group

  clrscr      Clears the display screen
  commit      Commit all changes made in this session
  do          Run commands from Exec mode
  end         End current mode and change to EXEC mode
  exit        End current mode and down to previous mode
  help        Description of the interactive help system
  revert      Revert changes
  service     Service Commands
  show        Show running system information
  write       Write running configuration to memory or terminal

rfs6000-81742D(config-radius-group-testgroup)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing RADIUS group |

**NOTE:** For more information on RADIUS user group commands, see *Chapter 16, RADIUS-POLICY*.

## 4.1.75 radius-server-policy

*Global Configuration Commands*

Creates an onboard device RADIUS policy

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
radius-server-policy <RADIUS-SERVER-POLICY-NAME>
```

**Parameters**

- `radius-server-policy <RADIUS-SERVER-POLICY-NAME>`

| | |
|---|---|
| <RADIUS-SERVER-POLICY-NAME> | Specify the RADIUS server policy name. If the policy does not exist, it is created. |

**Example**

```
rfs6000-81742D(config)#radius-server-policy testpolicy
rfs6000-81742D(config-radius-server-policy-testpolicy)#?
Radius Configuration commands:
  authentication           Radius authentication
  bypass                   Bypass Certificate Revocation List( CRL ) check
  chase-referral           Enable chasing referrals from LDAP server
  crl-check                Enable Certificate Revocation List( CRL ) check
  ldap-agent               LDAP Agent configuration parameters
  ldap-group-verification  Enable LDAP Group Verification setting
  ldap-server              LDAP server parameters
  local                    RADIUS local realm
  nas                      RADIUS client
  no                       Negate a command or set its defaults
  proxy                    RADIUS proxy server
  session-resumption       Enable session resumption/fast reauthentication by
                           using cached attributes
  termination              Enable Eap termination for proxy requests
  use                      Set setting to use

  clrscr                   Clears the display screen
  commit                   Commit all changes made in this session
  do                       Run commands from Exec mode
  end                      End current mode and change to EXEC mode
  exit                     End current mode and down to previous mode
  help                     Description of the interactive help system
  revert                   Revert changes
  service                  Service Commands
  show                     Show running system information
  write                    Write running configuration to memory or terminal

rfs6000-81742D(config-radius-server-policy-testpolicy)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing RADIUS server policy |

**NOTE:** For more information on RADIUS server policy commands, see *Chapter 16, RADIUS-POLICY*.

## 4.1.76 radius-user-pool-policy

*Global Configuration Commands*

Configures a RADIUS user pool

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
radius-user-pool-policy <RADIUS-USER-POOL-POLICY-NAME>
```

**Parameters**

- `radius-user-pool-policy <RADIUS-USER-POOL-POLICY-NAME>`

| | |
|---|---|
| <RADIUS-USER-POOL-POLICY-NAME> | Specify the RADIUS user pool policy name. If the policy does not exist, it is created. |

**Example**

```
rfs6000-81742D(config)#radius-user-pool-policy testpool
rfs6000-81742D(config-radius-user-pool-testpool)#?
Radius User Pool Mode commands:
  duration  Set a guest user's access duration
  no        Negate a command or set its defaults
  user      Radius user configuration

  clrscr    Clears the display screen
  commit    Commit all changes made in this session
  do        Run commands from Exec mode
  end       End current mode and change to EXEC mode
  exit      End current mode and down to previous mode
  help      Description of the interactive help system
  revert    Revert changes
  service   Service Commands
  show      Show running system information
  write     Write running configuration to memory or terminal

rfs6000-81742D(config-radius-user-pool-testpool)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing RADIUS user pool |

**NOTE:** For more information on RADIUS user group commands, see *Chapter 16, RADIUS-POLICY*.

## 4.1.77 rename

*Global Configuration Commands*

Renames and existing TLO

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
rename tlo <TLO-NAME>
```

**Parameters**

- `rename tlo <TLO-NAME> <NEW-TLO-NAME>`

| | |
|---|---|
| rename tlo <TLO-NAME> <NEW-TLO-NAME> | Renames an existing TLO object<br>• <TLO-NAME> – Specify the TLO's name. This is the TLO that is to be renamed.<br>• <NEW-TLO-NAME> – Specify the new name for this TLO |

**Example**

The following example shows the top level objects available for renaming:

Enter rename and press Tab to list top level objects available for renaming.

```
nx9500-6C8809(config)#rename
aaa_policy                          aaa_tacacs_policy
address_range_alias                 aif_policy
ap300                               app_group
app_policy                          application
assoc_acl                           auto_provisioning_policy
bgp_as_path_list                    bgp_community_list
bgp_extcommunity_list               bgp_ip_access_list
bgp_ip_prefix_list                  bonjour_gw_discovery_policy
bonjour_gw_forwarding_policy        bonjour_gw_query_forwarding_policy
bridging_policy                     captive_portal
centro_policy                       client_identity
client_identity_group               content_cache_policy
content_filter_policy               crypto_cmp_policy
database_client_policy              database_policy
device_categorization               dhcp_server_policy
dhcpv6_server_policy                dns_whitelist
dr_route_map                        encrypted_string_alias
event_system_policy                 ex3500_ext_ip_acl
ex3500_management_policy            ex3500_qos_class_map_policy
ex3500_qos_policy_map               ex3500_std_ip_acl
ex3500_time_range                   firewall_policy
global_assoc_list                   guest_management
hashed_string_alias                 host_alias
ip_acl                              ip_snmp_acl
ipv6_acl                            ipv6_radv_policy
l2tpv3_policy                       mac_acl
management_policy                   meshpoint
meshpoint_qos                       mint_policy
mint_security_policy                nac_list

--More--
nx9500-6C8809(config)#
```

The following examples first clones the existing IP access list BROADCAST-MULTICAST-CONTROL, and then renames the cloned IP access list:

```
nx9500-6C8809(config)#show context include-factory | include ip access-list
ip access-list BROADCAST-MULTICAST-CONTROL
nx9500-6C8809(config)#

nx9500-6C8809(config)#clone ip_acl BROADCAST-MULTICAST-CONTROL Test_IP_CLONED
nx9500-6C8809(config)#commit

nx9500-6C8809(config)#show context include-factory | include ip access-list
ip access-list BROADCAST-MULTICAST-CONTROL
ip access-list Test_IP_CLONED
nx9500-6C8809(config)#

rfs4000-229D58(config)#rename ip_acl TestIP_CLONED TestIP_RENAMED
rfs4000-229D58(config)#commit

nx9500-6C8809(config)#rename ip_acl Test_IP_CLONED Test_IP_RENAMED
nx9500-6C8809(config)#

nx9500-6C8809(config)#show context include-factory | include ip access-list
ip access-list BROADCAST-MULTICAST-CONTROL
ip access-list Test_IP_RENAMED
nx9500-6C8809(config)#
```

**Related Commands**

| | |
|---|---|
| *clone* | Creates a replica of an existing TLO or device |

## 4.1.78 replace

*Global Configuration Commands*

Selects an existing device by its MAC address or hostname and replaces it with a new device having a different MAC address. Internally, a new device is created with the new MAC address. The old device's configuration is copied to the new device, and then removed from the controller's configuration (i.e., the old device's configuration is no longer staged on the controller).

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
replace device [<MAC-ADDRESS>|<HOSTNAME>] <NEW-MAC-ADDRESS>
```

**Parameters**

- `replace device [<MAC-ADDRESS>|<HOSTNAME>] <NEW-MAC-ADDRESS>`

| | |
|---|---|
| replace device | Replaces an existing device with a new device, such that the old device's configuration is copied on to the new device |
| [<MAC-ADDRESS>\|<HOSTNAME>] | Identifies the device to replace by its MAC address or hostname<br>• <MAC-ADDRESS> – Identifies the device to replace by its MAC address. Specify the device's existing MAC address.<br>• <HOSTNAME> – Identifies the device to replace by its hostname. Specify the device's hostname. |
| <NEW-MAC-ADDRESS> | Specifies the new device's MAC address<br>Both the new and old devices should of the same model type. |

**Example**

```
rfs4000-882A17(config)#replace device ap7131-4BF364 ?
  AA-BB-CC-DD-EE-FF New device MAC address
rfs4000-882A17(config)#replace device ap7131-4BF364 00-15-0F-BB-98-30
```

The following example shows an existing AP7502 (MAC: DD-AA-BB-88-12-43) configuration staged on a VX9000 controller:

```
VX9000-NOC-DE9D(config-device-DD-AA-BB-88-12-43)#show context
ap7502 DD-AA-BB-88-12-43
 use profile default-ap7502
 use rf-domain default
 hostname ap7502-881243
 interface radio1
  wlan theMOZART bss 1 primary
 interface radio2
  wlan theMOZART bss 1 primary
 interface ge1
  switchport mode access
  switchport access vlan 1
 controller host 12.12.12.2
VX9000-NOC-DE9D(config-device-DD-AA-BB-88-12-43)#
```

The following example shows AP7502 (MAC: DD-AA-BB-88-12-43) replaced by another AP7502 having MAC address 11-22-33-44-55-66:

Note that the new AP7502 device has the same configuration as the old AP7502 device. The HOSTNAME remains the same. Consequently, objects that refer to this particular hostname need not be updated. For example, an hostname alias identifying this particular device, and TLOs using this alias, such as IP/MAC ACLs, remain unchanged.

```
VX9000-NOC-DE9D(config)#replace device DD-AA-BB-88-12-43 11-22-33-44-55-66
VX9000-NOC-DE9D(config)#ap7502 11-22-33-44-55-66
VX9000-NOC-DE9D(config-device-11-22-33-44-55-66)#show context
ap7502 11-22-33-44-55-66
 use profile default-ap7502
 use rf-domain default
 hostname ap7502-881243
 interface radio1
  wlan theMOZART bss 1 primary
 interface radio2
  wlan theMOZART bss 1 primary
 interface ge1
  switchport mode access
  switchport access vlan 1
 controller host 12.12.12.2
VX9000-NOC-DE9D(config-device-11-22-33-44-55-66)#
```

## 4.1.79 rf-domain

*Global Configuration Commands*

An RF Domain groups devices that can logically belong to one network.

The following table lists the RF Domain configuration mode commands:

**Table 4.43** *RF-Domain Config Commands*

| Command | Description | Reference |
|---|---|---|
| *rf-domain* | Creates a RF Domain policy and enters its configuration mode | *page 4-367* |
| *rf-domain-mode commands* | Invokes RF Domain configuration mode commands | *page 4-369* |

### 4.1.79.1 rf-domain

*rf-domain*

Creates an RF Domain or enters the RF Domain configuration context for one or more RF Domains. If the RF Domain does not exist, it is created.

The configuration of controllers (wireless controllers, service platforms, and access points) comprises of RF Domains that define regulatory, location, and other relevant policies. At least one default RF Domain is assigned to each controller. RF Domains allow administrators to assign configuration data to multiple devices deployed in a common coverage area, such as in a floor, building, or site. Each RF Domain contains policies that set the Smart RF or WIPS configuration.

RF Domains also enable administrators to override WLAN SSID name and VLAN assignments. This enables the deployment of a global WLAN across multiple sites and unique SSID name or VLAN assignments to groups of access points servicing the global WLAN. This WLAN override eliminates the need to define and manage a large number of individual WLANs and profiles.

A controller's configuration contains:

- A default RF Domain - Each controller utilizes a default RF Domain. Access Points are assigned to this default RF Domain as they are discovered by the controller. A default RF Domain can be used for single-site and multi-site deployments.
- Single-site deployment – The default RF Domain can be used for single site deployments, where regional, regulatory, and RF policies are common between devices.
- Multi-site deployment – A default RF Domain can omit configuration parameters to prohibit regulatory configuration from automatically being inherited by devices as they are discovered. This is desirable in multi-site deployments with devices spanning multiple countries. Omitting specific configuration parameters eliminates the risk of an incorrect country code from being automatically assigned to a device.
- A user-defined RF Domain - Created by administrators. A user-defined RF Domain can be assigned to multiple devices manually or automatically.
- Manually assigned – Use the CLI or UI to manually assign a user-defined RF Domain to controllers and service platforms.
- Automatically assigned – Use a AP provisioning policy to automatically assign specific RF Domains to access points based on the access point's model, serial number, VLAN, DHCP option, and IP address or MAC address. Automatic RF Domain assignments are useful in large deployments, as they enable plug-n-play access point deployments by automatically applying RF Domains to remote access points. For more information on auto provisioning policy, see *AUTO-PROVISIONING-POLICY*.

Configure and deploy user-defined RF Domains for single or multiple sites where devices require unique regulatory and regional configurations, or unique Smart RF and WIPS policies. User-defined RF Domains can be used to:

- Assign unique Smart RF or WIPS policies to access points deployed on different floors or buildings within in a site.
- Assign unique regional or regulatory configurations to devices deployed in different states or countries.
- Assign unique WLAN SSIDs and/or VLAN IDs to sites assigned a common WLAN without having to define individual WLANs for each site.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
rf-domain {<RF-DOMAIN-NAME>|containing <RF-DOMAIN-NAME>}
```

**Parameters**

- `rf-domain {<RF-DOMAIN-NAME>|containing <RF-DOMAIN-NAME>}`

| | |
|---|---|
| rf-domain | Creates a new RF Domain or enters its configuration context |
| <RF-DOMAIN-NAME> | Optional. Specify the RF Domain name (should not exceed 32 characters and should represent the intended purpose). Once created, the name cannot be edited. |
| containing <RF-DOMAIN-NAME> | Optional. Identifies an existing RF Domain that contains a specified sub-string in the domain name<br>• <RF-DOMAIN-NAME> – Specify a sub-string of the RF Domain name. |

**Example**

```
rfs6000-81742D(config)#rf-domain rfs6000
rfs6000-81742D(config-rf-domain-rfs6000)#?
RF Domain Mode commands:
  alias               Alias
  channel-list        Configure channel list to be advertised to wireless
                      clients
  contact             Configure the contact
  control-vlan        VLAN for control traffic on this RF Domain
  controller-managed  RF Domain manager for this domain will be an adopting
                      controller
  country-code        Configure the country of operation
  geo-coordinates     Configure geo coordinates for this device
  layout              Configure layout
  location            Configure the location
  location-server     LSENSE server configuration
  mac-name            Configure MAC address to name mappings
  no                  Negate a command or set its defaults
  nsight-sensor       Enable sensor for Nsight
  override-smartrf    Configured RF Domain level overrides for smart-rf
  override-wlan       Configure RF Domain level overrides for wlan
  sensor-server       AirDefense sensor server configuration
  stats               Configure the stats related setting
  timezone            Configure the timezone
  tree-node           Configure tree node under which this rf-domain appears
  use                 Set setting to use

  clrscr              Clears the display screen
  commit              Commit all changes made in this session
  do                  Run commands from Exec mode
  end                 End current mode and change to EXEC mode
  exit                End current mode and down to previous mode
  help                Description of the interactive help system
  revert              Revert changes
  service             Service Commands
  show                Show running system information
  write               Write running configuration to memory or terminal
rfs6000-81742D(config-rf-domain-rfs6000)#
```

### 4.1.79.2 rf-domain-mode commands

*rf-domain*

This section describes the default commands under RF Domain.

The following table summarizes RF Domain configuration commands:

**Table 4.44** *RF-Domain-Mode Commands*

| Command | Description | Reference |
|---|---|---|
| *alias* | Creates various types of aliases, such as network, VLAN, network-group, network-service, encrypted-string, hashed -string, etc. at the RF Domain level | *page 4-370* |
| *channel-list* | Configures the channel list advertised by radios | *page 4-377* |
| *contact* | Configures network administrator's contact information (needed in case of any problems impacting the RF Domain) | *page 4-378* |
| *control-vlan* | Configures VLAN for traffic control on a RF Domain | *page 4-379* |
| *controller-managed* | Configures the adopting controller or service platform as this RF Domain's manager | *page 4-380* |
| *country-code* | Configures the country of operation | *page 4-381* |
| *geo-coordinates* | Configures the longitude and latitude of the RF Domain in order to fix its exact geographical location on a map | *page 4-382* |
| *layout* | Configures layout information | *page 4-383* |
| *location* | Configures the physical location of a RF Domain | *page 4-385* |
| *location-server* | Configures an LSENSE server on the selected RF Domain. This command is supported only on the NX95XX series service platforms. | *page 4-386* |
| *mac-name* | Maps MAC addresses to names | *page 4-387* |
| *no* | Negates a command or reverts configured settings to their default | *page 4-388* |
| *override-smart-rf* | Configures RF Domain level overrides for Smart RF | *page 4-390* |
| *override-wlan* | Configures RF Domain level overrides for a WLAN | *page 4-391* |
| *sensor-server* | Configures an AirDefense sensor server on this RF Domain | *page 4-394* |
| *stats* | Configures stats related settings on this RF Domain. These settings define how RF Domain statistics are updated. | *page 4-396* |
| *timezone* | Configures a RF Domain's geographic time zone | *page 4-397* |
| *tree-node* | Configures the hierarchical (tree-node) structure under which this RF Domain appears | *page 4-399* |
| *use* | Enables the use of a specified Smart RF and/or WIPS policy | *page 4-401* |

### 4.1.79.2.1 alias

*rf-domain-mode commands*

Configures network, VLAN, host, string, network-service, etc. aliases at the RF Domain level

For information on aliases, see *alias*.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
alias [address-range|encrypted-string|hashed-string|host|network|network-group|
network-service|number|string|vlan]

alias encrypted-string <ENCRYPTED-STRING-ALIAS-NAME> [0|2] <LINE>

alias hashed-string <HASHED-STRING-ALIAS-NAME> 1 <LINE>

alias address-range <ADDRESS-RANGE-ALIAS-NAME> <STARTING-IP> to <ENDING-IP>

alias host <HOST-ALIAS-NAME> <HOST-IP>

alias network <NETWORK-ALIAS-NAME> <NETWORK-ADDRESS/MASK>

alias network-group <NETWORK-GROUP-ALIAS-NAME> [address-range|host|network]
alias network-group <NETWORK-GROUP-ALIAS-NAME> [address-range <STARTING-IP> to
<ENDING-IP> {<STARTING-IP> to <ENDING-IP>}|host <HOST-IP> {<HOST-IP>}|
network <NETWORK-ADDRESS/MASK> {<NETWORK-ADDRESS/MASK>}]

alias network-service <NETWORK-SERVICE-ALIAS-NAME> proto [<0-254>|<WORD>|eigrp|
gre|igmp|igp|ospf|vrrp] {(<1-65535>|<WORD>|bgp|dns|ftp|ftp-data|gopher|https|
ldap|nntp|ntp|pop3|proto|sip|smtp|sourceport|ssh|telnet|tftp|www)}

alias number <NUMBER-ALIAS-NAME> <0-4294967295>

alias network-service <NETWORK-SERVICE-ALIAS-NAME> proto [<0-254>|<WORD>|eigrp|
gre|igmp|igp|ospf|vrrp] {(<1-65535>|<WORD>|bgp|dns|ftp|ftp-data|gopher|https|
ldap|nntp|ntp|pop3|proto|sip|smtp|sourceport [<1-65535>|<WORD>]|ssh|telnet|
tftp|www)}

alias string <STRING-ALIAS-NAME> <LINE>

alias vlan <VLAN-ALIAS-NAME> <1-4094>
```

**Parameters**

- `alias address-range <ADDRESS-RANGE-ALIAS-NAME> <STARTING-IP> to <ENDING-IP>`

| | |
|---|---|
| address-range <ADDRESS-RANGE-ALIAS-NAME> | Creates a new address-range alias for this RF Domain. Or associates an existing address-range alias with this RF Domain. An address-range alias maps a name to a range of IP addresses.<br>• <ADDRESS-RANGE-ALIAS-NAME> – Specify the address range alias name.<br>Alias name should begin with '$'. |

| | |
|---|---|
| <STARTING-IP> to <ENDING-IP> | Associates a range of IP addresses with this address range alias<br>• <STARTING-IP> – Specify the first IP address in the range.<br>• to <ENDING-IP> – Specify the last IP address in the range.<br>Aliases defined at any given level can be overridden at the next lower level. For example, a global alias can be redefined on a selected set of RF Domains, profiles, or devices. Overrides applied at the device level take precedence. |

- `alias encrypted-string <ENCRYPTED-STRING-ALIAS-NAME> [0|2] <LINE>`

| | |
|---|---|
| encrypted-string <ENCRYPTED-STRING-ALIAS-NAME> | Creates an alias for an encrypted string. Use this alias for string configuration values that are encrypted when "password-encryption" is enabled. For example, in the management-policy, use it to define the SNMP community string. For more information, see *snmp-server*.<br>• <ENCRYPTED-STRING-ALIAS-NAME> – Specify the encrypted-string alias name.<br>Alias name should begin with '$'. |
| [0\|2] <LINE> | Configures the value associated with the alias name specified in the previous step<br>• [0\|2] <LINE> – Configures the alias value<br>Note, if password-encryption is enabled, in the *show > running-config* output, this clear text is displayed as an encrypted string, as shown below:<br>`nx9500-6C8809(config)#show running-config`<br>`!.............................`<br>`alias encrypted-string $enString 2`<br>`fABMK2is7UToNiZE3MQXbgAAAAxB0ZIysdqsEJwr6AH/Da//`<br>`!`<br>`--More--`<br>`nx9500-6C8809`<br>In the above output, the '2' displayed before the encrypted-string alias value indicates that the displayed text is encrypted and not a clear text.<br>However, if password-encryption is disabled the clear text is displayed as is:<br>`nx9500-6C8809(config)#show running-config`<br>`!.............................`<br>`!`<br>`alias encrypted-string $enString 0 test11223344`<br>`!`<br>`--More--`<br>`nx9500-6C8809`<br>For more information on enabling password-encryption, see *password-encryption*. |

- `alias hashed-string <HASHED-STRING-ALIAS-NAME> <LINE>`

| | |
|---|---|
| hashed-string <HASHED-STRING-ALIAS-NAME> | Creates an alias for a hashed string. Use this alias for configuration values that are hashed string, such as passwords. For example, in the management-policy, use it to define the privilege mode password. For more information, see *privilege-mode-password*.<br>• <HASHED-STRING-ALIAS-NAME> – Specify the hashed-string alias name.<br>Alias name should begin with '$'. |

| | |
|---|---|
| <LINE> | Configures the hashed-string value associated with this alias.<br>`nx9500-6C8809(config)#show running-config`<br>`!`<br>`alias encrypted-string $WRITE 2 sBqVCDAoxs3oByF5PCSuFAAAAAd7HT2+EiT/l/BXm9c4SBDv`<br>`!`<br>`alias hashed-string $PriMode 1 faffdde27cb49ad634ea20df4f7c8ef2685894d10ffcb1b2efba054112ecfc75`<br>`--More--`<br>`nx9500-6C8809`<br>In the above *show > running-config* output, the '1' displayed before the hashed-string alias value indicates that the displayed text is hashed and not a clear text. |

- `alias host <HOST-ALIAS-NAME> <HOST-IP>`

| | |
|---|---|
| host <HOST-ALIAS-NAME> | Creates a host alias for this RF Domain. Or associates an existing host alias with this RF Domain. A host alias maps a name to a single network host.<br>• <HOST-ALIAS-NAME> – Specify the host alias name.<br>Alias name should begin with '$'. |
| <HOST-IP> | Associates the network host's IP address with this host alias<br>• <HOST-IP> – Specify the network host's IP address.<br>Aliases defined at any given level can be overridden at the next lower levels. For example, a global alias can be redefined on a selected set of RF Domains, profiles, or devices. Overrides applied at the device level take precedence. |

- `alias network <NETWORK-ALIAS-NAME> <NETWORK-ADDRESS/MASK>`

| | |
|---|---|
| network <NETWORK-ALIAS-NAME> | Creates a network alias for this RF Domain. Or associates an existing network alias with this RF Domain. A network alias maps a name to a single network address.<br>• <NETWORK-ALIAS-NAME> – Specify the network alias name.<br>Alias name should begin with '$'. |
| <NETWORK-ADDRESS/MASK> | Associates a single network with this network alias<br>• <NETWORK-ADDRESS/MASK> – Specify the network's address and mask.<br>Aliases defined at any given level can be overridden at the next lower levels. For example, a global alias can be redefined on a selected set of RF Domains, profiles, or devices. Overrides applied at the device level take precedence. |

- `alias network-group <NETWORK-GROUP-ALIAS-NAME> [address-range <STARTING-IP> to <ENDING-IP> {<STARTING-IP> to <ENDING-IP>}|host <HOST-IP> {<HOST-IP>}| network <NETWORK-ADDRESS/MASK> {<NETWORK-ADDRESS/MASK>}]`

| | |
|---|---|
| network-group <NETWORK-GROUP-ALIAS-NAME> | Creates a network-group alias for this RF Domain. Or associates an existing network-group alias with this RF Domain.<br>• <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name.<br>Alias name should begin with '$'.<br>Contd.. |

| | |
|---|---|
| | After specifying the name, specify the following: a range of IP addresses, host addresses, or a range of network addresses.<br>Aliases defined at any given level can be overridden at the next lower levels. For example, a global alias can be redefined on a selected set of RF Domains, profiles, or devices. Overrides applied at the device level take precedence. |
| address-range <STARTING-IP> to <ENDING-IP> {<STARTING-IP> to <ENDING-IP>} | Associates a range of IP addresses with this network-group alias<br>• <STARTING-IP> – Specify the first IP address in the range.<br>• to <ENDING-IP> – Specify the last IP address in the range.<br>• <STARTING-IP> to <ENDING-IP> – Optional. Specifies more than one range of IP addresses. A maximum of eight (8) IP address ranges can be configured. |
| host <HOST-IP> {<HOST-IP>} | Associates a single or multiple hosts with this network-group alias<br>• <HOST-IP> – Specify the hosts' IP address.<br>• <HOST-IP> – Optional. Specifies more than one host. A maximum of eight (8) hosts can be configured. |
| network <NETWORK-ADDRESS/MASK> {<NETWORK-ADDRESS/MASK>} | Associates a single or multiple networks with this network-group alias<br>• <NETWORK-ADDRESS/MASK> – Specify the network's address and mask.<br>• <NETWORK-ADDRESS/MASK> – Optional. Specifies more than one network. A maximum of eight (8) networks can be configured. |

• `alias network-service <NETWORK-SERVICE-ALIAS-NAME> proto [<0-254>|<WORD>|eigrp|gre|igmp|igp|ospf|vrrp] {(<1-65535>|<WORD>|bgp|dns|ftp|ftp-data|gopher|https|ldap|nntp|ntp|pop3|proto|sip|smtp|sourceport [<1-65535>|<WORD>]|ssh|telnet|tftp|www)}`

| | |
|---|---|
| alias network-service <NETWORK-SERVICE-ALIAS-NAME> | Creates a network-service alias for this RF Domain. Or associates an existing network-service alias with this RF Domain. A network-service alias maps a name to network services and the corresponding source and destination software ports.<br>• <NETWORK-SERVICE-ALIAS-NAME> – Specify a network-service alias name.<br>Alias name should begin with '$'.<br>Aliases defined at any given level can be overridden at the next lower levels. For example, a global alias can be redefined on a selected set of RF Domains, profiles, or devices. Overrides applied at the device level take precedence. |
| proto [<0-254>\|<WORD>\|eigrp\|gre\|igmp\|igp\|ospf\|vrrp] | Use one of the following options to associate an Internet protocol with this network-service alias:<br>• <0-254> – Identifies the protocol by its number. Specify the protocol number from 0 - 254. This is the number by which the protocol is identified in the *Protocol* field of the IPv4 header and the *Next Header* field of IPv6 header. For example, the *User Datagram Protocol's* (UDP) designated number is 17.<br>• <WORD> – Identifies the protocol by its name. Specify the protocol name.<br>• eigrp – Selects *Enhanced Interior Gateway Routing Protocol* (EIGRP). The protocol number 88.<br>• gre – Selects *Generic Routing Encapsulation* (GRE). The protocol number is 47.<br>• igmp – Selects *Internet Group Management Protocol* (IGMP). The protocol number is 2.<br>• igp – Selects *Interior Gateway Protocol* (IGP). The protocol number is 9.<br>• ospf – Selects *Open Shortest Path First* (OSPF). The protocol number is 89.<br>• vrrp – Selects *Virtual Router Redundancy Protocol* (VRRP). The protocol number is 112. |

| | |
|---|---|
| {(<1-65535>\|<WORD>\|bgp\|dns\|ftp\|ftp-data\|gopher\|https\|ldap\|nntp\|ntp\|pop3\|proto\|sip\|smtp\|sourceport [<1-65535>\|<WORD>]\|ssh\|telnet\|tftp\|www)} | After specifying the protocol, you may configure a destination port for this service. These keywords are recursive and you can configure multiple protocols and associate multiple destination and source ports.<br>• <1-65535> – Optional. Configures a destination port number from 1 - 65535<br>• <WORD> – Optional. Identifies the destination port by the service name provided. For example, the *secure shell* (SSH) service uses TCP port 22.<br>• bgp – Optional. Configures the default *Border Gateway Protocol* (BGP) services port (179)<br>• dns – Optional. Configures the default *Domain Name System* (DNS) services port (53)<br>• ftp – Optional. Configures the default *File Transfer Protocol* (FTP) control services port (21)<br>• ftp-data – Optional. Configures the default FTP data services port (20)<br>• gopher – Optional. Configures the default gopher services port (70)<br>• https – Optional. Configures the default HTTPS services port (443)<br>• ldap – Optional. Configures the default *Lightweight Directory Access Protocol* (LDAP) services port (389)<br>• nntp – Optional. Configures the default Newsgroup (NNTP) services port (119)<br>• ntp – Optional. Configures the default *Network Time Protocol* (NTP) services port (123)<br>• POP3 – Optional. Configures the default *Post Office Protocol* (POP3) services port (110)<br>• proto – Optional. Use this option to select another Internet protocol in addition to the one selected in the previous step.<br>• sip – Optional. Configures the default *Session Initiation Protocol* (SIP) services port (5060)<br>• smtp – Optional. Configures the default *Simple Mail Transfer Protocol* (SMTP) services port (25)<br>• sourceport [<1-65535>\|<WORD>] – Optional. After specifying the destination port, you may specify a single or range of source ports.<br>  • <1-65535> – Specify the source port from 1 - 65535.<br>  • <WORD> – Specify the source port range, for example 1-10.<br>• ssh – Optional. Configures the default SSH services port (22)<br>• telnet – Optional. Configures the default Telnet services port (23)<br>• tftp – Optional. Configures the default *Trivial File Transfer Protocol* (TFTP) services port (69)<br>• www – Optional. Configures the default HTTP services port (80) |

- `alias number <NUMBER-ALIAS-NAME> <0-4294967295>`

| | |
|---|---|
| alias number <NUMBER-ALIAS-NAME> <0-4294967295> | Creates a new number alias or applies an existing number, identified by the <NUMBER-ALIAS-NAME> keyword,<br>• <NUMBER-ALIAS-NAME> – Specify the number alias name.<br>  • <0-4294967295> – Specify the number, from 0 - 4294967295, assigned to the number alias created.<br>Contd.. |

| | |
|---|---|
| | Number aliases map a name to a numeric value. For example, 'alias number $NUMBER 100'.<br>• The number alias name is: $NUMBER<br>• The value assigned is: 100<br>The value referenced by alias $NUMBER, wherever used, is 100. |

- `alias string <STRING-ALIAS-NAME> <LINE>`

| | |
|---|---|
| alias string <STRING-ALIAS-NAME> | Creates a string alias for this RF Domain. Or associates an existing string alias with this RF Domain. String aliases map a name to an arbitrary string value. For example, 'alias string $DOMAIN test.example_company.com'. In this example, the string alias name is: *$DOMAIN* and the string value it is mapped to is: *test.example_company.com*. In this example, the string alias refers to a domain name.<br>• <STRING-ALIAS-NAME> – Specify the string alias name.<br>• <LINE> – Specify the string value.<br>Alias name should begin with '$'.<br>Aliases defined at any given level can be overridden at the next lower levels. For example, a global alias can be redefined on a selected set of RF Domains, profiles, or devices. Overrides applied at the device level take precedence. |

- `alias vlan <VLAN-ALIAS-NAME> <1-4094>`

| | |
|---|---|
| alias vlan <VLAN-ALIAS-NAME> | Creates a VLAN alias for this RF Domain. Or associates an existing VLAN alias with this RF Domain. A VLAN alias maps a name to a VLAN ID.<br>• <VLAN-ALIAS-NAME> – Specify the VLAN alias name.<br>Alias name should begin with '$'. |
| <1-4094> | Maps the VLAN alias to a VLAN ID<br>• <1-4094> – Specify the VLAN ID from 1 - 4094.<br>Aliases defined at any given level can be overridden at the next lower levels. For example, a global alias can be redefined on a selected set of RF Domains, profiles, or devices. Overrides applied at the device level take precedence. |

**Example**

```
rfs4000-229D58(config)#show context
!
! Configuration of RFS4000 version 5.9.1.0-008B

!
!
version 2.5
!
!
alias network-group $TestNetGrpAlias network 192.168.13.0/24 192.168.16.0/24
alias network-group $TestNetGrpAlias address-range 192.168.13.7 to 192.168.13.16
192.168.13.20 to 192.168.13.25
!
alias network $TestNetworkAlias 192.168.13.0/24
!
alias host $TestHostAlias 192.168.13.10
!
alias address-range $TestAddRanAlias 192.168.13.10 to 192.168.13.13
!
alias network-service $NetworkServAlias proto udp
!
alias network-service $kerberos proto tcp 749 750 80 proto udp 68 sourceport 67
!
```

```
alias vlan $TestVLANAlias 1
--More--
rfs4000-229D58(config)#
```

In the following examples, the global aliases '$kerberos' and '$TestVLANAlias' are associated with the RF Domain 'test' and overrides applied:

```
rfs4000-229D58(config-rf-domain-test)#alias network-service $kerberos proto tcp
749 750 80

rfs4000-229D58(config-rf-domain-test)#alias vlan $TestVLANAlias 10

rfs4000-229D58(config-rf-domain-test)#show context
rf-domain test
 no country-code
 alias network-service $kerberos proto tcp 749 750 80
  alias vlan $TestVLANAlias 10
rfs4000-229D58(config-rf-domain-test)#

nx9500-6C8809(config-rf-domain-test)#alias string $test example_company.com

nx9500-6C8809(config-rf-domain-test)#show context
rf-domain test
 no country-code
 alias string $test example_company.com
nx9500-6C8809(config-rf-domain-test)#
```

**Example 1:**

In the following examples, the network-group alias '$test' is configured to include hosts 192.168.1.10 and 192.168.1.11, networks 192.168.2.0/24 and 192.168.3.0/24 and address-range 192.168.4.10 to 192.168.4.20.

```
rfs4000-229D58(config)#alias network-group $test host 192.168.1.10 192.168.1.11
rfs4000-229D58(config)#alias network-group $test network 192.168.2.0/24
192.168.3.0/24
rfs4000-229D58(config)#alias network-group $test address-range 192.168.4.10 to
192.168.4.20
```

Associate this network-group alias '$test' to the RF Domain 'test' and override the 'host' element of the alias.

```
rfs4000-229D58(config-rf-domain-test)#alias network-group $test host
192.168.10.10
rfs4000-229D58(config-rf-domain-test)#show context
rf-domain test
 no country-code
 alias network-service $kerberos proto tcp 749 750 80
  alias network-group $test host 192.168.10.10
  alias network-group $test network 192.168.2.0/24 192.168.3.0/24
  alias network-group $test address-range 192.168.4.10 to 192.168.4.20
  alias vlan $TestVLANAlias 10
rfs4000-229D58(config-rf-domain-test)#
```

In the preceding example, the 'host' element of the network-group alias '$test' has been overridden. But the 'network' and 'address-range' elements have been retained as is.

**Related Commands**

| | |
|---|---|
| *no* | Removes a network, network-group, network-service, VLAN, or string alias from this RF Domain |

### 4.1.79.2.2 channel-list

*rf-domain-mode commands*

Configures the channel list advertised by radios. This command also enables a dynamic update of a channel list.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
channel-list [2.4GHz|5GHz|dynamic]

channel-list dynamic

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

**Parameters**

- `channel-list dynamic`

| | |
|---|---|
| dynamic | Enables a dynamic update of a channel list |

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

| | |
|---|---|
| 2.4GHz <CHANNEL-LIST> | Configures the channel list advertised by radios operating in the 2.4 GHz mode<br>• <CHANNEL-LIST> – Specify the list of channels separated by commas or hyphens. |
| 5GHz <CHANNEL-LIST> | Configures the channel list advertised by radios operating in the 5.0 GHz mode<br>• <CHANNEL-LIST> – Specify the list of channels separated by commas or hyphens. |

**Example**

```
rfs6000-81742D(config-rf-domain-default)#channel-list 2.4GHz 1-10

rfs6000-81742D(config-rf-domain-default)#show context
rf-domain default
 no country-code
 channel-list 2.4GHz 1,2,3,4,5,6,7,8,9,10
rfs6000-81742D(config-rf-domain-default)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the list of channels configured on the selected RF Domain for 2.4 GHz and 5.0 GHz bands. Also disables dynamic update of a channel list. |

### 4.1.79.2.3 contact

*rf-domain-mode commands*

Configures the network administrator's contact details. The network administrator is responsible for addressing problems impacting the network.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
contact <WORD>
```

**Parameters**

- `contact <WORD>`

| | |
|---|---|
| contact <WORD> | Specify contact details, such as name and number. |

**Example**

```
rfs6000-81742D(config-rf-domain-default)#contact Bob+14082778691

rfs6000-81742D(config-rf-domain-default)#show context
rf-domain default
 contact Bob+14082778691
 no country-code
 channel-list 2.4GHz 1,2,3,4,5,6,7,8,9,10
rfs6000-81742D(config-rf-domain-default)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes a network administrator's contact details |

### 4.1.79.2.4 control-vlan

*rf-domain-mode commands*

Configures the VLAN designated for traffic control in this RF Domain

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
control-vlan [<1-4094>|<VLAN-ALIAS-NAME>]
```

**Parameters**

- `control-vlan [<1-4094>|<VLAN-ALIAS-NAME>]`

| | |
|---|---|
| [<1-4094>\| <VLAN-ALIAS-NAME>] | Specify the VLAN ID from 1 - 4094. Alternately, use a vlan-alias to identify the control VLAN. If using a vlan-alias, ensure that the alias is existing and configured. |

**Example**

```
rfs6000-81742D(config-rf-domain-default)#control-vlan 1

rfs6000-81742D(config-rf-domain-default)#show context
rf-domain default
 contact Bob+14082778691
 no country-code
 channel-list 2.4GHz 1,2,3,4,5,6,7,8,9,10
 control-vlan 1
rfs6000-81742D(config-rf-domain-default)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables the VLAN designated for controlling RF Domain traffic |

### 4.1.79.2.5 controller-managed

*rf-domain-mode commands*

Configures the adopting controller (wireless controller, access point, or service platform) as this RF Domain's manager. In other words, the RF Domain is controller managed, and the managing controller is the device managing the RF Domain.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
controller-managed
```

**Parameters**

None

**Example**

```
rfs4000-229D58(config-rf-domain-test)#controller-managed
rfs4000-229D58(config-rf-domain-test)#commit

rfs4000-229D58(config-rf-domain-test)#show context
rf-domain test
 country-code in
 controller-managed
 network-alias techPubs host 192.168.13.8
 network-alias techPubs address-range 192.168.13.10 to 192.168.13.15
 service-alias testing index 10 proto 9 destination-port range 21 21
rfs4000-229D58(config-rf-domain-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the adopting controller or service platform as this RF Domain's manager |

### 4.1.79.2.6 country-code

*rf-domain-mode commands*

Configures a RF Domain's country of operation. Since device channels transmit in specific channels unique to the country of operation, it is essential to configure the country code correctly or risk using illegal operation.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
country-code <WORD>
```

**Parameters**

- `country-code <WORD>`

| | |
|---|---|
| country-code | Configures the RF Domain's country of operation |
| <WORD> | Specify the two (2) letter ISO-3166 country code. |

**Example**

```
rfs6000-81742D(config-rf-domain-default)#country-code ?
  WORD  The 2 letter ISO-3166 country code
  ae    United Arab Emirates
  ag    Antigua and Barbuda
  ai    Anguilla
  al    Albania
  an    Dutch Antilles
  ar    Argentina
  at    Austria
  au    Australia
  ba    Bosnia-Herzegovina
  bb    Barbados
  bd    Bangladesh
  be    Belgium
  bf    Burkina Faso
--More--
rfs6000-81742D(config-rf-domain-default)#

rfs6000-81742D(config-rf-domain-default)#country-code us

rfs6000-81742D(config-rf-domain-default)#show context
rf-domain default
 contact Bob+14082778691
 country-code us
 channel-list 2.4GHz 1,2,3,4,5,6,7,8,9,10
 control-vlan 1
rfs6000-81742D(config-rf-domain-default)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes or resets this RF Domain's configured country of operation |

### 4.1.79.2.7 geo-coordinates

*rf-domain-mode commands*

Configures the longitude and latitude of the RF Domain in order to fix its exact geographical location on a map. Use this command to define the geographical area where a common set of device configurations are deployed and managed by this RF Domain policy.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
geo-coordinates <-90.0000-90.0000> <-180.0000-180.0000>
```

**Parameters**

- `geo-coordinates <-90.0000-90.0000> <-180.0000-180.0000>`

| | |
|---|---|
| geo-coordinates <-90.0000-90.0000> <-180.0000-180.0000> | Configures the geo-coordinates of this RF Domain<br>• <-90.0000-90.0000> – Specify the latitude from -90.0000 - 90.0000.<br>• -180.0000-180.0000 – Specify the longitude from -180.0000 - 180.0000. |

**Example**

```
nx9500-6C8809(config-rf-domain-TechPubs)#geo-coordinates 12.971599 77.594563

nx9500-6C8809(config-rf-domain-TechPubs)#show context
rf-domain TechPubs
 location Bangalore
 geo-coordinates 12.9716 77.5946
 timezone Asia/Calcutta
 country-code in
 use database-policy default
 use nsight-policy AP-rfd
 control-vlan 1
 controller-managed
 use license WEBF
nx9500-6C8809(config-rf-domain-TechPubs)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes or resets this RF Domain's configured geo-coordinates |

### 4.1.79.2.8 layout

*rf-domain-mode commands*

Configures the RF Domain layout in terms of area, floor, and location on a map. It allows users to place APs across the deployment map. A maximum of 256 layouts is permitted.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
layout [area|description|floor|map-location] {(area|description|floor|map-
location)}

layout [area <AREA-NAME>|description <LINE>|floor <FLOOR-NAME> {<1-4094>}|
map-location <URL> units [feet|meters]] {(area <AREA-NAME>|description <LINE>|
floor <FLOOR-NAME> {<1-4094>}|map-location <URL> units [feet|meters])}
```

**Parameters**

```
• layout [area <AREA-NAME>|description <LINE>|floor <FLOOR-NAME> {<1-4094>}|
map-location <URL> units [feet|meters]] {(area <AREA-NAME>|description <LINE>|
floor <FLOOR-NAME> {<1-4094>}|map-location <URL> units [feet|meters])}
```

| | |
|---|---|
| layout | Configures the RF Domain's layout in terms of area, floor, and location on a map<br>These are recursive parameters and you can configure one or all of these parameters. |
| area <AREA-NAME> | Configures the RF Domain's layout in terms of the area of location<br>• <AREA-NAME> – Specify the area name.<br>After configuring the RF Domain's area of functioning, optionally specify the floor name (and number), description, and/or the location on map. |
| description <LINE> | Configures a description for this RF Domain<br>• <LINE> – Specify a description that enables you to identify the RF Domain. For a multi-worded string, use double quotes. |
| floor <FLOOR-NAME> <1-4094> | Configures the RF Domain's layout in terms of the floor name and number<br>• <FLOOR-NAME> – Specify the floor name.<br>• <1-4094> – Optional. Specifies the floor number from 1 - 4094. The default floor number is 1.<br>After configuring the RF Domain's floor name (and number), optionally specify the area name, description, and/or the location on map. |
| map-location <URL> units [feet\|meters] | Configures the location of the RF Domain on the map<br>• <URL> – Specify the URL to configure the map location.<br>• units [feet\|meters] – Configures the map units. The options are: feet or meters<br>• feet – Configures the map units in terms of feet<br>• meters – Configures the map units in terms of meter<br>After configuring the location of the RF Domain on the map, optionally specify the area name, floor name (and number), and/or description. |

**Example**

```
rfs6000-81742D(config-rf-domain-default)#layout map-location www.firstfloor.com
units meters area HamiltonAve floor Floor1

rfs6000-81742D(config-rf-domain-default)#show context
rf-domain default
 contact Bob+14082778691
 country-code us
 channel-list 2.4GHz 1,2,3,4,5,6,7,8,9,10
 layout area HamiltonAve floor Floor1 map-location www.firstfloor.com units meters
 control-vlan 1
rfs6000-81742D(config-rf-domain-default)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the RF Domain layout details |

### 4.1.79.2.9 location

*rf-domain-mode commands*

Configures the RF Domain's physical location's name. The location could be as specific as the building name or floor number. Or it could be generic and include an entire site. The location defines the physical area where a set of devices with common configurations are deployed and managed by a RF Domain policy.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
location <WORD>
```

**Parameters**

- `location <WORD>`

| | |
|---|---|
| location <WORD> | Configures the RF Domain location by specifying the area or building name<br>• <WORD> – Specify the location. |

**Example**

```
rfs6000-81742D(config-rf-domain-default)#location SanJose

rfs6000-81742D(config-rf-domain-default)#show context
rf-domain default
 location SanJose
 contact Bob+14082778691
 country-code us
 channel-list 2.4GHz 1,2,3,4,5,6,7,8,9,10
 layout area HamiltonAve floor Floor1 map-location www.firstfloor.com units meters
 control-vlan 1
rfs6000-81742D(config-rf-domain-default)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the RF Domain location |

### 4.1.79.2.10 location-server

*rf-domain-mode commands*

Configures the L-Sense server's IP address or hostname on the selected RF Domain. When configured, the AP7522, AP7532, AP7562, AP8432 and AP8533 model access points, within the RF Domain, extract and forward client-location related data to the specified L-Sense server.

L-Sense is a highly scalable indoor locationing platform that gathers location-related analytics, such as visitor trends, peak and off-peak times, dwell time, heat-maps, etc. to enable entrepreneurs deeper visibility at a venue. To enable the location tracking system, the L-Sense server should be up and running and the RF Domain Sensor configuration should point to the L-sense server.

**Supported in the following platforms:**

- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510

**Syntax**

```
location-server 1 ip <LSENSE-SERVER-IP/HOSTNAME> {port [443|<1-65535>]}
```

**Parameters**

- `location-server 1 ip <LSENSE-SERVER-IP/HOSTNAME> {port [443|<1-65535>]}`

| | |
|---|---|
| location-server 1 ip <LSENSE-SERVER-IP/HOSTNAME> | Configures the LSENSE server parameters<br>• 1 – Sets the server ID as 1. As of now only one L-Sense server can be configured.<br>• ip <LSENSE-SERVER-IP/HOSTNAME> – Specify the server's IPv4 address/host-name. This is the L-Sense server designated to receive RSSI scan data from a WiNG dedicated sensor. |
| port [443\|<1-65535>] | Optional. Configures the port where the LSENSE server is reachable. The options are:<br>• 443 – Configures port 443. This is the default setting.<br>• <1-65535> – Alternately, specify a port as the LSENSE server port from 1 - 65535. |

**Example**

```
nx9500-6C8809(config-rf-domain-test)#location-server 1 ip 192.168.13.20 port 200

nx9500-6C8809(config-rf-domain-test)#show context
rf-domain test
 no country-code
 location-server 1 ip 192.168.13.20 port 200
nx9500-6C8809(config-rf-domain-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the LSENSE server configurations |

### 4.1.79.2.11 mac-name

*rf-domain-mode commands*

Configures a relevant name for each MAC address. Use this command to associate client names to specific connected client MAC addresses for improved client management.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
mac-name <MAC> <NAME>
```

**Parameters**

- `mac-name <MAC> <NAME>`

| | |
|---|---|
| mac-name <MAC> <NAME> | Assigns a user-friendly name to this RF Domain's member access point's connected client to assist in its easy recognition<br>• <MAC> – Specify the MAC address<br>• <NAME> – Specify the client name for the specified MAC address. The name specified here will be used in events and statistics. |

**Example**

```
rfs6000-81742D(config-rf-domain-default)#mac-name 11-22-33-44-55-66 TestDevice

rfs6000-81742D(config-rf-domain-default)#show context
rf-domain default
 location SanJose
 contact Bob+14082778691
 country-code us
 channel-list 2.4GHz 1,2,3,4,5,6,7,8,9,10
 mac-name 11-22-33-44-55-66 TestDevice
 layout area Ecospace floor Floor1 map-location www.firstfloor.com units meters
 control-vlan 1
rfs6000-81742D(config-rf-domain-default)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the MAC address to name mapping |

### 4.1.79.2.12 no

*rf-domain-mode commands*

Negates a command or reverts configured settings to their default. When used in the config RF Domain mode, the `no` command negates or reverts

RF Domain settings.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
no [alias|channel-list|contact|control-vlan|controller-managed|country-code|
geo-coordinates|layout|location|location-server|mac-name|nsight-sensor|
override-smartrf|override-wlan|sensor-server|stats|timezone|tree-node|use]

no [adoption-mode|channel-list [2.4GHz|5GHz|dynamic]|contact|control-vlan|
controller-managed|country-code|location|location-server 1|mac-name <MAC>||
nsight-sensor|sensor-server <1-3>|stats update-interval|timezone|tree-node]

no alias [address-range|host|network|network-group [address-range|host|network]|
network-service|number|string|vlan] <ALIAS-NAME>

no layout {(area <AREA-NAME>|floor <FLOOR-NAME>)}

no override-smartrf channel-list [2.4GHz|5GHz]

no override-wlan <WLAN-NAME> [shutdown|ssid|template|vlan-pool [<1-4094>|all]|
wep128 [key <1-3>|transmit-key]|wpa-wpa2-psk]

no use [database-policy|license|nsight-policy|smart-rf-policy|wips-policy]
```

**Parameters**

- `no <PARAMETERS>`

| | |
|---|---|
| no <PARAMETERS> | Removes or reverts this RF Domain's settings based on the parameters passed |

**Example**

The following example shows the default RF Domain settings before the 'no' commands are executed:

```
rfs6000-81742D(config-rf-domain-default)#show context
rf-domain default
 location SanJose
 contact Bob+14082778691
 country-code us
 channel-list 2.4GHz 1,2,3,4,5,6,7,8,9,10
 mac-name 11-22-33-44-55-66 TestDevice
 layout area Ecospace floor Floor1 map-location www.firstfloor.com units meters
 control-vlan 1
rfs6000-81742D(config-rf-domain-default)#

rfs6000-81742D(config-rf-domain-default)#no channel-list 2.4GHz 1-10
rfs6000-81742D(config-rf-domain-default)#no mac-name 11-22-33-44-55-66
rfs6000-81742D(config-rf-domain-default)#no location
rfs6000-81742D(config-rf-domain-default)#no control-vlan
```

The following example shows the default RF Domain settings after the ‘no’ commands are executed:

```
rfs6000-81742D(config-rf-domain-default)#show context
rf-domain default
 contact Bob+14082778691
 country-code us
 layout area Ecospace floor Floor1 map-location www.firstfloor.com units meters
rfs6000-81742D(config-rf-domain-default)#
```

### 4.1.79.2.13 override-smart-rf

*rf-domain-mode commands*

Enables dynamic channel switching for Smart RF radios. This command allows you to configure an override list of channels that Smart RF can use for channel compensations on 2.4 GHz and 5.0 GHz radios.

When a radio fails or is faulty, a Smart RF policy provides automatic recovery by instructing neighboring access points to increase their transmit power to compensate for the coverage loss. Once correct access point placement has been established, Smart-RF can optionally be leveraged for automatic detector radio selection. Smart-RF uses detector radios to monitor RF events and can ensure availability of adequate detector coverage.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

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

**Parameters**

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

| | |
|---|---|
| override-smartrf | Enables dynamic channel switching for Smart RF radios |
| channel-list | Configures a list of channels for 2.4 GHz and 5.0 GHz Smart RF radios |
| 2.4GHz <CHANNEL-LIST> | Selects the 2.4 GHz Smart RF radio channels<br>• <CHANNEL-LIST> – Specify a list of channels separated by commas. |
| 5GHz <CHANNEL-LIST> | Selects the 5.0 GHz Smart RF radio channels<br>• <CHANNEL-LIST> – Specify a list of channels separated by commas. |

**Example**

```
rfs6000-81742D(config-rf-domain-default)#override-smartrf channel-list 2.4GHz
1,2,3

rfs6000-81742D(config-rf-domain-default)#show context
rf-domain default
 contact Bob+14082778691
 country-code us
 override-smartrf channel-list 2.4GHz 1,2,3
 layout area Ecospace floor Floor1 map-location www.firstfloor.com units meters
rfs6000-81742D(config-rf-domain-default)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the override-smartrf list of channels configured for 2.4 GHz and 5.0 GHz radios |

### 4.1.79.2.14 override-wlan

*rf-domain-mode commands*

Configures RF Domain level overrides for a WLAN

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
override-wlan <WLAN-NAME> [shutdown|ssid|template|vlan-pool|wep128|wpa-wpa2-psk]

override-wlan <WLAN-NAME> [shutdown|ssid <SSID>|template <TEMPLATE-NAME>|vlan-
pool <1-4094> {limit <0-8192>}]

override-wlan <WLAN-NAME> wpa-wpa2-psk [0 <WORD>|2 <WORD>]

override-wlan <WLAN-NAME> wep128 [key <1-4> hex [0 <WORD>|2 <WORD>]|transmit-key
<1-4>]
```

**Parameters**

```
• override-wlan <WLAN-NAME> [shutdown|ssid <SSID>|template <TEMPLATE-NAME>|vlan-
pool <1-4094> {limit <0-8192>}]
```

| | |
|---|---|
| <WLAN-NAME> | Configures the WLAN name<br>If applying RF Domain level overrides to an existing WLAN, specify its name. If creating a new WLAN, specify a name not exceeding 32 characters and representing the WLAN's coverage area. After creating the WLAN, configure its override parameters. |
| shutdown | Shuts down WLAN operation on all mapped radios |
| ssid <SSID> | Configures a override SSID associated with this WLAN<br>• <SSID> – Specify the SSID (should not exceed 32 characters in length).<br>Each WLAN provides associated wireless clients with a SSID. This has limitations, because it requires wireless clients to associate with different SSIDs to obtain QoS and security policies. However, a WiNG-managed RF Domain can have WLANs assigned and advertise a single SSID, and yet allow users to inherit different QoS or security policies. |
| template <TEMPLATE-NAME> | Configures a template name for this RF Domain<br>• <TEMPLATE-NAME> – Specify the template name (should not exceed 32 characters in length). |
| vlan-pool <1-4094> {limit <0-8192>} | Configures the override VLANs available to this WLAN<br>• <1-4094> – Specify the VLAN ID from 1 - 4094.<br>• limit <0-8192> – Optional. Sets a limit to the number of users on this VLAN from 0 - 8192. The default is 0.<br>Controllers and service platforms allow the mapping of a WLAN to more than one VLAN. Wireless clients associating with a WLAN are assigned VLANs, from the pool representative of the WLAN, in a way that ensures proper load balancing across VLANs. Clients are tracked per VLAN, and assigned to the least used/loaded VLAN. Client VLAN usage is tracked on a per-WLAN basis. The maximum allowed client limit is 8192 per VLAN. |

- `override-wlan <WLAN-NAME> wpa-wpa2-psk [0 <WORD>|2 <WORD>]`

| | |
|---|---|
| <WLAN-NAME> | Configures the WLAN name<br>If applying RF Domain level overrides to an existing WLAN, specify its name. If creating a new WLAN, specify a name not exceeding 32 characters and representing the WLAN's coverage area. After creating the WLAN, configure its override parameters. |
| wpa-wpa2-psk <PASSPHRASE> | Overrides a WLAN's existing WPA-WPA2 pre-shared key or passphrase at the RF Domain level. WPA2 is a newer 802.11i standard that provides wireless security that is stronger than *Wi-Fi Protected Access* (WPA) and WEP.<br>• <PASSPHRASE> – Specify a WPA-WPA2 key or passphrase. It is an alphanumeric string of 8 to 64 ASCII characters or 64 HEX characters as the primary string, which both the transmitting and receiving authenticators must share in this new override PSK. The alphanumeric string allows character spaces. The string is converted to a numeric value. This passphrase saves the you the necessity of entering the 256-bit key each time keys are generated. |

- `override-wlan <WLAN-NAME> wep128 [key <1-4> hex [0 <WORD>|2 <WORD>]|transmit-key <1-4>]`

| | |
|---|---|
| <WLAN-NAME> | Configures the WLAN name<br>If applying RF Domain level overrides to an existing WLAN, specify its name. If creating a new WLAN, specify a name not exceeding 32 characters and representing the WLAN's coverage area. After creating the WLAN, configure its override parameters. |
| wep128 | Overrides a WLAN's existing WEP128 keys at the RF Domain level (not the profile level). WEP128 uses a 104 bit key, which is concatenated with a 24-bit *initialization vector* (IV) to form the RC4 traffic key. WEP may be all a small-business user needs for the simple encryption of wireless data on the WLAN. However, networks that require more security are at risk from a WEP flaw. WEP is only recommended if there are client devices incapable of using higher forms of security. The existing 802.11 standard alone offers administrators no effective method to update keys. |
| key <1-4> hex [0 <WORD>\| 2 <WORD>] | Configures the WEP128 key.<br>A total of four keys can be configured.<br>• <1-4> – Select the key index from 1- 4.<br>  • hex – Configures a hexadecimal key<br>  • 0 <WORD> – Configures a clear text key<br>  • 2 <WORD> – Configures an encrypted key<br>The following parameter is common to both clear-text and encrypted key options:<br>• <WORD> – Specify the WEP128/Keyguard key (should not exceed 26 hexadecimal characters in length). |
| transmit-key <1-4> | Configures transmit WEP/Keyguard key settings<br>• <1-4> – Transmit the key identified by the key index specified here. Specify the index from 1 - 4. |

**Example**

```
rfs6000-81742D(config-rf-domain-default)#override-wlan test vlan-pool 2 limit 20

rfs6000-81742D(config-rf-domain-default)#show context
rf-domain default
 contact Bob+14082778691
 country-code us
 override-smartrf channel-list 2.4GHz 1,2,3
 override-wlan test vlan-pool 2 limit 20
 layout area Ecospace floor Floor1 map-location www.firstfloor.com units meters
rfs6000-81742D(config-rf-domain-default)#
```

**Related Commands**

| | |
|---|---|
| *no* | Resets the override WLAN settings its default |

### 4.1.79.2.15 sensor-server

*rf-domain-mode commands*

Configures an AirDefense sensor server on this RF Domain. Sensor servers allow network administrators to monitor and download data from multiple sensors remote locations using Ethernet TCP/IP or serial communications. This enables administrators to respond quickly to interferences and coverage problems.

The *Wireless Intrusion Protection System* (WIPS) protects the controller managed network, wireless clients and access point radio traffic from attacks and unauthorized access. WIPS provides tools for standards compliance and around-the-clock wireless network security in a distributed environment. WIPS allows administrators to identify and accurately locate attacks, rogue devices and network vulnerabilities in real time and permits both a wired and wireless lockdown of wireless device connections upon acknowledgement of a threat.

In addition to dedicated AirDefense sensors, an access point radio can function as a sensor and upload information to a dedicated WIPS server (external to the controller). Unique WIPS server configurations can be used by RF Domains to ensure a WIPS server configuration is available to support the unique data protection needs of individual RF Domains.

WIPS is not supported on a WLAN basis, rather sensor functionality is supported on the access point radio(s) available to each controller managed WLAN. When an access point radio is functioning as a WIPS sensor, it is able to scan in sensor mode across all legal channels within the 2.4 and 5.0 GHz bands. Sensor support requires a AirDefense WIPS Server on the network. Sensor functionality is not provided by the access point alone. The access point works in conjunction with a dedicated WIPS server.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
sensor-server <1-3> ip <IP/HOSTNAME> {port [443|<1-65535>]}
```

**Parameters**

- `sensor-server <1-3> ip <IP/HOSTNAME> {port [443|<1-65535>]}`

| | |
|---|---|
| sensor-server <1-3> | Configures an AirDefense sensor server parameters<br>• <1-3> – Select the server ID from 1 - 3. The server with the lowest defined ID is reached first. The default is 1. |
| ip <IP/HOSTNAME> | Configures the (non DNS) IPv4 address of the sensor server<br>• <IP/HOSTNAME> – Specify the sensor server's IPv4 address or hostname. |
| port [443\|<1-65535>] | Optional. Configures the sensor server port. The options are:<br>• 443 – Configures port 443, the default port used by the AirDefense server. This is the default setting.<br>• <1-65535> – Allows you to select a WIPS/AirDefense sensor server port from 1 - 65535 |

**Example**

```
rfs6000-81742D(config-rf-domain-default)#sensor-server 2 ip 172.16.10.3 port 443

rfs6000-81742D(config-rf-domain-default)#show context
rf-domain default
 contact Bob+14082778691
 country-code us
 sensor-server 2 ip 172.16.10.3
 override-smartrf channel-list 2.4GHz 1,2,3
 override-wlan test vlan-pool 2 limit 20
 layout area Ecospace floor Floor1 map-location www.firstfloor.com units meters
rfs6000-81742D(config-rf-domain-default)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables an AirDefense sensor server parameters |

### 4.1.79.2.16 stats

*rf-domain-mode commands*

Configures stats settings that define how RF Domain statistics are updated

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
stats update-interval

stats update-interval [<5-300>|auto]
```

**Parameters**

- `stats update-interval [<5-300>|auto]`

| | |
|---|---|
| stats | Configures stats related settings on this RF Domain |
| update-interval [<5-300>\|auto] | Configures the interval at which RF Domain statistics are updated. The options are:<br>• <5-300> – Specify an update interval from 5 - 300 seconds.<br>• auto – The RF Domain manager automatically adjusts the update interval based on the load. This is the default setting. |

**Example**

```
rfs6000-81742D(config-rf-domain-default)#stats update-interval 200
rfs6000-81742D(config-rf-domain-default)#show context
rf-domain default
 contact Bob+14082778691
 stats update-interval 200
 country-code us
 sensor-server 2 ip 172.16.10.3
 override-smartrf channel-list 2.4GHz 1,2,3
 override-wlan test vlan-pool 2 limit 20
 layout area Ecospace floor Floor1 map-location www.firstfloor.com units meters
rfs6000-81742D(config-rf-domain-default)#
```

**Related Commands**

| | |
|---|---|
| *no* | Resets stats related settings |

### 4.1.79.2.17 timezone

*rf-domain-mode commands*

Configures the RF Domain's geographic time zone. By default all WiNG devices are shipped with the time zone and time format set to *Universal Time Coordinated* (UTC) and 24-hour clock respectively. If the time zone is not reset, all devices within the RF Domain will display time relative to the UTC - Greenwich Time. Resetting the time zone is recommended, especially for RF Domains deployed across different geographical locations. The time zone can either be set on a specific device or on an RF Domain. When configured as RF Domain setting, it applies to all devices within the domain. For more information on configuring the time zone on a device, see *timezone*.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
timezone <TIMEZONE>
```

**Parameters**

- `timezone <TIMEZONE>`

| | |
|---|---|
| time <TIMEZONE> | Specify the RF Domain's time zone. The configured time zone will apply to all devices within the selected RF Domain. |

**Example**

```
rfs6000-81742D(config-rf-domain-default)#timezone America/Los_Angeles

rfs6000-81742D(config-rf-domain-default)#show context
rf-domain default
 contact Bob+14082778691
 timezone America/Los_Angeles
 stats update-interval 200
 country-code us
 sensor-server 2 ip 172.16.10.3
 override-smartrf channel-list 2.4GHz 1,2,3
 override-wlan test vlan-pool 2 limit 20
 layout area Ecospace floor Floor1 map-location www.firstfloor.com units meters
rfs6000-81742D(config-rf-domain-default)#

The built-in WiNG timezones are:

nx9500-6C8809(config-rf-domain-test)#timezone <TAB>
Africa/     Asia/       Atlantic/   Australia/  CET         CST6CDT
EET         EST5EDT     Etc/        Europe/     MST7MDT     Pacific/
PST8PDT     US/         America/
nx9500-6C8809(config-rf-domain-test)#
```

Each of these time zones are further differentiated into sub time zones. For example, as shown in the following example:

```
nx9500-6C8809(config-rf-domain-test)#timezone Africa/
Africa/Cairo         Africa/Casablanca    Africa/Harare
Africa/Johannesburg  Africa/Lagos         Africa/Nairobi
nx9500-6C8809(config-rf-domain-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes a RF Domain's time zone |

### 4.1.79.2.18 tree-node

*rf-domain-mode commands*

Configures the hierarchical (tree-node) structure under which this RF Domain is located

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
tree-node [campus|city|country|region] {(campus|city|country|region)}
```

**Parameters**

- `tree-node [campus|city|country|region] {(campus|city|country|region)}`

| | |
|---|---|
| tree-node | Configures the hierarchical tree structure defining the RF Domain's location. The tree node hierarchy can be configured in any order, but will always appear as: *country > region > city > campus*. Further, a higher node, such as country, cannot be defined under a lower node, such as region. An RF Domain can be placed under any one of the tree nodes. But, an RF Domain at the country level may have all four nodes defined. Whereas, an RF Domain restricted to a campus, cannot have the country, city, and region nodes.<br>At least one of these four nodes must be defined. This feature is disabled by default. |
| campus | Configures the campus name for this RF Domain |
| city | Configures the city for this RF Domain |
| country | Configures the country for this RF Domain |
| region | Configures the region for this RF Domain |

**Usage Guidelines**

The following points need to be taken into consideration when creating the tree-node structure:

- Adding a *country* first is a good idea since *region*, *city*, and *campus* can all be added as sub-nodes in the tree structure. However, the selected country is an invalid tree node until a RF Domain is mapped.
- A city and campus can be added in the tree structure as sub-nodes under a region. An RF Domain can be mapped anywhere down the hierarchy for a region and not just directly under a country. For example, a region can have city, campus, and one RF Domain mapped.
- Only a campus can be added as a sub-node under a city. The city is an invalid tree node until a RF Domain is mapped somewhere within the directory tree.
- A campus is the last node in the hierarchy before a RF Domain, and it is not valid unless it has a RF Domain mapped.
- After creating the tree structure do a *commit* and *save* for the tree configuration to take effect and persist across reboots.

**Example**

```
rfs4000-229D58(config-rf-domain-test)#tree-node campus EcoSpace City Bangalore
country India region South
rfs4000-229D58(config-rf-domain-test)#

rfs4000-229D58(config-rf-domain-test)#show context
rf-domain test
 country-code in
 tree-node country India region South city Bangalore campus EcoSpace
rfs4000-229D58(config-rf-domain-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the RF Domain's tree-node configuration |

### 4.1.79.2.19 use

*rf-domain-mode commands*

Associates the following with an RF Domain: database policy, NSight policy, sensor policy, Smart RF policy, WIPS policy, RTL server policy, and Web filtering license.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
use [database-policy|license|nsight-policy|rtl-server-policy|sensor-policy|
smart-rf-policy|wips-policy]

use [database-policy <DATABASE-POLICY-NAME>|license <WEB-FILTERING-LICENSE>|
nsight-policy <NSIGHT-POLICY-NAME>|rtl-server-policy <RTL-SERVER-POLICY-NAME>
sensor-policy <SENSOR-POLICY-NAME>|smart-rf-policy <SMART-RF-POLICY-NAME>|
wips-policy <WIPS-POLICY-NAME>]
```

**Parameters**

```
• use [database-policy <DATABASE-POLICY-NAME>|license <WEB-FILTERING-LICENSE>|
nsight-policy <NSIGHT-POLICY-NAME>|rtl-server-policy <RTL-SERVER-POLICY-NAME>|
sensor-policy <SENSOR-POLICY-NAME>|smart-rf-policy <SMART-RF-POLICY-NAME>|
wips-policy <WIPS-POLICY-NAME>]
```

| | |
|---|---|
| use | Associates the following policies with the RF Domain: database policy, NSight policy, sensor policy, Smart RF policy, WIPS policy. It also applies a Web filtering license to the selected RF Domain. |
| database-policy <DATABASE-POLICY-NAME> | Associates a database policy with the selected RF Domain<br>• <DATABASE-POLICY-NAME> – Specify the database policy name (should be existing and configured). |
| license <WEB-FILTERING-LICENSE> | Obtains the specified Web filtering license from the adopting controller<br>• <WEB-FILTERING-LICENSE> – Specify the WEBF license name. |
| nsight-policy <NSIGHT-POLICY-NAME> | Associates an NSight policy to this RF Domain<br>• Specify the NSight policy name (should be existing and configured). When applied, it enables the RF Domain manager to gather statistical data from access points within the domain and forward to the NOC running the NSight server. For information on configuring NSight policy, see *nsight-policy*. |
| rtl-server-policy <RTL-SERVER-POLICY-NAME> | Associates an *Real Time Locationing* (RTL) server policy with the selected RF Domain<br>• <RTL-SERVER-POLICY-NAME> – Specify the RTL server policy name (should be existing and configured |
| sensor-policy <SENSOR-POLICY-NAME> | Associates a sensor policy with the selected RF Domain<br>• <SENSOR-POLICY-NAME> – Specify the sensor policy name (should be existing and configured). |

| | |
|---|---|
| smart-rf-policy <SMART-RF-POLICY-NAME> | Associates a Smart RF policy. When associated, the Smart RF policy provides automatic recovery from coverage loss (due to failed or faulty radio) by instructing neighboring access points to increase their transmit power.<br>Once correct access point placement has been established, Smart-RF can optionally be leveraged for automatic detector radio selection. Smart-RF uses detector radios to monitor RF events to ensure availability of adequate detector coverage.<br>• <SMART-RF-POLICY-NAME> – Specify the Smart RF policy name (should be existing and configured). For more information on configuring smart RF policy, see *SMART-RF-POLICY*. |
| wips-policy <WIPS-POLICY-NAME> | Associates a WIPS policy. A WIPS policy provides protection against wireless threats and acts as a key layer of security complementing wireless VPNs, encryption and authentication. A WIPS policy uses a dedicated sensor for actively detecting and locating rogue AP devices. After detection, WIPS uses mitigation techniques to block the devices by manual termination, air lockdown, or port suppression.<br>• <WIPS-POLICY-NAME> – Specify the WIPS policy name (should be existing and configured). For more information on configuring WIPS policy, see *WIPS-POLICY*. |

**Example**

```
rfs6000-81742D(config-rf-domain-default)#use smart-rf-policy Smart-RF1
rfs6000-81742D(config-rf-domain-default)#use wips-policy WIPS1

rfs6000-81742D(config-rf-domain-default)#show context
rf-domain default
 contact Bob+14082778691
 timezone America/Los_Angeles
 stats update-interval 200
 country-code us
 use smart-rf-policy Smart-RF1
 use wips-policy WIPS1
 sensor-server 2 ip 172.16.10.3
 override-smartrf channel-list 2.4GHz 1,2,3
 override-wlan test vlan-pool 2 limit 20
 layout area Ecospace floor Floor1 map-location www.firstfloor.com units meters
rfs6000-81742D(config-rf-domain-default)#
```

**Related Commands**

| | |
|---|---|
| *no* | Resets profiles used with this RF Domain |
| *sensor-server* | Configures an AirDefense sensor server on this RF Domain |
| *wips-policy* | Configures a WIPS policy |
| *smart-rf-policy* | Configures a Smart RF policy |

## 4.1.80 rfs6000

*Global Configuration Commands*

Adds a RFS6000 wireless controller to the network

**Supported in the following platforms:**

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
rfs6000 <DEVICE-RFS6000-MAC>
```

**Parameters**

- `rfs6000 <DEVICE-RFS6000-MAC>`

| | |
|---|---|
| <DEVICE-RFS6000-MAC> | Specify the RFS6000's MAC address. |

**Example**

```
rfs6000-81742D(config)#rfs6000 11-20-30-40-50-61
rfs6000-81742D(config-device-11-20-30-40-50-61)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes a RFS6000 wireless controller from the network |

## 4.1.81 rfs4000

*Global Configuration Commands*

Adds an RFS4000 wireless controller to the network

**Supported in the following platforms:**

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
rfs4000 <DEVICE-RFS4000-MAC>
```

**Parameters**

- `rfs4000 <DEVICE-RFS4000-MAC>`

| | |
|---|---|
| <DEVICE-RFS4000-MAC> | Specify the RFS4000's MAC address. |

**Example**

```
rfs6000-81742D(config)#rfs4000 10-20-30-40-50-60
rfs6000-81742D(config-device-10-20-30-40-50-60)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an RFS4000 wireless controller from the network |

## 4.1.82 nx5500

*Global Configuration Commands*

Adds an integrated NX5500 series service platform to the network. If a profile for this service platform is not available, a new profile is created.

**Supported in the following platforms:**

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
nx5500 <DEVICE-NX5500-MAC>
```

**Parameters**

- `nx5500 <DEVICE-NX5500-MAC>`

| | |
|---|---|
| <DEVICE-NX5500-MAC> | Specifies the MAC address of a NX5500 series service platform. |

**Example**

```
nx9500-6C8809(config)#nx5500 B4-C7-02-3C-FA-6E
nx9500-6C8809(config-device-B4-C7-02-3C-FA-6E)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes a NX5500 series service platform from the network |

## 4.1.83 nx75xx

*Global Configuration Commands*

Adds an integrated NX75XX series service platform to the network. If a profile for service platform is not available, a new profile is created.

**Supported in the following platforms:**

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**NOTE:** In this guide, NX7500, NX7510, NX7520, and NX7530 are collectively represented as a NX75XX series service platform.

**Syntax**

```
nx75xx <DEVICE-NX75XX-MAC>
```

**Parameters**

- `nx75xx <DEVICE-NX75XX-MAC>`

| | |
|---|---|
| <DEVICE-NX75XX-MAC> | Specifies the MAC address of a NX75XX series service platform. |

**Example**

```
nx9500-6C8809(config)#nx75xx B4-C9-81-6C-FA-7C
nx9500-6C8809(config-device-B4-C9-81-6C-FA-7C)#show context
nx75xx B4-C9-81-6C-FA-7C
 use profile default-nx75xx
 use rf-domain default
 hostname nx75xx-6CFA7C
nx9500-6C8809(config-device-B4-C9-81-6C-FA-7C)#

nx75xx-6CFA7C>show adoption status
Adopted by:
Type          : nx9000
System Name   : nx9500-6C8809
MAC address   : B4-C7-99-6C-88-09
MiNT address  : 19.6C.88.09
Time          : 1 days 01:57:50 ago

Adopted Devices:
-------------------------------------------------------------------------------
-------
DEVICE-NAME   VERSION       CFG-STAT    MSGS ADOPTED-BY   LAST-ADOPTION    UPTIME
-------------------------------------------------------------------------------
-------
ap7131-11E6C4 5.8.6.0-008B  configured  No   nx75xx-6CFA7C 1 days 01:49:44 1 days
01:59:34
-------------------------------------------------------------------------------
-------
Total number of devices displayed: 1
nx75xx-6CFA7C>
```

**Related Commands**

| | |
|---|---|
| *no* | Removes a NX75XX series service platform from the network |

## 4.1.84 nx9000

*Global Configuration Commands*

Adds a NX95XX series service platform to the network

**Supported in the following platforms:**

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
nx9000 <DEVICE-NX95XX-MAC>
```

**Parameters**

- `nx9000 <DEVICE-NX95XX-MAC>`

| | |
|---|---|
| <DEVICE-NX95XX-MAC> | Specifies the MAC address of a NX95XX series service platform. |

**Example**

```
nx9500-6C8809(config)#nx9000 B4-C7-89-7C-81-08
nx9500-6C8809(config-device-B4-C7-89-7C-81-08)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes a NX95XX series service platform from the network |

## 4.1.85 roaming-assist-policy

*Global Configuration Commands*

Configures a roaming assist policy that enables access points to assist wireless clients in making roaming decisions, such as which access point to connect, etc.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
roaming-assist-policy <POLICY-NAME>
```

**Parameters**

- `roaming-assist-policy <POLICY-NAME>`

| | |
|---|---|
| <POLICY-NAME> | Specify the roaming assist policy name. If the policy does not exist, it is created. |

**Example**

```
rfs6000-81742D(config)#roaming-assist-policy testPolicy
rfs6000-81742D(config-roaming-assist-policy-testPolicy)#?
Roaming Assist Mode commands:
  action                Configure action - action is either to log / deauth
  aggressiveness        Configure the roaming aggressiveness for a wireless
                        client
  detection-threshold   Configure the detection threshold - when exceeded,
                        client monitoring starts
  disassoc-time         Configure the disassociation time - time after which a
                        disassociation is sent
  handoff-count         Configure the handoff count - number of times client
                        can exceed handoff threshold
  handoff-threshold     Configure the handoff threshold - when exceeds an
                        action is taken.
  monitoring-interval   Configure the monitoring interval - interval at which
                        client monitoring occurs
  no                    Negate a command or set its defaults
  sampling-interval     Configure the sampling interval - interval at which
                        client rssi values are checked

  clrscr                Clears the display screen
  commit                Commit all changes made in this session
  end                   End current mode and change to EXEC mode
  exit                  End current mode and down to previous mode
  help                  Description of the interactive help system
  revert                Revert changes
  service               Service Commands
  show                  Show running system information
  write                 Write running configuration to memory or terminal

rfs6000-81742D(config-roaming-assist-policy-testPolicy)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing roaming assist policy |

**NOTE:** For more information on roaming assist policy commands, see *Chapter 30, ROAMING ASSIST POLICY*.

## 4.1.86 role-policy

*Global Configuration Commands*

Configures a role-based firewall policy

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
role-policy <ROLE-POLICY-NAME>
```

**Parameters**

- `role-policy <ROLE-POLICY-NAME>`

| | |
|---|---|
| <ROLE-POLICY-NAME> | Specify the role policy name. If the policy does not exist, it is created. |

**Example**

```
rfs6000-81742D(config)#role-policy role1
rfs6000-81742D(config-role-policy-role1)#?
Role Policy Mode commands:
  default-role      Configuration for Wireless Clients not matching any role
  ldap-deadperiod   Ldap dead period interval
  ldap-query        Set the ldap query mode
  ldap-server       Add a ldap server
  ldap-timeout      Ldap query timeout interval
  no                Negate a command or set its defaults
  user-role         Create a role

  clrscr            Clears the display screen
  commit            Commit all changes made in this session
  do                Run commands from Exec mode
  end               End current mode and change to EXEC mode
  exit              End current mode and down to previous mode
  help              Description of the interactive help system
  revert            Revert changes
  service           Service Commands
  show              Show running system information
  write             Write running configuration to memory or terminal

rfs6000-81742D(config-role-policy-role1)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing role policy |

**NOTE:** For more information on role policy commands, see *Chapter 18, ROLE-POLICY*.

## 4.1.87 route-map

*Global Configuration Commands*

Creates a dynamic BGP route map and enters its configuration mode

BGP route maps are used by network administrators to define rules controlling redistribution of routes between routers and routing processes. These route maps are also used to control and modify routing information.

**Supported in the following platforms:**

- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9600, VX9000

**Syntax**

```
route-map <ROUTE-MAP-NAME>
```

**Parameters**

- `route-map <ROUTE-MAP-NAME>`

| | |
|---|---|
| route-map <ROUTE-MAP-NAME> | Creates a new BGP route map and enters its configuration mode |

**Example**

```
nx9500-6C8809(config)#route-map test

nx9500-6C8809(config-dr-route-map-test)#?
Route Map Mode commands:
  deny      Add a deny route map rule to deny set operations
  no        Negate a command or set its defaults
  permit    Add a permit route map rule to permit set operations

  clrscr    Clears the display screen
  commit    Commit all changes made in this session
  do        Run commands from Exec mode
  end       End current mode and change to EXEC mode
  exit      End current mode and down to previous mode
  help      Description of the interactive help system
  revert    Revert changes
  service   Service Commands
  show      Show running system information
  write     Write running configuration to memory or terminal

nx9500-6C8809(config-dr-route-map-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing dynamic BGP route map |

**NOTE:** For more information on BGP route maps, see *Chapter 28, BORDER GATEWAY PROTOCOL*.

## 4.1.88 routing-policy

*Global Configuration Commands*

Configures a routing policy

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
routing-policy <ROUTING-POLICY-NAME>
```

**Parameters**

- `routing-policy <ROUTING-POLICY-NAME>`

| | |
|---|---|
| <ROUTING-POLICY-NAME> | Specify the routing policy name. If the policy does not exist, it is created. |

**Example**

```
rfs6000-81742D(config)#routing-policy TestRoutingPolicy
rfs6000-81742D(config-routing-policy-TestRoutingPolicy)#?
Routing Policy Mode commands:
  apply-to-local-packets  Use Policy Based Routing for packets generated by
                          the device
  logging                 Enable logging for this Route Map
  no                      Negate a command or set its defaults
  route-map               Create a Route Map
  use                     Set setting to use

  clrscr                  Clears the display screen
  commit                  Commit all changes made in this session
  do                      Run commands from Exec mode
  end                     End current mode and change to EXEC mode
  exit                    End current mode and down to previous mode
  help                    Description of the interactive help system
  revert                  Revert changes
  service                 Service Commands
  show                    Show running system information
  write                   Write running configuration to memory or terminal

rfs6000-81742D(config-routing-policy-TestRoutingPolicy)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing routing policy |

**NOTE:** For more information on routing policy commands, see *Chapter 24, ROUTING-POLICY*.

## 4.1.89 rtl-server-policy

*Global Configuration Commands*

The following table lists the *Real Time Locationing* (RTL) server policy configuration commands:

**Table 4.45** *RTL-Server-Policy Config Command*

| Command | Description | Reference |
|---|---|---|
| *rtl-server-policy* | Configures an RTL server policy and enters its configuration mode | *page 4-414* |
| *rtl-server-policy-mode commands* | Summarizes RTL server policy configuration mode commands | *page 4-416* |

### 4.1.89.1 rtl-server-policy

*rtl-server-policy*

Creates an RTL server policy and enters its configuration mode. When configured and applied on an access point (AP7522, AP7532, AP8432, AP8533), this policy enables the sending of RSSI feeds from the access point to a
third-party Euclid server. The RTL server policy provides the exact location (URL) of the Euclid server. The RSSI feeds sent are as per the sensor-policy configured and applied on the access point. Therefore, ensure that a sensor-policy, with the *rssi-interval-duration* specified, is existing, configured, and applied on the access points.

To initiate RSSI feed posts to the Euclid locationing server, use the RTL server policy on the:

- AP's device/profile context, or
- AP's RF Domain context.

**Supported in the following platforms:**

- Access Points — AP7522, AP7532, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX9500, NX9510, NX9600, VX9000

**Syntax**

```
rtl-server-policy <RTL-POLICY-NAME>
```

**Parameters**

- `rtl-server-policy <RTL-POLICY-NAME>`

| | |
|---|---|
| <RTL-SERVER-POLICY-NAME> | Specify the RTL server policy name. If a RTL server policy with the specified name does not exist, it is created. |

**Example**

```
nx9500-6C8809(config)#rtl-server-policy test
nx9500-6C8809(config-rtl-server-policy-test)#?
RTL Server Policy Mode commands:
  no       Negate a command or set its defaults
  url      Configure the url to send the real time RSSI feed to

  clrscr   Clears the display screen
  commit   Commit all changes made in this session
  do       Run commands from Exec mode
  end      End current mode and change to EXEC mode
  exit     End current mode and down to previous mode
  help     Description of the interactive help system
  revert   Revert changes
  service  Service Commands
  show     Show running system information
  write    Write running configuration to memory or terminal


nx9500-6C8809(config-rtl-server-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing RTL server policy |
| *use* (profile/device configuration mode command) | Documents the 'use' command in a device's profile or device configuration context. Use this option to associate this RTL server policy to an access point's profile or device. |
| *use* (RF Domain configuration mode command) | Documents the 'use' command in the RF Domain configuration context. Use this option to associate this RTL server policy to an RF Domain. When associated, the policy is applied to all access points within the RF Domain. |

### 4.1.89.2 rtl-server-policy-mode commands

*rtl-server-policy*

The following table summarizes the RTL server policy configuration mode commands:

**Table 4.46** *RTL-Server-Policy Mode Commands*

| Command | Description | Reference |
|---|---|---|
| *url* | Configures the third-party Euclid RTL server's URL | *page 4-417* |
| *no* | Removes the Euclid RTL server's URL configuration | *page 4-418* |

### 4.1.89.2.1 url

*rtl-server-policy-mode commands*

Configures the third-party Euclid RTL server's exact location. This is the URL at which the server can be reached.

**Supported in the following platforms:**

- Access Points — AP7522, AP7532, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX9500, NX9510, NX9600, VX9000

**Syntax**

```
url <URL>
```

**Parameters**

- `url <URL>`

| | |
|---|---|
| url <URL> | Configures the Euclid server's URL<br>• <URL> – Specify the URL. |

**Example**

```
nx9500-6C8809(config-rtl-server-policy-test)#url https://testrtlsever.com

nx9500-6C8809(config-rtl-server-policy-test)#show context
rtl-server-policy test
 url https://testrtlsever.com
nx9500-6C8809(config-rtl-server-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the Euclid server's configured URL |

### 4.1.89.2.2 no

*rtl-server-policy-mode commands*

Removes the Euclid locationing server's URL configuration

**Supported in the following platforms:**

- Access Points — AP7522, AP7532, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX9500, NX9510, NX9600, VX9000

**Syntax**

```
no url
```

**Parameters**

- `no url`

| | |
|---|---|
| no url | Removes the Euclid server's URL |

**Example**

The following example displays the RTL server policy 'test' settings before the 'no' command is executed:

```
nx9500-6C8809(config-rtl-server-policy-test)#show context
rtl-server-policy test
 url https://testrtlsever.com
nx9500-6C8809(config-rtl-server-policy-test)#

nx9500-6C8809(config-rtl-server-policy-test)#no url
```

The following example displays the RTL server policy 'test' settings after the 'no' command is executed:

```
nx9500-6C8809(config-rtl-server-policy-test)#show context
rtl-server-policy test
nx9500-6C8809(config-rtl-server-policy-test)#
```

## 4.1.90 schedule-policy

*Global Configuration Commands*

The following table summarizes the config schedule policy commands:

**Table 4.47** *Schedule-Policy Config Commands*

| Command | Description | Reference |
|---|---|---|
| *schedule-policy* | Creates a schedule policy and enters its configuration mode | *page 4-420* |
| *schedule-policy-mode commands* | Lists schedule policy configuration mode commands | *page 4-421* |

### 4.1.90.1 schedule-policy

*schedule-policy*

Creates a schedule policy and enters its configuration mode. A schedule policy strategically enforces application filter policy rules during administrator assigned intervals.

**Supported in the following platforms:**

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
schedule-policy <SCHEDULE-POLICY-NAME>
```

**Parameters**

- `schedule-policy <SCHEDULE-POLICY-NAME>`

| | |
|---|---|
| schedule-policy <SCHEDULE-POLICY-NAME> | Specify the Schedule policy name. If the policy does not exist, it is created. The name should not exceed 32 characters in length. |

**Example**

```
nx9500-6C8809(config)#schedule-policy test
nx9500-6C8809(config-schedule-policy-test)#?
Schedule Policy Mode commands:
  description  Schedule policy description
  no           Negate a command or set its defaults
  time-rule    Configure a time rule

  clrscr       Clears the display screen
  commit       Commit all changes made in this session
  do           Run commands from Exec mode
  end          End current mode and change to EXEC mode
  exit         End current mode and down to previous mode
  help         Description of the interactive help system
  revert       Revert changes
  service      Service Commands
  show         Show running system information
  write        Write running configuration to memory or terminal

nx9500-6C8809(config-schedule-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing schedule policy |

### 4.1.90.2 schedule-policy-mode commands

*schedule-policy*

The following table summarizes schedule-policy configuration mode commands:

**Table 4.48** *Schedule-Policy-Config-Mode Commands*

| Command | Description | Reference |
|---|---|---|
| *description* | Configures a description for this schedule policy that differentiates it from other policies with similar time rule configurations | *page 4-422* |
| *time-rule* | Configures a time rule specifying the days and optionally the start and end times | *page 4-423* |
| *no* | Removes the selected schedule policy's settings | *page 4-425* |

### 4.1.90.2.1 description

*schedule-policy-mode commands*

Configures a description for this schedule policy that differentiates it from other policies with similar time rule configurations

**Supported in the following platforms:**

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
description <WORD>
```

**Parameters**

- `description <WORD>`

| | |
|---|---|
| description <WORD> | Configures this schedule policy's description<br>• <WORD> – Enter a description not exceeding 80 characters in length. The description should uniquely identify the policy from other policies with similar configuration. |

**Example**

```
nx9500-6C8809(config-schedule-policy-test)#description "Denies social networking
 sites on weekdays."

nx9500-6C8809(config-schedule-policy-test)#show context
schedule-policy test
 description "Denies social networking sites on weekdays."
nx9500-6C8809(config-schedule-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes this schedule policy's description |

### 4.1.90.2.2 time-rule

*schedule-policy-mode commands*

Configures a time rule specifying the days and optionally the start and end times. When applied to an application-policy rule, the schedule policy defines the enforcement time of the rule. For more information, see *application-policy*.

**Supported in the following platforms:**

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
time-rule days [sunday|monday|tuesday|wednesday|thursday|friday|saturday|all|
weekends|weekdays] {start-time <HH:MM> [end-time <HH:MM>]}
```

**Parameters**

```
• time-rule days [sunday|monday|tuesday|wednesday|thursday|friday|saturday|all|
weekends|weekdays] {start-time <HH:MM> [end-time <HH:MM>]}
```

| | |
|---|---|
| time-rule | Configures a time rule in days and hours and minutes<br>A schedule policy can have more than one non-overlapping time-rules. The following time-rules, having overlapping time periods, are invalid: '*weekdays, start-time 9:30 am, end-time 11:30 pm*' and '*all, start-time 12:00 am, end-time 12:00 p*m'. |
| days [sunday\|monday\| tuesday\|wednesday\| thursday\|friday\| saturday\|all\| weekends\| weekdays] | Specifies the days on which the time rule is applicable<br>• sunday – Applicable on Sundays only<br>• monday – Applicable on Mondays only<br>• tuesday – Applicable on Tuesdays only<br>• wednesday – Applicable on Wednesdays only<br>• thursday – Applicable on Thursdays only<br>• friday – Applicable on Fridays only<br>• saturday – Applicable on Saturdays only<br>• weekends – Applicable on weekends only<br>• weekdays – Applicable on weekdays only<br>• all – Applicable on all days |
| start-time <HH:MM> [end-time <HH:MM>] | After specifying the days of enforcement, specify the following:<br>• start-time – Optional. Specifies the enforcement start time<br>• <HH:MM> – Specify the start time in hours and minutes in the HH:MM format.<br>If no start time is specified, the time rule is enforced, on the specified days, at all time.<br>• end-time – Specifies the enforcement end time<br>• <HH:MM> – Specify the time in hours and minutes in the HH:MM format. |

**Example**

```
nx9500-6C8809(config-schedule-policy-test)#time-rule days weekdays start-time
10:00 end-time 23:30

nx9500-6C8809(config-schedule-policy-test)#show context
schedule-policy test
 description "Denies social networking sites on weekdays."
 time-rule days weekdays start-time 10:00 end-time 23:30
nx9500-6C8809(config-schedule-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the time-rule from the schedule policy |

### 4.1.90.2.3 no

*schedule-policy-mode commands*

Removes the selected schedule policy's settings

**Supported in the following platforms:**

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
no [description|time-rule]

no description

no time-rule days [sunday|monday|tuesday|wednesday|thursday|friday|saturday|
all|weekends|weekdays]
```

**Parameters**

- `no <PARAMETERS>`

| | |
|---|---|
| no <PARAMETERS> | Removes the schedule policy's settings based on the parameters passed |

**Example**

The following example displays the schedule policy 'test' settings before the 'no' commands have been executed:

```
nx9500-6C8809(config-schedule-policy-test)#show context
schedule-policy test
 description "Denies social networking sites on weekdays."
 time-rule days weekdays start-time 10:00 end-time 23:30
nx9500-6C8809(config-schedule-policy-test)#
```

The following example displays the schedule policy 'test' settings after the 'no' commands have been executed:

```
nx9500-6C8809(config-schedule-policy-test)#no description
nx9500-6C8809(config-schedule-policy-test)#no time-rule days weekdays

nx9500-6C8809(config-schedule-policy-test)#show context
schedule-policy test
nx9500-6C8809(config-schedule-policy-test)#
```

## 4.1.91 self

*Global Configuration Commands*

Displays the logged device's configuration context

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
self
```

**Parameters**

None

**Example**

```
rfs6000-81742D(config)#self
rfs6000-81742D(config-device-00-15-70-37-FA-BE)#
```

## 4.1.92 sensor-policy

*Global Configuration Commands*

The following table summarizes the config sensor policy commands:0

**Table 4.49** *Sensor-Policy Config Commands*

| Command | Description | Reference |
|---|---|---|
| *sensor-policy* | Creates a sensor policy and enters its configuration mode | *page 4-428* |
| *sensor-policy-mode commands* | Lists sensor policy configuration mode commands | *page 4-430* |

### 4.1.92.1 sensor-policy

*sensor-policy*

In addition to WIPS support, sensor functionality has now been added for the Extreme Network's MPact locationing system. The MPact system for Wi-Fi locationing includes WiNG controllers, and access points functioning as sensors. Within the MPact architecture, sensors scan for RSSI data on an administrator defined interval and send to a dedicated MPact Server resource, as opposed to an ADSP server. The MPact Server collects the RSSI data from WiNG sensor devices, and calculates the location of Wi-Fi devices for MPact administrators.

Use this command to configure a policy defining the mode of scanning, the channels to scan (in case scan-mode is set to custom-scan), and the RSSI interval. For the sensor policy to take effect, use the policy either in the access point's RF Domain context or in the access point's device context.

**NOTE:** If a dedicated sensor is utilized with WIPS for rogue detection, any sensor policy used is discarded and not utilized by the sensor. To avoid this situation, use ADSP channel settings exclusively to configure the sensor and not the WiNG interface.

**Supported in the following platforms:**

- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510

**Syntax**

```
sensor-policy <SENSOR-POLICY-NAME>
```

**Parameters**

- `sensor-policy <SENSOR-POLICY-NAME>`

| | |
|---|---|
| sensor-policy <SENSOR-POLICY-NAME> | Specify the Sensor policy name. If a sensor policy with the specified name does not exist, it is created. The name should not exceed 32 characters in length. No character spaces are permitted within the name. Define a name unique to the policy's channel and scan mode configuration to help differentiate it from other policies. |

**Usage GuidelinesADSP WIPS/MPact**

Access point radios, functioning as sensors, along with AirDefense WIPS servers protect networks from attacks and unauthorized access. These access point sensors scan legal channels and (based on a WIPS policy settings) identify events potential threats to the managed network. These events are reported to the AirDefense WIPS server, which determines the action taken.

In addition to WIPS support, sensor functionality has now been added for the MPact locationing system. The MPact system for Wi-Fi locationing includes WiNG controllers and access points functioning as sensors. Within the MPact architecture, sensors scan for RSSI data on an administrator-defined interval and send to a dedicated MPact server resource, as opposed to an ADSP server. The MPact server collects the RSSI data from WiNG sensor devices, and calculates the location of Wi-Fi devices. With the introduction of the MPact platform, the data collected by access point radios, functioning as sensors, is also used by the MPact server to provide real-time locationing services.

**Example**

```
nx9500-6C8809(config)#sensor-policy test
nx9500-6C8809(config-sensor-policy-test)#?
Sensor Policy Mode commands:
  custom-scan             Channel configuration in Custom Scan channels
  no                      Negate a command or set its defaults
  rssi-interval-duration  Configure the periodicity of sensding RSSI info from
                          sensor to server
  scan-mode               Configure the Scan mode

  clrscr                  Clears the display screen
  commit                  Commit all changes made in this session
  do                      Run commands from Exec mode
  end                     End current mode and change to EXEC mode
  exit                    End current mode and down to previous mode
  help                    Description of the interactive help system
  revert                  Revert changes
  service                 Service Commands
  show                    Show running system information
  write                   Write running configuration to memory or terminal

nx9500-6C8809(config-sensor-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing sensor policy |

### 4.1.92.2 sensor-policy-mode commands

- *sensor-policy*

The following table summarizes sensor-policy configuration mode commands:

**Table 4.50** *Sensor-Policy-Config-Mode Commands*

| Command | Description | Reference |
|---|---|---|
| *custom-scan* | Configures the channel scanning settings when the scan-mode is set to custom-scan | *page 4-431* |
| *rssi-interval-duration* | Configures the interval at which dedicated sensors scan channels for RSSI assessments and send the collected data to a specified MPact server resource | *page 4-433* |
| *scan-mode* | Configures the mode of scanning used by dedicated sensors (access point radios) | *page 4-434* |
| *no* | Removes or reverts to default a sensor policy's settings | *page 4-435* |

### 4.1.92.2.1 custom-scan

*sensor-policy-mode commands*

Configures the channel scanning settings when the *scan-mode* is set to *custom-scan*

**NOTE:** If the mode of scanning is set to *Custom-Scan*, use this command to configure the channels to be scanned. To set the mode of scanning to custom-scan, use the *scan-mode > Custom-Scan* command. For more information, see *scan-mode*.

**Supported in the following platforms:**

- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
custom-scan channel-frequency <CHANNEL-FREQUENCY> width [20MHz|40MHz-Bth|40MHz-Lower|40MHz-Upper|80MHz] scan-weight <SCAN-WEIGHT>
```

**Parameters**

```
• custom-scan channel-frequency <CHANNEL-FREQUENCY> width [20MHz|40MHz-Both|40MHz-Lower|40MHz-Upper|80MHz] scan-weight <SCAN-WEIGHT>
```

| | |
|---|---|
| custom-scan | Configures the custom-scan channel frequency, channel width, and scan weight |
| channel-frequency <CHANNEL-FREQUENCY> | Configures the channel frequency. A list of unique channels in the 2.4, 4.9, 5 and 6 GHz band can be collectively or individually enabled for customized channel scans and RSSI reporting.<br>• <CHANNEL-FREQUENCY> – Specify a single or multiple, 'comma-separated' channel frequencies. |
| width [20MHz\| 40MHz-Both\| 40MHz-Lower\| 40MHz-Upper\| 80MHz] | Configures the channel width. When custom channels are selected for RSSI scans, each selected channel can have its own width defined. Numerous channels have their width fixed at 20MHz, 802.11a radios support 20 and 40 MHz channel widths.<br>• 20MHz – Sets the channel width as 20 Mhz<br>• 40Mhz-Both – Sets the channel width as 40Mhz-Both<br>• 40Mhz-Lowe – Sets the channel width as 40Mhz-Lower<br>• 40Mhz-Upper – Sets the channel width as 40Mhz-Upper<br>• 80Mhz – Sets the channel width as 80Mhz |
| scan-weight <SCAN-WEIGHT> | Configures the scan-weight (scanning duration) for each of the selected channels. Each selected channel can have its weight prioritized in respect to the amount of time a scan is permitted within the defined RSSI scan interval.<br>• <SCAN-WEIGHT> – Specify the scan weightage given to each selected channel. |

**Example**

```
nx9500-6C8809(config-sensor-policy-test)#custom-scan channel-frequency 2412 width 20MHz scan-weight 1000

nx9500-6C8809(config-sensor-policy-test)#custom-scan channel-frequency 2417 width 20MHz scan-weight 1000
```

```
nx9500-6C8809(config-sensor-policy-test)#show context
sensor-policy test
 scan-mode Custom-Scan
 custom-scan channel-frequency 2412 width 20MHz scan-weight 1000
 custom-scan channel-frequency 2417 width 20MHz scan-weight 1000
nx9500-6C8809(config-sensor-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes channels from the channels-to-scan list in case of scan-mode being set to Custom-Scan |

### 4.1.92.2.2 rssi-interval-duration

*sensor-policy-mode commands*

Configures the interval, in seconds, at which dedicated sensors scan channels for RSSI assessments and send the RSSI data obtained to a specified server resource

**Supported in the following platforms:**

- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
rssi-interval-duration <1-60>
```

**Parameters**

- `rssi-interval-duration <1-60>`

| | |
|---|---|
| rssi-interval-duration <1-60> | Configures the RSSI interval duration in seconds. This is the interval at which the sensor scans channels for RSSI data and forwards the data to a dedicated server resource. The server calculates real-time locations of Wi-Fi devices based on the this data.<br>• <1-60> – Specify the RSSI interval duration from 1 - 60 seconds. The default is 1 second.<br>The channels scanned for RSSI assessment depends on the scan-mode selected. For more information, see *scan-mode* and *custom-scan*.<br>Ensure that the server's IP address or hostname has been configured in the access point sensor's RF Domain context. |

**Example**

```
nx9500-6C8809(config-sensor-policy-test)#rssi-interval-duration 30

nx9500-6C8809(config-sensor-policy-test)#show context
sensor-policy test
 rssi-interval-duration 30
 scan-mode Custom-Scan
 custom-scan channel-frequency 2412 width 20MHz scan-weight 1000
 custom-scan channel-frequency 2417 width 20MHz scan-weight 1000
nx9500-6C8809(config-sensor-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Resets the interval at which RSSI data is collected and sent by the sensor to the MPact server host to default (1 second) |

### 4.1.92.2.3 scan-mode

*sensor-policy-mode commands*

Configures the mode of scanning used by dedicated sensors (access point radios)

**Supported in the following platforms:**

- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
scan-mode [Channel-Lock|Custom-Scan|Default-Scan]

scan-mode Channel-Lock lock-frequency <LOCK-FREQUENCY>

scan-mode [Custom-Scan|Default-Scan]
```

**Parameters**

- `scan-mode Channel-Lock lock-frequency <LOCK-FREQUENCY>`

| | |
|---|---|
| scan-mode | Configures the mode of scanning used by the sensors to scan system-defined or user-defined channels for RSSI assessments. The options are: Channel-Lock, Custom-Scan, and Default-Scan. |
| Channel-Lock lock-frequency <LOCK-FREQUENCY> | Configures the mode of scanning as Channel-Lock<br>• lock-frequency <LOCK-FREQUENCY> – Locks scanning for RSSI data to one specific channel identified by the <LOCK-FREQUENCY> parameter.<br>• <LOCK-FREQUENCY> – Specify the channel frequency in MHz. When specified, the sensor scans only this specified channel. |

- `scan-mode [Custom-Scan|Default-Scan]`

| | |
|---|---|
| scan-mode | Configures the mode of scanning used by the sensor. The options are: channel-lock, custom-scan, and default-scan. |
| Custom-Scan | Configures the mode of scanning as Custom-Scan<br>Select this option to restrict scanning to user-defined channels. If selecting this option, use the *custom-scan > channel-frequency* command to configure the channels scanned by the dedicated sensor. For more information, see *custom-scan*. |
| Default-Scan | Configures the mode of scanning as Default-Scan. This is the default setting.<br>By default the system has a fixed, built-in list of channels that are scanned. These channels are hard coded in a spread pattern of 1, 6, 11, 36, 40, 44, and 48. When selected, the dedicated sensor scans only these default channels. |

**Example**

```
nx9500-6C8809(config-sensor-policy-test)#scan-mode Custom-Scan

nx9500-6C8809(config-sensor-policy-test)#show context
sensor-policy test
 rssi-interval-duration 30
 scan-mode Custom-Scan
 custom-scan channel-frequency 2412 width 20MHz scan-weight 1000
 custom-scan channel-frequency 2417 width 20MHz scan-weight 1000
nx9500-6C8809(config-sensor-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Reverts the scan-mode to default (Default-Scan) |

#### 4.1.92.2.4 no

*sensor-policy-mode commands*

Removes or reverts to default a sensor policy's settings

**Supported in the following platforms:**

- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
no [custom-scan|rss1-interval-duration|scan-mode]

no custom-scan channel-frequency <CHANNEL-FREQUENCY-LIST>

no rssi-interval-duration

no scan-mode
```

**Parameters**

- `no <PARAMETERS>`

| | |
|---|---|
| no <PARAMETERS> | Removes or reverts to default a sensor policy settings based on the parameters passed |

**Example**

The following example shows the sensor-policy 'test' settings before the 'no' commands are executed:

```
nx9500-6C8809(config-sensor-policy-test)#show context
sensor-policy test
 rssi-interval-duration 30
 scan-mode Custom-Scan
 custom-scan channel-frequency 2412 width 20MHz scan-weight 1000
 custom-scan channel-frequency 2417 width 20MHz scan-weight 1000
nx9500-6C8809(config-sensor-policy-test)#
```

The scan-mode is reverted back to the default setting of 'Default-Scan', as show in the following output:

```
nx9500-6C8809(config-sensor-policy-test)#no scan-mode
nx9500-6C8809(config-sensor-policy-test)#show context
sensor-policy test
 rssi-interval-duration 30
 scan-mode Default-Scan
 custom-scan channel-frequency 2412 width 20MHz scan-weight 1000
 custom-scan channel-frequency 2417 width 20MHz scan-weight 1000
nx9500-6C8809(config-sensor-policy-test)#

nx9500-6C8809(config-sensor-policy-test)#no custom-scan channel-frequency 2412

nx9500-6C8809(config-sensor-policy-test)#no custom-scan channel-frequency 2417

nx9500-6C8809(config-sensor-policy-test)#show context
sensor-policy test
 rssi-interval-duration 30
 scan-mode Default-Scan
nx9500-6C8809(config-sensor-policy-test)#
```

## 4.1.93 smart-rf-policy

*Global Configuration Commands*

Configures a Smart RF policy

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
smart-rf-policy <SMART-RF-POLICY-NAME>
```

**Parameters**

- `smart-rf-policy <SMART-RF-POLICY-NAME>`

| | |
|---|---|
| <SMART-RF-POLICY-NAME> | Specify the Smart RF policy name. If the policy does not exist, it is created. |

**Example**

```
rfs6000-81742D(config)#smart-rf-policy test
rfs6000-81742D(config-smart-rf-policy-test)#?
Smart RF Mode commands:
  area                      Specify channel list/ power for an area
  assignable-power          Specify the assignable power during power-assignment
  avoidance-time            Time to avoid a channel once dfs/adaptivity
                            avoidance is necessary
  channel-list              Select channel list for smart-rf
  channel-width             Select channel width for smart-rf
  coverage-hole-recovery    Recover from coverage hole
  enable                    Enable this smart-rf policy
  group-by                  Configure grouping parameters
  interference-recovery     Recover issues due to excessive noise and
                            interference
  neighbor-recovery         Recover issues due to faulty neighbor radios
  no                        Negate a command or set its defaults
  sensitivity               Configure smart-rf sensitivity (Modifies various
                            other smart-rf configuration items)
  smart-ocs-monitoring      Smart off channel scanning

  clrscr                    Clears the display screen
  commit                    Commit all changes made in this session
  end                       End current mode and change to EXEC mode
  exit                      End current mode and down to previous mode
  help                      Description of the interactive help system
  revert                    Revert changes
  service                   Service Commands
  show                      Show running system information
  write                     Write running configuration to memory or term

rfs6000-81742D(config-smart-rf-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing Smart RF policy |

**NOTE:** For more information on Smart RF policy commands, see *Chapter 19, SMART-RF-POLICY*.

## 4.1.94 t5

*Global Configuration Commands*

Invokes the configuration mode of a t5 wireless controller

A T5 controller uses the IPX operating system to manage its connected radio devices, as opposed to the WiNG operating system used by RFS controllers and NX service platforms. However, a T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5's management within a WiNG supported subnet populated by both types of devices.

**Supported in the following platforms:**

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
t5 <T5-DEVICE-MAC>
```

**Parameters**

- `t5 <T5-DEVICE-MAC>`

| | |
|---|---|
| t5 <T5-DEVICE-MAC> | Specify the t5 device's MAC address. The system enters the identified device's configuration mode.<br>A T5 controller uses the IPX operating system to manage its connected radio devices, as opposed to the WiNG operating system used by RFS wireless controllers and NX service platforms. However, a T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5's management within a WiNG supported subnet populated by both types of devices. The *Customer Premises Equipment* (CPEs) are the T5 controller managed radio devices using the IPX operating system. These CPEs use a *Digital Subscriber Line* (DSL) as their high speed Internet access mechanism using the CPE's physical wallplate connection and phone jack.<br>After logging on to the T5 device, use the 'cpe' keyword and configure the following mandatory settings:<br>• vlan – Set a VLAN from 1 - 4,094 used as a virtual interface for connections between the T5 controller and its managed CPE devices.<br>• start ip – Set a starting IP address used in a range of addresses available to T5 controller connecting CPE devices.<br>• end ip – Set an end IP address used in a range of addresses available to T5 controller connecting CPE devices. |

**Example**

```
rfs6000-81742D(config)#t5 B4:C7:99:ED:5C:2C
rfs6000-81742D(config-device-B4:C7:99:ED:5C:2C)#?
T5 Device Mode commands:
  adsp-sensor-server  Configure WIPS server
  bridge              Sets MAC address expiration time in the bridge address
                      table
  clock               Configure clock options
  cpe                 T5 CPE configuration
  hostname            Set system's network name
  interface           Select an interface to configure
  ip                  Internet Protocol (IP)
  no                  Negate a command or set its defaults
  ntp                 Configure NTP
  override-wlan       Configure RF Domain level overrides for wlan
  password            T5 password configuration
  qos                 QOS settings
  radius-server       Radius server settings
  t5                  T5 configuration
  t5-logging          Modify message logging facilities
  use                 Set setting to use

  clrscr              Clears the display screen
  commit              Commit all changes made in this session
  do                  Run commands from Exec mode
  end                 End current mode and change to EXEC mode
  exit                End current mode and down to previous mode
  help                Description of the interactive help system
  revert              Revert changes
  service             Service Commands
  show                Show running system information
  write               Write running configuration to memory or terminal

rfs6000-81742D(config-device-B4:C7:99:ED:5C:2C)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the t5 wireless controller identified by the device's MAC address |

## 4.1.95 web-filter-policy

*Global Configuration Commands*

The following table lists commands that enable you to enter the Web Filter policy configuration mode:

**Table 4.51** *Commands Creating a Web-Filter-Policy*

| Command | Description | Reference |
|---|---|---|
| *web-filter-policy* | Creates a new Web Filter policy and enters its configuration mode | *page 4-552* |
| *web-filter-policy-config-mode commands* | Summarizes the Web Filter policy configuration mode commands | *page 4-443* |

### 4.1.95.1 web-filter-policy

*web-filter-policy*

Creates a Web Filtering policy and enters its configuration mode. This policy defines rules managing the local classification database and the cached data. When configured and applied, this policy also enables caching of URL classification records in a local database in a controller-based, *hierarchically managed* (HM) deployment. Use this option to specify the following: classification server details, size of the local database, time for which records are cached in the database, the action taken in case the classification server is unavailable, etc.

The Web filter policy is applied at the profile or device level.

For more information on URL filtering, see *url-filter*.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
web-filter-policy <WEB-FILTER-POLICY-NAME>
```

**Parameters**

- `web-filter-policy <WEB-FILTER-POLICY-NAME>`

| | |
|---|---|
| <WEB-FILTER-POLICY-NAME> | Specify the Web filter policy name. If the policy does not exist, it is created. |

**Example**

```
nx9500-6C8809(config)#web-filter-policy test
nx9500-6C8809(config-web-filter-policy-test)#?
Content Filter Mode commands:
  cache-max-recs       Configure the maximum number of records in local cache
  cache-save-interval  Configure the time a record is saved in local cache
  logging              Select logging method
  no                   Negate a command or set its defaults
  server-host          Configure URL classification server if it is not the
                       adopted controller
  server-unreachable   Permission to access website when classification server
                       is unreachable (default is pass)
  uncategorized-url    Permission to website when server fails to classify the
                       URL request (default is pass)

  clrscr               Clears the display screen
  commit               Commit all changes made in this session
  do                   Run commands from Exec mode
  end                  End current mode and change to EXEC mode
  exit                 End current mode and down to previous mode
  help                 Description of the interactive help system
  revert               Revert changes
  service              Service Commands
  show                 Show running system information
  write                Write running configuration to memory or terminal

nx9500-6C8809(config-web-filter-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing Web filter policy |

### 4.1.95.2 web-filter-policy-config-mode commands

*web-filter-policy*

The following table summarizes Web Filter policy configuration mode commands:

**Table 4.52** *Web-Filter-Policy-Config-Mode Commands*

| Command | Description | Reference |
|---|---|---|
| *cache-max-recs* | Configures the maximum number of records (URLs and Web pages) cached in the local database | *page 4-444* |
| *cache-save-interval* | Configures the maximum time period for which a record (URL and Web page classification entry) is cached in the local database | *page 4-445* |
| *logging* | Configures the method used to log Web filtering events | *page 4-446* |
| *no* | Reverts the selected Web Filter policy settings to default | *page 4-447* |
| *server-host* | Configures the URL classification server in case it is not the adopted controller | *page 4-448* |
| *server-unreachable* | Configures the action taken in case the classification server is unreachable | *page 4-449* |
| *uncategorized-url* | Configures the action taken in case the classification server fails to classify a URL/Website | *page 4-450* |

### 4.1.95.2.1 cache-max-recs

*web-filter-policy-config-mode commands*

Configures the maximum number of records (URL and Web page classification entries) cached in the local database

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
cache-max-recs <1-1000000>
```

**Parameters**

- `cache-max-recs <1-1000000>`

| | |
|---|---|
| cache-max-recs <1-1000000> | Specify the maximum number of records cached in the local database from 1 - 1000000.<br>When configuring this value take into consideration the type of device using the Web Filter policy. The value should approximately be as per the following information:<br>• NX95XX – <1-1000000> (default is 100000)<br>• NX75XX – <1-100000> (default is 10000)<br>• RFS Switches – <1-10000> (default is 1000)<br>• Access Points – <1-1500> (default is 500) |

**Example**

```
nx9500-6C8809(config-web-filter-policy-test)#cache-max-recs 9000

nx9500-6C8809(config-web-filter-policy-test)#show context
web-filter-policy test
 cache-max-recs 9000
nx9500-6C8809(config-web-filter-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Reverts the maximum number of stored records to default. Please see the parameter table for default values for the different device types. |

### 4.1.95.2.2 cache-save-interval

*web-filter-policy-config-mode commands*

Configures the maximum time period, in seconds, for which a record (URL and Web page classification entry) is cached in the local database. Once the specified time has expired the record is removed from the cache.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
cache-save-interval <1-86400>
```

**Parameters**

- `cache-save-interval <1-86400>`

| | |
|---|---|
| cache-save-interval <1-86400> | Specify the maximum time period, in seconds, for which a record is cached in the local database from 1 - 86400 seconds. The default is 60 seconds. |

**Example**

```
nx9500-6C8809(config-web-filter-policy-test)#cache-save-interval 1000

nx9500-6C8809(config-web-filter-policy-test)#show context
web-filter-policy test
 cache-max-recs 9000
 cache-save-interval 1000
nx9500-6C8809(config-web-filter-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Reverts the maximum time period for which a record (URL and Web page classification entry) is cached in the local database to default (60) |

### 4.1.95.2.3 logging

*web-filter-policy-config-mode commands*

Configures the method used to log Web filtering events

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
logging [logfile|syslog]
```

**Parameters**

- `logging [logfile|syslog]`

| | |
|---|---|
| logging [logfile\|syslog] | Selects the method used to log Web filtering events. The options are:<br>• logfile – Logs to a file.<br>• syslog – Logs to the syslog server. This is the default setting. |

**Example**

```
nx9500-6C8809(config-web-filter-policy-test)#logging logfile

nx9500-6C8809(config-web-filter-policy-test)#show context
web-filter-policy test
 logging logfile
nx9500-6C8809(config-web-filter-policy-test)#
```

### 4.1.95.2.4 no

*web-filter-policy-config-mode commands*

Reverts the selected Web Filter policy settings to default, based on the parameters passed

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
no [cache-max-recs|cache-save-interval|server-host|server-unreachable|
uncategorized-url]
```

**Parameters**

- `no <PARAMETERS>`

| | |
|---|---|
| no <PARAMETERS> | Reverts the selected Web Filter policy settings to default, based on the parameters passed. Specify the parameters to revert back to default value. |

**Example**

The following example shows the Web Filter policy 'test' settings before the 'no' command is executed:

```
nx9500-6C8809(config-web-filter-policy-test)#show context
web-filter-policy test
 cache-max-recs 9000
 cache-save-interval 1000
 uncategorized-url block
 server-unreachable block
 server-host ip-address 192.168.13.13
nx9500-6C8809(config-web-filter-policy-test)#

nx9500-6C8809(config-web-filter-policy-test)#no cache-max-recs
nx9500-6C8809(config-web-filter-policy-test)#no server-unreachable
nx9500-6C8809(config-web-filter-policy-test)#no uncategorized-url
```

The following example shows the Web Filter policy 'test' settings after the 'no' command has been executed:

```
nx9500-6C8809(config-web-filter-policy-test)#show context
web-filter-policy test
 cache-save-interval 1000
 server-host ip-address 192.168.13.13
nx9500-6C8809(config-web-filter-policy-test)#
```

### 4.1.95.2.5 server-host

*web-filter-policy-config-mode commands*

Configures the URL classification server in case it is not the adopted controller

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
server-host [host-name <SERVER-HOST-NAME>|ip-address <SERVER-IPv4>|mint-id
<SERVER-MiNT-ID>]
```

**Parameters**

```
• server-host [host-name <SERVER-HOST-NAME>|ip-address <SERVER-IPv4>|mint-id
<SERVER-MiNT-ID>]
```

| | |
|---|---|
| server-host [host-name <SERVER-HOST-NAME>\| ip-address <SERVER-IPv4>\| mint-id <SERVER-MiNT-ID>] | Use one of the following options to identify the URL classification server:<br>• host-name <SERVER-HOST-NAME> – Identifies the classification server by its hostname.<br>• ip-address <SERVER-IPv4> – Identifies the classification server by its IP address.<br>• mint-id <SERVER-MiNT-ID> – Identifies the classification server by its MiNT ID. |

**Example**

```
nx9500-6C8809(config-web-filter-policy-test)#server-host ip-address 192.168.13.13

nx9500-6C8809(config-web-filter-policy-test)#show context
web-filter-policy test
 cache-max-recs 9000
 cache-save-interval 1000
 server-host ip-address 192.168.13.13
nx9500-6C8809(config-web-filter-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the URL classification server's configured details, such as hostname, ip-address, or MiNT ID. |

### 4.1.95.2.6 server-unreachable

*web-filter-policy-config-mode commands*

Configures the action taken in case the classification server is unreachable. Based on the value configured the an end user's request for a URL/Website is either blocked or passed.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
server-unreachable [block|pass]
```

**Parameters**

- `server-unreachable [block|pass]`

| | |
|---|---|
| server-unreachable [block\|pass] | Configures the action taken in case the classification server is unreachable. The options are:<br>• block – Denies access to the requested URL/Website<br>• pass – Allows access to the requested URL/Website. This is the default value. |

**Example**

```
nx9500-6C8809(config-web-filter-policy-test)#server-unreachable block

nx9500-6C8809(config-web-filter-policy-test)#show context
web-filter-policy test
 cache-max-recs 9000
 cache-save-interval 1000
 server-unreachable block
 server-host ip-address 192.168.13.13
nx9500-6C8809(config-web-filter-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Reverts the action taken in case the classification server is unreachable to default (pass) |

### 4.1.95.2.7 uncategorized-url

*web-filter-policy-config-mode commands*

Configures the action taken in case the classification server fails to classify a URL/Website. Based on the value configured the an end user's request for a non-classified URL/Website is either blocked or passed.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
uncategorized-url [block|pass]
```

**Parameters**

- `uncategorized-url [block|pass]`

| | |
|---|---|
| uncategorized-url [block\|pass] | Configures the action taken in case the classification server fails to classify a URL/ Website. The options are:<br>• block – Denies access to the requested non-classified URL/Website<br>• pass – Allows access to the requested non-classified URL/Website. This is the default value. |

**Example**

```
nx9500-6C8809(config-web-filter-policy-test)#uncategorized-url block

nx9500-6C8809(config-web-filter-policy-test)#show context
web-filter-policy test
 cache-max-recs 9000
 cache-save-interval 1000
 uncategorized-url block
 server-unreachable block
 server-host ip-address 192.168.13.13
nx9500-6C8809(config-web-filter-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Reverts the action taken in case the classification server fails to classify a URL/ Website to default (pass) |

## 4.1.96 wips-policy

*Global Configuration Commands*

Configures a WIPS policy

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
wips-policy <WIPS-POLICY-NAME>
```

**Parameters**

- `wips-policy <WIPS-POLICY-NAME>`

| | |
|---|---|
| <WIPS-POLICY-NAME> | Specify the WIPS policy name. If the policy does not exist, it is created. |

**Example**

```
rfs6000-81742D(config)#wips-policy test
rfs6000-81742D(config-wips-policy-test)#?
Wips Policy Mode commands:
  ap-detection                Rogue AP detection
  enable                      Enable this wips policy
  event                       Configure an event
  history-throttle-duration   Configure the duration for which event duplicates
                              are not stored in history
  interference-event          Specify events which will contribute to smart-rf
                              wifi interference calculations
  no                          Negate a command or set its defaults
  signature                   Signature to configure
  use                         Set setting to use

  clrscr                      Clears the display screen
  commit                      Commit all changes made in this session
  do                          Run commands from Exec mode
  end                         End current mode and change to EXEC mode
  exit                        End current mode and down to previous mode
  help                        Description of the interactive help system
  revert                      Revert changes
  service                     Service Commands
  show                        Show running system information
  write                       Write running configuration to memory or terminal

rfs6000-81742D(config-wips-policy-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing WIPS policy |

**NOTE:** For more information on WIPS policy commands, see *Chapter 20, WIPS-POLICY*.

## 4.1.97 wlan

*Global Configuration Commands*

Configures a *Wireless Local Area Network* (WLAN)

The following table lists WLAN configuration mode commands:

**Table 4.53** *WLAN-Policy Config Commands*

| Command | Description | Reference |
|---|---|---|
| *wlan* | Creates a new wireless LAN and enters its configuration mode | *page 4-453* |
| *wlan-mode commands* | Summarizes WLAN configuration mode commands | *page 4-457* |

### 4.1.97.1 wlan

*wlan*

Configures a WLAN and enters its configuration mode. Use this command to modify an existing WLAN's settings.

A WLAN is a data-communications system that flexibly extends the functionality of a wired LAN. A WLAN links two or more computers or devices using spread-spectrum or *Orthogonal Frequency Division Multiplexing* (OFDM) modulation based technology. WLANs do not require lining up devices for line-of-sight transmission, and are thus, desirable for wireless networking. Roaming users can be handed off from one access point to another, like a cellular phone system. WLANs can therefore be configured around the needs of specific user groups, even when they are not in physical proximity.

WLANs can provide an abundance of services, including data communications (allowing mobile devices to access applications), e-mail, file, and print services or even specialty applications (such as guest access control and asset tracking).

Each WLAN configuration contains encryption, authentication and QoS policies and conditions for user connections. Connected access point radios transmit periodic beacons for each BSS. A beacon advertises the SSID, security requirements, supported data rates of the wireless network to enable clients to locate and connect to the WLAN.

WLANs are mapped to radios on each access point. A WLAN can be advertised from a single access point radio or can span multiple access points and radios. WLAN configurations can be defined to provide service to specific areas of a site. For example, a guest access WLAN may only be mapped to a 2.4 GHz radio in a lobby or conference room providing limited coverage, while a data WLAN is mapped to all 2.4 GHz and 5.0 GHz radios at the branch site to provide complete coverage.

The maximum number of WLANs supported by different devices is as follows:

- RFS4000 and RFS6000 wireless controllers – 32 WLANs
- NX95XX series service platforms – 1000 WLANs
- Access Points – 16 WLANs

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
wlan {<WLAN-NAME>|containing <WLAN-NAME>}
```

**Parameters**

- `wlan {<WLAN-NAME>|containing <WLAN-NAME>}`

| | |
|---|---|
| wlan <WLAN-NAME> | Configures a new WLAN<br>• <WLAN-NAME> – Optional. Specify the WLAN name.<br>The WLAN name could be a logical representation of its coverage area (for example, engineering, marketing, etc.).The name cannot exceed 32 characters. |
| containing <WLAN-NAME> | Optional. Configures an existing WLAN's settings<br>• <WLAN-NAME> – Specify a sub-string in the WLAN name. Use this parameter to filter a WLAN. This option allows you to select and enter the configuration mode of one or more WLANs. |

**Example**

```
rfs6000-81742D(config)#wlan 1
rfs6000-81742D(config-wlan-1)#?
Wireless LAN Mode commands:
  accounting                          Configure how accounting records are
                                      created for this wlan
  acl                                 Actions taken based on ACL
                                      configuration [packet drop being one
                                      of them]
  answer-broadcast-probes             Include this wlan when responding to
                                      probe requests that do not specify an
                                      SSID
  assoc-response                      Association response threshold
  association-list                    Configure the association list for
                                      the wlan
  authentication-type                 The authentication type of this WLAN
  bridging-mode                       Configure how packets to/from this
                                      wlan are bridged
  broadcast-dhcp                      Configure broadcast DHCP packet
                                      handling
  broadcast-ssid                      Advertise the SSID of the WLAN in
                                      beacons
  captive-portal-enforcement          Enable captive-portal enforcement on
                                      the wlan
  client-access                       Enable client-access (normal data
                                      operations) on this wlan
  client-client-communication         Allow switching of frames from one
                                      wireless client to another on this
                                      wlan
  client-load-balancing               Configure load balancing of clients
                                      on this wlan
  controller-assisted-mobility        Enable controller assisted mobility
                                      to determine wireless clients' VLAN
                                      assignment
  data-rates                          Specify the 802.11 rates to be
                                      supported on this wlan
  description                         Configure a description of the usage
                                      of this wlan
  downstream-group-addressed-forwarding  Enable downstream group addressed
                                      forwarding of packets
  dpi                                 Deep-Packet-Inspection (Application
                                      Assurance)
  dynamic-vlan-assignment             Dynamic VLAN assignment configuration
  eap-types                           Configure client access based on
                                      eap-type used for authentication
  encryption-type                     Configure the encryption to use on
                                      this wlan
  enforce-dhcp                        Drop packets from Wireless Clients
                                      with static IP address
  fast-bss-transition                 Configure support for 802.11r Fast
```

```
                                        BSS Transition
  http-analyze                          Enable HTTP URL analysis on the wlan
  ip                                    Internet Protocol (IP)
  ipv6                                  Internet Protocol version 6 (IPv6)
  kerberos                              Configure kerberos authentication
                                        parameters
  mac-authentication                    Configure mac-authentication related
                                        parameters
  no                                    Negate a command or set its defaults
  nsight                                Nsight Server
  opendns                               OpenDNS related config for this wlan
  protected-mgmt-frames                 Protected Management Frames (IEEE
                                        802.11w) related configuration (DEMO
                                        FEATURE)
  proxy-arp-mode                        Configure handling of ARP requests
                                        with proxy-arp is enabled
  proxy-nd-mode                         Configure handling of IPv6 ND
                                        requests with proxy-nd is enabled
  qos-map                               Support the 802.11u QoS map element
                                        and frame
  radio-resource-measurement            Configure support for 802.11k Radio
                                        Resource Measurement
  radius                                Configure RADIUS related parameters
  registration                          Enable dynamic registration of device
                                        (or) user
  relay-agent                           Configure dhcp relay agent info
  shutdown                              Shutdown this wlan
  ssid                                  Configure the Service Set Identifier
                                        for this WLAN
  t5-client-isolation                   Isolate traffic among clients
  t5-security                           Configure encryption and
                                        authentication
  time-based-access                     Configure client access based on time
  use                                   Set setting to use
  vlan                                  Configure the vlan where traffic from
                                        this wlan is mapped
  vlan-pool-member                      Add a member vlan to the pool of
                                        vlans for the wlan (Note:
                                        configuration of a vlan-pool
                                        overrides the 'vlan' configuration)
  wep128                                Configure WEP128 parameters
  wep64                                 Configure WEP64 parameters
  wing-extensions                       Enable support for WiNG-Specific
                                        extensions to 802.11
  wireless-client                       Configure wireless-client specific
                                        parameters
  wpa-wpa2                              Modify tkip-ccmp (wpa/wpa2) related
                                        parameters

  clrscr                                Clears the display screen
  commit                                Commit all changes made in this
                                        session
  do                                    Run commands from Exec mode
  end                                   End current mode and change to EXEC
                                        mode
  exit                                  End current mode and down to previous
                                        mode
  help                                  Description of the interactive help
                                        system
  revert                                Revert changes
  service                               Service Commands
  show                                  Show running system information
  write                                 Write running configuration to memory
                                        or terminal

rfs6000-81742D(config-wlan-1)#
```

The following example shows how to use the ‘containing’ keyword to enter the configuration mode of an existing WLAN:

```
rfs6000-81742D(config)#wlan containing wlan1
rfs6000-81742D(config-wlan-{'containing': 'wlan1'})#
```

### 4.1.97.2 wlan-mode commands

*wlan*

This section documents the WLAN configuration mode commands in detail.

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

To navigate to this instance, use the following command:

```
<DEVICE>(config)#wlan <WLAN-NAME>
```

The following table summarizes WLAN configuration mode commands:

**Table 4.54** *WLAN-Mode Commands*

| Command | Description | Reference |
|---|---|---|
| *accounting* | Defines a WLAN accounting configuration | *page 4-460* |
| *acl* | Defines the actions based on an ACL rule configuration | *page 4-462* |
| *answer-broadcast-probes* | Allows a WLAN to respond to probes for broadcast ESS | *page 4-464* |
| *assoc-response* | Configures a minimum *receive signal strength indication* (RSSI) value, below which the WLAN does not send a response to a client's association request | *page 4-465* |
| *association-list* | Attaches an existing global association list to a WLAN | *page 4-466* |
| *authentication-type* | Sets a WLAN's authentication type | *page 4-467* |
| *bridging-mode* | Configures how packets to/from this WLAN are bridged | *page 4-469* |
| *broadcast-dhcp* | Configures broadcast DHCP packet handling | *page 4-470* |
| *broadcast-ssid* | Advertises a WLAN's SSID in beacons | *page 4-471* |
| *captive-portal-enforcement* | Configures a WLAN's captive portal enforcement | *page 4-472* |
| *client-access* | Enables WLAN client access (normal data operations) | *page 4-473* |
| *client-client-communication* | Allows the switching of frames from one wireless client to another on a WLAN | *page 4-474* |
| *client-load-balancing* | Enables load balancing of WLAN clients | *page 4-475* |
| *controller-assisted-mobility* | Enables controller assisted mobility to determine wireless clients' VLAN assignment | *page 4-477* |
| *data-rates* | Specifies the 802.11 rates supported on the WLAN | *page 4-478* |
| *description* | Sets a WLAN's description | *page 4-481* |
| *downstream-group-addressed-forwarding* | Enables forwarding of downstream packets addressed to a group | *page 4-482* |
| *dpi* | Enables extraction of metadata flows on the WLAN | *page 4-483* |
| *dynamic-vlan-assignment* | Configures dynamic VLAN assignment on this WLAN | *page 4-485* |
| *eap-types* | Configures client access based on eap-type used for authentication | *page 4-486* |
| *encryption-type* | Sets a WLAN's encryption type | *page 4-488* |

**Table 4.54** *WLAN-Mode Commands*

| Command | Description | Reference |
|---|---|---|
| *enforce-dhcp* | Drops packets from clients with a static IP address | *page 4-489* |
| *fast-bss-transition* | Configures support for 802.11r fast BSS transition on a WLAN | *page 4-490* |
| *http-analyze* | Enables HTTP URL analysis on the WLAN | *page 4-491* |
| *ip* | Configures IPv4 settings on this WLAN | *page 4-493* |
| *ipv6* | Configures IPv6 settings on this WLAN | *page 4-494* |
| *kerberos* | Configures Kerberos authentication parameters | *page 4-495* |
| *mac-authentication* | Configures MAC authentication parameters | *page 4-497* |
| *no* | Negates a command or reverts settings to their default | *page 4-498* |
| *nsight* | Enables retention of guest client history in the NSight database | *page 4-502* |
| *opendns* | Configures the device ID, which is embedded in each DNS query packet going out from an access point, wireless controller, or service platform to the OpenDNS server | *page 4-503* |
| *protected-mgmt-frames* | Enables and configures the WLAN's frame protection mode and security association | *page 4-505* |
| *proxy-arp-mode* | Enables the proxy ARP mode for ARP requests | *page 4-507* |
| *proxy-nd-mode* | Configures the proxy ND mode for this WLAN member clients as either strict or dynamic | *page 4-508* |
| *qos-map* | Enables support for 802.11u QoS map element and frames | *page 4-509* |
| *radio-resource-measurement* | Enables support for 802.11k radio resource measurement | *page 4-510* |
| *radius* | Configures RADIUS parameters | *page 4-511* |
| *registration* | Configures settings enabling dynamic registration of devices. Use this command to specify the mode of registration and to configure corresponding parameters. | *page 4-513* |
| *relay-agent* | Enables support for DHCP relay agent information (option 82) feature on this WLAN | *page 4-516* |
| *shutdown* | Auto shuts down a WLAN | *page 4-518* |
| *ssid* | Configures a WLAN's SSID | *page 4-520* |
| *t5-client-isolation* | Disallows clients connecting to the WLAN to communicate with one another | *page 4-521* |
| *t5-security* | Configures T5 PowerBroadband security settings | *page 4-522* |
| *time-based-access* | Configures time-based client access | *page 4-524* |
| *use* | Defines WLAN mode configuration settings | *page 4-525* |
| *vlan* | Sets VLAN assignment for a WLAN | *page 4-529* |
| *vlan-pool-member* | Adds a member VLAN to the pool of VLANs for a WLAN | *page 4-530* |
| *wep128* | Configures WEP128 parameters | *page 4-532* |
| *wep64* | Configures WEP64 parameters | *page 4-534* |

**Table 4.54** *WLAN-Mode Commands*

| Command | Description | Reference |
|---|---|---|
| *wing-extensions* | Enables support for WiNG specific extensions to 802.11 | *page 4-536* |
| *wireless-client* | Configures the transmit power for wireless clients transmission | *page 4-539* |
| *wpa-wpa2* | Modifies TKIP and CCMP (WPA/WPA2) related parameters | *page 4-542* |
| *service* | Invokes service commands applicable in the WLAN configuration mode | *page 4-545* |

### 4.1.97.2.1 accounting

*wlan-mode commands*

Defines the WLAN's accounting configuration

Accounting is the method of collecting user data, such as start and stop times, executed commands (for example, PPP), number of packets and number of bytes received and transmitted. This data is sent to the security server for billing, auditing, and reporting purposes. Accounting enables wireless network administrators to track the services and network resources accessed and consumed by users. When enabled, this feature allows the network access server to report and log user activity to a RADIUS security server in the form of accounting records. Each accounting record is comprised of AV pairs and is stored on the access control server. The data can be analyzed for network management, client billing, and/or auditing. Accounting methods must be defined through AAA policies.

Accounting can be enabled and applied to access point, wireless controller, or service platform managed WLANs. Once enabled, it uniquely logs accounting events specific to the managed WLAN. Accounting logs contain information about the use of remote access services by users. This information is of great assistance in partitioning local versus remote users and how to best accommodate each. Remote user information can be archived to a location outside of the access point for periodic network and user permission administration.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
accounting [radius|syslog|wait-client-ip]

accounting [radius|wait-client-ip]

accounting syslog [host|mac-address-format]

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

accounting syslog mac-address-format [middle-hyphen|no-delim|pair-colon|pair-hyphen|quad-dot] case [lower|upper]
```

**Parameters**

- `accounting [radius|wait-client-ip]`

| | |
|---|---|
| accounting radius | Enables support for WLAN RADIUS accounting messages. This option is disabled by default.<br>When enabled, the WLAN uses an external RADIUS resource for accounting.<br>Use the *use > aaa-policy > <AAA-POLICY-NAME>* command to associate an appropriate AAA policy with this WLAN. This AAA policy should be existing and should define the accounting, authentication, and authorization parameters. |
| accounting wait-client-ip | Enables waiting for client's IP before commencing the accounting procedure |

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

| | |
|---|---|
| accounting syslog | Enables support for WLAN syslog accounting messages in standard syslog format (RFC 3164). This option is disabled by default. |
| host <IP/HOSTNAME> | Configures a syslog destination hostname or IP address for accounting records<br>• <IP/HOSTNAME> – Specify the IP address or name of the destination host. |
| port <1-65535> | Optional. Configures the syslog server's UDP port (this port is used to connect to the server)<br>• <1-65535> – Specify the port from 1 - 65535. Default port is 514. |
| proxy-mode [none\| through-controller\| through-rf-domain-manager] | Optional. Configures the request proxying mode<br>• none – Requests are directly sent to the server from the device<br>• through-controller – Proxies requests through the controller (access point, wireless controller, or service platform) configuring the device<br>• through-rf-domain-manager – Proxies requests through the local RF Domain manager |

```
• accounting syslog mac-address-format [middle-hyphen|no-delim|pair-colon|pair-
hyphen|quad-dot] case [lower|upper]
```

| | |
|---|---|
| accounting syslog | Enables support for WLAN syslog accounting messages |
| mac-address-format | Configures the MAC address format used in syslog messages |
| middle-hyphen | Configures the MAC address format with middle hyphen (AABBCC-DDEEFF) |
| no-delim | Configures the MAC address format without delimitors (AABBCCDDEEFF) |
| pair-colon | Configures the MAC address format with pair-colon delimitors (AA:BB:CC:DD:EE:FF) |
| pair-hyphen | Configures the MAC address format with pair-hyphen deli mi tors (AA-BB-CC-DD-EE-FF). This is the default setting. |
| quad-dot | Configures the MAC address format with quad-dot delimitors (AABB.CCDD.EEFF) |
| case [lower\|upper] | The following keywords are common to all:<br>• case – Specifies MAC address case (upper or lower)<br>• lower – Specifies MAC address is filled in lower case (for example, aa-bb-cc-dd-ee-ff)<br>• upper – Specifies MAC address is filled in upper case (for example, AA-BB-CC-DD-EE-FF) |

**Example**

```
rfs6000-81742D(config-wlan-test)#accounting syslog host 172.16.10.4 port 2 proxy-
mode none

rfs6000-81742D(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 accounting syslog host 172.16.10.4 port 2
rfs6000-81742D(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables sending of accounting message to the RADIUS server, disables syslog accounting, or disables waiting for client's IP before sending accounting messages |

### 4.1.97.2.2 acl

*wlan-mode commands*

Defines the actions taken based on an ACL rule configuration

Use the *use > ip-access-list <IP-ACCESS-LIST-NAME>* command to associate an ACL with the WLAN. The ACL rule is determined by the associated ACL's configuration.

A firewall is a mechanism enforcing access control, and is considered a first line of defense in protecting proprietary information within the network. The means by which this is accomplished varies, but in principle, a firewall can be thought of as mechanisms allowing and denying data traffic in respect to administrator defined rules. For an overview of firewalls, see *FIREWALL-POLICY*.

WLANs use firewalls like *Access Control Lists* (ACLs) to filter/mark packets based on the WLAN from which they arrive, as opposed to filtering packets on layer 2 ports. An ACL contains an ordered list of *Access Control Entries* (ACEs). Each ACE specifies an action and a set of conditions (rules) a packet must satisfy to match the ACE. The order of conditions in the list is critical since filtering is stopped after the first match.

IP based firewall rules are specific to source and destination IP addresses and the unique rules and precedence orders assigned. Both IP and non-IP traffic on the same layer 2 interface can be filtered by applying both an IP ACL and a MAC.

Additionally, administrators can filter layer 2 traffic on a physical layer 2 interface using MAC addresses. A MAC Firewall rule uses source and destination MAC addresses for matching operations, where the result is a typical allow, deny or mark designation to WLAN packet traffic.

Keep in mind IP and non-IP traffic on the same layer 2 interface can be filtered by applying both an IP ACL and a MAC ACL to the interface.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
acl exceed-rate wireless-client-denied-traffic <0-1000000> {blacklist <0-86400>|
  disassociate}
```

**Parameters**

- `acl exceed-rate wireless-client-denied-traffic <0-1000000> {blacklist <0-86400>| disassociate}`

| | |
|---|---|
| acl exceed-rate | Sets the action taken based on an ACL rule configuration (for example, drop a packet)<br>• exceed-rate – Action is taken when the rate exceeds a specified value |

| | |
|---|---|
| wireless-client-denied-traffic <0-1000000> | Sets the action to deny traffic to the wireless client when the rate exceeds the specified value<br>• <0-1000000> – Specify a allowed rate threshold of disallowed traffic in packets/sec.<br>If enabled, this option allows an associated client, exceeding the thresholds configured for storm traffic, to be either de-authenticated or blacklisted depending on the action selected. This option is disabled by default. |
| blacklist <0-86400> | Optional. When enabled, sets the time interval, in seconds, to blacklist a wireless client.<br>• <0-86400> – Configures the blacklist duration from 0 - 86400 seconds. Offending clients are re-authenticated once the blacklist duration, configured here, has exceeded. |
| disassociate | Optional. When enabled, disassociates a wireless client |

**Example**

```
rfs6000-81742D(config-wlan-test)#acl exceed-rate wireless-client-denied-traffic
20 disassociate

rfs6000-81742D(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 accounting syslog host 172.16.10.4 port 2
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
rfs6000-81742D(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the action (de-authenticate or blacklist) to be taken when an associated client exceeds the thresholds configured for storm traffic |

### 4.1.97.2.3 answer-broadcast-probes

*wlan-mode commands*

Allows the WLAN to respond to probe requests that do not specify a SSID. These probes are for broadcast ESS. This feature is enabled by default.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
answer-broadcast-probes
```

**Parameters**

None

**Example**

```
rfs6000-81742D(config-wlan-1)#answer-broadcast-probes
rfs6000-81742D(config-wlan-1)#
```

**Related Commands**

| | |
|---|---|
| *no* | Does not allow this WLAN to respond to probe requests that do not specify a SSID |

### 4.1.97.2.4 assoc-response

*wlan-mode commands*

Configures the deny-threshold and rssi-threshold values. These threshold values are considered when responding to a client's association/authentication request.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
assoc-response [deny-threshold <1-12>|rssi-threshold <-100--40>]
```

**Parameters**

- `assoc-response [deny-threshold <1-12>|rssi-threshold <-100--40>]`

| | |
|---|---|
| assoc-response | Configures the association response thresholds |
| deny-threshold <1-12> | Configures the number of times association/authentication request, from a client, is ignored if the RSSI is less than the configured RSSI threshold. This option is disabled by default.<br>• <1-12> – Specify the deny-threshold from 1 - 12. |
| rssi-threshold <-100--40> | Configures an association response RSSI threshold value. If the RSSI is below the configured threshold value, the client's association/authentication request is ignored. This option is disabled by default.<br>• rssi-threshold <-100--40> – Specify a value from -100 - -40 dBm. |

**Example**

```
nx9500-6C8809(config-wlan-test)#assoc-response rssi-threshold -60
nx9500-6C8809(config-wlan-test)#assoc-response deny-threshold 4

nx9500-6C8809(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode local
 encryption-type none
 authentication-type none
 assoc-response rssi-threshold -60
 assoc-response deny-threshold 4
 registration user group-name guest expiry-time 2000 agreement-refresh 14400
nx9500-6C8809(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the configured deny-threshold and rssi-threshold values |

### 4.1.97.2.5 association-list

*wlan-mode commands*

Attaches an existing global association list with this WLAN. For more information on global association lists, see *global-association-list*.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
association-list global <GLOBAL-ASSO-LIST-NAME>
```

**Parameters**

- `association-list global <GLOBAL-ASSO-LIST-NAME>`

| | |
|---|---|
| association-list global <GLOBAL-ASSO-LIST-NAME> | Attaches an existing global association list with this WLAN<br>• <GLOBAL-ASSO-LIST-NAME> – Specify the global association list name (should be existing and configured). |

**Example**

```
rfs4000-229D58(config-wlan-test)#association-list global my-clients

rfs4000-229D58(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 association-list global my-clients
rfs4000-229D58(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the global association list's association with this WLAN |

### 4.1.97.2.6 authentication-type

*wlan-mode commands*

Sets the WLAN's authentication type

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
authentication-type [eap|eap-mac|eap-psk|kerberos|mac|none]
```

**Parameters**

- `authentication-type [eap|eap-mac|eap-psk|kerberos|mac|none]`

| | |
|---|---|
| authentication-type | Configures a WLAN's authentication type<br>The authentication types are: EAP, EAP-MAC, EAP-PSK, Kerberos, MAC, and none. |
| eap | Configures EAP authentication (802.1X)<br>EAP is the de-facto standard authentication method used to provide secure authenticated access to controller managed WLANs. EAP provides mutual authentication, secured credential exchange, dynamic keying and strong encryption. 802.1X EAP can be deployed with WEP, WPA or WPA2 encryption schemes to further protect user information forwarded over controller managed WLANs.<br>The EAP process begins when an unauthenticated supplicant (client device) tries to connect with an authenticator (in this case, the authentication server). An access point passes EAP packets from the client to an authentication server on the wired side of the access point. All other packet types are blocked until the authentication server (typically, a RADIUS server) verifies the client's identity.<br>If using EAP authentication ensure that a AAA policy is mapped to the WLAN. |
| eap-mac | Configures EAP or MAC authentication depending on client. (This setting is valid only with the None encryption type.<br>EAP-MAC is useful when in a hotspot environment, as some clients support EAP and an administrator may want to authenticate based on just the MAC address of the device. |
| eap-psk | Configures EAP authentication or pre-shared keys depending on client (This setting is only valid with *Temporal Key Integrity Protocol* (TKIP) or *Counter Mode with Cipher Block Chaining Message Authentication Code Protocol* (CCMP) encryption types).<br>When using PSK with EAP, the controller sends a packet requesting a secure link using a pre-shared key. The controller and authenticating device must use the same authenticating algorithm and pass code during authentication. EAP-PSK is useful when transitioning from a PSK network to one that supports EAP.<br>If using eap-psk authentication ensure that a AAA policy is mapped to the WLAN. |

| | |
|---|---|
| kerberos | Configures Kerberos authentication (encryption will change to WEP128 if it's not already WEP128 or Keyguard)<br>Kerberos (designed and developed by MIT) provides strong authentication for client/server applications using secret-key cryptography. Using Kerberos, a client must prove its identity to a server (and vice versa) across an insecure network connection.<br>Once a client and server use Kerberos to validate their identity, they encrypt all communications to assure privacy and data integrity. Kerberos can only be used on the access point with 802.11b clients. Kerberos uses *Network Time Protocol* (NTP) for synchronizing the clocks of its *Key Distribution Center* (KDC) server(s). |
| mac | Configures MAC authentication (RADIUS lookup of MAC address)<br>MAC is a device level authentication method used to augment other security schemes when legacy devices are deployed using static WEP.<br>MAC authentication can be used for device level authentication by permitting WLAN access based on device MAC address. MAC authentication is typically used to augment WLAN security options that do not use authentication (such as static WEP, WPA-PSK and WPA2-PSK) MAC authentication can also be used to assign VLAN memberships, Firewall policies and time and date restrictions.<br>MAC authentication can only identify devices, not users.<br>If using mac authentication ensure that an AAA policy is mapped to the WLAN. |
| none | No authentication is used or the client uses pre-shared keys. This is the default value. |

**Example**

```
rfs6000-81742D(config-wlan-test)#authentication-type eap

rfs6000-81742D(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode tunnel
 encryption-type none
 authentication-type eap
 accounting syslog host 172.16.10.4 port 2
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
rfs6000-81742D(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Resets the authentication mode used with this WLAN to default (none/pre-shared keys) |

### 4.1.97.2.7 bridging-mode

*wlan-mode commands*

Configures how packets are bridged to and from a WLAN

Use this command to define which VLANs are bridged, and how local VLANs are bridged between the wired and wireless sides of the network.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
bridging-mode [local|tunnel]
```

**Parameters**

```
• bridging-mode [local|tunnel]
```

| | |
|---|---|
| bridging-mode | Configures how packets are bridged to and from a WLAN. The options are local and tunnel. |
| local | Bridges packets between WLAN and local ethernet ports. This is the default mode. |
| tunnel | Tunnels packets to other devices (typically a wireless controller or service platform) |

**Example**

```
rfs6000-81742D(config-wlan-test)#bridging-mode local

rfs6000-81742D(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode local
 encryption-type none
 authentication-type eap
 accounting syslog host 172.16.10.4 port 2
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
rfs6000-81742D(config-wlan-test)#
```

### 4.1.97.2.8 broadcast-dhcp

*wlan-mode commands*

Configures broadcast DHCP packet handling parameters

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
broadcast-dhcp validate-offer
```

**Parameters**

- `broadcast-dhcp validate-offer`

| | |
|---|---|
| validate-offer | Enables validation of the broadcast DHCP packet destination (a wireless client associated to the radio) before forwarding over the air. This option is disabled by default. |

**Example**

```
rfs6000-81742D(config-wlan-test)#broadcast-dhcp validate-offer

rfs6000-81742D(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode local
 encryption-type none
 authentication-type eap
 accounting syslog host 172.16.10.4 port 2
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 broadcast-dhcp validate-offer
rfs6000-81742D(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables validation of the broadcast DHCP packet destination (a wireless client associated to the radio) before forwarding over the air |

### 4.1.97.2.9 broadcast-ssid

*wlan-mode commands*

Advertises the WLAN SSID in beacons. If a hacker tries to isolate and hack a SSID from a client, the SSID will display since the ESSID is in the beacon. This feature is enabled by default.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
broadcast-ssid
```

**Parameters**

None

**Example**

```
rfs6000-81742D(config-wlan-1)#broadcast-ssid
rfs6000-81742D(config-wlan-1)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables the broadcasting of the WLAN's SSID in beacons |

### 4.1.97.2.10 captive-portal-enforcement

*wlan-mode commands*

Configures the captive portal enforcement on this WLAN. When enabled, provides successfully authenticated guests temporary and restricted access to the network. If enforcing captive-portal authentication, specify the captive-portal policy to use. For more information, see *use*.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
captive-portal-enforcement {fall-back}
```

**Parameters**

- `captive-portal-enforcement {fall-back}`

| | |
|---|---|
| captive-portal-enforcement | Enables captive portal enforcement on a WLAN. This option is disabled by default. |
| fall-back | Optional. Enforces captive portal validation if WLAN authentication fails (applicable to EAP or MAC authentication only) |

**Example**

```
rfs6000-81742D(config-wlan-test)#captive-portal-enforcement fall-back

rfs6000-81742D(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode local
 encryption-type none
 authentication-type eap
 accounting syslog host 172.16.10.4 port 2
 captive-portal-enforcement fall-back
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 broadcast-dhcp validate-offer
rfs6000-81742D(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables captive portal enforcement |

### 4.1.97.2.11 client-access

*wlan-mode commands*

Enables WLAN client access (for normal data operations)

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
client-access
```

**Parameters**

None

**Example**

```
rfs6000-81742D(config-wlan-1)#client-access
rfs6000-81742D(config-wlan-1)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables WLAN client access |

### 4.1.97.2.12 client-client-communication

*wlan-mode commands*

Allows frame switching from one client to another on a WLAN

This option is enabled by default. It allows clients to exchange packets with other clients. It does not necessarily prevent clients on other WLANs from sending packets to this WLAN, but as long as this setting is also disabled on that WLAN, clients are not permitted to interoperate.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
client-client-communication
```

**Parameters**

None

**Example**

```
rfs6000-81742D(config-wlan-1)#client-client-communication
rfs6000-81742D(config-wlan-1)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables frame switching from one client to another on a WLAN |

### 4.1.97.2.13 client-load-balancing

*wlan-mode commands*

Enforces client load balancing on a WLAN's access point radios. AP6522, AP6532, AP6562, AP81XX, and AP82XX models can support 256 clients per access point. AP6511 and AP6521 models can support up to 128 clients per access point. When enforced, loads are balanced by ignoring association and probe requests. Probe and association requests are not responded to, forcing a client to associate with another access point radio.

This feature is disabled by default.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
client-load-balancing {allow-single-band-clients|band-discovery-intvl|
capability-ageout-time|max-probe-req|probe-req-invl}

client-load-balancing {allow-single-band-clients [2.4ghz|5ghz]|band-discovery-
intvl <0-10000>|capability-ageout-time <0-10000>}

client-load-balancing {max-probe-req|probe-req-intvl} [2.4ghz|5ghz] <0-10000>
```

**Parameters**

- `client-load-balancing {allow-single-band-clients [2.4ghz|5ghz]|band-discovery-intvl <0-10000>|capability-ageout-time <0-10000>}`

| | |
|---|---|
| client-load-balancing | Configures client load balancing on a WLAN |
| allow-single-band-clients [2.4ghz\|5ghz] | Optional. Allows single band clients to associate even during load balancing<br>• 2.4ghz – Enables load balancing across 2.4 GHz channels<br>• 5ghz – Enables load balancing across 5.0 GHz channels<br>This option is enabled by default for 2.4 and 5.0 GHz radios. |
| band-discovery-intvl <0-10000> | Optional. Configures the interval to discover a client's band capability before connection<br>• <0-10000> – Specify a value from 0 - 10000 seconds. The default is 10 seconds. |
| capability-ageout-time <0-10000> | Optional. Configures a client's capability ageout interval. This is the time for which a client's capabilities are retained in the device's internal table. Once this time is exceeded the client's capabilities are aged out.<br>• <0-10000> – Specify a value from 0 - 10000 seconds. The default is 3600 seconds. |

- `client-load-balancing {max-probe-req|probe-req-intvl} [2.4ghz|5ghz] <0-10000>`

| | |
|---|---|
| client-load-balancing | Configures WLAN client load balancing |
| max-probe-req [2.4ghz\|5ghz] <0-10000> | Optional. Configures client probe request interval limits for device association<br>• 2.4ghz – Configures maximum client probe requests on 2.4 GHz radios<br>• 5ghz – Configures maximum client probe requests on 5.0 GHz radios<br>• <0-10000> – Specify a client probe request threshold from 0 - 10000. The default for both 2.4 and 5.0 GHz radios is 60. |

| | |
|---|---|
| probe-req-intvl [2.4ghz\|5ghz] <0-10000> | Optional. Configures client probe request interval limits for device association<br>• 2.4ghz – Configures the client probe request interval on 2.4 GHz radios<br>• 5ghz – Configures the client probe request interval on 5.0 GHz radios<br>• <0-10000> – Specify a value from 0 - 10000. The default for both 2.4 and 5.0 GHz radios is 10 seconds. |

**Example**

```
rfs6000-81742D(config-wlan-test)#client-load-balancing band-discovery-intvl 2

rfs6000-81742D(config-wlan-test)#client-load-balancing probe-req-intvl 5ghz 5

rfs6000-81742D(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode local
 encryption-type none
 authentication-type eap
 accounting syslog host 172.16.10.4 port 2
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 captive-portal-enforcement fall-back
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 broadcast-dhcp validate-offer
rfs6000-81742D(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables client load balancing on a WLAN's access point radios |

### 4.1.97.2.14 controller-assisted-mobility

*wlan-mode commands*

Enables controller or service platform assisted mobility to determine a wireless client's VLAN assignment. When enabled, a controller or service platform's mobility database is used to assist in roaming between RF Domains. This option is disabled by default.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
controller-assisted-mobility
```

**Parameters**

None

**Example**

```
rfs4000-229D58(config-wlan-test)#controller-assisted-mobility

rfs4000-229D58(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 controller-assisted-mobility
rfs4000-229D58(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables controller or service platform assisted mobility to determine a wireless client's VLAN assignment |

### 4.1.97.2.15 data-rates

*wlan-mode commands*

Specifies the 802.11 rates supported on a WLAN

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
data-rates [2.4GHz|5GHz]

data-rates 2.4GHz [b-only|bg|bgn|custom|default|g-only|gn]

data-rates 2.4GHz custom [1|11|12|18|2|24|36|48|5.5|54|6|9|basic-1|basic-11|
basic-12|basic-18|basic-2|basic-24|basic-36|basic-48|basic-5.5|basic-54|
basic-6|basic-9|basic-mcs-1s|mcs-1s|mcs-2s|mcs-3s]

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

data-rates 5GHz custom [12|18|24|36|48|54|6|9|basic-1|basic-11|basic-12|
basic-18|basic-2|basic-24|basic-36|basic-48|basic-5.5|basic-54|basic-6|basic-9|
basic-mcs-1s|mcs-1s|mcs2s|mcs3s]
```

**Parameters**

- `data-rates 2.4GHz [b-only|bg|bgn|default|g-only|gn]`

| | |
|---|---|
| data-rates | Specifies the 802.11 rates supported when mapped to a 2.4 GHz radio |
| b-only | Uses rates that support only 11b clients |
| bg | Uses rates that support both 11b and 11g clients |
| bgn | Uses rates that support 11b, 11g and 11n clients |
| default | Uses the default rates configured for a 2.4 GHz radio |
| g-only | Uses rates that support operation in 11g only |
| gn | Uses rates that support 11g and 11n clients |

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

| | |
|---|---|
| data-rates | Specifies the 802.11 rates supported when mapped to a 5.0 GHz radio |
| a-only | Uses rates that support operation in 11a only |
| an | Uses rates that support 11a and 11n clients |
| default | Uses default rates configured for a 5.0 GHz |

- `data-rates [2.4GHz|5GHz] custom [1|11|12|18|2|24|36|48|5.5|54|6|9|basic-1|basic-11|basic-12|basic-18|basic-2|basic-24|basic-36|basic-48|basic-5.5|basic-54|basic-6|basic-9|basic-mcs-1s|mcs-1s|mcs-2s|mcs-3s]`

| | |
|---|---|
| data-rates [2.4GHz\|5GHz] | Specifies the 802.11 rates supported when mapped to a 2.4 GHz or 5.0 GHz radio |

| | |
|---|---|
| custom | Configures a data rates list by specifying each rate individually. Use 'basic-' prefix before a rate to indicate it is used as a basic rate (For example, 'data-rates custom basic-1 basic-2 5.5 11').<br>The data-rates for 2.4 GHz and 5.0 GHz channels are the same with a few exceptions. The 2.4 GHz channel has a few extra data rates: 1, 11, 2, and 5.5. |
| 1,11,2,5.5 | The following data rates are specific to the 2.4 GHz channel:<br>• 1 – 1-Mbps<br>• 11 – 11-Mbps<br>• 2 – 2-Mbps<br>• 5.5 – 5.5-Mbps |
| [12,18,24,36,48,54,6,9, basic-1,basic-11, basic-12,basic-18, basic-2,basic-36, basic-48,basic-5.5, basic-54,basic-6, basic-9, basic-mcs-1s, mcs-1s,mcs2s, mcs-3s] | The following data rates are common to both the 2.4 GHz and 5.0 GHz channels:<br>• 12 – 12 Mbps<br>• 18 – 18-Mbps<br>• 24 – 24 Mbps<br>• 36 – 36-Mbps<br>• 48 – 48-Mbps<br>• 54 – 54-Mbps<br>• 6 – 6-Mbps<br>• 9 – 9-Mbps<br>• basic-1 – basic 1-Mbps<br>• basic-11 – basic 11-Mbps<br>• basic-12 – basic 12-Mbps<br>• basic-18 – basic 18-Mbps<br>• basic-2 – basic 2-Mbps<br>• basic-36 – basic 36-Mbps<br>• basic-48 – basic 48-Mbps<br>• basic-5.5 – basic 5.5-Mbps<br>• basic-54 – basic 54-Mbps<br>• basic-6 – basic 6-Mbps<br>• basic-9 – basic 9-Mbps<br>• basic-mcs-1s – Modulation and coding scheme data rates for 1 Spatial Stream<br>• mcs-1s – Applicable to 1-spatial stream data rates<br>• mcs-2s – Applicable to 2-spatial stream data rates<br>• mcs-3s – Applicable to 3-spatial stream data rates |

**Example**

```
rfs6000-81742D(config-wlan-test)#data-rates 2.4GHz gn

rfs6000-81742D(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode local
 encryption-type none
 authentication-type eap
 accounting syslog host 172.16.10.4 port 2
 data-rates 2.4GHz gn
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 captive-portal-enforcement fall-back
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 broadcast-dhcp validate-offer
rfs6000-81742D(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Resets the 802.11 data rates supported on a WLAN for the 2.4 GHz or 5.0 GHz radios |

### 4.1.97.2.16 description

*wlan-mode commands*

Defines the WLAN description

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
description <LINE>
```

**Parameters**

- `description <LINE>`

| | |
|---|---|
| <LINE> | Specify a WLAN description<br>The WLAN's description should help differentiate it from others with similar configurations. The description should not exceed 64 characters. |

**Example**

```
rfs6000-81742D(config-wlan-test)#description TestWLAN

rfs6000-81742D(config-wlan-test)#show context
wlan test
 description TestWLAN
 ssid test
 bridging-mode local
 encryption-type none
 authentication-type eap
 accounting syslog host 172.16.10.4 port 2
 data-rates 2.4GHz gn
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 captive-portal-enforcement fall-back
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 broadcast-dhcp validate-offer
rfs6000-81742D(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes a WLAN's configured description |

### 4.1.97.2.17 downstream-group-addressed-forwarding

*wlan-mode commands*

Enables forwarding of downstream *broadcast/multicast* (BC/MC) packets to a group on this WLAN. This feature is enabled by default.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
downstream-group-addressed-forwarding
```

**Parameters**

None

**Example**

```
rfs4000-229D58(config-wlan-test)#downstream-group-addressed-forwarding
rfs4000-229D58(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables forwarding of downstream BCMC packets to a group on this WLAN |

### 4.1.97.2.18 dpi

*wlan-mode commands*

Enables DPI on this WLAN. When enabled, all traffic is subjected to DPI for detection of applications, application categories, custom applications, and metadata extraction.

DPI is an advanced packet analysis technique, which analyzes packet and packet content headers to determine the nature of network traffic. When enabled, DPI inspects packets of all flows to identify applications (such as, Netflix, Twitter, Facebook, etc.) and extract metadata (such as, host name, server name, TCP-RTT, etc.) for further use by the WiNG firewall.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
dpi metadata [http|ssl|tcp-rtt|voice-video]
```

**Parameters**

- `dpi metadata [http|ssl|tcp-rtt|voice-video]`

| | |
|---|---|
| dpi metadata [http\|ssl\|tcp-rtt\|voice-video] | Enables extraction of the following metadata flows:<br>• http – Extracts HTTP flows. When enabled, administrators can track HTTP Websites accessed by both internal and guest clients and visualize HTTP data usage, hits, active time and total clients on the NSight application's dashboard. This setting is disabled by default.<br>• ssl – Extracts SSL flows. When enabled, administrators can track SSL Websites accessed by both internal and guest clients and visualize SSL data usage, hits, active time and total clients on the NSight application's dashboard.This setting is disabled by default<br>• tcp-rtt – Extracts *Round Trip Time* (RTT) information from *Transmission Control Protocol* (TCP) flows. However, this TCP-RTT metadata is viewable only on the NSight dashboard. Therefore, ensure the NSight server is up and NSight analytics data collection is enabled.<br>• voice-video – Extracts voice and video flows. When enabled, voice and video calls can be tracked by extracting parameters, such as packets transferred and lost, jitter, and application name. Most Enterprise VoIP applications like facetime, skype for business and VoIP terminals can be monitored for call quality and visualized on the NSight dashboard in manner similar to HTTP and SSL. Call quality and metrics can only be determined from calls established unencrypted. This setting is disabled by default. |

**Example**

```
rfs6000-81742D(config-wlan-test)#dpi metadata http
rfs6000-81742D(config-wlan-test)#dpi metadata ssl
rfs6000-81742D(config-wlan-test)#dpi metadata voice-video

rfs6000-81742D(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 dpi metadata voice-video
 dpi metadata http
 dpi metadata ssl
rfs6000-81742D(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables extraction of metadata flows on the WLAN |

### 4.1.97.2.19 dynamic-vlan-assignment

*wlan-mode commands*

Enables dynamic VLAN assignment on this WLAN, and adds or removes VLANs for the selected WLAN. Configure this feature to allow an override to the WLAN configuration. If, as part of the authentication process, the RADIUS server returns a client's VLAN-ID in a RADIUS Access-Accept packet, and this feature is enabled, all client traffic is forward on that VLAN. If disabled, the RADIUS server returns VLAN-ID is ignored and the WLAN's VLAN configuration is used. For more information, see *vlan*. This option is disabled by default.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
dynamic-vlan-assignment allowed-vlans <VLAN-ID>
```

**Parameters**

- `dynamic-vlan-assignment allowed-vlans <VLAN-ID>`

| | |
|---|---|
| dynamic-vlan-assignment allowed-vlans | Enables dynamic VLAN assignment and configures a list of VLAN IDs or VLAN alias allowed access to the WLAN |
| <VLAN-ID> | Specify the list of VLAN IDs or the VLAN alias names. For example, 10-20, 25, 30-35, $guest.<br>For information on VLAN aliases, see *alias*. |

**Example**

```
rfs4000-229D58(config-wlan-test)#dynamic-vlan-assignment allowed-vlans 10-20

rfs4000-229D58(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 dynamic-vlan-assignment allowed-vlans 10-20
rfs4000-229D58(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables dynamic VLAN assignment on this WLAN |

### 4.1.97.2.20 eap-types

*wlan-mode commands*

Configures client access based on the EAP type used

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
eap-types [allow|deny] [aka|all|fast|peap|sim|tls|ttls] {(aka|all|fast|peap|sim|
tls|ttls)}
```

**Parameters**

```
• eap-types [allow|deny] [aka|all|fast|peap|sim|tls|ttls] {(aka|all|fast|
peap|sim|tls|ttls)}
```

| | |
|---|---|
| eap-types [allow\|deny] | Configures a list of allowed or denied EAP types<br>• allow – Configures a list of EAP types allowed for WLAN client authentication<br>• deny – Configures a list of EAP types not allowed for WLAN client authentication |
| [aka\|all\|fast\|peap\|sim\|tls\|ttls] | The following EAP types are common to the 'allow' and 'deny' keywords:<br>• aka – Configures EAP *Authentication and Key Agreement* (AKA) and EAP-AKA' (AKA Prime). EAP-AKA is one of the methods in the EAP authentication framework. It uses *Universal Mobile Telecommunications System* (UMTS) and *Universal Subscriber Identity Module* (USIM) for client authentication and key distribution.<br>• all – Allows or denies usage of all EAP types on the WLAN. This is the default setting.<br>• fast – Configures EAP *Flexible Authentication via Secure Tunneling* (FAST). EAP-FAST establishes a *Transport Layer Security* (TLS) tunnel, to verify client credentials, using *Protected Access Credentials* (PAC).<br>• peap – Configures *Protected Extensible Authentication Protocol* (PEAP). PEAP or Protected EAP uses encrypted and authenticated TLS tunnel to encapsulate EAP.<br>• sim – Configures EAP *Subscriber Identity Module* (SIM). EAP-SIM uses *Global System for Mobile Communications* (GSMC) SIM for client authentication and key distribution.<br>• tls – Configures EAP *Transport Layer Security* (TLS). EAP-TLS is an EAP authentication method that uses PKI to communicate with a RADIUS server or any other authentication server.<br>• ttls – Configures *Tunneled Transport Layer Security* (TTLS). EAP-TTLS is an extension of TLS. Unlike TLS, TTLS does not require every client to generate and install a CA-signed certificate.<br>These options are recursive, and more than one EAP type can be selected. The selected options are added to the allowed or denied EAP types list. |

**Example**

```
rfs6000-81742D(config-wlan-test)#eap-types allow fast sim tls

rfs6000-81742D(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 eap-types allow fast sim tls
rfs6000-81742D(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Reverts to default setting - eap-types allow all |

### 4.1.97.2.21 encryption-type

*wlan-mode commands*

Sets a WLAN's encryption type

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
encryption-type [ccmp|keyguard|none|tkip-ccmp|wep128|web128-keyguard|wep64]
```

**Parameters**

- `encryption-type [ccmp|keyguard|none|tkip-ccmp|wep128|web128-keyguard|wep64]`

| | |
|---|---|
| encryption-type | Configures the WLAN's data encryption parameters |
| ccmp | Configures *Advanced Encryption Standard* (AES) *Counter Mode CBC-MAC Protocol* (AES-CCM/CCMP) |
| keyguard | Configures Keyguard-MCM *(Mobile Computing Mode)* |
| none | No encryption used. This is the default setting. |
| tkip-ccmp | Configures the TKIP and AES-CCM/CCMP encryption modes |
| wep128 | Configures WEP with 128 bit keys |
| wep128-keyguard | Configures WEP128 as well as Keyguard-MCM encryption modes |
| wep64 | Configures WEP with 64 bit keys. A WEP64 configuration is insecure when two WLANs are mapped to the same VLAN, and one uses no encryption while the other uses WEP. |

**Example**

```
rfs6000-81742Dconfig-wlan-test)#encryption-type tkip-ccmp

rfs6000-81742D(config-wlan-test)#show context
wlan test
 description TestWLAN
 ssid test
 bridging-mode local
 encryption-type tkip-ccmp
 authentication-type eap
 accounting syslog host 172.16.10.4 port 2
 data-rates 2.4GHz gn
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 captive-portal-enforcement fall-back
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 broadcast-dhcp validate-offer
rfs6000-81742D(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Resets the WLAN's encryption type to default (none) |

### 4.1.97.2.22 enforce-dhcp

*wlan-mode commands*

Enables dropping of packets from clients with a static IP address. This option is disabled by default.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
enforce-dhcp
```

**Parameters**

None

**Example**

```
rfs6000-81742D(config-wlan-test)#enforce-dhcp

rfs6000-81742D(config-wlan-test)#show context
wlan test
 description TestWLAN
 ssid test
 bridging-mode local
 encryption-type tkip-ccmp
 authentication-type eap
 accounting syslog host 172.16.10.4 port 2
 data-rates 2.4GHz gn
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 captive-portal-enforcement fall-back
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 enforce-dhcp
 broadcast-dhcp validate-offer
rfs6000-81742D(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables dropping of packets from clients with a static IP address |

### 4.1.97.2.23 fast-bss-transition

*wlan-mode commands*

Enables support for 802.11r *Fast-BSS Transition* (FT) on the selected WLAN. This feature is disabled by default.

802.11r is an attempt to undo the burden that security and QoS added to the handoff process, and restore it back to an original four message exchange process. The central application for the 802.11r standard is VOIP using mobile phones within wireless Internet networks. 802.11r FT redefines the security key negotiation protocol, allowing parallel processing of negotiation and requests for wireless resources.

Enabling FT standards provides wireless clients fast, secure and seamless transfer from one base station to another, ensuring continuous connectivity.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
fast-bss-transition {over-ds}
```

**Parameters**

- `fast-bss-transition {over-ds}`

| | |
|---|---|
| fast-bss-transition over-ds | Enables 802.11r FT support on this WLAN<br>• over-ds – Optional. Enables 802.11r client roaming over the *Distribution System* (DS). When enabled, all client communication with the target AP is via the current AP. This communication, carried in FT action frames, is first sent by the client to the current AP, then forwarded to the target AP through the controller. |

**Example**

```
rfs6000-81742D(config-wlan-test)#fast-bss-transition

rfs6000-81742D(config-wlan-test)#show context
wlan test
 ssid test
 vlan 1
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 fast-bss-transition
rfs6000-81742D(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables support for 802.11r *Fast-BSS Transition* (FT) on a WLAN |

### 4.1.97.2.24 http-analyze

*wlan-mode commands*

Enables HTTP URL analysis on the WLAN

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

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

**Parameters**

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

| | |
|---|---|
| filter | Filters URLs, based on the parameters set, before forwarding them |
| images | Filters out URLs referring to images (does not forward URL requesting images) |
| post | Filters out URLs requesting POST (does not forward POST requests). This option is disabled by default. |
| query-string | Removes query strings from URLs before forwarding them (forwards requests and no data). This option is disabled by default. |

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

| | |
|---|---|
| syslog host <IP/ HOSTNAME> | Forwards client and URL information to a syslog server<br>• host <IP/HOSTNAME> – Specify the syslog server's IP address or hostname |
| port <1-65535> | Optional. Specifies the UDP port to connect to the syslog server from 1 - 65535 |
| proxy-mode [none\| through-controller\| through-rf-domain-manager] | Optional. Specifies if the request is to be proxied through another device<br>• none – Requests are sent directly to syslog server from device<br>• through-controller – Proxies requests, to the syslog server, through the controller configuring the device<br>• through-rf-domain-manager – Proxies requests, to the syslog server, through the local RF Domain manager |

**Example**

```
rfs4000-229D58(config-wlan-test)#http-analyze syslog host 192.168.13.10 port 21
proxy-mode through-controller

rfs4000-229D58(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 http-analyze syslog host 192.168.13.10 port 21 proxy-mode through-controller
rfs4000-229D58(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables HTTP URL analysis on the WLAN |

### 4.1.97.2.25 ip

*wlan-mode commands*

Configures *Internet Protocol* (IP) settings

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ip [arp|dhcp]

ip arp [header-mismatch-validation|trust]

ip dhcp trust
```

**Parameters**

- `ip arp [header-mismatch-validation|trust]`

| | |
|---|---|
| ip arp | Configures the IP settings for ARP packets |
| header-mismatch-validation | Verifies mismatch of source MAC address in the ARP and Ethernet headers. This option is enabled by default. |
| trust | Sets ARP responses as trusted for a WLAN/range. This option is disabled by default. |

- `ip dhcp trust`

| | |
|---|---|
| ip dhcp | Configures the IP settings for DHCP packets |
| trust | Sets DHCP responses as trusted for a WLAN/range. This option is disabled by default. |

**Example**

```
rfs6000-81742D(config-wlan-test)#ip dhcp trust

rfs6000-81742D(config-wlan-test)#show context
wlan test
 description TestWLAN
 ssid test
 bridging-mode local
 encryption-type tkip-ccmp
 authentication-type eap
 accounting syslog host 172.16.10.4 port 2
 data-rates 2.4GHz gn
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 captive-portal-enforcement fall-back
 ip dhcp trust
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 enforce-dhcp
 broadcast-dhcp validate-offer
 http-analyze controller
rfs6000-81742D(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Resets IP ARP or DHCP trust parameters to default. ARP trust is disabled, ARP mismatch verification is enabled, or DHCP trust is disabled. |

### 4.1.97.2.26 ipv6

*wlan-mode commands*

Sets the DHCPv6 and ICMPv6 *neighbor discovery* (ND) components for this WLAN

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ipv6 [dhcpv6|nd]

ipv6 dhcpv6 trust

ipv6 nd [header-mismatch-validation|raguard|trust]
```

**Parameters**

- `ipv6 dhcpv6 trust`

| | |
|---|---|
| ipv6 dhcpv6 trust | Enables DHCPv6 trust state for DHCPv6 responses on this WLAN. When enabled, all DHCPv6 responses received on this WLAN are trusted and forwarded. This option is disabled by default. |

- `ipv6 nd [header-mismatch-validation|raguard|trust]`

| | |
|---|---|
| ipv6 nd | Sets the IPv6 ND settings for this WLAN |
| header-mismatch-validation | Checks for mismatch of source MAC address in the ICMPv6 ND message and Ethernet header (link layer option). This option is enabled by default. |
| raguard | Allows redirection of *router advertisements* (RAs) and ICMPv6 packets originating on this WLAN. This option is disabled by default. |
| trust | Enables trust state for ND requests received on this WLAN. When enabled, all ND requests on an IPv6 firewall, on this WLAN, are trusted. This option is disabled by default. |

**Example**

```
rfs6000-81742D(config-wlan-test)#ipv6 dhcpv6 trust

rfs6000-81742D(config-wlan-test)#ipv6 nd trust

rfs6000-81742D(config-wlan-test)#show context
wlan test
 ssid test
 vlan 1
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 ipv6 dhcpv6 trust
 ipv6 nd trust
rfs6000-81742D(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Resets IPv6 ND or DHCPv6 trust parameters to default. ND request trust is disabled, ND header mismatch verification is enabled, ND RA and ICMPv6 redirection is disabled, or DHCPv6 trust is disabled. |

### 4.1.97.2.27 kerberos

*wlan-mode commands*

Configures Kerberos authentication parameters on a WLAN

Kerberos (designed and developed by MIT) provides strong authentication for client/server applications using secret-key cryptography. Using Kerberos, a client must prove its identity to a server (and vice versa) across an insecure network connection.

Once a client and server use Kerberos to validate their identity, they encrypt all communications to assure privacy and data integrity. Kerberos can only be used on the access point with 802.11b clients. Kerberos uses *Network Time Protocol* (NTP) for synchronizing the clocks of its *Key Distribution Center* (KDC) server(s).

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
kerberos [password|realm|server]

kerberos password [0 <LINE>|2 <LINE>|<LINE>]

kerberos realm <REALM>

kerberos server [primary|secondary|timeout]

kerberos server [primary|secondary] host <IP/HOSTNAME> {port <1-65535>}

kerberos server timeout <1-60>
```

**Parameters**

- `kerberos password [0 <LINE>|2 <LINE>|<LINE>]`

| | |
|---|---|
| kerberos | Configures a WLAN's Kerberos authentication parameters<br>The parameters are: password, realm, and server. |
| password | Configures a Kerberos KDC server password. The password should not exceed 127 characters. The password options are:<br>• 0 <LINE> – Configures a clear text password<br>• 2 <LINE> – Configures an encrypted password<br>• <LINE> – Specify the password. |

- `kerberos realm <REALM>`

| | |
|---|---|
| kerberos | Configures a WLAN's Kerberos authentication parameters<br>The parameters are: password, realm, and server. |
| realm <REALM> | Configures a Kerberos KDC server realm. The REALM should not exceed 127 characters. |

- `kerberos server [primary|secondary] host <IP/HOSTNAME> {port <1-65535>}`

| | |
|---|---|
| kerberos | Configures a WLAN's Kerberos authentication parameters<br>The parameters are: password, realm, and server. |
| server [primary\|secondary] | Configures the primary and secondary KDC server parameters<br>• primary – Configures the primary KDC server parameters<br>• secondary – Configures the secondary KDC server parameters |
| host <IP/HOSTNAME> | Sets the primary or secondary KDC server address<br>• <IP/HOSTNAME> – Specify the IP address or name of the KDC server. |
| port <1-65535> | Optional. Configures the UDP port used to connect to the KDC server<br>• <1-65535> – Specify the port from 1 - 65535. The default is 88. |

- `kerberos server timeout <1-60>`

| | |
|---|---|
| kerberos | Configures a WLAN's Kerberos authentication parameters<br>The parameters are: password, realm, and server. |
| timeout <1-60> | Modifies the Kerberos KDC server's timeout parameters<br>• <1-60> – Specifies the wait time for a response from the Kerberos KDC server before retrying. Specify a value from 1 - 60 seconds. |

**Example**

```
rfs6000-81742D(config-wlan-test)#kerberos server timeout 12

rfs6000-81742D(config-wlan-test)#kerberos server primary host 172.16.10.2 port 88

rfs6000-81742D(config-wlan-test)#show context
wlan test
 description TestWLAN
 ssid test
 bridging-mode local
 encryption-type tkip-ccmp
 authentication-type eap
 kerberos server timeout 12
 kerberos server primary host 172.16.10.2
 accounting syslog host 172.16.10.4 port 2
 data-rates 2.4GHz gn
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 captive-portal-enforcement fall-back
 ip dhcp trust
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 enforce-dhcp
 broadcast-dhcp validate-offer
 http-analyze controller
rfs6000-81742D(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes Kerberos authentication related parameters on a WLAN |

### 4.1.97.2.28 mac-authentication

*wlan-mode commands*

Enables MAC authentication. When enabled, the system uses cached credentials (RADIUS server lookups are skipped) to authenticate clients.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
mac-authentication [cached-credentials|enforce-always]
```

**Parameters**

- `mac-authentication [cached-credentials|enforce-always]`

| | |
|---|---|
| mac-authentication | Enables MAC authentication on this WLAN and configures related parameters |
| cached-credentials | Uses cached credentials to skip RADIUS lookups. This option is disabled by default. |
| enforce-always | Enforces MAC authentication on this WLAN. When enabled, MAC authentication is enforced, each time a client logs in, even when the authentication type specified (using the authentication-type command) is not MAC authentication. This option is disabled by default. |

**Example**

```
rfs4000-229D58(config-wlan-test)#mac-authentication cached-credentials
rfs4000-229D58(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables MAC authentication related parameters: Disables use of cached credentials to skip RADIUS lookups, or disables enforcement of MAC authentication on this WLAN. |

### 4.1.97.2.29 no

*wlan-mode commands*

Negates WLAN mode commands and reverts values to their default

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
no [accounting|acl|answer-broadcast-probes|assoc-response|association-list|
authentication-type|broadcast-dhcp|broadcast-ssid|captive-portal-enforcement|
client-access|client-client-communication|client-load-balancing|
controller-assisted-mobility|data-rates|description|downstream-group-addressed-
forwarding|dpi|dynamic-vlan-assignment|eap-types|encryption-type|enforce-
dhcp|fast-bss-transition|http-analyze|ip|ipv6|kerberos|mac-authentication|
nsight|opendns|protected-mgmt-frames|proxy-arp-mode|proxy-nd-mode|qos-map|radio-
resource-measurement|radius|registration|relay-agent|shutdown|ssid|t5-client-
isolation|t5-security|time-based-access|use|vlan|vlan-pool-member|wep128|wep64|
wing-extensions|wireless-client|wpa-wpa2|service]

no accounting [radius|syslog|wait-client-ip]

no acl exceed-rate wireless-client-denied-traffic

no [answer-broadcast-probes|association-list global|authentication-type|
broadcast-dhcp validate-offer|broadcast-ssid|captive-portal-enforcement|
client-access|client-client-communication|client-load-balancing allow-single-
band-clients|controller-assisted-mobility|data-rates [2.4GHz|5GHz]|description|
downstream-group-addressed-forwarding|dynamic-vlan-assignment allowed-vlans|
eap-types|encryption-type|enforce-dhcp|fast-bss-transition over-ds|
opendns device-id|protected-mgmt-frames {sa-query}|proxy-arp-mode|proxy-nd-mode|
qos-map|ssid|t5-client-isolation|t5-security|vlan]

no assoc-response [deny-threshold|rssi-threshold]

no http-analyze {filter|syslog}
no http-analyze {filter [images|post|query-string]}

no ip [arp|dhcp]
no ip arp [header-mismatch-validation|trust]
no ip dhcp trust

no dpi metadata [http|ssl|voice-video]

no ipv6 [dhcpv6|nd]
no ipv6 dhcpv6 trust
no ipv6 nd [header-mismatch-validation|raguard|trust]

no kerberos [password|realm|server]
no kerberos server [primary host|secondary host|timeout]

no mac-authentication [cached-credentials|enforce-always]

no nsight client-history

no radio-resource-measurement {channel-report|neighbor-report {hybrid}}

no radius [dynamic-authorization|nas-identifier|nas-port-id|vlan-assignment]
```

```
no registration {external}

no relay-agent [dhcp-option82|dhcpv6-ldra]

no shutdown {on-critical-resource|on-meshpoint-loss|on-primary-port-link-loss|
on-unadoption}

no time-based-access days [all|friday|monday|saturday|sunday|thursday|tuesday|
wednesday|weekdays|weekends]

no use [aaa-policy|association-acl-policy|bonjour-gw-discovery-policy|captive-
portal|ip-access-list|ipv6-access-list|mac-access-list|passpoint-policy|
roaming-assist-policy|url-filter|wlan-qos-policy]

no vlan-pool-member [<1-40 95>|<VLAN-ALIAS-NAME>]

no [wep128|wep64] [key {1-4}|transmit-key]

no wing-extension [move-command|smart-scan|wing-load-information|wmm-load-
information]

no wireless-client [count-per-radio|cred-cache-ageout|hold-time|inactivity-
timeout|max-firewall-sessions|reauthentication|roam-notification|t5-inactivity-
timeout|tx-power|vlan-cache-ageout]
```

**Parameters**

- no <PARAMETERS>

| | |
|---|---|
| no <PARAMETERS> | Removes or reverts this WLAN's settings based on the parameters passed |

**Usage Guidelines**

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

**Example**

```
rfs6000-81742D(config-wlan-test)#no ?
  accounting                          Configure how accounting records are
                                      created for this wlan
  acl                                 Actions taken based on ACL
                                      configuration [ packet drop being one
                                      of them]
  answer-broadcast-probes             Do not Include this wlan when
                                      responding to probe requests that do
                                      not specify an SSID
  assoc-response                      Association response threshold
  association-list                    Configure the association list for
                                      the wlan
  authentication-type                 Reset the authentication to use on
                                      this wlan to default (none/Pre-shared
                                      keys)
  broadcast-dhcp                      Configure broadcast DHCP packet
                                      handling
  broadcast-ssid                      Do not advertise the SSID of the WLAN
                                      in beacons
  captive-portal-enforcement          Configure how captive-portal is
                                      enforced on the wlan
  client-access                       Disallow client access on this wlan
                                      (no data operations)
  client-client-communication         Disallow switching of frames from one
                                      wireless client to another on this
                                      wlan
  client-load-balancing               Disable load-balancing of clients on
                                      this wlan
  controller-assisted-mobility        Disable configure assisted mobility
```

```
  data-rates                                Reset data rate configuration to
                                            default
  description                               Reset the description of the wlan
  downstream-group-addressed-forwarding     Disable downstream group addressed
                                            forwarding of packets
  dpi                                       Deep-Packet-Inspection (Application
                                            Assurance)
  dynamic-vlan-assignment                   Dynamic VLAN assignment configuration
  eap-types                                 Allow all EAP types on this wlan
  encryption-type                           Reset the encryption to use on this
                                            wlan to default (none)
  enforce-dhcp                              Drop packets from Wireless Clients
                                            with static IP address
  fast-bss-transition                       Disable support for 802.11r Fast BSS
                                            Transition
  http-analyze                              Enable HTTP URL analysis on the wlan
  ip                                        Internet Protocol (IP)
  ipv6                                      Internet Protocol version 6 (IPv6)
  kerberos                                  Configure kerberos authentication
                                            parameters
  mac-authentication                        Configure mac-authentication related
                                            parameters
  nsight                                    Nsight Server
  opendns                                   OpenDNS related config for this wlan
  protected-mgmt-frames                     Disable support for Protected
                                            Management Frames (IEEE 802.11w)
  proxy-arp-mode                            Configure handling of ARP requests
                                            with proxy-arp is enabled
  proxy-nd-mode                             Configure handling of IPv6 ND
                                            requests with proxy-nd is enabled
  qos-map                                   Disable the 802.11u QoS map element
                                            and frame
  radio-resource-measurement                Disable support for 802.11k Radio
                                            Resource Measurement
  radius                                    Configure RADIUS related parameters
  registration                              Dynamic registration of device (or)
                                            user
  relay-agent                               Configure dhcp relay agent info
  shutdown                                  Enable the use of this wlan
  ssid                                      Configure ssid
  t5-client-isolation                       Do not Isolate traffic among clients
  t5-security                               Configure encryption and
                                            authentication
  time-based-access                         Reset time-based-access parameters to
                                            default
  use                                       Set setting to use
  vlan                                      Map the default vlan (vlan-id 1) to
                                            the wlan
  vlan-pool-member                          Delete a mapped vlan from this wlan
  wep128                                    Reset WEP128 parameters
  wep64                                     Reset WEP64 parameters
  wing-extensions                           Disable support for WiNG-Specific
                                            extensions to 802.11
  wireless-client                           Configure wireless-client specific
                                            parameters
  wpa-wpa2                                  Modify tkip-ccmp (wpa/wpa2) related
                                            parameters


  service                                   Service to monitor to show no-service
                                            page to user

rfs6000-81742D(config-wlan-test)#
```

The test settings before execution of the no command:

```
rfs6000-81742D(config-wlan-test)#show context
wlan test
 description TestWLAN
 ssid test
 bridging-mode local
 encryption-type tkip-ccmp
 authentication-type eap
 kerberos server timeout 12
 kerberos server primary host 172.16.10.2
 accounting syslog host 172.16.10.4 port 2
 data-rates 2.4GHz gn
 wing-extensions wmm-load-information
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 captive-portal-enforcement fall-back
 ip dhcp trust
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 enforce-dhcp
 broadcast-dhcp validate-offer
 http-analyze controller
rfs6000-81742D(config-wlan-test)#

rfs6000-81742D(config-wlan-test)#no accounting syslog

rfs6000-81742D(config-wlan-test)#no description

rfs6000-81742D(config-wlan-test)#no authentication-type

rfs6000-81742D(config-wlan-test)#no encryption-type

rfs6000-81742D(config-wlan-test)#no enforce-dhcp

rfs6000-81742D(config-wlan-test)#no kerberos server primary host

rfs6000-81742D(config-wlan-test)#no kerberos server timeout

rfs6000-81742D(config-wlan-test)#no data-rates 2.4GHz

rfs6000-81742D(config-wlan-test)#no ip dhcp trust

rfs6000-81742D(config-wlan-test)#no captive-portal-enforcement
```

The test settings after the execution of the no command:

```
rfs6000-81742D(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode local
 encryption-type none
 authentication-type none
 wing-extensions wmm-load-information
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 broadcast-dhcp validate-offer
 http-analyze controller
rfs6000-81742D(config-wlan-test)#
```

### 4.1.97.2.30 nsight

*wlan-mode commands*

Enables retention of client-history

A typical NSight-server enabled, guest access environment may be visited by thousands of unique clients on a daily basis. Some of these guest clients are not regular visitors, accessing the network infrequently. However, by default, historical data of all guest clients, irrespective of their network access frequency, is retained by the NSight server for up to 180 days. This results in the database containing thousands if not millions of unique MAC addresses of infrequent guest clients. To address this potential problem it is recommended to disable client-history retention on a guest WLAN, and use the nsight-policy context to configure a separate timer (8 hours by default) specifying the guest client data lifespan in the database.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
nsight client-history
```

**Parameters**

- `nsight client-history`

| | |
|---|---|
| nsight client-history | Enables retention of client-history in the database. This option is enabled by default. |

**Example**

On a WLAN, the client-history option is enabled by default. When enabled, all client history (including guest-clients) is retained in the NSight server database for 180 days.

To disable this option, execute the *no > nsight > client-history* command. When disabled, guest client history is retained only for 8 hours, which is the default setting defined by the NSight policy applied on the access point (through which the guest client accesses the WLAN) or the access point's RF Domain. However, the default historical data retention duration for regular clients and devices (access point and controllers) remains unchanged (180 days) as per the NSight policy settings.

```
nx9500-6C8809(config-wlan-test3)#no nsight client-history
nx9500-6C8809(config-wlan-test3)#show context
wlan test3
 ssid test3
 bridging-mode local
 encryption-type none
 authentication-type none
 no nsight client-history
nx9500-6C8809(config-wlan-test3)#
```

Use the NSight policy context to define separate client-history retention time for regular clients, devices, and guest clients. For more information, see *nsight-policy*.

**Related Commands**

| | |
|---|---|
| *no* | Disables client-history retention in the NSight database |

### 4.1.97.2.31 opendns

*wlan-mode commands*

Configures the pre-fetched OpenDNS device_id. Once configured, all DNS queries originating from wireless clients associating with the WLAN are appended with an additional 31 bytes of data (representing the device ID) at the end of the DNS packet. The device ID is a sixteen (16) character hex string representing a 64 bit unsigned integer and is fetched from the OpenDNS site.

This command is part of a series of configurations that are required to integrate WiNG access points, wireless controllers, and service platforms with OpenDNS. When all the parameters have been configured, DNS queries from wireless clients, associating with the WLAN, are redirected to OpenDNS (208.67.220.220 OR 208.67.222.222). These OpenDNS resolvers act as proxy DNS servers that provide additional functionalities, such as Web filtering, reporting, and performance enhancement. For more information on the entire configuration, see *opendns*.

This option is disabled by default.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
opendns device-id <DEVICE-ID>
```

**Parameters**

- `opendns device-id <DEVICE-ID>`

| | |
|---|---|
| opendns device-id <DEVICE-ID> | Configures the device ID to embed in DNS queries sent to OpenDNS<br>• <DEVICE-ID> – Specify the device ID. |

**Example**

The following command fetches the device_id from the OpenDNS site.

```
ap7131-E6D512#opendns ApiToken 9110B39543DEB2ECA1F473AE03E8899C00019073
device_id = 0014AADF8EDC6C59
ap7131-E6D512#
```

Use this device_id in the WLAN configuration context.

```
ap7131-E6D512(config)#wlan opendns
ap7131-E6D512(config-wlan-opendns)#opendns device-id 0014AADF8EDC6C59
ap7131-E6D512(config-wlan-opendns)#commit

ap7131-E6D512(config-wlan-opendns)#show context
wlan opendns
 ssid opendns
 vlan 1
 bridging-mode local
 encryption-type none
 authentication-type none
 opendns device-id 0014AADF8EDC6C59
ap7131-E6D512(config-wlan-opendns)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the device ID configured to be embedded in the DNS queries originating from the WiNG devices |

### 4.1.97.2.32 protected-mgmt-frames

*wlan-mode commands*

Configures the WLAN's frame protection mode and *security association* (SA) query parameters

802.11w provides protection for both unicast management frames and broadcast/multicast management frames. The 'robust management frames' are *action*, *disassociation,* and *deauthentication* frames. The standard provides one security protocol CCMP for protection of unicast robust management frames. *Protected management frames* (PMF) protocol only applies to robust management frames after establishment of RSNA PTK. Robust management frame protection is achieved by using CCMP for unicast management frames, *broadcast/multicast integrity protocol* (BIP) for broadcast/multicast management frames and SA query protocol for protection against (re)association attacks.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
protected-mgmt-frames [mandatory|optional|sa-query [attempts <1-10>|timeout <100-1000>]]
```

**Parameters**

```
• protected-mgmt-frames [mandatory|optional|sa-query [attempts <1-10>|timeout <100-1000>]]
```

| | |
|---|---|
| protected-mgmt-frames | Enables and configures WLAN's frame protection mode and SA query parameters. Use this command to specify whether management frames are continually or optionally protected. Frame protection mode is disabled by default. |
| mandatory | Enforces *protected management frames* (PMF) on this WLAN (management frames are continually optionally protected) |
| optional | Provides PMF only for those clients that support PMF (management frames are optionally protected) |
| sa-query [attempts <1-10>\| timeout <100-1000>] | Configures the following SA parameters:<br>• attempts <1-10> – Configures the number of SA query attempts from 1 - 10. The default is 5.<br>• timeout <100-1000> – Configures the interval, in milliseconds, used to timeout association requests that exceed the defined interval. Specify a value from 100 - 1000 milliseconds. The default value is 201 milliseconds. |

**Example**

```
rfs6000-81742D(config-wlan-test)#protected-mgmt-frames mandatory

rfs6000-81742D(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 protected-mgmt-frames mandatory
rfs6000-81742D(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables enforcement of protected management frames on this WLAN. And reverts protected management frames sa-query timeout and attempts to 201 milliseconds and 5 respectively. |

### 4.1.97.2.33 proxy-arp-mode

*wlan-mode commands*

Enables proxy ARP mode for handling ARP requests

Proxy ARP is the technique used to answer ARP requests intended for another system. By faking its identity, the access point accepts responsibility for routing packets to the actual destination.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
proxy-arp-mode [dynamic|strict]
```

**Parameters**

- `proxy-arp-mode [dynamic|strict]`

| | |
|---|---|
| proxy-arp-mode | Enables proxy ARP mode for handling ARP requests. The options available are dynamic and strict. |
| dynamic | Forwards ARP requests to the wireless side (for which a response could not be proxied). This is the default setting. |
| strict | Does not forward ARP requests to the wireless side |

**Example**

```
rfs6000-81742D(config-wlan-test)#proxy-arp-mode strict

rfs6000-81742D(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode local
 encryption-type none
 authentication-type none
 protected-mgmt-frames mandatory
 wing-extensions wmm-load-information
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 proxy-arp-mode strict
 broadcast-dhcp validate-offer
 http-analyze controller
rfs6000-81742D(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Reverts the proxy ARP mode to default (dynamic) |

### 4.1.97.2.34 proxy-nd-mode

*wlan-mode commands*

Configures the proxy ND mode for this WLAN member clients as either strict or dynamic

ND proxy is used in IPv6 to provide reachability by allowing a client to act as proxy. Proxy certificate signing can be done either dynamically (requiring exchanges of identity and authorization information) or statically when the network topology is defined.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
proxy-nd-mode [dynamic|strict]
```

**Parameters**

- `proxy-nd-mode [dynamic|strict]`

| | |
|---|---|
| proxy-nd-mode [dynamic\|strict] | Configures the proxy ND mode for this WLAN member clients. The options are: dynamic and strict<br>• dynamic – Forwards ND request to wireless for which a response could not be proxied. This is the default value.<br>• strict – Does not forward ND requests to the wireless side |

**Example**

```
rfs6000-81742D(config-wlan-test)#proxy-nd-mode strict

rfs6000-81742D(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 wpa-wpa2 server-only-authentication
 proxy-nd-mode strict
 opendns device-id 44-55-66
rfs6000-81742D(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Reverts the proxy ND mode to default (dynamic) |

### 4.1.97.2.35 qos-map

*wlan-mode commands*

Enables support for 802.11u QoS map element and frames

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
qos-map
```

**Parameters**

None

**Example**

```
rfs6000-81742D(config-wlan-test)#qos-map

rfs6000-81742D(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 qos-map
 wpa-wpa2 server-only-authentication
 proxy-nd-mode strict
 opendns device-id 44-55-66
rfs6000-81742D(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables support for 802.11u QoS map element and frames |

### 4.1.97.2.36 radio-resource-measurement

*wlan-mode commands*

Enables support for 802.11k radio resource measurement capabilities (IEEE 802.11k) on this WLAN

802.11k improves how traffic is distributed. In a WLAN, devices normally connect to the access point with the strongest signal. Depending on the number and location of clients, this arrangement can lead to excessive demand on one access point and under utilization of others, resulting in degradation of overall network performance. With 802.11k, if the access point with the strongest signal is loaded to its capacity, a client connects to an under-utilized access point. Even if the signal is weaker, the overall throughput is greater since it's an efficient use of the network's resources. This feature is disabled by default.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
radio-resource-measurement {channel-report|neighbor-report {hybrid}}
```

**Parameters**

- `radio-resource-measurement {channel-report|neighbor-report {hybrid}}`

| | |
|---|---|
| radio-resource-measurement | Enables support for 802.11k radio resource measurement capabilities |
| channel-report | Optional. Includes the channel-report element in beacons and probe responses |
| neighbor-report {hybrid} | Optional. Enables responding to neighbor-report requests<br>• hybrid – Optional. Uses the hybrid model of smart-rf neighbors and roaming frequency to neighbors |

**Example**

```
rfs4000-229D58(config-wlan-test)#radio-resource-measurement

rfs4000-229D58(config-wlan-test)#show context
wlan test
 ssid test
 vlan 1
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 radio-resource-measurement
 controller-assisted-mobility
rfs4000-229D58(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables support for 802.11k radio resource measurement capabilities (IEEE 802.11k) on this WLAN |

### 4.1.97.2.37 radius

*wlan-mode commands*

Configures RADIUS related parameters

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
radius [dynamic-authorization|nas-identifier|nas-port-id|vlan-assignment]

radius [dynamic-authorization|nas-identifier <NAS-ID>|nas-port-id <NAS-PORT-ID>|
  vlan-assignment]
```

**Parameters**

```
• radius [dynamic-authorization|nas-identifier <NAS-ID>|nas-port-id <NAS-PORT-
ID>|vlan-assignment]
```

| | |
|---|---|
| dynamic-authorization | Enables support for disconnect and change of authorization messages (RFC5176)<br>When enabled, this option extends the RADIUS protocol to support unsolicited messages from the RADIUS server. These messages allow administrators to issue *change of authorization* (CoA) messages, which affect session authorization, or *disconnect messages* (DM) that terminate a session immediately. This option is disabled by default. |
| nas-identifier <NAS-ID> | Configures the *network access server* (NAS) identifier attribute, a value that identifies the access point or controller where the RADIUS messages originate. The value specified here is included in the RADIUS NAS-Identifier field for WLAN authentication and accounting packets.<br>• <NAS-ID> – Specify the NAS identifier attribute (should not exceed 256 characters in length). |
| nas-port-id <NAS-PORT-ID> | Configures the NAS port ID attribute, a value that identifies the port from where the RADIUS messages originate<br>• <NAS-PORT-ID> – Specify the NAS port ID attribute (should not exceed 256 characters in length).<br>The profile database on the RADIUS server consists of user profiles for each connected NAS port. Each profile is matched to a username representing a physical port. When authorizing users, it queries the user profile database using a username representative of the physical NAS port making the connection. Set the numeric port value from 0 - 4294967295. |

| | |
|---|---|
| vlan-assignment | Configures the VLAN assignment of a WLAN. RADIUS VLAN assignment is disabled by default.<br>When enabled, this option assigns clients to the RADIUS server specified VLANs, overriding the WLAN configuration. This option is disabled by default. If, as part of the authentication process, the RADIUS server returns a client's VLAN-ID in a RADIUS access-accept packet, and this feature is enabled, all client traffic is forwarded on that VLAN. If disabled, the RADIUS server returned VLAN-ID is ignored and the VLAN specified using the *vlan*/*vlan-pool-member* options (in the WLAN config mode) is used.<br>If both the RADIUS VLAN assignment and the post authentication VLAN options are enabled, then RADIUS VLAN assignment takes priority over post authentication VLAN configuration. |

**Example**

```
rfs6000-81742D(config-wlan-test)#radius vlan-assignment

rfs6000-81742D(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode local
 encryption-type none
 authentication-type none
 protected-mgmt-frames mandatory
 radius vlan-assignment
 wing-extensions wmm-load-information
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 --More--
rfs6000-81742D(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables support for disconnect and change of authorization messages. Disables the use of VLAN information received in RADIUS server responses, instead uses the VLAN provided in the WLAN configuration. Removes the NAS identifier and NAS port identifiers configured. |

### 4.1.97.2.38 registration

*wlan-mode commands*

Configures settings enabling dynamic registration and validation of devices by their MAC addresses. When configured, this option registers a device's MAC address, and allows direct access to a previously registered device.

This command also configures the external guest registration and validation server details. If using an external server to perform guest registration, authentication and accounting, use this command to configure the external server's IP address/hostname. When configured, access points and controllers forward guest registration requests to the specified registration server. In case of EGuest deployment, this external resource should point to the EGuest registration server.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
registration [device|device-OTP|external|user]

registration [device|device-OTP|user] group-name <RAD-GROUP-NAME> {agreement-refresh <0-144000>|expiry-time <1-43800>}

registration external [follow-aaa|host]

registration external follow-aaa {send-mode [http|https|udp]}

registration external host <IP/HOSTNAME> {proxy-mode|send-mode}

registration external host <IP/HOSTNAME> {proxy-mode [none|through-controller|through-rf-domain-manager|through-centralized-controller]|send-mode [https|https|udp]}
```

**Parameters**

- `registration external follow-aaa {send-mode [http|https|udp]}`

| | |
|---|---|
| registration | Enables dynamic guest-user registration and validation. This option is disabled by default. |
| external | Specifies that the guest registration is handled by an external resource. Access points/controllers send registration requests to the external registration server. |
| follow-aaa | Uses an AAA policy to point to the guest registration, authentication, and accounting server. When used, guest registration is handled by the RADIUS server specified in the AAA policy used in the WLAN context.<br>In case of EGuest deployment, the RADIUS authentication and accounting server configuration in the AAA policy should point to the EGuest server. The use of 'follow-aaa' option is recommended in EGuest replica-set deployments.<br>For more information on enabling the EGuest server, see *eguest-server (VX9000 only)*.<br>For more information on configuring an EGuest deployment, see *configuring ExtremeGuest captive-portal*. |

| | |
|---|---|
| send-mode [https\|https\|udp] | Optional. Specifies the protocol used to forward registration requests to the external AAA policy servers. The options are;<br>• HTTPS – Sends registration requests as HTTPS packet<br>• HTTP – Sends registration requests as HTTP packet<br>• UDP – Sends registration requests as UDP packet, using the UPD port 12322. This is the default setting. |

• `registration external host <IP/HOSTNAME> {proxy-mode [none|through-controller|through-rf-domain-manager|through-centralized-controller]|send-mode [https|https|udp]}`

| | |
|---|---|
| registration | Configures dynamic guest registration and validation parameters. This option is disabled by default. |
| external | Specifies that the guest registration is handled by an external resource. Access points/controllers send registration requests to the external registration server. |
| host <IP/HOSTNAME> | Specifies the external registration server's IP address or hostname. When configured, access points/ controllers forward guest registration requests to the external registration server specified here. |
| proxy-mode {none\| through-controller\| through-rf-domain-manager\|through-centralized-controller} | Optional. Specifies the proxy mode. If a proxy is needed for connection, specify the proxy mode as through-controller, through-rf-domain. If no proxy is needed, select none.<br>• none – Optional. Requests are sent directly to the controller from the requesting device<br>• through-controller – Optional. Requests are proxied through the controller configuring the device<br>• through-rf-domain-manager – Optional. Requests are proxied through the local RF Domain manager<br>• through-centralized-controller – Optional. Request are proxied through one of the controllers in a cluster.that is operating as the designated forwarder. Select this option if capture and redirection is on a cluster of wireless controller/service platforms managing dependent/independent access points when redundancy is required.<br>After specifying the proxy-mode, optionally specify the protocol used to send the requests to the external registration server host. |
| send-mode [https\|https\|udp] | Optional. Specifies the communication protocol used. The options are;<br>• HTTPS – Sends registration requests as HTTPS packets<br>• HTTP – Sends registration requests as HTTP packets<br>• UDP – Sends registration requests as UDP packet, using the UPD port 12322. This is the default setting. |

• `registration [device|device-OTP|user] group-name <RAD-GROUP-NAME> {agreement-refresh <0-144000>|expiry-time <1-43800>}`

| | |
|---|---|
| registration | Configures dynamic guest registration and validation parameters. This option is disabled by default. |

| | |
|---|---|
| [device\|device-OTP\|user] | Configures the mode used to register guest users of this WLAN. Options include device, external, user, and device-OTP<br>• device-OTP – Registers a device by its MAC address. During registration, the user, using the registered device, has to provide the e-mail address, mobile number, or member id, and the *one-time-passcode (*OTP) sent to the registered e-mail id or mobile number to complete registration. On subsequent logins, the user has to enter the OTP. If the MAC address of the device attempting login and the OTP combination matches, the user is allowed access. If using this option, set the WLAN authentication type as *MAC authentication.*<br>• device – Registers a device by its MAC address. On subsequent logins, already registered MAC addresses are allowed access. If using this option, set the WLAN authentication type as *MAC authentication.*<br>• user – Registers guest users using one of the following options: e-mail address, mobile-number, or member-id.<br>If using any one of the above modes of registration, specify the RADIUS group to which the registered device or user is to be assigned post authentication. |
| group-name <RAD-GROUP-NAME> | Configures the RADIUS group name to which registered users are associated. When left blank, users are not associated with a RADIUS group.<br>• <RAD-GROUP-NAME> – Specify the RADIUS group name (should not exceed 64 characters). |
| expiry-time <1-43800> | Optional. Configures the amount of time, in hours, before registered addresses expire and must be re-entered<br>• <1-43800> – Specify a value from 1 - 43800 hrs. The default is 1500 hrs. |
| agreement-refresh <0-144000> | Optional. Sets the time, in minutes, after which an inactive user has to refresh the WLAN's terms of agreement. For example, if the agreement refresh period is set to 1440 minutes, a user, who has been inactive for more than 1440 minutes (1 day) is served the agreement page, and is allowed access only after refreshing the terms of agreement.<br>• <0-100> – Specify a value from 0 - 144000. The default is 0 minutes. |

**Example**

```
nx9500-6C8809(config-wlan-test)#registration user group-name guest agreement-ref
resh 14400 expiry-time 2000

nx9500-6C8809(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode local
 encryption-type none
 authentication-type none
 registration user group-name guest expiry-time 2000 agreement-refresh 14400
nx9500-6C8809(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables dynamic user registration and removes associated configurations. ALso disables forwarding of user information to an external device. |

### 4.1.97.2.39 relay-agent

*wlan-mode commands*

Enables support for DHCP/DHCPv6 relay agent information (option 82 and DHCPv6-LDRA) feature on this WLAN. This option is disabled by default.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
relay-agent [dhcp-option82|dhcpv6-ldra]
```

**Parameters**

- `relay-agent [dhcp-option82|dhcpv6-ldra]`

| | |
|---|---|
| relay-agent | Enables support for the following DHCP and DHCPv6 options: option 82 and *Lightweight DHCPv6 Relay Agent* (LDRA) respectively. When enabled, this feature allows the DHCP/DHCPv6 relay agent to insert the relay agent information option (option 82, LDRA) in client requests forwarded to the DHCP/DHCPv6 server.<br>This information provides the following:<br>• circuit ID suboption – Provides the SNMP port interface index<br>• remote ID – Provides the controller's MAC address |
| dhcp-option82 | Enables DHCP option 82. DHCP option 82 provides client physical attachment information. This option is disabled by default. |
| dhcpv6-ldra | Enables the DHCPv6 relay agent. The LDRA feature allows DHCPv6 messages to be transmitted on existing networks that do not currently support IPv6 or DHCPv6. This option is disabled by default. |

**Example**

```
rfs4000-229D58(config-wlan-test)#relay-agent dhcp-option82

rfs4000-229D58(config-wlan-test)#show context
wlan test
 ssid test
 vlan 1
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 radio-resource-measurement
 relay-agent dhcp-option82
 controller-assisted-mobility
rfs4000-229D58(config-wlan-test)#

rfs6000-81701D(config-wlan-test)#relay-agent dhcpv6-ldra

rfs6000-81701D(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 relay-agent dhcpv6-ldra
rfs6000-81701D(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables support for DHCP/DHCPv6 relay agent information (option 82 and DHCPv6-LDRA) feature on this WLAN |

### 4.1.97.2.40 shutdown

*wlan-mode commands*

Auto shuts down a WLAN

The auto shutdown mechanism helps regulate the availability of a WLAN based on an administrator defined access period. Use this feature to shut down a WLAN on specific days and hours and restrict periods when the WLAN traffic is either not desired or cannot be properly administrated. The normal practice is to shut down WLANs when there are no users on the network, such as after hours, weekends or holidays. This allows administrators more time to manage mission critical tasks since the WLAN's availability is automated.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
shutdown {on-critical-resource <CR-NAME>|on-meshpoint-loss|on-primary-port-link-loss|on-unadoption}
```

**Parameters**

- `shutdown {on-critical-resource <CR-NAME>|on-meshpoint-loss|on-primary-port-link-loss|on-unadoption}`

| | |
|---|---|
| shutdown | Auto shuts down the WLAN when specified events occur. Disabled by default. |
| on-critical-resource <CR-NAME> | Optional. Auto shuts down the WLAN when critical resource failure occurs. Disabled by default.<br>• <CR-NAME> – Specifies the name of the critical resource being monitored for this WLAN. |
| on-meshpoint-loss | Optional. Auto shuts down the WLAN when the root meshpoint link fails (is unreachable). Disabled by default. |
| on-primary-port-link-loss | Optional. Auto shuts down the WLAN when a device losses its primary Ethernet port (ge1/up1) link. Disabled by default. |
| on-unadoption | Optional. Auto shuts down the WLAN when an adopted device becomes unadopted. Disabled by default. |

**Usage Guidelines**

If the shutdown on-meshpoint-loss feature is enabled, the WLAN status changes only if the meshpoint and the WLAN are mapped to the same VLAN. If the meshpoint is mapped to VLAN 1 and the WLAN is mapped to VLAN 2, then the WLAN status does not change on loss of the meshpoint.

**Example**

```
rfs6000-81742D(config-wlan-test)#shutdown on-unadoption

rfs6000-81742D(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode local
 encryption-type none
 authentication-type none
 protected-mgmt-frames mandatory
 radius vlan-assignment
 wing-extensions wmm-load-information
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 proxy-arp-mode strict
 broadcast-dhcp validate-offer
 shutdown on-unadoption
 http-analyze controller
rfs6000-81742D(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables auto shut down WLAN. Use the optional keywords provided to disable auto shut down of the WLAN upon critical resource failure, when meshpoint links fail, when the primary Ethernet port (e1/up1) loses link, or when the WLAN gets unadopted. |

### 4.1.97.2.41 ssid

*wlan-mode commands*

Configures a WLAN's SSID

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ssid <SSID>
```

**Parameters**

```
• ssid <SSID>
```

| | |
|---|---|
| <SSID> | Specify the WLAN's SSID. The WLAN SSID is case sensitive and alphanumeric. Its length should not exceed 32 characters. |

**Example**

```
rfs6000-81742D(config-wlan-test)#ssid testWLAN1

rfs6000-81742D(config-wlan-test)#show context
wlan test
 ssid testWLAN1
 bridging-mode local
 encryption-type none
 authentication-type none
 protected-mgmt-frames mandatory
 radius vlan-assignment
 wing-extensions wmm-load-information
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 proxy-arp-mode strict
 broadcast-dhcp validate-offer
 shutdown on-unadoption
 http-analyze controller
rfs6000-81742D(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the WLAN's SSID |

### 4.1.97.2.42 t5-client-isolation

*wlan-mode commands*

Disallows clients connecting to the WLAN to communicate with one another. This setting applies exclusively to CPE devices managed by aT5 controller and is disabled by default.

A T5 controller uses the IPX operating system to manage its connected radio devices, as opposed to the WiNG operating system used by RFS wireless controllers and NX service platforms. However, a T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5's management within a WiNG supported subnet populated by both types of devices. The CPEs are the T5 controller managed radio devices using the IPX operating system. These CPEs use a DSL as their high speed Internet access mechanism using the CPE's physical wallplate connection and phone jack.

**NOTE:** This setting is applicable only when this WLAN supports T5 controllers and their connected CPEs.

**Supported in the following platforms:**

- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
t5-client-isolation
```

**Parameters**

None

**Example**

```
nx9500-6C8809(config-wlan-test)#t5-client-isolation

nx9500-6C8809(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode local
 encryption-type none
 authentication-type none
 t5-client-isolation
nx9500-6C8809(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Allows clients connecting to the WLAN to communicate with one another |

### 4.1.97.2.43 t5-security

*wlan-mode commands*

Configures T5 PowerBroadband security settings

A T5 controller uses the IPX operating system to manage its connected radio devices, as opposed to the WiNG operating system used by RFS controllers and NX service platforms. However, a T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5's management within a WiNG supported subnet populated by both types of devices. The CPEs are the T5 controller managed radio devices using the IPX operating system. These CPEs use DSL as their high speed Internet access mechanism using the CPE's physical wallplate connection and phone jack.

**NOTE:** This setting is applicable only when this WLAN supports T5 controllers and their connected CPEs.

**Supported in the following platforms:**

- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
t5-security [static-wep|wpa-enterprise|wpa-personal]

t5-security static-wep encryption-type [wep128|wep64] [hex <STRING>|passphrase
<STRING>]

t5-security [wpa-enterprise|wpa-personal] encryption-type [ccmp|tkip|tkip-ccmp]
version [mixed|wpa|wpa2]
```

**Parameters**

```
• t5-security static-wep encryption-type [wep128|wep64] [hex <STRING>|passphrase
<STRING>]
```

| | |
|---|---|
| t5-security static-wep | Configures the T5 WLAN security type as static-wep |
| encryption-type [wep128\|wep64] | Applies one of the following encryption algorithms to the T5 support WLAN configuration: WEP64 or WEP128 |
| hex <STRING> | Configures the hex password (used to derive the security key)<br>• <STRING> – Specify the hex password (should not exceed the 10 - 26 characters). |
| passphrase <STRING> | Configures the passphrase shared by both transmitting and receiving authenticators<br>• <STRING> – Specify the passphrase. It could either be an alphanumeric string of 8 to 63 ASCII characters or 64 HEX characters. The alphanumeric string allows character spaces. This string is converted to a numeric value. Configuring a passphrase saves you the need to create a 256-bit key each time keys are generated. |

```
• t5-security [wpa-enterprise|wpa-personal] encryption-type [ccmp|tkip|tkip-ccmp]
version [mixed|wpa|wpa2]
```

| | |
|---|---|
| t5-security [wpa-enterprise\| wpa-personal] | Configures the T5 WLAN security type as: wpa-enterprise OR wpa-personal |

| | |
|---|---|
| encryption-type [ccmp\|tkip\|tkip-ccmp] | The following parameters are common to the *wpa-enterprise* and *wpa-personal* keywords:<br>Applies one of the following encryption algorithms to the T5 support WLAN configuration: CCMP, TKIP, or TKIP-CCMP |
| version [mixed\|wpa\|wpa2] | The following parameters are common to the *wpa-enterprise* and *wpa-personal* keywords:<br>• version – Applies one of the following encryption schemes to the T5 support WLAN configuration: WPA, WPA2, or mixed |

**Example**

```
nx9500-6C8809(config-wlan-test)#t5-security wpa-enterprise encryption-type ccmp
version wpa

nx9500-6C8809(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode local
 encryption-type none
 authentication-type none
 t5-security wpa-enterprise encryption-type ccmp version wpa
 t5-client-isolation
nx9500-6C8809(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the configured T5 PowerBroadband security settings |

### 4.1.97.2.44 time-based-access

*wlan-mode commands*

Configures time-based client access to the network resources

Administrators can use this feature to assign fixed days and time of WLAN access for wireless clients

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

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

**Parameters**

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

| | |
|---|---|
| day <option> | Specifies the day or days on which the client can access the WLAN<br>• sunday – Allows access on Sundays only<br>• monday – Allows access on Mondays only<br>• tuesday – Allows access on Tuesdays only<br>• wednesday – Allows access on Wednesdays only<br>• thursday – Allows access on Thursdays only<br>• friday – Allows access on Fridays only<br>• saturday – Allows access on Saturdays only<br>• weekends – Allows access on weekends only<br>• weekdays – Allows access on weekdays only<br>• all – Allows access on all days |
| start <START-TIME> | Optional. Specifies the access start time in hours and minutes (HH:MM) |
| end <END-TIME> | Specifies the access end time in hours and minutes (HH:MM) |

**Example**

```
rfs6000-81742D(config-wlan-test)#time-based-access days weekdays start 10:00 end
 16:30

rfs6000-81742D(config-wlan-test)#show context
wlan test
 ssid testWLAN1
 bridging-mode local
 encryption-type none
 authentication-type none
 protected-mgmt-frames mandatory
 radius vlan-assignment
 time-based-access days weekdays start 10:00 end 16:30
 --More--
rfs6000-81742D(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the configured time-based-access settings |

### 4.1.97.2.45 use

*wlan-mode commands*

This command associates an existing captive portal with a WLAN.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
use [aaa-policy|application-policy|association-acl-policy|bonjour-gw-discovery-policy|captive-portal|ip-access-list|ipv6-access-list|mac-access-list|passpoint-policy|roaming-assist-policy|url-filter|wlan-qos-policy]

use [aaa-policy <AAA-POLICY-NAME>|application-policy <POLICY-NAME>|association-acl-policy <ASSOCIATION-POLICY-NAME>|bonjour-gw-discovery-policy <POLICY-NAME>|captive-portal <CAPTIVE-PORTAL-NAME>|passpoint-policy <PASSPOINT-POLICY-NAME>|roaming-assist-policy <POLICY-NAME>|url-filter <URL-FILTER-NAME>|wlan-qos-policy <WLAN-QOS-POLICY-NAME>]

use ip-access-list [in|out] <IP-ACCESS-LIST-NAME>
use ipv6-access-list [in|out] <IPv6-ACCESS-LIST-NAME>
use mac-access-list [in|out] <MAC-ACCESS-LIST-NAME>
```

**Parameters**

```
• use [aaa-policy <AAA-POLICY-NAME>|application-policy <POLICY-NAME>|
association-acl-policy <ASSOCIATION-POLICY-NAME>|bonjour-gw-discovery-policy
<POLICY-NAME>|captive-portal <CAPTIVE-PORTAL-NAME>|passpoint-policy <PASSPOINT-
POLICY-NAME>|roaming-assist-policy <POLICY-NAME>|url-filter <URL-FILTER-NAME>|
wlan-qos-policy <WLAN-QoS-POLICY-NAME>]
```

| | |
|---|---|
| aaa-policy <AAA-POLICY-NAME> | Uses an existing AAA policy with a WLAN<br>• <AAA-POLICY-NAME> – Specify the AAA policy name. |
| application-policy <POLICY-NAME> | Uses an existing application policy with a WLAN. An application policy defines actions to perform on a packet when it matches a specified set of pre-defined applications or application categories. For more information, see *application-policy*.<br>• <POLICY-NAME> – Specify the policy name. |
| association-acl <ASSOCIATION-POLICY-NAME> | Uses an existing association ACL policy with a WLAN<br>• <ASSOCIATION-POLICY-NAME> – Specify the association ACL policy name. |
| bonjour-gw-discovery-policy <POLICY-NAME> | Uses an existing Bonjour GW Discovery policy with a WLAN. When associated, the Bonjour GW Discovery policy defines a list of services clients can discover across subnets.<br>Contd.. |

| | |
|---|---|
| | Bonjour enables discovery of services on a LAN. Bonjour allows the setting up a network (without any configuration) in which services such as printers, scanners and file-sharing servers can be found using Bonjour. Bonjour only works within a single broadcast domain. However, with a special DNS configuration, it can be extended to find services across broadcast domains.<br>• <POLICY-NAME> – Specify the Bonjour GW Discovery policy name (should be existing and configured).<br>For more information on Bonjour GW Discovery policy, see *bonjour-gw-discovery-policy*. |
| captive-portal <CAPTIVE-PORTAL-NAME> | Specifies the captive-portal policy to use if enforcing captive-portal authentication on this WLAN<br>• <CAPTIVE-PORTAL-NAME> – Specify the captive-portal policy name. Should be existing and configured. |
| passpoint-policy <PASSPOINT-POLICY-NAME> | Associates a passpoint policy (Hotspot2 configuration) with this WLAN<br>• <PASSPOINT-POLICY-NAME> – Specify the Hotspot 2.0 policy name.<br>For more information on passpoint policy, see *passpoint-policy*.<br>Map a passpoint policy to a WLAN. Since the configuration gets applied to the radio by BSS, only the Hotspot 2.0 configuration of primary WLANs on a BSSID is used. Incoming Hotspot 2.0 GAQ/ANQP requests from clients are identified by their destination MAC addresses and are handled by the passpoint policy from the primary WLAN on that BSS.<br>Define one passpoint policy for every WLAN configured. |
| roaming-assist-policy <POLICY-NAME> | Associates an existing roaming assist policy with this WLAN<br>• <POLICY-NAME> – Specify the Roaming Assist policy name.<br>For more information on roaming assist policy, see *roaming-assist-policy*. |
| url-filter <URL-FILTER-NAME> | Associates an existing URL list with this WLAN<br>• <URL-FILTER-NAME> – Specify the URL filter name.<br>For more information on configuring a URL list, see *url-list*. |
| wlan-qos-policy <WLAN-QOS-POLICY-NAME> | Uses an existing WLAN QoS policy with a WLAN<br>• <wlan-qos-policy-name> – Specify the WLAN QoS policy name. |

• `use ip-access-list [in|out] <IP-ACCESS-LIST-NAME>`

| | |
|---|---|
| ip-access-list [in\|out] <IP-ACCESS-LIST-NAME> | Specifies the IP access list for incoming and outgoing packets<br>• in – Applies the IP ACL to incoming packets<br>• out – Applies IP ACL to outgoing packets<br>  • <IP-ACCESS-LIST-NAME> – Specify the IP access list name. |

• `use ipv6-access-list [in|out] <IPv6-ACCESS-LIST-NAME>`

| | |
|---|---|
| ipv6-access-list [in\|out] <IPv6-ACCESS-LIST-NAME> | Specifies the IPv6 access list for incoming and outgoing packets<br>• in – Applies the IPv6 ACL to incoming packets<br>• out – Applies IPv6 ACL to outgoing packets<br>  • <IPv6-ACCESS-LIST-NAME> – Specify the IPv6 access list name. |

- `use mac-access-list [in|out] <MAC-ACCESS-LIST-NAME>`

| | |
|---|---|
| mac-access-list [in\|out] <MAC-ACCESS-LIST-NAME> | Specifies the MAC access list for incoming and outgoing packets.<br>• in – Applies the MAC ACL to incoming packets<br>• out – Applies MAC ACL to outgoing packets<br>  • <MAC-ACCESS-LIST-NAME> – Specify the MAC access list name. |

**Usage Guidelines**

IP and MAC ACLs act as firewalls within a WLAN. WLANs use ACLs as firewalls to filter or mark packets based on the WLAN from which they arrive, as opposed to filtering packets on layer 2 ports. An ACL contains an ordered list of *Access Control Entries* (ACEs). Each ACE specifies a set of conditions (rules) and the action taken in case of a match. The action can be permit, deny, or mark. Therefore, when a packet matches an ACE's conditions, it is either forwarded, dropped, or marked depending on the action specified in the ACE. The order of conditions in the list is critical since filtering is stopped after the first match.

IP ACLs contain deny and permit rules specifying source and destination IP addresses. Each rule has a precedence order assigned. Both IP and non-IP traffic on the same layer 2 interface can be filtered by applying both an IP ACL and a MAC.

Additionally, you can filter layer 2 traffic on a physical layer 2 interface using MAC addresses. A MAC firewall rule uses source and destination MAC addresses for matching operations, where the result is a typical allow, deny, or mark designation to WLAN packet traffic.

Keep in mind IP and non-IP traffic on the same layer 2 interface can be filtered by applying both an IP ACL and a MAC ACL to the interface.

**Example**

```
rfs6000-81742D(config-wlan-test)#use aaa-policy test

rfs6000-81742D(config-wlan-test)#use association-acl-policy test
rfs6000-81742D(config-wlan-test)#show context
wlan test
 ssid testWLAN1
 bridging-mode local
 encryption-type none
 authentication-type none
 protected-mgmt-frames mandatory
 radius vlan-assignment
 time-based-access days weekdays start 10:00 end 16:30
 wing-extensions wmm-load-information
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 use aaa-policy test
 use association-acl-policy test
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 proxy-arp-mode strict
 broadcast-dhcp validate-offer
 shutdown on-unadoption
 http-analyze controller
rfs6000-81742D(config-wlan-test)#
```

```
rfs6000-81742D(config-wlan-ipad_clients)#use bonjour-gw-discovery-policy generic
rfs6000-81742D(config-wlan-ipad_clients)#show context
wlan ipad_clients
 ssid ipad_clients
 vlan 41
 bridging-mode local
 encryption-type none
 authentication-type none
 use bonjour-gw-discovery-policy generic
rfs6000-81742D(config-wlan-ipad_clients)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the following policies associated with a WLAN: aaa-policy, application-policy, association-acl-policy, bonjour-gw-discovery-policy, captive-portal, ip-access-list, ipv6-access-list, mac-access-list, passpoint-policy, roaming-assist-policy, url-filter, or wlan-qos-policy. |

### 4.1.97.2.46 vlan

*wlan-mode commands*

Sets the VLAN where traffic from a WLAN is mapped

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
vlan [<1-4094>|<VLAN-ALIAS-NAME>]
```

**Parameters**

- `vlan [<1-4094>|<VLAN-ALIAS-NAME>]`

| | |
|---|---|
| <1-4094> | Sets a WLAN's VLAN ID. This command starts a new VLAN assignment for a WLAN index. All prior VLAN settings are erased.<br>Use this command to assign just one VLAN to the WLAN. Utilizing a single VLAN per WLAN is a more typical deployment scenario than using a VLAN pool. |
| <VLAN-ALIAS-NAME> | Assigns a VLAN alias to the WLAN. The VLAN alias should to existing and configured.<br>A VLAN alias maps a name to a VLAN ID. When applied to ports (for example GE ports) using the trunk mode, a VLAN alias denies or permits traffic, on the port, to and from the VLANs specified in the alias. For more information on aliases, see *alias*. |

**Example**

```
rfs6000-81742D(config-wlan-test)#vlan 4

rfs6000-81742D(config-wlan-test)#show context
wlan test
 ssid testWLAN1
 vlan 4
 bridging-mode local
 encryption-type none
 authentication-type none
 protected-mgmt-frames mandatory
 radius vlan-assignment
 time-based-access days weekdays start 10:00 end 16:30
 wing-extensions wmm-load-information
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 use aaa-policy test
 use association-acl-policy test
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 proxy-arp-mode strict
 broadcast-dhcp validate-offer
 shutdown on-unadoption
 http-analyze controller
rfs6000-81742D(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes a WLAN's default VLAN mapping |

### 4.1.97.2.47 vlan-pool-member

*wlan-mode commands*

Adds a member VLAN to a WLAN's VLAN pool. Use this option to define the VLANs available to this WLAN. Additionally, define the number of wireless clients supported by each VLAN.

**NOTE:** Configuration of a VLAN pool overrides the 'vlan' configuration.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
vlan-pool-member <WORD> {limit <0-8192>}
```

**Parameters**

- `vlan-pool-member <WORD> {limit <0-8192>}`

| | |
|---|---|
| vlan-pool-member | Adds a member VLAN to a WLAN's VLAN pool<br>Since users belonging to separate VLANs can share the same WLAN, it is not necessary to create a new WLAN for every VLAN in the network. |
| <WORD> | Define the VLANs available to this WLAN. It is either a single index, or a list of VLAN IDs (for example, 1,3,7), or a range (for example, 1-10) |
| limit <0-8192> | Optional. Is ignored if the number of clients are limited and well within the limits of the DHCP pool on the VLAN<br>• <0-8192> – Specifies the number of users allowed |

**Example**

```
rfs6000-81742D(config-wlan-test)#vlan-pool-member 1-10 limit 1

rfs6000-81742D(config-wlan-test)#show context
wlan test
 ssid testWLAN1
 vlan-pool-member 1 limit 1
 vlan-pool-member 2 limit 1
 vlan-pool-member 3 limit 1
 vlan-pool-member 4 limit 1
 vlan-pool-member 5 limit 1
 vlan-pool-member 6 limit 1
 vlan-pool-member 7 limit 1
 vlan-pool-member 8 limit 1
 vlan-pool-member 9 limit 1
 vlan-pool-member 10 limit 1
 bridging-mode local
 encryption-type none
 authentication-type none
 protected-mgmt-frames mandatory
 radius vlan-assignment
 time-based-access days weekdays start 10:00 end 16:30
--More--
rfs6000-81742D(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the list of VLANs mapped to a WLAN |

### 4.1.97.2.48 wep128

*wlan-mode commands*

Configures WEP128 parameters

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
wep128 [key|keys-from-passkey|transmit-key]

wep128 key <1-4> [ascii|hex] [0 <WORD>|2 <WORD>|<WORD>]

wep128 keys-from-passkey <WORD>

wep128 transmit-key <1-4>
```

**Parameters**

- `wep128 key <1-4> [ascii|hex] [0 <WORD>|2 <WORD>|<WORD>]`

| | |
|---|---|
| wep128 | Configures WEP128 parameters. The parameters are: key, key-from-passkey, and transmit-key. |
| key <1-4> | Configures pre-shared hex keys<br>• <1-4> – Configures a maximum of four key indexes. Select the key index from 1 - 4. |
| ascii<br>[0 <WORD>\|<br>2 <WORD>\|\|<br><WORD>] | Sets keys as ASCII characters (5 characters for WEP64, 13 for WEP128)<br>• 0 <WORD> – Configures a clear text key<br>• 2 <WORD> – Configures an encrypted key<br>• <WORD> – Configures keys as 13 ASCII characters converted to hex, or 26 hexadecimal characters |
| hex<br>[0 <WORD>\|<br>2 <WORD>\|<br><WORD>] | Sets keys as hexadecimal characters (10 characters for WEP64, 26 for WEP128)<br>• 0 <WORD> – Configures a clear text key<br>• 2 <WORD> – Configures an encrypted key<br>• <WORD> – Configures keys as 13 ASCII characters converted to hex, or 26 hexadecimal characters |

- `wep128 keys-from-passkey <WORD>`

| | |
|---|---|
| keys-from-passkey <WORD> | Specifies a passphrase from which keys are derived<br>• <WORD> – Specify a passphrase from 4 - 32 characters. |

- `wep128 transmit-key <1-4>`

| | |
|---|---|
| transmit-key <1-4> | Configures the key index used for transmission from an AP to a wireless client or service platform<br>• <1-4> – Specify a key index from 1 - 4. |

**Example**

```
rfs6000-81742D(config-wlan-test)#wep128 keys-from-passkey example@123

rfs6000-81742D(config-wlan-test)#show context
wlan test
 ssid testWLAN1
 vlan-pool-member 1 limit 1
 vlan-pool-member 2 limit 1
 vlan-pool-member 3 limit 1
 vlan-pool-member 4 limit 1
 vlan-pool-member 5 limit 1
 vlan-pool-member 6 limit 1
 vlan-pool-member 7 limit 1
 vlan-pool-member 8 limit 1
 vlan-pool-member 9 limit 1
 vlan-pool-member 10 limit 1
 bridging-mode local
 encryption-type none
 authentication-type none
 protected-mgmt-frames mandatory
 wep128 key 1 hex 0 25f6e7ed9718918a87a75acc75
 wep128 key 2 hex 0 2b3fb36924b22dffe98c86c315
 wep128 key 3 hex 0 1ebf3394431700194762ebd5b2
 wep128 key 4 hex 0 e3de75be311bd787aeac5e4e8b
 radius vlan-assignment
 time-based-access days weekdays start 10:00 end 16:30
--More--
rfs6000-81742D(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Resets the WEP128 PSK and transmission keys to factory-default values. |

### 4.1.97.2.49 wep64

*wlan-mode commands*

Configures WEP64 parameters

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
wep64 [key|keys-from-passkey|transmit-key]

wep64 key <1-4> [ascii|hex] [0 <WORD>|2 <WORD>|<WORD>]

wep64 keys-from-passkey <WORD>

wep64 transmit-key <1-4>
```

**Parameters**

- `wep64 key <1-4> [ascii|hex] [0 <WORD>|2 <WORD>|<WORD>]`

| | |
|---|---|
| wep64 | Configures WEP64 parameters<br>The parameters are: key, key-from-passkey, and transmit-key. |
| key <1-4> | Configures pre-shared hex keys<br>• <1-4> – Configures a maximum of four key indexes. Select a key index from 1 - 4. |
| ascii<br>[0 <WORD>\|<br>2 <WORD>\|<br><WORD>] | Sets keys as ASCII characters (5 characters for WEP64, 13 for WEP128)<br>• 0 <WORD> – Configures a clear text key<br>• 2 <WORD> – Configures an encrypted key<br>• <WORD> – Configures key (10 hex or 5 ASCII characters for WEP64, 26 hex or 13 ASCII characters for WEP128). |
| hex<br>[0 <WORD>\|<br>2 <WORD>\|<br><WORD>] | Sets keys as hexadecimal characters (10 characters for WEP64, 26 for WEP128)<br>• 0 <WORD> – Configures a clear text key<br>• 2 <WORD> – Configures an encrypted key<br>• <WORD> – Configures the key (10 hex or 5 ASCII characters for WEP64, 26 hex or 13 ASCII characters for WEP128) |

- `wep64 keys-from-passkey <WORD>`

| | |
|---|---|
| keys-from-passkey <WORD> | Specifies a passphrase from which keys are derived<br>• <WORD> – Specify a passphrase from 4 - 32 characters. |

- `wep64 transmit-key <1-4>`

| | |
|---|---|
| transmit-key <1-4> | Configures the key index used for transmission from an AP to a wireless client or service platform<br>• <1-4> – Specify a key index from 1 - 4. |

**Example**

```
rfs6000-81742D(config-wlan-test)#wep64 key 1 ascii test1

rfs6000-81742D(config-wlan-test)#wep64 transmit-key 1

rfs6000-81742D(config-wlan-test)#show context
wlan test
 ssid testWLAN1
 vlan-pool-member 1 limit 1
 vlan-pool-member 2 limit 1
 vlan-pool-member 3 limit 1
 vlan-pool-member 4 limit 1
 vlan-pool-member 5 limit 1
 vlan-pool-member 6 limit 1
 vlan-pool-member 7 limit 1
 vlan-pool-member 8 limit 1
 vlan-pool-member 9 limit 1
 vlan-pool-member 10 limit 1
 bridging-mode local
 encryption-type none
 authentication-type none
 protected-mgmt-frames mandatory
 wep64 key 1 hex 0 7465737431
 radius vlan-assignment
 time-based-access days weekdays start 10:00 end 16:30
 wing-extensions wmm-load-information
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 use aaa-policy test
--More--
rfs6000-81742D(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Resets the WEP64 PSK and transmission keys to factory-default values |

### 4.1.97.2.50 wing-extensions

*wlan-mode commands*

Enables support for WiNG-specific client extensions to the IEEE 802.11x WLAN standards that potentially increase client roaming reliability and handshake speed

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
wing-extensions [ap-attributes-information {include-hostname}|
coverage-hole-detection {11k-clients|offset <5-20>|threshold <-80--60}|
ft-over-ds-aggregate|move-command|scan-assist {channel-info-interval <6-9>}|
smart-scan|wing-load-information|wmm-load-information]
```

**Parameters**

```
• wing-extensions [ap-attributes-information {include-hostname}|
coverage-hole-detection {11k-clients|offset <5-20>|offset <5-20>|threshold <-80--
60}|ft-over-ds-aggregate|move-command|scan-assist {channel-info-interval <6-9>}|
smart-scan|wing-load-information|wmm-load-information]
```

| | |
|---|---|
| wing-extensions | Enables support for inclusion of WiNG-specific client extensions in radio transmissions |
| ap-attributes-information {include-hostname} | Enables support for AP attributes *information element* (IE)<br>• include-hostname – Optional. When enabled, includes AP's hostname, as a sub-element, in the AP attributes IE.<br>The AP attributes IE is vendor-specific and, when enabled, is added to beacons and probe responses. Inclusion of AP attributes IE allows Extreme Networks terminals to:<br>- Recognize Extreme APs<br>- Determine if the AP supports PAN BU features, irrespective of whether these features are enabled or not.<br>AP attributes IE is not added to beacons and probe responses by default. |
| overage-hole-detection {11k-clients\| offset <5-20>\| threshold <-80--60>} | Enables *coverage hole detection* (CHD) and configures CHD parameters. When enabled, allows clients (MUs) to inform an access point when it experiences a coverage hole. A coverage hole is an area of poor wireless coverage not supported by a WiNG managed access point radio. Enable *radio resource measurement* prior to enabling CHD. For enabling radio resource measurement, see *radio-resource-measurement*. CHD is disabled by default.<br>After enabling CHD, optionally configure the following parameters:<br>• 11k-clients – Optional. Provides coverage hole detection to 802.11k-only-capable clients. This is a reduced set of coverage hole detection capabilities (standard 11k messages and behaviors). This option is disabled by default.<br>Contd.. |

| | |
|---|---|
| | • offset <5-20> – Optional. Configures the offset added to the threshold to obtain the access point's signal strength (as seen by the client) considered adequate.<br>  • <5-20> – Specify the offset value from 5 - 20. The default is 5.<br>• threshold – Optional. Configures the access point's signal strength threshold. When *Radio Resource Measurement* and *CVG Hole* are enabled, specify a threshold for the AP's signal strength (as seen by the client) below which a coverage hole incident is reported by the client.<br>  • <-80--60> – Specify the threshold from -80 - -60 dBm. The default is -70 dBm. |
| ft-over-ds-aggregate | Enables *fast-transition* (FT) aggregation of action frames. When enabled, increases roaming speed by eliminating separate key exchange handshake frames with potential roam candidates. Enable fast transition to complete an initial FT over *distribution system* (DS) handshake with multiple roam candidates (up to 6) at once, eliminating the need to send separate FT over DS handshakes to each roam candidate.<br>This option is disabled by default. |
| move-command | Enables use of *Hyper Fast Secure Roaming* (HFSR) for clients on this WLAN. This feature applies only to certain client devices. This option is disabled by default. |
| scan-assist {channel-info-interval <6-9>} | Enables support for scanning assist. When enabled, allows faster roams on *Dynamic Frequency Selection* (DFS) channels by eliminating passive scans. Clients get channel information directly from possible roam candidates. This option is disabled by default.<br>• channel-info-interval <6-9> – Optional. Configures the interval at which channel information is periodically retrieved from potential roam candidates without requesting scan assist.<br>  • <6-9> – Specify the interval from 6 - 9 seconds. When enabled, the default value is 8 seconds. |
| smart-scan | Enables a smart scan to refine a clients channel scans to just a few channels as opposed to all available channels. This option is disabled by default. |
| wing-load-information | Enables support for the WiNG load information element (Element ID 173) with legacy Symbol Technology clients, thus making them optimally interoperable with the latest Extreme Networks access points. This option is enabled by default. |
| wmm-load-information | Enables support for WiNG *Wi-Fi MultiMedia* (WMM) Load Information Element in radio transmissions with legacy clients. This option is disabled by default. |

**Example**

```
rfs6000-81742D(config-wlan-test)#wing-extensions wmm-load-information

rfs6000-81742D(config-wlan-test)#show context
wlan test
 description TestWLAN
 ssid test
 bridging-mode local
 encryption-type tkip-ccmp
 authentication-type eap
 kerberos server timeout 12
 kerberos server primary host 172.16.10.2
 accounting syslog host 172.16.10.4 port 2
 data-rates 2.4GHz gn
 wing-extensions wmm-load-information
 client-load-balancing probe-req-intvl 5ghz 5
 --More--
rfs6000-81742D(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables support for WiNG-specific client extensions to the IEEE 802.11x WLAN standards. Use the keywords provided to disable a specific wing-extension. |

### 4.1.97.2.51 wireless-client

*wlan-mode commands*

Configures the transmit power indicated to clients

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
wireless-client [count-per-radio|cred-cache-ageout|hold-time|inactivity-timeout|
max-firewall-sessions|reauthentication|roam-notification|t5-inactivity-timeout|
tx-power|vlan-cache-ageout]

wireless-client [count-per-radio <0-256>|cred-cache-ageout <60-86400>|hold-time
<1-86400>|inactivity-timeout <60-86400>|max-firewall-sessions <10-10000>|
reauthentication <30-86400>|t5-inactivity-timeout <60-86400>|tx-power <0-20>|
vlan-cache-ageout <60-86400>]

wireless-client roam-notification [after-association|after-data-ready|auto]
```

**Parameters**

```
• wireless-client [count-per-radio <0-256>|cred-cache-ageout <60-86400>|hold-time
<1-86400>|inactivity-timeout <60-86400>|max-firewall-sessions <10-10000>|
reauthentication <30-86400>|t5-inactivity-timeout <60-86400>|tx-power <0-20>|
vlan-cache-out <60-86400>]
```

| | |
|---|---|
| wireless-client | Configures the transmit power indicated to wireless clients for transmission |
| count-per-radio <0-256> | Configures the maximum number of clients allowed on this WLAN per radio<br>• <0-256> – Specify a value from 0 - 256. |
| cred-cache-ageout <60-86400> | Configures the timeout period for which client credentials are cached across associations<br>• <60-86400> – Specify a value from 60 - 86400 seconds. |
| hold-time <1-86400> | Configures the time period for which wireless client state information is cached post roaming<br>• <1-86400> – Specify a value from 1 - 86400 seconds. |
| inactivity-timeout <60-86400> | Configures an inactivity timeout period in seconds. If a frame is not received from a wireless client for this period of time, the client is disassociated.<br>• <60-86400> – Specify a value from 60 - 86400 seconds. |
| max-firewall-sessions <10-10000> | Configures the maximum firewall sessions allowed per client on a WLAN<br>• <10-10000> – Specify the maximum number of firewall sessions allowed from 10 - 10000. |
| reauthentication <30-86400> | Configures periodic reauthentication of associated clients<br>• <30-86400> – Specify the client reauthentication interval from 30 - 86400 seconds. |
| t5-inactivity-timeout <60-86400> | Configures and inactivity timeout, in seconds, for T5 devices. When configured, the T5 device is disassociated if the time lapsed after the last frame received from it exceeds the value specified here.<br>• <60-86400> – Specify a value from 60 - 86400 seconds. The default is 60 seconds. |

| | |
|---|---|
| tx-power <0-20> | Configures the transmit power indicated to clients<br>• <0-20> – Specify a value from 0 - 20 dBm. |
| vlan-cache-ageout <60-86400> | Configures the timeout period for which client VLAN information is cached across associations.<br>• <60-86400> – Specify a value from 60 - 86400 seconds. |

- `wireless-client roam-notification [after-association|after-data-ready|auto]`

| | |
|---|---|
| wireless-client | Configures the transmit power indicated to wireless clients for transmission |
| roam-notification | Configures when a roam notification is transmitted |
| after-association | Transmits a roam notification after a client has associated |
| after-data-ready | Transmits a roam notification after a client is data-ready (after completion of authentication, handshakes, etc.) |
| auto | Transmits a roam notification upon client association (if the client is known to have authenticated to the network) |

**Example**

```
rfs6000-81742D(config-wlan-test)#wireless-client cred-cache-ageout 65

rfs6000-81742D(config-wlan-test)#wireless-client hold-time 200

rfs6000-81742D(config-wlan-test)#wireless-client max-firewall-sessions 100

rfs6000-81742D(config-wlan-test)#wireless-client reauthentication 35

rfs6000-81742D(config-wlan-test)#wireless-client tx-power 12

rfs6000-81742D(config-wlan-test)#show context
wlan test
 ssid testWLAN1
 vlan-pool-member 1 limit 1
 vlan-pool-member 2 limit 1
 vlan-pool-member 3 limit 1
 vlan-pool-member 4 limit 1
 vlan-pool-member 5 limit 1
 vlan-pool-member 6 limit 1
 vlan-pool-member 7 limit 1
 vlan-pool-member 8 limit 1
 vlan-pool-member 9 limit 1
 vlan-pool-member 10 limit 1
 bridging-mode local
 encryption-type none
 authentication-type none
 wireless-client hold-time 200
 wireless-client cred-cache-ageout 65
 wireless-client max-firewall-sessions 100
 protected-mgmt-frames mandatory
 wireless-client reauthentication 35
 wep64 key 1 hex 0 7465737431
 wep128 key 1 hex 0 25f6e7ed9718918a87a75acc75
 wep128 key 2 hex 0 2b3fb36924b22dffe98c86c315
 wep128 key 3 hex 0 1ebf3394431700194762ebd5b2
 wep128 key 4 hex 0 e3de75be311bd787aeac5e4e8b
 radius vlan-assignment
 time-based-access days weekdays start 10:00 end 16:30
 wing-extensions wmm-load-information
 wireless-client tx-power 12
 client-load-balancing probe-req-intvl 5ghz 5
--More--
rfs6000-81742D(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes or reverts to default configured wireless client related parameters |

### 4.1.97.2.52 wpa-wpa2

*wlan-mode commands*

Modifies TKIP-CCMP (WPA/WPA2) related parameters

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
wpa-wpa2 [exclude-wpa2-tkip|handshake|key-rotation|opp-pmk-caching|pmk-caching|
preauthentication|server-only-authentication|psk|tkip-countermeasures|
use-sha256-akm]

wpa-wpa2 [exclude-wpa2-tkip|opp-pmk-caching|pmk-caching|preauthentication|
server-only-authentication|use-sha256-akm]

wpa-wpa2 handshake [attempts|init-wait|priority|timeout]
wpa-wpa2 handshake [attempts <1-5>|init-wait <5-1000000>|priority [high|normal]|
timeout <10-5000> {10-5000}]

wpa-wpa2 key-rotation [broadcast|unicast] <30-86400>

wpa-wpa2 psk [0 <LINE>|2 <LINE>|<LINE>]

wpa-wpa2 tkip-countermeasures holdtime <0-65535>
```

**Parameters**

- `wpa-wpa2 [exclude-wpa2-tkip|opp-pmk-caching|pmk-caching|preauthentication|server-only-authentication|use-sha256-akm]`

| | |
|---|---|
| wpa-wpa2 | Modifies TKIP-CCMP (WPA/WPA2) related parameters |
| exclude-wpa2-tkip | Excludes the *Wi-Fi Protected Access II* (WPA2) version of TKIP. It supports the WPA version of TKIP only. This option is disabled by default. |
| opp-pmk-caching | Uses opportunistic key caching (same *Pairwise Master Key* (PMK) across APs for fast roaming with EAP.802.1x. This option is enabled by default. |
| pmk-caching | Uses cached pair-wise master keys (fast roaming with eap/802.1x). This option is enabled by default. |
| preauthentication | Uses pre-authentication mode (WPA2 fast roaming) |
| server-only-authentication | Uses online sign up server-only-authenticated encryption network. This option is disabled by default. |
| use-sha256-akm | Uses sha256 authentication key management suite. This option is disabled by default. |

- `wpa-wpa2 handshake [attempts <1-5>|init-wait <5-1000000>|priority [high|normal]|timeout <10-5000> {10-5000}]`

| | |
|---|---|
| wpa-wpa2 | Modifies TKIP-CCMP (WPA/WPA2) related parameters |
| handshake | Configures WPA/WPA2 handshake parameters |
| attempts <1-5> | Configures the total number of times a message is transmitted towards a non-responsive client<br>• <1-5> – Specify a value from 1 - 5. The default is 2. |

| | |
|---|---|
| init-wait <5-1000000> | Configures a minimum wait-time period, in microseconds, before the first handshake message is transmitted from the AP. This option is disabled by default.<br>• <5-1000000> – Specify a value from 5 - 1000000 microseconds. |
| priority [high\|normal] | Configures the relative priority of handshake messages compared to other data traffic<br>• high – Treats handshake messages as high priority packets on a radio. This is the default setting.<br>• normal – Treats handshake messages as normal priority packets on a radio |
| timeout <10-5000> <10-5000> | Configures the timeout period, in milliseconds, for a handshake message to retire. Once this period is exceed, the handshake message is retired.<br>• <10-5000> – Specify a value from 10 - 5000 milliseconds. The default is 500 milliseconds.<br>• <10-5000> – Optional. Configures a different timeout between the second and third attempts |

- `wpa-wpa2 key-rotation [broadcast|unicast] <30-86400>`

| | |
|---|---|
| wpa-wpa2 | Modifies TKIP-CCMP (WPA/WPA2) related parameters |
| key-rotation | Configures parameters related to periodic rotation of encryption keys. The periodic key rotation parameters are broadcast, multicast, and unicast traffic. |
| broadcast <30-86400> | Configures the periodic rotation of keys used for broadcast and multicast traffic. This parameter specifies the interval, in seconds, at which keys are rotated. This option is disabled by default.<br>• <30-86400> – Specify a value from 30 - 86400 seconds. |
| unicast <30-86400> | Configures a periodic interval for the rotation of keys, used for unicast traffic. This option is disabled by default.<br>• <30-86400> – Specify a value from 30 - 86400 seconds. |

- `wpa-wpa2 psk [0 <LINE>|2 <LINE>|<LINE>]`

| | |
|---|---|
| wpa-wpa2 | Modifies TKIP-CCMP (WPA/WPA2) related parameters |
| psk | Configures a pre-shared key. The key options are: 0, 2, and LINE |
| 0 <LINE> | Configures a clear text key |
| 2 <LINE> | Configures an encrypted key |
| <LINE> | Enter the pre-shared key either as a passphrase not exceeding 8 - 63 characters, or as a 64 character (256bit) hexadecimal value |

- `wpa-wpa2 tkip-countermeasures holdtime <0-65535>`

| | |
|---|---|
| wpa-wpa2 | Modifies TKIP-CCMP (WPA/WPA2) parameters |
| tkip-countermeasures | Configures a hold time period for implementation of TKIP counter measures |
| holdtime <0-65535> | Configures the amount of time a WLAN is disabled when TKIP counter measures are invoked<br>• <0-65535> – Specify a value from 0 - 65535 seconds. The default is 60 seconds. |

**Example**

```
rfs6000-81742D(config-wlan-test)#wpa-wpa2 tkip-countermeasures hold-time 2

rfs6000-81742D(config-wlan-test)#show context
wlan test
 ssid testWLAN1
 vlan-pool-member 1 limit 1
 vlan-pool-member 2 limit 1
 vlan-pool-member 3 limit 1
 vlan-pool-member 4 limit 1
 vlan-pool-member 5 limit 1
 vlan-pool-member 6 limit 1
 vlan-pool-member 7 limit 1
 vlan-pool-member 8 limit 1
 vlan-pool-member 9 limit 1
 vlan-pool-member 10 limit 1
 bridging-mode local
 encryption-type none
 authentication-type none
 wireless-client hold-time 200
 wireless-client cred-cache-ageout 65
 wireless-client max-firewall-sessions 100
 protected-mgmt-frames mandatory
 wireless-client reauthentication 35
 wpa-wpa2 tkip-countermeasures hold-time 2
 wep64 key 1 hex 0 7465737431
 wep128 key 1 hex 0 25f6e7ed9718918a87a75acc75
--More--
rfs6000-81742D(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes or reverts to default TKIP-CCMP (WPA/WPA2) related parameters |

### 4.1.97.2.53 service

*wlan-mode commands*

Invokes service commands applicable in the WLAN configuration mode

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
service [allow-ht-only|allow-open-passpoint|client-load-balancing|cred-cache|
eap-mac-mode|eap-mac-multicopy|eap-mac-multikeys|eap-throttle|
enforce-pmkid-validation|key-index|monitor|radio-crypto|reauthentication|
session-timeout|tx-deauth-on-roam-detection|unresponsive-client|wpa-wpa2|show]

service [allow-ht-only|allow-open-passpoint|cred-cache [clear-on-4way-timeout|
clear-on-disconnect]|eap-mac-multicopy|eap-mac-multikeys|enforce-pmkid-
validation|radio-crypto|reauthentication seamless|session-timeout mac|
tx-deauth-on-roam-detection|show cli]

service eap-mac-mode [mac-always|normal]

service eap-throttle <0-254>

service key-index eap-wep-unicast <1-4>

service monitor [aaa-server|adoption|captive-portal|dhcp|dns]

service monitor [aaa-server|adoption vlan <1-4094>|captive-portal external-server]
service monitor [dhcp|dns] crm <RESOURCE-NAME> vlan <1-4094>

service unresponsive-client [attempts <1-1000>|ps-detect {threshold <1-1000>}|
timeout <1-60>]

service wpa-wpa2 exclude-ccmp
```

**Parameters**

```
• service [allow-ht-only|allow-open-passpoint|cred-cache [clear-on-4way-timeout|
clear-on-disconnect]|eap-mac-multicopy|eap-mac-multikeys|enforce-pmkid-
validation|radio-crypto|reauthentication seamless|session-timeout mac|tx-deauth-
on-roam-detection|show cli]
```

| | |
|---|---|
| allow-ht-only | Only allows clients capable of High Throughput (802.11n) data rates to associate. This option is disabled by default. |
| allow-open-passpoint | Enables non-WPA2 security for passpoint WLANs. This option is disabled by default.<br>For more information on passpoint policy and configuration, see *PASSPOINT POLICY*. |
| cred-cache [clear-on-4way-timeout\| clear-on-disconnect] | Clears credential cache based on the parameter passed<br>• clear-on-4way-timeout – Clears cached client credentials after the 4way handshake with a client has timed out. This option is enabled by default.<br>• clear-on-disconnect – Clears cached client credentials after the client has disconnected from the network. This option is disabled by default. |
| eap-mac-multicopy | Enables sending of multiple copies of broadcast and unicast messages. This option is disabled by default. |

| | |
|---|---|
| eap-mac-multikeys | Enables configuration of different key indices for MAC authentication. This option is disabled by default. |
| enforce-pmkid-validation | Validates the *Predictive real-time pairwise master key identifier* (PMKID) contained in a client's association request against the one present in the wpa-wpa2 handshake. This option is enabled by default.<br>This functionality is based on the *Proactive Key Caching* (PKC) extension of the 802.11i EEEE standard. Whenever a wireless client successfully authenticates with a AP it receives a *pairwise master key* (PMK). PKC allows clients to cache this PMK and reuse it for future re-authentications with the same AP. The PMK is unique for every client and is identified by the PMKID. The PMKID is a combination of the hash of the PMK, a string, the station and the MAC addresses of the AP. |
| radio-crypto | Uses radio hardware for encryption and decryption. This is applicable only for devices using *Counter Cipher Mode with Block Chaining Message Authentication Code Protocol* (CCMP) encryption mode. This option is enabled by default. |
| reauthentication seamless | Enables seamless EAP client reauthentication without disconnecting client after the session has timed out. This option is enabled by default. |
| session-timeout mac | Enables reauthentication of MAC authenticated clients without disconnecting client after the session has timed out. This option is enabled by default. |
| tx-deauth-on-roam-detection | Transmits a deauthentication on the air while disassociating a client because its roam is detected on the wired side. This option is disabled by default. |
| show cli | Displays the CLI tree of the current mode. When used in the WLAN mode, this command displays the WLAN CLI structure. |

- `service eap-mac-mode [mac-always|normal]`

| | |
|---|---|
| eap-mac-mode | Configures the EAP and/or MAC authentication mode used with this WLAN. This option is enabled by default. |
| mac-always | Enables both EAP and MAC authentication. MAC authentication is performed first, followed by EAP authentication. Clients are granted access based on the EAP authentication result. If a client does not have EAP, the MAC authentication result is used to grant access. |
| normal | Grants client access if the client clears either EAP or MAC authentication. This is the default setting. |

- `service eap-throttle <0-254>`

| | |
|---|---|
| eap-throttle <0-254> | Enables EAP request throttling. Use this command to specify the maximum number of parallel EAP sessions allowed on this WLAN. Once this specified value is exceeded, all incoming EAP session requests are throttled. This option is enabled by default.<br>• <0-254> – Specify a value from 0 - 254. This default value is 0. |

- `service key-index eap-wep-unicast <1-4>`

| | |
|---|---|
| key-index eap-wep-unicast <1-4> | Configures an index with each key during EAP authentication with WEP. This option is enabled by default.<br>• <1-4> – Select a index from 1 - 4. The default value is 1. |

- `service wpa-wpa2 exclude-ccmp`

| | |
|---|---|
| wpa-wpa2 exclude-ccmp | Configures exclusion of CCMP requests when the authentication mode is set to tkip-ccmp. When enabled, it provides compatibility for client devices not compliant with tkip-ccmp. This option is disabled by default. |

- `service monitor [aaa-server|adoption vlan <1-4094>|captive-portal external-server]`

| | |
|---|---|
| monitor | Enables critical resource monitoring. In a WLAN, service monitoring enables regular monitoring of external AAA servers, captive portal servers, access point adoption, DHCP and DNS servers. When enabled, it allows administrators to notify users of a service's availability and make resource substitutions in case of unavailability of a service. |
| aaa-server | Enables external AAA server failure monitoring. When enabled monitors an external RADIUS server resource's AAA activity and ensures its adoption and availability. This feature is disabled by default. |
| adoption vlan <1-4094> | Enables adoption failure monitoring on an adopted AP. Also configures a adoption failover VLAN. This feature is disabled by default.<br>• VLAN <1-4094> – Specify the VLAN on which clients are placed when the connectivity between the AAP and the controller is lost.<br>Configure a DHCP pool and gateway for the failover VLAN. Ensure the DHCP server is running on the AP. Also ensure that the DHCP pool is configured to have less lease time.<br>When this feature is enabled on a WLAN, it allows adopted APs to monitor their connectivity with the controller. If and when this connectivity is lost, all new clients are placed in the configured adoption failover VLAN. They are served an IP by the DHCP server running on the AP. In this situation if a client tries to access a Web URL, the AP redirects the client to a page stating that the service is down.<br>When the AAP's link to the switch is restored, clients are placed back in the WLAN's configured VLAN, and are served an IP from the corresponding configured DHCP server (external or on the AP/controller). |
| captive-portal external-server | Enables external captive portal server failure monitoring. When enabled, monitors externally hosted captive portal activity, and user access to the controller or service platform managed network. This feature is disabled by default.<br>When enabled, this feature enables APs to display, to an externally located captive portal's user, the no-service page when the captive portal's server is not reachable. |

- `service monitor [dhcp|dns] crm <RESOURCE-NAME> vlan <1-4094>]`

| | |
|---|---|
| monitor | Enables DHCP and/or DNS server monitoring on this WLAN. |
| dhcp | Enables monitoring of a specified DHCP server. When the connection to the DHCP server is lost, captive portal users automatically migrate to a pre-defined VLAN. The feature is disabled by default.<br>Use the *crm* keyword to specify the DHCP server to monitor. |
| dns | Enables monitoring of a specified DNS server. When the connection to the DNS server is lost, captive portal users automatically migrate to a pre-defined VLAN. The feature is disabled by default.<br>Use the *crm* keyword to specify the DNS server to monitor. |
| crm <RESOURCE-NAME> | This keyword is common to the 'dhcp' and 'dns' parameters.<br>• crm – Identifies the DHCP and/or DNS server to monitor<br>  • <RESOURCE-NAME> – Specify the name of the DHCP or DNS server.<br>Once enabled, the CRM server monitors the DHCP/DNS server and updates their status as 'up' or 'down' depending on the availability of the resource. When either of these resources is down the wireless client is mapped to the failover VLAN and served with the 'no-service' page through the access point. |

| | |
|---|---|
| vlan <1-4094> | This keyword is common to the 'dhcp' and 'dns' parameters.<br>After specifying the DHCP/DNS sever resource, specify the failover VLAN.<br>• VLAN <1-4094> – Configures the failover VLAN from 1 - 4094.<br>When the DHCP server resource becomes unavailable, the device falls back to the VLAN defined here. This VLAN has a DHCP server configured that provides a pool of IP addresses with a lease time less than the main DHCP server.<br>When this DNS server resource becomes unavailable, the device falls back to the VLAN defined here. This VLAN has a DNS server configured that provides DNS address resolution until the main DNS server becomes available. |

```
• service unresponsive-client [attempts <1-1000>|ps-detect {threshold <1-1000>}|
timeout <1-60>]
```

| | |
|---|---|
| eap-mac-mode | Configures handling of unresponsive clients |
| attempts <1-1000> | Configures the maximum number of successive packets that failed transmission<br>• <1-1000> – Specify a value from 1 - 1000. The default is 7. |
| ps-detect {threshold <1-1000>} | Enables the detection of power-save mode clients, whose PS stats has not been updated on the AP. This option is enabled by default.<br>• threshold – Optional. Configures the threshold at which power-save client detection is triggered<br>• <1-1000> – Configures the number of successive unacknowledged packets received before power-save detection is triggered. Specify a value from 1 - 1000. The default is 3. |
| timeout <1-60> | Configures the interval, in seconds, for successive packets not acknowledged by the client<br>• <1-60> – Specify a value from 1 - 60 seconds. The default is 3 seconds. |

**Example**

```
rfs4000-229D58(config-wlan-test)#service allow-ht-only

rfs4000-229D58(config-wlan-test)#service monitor aaa-server

rfs4000-229D58(config-wlan-test)#show context
wlan test
 ssid test
 vlan 1
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 service monitor aaa-server
 service allow-ht-only
 controller-assisted-mobility
rfs4000-229D58(config-wlan-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes or reverts to default WLAN settings configured using the 'service' command |

## 4.1.98 wlan-qos-policy

*Global Configuration Commands*

Configures a WLAN QoS policy

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
wlan-qos-policy <WLAN-QOS-POLICY-NAME>
```

**Parameters**

- `wlan-qos-policy <WLAN-QOS-POLICY-NAME>`

| | |
|---|---|
| <WLAN-QOS-POLICY-NAME> | Specify the WLAN QoS policy name. If the policy does not exist, it is created. |

**Example**

```
rfs6000-81742D(config)#wlan-qos-policy test
rfs6000-81742D(config-wlan-qos-test)#?
WLAN QoS Mode commands:
  accelerated-multicast  Configure accelerated multicast streams address assnd
                         forwarding QoS classification
  classification         Select how traffic on this WLAN must be classified
                         (relative prioritization on the radio)
  multicast-mask         Egress multicast mask (frames that match bypass the
                         PSPqueue. This permits intercom mode operation
                         without delay even in the presence of PSP clients)
  no                     Negate a command or set its defaults
  qos                    Quality of service
  rate-limit             Configure traffic rate-limiting parameters on a
                         per-wlan/per-client basis
  svp-prioritization     Enable spectralink voice protocol support on this
                         wlan
  voice-prioritization   Prioritize voice client over other client (for
                         non-WMM clients)
  wmm                    Configure 802.11e/Wireless MultiMedia parameters

  clrscr                 Clears the display screen
  commit                 Commit all changes made in this session
  do                     Run commands from Exec mode
  end                    End current mode and change to EXEC mode
  exit                   End current mode and down to previous mode
  help                   Description of the interactive help system
  revert                 Revert changes
  service                Service Commands
  show                   Show running system information
  write                  Write running configuration to memory or terminal

rfs6000-81742D(config-wlan-qos-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an existing WLAN QoS Policy |

**NOTE:** For more information on WLAN QoS policy commands, see *Chapter 21, WLAN-QOS-POLICY*.

## 4.1.99 url-filter

*Global Configuration Commands*

The following table lists the commands that allow you to enter the URL filter configuration mode:

**Table 4.55** *Commands Creating a URL Filter*

| Command | Description | Reference |
|---|---|---|
| *url-filter* | Creates a new URL filter and enters its configuration mode | *page 4-552* |
| *url-filter-config-mode commands* | Summarizes the URL filter configuration mode commands | *page 4-555* |

### 4.1.99.1 url-filter

*url-filter*

Creates a new URL filter (Web filter) and enters its configuration mode. URL filtering is a licensed feature. When applied to a WiNG device the license allows you to enable URL filtering on the device, create and apply a URL filter defining the banned and/or allowed URLs. When enabled, the URL filter is applied to all user-initiated URL requests to determine if the requested URL is banned or allowed. Only if allowed is the user's request (in the form of a HTTP request packet) forwarded to the Web server.

URL filters can be applied at any of the following points: the user's application (browser/email reader), the network's gateway, at the *Internet service provider's* (ISP) end, and also on a Web portal. For wireless clients, the WLAN infrastructure is the best place to implement these filters.

A URL filter is a set of whitelist and/or blacklist rules. The whitelist allows access only to those Websites and URLs specified in it. All other Websites and URLs, apart from those specified in the whitelist, are banned. On the other hand, the blacklist bans all Websites and URLs specified in it. All other Websites and URLs, apart from those specified in the blacklist, are allowed.

To simplify URL filter configuration, Websites have been classified into pre-defined category-types and categories. The system provides 12 category-types and 64 categories. To further simplify configuration, these 12 category-types have been grouped into *five* (5) pre-defined levels. (See Usage Guidelines section for the list of category-types, categories, and levels). The actual classification of URLs (on the basis of the pre-defined factors mentioned above) is done by the classification server. A local database also helps by caching URL records for a user-defined time period. The classification server host is specified in the Web filter policy. The Web filter policy also defines the URL database parameters. For more information, see *web-filter-policy*.

The WiNG software also allows you to create URL lists. Each URL list contains a list of user-defined URLs. Use the URL list in a URL filter (whitelist or blacklist rule) to identify the URLs to ban or allow. For example, a URL list named SocialNetworking is created listing the following three sites: Facebook, Twitter, and LinkedIn. When applied to a URL filter's blacklist these three sites are banned. Where as, when applied to a whitelist only these three sites are allowed. For more information on configuring a URL list, see *url-list*.

**NOTE:** URL filtering is a licensed feature. Procure and install the license in the device configuration mode. For more information, see *license*.

**Supported in the following platforms:**

- Access Points — AP6522, AP6532, AP7131, AP7502, AP7522, AP7532, AP7562, AP8132
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
url-filter <URL-FILTER-NAME>
```

**Parameters**

- `url-filter <URL-FILTER-NAME>`

| | |
|---|---|
| <URL-FILTER-NAME> | Creates a new URL filter and enters its configuration mode. Specify the URL filter name. If the filter does not exist, it is created. |

**Usage Guidelines**

| | Category Type | Category |
|---|---|---|
| 1 | Adult Content | Alcohol & Tobacco, Dating & Personals, Gambling, Nudity, Pornography/Sexually Explicit, Sex Education, Weapons |
| 2 | Business | Web-based Email |
| 3 | Communication | Chat, Instant Messaging |
| 4 | Entertainment | Streaming Media & Downloads |
| 5 | File Sharing and Backup | Download Sites |
| 6 | Gaming | Games |
| 7 | News Sports and General | Arts, Business, Computer & Technology, Education, Entertainment, Fashion & Beauty, Finance, Forum & Newsgroups, General, Government, Greeting Card, Health & Medicine, Information Security, Job Search, Leisure & Recreation, Network Errors, News, Non-Profits & NGO, Personal Sites, Politics, Private IP Addresses, Real Estates, Religion, Restaurants & Dinning, Search Engine & Portals, Shopping, Sports, Transportation, Translators, Travel |
| 8 | Peer-to-Peer (P2P) | Peer to Peer |
| 9 | Questionable/ Unethical | Child Abuse Images, Cults, Hacking, Hate & Intolerance, Illegal Drug, Illegal Sharing, Illegal Software, School Cheating, Tasteless, Violence |
| 10 | Security Risk | Advertisement & Pop-ups, Anonymizers, Botnets, Compromised, Criminal Activity, Malware, Parked Domains, Phishing & Fraud, Spam Sites |
| 11 | Social and Photo Sharing | Social Networking |
| 12 | Software Update | N/A |

| | Level | Description |
|---|---|---|
| 1 | Basic | Blocks sites/URL categorized as Security Risk |
| 2 | Low | Blocks sites/URL categorized as Adult Content + Basic |
| 3 | Medium | Blocks sites/URL categorized as File Sharing and Backup, P2P, Questionable / Unethical + Low |
| 4 | Medium High | Blocks sites/URL categorized as Gaming + Medium |
| 5 | High | Blocks sites/URL categorized as Communication, Entertainment, Social and Photo Sharing + Medium High |

**Example**

```
nx9500-6C8809(config-url-filter-test)#?
URL Filter Mode commands:
  blacklist    Block access to URL
  blockpage    Configure blocking page parameters
  description  Url filter description
  no           Negate a command or set its defaults
  whitelist    Allow access to URL

  clrscr       Clears the display screen
  commit       Commit all changes made in this session
  do           Run commands from Exec mode
  end          End current mode and change to EXEC mode
  exit         End current mode and down to previous mode
  help         Description of the interactive help system
  revert       Revert changes
  service      Service Commands
  show         Show running system information
  write        Write running configuration to memory or terminal

nx9500-6C8809(config-url-filter-test)#
```

### 4.1.99.2 url-filter-config-mode commands

*url-filter*

The following table summarizes URL filter configuration mode commands:

**Table 4.56** *URL-Filter-Config-Mode Commands*

| Command | Description | Reference |
|---|---|---|
| *blacklist* | Creates a blacklist rule defining a list of banned Websites and URLs | *page 4-556* |
| *blockpage* | Configures the parameters that retrieve the page or content displayed by the client's browser when a requested URL is blocked and cannot be viewed | *page 4-559* |
| *description* | Configures an appropriate description for this URL filter | *page 4-561* |
| *no* | Removes this URL filter's configured parameters | *page 4-562* |
| *whitelist* | Creates a whitelist rule defining a list of Websites and URLs allowed access by clients. | *page 4-563* |

### 4.1.99.2.1 blacklist

*url-filter-config-mode commands*

Creates a blacklist rule. A blacklist is a list of Websites and URLs denied access by clients. Clients requesting blacklisted URLs are presented with a page displaying the 'Web page blocked' message. Parameters relating to this page are configured using the 'blockpage' option.

URL filtering is based on the classification of Websites into pre-defined category-types. Some of the category-types are further divided into multiple categories. Currently available are 12 built-in category types, and 64 categories. These built-in category-types and categories cannot be modified.

Use the available options to identify the URL category-types and categories to include in the blacklist.

In addition to identifying URLs by the categories and category-types they are classified into, the system also provides *five* (5) levels of Web filtering (basic, high, low, medium, and medium-high). Each level identifies a specific set of URL categories to blacklist. For more information on category-types, categories, and URL filtering levels, see *url-filter*.

**Supported in the following platforms:**

- Access Points — AP6522, AP6532, AP7131, AP7502, AP7522, AP7532, AP7562, AP8132
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
blacklist [category-type|level|url-list]

blacklist category-type [adult-content|all|business|communication|entertainment|
file-sharing-backup|gaming|news-sports-general|p2p|questionable|security-risk|
social-photo-sharing|software-updates] precedence <1-500> {description <LINE>}

blacklist level [basic|high|low|medium|medium-high] precedence <1-500>
{description <LINE>}

blacklist url-list <URL-LIST-NAME> precedence <1-500> {description <LINE>}
```

**Parameters**

```
• blacklist category-type [adult-content|all|business|communication|
entertainment|file-sharing-backup|gaming|news-sports-general|p2p|questionable|
security-risk|social-photo-sharing|software-updates] precedence <1-500>
{description <LINE>}
```

| | |
|---|---|
| blacklist category-type <SELECT-CATEGORY-TYPE> | Selects the category-type to blacklist. A category is a pre-defined URL list available in the WiNG software. Categories are based on an external database, and cannot be modified or removed. Custom categories can created with the URL List and added to the database.<br>Websites have been classified into the following 12 category types:<br>adult-content, business, communication, entertainment, file-sharing-backup, gaming, news-sports-general, p2p, questionable, security-risk, social-photo-sharing, and software-updates<br>Contd.. |

| | |
|---|---|
| | Select 'all' to blacklist all category-types.<br>Some of the category-types are further classified into categories. For example, the '*adult-content*' category-type is differentiated into the following categories:<br>• alcohol-tobacco, dating-personals, gambling, nudity, pornography-sexually-explicit, sex-education, and weapons.<br>The system blocks all categories (URLs falling within their limits) within the selected category-type. |
| precedence <1-500> | Configures the precedence value for this blacklist rule. Rules are applied in the increasing order of their precedence. Therefore, rules with lower precedence are applied first. |
| description <LINE> | Optional. Configures a description (not exceeding 80 characters) for this blacklist rule. Enter a description that allows you to identify the purpose of the rule. |

- `blacklist level [basic|high|low|medium|medium-high] precedence <1-500> {description <LINE>}`

| | |
|---|---|
| blacklist level [basic\|high\|low\|medium\|medium-high] | Configures the Web filtering level as basic, high, low, medium, or medium-high. Each of these filter-levels are pre-configured to use a set of category types and this mapping cannot be modified. |
| precedence <1-500> | Configures the precedence value for this blacklist rule. Rules are applied in the increasing order of their precedence. Therefore, rules with lower precedence are applied first. |
| description <LINE> | Optional. Configures a description (not exceeding 80 characters) for this blacklist rule. Enter a description that allows you to identify the purpose of the rule. |

- `blacklist url-list <URL-LIST-NAME> precedence <1-500> {description <LINE>}`

| | |
|---|---|
| blacklist url-list <URL-LIST-NAME> | Associates a URL list with this URL filter. When associated with a blacklist rule, all URLs listed in the specified URL list are blacklisted.<br>URL lists are customized categories included in the custom filter-level setting. URL lists enable an administrator to blacklist or whitelist URLs in addition to the built-in categories. For more information on configuring a URL list, see *url-list*.<br>• <URL-LIST-NAME> – Enter URL list name (should be existing and configured) |
| precedence <1-500> | Configures the precedence value for this blacklist rule. Rules are applied in the increasing order of their precedence. Therefore, rules with lower precedence are applied first. |
| description <LINE> | Optional. Configures a description (not exceeding 80 characters) for this blacklist rule. Enter a description that allows you to identify the purpose of the rule. |

**Example**

```
rfs6000-81742D(config-url-filter-test)#blacklist level medium-high precedence 10

rfs6000-81742D(config-url-filter-test)#blacklist category-type adult-content
category alcohol-tobacco precedence 1

rfs6000-81742D(config-url-filter-test)#blacklist category-type security-risk
category botnets precedence 3
```

```
rfs6000-81742D(config-url-filter-test)#show context
url-filter test
 blacklist level medium-high precedence 10
 blacklist category-type security-risk category botnets precedence 3
 blacklist category-type adult-content category alcohol-tobacco precedence 1
rfs6000-81742D(config-url-filter-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes a blacklist rule from this URL filter. Specify the category-type, category, and precedence to identify the blacklist rule. The identified rule is removed form the URL filter. |

### 4.1.99.2.2 blockpage

*url-filter-config-mode commands*

Configures the parameters that retrieve the page or content displayed by the client's browser when a requested URL is blocked and cannot be viewed

**Supported in the following platforms:**

- Access Points — AP6522, AP6532, AP7131, AP7502, AP7522, AP7532, AP7562, AP8132
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
blockpage [external|internal|path]

blockpage path [external|internal]
blockpage external url <URL>
blockpage internal [content|footer|header|main-logo|org-name|org-signature|
small-logo|title] <LINE/IMAGE-URL>
```

**Parameters**

- `blockpage path [external|internal]`

| | |
|---|---|
| blockpage path [external\|internal] | Specifies if the location of the page displayed, to the client when a requested URL is blocked, is external or internal<br>• external – Indicates the page displayed is hosted on an external Web server resource. If selecting this option, use the *blockpage > external > url <URL>* command to provide the path to the external Web server hosting the page.<br>internal – Indicates the page displayed is hosted internally. This is the default setting. If selecting this option, use the *blockpage > internal > <SELECT-PAGE-TYPE> > <LINE/IMAGE-URL>* command to define the page configuration. |

- `blockpage external url <URL>`

| | |
|---|---|
| blockpage external url <URL> | Configures the URL of the external Web server hosting the page (displayed to the client when a requested URL is blocked).<br>• url <URL> – Specify the URL of the Web server and the blocking page name<br>Valid URLs should begin with http:// or https://<br>The URL can contain query strings.<br>Use '&' or '?' character to separate field-value pair.<br>Enter 'ctrl-v' followed by '?' to configure query strings |

- `blockpage internal [content|footer|header|main-logo|org-name|org-signature| small-logo|title] <LINE/IMAGE-URL>`

| | |
|---|---|
| blockpage internal [content\|footer\|header\|main-logo\|org-name\|org-signature\|small-logo\|title] <LINE/IMAGE-URL> | Configures the internally hosted blocking page parameters, such as the content displayed, page footer and header, organization (the organization enforcing the Web page blocking) details (name, signature, and logo), and page title<br>• content – Configures the text (message) displayed on the blocking page<br>• footer – Configures the text displayed as the blocking page footer<br>Contd... |

| | |
|---|---|
| | • header – Configures the text displayed as the blocking page header<br>• org-name – Configures the organization's name displayed on the blocking page<br>• org-signature – Configures the organization's signature displayed on the blocking page<br>• title – Configures the title of the blocking page.<br>• main-logo – Configures the location of the main logo (organization's large logo)<br>• small-logo – Configures the location of the small logo (organization's small logo)<br>The following keyword is common to all of the above parameters:<br>• <LINE/IMAGE-URL> – Specify the location of the logo (main and small) image file. The image is retrieved and displayed from the location configured here. If you are using this option to provide content, such as organization name, footer, header, etc. enter a text string not exceeding 255 characters in length. |

**Example**

```
rfs6000-81742D(config-url-filter-test)#blockpage internal content "The requested
Web page is blocked and cannot be displayed for viewing"

rfs6000-81742D(config-url-filter-test)#show context
url-filter test
 blacklist level medium-high precedence 10
 blacklist category-type security-risk category botnets precedence 3
 blacklist category-type adult-content category alcohol-tobacco precedence 1
 blockpage internal content "The requested Web page is blocked and cannot be
displayed for viewing"
rfs6000-81742D(config-url-filter-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the blocking page configurations |

### 4.1.99.2.3 description

*url-filter-config-mode commands*

Configures a description for this URL filter. Provide a description that enables you to identify the purpose of this URL filter.

**Supported in the following platforms:**

- Access Points — AP6522, AP6532, AP7131, AP7502, AP7522, AP7532, AP7562, AP8132
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
description <LINE>
```

**Parameters**

- `description <LINE>`

| | |
|---|---|
| description <LINE> | Enter an appropriate description for this URL filter. The description should identify the URL filter's purpose and should not exceed 80 characters in length. |

**Example**

```
rfs6000-81742D(config-url-filter-test)#description Blacklists sites inappropriate
for children and are security risks.

rfs6000-81742D(config-url-filter-test)#show context
url-filter test
 description "Blacklists sites inappropriate for children and are security risks."
 blacklist level medium-high precedence 10
 blacklist category-type security-risk category botnets precedence 3
 blacklist category-type adult-content category alcohol-tobacco precedence 1
 blockpage internal content "The requested Web page is blocked and cannot be
displayed for viewing"
rfs6000-81742D(config-url-filter-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes this URL filter's description |

### 4.1.99.2.4 no

*url-filter-config-mode commands*

Use the no command to remove this URL filter's configured parameters

**Supported in the following platforms:**

- Access Points — AP6522, AP6532, AP7131, AP7502, AP7522, AP7532, AP7562, AP8132
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
no [blacklist|blockpage|description|whitelist]

no blacklist [category-type|level|url-list]
no blacklist [category-type <SELECT-CATEGORY-TYPE>|level <SELECT-LEVEL>|
url-list <URL-LIST-NAME>] precedence <1-500>

no blockpage [external|internal [content|footer|header|main-logo|org-name|
org-signature|small-logo|title]|path]

no description

no whitelist [category-type|url-list]
no whitelist [category-type <SELECT-CATEGORY-TYPE>|url-list <URL-LIST-NAME>]
precedence <1-500>
```

**Parameters**

- no <PARAMETERS>

| | |
|---|---|
| no <PARAMETERS> | Removes this URL filter's configured parameters based on the values passed here |

**Example**

The following example displays the URL filter 'test' settings before the 'no' is executed:

```
rfs6000-81742D(config-url-filter-test)#show context
url-filter test
 description "Blacklists sites inappropriate for children and are security risks."
 blacklist level medium-high precedence 10
 whitelist category-type communication category chat precedence 7
 blacklist category-type security-risk category botnets precedence 3
 blacklist category-type adult-content category alcohol-tobacco precedence 1
 blockpage internal content "The requested Web page is blocked and cannot be
displayed for viewing"
rfs6000-81742D(config-url-filter-test)#

rfs6000-81742D(config-url-filter-test)#no description

rfs6000-81742D(config-url-filter-test)#no blacklist category-type adult-content
category alcohol-tobacco precedence 1

rfs6000-81742D(config-url-filter-test)#no whitelist category-type communication
category chat precedence 7
```

The following example displays the URL filter 'test' settings after the 'no' is executed:

```
rfs6000-81742D(config-url-filter-test)#show context
url-filter test
 blacklist level medium-high precedence 10
 blacklist category-type security-risk category botnets precedence 3
 blockpage internal content "The requested Web page is blocked and cannot be
displayed for viewing"
rfs6000-81742D(config-url-filter-test)#
```

### 4.1.99.2.5 whitelist

*url-filter-config-mode commands*

Creates a whitelist rule. A whitelist is a list of Websites and URLs allowed access by clients.

URL filtering is based on the classification of Websites into pre-defined category-types. Some of the category-types are further divided into multiple categories. Currently available are 12 built-in category types, and 64 categories. These built-in category-types and categories cannot be modified.

Use the available options to identify the category-types and categories to include in the whitelist.

**Supported in the following platforms:**

- Access Points — AP6522, AP6532, AP7131, AP7502, AP7522, AP7532, AP7562, AP8132
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
whitelist [category-type|url-list]

whitelist category-type [adult-content|all|business|communication|entertainment|
file-sharing-backup|gaming|news-sports-general|p2p|questionable|security-risk|
social-photo-sharing|software-updates] precedence <1-500> {description <LINE>}

whitelist url-list <URL-LIST-NAME> precedence <1-500> {description <LINE>}
```

**Parameters**

```
• whitelist category-type [adult-content|all|business|communication|
entertainment|file-sharing-backup|gaming|news-sports-general|p2p|questionable|
security-risk|social-photo-sharing|software-updates] precedence <1-500>
{description <LINE>}
```

| | |
|---|---|
| whitelist category-type <SELECT-CATEGORY-TYPE> | Selects the category-type to add to this whitelist. A category is a pre-defined URL list available in the WiNG software. Categories are based on an external database, and cannot be modified or removed. Custom categories can created with the URL List and added to the database.<br>Websites have been classified into the following 12 category types: adult-content, business, communication, entertainment, file-sharing-backup, gaming, news-sports-general, p2p, questionable, security-risk, social-photo-sharing, and software-updates.<br>Select 'all' to whitelist all category-types.<br>Some of the category-types are further classified into categories. For example, the '*adult-content*' category-type is differentiated into the following categories:<br>• alcohol-tobacco, dating-personals, gambling, nudity, pornography-sexually-explicit, sex-education, and weapons.<br>The system allows all categories (URLs falling within their limits) within the selected category-type. |
| precedence <1-500> | Configures the precedence value for this whitelist rule. Rules are applied in the increasing order of their precedence. Therefore, rules with lower precedence are applied first. |
| description <LINE> | Optional. Configures a description (not exceeding 80 characters) for this whitelist rule. Enter a description that allows you to identify the purpose of the rule. |

- `whitelist url-list <URL-LIST-NAME> precedence <1-500> {description <LINE>}`

| | |
|---|---|
| whitelist url-list <URL-LIST-NAME> | Associates a URL list with this URL filter. When associated with a whitelist rule, all URLs listed in the specified URL list are allowed access.<br>URL lists are customized categories included in the custom filter-level setting. URL lists enable an administrator to blacklist or whitelist URLs in addition to the built-in categories. For more information on configuring a URL list, see *url-list*.<br>• <URL-LIST-NAME> – Enter URL list name (should be existing and configured) |
| precedence <1-500> | Configures the precedence value for this whitelist rule. Rules are applied in the increasing order of their precedence. Therefore, rules with lower precedence are applied first. |
| description <LINE> | Optional. Configures a description (not exceeding 80 characters) for this whitelist rule. Enter a description that allows you to identify the purpose of the rule. |

**Example**

```
rfs6000-81742D(config-url-filter-test)#whitelist category-type communication
category chat precedence 7

rfs6000-81742D(config-url-filter-test)#show context
url-filter test
 description "Blacklists sites inappropriate for children and are security risks."
 blacklist level medium-high precedence 10
 whitelist category-type communication category chat precedence 7
 blacklist category-type security-risk category botnets precedence 3
 blacklist category-type adult-content category alcohol-tobacco precedence 1
 blockpage internal content "The requested Web page is blocked and cannot be
displayed for viewing"
rfs6000-81742D(config-url-filter-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes a whitelist rule from this URL filter. Specify the category-type, category, and precedence to identify the blacklist rule. The identified rule is removed form the URL filter. |

## 4.1.100 url-list

*Global Configuration Commands*

The following table lists the commands that allow you to enter the URL list configuration mode:

**Table 4.57** *Commands Creating a URL List*

| Command | Description | Reference |
|---|---|---|
| *url-list* | Creates a new URL list and enters its configuration mode | *page 4-566* |
| *url-list-config-mode commands* | Summarizes the URL list configuration mode commands | *page 4-567* |

### 4.1.100.1 url-list

*url-list*

Creates a URL list and enters its configuration mode. URL lists are a means of categorizing URLs on the basis of various criteria, such as frequently used, not-permitted, etc. It is used in URL filters to identify whitelisted/blacklisted URLs. Web requests are blocked or approved based on URL filter whitelist/blacklist rules. A whitelist bans all sites except the categories and URL lists defined in the whitelist. The blacklist allows all sites except the categories and URL lists defined in the blacklist

**Supported in the following platforms:**

- Access Points — AP6522, AP6532, AP7131, AP7502, AP7522, AP7532, AP7562, AP8132
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
url-list <URL-LIST-NAME>
```

**Parameters**

- `url-list <URL-LIST-NAME>`

| | |
|---|---|
| <URL-LIST-NAME> | Specify the URL list name. The URL list is created if another list with the same name does not exist. |

**Example**

```
nx9500-6C8809(config)#url-list URLlist1
nx9500-6C8809(config-url-list-URLlist1)#?
URL List Mode commands:
  description  Description of the category
  no           Negate a command or set its defaults
  url          Add a URL entry

  clrscr       Clears the display screen
  commit       Commit all changes made in this session
  do           Run commands from Exec mode
  end          End current mode and change to EXEC mode
  exit         End current mode and down to previous mode
  help         Description of the interactive help system
  revert       Revert changes
  service      Service Commands
  show         Show running system information
  write        Write running configuration to memory or terminal

nx9500-6C8809(config-url-list-URLlist1)#

nx9500-6C8809(config-url-list-URLlist1)#url http://www.example_company.com depth
10

nx9500-6C8809(config-url-list-test)#show context
url-list test
 url http://www.example_company.com depth 10
nx9500-6C8809(config-url-list-URLlist1)#
```

### 4.1.100.2 url-list-config-mode commands

*url-list*

The following table summarizes URL list configuration mode commands:

**Table 4.58** *URL-Filter-Config-Mode Commands*

| Command | Description | Reference |
|---|---|---|
| *description* | Creates a blacklist rule defining a list of banned Web sites and URLs | *page 4-568* |
| *url* | Adds URL entries to this URL list | *page 4-569* |
| *no* | Removes this URL list's settings | *page 4-570* |

### 4.1.100.2.1 description

*url-list-config-mode commands*

Configures a description for this URL list. The description should be unique and enable you to identify the type of URLs listed in the URL list.

**Supported in the following platforms:**

- Access Points — AP6522, AP6532, AP7131, AP7502, AP7522, AP7532, AP7562, AP8132
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
description <LINE>
```

**Parameters**

- `description <LINE>`

| | |
|---|---|
| description <LINE> | Provide a unique description for this URL list (should not exceed 500 characters in length) |

**Example**

```
nx9500-6C8809(config-url-list-test)#description "This URL list contains social
media URLs"

nx9500-6C8809(config-url-list-test)#show context
url-list test
 description "This URL list contains social media URLs"
nx9500-6C8809(config-url-list-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes this URL list's description |

### 4.1.100.2.2 url

*url-list-config-mode commands*

Adds URL entries to this URL list

**Supported in the following platforms:**

- Access Points — AP6522, AP6532, AP7131, AP7502, AP7522, AP7532, AP7562, AP8132
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
url <WORD> {depth <1-10>}
```

**Parameters**

- `url <WORD> {depth <1-10>}`

| | |
|---|---|
| url <WORD> {depth <1-10>} | Adds a URL entry<br>• <WORD> – Specify the URL to add.<br>• depth – Optional. Sets number of levels to be cached. Since Web sites have different parameters to uniquely identify specific content, the same content may be stored on multiple origin servers. Smart caching uses subsets of these parameters to recognize that the content is the same and serves it from cache.<br>• <1-10> – Specify the depth from 1 - 10. |

**Example**

```
nx9500-6C8809(config-url-list-test)#url http://www.facebook.com

nx9500-6C8809(config-url-list-test)#show context
url-list test
 description "This URL list contains social communication URLS"
 url https://www.facebook.com depth 5
nx9500-6C8809(config-url-list-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes a URL entry from this URL list |

### 4.1.100.2.3 no

*url-list-config-mode commands*

Removes this URL list's settings

**Supported in the following platforms:**

- Access Points — AP6522, AP6532, AP7131, AP7502, AP7522, AP7532, AP7562, AP8132
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
no [description|url]

no description

no url <WORD>
```

**Parameters**

- `no <PARAMETERS>`

| | |
|---|---|
| no <PARAMETERS> | Removes this URL's settings based on the parameters passed |

**Example**

The following example displays the URL list 'test' settings before the 'no' command is executed:

```
nx9500-6C8809(config-url-list-test)#show context
url-list test
 description "This URL list contains social communication URLS"
 url https://www.facebook.com depth 5
nx9500-6C8809(config-url-list-test)#

nx9500-6C8809(config-url-list-test)#no url www.facebook.com
```

The following example displays the URL list 'test' settings after the 'no' command is executed:

```
nx9500-6C8809(config-url-list-test)#show context
url-list test
 description "This URL list contains social communication URLS"
nx9500-6C8809(config-url-list-test)#
```

## 4.1.101 vx9000

*Global Configuration Commands*

Configures a *Virtual WLAN Controller* (V-WLC) in a *virtual machine* (VM) environment. V-WLC can be deployed on a shared, third-party server hardware, thereby reducing overhead costs of procuring and maintaining dedicated appliances. The external, third-party hardware needs to have installed hypervisors, such as VmWare, Xen, VirtualBox, KVM, Amazon EC2 or Hyper-V, enabling it to communicate with V-WLC software.

The V-WLC controls and manages access points and other controllers (at NOC or as a site-controller) in the network. The traffic between the access points and the V-WLC is over the layer-3 MINT protocol.

V-WLC is a licensed feature, and the WiNG software provides the following two new licenses:

- VX – When installed, this license activates VM controller instance, and enables the V-WLC to trigger adoption process allowing access points to adopt to the V-WLC. The adoption capacity of the V-WLC is determined by the number of licenses installed on it.
- VX-DEMO – This is a 60 day trial license. This license also activates VM controller instance, and enables the V-WLC to adopt access points. But, the access point adoption capacity is limited to 16. Having installed this license on a device, the only other license that you can install on it is the VX license. All existing installed licenses will continue to work as before. Since this license has a limited validity period, ensure that the system clock on the license generating tool and the device are in sync. preferably through NTP.

To install the VX or VX-DEMO license on an existing V-WLC instance, use the license command. For more information, see the examples provided in this section.

**Supported in the following platforms:**

- Service Platforms — NX9500, NX9510, NX9600

**Syntax**

```
vx9000 <MAC>
```

**Parameters**

- `vx9000 <MAC>`

| | |
|---|---|
| vx <MAC> | Configures a V-WLC and enters its configuration mode<br>The V-WLC configuration is the same as that of a normal controller. |

**Example**

```
nx9500-6C8809(config)#vx9000 11-22-33-44-55-66
nx9500-6C8809(config-device-11-22-33-44-55-66)#?
Device Mode commands:
  adopter-auto-provisioning-policy-lookup  Use centralized auto-provisioning
                                           policy when adopted by another
                                           controller
  adoption                                 Adoption configuration

  adoption-site                            Set system's adoption site
  adoption-mode                            Configure the adoption mode for the
                                           access-points in this RF-Domain
  alias                                    Alias
  application-policy                       Application Poicy configuration
  area                                     Set name of area where the system
                                           is located
  arp                                      Address Resolution Protocol (ARP)
  auto-learn                               Auto learning
```

```
autogen-uniqueid                Autogenerate a unique id
autoinstall                     Autoinstall settings
bluetooth-detection             Detect Bluetooth devices using the
                                Bluetooth USB module - there will
                                be interference on 2.4 Ghz radio in
                                wlan mode
bridge                          Ethernet bridge
captive-portal                  Captive portal
cdp                             Cisco Discovery Protocol
channel-list                    Configure channel list to be
                                advertised to wireless clients
cluster                         Cluster configuration
configuration-persistence       Enable persistence of configuration
                                across reloads (startup configfile)
contact                         Configure the contact
controller                      WLAN controller configuration
country-code                    Configure the country of operation
critical-resource               Critical Resource
crypto                          Encryption related commands
database                        Database command
device-upgrade                  Device firmware upgrade
dot1x                           802.1X
dpi                             Enable Deep-Packet-Inspection
                                (Application Assurance)
dscp-mapping                    Configure IP DSCP to 802.1p
                                priority mapping for untagged
                                frames
email-notification              Email notification configuration
enforce-version                 Check the firmware versions of
                                devices before interoperating
environmental-sensor            Environmental Sensors Configuration
events                          System event messages
export                          Export a file
file-sync                       File sync between controller and
                                adoptees
floor                           Set the floor within a area where
                                the system is located
geo-coordinates                 Configure geo coordinates for this
                                device
gre                             GRE protocol
hostname                        Set system's network name
http-analyze                    Specify HTTP-Analysis configuration
interface                       Select an interface to configure
ip                              Internet Protocol (IP)
ipv6                            Internet Protocol version 6 (IPv6)
l2tpv3                          L2tpv3 protocol
l3e-lite-table                  L3e lite Table
layout-coordinates              Configure layout coordinates for
                                this device
led                             Turn LEDs on/off on the device
led-timeout                     Configure the time for the led to
                                turn off after the last radio state
                                change
legacy-auto-downgrade           Enable device firmware to auto
                                downgrade when other legacy devices
                                are detected
legacy-auto-update              Auto upgrade of legacy devices
license                         License management command
lldp                            Link Layer Discovery Protocol
load-balancing                  Configure load balancing parameter
location                        Configure the location
logging                         Modify message logging facilities
mac-address-table               MAC Address Table
mac-auth                        802.1X
mac-name                        Configure MAC address to name
                                mappings
management-server               Configure management server address
memory-profile                  Memory profile to be used on the
```

```
                                         device
meshpoint-device                         Configure meshpoint device
                                         parameters
meshpoint-monitor-interval               Configure meshpoint monitoring
                                         interval
min-misconfiguration-recovery-time       Check controller connectivity after
                                         configuration is received
mint                                     MiNT protocol
mirror                                   Mirroring
misconfiguration-recovery-time           Check controller connectivity after
                                         configuration is received
mpact-server                             MPACT server configuration
neighbor-inactivity-timeout              Configure neighbor inactivity
                                         timeout
neighbor-info-interval                   Configure neighbor information
                                         exchange interval
no                                       Negate a command or set its
                                         defaults
noc                                      Configure the noc related setting
nsight                                   NSight
ntp                                      Ntp server WORD
offline-duration                         Set duration for which a device
                                         remains unadopted before it
                                         generates offline event
override                                 Override a command
override-wlan                            Configure RF Domain level overrides
                                         for wlan
power-config                             Configure power mode
preferred-controller-group               Controller group this system will
                                         prefer for adoption
preferred-tunnel-controller              Tunnel Controller Name this system
                                         will prefer for tunneling extended
                                         vlan traffic
radius                                   Configure device-level radius
                                         authentication parameters
raid                                     RAID
remove-override                          Remove configuration item override
                                         from the device (so profile value
                                         takes effect)
rf-domain-manager                        RF Domain Manager
router                                   Dynamic routing
rsa-key                                  Assign a RSA key to a service
sensor-server                            AirDefense sensor server
                                         configuration
slot                                     PCI expansion Slot
spanning-tree                            Spanning tree
timezone                                 Configure the timezone
traffic-class-mapping                    Configure IPv6 traffic class to
                                         802.1p priority mapping for
                                         untagged frames
trustpoint                               Assign a trustpoint to a service
tunnel-controller                        Tunnel Controller group this
                                         controller belongs to
use                                      Set setting to use
vrrp                                     VRRP configuration
vrrp-state-check                         Publish interface via OSPF/BGP only
                                         if the interface VRRP state is not
                                         BACKUP
wep-shared-key-auth                      Enable support for 802.11 WEP
                                         shared key authentication

clrscr                                   Clears the display screen
commit                                   Commit all changes made in this
                                         session
do                                       Run commands from Exec mode
end                                      End current mode and change to EXEC
                                         mode
exit                                     End current mode and down to
```

```
                                                previous mode
  help                                          Description of the interactive help
                                                system
  revert                                        Revert changes
  service                                       Service Commands
  show                                          Show running system information
  write                                         Write running configuration to
                                                memory or terminal

nx9500-6C8809(config-device-11-22-33-44-55-66)#
vx-0099CC(config-device-00-0C-29-00-99-CC)~*#license ?
  WORD  Feature name (AP/AAP/ADSEC/HTANLT/VX) for
        which license is to be added

vx-0099CC(config-device-00-0C-29-00-99-CC)~*#license vx 80ee9649eddc94b48b5a35d7
eaf8e73b376a51649291714d04c84769b0fc4b3766816878d2739c24
vx-0099CC(config-device-00-0C-29-00-99-CC)~*#com wr
Jan 16 13:48:11 2014: vx-0099CC : %SYSTEM-6-CONFIG_COMMIT: Configuration commit by
user 'root' (mapsh) from 'Console'
Jan 16 13:48:11 2014: vx-0099CC : %SYSTEM-6-CONFIG_REVISION: Configuration
revision updated to 9 from 8
Jan 16 13:48:12 2014: vx-0099CC : %LICMGR-6-LIC_INSTALLED: VX license installed
[OK]
vx-0099CC(config-device-00-0C-29-00-99-CC)~*#Jan 16 13:48:12 2014: vx-0099CC :
%SYSTEM-6-CONFIG_REVISION: Configuration revision updated to 10 from 9

vx-0099CC(config-device-00-0C-29-00-99-CC)~*#
vx-0099CC(config-device-00-0C-29-00-99-CC)~*#
vx-0099CC(config-device-00-0C-29-00-99-CC)~*#sh licenses
Serial Number : 000C290099CCC0A80001

WARNING: Recommended minimum system resource requirements not met for the current
license pack or cluster configs. Please check user guide and reconfigure the system

Device Licenses:
  AP-LICENSE
    String     :
    Value      : 10240
  AAP-LICENSE
    String     :
    Value      : 10240
  ADVANCED-SECURITY
    String     : DEFAULT-ADV-SEC-LICENSE
  VX-LICENSE
    String     :
80ee9649eddc94b48b5a35d7eaf8e73b376a51649291714d04c84769b0fc4b3766816878d2739c24

Cluster Licenses:
  AP-LICENSE
    Value      : 10240
    Used       : 0
  AAP-LICENSE
    Value      : 10240
    Used       : 0

Cluster MAX AP Capacity:
  Value        : 10240
  Used         : 0

Active Members:
-------------------------------------------------------------------------------
-------------------
MEMBER           SERIAL            LIC TYPE  VALUE    BORROWED  TOTAL    NO.APS
NO.AAPS
-------------------------------------------------------------------------------
-------------------
00-0C-29-00-99-CC  000C290099CCC0A80001 AP     10240    0      10240    0     0
```

```
 00-0C-29-00-99-CC  000C290099CCC0A80001 AAP      10240    0       10240    -
-
-------------------------------------------------------------------------------
-------------------
vx-0099CC(config-device-00-0C-29-00-99-CC)~*#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes a VX9000 wireless controller |

# 5 COMMON COMMANDS

This chapter describes the CLI commands used in the USER EXEC, PRIV EXEC, and GLOBAL CONFIG modes.

The PRIV EXEC command set contains commands available within the USER EXEC mode. Some commands can be entered in either mode. Commands entered in either the USER EXEC or PRIV EXEC mode are referred to as EXEC mode commands. If a user or privilege is not specified, the referenced command can be entered in either mode.

# 5.1 Common Commands

*COMMON COMMANDS*

The following table summarizes commands common to the User Exec, Priv Exec, and Global Config modes:

**Table 5.1** *Commands Common to Controller CLI Modes*

| Command | Description | Reference |
|---|---|---|
| *clrscr* | Clears the display screen | *page 5-3* |
| *commit* | Commits (saves) changes made in the current session | *page 5-4* |
| *exit* | Ends and exits the current mode and moves to the PRIV EXEC mode | *page 5-5* |
| *help* | Displays the interactive help system | *page 5-6* |
| *no* | Negates a command or reverts values to their default settings | *page 5-9* |
| *revert* | Reverts changes to their last saved configuration | *page 5-12* |
| *service* | Invokes service commands to troubleshoot or debug `(config-if)` instance configurations | *page 5-13* |
| *show* | Displays running system information | *page 5-58* |
| *write* | Writes the system's running configuration to memory or to the terminal | *page 5-60* |

**NOTE:** The input parameter <HOSTNAME> cannot include an underscore character. In other words, a device's hostname cannot contain an underscore.

## 5.1.1 clrscr

*Common Commands*

Clears the screen and refreshes the prompt, irrespective of the mode

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
clrscr
```

**Parameters**

None

**Example**

The terminal window or screen before the clrscr command is executed:

```
rfs4000-229D58#device-upgrade ?
  DEVICE-NAME     Name/MAC address of device
  all             Upgrade all devices
  ap650           Upgrade AP650 Device
  ap6511          Upgrade AP6511 Device
  ap6521          Upgrade AP6521 Device
  ap6522          Upgrade AP6522 Device
  ap6532          Upgrade AP6532 Device
  ap6562          Upgrade AP6562 Device
  ap71xx          Upgrade AP7161 Device
  ap7502          Upgrade AP7502 Device
  ap7522          Upgrade AP7522 Device
  ap7532          Upgrade AP7532 Device
  ap7562          Upgrade AP7562 Device
  ap81xx          Upgrade AP81XX Device
  ap82xx          Upgrade AP82XX Device
  ap8432          Upgrade AP8432 Device
  ap8533          Upgrade AP8533 Device
  cancel-upgrade  Cancel upgrading the device
  load-image      Load the device images to controller for device-upgrades
  rf-domain       Upgrade all devices belonging to an RF Domain
  rfs4000         Upgrade RFS4000 Device

rfs4000-229D58#
```

The terminal window or screen after the clrscr command is executed:

```
rfs4000-229D58#
```

## 5.1.2 commit

*Common Commands*

Commits changes made in the active session. Use the commit command to save and invoke settings entered during the current transaction.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
commit {write}{memory}
```

**Parameters**

- `commit {write}{memory}`

| | |
|---|---|
| write | Optional. Commits changes made in the current session |
| memory | Optional. Writes to memory. This option ensures current changes persist across reboots. |

**Example**

```
nx9500-6C8809#commit write memory
[OK]
nx9500-6C8809#
```

## 5.1.3 exit

*Common Commands*

The exit command works differently in the User Exec, Priv Exec, and Global Config modes. In the Global Config mode, it ends the current mode and moves to the previous mode, which is Priv Exec mode. The prompt changes from `(config)#` to `#`. When used in the Priv Exec and User Exec modes, the exit command ends the current session, and connection to the terminal device is terminated. If the current session has changes that have not been committed, the system prompts you to either do a commit or a revert before terminating the session.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
exit
```

**Parameters**

None

**Example**

```
nx9500-6C8809(config)#exit
nx9500-6C8809#
```

## 5.1.4 help

*Common Commands*

Describes the interactive help system

Use this command to access the advanced help feature. Use “?” anytime at the command prompt to access the help topic.

Two kinds of help are provided:

- Full help is available when ready to enter a command argument
- Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (for example 'show ve?').

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
help {search}
help {search <WORD>} {detailed|only-show|skip-no|skip-show}
```

**Parameters**

- `help {search <WORD>} {detailed|only-show|skip-no|skip-show}`

| | |
|---|---|
| search <WORD> | Optional. Searches for CLI commands related to a specified target term<br>• <WORD> – Specify a target term (for example, a feature or a configuration parameter). After specifying the term, select one of the following options: detailed, only-show, skip-no, or skip-show. The system displays information based on the option selected. |
| detailed | Optional. Searches and displays help strings in addition to mode and commands |
| only-show | Optional. Displays only “show” commands. Does not display configuration commands |
| skip-no | Optional. Displays only configuration commands. Does not display “no” commands |
| skip-show | Optional. Displays only configuration commands. Does not display “show” commands |

**Example**

```
nx9500-6C8809>help search crypto detailed
found more than 64 references, showing the first 64

Context : Command
Command : clear crypto ike sa (A.B.C.D|all)(|on DEVICE-NAME)
           \ Clear
            \ Encryption Module
             \ IKE SA
              \ Flush IKE SAs
               \ Flush IKE SAs for a given peer
                \ Flush all IKE SA
                 \ On AP/Controller
                  \ AP/Controller name

        : clear crypto ipsec sa(|on DEVICE-NAME)
                  \ Clear
                  \ Encryption Module
                  \ IPSec database
                  \ Flush IPSec SAs
                  \ On AP/Controller
                  \ AP/Controller name

        : crypto key export rsa WORD URL (passphrase WORD|) (background|) ...
                  \ Encryption related commands
--More--
nx9500-6C8809>



nx9500-6C8809>help search crypto only-show

Context : Command
Command : show crypto cmp request status(|on DEVICE-NAME)
        : show crypto ike sa (version 1|version 2|)(peer A.B.C.D|) (detail...
        : show crypto ipsec sa (peer A.B.C.D|) (detail|)  (|on DEVICE-NAME...
        : show crypto key rsa (|public-key-detail) (|on DEVICE-NAME)
        : show crypto pki trustpoints (WORD|all|)(|on DEVICE-NAME)
nx9500-6C8809>

nx9500-6C8809>help search service skip-show
found more than 64 references, showing the first 64

Context : Command
Command : service block-adopter-config-update
        : service clear adoption history(|on DEVICE-NAME)
        : service clear captive-portal-page-upload history (|(on DOMAIN-NA...
        : service clear command-history(|on DEVICE-NAME)
        : service clear device-upgrade history (|on DOMAIN-NAME)
        : service clear noc statistics
        : service clear reboot-history(|on DEVICE-NAME)
        : service clear unsanctioned aps (|on DEVICE-OR-DOMAIN-NAME)
        : service clear upgrade-history(|on DEVICE-NAME)
        : service clear web-filter cache(|on DEVICE-NAME)
        : service clear wireless ap statistics (|(AA-BB-CC-DD-EE-FF)) (|on...
        : service clear wireless client statistics (|AA-BB-CC-DD-EE-FF) (|...
        : service clear wireless controller-mobility-database
        : service clear wireless dns-cache(|on DEVICE-OR-DOMAIN-NAME)
        : service clear wireless radio statistics (|(DEVICE-NAME (|<1-3>))...
        : service clear wireless wlan statistics (|WLAN) (|on DEVICE-OR-DO...
        : service clear xpath requests (|<1-100000>)
        : service show block-adopter-config-update
        : service show captive-portal servers(|on DEVICE-NAME)
        : service show captive-portal user-cache(|on DEVICE-NAME)
        : service show cli
  --More--
nx9500-6C8809>
```

```
nx9500-6C8809>help search mint only-show
Found 25 references for "mint"

Context : Command
Command : show debugging mint (|on DEVICE-OR-DOMAIN-NAME)
        : show mint config(|on DEVICE-NAME)
        : show mint dis (|details)(|on DEVICE-NAME)
        : show mint id(|on DEVICE-NAME)
        : show mint info(|on DEVICE-NAME)
        : show mint known-adopters(|on DEVICE-NAME)
        : show mint links (|details)(|on DEVICE-NAME)
        : show mint lsp
        : show mint lsp-db (|details AA.BB.CC.DD)(|on DEVICE-NAME)
        : show mint mlcp history(|on DEVICE-NAME)
        : show mint mlcp(|on DEVICE-NAME)
        : show mint neighbors (|details)(|on DEVICE-NAME)
        : show mint route(|on DEVICE-NAME)
        : show mint stats(|on DEVICE-NAME)
        : show mint tunnel-controller (|details)(|on DEVICE-NAME)
        : show mint tunneled-vlans(|on DEVICE-NAME)
        : show wireless mint client (|on DEVICE-OR-DOMAIN-NAME)
        : show wireless mint client portal-candidates(|(DEVICE-NAME (|<1-3...
        : show wireless mint client statistics (|on DEVICE-OR-DOMAIN-NAME)...
        : show wireless mint client statistics rf (|on DEVICE-OR-DOMAIN-NA...
        : show wireless mint detail (|(DEVICE-NAME (|<1-3>))) (|(filter {|...
        : show wireless mint links (|on DEVICE-OR-DOMAIN-NAME)
        : show wireless mint portal (|on DEVICE-OR-DOMAIN-NAME)
        : show wireless mint portal statistics (|on DEVICE-OR-DOMAIN-NAME)...
        : show wireless mint portal statistics rf (|on DEVICE-OR-DOMAIN-NA...
nx9500-6C8809>
```

## 5.1.5 no

*Common Commands*

Negates a command or sets its default. Though the no command is common to the User Exec, Priv Exec, and Global Config modes, it negates a different set of commands in each mode.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
no <PARAMETERS>
```

**Parameters**

- no <PARAMATERS>

| | |
|---|---|
| no <PARAMETERS> | The no command is common across all configuration modes and sub modes. It resets or reverts settings based on the mode in which executed. For example, when executed in the AAA policy configuration mode, it allows you to reset or revert a specific AAA policy settings. Similarly, when executed in the global configuration mode, it only resets or reverts settings configured in the global configuration mode. |

**Usage Guidelines**

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

**Example**

Global Config mode: No command options

```
rfs6000-81742D(config)##no ?
  aaa-policy                    Delete a aaa policy
  aaa-tacacs-policy             Delete a aaa tacacs policy
  alias                         Alias
  ap621                         Delete an AP621 access point
  ap622                         Delete an AP622 access point
  ap650                         Delete an AP650 access point
  ap6511                        Delete an AP6511 access point
  ap6521                        Delete an AP6521 access point
  ap6522                        Delete an AP6522 access point
  ap6532                        Delete an AP6532 access point
  ap6562                        Delete an AP6562 access point
  ap71xx                        Delete an AP71XX access point
  ap7502                        Delete an AP7502 access point
  ap7522                        Delete an AP7522 access point
  ap7532                        Delete an AP7532 access point
  ap7562                        Delete an AP7562 access point
  ap81xx                        Delete an AP81XX access point
  ap82xx                        Delete an AP82XX access point
  ap8432                        Delete an AP8432 access point
  ap8533                        Delete an AP8533 access point
  application                   Delete an application
  application-group             Delete an application-group
  application-policy            Delete an application policy
  association-acl-policy        Delete an association-acl policy
  auto-provisioning-policy      Delete an auto-provisioning policy
  bgp                           BGP Configuration
  bonjour-gw-discovery-policy   Disable Bonjour Gateway discovery policy
```

```
bonjour-gw-forwarding-policy        Disable Bonjour Gateway Forwarding
                                    policy
bonjour-gw-query-forwarding-policy  Disable Bonjour Gateway Query Forwarding
                                    policy
captive-portal                      Delete a captive portal
client-identity                     Client identity (DHCP Device
                                    Fingerprinting)
client-identity-group               Client identity group (DHCP Fingerprint
                                    Database)
crypto-cmp-policy                   CMP policy
customize                           Restore the custom cli commands to
                                    default
device                              Delete multiple devices
device-categorization               Delete  device categorization object
dhcp-server-policy                  DHCP server policy
dhcpv6-server-policy                DHCPv6 server related configuration
dns-whitelist                       Delete a whitelist object
event-system-policy                 Delete a event system policy
ex3500                              Ex3500 device
ex3500-management-policy            Delete a ex3500 management policy
ex3500-qos-class-map-policy         Delete a ex3500 qos class-map policy
ex3500-qos-policy-map               Delete a ex3500 qos policy-map
ex3524                              Delete an EX3524 wireless controller
ex3548                              Delete an EX3548 wireless controller
firewall-policy                     Configure firewall policy
global-association-list             Delete a global association list
igmp-snoop-policy                   Remove device onboard igmp snoop policy
inline-password-encryption          Disable storing encryption key in the
                                    startup configuration file
ip                                  Internet Protocol (IP)
ipv6                                Internet Protocol version 6 (IPv6)
ipv6-router-advertisement-policy    IPv6 Router Advertisement related
                                    configuration
l2tpv3                              Negate a command or set its defaults
mac                                 MAC configuration
management-policy                   Delete a management policy
meshpoint                           Delete a meshpoint object
meshpoint-qos-policy                Delete a mesh point QoS configuration
                                    policy
nac-list                            Delete an network access control list
nsight-policy                       Delete a nsight policy
passpoint-policy                    Delete a passpoint configuration policy
password-encryption                 Disable password encryption in
                                    configuration
profile                             Delete a profile and all its associated
                                    configuration
radio-qos-policy                    Delete a radio QoS configuration policy
radius-group                        Local radius server group configuration
radius-server-policy                Remove device onboard radius policy
radius-user-pool-policy             Configure Radius User Pool
rf-domain                           Delete one or more RF-domains and all
                                    their associated configurations
rfs4000                             Delete an RFS4000 wireless controller
rfs6000                             Delete an RFS6000 wireless controller
roaming-assist-policy               Delete a roaming-assist policy
role-policy                         Role based firewall policy
route-map                           Dynamic routing route map Configuration
routing-policy                      Policy Based Routing Configuratino
rtl-server-policy                   Delete a rtl server policy
schedule-policy                     Delete a schedule policy
sensor-policy                       Delete a sensor policy
smart-rf-policy                     Delete a smart-rf-policy
t5                                  Delete an T5 DSL switch
url-filter                          Delete a url filter
url-list                            Delete a URL list
web-filter-policy                   Delete a web filter policy
wips-policy                         Delete a wips policy
wlan                                Delete a wlan object
```

```
  wlan-qos-policy                    Delete a wireless lan QoS configuration
                                     policy

  service                            Service Commands

rfs6000-81742D(config)#
```

Priv Exec mode: No command options

```
rfs6000-81742D#no ?
  adoption         Reset adoption state of the device (& all devices adopted to
                   it)
  captive-portal   Captive portal commands
  cpe              T5 CPE configuration
  crypto           Encryption related commands
  debug            Debugging functions
  logging          Modify message logging facilities
  page             Toggle paging
  service          Service Commands
  terminal         Set terminal line parameters
  upgrade          Remove a patch
  wireless         Wireless Configuration/Statistics commands

rfs6000-81742D#
```

user Exec mode: No command options

```
rfs6000-81742D>no ?
  adoption         Reset adoption state of the device (& all devices adopted to
                   it)
  captive-portal   Captive portal commands
  crypto           Encryption related commands
  debug            Debugging functions
  logging          Modify message logging facilities
  page             Toggle paging
  service          Service Commands
  terminal         Set terminal line parameters
  wireless         Wireless Configuration/Statistics commands

rfs6000-81742D>
```

## 5.1.6 revert

*Common Commands*

Reverts changes made, in the current session, to their last saved configuration

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
revert
```

**Parameters**

None

**Example**

```
nx9500-6C8809>revert
nx9500-6C8809>
```

## 5.1.7 service

*Common Commands*

Service commands are used to view and manage configurations. The service commands and their corresponding parameters vary from mode to mode. The User Exec mode and Priv Exec mode commands provide same functionalities with a few minor changes. The Global Config service command sets the size of history files. It also enables viewing the current mode's CLI tree.

This section consists of the following sub-sections:

- Syntax *(User Exec Mode)*
- Syntax *(Privilege Exec Mode)*
- Syntax *(Privilege Exec Mode: NX9500 and NX9510)*

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax (User Exec Mode)**

```
service [block-adopter-config-update|clear|cli-tables-skin|cluster|database|
delete-offline-aps|force-send-config|force-update-vm-stats|guest-registration|
load-balancing|load-ssh-authorized-keys|locator|nsight|radio|radius|
request-full-config-from-adopter|set|show|smart-rf|ssm|snmp|syslog|wireless]

service [block-adopter-config-update|request-full-config-from-adopter]

service clear [adoption|captive-portal-page-upload|command-history|device-
upgrade|diag|dpi|file-sync|noc|reboot-history|unsanctioned|upgrade-history|
virtual-machine-history|web-filter|wireless|xpath]

service clear adoption history {on <DEVICE-NAME>}
service clear device-upgrade history {on <DOMAIN-NAME>}
service clear dpi [all|app|app-category] stats {on <DEVICE-OR-DOMAIN-NAME>}
service clear diag pkts
service clear file-sync history {on <DOMAIN-NAME>}
service clear captive-portal-page-upload history {on <DOMAIN-NAME>}

service clear [command-history|reboot-history|upgrade-history|virtual-machine-
history] {on <DEVICE-NAME>}
service clear noc statistics
service clear unsanctioned aps {on <DEVICE-OR-DOMAIN-NAME>}
service clear web-filter cache {on <DEVICE-NAME>}

service clear wireless [ap|client|controller-mobility-database|dns-
cache|radio|wlan]
service clear wireless controller-mobility-database
service clear wireless [ap|client] statistics {<MAC>} {(on <DEVICE-OR-DOMAIN-
NAME>)}
service clear wireless dns-cache on {(on <DEVICE-OR-DOMAIN-NAME)}
service clear wireless radio statistics {<MAC/HOSTNAME>} {<1-3>} {(on <DEVICE-OR-
DOMAIN-NAME>)}
service clear wireless wlan statistics {<WLAN-NAME>} {(on <DEVICE-OR-DOMAIN-NAME)}
service clear xpath requests {<1-100000>}

service cli-tables-skin [ansi|hashes|minimal|none|percent|stars|thick|thin|utf-8]
{grid}
```

```
service cluster force [active|configured-state|standby]

service database [authentication|start-shell]

service database authentication [create-user|delete-user]
service database authentication create-user username <USER-NAME> password
<PASSWORD>
service database authentication delete-user username <USER-NAME>

Note, the other service > database command options are documented latter in this
section under the (Privilege Exec Mode) section.

service database start-shell

service delete-offline-aps [all|offline-for]
service delete-offline-aps offline-for days <0-999> {time <TIME>}

service force-send-config {on <DEVICE-OR-DOMAIN-NAME>}

service force-update-vm-stats {on <DEVICE-NAME>}

service guest-registration [backup|delete|export|import]

service guest-registration backup [delete|restore]

service guest-registration delete [all|email <EMAIL-ADD>|group <RAD-GROUP-NAME>|
mac <MAC>|mobile <MOBILE-NUMBER>|name <CLIENT-FULL-NAME>|non-social|offline-for
days <1-999>|otp-incomplete-for days <1-999>|social [facebook|google]|
wlan <WLAN-NAME>]

service guest-registration export format [csv|json] <DEST-URL> {(rfdomain <DOMAIN-
NAME>|time [1-Day|1-Month|1-Week|2-Hours|30-Mins|5-Hours|all]|wlan <WLAN-NAME>)}

service guest-registration import format <JSON> <SOURCE-URL>

service load-balancing clear-client-capability [<MAC>|all] {on <DEVICE-NAME>}

service load-ssh-authorized-keys <PUBLIC-KEY> {on <DEVICE-NAME>}

service locator {<1-60>} {(on <DEVICE-NAME>)}

service nsight clear-offline [all|offline-for days <0-999> {time <TIME>}]

service radio <1-3> [adaptivity|channel-switch|dfs]

service radio <1-3> adaptivity

service radio <1-3> channel-switch <36-196> [160|20|40|80]

service radio <1-3> dfs simulator-radar [extension|primary]

service radius test [<IP>|<HOSTNAME>] [<WORD>|port]

service radius test [<IP>|<HOSTNAME>] <WORD> <USERNAME> <PASSWORD> {wlan <WLAN-
NAME> ssid <SSID>} {(on <DEVICE-NAME>)}

service radius test [<IP>|<HOSTNAME>] port <1024-65535> <WORD> <USERNAME>
<PASSWORD> {wlan <WLAN-NAME> ssid <SSID>} {(on <DEVICE-NAME>)}

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

service show [block-adopter-config-update|captive-portal|cli|client-identity-
defaults|command-history|configuration-revision|crash-info|dhcp-lease|diag|fast-
switching|fib|fib6|guest-registration|info|ip-access-list|mac-vendor|mem|mint|
noc|nsight|pm|process|reboot-history|rf-domain-manager|sites|snmp|
ssh-authorized-keys|startup-log|sysinfo|top|upgrade-history|virtual-machine-
history|watch-dog|wireless|xpath-history]
```

```
service show block-adopter-config-update

service show captive-portal [log-internal|servers|user-cache]

service show captive-portal log-internal
service show captive-portal [servers|user-cache] {on <DEVICE-NAME>}

service show [cli|client-identity-defaults|configuration-revision|mac-vendor
<OUI/MAC>|noc diag|snmp session|xpath-history]

service show [command-history|crash-info|info|mem|process|reboot-history|startup-
log|ssh-authorized-keys|sysinfo|top|upgrade-history|watchdog] {on <DEVICE-NAME>}

service show ip-access-list wlan <WLAN-NAME> status {detail} {on <DEVICE-OR-
DOMAIN-NAME>}

service show dhcp-lease {<INTERFACE-NAME>|pppoe1|vlan <1-4094>|wwan1} (on <DEVICE-
NAME>)}

service show diag [fds|led-status|pkts|psu|stats]
service show diag [fds|pkts]
service show diag [led-status|psu|stats] {on <DEVICE-NAME>}

service show fast-switching {on <DEVICE-NAME>}

service show [fib|fib6] {table-id <0-255>}

service show guest-registration [export-status|import-status|restore-status]

service show mint [adopted-devices {on <DEVICE-NAME>}|ports]

service show pm {history} {(on <DEVICE-NAME>)}

service show rf-domain-manager [diag|info] {<MAC/HOSTNAME>} {(on <DEVICE-OR-
DOMAIN-NAME>)}

service show sites

service show virtual-machine-history {on <DEVICE-NAME>}

service show wireless [aaa-stats|adaptivity-status|client|config-internal|
credential-cache|dns-cache|log-internal|meshpoint|neighbors|radar-status|
radio-internal|reference|stats-client|vlan-usage]

service show wireless [aaa-stats|adaptivity-status|credential-cache|dns-cache|
radar-status|vlan-usage] {on <DEVICE-NAME>}

service show wireless [config-internal|log-internal|neighbors]

service show wireless [client|meshpoint neighbor] proc [info|stats] {<MAC>}
{{on <DEVICE-OR-DOMAIN-NAME>)}

service show wireless radio-internal [radio1|radio2] <LINE>

service show wireless reference [channels|frame|handshake|mcs-rates|reason-codes|
status-codes]

service show wireless stats-client diag {<MAC/HOSTNAME>} {(on <DEVICE-OR-DOMAIN-
NAME>)}

service smart-rf [clear-config|clear-history|clear-interfering-aps|save-config]
service smart-rf clear-config {<MAC>|<DEVICE-NAME>|on <DOMAIN-NAME>}

service smart-rf [clear-history||clear-interfering-aps|save-config] {on <DOMAIN-
NAME>}

service snmp sysoid wing5
```

```
service ssm [dump-core-snapshot|trace]

service ssm trace pattern <WORD> {on <DEVICE-NAME>}

service syslog test {level [<0-7>|alerts|critical|debugging|emergencies|errors|
informational|notifications|warnings]} {(on <DEVICE-NAME>)}

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

service wireless client [beacon-request|quiet-element|trigger-bss-transition|
trigger-wnm]

service wireless client beacon-request <MAC> mode [active|passive|table] ssid
[<SSID>|any] channel-report [<CHANNEL-LIST>|none] {on <DEVICE-NAME>}
service wireless client quiet-element [start|stop]

service wireless client trigger-bss-transition mac <MAC> {timeout <0-65535>} {url
<URL>} {on <DEVICE-OR-DOMAIN-NAME>}

service wireless client trigger-wnm mac <MAC> type [deauth-imminent|subscription-
remediation] {uri <WORD>}

service wireless dump-core-snapshot

service wireless meshpoint zl <MESHPOINT-NAME> [on <DEVICE-NAME>] {<ARGS>|timeout
<1-65535>}

service wireless qos delete-tspec <MAC> tid <0-7>

service wireless trace pattern <WORD> {on <DEVICE-NAME>}

service wireless unsanctioned ap air-terminate <MAC> {on <DOMAIN-NAME>}

service wireless wips [clear-client-blacklist|clear-event-history|dump-managed-
config]

service wireless wips clear-client-blacklist [all|mac <MAC>]

service wireless wips clear-event-history {on <DEVICE-OR-DOMAIN-NAME>}
```

**Parameters (User Exec Mode)**

*service*

- `service [block-adopter-config-update|request-full-config-from-adopter]`

| | |
|---|---|
| block-adopter-config-update | Blocks the configuration updates sent from the NOC server |
| request-full-config-from-adopter | Configures a request for full configuration updates from the adopter device<br>In an *hierarchically managed* (HM) network devices are deployed in two levels. The first level consists of the *Network Operations Center* (NOC) controllers. The second level consists of the site controllers that can be grouped to form clusters. The NOC controllers adopt and manage the site controllers. Access points within the network are adopted and managed by the site controllers. The adopted devices (access points and site controllers) are referred to as the adoptee. The devices adopting the adoptee are the 'adopters'. |

- `service clear adoption history {on <DEVICE-NAME>}`

| | |
|---|---|
| clear adoption history | Clears adoption history on this device and its adopted access points |

| | |
|---|---|
| on <DEVICE-NAME> | Optional. Clears adoption history on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `service clear device-upgrade history` *`{on <DOMAIN-NAME>}`*

| | |
|---|---|
| clear device-upgrade history | Clears device upgrade history |
| on <DOMAIN-NAME> | Optional. Clears all firmware upgrade history in a specified RF Domain<br>• <DOMAIN-NAME> – Specify the RF Domain name. |

- `service clear diag pkts`

| | |
|---|---|
| clear diag pkts | Clears the looped packets queue logged by the dataplane. The dataplane logs up to 16 looped packets at a time in a separate queue, which has to be manually cleared to make space for new packet logging.<br>For more information on viewing logged looped packet information execute the *service > show > diag > pkts* command. |

- `service clear dpi [all|app|app-category] stats` *`{on <DEVICE-OR-DOMAIN-NAME>}`*

| | |
|---|---|
| clear dpi | Clears *Deep Packet Inspection* (DPI) statistics<br>When enabled, DPI allows application and/or application category recognition. The DPI statistics are maintained by the system for every hit registered by the DPI engine. |
| [all\|app\|app-category] stats | Use the following filter options to clear all or specific DPI statistics:<br>• all – Clears all DPI related (application and app-category) statistics<br>• app – Clears only application related statistics<br>• app-category – Clears only app-category related statistics |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Clears DPI statistics based on the parameters passed on a specified device or RF Domain<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the access point, controller, service platform, or RF Domain. |

- `service clear file-sync history` *`{on <DOMAIN-NAME>}`*

| | |
|---|---|
| clear file-sync history | Clears client-bridge certificate synchronization statistics<br>When an AP6522/AP6562 access point is configured as a client bridge, the EAP-TLS X.509 (PKCS#12) certificate is synchronized between the staging-controller and adoptee AP6522/AP6562 client-bridge access points. This command allows you to clear client-bridge certificate synchronization statistics. |
| on <DOMAIN-NAME> | Optional. Clears file synchronization history on all devices within a specified RF Domain<br>• <DOMAIN-NAME> – Specify the RF Domain name. |

- `service clear captive-portal-page-upload history` *`{on <DOMAIN-NAME>}`*

| | |
|---|---|
| clear captive-portal-page-upload history | Clears captive portal page upload history |
| on <DOMAIN-NAME> | Optional. Clears captive portal page upload history on a specified RF Domain<br>• <DOMAIN-NAME> – Specify the RF Domain name. |

- `service clear [command-history|reboot-history|upgrade-history|virtual-machine-history] {on <DEVICE-NAME>}`

| | |
|---|---|
| clear [command-history\|reboot-history\|upgrade-history] | Clears command history, reboot history, or device upgrade history |
| clear virtual-machine-history | Clears virtual-machine history on the logged device or a specified device<br>This command is applicable only on the NX9500 and NX9510 series service platforms. |
| on <DEVICE-NAME> | Optional. Clears history on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.<br>When executing the clear virtual-machine-history command, provide the name of the service platform running the VMs. |

- `service clear noc statistics`

| | |
|---|---|
| clear noc statistics | Clears *Network Operations Center* (NOC) applicable statistics counters |

- `service clear unsanctioned aps {on <DEVICE-OR-DOMAIN-NAME>}`

| | |
|---|---|
| clear unsanctioned aps | Clears the unsanctioned APs list |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Clears the unsanctioned APs list on a specified device or RF Domain<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |

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

| | |
|---|---|
| clear wireless [ap\|client] statistics | Clears wireless statistics counters based on the parameters passed<br>• ap statistics – Clears applicable AP statistics counters<br>• client statistics – Clears applicable wireless client statistics counters<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |
| <MAC><br>{on <DEVICE-OR-DOMAIN-NAME>} | The following keywords are common to the 'ap' and 'client' parameters:<br>• <MAC> – Optional. Clears statistics counters for a specified AP or client. Specify the AP/client MAC address.<br>• on <DEVICE-OR-DOMAIN-NAME> – Optional. Clears AP/client statistics counters on a specified device or RF Domain. Specify the name of the AP, wireless controller, service platform, or RF Domain. |

- `service clear wireless controller-mobility-database`

| | |
|---|---|
| clear wireless controller-mobility-database | Clears the controller assisted mobility database |

- `service clear web-filter cache {on <DEVICE-NAME>}`

| | |
|---|---|
| clear web-filter cache | Clears the cache used for Web filtering |

| | |
|---|---|
| on <DEVICE-NAME> | Optional. Clears the Web filtering cache on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

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

| | |
|---|---|
| clear wireless radio statistics | Clears applicable wireless radio statistics counters |
| <MAC/HOSTNAME> <1-3> | Optional. Specify the MAC address or hostname of the radio, or append the interface number to form the radio ID in the AA-BB-CC-DD-EE-FF:RX or HOSTNAME:RX format.<br>• <1-3> – Optional. Specify the radio interface index, if not specified as part of the radio ID. |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. This is a recursive parameter, which clears wireless radio statistics on a specified device or RF Domain. Specify the name of the device.<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |

• `service clear wireless wlan statistics {<WLAN-NAME>} {(on <DEVICE-OR-DOMAIN-NAME>)}`

| | |
|---|---|
| clear wireless wlan statistics | Clears WLAN statistics counters |
| <WLAN-NAME> | Optional. Clears statistics counters on a specified WLAN. Specify the WLAN name. |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. This is a recursive parameter, which clears WLAN statistics on a specified device or RF Domain. Specify the name of the device.<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |

• `service clear xpath requests {<1-100000>}`

| | |
|---|---|
| clear xpath | Clears XPATH related information |
| requests | Clears pending XPATH get requests |
| <1-100000> | Optional. Specifies the session number (cookie from show sessions)<br>• <1-100000> – Specify the session number from 1 - 100000.<br>**Note:** Omits clearing the current session's pending XPATH get requests. |

• `service cli-tables-skin [ansi|hashes|minimal|none|percent|stars|thick|thin|utf-8] {grid}`

| | |
|---|---|
| cli-tables-skin [ansi\|hashes\|minimal\| none\|percent\|stars\| thick\|thin\|uf-8] | Selects a formatting layout or skin for CLI tabular outputs<br>• ansi – Uses ANSI characters for borders<br>• hashes – Uses hashes (#) for borders<br>• minimal – Uses one horizontal line between title and data rows<br>• none – Displays space separated items with no decoration<br>• percent – Uses the percent sign (%) for borders<br>• stars – Uses asterisks (*) for borders<br>• thick – Uses thick lines for borders<br>Contd.. |

| | |
|---|---|
| | • thin – Uses thin lines for borders<br>• utf-8 – Uses UTF-8 characters for borders |
| grid | Optional. Uses a complete grid instead of just title lines |

- `service cluster force [active|configured-state|standby]`

| | |
|---|---|
| cluster | Enables cluster protocol management |
| force | Forces action commands on a cluster (active, configured-state, and standby) |
| active | Changes the cluster run status to active |
| configured-state | Restores a cluster to the configured state |
| standby | Changes the cluster run status to standby |

- `service database authentication create-user username <USER-NAME> password <PASSWORD>`

| | |
|---|---|
| database | Performs database related actions<br>This command is supported only on the NX95XX, NX9600, and VX9000 platforms. |
| authentication create-user username <USER-NAME> password <PASSWORD> | Creates users having access rights to the database. Execute this command on the database host. However, before creating users, on the database, generate the database keyfile. For more information on generating the keyfile, see *database*.<br>• username <USER-NAME> – Configures databse username<br>• password <PASSWORD> – Configures a password for the username specified above<br>In the database-policy ensure that authentication is enabled and username and password is configured. The database-client-policy also should have the same username and password configured. For more information on database-policy and database-client-policy, see *database-policy* and *database-client-policy*. |

- `database authentication delete-user username <USER-NAME>`

| | |
|---|---|
| database | Performs database related actions<br>This command is supported only on the NX95XX, NX9600, and VX9000 platforms. |
| database authentication delete-user username <USER-NAME> | Deletes the username requires to access rights the captive-portal/NSight database<br>• username <USER-NAME> – Deletes the username identified by the <USER-NAME> keyword<br>Once deleted, the database cannot be accessed using the specified combination of username and password. |

- `service database start-shell`

| | |
|---|---|
| database | Performs database related actions<br>This command is supported only on the NX95XX, NX9600, and VX9000 platforms. |
| start-shell | Starts the database shell |

- `service delete-offline-aps all`

| | |
|---|---|
| delete-offline-aps all | Deletes all off-line access points |

- `service delete-offline-aps offline-for days <0-999> {time <TIME>}`

| | |
|---|---|
| delete-offline-aps | Deletes off-line access points for a specified interval |

| | |
|---|---|
| day <0-999> | Deletes off-line access points for a specified number of days<br>• <0-999> – Specify the number of off-line days from 0 - 999. |
| time <TIME> | Optional. Deletes off-line access points for a specified time<br>• <TIME> – Specify the time in HH:MM:SS format. |

- `service force-send-config` *`{on <DEVICE-OR-DOMAIN-NAME>}`*

| | |
|---|---|
| force-send-config | Resends configuration to device(s) |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Resends configuration to a specified device or all devices in a specified RF Domain<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |

- `service force-update-vm-stats` *`{on <DEVICE-NAME>}`*

| | |
|---|---|
| force-update-vm-stats | Forcefully pushes VM statistics on to the NOC |
| on <DEVICE-NAME> | Optional. Executes the command on a specified device<br>• <DEVICE-NAME> – Specify the name of the device. |

- `service guest-registration backup [delete|restore]`

| | |
|---|---|
| service guest-registration backup [delete\|restore] | Deletes or restores all guest registration backup snapshots based on the parameter passed<br>• delete – Deletes all guest registration backup snapshots<br>• restores – Restores all guest registration backup snapshots<br>**Note:** To view the status of the restore process, use the *service > show > guest-registration > restore-status* command. |

- `service guest-registration delete [all|email <EMAIL-ADD>|group <RAD-GROUP-NAME>|mac <MAC>|mobile <MOBILE-NUMBER>|name <CLIENT-FULL-NAME>|non-social|offline-for days <1-999>|wlan <WLAN-NAME>|otp-incomplete-for days <1-999>|social [facebook|google]`

| | |
|---|---|
| service guest-registration delete | Deletes a specified user or all user records from the guest-registration database<br>To delete a specific user, use one of the following options as an identification parameter: email, group, mac, mobile number, name, offline-for, wlan, otp-incomplete-for, or social. |
| [all\|email <EMAIL-ADD>\|group <RAD-GROUP-NAME>\| mac <MAC>\|mobile <MOBILE-NUMBER>\| name <CLIENT-FULL-NAME>]\|non-social\| offline-for days <1-999>\|wlan <WLAN-NAME>\|otp-incomplete-for days <1-999>\|social [facebook\|google] | Following are the user filtering options: The user identified by one of the following parameters is deleted from the guest-registration database.<br>• email <EMAIL-ADD> – Identifies user by the e-mail address<br>  • <EMAIL-ADD> – Provide the user's e-mail address.<br>• mac <MAC> – Identifies user by the MAC address<br>  • <MAC> – Provide the user's MAC address.<br>• group <RAD-GROUP-NAME> – Identifies users by their RADIUS group association<br>  • <RAD-GROUP-NAME> – Specify the RADIUS group name.<br>• mobile <MOBILE-NUMBER> – Identifies user by the registered mobile number<br>  • <MOBILE-NUMBER> – Provide the user's mobile number.<br>Contd.. |

| | |
|---|---|
| | • name <CLIENT-FULL-NAME> – Identifies user by the registered full name<br>  • <CLIENT-FULL-NAME> – Provide the user's full name.<br>• non-social – Identifies users that have not registered through social authentication<br>• offline-for days <1-999> – Filters users who have not accessed the network for a specified number of days<br>  • days <1-999> – Specify the number of days from 1 - 999.<br>• wlan <WLAN-NAME> – Identifies users accessing a specified WLAN<br>  • <WLAN-NAME> – Specify the WLAN name.<br>• otp-incomplete-for days <1-999> – Identifies records of users that have not used their *one-time-password* (OTP) to complete registration within a specified number of days<br>  • days <1-999> – Specify the number of days from 1 - 999.<br>• social [facebook\|google] – Identifies users using either Facebook or Google credentials to access the network<br>  • facebook – Identifies users using Facebook authentication<br>  • google – Identifies users using Google authentication |

• `service guest-registration export format [csv|json] <DEST-URL> {(rfdomain <DOMAIN-NAME>|time [1-Day|1-Month|1-Week|2-Hours|30-Mins|5-Hours|all]|wlan <WLAN-NAME>)}`

| | |
|---|---|
| service guest-registration export | Exports guest registration user data files in the *Comma-Separated Values* (CSV) or *JavaScript Object Notation* (JSON) format<br>Use the 'rfdomain', 'wlan', and 'time' options to filter users for a specified RF Domain, WLAN, and/or time period. These are recursive parameters and you can apply all or any of these three filters. |
| format [csv\|json] | Specifies the file format. The options are:<br>• csv – Exports user data files in the CSV format<br>• json – Exports user data files in the JSON format |
| <DEST-URL> | Configures the destination URL. The files are exported to the specified location. Both IPv4 and IPv6 address formats are supported.<br>IPv4 URLs:<br>tftp://<hostname\|IP>[:port]/path/file<br>ftp://<user>:<passwd>@<hostname\|IP>[:port]/path/file<br>sftp://<user>:<passwd>@<hostname\|IP>[:port]>/path/file<br>IPv6 URLs:<br>tftp://<hostname\|[IPv6]>[:port]/path/file<br>ftp://<user>:<passwd>@<hostname\|[IPv6]>[:port]/path/file<br>sftp://<user>:<passwd>@<hostname\|[IPv6]>[:port]>/path/file |
| rfdomain <DOMAIN-NAME> | Optional. Filters user data based on RF Domain name. Only the filtered data are exported.<br>• <DOMAIN-NAME> – Specify the RF Domain name. |
| wlan <WLAN-NAME> | Optional. Filters user data based on WLAN name. Only the filtered data are exported.<br>• <WLAN-NAME> – Specify the WLAN name. |

| | |
|---|---|
| time [1-Day\|1-Month\|<br>1-Week\|2-Hours\|<br>30-Mins\|5-Hours\|all] | Optional. Filters user data for a specified time period. Only the filtered data are exported.<br>• 1-Day – Filters and exports previous day's data<br>• 1-Month – Filters and exports previous month's data<br>• 1-Week – Filters and exports previous week's data<br>• 2-Hours – Filters and exports last 2 hours data<br>• 30-Mins – Filters and exports last 30 minutes data<br>• 5-Hours – Filters and exports last 5 hours data<br>• all – Exports the entire database |

- `service guest-registration import format json <SOURCE-URL>`

| | |
|---|---|
| service<br>guest-registration<br>import | Imports user data from a specified location |
| format json | Specifies the file format<br>• json – Imports user data files in the JSON format |
| <SOURCE-URL> | Configures the Source URL. The files are imported from the specified location. Both IPv4 and IPv6 address formats are supported.<br>IPv4 URLs:<br>tftp://<hostname\|IP>[:port]/path/file<br>ftp://<user>:<passwd>@<hostname\|IP>[:port]/path/file<br>sftp://<user>:<passwd>@<hostname\|IP>[:port]>/path/file<br>IPv6 URLs:<br>tftp://<hostname\|[IPv6]>[:port]/path/file<br>ftp://<user>:<passwd>@<hostname\|[IPv6]>[:port]/path/file<br>sftp://<user>:<passwd>@<hostname\|[IPv6]>[:port]>/path/file |

- `service load-balancing clear-client-capability [<MAC>|all] {on <DEVICE-NAME>}`

| | |
|---|---|
| load-balancing | Enables wireless load balancing by clearing client capability records |
| clear-client-capability<br>[<MAC>\|all] | Clears a specified client or all client's capability records<br>• <MAC> – Clears capability records of a specified client. Specify the client's MAC address in the AA-BB-CC-DD-EE-FF format.<br>• all – Clears the capability records of all clients |
| on <DEVICE-NAME> | Optional. Clears client capability records on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `service load-ssh-authorized-keys <PUBLIC-KEY> {on <DEVICE-NAME>}`

| | |
|---|---|
| load-ssh-authorized-keys | Loads SSH public (client) key on a device |
| <PUBLIC-KEY> | Enter the public key. The public key should be in the OpenSSH rsa/dsa format. |
| on <DEVICE-NAME> | Optional. Loads the specified public key on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `service locator {<1-60>} {(on <DEVICE-NAME>)}`

| | |
|---|---|
| locator | Enables LEDs |
| <1-60> | Sets LED flashing time from 1 - 60 seconds. |
| on <DEVICE-NAME> | The following keyword is recursive and common to the <1-60> parameter:<br>• on <DEVICE-NAME> – Optional. Enables LEDs on a specified device<br>• <DEVICE-NAME> – Specify name of the AP, wireless controller, or service platform. |

- `service nsight clear-offline [all|offline-for days <0-999> {time <TIME>}]`

| | |
|---|---|
| nsight clear-offline [all\|offline-for days <0-999> {time <TIME>}] | Clears NSight data received from offline controllers, based on the parameters passed. Select one of the following options:<br>• all – Clears NSight data received from all offline controllers<br>• offline-for days <0-999> time <TIME> – Clears NSight data received from controllers that have been offline for a specified time period<br>• days <0-999> – Specifies the number of days controllers have been offline<br>• <0-999> – Specify the number of days from 0 - 999 days. Select "0" to identify controllers offline less than 24 hours.<br>• time <TIME> – Optional. Specifies the total time for which controllers have been offline<br>• <TIME> – Specify the time in HH:MM:SS format.<br>**Note:** This command is applicable only to the NX95XX, NX9600, and VX9000 platforms. |

- `service radio <1-3> adaptivity`

| | |
|---|---|
| radio <1-3> | Configures radio's parameters<br>• <1-3> – Specify the radio index from 1 - 3. |
| adaptivity | Simulates the presence of interference on the current channel |

- `service radio <1-3> channel-switch <36-196> [160|20|40|80|80-80]`

| | |
|---|---|
| radio <1-3> | Configures radio's parameters<br>• <1-3> – Specify the radio index from 1 - 3. |
| channel-switch <36-196> [160\|20\|40\|80\|80-80] | Enables channel switching<br>• <36-196> – Specifies the channel to switch to from 36 - 196.<br>• 160\|20\|40\|80\|80-80] – Specifies the bandwidth for the above specified channel. Select the appropriate option. |

- `service radio <1-3> dfs simulate-radar [extension|primary]`

| | |
|---|---|
| radio <1-3> | Configures radio's parameters<br>• <1-3> – Specify the radio index from 1 - 3. |
| dfs | Enables *Dynamic Frequency Selection* (DFS) |
| simulate-radar [extension\|primary] | Simulates the presence of a radar on a channel. Select the channel type from the following options:<br>• extension – Simulates a radar on the radio's current extension channel<br>• primary – Simulates a radar on the radio's current primary channel |

- `service radius test [<IP>|<HOSTNAME>] <WORD> <USERNAME> <PASSWORD> {wlan <WLAN-NAME> ssid <SSID>} {(on <DEVICE-NAME>)}`

| | |
|---|---|
| radius test | Tests RADIUS server's account. This command sends an access-request packet to the RADIUS server. Use this command to confirm time and data/bandwidth parameters for valid wireless clients.<br>• test – Tests the RADIUS server's account with user provided parameters |
| [<IP>\|<HOSTNAME>] | Sets the RADIUS server's IP address or hostname<br>• <IP> – Specifies the RADIUS server's IP address<br>• <HOSTNAME> – Specifies the RADIUS server's hostname |
| <WORD> | Specify the RADIUS server's shared secret. |
| <USERNAME> | Specify username for authentication. |
| <PASSWORD> | Specify the password. |
| wlan <WLAN-NAME> ssid <SSID> | Optional. Tests the RADIUS server on the local WLAN. Specify the local WLAN name.<br>• ssid <SSID> – Specify the local RADIUS server's SSID. |
| on <DEVICE-NAME> | Optional. This is a recursive parameter also applicable to the WLAN parameter. Performs tests on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `service radius test [<IP>|<HOSTNAME>] port <1024-65535> <WORD> <USERNAME> <PASSWORD> {wlan <WLAN-NAME> ssid <SSID>} {(on <DEVICE-NAME>)}`

| | |
|---|---|
| radius test | Tests a RADIUS server's account. This command sends an access-request packet to the RADIUS server. Use this command to confirm time and data/bandwidth parameters for valid wireless clients.<br>• test – Tests the RADIUS server's account with user provided parameters |
| [<IP>\|<HOSTNAME>] | Sets the IP address or hostname of the RADIUS server<br>• <IP> – Specify the RADIUS server's IP address.<br>• <HOSTNAME> – Specify the RADIUS server's hostname. |
| port <1024-65535> | Specify the RADIUS server port from 1024 - 65535. The default port is 1812. |
| <WORD> | Specify the RADIUS server's shared secret. |
| <USERNAME> | Specify username for authentication. |
| <PASSWORD> | Specify the password. |
| wlan <WLAN-NAME> ssid <SSID> | Optional. Tests the RADIUS server on the local WLAN. Specify the local WLAN name.<br>• ssid <SSID> – Specify the RADIUS server's SSID. |
| on <DEVICE-NAME> | Optional. This is a recursive parameter also applicable to the WLAN parameter. Performs tests on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

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

| | |
|---|---|
| set | Sets the validation mode for running configuration validation |

| | |
|---|---|
| validation-mode [full\|partial] | Sets the validation mode<br>• full – Performs a full configuration validation<br>• partial – Performs a partial configuration validation |
| on <DEVICE-NAME> | Optional. Performs full or partial configuration validation on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `service show block-adopter-config-update`

| | |
|---|---|
| show | Displays running system statistics based on the parameters passed |
| block-adopter-config-update | Displays NOC configuration blocking status |

- `service show captive-portal log-internal`

| | |
|---|---|
| show | Displays running system statistics based on the parameters passed |
| captive-portal | Displays captive portal information |
| log-internal | Displays recent captive portal debug logs (information and above severity level) |

- `service show captive-portal [servers|user-cache] {on <DEVICE-NAME>}`

| | |
|---|---|
| show | Displays running system statistics based on the parameters passed |
| captive-portal | Displays captive portal information |
| servers | Displays server information for active captive portals |
| user-cache | Displays cached user details for a captive portal |
| on <DEVICE-NAME> | Optional. Displays server information or cached user details on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `service show [cli|client-identity-defaults|configuration-revision|mac-user-import-status|mac-vendor <OUI/MAC>|noc diag|snmp session|xpath-history]`

| | |
|---|---|
| show | Displays running system statistics based on the parameters passed |
| cli | Displays CLI tree of the current mode |
| client-identity-defaults | Displays default client-identities and their configuration |
| configuration-revision | Displays current configuration revision number |
| mac-user-import-status | Displays status of file import initiated by a MAC-user |
| mac-vendor <OUI/MAC> | Displays vendor name for a specified MAC address or *Organizationally Unique Identifier* (OUI) part of the MAC address<br>• <OUI/MAC> – Specify the MAC address or its OUI. The first six digits of the MAC address is the OUI. Use the AABBCC or AA-BB-CC format to provide the OUI. |
| noc diag | Displays NOC diagnostic details |
| snmp session | Displays SNMP session details |
| xpath-history | Displays XPath history |

- `service show [command-history|crash-info|info|mem|process|reboot-history|startup-log|ssh-authorized-keys|sysinfo|top|upgrade-history|watchdog] {on <DEVICE-NAME>}`

| | |
|---|---|
| show | Displays running system statistics based on the parameters passed |
| command-history | Displays command history (lists all commands executed) |
| crash-info | Displays information about core, panic, and AP dump files |
| info | Displays snapshot of available support information |
| mem | Displays a system's current memory usage (displays the total memory and available memory) |
| process | Displays active system process information (displays all processes currently running on the system) |
| reboot-history | Displays the device's reboot history |
| startup-log | Displays the device's startup log |
| ssh-authorized-keys | Displays all devices (device hostnames) that have ssh authorized keys loaded |
| sysinfo | Displays system's memory usage information |
| top | Displays system resource information |
| upgrade-history | Displays the device's upgrade history (displays details, such as date, time, and status of the upgrade, old version, new version, etc.) |
| watchdog | Displays the device's watchdog status |
| on <DEVICE-NAME> | The following keywords are common to all of the above:<br>• on <DEVICE-NAME> – Optional. Displays information for a specified device. If no device is specified, the system displays information for logged device(s)<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `service show ip-access-list wlan <WLAN-NAME> status {detail} {on <DEVICE-OR-DOMAIN-NAME>}`

| | |
|---|---|
| show ip-access-list | Displays status of IP *Access Control List* (ACL) to WLAN mappings on a specified device or all devices within a specified RF Domain. This command also displays if IP ACLs are properly applied in the dataplane. |
| wlan <WLAN-NAME> | Specifies the WLAN, for which the IP ACL to WLAN mapping status is required<br>• <WLAN-NAME> – Specify the WLAN name. |
| status detail | Displays only failed IP ACL to WLAN mappings<br>• details – Optional. Displays all (failed as well as successful) IP ACL to WLAN mapping status |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Specifies the device name or the RF Domain name.<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the device name or the RF Domain. When specified, the system displays IP ACL to WLAN mapping status on the specified device or all devices within the specified RF Domain. |

- `service show dhcp-lease {<INTERFACE-NAME>|on|pppoe1|vlan <1-4094>|wwan1} {(on <DEVICE-NAME>)}`

| | |
|---|---|
| show | Displays running system statistics based on the parameters passed |
| dhcp-lease | Displays DHCP lease information received from the server |

| | |
|---|---|
| <INTERFACE-NAME> | Optional. Displays DHCP lease information for a specified router interface<br>• <INTERFACE-NAME> – Specify the router interface name. |
| on | Optional. Displays DHCP lease information for a specified device |
| pppoe1 | Optional. Displays DHCP lease information for a PPP over Ethernet interface |
| vlan <1-4094> | Optional. Displays DHCP lease information for a VLAN interface<br>• <1-4094> – Specify a VLAN index from 1 - 4094. |
| wwan1 | Optional. Displays DHCP lease information for a Wireless WAN interface |
| on <DEVICE-NAME> | The following keywords are common to all of the above:<br>• on <DEVICE-NAME> – Optional. Displays DHCP lease information for a specified device. If no device is specified, the system displays information for the logged device.<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `service show diag [fds|pkts]`

| | |
|---|---|
| show diag | Displays diagnostic statistics, such as LED status, fan speed, sensor temperature, open file descriptors, looped packets etc. |
| fds | Displays the number of *file descriptors* (fds) opened by key processes, such as the CFGD. When executed, the command displays only the file name and FD. |
| pkts | Displays details of looped packets captured by the dataplane and pushed to a separate queue. These queued packets are written to a log file (named *loop_pkt_info.log*) available at the /var2/log/ directory. Use the *service > start-shell* command and enter the path 'cat /var2/log/' to view if the *loop_pkt_info.log* file exists. However, looped packet logging has to be enabled in the profile/device context. For more information, see *diag*.<br>The dataplane can log up to 16 looped packets at a time. Once the queue is full, no new loop packet is logged until the existing queue is cleared. To clear the logged looped packet queue execute the *service > clear > diag > pkts* command.<br>Following are the loop codes and the corresponding loop reasons:<br>(5) - "pkt looping in dataplane"<br>(51) - "loop in packet path"<br>(367) - "wispe encapsulation loop"<br>(432) - "mcx loop prevention"<br>(532) - "Port loop detected"<br>(536) - "packet loop detected by wireless bridge"<br>(41) - "IPv4 TTL exceeded"<br>(493) - "IPv6 TTL exceeded"<br>(540) - "mint TTL exceeded" |

- `service show diag [led-status|psu|stats]` *`{(on <DEVICE-NAME>)}`*

| | |
|---|---|
| show | Displays running system statistics based on the parameters passed |
| diag | Displays diagnostic statistics, such as LED status, fan speed, and sensor temperature |
| led-status | Displays LED state variables and the current state |
| psu | Displays power supply information |

| | |
|---|---|
| stats | Displays fan speed and sensor temperature statistics |
| on <DEVICE-NAME> | Optional. Displays diagnostic statistics for a specified device. If no device is specified, the system displays information for the logged device.<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `service show guest-registration [export-status|import-status|restore-status]`

| | |
|---|---|
| show | Displays running system statistics based on the parameters passed |
| guest-registration | Displays status of the guest-registration database snapshot related processes (export, import, and restore)<br>**Note:** To export, import, or restore a guest-registration database, use the *service > guest-registration > [backup\|export\|import]* command.] |
| export-status | Displays the status of the latest export process initiated |
| import-status | Displays the status of the latest import process initiated |
| export-status | Displays the status of the latest restore process initiated |

- `service show fast-switching` *`{on <DEVICE-NAME>}`*

| | |
|---|---|
| show | Displays running system statistics based on the parameters passed |
| fast-switching | Displays fast switching state (enabled or disabled) |
| on <DEVICE-NAME> | Optional. Displays fast switching state for a specified device. If no device is specified, the system displays information for the logged device.<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `service show [fib|fib6]` *`{table-id <0-255>}`*

| | |
|---|---|
| show | Displays running system statistics based on the parameters passed |
| fib | Displays entries in the *Forwarding Information Base* (FIB) |
| fib6 | Displays FIB IPv6 static routing entries<br>The WiNG software allows the IPv6 FIB to maintain only IPv6 static and interface routes.<br>FIB is a collection of routing entries. A route entry consists of IPv6 network (which can also be a host) address, the prefix length for the network (for IPv6 routes this is between 0 - 128), and the next hop's (gateway) IPv6 address. Since a destination can be reached through multiple next hops, you can configure multiple routes to the same destination with multiple next hops. |
| table-id <0-255> | Optional. Displays FIB information maintained by the system based on the table ID<br>• <0-255> – Specify the table ID from 0 - 255. |

- `service show mint [adopted-devices` *`{on <DEVICE-NAME>}`*`|ports]`

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

| | |
|---|---|
| adopted-devices on <DEVICE-NAME> | Displays adopted devices status in dpd2<br>• on <DEVICE-NAME> – Optional. Displays MiNT protocol details for a specified device. If no device is specified, the system displays information for the logged device.<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |
| ports | Displays MiNT ports used by various services and features |

- `service show pm {history} {(on <DEVICE-NAME>)}`

| | |
|---|---|
| show | Displays running system statistics based on the parameters passed |
| pm | Displays the *Process Monitor* (PM) controlled process details |
| history | Optional. Displays process change history (the time at which the change was implemented, and the events that triggered the change) |
| on <DEVICE-NAME> | Optional. Displays process change history for a specified device. If no device is specified, the system displays information for the logged device.<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `service show rf-domain-manager [diag|info] {<MAC/HOSTNAME>} {(on <DEVICE-OR-DOMAIN-NAME>)}`

| | |
|---|---|
| show | Displays running system statistics based on the parameters passed |
| rf-domain-manager | Displays RF Domain manager information |
| diag | Displays RF Domain manager related diagnostics statistics |
| info | The following keyword is common to the 'diag' and 'info' parameters:<br>Displays RF Domain manager related information |
| <MAC/HOSTNAME> | Optional. Specify the MAC address or hostname of the RF Domain manager. |
| on <DEVICE-OR-DOMAIN-NAME> | The following keyword is common to the 'diag' and 'info' parameters:<br>Optional. Displays diagnostics statistics on a specified device or domain<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |

- `service show sites`

| | |
|---|---|
| show | Displays running system statistics based on the parameters passed |
| sites | Displays NOC sites related information |

- `service show virtual-machine-history {on <DEVICE-NAME>}`

| | |
|---|---|
| show virtual-machine-history | Displays virtual machine history based on the parameters passed<br>This command is applicable only to the NX9500, and NX9510 series service platforms. It is also available on the Privilege Executable Mode of these devices. |
| on <DEVICE-NAME> | Optional. Displays virtual machine history on a specified device. If no device is specified, the system displays information for the logged device.<br>• <DEVICE-NAME> – Specify the name of the service platform. |

- `service show wireless [aaa-stats|adaptivity-status|credential-cache|dns-cache|radar-status|vlan-usage] {on <DEVICE-NAME>}`

| | |
|---|---|
| show | Displays running system statistics based on the parameters passed |

| | |
|---|---|
| wireless | Displays WLAN statistics (WLAN AAA policy, configuration parameters, VLAN assignment, etc.) |
| aaa-stats | Displays AAA policy statistics |
| adaptivity-status | Displays the current list of channels (with interference levels exceeding the configured threshold resulting in adaptivity kicking in) and time when adaptivity kicked in on a device |
| credential-cache | Displays clients cached credentials statistics (VLAN, keys, etc.) |
| dns-cache | Displays cache of resolved names of servers related to wireless networking |
| radar-status | Displays radar discovery status. This option displays following information:<br>• If a radar has been discovered by the AP<br>• The time of discovery |
| vlan-usage | Displays VLAN statistics across WLANs |
| on <DEVICE-NAME> | The following keywords are common to all of the above:<br>• on <DEVICE-NAME> – Optional. Displays running system statistics on a specified device. If no device is specified, the system displays information for the logged device.<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `service show wireless [config-internal|log-internal|neighbors]`

| | |
|---|---|
| show | Displays running system statistics based on the parameters passed |
| wireless | Displays WLAN statistics (WLAN AAA policy, configuration parameters, VLAN usage, etc.) |
| config-internal | Displays internal configuration parameters |
| log-internal | Displays recent internal wireless debug logs (info and above severity) |
| neighbors | Displays neighboring device statistics for roaming and flow migration |

- `service show wireless [client|meshpoint neighbor] proc [info|stats]` *`{<MAC>} {(on <DEVICE-OR-DOMAIN-NAME)}`*

| | |
|---|---|
| show | Displays running system statistics based on the parameters passed |
| wireless | Displays WLAN statistics (WLAN AAA policy, configuration parameters, VLAN usage, etc.) |
| client | Displays WLAN client statistics |
| meshpoint neighbor | Displays meshpoint related proc entries |
| proc | The following keyword is common to client and meshpoint neighbor parameters:<br>• proc – Displays dataplane proc entries based on the parameter selected<br>**Note:** These proc entries provide statistics on each wireless client on the WLAN.<br>**Note:** For the meshpoint parameter, it displays proc entries about neighbors. |
| info | This parameter is common to client and meshpoint neighbor parameters. Displays information for a specified device (wireless client or neighbor) or RF Domain |
| stats | This parameter is common to client and meshpoint neighbor parameters. Displays information for a specified device (wireless client or neighbor) or RF Domain |

| | |
|---|---|
| <MAC> | Displays information for a specified device (wireless client or neighbor) or RF Domain |
| on <DEVICE-OR-DOMAIN-NAME> | This parameter is common to client and meshpoint neighbor parameters. Displays information for a specified device (wireless client or neighbor) or RF Domain.<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |

- `service show wireless radio-internal [radio1|radio2] <LINE>`

| | |
|---|---|
| show | Displays running system statistics based on the parameters passed |
| wireless | Displays WLAN statistics (WLAN AAA policy, configuration parameters, VLAN usage, etc.) |
| radio-internal [radio1\|radio2] | Displays radio internal debug logs. Select the radio from the following options:<br>• radio1 – Selects radio 1<br>• radio2 – Selects radio 2. |
| <LINE> | Specify the radio internal debug command to enable. |

- `service show wireless reference [channels|frame|handshake|mcs-rates|reason-codes|status-codes]`

| | |
|---|---|
| show | Displays running system statistics based on the parameters passed |
| wireless | Displays WLAN statistics (WLAN AAA policy, configuration parameters, VLAN usage, etc.) |
| reference | Displays look up reference information related to standards, protocols, etc. |
| channels | Displays 802.11 channels information |
| frame | Displays 802.11 frame structure |
| handshake | Displays a flow diagram of 802.11 handshakes |
| mcs-rates | Displays MCS rate information |
| reason-codes | Displays 802.11 reason codes (for deauthentication, disassociation, etc.) |
| status-codes | Displays 802.11 status codes (for association response) |

- `service show wireless stats-client diag {<MAC/HOSTNAME>} {(on <DEVICE-OR-DOMAIN-NAME)}`

| | |
|---|---|
| show | Displays running system statistics based on the parameters passed |
| wireless | Displays WLAN statistics (WLAN AAA policy, configuration parameters, VLAN usage, etc.) |
| stats-client | Displays managed AP statistics |
| <MAC/HOSTNAME> | Optional. Specify the MAC address or hostname of the AP. |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Displays statistics on a specified AP, or all APs on a specified domain.<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |

- `service smart-rf clear-config {<MAC>|<DEVICE-NAME>|on <DOMAIN-NAME>}`

| | |
|---|---|
| smart-rf | Enables Smart RF management |
| clear-config | Clears WLAN Smart RF configuration on a specified device or on all devices |

| | |
|---|---|
| <MAC> | Optional. Clears WLAN Smart RF configuration on a device identified by its MAC address. Specify the device's MAC address in the AA-BB-CC-DD-EE-FF format. |
| <DEVICE-NAME> | Optional. Clears WLAN Smart RF configuration on a device identified by its hostname. Specify the device's hostname. |
| on <DOMAIN-NAME> | Optional. Clears WLAN Smart RF configuration on all devices in a specified RF Domain<br>• <DOMAIN-NAME> – Specify the RF Domain name. |

- `service smart-rf [clear-history|clear-interfering-aps|save-config] {on <DOMAIN-NAME>}`

| | |
|---|---|
| smart-rf | Enables Smart RF management |
| clear-history | Clears WLAN Smart RF history on all devices |
| clear-interfering-aps | Clears Smart-RF interfering APs |
| save-config | Saves the Smart RF configuration on all devices, and also saves the history on the RF Domain Manager |
| on <DOMAIN-NAME> | Optional. Clears WLAN Smart RF configuration on all devices in a specified RF Domain<br>• <DOMAIN-NAME> – Specify the RF Domain name. |

- `service snmp sysoid wing5`

| | |
|---|---|
| snmp sysoid wing5 | Configures a new *sysObjectID* (sysoid), in the MIB, for devices running WiNG 5.X devices<br>When configured, the SNMP manager returns sysoid for WiNG 5.X OS. Hardwares running the WiNG 4.X and WiNG 5.X images have different sysoids. For example, the sysoid for a RFS4000 using the WiNG 4.X image differs from another RFS4000 running the WiNG 5.X image.<br>This command is applicable only to RFS4000 and RFS6000 platforms, since they have the same sysoid supported in WiNG 4.X and WiNG 5.X.<br>The WiNG 4.X sysoids are:<br>• RFS4000 – 1.3.6.1.4.1.388.18<br>• RFS6000 – 1.3.6.1.4.1.388.16<br>The WiNG 5.X sysoids are:<br>• RFS4000 – 1.3.6.1.4.1.388.50.1.1.35<br>• RFS6000 – 1.3.6.1.4.1.388.50.1.1.36 |

- `service ssm dump-core-snapshot`

| | |
|---|---|
| ssm dump-core-snapshot | Triggers a debug core dump of the SSM module |

- `service syslog test {level [<0-7>|alerts|critical|debugging|emergencies|errors|informational|notifications|warnings]} {(on <DEVICE-NAME>)}`

| | |
|---|---|
| syslog test | Sends a test message to the syslog server to confirm server availability |

| | |
|---|---|
| level | Optional. Sets the logging level. In case syslog server is unreachable, an event is logged based on the logging level defined. This is an optional parameter, and the system configures default settings, if no logging severity level is specified.<br>• <0-7> – Optional. Specify the logging severity level from 0-7. The various levels and their implications are as follows:<br>  • alerts – Optional. Immediate action needed (severity=1)<br>  • critical – Optional. Critical conditions (severity=2)<br>  • debugging – Optional. Debugging messages (severity=7)<br>  • emergencies – Optional. System is unusable (severity=0)<br>  • errors – Optional. Error conditions (severity=3)<br>  • informational – Optional. Informational messages (severity=6)<br>  • notifications – Optional. Normal but significant conditions (severity=5)<br>  • warnings – Optional. Warning conditions (severity=4). This is the default setting. |
| on <DEVICE-NAME> | Optional. Executes the command on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `service ssm trace pattern <WORD> {on <DEVICE-NAME>}`

| | |
|---|---|
| ssm trace | Displays the SSM module trace based on parameters passed |
| pattern <WORD> | Configures the pattern to match<br>• <WORD> – Specify the pattern to match. |
| on <DEVICE-NAME> | Optional. Displays the SSM module trace on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `service wireless client beacon-request <MAC> mode [active|passive|table] ssid [<SSID>|any] channel-report [<CHANNEL-LIST>|none] {on <DEVICE-NAME>}`

| | |
|---|---|
| wireless client beacon-requests | Sends beacon measurement requests to a wireless client |
| <MAC> | Specify the wireless client's MAC address. |
| mode [active\|passive\|table] | Specifies the beacon measurement mode. The following modes are available:<br>• Active – Requests beacon measurements in the active mode<br>• Passive – Requests beacon measurements in the passive mode<br>• Table – Requests beacon measurements in the table mode |
| ssid [<SSID>\|any] | Specifies if the measurements have to be made for a specified SSID or for any SSID<br>• <SSID> – Requests beacon measurement for a specified SSID<br>• any – Requests beacon measurement for any SSID |
| channel-report [<CHANNEL-LIST>\| none] | Configures channel report in the request. The request can include a list of channels or can apply to all channels.<br>• <CHANNEL-LIST> – Request includes a list of channels. The client has to send beacon measurements only for those channels included in the request<br>• none – Request applies to all channels |
| on <DEVICE-NAME> | Optional. Sends requests on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `service wireless client quiet-element [start|stop]`

| | |
|---|---|
| wireless client quiet-element | Enables the quite-element information in beacons sent to wireless clients |
| start | Enables the quite-element information in beacons sent to wireless clients. This is the interval for which all wireless clients are to remain quiet. |
| stop | Disables the quite-element information in beacons sent to wireless clients. Once disabled, this information is no longer included in beacons. |

- `service wireless client trigger-bss-transition mac <MAC> {timeout <0-65535} {url <URL>} {on <DEVICE-OR-DOMAIN-NAME>}`

| | |
|---|---|
| wireless client trigger-bss-transition | Sends a 80211v-Wireless Network Management BSS transition request to a client |
| mac <MAC> | Specifies the wireless client's MAC address |
| timeout <0-65535> | Specifies the time remaining, for this client. before BSS transition is initiated. In other words on completion of the specified time period, BSS transition is triggered.<br>• <0-65535> – Specify a time from 0 -65535 seconds. |
| url <URL> | Optional. Specifies session termination URL |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Sends request on a specified device<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |

- `service wireless client trigger-wnm mac <MAC> type [deauth-imminent| subscription-remediation] {uri <WORD>}`

| | |
|---|---|
| wireless client trigger-wnm | Sends a WNM notification (action frame) to a wireless client |
| mac <MAC> | Specifies the wireless client's MAC address |
| type [deauth-imminent\| subscription-remediation] | Configures the WNM notification type<br>• deauth-imminent – Sends a de-authentication imminent frame<br>• subscription-remediation – Sends a subscription remediation needed frame |
| uri <WORD> | Optional. Specifies the *unique resource identifier* (URI) |

- `service wireless dump-core-snapshot`

| | |
|---|---|
| wireless client dump-core-snapshot | Triggers a debug core dump of the wireless module |

- `service wireless meshpoint zl <MESHPOINT-NAME> [on <DEVICE-NAME>] {<ARGS>| timeout <1-65535>}`

| | |
|---|---|
| service wireless meshpoint zl | Triggers a zonal level debug of a specified meshpoint's modules |
| <MESHPOINT-NAME> | Specify the meshpoint name |
| on <DEVICE-NAME> | Triggers zonal level debug of a specified meshpoint's modules on a specified device<br>• <DEVICE-NAME> – Specify the name of the device (AP, wireless controller, or service platform) |

| | |
|---|---|
| <ARGS> | Optional. Specifies the zonal arguments. These zonal arguments represent the meshpoint modules identified by the zonal and subzonal arguments passed here. Also specify the debug level from 0 -7. Please see the *Examples* section, at the end of this topic, for more information. |
| timeout <1-65535> | Optional. Specifies a timeout value from 1 - 65535 seconds. When specified, meshpoint logs are debugged for the time specified here. |

- `service wireless qos delete-tspec <MAC> tid <0-7>`

| | |
|---|---|
| wireless qos delete-tspec | Sends a delete TSPEC request to a wireless client |
| <MAC> | Specify the MAC address of the wireless client. |
| tid <0-7> | Deletes the *Traffic Identifier* (TID)<br>• <0-7> – Select the TID from 0 - 7. |

- `service wireless trace pattern <WORD> {on <DEVICE-NAME>}`

| | |
|---|---|
| wireless trace | Displays the wireless module trace based on parameters passed |
| pattern <WORD> | Configures the pattern to match<br>• <WORD> – Specify the pattern to match. |
| on <DEVICE-NAME> | Optional. Displays the wireless module trace on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `service wireless unsanctioned ap air-terminate <MAC> {on <DOMAIN-NAME>}`

| | |
|---|---|
| wireless unsanctioned ap air-terminate | Enables unsanctioned access points termination |
| <MAC> | Configures the unsanctioned access points' BSSID (MAC address) |
| on <DOMAIN-NAME> | Optional. Specifies the RD Domain of the access point<br>• <DOMAIN-NAME> – Specify the name of the RF Domain. |

- `service wireless wips clear-client-blacklist [all|mac <MAC>]`

| | |
|---|---|
| wireless wips | Enables management of WIPS parameters |
| clear-client-blacklist [all\|mac <MAC>] | Removes a specified client or all clients from the blacklist<br>• all – Removes all clients from the blacklist<br>• mac <MAC> – Removes a specified client form the blacklist<br>  • <MAC> – Specify the wireless client's MAC address. |

- `service wireless wips clear-event-history {on <DEVICE-OR-DOMAIN-NAME}`

| | |
|---|---|
| wireless wips | Enables WIPS management |
| clear-event-history | Clears event history |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Clears event history on a device or RF Domain<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |

**Syntax (Privilege Exec Mode)**

**NOTE:** The “service” command of the Priv Exec Mode is the same as the service command in the User Exec Mode. There a few modifications that have been documented in this section. For the syntax and parameters of the other commands refer to the *(User Exec Mode)* syntax and *(User Exec Mode)* parameters sections of this chapter.

*service*

```
service [block-adopter-config-updates|clear|cli-tables-skin|cluster|copy|
database|delete|delete-offline-aps|force-send-config|force-update-vm-stats|
guest-registration|load-balancing|locator|mint|pktcap|pm|radio|radius|
request-full-config-from-adopter|restore|set|show|signal|smart-rf|snmp|ssm|
start-shell|syslog|trace|wireless]

service clear crash-info {on <DEVICE-NAME>}

service copy [stats-report|tech-support]

service copy stats-report [global|rf-domain <DOMAIN-NAME>] (<FILE>|<URL>)

service copy tech-support [<FILE>|<URL>]

service database [authentication|compact|drop|maintenance-mode|primary-stepdown|
remove-all-files|replica-set|server|start-shell]

service database authentication [create-user|delete-user]

service database authentication create-user username <USER-NAME> password
<PASSWORD>

service database authentication delete-user username <USER-NAME>

service database compact [all|captive-portal|nsight]

service database drop [captive-portal|nsight] collection <COLLECTION-NAME>

service database [maintenance-mode|primary-stepdown|remove-all-files|start-shell]

service database replica-set [add|delete]

service database replica-set add member [<IP>|<FQDN>] [arbiter|priority <0-255>]

service database replica-set delete member [<IP>|<FQDN>]

service database server [restart|start|stop]

service delete sessions <SESSION-COOKIES>

service mint [clear|debug-log|expire|flood]

service mint [clear [lsp-db|mlcp]|debug-log [flash-and-syslog|flash-only]|expire
[lsp|spf]|flood [csnp|lsp]]

service pktcap on [bridge|deny|drop|ext-vlan|interface|radio|rim|router|vpn|
wireless]

service pktcap on [bridge|deny|drop|ext-vlan|rim|router|vpn|wireless] {(acl-name
<ACL>,count <1-1000000>,direction [any|inbound|outbound],filter <LINE>,hex,rate
<1-100>,snap <1-2048>,tcpdump,verbose,write [file|url|tzsp [<IP/TZSP-HOSTNAME>])}

service pktcap on interface [<INTERFACE-NAME>|ge <1-4>|me1|port-channel <1-2>|
pppoe1|vlan <1-4094>|wwan1] {(acl-name <ACL>,count <1-1000000>,direction
[any|inbound|outbound],filter <LINE>,hex,rate <1-100>,snap <1-2048>,tcpdump,
verbose,write [file|url|tzsp [<IP/TZSP-HOSTNAME>])}
```

```
service pktcap on radio [<1-1024>|all] {(acl-name <ACL>,count <1-1000000>,
direction [any|inbound|outbound],filter <LINE>,hex,promiscuous,rate <1-100>,
snap <1-2048>,tcpdump,verbose,write [file|url|tzsp [<IP/TZSP-HOSTNAME>])}

service pm stop {on <DEVICE-NAME>}

service restore analytics-support [<FILE>|<URL>]

service show last-passwd

service signal [abort <PROCESS-NAME>|kill <PROCESS-NAME>]

service start-shell

service trace <PROCESS-NAME> {summary}
```

**Parameters (Privilege Exec Mode)**

*service*

- `service copy tech-support [<FILE>|<URL>]`

| | |
|---|---|
| copy tech-support | Copies extensive system information used for troubleshooting |
| <FILE> | Specify the location to copy file using the following format:<br>• usbX:/path/file |
| <URL> | Specify the location URL to copy file. Both IPv4 andIPv6 address formats are supported.<br>tftp://<hostname\|IPv4/IPv6>[:port]/path/file<br>ftp://<user>:<passwd>@<hostname\|IPv4/IPv6>[:port]/path/file<br>sftp://<user>:<passwd>@<hostname\|IPv4/IPv6>[:port]>/path/file |

- `service copy stats-report [global|rf-domain <DOMAIN-NAME>] (<FILE>|<URL>)`

| | |
|---|---|
| copy stats-report | Copies extensive statistical data useful for troubleshooting |
| [global\|rf-domain <DOMAIN-NAME>] | Identifies the RF Domain to copy statistical data<br>• global – Copies extensive statistical data of all configured RF Domains<br>• rf-domain <DOMAIN-NAME> – Copies extensive statistical data of a specified RF Domain. Specify the domain name. |
| <FILE> | Specify the location to copy file using the following format:<br>• usbX:/path/file |
| <URL> | Specify the location URL to copy file. Both IPv4 andIPv6 address formats are supported.<br>tftp://<hostname\|IPv4/IPv6>[:port]/path/file<br>ftp://<user>:<passwd>@<hostname\|IPv4/IPv6>[:port]/path/file<br>sftp://<user>:<passwd>@<hostname\|IPv4/IPv6>[:port]>/path/file |

- `service clear crash-info {on <DEVICE-NAME>}`

| | |
|---|---|
| clear crash-info | Clears all crash files |
| on <DEVICE-NAME> | Optional. Clears crash files on a specified device. These crash files are core, panic, and AP dump.<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `service database authentication create-user username <USER-NAME> password <PASSWORD>`

| | |
|---|---|
| database | Performs captive-portal/NSight database related actions<br>This command is supported only on the NX95XX, NX9600, and VX9000 platforms. |
| database authentication create-user username <USER-NAME> password <PASSWORD> | Creates the username and password required to access the database. Execute this command on the database host. However, before creating users, on the database, generate the database keyfile. For more information on generating the keyfile, see *database*.<br>• username <USER-NAME> – Configures a database username<br>• password <PASSWORD> – Configures a password for the username created above<br>In the database-policy context, enable authentication and configure this username and password. The database-client-policy also should have the same user credentials configured. For more information on database-policy and database-client-policy, see *database-policy* and *database-client-policy*. |

- `database authentication delete-user username <USER-NAME>`

| | |
|---|---|
| database | Performs database related actions<br>This command is supported only on the NX95XX, NX9600, and VX9000 platforms. |
| database authentication delete-user username <USER-NAME> | Deletes existing users having access rights to the database<br>• username <USER-NAME> – Identifies the user to delete by the username<br>• <USER-NAME> – Specify the user name.<br>Once deleted, the database cannot be accessed using the specified combination of username and password. |

- `service database compact [all|captive-portal|nsight]`

| | |
|---|---|
| database | Performs database related actions<br>**Note:** This command is supported only on the NX95XX, NX9600, and VX9000 platforms. |
| compact [all\| captive-portal\|nsight] | Compacts collections within the database. Each database (captive-portal and NSight) contains one or more collection, where each collection is a set of records. Use this command to make a single compact set of all collections within a database.<br>• all – Compacts collections within all databases (captive-portal and NSight) being maintained<br>• captive-portal – Compacts all collections within the captive portal database only<br>• nsight – Compacts all collections within the NSight database only |

- `service database drop [captive-portal|nsight] collection <COLLECTION-NAME>`

| | |
|---|---|
| database | Performs database related actions<br>**Note:** This command is supported only on the NX95XX, NX9600, and VX9000 platforms. |

| | |
|---|---|
| drop [captive-portal\|nsight] collection <COLLECTION-NAME> | Drops the specified collection from the selected database. Select the database type and specify the collection.<br>• captive-portal – Drops a captive portal database collection<br>• nsight – Drops an NSight database collection<br>The following keyword is common to both the 'captive-portal' and 'NSight' databases:<br>• collection <COLLECTION-NAME> – Drops the collection identified by the <COLLECTION-NAME> parameter.<br>• <COLLECTION-NAME> – Specify the collection name. |

- `service database [maintenance-mode|primary-stepdown|remove-all-files|start-shell]`

| | |
|---|---|
| database | Performs database related actions<br>**Note:** This command is supported only on the NX95XX, NX9600, and VX9000 platforms. |
| maintenance-mode | Places the database server in the maintenance mode |
| primary-stepdown | Requests the primary replica-set to step down. For more information on replica-sets and its creation, see *database-policy*. |
| remove-all-files | Removes all database-server related files (captive-portal and NSight). Use in a scenario where complete removal of all database related files is necessary, such as when downgrading to 5.8.1 or 5.8.0 version. Extreme caution is recommended when using this command. |
| start-shell | Starts the database shell |

- `service database replica-set add member [<IP>|<FQDN>] [arbiter|priority <0-255>]`

| | |
|---|---|
| database | Performs database related actions<br>**Note:** This command is supported only on the NX95XX, NX9600, and VX9000 platforms. |
| replica-set | Adds members to the database replica set. A replica set is a group of devices running the database instances that maintain the same data set. Replica sets provide redundancy and high availability, and are the basis for all production deployments. The replica set can contain a maximum of fifty (50) members, with each member (with the exception of the arbiter) hosting an instance of the database. For more information on creating replica sets, see *database-policy*. |
| add member [<IP>\|<FQDN>] | Adds members to the database replica set<br>• <IP> – Identifies the member by its IP address. Specify the member's IP address.<br>• <FQDN> – Identifies the member by its *Fully Qualified Domain Name* (FQDN). Specify the member's FQDN address.<br>**Note:** Ensure that the identified members have the database instance running prior to being added to the replica set. |

| | |
|---|---|
| [arbiter\|<br>priority <0-255>] | After identifying the new member, optionally specify if the member is the arbiter or not. If not the arbiter, specify the member's priority value.<br>• arbiter – Identifies the new member as the arbiter. The arbiter does not maintain a data set and is added to the replica set to facilitate the election of the fall-back primary member. It provides that one extra vote required in the election of the primary member.<br>• priority <0-255> – Identifies the new member as not being the arbiter and configures its priority value.<br>  • <0-255> – Specify the priority value from 0 - 255. Not applicable for the arbiter.<br>The priority value determines the member's position within the replica set as primary or secondary. It also helps in electing the fall-back primary member in the eventuality of the current primary member being unreachable.<br>All identified members should have the database instances running prior to being added to the replica set. |

- `service database replica-set delete member [<IP>|<FQDN>]`

| | |
|---|---|
| database | Performs database related actions<br>**Note:** This command is supported only on the NX95XX, NX9600, and VX9000 platforms. |
| replica-set | Allows deletion of members in a database replica set. For each database a single three-member replica-set can be created and maintained. For more information on creating replica sets, see *database-policy*. |
| delete member [<IP>\|<FQDN>] | Deletes members from an existing database replica set<br>• <IP> – Identifies the member by its IP address. Specify the member's IP address.<br>• <FQDN> – Identifies the member by its FQDN. Specify the member's FQDN address. |

- `service database server [restart|start|stop]`

| | |
|---|---|
| database | Performs database related actions<br>**Note:** This command is supported only on the NX95XX, NX9600, and VX9000 platforms. |
| server [restart\|start\|stop] | Performs the following actions on the database server:<br>• restart – Restarts the server<br>• start – Starts the server<br>• stop – Stops the server |

- `service delete sessions <SESSION-COOKIES>`

| | |
|---|---|
| delete sessions <SESSION-COOKIES> | Deletes session cookies<br>• <SESSION-COOKIES> – Provide a list of cookies to delete. |

- `service mint [clear [lsp-dp|mlcp]|debug-log [flash-and-syslog|flash-only]|expire [lsp|spf]|flood [csnp|lsp]]`

| | |
|---|---|
| mint | Enables MiNT protocol management (clears LSP database, enables debug logging, enables running silence, etc.) |
| clear [lsp-dp\|mlcp] | Clears LSP database and *MiNT Link Control Protocol* (MLCP) links<br>• lsp-dp – Clears MiNT *Label Switched Path* (LSP) database<br>• mlcp – Clears MLCP links |

| | |
|---|---|
| debug-log [flash-and-syslog\| flash-only] | Enables debug message logging<br>• flash-and-syslog – Logs debug messages to the flash and syslog files<br>• flash-only – Logs debug messages to the flash file only |
| expire [lsp\|spf] | Forces expiration of LSP and recalculation of *Shortest Path First* (SPF)<br>• lsp – Forces expiration of LSP<br>• spf – Forces recalculation of SPF |
| flood [csnp\|lsp] | Floods control packets<br>• csnp – Floods our *Complete Sequence Number Packets* (CSNP)<br>• lsp – Floods our LSP |

- `service pm stop` *`{on <DEVICE-NAME>}`*

| | |
|---|---|
| pm | Stops the *Process Monitor* (PM) |
| stop | Stop the PM from monitoring all daemons |
| on <DEVICE-NAME> | Optional. Stops the PM on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `service pktcap on [bridge|deny|drop|ext-vlan|rim|router|vpn|wireless]` *`{(acl-name <ACL>,count <1-1000000>,direction [any|inbound|outbound],filter,hex, rate <1-100>,snap <1-2048>,tcpdump,verbose,write [file|url|tzsp <IP/TZSP-HOSTNAME>])}`*

| | |
|---|---|
| pktcap on | Captures data packets crossing at a specified location<br>• on – Defines the packet capture location |
| bridge | Captures packets transiting through the Ethernet bridge |
| deny | Captures packets denied by an *Access Control List* (ACL) |
| drop | Captures packets at the drop locations |
| ext-vlan | Captures packets forwarded to or from an extended VLAN |
| rim | Captures packets at the *Radio Interface Module* (RIM) |
| router | Captures packets transiting through an IP router |
| vpn | Captures packets forwarded to or from a VPN link |
| wireless | Captures packets forwarded to or from a wireless device |
| acl-name <ACL> | Optional. Specify the ACL that matches the acl-name for the 'deny' location |
| count <1-1000000> | Optional. Limits the captured packet count. Specify a value from 1 -1000000. |
| direction [any\|inbound\| outbound] | Optional. Changes the packet direction with respect to a device. The direction can be set as any, inbound, or outbound. |

| | |
|---|---|
| filter [<LINE>\|arp\|capwap\|cdp\|dot11\|dropreason\|dst\|ether\|failed\|host\|icmp\|icmp6\|igmp\|ip\|ipv6\|l2\|l3\|l4\|lldp\|mint\|net\|not\|port\|priority\|radio\|rssi\|src\|stp\|tcp\|tcp6\|udp\|udp6\|vlan\|wlan] | Optional. Filters packets based on the option selected (must be used as a last option)<br>The filter options are:<br>• <LINE> – Defines user defined packet capture filter<br>• arp – Matches ARP packets<br>• capwap – Matches CAPWAP packets<br>• cdp – Matches CDP packets<br>• dot11 – Matches 802.11 packets<br>• dropreason – Matches packet drop reason<br>• dst – Matches IP destination<br>• ether – Matches Ethernet packets<br>• failed – Matches failed 802.11 transmitted frames<br>• host – Matches host destination<br>• icmp – Matches ICMP packets<br>• icmp6 – Matches ICMPv6 frames<br>• ip – Matches IPV4 packets<br>• ipv6 – Matches IPV6 packets<br>• l2 – Matches L2 header<br>• l3 – Matches L3 header<br>• l4 – Matches L4 header<br>• mint – Matches MiNT packets<br>• lldp – Matches LLDP packets<br>• net – Matches IP in subnet<br>• not – Filters out any packet that matches the filter criteria (For example, if not TCP is used, all tcp packets are filtered out)<br>• port – Matches TCP or UDP port<br>• priority – Matches packet priority<br>• radio – Matches radio<br>• rssi – Matches *Received Signal Strength Indication* (RSSI) of received radio signals<br>• src – Matches IP source<br>• stp – Matches STP packets<br>• tcp – Matches TCP packets<br>• tcp6 – Matches TCP over IPv6 packets<br>• udp – Matches UDP packets<br>• udp6 – Matches UDP over IPv6 packets<br>• vlan – Matches VLAN<br>• wlan – Matches WLAN |
| hex | Optional. Provides binary output of the captured packets |
| rate <1-100> | Optional. Specifies the packet capture rate<br>• <1-100> – Specify a value from 1 - 100 seconds. |
| snap <1-2048> | Optional. Captures the data length<br>• <1-2048> – Specify a value from 1 - 2048 characters. |
| tcpdump | Optional. Decodes tcpdump. The tcpdump analyzes network behavior, performance, and infrastructure. It also analyzes applications that generate or receive traffic. |

| | |
|---|---|
| verbose | Optional. Displays full packet body |
| write | Captures packets to a specified file. Specify the location to capture file:<br>FILE – flash:/path/file<br>usbX:/path/file<br>vram:startup-config<br>URL – Specify the location URL to capture file. Both IPv4 and IPv6 address formats are supported.<br>tftp://<hostname\|IPv4/IPv6>[:port]/path/file<br>ftp://<user>:<passwd>@<hostname\|IPv4/IPv6>[:port]/path/file<br>sftp://<user>@<hostname\|IPv4/IPv6>[:port]>/path/file<br>tzsp – *Tazman Sniffer Protocol* (TZSP) host. Specify the TZSP host's IP address or hostname. |

- `service pktcap on radio [<1-1024>|all] {(acl-name <ACL>,count <1-1000000>, direction [any|inbound|outbound],filter <LINE>,hex,promiscuous,rate <1-100>,snap <1-2048>,tcpdump,verbose,write [file|url|tzsp <IP/TZSP-HOSTNAME>])}`

| | |
|---|---|
| pktcap on radio | Captures data packets on a radio (802.11) |
| <1-1024> | Captures data packets on a specified radio<br>• <1-1024> – specify the radio index from 1 - 1024. |
| all | Captures data packets on all radios |
| acl-name <ACL> | Optional. Specify the ACL that matches the ACL name for the 'deny' location |
| count <1-1000000> | Optional. Sets a specified number of packets to capture<br>• <1-1000000> – Specify a value from 1 - 1000000. |
| direction [any\|inbound\| outbound] | Optional. Changes the packet direction with respect to a device. The direction can be set as any, inbound, or outbound. |
| filter <LINE> | Optional. Filters packets based on the option selected (must be used as a last option)<br>• <LINE> – Define a packet capture filter or select any one of the available options. |
| hex | Optional. Provides binary output of the captured packets |
| rate <1-100> | Optional. Specifies the packet capture rate<br>• <1-100> – Specify a value from 1 - 100 seconds. |
| snap <1-2048> | Optional. Captures the data length<br>• <1-2048> – Specify a value from 1 - 2048 characters. |
| tcpdump | Optional. Decodes the TCP dump |
| verbose | Optional. Provides verbose output |

| | |
|---|---|
| write | Captures packets to a specified file. Specify the location to capture file:<br>FILE – flash:/path/file<br>usbX:/path/file<br>nvram:startup-config<br>URL – Specify the location URL to capture file. Both IPv4 and IPv6 address formats are supported.<br>tftp://<hostname\|IPv4/IPv6>[:port]/path/file<br>ftp://<user>:<passwd>@<hostname\|IPv4/IPv6>[:port]/path/file<br>sftp://<user>@<hostname\|IPv4/IPv6>[:port]>/path/file<br>tzsp – The TZSP host. Specify the TZSP host's IP address or hostname. |

- `service pktcap on interface [<INTERFACE>|ge <1-4>|me|port-channel <1-2>|vlan <1-4094>] {(acl-name <ACL>,count <1-1000000>,direction [any|inbound|outbound], filter <LINE>,hex,rate <1-100>,snap <1-2048>,tcpdump,verbose,write [file|url|tzsp <IP/TZSP-HOSTNAME>])}`

| | |
|---|---|
| pktcap on | Captures data packets at a specified interface<br>• on – Specify the capture location. |
| interface [<INTERFACE>\| ge <1-4>\|me1\| port-channel <1-2>\| vlan <1-4094>] | Captures packets at a specified interface. The options are:<br>• <INTERFACE> – Specify the interface name.<br>• ge <1-4> – Selects a GigabitEthernet interface index from 1 - 4<br>• me1 – Selects the FastEthernet interface<br>• port-channel <1-2> – Selects a port-channel interface index from 1- 2<br>• vlan <1-4094> – Selects a VLAN ID from 1 - 4094 |
| acl-name <ACL> | Optional. Specify the ACL that matches the ACL name for the 'deny' location |
| count <1-1000000> | Optional. Sets a specified number of packets to capture<br>• <1-1000000> – Specify a value from 1 - 1000000. |
| direction [any\|inbound\| outbound] | Optional. Changes the packet direction with respect to a device. The direction can be set as any, inbound, or outbound. |
| filter <LINE> | Optional. Filters packets based on the option selected (must be used as a last option)<br>• <LINE> – Define a packet capture filter or select any one of the available options. |
| hex | Optional. Provides binary output of the captured packets |
| rate <1-100> | Optional. Specifies the packet capture rate<br>• <1-100> – Specify a value from 1 - 100 seconds. |
| snap <1-2048> | Optional. Captures the data length<br>• <1-2048> – Specify a value from 1 - 2048 characters. |
| tcpdump | Optional. Decodes the TCP dump |
| verbose | Optional. Provides verbose output |

| | |
|---|---|
| write | Captures packets to a specified file. Specify the location to capture file:<br>FILE – flash:/path/file<br>usbX:/path/file<br>nvram:startup-config<br>URL – Specify the location URL to capture file. Both IPv4 and IPv6 address formats are supported.<br>tftp://<hostname\|IPv4/IPv6>[:port]/path/file<br>ftp://<user>:<passwd>@<hostname\|IPv4/IPv6>[:port]/path/file<br>sftp://<user>@<hostname\|IPv4/IPv6>[:port]>/path/file<br>tzsp – The TZSP host. Specify the TZSP host's IP address or hostname. |

- `service show last-passwd`

| | |
|---|---|
| show | Displays running system statistics based on the parameters passed |
| last-passwd | Displays the last password used to enter shell |

- `service signal [abort <PROCESS-NAME>|kill <PROCESS-NAME>]`

| | |
|---|---|
| signal | Sends a signal to a process<br>• tech-support – Copies extensive system information useful for troubleshooting |
| abort | Sends an abort signal to a process, and forces it to dump to core<br>• <PROCESS-NAME> – Specify the process name. |
| kill | Sends a kill signal to a process, and forces it to terminate without a core<br>• <PROCESS-NAME> – Specify the process name. |

- `service start-shell`

| | |
|---|---|
| start-shell | Provides shell access |

- `service trace <PROCESS-NAME> {summary}`

| | |
|---|---|
| trace | Traces a process for system calls and signals |
| <PROCESS-NAME> | Specifies the process name |
| summary | Optional. Generates summary report of the specified process |

**Syntax (Privilege Exec Mode: NX9500 and NX9510)**

*service*

The following service commands are specific to the NX9500 and NX9510 series service platforms:

`service copy analytics-support [<FILE>|<URL>]`

**Parameters (Privilege Exec Mode: NX9500 and NX9510)**

- `service copy analytics-support [<FILE>|<URL>]`

| | |
|---|---|
| copy analytics-support | Enables copying of analytics information to a specified. Use one of the following options to specify the file:<br>This information is useful to troubleshoot issues by the Technical Support team. |
| <FILE> | Specify the file name and location using one of the following formats:<br>usb1:/path/file<br>usb2:/path/file |

| | |
|---|---|
| <URL> | Specify the location URL to copy file. Both IPv4 and IPv6 formats are supported.<br>tftp://<hostname\|IPv4/IPv6>[:port]/path/file<br>ftp://<user>:<passwd>@<hostname\|IPv4/IPv6>[:port]/path/file<br>sftp://<user>:<passwd>@<hostname\|IPv4/IPv6>[:port]>/path/file |

**Usage Guidelines**

The NX9500 and NX9510 model service platforms (NOC) provide granular and robust analytic reporting for a RFS4000 or RFS6000 device managed network. The data analyzed is collected at intervals specified by the administrator.

To enable data analytics, procure and apply a separate hot spare analytics license at the NOC. The license restricts the number of access point streams processed at the NOC or forwarded to partner systems for further processing. The analytics feature can be turned on at select APs by enabling them in configuration. This way the customer can enable analytics on a select set of APs and not the entire system as long as the number of APs on which it is enabled is less than or equal to the total number of AP analytics licenses available at the NOC controller.

In an NOC managed network, the analytics engine parses and processes Smart RF events as they are received. The analytics engine parses the new channel and power information from the Smart RF event, as opposed to retrieving the event from the devices themselves.

**Syntax (Global Config Mode)**

*service*

```
service [set|show cli]

service set [command-history <10-300>|upgrade-history <10-100>|reboot-history <10-
100>|virtual-machine-history <10-200>] {on <DEVICE-NAME>}

service show cli
```

**Parameters (Global Config Mode)**

```
• service set [command-history <10-300>|upgrade-history <10-100>|reboot-history
<10-100>|virtual-machine-history <10-200>] {on <DEVICE-NAME>}
```

| | |
|---|---|
| set | Sets the size of history files |
| command-history <10-300> | Sets the size of the command history file<br>• <10-300> – Specify a value from 10 - 300. The default is 200. |
| upgrade-history <10-100> | Sets the size of the upgrade history file<br>• <10-100> – Specify a value from 10 - 100. The default is 50. |
| reboot-history <10-100> | Sets the size of the reboot history file<br>• <10-100> – Specify a value from 10 - 100. The default is 50. |
| virtual-machine-history <10-200> | Sets the size of the virtual-machine history file<br>• <10-200> – Specify a value from 10 - 200. The default is 100.<br>This command is applicable only to the NX9500 and NX9510 series service platforms. Use the *no > service > set > virtual-machine-history > {on <DEVICE-NAME>}* command to revert the history file size to 100. |
| on <DEVICE-NAME> | Optional. Sets the size of history files on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- service show cli

| | |
|---|---|
| show cli | Displays running system configuration details<br>• cli – Displays the CLI tree of the current mode |

**Example**

```
rfs6000-81742D>service show cli
Command mode:  +-do
+-help [help]
  +-search
    +-WORD [help search WORD (|detailed|only-show|skip-show|skip-no)]
      +-detailed [help search WORD (|detailed|only-show|skip-show|skip-no)]
      +-only-show [help search WORD (|detailed|only-show|skip-show|skip-no)]
      +-skip-show [help search WORD (|detailed|only-show|skip-show|skip-no)]
      +-skip-no [help search WORD (|detailed|only-show|skip-show|skip-no)]
+-show
  +-commands [show commands]
  +-adoption
    +-log
      +-adoptee [show adoption log adoptee(|on DEVICE-NAME)]
        +-on
          +-DEVICE-NAME [show adoption log adoptee(|on DEVICE-NAME)]
      +-adopter [show adoption log adopter (|mac AA-BB-CC-DD-EE-FF)(|on DEVICE-
NAME)]
        +-mac
          +-AA-BB-CC-DD-EE-FF [show adoption log adopter (|mac AA-BB-CC-DD-EE-
FF)(|on DEVICE-NAME)]
            +-on
            +-DEVICE-NAME [show adoption log adopter (|mac AA-BB-CC-DD-EE-FF)(|on
DEVICE-NAME)]
--More--
rfs6000-81742D>

rfs6000-81742D#service signal abort testprocess
Sending an abort signal to testprocess
rfs6000-81742D#

nx9500-6C8809*#service show crash-info
-------------------------------------------------------------------------------
                CRASH FILE                  SIZE          LAST MODIFIED
-------------------------------------------------------------------------------
  cfgd.log_NX9500_5.9.0.0-014D.error.1     8369     Tue Apr 12 03:54:54 2017
-------------------------------------------------------------------------------
nx9500-6C8809*#

rfs6000-81742D#service show command-history
Configured size of command history is 200

  Date & Time          User      Location           Command
================================================================
Apr 12 09:31:41 2017   admin     192.168.13.10 22      rf-domain test
Apr 11 03:00:56 2017   admin     192.168.13.10 93      reload force
Apr 11 03:00:35 2017   admin     192.168.13.10 93      write memory
Apr 11 03:00:31 2017   admin     192.168.13.10 93      commit
Apr 11 03:00:24 2017   admin     192.168.13.10 93      no cluster name
Apr 10 21:29:50 2017   admin     192.168.13.10 93      commit
Apr 10 21:29:48 2017   admin     192.168.13.10 93      use rf-domain TechPubs
Apr 10 21:29:44 2017   admin     192.168.13.10 93      self
Apr 10 21:29:40 2017   admin     192.168.13.10 93      write memory
Apr 10 21:29:34 2017   admin     192.168.13.10 93      commit
Apr 10 21:29:27 2017   admin     192.168.13.10 93       use license WEBF
Apr 10 21:29:27 2017   admin     192.168.13.10 93       controller-managed
Apr 10 21:29:27 2017   admin     192.168.13.10 93       control-vlan 1

--More--
rfs6000-81742D#
```

```
rfs6000-81742D#service show diag stats

fan 1 (fan 1) current speed: 0 min_speed: 2000 hysteresis: 250
fan 2 (fan 2) current speed: 10320 min_speed: 2000 hysteresis: 250
fan 3 (fan 3) current speed: 10620 min_speed: 2000 hysteresis: 250
fan 4 (fan 4) current speed: 10740 min_speed: 2000 hysteresis: 250

Sensor 1 (upwind of CPU) Temperature 31.0 C
Sensor 2 (CPU die) Temperature 47.0 C
Sensor 3 (left side) Temperature 37.0 C
Sensor 4 (by FPGA) Temperature 31.0 C
Sensor 5 (front right) Temperature 30.0 C
Sensor 6 (front left) Temperature 31.0 C

rfs6000-81742D#

rfs6000-81742D#service show info

7.7M out of 8.0M available for logs.
32.9M out of 34.0M available for history.
20.4M out of 84.0M available for crashinfo.

List of Files:

adopts.log                                1.7K    Apr 12 11:20
anald.log                                 1.1K    Apr 12 11:20
cfgd.log                                  48.8K   Apr 12 12:35
dpd2.log                                  40.1K   Apr 12 12:07
messages.log                              22.4K   Apr 12 12:27
startup.log                               6.0K    Apr 11 09:08
upgrade.log                               60.9K   Apr 12 11:40
vlan-usage.log                            0       Apr 12 12:18
command.history                           10.5K   Apr 12 09:31
reboot.history                            1.1K    Apr 11 09:07
ugrade.history                            116     Apr 11 09:05

Please export these files or delete them for more space.

rfs6000-81742D#

rfs6000-81742D#service show mac-vendor B4-C7-99-6C-88-09
B4-C7-99 : Extreme Networks
rfs6000-81742D#

nx9500-6C8809>service show upgrade-history
Configured size of upgrade history is 50
  Date & Time            Old Version     New Version     Status
 Date & Time           Old Version     New Version     Status
=============================================================================
Apr 11 07:57:33 2017 5.9.0.0-012D 5.9.0.0-014D Successful
Mar 30 15:00:48 2017 5.9.0.0-010D 5.9.0.0-012D Successful
Mar 22 13:35:20 2017 5.9.0.0-009D 5.9.0.0-010D Successful
Mar 22 11:54:25 2017 5.8.6.0-010R 5.9.0.0-009D Successful
Feb 21 08:40:22 2017 5.8.6.0-009R 5.8.6.0-010R Successful
Feb 21 08:22:45 2017 5.8.6.0-009R 5.8.6.0-009R Failure in openssl. Verification
failure.
Feb 15 10:55:00 2017 5.8.6.0-007B 5.8.6.0-009R Successful
Feb 15 10:45:40 2017 5.8.6.0-007B 5.8.6.0-008B Successful
Feb 15 10:45:07 2017 5.8.6.0-007B 5.8.6.0-007B Unable to get update file. ftpget:
unexpected server response to RETR: 550 LatestBuilds/W586/NX9000.img: The system
cannot find the file specified.
Feb 11 12:26:20 2017 5.8.6.0-007B 5.8.6.0-008B Successful
Feb 11 12:21:04 2017 5.8.6.0-007B 5.8.6.0-008B Successful
Feb 11 12:20:34 2017 5.8.6.0-007B 5.8.6.0-007B Unable to get update file. ftpget:
bad address '1921.68.13.10'
---More--
nx9500-6C8809>
```

```
rfs6000-81742Drfs6000-81742D#service show wireless reference reason-codes
 CODE  DESCRIPTION
  0    Success
  1    Unspecified Reason
  2    Previous authentication no longer valid
  3    Deauth because sending STA is leaving IBSS or ESS
  4    Disassoc due to inactivity
  5    Disassoc because AP is unable to handle all currently assoc STA
  6    Class 2 frame received from non-authenticated STA
  7    Class 3 frame received from nonassociated STA
  8    Disassoc because STA is leaving BSS
  9    STA requesting association is not authentication with corresponding STA
 10    Disassoc because info in the power capability elem is unacceptable
--More--
rfs6000-81742D#

rfs6000-81742D#service show wireless reference status-codes
 CODE  DESCRIPTION
  0   Successful
  1   Unspecified failure
 2-9  Reserved
 10   Cannot support all requested capabilities in the Capability Information field
 11   Reassociation denied due to inability to confirm that association exists
 12   Association denied due to reason outside the scope of this standard
 13   Responding STA does not support the specified authentication algorithm
 14   Received an auth frame with authentication transaction seq number out of
expected sequence
 15   Authentication rejected because of challenge failure
--More--
rfs6000-81742D#

nx9500-6C8809>service show wireless config-internal
! Startup-Config-Playback Completed: Yes
no debug wireless
country-code in
nx9500-6C8809>

nx9500-6C8809>service show wireless log-internal
08:16:45.901: wlan:Starting credcache checkup/sync (credcache.c:1536)
07:56:41.900: wlan:Starting credcache checkup/sync (credcache.c:1536)
07:36:40.899: wlan:Starting credcache checkup/sync (credcache.c:1536)
07:16:32.898: wlan:Starting credcache checkup/sync (credcache.c:1536)
06:56:31.898: wlan:Starting credcache checkup/sync (credcache.c:1536)
06:36:24.897: wlan:Starting credcache checkup/sync (credcache.c:1536)
06:16:22.897: wlan:Starting credcache checkup/sync (credcache.c:1536)
05:56:18.896: wlan:Starting credcache checkup/sync (credcache.c:1536)
05:16:09.895: wlan:Starting credcache checkup/sync (credcache.c:1536)
04:56:01.894: wlan:Starting credcache checkup/sync (credcache.c:1536)
04:35:58.893: wlan:Starting credcache checkup/sync (credcache.c:1536)
04:34:41.63: config:commit done in cfgd (config.c:5382)
04:15:55.893: wlan:Starting credcache checkup/sync (credcache.c:1536)
03:55:54.891: wlan:Starting credcache checkup/sync (credcache.c:1536)
03:20:30.397: config:commit done in cfgd (config.c:5382)
03:19:50.188: config:commit done in cfgd (config.c:5382)
--More--
nx9500-6C8809>

nx9500-6C8809#service show xpath-history
*************************************************************************
*************************************************************
*     DATE&TIME     *      USER     *                  XPATH
* DURATION(MS)*
*************************************************************************
*************************************************************
* Wed Apr 12 12:45:28 2017 * system @ rfs6000-81742D * wing-stats/device/B4-C7-99-
6C-88-09/_internal/feature_license_request * 0           *
```

```
* Wed Apr 12 12:45:24 2017 * system @ rfs6000-81742D * wing-stats/device/B4-C7-99-
6C-88-09/_internal/feature_license_request * 0           *
* Wed Apr 12 12:45:13 2017 * system @ rfs6000-81742D * wing-stats/device/B4-C7-99-
6C-88-09/_internal/feature_license_request * 0           *
* Wed Apr 12 12:45:02 2017 * system                  * wing-stats/device/B4-C7-99-
6C-88-09/_internal/feature_license_request * 0           *
--More--
nx9500-6C8809#
```

The following example shows the *service > show > virtual-machine-history* output on a NX9500 service platform:

```
nx9500-6C874D>service show virtual-machine-history
Configured size of virtual machine history is 100

  Date & Time        Virtual Machine  Event
==================================================
Jan 16 05:39:46 2017  Domain-0         autostart
Jan 10 03:47:09 2017  Domain-0         autostart
Jan 02 05:53:48 2017  Domain-0         autostart
Dec 27 10:52:59 2016  Domain-0         autostart
Oct 14 05:56:14 2016  Domain-0         autostart
Oct 14 03:01:48 2016  Domain-0         autostart
Oct 12 04:11:52 2016  Domain-0         autostart
Sep 30 04:41:08 2016  Domain-0         autostart
--More--
nx9500-6C874D>

rfs4000-229D58#service show fib6
--------------------------------------------------------------------------------
Route Table ID : 254
  ::1/128
   Next Hop: ::           Interface: lo           Route Type: ROUTE_TYPE_CONNECT
Route Status: ROUTE_STATUS_KERNEL  Metric: 0 Distance: 0
  fe80::/64
   Next Hop: ::          Interface: vlan2         Route Type: ROUTE_TYPE_CONNECT
Route Status: ROUTE_STATUS_KERNEL  Metric: 256 Distance: 0
  2001::/64
   Next Hop: 2001::6       Interface:             Route Type: ROUTE_TYPE_STATIC
Route Status: ROUTE_STATUS_PENDING Metric: 256 Distance: 1
rfs4000-229D58#
```

Examples for the *service > wireless > meshpoint* command.

The following example displays meshpoint modules:

```
ROOT1-ap81xx-71174C#service wireless meshpoint zl mesh_root on ROOT1-ap81xx-71174C
       | SUBZONE
       | 0    1    2    3    4    5    6    7
-------+-----------------------------------------
  ZONE |
       | GEN  TX   RX   BEA  TXF
 2-LLC | 0    0    0    0    0
       | GEN  TX   RX   NBR  LQM  LSA
 3-ND  | 0    0    0    0    0    0
       | GEN
 4-ORL | 0
       | GEN  TX   RX   HEL  PRO
 5-LQ  | 0    0    0    0    0
       | GEN
 6-PS  | 0
       | GEN  ROOT NBR  REC
 7-RS  | 0    0    0    0
       | GEN
 8-IA  | 0
       | GEN  SET  GET
11-MGT | 0    0    0
       | GEN  RX   TX   R0   LMST LSUP LKEY KEY
13-LSA | 0    0    0    0    0    0    0    0
```

```
        | GEN  SCAN TRIG
14-ACS  | 0    0    0
        | GEN
15-EAP  | 0
        | GEN
16-L2P  | 0

ROOT1-ap81xx-71174C#
```

In the preceding example,

- The meshpoint name is mesh_root
- The device on which the command is executed is ROOT1-ap81xx-71174C
- The vertical ZONE column represents meshpoint modules. For example, 3-ND presents the Neighbor Discovery module.
- The SUBZONE 0 to 7 represents the available processes for each of the zonal modules.
- Debugging is disabled for all modules for the mesh-root meshpoint. A value of 0 (Zero) represents debugging disabled.

To enable meshpoint module debugging, specify the module number and the process number separated by a period (.). And then specify the debugging level from 0 - 7.

```
ROOT1-ap81xx-71174C#service wireless meshpoint zl mesh_root on ROOT1-ap81xx-71174C
3.2 7
```

In the preceding command,

- The meshpoint module number provided is 3 (ND)
- The process number provided is 2 (RX - Received signals from neighbors)
- The debugging level provided is 7 (highest level - warning)

```
ROOT1-ap81xx-71174C#service wireless meshpoint zl mesh_root on ROOT1-ap81xx-71174C
        | SUBZONE
        | 0    1    2    3    4    5    6    7
--------+-----------------------------------------
  ZONE  |
        | GEN  TX   RX   BEA  TXF
 2-LLC  | 0    0    0    0    0
        | GEN  TX   RX   NBR  LQM  LSA
 3-ND   | 0    0    7(D) 0    0    0
        | GEN
 4-ORL  | 0
        | GEN  TX   RX   HEL  PRO
 5-LQ   | 0    0    0    0    0
        | GEN
 6-PS   | 0
        | GEN  ROOT NBR  REC
 7-RS   | 0    0    0    0
        | GEN
 8-IA   | 0
        | GEN  SET  GET
11-MGT  | 0    0    0
        | GEN  RX   TX   R0   LMST LSUP LKEY KEY
13-LSA  | 0    0    0    0    0    0    0    0
        | GEN  SCAN TRIG
14-ACS  | 0    0    0
        | GEN
15-EAP  | 0
        | GEN
16-L2P  | 0

ROOT1-ap81xx-71174C#
```

In the preceding example, level 7 debugging has been enabled only for the ND module's received signals. Note that debugging for all other modules and processes are still disabled.

To disable debugging for all modules, specify 0 (zero) in the command. For example:

```
ROOT1-ap81xx-71174C#service wireless meshpoint zl mesh_root on ROOT1-ap81xx-71174C
0
```

To enable debugging for all modules, specify the debugging level number. For example:

```
ROOT1-ap81xx-71174C#service wireless meshpoint zl mesh_root on ROOT1-ap81xx-71174C
5

ROOT1-ap81xx-71174C#service wireless meshpoint zl mesh_root on ROOT1-ap81xx-71174C
       | SUBZONE
       | 0    1    2    3    4    5    6    7
-------+---------------------------------------
  ZONE |
       | GEN  TX   RX   BEA  TXF
 2-LLC | 5(N) 5(N) 5(N) 5(N) 5(N)
       | GEN  TX   RX   NBR  LQM  LSA
 3-ND  | 5(N) 5(N) 5(N) 5(N) 5(N) 5(N)
       | GEN
 4-ORL | 5(N)
       | GEN  TX   RX   HEL  PRO
 5-LQ  | 5(N) 5(N) 5(N) 5(N) 5(N)
       | GEN
 6-PS  | 5(N)
       | GEN  ROOT NBR  REC
 7-RS  | 5(N) 5(N) 5(N) 5(N)
       | GEN
 8-IA  | 5(N)
       | GEN  SET  GET
11-MGT | 5(N) 5(N) 5(N)
       | GEN  RX   TX   R0   LMST LSUP LKEY KEY
13-LSA | 5(N) 5(N) 5(N) 5(N) 5(N) 5(N) 5(N) 5(N)
       | GEN  SCAN TRIG
14-ACS | 5(N) 5(N) 5(N)
       | GEN
15-EAP | 5(N)
       | GEN
16-L2P | 5(N)

ROOT1-ap81xx-71174C#

rfs4000-1BE644#service show ssh-authorized-keys
'extreme@extreme-quadcore'
rfs4000-1BE644#

rfs4000-1BE644#service load-ssh-autorized-keys "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDPERY9aTibRYlFMnERTYP2iyylJ00YElxjUElY7Zm9Ky2yeSmg
15UKerJ+IP161Gdm0AoEfXyeheRntK+Z6NWHa341RWJ0UrQMcp7hSEE5jbDpLKJOuEoW22Ag45BZzMV7
EnM7lHowboNsQhSzX5uBBlVViWlBxBqDroX4BcuB/
CFugezHTt95UQ2ZRUfHvePS6jQdOArf1alwk0Slcsz4HNSl5KDutJ4VY+6vRvlf5Gy/
3GNehMwNsmsRKK4UVKV5RpuuKIjkbZE+goPFAKYVPNmZngjaOyDfvNGE7JIwmYlti/
AId6tv2zAbM4qSomWAgUOO0hkXS9m4m74FnHPr extreme@extreme-quadcore"
Successfully added the ssh key
rfs4000-1BE644#

rfs4000-1BE644#no service load-ssh-autorized-keys rfs4000-1BE644
Successfully removed the ssh key
rfs4000-1BE644#

nx9500-6C8809#service show diag fds
Process  open fds
cfgd      86
nx9500-6C8809#

nx9500-6C8809#service show diag pkts
Date: 11-4-2016, Time: 8:41:08.501033, Len: 64, 802.3, Proto: 0x8783, Vlan: 1,
Priority: 0, Ingress: ge1, vlan1
```

```
Loop reason: Unknown(540)
TRUNCATED BB-7C-4D-80-C2-AC > 10-01-00-D2-68-99 at 64 bytes


Date: 11-4-2016, Time: 8:41:08.707631, Len: 64, 802.3, Proto: 0x8783, Vlan: 1,
Priority: 0, Ingress: ge1, vlan1
Loop reason: Unknown(540)
TRUNCATED BB-7C-4D-80-C2-AC > 10-01-00-D2-68-99 at 64 bytes


Date: 11-4-2016, Time: 8:41:08.830963, Len: 64, 802.3, Proto: 0x8783, Vlan: 1,
Priority: 0, Ingress: ge1, vlan1
Loop reason: Unknown(540)
TRUNCATED BB-7C-4D-83-30-A4 > 10-01-00-42-68-99 at 64 bytes

--More--
nx9500-6C8809#

nx9500-6C8809#service clear diag pkts
nx9500-6C8809#service show diag pkts
nx9500-6C8809#

nx9500-6C8809#service show diag psu
PSU1 (upper):
 status unplugged
PSU2 (lower):
 status normal
nx9500-6C8809#
```

The following examples show the purging of users from the guest-registration database:

```
nx7500-112233#service guest-registration delete ?
  all                 Delete all users
  email               Email address
  group               Group
  mac                 MAC address
  mobile              Mobile phone number
  name                Full name
  offline-for         Specify minimum amount of time offline
  otp-incomplete-for  Specify minimum amount of time registration with
                      one-time-passcode incomplete
  social              Social site used to log in
  wlan                Wireless LAN

nx7500-112233#
```

Purges users belonging to a specified RADIUS group.

```
nx7500-112233#service guest-registration delete group mac_reg_gr1
delete user status: delete users matching a group will take time, please wait
nx7500-112233#
```

Purges users using social-site (Facebook or Google) credentials to login.

```
nx7500-112233#service guest-registration delete social facebook
delete user status: delete users matching a social category will take time,
please wait
nx7500-112233#
```

Purges users inactive for a specified time period.

```
nx7500-112233#service guest-registration delete offline-for days 5
delete user status: Deleting users offline for minimum 5 days. This will take
time, please wait
nx7500-112233#
```

Purges users who have failed to complete registration using the *one-time-passcode* (OTP) within a specified time period.

```
nx7500-112233#service guest-registration delete otp-incomplete-for days 5
```

```
delete user status: Deleting registration with one-time-passcode incomplete for
minimum 5 days. This will take time, please wait
nx7500-112233#
```

The following example displays IP ACLs to WLAN mapping summary on the 'TechPubs' RF Domain:

```
nx9500-6C8809#service show ip-access-list wlan TechPubs status
Reporting Device: ap7131-99BB7C - success
Reporting Device: ap7532-80C2AC - success
Reporting Device: ap7562-84A224 - success
Reporting Device: nx9500-6C8809 - success
Reporting Device: ap8132-74B45C - success
Total reporting devices: 5
nx9500-6C8809#
```

Consider an RF Domain (name guest-domain) with 3 APs adopted to a controller. The CLI output for the *service > show > ip-access-list* command in this set up varies for different scenarios, as shown in the following examples:

Scenario 1: Executing the command on a device (access point).

```
AP01#service show ip-access-list wlan status
Reporting Device: AP01 - fail
WLAN: XPO-Guest-PSK
  use ip-access-list in guest_access_inbound : fail
Total reporting devices: 1
AP01#
AP01#service show ip-access-list wlan status detail
================================================================================
==
Reporting Device: AP01
--------------------------------------------------------------------------------
--
WLAN: XPO-Guest-PSK
  use ip-access-list in guest_access_inbound : fail
  use ip-access-list out BC-MC-CONTROL : success
--------------------------------------------------------------------------------
--
WLAN: PartnerNet
  use ip-access-list in default : success
  use ip-access-list out default : success
--------------------------------------------------------------------------------
--
Total reporting devices: 1
AP01#
```

Scenario 2: IP ACL to WLAN mapping is successful for all APs in a specified RF Domain.

```
SW01#service show ip-access-list wlan status on guest-domain
Reporting Device: AP01 - success
Reporting Device: AP02 - success
Reporting Device: AP03 - success
Total reporting devices: 3
SW01#
```

Scenario 3: IP ACL has failed in dataplane due to unknown reasons.

```
SW01#service show ip-access-list wlan status on guest-domain
Reporting Device: AP01 - fail
WLAN: XPO-Guest-PSK
  use ip-access-list in guest_access_inbound : fail
Reporting Device: AP02 - success
Reporting Device: AP03 - success
Total reporting devices: 3

SW01#service show ip-access-list wlan status detail on guest-domain
================================================================================
==
Reporting Device: AP01
--------------------------------------------------------------------------------
--
```

```
WLAN: XPO-Guest-PSK
  use ip-access-list in guest_access_inbound : fail
  use ip-access-list out BC-MC-CONTROL : success
--------------------------------------------------------------------------------
--
WLAN: PartnerNet
  use ip-access-list in guest_access_inbound : success
  use ip-access-list out BC-MC-CONTROL : success
--------------------------------------------------------------------------------
--

================================================================================
==
Reporting Device: AP02
--------------------------------------------------------------------------------
--
WLAN: PartnerNet
  use ip-access-list in guest_access_inbound : success
  use ip-access-list out BC-MC-CONTROL : success
--------------------------------------------------------------------------------
--

================================================================================
==
Reporting Device: AP03
--------------------------------------------------------------------------------
--
WLAN: PartnerNet
  use ip-access-list in guest_access_inbound : success
  use ip-access-list out BC-MC-CONTROL : success
--------------------------------------------------------------------------------
--
Total reporting devices: 3
SW01#
```

Scenario 4: AP in RF Domain is unreachable or does not support this functionality.

```
SW01#service show ip-access-list wlan status on guest-domain
Reporting Device: AP01 - unreachable
Reporting Device: AP02 - success
Reporting Device: AP03 - success
Total reporting devices: 3
SW01#

SW01#service show ip-access-list wlan status detail on guest-domain

================================================================================
==
Reporting Device: AP01
Timed out waiting for remote device: xpath=wing-stats/device/00-23-68-0B-86-38/
firewall/ip_acl_intf_status/wlan[mac='*']

================================================================================
==
Reporting Device: AP02
--------------------------------------------------------------------------------
--
WLAN: PartnerNet
  use ip-access-list in guest_access_inbound : success
  use ip-access-list out BC-MC-CONTROL : success
--------------------------------------------------------------------------------
--

================================================================================
==
Reporting Device: AP03
--------------------------------------------------------------------------------
--
WLAN: PartnerNet
```

```
  use ip-access-list in guest_access_inbound : success
  use ip-access-list out BC-MC-CONTROL : success
-------------------------------------------------------------------------------
--
Total reporting devices: 3
```

## 5.1.8 show

*Common Commands*

Displays specified system component settings. There are a number of ways to invoke the show command:

- When invoked without any arguments, it displays information about the current context. If the current context contains instances, the show command (usually) displays a list of these instances.
- When invoked with the display parameter, it displays information about that component.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show <PARAMETERS>
```

**Parameters**

- `show <PARAMATERS>`

| | |
|---|---|
| show <PARAMETERS> | The show command displays configuration details based on the configuration mode, in which the command is executed, and the parameters passed. For example, when executed in the AAA policy configuration mode, it displays the logged AAA policy's current settings. The example below shows the configuration details that can be viewed in the Priv Executable mode. |

**Example**

```
nx9500-6C8809#show ?
  adoption                      Adoption related information
  bluetooth                     Bluetooth Configuration/Statistics commands
  bonjour                       Bonjour Gateway related commands
  boot                          Display boot configuration.
  captive-portal                Captive portal commands
  captive-portal-page-upload    Captive portal internal and advanced page upload
  cdp                           Cisco Discovery Protocol
  classify-url                  Query the category of an URL
  clock                         Display system clock
  cluster                       Cluster Protocol
  cmp-factory-certs             Display the CMP certificate status
  commands                      Show command lists
  context                       Information about current context
  critical-resources            Critical Resources
  crypto                        Encryption related commands
  database                      Database
  debug                         Debugging functions
  debugging                     Debugging functions
  device-upgrade                Device Upgrade
  dot1x                         802.1X
  dpi                           Deep Packet Inspection
  eguest                        Registration EGuest process
  environmental-sensor          Display Environmental Sensor Module status
  event-history                 Display event history
  event-system-policy           Display event system policy
  ex3500                        EX3500 device details
  extdev                        External device (T5, Ex3500..)
  file                          Display filesystem information
  file-sync                     File sync between controller and adoptees
  firewall                      Wireless Firewall
```

```
  global                        Global-level information
  gre                           Show l2gre tunnel info
  guest-notification-config     Show guest-notification information
  guest-registration            Guest registration commands
  interface                     Interface Configuration/Statistics commands
  ip                            Internet Protocol (IP)
  ip-access-list                IP ACL
  ipv6                          Internet Protocol version 6 (IPv6)
  ipv6-access-list              IPV6 ACL
  l2tpv3                        L2TPv3 information
  lacp                          LACP commands
  ldap-agent                    LDAP Agent Configuration
  licenses                      Show installed licenses and usage
  lldp                          Link Layer Discovery Protocol
  logging                       Show logging information
  mac-access-list               MAC ACL
  mac-address-table             Display MAC address table
  mac-auth                      MAC authentication
  mac-auth-clients              MAC authenticated clients
  mint                          MiNT protocol
  mirroring                     Show mirroring sessions
  nsight                        Nsight Server Module
  ntp                           Network time protocol
  password-encryption           Pasword encryption
  pppoe-client                  PPP Over Ethernet client
  privilege                     Show current privilege level
  radius                        RADIUS statistics commands
  raid                          Show RAID status
  reload                        Scheduled reload information
  remote-debug                  Show details of remote debug sessions
  rf-domain-manager             Show RF Domain Manager selection details
  role                          Role based firewall
  route-maps                    Display Route Map Statistics
  rtls                          RTLS Statistics
  running-config                Current operating configuration
  session-changes               Configuration changes made in this session
  session-config                This session configuration
  sessions                      Display sessions
  site-config-diff              Difference between site configuration on the NOC
                                and actual site configuration
  slot                          Expansion slots stats
  smart-rf                      Smart-RF Management Commands
  spanning-tree                 Display spanning tree information
  startup-config                Startup configuration
  t5                            Display T5 inventory information
  terminal                      Display terminal configuration parameters
  timezone                      The timezone
  traffic-shape                 Display traffic shaping
  upgrade-status                Display last image upgrade status
  version                       Display software & hardware version
  virtual-machine               Virtual Machine
  vrrp                          VRRP protocol
  web-filter                    Web filter
  what                          Perform global search
  wireless                      Wireless commands
  wwan                          Display wireless WAN Status

nx9500-6C8809#
```

**NOTE:** For more information on the show command, see *Chapter 6, SHOW COMMANDS*.

## 5.1.9 write

*Common Commands*

Writes the system running configuration to memory or terminal

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
write [memory|terminal]
```

**Parameters**

- `write [memory|terminal]`

| | |
|---|---|
| memory | Writes to the *non-volatile* (NV) memory |
| terminal | Writes to the terminal |

**Example**

```
nx9500-6C8809>write memory
[OK]
nx9500-6C8809>
```

# 6 SHOW COMMANDS

Show commands display configuration settings or statistical information. Use this command to view the current running configuration as well as the start-up configuration. The show command also displays the current context's configuration.

This chapter describes the 'show' CLI commands used in the USER EXEC, PRIV EXEC, and GLOBAL CONFIG modes. Commands entered in either USER EXEC mode or PRIV EXEC mode are referred to as EXEC mode commands. If a user or privilege is not specified, the referenced command can be entered in either mode.

This chapter also describes the 'show' commands in the 'GLOBAL CONFIG' mode. The commands can be entered in all three modes, except commands like file, IP access list statistics, MAC access list statistics, and upgrade statistics, which cannot be entered in the USER EXEC mode.

**NOTE:** The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.

# 6.1 show commands

*SHOW COMMANDS*

The following table summarizes show commands:

**Table 6.1** *Show Commands*

| Command | Description | Reference |
|---|---|---|
| *show* | Displays settings for the specified system component | *page 6-5* |
| *adoption* | Displays information related to adoption | *page 6-10* |
| *bluetooth* | Displays Bluetooth radio statistics for RF Domain member access points | *page 6-14* |
| *boot* | Displays a device boot configuration | *page 6-16* |
| *bonjour* | Displays the configured Bonjour services available on local and remote sites | *page 6-17* |
| *captive-portal* | Displays WLAN hotspot functions | *page 6-18* |
| *captive-portal-page-upload* | Displays captive portal page related information | *page 6-20* |
| *cdp* | Displays a *Cisco Discovery Protocol* (CDP) neighbor table | *page 6-22* |
| *classify-url* | Queries a specified global data center or a pre-configured classification server for the category of a specified URL. | *page 6-24* |
| *clock* | Displays the software system clock | *page 6-25* |
| *cluster* | Displays cluster commands | *page 6-26* |
| *cmp-factory-certs* | Displays factory installed CMP certificates | *page 6-28* |
| *commands* | Displays command list | *page 6-29* |
| *context* | Displays information about the current context | *page 6-30* |
| *critical-resources* | Displays critical resource information | *page 6-31* |
| *crypto* | Displays encryption mode information | *page 6-32* |
| *database* | Displays database-related statistics and status | *page 6-35* |
| *device-upgrade* | Displays device firmware upgradation information for devices adopted by a wireless controller or access point | *page 6-37* |
| *dot1x* | Displays dot1x information on interfaces | *page 6-39* |
| *dpi* | Displays statistics for all configured and canned applications | *page 6-41* |
| *eguest* | Displays EGuest server status and EGuest registration statistics | *page 6-44* |
| *environmental-sensor* | Displays environmental sensor's historical data (applicable only to AP8132) | *page 6-45* |
| *event-history* | Displays event history | *page 6-48* |
| *event-system-policy* | Displays event system policy configuration information | *page 6-49* |
| *ex3500* | Displays EX3500-related statistical data | *page 6-50* |
| *extdev* | Displays external device (T5 or EX3500) configuration error history | *page 6-53* |

**Table 6.1** *Show Commands*

| Command | Description | Reference |
|---|---|---|
| *file-sync* | Displays file synchronization settings and status on a controller. The *file-sync* command syncs trustpoint/wireless-bridge certificate between the staging-controller and its adopted access points | *page 6-54* |
| *firewall* | Displays wireless firewall information | *page 6-56* |
| *global* | Displays global information for network devices based on the parameters passed | *page 6-60* |
| *gre* | Displays GRE tunnel related information | *page 6-62* |
| *guest-registration* | Displays guest registration statistics based on the option and time entered | *page 6-63* |
| *interface* | Displays interface status | *page 6-71* |
| *ip* | Displays IP related information | *page 6-75* |
| *ip-access-list* | Displays IP access list statistics | *page 6-82* |
| *ipv6* | Displays IPv6 related information | *page 6-84* |
| *ipv6-access-list* | Displays IPv6 access list statistics | *page 6-88* |
| *l2tpv3* | Displays *Layer 2 Tunnel Protocol Version 3* (L2TPV3) information | *page 6-89* |
| *lacp* | Displays *Link Aggregation Control Protocol* (LACP) related information | *page 6-92* |
| *ldap-agent* | Displays an LDAP agent's join status (join status to a LDAP server domain) | *page 6-95* |
| *licenses* | Displays installed licenses and usage information | *page 6-96* |
| *lldp* | Displays *Link Layer Discovery Protocol* (LLDP) information | *page 6-99* |
| *logging* | Displays logging information | *page 6-100* |
| *mac-access-list* | Displays MAC access list statistics | *page 6-101* |
| *mac-address-table* | Displays MAC address table entries | *page 6-102* |
| *mac-auth* | Displays details of wired ports that have MAC address-based authentication enabled | *page 6-103* |
| *mac-auth-clients* | Displays MAC-authenticated clients based on the parameters passed | *page 6-105* |
| *mint* | Displays MiNT protocol configuration commands | *page 6-107* |
| *nsight* | Displays NSight module related statistics and also displays the database server status (reachable or not) | *page 6-111* |
| *ntp* | Displays *Network Time Protocol* (NTP) information | *page 6-112* |
| *password-encryption* | Displays password encryption status | *page 6-114* |
| *pppoe-client* | Displays *Point to Point Protocol over Ethernet* (PPPoE) client information | *page 6-115* |
| *privilege* | Displays current privilege level information | *page 6-116* |
| *radius* | Displays the amount of access time consumed and the access time remaining for all guest users configured on a RADIUS server | *page 6-117* |
| *reload* | Displays scheduled reload information | *page 6-119* |

**Table 6.1** *Show Commands*

| Command | Description | Reference |
|---|---|---|
| *rf-domain-manager* | Displays RF Domain manager selection details | *page 6-120* |
| *role* | Displays role-based firewall information | *page 6-121* |
| *route-maps* | Display route map statistics | *page 6-122* |
| *rtls* | Displays *Real Time Location Service* (RTLS) statistics of access points | *page 6-123* |
| *running-config* | Displays configuration file contents | *page 6-125* |
| *session-changes* | Displays configuration changes made in this session | *page 6-132* |
| *session-config* | Displays a list of currently active open sessions on the device | *page 6-133* |
| *sessions* | Displays CLI sessions | *page 6-134* |
| *site-config-diff* | Displays the difference between site configuration available on NOC and the actual site configuration | *page 6-135* |
| *smart-rf* | Displays Smart RF management commands | *page 6-136* |
| *spanning-tree* | Displays spanning tree information | *page 6-140* |
| *startup-config* | Displays complete startup configuration script on the console | *page 6-142* |
| *t5* | Displays adopted T5 controller details. This command is applicable only on the RFS4000, RFS6000, NX9500, NX9510, and VX9000. | *page 6-143* |
| *terminal* | Displays terminal configuration parameters | *page 6-151* |
| *timezone* | Displays timezone information for the system and managed devices | *page 6-152* |
| *traffic-shape* | Displays traffic-shaping related configuration details and statistics | *page 6-153* |
| *upgrade-status* | Displays image upgrade status | *page 6-155* |
| *version* | Displays a device's software and hardware version | *page 6-156* |
| *vrrp* | Displays *Virtual Router Redundancy Protocol* (VRRP) protocol details | *page 6-157* |
| *web-filter* | Displays pre-configured, in-built Web filter options available. These options are: category (URL category), category-types, filter-level, etc. This command also displays Web filter statistics and status. | *page 6-159* |
| *what* | Displays details of a specified search phrase | *page 6-161* |
| *wireless* | Displays wireless configuration parameters | *page 6-162* |
| *wwan* | Displays the wireless WAN status | *page 6-185* |
| *virtual-machine* | Displays the *virtual-machine* (VM) configuration, logs, and statistics | *page 6-186* |
| *raid* | Displays *Redundant Array of Independent Disks* (RAID) related information, such as array status, consistency check status, and RAID log. | *page 6-189* |

## 6.1.1 show

*show commands*

The show command displays following information:

- A device's current configuration
- A device's start-up configuration
- A device's current context configuration, such as profiles and policies

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show <PARAMETERS>
```

**Parameters**

- `show <PARAMATERS>`

| | |
|---|---|
| show <PARAMETERS> | The show command displays configuration details based on the configuration mode, in which the command is executed, and the parameters passed. For example, when executed in the AAA policy configuration mode, it displays the logged AAA policy's current settings. The examples below show the configuration parameters that can be viewed in the User Executable, Priv Executable, and Global Configurable modes. |

**Example**

The following examples list the *show* commands in the User Exec, Priv Exec, and Global Config modes:

GLOBAL CONFIG Mode

```
<DEVICE>(config)#show ?
  adoption                    Adoption related information
  bluetooth                   Bluetooth Configuration/Statistics commands
  bonjour                     Bonjour Gateway related commands
  boot                        Display boot configuration.
  captive-portal              Captive portal commands
  captive-portal-page-upload  Captive portal internal and advanced page upload
  cdp                         Cisco Discovery Protocol
  classify-url                Query the category of an URL
  clock                       Display system clock
  cluster                     Cluster Protocol
  cmp-factory-certs           Display the CMP certificate status
  commands                    Show command lists
  context                     Information about current context
  critical-resources          Critical Resources
  crypto                      Encryption related commands
  database                    Database
  debug                       Debugging functions
  debugging                   Debugging functions
  device-upgrade              Device Upgrade
  dot1x                       802.1X
  dpi                         Deep Packet Inspection
  eguest                      ExtremeGuest
  environmental-sensor        Display Environmental Sensor Module status
  event-history               Display event history
```

```
  event-system-policy          Display event system policy
  ex3500                       EX3500 device details
  extdev                       External device (T5, Ex3500..)
  file                         Display filesystem information
  file-sync                    File sync between controller and adoptees
  firewall                     Wireless Firewall
  global                       Global-level information
  gre                          Show l2gre tunnel info
  guest-notification-config    Show guest-notification information
  guest-registration           Guest registration commands
  interface                    Interface Configuration/Statistics commands
  ip                           Internet Protocol (IP)
  ip-access-list               IP ACL
  ipv6                         Internet Protocol version 6 (IPv6)
  ipv6-access-list             IPV6 ACL
  l2tpv3                       L2TPv3 information
  lacp                         LACP commands
  ldap-agent                   LDAP Agent Configuration
  licenses                     Show installed licenses and usage
  lldp                         Link Layer Discovery Protocol
  logging                      Show logging information
  mac-access-list              MAC ACL
  mac-address-table            Display MAC address table
  mac-auth                     MAC authentication
  mac-auth-clients             MAC authenticated clients
  mint                         MiNT protocol
  mirroring                    Show mirroring sessions
  nsight                       Nsight Server Module
  ntp                          Network time protocol
  password-encryption          Pasword encryption
  pppoe-client                 PPP Over Ethernet client
  privilege                    Show current privilege level
  radius                       RADIUS statistics commands
  raid                         Show RAID status
  reload                       Scheduled reload information
  remote-debug                 Show details of remote debug sessions
  rf-domain-manager            Show RF Domain Manager selection details
  role                         Role based firewall
  route-maps                   Display Route Map Statistics
  rtls                         RTLS Statistics
  running-config               Current operating configuration
  session-changes              Configuration changes made in this session
  session-config               This session configuration
  sessions                     Display sessions
  site-config-diff             Difference between site configuration on the NOC
                               and actual site configuration
  slot                         Expansion slots stats
  smart-rf                     Smart-RF Management Commands
  spanning-tree                Display spanning tree information
  startup-config               Startup configuration
  t5                           Display T5 inventory information
  terminal                     Display terminal configuration parameters
  timezone                     The timezone
  traffic-shape                Display traffic shaping
  upgrade-status               Display last image upgrade status
  version                      Display software & hardware version
  virtual-machine              Virtual Machine
  vrrp                         VRRP protocol
  web-filter                   Web filter
  what                         Perform global search
  wireless                     Wireless commands
  wwan                         Display wireless WAN Status

<DEVICE>(config)#
```

```
rfs6000-81742D(config)#show clock
2017-04-06 15:49:10 IST
rfs6000-81742D(config)#
```

PRIVILEGE EXEC Mode

```
<DEVICE>#show ?
  adoption                    Adoption related information
  bluetooth                   Bluetooth Configuration/Statistics commands
  bonjour                     Bonjour Gateway related commands
  boot                        Display boot configuration.
  captive-portal              Captive portal commands
  captive-portal-page-upload  Captive portal internal and advanced page upload
  cdp                         Cisco Discovery Protocol
  classify-url                Query the category of an URL
  clock                       Display system clock
  cluster                     Cluster Protocol
  cmp-factory-certs           Display the CMP certificate status
  commands                    Show command lists
  context                     Information about current context
  critical-resources          Critical Resources
  crypto                      Encryption related commands
  database                    Database
  debug                       Debugging functions
  debugging                   Debugging functions
  device-upgrade              Device Upgrade
  dot1x                       802.1X
  dpi                         Deep Packet Inspection
  eguest                      ExtremeGuest
  environmental-sensor        Display Environmental Sensor Module status
  event-history               Display event history
  event-system-policy         Display event system policy
  ex3500                      EX3500 device details
  extdev                      External device (T5, Ex3500..)
  file                        Display filesystem information
  file-sync                   File sync between controller and adoptees
  firewall                    Wireless Firewall
  global                      Global-level information
  gre                         Show l2gre tunnel info
  guest-notification-config   Show guest-notification information
  guest-registration          Guest registration commands
  interface                   Interface Configuration/Statistics commands
  ip                          Internet Protocol (IP)
  ip-access-list              IP ACL
  ipv6                        Internet Protocol version 6 (IPv6)
  ipv6-access-list            IPV6 ACL
  l2tpv3                      L2TPv3 information
  lacp                        LACP commands
  ldap-agent                  LDAP Agent Configuration
  licenses                    Show installed licenses and usage
  lldp                        Link Layer Discovery Protocol
  logging                     Show logging information
  mac-access-list             MAC ACL
  mac-address-table           Display MAC address table
  mac-auth                    MAC authentication
  mac-auth-clients            MAC authenticated clients
  mint                        MiNT protocol
  mirroring                   Show mirroring sessions
  nsight                      Nsight Server Module
  ntp                         Network time protocol
  password-encryption         Pasword encryption
  pppoe-client                PPP Over Ethernet client
  privilege                   Show current privilege level
  radius                      RADIUS statistics commands
  raid                        Show RAID status
  reload                      Scheduled reload information
  remote-debug                Show details of remote debug sessions
  rf-domain-manager           Show RF Domain Manager selection details
```

```
  role                          Role based firewall
  route-maps                    Display Route Map Statistics
  rtls                          RTLS Statistics
  running-config                Current operating configuration
  session-changes               Configuration changes made in this session
  session-config                This session configuration
  sessions                      Display sessions
  site-config-diff              Difference between site configuration on the NOC
                                and actual site configuration
  slot                          Expansion slots stats
  smart-rf                      Smart-RF Management Commands
  spanning-tree                 Display spanning tree information
  startup-config                Startup configuration
  t5                            Display T5 inventory information
  terminal                      Display terminal configuration parameters
  timezone                      The timezone
  traffic-shape                 Display traffic shaping
  upgrade-status                Display last image upgrade status
  version                       Display software & hardware version
  virtual-machine               Virtual Machine
  vrrp                          VRRP protocol
  web-filter                    Web filter
  what                          Perform global search
  wireless                      Wireless commands
  wwan                          Display wireless WAN Status

<DEVICE>#

rfs6000-81742D#show terminal
Terminal Type: xterm
Length: 24     Width: 80
rfs6000-81742D#
```

## USER EXEC Mode

```
<DEVICE>>show ?
  adoption                      Adoption related information
  bluetooth                     Bluetooth Configuration/Statistics commands
  bonjour                       Bonjour Gateway related commands
  boot                          Display boot configuration.
  captive-portal                Captive portal commands
  captive-portal-page-upload    Captive portal internal and advanced page upload
  cdp                           Cisco Discovery Protocol
  classify-url                  Query the category of an URL
  clock                         Display system clock
  cluster                       Cluster Protocol
  cmp-factory-certs             Display the CMP certificate status
  commands                      Show command lists
  context                       Information about current context
  critical-resources            Critical Resources
  crypto                        Encryption related commands
  database                      Database
  debug                         Debugging functions
  debugging                     Debugging functions
  device-upgrade                Device Upgrade
  dot1x                         802.1X
  dpi                           Deep Packet Inspection
  eguest                        ExtremeGuest
  environmental-sensor          Display Environmental Sensor Module status
  event-history                 Display event history
  event-system-policy           Display event system policy
  ex3500                        EX3500 device details
  extdev                        External device (T5, Ex3500..)
  file-sync                     File sync between controller and adoptees
  firewall                      Wireless Firewall
  global                        Global-level information
  gre                           Show l2gre tunnel info
  guest-notification-config     Show guest-notification information
```

```
  guest-registration          Guest registration commands
  interface                   Interface Configuration/Statistics commands
  ip                          Internet Protocol (IP)
  ipv6                        Internet Protocol version 6 (IPv6)
  lacp                        LACP commands
  licenses                    Show installed licenses and usage
  lldp                        Link Layer Discovery Protocol
  logging                     Show logging information
  mac-address-table           Display MAC address table
  mac-auth                    MAC authentication
  mac-auth-clients            MAC authenticated clients
  mint                        MiNT protocol
  mirroring                   Show mirroring sessions
  nsight                      Nsight Server Module
  ntp                         Network time protocol
  password-encryption         Pasword encryption
  pppoe-client                PPP Over Ethernet client
  privilege                   Show current privilege level
  radius                      RADIUS statistics commands
  raid                        Show RAID status
  rf-domain-manager           Show RF Domain Manager selection details
  role                        Role based firewall
  route-maps                  Display Route Map Statistics
  rtls                        RTLS Statistics
  running-config              Current operating configuration
  session-changes             Configuration changes made in this session
  session-config              This session configuration
  sessions                    Display sessions
  site-config-diff            Difference between site configuration on the NOC
                              and actual site configuration
  slot                        Expansion slots stats
  smart-rf                    Smart-RF Management Commands
  spanning-tree               Display spanning tree information
  startup-config              Startup configuration
  t5                          Display T5 inventory information
  terminal                    Display terminal configuration parameters
  timezone                    The timezone
  traffic-shape               Display traffic shaping
  version                     Display software & hardware version
  virtual-machine             Virtual Machine
  vrrp                        VRRP protocol
  web-filter                  Web filter
  what                        Perform global search
  wireless                    Wireless commands
  wwan                        Display wireless WAN Status

<DEVICE>>

nx9500-6C8809(config)#show wireless ap configured
-------------------------------------------------------------------------------
-------
 IDX      NAME              MAC             PROFILE      RF-DOMAIN       ADOPTED-BY
-------------------------------------------------------------------------------
-------
  1    ap7532-80C2AC    84-24-8D-80-C2-AC   default-ap7532    TechPubs    B4-C7-
99-6C-88-09
  2    ap8132-711728    B4-C7-99-71-17-28   default-ap81xx    TechPubs    B4-C7-
99-6D-B5-D4
  3    t5-ED7C6C        B4-C7-99-ED-7C-6C   default-t5        TechPubs    B4-C7-
99-6C-88-09
  4    rfs4000-880DA7   00-23-68-88-0D-A7   default-rfs4000   TechPubs    B4-C7-
99-6C-88-09
  5    ap7131-99BB7C    00-23-68-99-BB-7C   default-ap71xx    TechPubs    B4-C7-
99-6C-88-09

--More--
nx9500-6C8809(config)#
```

## 6.1.2 adoption

*show commands*

Displays adoption related information, and is common to the User Exec, Priv Exec, and Global Config modes.

In an *hierarchically managed* (HM) network devices are deployed in two levels. The first level consists of the *Network Operations Center* (NOC) controllers. The second level consists of the site controllers. that can be grouped to form clusters. The NOC controllers adopt and manage the site controllers. Access points within the network are adopted and managed by the site controllers.

Use this command to confirm if a device is an adoptee or an adopter. This command also allows you to determine the devices adopted by an adopter device.

**NOTE:** A NOC controller's capacity is equal to or higher than a site controller's capacity. The following devices can be deployed at NOC and sites:

- NOC controller – RFS6000, NX65XX, NX9500, NX9510, or NX9600.
- Site controller – RFS6000 or RFS4000.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show adoption [config-errors|controllers|history|info|log|offline|pending|status|
timeline]

show adoption offline

show adoption config-errors <DEVICE-NAME>

show adoption log [adoptee|adopter {<MAC>}] {on <DEVICE-NAME>}

show adoption [controllers {include-ipv6}|history|info|pending|status {summary}|
timeline] {on <DEVICE-NAME>}
```

**Parameters**

- `show adoption offline`

| | |
|---|---|
| adoption | Displays adoption related information. It also displays configuration errors. |
| offline | Displays non-adopted status of the logged device and its adopted access points |

- `show adoption config-errors <DEVICE-NAME>`

| | |
|---|---|
| adoption | Displays adoption related information. It also displays configuration errors. |
| config-errors <DEVICE-NAME> | Displays configuration errors for a specified adopted device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `show adoption log [adoptee|adopter {<MAC>}] {on <DEVICE-NAME>}`

| | |
|---|---|
| adoption | Displays adoption related information. It also displays configuration errors. |

| | |
|---|---|
| log [adoptee\| adopter {MAC}] {on <DEVICE-NAME>} | Displays adoption logs, for the specified device. If no device name is specified, the system displays logs for the logged device.<br>• adoptee – Displays adoption logs for adoptee devices (APs, wireless controllers, and service platforms). To view logs for a specified adoptee, specify the device's name. If no device name is specified, the system displays logs for the logged device. If the logged device is not an adoptee, the system states that the device is a controller. For example, `2013-01-19 22:00:13:MLCP_TAG_CLUSTER_MASTER not present and this device is a controller. Ignoring`<br>• on <DEVICE-NAME> – Optional. Displays adoptee status and details for the device identified by the <DEVICE-NAME> keyword<br>• <DEVICE-NAME> – Specify the device's name.<br>• adopter – Displays adoption logs for adopter devices (APs, wireless controllers, and service platforms). To view logs for a specified adopter, specify the device's name. If no device name is specified, the system displays logs for the logged device.<br>• <MAC> – Optional. Filters adopters by the adoptee device's MAC address. Specify the adoptee device's MAC address. The system displays logs for the device that has adopted the device identified by the <MAC> keyword.<br>• on <DEVICE-NAME> – Optional. Displays adopter status and details for the device identified by the <DEVICE-NAME> keyword.<br>• <DEVICE-NAME> – Specify the adopter device's name.<br>A wireless controller or service platform cannot be configured as an adoptee and an adopter simultaneously. In other words, an adopted wireless controller or service platform cannot be configured to adopt another device and vice versa. |

• `show adoption [history|controllers {include-ipv6}|info|pending|status {summary}|timeline] {on <DEVICE-NAME>}`

| | |
|---|---|
| adoption | Displays adoption related information. It also displays configuration errors. |
| controllers {include-ipv6} | Displays information about adopted controllers. This is applicable in a Hierarchically managed network, where site controllers are adopted by the NOC controllers.<br>• include-ipv6 – Optional. Displays the controller's IPv6 address, if assigned, in the output |
| history | Displays adoption history of the logged device and its adopted access points |
| info | Displays adopted device information |
| pending | Displays information for devices pending adoption |
| status {summary} | Displays adoption status for the logged device. When executed without using the 'on <DEVICE-NAME>' parameter, this command displays detailed information of all devices adopted by the device on which the command is executed.<br>• summary – Optional. Displays a summary of all devices adopted by the logged device. |
| timeline | Displays the logged device's adoption timeline. It also shows the adoption time for logged device's adopted APs. To view the adoption timeline of a specific device, use the *on <device-name>* option to specify the device. |
| on <DEVICE-NAME> | The following keywords are common to all of the above parameters:<br>• on <DEVICE-NAME> – Optional. Displays a device's adoption information, based on the parameter passed.<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

**Usage Guidelines**

In a device's Global Config mode, use the *customize > show-adoption-status* command to customize the *show > adoption > status* command output. The following columns can be added to the output:

```
nx9500-6C8809(config)#customize show-adoption-status ?
  adopted-by     Device name to which the AP is adopted
  ap-name        Host-name of the adopted AP
  cdp-lldp-info  Cdp/lldp info of the Adopted AP
  config-status  Configuration status of the adopted AP
  last-adoption  Last known adoption time
  msgs           Messages status
  uptime         Uptime of the adopted AP
  version        Current version of the adopted AP

nx9500-6C8809(config)#
```

For more information on the customise command, see *customize*.

**Example**

The following example displays details of the:

- device to which the logged device (`rfs6000-81742D`) is adopted, and
- devices adopted (`ap7532-A2A4B0, ap7532-80C2AC, ap7562-84A224, etc.`) by the logged device.

```
rfs6000-81742D(config)#show adoption status
Adopted by:
Type           : nx9000
System Name    : nx9500-6C8809
MAC address    : B4-C7-99-6C-88-09
MiNT address   : 19.6C.88.09
Time           :   7 days 01:02:34 ago

Adopted Devices:
--------------------------------------------------------------------------------
--------------------------------
DEVICE-NAME       VERSION         CFG-STAT         MSGS ADOPTED-BY        LAST-
ADOPTION                  UPTIME
--------------------------------------------------------------------------------
--------------------------------
ap7532-A2A4B0     5.9.1.0-012D    configured       No   rfs6000-81742D     0 days
23:42:11     0 days 23:46:12
Snap004...ssPoint 5.9.1.0-012D    configured       No   rfs6000-81742D     1 days
00:25:33     1 days 02:30:57
ap7532-80C2AC     5.9.1.0-012D    error            Yes  rfs6000-81742D     1 days
00:10:00     1 days 00:11:40
ap7562-84A224     5.9.1.0-012D    configured       No   rfs6000-81742D     1 days
00:23:12     1 days 02:13:48
-More--

rfs6000-81742D(config)#

nx9500-6C8809#show adoption info
--------------------------------------------------------------------------------
--------------------
              HOST-NAME                MAC       TYPE              MODEL
SERIAL-NUMBER
--------------------------------------------------------------------------------
--------------------
        rfs6000-81742D   00-15-70-81-74-2D    rfs6000    RFS-6010-1000-WR
7295520400121
              t5-ED7C6C   B4-C7-99-ED-7C-6C         t5          TS-0524-WR
14213522400004
--------------------------------------------------------------------------------
--------------------
Total number of devices displayed: 2
nx9500-6C8809#
```

```
nx9500-6C8809#show adoption status
-------------------------------------------------------------------------------
-------------------------------
DEVICE-NAME       VERSION         CFG-STAT         MSGS ADOPTED-BY        LAST-
ADOPTION                  UPTIME
-------------------------------------------------------------------------------
-------------------------------
rfs6000-81742D    5.9.1.0-012D    configured       No   nx9500-6C8809      7 days
01:06:02     7 days 01:08:45
t5-ED7C6C         5.4.2.0-010R    configured       No   nx9500-6C8809      7 days
01:22:09   114 days 04:37:10
-------------------------------------------------------------------------------
-------------------------------
Total number of devices displayed: 2
nx9500-6C8809#

nx9500-6C8809#show adoption offline
-----------------------------------------
MAC              HOST-NAME         TYPE     RF-DOMAIN           TIME OFFLINE
CONNECTED-TO
-------------------------------------------------------------------------------
-------
00-23-68-11-E6-C4 ap71xx-11E6C4      ap71xx   TechPubs          unknown
None
00-23-68-9C-63-D4 ap7131-9C63D4      ap71xx   default           unknown
None
5C-0E-8B-A6-57-80 ap650-A65780       ap650    default           unknown
None
5C-0E-8B-A6-ED-14 ap650-A6ED14       ap650    default           unknown
None
84-24-8D-16-01-C4 ap7532-1601C4      ap7532   default           unknown
None
B4-C7-99-4B-F3-64 ap7131-4BF364      ap71xx   default           unknown
None
-------------------------------------------------------------------------------
-------
Total number of devices displayed: 6
nx9500-6C8809#

rfs6000-81742D#show adoption log adoptee on ap7532-80C2AC
2017-04-05 10:19:56:Received OK from cfgd, adoption complete to 70.81.74.2D
2017-04-05 10:19:56:Waiting for cfgd OK, adopter should be 70.81.74.2D
2017-04-05 10:19:56:Adoption state change: 'Connecting to adopter' to 'Waiting for
Adoption OK'
2017-04-05 10:19:56:Adoption state change: 'Adoption failed' to 'Connecting to
adopter'
2017-04-05 10:19:56:Try to adopt to 70.81.74.2D (cluster master 70.81.74.2D in
adopters)
2017-04-05 10:19:27:Ignoring MLCP Offer, vlan_state MLCP_DONE != MLCP_DISCOVERING
/ MLCP_STP_WAITING
--More--
rfs6000-81742D#

nx9500-6C8809#show adoption controllers include-ipv6
-------------------------------------------------------------------------------
-------------------------------------------------
                 NAME      RF-DOMAIN               MAC       MINT-ID
IP              IPV6          ADOPTED-BY
-------------------------------------------------------------------------------
-------------------------------------------------
         rfs6000-81742D       TechPubs   00-15-70-81-74-2D   70.81.74.2D
192.168.13.24                ::        nx9500-6C8809
-------------------------------------------------------------------------------
-------------------------------------------------
Total number of devices displayed: 1
nx9500-6C8809#
```

## 6.1.3 bluetooth

*show commands*

Displays Bluetooth radio statistics for RF Domain member access points

AP8432 and AP8533 model access points utilize a built-in Bluetooth chip for specific Bluetooth functional behaviors in a WiNG managed network. AP8432 and AP8533 models support both Bluetooth classic and *Bluetooth low energy* (BLE) technology. These platforms use their Bluetooth classic enabled radio to sense other Bluetooth enabled devices and report device data (MAC address, RSSI and device calls) to an ADSP server for intrusion detection. If the device presence varies in an unexpected manner, ADSP can raise an alarm.

**NOTE:** AP8132 model access points support an external USB Bluetooth radio providing ADSP Bluetooth classic sensing functionality only, not the BLE beaconing functionality available for AP8432 and AP8533 model access points described in this section.

AP8432 and AP8533 model access points support Bluetooth beaconing to emit either iBeacon or Eddystone-URL beacons. The access point's Bluetooth radio sends non-connectable, undirected *low-energy* (LE) advertisement packets periodically. These advertisement packets are short and sent on Bluetooth advertising channels that conform to already-established iBeacon and Eddystone-URL standards.

**Supported in the following platforms:**

- Access Points — AP8432, AP8533

**Syntax**

```
show bluetooth radio {detail|on}

show bluetooth radio {detail {<DEVICE-NAME> <1-1>|filter bluetooth-radio-mac <BT-RADIO-MAC>}} {(on <DEVICE-OR-DOMAIN-NAME>)}
```

**Parameters**

- `show bluetooth radio {detail {<DEVICE-NAME> <1-1>|filter bluetooth-radio-mac <BT-RADIO-MAC>}} {(on <DEVICE-OR-DOMAIN-NAME>)}`

| | |
|---|---|
| bluetooth radio | Displays Bluetooth radio utilization statistics based on the parameters passed |
| detail <DEVICE-NAME> <1-1> | Optional. Displays detailed Bluetooth radio utilization statistics. Optionally, to view detailed information for a specific access point's Bluetooth radio, specify the access point's and the radio's MAC addresses.<br>• <DEVICE-NAME> <1-1> – Optional. Specify the access point's hostname or MAC address.<br>• <1-1> – Specify the bluetooth radio interface index number from 1 - 1. As of now only one Bluetooth radio interface is supported. The Interface index number is appended to the AP's hostname or MAC address in the following format: ap8533-06FBE1:B1 OR 74-67-F7-06-FB-E1:B1<br>The following information is displayed:<br>• access point's hostname as its network identifier<br>• access point's alias. If an alias has been defined for the access point its listed here. The alias value is expressed in the form of <hostname>:B<Bluetooth_radio_number>. If the access point has a administrator assigned hostname, it is used in place of the access point's default hostname.<br>Contd.. |

| | |
|---|---|
| contd.. | • access point's factory encoded MAC address<br>• access point and bluetooth radio's administrator assigned area of deployment (the AP's geographical location)<br>• bluetooth radio's state (on/off)<br>• bluetooth radio's reason for inactivity (in case the radio is off)<br>• bluetooth radio's factory encoded MAC address serving as this device's hardware identifier on the network<br>• bluetooth radio's functional mode: bt-sensor or le-beacon<br>• bluetooth radio's beacon period<br>• bluetooth radio's beacon type<br>• descriptive text on any error that's preventing the Bluetooth radio from operating |
| filter bluetooth-radio-mac <BT-RADIO-MAC> | Optional. Specifies additional filters to get table values. Filters data based on the Bluetooth radio's MAC address.<br>• <BT-RADIO-MAC> – Specify the Bluetooth radio's MAC address. The system only displays statistics related to the specified Bluetooth radio. |
| on <DEVICE-OR-DOMAIN-NAME> | The following keywords are recursive and common to all of the above.<br>• on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays Bluetooth radio statistics on a specified device or RF Domain<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the device or RF Domain. If the device name is explicitly given, the results display data for the specified AP only. If the RF Domain is explicitly given, the results display data for all APs within the specified RF Domain.<br>If no device/RF Domain is specified, the results include data for all Bluetooth radios within the controller's RF Domain.<br>If the controller is in the "on rf-domain all" mode, the results include data for all Bluetooth radios for all APs in each domain known to the controller. |

**Example**

```
nx9500-6C8809(config)#show bluetooth radio on ap8533-06F808
-------------------------------------------------------------------------------
 BLUETOOTH RADIO      RADIO MAC           MODES                      STATE
-------------------------------------------------------------------------------
ap8533-06F808:B1  74-67-F7-08-A3-B0    BLE-Beacon                  On
-------------------------------------------------------------------------------
Total number of Bluetooth radios displayed: 0
nx9500-6C8809(config)#

nx9500-6C8809(config)#show bluetooth radio detail 74-67-F7-06-F8-08 1
Radio: 74-67-F7-06-F8-08:B1, alias ap8533-06F808:B1
 STATE          : Off [shutdown in cfg]
 PHY INFO       : MAC: 74-67-F7-08-A3-B0
 ACCESS POINT   : Name: ap8533-06F808  Location: default  Placement: Indoor
 ENABLED MODES  : BLE-Beacon
 BEACON TYPES   : Eddystone-URL
 BEACON PERIOD  : 1000ms
 Last error     :
nx9500-6C8809(config)#
```

## 6.1.4 boot

*show commands*

Displays a device's boot configuration. Use this command to view the primary and secondary image details, such as Build Date, Install Date, and Version. This command also displays the current boot and next boot information.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show boot {on <DEVICE-NAME>}
```

**Parameters**

- `show boot {on <DEVICE-NAME>}`

| | |
|---|---|
| boot | Displays primary and secondary image boot configuration details (build date, install date, version, and the image used to boot the current session) |
| on <DEVICE-NAME> | Optional. Displays a specified device's boot configuration<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.<br>**Note:** Use the *on <DEVICE-NAME>* option to view a remote device's boot configuration. |

**Example**

```
nx9500-6C8809#show boot
------------------------------------------------------------------------------
     IMAGE            BUILD DATE              INSTALL DATE          VERSION
------------------------------------------------------------------------------
  Primary       05/31/2017 22:24:22     06/02/2017 14:22:51     5.9.0.0-029R
  Secondary     05/27/2017 01:00:26     05/30/2017 10:35:55     5.9.0.0-028B
------------------------------------------------------------------------------
Current Boot       : Primary
Next Boot          : Primary
Software Fallback  : Enabled
VM support         : Not present
nx9500-6C8809#

nx9500-6C8809#show boot on TechPubs/rfs6000-6DB5D4
------------------------------------------------------------------------------
     IMAGE            BUILD DATE              INSTALL DATE          VERSION
------------------------------------------------------------------------------
  Primary       05/31/2017 22:24:22     06/02/2017 14:22:51     5.9.0.0-029R
  Secondary     05/27/2017 01:00:26     05/30/2017 10:35:55     5.9.0.0-028B
------------------------------------------------------------------------------
Current Boot       : Primary
Next Boot          : Primary
Software Fallback  : Enabled
VM support         : Not present
nx9500-6C8809#
```

## 6.1.5 bonjour

*show commands*

Displays the configured Bonjour services available on local and remote sites

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show bonjour services {on <DEVICE-NAME>}
```

**Parameters**

- `show bonjour services {on <DEVICE-NAME>}`

| | |
|---|---|
| bonjour services | Displays the configured Bonjour services available on local and remote sites |
| on <DEVICE-NAME> | Optional. Displays Bonjour services available on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

**Example**

```
rfs6000-81742D#show bonjour services on ap7131-11E6C4
-------------------------------------------------------------------------------
-------------------------------------------------------------------
        SERVICE_NAME                    INSTANCE_NAME                IP:PORT
VLAN-ID VLAN_TYPE           EXPIRY
-------------------------------------------------------------------------------
-------------------------------------------------------------------
  _pdl-datastream._tcp.local      Brother MFC-8510DN._pdl-datastream._tcp.local
172.110.0.146:9100    110     Local     Tue Sep 12 02:07:44 2017

  _universal._sub._ipp._tcp.local   Brother MFC-8510DN._ipp._tcp.local
172.110.0.146:631     110     Local     Tue Sep 12 02:36:13 2017

  _ipp._tcp.local                 Brother MFC-8510DN._ipp._tcp.local
172.110.0.146:631     110     Local     Tue Sep 12 02:36:13 2017
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
--------------
rfs6000-81742D#
```

## 6.1.6 captive-portal

*show commands*

Displays WLAN captive portal information. Use this command to view a configured captive portal's client information.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show captive-portal sessions {include-ipv6|on <DEVICE-OR-DOMAIN-NAME>|
statistics} {(filter [captive-portal [<CAPTIVE-PORTAL>|not <CAPTIVE-PORTAL>]|
ip [<IPv4>|not <IPv4>]|ipv6 [<IPv6>|not <IPv6>]|state [pending|success|not
[pending|success]|vlan [<VLAN-ID>|not <VLAN-ID>]|wlan [<WLAN-NAME>|not <WLAN-
NAME>]])}
```

**Parameters**

```
• show captive-portal sessions {include-ipv6|on <DEVICE-OR-DOMAIN-NAME>|
statistics} {(filter [captive-portal [<CAPTIVE-PORTAL>|not <CAPTIVE-PORTAL>]|ip
[<IPv4>|not <IPv4>]|ipv6 [<IPv6>|not <IPv6>]|state [pending|success|not
[pending|success]|vlan [<VLAN-ID>|not <VLAN-ID>]|wlan [<WLAN-NAME>|not <WLAN-
NAME>]])}
```

| | |
|---|---|
| captive-portal sessions | Displays active captive portal client session details |
| include-ipv6 | Optional. Includes IPv6 address (if known) of captive portal clients<br>By default the system only displays IPv4 addresses. The include-ipv6 parameter includes IPv6 address (if known) of each client. |
| statistics | Optional. Displays statistical information regarding client sessions |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Displays active captive portal session details on a specified device or RF Domain.<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |
| filter | This parameter is recursive and can be used with any of the above parameters to define additional filters.<br>Optional. Defines additional filters. Use one of the following options: captive-portal, ip, ipv6, state, vlan, or wlan. |
| captive-portal [<CAPTIVE-PORTAL>\| not <CAPTIVE-PORTAL>] | Optional. Displays captive portal client and client session information, based on the captive portal name passed<br>• <CAPTIVE-PORTAL> – Specify the captive portal name. Displays client details for the specified captive portal.<br>• not <CAPTIVE-PORTAL> – Inverts the match selection. Displays client details for all captive portals other than the specified captive portal. |

| | |
|---|---|
| ip [<IPv4>\|not <IPv4>] | Optional. Displays captive portal client/client sessions information, based on the IPv4 address passed<br>• <IPv4> – Specify the client's IPv4 address. Displays information of the client identified by the <IPv4> parameter<br>• not <IPv4> – Inverts the match selection. Displays client details for all clients other than the one identified by the <IPv4> parameter. |
| ipv6 [<IPv6>\|not <IPv6>] | This filter option is available only for the 'include-ipv6' keyword.<br>Optional. Displays captive portal client/client sessions information, based on the IPv6 address passed<br>• <IPv6> – Specify the client's IPv6 address. Displays information of the client identified by the <IPv6> parameter<br>• not <IPv6> – Inverts the match selection. Displays client details for all clients other than the one identified by the <IPv6> parameter. |
| state [pending\|success\| not [pending\|success]] | Optional. Filters clients/client sessions based on the client's authentication state<br>• pending – Displays information of clients redirected for authentication<br>• success – Displays information of successfully authenticated clients<br>• not [pending\|success] – Inverts match selection<br>• pending – Displays information of successfully authenticated clients (opposite of pending authentication)<br>• success – Displays information of clients redirected for authentication (opposite of successful authentication) |
| vlan [<VLAN-ID>\| not <VLAN-ID>] | Optional. Displays captive portal client/client sessions information based on the VLAN ID passed<br>• <VLAN-ID> – Specify the VLAN ID. Displays client details for the specified VLAN.<br>• not <VLAN-ID> – Inverts match selection. Displays client details for all VLANs other than the one identified by the <VLAN-ID> parameter. |
| wlan [<WLAN-NAME>\| not <WLAN-NAME>] | Optional. Displays captive portal client/client sessions information based on the WLAN name passed<br>• <WLAN-NAME> – Specify the WLAN name. Displays client details for the specified WLAN.<br>• not <WLAN-NAME> – Inverts match selection. Displays client details for all WLANs other than the one identified by the <WLAN-NAME> parameter. |

**Example**

```
rfs4000-229D58#show captive-portal sessions
================================================================================
=======
CLIENT             IPv4     CAPTIVE-PORTAL   WLAN/PORT    VLAN  STATE SESSION  TIME
--------------------------------------------------------------------------------
-------
00-26-55-F4-5F-79  192.168.3.99 cappo     rfs4000-229D58:ge2    400     Success
23:58:35
================================================================================
=======
Total number of captive portal sessions displayed: 1
rfs4000-229D58#
```

## 6.1.7 captive-portal-page-upload

*show commands*

Displays captive portal page information, such as upload history, upload status, and page file download status

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show captive-portal-page-upload [history|list-files|load-image-status|status]

show captive-portal-page-upload load-image-status

show captive-portal-page-upload history {on <RF-DOMAIN-NAME>}

show captive-portal-page-upload status {on [<RF-DOMAIN-NAME>|<RF-DOMAIN-MANAGER>]}

show captive-portal-page-upload list-files <CAPTIVE-PORTAL-NAME>
```

**Parameters**

- `show captive-portal-page-upload load-image-status`

| | |
|---|---|
| load-image-status | Displays captive portal advanced page file download status on the logged device |

- `show captive-portal-page-upload history {on <RF-DOMAIN-NAME>}`

| | |
|---|---|
| history {on <RF-DOMAIN-NAME>} | Displays captive portal page upload history<br>• on <RF-DOMAIN-NAME> – Optional. Displays captive portal page upload history within a specified RF Domain. Specify the RF Domain name. |

- `show captive-portal-page-upload status {on [<RF-DOMAIN-NAME>|<RF-DOMAIN-MANAGER>]}`

| | |
|---|---|
| status {on <RF-DOMAIN-NAME>\| on <RF-DOMAIN-MANAGER>} | Displays captive portal page upload status<br>• on <RF-DOMAIN-NAME> – Optional. Displays captive portal page upload status within a specified RF Domain. Specify the RF Domain name.<br>• on <RF-DOMAIN-MANAGER> – Optional. Displays captive portal page upload status for a specified RF Domain Manager. Specify the RF Domain Manager name. |

- `show captive-portal-page-upload list-files <CAPTIVE-PORTAL-NAME>`

| | |
|---|---|
| list-files <CAPTIVE-PORTAL-NAME> | Displays a list of all captive portal Web page files, of a specified captive portal, uploaded (internal and advanced page files)<br>• <CAPTIVE-PORTAL-NAME> – Specify the captive portal name. |

**Example**

```
nx7500-7F2C13#captive-portal-page-upload CP-BW all
-------------------------------------------------------------------------------
         CONTROLLER             STATUS                   MESSAGE
-------------------------------------------------------------------------------
  84-24-8D-7F-2C-13         Success         Added 1 APs to upload queue
-------------------------------------------------------------------------------
nx7500-7F2C13#

nx7500-7F2C13#show captive-portal-page-upload load-file-status
Download of CP-BW page file is complete
nx7500-7F2C13#

nx7500-7F2C13#show captive-portal-page-upload list-files CP-BW
-------------------------------------------------------------------------------
       NAME                   SIZE                LAST MODIFIED
-------------------------------------------------------------------------------
  CP-BW-1.tar.gz              6133              2016-05-16 10:38:40
  CP-BW.tar.gz                3370              2016-05-16 10:45:44
-------------------------------------------------------------------------------
nx7500-7F2C13#
```

## 6.1.8 cdp

*show commands*

Displays the *Cisco Discovery Protocol* (CDP) neighbor table

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show cdp [neighbors|report] {detail {on <DEVICE-NAME>}|on <DEVICE-NAME>}
```

**Parameters**

- `show cdp [neighbors|report] {detail {on <DEVICE-NAME>}|on <DEVICE-NAME>}`

| | |
|---|---|
| cdp [neighbors\|report] | Displays CDP neighbors table or aggregated CDP neighbors table |
| detail {on <DEVICE-NAME>} | Optional. Displays detailed CDP neighbors table or aggregated CDP neighbors table<br>• on <DEVICE-NAME> – Optional. Displays table details on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |
| on <DEVICE-NAME> | Optional. Displays table details on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

**Example**

The following example shows detailed CDP neighbors table:

```
nx9500-6C8809#show cdp neighbors detail
-------------------------
Device ID: ap8132-74B45C
Entry address(es):
  IP Address: 192.168.13.26
Platform: AP-8132-66040-WR, Capabilities: Router Switch
Interface: ge1, Port ID (outgoing port): ge1
Hold Time: 165 sec

advertisement version: 2
Native VLAN: 1
Duplex: full
Version :
5.8.6.0-008B
-------------------------
Device ID: ap7532-80C2AC
Entry address(es):
  IP Address: 192.168.13.28
Platform: AP-7532-67040-WR, Capabilities: Router Switch
Interface: ge1, Port ID (outgoing port): ge1
Hold Time: 169 sec

--More--
nx9500-6C8809#
```

The following example shows a non-detailed CDP neighbors table:

```
rfs6000-81742D#show cdp neighbors
-------------------------------------------------------------------------------
     Device ID           Platform        Local Interface    Port ID     Duplex
-------------------------------------------------------------------------------
 nx9500-6C8809     NX-9500-100R0-WR     ge2                ge1         full
 rfs6000-81742D    RFS-6010-1000-WR     ge2                ge1         full
 rfs4000-880DA7    RFS-4011-11110-US    ge2                ge1         full
 ap6521-42936C     AP-6521E-60020-WR    ge2                ge1         full
-------------------------------------------------------------------------------
rfs6000-81742D#
```

## 6.1.9 classify-url

*show commands*

Displays a specified URL's category. Use this command to query the category of a specific URL. The query is sent to a configured classification server. This option is available only if a valid URL filter license is available.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show classify-url [<URL-TO-QUERY>|datacenter <URL-TO-QUERY>]
```

**Parameters**

- `show classify-url [<URL-TO-QUERY>|datacenter <URL-TO-QUERY>]`

| | |
|---|---|
| classify-url | Queries the category of a specified URL |
| <URL-TO-QUERY> | Specify the URL to query. The query is sent to the configured classification server. |
| datacenter <URL-TO-QUERY> | The query is sent to a global classification datacenter<br>• <URL-TO-QUERY> – Specify the URL to query. |

**Example**

```
nx9500-6C8809#show classify-url www.google.com
  Categories: search-engines-portals,
  Custom Categories:
nx9500-6C8809#

nx9500-6C8809#show classify-url www.ndtv.com
  Categories: news,
  Custom Categories: list1,
nx9500-6C8809#
```

## 6.1.10 clock

*show commands*

Displays a selected system's clock

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show clock {on <DEVICE-NAME>}
```

**Parameters**

- `show clock {on <DEVICE-NAME>}`

| | |
|---|---|
| clock | Displays a system's clock |
| on <DEVICE-NAME> | Optional. Displays system clock on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |

**Example**

```
rfs6000-81742D#show clock
2017-04-06 15:50:42 IST
rfs6000-81742D#
```

## 6.1.11 cluster

*show commands*

Displays cluster information (cluster configuration parameters, members, status, etc.)

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show cluster [configuration|history|members|status]

show cluster [configuration|history {on <DEVICE-NAME>}|members {detail}|status]
```

**Parameters**

- `show cluster [configuration|members {detail}|status]`

| | |
|---|---|
| cluster | Displays cluster information |
| configuration | Displays cluster configuration details |
| history on <DEVICE-NAME> | Displays cluster history status<br>• <DEVICE-NAME> – Optional. Specify the controller or access point name. If the device name is not specified, the system displays all cluster history. |
| members {detail} | Displays cluster members configured on the logged device<br>• detail – Optional. Displays detailed information of known cluster members |
| status | Displays cluster status |

**Example**

```
rfs6000-380649(config)#show cluster configuration
Cluster Configuration Information
 Name                          : SiteConRFS6k
 Configured Mode               : Active
 Master Priority               : 128
 Force configured state        : Disabled
 Force configured state delay : 5 minutes
 Handle STP                    : Disabled
 Radius Counter DB Sync Time   : 5 minutes
rfs6000-380649(config)#

rfs6000-380649(config)#show cluster members detail
-------------------------------------------------------------------------------
-------
       ID              MAC           MODE   AP COUNT AAP COUNT AP LICENSE AAP
LICENSE      VERSION
-------------------------------------------------------------------------------
-------
70.38.06.49   00-15-70-38-06-49  Active   0        1         0          0
5.8.6.0-008B
70.81.74.2D   00-15-70-81-74-2D  Active   0        0         1          0
5.8.6.0-008B
-------------------------------------------------------------------------------
-------
rfs6000-380649(config)#
```

```
rfs6000-380649(config)#show cluster status

Cluster Runtime Information
 Protocol version             : 1
 Cluster operational state    : active
 AP license                   : 1
 AAP license                  : 0
 AP count                     : 0
 AAP count                    : 1
 Max AP adoption capacity     : 256
 Number of connected member(s): 1
rfs6000-380649(config)#
```

## 6.1.12 cmp-factory-certs

*show commands*

Displays factory installed CMP certificates

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show cmp-factory-certs {all}
```

**Parameters**

- `show cmp-factory-certs {all}`

| | |
|---|---|
| cmp-factory-certs {all} | Displays factory installed CMP certificates on the logged device. Optionally use the 'all' keyword to view certificate details. |

**Example**

```
nx9500-6C8809>show cmp-factory-certs
No CMP factory certificate exist
nx9500-6C8809>
```

## 6.1.13 commands

*show commands*

Displays commands available for the current mode

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show commands
```

**Parameters**

None

**Example**

```
rfs4000-880DA7(config)#show commands
  help
  help search WORD (|detailed|only-show|skip-show|skip-no)
  show commands
  show adoption log adoptee(|on DEVICE-NAME)
  show adoption log adopter (|mac AA-BB-CC-DD-EE-FF)(|on DEVICE-NAME)
  show adoption info (|on DEVICE-NAME)
  show adoption status (|on DEVICE-NAME)
  show adoption status summary (|on DEVICE-NAME)
  show adoption config-errors DEVICE-NAME
  show adoption offline
  show adoption pending (|on DEVICE-NAME)
  show adoption history (|on DEVICE-NAME)
  show adoption timeline (|on DEVICE-NAME)
  show adoption controllers (|on DEVICE-NAME)
  show adoption controllers include-ipv6(|on DEVICE-NAME)
  show debugging (|on DEVICE-OR-DOMAIN-NAME)
  show debugging cfgd(|on DEVICE-NAME)
  show debugging fib(|on DEVICE-NAME)
  show debugging adoption (|on DEVICE-OR-DOMAIN-NAME)
  show debugging wireless (|on DEVICE-OR-DOMAIN-NAME)
  show debugging snmp (|on DEVICE-NAME)
  show debugging ssm (|on DEVICE-NAME)
  show debugging voice (|on DEVICE-OR-DOMAIN-NAME)
--More--
rfs4000-880DA7(config)#
```

## 6.1.14 context

*show commands*

Displays the current context details

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, NX7500, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show context {include-factory|session-config {include-factory}}
```

**Parameters**

- `show context {include-factory|session-config {include-factory}}`

| | |
|---|---|
| include-factory | Optional. Includes factory defaults |
| session-config {include-factory} | Optional. Displays running system information in the current context<br>• include-factory – Optional. Includes factory defaults |

**Example**

```
rfs4000-880DA7(config)#show context
!
! Configuration of RFS4000 version 5.9.1.0-015D
!
!
version 2.5
!
!
client-identity-group default
 load default-fingerprints
!
ip snmp-access-list default
 permit any
!
firewall-policy default
 no ip dos tcp-sequence-past-window
!
!
mint-policy global-default
!
radio-qos-policy default
!
auto-provisioning-policy 4K
!
--More--
rfs4000-880DA7(config)#
```

## 6.1.15 critical-resources

*show commands*

Displays critical resource information. Critical resources are resources vital to the network.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show critical-resources {on <DEVICE-NAME>}
```

**Parameters**

- `show critical-resources {on <DEVICE-NAME>}`

| | |
|---|---|
| critical-resources | Displays critical resources information |
| on <DEVICE-NAME> | Optional. Displays critical resource information on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

**Example**

```
rfs4000-229D58(config)#show critical-resources
-------------------------------------------------------------------------
CRITICAL RESOURCE IP        VLAN          PING-MODE             STATE
-------------------------------------------------------------------------
172.168.1.103                1             arp-icmp              up
-------------------------------------------------------------------------
rfs4000-229D58(config)#
```

## 6.1.16 crypto

*show commands*

Displays encryption mode information

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show crypto [cmp|ike|ipsec|key|pki]
show crypto cmp request status
show crypto ike sa {detail|on|peer|version}
show crypto ike sa {detail|peer <IP>} {on <DEVICE-NAME>}
show crypto ike sa {version [1|2]} {peer <IP>} {(on <DEVICE-NAME>)}
show crypto ipsec sa {detail|on|peer}
show crypto ipsec sa {detail} {on <DEVICE-NAME>}
show crypto ipsec sa {peer <IP>} {detail} {(on <DEVICE-NAME>)}
show crypto key rsa {on|public-key-detail}
show crypto key rsa {public-key-detail} {(on <DEVICE-NAME>)}
show crypto pki trustpoints {<TRUSTPOINT-NAME>|all|on}
show crypto pki trustpoints {<TRUSTPOINT-NAME>|all} {(on <DEVICE-NAME>)}
```

**Parameters**

- `show crypto cmp request status`

| | |
|---|---|
| crypto cmp request status | Displays current status of in-progress *certificate management protocol* (CMP) requests<br>For more information, see *CRYPTO-CMP-POLICY*. |

- `show crypto ike sa {detail|peer <IP>} {on <DEVICE-NAME>}`

| | |
|---|---|
| crypto ike sa | Displays *Internet Key Exchange* (IKE) *security association* (SA) statistics |
| detail | Displays detailed IKE SA statistics |
| peer <IP> | Optional. Displays IKE SA statistics for a specified peer<br>• <IP> – Specify the peer's IP address in the A.B.C.D format |
| on <DEVICE-NAME> | Optional. Displays IKE SA statistics on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `show crypto ike sa {version [1|2]} {peer <IP>} {(on <DEVICE-NAME>)}`

| | |
|---|---|
| crypto ike sa | Displays IKE SA details |
| version [1\|2] | Optional. Displays IKE SA version statistics<br>• 1 – Displays IKEv1 statistics<br>• 2 – Displays IKEv2 statistics |
| peer <IP> | Optional. Displays IKE SA version statistics for a specified peer<br>• <IP> – Specify the peer's IP address in the A.B.C.D format |
| on <DEVICE-NAME> | The following keyword is recursive and common to the 'peer ip' parameter:<br>• on <DEVICE-NAME> – Optional. Displays IKE SA statistics on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

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

| | |
|---|---|
| crypto ipsec sa | Displays *Internet Protocol Security* (IPSec) SA statistics. The IPSec encryption authenticates and encrypts each IP packet in a communication session |
| detail | Optional. Displays detailed IPSec SA statistics |
| on <DEVICE-NAME> | Optional. Displays IPSec SAs on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `show crypto sa {peer <IP>} {detail} {(on <DEVICE-NAME>)}`

| | |
|---|---|
| crypto ipsec sa | Displays IPSec SA statistics. The IPSec encryption authenticates and encrypts each IP packet in a communication session |
| peer <IP> detail | Optional. Displays IPSec SA statistics for a specified peer<br>• <IP> – Specify the peer's IP address in the A.B.C.D format.<br>• detail – Displays detailed IPSec SA statistics for the specified peer |
| on <DEVICE-NAME> | The following keyword is recursive:<br>• on <DEVICE-NAME> – Optional. Displays IPSec SAs on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `show crypto key rsa {public-key-detail} {(on <DEVICE-NAME>)}`

| | |
|---|---|
| crypto key rsa | Displays RSA public keys |
| public-key-detail | Optional. Displays public key in the *Privacy-Enhanced Mail* (PEM) format |
| on <DEVICE-NAME> | The following keyword is recursive:<br>• on <DEVICE-NAME> – Optional. Displays public key on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `show crypto pki trustpoints {<TRUSTPOINT-NAME>|all} {(on <DEVICE-NAME>)}`

| | |
|---|---|
| crypto pki | Displays PKI related information |
| trustpoints | Displays WLAN trustpoints<br>This command displays all trustpoints including CMP-generated trustpoints. |
| <TRUSTPOINT-NAME> | Optional. Displays a specified trustpoint details. Specify the trustpoint name. |

| | |
|---|---|
| all | Optional. Displays details of all trustpoints |
| on <DEVICE-NAME> | The following keyword is recursive and common to the 'trustpoint-name' and 'all' parameters:<br>• on <DEVICE-NAME> – Optional. Displays trustpoints configured on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

**Example**

```
nx9500-6C8809(config)#show crypto key rsa public-key-detail

RSA key name: ting        Key-length: 2048
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtLj11yR38+/mcInGRlrw
3DaasuTJhKsWg7kcSVkM7RLd/Wq/mPZEsqwFLnvFIm4rVIke+mVdWBqV4oGE1TUm
Z4YqKtzlANSAG7EZREr3MXEIHd49NHYeK8U+1EAmHN9F21XCxTO+yRMngKDJeHfz
Za2/64PdBsnRlV4nqCGMGHbbaaCwGe5X0a

RSA key name: default_rsa_key        Key-length: 2048
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA3hyJDk9aMk97X3PhoyMb
6nufFLFUkpF9YwSqO2fNyp9SutqpoML/VAMHHotmaa6SsxPURF8mC66bT7De32r7
wwPd7pIWwALTscwCzd3CrB1jY8s2OQ7ZHGCH6MLau+LeoNPE0c+uH3tNLloTAvSG
xtUAHfwFa4rM6vlzs/ejJ4InnboI8i4uIA
nx9500-6C8809(config)#

nx9500-6C8809(config)#show crypto key rsa
-------------------------------------------------------------------------------
         #                      KEY NAME                      KEY LENGTH
-------------------------------------------------------------------------------
  1                  ting                                 2048
  2                  default_rsa_key                      2048
-------------------------------------------------------------------------------
nx9500-6C8809(config)#

nx9500-6C8809(config)#show crypto pki trustpoints all

Trustpoint Name: default-trustpoint        (self signed)
-------------------------------------------------------------------------------
  CRL present: no
  Server Certificate details:
    Key used: default_rsa_key
    Serial Number: 051d
    Subject Name:
      /CN=NX9500-B4-C7-99-6C-88-09
    Issuer Name:
      /CN=NX9500-B4-C7-99-6C-88-09
    Valid From : Thu Dec  5 04:15:59 2013 UTC
    Valid Until: Sun Dec  3 04:15:59 2023 UTC

nx9500-6C8809(config)#

nx9500-6C8809>show crypto cmp request status
CMP Request Status: ir-req-reset
nx9500-6C8809>
```

## 6.1.17 database

*show commands*

Displays database-related statistics and status

**Supported in the following platforms:**

- Service Platforms — NX9500, NX9510, VX9000

**Syntax**

```
show database [backup-status|keyfile|restore-status|statistics|status|users] {on <DEVICE-NAME>}
```

**Parameters**

- `show database [backup-status|keyfile|restore-status|statistics|status|users] {on <DEVICE-NAME>}`

| | |
|---|---|
| database | Displays all configured database-related statistics and status |
| backup-status | Displays the last database backup status |
| keyfile | Displays the keyfiles generated on the database host to enable authenticated database access |
| back-restore | Displays the last database restore status |
| statistics | Displays database-related statistics, such as name of the database (NSight or captive portal), data size, storage size, free disk space available, etc. |
| status | Displays database status, such as online time. |
| users | Displays database users created. These are the users that can access the databases. |
| on <DEVICE-NAME> | Optional. Displays database-related information on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

**Example**

```
vx9000-D031F2(config)#show database backup-status detail
Last Database Backup Status : Failed(Error in ftp: 1)
Last Database Backup Time   : 2017-04-11 08:03:10
-----------------------------------------------
Starting backup of mart ...
connected to: 127.0.0.1
2015-05-20T14:02:46.340+0530 DATABASE: mart         to         dump/mart
2015-05-20T14:02:46.341+0530         mart.system.indexes to dump/mart/
system.indexes.bson
2015-05-20T14:02:46.341+0530                  61 documents
2015-05-20T14:02:46.341+0530         mart.wlan_info to dump/mart/wlan_info.bson
2015-05-20T14:02:46.341+0530                  5 documents
2015-05-20T14:02:46.342+0530         Metadata for mart.wlan_info to dump/mart/
wlan_info.metadata.json
2015-05-20T14:02:46.342+0530         mart.rf_domain_info to dump/mart/
rf_domain_info.bson
2015-05-20T14:02:46.342+0530                  21 documents
2015-05-20T14:02:46.342+0530        Metadata for mart.rf_domain_info to dump/mart/
rf_domain_info.metadata.json
--More--
vx9000-D031F2(config)#
```

```
vx9000-D031F2(config)#show database status
-------------------------------------------------------------------------------
        MEMBER             STATE                      ONLINE TIME
-------------------------------------------------------------------------------
  localhost           PRIMARY           2 days 3 hours 45 min 24 sec
-------------------------------------------------------------------------------
 Authentication: Disabled                Authentication User: None
-------------------------------------------------------------------------------
[*] indicates this device.
vx9000-D031F2(config)#

vx9000-D031F2(config)#show database statistics
-------------------------------------------------------------------------------
       DATABASE        STORAGE SIZE   DATA SIZE     INDEX SIZE     DISK FREE
-------------------------------------------------------------------------------
  admin               32k             335           48k            594.5G
  captive-portal      4k              0             24k            594.5G
  nsightcache         96k             2.0k          264k           594.5G
  nsight              26.1M           136.6M        18.9M          594.5G
-------------------------------------------------------------------------------
vx9000-D031F2(config)#

nx9500-6C8809#show database keyfile

SLz6lVXyi9vyTCChUKs04THRo3mWOjZheM58Dt6NC0MDkdgV+5+wWN9/IT6zfy1s
KPut4BPpUWyM8MEaRmapg4kRrN/SMSMlH6sPITMGTLMu6wRYFEUgKgO01Wn/BohE
5n+uuhY0xiZQsN0LS7IaA8Yb9rX859YRQ7v9By5aEpi1NIDR4KX09Xs3TqIB+5v2
jE3vv7OsKK+LX63bCIoYo35MX251T2pHdL+fMdLfKPMt8ZbzYzx2b22Yvukfg0gm
xHsMCB+bLAsfkjeCPgHCAq/WWi3Kxna6ysFjp8J4US2Bm+GL1COvALbCQBwkPPN+
o7M90qT40AubibBkeID2S9rkQkKcXqGESbL5xG6ip+26jIxiLv7GP6/SQZGFOqC/
ZZEkCNhGhkiyktiOIxBfoXwoy66sqQ4KBwLF449eqBe7Svel/dzpFPNfYZpW8SMY
LD6iLTPR9BddjsBBej8kGGc5R+M0R6lgQFEew2WX6Rqz45YTGEcfOkl8c9wl3taD
xn4imhI/esjMppFDu5muxRHF5RHa5RncTGnsMfc7ndvUl78QaGHLZvDqjNLBUnuP
c8QmyohEnKf70TYx/ruG9Vb2AP0Jw5OODTNh2lmaoFjicKYQr+xIHUJpHc0qY43C
5WzlWf84CK67cu7kOPiJoaxvufzSXhJB18BiCXTuv40+ZZ6e3PcisZuIrPXxCZup
GJ3KpuHq61IJyVCydFd5zl4Fho+RGaQ9dlDIlaLjbW+YT4CEH1bTiUmreUt+D/X2
zcB9nec77wIIAcdfl2qysgGIqmkI3jRI89d3XM5Y7Kc2TuXBVZOazYldPj+qE/yi
EgVWcbtvyS834jit35MGbVXhvQ2d45qgo42WZwdTVLXC9memzoKa3YIZoj32uP3U
iOrzD8E1gMte4gDE/KmGkYya+hsWswBmKC1v0gj5NQ6TejYS4z+nefqLHUSVXbQ8
NxRel1huGi8P1ns4dWCwClWp8GpxUTa7GuN1DySA7/l2OJM=

nx9500-6C8809#
```

## 6.1.18 device-upgrade

*show commands*

Displays device firmware upgradation information for devices adopted by a wireless controller or access point

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show device-upgrade [history|load-image-status|status|versions]

show device-upgrade [history {on <DOMAIN-NAME>}|load-image-status|versions {on
<DEVICE-OR-DOMAIN-NAME>}

show device-upgrade status {on [<DOMAIN-NAME>|rf-domain-manager]|summary {on
<DOMAIN-NAME>}}
```

**Parameters**

• `show device-upgrade [history {on <DOMAIN-NAME>}|load-image-status|versions {on <DEVICE-OR-DOMAIN-NAME>}]`

| | |
|---|---|
| device-upgrade | Displays device upgrade information based on the parameters passed |
| history {on <DOMAIN-NAME>} | Displays device upgrade history<br>• on <DOMAIN-NAME> – Optional. Displays upgrade history for all devices within a specified RF Domain. Specify the RF Domain name. |
| load-image-status | Displays firmware image loading status. The output displays the <DEVICE> image loading status in percentage.<br>For example:<br>`#show device-upgrade load-image-status`<br>`Download of ap81xx firmware file is 47 percent complete` |
| versions {on <DEVICE-OR-DOMAIN-NAME>} | Displays firmware image versions<br>• on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays firmware image versions loaded on specified device or RF Domain. Specify the name of the AP, wireless controller, service platform, or RF Domain.<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the AP, wireless controller, service platform, or RF Domain name. |

• `show device-upgrade status {on [<DOMAIN-NAME>|rf-domain-manager]|summary {on <DOMAIN-NAME>}}]`

| | |
|---|---|
| device-upgrade | Displays device upgrade information based on the parameters passed |
| status | Displays in progress device upgrade status |
| on [<DOMAIN-NAME>\| rf-domain-manager] | Optional. Displays in progress upgrade status of all devices within a specified RF Domain, or all devices upgraded by the RF Domain manager. Use this option to view upgrade status of multiple devices.<br>• <DOMAIN-NAME> – Specify the RF Domain name.<br>• rf-domain-manager – Select to view devices upgraded by the RF Domain manager. |

| | |
|---|---|
| summary {on <DOMAIN-NAME>} | Displays a summary of in-progress upgrade processes<br>• on <DOMAIN-NAME> – Optional. Displays in-progress upgrade processes within a specified RF Domain<br>• <DOMAIN-NAME> – Specify the RF Domain name. |

**Example**

```
nx9500-6C8809#device-upgrade load-image rfs6000 ftp://anonymous:anonymous@192.16
8.13.10/LatestBuilds/W59/RFS6000-LEAN.img

nx9500-6C8809#show device-upgrade load-image-status
Download of rfs6000 firmware file is complete
nx9500-6C8809#

nx9500-6C8809#show device-upgrade status
Number of devices currently being upgraded : 0
Number of devices waiting in queue to be upgraded : 1
Number of devices currently being rebooted : 0
Number of devices waiting in queue to be rebooted : 0
Number of devices failed upgrade : 0
--------------------------------------------------------------------------------
-------------------------
      DEVICE        STATE   UPGRADE TIME REBOOT TIME PROGRESS RETRIES LAST UPDATE
ERROR   UPGRADED BY
--------------------------------------------------------------------------------
-------------------------
  rfs6000-81742D   waiting   immediate    immediate   0       0      -
nx9500-6C8809
--------------------------------------------------------------------------------
-------------------------
nx9500-6C8809#
```

## 6.1.19 dot1x

*show commands*

Displays dot1x information on interfaces

Dot1x (or 802.1x) is an IEEE standard for network authentication. Devices supporting dot1x allow the automatic provision and connection to the wireless network without launching a Web browser at login. When within range of a dot1x network, a dot1X-enabled device automatically connects and authenticates without needing to manually login.

However, dot1x-enabled devices can be configured either as:

- supplicants only – Devices seeking network access
- authenticators only – Devices authenticating the supplicants, or
- supplicants as well authenticators

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**NOTE:** Dot.1x supplicant configuration is supported on the following platforms:

- Access Points – AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers – RFS4000
- Service Platforms – NX5500, NX7500

**NOTE:** Dot.1x authenticator configuration is supported on the following platforms:

- Access Points – AP6521, AP6522, AP6562, AP7161, AP7502, AP81XX
- Wireless Controllers – RFS4000, RFS6000
- Service Platforms – NX5500, NX7500

**Syntax**

```
show dot1x {all|interface|on}

show dot1x {all {on <DEVICE-NAME>}|on <DEVICE-NAME>}

show dot1x {interface [<INTERFACE-NAME>|ge <1-4>|port-channel <1-2>} {on <DEVICE-NAME>}
```

**Parameters**

- `show dot1x {all {on <DEVICE-NAME>}|on <DEVICE-NAME>}`

| | |
|---|---|
| dot1x all<br>{on <DEVICE-NAME>} | Optional. Displays dot1x information for all interfaces<br>• on <DEVICE-NAME> – Optional. Displays dot1x information for all interfaces on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

| | |
|---|---|
| dot1x {on <DEVICE-NAME>} | Optional. Displays dot1x information for interfaces on a specified device<br>• <DEVICE-NAME> – Specify the name of AP, wireless controller, or service platform. |

• `show dot1x {interface [<INTERFACE-NAME>|ge <1-4>|port-channel <1-2>]} {on <DEVICE-NAME>}`

| | |
|---|---|
| dot1x interface | Optional. Displays dot1x information for a specified interface or interface type |
| <INTERFACE-NAME> | Displays dot1x information for the layer 2 (Ethernet port) interface specified by the <INTERFACE-NAME> parameter |
| ge <1-4> | Displays dot1x for a specified GigabitEthernet interface<br>• <1-4> – Select the interface index from 1 - 4. |
| port-channel <1-2> | Displays dot1x for a specified port channel interface<br>• <1-2> – Select the interface index from 1 - 2. |
| on <DEVICE-NAME> | The following keywords are common to all of the above parameters:<br>• on <DEVICE-NAME> – Optional. Displays dot1x interface information on a specified device<br>• <DEVICE-NAME> – Specify the name of AP, wireless controller, or service platform. |

**Example**

```
rfs6000-81742D#show dot1x all
802.1X information
------------------------------
  SysAuthControl : disabled
  Guest-Vlan     : disabled
  AAA-Policy     : none
  Holdtime       : 60

802.1X information for interface GE1
--------------------------------------
Supplicant MAC N/A
  Auth SM State : FORCE AUTHORIZED
  Bend SM State : REQUEST
  Port Status   : AUTHORIZED
  Host Mode     : SINGLE
  Auth Vlan     : None
  Guest Vlan    : None

802.1X information for interface GE2
--------------------------------------
Supplicant MAC N/A
  Auth SM State : FORCE AUTHORIZED
  Bend SM State : REQUEST
  Port Status   : AUTHORIZED
--More--
rfs6000-81742D#

rfs6000-81742D#show dot1x interface ge 1
802.1X information for interface GE1
--------------------------------------
Supplicant MAC N/A
  Auth SM State : FORCE AUTHORIZED
  Bend SM State : REQUEST
  Port Status   : AUTHORIZED
  Host Mode     : SINGLE
  Auth Vlan     : None
  Guest Vlan    : None

rfs6000-81742D#
```

## 6.1.20 dpi

*show commands*

Displays *Deep Packet Inspection* (DPI) statistics for all configured and canned applications. DPI is an advanced packet analysis technique, which analyzes packet and packet content headers to determine the nature of network traffic. When DPI is enabled, packets of all flows are subjected to DPI to get accurate results. DPI identifies applications (such as, Netflix, Twitter, Facebook, etc.) and also extracts metadata (such as, host name, server name, TCP-RTT, etc.) for further use by the WiNG firewall.

**NOTE:** The *show > dpi* command returns results only if executed on a device that supports DPI and has DPI logging enabled. DPI logging can be enabled either on the device or on the profile applied to the device. For more information, see *dpi*.

**Supported in the following platforms:**

- Access Points — AP7522, AP7532, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8432, AP8533
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show dpi [app|app-category|application|application-policy|per-category]

show dpi app wireless-clients stats <MAC> {on <DEVICE-OR-DOMAIN-NAME>}

show dpi [app|app-category] stats [<APPLICATION/APP-CATEGORY-NAME>|all] {on
<DEVICE-OR-DOMAIN-NAME>}

show dpi application-policy stats <APPLICATION-POLICY-NAME> {on <DEVICE-OR-DOMAIN-
NAME>}

show dpi application brief

show dpi per-category stats <APP-CATEGORIES> [bytes-in|bytes-out|total-bytes] {on
<DEVICE-OR-DOMAIN-NAME>}
```

**Parameters**

- `show dpi app wireless-clients stats <MAC> {<DEVICE-OR-DOMAIN-NAME>}`

| | |
|---|---|
| dpi app wireless-clients <MAC> | Displays application-related statistics for all or a specified wireless clients<br>• <MAC> – Displays statistics for a specified wireless client. Specify the client's MAC address. |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Displays statistical data on a specified device or RF Domain<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the access point, wireless controller, service platform, or RF Domain. |

- `show dpi [app|app-category] stats [<APPLICATION/APP-CATEGORY-NAME>|all] {on <DEVICE-OR-DOMAIN-NAME>}`

| | |
|---|---|
| dpi [app\| app-category] stats | Displays statistics for a application or application category<br>• app – Displays statistics for a specified application or all applications<br>• app-category – Displays statistics for a specified application category or all categories.<br>**Note:** The applications are the RF Domain member allowed applications whose data (bytes) are passing through the WiNG managed network. And, the application categories are existing WiNG or user defined application groups (video, streaming, mobile, audio, etc.) that assist administrators to permit or deny forwarding of application data. |
| [<APPLICATION/APP-CATEGORY-NAME>\|all] | This parameter is common to the 'app' and 'app-category' keywords.<br>• <APPLICATION/APP-CATEGORY-NAME> – Displays statistics for a specified application or application category, depending on the option selected in the previous step. Specify the application name or application category name.<br>• all – Displays statistics for all applications or application categories, depending on the option selected in the previous step |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Displays statistical data on a specified device or RF Domain<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the access point, wireless controller, service platform, or RF Domain. |

- `show dpi application-policy stats <APPLICATION-POLICY-NAME> {on <DEVICE-OR-DOMAIN-NAME>}`

| | |
|---|---|
| dpi application-policy stats | Displays statistics for an existing application policy |
| <APPLICATION-POLICY-NAME> | Displays statistics for a specified application-policy. Specify the application-policy name. |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Displays application-policy related statistical data on a specified device or RF Domain<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the access point, wireless controller, service platform, or RF Domain. |

- `show dpi application brief`

| | |
|---|---|
| dpi application brief | Displays a brief summary of applications their status and configuration |

- `show dpi per-category stats <APP-CATEGORIES> [bytes-in|bytes-out|total-bytes] {on <DEVICE-OR-DOMAIN-NAME>}`

| | |
|---|---|
| dpi per-category stats | Displays statistics for the top ten applications based on the application category and the Sort ID specified. The Sort ID options are: bytes-in, bytes-out or total-bytes. |
| <APP-CATEGORIES> | Specify the application category name. The system displays statistics for the top ten applications in this category. |

| | |
|---|---|
| [bytes-in\|bytes-out\|total-bytes] | Filters and displays statistical data for the top ten utilized applications in respect to the following:<br>• bytes-in – Displays total data bytes uploaded through the controller managed network. If this application data is not aligned with application utilization expectations, consider allowing or denying additional applications and categories or adjusting their precedence (priority).<br>• bytes-out – Displays total data bytes downloaded through the controller managed network. If this application data is not aligned with application utilization expectations, consider allowing or denying additional applications and categories or adjusting their precedence (priority).<br>• total-bytes – Displays total data bytes (uploaded and downloaded) through the controller managed network. These are only the administrator allowed applications approved for proliferation within the managed network. |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Displays statistical data on a specified device or RF Domain<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the access point, wireless controller, service platform, or RF Domain. |

**Example**

```
nx9500-6C8809>show dpi application brief
    1-clickshare-com
        This application recognizes DirectDownloadLink 1-clickshare
        traffic
        Application Category   : filetransfer
        Predefined Application : Yes
    1-upload-com
        This application recognizes DirectDownloadLink 1-upload-com
        traffic
        Application Category   : filetransfer
        Predefined Application : Yes
    1-upload-to
        This application recognizes DirectDownloadLink 1-upload-to
        traffic
        Application Category   : filetransfer
        Predefined Application : Yes
    10upload-com
        This application recognizes DirectDownloadLink 10upload-com
        traffic
        Application Category   : filetransfer
        Predefined Application : Yes
    123upload-pl
        This application recognizes DirectDownloadLink 123upload-pl
        traffic
--More--
nx9500-6C8809>
```

## 6.1.21 eguest

*show commands*

Displays EGuest server status and EGuest registration statistics

**Supported in the following platforms:**

- Service Platforms — NX9500, NX9510, NX9600, VX9000

**Syntax**

```
eguest [registration statistics|status]
```

**Parameters**

- `eguest [registration statistics|status]`

| | |
|---|---|
| registration statistics | Displays the EGuest registration statistics |
| status | Displays the current status of EGuest servers |

**Example**

```
vx-eguest-primary#show eguest status
-----------------------------------
pid                 process
-----------------------------------
2521                 gmd
2529                 regserver
2539                 acct_server
2569                 guest_manager
2636                 acct_server
2642                 acct_server
2643                 acct_server
2649                 acct_server
2655                 acct_server
2708                 acct_server-helper
2770                 guest_manager
2776                 guest_manager
2777                 guest_manager
2783                 guest_manager
3628                 gmd
3630                 gmd
3631                 gmd
3632                 gmd
3633                 gmd
3634                 gmd
5729                 radiusd
-----------------------------------
Database server is local
Database server is reachable
vx-eguest-primary#

vx-eguest-primary#show eguest registration statistics
msg_received    - number of registration messages received
user_try_to_add - number of database add attempts
user_added      - number of messages succesfully added to db
user_failed     - number of messages failed adding to db
-------------------------------------------------------------------------
msg_received      user_try_to_add          user_added      user_failed
-------------------------------------------------------------------------
189                  11                         11            0
vx-eguest-primary#
```

## 6.1.22 environmental-sensor

*show commands*

Displays environmental sensor's recorded data. The environmental sensor has to be enabled and configured in order to collect data related to humidity, light, motion, and temperature.

**NOTE:** The environmental senor is supported only on an AP8132. When executed on any controller (other than an AP8132), the *show > environmental-sensor > <parameters>* command displays environmental-sensor details for adopted AP8132s (if any).

**Supported in the following platforms:**

- Access Points — AP8132

**Syntax**

```
show environmental-sensor [history|humidity|light|motion|summary|temperature|
version]

show environmental-sensor history {<1-HOUR>|<20-MINUTE>|<24-HOUR>}

show environmental-sensor [humidity|light|motion|summary|temperature|version]
```

**Parameters**

- `show environmental-sensor history {<1-HOUR>|<20-MINUTE>|<24-HOUR>}`

| | |
|---|---|
| environmental-sensor history | Displays environmental sensor history once in every hour, 20 minutes, or 24 hours<br>History includes the humidity, light, motion, and temperature data recorded by the sensor at specified time interval. |
| 1-hour | Optional. Displays environmental sensor history once in every 1 (one) hour |
| 20-minute | Optional. Displays environmental sensor history once in every 20 minutes |
| 24-hour | Optional. Displays environmental sensor history once in every 24 hours |

- `show environmental-sensor [humidity|light|motion|summary|temperature|version]`

| | |
|---|---|
| environmental-sensor | Displays environmental sensor's recorded data, based on the parameters passed. The system displays the specified recorded data.<br>The environmental sensor records data at the following intervals: 20 minutes, 1 hour, and 24 hours. |
| humidity | Displays the minimum, average, and maximum humidity recorded |
| light | Displays the minimum, average, and maximum light recorded |
| motion | Displays the minimum, average, and maximum motion recorded |
| temperature | Displays the minimum, average, and maximum temperature recorded |
| version | Displays the hardware and firmware versions |
| summary | Displays a summary of the data recorded at following intervals: |

**Example**

```
ap8132-711728#show environmental-sensor summary
Maat Device uptime: 0 days 15:25:11
ERROR: Maat device is offline!
threshold polling-interval: 5
historical data polled 0 times per 2-minutes interval since Maat online

motion-sensor: Enabled(Demo)
  current value: 0 detected
  -------------------------------
                motion detected
  -------------------------------
  20-minute           0
  1-hour              0
  6-hour              0
  24-hour             0

temperature-sensor: Enabled(Demo)
  current value: -40.00 deg. C
  -------------------------------
                min/average/max
  -------------------------------
  20-minute         0/0/0
  1-hour            0/0/0
  6-hour            0/0/0
  24-hour           0/0/0

light-sensor: Enabled
  threshold-high:+400.00 threshold-low:+200.00 holdtime:11
  action radio-shutdown: radio-1 and radio-2
  light-on:1
  light-on/off event sent:0/0
  current value: 0.00 lux
  -------------------------------
                min/average/max
  -------------------------------
  20-minute         0/0/0
  1-hour            0/0/0
  6-hour            0/0/0
  24-hour           0/0/0

humidity-sensor: Enabled(Demo)
  current value: 0.00 %
  -------------------------------
                min/average/max
  -------------------------------
  20-minute         0/0/0
  1-hour            0/0/0
  6-hour            0/0/0
  24-hour           0/0/0
ap8132-711728#

ap8132-711634#show env-sensor history
Current Time: 2015-06-20 14:08:01 UTC
-------------------------------------------------------------------------------
     Sample-Interval          Motion    Temperature     Light       Humidity
                                          (deg. C)       (lux)         (%)
                                        ----------- min/average/max ------------
-------------------------------------------------------------------------------
20-minute                       1         64/65/66      77/80        58/60/61
1-hour                         24         63/67/70      75/81        57/59/61
6-hour                        128         60/62/69      71/79        52/56/71
24-hour                       188         54/58/70      15/45        49/57/73
ap8132-711634#
```

```
ap8132-711634#show env-sensor history 20-min
-------------------------------------------------------------------------------
-
timestamp                  Motion    Temperature    Light        Humidity
-------------------------------------------------------------------------------
-
2015-11-20 13:51:35 UTC     0           66          79            59
2015-11-20 13:53:35 UTC     0           66          79            59
2015-11-20 13:55:35 UTC     0           65          79            58
2015-11-20 13:57:35 UTC     1           66          80            59
2015-11-20 13:59:35 UTC     0           66          79            59
2015-11-20 14:02:35 UTC     0           65          79            60
2015-11-20 14:03:35 UTC     0           64          79            60
2015-11-20 14:05:35 UTC     2           66          80            60
2015-11-20 14:07:35 UTC     0           66          80            61
2015-11-20 14:09:35 UTC     0           66          80            61
ap8132-711634#

ap8132-711634#show env-sensor history 1-hr
-------------------------------------------------------------------------------
--timestamp                 Motion    Temperature    Light        Humidity
-------------------------------------------------------------------------------
--
2015-11-20 13:51:35 UTC     0           66          79            59
2015-11-20 13:53:35 UTC     0           66          79            59
2015-11-20 13:55:35 UTC     0           65          79            58
2015-11-20 13:57:35 UTC     1           66          80            59
2015-11-20 13:59:35 UTC     0           66          79            59
2015-11-20 14:01:35 UTC     0           65          79            60
2015-11-20 14:03:35 UTC     0           64          79            60
2015-11-20 14:05:35 UTC     2           66          80            60
2015-11-20 14:07:35 UTC     0           66          80            61
2015-11-20 14:09:35 UTC     0           66          80            61
2015-11-20 14:42:35 UTC     0           65          81            60
2015-11-20 14:43:35 UTC     0           64          80            59
2015-11-20 14:45:35 UTC     3           66          80            60
ap8132-711634#

<DEVICE-NAME>#show env-sensor history 24-hr
-------------------------------------------------------------------------------
--
timestamp                  Motion    Temperature    Light        Humidity
-------------------------------------------------------------------------------
--
2015-11-20 10:10:20 UTC    27           66          80            60
2015-11-20 10:30:20 UTC    17           66          80            60
2015-11-20 10:50:20 UTC    17           66          81            60
2015-11-20 11:10:20 UTC    25           66          81            60
2015-11-20 11:30:20 UTC    24           66          81            60
2015-11-20 11:50:20 UTC    26           66          81            60
2015-11-21 08:10:20 UTC     9           65          80            59
2015-11-21 08:30:20 UTC     7           65          80            59
2015-11-21 08:50:20 UTC    12           65          80            60
2015-11-21 09:10:20 UTC    10           65          80            60
2015-11-21 09:30:20 UTC    15           65          80            60
2015-11-21 09:50:20 UTC    19           66          80            60
<DEVICE-NAME>#
```

## 6.1.23 event-history

*show commands*

Displays event history report

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show event-history {on <DEVICE-OR-DOMAIN-NAME>}
```

**Parameters**

- `show event-history {on <DEVICE-OR-DOMAIN-NAME>}`

| | |
|---|---|
| event-history | Displays event history report |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Displays event history report on a device or RF Domain<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |

**Example**

```
nx9500-6C8809#show event-history
Generated on '2016-09-21 05:19:55 UTC' by 'admin'

2017-06-06 10:40:19 nx9500-6C8809  SYSTEM     LOGIN                Successfully
logged in user 'admin' with privilege 'superuser' from 'ssh'
2017-06-06 10:38:36 nx9500-6C8809  SYSTEM     LOGOUT             Logged out user
'admin' with privilege 'superuser' from '192.168.100.214'
2017-06-06 10:27:34 nx9500-6C8809  SYSTEM     LOGIN                Successfully
logged in user 'admin' with privilege 'superuser' from 'ssh'
2017-06-06 10:27:34 nx9500-6C8809  SYSTEM     LOGOUT             Logged out user
'admin' with privilege 'superuser' from '192.168.100.214'
2016-09-20 23:52:49     nx9500-6C8809  SYSTEM     LOGIN              Successfully
logged in user 'admin' with privilege 'superuser' from 'ssh'
2016-09-20 05:39:01     nx9500-6C8809  SYSTEM     LOGOUT               Logged out
user 'admin' with privilege 'superuser' from '192.168.100.165'
2016-09-20 05:08:54     nx9500-6C8809  SYSTEM     LOGIN              Successfully
logged in user 'admin' with privilege 'superuser' from 'ssh'
--More--
nx9500-6C8809#
```

## 6.1.24 event-system-policy

*show commands*

Displays detailed event system policy configuration

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show event-system-policy [config|detail] <EVENT-SYSTEM-POLICY-NAME>
```

**Parameters**

- `show event-system-policy [config|detail] <EVENT-SYSTEM-POLICY-NAME>`

| | |
|---|---|
| event-system-policy | Displays event system policy configuration |
| config | Displays configuration for a specified policy |
| detail | Displays detailed configuration for a specified policy |
| <EVENT-SYSTEM-POLICY-NAME> | Specify the event system policy name. |

**Example**

```
rfs6000-81742D(config)#show event-system-policy config testpolicy
--------------------------------------------------------------------------------
MODULE          EVENT             SYSLOG    SNMP   FORWARD        EMAIL
--------------------------------------------------------------------------------
aaa       radius-discon-msg      on        on      on         default
--------------------------------------------------------------------------------
rfs6000-81742D(config)#
```

## 6.1.25 ex3500

*show commands*

Displays EX3500-related statistical data

**Supported in the following platforms:**

- Service Platforms — NX7500, NX9500

**Syntax**

```
show ex3500 [dir|interfaces|system|upgrade|version|whichboot]

show ex3500 dir {boot-rom|config|on|opcode} {<FILE-NAME>} {on <EX3500-DEVICE-NAME>}

show ex3500 interfaces counters [ether-like stats|ethernet <1-1> <1-52>|ext-if-table stats|if-table stats|portUtil stats|rmon stats] {on <EX3500-DEVICE-NAME>}

show ex3500 [system|upgrade|version|whichboot] {on <EX3500-DEVICE-NAME>}
```

**Parameters**

```
• show ex3500 dir {boot-rom|config|on|opcode} {<FILE-NAME>} {on <EX3500-DEVICE-NAME>}
```

| | |
|---|---|
| ex3500 dir | Displays EX3500 directory information based on the option selected. The options are: boot-rom, config, opcode<br>**Note:** If none of the specified options is selected, all EX3500 system-related information is displayed. |
| boot-rom | Optional. Displays only the Boot-ROM information |
| config | Optional. Displays only the configuration file |
| opcode | Optional. Displays only the run-time operation code |
| <FILE-NAME> | Displays the contents of a specified file identified by the <FILE-NAME> keyword. This is the name of configuration file or code image. |
| on <EX3500-DEVICE-NAME> | Optional. Executes the command on a specified EX3500 device<br>• <DEVICE-NAME> – Specify the device's name. |

```
• show ex3500 interfaces counters [ether-like stats|ethernet <1-1> <1-52>|ext-if-table stats|if-table stats|portUtil stats|rmon stats] {on <EX3500-DEVICE-NAME>}
```

| | |
|---|---|
| ex3500 interfaces counters | Displays EX3500 interface counter information based on the option selected. The options are: ether-like, ethernet, ext-if-table, if-table, portUtil, rmon |
| ether-like stats | Displays *Managed Information Base* (MIB) object statistics for Ethernet-like interfaces |
| ethernet <1-1> <1-52> | Displays the Ethernet port statistics based on the unit identifier and port number selected<br>• <1-1> – Specify the EX3500 unit's identifier from 1 - 1.<br>• <1-52> – Specify the port number from 1 - 52. This range varies for the EX3524 (1-28) and EX3548 (1-52) devices.<br>**Note:** This option displays the following for the selected Ethernet interface: extended interface table stats, interface table stats, port utilization information, and remote monitoring stats. |
| ext-if-table stats | Displays only the extended interface table statistics |

| | |
|---|---|
| if-table stats | Displays only the interface table statistics |
| portUtil stats | Displays only the port utilization information |
| rmon stats | Displays only *remote monitoring* (RMon) statistics |
| on <EX3500-DEVICE-NAME> | Optional. Executes the command on a specified EX3500 device<br>• <DEVICE-NAME> – Specify the device's name. |

- `show ex3500 [system|upgrade|version|whichboot] {on <EX3500-DEVICE-NAME>}`

| | |
|---|---|
| ex3500 | Displays the following information for a specified EX3500 device or all EX3500 devices in the managed network |
| system | Displays EX3500 system information, such as device description, OID string, up time, name, location, contact, MAC address, etc. Some of these information (example, system name) are configurable items, and if not configured are left blank. |
| upgrade | Displays the opcode upgrade configuration settings |
| version | Displays hardware and software version information for a EX3500 system |
| whichboot | Displays boot information |
| on <EX3500-DEVICE-NAME> | Optional. Executes the command on a specified EX3500 device<br>• <DEVICE-NAME> – Specify the device's name. |

**Example**

```
nx9500-6C8809#show ex3500 interfaces counters ethernet 1 17
Ethernet 1/ 17
===== IF table Stats =====
2166458 Octets Input
14734059 Octets Output
14707 Unicast Input
19806 Unicast Output
0 Discard Input
0 Discard Output
0 Error Input
0 Error Output
0 Unknown Protocols Input
0 QLen Output
===== Extended Iftable Stats =====
23 Multi-cast Input
5525 Multi-cast Output
170 Broadcast Input
11 Broadcast Output
===== Ether-like Stats =====
0 Alignment Errors
0 FCS Errors
0 Single Collision Frames
0 Multiple Collision Frames
0 SQE Test Errors
0 Deferred Transmissions
0 Late Collisions
0 Excessive Collisions
0 Internal Mac Transmit Errors
0 Internal Mac Receive Errors
0 Frames Too Long
0 Carrier Sense Errors
0 Symbol Errors
0 Pause Frames Input
0 Pause Frames Output
===== RMON Stats =====
0 Drop Events
16900558 Octets
40243 Packets
```

```
170 Broadcast PKTS
23 Multi-cast PKTS
0 Undersize PKTS
0 Oversize PKTS
0 Fragments
0 Jabbers
0 CRC Align Errors
0 Collisions
21065 Packet Size <= 64 Octets
3805 Packet Size 65 to 127 Octets
2448 Packet Size 128 to 255 Octets
797 Packet Size 256 to 511 Octets
2941 Packet Size 512 to 1023 Octets
9187 Packet Size 1024 to 1518 Octets
===== Port Utilization (recent 300 seconds) =====
0 Octets Input in kbits per second
0 Packets Input per second
0.00 % Input Utilization
0 Octets Output in kbits per second
0 Packets Output per second
0.00 % Output Utilization
nx9500-6C8809#
```

## 6.1.26 extdev

*show commands*

Displays external device (T5 or EX3500) configuration error history

**Supported in the following platforms:**

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510

**Syntax**

```
show extdev error history {on <T5/EX3500-DEVICE-NAME>}
```

**Parameters**

- `show extdev error history {on <T5/EX3500-DEVICE-NAME>}`

| | |
|---|---|
| extdev error history | Displays external device error history. This command is applicable only to the external devices T5, and EX3500 series switches. Use this command to view configuration error history for all or a specified external device adopted and managed by a WiNG NX9500 series service platform. |
| on <T5/EX3500-DEVICE-NAME> | Optional. Displays configuration error history on a specified T5 or EX3500 device<br>• <T5/EX3500-DEVICE-NAME> – Specify the name of the device. |

**Example**

```
nx9500-6C8809#show extdev error history on t5-ED5EAC
%% No History for this device
nx9500-6C8809#
```

## 6.1.27 file-sync

*show commands*

Displays file synchronization settings and status on a controller

The *file-sync* command syncs *wireless-bridge certificate* and *trustpoint* between the staging-controller and its adopted access points. The *show > file-sync* command displays information related to this process.

**Supported in the following platforms:**

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510

**Syntax**

```
show file-sync [configuration|history|load-file-status|status] {on <DEVICE-OR-DOMAIN-NAME>}
```

**Parameters**

```
• show file-sync [configuration|history|load-file-status|status] {on <DEVICE-OR-DOMAIN-NAME>}
```

| | |
|---|---|
| file-sync | Displays the following file-synchronization (trustpoint and wireless-bridge certificate) related information: configuration, history, load-file-status, and status |
| configuration | Displays the following file-synchronization configuration details:<br>• automatic file-syncing enabled or disabled. The default setting is disabled.<br>The X.509 certificate needs synchronization only if the access point's radio2 is configured to use EAP-TLS authentication. In which case PKCS#12 certificate needs to be pushed on AP adoption. To enable automatic file syncing, in the controller's device/profile configuration mode, execute the *file-sync > auto* command. For more information, see *file-sync*.<br>• Number of access points to which the certificate can be simultaneously uploaded. The default is 10.<br>To modify the number of simultaneous uploads, in the controller's device/profile configuration mode, execute the *file-sync > count <1-20>* command. For more information, see *file-sync*.<br>• Scheduled certificate upload, if any, details, such time and date of upload.<br>To schedule certificate upload, use the *file-sync > wireless-certificate* command. For more information, see *file-sync*. |
| history | Displays file synchronization history. Use this option to view statistical data relating to wireless-bridge certificate synchronization between staging controller and its access points. When executed, a list of all certificate transfers made to the APs is displayed, with the latest transfer listed at the top. |
| load-file-status | Displays the status of the file upload to the controller. Use this command to view the status of a in-progress certificate upload,<br>For more information on initiating a PKCS#12 certificate upload, see *file-sync*. |
| status | Displays status of the file synchronization between the controller and its adopted access point. |

| | |
|---|---|
| on <DEVICE-OR-DOMAIN- NAME> | Optional. Displays file synchronization settings and status on a specified device or RF Domain<br>• <DEVICE-OR-DOMAIN- NAME> – Specify the name of the controller, service platform, or RF Domain. |

**Example**

```
nx9500-6C8809#show file-sync configuration
File Sync Configuration Information
  Auto                           : Disabled
  Simultaneous Upload Count      : 128
  Wireless Bridge Cert Load Time : Thu May 29 23:23:35 2015
nx9500-6C8809#

nx9500-6C8809#show file-sync load-file-status
Download of wireless_bridge certificate is complete
nx9500-6C8809#

nx9500-6C8809#show file-sync history
-------------------------------------------------------------------------------------
     AP       RESULT          TIME    RETRIES    SYNCED-BY         LAST-SYNC-ERROR
-------------------------------------------------------------------------------------
AP6522-491220   done    2015-05-27 01:37:32   B4-C7-99-6C-88-09       -
ME733ANACBMOT21 done    2015-05-27 02:02:51   0 B4-C7-99-6C-88-09     -
nx9500-6C8809#
```

## 6.1.28 firewall

*show commands*

Displays wireless firewall information, such as *Dynamic Host Configuration Protocol* (DHCP) snoop table entries, denial of service statistics, active session summaries, etc.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show firewall [dhcp|flows|neighbors]

show firewall dhcp snoop-table {on <DEVICE-NAME>}

show firewall flows {filter|management|on|stats|wireless-client}

show firewall flows {filter} {(dir|dst port <1-65535>|ether|flow-type|icmp|
icmpv6|igmp|ip|ipv6|max-idle|min-bytes|min-idle|min-pkts|not|port|src|tcp|udp)}

show firewall flows {management {on <DEVICE-NAME>}|stats {on <DEVICE-NAME>}|
wireless-client <MAC>|on <DEVICE-NAME>}

show firewall neighbors snoop-table {on <DEVICE-NAME>}
```

**Parameters**

- `show firewall dhcp snoop-table {on <DEVICE-NAME>}`

| | |
|---|---|
| firewall dhcp snoop-table | Displays DHCP snoop table entries<br>• snoop-table – Displays DHCP snoop table entries<br>DHCP snooping acts as a firewall between non-trusted hosts and the DHCP server. Snoop table entries contain MAC address, IP address, lease time, binding type, and interface information of non-trusted interfaces. |
| on <DEVICE-NAME> | The following keyword is common to the 'DHCP snoop table' and 'DoS stats' parameters:<br>• on <DEVICE-NAME> – Optional. Displays snoop table entries, or DoS stats on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `show firewall flows {filter} {(dir|dst|ether|flow-type|icmp|icmpv6|igmp|ip|ipv6|max-idle|min-bytes|min-idle|min-pkts|not|port|src|tcp|udp)}`

| | |
|---|---|
| firewall flows | Notifies a session has been established |
| filter | Optional. Defines additional firewall flow filter parameters |
| dir [wired-wired\| wired-wireless\| wireless-wired\| wireless-wireless] | Optional. Matches the packet flow direction<br>• wired-wired – Wired to wired flows<br>• wired-wireless – Wired to wireless flows<br>• wireless-wired – Wireless to wired flows<br>• wireless-wireless – Wireless to wireless flows |

| | |
|---|---|
| dst port <1-65535> | Optional. Matches the destination port with the specified port<br>• port <1-65535> – Specifies the destination port number from 1 - 65535 |
| ether [dst <MAC>\| host <MAC>\| src <MAC>\| vlan <1-4094>] | Optional. Displays Ethernet filter options<br>• dst <MAC> – Matches only the destination MAC address<br>• host <MAC> – Matches flows containing the specified MAC address<br>• src <MAC> – Matches only the source MAC address<br>• vlan <1-4094> – Matches the VLAN number of the traffic with the specified value. Specify a value from 1- 4094. |
| flow-type [bridged\|natted\| routed\|wired\| wireless] | Optional. Matches the traffic flow type<br>• bridged – Bridged flows<br>• natted – Natted flows<br>• routed – Routed flows<br>• wired – Flows belonging to wired hosts<br>• wireless – Flows containing a mobile unit |
| icmp {code\|type} | Optional. Matches flows with the specified *Internet Control Message Protocol* (ICMP) version 4 code and type<br>• code – Optional. Matches flows with the specified ICMPv4 code<br>• type – Optional. Matches flows with the specified ICMPv4 type |
| icmpv6 {code\|type} | Optional. Matches flows with the specified ICMP version 6 code and type<br>• code – Optional. Matches flows with the specified ICMPv6 code<br>• type – Optional. Matches flows with the specified ICMPv6 type |
| igmp | Optional.Matches *Internet Group Management Protocol* (IGMP) flows |
| ip [dst <IP>\| host <IP>\| proto <0-254>\| src <IP>] | Optional. Filters firewall flows based on the IPv4 parameters passed<br>• dst <IP> – Matches destination IP address<br>• host <IP> – Matches flows containing IPv4 address<br>• proto <0-254> – Matches the IPv4 protocol number with the specified number<br>• src <IPv4> – Matches source IP address |
| ipv6 [dst <IPv6>\| host <IPv6>\| proto <0-254>\| src <IPv6>] | Optional. Filters firewall flows based on the IPv6 parameters passed<br>• dst <IPv6> – Matches destination IPv6 address<br>• host <IPv6> – Matches flows containing IPv6 address<br>• proto <0-254> – Matches the IPv6 protocol number with the specified number<br>• src <IPv6> – Matches source IPv6 address |
| max-idle <1-4294967295> | Optional. Filters firewall flows idle for at least the specified duration. Specify a max-idle value from 1 - 4294967295 bytes. |
| min-bytes <1-4294967295> | Optional. Filters firewall flows with at least the specified number of bytes. Specify a min-bytes value from 1 - 4294967295 bytes. |
| min-idle <1-4294967295> | Optional. Filters firewall flows idle for at least the specified duration. Specify a min-idle value from 1 - 4294967295 bytes. |
| min-pkts <1-4294967295> | Optional. Filters firewall flows with at least the given number of packets. Specify a min-bytes value from 1 - 4294967295 bytes. |
| not | Optional. Negates the filter expression selected |

| | |
|---|---|
| port <1-65535> | Optional. Matches either the source or destination port. Specify a port from 1 - 65535. |
| src <1-65535> | Optional. Matches only the source port with the specified port. Specify a port from 1 - 65535. |
| tcp | Optional. Matches TCP flows |
| udp | Optional. Matches UDP flows |

- `show firewall flows {management {on <DEVICE-NAME>}|stats {on <DEVICE-NAME>}| wireless-client <MAC>|on <DEVICE-NAME>}`

| | |
|---|---|
| firewall flows | Notifies a session has been established |
| management {on <DEVICE-NAME>} | Optional. Displays management traffic firewall flows<br>• on <DEVICE-NAME> – Optional. Displays firewall flows on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |
| stats {on <DEVICE-NAME>} | Optional. Displays active session summary<br>• on <DEVICE-NAME> – Optional. Displays active session summary on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |
| wireless-client <MAC> | Optional. Displays wireless clients firewall flows<br>• <MAC> – Specify the MAC address of the wireless client. |
| on <DEVICE-NAME> | Optional. Displays all firewall flows on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `show firewall neighbors snoop-table {on <DEVICE-NAME>}`

| | |
|---|---|
| firewall neighbors snoop-table | Displays IPv6 neighbors snoop table entries |
| on <DEVICE-NAME> | Optional. Displays IPv6 neighbors snoop table entries on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

**Example**

```
rfs6000-81742D(config)#show fi
file-sync  firewall   file
rfs6000-81742D(config)#show firewall dhcp snoop-table
Snoop Binding <192.168.13.24, 00-15-70-81-74-2D, Vlan 1>
Type switch-SVI, Touched 427779 seconds ago
--------------------------------------------------------------------------------
rfs6000-81742D(config)#
```

```
rfs6000-81742D(config)#show firewall dos stats
-------------------------------------------------------------------------------
            ATTACK TYPE                  COUNT             LAST OCCURENCE
-------------------------------------------------------------------------------
  udp-short-hdr                          0             Never
  multicast-icmpv6                       0             Never
  icmp-router-solicit                    0             Never
  tcp-xmas-scan                          0             Never
  ascend                                 0             Never
  twinge                                 0             Never
  tcp-post-syn                           0             Never
  land                                   0             Never
  broadcast-multicast-icmp               0             Never
  ftp-bounce                             0             Never
  spoof                                  0             Never
  source-route                           0             Never
  tcp-null-scan                          0             Never
  tcp-fin-scan                           0             Never
  ipv6-hop-limit-zero                    0             Never
  tcp-bad-sequence                       97            0 days 02:24:32 ago
  fraggle                                0             Never
  router-advt                            0             Never
  snork                                  0             Never
  raguard                                0             Never
--More--
rfs6000-81742D(config)#

rfs6000-81742D(config)#show firewall flows management
========== Flow# 1 Summary ==========
Forward:
IPv4 Vlan 1, TCP 192.168.13.10 port 1646 > 192.168.13.24 port 22
 00-02-B3-28-D1-55 > 00-15-70-81-74-2D, ingress port up1
 Egress port: <local>, Egress interface: vlan1, Next hop: <local> (00-15-70-81-74-
2D)
 1170 packets, 99960 bytes, last packet 0 seconds ago
Reverse:
IPv4 Vlan 1, TCP 192.168.13.24 port 22 > 192.168.13.10 port 1646
 00-15-70-81-74-2D > 00-02-B3-28-D1-55, ingress port local
 Egress port: up1, Egress interface: vlan1, Next hop: 192.168.13.10 (00-02-B3-28-
D1-55)
 873 packets, 98797 bytes, last packet 0 seconds ago
TCP state: Established
Flow times out in 1 hour 30 minutes

rfs6000-81742D(config)#


rfs6000-81742D(config)#show firewall flows stats
Active Flows       2
TCP/IPv4 flows     2
UDP/IPv4 flows     0
DHCP/IPv4 flows    0
ICMP/IPv4 flows    0
IPsec/IPv4 flows   0
TCP/IPv6 flows     0
UDP/IPv6 flows     0
DHCP/IPv6 flows    0
ICMP/IPv6 flows    0
IPsec/IPv6 flows   0
L3/Unknown flows   0
rfs6000-81742D(config)#
```

## 6.1.29 global

*show commands*

Displays global information for network devices based on the parameters passed

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show global [device-list|domain]

show global device-list {filter {offline|online|rf-domain}}
show global device-list {filter {offline|online}}
show global device-list {filter rf-domain [<DOMAIN-NAME>|not <DOMAIN-NAME>]}

show global domain managers
```

**Parameters**

- `show global device-list {filter {offline|online}}`

| | |
|---|---|
| global device-list | Displays global information for all network devices. Use the following keywords to specify additional filters: offline, online, and rf-domain. |
| filter {offline\|online} | Optional. Specifies additional filters<br>• offline – Optional. Displays global information for offline devices only<br>• online – Optional. Displays global information for online devices only |

- `show global device-list {filter rf-domain [<DOMAIN-NAME>|not <DOMAIN-NAME>]}`

| | |
|---|---|
| global device-list | Displays global information for all network devices. Use the following keywords to specify additional filters: offline, online, and rf-domain. |
| filter rf-domain [<DOMAIN-NAME>\| not <DOMAIN-NAME>] | Optional. Specifies additional filters<br>• rf-domain – Optional. Displays global information for all devices in a specified RF Domain<br>• <DOMAIN-NAME> – Optional. Displays information of all devices within the domain identified by the <DOMAIN-NAME> keyword<br>• not <DOMAIN-NAME> – Optional. Displays information of all devices in domains not matching the <DOMAIN-NAME> keyword |

- `show global domain managers`

| | |
|---|---|
| global domain managers | Displays global information for all RF Domains and managers in the network |

**Example**

```
rfs6000-81742D(config)#show global device-list filter rf-domain TechPubs
-------------------------------------------------------------------------------
------------------------------
           MAC      HOST-NAME       TYPE          CLUSTER        RF-DOMAIN
ADOPTED-BY     ONLINE
-------------------------------------------------------------------------------
------------------------------
 00-15-70-81-74-2D   rfs6000-81742D  rfs6000     SiteConRFS6k         TechPubs B4-
C7-99-6C-88-09   online
-------------------------------------------------------------------------------
------------------------------
Total number of clients displayed: 1
rfs6000-81742D(config)#


rfs6000-81742D(config)#show global domain managers
-------------------------------------------------------------------------------
---------------------
                     RF-DOMAIN                                MANAGER          HOST-
NAME  APS  CLIENTS
-------------------------------------------------------------------------------
---------------------
                        default   ? rf-domain manager 00-15-70-38-03-E7 not in
configuration
                       TechPubs                    00-15-70-81-74-2D     rfs6000-
81742D    0        0
-------------------------------------------------------------------------------
---------------------
Total number of RF-domain displayed: 2
rfs6000-81742D(config)#
```

## 6.1.30 gre

*show commands*

Displays layer 2 *Generic Routing Encapsulation* (GRE) tunnel traffic flow information

GRE is one of the available tunneling mechanisms which uses IP as the transport protocol and can be used for carrying many different passenger protocols. The tunnels behave as virtual point-to-point links that have two endpoints identified by the tunnel source and tunnel destination addresses at each endpoint.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show gre info {detail} {(on <DEVICE-NAME>)}
```

**Parameters**

- `show gre info {detail} {(on <DEVICE-NAME>)}`

| | |
|---|---|
| gre info | Displays GRE tunnel information |
| detail | Optional. Displays GRE tunnel information in detail, such as tunnel state, tunnel's remote-end peer device's IP address, session ID of an operational tunnel, total number of packets received and transmitted through the tunnel, and the number of dropped packets during tunneled exchanges between access point and a peer at the remote end of the tunnel. |
| on <DEVICE-NAME> | Optional. Executes the command on a specified device<br>• <DEVICE-NAME> – Specify the name of the access point, controller, or service platform. |

**Example**

```
rfs6000-81742D#show gre info
Gre Tunnel info:
 Tunnel info not found
rfs6000-81742D#
```

## 6.1.31 guest-registration

*show commands*

Displays information on the performance of clients using guest access permissions to obtain network resources within the WiNG network. The reporting timeline can be adjusted as needed, as can the RF Domain(s) and WLAN(s) used to filter and report guest client statistics.

**Supported in the following platforms:**

- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510

**Syntax**

```
show guest-registration [age-range|backup-snapshots|browsers|client|devices|
gender|loyalty-app-status|notification-status|os|social|user-trends|visitors]
{on <DEVICE-NAME>}

show guest-registration backup-snapshots

show guest-registration [age-range|browsers|devices|gender|os|user-trends|
visitors] time [1-Day|1-Month|1-Week|2-Hours|30-Mins|5-Hours|all] {(rfdomain
<DOMAIN-NAME>|wlan <WLAN-NAME>)}

show guest-registration client [email|mac|member|mobile|name|time]

show guest-registration client [email <EMAIL-ADDRESS>|mac <MAC>|member <MEMBER-
ID>|mobile <MOBILE-NUMBER>|name <NAME>]

show guest-registration client time [1-Hour|10-Mins|15-Mins|2-Mins|30-Mins|
30-Secs|5-Mins] {(rfdomain <DOMAIN-NAME>|wlan <WLAN-NAME>)}

show guest-registration loyalty-app-status time [1-Day|1-Month|1-Week|2-Hours|
30-Mins|5-Hours|all] {rfdomain <RF-DOMAIN-NAME>|wlan <WLAN-NAME>}

show guest-registration notification-status

show guest-registration social time [1-Day|1-Month|1-Week|2-Hours|30-Mins|
5-Hours|all] {(facebook|rfdomain <DOMAIN-NAME>|wlan <WLAN-NAME>|google)}
```

**Parameters**

- `show guest-registration backup-snapshots`

| | |
|---|---|
| guest-registration | Displays guest registration statistics based on the parameters passed |
| backup-snapshots | Displays a list of periodically backed up snapshots of the database. By default, the system maintains a snapshot of the database on a daily basis.<br>**Note:** Use the *service > guest-registration > backup [delete\|restore]* command to delete these snapshots and to restore deleted snapshots. For more information, see *service*. |

- `show guest-registration [age-range|browsers|devices|gender|os|user-trends|visitors] time [1-Day|1-Month|1-Week|2-Hours|30-Mins|5-Hours|all] {(rfdomain <DOMAIN-NAME>|wlan <WLAN-NAME>)}`

| | |
|---|---|
| guest-registration | Displays guest registration statistics based on the parameters and time entered. Optionally, use the 'rfdomain' and/or 'wlan' keywords to view guest registration statistics for a specified RF Domain and/or WLAN. |
| age-range | Displays the age ranges of logged guest users for a selected time period |
| browsers | Displays the browsers used by guest users logged in within a selected time period |
| devices | Displays the device types used by guest users logged in within a selected time period |

| | |
|---|---|
| gender | Displays the gender of guest users logged in within a selected time period |
| os | Displays the *operating system* (OS) of devices logged in within a selected time period |
| user-trends | Displays guest user login trends for a selected time period. It displays statistical data, such as number of new users, number of return users, and total of number users. |
| visitors | Displays type of visitors logged in within a selected time period |
| time [1-Day\|1-Month\|<br>1-Week\|2-Hours\|<br>30-Mins\|5-Hours\|all] | Displays guest registration statistics, for a specified time period. The stats displayed depends on the option selected in the previous step. Specify the time period using one of the following options:<br>• 1-Day – Displays previous day's statistics<br>• 1-Month – Displays previous month's statistics<br>• 1-Week – Displays previous week's statistics<br>• 2-Hours – Displays last 2 hours statistics<br>• 30-Mins – Displays last 30 minutes statistics<br>• 5-Hours – Displays last 5 hours statistics<br>• all – Displays statistics from the day the database was created |
| [rfdomain<br><DOMAIN-NAME\|<br>wlan <WLAN-NAME>] | Use the following options as additional filters:<br>• rfdomain <DOMAIN-NAME> – Optional. Displays guest registration statistics for a specified RF Domain.<br>  • <DOMAIN-NAME> – Specify the RF Domain name.<br>• wlan <WLAN-NAME> – Optional. Displays guest registration statistics for a specified WLAN.<br>  • <WLAN-NAME> – Specify the WLAN name. |

• `show guest-registration client [email <EMAIL-ADDRESS>|mac <MAC>|member <MEMBER-ID>|mobile <MOBILE-NUMBER>|name <NAME>]`

| | |
|---|---|
| guest-registration | Displays guest registration statistics based on the parameters and time entered. Optionally, use the 'rfdomain' and/or 'wlan' keywords to view guest registration statistics for a specified RF Domain and/or WLAN. |
| client | Displays statistical data for a specific client. Use the e-mail, mac, member, mobile, name to provide a match criteria. |
| email<br><EMAIL-ADDRESS> | Displays statistical data for the client with e-mail address matching the <EMAIL-ADDRESS> parameter<br>• <EMAIL-ADDRESS> – Specify the client's e-mail address. |
| mac <MAC> | Displays statistical data for the client with MAC address matching the <MAC> parameter<br>• <MAC> – Specify the client's MAC address |
| member<br><MEMBER-ID> | Displays statistical data for the client with member ID matching the <MEMBER-ID> parameter<br>• <MEMBER-ID> – Specify the client's member ID. |

| | |
|---|---|
| mobile <MOBILE-NUMBER> | Displays statistical data for the client with mobile number matching the <MOBILE-NUMBER> parameter<br>• <MOBILE-NUMBER> – Specify the client's mobile number. |
| name <NAME> | Displays statistical data for the client with name matching the <NAME> parameter<br>• <MOBILE-NUMBER> – Specify the client's name. |

• `show guest-registration client time [1-Hour|10-Mins|15-Mins|2-Mins|30-Mins|30-Secs|5-Mins] {(rfdomain <DOMAIN-NAME>|wlan <WLAN-NAME>)}`

| | |
|---|---|
| guest-registration | Displays guest registration statistics based on the parameters and time entered. Optionally, use the 'rfdomain' and/or 'wlan' keywords to view guest registration statistics for a specified RF Domain and/or WLAN. |
| client | Displays statistical data for all clients logged in within a specified time period |
| time [1-Day\|1-Month\| 1-Week\|2-Hours\| 30-Mins\|5-Hours\|all] | Use one of the following options to specify the time period:<br>• 1-Day – Displays previous day's statistics<br>• 1-Month – Displays previous month's statistics<br>• 1-Week – Displays previous week's statistics<br>• 2-Hours – Displays last 2 hours statistics<br>• 30-Mins – Displays last 30 minutes statistics<br>• 5-Hours – Displays last 5 hours statistics<br>• all – Displays entire statistics, from the day the database was created |
| [rfdomain <DOMAIN-NAME\| wlan <WLAN-NAME>] | Use the following options as additional filters:<br>• rfdomain <DOMAIN-NAME> – Optional. Displays guest registration statistics for a specified RF Domain.<br>  • <DOMIAIN-NAME> – Specify the RF Domain name.<br>• wlan <WLAN-NAME> – Optional. Displays guest registration statistics for a specified WLAN.<br>  • <WLAN-NAME> – Specify the WLAN name. |

• `show guest-registration loyalty-app-status time [1-Day|1-Month|1-Week|2-Hours|30-Mins|5-Hours|all] {rfdomain <RF-DOMAIN-NAME>|wlan <WLAN-NAME>}`

| | |
|---|---|
| guest-registration | Displays guest registration statistics based on the parameters and time entered |
| loyalty-app-status | Displays captive portal clients' Loyalty Application analytics, such as the number of guest clients with loyalty application detection enabled, associating with the captive portal's access point during a specified time period<br>Loyalty application detection occurs on the access point to which the guest client is associated, allowing a retail administrator to assess whether a captive portal client is using specific retail (loyalty) applications in their captive portal.<br>For more information on enabling loyalty application detection on a captive portal, see *report-loyalty-application*. |
| time [1-Day\|1-Month\| 1-Week\|2-Hours\| 30-Mins\|5-Hours\|all] | Specifies the time period, using one of the following options:<br>• 1-Day – Displays previous day's captive portal clients' Loyalty Application analytics<br>• 1-Month – Displays previous month's captive portal clients' Loyalty Application analytics<br>Contd.. |

| | |
|---|---|
| | • 1-Week – Displays previous week's captive portal clients' Loyalty Application analytics<br>• 2-Hours – Displays last 2 hours captive portal clients' Loyalty Application analytics<br>• 30-Mins – Displays last 30 minutes captive portal clients' Loyalty Application analytics<br>• 5-Hours – Displays last 5 hours captive portal clients' Loyalty Application analytics<br>• all – Displays the entire Loyalty Application analytics, from the day the database was created |
| {rfdomain <RF-DOMAIN-NAME>\| wlan <WLAN-NAME>} | Optional. Specifies the 'rfdomain' and/or 'wlan' to view guest registration statistics for a specified RF Domain and/or WLAN<br>• rfdomain <RF-DOMAIN-NAME> – Displays Loyalty App analytics for a specified RF Domain<br>  • <RF-DOMAIN-NAME> – Specify the RF Domain name.<br>• wlan <WLAN-NAME> – Displays Loyalty App analytics for a specified WLAN<br>  • <WLAN-NAME> – Specify the WLAN name. |

- `show guest-registration notification-status`

| | |
|---|---|
| guest-registration | Displays guest registration statistics based on the parameters and time entered. Optionally, use the 'rfdomain' and/or 'wlan' keywords to view guest registration statistics for a specified RF Domain and/or WLAN. |
| notification-status | Displays guest registration notification status |

- `show guest-registration social time [1-Day|1-Month|1-Week|2-Hours|30-Mins|5-Hours|all] {(facebook|rfdomain <DOMAIN-NAME>|wlan <WLAN-NAME>|google)}`

| | |
|---|---|
| guest-registration social | Displays the social sites used by guests to register. Optionally, use the 'rfdomain' and/or 'wlan' keywords to view social site used by guests of a specified RF Domain and/or WLAN. |
| time [1-Day\|1-Month\| 1-Week\|2-Hours\| 30-Mins\|5-Hours\|all] | Displays social site statistics for a specified time period. Use one of the following time options:<br>• 1-Day – Displays previous day's statistics<br>• 1-Month – Displays previous month's statistics<br>• 1-Week – Displays previous week's statistics<br>• 2-Hours – Displays last 2 hours statistics<br>• 30-Mins – Displays last 30 minutes statistics<br>• 5-Hours – Displays last 5 hours statistics<br>• all – Displays the entire database |
| facebook | Displays guest users using Facebook to log in |
| rfdomain <DOMAIN-NAME> | Displays guest users for a specific RF Domain<br>• <DOMAIN-NAME> – Specify the RF Domain name. |
| wlan <WLAN-NAME> | Displays guest users for a specific WLAN<br>• <WLAN-NAME> – Specify the WLAN name. |
| google | Displays guest users using Google to log in |

**Example**

```
nx9500-6C8809#show guest-registration age-range time all
Timeline: all
---------------------------------
AGE RANGE                  COUNT
---------------------------------
less_than_18              0 (  0%)
18_to_24                  1 ( 20%)
25_to_34                  0 (  0%)
35_to_44                  1 ( 20%)
45_to_54                  1 ( 20%)
55_to_64                  2 ( 40%)
greater_than_64           0 (  0%)
---------------------------------

nx9500-6C8809#

nx9500-6C8809#show guest-registration browsers time 1-Day rfdomain Test-rfdomain-
10
RFDomain: Test-rfdomain-10 Timeline: 1-Day
-----------------------------------
 BROWSER          COUNT
-----------------------------------
Safari            1 ( 50%)
Chrome            1 ( 50%)

nx9500-6C8809#

nx9500-6C8809#show guest-registration devices time 30-Mins wlan Test-ssid-9
WLAN: Test-ssid-9  Timeline: 30-Mins
-------------------------------
  DEVICE             COUNT
-------------------------------
Windows PC           1 (100%)

nx9500-6C8809#

nx9500-6C8809#show guest-registration gender time all wlan Test-ssid-10 rfdomain
Test-rfdomain-10
RF Domain: Test-rfdomain-10  WLAN: Test-ssid-10  Timeline: all
-----------------------------------------------
  GENDER           COUNT
-----------------------------------------------
Male               1 ( 50%)
Female             1 ( 50%)
Other              0 (  0%)

nx9500-6C8809#

nx9500-6C8809#show guest-registration gender time all wlan Test-ssid-10 rfdomain
Test-rfdomain-9
%% No guests registered for specified inputs.
nx9500-6C8809#

nx9500-6C8809#show guest-registration os time 1-Day
Timeline: 1-Day
-------------------------------
    OS               COUNT
-------------------------------
Windows 7            3 ( 30%)
Apple iOS            3 ( 30%)
Macintosh            3 ( 30%)
Windows 8            1 ( 10%)

nx9500-6C8809#
```

```
nx9500-6C8809#show guest-registration social time 30-Mins
Timeline: 30-Mins
-------------------------------------------
  SOCIAL            ONLINE          TOTAL
-------------------------------------------
google               1 (100%)       1 ( 10%)
Local                0 (  0%)       9 ( 90%)

nx9500-6C8809#

nx9500-6C8809#show guest-registration user-trends time all
Timeline: all
-------------------------------------------------------------------------------
            SAMPLE RANGE                     NEW USERS   RETURN USERS   TOTAL
-------------------------------------------------------------------------------
2014-2-16 - 2014-4-17                         0 (  0%)       0 (  0%)       0
2014-4-17 - 2014-6-16                         0 (  0%)       0 (  0%)       0
2014-6-16 - 2014-8-15                         0 (  0%)       0 (  0%)       0
2014-8-15 - 2014-10-14                        0 (  0%)       0 (  0%)       0
2014-10-14 - 2014-12-13                       0 (  0%)       0 (  0%)       0
2014-12-13 - 2015-2-11                       10 (100%)       0 (  0%)      10
-------------------------------------------------------------------------------

nx9500-6C8809#

nx9500-6C8809#show guest-registration user-trends time 1-Day
Timeline: 1-Day
-------------------------------------------------------------------------------
            SAMPLE RANGE                     NEW USERS   RETURN USERS   TOTAL
-------------------------------------------------------------------------------
23:16 - 3:16                                  0 (  0%)       0 (  0%)       0
3:16 - 7:16                                   0 (  0%)       0 (  0%)       0
7:16 - 11:16                                  0 (  0%)       0 (  0%)       0
11:16 - 15:16                                 0 (  0%)       0 (  0%)       0
15:16 - 19:16                                 0 (  0%)       0 (  0%)       0
19:16 - 23:16                                 0 (  0%)       0 (  0%)       0
-------------------------------------------------------------------------------

nx9500-6C8809#

nx9500-6C8809#show guest-registration visitors time 30-Mins
Timeline: 30-Mins
-----------------------------------
  VISITORS        COUNT
-----------------------------------
New Users                7 ( 70%)
Return Users             3 ( 30%)

nx9500-6C8809#

nx9500-6C8809#show guest-registration client time 30-Mins email Guest_9@abc.com
-----------------------------------
ATTRIBUTE      VALUE
-----------------------------------
city           Brooklyn
wlan           Test-ssid-10
name           Guest_9
zip            11204
mobile         9131373709
gender         female
llogintime     2015-01-20 19:11:14.001000
mobileok       on
devtype        Windows PC
createtime     2015-01-20 18:27:14.001000
email          Guest_9@abc.com
mac            10-00-00-10-00-09
reg_type       otp
rfd            Test-rfdomain-10
```

```
agerange        <18
group           mac_reg_gr1
mid             1234100009
os              Windows 7
exptime         2015-11-16 19:21:14.001000
browser         Safari
-----------------------------------

nx9500-6C8809#


nx9500-6C8809#show guest-registration client time 30-Mins rfdomain Test-rfdomain-8
-----------------------------------
ATTRIBUTE       VALUE
-----------------------------------
loggedin        yes
wlan            Test-ssid-8
name            Guest_1
locale          en_US
llogintime      2015-01-20 19:15:14
devtype         Macintosh
exptime         2015-11-16 19:21:14
lname           Guest_100000
source          google
mac             10-00-00-10-00-01
email           Guest_1@abc.com
id              657669862939196
reg_type        device
fname           Test-Guest_1
rfd             Test-rfdomain-8
agerange        35-44
timezone        7
profilePic      https://www.google.com/user_id/657669862939196/
os              Macintosh
createtime      2015-01-20 18:45:14
group           mac_reg_gr1
browser         Chrome
-----------------------------------
city            Santa Cruz
group           mac_reg_gr1
name            Guest_2
zip             95062
mobile          3700870747
mid             1234100001
llogintime      2015-01-20 19:18:14
mobileok        on
devtype         Apple iPad
exptime         2015-11-16 19:21:14
createtime      2015-01-20 19:11:14
mac             10-00-00-10-00-02
reg_type        otp
rfd             Test-rfdomain-8
agerange        55-64
wlan            Test-ssid-8
os              Apple iOS
email           Guest_2@abc.com
browser         Chrome
-----------------------------------
city            Los Angeles
group           mac_reg_gr1
name            Guest_5
zip             90001
mobile          9129618672
mid             1234100005
llogintime      2015-01-20 19:20:14
devtype         Macintosh
exptime         2015-11-16 19:21:14
createtime      2015-01-20 19:05:14
```

```
mac             10-00-00-10-00-05
reg_type        device
rfd             Test-rfdomain-8
agerange        18-24
wlan            Test-ssid-8
os              Macintosh
email           Guest_5@abc.com
browser         Chrome
-----------------------------------

nx9500-6C8809#

nx7500-112233#show guest-registration loyalty-app-status time all

Timeline: all
-------------------------------------------
  LOYALTY APP STATUS             COUNT
-------------------------------------------
Loyalty App Users                  491 ( 49%)
Others                             510 ( 51%)

nx7500-112233#
```

## 6.1.32 interface

*show commands*

Displays configured system interfaces and their status

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show interface {<INTERFACE-NAME>|brief|counters|ge|me1|port-channel|pppoe1|
switchport|vlan|wwan1}

show interface {<INTERFACE-NAME>|brief|counters|ge <1-4>|me1|port-channel <1-2>|
pppoe1|switchport|vlan <1-4094>|wwan1} {on <DEVICE-NAME>}
```

**Parameters**

```
• show interface {<INTERFACE-NAME>|brief|counters|ge <1-4>|me1|port-channel <1-
2>|pppoe1|switchport|vlan <1-4094>|wwan1} {on <DEVICE-NAME>}
```

| | |
|---|---|
| interface | Optional. Displays system interface status based on the parameters passed |
| <INTERFACE-NAME> | Optional. Displays status of the interface specified by the <INTERFACE-NAME> parameter. Specify the interface name. |
| brief | Optional. Displays a brief summary of the interface status and configuration |
| counters | Optional. Displays interface Tx or Rx counters |
| ge <1-4> | Optional. Displays Gigabit Ethernet interface status and configuration<br>• <1-4> – Select the Gigabit Ethernet interface index from 1 - 4. |
| me1 | Optional. Displays Fast Ethernet interface status and configuration |
| port-channel <1-2> | Optional. Displays port channel interface status and configuration<br>• <1-2> – Specify the port channel index from 1 - 2. |
| pppoe1 | Optional. Displays PPP over Ethernet interface status and configuration |
| switchport | Optional. Displays layer 2 interface status |
| vlan <1-4094> | Optional. Displays VLAN interface status and configuration<br>• <1-4094> – Specify the *Switch Virtual Interface* (SVI) VLAN ID from 1 - 4094. |
| wwan1 | Optional. Displays Wireless WAN interface status, configuration, and counters |
| on <DEVICE-NAME> | The following keywords are common to all of the above interfaces:<br>• on <DEVICE-NAME> – Optional. Displays interface related information on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

**Example**

Following interfaces are available on a RFS6000 controller:

```
rfs6000-81742D(config)#show interface ?

  WORD          Interface name
  brief         Brief summary of interface status and configuration
  counters      Interface tx/rx counters
  ge            GigabitEthernet interface
  me1           FastEthernet interface
  on            On AP/Controller
  port-channel  Port-Channel interface
  pppoe1        PPP Over Ethernet interface
  switchport    Status of Layer2 interfaces
  up1           WAN Ethernet interface
  vlan          Switch VLAN interface
  wwan1         Wireless WAN interface
  |             Output modifiers
  >             Output redirection
  >>            Output redirection appending
  <cr>


rfs6000-81742D(config)#

rfs6000-81742D(config)#show interface  switchport
-------------------------------------------------------------------------------
-------
 INTERFACE          STATUS   MODE     VLAN(S)
-------------------------------------------------------------------------------
-------
 ge1                DOWN     access   1
 ge2                DOWN     access   1
 ge3                DOWN     access   1
 ge4                DOWN     access   1
 ge5                DOWN     access   1
 ge6                DOWN     access   1
 ge7                DOWN     access   1
 ge8                DOWN     access   1
 up1                UP       access   1
--More--
rfs6000-81742D(config)#

rfs6000-81742D(config)#show interface ge 1
Interface ge1 is DOWN
  Hardware-type: ethernet, Mode: Layer 2, Address: 00-15-70-81-74-2E
  Index: 2001, Metric: 1, MTU: 1500
  Speed: Admin Auto, Operational n/a, Maximum 1G
  Duplex: Admin Auto, Operational n/a
  Active-medium: n/a
  Switchport settings: access, access-vlan: 1
    Input packets 0, bytes 0, dropped 0
    Received 0 unicasts, 0 broadcasts, 0 multicasts
    Input errors 0, runts 0, giants 0
    CRC 0, frame 0, fragment 0, jabber 0
    Output packets 0, bytes 0, dropped 0
    Sent 0 unicasts, 0 broadcasts, 0 multicasts
    Output errors 0, collisions 0, late collisions 0
    Excessive collisions 0

rfs6000-81742D(config)#
```

```
rfs6000-81742D(config)#show interface  counters
-------------------------------------------------------------------------------
------------------------------
    INTF            MAC           RX-PKTS     RX-BYTES     RX-DROP     TX-PKTS
TX-BYTES       TX-DROP
-------------------------------------------------------------------------------
------------------------------
 me1       00-15-70-81-74-36   0         0          0         0          0          0
 vlan1       00-15-70-81-74-2D   1578154     279596323    0           82096
14710688     0
 ge1       00-15-70-81-74-2E   0         0          0         0          0          0
 ge2       00-15-70-81-74-2F   0         0          0         0          0          0
 ge3       00-15-70-81-74-30   0         0          0         0          0          0
 ge4       00-15-70-81-74-31   0         0          0         0          0          0
 ge5       00-15-70-81-74-32   0         0          0         0          0          0
 ge6       00-15-70-81-74-33   0         0          0         0          0          0
 --More--
rfs6000-81742D(config)#

rfs6000-81742D(config)#show interface  vlan 1
Interface vlan1 is UP
  Hardware-type: vlan, Mode: Layer 3, Address: 00-15-70-81-74-2D
  Index: 5, Metric: 1, MTU: 1500
  IP-Address: 192.168.13.24/24
    input packets 1578392, bytes 279625825, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 82159, bytes 14717966, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
  IPv6 mode is disabled

rfs6000-81742D(config)#

nx9500-6C8809(config)#show interface switchport
-------------------------------------------------------------------------------
-------
 INTERFACE          STATUS   MODE     VLAN(S)
-------------------------------------------------------------------------------
-------
 ge1                UP       access   1
 ge2                DOWN     access   1
-------------------------------------------------------------------------------
-------
A '*' next to the VLAN ID indicates the native vlan for that trunk port
nx9500-6C8809(config)#

nx9500-6C8809(config)#show interface vlan 1
Interface vlan1 is UP
  Hardware-type: vlan, Mode: Layer 3, Address: B4-C7-99-6C-88-09
  Index: 5, Metric: 1, MTU: 1500
  IP-Address: 192.168.13.13/24
    input packets 4623946, bytes 568905032, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 458235, bytes 90317187, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
  IPv6 mode is disabled

nx9500-6C8809(config)#
```

```
nx9500-6C8809(config)#show interface ge 1
Interface ge1 is UP
  Hardware-type: ethernet, Mode: Layer 2, Address: 00-1E-67-4B-BF-BC
  Index: 2001, Metric: 1, MTU: 1500
  Speed: Admin Auto, Operational 1G, Maximum 1G
  Duplex: Admin Auto, Operational Full
  Active-medium: n/a
    Input packets 2326745, bytes 348775278, dropped 0
    Received 2326745 unicasts, 4367 broadcasts, 1219173 multicasts
    Input errors 0, runts 0, giants 0
    CRC 0, frame 0, fragment 0, jabber 0
    Output packets 1080901, bytes 244595966, dropped 0
    Sent 1080901 unicasts, 392 broadcasts, 132573 multicasts
    Output errors 0, collisions 0, late collisions 0
    Excessive collisions 0

nx9500-6C8809(config)#

nx9500-6C8809(config)#show interface counters
-------------------------------------------------------------------------------
------------------------------
    INTF            MAC           RX-PKTS     RX-BYTES     RX-DROP     TX-PKTS
TX-BYTES       TX-DROP
-------------------------------------------------------------------------------
------------------------------
 vlan1      B4-C7-99-6C-88-09   2571193     341672167    0           625888
90924957     0
 ge1        00-1E-67-4B-BF-BC   2326629     348759017    0           1080855
244588229    0
 ge2       00-1E-67-4B-BF-BD  0         0          0         0         0          0
 port..nel1 00-1E-67-4B-BF-BC   2326631     348759243    0           1080857
244588673    0
-------------------------------------------------------------------------------
------------------------------
nx9500-6C8809(config)#
```

## 6.1.33 ip

*show commands*

Displays IP related information

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show ip [arp|bgp|ddns|default-gateways|dhcp|dhcp-vendor-options|domain-name|
extcommunity-list|igmp|interface|name-server|nat|ospf|route|routing]

show ip arp {<VLAN-NAME>} {(on <DEVICE-NAME>)}

show ip bgp {<IP>|<IP/M>|community|community-list|filter-list|neighbors|on|paths|
prefix-list|regexp|route-map|state|summary}

show ip ddns bindings {on <DEVICE-NAME>}

show ip dhcp [binding|networks|status]
show ip dhcp binding {manual} {(on <DEVICE-NAME>)}
show ip dhcp [networks|status] {on <DEVICE-NAME>}

show ip [default-gateways|dhcp-vendor-options|domain-name|name-server|routing]
{on <DEVICE-NAME>}

show ip extcommunity-list [<1-500>|<NAME>]

show ip igmp snooping [mrouter|querier|vlan]
show ip igmp snooping [mrouter|querier] vlan <1-4095> {on <DEVICE-NAME>}
show ip igmp snooping vlan <1-4095> {<IP>} {(on <DEVICE-NAME>)}

show ip interface {<INTERFACE-NAME>|brief|on}
show ip interface {<INTERFACE-NAME>|brief} {(on <DEVICE-NAME>)}

show ip nat translations verbose {on <DEVICE-NAME>}

show ip route {<INTERFACE-NAME>|ge|me1|on|port-channel|pppoe1|vlan|wwan1}
show ip route {<INTERFACE-NAME>|ge <1-4>|me1|port-channel <1-2>|vlan <1-4094>|
pppoe1|wwan1} {(on <DEVICE-NAME>)}

show ip ospf {border-router|interface|neighbor|on|route|state}
show ip ospf {border-router|neighbor|route|on|state} {on <DEVICE-NAME>}
show ip ospf {interface} {vlan|on}
show ip ospf {interface} {vlan <1-4094>} {(on <DEVICE-NAME>)}
```

**NOTE:** The show ip ospf command is also available under the 'profile' and 'device' modes.

**Parameters**

- `show ip arp {<VLAN-NAME>} {(on <DEVICE-NAME>)}`

| | |
|---|---|
| ip arp | Displays *Address Resolution Protocol* (ARP) mappings |
| <VLAN-NAME> | Optional. Displays ARP mapping on a specified VLAN. Specify the VLAN name. |

| | |
|---|---|
| on <DEVICE-NAME> | The following keyword is recursive and common to the 'vlan-name' parameter:<br>• on <DEVICE-NAME> – Optional. Displays ARP configuration details on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

• `show ip bgp {<IP>|<IP/M>|community|community-list|filter-list|neighbors|on|paths|prefix-list|regexp|route-map|state|summary}`

| | |
|---|---|
| ip bgp | Displays BGP routing table statistics based on the match criteria specified here. Routes matching the specified criteria are filtered. Use available options to filter the information displayed.<br>This command is applicable to the RFS4000, RFS6000, NX9XXX model devices. |
| <IP> | Optional. Filters routes matching the specified IP address |
| <IP/M> | Optional. Filters routes matching the specified network |
| community | Optional. Filters routes based on the community attribute specified. The options are:<br>• AA:NN – Filters routes based on the community number (AA: is the *autonomous system number (*ASN), NN: is the community number within the specified ASN)<br>• local-as – Filters routes carrying the local-as attribute (these routes are not sent outside the local AS)<br>• no-advertise – Filters routes carrying the no-advertise attribute (these routes are not advertised to any peers)<br>• no-export – Filters routes carrying no-export attribute (these routes are not exported to next AS) |
| community-list | Optional. Displays routes that are members of communities included in the specified BGP community-list<br>• <1-500> – Specify the community-list number.<br>• <WORD> – Specify the community-list name. |
| filter-list | Optional. Filters routes having AS-path matching the specified AS-path access list. Specify the AS-path ACL name. |
| neighbors | Optional. Displays BGP neighbor details. Specify the IP address, to view a specific neighbor details. Use one of the following options to filter information:<br>• advertised-routes – Displays route information for routes advertised to the selected neighbor device<br>• received-routes – Displays route information for routes received from the selected neighbor device<br>• routes – Displays the route information for routes learned from the selected neighbor device<br>If no neighbor IP address is specified, the system displays all neighbor-related routes on the logged device. |
| on <DEVICE-NAME> | Optional. Displays BGP routing table statistics on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |
| paths | Optional. Displays BGP path details |
| prefix-list <PREFIX-LIST-NAME> | Optional. Displays routes confirming to the specified prefix-list<br>• <PREFIX-LIST-NAME> – Specify the prefix list name. |

| | |
|---|---|
| regexp <LINE> | Optional. Displays routes matching the specified AS path regular expression<br>• <LINE> – Specify the regular expression. |
| route-map <ROUTE-MAP-NAME> | Optional. Displays routes matching the specified route map<br>• <ROUTE-MAP-NAME> – Specify the route map name. |

- `show ip ddns bindings` *`{on <DEVICE-NAME>}`*

| | |
|---|---|
| ip ddns | Displays *Dynamic Domain Name Server* (DDNS) configuration details |
| bindings {on <DEVICE-NAME>} | Displays DDNS address bindings<br>• on <DEVICE-NAME> – Optional. Displays address bindings on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `show ip dhcp [networks|status]` *`{on <DEVICE-NAME>}`*

| | |
|---|---|
| ip dhcp | Displays DHCP server related details, such as network and status |
| networks | Displays DHCP server network details |
| status | Displays DHCP server status |
| on <DEVICE-NAME> | The following keyword is common to all of the above parameters:<br>• on <DEVICE-NAME> – Optional. Displays server status and network details on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `show ip dhcp binding` *`{manual} {(on <DEVICE-NAME>)}`*

| | |
|---|---|
| ip dhcp | Displays the DHCP server configuration details |
| bindings | Displays DHCP address bindings |
| manual | Optional. Displays static DHCP address bindings |
| on <DEVICE-NAME> | The following keyword is recursive and common to the 'manual' parameter:<br>• on <DEVICE-NAME> – Optional. Displays DHCP address bindings on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `show ip extcommunity-list [<1-500>|<NAME>]`

| | |
|---|---|
| ip extcommunity-list [<1-500>\|<NAME>] | Displays the specified extended community list details<br>• <1-500> – Specify the extended community number from 1 - 500.<br>• <NAME> – Specify the extended community name.<br>This command is applicable to the RFS4000, RFS6000, NX95XX model devices. |

- `show ip [default-gateways|dhcp-vendor-options|domain-name|name-server|routing]` *`{on <DEVICE-NAME>}`*

| | |
|---|---|
| ip default-gateways | Displays all learnt default gateways |
| ip dhcp-vendor-options | Displays DHCP 43 parameters received from the DHCP server. This output includes the interface from which the option was learned. |
| ip domain-name | Displays the DNS default domain |

| | |
|---|---|
| ip name-server | Displays the DNS name server details |
| ip routing | Displays routing status |
| on <DEVICE-NAME> | The following keywords are common to all of the above parameters:<br>• on <DEVICE-NAME> – Optional. Displays IP related information, based on the parameters passed, on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `show ip igmp snooping [mrouter|querier] vlan <1-4095> {on <DEVICE-NAME>}`

| | |
|---|---|
| ip igmp snooping | Displays the IGMP snooping configuration |
| mrouter | Displays the IGMP snooping multicast router (mrouter) configuration |
| querier | Displays the IGMP snooping multicast querier configuration |
| vlan <1-4095><br>{on <DEVICE-NAME>} | Displays the IGMP snooping multicast router configuration for a VLAN<br>• <1-4095> – Specify the VLAN ID from 1 - 4095.<br>• on <DEVICE-NAME> – Optional. Displays the IGMP snooping mrouter configuration on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP or wireless controller. |

- `show ip igmp snooping vlan <1-4095> {<IP>} {(on <DEVICE-NAME>)}`

| | |
|---|---|
| ip igmp snooping | Displays the IGMP snooping configuration |
| vlan <1-4095> | Displays the VLAN IGMP snooping configuration<br>• <1-4095> – Specify the VLAN ID from 1 - 4095. |
| <IP> | Optional. Specifies the multicast group IP address |
| on <DEVICE-NAME> | The following keyword is recursive and common to the 'ip' parameter:<br>• on <DEVICE-NAME> – Optional. Displays configuration details on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP or wireless controller. |

- `show ip interface {<INTERFACE-NAME>|brief} {(on <DEVICE-NAME>)}`

| | |
|---|---|
| ip interface | Displays an administrative and operational status of all layer 3 interfaces or a specified layer 3 interface |
| <INTERFACE-NAME> | Optional. Displays a specified interface status. Specify the interface name. |
| brief | Optional. Displays a brief summary of all interface status and configuration |
| on <DEVICE-NAME> | The following keyword is recursive and common to the 'interface-name' and 'brief' parameters:<br>• on <DEVICE-NAME> – Optional. Displays interface status and summary, based on the parameters passed, on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `show ip nat translations verbose {on <DEVICE-NAME>}`

| | |
|---|---|
| ip nat translations | Displays *Network Address Translation* (NAT) translations |
| verbose | Displays detailed NAT translations<br>• on <DEVICE-NAME> – Optional.Displays NAT translations on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `show ip route {<INTERFACE-NAME>|ge <1-4>|me1|port-channel <1-2>|vlan <1-4094>|pppoe1|wwan1} {(on <DEVICE-NAME>)}`

| | |
|---|---|
| ip route | Displays route table details. The route tables use flags to distinguish between routes. The different flags are:<br>• C – Connected<br>• G – Gateway<br>• O – OSPF route<br>• S – Static route<br>**Note:** Flags 'S' and 'O' identify static learned routes and dynamic learned routes respectively. |
| <INTERFACE-NAME> | Optional. Displays route table details for a specified interface. Specify the interface name |
| ge <1-4> | Optional. Displays GigabitEthernet interface route table details<br>• <1-4> – Specify the GigabitEthernet interface index from 1 - 4. |
| me1 | Optional. Displays FastEthernet interface route table details |
| port-channel <1-2> | Optional. Displays port channel interface route table details. Specify the port channel index from 1 - 2. |
| vlan <1-4094> | Optional. Displays VLAN interface route table details. Select the VLAN interface ID from 1 - 4094. |
| pppoe1 | Optional. Displays *Point-to-point Protocol over Ethernet* (PPPoE) interface route table details |
| wwan1 | Optional. Displays Wireless WAN route table details |
| on <DEVICE-NAME> | The following keywords are recursive and common to all of the above parameters:<br>• on <DEVICE-NAME> – Displays route table details, based on the parameters passed, on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `show ip ospf {border-router|interface|neighbor|route|on|state} {on <DEVICE-NAME>}`

| | |
|---|---|
| ip ospf | Displays overall OSPF information |
| border-router | Optional. Displays details of all the border routers connected |
| interface<br>{on\| vlan <1-4094>}<br>{on <DEVICE-NAME>} | Optional. Displays details of all the interfaces with OSPF enabled<br>• on <DEVICE-NAME> – Optional. Displays specified device details<br>• vlan <1-4094> – Displays VLAN interface details<br>• <DEVICE-NAME> – Specify the name of the AP or wireless controller. |
| neighbor | Optional. Displays an OSPF neighbors list |
| route | Optional. Displays OFPS routes information |
| on <DEVICE-NAME> | Optional. Displays overall OSPF information on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |
| state | Optional. Displays an OSPF process state |

| | |
|---|---|
| on <DEVICE-NAME> | The following keywords are recursive and common to all of the above parameters:<br>• on <DEVICE-NAME> – Optional. Displays overall OSPF information, based on the parameters passed, on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

**Example**

```
rfs6000-81742D(config)#show ip arp
-------------------------------------------------------------------------------
          IP                    MAC              INTERFACE          TYPE
-------------------------------------------------------------------------------
  192.168.13.10        00-02-B3-28-D1-55        vlan1          dynamic
  192.168.13.13        B4-C7-99-6C-88-09        vlan1          dynamic
  192.168.13.2         00-0F-8F-19-BA-4C        vlan1          dynamic
-------------------------------------------------------------------------------
rfs6000-81742D(config)#

rfs6000-81742D(config)#show ip interface brief
-------------------------------------------------------------------------------
 INTERFACE          IP-ADDRESS/MASK            TYPE         STATUS   PROTOCOL
-------------------------------------------------------------------------------
 me1                unassigned                 n/a          UP       down
 vlan1              192.168.13.24/24           primary      UP       up
-------------------------------------------------------------------------------
rfs6000-81742D(config)#

rfs6000-81742D(config)#show ip route
-------------------------------------------------------------------------------
     DESTINATION         GATEWAY       FLAGS   INTERFACE   METRIC    DISTANCE
-------------------------------------------------------------------------------
  default             192.168.13.2     S       vlan1       0         1
  192.168.13.0/24     0.0.0.0          C       vlan1       0         0
-------------------------------------------------------------------------------
Flags:  C - Connected G - Gateway O - OSPF  B - BGP  S - Static
Gateway: N - Normalized Gateway Address
rfs6000-81742D(config)#

rfs6000-81701D(config)#show ip route port-channel 1
-------------------------------------------------------------------------------
DESTINATION       GATEWAY        FLAGS    INTERFACE    METRIC  DISTANCE
-------------------------------------------------------------------------------
192.168.0.0/24    direct          C         me1          0        0
172.18.0.0/24     direct          C         vlan1        0        0
10.2.0.0/24       172.18.0.1      S         vlan1        0        1
default           192.168.13.2    S         vlan192      0        1
192.168.13.0/24   direct          C         vlan192      0        0
-------------------------------------------------------------------------------
Flags:  C - Connected G - Gateway O - OSPF  B - BGP  S - Static
Gateway: N - Normalized Gateway Address
rfs6000-81701D(config)#


nx9500-6C8809(config)#show ip routing on rfs6000-81742D
IP routing is enabled.
nx9500-6C8809(config)#
```

```
nx9500-6C8809(config)#show ip dhcp status
State of DHCP server: not-running
nx9500-6C8809(config)#

rfs6000-81701D(config)#show ip ospf state
 Maximum number of OSPF routes allowed: 9216
   Number of OSPF routes received: 0
   Ignore-count allowed: 5, current ingore-count: 0
   Ignore-time 60 seconds, reset-time 360 seconds
   Current OSPF process state: Running
rfs6000-81701D(config)#


rfs6000-81742D(config)#show ip route on ap7532-A2A56C
--------------------------------------------------------------------------------
    DESTINATION         GATEWAY      FLAGS   INTERFACE   METRIC     DISTANCE
--------------------------------------------------------------------------------
  169.254.0.0/16     0.0.0.0         C       vlan1       0        0
  default            192.168.9.2     CG      vlan1       0        1
  192.168.9.0/24     0.0.0.0         C       vlan1       0        0
--------------------------------------------------------------------------------
Flags:  C - Connected G - Gateway O - OSPF  B - BGP  S - Static
Gateway: N - Normalized Gateway Address
rfs6000-81742D(config)#


rfs6000-81742D(config)#show ip dhcp-vendor-options
--------------------------------------------------------------------------------
                  ITEM                          VALUE             INTERFACE
--------------------------------------------------------------------------------
  Server Info                              n/a               vlan1
  Firmware Image File                      n/a               vlan1
  Config File                              n/a               vlan1
  Legacy Adoption Info                     n/a               n/a
  AP Adoption Info                         n/a               n/a
  Controller Adoption Info                 n/a               n/a
--------------------------------------------------------------------------------
rfs6000-81742D(config)#
```

## 6.1.34 ip-access-list

*show commands*

Displays IP access list statistics

**NOTE:** This command is not available in the USER EXEC Mode.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show ip-access-list stats {<IP-ACCESS-LIST-NAME>|detail|on}
show ip-access-list stats {<IP-ACCESS-LIST-NAME>|detail <IP-ACCESS-LIST-NAME>}
{(on <DEVICE-NAME>)}
```

**Parameters**

```
• show ip-access-list stats {<IP-ACCESS-LIST-NAME>|detail <IP-ACCESS-LIST-NAME>}
{(on <DEVICE-NAME>)}
```

| | |
|---|---|
| ip-access-list stats | Displays IP access list statistics |
| <IP-ACCESS-LIST-NAME> | Optional. Displays statistics for a specified IP access list. Specify the IP access list name. |
| detail <IP-ACCESS-LIST-NAME> | Optional. Displays detailed statistics for a specified IP access list. Specify the IP access list name. |
| on <DEVICE-NAME> | The following keyword is recursive and common to the 'IP-ACCESS-LIST-NAME' and 'detail' parameters:<br>• on <DEVICE-NAME> – Optional. Displays all or a specified IP access list statistics on a specified device.<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

**Example**

```
rfs6000-81742D(config)#show ip-access-list stats
IP Access-list: # Restrict Management ACL #
  permit tcp any any eq ftp rule-precedence 1        Hitcount: 0
  permit tcp any any eq www rule-precedence 2        Hitcount: 4
  permit tcp any any eq ssh rule-precedence 3        Hitcount: 448
  permit tcp any any eq https rule-precedence 4        Hitcount: 0
  permit udp any any eq snmp rule-precedence 5       Hitcount: 0
  permit tcp any any eq telnet rule-precedence 6       Hitcount: 4
rfs6000-81742D(config)#
```

The following example displays the ‘auto-tunnel-acl’ IP ACL configuration:

```
rfs4000-229D58(config)#ip access-list auto-tunnel-acl
rfs4000-229D58(config-ip-acl-auto-tunnel-acl)#show context
ip access-list auto-tunnel-acl
permit ip host 200.200.200.99 30.30.30.1/24 rule-precedence 2
permit ip host 200.200.200.99 any rule-precedence 3
rfs4000-229D58(config-ip-acl-auto-tunnel-acl)#
```

The following example displays the statistics for the ‘auto-tunnel-acl’ ACL:

```
rfs4000-229D58#show ip-access-list stats
IP Access-list: auto-tunnel-acl
  permit ip host 200.200.200.99 30.30.30.1/24 rule-precedence 2        Hitcount: 0
  permit ip host 200.200.200.99 any rule-precedence 3         Hitcount: 0

rfs4000-229D58#

nx9500-6C8809#show ip-access-list stats scaleacl | i 125
  permit ip host 125.1.1.1 any rule-precedence 125      Hitcount: 893      Hardware
Hitcount: 3120
  permit ip host 125.2.1.1 any rule-precedence 346       Hitcount: 0       Hardware
Hitcount: 0
nx9500-6C8809#
```

## 6.1.35 ipv6

*show commands*

Displays IPv6 related information

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show ipv6 [default-gateways|delegated-prefix|dhcp|hop-limit|interface|mld|name-server|neighbors|route]

show ipv6 [default-gateways|delegated-prefix|hop-limit|name-server] {on <DEVICE-NAME>}

show ipv6 dhcp [client received-options|relay status|status] {on <DEVICE-NAME>}

show ipv6 interface {<IF-NAME>|brief} {(on <DEVICE-NAME>)}

show ipv6 mld snooping [mrouter vlan <1-4095>|querier vlan <1-4095>|vlan <1-4095>]
{on <DEVICE-NAME>}

show ipv6 neighbors <VLAN-NAME> {(on <DEVICE-NAME>)}

show ipv6 route {<IF-NAME>|ge <1-X>|me1|port-channel <1-2>|ppppoe1|serial <1-4>|
t1e1 <1-4> <1-1>|up|vlan <1-4095>|wwan1|xge} {(on <DEVICE-NAME>)}
```

**Parameters**

- `show ipv6 [default-gateways|delegated-prefix|hop-limit|name-server] {on <DEVICE-NAME>}`

| | |
|---|---|
| ipv6 | Displays IPv6 related information |
| default-gateways | Displays all learnt default gateways |
| delegated-prefix | Displays prefix delegation information |
| hop-limit | Displays the configured IPv6 hop count value |
| name-server | Displays DNS name servers |
| on <DEVICE-NAME> | This parameter is common to all of the above keywords.<br>• on <DEVICE-NAME> – Optional. Displays the specified information on a device (access point, wireless controller, or service platform)<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `show ipv6 dhcp [client received-options|relay status|status] {on <DEVICE-NAME>}`

| | |
|---|---|
| ipv6 | Displays IPv6 related information |
| dhcp | Displays DHCPv6 related information |
| client received-options | Displays DHCP options received from clients |
| relay status | Displays the DHCPv6 relay agent's running status |
| status | Displays the DHCPv6 stateless server daemon's status. In case the DHCPv6 server is up and running, it also displays interface names. |

| | |
|---|---|
| on <DEVICE-NAME> | This parameter is common to all of the above keywords.<br>• on <DEVICE-NAME> – Optional. Displays the specified information on a device (access point, wireless controller, or service platform)<br><DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `show ipv6 interface {<IF-NAME>|brief} {(on <DEVICE-NAME>)}`

| | |
|---|---|
| ipv6 | Displays IPv6 related information |
| interface {<IF-NAME>\|brief} | Displays IPv6 status and configuration on a specified interface related information<br>• <IF-NAME> – Optional. Specify the interface name.<br>• brief – Optional. Displays a brief summary of IPv6 status and configuration on the specified interface |
| on <DEVICE-NAME> | This parameter is common to all of the above keywords.<br>• on <DEVICE-NAME> – Optional. Displays the specified information on a device (access point, wireless controller, or service platform)<br><DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `show ipv6 mld snooping [mrouter vlan <1-4095>|querier vlan <1-4095>|vlan <1-4095>] {on <DEVICE-NAME>}`

| | |
|---|---|
| ipv6 | Displays IPv6 related information |
| mld snooping | Displays *Multicast Listener Discovery Protocol* (MLD) snooping related information |
| mrouter vlan <1-4095> | Displays IPv6 multicast router information on the specified VLAN |
| querier vlan <1-4095> | Displays IPv6 multicast querier information on the specified VLAN |
| vlan <1-4095> | Displays MLD snooping related information on the specified VLAN |
| on <DEVICE-NAME> | This parameter is common to all of the above keywords.<br>• on <DEVICE-NAME> – Optional. Displays the specified information on a device (access point, wireless controller, or service platform)<br><DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `show ipv6 neighbors <VLAN-NAME> {(on <DEVICE-NAME>)}`

| | |
|---|---|
| ipv6 | Displays IPv6 related information |
| neighbors <VLAN-NAME> | Displays IPv6 neighbors on the specified VLAN |
| on <DEVICE-NAME> | Optional. Displays IPv6 neighbors on a specified device (access point, wireless controller, or service platform)<br><DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `show ipv6 route {<IF-NAME>|ge <1-X>|me1|port-channel <1-2>|ppppoe1|serial <1-4>|t1e1 <1-4> <1-1>|up|vlan <1-4095>|wwan1|xge} {(on <DEVICE-NAME>)}`

| | |
|---|---|
| ipv6 | Displays IPv6 related information |

| | |
|---|---|
| route | Displays IPv6 route table |
| <IF-NAME> | Optional. Displays IPv6 route table for the interface identified by the <IF-NAME> keyword |
| ge <1-X> | Optional. Displays IPv6 route table for the selected GigabitEthernet interface |
| me1 | Optional. Displays IPv6 route table for the FastEthernet interface |
| port-channel <1-2> | Optional. Displays IPv6 route table for the selected port-channel interface |
| pppoe1 | Optional. Displays IPv6 route table for the PPP over Ethernet interface |
| vlan <1-4095> | Optional. Displays IPv6 route table for the selected VLAN interface |
| up | Optional. Displays IPv6 route table for the WAN Ethernet interface |
| wwan1 | Optional. Displays IPv6 route table for the wireless WAN interface |
| xge <1-4> | Optional. Displays IPv6 route table for the selected TenGigabitEthernet interface<br>Applicable only for the NX9500 and NX9510 service platforms. |
| on <DEVICE-NAME> | This parameter is common to all of the above keywords.<br>• on <DEVICE-NAME> – Optional. Displays the specified information on a device (access point, wireless controller, or service platform)<br><DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

**Example**

```
rfs6000-81742D(config)#show ipv6 dhcp client received-options
DHCPv6 Client received options:
 Interface:
                None
 Server Identifier:
                None
 Client Identifier:
                None
 DNS Servers:
                None
 Domain Name:
                None
 Sip Servers:
                None
 Sip Domain Name:
                None
 Refresh Time:
                None
 Server Preference:
                None
 Vendor Options:
                None
rfs6000-81742D(config)#
```

```
rfs4000-229D58(config)#show ipv6 route
-------------------------------------------------------------------------------
      DESTINATION            GATEWAY           FLAGS            INTERFACE
-------------------------------------------------------------------------------
      2000:abcd::/64       fe80::300:1       S                vlan300
      default              fe80::11:1        R                vlan11
      4444:1111::/64       direct            C                vlan1
-------------------------------------------------------------------------------
Flags:  C - Connected G - Gateway S - Static R - IPv6-RA
rfs4000-229D58(config)#

rfs4000-229D58#show ipv6 default-gateways
-------------------------------------------------------------------------------
 Source: IPv6-RA                  Gateway-address : fe80::100:1
         Preference: medium           Status      : not-monitored
         Insatlled : NO               Interface   : vlan100
         Remaining Lifetime: 1471 sec
-------------------------------------------------------------------------------
 Source: IPv6-RA                  Gateway-address : fe80::1:2
         Preference: low              Status      : not-monitored
         Insatlled : NO               Interface   : vlan1
         Remaining Lifetime: 1488 sec
-------------------------------------------------------------------------------
 Source: Static-Route             Gateway-address : fe80::2000:1
         Preference: NA               Status      : unreachable
         Insatlled : NO               Interface   : vlan2000
         Remaining Lifetime: forever
-------------------------------------------------------------------------------
 Source: IPv6-RA                  Gateway-address : fe80::11:1
         Preference: high             Status      : reachable
         Insatlled : YES              Interface   : vlan11
         Remaining Lifetime: 1471 sec
-------------------------------------------------------------------------------
rfs4000-229D58#
```

## 6.1.36 ipv6-access-list

*show commands*

Displays IPv6 access list statistics

**NOTE:** This command is not available in the USER EXEC Mode.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show ipv6-access-list stats <IPv6-ACCESS-LIST-NAME> {(on <DEVICE-NAME>)}
```

**Parameters**

- `show ipv6-access-list stats <IPv6-ACCESS-LIST-NAME> {(on <DEVICE-NAME>)}`

| | |
|---|---|
| ipv6-access-list stats | Displays IPv6 access list statistics |
| <IPv6-ACCESS-LIST-NAME> | Optional. Displays statistics for a specified IPv6 access list. Specify the IPv6 access list name.<br>If IPv6 ACL name is not provided, the system displays statistics for all ACLs configured and applied. |
| on <DEVICE-NAME> | Optional. Displays all or a specified IPv6 access list statistics on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

**Example**

```
rfs6000-81742D#show ipv6-access-list stats
IPV6 Access-list: test
  deny ipv6 any any rule-precedence 20        Hitcount: 4

rfs6000-81742D#
```

## 6.1.37 l2tpv3

*show commands*

Displays a *Layer 2 Tunnel Protocol Version 3 (L2TPV3)* session information

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**NOTE:** This command is not available in the USER EXEC mode.

**Syntax**

```
l2tpv3 {on|tunnel|tunnel-summary}

l2tpv3 {on <DEVICE-NAME>}

l2tpv3 {tunnel <L2TPV3-TUNNEL-NAME>} {session <L2TPV3-SESSION-NAME>} {(on <DEVICE-NAME>)}

l2tpv3 {tunnel-summary} {down|on|up}
l2tpv3 {tunnel-summary} {on <DEVICE-NAME>}
l2tpv3 {tunnel-summary} {down|up} {on <DEVICE-NAME>}
```

**Parameters**

- `l2tpv3 {on <DEVICE-NAME>}`

| | |
|---|---|
| l2tpv3 {on <DEVICE-NAME>} | Displays a L2TPv3 tunnel and session details or summary<br>• on <DEVICE-NAME> – Optional. Displays L2TPv3 information on a specified access point or wireless controller<br>• <DEVICE-NAME> – Specify the name of AP, wireless controller, or service platform. |

- `l2tpv3 {tunnel <L2TPV3-TUNNEL-NAME>} {session <L2TPV3-SESSION-NAME>} {(on <DEVICE-NAME>)}`

| | |
|---|---|
| l2tpv3 | Displays a L2TPv3 tunnel and session details or summary |
| tunnel <L2TPV3-TUNNEL-NAME> | Optional. Displays a specified L2TPv3 tunnel information<br>• <L2TPV3-TUNNEL-NAME> – Specify the L2TPv3 tunnel name. |
| session <L2TPV3-SESSION-NAME> | Optional. Displays a specified L2TPv3 tunnel session information<br>• <L2TPV3-SESSION-NAME> – Specify the session name. |
| on <DEVICE-NAME> | The following keyword is recursive and common to the 'session <L2TPV3-SESSION-NAME>' parameter.<br>• on <DEVICE-NAME> – Optional. Displays a L2TPv3 tunnel and session details, based on the parameters passed, on a specified device.<br>• <DEVICE-NAME> – Specify the name of AP, wireless controller, or service platform. |

- `l2tpv3 {tunnel-summary} {on <DEVICE-NAME>}`

| | |
|---|---|
| l2tpv3 | Displays L2TPv3 tunnel and session details or summary<br>For an L2TPv3 tunnel over Auto IPSec, the tunnel status is displayed as: Established (secured by ipsec) |
| tunnel-summary {on <DEVICE-NAME>} | Optional. Displays L2TPv3 tunnel summary<br>• on <DEVICE-NAME> – Optional. Displays a L2TPv3 tunnel summary on a specified device<br>• <DEVICE-NAME> – Specify the name of AP, wireless controller, or service platform. |

- `l2tpv3 {tunnel-summary} {down|up} {on <DEVICE-NAME>}`

| | |
|---|---|
| l2tpv3 | Displays a L2TPv3 tunnel and session details or summary |
| tunnel-summary | Optional. Displays a L2TPv3 tunnel summary, based on the parameters passed |
| down | Optional. Displays un-established tunnels summary |
| up | Optional. Displays established tunnels summary |
| on <DEVICE-NAME> | The following keyword is common to the 'down' and 'up' parameters:<br>• on <DEVICE-NAME> – Optional. Displays summary, for un-established or established tunnels, on a specified device<br>• <DEVICE-NAME> – Specify the name of AP, wireless controller, or service platform. |

**Example**

```
ap7131-11E6C4#show l2tpv3 tunnel-summary
-------------------------------------------------------------------------------
-------
Sl No  Tunnel Name     Tunnel State          Estd/Total  Sessions   Encapsulation
Protocol
-------------------------------------------------------------------------------
-------
1      testTunnel     Established (secured by ipsec)       1/1              IP
Total Number of Tunnels 1
ap7131-11E6C4#

ap7131-11E6C4#show l2tpv3
-------------------------------------------------------------------------------
Tunnel Name : testTunnel
  Control connection id : 2238970979
  Peer Address : 30.1.1.1
  Local Address : 30.1.1.30
  Encapsulation Protocol : IP
  MTU : 1460
  Peer Host Name : rfss
  Peer Vendor Name : Example Company
  Peer Control Connection ID : 322606389
  Tunnel State : Established (secured by ipsec)
  Establishment Criteria : always
  Sequence number of the next msg to the peer : 29
  Expected sequence number of the next msg from the peer :42
  Sequence number of the next msg expected by the peer : 29
  Retransmission count : 0
  Reconnection count : 0
  Uptime : 0 days 1 hours 2 minutes 47 seconds
  -------------------------------------------------------------------------------
  Session Name : session1
    VLANs : 30
    Pseudo Wire Type : Ethernet_VLAN
    Serial number for the session : 6
```

```
    Local Session ID : 129538998
    Remote Session ID : 8151374
    Size of local cookie (0, 4 or 8 bytes) : 0
    First word of local cookie : 0
    Second word of local cookie : 0
    Size of remote cookie (0, 4 or 8 bytes) : 0
    First word of remote cookie : 0
    Second word of remote cookie : 0
    Session state : Established
    Remote End ID : 444
    Trunk Session : 1
    Native VLAN tagged : Enabled
    Native VLAN ID : 0
    Number of packets received : 0
    Number of bytes received : 0
    Number of packets sent : 0
    Number of bytes sent : 0
    Number of packets dropped : 0
ap7131-11E6C4#
```

## 6.1.38 lacp

*show commands*

Displays *Link Aggregation Control Protocol* (LACP) related information

**NOTE:** For more information on enabling dynamic LACP, see *lacp*, *lacp-channel-group*, and *lacp*.

**Supported in the following platforms:**

- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show lacp [<1-4>|counters|details|sys-id]

show lacp <1-4> ([counters|details])

show lacp sys-id
```

**Parameters**

- `show lacp <1-4> ([counters|details])`

| | |
|---|---|
| show lacp <1-4> | Shows the LACP related information for a specified port-channel or all port-channels using LACP<br>• <1-4> – Select the port-channel index number from 1 - 4. Note, LACP is supported only on the NX5500, NX7500, and NX9500 model service platforms. However, the NX9500 series service platforms support only two (2) port-channels. Where as the other model service platforms support four (4) port-channels.<br>If the port-channel index number is not specified, the system displays LACP counters and details for all port-channels configured on the device. |
| counters | Shows LACP counters for LACP-enabled port-channels. When passed without the <1-4> keyword, the system displays LACP counters for all configured port-channels. However, if the port-channel index number is specified, the system displays LACP counters only for the specified port-channel. |
| details | Shows details for LACP-enabled port-channels. When passed without the <1-4> keyword, the system displays LACP details for all configured port-channels. However, if the port-channel index number is specified, the system displays LACP details only for the specified port-channel. |

- `show lacp sys-id`

| | |
|---|---|
| show lacp sys-id | Shows the LACP related information for all LACP-enabled port-channels<br>• sys-id – Shows the LACP system identifier and priority. This is the identifier assigned to the LACP peers (devices). |

**Example**

```
NOC-controller#show interface port-channel 1
Interface port-channel1 is UP
  Hardware-type: aggregate, Mode: Layer 2, Address: 84-24-8D-7F-35-C8
  Index: 2018, Metric: 1, MTU: 1500
  Speed: Admin Auto, Operational 20G, Maximum 20G
  Duplex: Admin Auto, Operational Full
  Active-medium: n/a
  Channel-members: xge1 xge2
  Switchport settings: trunk, access-vlan: n/a
    Input packets 5121052, bytes 807510883, dropped 0
    Received 5121052 unicasts, 0 broadcasts, 516544 multicasts
    Input errors 0, runts 0, giants 0
    CRC 0, frame 0, fragment 0, jabber 0
    Output packets 4804420, bytes 1053174746, dropped 0
    Sent 4804420 unicasts, 0 broadcasts, 0 multicasts
    Output errors 0, collisions 0, late collisions 0
    Excessive collisions 0

NOC-controller#

NOC-controller#show interface port-channel 4
Interface port-channel4 is UP
  Hardware-type: aggregate, Mode: Layer 2, Address: 84-24-8D-7F-35-C4
  Index: 2016, Metric: 1, MTU: 1500
  Speed: Admin Auto, Operational 4G, Maximum 4G
  Duplex: Admin Auto, Operational Full
  Active-medium: n/a
  Channel-members: ge2 ge3 ge4 ge5
  Switchport settings: trunk, access-vlan: n/a
    Input packets 5848499493, bytes 8772550780653, dropped 0
    Received 5848499493 unicasts, 0 broadcasts, 120167 multicasts
    Input errors 0, runts 0, giants 0
    CRC 0, frame 0, fragment 0, jabber 0
    Output packets 362245, bytes 33129264, dropped 0
    Sent 362245 unicasts, 0 broadcasts, 0 multicasts
    Output errors 0, collisions 0, late collisions 0
    Excessive collisions 0

NOC-controller#

NOC-controller#show lacp counters
Port-Channel    Interface                LACPDU              Marker
Packet error
                                 Sent     Recv     Sent     Recv     Sent     Recv
pc1             xge1             11548    12479    0        0        0        0
pc1             xge2             11550    12469    0        0        0        0
pc4             ge2              14081    14041    0        0        0        0
pc4             ge3              15877    15874    0        0        0        0
pc4             ge4              15875    15874    0        0        0        0
pc4             ge5              14064    14052    0        0        0        0
NOC-controller#

NOC-controller#show lacp details
Port-Channel pc1 Interface xge1:
  Actor admin port key                : 1
  Actor oper port key                 : 1
  Actor port priority                 : 32768
  Actor port number                   : 2011
  Actor admin port state              : ActiveLACP LongTimeout Aggregatable
OUT_OF_SYNC Defaulted
  Actor oper port state             : ActiveLACP LongTimeout Aggregatable IN_SYNC
Collecting Distributing
  Partner admin system ID             : 32768, 00-00-00-00-00-00
  Partner oper system ID              : 32768, 44-03-A7-BF-00-00
  Partner admin key                   : 0
  Partner oper key                    : 1
```

```
  Partner admin port priority         : 0
  Partner oper port priority          : 32768
  Partner admin port number           : 0
  Partner oper port number            : 286
  Partner admin port state            : PassiveLACP LongTimeout Aggregatable
OUT_OF_SYNC Defaulted
  Partner oper port state           : ActiveLACP LongTimeout Aggregatable IN_SYNC
Collecting Distributing
  Receive machine state               : Current
  Periodic transmission machine state : Slow periodic
  Mux machine state                   : Collecting/Distributing
Port-Channel pc1 Interface xge2:
  Actor admin port key                : 1
  Actor oper port key                 : 1
  Actor port priority                 : 32768
  Actor port number                   : 2012
  Actor admin port state              : ActiveLACP LongTimeout Aggregatable
OUT_OF_SYNC Defaulted
 --More--
NOC-controller#
```

## 6.1.39 ldap-agent

*show commands*

Displays an LDAP agent's join status (join status to a LDAP server domain)

Use this command When LDAP is specified the external resource (as opposed to local RADIUS resources) to validate PEAP-MS-CHAP v2 authentication requests, user credentials, and password information needs to be made available locally to successfully connect to the external LDAP server. Up to two LDAP Agents (primary and secondary external resources) can be defined as external resources for PEAP-MS-CHAP v2 authentication requests.

**NOTE:** This command is not available in the USER EXEC Mode.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show ldap-agent join-status {on <DEVICE-NAME>}
```

**Parameters**

- `show ldap-agent join-status {on <DEVICE-NAME>}`

| | |
|---|---|
| ldap-agent | Displays LDAP agent related configuration |
| join-status | Displays if the LDAP agent has successfully joined a LDAP server's domain |
| on <DEVICE-NAME> | Optional. Displays if the LDAP agent has successfully joined a specified LDAP server's domain.<br>• <DEVICE-NAME> – Specify the name of the device running the LDAP server (access point, wireless controller, or service platform). |

**Example**

```
rfs6000-81701D#show ldap-agent join-status
Primary LDAP Server's agent join-status : Joined domain TEST.

Secondary LDAP Server's agent join-status : Not Configured
rfs6000-81701D#
```

## 6.1.40 licenses

*show commands*

Displays installed licenses and usage information

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show licenses {borrowed|lent}
```

**Parameters**

- `show licenses {borrowed|lent}`

| | |
|---|---|
| licenses {borrowed\|lent} | Displays installed licenses and usage information<br>• borrowed – Optional. Displays information on licenses borrowed<br>• lent – Optional. Displays information on licenses lent |

**Usage Guidelines**

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

At the time of adoption, access points and adaptive access points are provided license by the adopting controller. These license packs can be installed on both the NOC and site controllers. When a AP/AAP is adopted by a controller, the controller pushes a license on to the device. At this point the various possible scenarios are:

- AP/AAP license packs installed on the NOC controller only.

  The NOC controller provides the site controllers with the AP licenses, ensuring that per platform limits are not exceeded.

- AP/AAP license packs installed on the NOC and site controllers.

  The site controller uses its installed licenses and, in case of a shortage, the site controller borrows additional licenses from the NOC. If the NOC controller is unable to allocate sufficient licenses, the site controller unadopts some of the AP/AAPs.

- AP/AAP license packs installed on one controller within a cluster.

  The site controller shares its installed and borrowed licenses with other cluster controllers.

**Example**

```
rfs4000-229D58#show licenses
Serial Number : 9184521800027

Device Licenses:
  AP-LICENSE
    String     : DEFAULT-6AP-LICENSE
    Value      : 6
    Borrowed   : 0
    Total      : 6
    Used       : 0
  AAP-LICENSE
    String     :
    Value      : 0
    Borrowed   : 0
    Total      : 0
    Used       : 0
  ADVANCED-SECURITY
    String     : DEFAULT-ADV-SEC-LICENSE
rfs4000-229D58#
```

The following example shows the show > licenses command output on a NOC controller:

```
nx9500-6C8809#show licenses
Serial Number : B4C7996C8809

Device Licenses:
  AP-LICENSE
    String     :
    Value      : 0
    Lent       : 0
    Total      : 0
    Used       : 0
  AAP-LICENSE
    String     :
66069c24b3bb1259b34ff016c723a9e299dd408f0ff891e7c5f7e279a382648397d6b3e975e356a1
    Value      : 10250
    Lent       : 0
    Total      : 10250
    Used       : 7
  HOTSPOT-ANALYTICS
    String     :
66069c24b3bb1259eb36826cab3cc83999dd408f0ff891e74b62b2d3594f0b3dde7967f30e49e497

Total Licenses Including Licenses in Adopted Controllers:
  AP-LICENSE
    Value      : 14
    Used       : 1
  AAP-LICENSE
    Value      : 10250
    Used       : 7
nx9500-6C8809#
```

In the following example, the 'VALIDITY(HRS)' column specifies the validity period, in days and hours, of a lent license. On a NOC controller, a 'VALIDITY(HRS)' value of 'current' implies that the site controller is currently adopted. Whereas, a numerical 'VALIDITY(HRS)' value indicates the days and hours the lent license is valid for a site controller that is not reachable.

```
nx9500-6C8809#show licenses lent
-------------------------------------------------------------------------------
---------------------------
 MAC                HOST-NAME          TYPE  LENT  BORROWER-MAC       BORROWER-
HOST-NAME  VALIDITY
-------------------------------------------------------------------------------
---------------------------
 B4-C7-99-6C-88-09  nx9500-6C8809      AAP   5     00-15-70-81-74-2D  rfs6000-
81742D      current
 B4-C7-99-6C-88-09  nx9500-6C8809      AAP   9     B4-C7-99-6D-CD-4B  rfs7000-
6DCD4B      97 days, 21 hours
-------------------------------------------------------------------------------
---------------------------
nx9500-6C8809#

rfs4000-881E4B#show licenses borrowed
-------------------------------------------------------------------------------
MAC                HOST-NAME          TYPE      BORROWED  VALIDITY
-------------------------------------------------------------------------------
00-15-70-37-FD-89  rfs7000-37FD89     AAP       2         99 days, 23 hours
00-15-70-81-70-1D  rfs6000-81701D     AP        1         99 days, 23 hours
-------------------------------------------------------------------------------
rfs4000-881E4B#
```

The following examples show the 'show > licenses' output on the devices participating in the process:

```
nx9500-6C8809>show licenses lent
-------------------------------------------------------------------------------
---------------------------
 MAC                HOST-NAME          TYPE  LENT  BORROWER-MAC       BORROWER-
HOST-NAME  VALIDITY
-------------------------------------------------------------------------------
---------------------------
 B4-C7-99-6C-88-09  nx9500-6C8809      AAP   1     00-15-70-81-74-2D  rfs6000-
81742D      current
 B4-C7-99-6C-88-09  nx9500-6C8809      AAP   9     B4-C7-99-6D-CD-4B  rfs7000-
6DCD4B      99 days, 23 hours
-------------------------------------------------------------------------------
---------------------------

nx9500-6C8809>

rfs6000-81742D(config)#show licenses borrowed
-------------------------------------------------------------------------------
 MAC                HOST-NAME          TYPE      BORROWED  VALIDITY
-------------------------------------------------------------------------------
 B4-C7-99-6C-88-09  nx9500-6C8809      AAP       1         current
-------------------------------------------------------------------------------
rfs6000-81742D(config)#
```

## 6.1.41 lldp

*show commands*

Displays *Link Layer Discovery Protocol* (LLDP) information

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show lldp [neighbors|report]
show lldp neighbors {on <DEVICE-NAME>}
show lldp report {detail|on}
show lldp report {detail} {(on <DEVICE-OR-DOMAIN-NAME>)}
```

**Parameters**

- `show lldp neighbors {on <DEVICE-NAME>}`

| | |
|---|---|
| lldp | Displays an LLDP neighbors table or aggregated LLDP neighbors table |
| neighbors | Displays an LLDP neighbors table |
| on <DEVICE-NAME> | Optional. Displays an LLDP neighbors table on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `show lldp report {detail} {(on <DEVICE-OR-DOMAIN-NAME>)}`

| | |
|---|---|
| lldp | Displays an LLDP neighbors table or aggregated LLDP neighbors table |
| report detail | Displays an aggregated LLDP neighbors table<br>• detail – Optional. Displays detailed aggregated LLDP neighbors table<br>**Note:** If the 'on' keyword is used without the 'detail' keyword, the system displays LLDP neighbors table summary on the specified device or RF Domain. |
| on <DEVICE-OR-DOMAIN-NAME> | The following keyword is recursive and common to the 'report detail' parameter:<br>• on <DEVICE-OR-DOMAIN-NAME> – Displays an aggregated LLDP neighbors table on a specified device or RF Domain<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |

**Example**

```
nx9500-6C8809#show lldp neighbors
-------------------------
Chassis ID: 00-18-71-D0-0B-00
System Name: TechPubs-ProCurve-Switch
Platform: ProCurve J8697A Switch 5406zl, revision K.12.1X, ROM K.11.03 (/sw/code/
build/btm(sw_esp1))
Capabilities: Bridge  Router
Enabled Capabilities: Bridge
Local Interface: ge1, Port ID(Port Description) (outgoing port): 5(A5)
TTL: 113 sec
Management Addresses: 192.168.13.40
nx9500-6C8809#
```

## 6.1.42 logging

*show commands*

Displays the network's activity log

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show logging {on <DEVICE-NAME>}
```

**Parameters**

- `show logging {on <DEVICE-NAME>}`

| | |
|---|---|
| logging<br>{on <DEVICE-NAME>} | Displays logging information on a specified device<br>• on <DEVICE-NAME> – Optional. Executes the command on a specified device.<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

**Example**

```
nx9500-6C8809#show logging

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

Log Buffer (1666269 bytes):


May 14 05:30:23 2015: nx9500-6C8809 : %DIAG-4-PWRSPLY_FAIL: Power supply failure,
no longer redundant
May 14 05:30:13 2015: nx9500-6C8809 : %DEVICE-4-OFFLINE: Device B4-C7-99-74-B4-
5C(ap8132-74B45C) is offline, last seen:10 minutes ago on switchport rfs6000-
6DB5D4:ge1
May 14 05:20:16 2015: nx9500-6C8809 : %DIAG-4-PWRSPLY_FAIL: Power supply failure,
no longer redundant
May 14 05:19:43 2015: nx9500-6C8809 : %DEVICE-4-OFFLINE: Device B4-C7-99-74-B4-
5C(ap8132-74B45C) is offline, last seen:10 minutes ago on switchport rfs6000-
380649:ge1
--More--
nx9500-6C8809#
```

## 6.1.43 mac-access-list

*show commands*

Displays MAC access list statistics

**NOTE:** This command is not present in USER EXEC mode.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show mac-access-list stats {<MAC-ACCESS-LIST-NAME>|on}
show mac-access-list stats {<MAC-ACCESS-LIST-NAME>} {(on <DEVICE-NAME>)}
```

**Parameters**

- `show mac-access-list stats {<MAC-ACCESS-LIST-NAME>} {(on <DEVICE-NAME>)}`

| | |
|---|---|
| mac-access-list stats | Displays MAC access list statistics |
| <MAC-ACCESS-LIST> | Optional. Displays statistics for a specified MAC access list. Specify the MAC access list name.<br>**Note:** The system displays all configured ACL statistics if no ACL name is specified. |
| on <DEVICE-NAME> | Optional. Displays all or a specified MAC access list statistics on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

**Example**

```
nx9500-6C8809#show mac-access-list stats scalemacacl | i 311
  permit D0-67-E5-3F-C0-00 FF-FF-FF-FF-F0-00  host 00-1E-EC-F2-0A-76 rule-
precedence 311        Hitcount: 0        Hardware Hitcount: 0
nx9500-6C8809#
```

## 6.1.44 mac-address-table

*show commands*

Displays MAC address table entries

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show mac-address-table {on <DEVICE-NAME>}
```

**Parameters**

- `show mac-address-table {on <DEVICE-NAME>}`

| | |
|---|---|
| mac-address-table | Displays MAC address table entries |
| on <DEVICE-NAME> | Optional. Displays MAC address table entries on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

**Example**

```
rfs6000-81742D(config)#show mac-address-table
------------------------------------------------------------
 BRIDGE VLAN PORT             MAC               STATE
------------------------------------------------------------
 1      1    up1              00-02-B3-28-D1-55 forward
 1      1    up1              00-0F-8F-19-BA-4C forward
 1      1    up1              84-24-8D-80-C2-AC forward
 1      1    up1              84-24-8D-80-BF-34 forward
 1      1    up1              1C-7E-E5-18-FA-67 forward
 1      1    up1              84-24-8D-83-30-A4 forward
 1      1    up1              B4-C7-99-DD-31-C8 forward
 1      1    up1              B4-C7-99-6C-88-09 forward
 1      1    up1              00-18-71-D0-1B-F3 forward
 1      1    up1              B4-C7-99-71-17-28 forward
 1      1    up1              FC-0A-81-42-93-6C forward
 1      1    up1              B4-C7-99-6D-CD-4B forward
 1      1    up1              84-24-8D-84-A2-24 forward
 1      1    up1              3C-CE-73-F4-47-83 forward
 1      1    up1              B4-C7-99-74-B4-5C forward
------------------------------------------------------------
Total number of MACs displayed: 15
rfs6000-81742D(config)#
```

## 6.1.45 mac-auth

*show commands*

Displays details of wired ports that have MAC address authentication enabled

Use this command to view MAC authentication configuration and authentication state. The command displays the current authentication state of the wired host, the authorization state of the Ge1 port, and the wired hosts' MAC address. The port status displays as *Authorized* if the wired host has successfully authenticated and *Not Authorized* if the wired host has not authenticated or has failed MAC authentication.

For more information on enabling MAC address authentication on a wired port, see *mac-auth*.

**Supported in the following platforms:**

- Access Points — AP6511
- Wireless Controllers — RFS4000, RFS6000

**Syntax**

```
show mac-auth {all|interface|on}

show mac-auth {all|interface [<INTERFACE-NAME>|ge <1-5>|port-channel <1-3>|t1e1
<1-4>|up <1-2>|xge <1-4>]} {(on <DEVICE-NAME>)}
```

**Parameters**

```
• show mac-auth {all|interface [<INTERFACE-NAME>|ge <1-5>|port-channel <1-3>|t1e1
<1-4>|up <1-2>|xge <1-4>]} {(on <DEVICE-NAME>)}
```

| | |
|---|---|
| mac-auth | Displays MAC authentication related information for all interfaces or all interfaces |
| all | Optional. Displays MAC authentication related information for all interfaces |
| interface [<INTERFACE-NAME>\|ge <1-5>\| port-channel <1-3>\| t1e1 <1-4>\|up <1-2>\| xge <1-4>] | Optional. Displays MAC authentication related information for a specified interface. Specify the interface using one of the following options:<br>• <INTERFACE-NAME> – Selects the interface identified by the <INTERFACE-NAME> keyword<br>• ge <1-5> – Selects the GigabitEthernet interface identified by the index number<br>• port-channel <1-3> – Selects the port channel interface identified by the index number<br>• t1e1 <1-4> – Selects the layer 2 interface (Ethernet port)<br>• up <1-2> – Selects the WAN Ethernet interface identified by the index number<br>• xge <1-4> – Selects the TenGigabitEthernet interface identified by the index number |
| on <DEVICE-NAME> | The following keywords are common to the 'all' and 'interface' parameters:<br>• on <DEVICE-NAME> – Optional. Displays MAC authentication related information on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.<br>**Note:** When the 'on' keyword is used exclusively, without the 'all' and 'interface' options, the system displays MAC authentication related information for interfaces configured on the specified device. |

**Example**

```
rfs4000-229D58(config)#show mac-auth all
AAA-Policy is none

Mac Auth info for interface GE1
-----------------------------------
 Mac Auth Enabled
 Mac Auth Not Authorized

Mac Auth info for interface GE2
-----------------------------------
 Mac Auth Disabled
 Mac Auth Not Authorized

Mac Auth info for interface GE3
-----------------------------------
 Mac Auth Disabled
 Mac Auth Not Authorized

Mac Auth info for interface GE4
-----------------------------------
 Mac Auth Disabled
 Mac Auth Authorized

Mac Auth info for interface GE5
-----------------------------------
 Mac Auth Disabled
 Mac Auth Not Authorized

Mac Auth info for interface UP1
-----------------------------------
 Mac Auth Disabled
 Mac Auth Not Authorized
rfs4000-229D58(config)#
```

## 6.1.46 mac-auth-clients

*show commands*

Displays MAC authenticated clients

**Supported in the following platforms:**

- Access Points — AP6511
- Wireless Controllers — RFS4000, RFS6000

**Syntax**

```
show mac-auth-clients [all|interface]

show mac-auth-clients all {on <DEVICE-NAME>}
show mac-auth-clients interface {<INF-NAME>|ge <1-X>|port-channel <1-2>|xge <1-4>}
```

**Parameters**

- `show mac-auth-clients all {on <DEVICE-NAME>}`

| | |
|---|---|
| mac-auth-clients | Displays MAC authenticated clients based on the parameters passed. The options are: all and interface. |
| all | Displays MAC authenticated clients for all interfaces |
| on <DEVICE-NAME> | Optional. Displays MAC authenticated clients for all interfaces on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `show mac-auth-clients interface {<INF-NAME>|ge <1-X>|port-channel <1-2>|xge <1-4>}`

| | |
|---|---|
| mac-auth-clients | Displays MAC authenticated clients based on the parameters passed. The options are: all and interface. |
| interface [<INF-NAME>\| ge <1-X>\| port-channel <1-2>\| xge <1-4>] | Displays MAC authenticated clients for the specified interface. Select the interface type from the following options:<br>• <INF-NAME> – Optional. Displays MAC authenticated clients for the interface identified by the <INF-NAME> keyword. Specify the layer 2 (ethernet port) interface name.<br>• ge <1-X> – Optional. Displays MAC authenticated clients for the selected GigabitEthernet interface. Specify the GE interface index from 1 - X. This will vary for different device types.<br>• port-channel <1-2> – Optional. Displays MAC authenticated clients for the selected port channel interface. Specify the port channel interface index from 1 - 2.<br>• xge <1-4> – Optional. Displays MAC authenticated clients for the selected TenGigabitEthernet interface. Specify the interface index from 1 - 4. |
| on <DEVICE-NAME> | Optional. Displays MAC authenticated clients for the specified interface on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

**Example**

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#show mac-auth-clients interface ge
1
------------------------------------------------
 MAC               STATE            INTERFACE
------------------------------------------------
------------------------------------------------
Total number of MACs displayed: 0
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#
```

## 6.1.47 mint

*show commands*

Displays MiNT protocol related statistics

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show mint [config|dis|id|info|known-adopters|links|lsp|lsp-db|mlcp|neighbors|
route|stats|tunnel-controller|tunneled-vlans]

show mint [config|id|info|known-adopters|route|stats|tunneled-vlans] {on <DEVICE-
NAME>}

show mint [dis|links|neighbors|tunnel-controller] {details} {(on <DEVICE-NAME>)}

show mint lsp

show mint lsp-db {details <MINT-ADDRESS>} {(on <DEVICE-NAME>)}

show mint mlcp {history} {(on <DEVICE-NAME>)}
```

**Parameters**

- `show mint [config|id|info|known-adopters|route|stats|tunneled-vlans] {on <DEVICE-NAME>}`

| | |
|---|---|
| mint | Displays MiNT protocol information based on the parameters passed |
| config | Displays MiNT configuration |
| id | Displays local MiNT ID |
| info | Displays MiNT status |
| known-adopters | Displays known, possible, or reachable adopters |
| route | Displays MiNT route table details |
| stats | Displays MiNT related statistics |
| tunneled-vlans | Displays MiNT tunneled VLAN details |
| on <DEVICE-NAME> | The following keywords are common to all of the above parameters:<br>• on <DEVICE-NAME> – Optional. Displays MiNT protocol details on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `show mint [dis|links|neighbors|tunnel-controller] {details} {(on <DEVICE-NAME>)}`

| | |
|---|---|
| mint | Displays MiNT protocol information based on the parameters passed |
| dis | Displays MiNT network *Designated Intermediate Systems* (DISes) and *Ethernet Virtualization Interconnects* (EVISes) |
| links | Displays MiNT networking link details |
| neighbors | Displays adjacent MiNT peer details |

| | |
|---|---|
| tunnel-controller | Displays details of MiNT VLAN network tunnel wireless controllers for extended VLAN load balancing |
| details {(on <DEVICE-NAME>)} | The following keywords are common to the 'dis', 'links', 'neighbors', and 'tunnel-controller' parameters:<br>• details – Optional. Displays detailed MiNT information<br>• on <DEVICE-NAME> – Optional. This is a recursive parameter, which displays MiNT information on a specified device.<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `show mint lsp`

| | |
|---|---|
| mint | Displays MiNT protocol information based on the parameters passed |
| lsp | Displays this router's MiNT *Label Switched Paths* (LSPs) |

- `show mint lsp-db {details <MINT-ADDRESS>} {(on <DEVICE-NAME>)}`

| | |
|---|---|
| mint | Displays MiNT protocol information based on the parameters passed |
| lsp-db | Displays MiNT LSP database entries |
| details <MINT-ADDRESS> | Optional. Displays detailed MiNT LSP database entries<br>• <MINT-ADDRESS> – Specify the MiNT address in the AA.BB.CC.DD format. |
| on <DEVICE-NAME> | The following keyword is recursive and common to the 'details' parameter:<br>• on <DEVICE-NAME> – Optional. Displays MiNT LSP database entries on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP or wireless controller |

- `show mint mlcp {history} {(on <DEVICE-NAME>)}`

| | |
|---|---|
| mint | Displays MiNT protocol information based on the parameters passed<br>This command displays the 'hello-interval' and 'hold-time' default values for both IP and VLAN links. |
| mlcp | Displays IPv4 and IPv6 *MiNT Link Creation Protocol* (MLCP) status |
| history | Optional. Displays MLCP client history<br>• on <DEVICE-NAME> – Optional. Displays MLCP client history on a specified device |
| on <DEVICE-NAME> | The following keyword is recursive and common to the 'history' parameter:<br>• on <DEVICE-NAME> – Optional. Displays MLCP client history on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

**Example**

```
nx9500-6C8809#show mint stats
9 Level-1 neighbors
Level-1 LSP DB size 26 LSPs (4 KB)
Last Level-1 SPFs took 0.000s
Level-1 SPF (re)calculated 818 times.
26 Level-1 paths.
0 Level-2 neighbors
Level-2 LSP DB size 0 LSPs (0 KB)
Last Level-2 SPFs took 0.000s
Level-2 SPF (re)calculated 0 times.
0 Level-2 paths.
nx9500-6C8809#
```

```
nx9500-6C8809#show mint lsp
id 19.6C.88.09, level 1, 9 adjacencies, 0 extended-vlans
seqnum 1476782, expires in 29 minutes, republish in 1362 seconds
161 bytes, can-adopt: True, adopted-by: 00.00.00.00, dis-priority 5, Level-2-
gateway: False
hostname "nx9500-6C8809"
cluster id "TechPubs"
rf-domain "TechPubs", priority vector: 0x60dc0000
adjacent to 4D.83.30.A4, cost 10
adjacent to 4D.84.A2.24, cost 10
adjacent to 19.74.B4.5C, cost 10
adjacent to 19.6D.CD.4B, cost 10
adjacent to 19.DD.31.C8, cost 10
adjacent to 4D.80.C2.AC, cost 10
adjacent to 4D.80.BF.34, cost 10
adjacent to 19.71.17.28, cost 10
adjacent to 70.81.74.2D, cost 10
nx9500-6C8809#

nx9500-6C8809#show mint lsp-db
26 LSPs in LSP-db of 19.6C.88.09:
LSP 19.6C.88.09 at level 1, hostname "nx9500-6C8809", 9 adjacencies, seqnum 1476782
LSP 19.6C.8A.49 at level 1, hostname "nx9500-6C8A49pp", 9 adjacencies, seqnum 67397
LSP 19.6D.CD.4B at level 1, hostname "rfs7000-6DCD4B", 9 adjacencies, seqnum
1143297
LSP 19.71.17.28 at level 1, hostname "ap8132-711728", 9 adjacencies, seqnum 837272
LSP 19.72.D4.F4 at level 1, hostname "ap650-72D4F4", 2 adjacencies, seqnum 107768
LSP 19.72.D5.44 at level 1, hostname "ap4600-72D544", 9 adjacencies, seqnum 10889
LSP 19.72.E6.C4 at level 1, hostname "ap6532-72E6C4", 2 adjacencies, seqnum 109985
LSP 19.74.B4.5C at level 1, hostname "ap8132-74B45C", 9 adjacencies, seqnum 1659590
LSP 19.DD.31.C8 at level 1, hostname "rfs4000-DD31C8", 25 adjacencies, seqnum
1787045
LSP 1A.7C.D5.A4 at level 1, hostname "ap8222-7CD5A4", 9 adjacencies, seqnum 440488
LSP 1A.7E.79.E8 at level 1, hostname "ap8122-7E79E8", 9 adjacencies, seqnum 100282
LSP 1A.B1.9C.40 at level 1, hostname "ap7131-B19C40", 9 adjacencies, seqnum 95001
LSP 4D.80.BF.34 at level 1, hostname "Rajeev-AP", 9 adjacencies, seqnum 232516
LSP 4D.80.C2.AC at level 1, hostname "ap7532-80C2AC", 9 adjacencies, seqnum 842369
LSP 4D.83.30.A4 at level 1, hostname "ap7522-8330A4", 9 adjacencies, seqnum 478482
LSP 4D.84.A2.24 at level 1, hostname "ap7562-84A224", 9 adjacencies, seqnum 562219
LSP 4D.8A.15.C8 at level 1, hostname "AP1", 1 adjacencies, seqnum 92687
LSP 68.88.10.D1 at level 1, hostname "rfs4000-8810D1", 9 adjacencies, seqnum 115580
LSP 70.38.03.E7 at level 1, hostname "rfs7000-3803E7", 9 adjacencies, seqnum 947279
LSP 70.81.74.2D at level 1, hostname "rfs6000-81742D", 9 adjacencies, seqnum 487287
LSP 75.A2.A4.90 at level 1, hostname "ap7532-A2A490", 4 adjacencies, seqnum 181692
LSP 75.A2.A4.B0 at level 1, hostname "ap7532-A2A4B0", 4 adjacencies, seqnum 180804
LSP 75.A2.A5.54 at level 1, hostname "ap7532-A2A554", 4 adjacencies, seqnum 156084
LSP 75.A2.A5.6C at level 1, hostname "Snap004-AceessPoint", 4 adjacencies, seqnum
169181
LSP 75.D1.AA.7A at level 1, hostname "ap7622-D1AA7A", 9 adjacencies, seqnum 5471
LSP 75.D1.B2.68 at level 1, hostname "ap7602-D1B268", 9 adjacencies, seqnum 6054
nx9500-6C8809#

nx9500-6C8809#show mint route
Destination : Next-Hop(s)
4D.84.A2.24 : 4D.84.A2.24 via vlan-1
1A.7C.D5.A4 : 19.DD.31.C8 via vlan-1
68.88.10.D1 : 19.DD.31.C8 via vlan-1
19.72.E6.C4 : 19.DD.31.C8 via vlan-1
75.A2.A5.54 : 19.DD.31.C8 via vlan-1
1A.B1.9C.40 : 19.DD.31.C8 via vlan-1
70.81.74.2D : 70.81.74.2D via vlan-1
19.6C.8A.49 : 19.DD.31.C8 via vlan-1
19.74.B4.5C : 19.74.B4.5C via vlan-1
19.6D.CD.4B : 19.6D.CD.4B via vlan-1
19.72.D5.44 : 19.DD.31.C8 via vlan-1
75.D1.AA.7A : 19.DD.31.C8 via vlan-1
75.A2.A4.B0 : 19.DD.31.C8 via vlan-1
19.71.17.28 : 19.71.17.28 via vlan-1
```

```
70.38.03.E7 : 19.DD.31.C8 via vlan-1
4D.80.C2.AC : 4D.80.C2.AC via vlan-1
19.6C.88.09 : 19.6C.88.09 via self
75.A2.A4.90 : 19.DD.31.C8 via vlan-1
1A.7E.79.E8 : 19.DD.31.C8 via vlan-1
19.DD.31.C8 : 19.DD.31.C8 via vlan-1
75.A2.A5.6C : 19.DD.31.C8 via vlan-1
19.72.D4.F4 : 19.DD.31.C8 via vlan-1
4D.83.30.A4 : 4D.83.30.A4 via vlan-1
4D.80.BF.34 : 4D.80.BF.34 via vlan-1
4D.8A.15.C8 : 19.DD.31.C8 via vlan-1
75.D1.B2.68 : 19.DD.31.C8 via vlan-1
nx9500-6C8809#

nx9500-6C8809#show mint known-adopters
19.6C.8A.49
nx9500-6C8809#

nx9500-6C8809#show mint known-adopters
19.6C.8A.49
nx9500-6C8809#
nx9500-6C8809#show min config
Base priority 5
DIS priority 5
Control priority 220
UDP/IP Mint encapsulation port 24576
Global Mint MTU 1500
nx9500-6C8809#

ap7532-15E6E4#show mint mlcp
MLCP VLAN state: MLCP_DONE
  Potential VLAN links: 1
  All VLANs were scanned 2 times
Link created on VLAN 1
MLCP IP state: MLCP_DISCOVERING
  Potential L3 Links:
    192.168.1.43
MCLP IP Hello Interval: 15s(default), Adjacency hold time: 46s(default)
MCLP VLAN Hello Interval: 4s(default), Adjacency hold time: 13s(default)
ap7532-15E6E4#
```

## 6.1.48 nsight

*show commands*

Displays NSight related information and also displays the database server status (reachable or not)

**Supported in the following platforms:**

- Service Platforms — NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show nsight status
```

**Parameters**

- `show nsight status`

| | |
|---|---|
| nsight | Displays the NSight module related status, such as:<br>• NSight is enabled or not on the device<br>• NSight report and aggregation daemon is running or not<br>• NSight alarm daemon is running or not<br>• NSight server daemon is running or not<br>• Database server is reachable or not |

**Example**

```
nx9500-6C8809(config)#show nsight status
Nsight is enabled
 Nsight report and aggregation daemon is running
 Nsight alarm daemon is running
 Nsight server daemon is running
 Database server is local
 Database server is reachable
nx9500-6C8809(config)#
```

## 6.1.49 ntp

*show commands*

Displays *Network Time Protocol* (NTP) information. NTP enables clock synchronization within a network.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show ntp [associations|status]
show ntp [associations {detail|on}|status {on <DEVICE-NAME>}]
```

**Parameters**

- `show ntp [associations {detail|on}|status {on <DEVICE-NAME>}]`

| | |
|---|---|
| ntp associations {detail\|on} | Displays existing NTP associations. The interaction between the controller or service platform and a SNTP server constitutes an association. SNTP associations are of two kinds:<br>- peer associations - where a controller or service platform synchronizes to another system or allows another system to synchronize to it, or<br>- server associations - where only the controller or service platform synchronizes to the SNTP resource, not the other way around.<br>• detail – Optional. Displays detailed NTP associations<br>  • on <DEVICE-NAME> – Optional. Displays NTP associations on a specified device<br>  • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.<br>**Note:** If the 'on' keyword is used without the 'detail' keyword, the system displays a summary of existing NTP associations on the specified device or RF Domain. |
| ntp status {on <DEVICE-NAME>} | Displays the performance (status) information relative to the NTP association status. Use this command to view the access point, controller, or service platform's current NTP resource.<br>• on <DEVICE-NAME> – Optional. Displays NTP association status on a specified device<br>  • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

**Example**

```
nx9500-6C8809#show ntp associations
-------------------------------------------------------------------------------
-----------------------------------
 STATUS NTP SERVER IP ADDR REF CLOCK IP ADDR STRATUM   WHEN     POLL     REACH
DELAY     OFFSET    DISPERSION
-------------------------------------------------------------------------------
-----------------------------------
   ~    12.12.12.12       INIT            16     -       1024     0        0.0
0.0       15937.5
   ~    11.11.11.11       INIT            16     -       1024     0        0.0
0.0       15937.5
-------------------------------------------------------------------------------
-------
STATUS Notation: * master (synced), # master (unsynced), + selected, - candidate,
~ configured
nx9500-6C8809#


nx9500-6C8809#show ntp status
-------------------------------------------------------------------------------
           ITEM                                    VALUE
-------------------------------------------------------------------------------
  Leap                     Clock is unsynchronized
  Stratum                  16
  Reference                INIT
  Frequency                0.0000 Hz
  Precision                2^-20
  Reference time           00000000.00000000 (Feb 07 11:58:16 UTC 2036)
  Clock Offset             0.000 msec
  Root delay               0.000 msec
  Root Dispersion          0.000 msec
-------------------------------------------------------------------------------
nx9500-6C8809#
```

## 6.1.50 password-encryption

*show commands*

Displays password encryption status (enabled/disabled)

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show password-encryption status
```

**Parameters**

- `show password-encryption status`

| | |
|---|---|
| password-encryption status | Displays password encryption status (enabled/disabled) |

**Example**

```
rfs6000-81742D(config)#show password-encryption status
Password encryption is enabled
rfs6000-81742D(config)#
```

## 6.1.51 pppoe-client

*show commands*

Displays *Point-to-Point Protocol over Ethernet* (PPPoE) client information

Use this command to view PPPoE statistics derived from access to high-speed data and broadband networks. PPPoE uses standard encryption, authentication, and compression methods as specified by the PPPoE protocol. PPPoE enables point-to-points connection to an ISP over existing Ethernet interface.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show pppoe-client [configuration|status] {on <DEVICE-NAME>}
```

**Parameters**

- `show pppoe-client [configuration|status] {on <DEVICE-NAME>}`

| | |
|---|---|
| pppoe-client | Displays PPPoE client information (configuration and status) |
| configuration | Displays detailed PPPoE client configuration |
| status | Displays detailed PPPoE client status |
| on <DEVICE-NAME> | The following keywords are common to 'configuration' and 'status' parameters:<br>• on <DEVICE-NAME> – Optional. Displays detailed PPPoE client status or configuration on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

**Example**

```
nx9500-6C8809#show pppoe-client configuration
 PPPoE Client Configuration:
+-----------------------------------------
|  Mode          : Disabled
|  Service Name  :
|  Auth Type     : pap
|  Username      :
|  Password      : fJx5O+5duPjaOaPuXmtLDQAAAAAmvgEXcQ1+eUK4ByHK4aRi
|  Idle Time     : 600
|  Keepalive     : Disabled
|  Local n/w     : vlan1
|  Static IP     : __wing_internal_not_set__
|  MTU           : 1492
+-----------------------------------------

nx9500-6C8809#
```

## 6.1.52 privilege

*show commands*

Displays a device's existing privilege level

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show privilege
```

**Parameters**

None

**Example**

```
rfs6000-81742D(config)#show privilege
Current user privilege: superuser
rfs6000-81742D(config)#
```

## 6.1.53 radius

*show commands*

Displays the amount of access time consumed and the amount of access time remaining for all guest users configured on a RADIUS server

Every captive portal guest user can access the captive portal for a specified duration. This results in following three scenarios:

- Scenario 1: Access duration not specified (in this case the default of 1440 minutes is applied)
- Scenario 2: Access duration is specified and is greater than 0
- Scenario 3: Access duration is specified and equals to 0 (in this case the guest user has unlimited access)

In all the three scenarios the access time consumed is the duration for which the guest user has logged.

But the access time remaining varies. It is calculated as follows:

- Scenarios 1 & 2 - It is the lesser of the following two values: difference between the configured access duration and the time consumed AND the time until user account expiration.
- Scenario 3 - It is the time until user account expiration

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show radius [guest-users|server]

show radius guest-users {brief|<GUEST-USER-NAME>}

show radius server
```

**Parameters**

- `show radius guest-users {brief|<GUEST-USER-NAME>}`

| | |
|---|---|
| radius guest-users {brief\|<GUEST-USER-NAME>} | Displays RADIUS server's guest user's access details: total time for which the user has logged in, and the amount of access time remaining.<br>• brief – Displays the total number of guest users provided RADIUS access<br>• <GUEST-USER-NAME> – Optional. Provide the name of the guest user (whose access details are to be viewed). If no name is provided, the system displays details of all guest users who have successfully logged in at least once.<br><br>Use this command in the captive-portal context to view time and data statistics for guest user(s) having bandwidth-based or time-based vouchers configured. In such a scenario, the system displays the following information: data configured, data remaining, configured and current bandwidths (for both downlink and uplink), time configured, and time remaining.<br>Contd.. |

| | |
|---|---|
| | If bandwidth-based voucher is not applicable to a guest user, the data configured and data remaining values are displayed as 'unlimited'. The bandwidth columns are blank. If time-based voucher is not applicable to a guest user, the only value displayed is the time remaining (which is the time till the expiration of the guest user's account).<br>**Note:** For more information on configuring bandwidth-based and time-based vouchers, see *user*. |

- `show radius server`

| | |
|---|---|
| show radius server | Displays RADIUS server related statistical data |

**Example**

```
rfs4000-229D58#show radius guest-users
         TIME (min:sec)
       USED    REMAINING   GUEST USER
       0:00         9:00   time9
       0:00         5:00   time5
       0:00        15:00   time15
       0:00    305416:35   notime
       2:31         7:29   time10
rfs4000-229D58#
```

The following example shows a RADIUS user pool with guest users having bandwidth-based, time-based, bandwidth and time based, and no bandwidth or time based vouchers:

```
rfs4000-229D58(config-captive-portal-wdws)#show context
radius-user-pool-policy wdws
 user time_and_data password 0 both group wdws guest expiry-time 12:00 expiry-date 12/31/2015 access-duration  8000 data-limit  500 committed-downlink  3000 committed-uplink  2000 reduced-downlink  1000 reduce4
 user neither password 0 nine group wdws guest expiry-time 12:00 expiry-date 12/31/2015
 user data_only password 0 data group wdws guest expiry-time 12:00 expiry-date 12/31/2015 data-limit  125 committed-downlink  1000 committed-uplink  800 reduced-downlink  500 reduced-uplink  400
rfs4000-229D58(config-captive-portal-wdws)#
```

The following example shows the captive portal access details for the above mentioned RADIUS user pool users:

```
rfs4000-229D58(config-captive-portal-wdws)#show radius guest-users
                    TIME (DD:HH:MM:SS)           DATA (kilobytes)
BANDWIDTH (kbps)
GUEST USER          CONFIGURED     REMAINING    CONFIGURED    REMAINING    CFGD
DN   CURR DN   CFGD UP   CURR UP
time_and_data      5:13:20:00   5:12:00:50      512000     433727     3000
0      2000         0
neither             till expiry  221:19:44:54     unlimited    unlimited
data_only         till expiry  221:19:44:54      128000     127587     1000
0       800         0
time_only            3:11:20:00    3:11:19:47     unlimited    unlimited
Current time: 17:15:07
rfs4000-229D58(config-captive-portal-wdws)#
```

## 6.1.54 reload

*show commands*

Displays scheduled reload information for a specific device

**NOTE:** This command is not present in the USER EXEC mode.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show reload {on <DEVICE-OR-DOMAIN-NAME>}
```

**Parameters**

- `show reload {on <DEVICE-OR-DOMAIN-NAME>}`

| | |
|---|---|
| reload<br>{on <DEVICE-OR-DOMAIN-NAME>} | Displays scheduled reload information for a specified device<br>• on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays configuration on a specified device<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |

**Example**

```
rfs6000-81742D(config)#show reload
No reload is scheduled.
rfs6000-81742D(config)#
```

## 6.1.55 rf-domain-manager

*show commands*

Displays RF Domain manager selection details

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show rf-domain-manager {on <DEVICE-OR-DOMAIN-NAME>}
```

**Parameters**

- `show rf-domain-manager {on <DEVICE-OR-DOMAIN-NAME>}`

| | |
|---|---|
| rf-domain-manager | Displays RF Domain manager selection details |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Displays RF Domain manager selection details on a specified device or domain<br>• <DEVICE-OR-DOMAIN-NAME> – specify the name of the AP, wireless controller, service platform, or RF Domain. |

**Example**

```
nx9500-6C8809#show rf-domain-manager
 RF Domain TechPubs
 RF Domain Manager:
    ID: 19.6C.88.09
 Controller Managed
 Device under query:
    Priority: 220
    Has IP MiNT links
    Has wired MiNT links
nx9500-6C8809#
```

## 6.1.56 role

*show commands*

Displays role based firewall information

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show role [ldap-stats|wireless-clients]
show role [ldap-stats|wireless-clients] {on <DEVICE-NAME>}
```

**Parameters**

- `show role [ldap-stats|wireless-clients] {on <DEVICE-NAME>}`

| | |
|---|---|
| role ldap-stats | Displays LDAP server status and statistics |
| role wireless-clients | Displays clients associated with roles |
| on <DEVICE-NAME> | The following parameters are common to the 'ldap-stats' and 'wireless-clients' keywords:<br>• on <DEVICE-NAME> – Optional. Displays clients associated with roles on a specified device<br>  • <DEVICE-NAME> – Specify the name of the AP, wireless controller, and service platform. |

**Example**

```
nx9500-6C8809(config)#show role wireless-clients
No ROLE statistics found.
nx9500-6C8809(config)#
```

## 6.1.57 route-maps

*show commands*

Displays route map statistics for defined device routes

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show route-maps {on <DEVICE-NAME>}
```

**Parameters**

- `show route-maps {on <DEVICE-NAME>}`

| | |
|---|---|
| route-maps | Displays configured route map statistics for all defined routes<br>For more information on route maps, see *route-map*. |
| on <DEVICE-NAME> | Optional. Displays route map statistics on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

**Example**

```
nx9500-6C8809(config)#show route-maps
nx9500-6C8809(config)#
```

## 6.1.58 rtls

*show commands*

Displays *Real Time Location Service* (RTLS) statistics for access points contributing locationing information

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show rtls [aeroscout|ekahau|omnitrail] {<MAC/HOSTNAME>} {(on <DEVICE-OR-DOMAIN-NAME>)}
```

**Parameters**

```
• show rtls [aeroscout|ekahau|omnitrail] {<MAC/HOSTNAME>} {(on <DEVICE-OR-DOMAIN-NAME>)}
```

| | |
|---|---|
| rtls | Displays access point RTLS statistics |
| aeroscout | Displays access point Aeroscout statistics |
| ekahau | Displays access point Ekahau statistics |
| omnitrail | Displays access point Omnitrail statistics |
| <MAC/HOSTNAME> | Optional. Displays Aeroscout or Ekahau statistics for a specified access point. Specify the MAC address or hostname of the access point. |
| on <DEVICE-OR-DOMAIN-NAME> | The following keyword is recursive and common to 'Aeroscout' and 'Ekahau' parameters:<br>• on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays Aeroscout or Ekahau statistics on a specified device or domain.<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |

**Example**

```
rfs4000-229D58(config)#show rtls aeroscout

 Aeroscout Engine IP: 0.0.0.0 Port: 0
 Send Count           : 0
 Recv Count           : 0
 Tag Reports          : 0
 Nacks                : 0
 Acks                 : 0
 Lbs                  : 0
 AP Status            : 0
 AP Notif             : 0
 Send Err             : 0
 Errmsg Count         : 0

Total number of APs displayed: 1
rfs4000-229D58(config)#
```

```
ap8533-84A224##show rtls omnitrail
Engine IP: 157.235.90.41
 Control Port: 8890
 Otls 2.4 GHz Engine status: CONNECTED
 Otls 5 GHz Engine status: CONNECTED
 Data Port configured for forwarding 2.4GHz Radio detected beacons: 8888
 Data Port configured for forwarding 5GHz Radio detected beacons:8889
 Heart beats sent for 2.4GHz Port : 1
 Heart beats sent for 5GHz Port : 0
 Beacon tags received on 2.4GHz Radio and forwarded: 6883
 Beacon tags received on 5GHz Radio and forwarded: 0
 Beacon tags received on Sensor Radio (2.4GHz Band) and forwarded: 5187
 Beacon tags received on Sensor Radio (5Ghz Band) and forwarded: 0
Total number of APs displayed: 1
ap8533-84A224#
```

## 6.1.59 running-config

*show commands*

Displays configuration files (where all configured MAC and IP access lists are applied to an interface)

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show running-config {aaa-policy|application|application-group|
application-policy|association-acl-policy|auto-provisioning-policy|
captive-portal-policy|device|database-client-policy|database-policy|device|
device-overrides|dhcp-server-policy|dhcpv6-server-policy|ex3500-management-
policy|ex3500-qos-class-map-policy|ex3500-qos-policy-map|exclude-devices|
firewall-policy|flag-unwritten-changes|guest-management-policy|hide-encrypted-
values|include-factory|interface|ip-access-list|ipv6-access-list|mac-access-
list|management-policy|meshpoint|nsight-policy|profile|radio-qos-policy|
rf-domain|roaming-assist-policy|rtl-server-policy|schedule-policy|smart-rf-
policy|url-filter|url-list|web-filter-policy|wlan|wlan-qos-policy}

show running-config {aaa-policy|application-policy|association-acl-policy|auto-
provisioning-policy|captive-portal-policy|database-client-policy|database-
policy|dhcp-server-policy|dhcpv6-server-policy|ex3500-management-policy|ex3500-
qos-class-map-policy|ex3500-qos-policy-map|guest-management-policy|firewall-
policy|management-policy|nsight-policy|radio-qos-policy|roaming-assist-policy|
rtl-server-policy|schedule-policy|smart-rf-policy|web-filter-policy|wlan-qos-
policy} <POLICY-NAME> {include-factory}

show running-config {flag-unwritten-changes}

show running-config {application <APPLICATION-NAME>|application-group
<APPLICATION-GROUP-NAME>}

show running-config exclude-devices

show running-config {device [<MAC>|self]} {include-factory}

show running-config {device-overrides {brief}}

show running-config {hide-encrypted-values {exclude-devices|include-factory}}

show running-config {include-factory}

show running-config {interface} {<INTERFACE-NAME>|ge|include-factory|me|port-
channel|pppoe1|vlan|wwan1}

show running-config {interface} {<INTERFACE-NAME>|ge <1-4>|include-
factory|me1|port-channel <1-2>|pppoe1|vlan <1-4094>|wwan1} {include-factory}

show running-config {ip-access-list <IP-ACCESS-LIST-NAME>|ipv6-access-list <IPv6-
ACCESS-LIST-NAME>|mac-access-list <MAC-ACCESS-LIST-NAME} {include-factory}

show running-config {meshpoint <MESHPOINT-NAME>} {include-factory}

show running-config {profile [anyap|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|
ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|
ap8533|rfs4000|rfs6000|nx5500|nx75xx|nx9000|nx9600] <PROFILE-NAME>}
{include-factory}
```

```
show running-config {rf-domain <DOMAIN-NAME>} {include-factory}

show running-config {wlan <WLAN-NAME>} {include-factory}

show running-config url-filter <URL-FILTER-NAME>

show running-config url-list <URL-LIST-NAME> {include-factory}
```

**Parameters**

- `show running-config {flag-unwritten-changes}`

| | |
|---|---|
| running-config flag-unwritten-changes | Flags unsaved changes in the *show > running-config* command output. Optionally use the *flag-unwritten-changes* keyword to view changes that have been committed but not saved in the startup configuration. When used, all unsaved changes are marked with a "===" marker, as shown in the following *show > running-config > flag-unwritten-changes* output:<br>`nx9500-6C8809(config)#show running-config flag-unwritten-changes`<br>`!`<br>`! Configuration of NX9500 version 5.9.1.0-017D`<br>`!`<br>`!`<br>`version 2.5`<br>`!`<br>`!`<br>`client-identity-group default`<br>`load default-fingerprints`<br>`!`<br>`client-identity-group test2`<br>`load default-fingerprints`<br>`!`<br>`===alias encrypted-string $WRITE 2 o5gA2zqj/q/REWi8rTa7vQAAAAh4yA1YNBjqTVf4mMBsGA4i`<br>`!`<br>`===alias encrypted-string $enAlias2 2 JI4lPuMaCdMMx7rfBeyIAwAAAAoZ6tR1FfTlFXWvSicTMVZc`<br>`!`<br>`--More--`<br>`nx9500-6C8809(config)#`<br>Execute the *write > memory* command to save these changes. |

- `show running-config {aaa-policy|application-policy|association-acl-policy|auto-provisioning-policy|captive-portal-policy|database-client-policy|database-policy|dhcp-server-policy|dhcpv6-server-policy|ex3500-management-policy|ex3500-qos-class-map-policy|ex3500-qos-policy-map|guest-management-policy|firewall-policy|management-policy|nsight-policy|radio-qos-policy|roaming-assist-policy|rtl-server-policy|schedule-policy|smart-rf-policy|web-filter-policy|wlan-qos-policy} <POLICY-NAME> {include-factory}`

| | |
|---|---|
| running-config | Displays current running configuration<br>Optionally, execute the command along with one of the associated keywords to view the running configuration for that top-level object. For example, to view a policy and its configuration, specify the policy type and provide the policy name.<br>**Note:** If the command is executed without a keyword, the system displays the entire running configuration. |
| <POLICY-TYPE> <POLICY-NAME> | Optional. Select the policy type, for example, aaa-policy, auto-provisioning-policy, captive-portal-policy, etc. and then specify the policy name. The system displays the selected policy's configuration.<br>• <POLICY-NAME> – Specify the name of the policy (should be existing and configured). |

| | |
|---|---|
| include-factory | The following keyword is common to all policies:<br>• include-factory – Optional. Includes factory defaults |

• `show running-config {application <APPLICATION-NAME>|apllication-group <APPLICATION-GROUP-NAME>}`

| | |
|---|---|
| running-config | Displays current running configuration<br>Optionally, execute the command along with one of the associated keywords to view the running configuration for that top-level object. For example, to view a policy and its configuration, specify the policy type and provide the policy name.<br>If the command is executed without a keyword, the system displays the entire running configuration. |
| application <APPLICATION-NAME> | Displays an application's configuration. The application can be system-provided or user-defined.<br>• <APPLICATION-NAME> – Specify the application name (should be existing). |
| application-group <APPLICATION-GROUP-NAME> | Displays an application-group's configuration<br>• <APPLICATION-GROUP-NAME> – Specify the application-group name (should be existing and configured). |

• `show running-config {device [<MAC>|self]} {include-factory}`

| | |
|---|---|
| running-config | Displays current running configuration<br>Optionally, execute the command along with one of the associated keywords to view the running configuration for that top-level object. For example, to view a policy and its configuration, specify the policy type and provide the policy name.<br>If the command is executed without a keyword, the system displays the entire running configuration. |
| device [<MAC>\|self] | Optional. Displays device configuration<br>• <MAC> – Displays a specified device configuration. Specify the MAC address of the device.<br>• self – Displays the logged device's configuration |
| include-factory | The following keyword is common to the '<MAC>' and 'self' parameters:<br>• Optional. Displays factory defaults |

• `show running-config {hide-encrypted-values {exclude-devices|include-factory}}`

| | |
|---|---|
| running-config | Displays current running configuration<br>Optionally, execute the command along with one of the associated keywords to view the running configuration for that top-level object. For example, to view a policy and its configuration, specify the policy type and provide the policy name.<br>If the command is executed without a keyword, the system displays the entire running configuration. |
| hide-encrypted-values {exclude-devices\|include-factory} | Optional. Replaces all encrypted passwords with the standard characters ****** in the *show > running-config* output<br>• exclude-devices – Optional. Excludes devices from the running configuration displayed<br>• include-factory – Optional. Includes factory default values in the running configuration displayed |

- `show running-config {device-overrides {brief}}`

| | |
|---|---|
| running-config | Displays current running configuration |
| device-overrides brief | Optional. Displays overrides applied at the device's configuration<br>• brief – Optional. Displays a brief summary of device overrides |

- `show running-config {exclude-devices}`

| | |
|---|---|
| running-config | Displays current running configuration |
| exclude-devices | Optional. Excludes device configuration details from the running configuration displayed |

- `show running-config {include-factory}`

| | |
|---|---|
| running-config | Displays current running configuration |
| include-factory | Optional. Includes factory defaults |

- `show running-config {interface} {<INTERFACE-NAME>|ge <1-4>|include-factory|me1|port-channel <1-2>|pppoe1|vlan <1-4094>|wwan1} {include-factory}`

| | |
|---|---|
| running-config | Displays current running configuration |
| interface | Optional. Displays interface configuration |
| <INTERFACE-NAME> | Optional. Displays a specified interface configuration. Specify the interface name. |
| ge <1-4> | Optional. Displays GigabitEthernet interface configuration<br>• <1-4> – Specify the GigabitEthernet interface index from 1 - 4. |
| me1 | Optional. Displays FastEthernet interface configuration |
| port-channel <1-2> | Optional. Displays port channel interface configuration<br>• <1-2> – Specify the port channel interface index from 1 - 2. |
| pppoe1 | Optional. Displays PPP over Ethernet interface configuration |
| vlan <1-4094> | Displays VLAN interface configuration<br>• <1-4094> – Specify the VLAN interface number from 1 - 4094. |
| wwan1 | Optional. Displays Wireless WAN interface configuration |
| include-factory | The following keyword is common to all interfaces:<br>• Optional. Includes factory defaults |

- `show running-config {ip-access-list <IP-ACCESS-LIST-NAME>|ipv6-access-list <IPv6-ACCESS-LIST-NAME>|mac-access-list <MAC-ACCESS-LIST-NAME} {include-factory}`

| | |
|---|---|
| running-config | Displays current running configuration<br>Optionally, you can execute the command along with one of the associated keywords to view the running configuration for that top-level object. To view a access-list and its configuration, specify the ACL type and provide the ACL name.<br>**Note:** If the command is executed without a keyword, the system displays the entire running configuration. |
| <ACL-TYPE> <IP/IPv6/MAC-ACL-NAME> | Optional. Select the ACL type, for example, ip-access-list, ipv6-access-list, or mac-access-list, and then specify the ACL name. The system displays the selected ACL's configuration.<br>• <IP/IPv6/MAC-ACL-NAME> – Specify the name of the ACL (should be existing and configured). |

| | |
|---|---|
| include-factory | The following keyword is common to the 'ip-access-list' and 'mac-access-list' parameters:<br>• Optional. Includes factory defaults |

- `show running-config {meshpoint <MESHPOINT-NAME>} {include-factory}`

| | |
|---|---|
| running-config | Displays current running configuration |
| meshpoint <MESHPOINT-NAME> | Optional. Displays meshpoint configuration<br>• <MESHPOINT-NAME> – Specify the meshpoint name |
| include-factory | Optional. Includes factory defaults along with running configuration details |

- `show running-config {profile [anyap|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|rfs6000|nx5500|nx75xx|nx9000|nx9600] <PROFILE-NAME>} {include-factory}`

| | |
|---|---|
| running-config | Displays current running configuration |
| profile <DEVICE-TYPE> <PROFILE-NAME> | Optional. Displays current configuration for a specified profile. Select the device type, and then specify the profile name.<br>• <DEVICE-TYPE> – Select the device type. The options are: AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533, RFS4000, RFS6000, NX5500, NX75XX, NX95XX, NX9600, and VX9000.<br>• <PROFILE-NAME> – Specify the profile name for the selected <DEVICE-TYPE>.<br>**Note:** Select the 'anyap' option to view the running configuration of any type of device. |
| include-factory | Optional. This parameter is common to all profiles. When selected, it includes factory defaults in the output. |

- `show running-config {rf-domain <DOMAIN-NAME>} {include-factory}`

| | |
|---|---|
| running-config | Displays current running configuration |
| rf-domain <DOMAIN-NAME> | Optional. Displays current configuration for a RF Domain<br>• <DOMAIN-NAME> – Displays current configuration for a specified RF Domain. Specify the RF Domain name. |
| include-factory | Optional. Includes factory defaults |

- `show running-config {wlan <WLAN-NAME>} {include-factory}`

| | |
|---|---|
| running-config | Displays current running configuration |
| wlan <WLAN-NAME> | Optional. Displays current configuration for a WLAN<br>• <WLAN-NAME> – Displays current configuration for a specified WLAN. Specify the WLAN name. |
| include-factory | Optional. Includes factory defaults |

- `show running-config url-filter <URL-FILTER-NAME>`

| | |
|---|---|
| running-config | Displays current running configuration |
| url-filter <URL-FILTER-NAME> | Optional. Displays current configuration for the URL filter identified by the <URL-FILTER-NAME> keyword<br>• <URL-FILTER-NAME> – Specify the URL filter's name. |

- `show running-config url-list <URL-LIST-NAME> {include-factory}`

| | |
|---|---|
| running-config | Displays current running configuration |
| url-list <URL-LIST-NAME> | Optional. Displays current configuration for the URL list identified by the <URL-LIST-NAME> keyword<br>• <URL-FILTER-NAME> – Specify the URL list's name. |
| include-factory | Optional. Includes factory defaults |

**Example**

```
rfs6000-81742D#show running-config device self
!
version 2.5
!
!
ip snmp-access-list default
 permit any
!
firewall-policy default
 no ip dos tcp-sequence-past-window
!
!
mint-policy global-default
!
!
management-policy default
 no telnet
 no http server
 https server
 no ftp
 ssh
 user admin password 1
fd07f19c6caf46e5b7963a802d422a708ad39a24906e04667c8642299c8462f1 role superuser
access all
--More--
rfs6000-81742D#

rfs6000-81742D#show running-config profile ap81xx default-ap81xx
profile ap81xx default-ap81xx
 autoinstall configuration
 autoinstall firmware
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 crypto remote-vpn-client
 interface radio1
 interface radio2
 interface radio3
 interface ge1
--More--
rfs6000-81742D#

nx9500-6C8809#show running-config url-filter URL_FILTER_Shopping include-factory

url-filter URL_FILTER_Shopping
 no description
 blacklist category-type p2p precedence 20 description description
 blacklist category-type news-sports-general category shopping precedence 10
description description
 blockpage path internal
 blockpage internal org-name Your Organization Name
```

```
 blockpage internal org-signature Your Organization Name, All Rights Reserved.
 blockpage internal title This URL may have been filtered.
 blockpage internal header The requested URL could not be retrieved.
 blockpage internal footer If you have any questions please contact your IT
department.
 blockpage internal content The site you have attempted to reach may be considered
inappropriate for access.
 no blockpage internal main-logo
 no blockpage internal small-logo
 no blockpage external
nx9500-6C8809#

nx9500-6C8809#show running-config url-list AllowedShopping
url-list AllowedShopping
 url ebay.com depth 10
 url amazon.com depth 10
nx9500-6C8809#

nx9500-6C8809#show running-config application Bing
application Bing
 app-category streaming
 use url-list Bing
nx9500-6C8809#


nx9500-6C8809#sho running-config application-group amazon
application-group amazon
 application amazon_cloud
 application amazon_shop
 application amazon-prime-music
 application amazon-prime-video
nx9500-6C8809#
```

## 6.1.60 session-changes

*show commands*

Displays configuration changes made in the current session

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show session-changes
```

**Parameters**

None

**Example**

```
rfs6000-81742D(config)#show session-changes

No changes in this session

rfs6000-81742D(config)#
```

## 6.1.61 session-config

*show commands*

Lists active open sessions on a device

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show session-config {exclude-devices|include-factory}
```

**Parameters**

- `show session-config {exclude-devices|include-factory}`

| | |
|---|---|
| session-config {exclude-devices\| include-factory} | Displays current session configuration<br>• exclude-devices – Optional. Excludes device configuration details from the output<br>• include-factory – Optional. Includes factory defaults |

**Example**

```
nx9500-6C8809(config)#show session-config
!
! Configuration of NX9500 version 5.9.1.0-017D
!
!
version 2.5
!
!
client-identity-group default
 load default-fingerprints
!
ip access-list BROADCAST-MULTICAST-CONTROL
 permit tcp any any rule-precedence 10 rule-description "permit all TCP traffic"
 permit udp any eq 67 any eq dhcpc rule-precedence 11 rule-description "permit DHCP
replies"
 deny udp any range 137 138 any range 137 138 rule-precedence 20 rule-description
"deny windows netbios"
 deny ip any 224.0.0.0/4 rule-precedence 21 rule-description "deny IP multicast"
 deny ip any host 255.255.255.255 rule-precedence 22 rule-description "deny IP
local broadcast"
 permit ip any any rule-precedence 100 rule-description "permit all IP traffic"
!
mac access-list PERMIT-ARP-AND-IPv4
 permit any any type ip rule-precedence 10 rule-description "permit all IPv4 tra
--More--
nx9500-6C8809(config)#
```

## 6.1.62 sessions

*show commands*

Displays CLI sessions initiated on a device

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show sessions all {on <DEVICE-NAME>}
```

**Parameters**

- `show sessions all {on <DEVICE-NAME>}`

| | |
|---|---|
| sessions | Displays CLI sessions initiated on a device |
| all | Displays all sessions including internal |
| on <DEVICE-NAME> | Optional. This is a recurring keyword and is common to the 'all' parameter. Displays CLI sessions on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

**Example**

```
nx9500-6C8809#show sessions
INDEX   COOKIE  NAME          START TIME            FROM              ROLE
1       2       snmp          2017-06-02 14:31:23   127.0.0.1         superuser
2       3       snmp2         2017-06-02 14:31:23   127.0.0.1         superuser
3       18      admin         2017-06-06 10:38:36   192.168.13.17     superuser

nx9500-6C8809#
```

## 6.1.63 site-config-diff

*show commands*

Displays the difference in site configuration available on the NOC and a site.

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

NOC controllers possess default site configuration details. Overrides applied at the site level result in a mismatch of configuration at the site and the default site configuration available on the NOC controller. Use this command to view this difference.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show site-config-diff <SITE-NAME>
```

**Parameters**

```
• show site-config-diff <SITE-NAME>
```

| | |
|---|---|
| site-config-diff <SITE-NAME> | Displays the configuration difference for the specified site<br>• <SITE-NAME> – Specify the site name. |

**Example**

```
nx9500-6C874D#show site-config-diff 5C-0E-8B-18-06-F4
---- Config diff for switch 5C-0E-8B-18-06-F4 ----
rfs6000 5C-0E-8B-18-06-F4
interface pppoe1
  no shutdown
nx9500-6C874D#
```

## 6.1.64 smart-rf

*show commands*

Displays *Self-Monitoring At Run Time* (Smart RF) statistical history to assess adjustments made to device configurations to compensate for detected coverage holes or device failures

When invoked by an administrator, Smart RF instructs access point radios to change to a specific channel and begin beaconing using the maximum available transmit power. Within a well-planned deployment, any RF Domain member access point radio should be reachable by at least one other radio. Smart RF records signals received from its neighbors as well as signals from external, un-managed radios. AP-to-AP distance is recorded in terms of signal attenuation. The information from external radios is used during channel assignment to minimize interference.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show smart-rf [ap|channel-distribution|history|history-timeline|interfering-ap|
interfering-neighbors|radio]

show smart-rf ap {<MAC>|<DEVICE-NAME>|activity|energy|neighbors|on <DOMAIN-NAME>}

show smart-rf ap {<MAC>|<DEVICE-NAME>} {on <DOMAIN-NAME>}

show smart-rf ap (activity|energy|neighbors} [<MAC>|<DEVICE-NAME>] {(on <DOMAIN-
NAME>)}

show smart-rf [channel-distribution|history|history-timeline] {on <DOMAIN-NAME>}

show smart-rf radio {<MAC>|activity|all-11an|all-11bgn|channel|energy|neighbors|
on <DOMAIN-NAME>}

show smart-rf radio {<MAC>|all-11an|all-11bgn|energy <MAC>} {on <DOMAIN-NAME>}

show smart-rf radio {activity|neigbors} {<MAC>|all-11an|all-11bgn} {on <DOMAIN-
NAME>}

show smart-rf interfering-ap {<MAC>|<DEVICE-NAME>|on <DOMAIN-NAME>}

show smart-rf interfering-neighbors {<MAC>|<DEVICE-NAME>|on <DOMAIN-NAME>|
threshold <50-100>}
```

**Parameters**

- `show smart-rf ap {<MAC>|<DEVICE-NAME>} {on <DOMAIN-NAME>}`

| | |
|---|---|
| smart-rf | Displays Smart RF related information |
| ap | Displays access point related Smart RF information |
| <MAC> | Optional. Uses MAC addresses to identify access points. Displays all access points, if no MAC address is specified. |
| <DEVICE-NAME> | Optional. Uses an administrator defined name to identify an access point |
| on <DOMAIN-NAME> | Optional. Displays access point details on a specified RF Domain<br>• <DOMAIN-NAME> – Specify the domain name. |

- `show smart-rf ap` *`(activity|energy|neighbors} [<MAC>|<DEVICE-NAME>] {(on <DOMAIN-NAME>)}`*

| | |
|---|---|
| smart-rf | Displays Smart RF related information |
| ap | Displays AP related Smart RF information |
| activity | Optional. Displays Smart RF activity related information<br>Use this option to view the following:<br>• Time-period – Lists the frequency Smart RF activity is trended for the RF Domain. Trending periods include the current hour, last 24 hours, or the last seven days. Comparing Smart RF adjustments versus the last seven days enables an administrator to assess whether periods of interference and poor performance were relegated to just specific periods.<br>• Power changes – Displays the number of Smart RF initiated power level changes needed for RF Domain member devices during each of the three trending periods. Determine whether power compensations were relegated to known device outages or if compensations were consistent over the course of a day or week.<br>• Channel changes – Lists the number of Smart RF initiated channel changes needed for RF Domain member devices during each of the three trending periods. Determine if channel adjustments were relegated to known device count increases or decreases over the course of a day or week.<br>• Coverage changes – Displays the number of Smart RF initiated coverage changes needed for RF Domain member devices during each of the three trending periods. Determine if coverage changes were relegated to known device failures or known periods of interference over the course of a day or week. |
| energy | Optional. Displays AP energy for a specified AP or all APs<br>Use this option to view an RF Domain member access point's operating channels, noise level and neighbor count. This information helps assess whether Smart RF neighbor recovery is needed in respect to poorly performing access points. |
| neighbors | Optional. Displays AP neighbors<br>Use this option to view attributes of neighbor radio resources available for Smart RF radio compensations for other RF Domain member device radios. |
| {<MAC>\|<br><DEVICE-NAME>} | The following keywords are common to all of the above parameters:<br>• <MAC> – Displays all of the above mentioned information for a specified AP, identified by its MAC address. Specify the AP's MAC address.<br>• <DEVICE-NAME> – Displays all of the above mentioned information for a specified AP, identified by its hostname. Specify the AP's hostname. |
| on <DOMAIN-NAME> | Optional.Displays access point details on a specified RF Domain<br>• <DOMAIN-NAME> – Specify the domain name. |

- `show smart-rf [channel-distribution|history|history-timeline]` *`{on <DOMAIN-NAME>}`*

| | |
|---|---|
| smart-rf | Displays Smart RF related information |
| channel-distribution | Displays Smart RF channel distribution information. This provides an overview of how RF Domain member devices are utilizing different channels to optimally support connect devices and avoid congestion and interference with neighboring devices. Assess whether the channel spectrum is being effectively utilized and whether channel changes are warranted to improve RF Domain member device performance. |

| | |
|---|---|
| history | Displays Smart RF calibration history<br>Use this option to view description and types of Smart RF events impacting RF Domain member devices. |
| history-timeline | Displays extended Smart RF calibration history on an hourly or daily timeline<br>Use this option to view the time stamp when Smart RF status was updated on behalf of a Smart RF adjustment within the selected RF Domain. |
| on <DOMAIN-NAME> | The following keyword is common to all of the above parameters:<br>• on <DOMAIN-NAME> – Optional. Displays Smart RF configuration, based on the parameters passed, on a specified RF Domain<br>  • on <DOMAIN-NAME> – Specify the RF Domain name. |

- `show smart-rf radio {<MAC>|all-11an|all-11bgn|energy <MAC>} {on <DOMAIN-NAME>}`

| | |
|---|---|
| smart-rf | Displays Smart RF related information |
| radio | Displays radio related commands |
| <MAC> | Optional. Displays details of a specified radio. Specify the radio's MAC address in the AA-BB-CC-DD-EE-FF format. |
| all-11an | Optional. Displays all 11a radios currently in the configuration |
| all-11bgn | Optional. Displays all 11bg radios currently in the configuration |
| energy {<MAC>} | Optional. Displays radio energy<br>• <MAC> – Optional. Specify the radio's MAC address in the AA-BB-CC-DD-EE-FF format.<br>Use this option to view an RF Domain member access point radio's operating channel, noise level and neighbor count. This information helps assess whether Smart RF neighbor recovery is needed in respect to poorly performing radios. |
| on <DOMAIN-NAME> | The following keyword is common to all of the above parameters:<br>• on <DOMAIN-NAME> – Optional. Displays radio details on a specified RF Domain<br>  • <DOMAIN-NAME> – Specify the RF Domain name. |

- `show smart-rf radio {activity|neighbors} {<MAC>|all-11an|all-11bgn} {on <DOMAIN-NAME>}`

| | |
|---|---|
| smart-rf | Displays Smart RF related information |
| radio | Displays Smart RF radio related commands |
| activity | Optional. Displays changes related to radio power, number of radio channels, or coverage holes. Use additional filters to view specific details. |
| <MAC> | Optional. Displays radio activity for a specified radio<br>• <MAC> – Specify the radio's MAC address. |
| all-11an | Optional. Displays radio activity of all 11a radios in the configuration |
| all-11bgn | Optional. Displays radio activity of all 11bg radios in the configuration |
| on <DOMAIN-NAME> | Optional. Displays radio activity of all radios within a specified RF Domain<br>• <DOMAIN-NAME> – Specify the RF Domain name. |

- `show smart-rf interfering-ap {<MAC>|<DEVICE-NAME>|on <DOMAIN-NAME>}`

| | |
|---|---|
| smart-rf | Displays Smart RF related information |
| interfering-ap | Displays interfering access points (requiring potential isolation) information |

| | |
|---|---|
| <MAC> | Optional. Displays information of a specified interfering access point<br>• <MAC> – Specify the access point's MAC address.<br>**Note:** Considers all APs if this parameter is omitted |
| <DEVICE-NAME> | Optional. Displays interfering access point information on a specified device<br>• <DEVICE-NAME> – Specify the device name.<br>**Note:** Considers all APs if this parameter is omitted |
| on <DOMAIN-NAME> | Optional. Displays all interfering access point information within a specified RF Domain<br>• <DOMAIN-NAME> – Specify the RF Domain name. |

- `show smart-rf interfering-neighbors {<MAC>|<DEVICE-NAME>|on <DOMAIN-NAME>| threshold <50-100>}`

| | |
|---|---|
| smart-rf | Displays Smart RF related information |
| interfering-ap | Displays interfering neighboring access point information |
| <MAC> | Optional. Displays interfering neighboring access point information<br>• <MAC> – Specify the access point's MAC address.<br>Considers all APs if this parameter is omitted |
| <DEVICE-NAME> | Optional. Displays all interfering neighboring access point information on a specified device<br>• <DEVICE-NAME> – Specify the device name.<br>Considers all APs if this parameter is omitted |
| threshold <50-100> | Optional. Specifies the maximum attenuation threshold of interfering neighbors.<br>• <50-100> – Specify a value from 50 -100 dB.<br>Attenuation is a measure of the reduction of signal strength during transmission. Attenuation is the opposite of amplification, and is normal when a signal is sent from one point to another. If the signal attenuates too much, it becomes unintelligible. Attenuation is measured in decibels. |
| on <DOMAIN-NAME> | Optional. Displays radio activity of all radios within a specified RF Domain<br>• <DOMAIN-NAME> – Specify the RF Domain name. |

**Example**

```
rfs6000-81742D(config)#show smart-rf calibration-status
No calibration currently in progress
rfs6000-81742D(config)#

rfs6000-81742D(config)#show smart-rf history
-------------------------------------------------------------------------------
-------
      TIME                      EVENT                      DESCRIPTION
-------------------------------------------------------------------------------
-------
-------------------------------------------------------------------------------
-------
Total number of history entries displayed: 0
rfs6000-81742D(config)#
```

## 6.1.65 spanning-tree

*show commands*

Displays spanning tree utilization information

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show spanning-tree mst {configuration|detail|instance|on <DEVICE-NAME>}

show spanning-tree mst {configuration} {(on <DEVICE-NAME>)}

show spanning-tree mst {detail} {interface|on}

show spanning-tree mst {detail} interface {<INTERFACE-NAME>|ge <1-4>|me1|port-channel <1-2>|pppoe1|vlan <1-4094>|wwan1} {(on <DEVICE-NAME>)}

show spanning-tree mst {instance <1-15>} {interface <INTERFACE-NAME>} {(on <DEVICE-NAME>)}
```

**Parameters**

- `show spanning-tree mst {configuration} {(on <DEVICE-NAME>)}`

| | |
|---|---|
| spanning-tree | Displays spanning tree utilization information |
| mst | Displays *Multiple Spanning Tree* (MST) related information |
| configuration {on <DEVICE-NAME>} | Optional. Displays MST configuration<br>• on <DEVICE-NAME> – Optional. Displays MST configuration on a specified device<br>  • <DEVICE-NAME> – Specify the name of the AP or wireless controller.<br>**Note:** If the 'on' keyword is used without any of the other options, the system displays a summary of spanning tree utilization information on the specified device. |

- `show spanning-tree mst {detail} interface {<INTERFACE-NAME>|ge <1-4>|me1|port-channel <1-2>|pppoe1|vlan <1-4094>|wwan1} {(on <DEVICE-NAME>)}`

| | |
|---|---|
| spanning-tree | Displays spanning tree information |
| mst | Displays MST configuration |
| detail | Optional. Displays detailed MST configuration, based on the parameters passed |
| interface [<INTERFACE>\| ge <1-4>\|me1\| port-channel <1-2>\| pppoe1\| vlan <1-4094> wwan1] | Displays detailed MST configuration for a specified interface<br>• <INTERFACE> – Displays detailed MST configuration for a specified interface. Specify the interface name.<br>• ge <1-4> – Displays GigabitEthernet interface MST configuration<br>  • <1-4> – Select the GigabitEthernet interface index from 1 - 4.<br>• me1 – Displays FastEthernet interface MST configuration<br>• port-channel – Displays port channel interface MST configuration<br>  • <1-2> – Select the port channel interface index from 1 - 2.<br>Contd.. |

| | |
|---|---|
| | • pppoe1 – Displays PPP over Ethernet interface MST configuration<br>• vlan – Displays VLAN interface MST configuration<br>• <1-4094> – Select the SVI VLAN ID from 1 - 4094.<br>• wwan1 – Displays Wireless WAN interface MST configuration |
| on <DEVICE-NAME> | The following keyword is common to all interfaces:<br>• on <DEVICE-NAME> – Optional. Displays detailed MST configuration on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

• `show spanning-tree mst {instance <1-15>} {interface <INTERFACE-NAME>} {(on <DEVICE-NAME>)}`

| | |
|---|---|
| spanning-tree | Displays spanning tree information |
| mst | Displays MST configuration. Use additional filters to view specific details. |
| instance <1-15> | Optional. Displays information for a particular MST instance<br>• <1-15> – Specify the instance ID from 1 - 15. |
| interface <INTERFACE-NAME> | Optional. Displays MST configuration for a specific interface instance. The options are:<br>• <INTERFACE-NAME> – Displays MST configuration for a specified interface. Specify the interface name. |
| on <DEVICE-NAME> | Optional. Displays MST configuration on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

**Example**

```
rfs6000-81742D#show spanning-tree mst configuration
%%
%  MSTP Configuration Information for bridge 1 :
%%--------------------------------------------------------
%  Format Id      : 0
%  Name           : My Name
%  Revision Level : 0
%  Digest         : 0xac36177f50283cd4b83821d8ab26de62
%%--------------------------------------------------------

rfs6000-81742D#

rfs6000-81742D#show spanning-tree mst detail interface ge 1
% Bridge up - Spanning Tree Disabled
% CIST Root Path Cost 0  - CIST Root Port 0 - CIST Bridge Priority 32768
% Forward Delay 15 - Hello Time 2 - Max Age 20 - Max hops 20
% 1: CIST Root Id 800000157081742e
% 1: CIST Reg Root Id 800000157081742e
% 1: CIST Bridge Id 800000157081742e
% portfast bpdu-filter disabled
% portfast bpdu-guard disabled
% portfast portfast errdisable timeout disabled
% portfast errdisable timeout interval 300 sec
% cisco interoperability not configured - Current cisco interoperability off

%   ge1: Port 2001 - Id 87d1 - Role Disabled - State Forwarding
%   ge1: Designated External Path Cost 0 - Internal Path Cost 0
%
--More--
rfs6000-81742D#
```

## 6.1.66 startup-config

*show commands*

Displays complete startup configuration script

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show startup-config {include-factory}
```

**Parameters**

- `show startup-config {include-factory}`

| | |
|---|---|
| startup-config include-factory | Displays startup configuration script<br>• include-factory – Optional. Includes factory defaults |

**Example**

```
nx9500-6C8809#show startup-config
!
! Configuration of NX9500 version 5.9.1.0-017D
!
!
version 2.5
!
password-encryption-version 1.0
inline-password-encryption
password-encryption-key secret 2
2cd258b63fa0e16a753394d779cbc5a20000002065d2c29edf373ed42131fa410426d5cb8b0296ff
ea49331cb72e122e421acc9c
!
client-identity-group default
 load default-fingerprints
!
client-identity-group test2
 load default-fingerprints
!
alias network-group $NetGrpAlias address-range 192.168.13.7 to 192.168.13.16
192.168.13.20 to 192.168.13.25
alias network-group $NetGrpAlias network 192.168.13.0/24 192.168.16.0/24
!
alias network $NetworkAlias 192.168.13.0/24
!
--More--
nx9500-6C8809#
```

## 6.1.67 t5

*show commands*

Displays adopted T5 controller statistics

**Supported in the following platforms:**

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX7500, NX7510, NX7510, NX7520, NX9500, NX9510, NX9600, VX9000

**NOTE:** This command is applicable only on WiNG controllers with adopted and managed T5 controllers.

**Syntax**

```
show t5 [boot|clock|cpe|interface|mac|system|temperature|uptime|version|
wireless] {on <T5-DEVICE-NAME>}

show t5 [boot|clock|system|temperature|uptime|version] {on <T5-DEVICE-NAME>}

show t5 cpe [address|boot|ether port status|led|reset|system|uptime|version] {on
<T5-DEVICE-NAME>}

show t5 interface [dsl|fe|ge|radio]

show t5 interface [dsl|fe|ge] [counter|description|errors|status|utilization] {on
<T5-DEVICE-NAME>}

show t5 interface dsl custom [avg|dses|dsses|peak|uses|usses] {on <T5-DEVICE-
NAME>}

show t5 interface radio [stats|status|wlam-map] {on <T5-DEVICE-NAME>}

show t5 mac table [filter name [dsl<1-24>|ge <1-2>|vlan <1-4094>|wlan <1-24>] {on
<T5-DEVICE-NAME>}]

show t5 wireless [client|wlan]

show t5 wireless client {filter name [association-status|authentication-
status|bss|mac-address|retry-percentage|rssi-value]} {on <T5-DEVICE-NAME>}

show t5 wireless wlan counters [qos|rate|size] {on <T5-DEVICE-NAME>}
```

**Parameters**

- `show t5 [boot|clock|system|temperature|uptime|version] {on <T5-DEVICE-NAME>}`

| | |
|---|---|
| t5 | Displays adopted T5 controller statistics |
| boot | Displays the T5 device's boot details. Use this option to view the primary and secondary image files available to use for booting up. |
| clock | Displays the T5 controller's system time, as reported from the controller itself or its remote NTP time resource |
| system | Displays T5 controller's system information, which includes the T5 controller's hostname, MAC address, RF Domain, system clock, uptime |
| temperature | Displays T5 controller's current temperature |
| uptime | Displays the T5 controller's uptime (the time it has been actively deployed and operational) |

| | |
|---|---|
| version | Displays the T5 controller's primary and secondary firmware images |
| on <T5-DEVICE-NAME> | Optional. Executes the command on a specified T5 device<br>• <T5-DEVICE-NAME> – Specify the T5 device's hostname. An error message is displayed if no T5 device name is specified. |

- `show t5 cpe [address|boot|ether port status|led|reset|system|uptime|version] {on <T5-DEVICE-NAME>}`

| | |
|---|---|
| t5 | Displays adopted T5 controller statistics |
| cpe | Displays the T5 controller managed *Customer Premises Equipment* (CPE) statistics based on the parameters passed. Use this command to verify each CPE address credentials and whether currently disconnected or ready for radio coverage area support. |
| address | Displays each linked CPE's current IP address used as its network identifier |
| boot | Displays the primary and secondary firmware versions available to each CPE, along with status of the most recent upgrade operation details |
| ether port status | Displays Ethernet port status |
| led | Displays whether the CPEs currently have their LEDs enabled or disabled. In places like hospitals, its not uncommon for access points to be operational, but their LEDs off as to not disturb patients. |
| reset | Displays the number times a CPE has been reset |
| system | Displays device hardware and SKU information for each CPE. Use this information to assess whether a controller is managing the correct CPE devices out of the total number of CPEs available. |
| uptime | Displays the time each CPE device has been actively deployed and operational |
| version | Displays the application and boot versions utilized by the CPE devices |
| on <T5-DEVICE-NAME> | Optional. Executes the command on a specified T5 device<br>• <T5-DEVICE-NAME> – Specify the T5 device's hostname. An error message is displayed if no T5 device name is specified. |

- `show t5 interface [dsl|fe|ge] [counter|description|errors|status|utilization] {on <T5-DEVICE-NAME>}`

| | |
|---|---|
| t5 | Displays adopted T5 controller statistics |
| interface | Displays T5 interface-related statistics based on the interface selected |
| [dsl\|fe\|ge\|radio] [counter\|description\| errors\|status\| utilization] | Select the interface type. The options are: dsl, fe, ge.<br>• dsl – Displays *Digital Subscriber Line* (DSL) interface related information<br>• fe – Displays *Fast Ethernet* (FE) interface related information<br>• ge – Displays *Gigabit Ethernet* (GE) interface related information<br>The system displays the following information for the DSL, GE, and FE ports:<br>• counter – Displays the following:<br>  • Number of octets (bytes) received and transmitted on this port<br>  • Number of data packets received and transmitted on this port<br>  • Number of flow control (layer 2) packets received and transmitted on this port<br>Contd.. |

| | |
|---|---|
| contd.. | • description – Displays the following:<br>• The selected port's name<br>• The numeric index assignable to each port<br>• The 64 character maximum, unique, administrator-assigned description to each port<br>• errors – Displays the following DSL interface related errors:<br>• The name of the DSL utilized by each T5 controller connected CPE device.<br>• The number of FECs detected in the downstream direction.<br>*Forward Error Correction* (FEC) or channel coding is used for controlling errors over unreliable or noisy communication channels.<br>• The number of CPE DSL coding violations (badly coded packets) detected in the downstream direction.<br>• The number of FECs detected in the upstream direction.<br>• The number of CPE DSL coding violations (badly coded packets) detected in the upstream direction.<br>• status – Displays the following:<br>• The selected port's name<br>• Whether the port is currently up or down as a T5 controller transmit and receive resource<br>• The port's current speed in MB<br>• Whether pause packet utilization is currently off or on for the selected port<br>• Whether each listed port is enabled or disabled by the administrator<br>• utilization – Displays the following:<br>• The selected port's name<br>• The port's receive and transmit data rates (in Kbps)<br>• The packet per second port receive and transmit rates (p/s)<br>• Each port's receive and transmit direction utilization as a percentage of the total transmit bandwidth available. |
| on <T5-DEVICE-NAME> | Optional. Executes the command on a specified T5 device<br>• <T5-DEVICE-NAME> – Specify the T5 device's hostname. An error message is displayed if no T5 device name is specified. |

• `show t5 interface dsl custom [avg|dses|dsses|peak|uses|usses] {on <T5-DEVICE-NAME>}`

| | |
|---|---|
| t5 | Displays adopted T5 controller statistics |
| interface | Displays T5 interface-related statistics based on the interface selected |
| dsl | Selects A T5 controller's DSL interface.<br>A T5 controller uses the operating system to manage its connected radio devices, as opposed to the WiNG operating used by RFS controllers and NX service platforms. However, a T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5's management within a WiNG supported subnet populated by both types of devices. The CPEs are the T5 controller managed radio devices using the operating system. These CPEs use a DSL as their high speed Internet access mechanism using the CPE's physical wallplate connection and phone jack. |

| | |
|---|---|
| custom [avg\|dses\|dsses\|peak\|uses\|usses] | Displays following custom CPE DSL data:<br>• avg – Each DSL's average response time in microseconds<br>• dses – The number of seconds downstream DSL transmissions were negatively impacted by code violations.<br>• dsses – The number of seconds downstream DSL transmissions were severely negatively impacted by code violations.<br>• peak – Each DSL's maximum (best to date since the screen was refreshed) response time in microseconds.<br>• uses – The number of seconds upstream DSL transmissions were negatively impacted by code violations.<br>• usses – The number of seconds upstream DLS transmissions were severely negatively impacted by code violations. |
| on <T5-DEVICE-NAME> | Optional. Executes the command on a specified T5 device<br>• <T5-DEVICE-NAME> – Specify the T5 device's hostname. An error message is displayed if no T5 device name is specified. |

- `show t5 interface radio [stats|status|wlam-map] {on <T5-DEVICE-NAME>}`

| | |
|---|---|
| t5 | Displays adopted T5 controller statistics |
| interface | Displays T5 interface-related statistics based on the interface selected |
| radio [stats\|status\|wlan-map] | Displays following radio interface related information:<br>• stats – Displays T5 radio interface statistics. A T5 controller uses the operating system to manage its connected radio devices, as opposed to the WiNG operating used by RFS controllers and NX service platforms. However, a T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5's management within a WiNG supported subnet populated by both types of devices. The CPEs are the T5 controller managed radio devices using the operating system. Use this option to view the following:<br>• name – The administrator assigned name of each listed CPE radio as its unique identifier<br>• Rx (Kbps) – The listed CPE radio's receive data rate (in Kbps). Use this information to assess RF activity versus other T5 managed CPE radios in the same radio coverage area.<br>• Rx Octets – The number of octets (bytes) received with no errors by the listed T5 controller managed CPE radio.<br>• Rx Packets – The number of data packets received for the listed T5 managed CPE radio since this screen was last refreshed.<br>• Tx (Kbps) – The listed CPE radio's transmit data rate (in Kbps). Use this information to assess RF activity versus other T5 managed CPE radios in the same radio coverage area.<br>• Tx Octets – Displays the number of octets (bytes) transmitted with no errors by the listed T5 controller managed CPE radio.<br>• Tx Packets – The number of data packets transmitted from the listed T5 managed CPE radio since this screen was last refreshed.<br>Contd.. |

| | |
|---|---|
| contd.. | • status – Displays T5 radio interface status information<br>• name – The administrator assigned name of each listed CPE radio as its unique identifier.<br>• Operational status – The radio interface's operational status (enabled/disabled).<br>• mac – The T5 radio interface's MAC address.<br>• transmit power – The T5 radio interface's transmit power.<br>• Channel – The T5 radio interface's channel of operation.<br>• wlan-map – Displays WLAN map membership data for T5 controller managed CPE radio devices. Use this option to view the following:<br>• name – The administrator assigned name of each listed CPE radio as its unique identifier.<br>• status – Whether a CPE radio is currently enabled or disabled as a radio resource for the WLAN(s) the CPE radio has been mapped to.<br>• wlan-radio-mapping – The managed WLAN(s) each listed radio has been mapped to. |
| on <T5-DEVICE-NAME> | Optional. Executes the command on a specified T5 device<br>• <T5-DEVICE-NAME> – Specify the T5 device's hostname. An error message is displayed if no T5 device name is specified. |

- `show t5 mac table [filter name [dsl<1-24>|ge <1-2>|vlan <1-4094>|wlan <1-24>] {on <T5-DEVICE-NAME>}`

| | |
|---|---|
| t5 | Displays adopted T5 controller statistics |
| mac table [dsl<1-24>\|ge <1-2>\| vlan <1-4094>\| wlan <1-24>] | Displays T5 MAC address table. The T5 MAC table displays a dynamic list of MAC addresses learned by the T5 controller over its ethernet interfaces. Use this information to identify devices and the interfaces on which they can be found.<br>Use the following additional filters to filter on the basis of the VLAN or DSL interface:<br>• dsl <1-24> – Filters information on the basis of the selected DSL port<br>• ge <1-2> – Filters information on the basis of the selected GE port<br>• vlan <1-4094 – Filters information on the basis of the selected VLAN port<br>• wlan <1-24> – Filters on the basis of the selected CPE |
| on <T5-DEVICE-NAME> | Optional. Executes the command on a specified T5 device<br>• <T5-DEVICE-NAME> – Specify the T5 device's hostname. An error message is displayed if no T5 device name is specified. |

- `show t5 wireless client {filter name [association-status|authentication-status|bss|mac-address|retry-percentage|rssi-value]} {on <T5-DEVICE-NAME>}`

| | |
|---|---|
| t5 | Displays adopted T5 controller statistics |
| wireless client | Displays the T5 wireless client and WLAN related statistics<br>• client – Displays read-only device information for wireless clients associated with the selected T5 controller and its connected CPE device radios. Use this information to assess if configuration changes are required to improve client performance.<br>Use the additional filters available to view specific client-related information. The options are:<br>• association-status<br>Contd.. |

| | |
|---|---|
| | • authentication-status<br>• bss<br>• retry-percentage<br>• rssi-value |
| on <T5-DEVICE-NAME> | Optional. Executes the command on a specified T5 device<br>• <T5-DEVICE-NAME> – Specify the T5 device's hostname. An error message is displayed if no T5 device name is specified. |

- `show t5 wireless wlan counters [qos|rate|size] {on <T5-DEVICE-NAME>}`

| | |
|---|---|
| t5 | Displays adopted T5 controller statistics |
| wireless wlan [qos\|rate\|size] | Displays the T5 wireless WLAN related statistics<br>• wlan – Displays following T5 controller traffic counter statistics:<br>• qos – T5 controller WLAN QoS utilization. Displays the number of background (low priority) and best-effort packets received and transmitted on each listed T5 controller managed WLANs<br>• rates – Displays T5 controller's WLAN utilization data rate statistics<br>• Lists the number of data packets received and transmitted in the WLAN that have been relegated to a 1 Mbps data rate<br>• Lists the number of data packets received and transmitted in the WLAN by T5 controller connected devices at 54Mbps<br>• size – Displays the number of data packets received and transmitted, in each listed WLAN, greater than 1024 bytes |
| on <T5-DEVICE-NAME> | Optional. Executes the command on a specified T5 device<br>• <T5-DEVICE-NAME> – Specify the T5 device's hostname. An error message is displayed if no T5 device name is specified. |

**Example**

The following examples are for show commands executed on the 't5-ED7C6C' controller adopted by the 'nx9500-6C8809' wireless controller:

```
nx9500-6C8809(config)#show t5 boot on t5-ED7C6C
Primary Version:  5.4.2.0-010R
Secondary Version:  5.4.2.0-006B
Next Boot: Primary
Upgrade Status: none
Upgrade Progress %:  0
nx9500-6C8809(config)#

nx9500-6C8809(config)#show t5 version on t5-ED7C6C
Bootloader Version:   5.4.2.0-010R
Application Version:  5.4.2.0-010R
nx9500-6C8809(config)#
```

```
nx9500-6C8809(config)#show t5 system on t5-ED7C6C
Serial Number           14213522400004
SKU                     TS-0524-WR
Hardware Rev            5
Mac Address             B4-C7-99-ED-7C-6C
Description             24-port PowerBroadband VDSL2 Switch Version 5.4.2.0-010R
Contact                 NULL
Name                    t5-ED7C6C
Location                NULL
nx9500-6C8809(config)#

nx9500-6C8809(config)#show t5 clock on t5-ED7C6C
Time 6-6-2017 17:14:30 UTC
nx9500-6C8809(config)#

nx9500-6C8809(config)#show t5 interface ge counter on t5-ED7C6C
-------------------------------------------------------------------------------
-----------------------------------
 INTERFACE RECEIVE OCTETS RECEIVE PACKETS RECEIVE PAUSE PKTS TRANSMIT OCTETS
TRANSMIT PACKETS TRANSMIT PAUSE PKTS
-------------------------------------------------------------------------------
-----------------------------------
 ge1     711128918    89636040       0             2558110037    133720283
0
 ge2     2515775064   133311355      0             3422167586    78735853
0
-------------------------------------------------------------------------------
-----------------------------------
nx9500-6C8809(config)#

nx9500-6C8809(config)#show t5 uptime on t5-ED7C6C
Up Time 0 days 1 day, 3:19:43
nx9500-6C8809(config)#

nx9500-6C8809(config)#show t5 temperature on t5-ED7C6C
============ Temperature  ============
-----------------------------------------------------------------------
 INDEX CURRENT (C) FANS @ FULL SPEED (C) FANS @ VARIABLE SPEED (C)
-----------------------------------------------------------------------
 1      39          70                    60
-----------------------------------------------------------------------
nx9500-6C8809(config)#

nx9500-6C8809(config)#show t5 cpe address on t5-ED7C6C
-------------------------------------------------------------------------------
DEVICE             STATUS             IP ADDRESS                MAC ADDRESS
-------------------------------------------------------------------------------
 cpe1              ready              192.168.13.32             00-C0-23-69-80-CD
 cpe2              ready              192.168.13.33             74-6F-F7-40-16-62
 cpe3              disconnected       0.0.0.0                   00-00-00-00-00-00
 cpe4              disconnected       0.0.0.0                   00-00-00-00-00-00
 cpe5              disconnected       0.0.0.0                   00-00-00-00-00-00

--More--
nx9500-6C8809(config)#
```

```
nx9500-6C8809(config)#show t5 cpe led on t5-ED7C6C
-------------------------------------------------------------------------------
-------
 DEVICE                                  LED STATUS
-------------------------------------------------------------------------------
---
 cpe1                                   enable
 cpe2                                   enable
 cpe3                                   enable
 cpe4                                   enable
 cpe5                                   enable
--More--
nx9500-6C8809(config)#

nx9500-6C8809(config)#show t5 mac table filter name vlan 1 on t5-ED7C6C
-------------------------------------------------------------------------------
-------
       T5-MAC       VLAN         ADDRESS            INTERFACE               VENDOR
-------------------------------------------------------------------------------
-------
 B4-C7-99-ED-7C-6C   1           00-02-B3-28-D1-55   ge1               Intel Corp
 B4-C7-99-ED-7C-6C   1           00-1E-67-4B-BF-BD   ge1               Intel Corp
 B4-C7-99-ED-7C-6C   1            00-23-68-11-E6-C4   ge1                Extreme
Tech
 B4-C7-99-ED-7C-6C   1            00-23-68-88-0D-A7   ge1                Extreme
Tech
 B4-C7-99-ED-7C-6C   1            00-23-68-99-BB-7C   ge1                Extreme
Tech
 B4-C7-99-ED-7C-6C   1            00-A0-F8-68-D5-70   ge1                Extreme
Tech
 B4-C7-99-ED-7C-6C   1           00-C0-23-69-80-CD   dsl1               00-C0-23
 B4-C7-99-ED-7C-6C   1              1C-7E-E5-18-FA-67     ge1                  D-
Link Corp
 B4-C7-99-ED-7C-6C   1             3C-CE-73-F4-47-83    ge1                Cisco
Systems
 B4-C7-99-ED-7C-6C   1            74-6F-F7-40-16-62    dsl2               Wistron
Corp
--More--
nx9500-6C8809(config)#
```

## 6.1.68 terminal

*show commands*

Displays terminal configuration parameters

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show terminal
```

**Parameters**

None

**Example**

```
rfs6000-81742D(config)#show terminal
Terminal Type: xterm
Length: 24     Width: 200
rfs6000-81742D(config)#
```

## 6.1.69 timezone

*show commands*

Displays a device's timezone

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show timezone
```

**Parameters**

None

**Example**

```
rfs6000-81742D(config)#show timezone
Timezone is America/Los_Angeles
rfs6000-81742D(config)#
```

## 6.1.70 traffic-shape

*show commands*

Displays traffic-shaping related configuration details and statistics

Traffic shaping regulates network data transfers to ensure a specific performance level. Traffic shaping delays the flow of packets defined as less important than prioritized traffic streams. Traffic shaping enables traffic control out an interface to match its flow to the speed of a remote target's interface and ensure traffic conforms applied policies. Traffic can be shaped to meet downstream requirements and eliminate network congestion when data rates are in conflict.

Apply traffic shaping to specific applications to apply application categories. When application and ACL rules are conflicting, ACL rules take precedence for the traffic shaping class. Using traffic shaping, an application takes precedence over an application category.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530

**Syntax**

```
show traffic-shape [priority-map|statistics {class <1-4>}|status] {on <DEVICE-NAME>}
```

**Parameters**

```
• show traffic-shape [priority-map|statistics {class <1-4>}|status] {on <DEVICE-NAME>}
```

| | |
|---|---|
| traffic-shape | Displays traffic-shaping related configuration details and statistics |
| priority-map | Displays the traffic shaper queue priority. There are 8 queues (0 - 7), and traffic is queued in each based on incoming packets 802.1p markings. |
| statistics class <1-4> | Displays traffic-shaping related statistics for all traffic shaper classes or for a selected class<br>• class <1-4> – Optional. Specify the traffic class from 1 - 4. The system displays traffic shaping statistics for the selected class. If not selected, the system statistics for all classes. |
| status | Displays the controller or service platform's traffic shaping status (whether running or not) |
| on <DEVICE-NAME> | Optional. Displays traffic-shaping related configuration details and statistics on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

**Example**

```
ap7532-DEB9B0#show traffic-shape priority-map
----------------------------------------
  DOT1P-PRIORITY    TX-SHAPER-PRIORITY
----------------------------------------
 0                 2
 1                 0
 2                 1
 3                 3
 4                 4
 5                 5
 6                 6
 7                 7
----------------------------------------
ap7532-DEB9B0#

ap7532-DEB9B0#show traffic-shape status
State of Traffic shaper:  running
ap7532-DEB9B0#

ap7532-DEB9B0#show traffic-shape statistics

Traffic shaper class : 1
Class 1 is not configured:

Traffic shaper class : 3
Class 3 is not configured:

Traffic shaper class : 2
Rate: 1500 Kbps
--------------------------------------------------------------------------------
-------
 PRIORITY  PKTS-SENT  PKTS-DELAYED PKTS-DROPPED CURRENT-QUEUE-LEN  CURRENT-
LATENCY(IN USECS)
--------------------------------------------------------------------------------
-------
  1        0           0            0            0                0
  0        0           0            0            0                0
  3        0           0            0            0                0
  2        152153035   151924251    1508343      11               33447
  5        0           0            0            0                0
  4        0           0            0            0                0
  7        0           0            0            0                0
  6        0           0            0            0                0
--------------------------------------------------------------------------------
-------

Traffic shaper class : 4
Class 4 is not configured:
ap7532-DEB9B0#
```

## 6.1.71 upgrade-status

*show commands*

Displays the last image upgrade status

**NOTE:** This command is not available in the USER EXEC Mode.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show upgrade-status {detail|on}
show upgrade-status {detail} {(on <DEVICE-NAME>)}
```

**Parameters**

- `show upgrade-status {detail} {(on <DEVICE-NAME>)}`

| | |
|---|---|
| upgrade-status | Displays last image upgrade status and log |
| detail | Optional. Displays last image upgrade status in detail |
| on <DEVICE-NAME> | The following keyword is recursive and common to the 'detail' parameter:<br>• on <DEVICE-NAME> – Optional. Displays last image upgrade status on a specified device<br>  • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.<br>**Note:** If the 'on' keyword is used without the 'detail' keyword, the system displays a summary of upgrade status and log on the specified device. |

**Example**

```
nx9500-6C8809#show upgrade-status
Last Image Upgrade Status :In_Progress(17 percent completed)
Last Image Upgrade Time   : 2017-02-11 12:26:29
nx9500-6C8809#

nx9500-6C8809#show upgrade-status detail
Last Image Upgrade Status : Successful
Last Image Upgrade Time   : 2017-06-02 14:22:51
-----------------------------------------------
Running from partition /dev/sda8
var2 is 1 percent full
/tmp is 4 percent full
Free Memory 33357504 kB
FWU invoked via Linux shell
Validating image file header
Removing other partition
Tue May 30 10:43:36 IST 2017
debug: cmdline -C /boot/lilo.conf -R 5.9.0.0-028B -P fix
LILO version 22.6-CCB, Copyright (C) 1992-1998 Werner Almesberger


--More--
nx9500-6C8809#
```

## 6.1.72 version

*show commands*

Displays a device's software and hardware version

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show version {on <DEVICE-NAME>}
```

**Parameters**

- `show version {on <DEVICE-NAME>}`

| | |
|---|---|
| version {on <DEVICE-NAME>} | Displays software and hardware versions on all devices or a specified device<br>• on <DEVICE-NAME> – Optional. Displays software and hardware versions on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

**Example**

```
nx9500-6C8809#show version
NX9500 version 5.9.0.0-029R
Copyright (c) 2004-2017 Extreme Networks, Inc. All rights reserved.
Booted from primary

nx9500-6C8809 uptime is 3 days, 20 hours 49 minutes
CPU is Intel(R) Xeon(R) CPU           E5645  @ 2.40GHz, No. of CPUs 24
Base ethernet MAC address is B4-C7-99-6C-88-09
System serial number is B4C7996C8809
Model number is NX-9500-100R0-WR

nx9500-6C8809#
```

## 6.1.73 vrrp

*show commands*

Displays the following *Virtual Router Redundancy Protocol* (VRRP) related statistics: configuration error, router redundancy information in brief and detail. VRRP configuration errors include mismatch of authentication credentials, invalid packet checksums, invalid packet types, invalid virtual route IDs, TTL errors, packet length errors and invalid (non matching) VRRP versions.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show vrrp [brief|details|error-stats|stats]
show vrrp [brief|details|stats] {<1-255>} {(on <DEVICE-NAME>)}
show vrrp error-stats {on <DEVICE-NAME>}
```

**Parameters**

- `show vrrp [brief|details|stats] {<1-255>} {(on <DEVICE-NAME>)}`

| | |
|---|---|
| vrrp | Displays VRRP related statistics in brief or in detail depending on the option selected |
| brief | Displays virtual router information in brief |
| details | Displays virtual router information in detail |
| stats | Displays virtual router statistics |
| <1-255> | The following keyword is common to all of the above parameters:<br>• <1-255> – Optional. Displays information for a specified Virtual Router. Specify the router's ID from 1 - 255. |
| on <DEVICE-NAME> | The following keyword is recursive and common to the '<1-255>' parameter:<br>• on <DEVICE-NAME> – Optional. Displays specified router information on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `show vrrp error-stats {on <DEVICE-NAME>}`

| | |
|---|---|
| vrrp | Displays VRRP related statistics in brief or in detail depending on the option selected |
| error-stats {on <DEVICE-NAME>} | Displays global error statistics<br>• on <DEVICE-NAME> – Optional. Displays global error statistics on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

**Example**

```
rfs6000-81742D(config)#show vrrp error-stats
Last protocol error reason: none
IP TTL errors: 0
Version mismatch: 0
Packet Length error: 0
Checksum error: 0
Invalid virtual router id: 0
Authentication mismatch: 0
Invalid packet type: 0
rfs6000-81742D(config)#

rfs6000-81742D(config)#show vrrp details
VRRP Group 1:
  version 2
  interface none
  configured priority 1
  advertisement interval 1 sec
  preempt enable, preempt-delay 0
  virtual mac address 00-00-5E-00-01-01
  sync group disable
rfs6000-81742D(config)#
```

## 6.1.74 web-filter

*show commands*

Displays Web filtering related information

Use this command to view information on Web requests for content and whether the requests were blocked or approved based on URL filter settings defined for the selected controller or service platform. A URL filter is comprised of several filter rules. A whitelist bans all sites except the categories and URL lists defined in the whitelist. The blacklist allows all sites except the categories and URL lists defined in the blacklist.

**Supported in the following platforms:**

- Access Points — AP6522, AP6532, AP7161, AP7502, AP7522, AP7532, AP7562, AP8132
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show web-filter [category|category-type|config|filter-level [basic|high|low|
medium|medium-high]|statistics {on <DEVICE-NAME>}|status]
```

**Parameters**

```
• show web-filter [category|category-type|config|filter-level [basic|high|low|
medium|medium-high]|statistics {on <DEVICE-NAME>}|status]
```

| | |
|---|---|
| web-filter | Displays an existing and configured Web filter details |
| category | Displays Web filter categories. A category is a pre-defined URL list available in the WiNG software. |
| category-type | Displays the Web filter category types. This is a pre-configured list of categories and sub-categories in to which commonly accessed URLs have been classified. |
| config | Displays all existing Web filters and their configuration details |
| filter-level [basic\|high\|low\|medium\|medium-high] | Displays category types for the selected filter-level. Each filter level is pre-configured to use a set of category types. You cannot change the categories in the category types used for these pre-configured filter-level setting. Nor can you add, modify, or remove the category types mapped to a filter-level setting.The options are:<br>• basic – Displays all category types configured for the basic filter-level<br>• high – Displays all category types configured for the high filter-level<br>• low – Displays all category types configured for the low filter-level<br>• medium – Displays all category types configured for the medium filter-level<br>• medium-high – Displays all category types configured for the medium-high filter-level |
| statistics {on <DEVICE-NAME>} | Displays Web filter statistics on a specified device<br>• on <DEVICE-NAME> – Optional. Specifies the device name<br>  • <DEVICE-NAME> – Specify the name of the AP, controller, or service platform.<br>**Note:** Web filtering is a licensed feature, and only when enforced can the system display Web filtering statistics. |

| | |
|---|---|
| status {on <DEVICE-NAME>} | Displays Web filter status on a specified device<br>• on <DEVICE-NAME> – Optional. Specifies the device name<br>• <DEVICE-NAME> – Specify the name of the AP, controller, or service platform.<br>**Note:** Web filtering is a licensed feature, and only when enforced can the system display Web filtering status. |

**Example**

```
nx9500-6C8809(config)#show web-filter category
    advertisement-popups
        Sites that provide advertising graphics or other ad content
        files such as banners and pop-ups.
    alcohol-tobacco
        Sites that promote or sell alcohol- or tobacco-related
        products or services.
    anonymizers
        Sites and proxies that act as an intermediary for surfing to
        other websites in an anonymous fashion, whether to
        circumvent web filtering or for other reasons.
    arts
        Sites with artistic content or relating to artistic
        institutions such as theaters, museums, galleries, dance
        companies, photography, and digital graphic resources.
    botnets
        Sites that use bots (zombies) including command-and-control
        sites.
--More--
nx9500-6C8809(config)#

nx9500-6C8809(config)#show web-filter config
URL filters configured for this device are:
    WebFilter_ShoppingSites
        Blacklisted categories:
            shopping,
        Whitelisted categories:
            <AllowedShopping>,
nx9500-6C8809(config)#
```

## 6.1.75 what

*show commands*

Displays details of a specified search phrase (performs global search)

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show what [contain|is] <WORD> {on <DEVICE-OR-DOMAIN-NAME>}
```

**Parameters**

- `show what [contain|is] <WORD> {on <DEVICE-OR-DOMAIN-NAME>}`

| | |
|---|---|
| contain <WORD> | Searches on all the items that contain a specified word<br>• <WORD> – Specify a word to search (for example, MAC address, hostname, etc.). |
| is <WORD> | Searches on an exact match<br>• <WORD> – Specify a word to search (for example, MAC address, hostname, etc.). |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Performs global search on a specified device or RF Domain<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |

**Example**

```
rfs4000-229D58#show what contain default
-------------------------------------------------------------------------------
-------------------------------------------------------------------
NO. CATEGORY            MATCHED                      OTHER KEY INFO (1)
OTHER KEY INFO (2)             OTHER KEY INFO (3)
                     NAME/VALUE                  NAME/VALUE                  NAME/
VALUE                     NAME/VALUE
-------------------------------------------------------------------------------
-------------------------------------------------------------------

               https-trustpoint         type                mac
rf_domain_name
1  device-cfg         default-trustpoint          rfs4000                    00-
23-68-22-9D-58             default

              __obj_name__           name
2 firewall_policy  default           default

                __obj_name__            name                https
idle_session_timeout
3 management_policy  default              default             True
30

               qos_policy             name                control_vlan
beacon_format

--More--
rfs4000-229D58#
```

## 6.1.76 wireless

*show commands*

Displays wireless configuration parameters

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show wireless [ap|bridge|client|coverage-hole-incidents|meshpoint|mint|mobility-
database|radio|regulatory|rf-domain|sensor-server|unsanctioned|wips|wlan]

show wireless ap {configured|detail|load-balancing|on <DEVICE-NAME>}

show wireless ap {configured}

show wireless ap {detail} {<MAC/HOST-NAME>} {(on <DEVICE-OR-DOMAIN-NAME>)}

show wireless ap {load-balancing} {client-capability|events|neighbors} {(on
<DEVICE-NAME>)}

show wireless bridge {candidate-ap|certificate|config|hosts|on|statistics}

show wireless bridge {candidate-ap} {<MAC/HOSTNAME> {<1-3>}} {(filter radio-mac
<RADIO-MAC>)} {(on <DEVICE-OR-DOMAIN-NAME>)}

show wireless bridge {certificate} status {on <DEVICE-NAME>}

show wireless bridge {config}

show wireless bridge {hosts} {on <DEVICE-OR-DOMAIN-NAME>}

show wireless bridge {statistics} {rf|traffic} {(on <DEVICE-OR-DOMAIN-NAME>)}

show wireless client {association-history|detail|filter|include-ipv6|on <DEVICE-
OR-DOMAIN-NAME>|statistics|tspec}

show wireless client {association-history <MAC>} {on <DEVICE-OR-DOMAIN-NAME>}

show wireless client {detail <MAC>} {(on <DEVICE-OR-DOMAIN-NAME>)}

show wireless client {filter [ip|on|state|wlan]}

show wireless client {filter} {ip [<IP>|not <IP>]} {on <DEVICE-OR-DOMAIN-NAME>}

show wireless client {filter} {on <DEVICE-OR-DOMAIN-NAME>}

show wireless client {filter} {state [data-ready|not [data-ready|roaming]|
roaming]} {on <DEVICE-OR-DOMAIN-NAME>}

show wireless client {filter} {wlan [<WLAN-NAME>|not <WLAN-NAME>]} {on <DEVICE-OR-
DOMAIN-NAME>}

show wireless client {include-ipv6} {detail|on|filter}

show wireless client {include-ipv6} {detail <MAC>} {(on <DEVICE-OR-DOMAIN-NAME>)}
show wireless client {include-ipv6} {filter {ip|ipv6|state|wlan}}

show wireless client {statistics} {detail|on|rf|window-data}
```

```
show wireless client {statistics} {detail <MAC>|rf|window-data <MAC>} {(on
<DEVICE-OR-DOMAIN-NAME>)}

show wireless client {tspec <MAC>} {(on <DEVICE-OR-DOMAIN-NAME>)}

show wireless coverage-hole-incidents [detail|on|summary]

show wireless coverage-hole-incidents detail {filter [ap <MAC/HOSTNAME>|client-mac
<MAC>]|summary} {(on <DOMAIN-NAME>)}]

show wireless meshpoint {config|detail|multicast|neighbor|on|path|proxy|root|
security|statistics|tree|usage-mappings}

show wireless meshpoint {config} {filter [device <DEVICE-NAME>|rf-domain <DOMAIN-
NAME>]}

show wireless meshpoint {detail} {<MESHPOINT-NAME>}

show wireless meshpoint {on <DEVICE-OR-DOMAIN-NAME>}
show wireless meshpoint {multicast|path|proxy|root|security|statistics}
[<MESHPOINT-NAME>|detail] {on <DEVICE-OR-DOMAIN-NAME>}

show wireless meshpoint neighbor [<MESHPOINT-NAME>|detail|statistics {rf}] {on
<DEVICE-OR-DOMAIN-NAME>}
show wireless meshpoint {tree} {on <DEVICE-OR-DOMAIN-NAME>}


show wireless meshpoint {usage-mappings}

show wireless mobility-database {on <DEVICE-NAME>}

show wireless mint [client|detail|links|portal]

show wireless [client|detail] {on|portal-candidates {<DEVICE-NAME>|filter <RADIO-
MAC>}|statistics} (<DEVICE-OR-DOMAIN-NAME>)

show wireless mint links {on <DEVICE-OR-DOMAIN-NAME>}

show wireless mint portal statistics {on <DEVICE-OR-DOMAIN-NAME>}

show wireless radio {detail|on <DEVICE-OR-DOMAIN-NAME>|statistics|tspec|wlan-map}
show wireless radio {detail} {<DEVICE-NAME>|filter|on <DEVICE-OR-DOMAIN-NAME>}

show wireless radio {detail} {<DEVICE-NAME> {<1-3>|filter|on}}

show wireless radio {detail} {filter <RADIO-MAC>} {(on <DEVICE-OR-DOMAIN-NAME>)}

show wireless radio {statistics} {detail|on|rf|windows-data}

show wireless radio {statistics} {on <DEVICE-OR-DOMAIN-NAME>|rf {on <DEVICE-OR-
DOMAIN-NAME>}}

show wireless radio {statistics} {detail|window-data} {<DEVICE-NAME>} {<1-
3>|filter <RADIO-MAC>} {(on <DEVICE-OR-DOMAIN-NAME>)}

show wireless radio {tspec} {<DEVICE-NAME>|filter|on <DEVICE-OR-DOMAIN-
NAME>|option}

show wireless radio {wlan-map} {on <DEVICE-OR-DOMAIN-NAME>}

show wireless regulatory [channel-info <WORD>|country-code <WORD>|device-type]
show wireless regulatory device-type [ap6521|ap6522|ap6532|ap6562|ap7131|ap7161|
ap7181|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap8132|
ap8163|ap82xx|ap8432|ap8533|rfs4000] <WORD>

show wireless rf-domain statistics {detail} {(on <DEVICE-OR-DOMAIN-NAME>)}
```

```
show wireless sensor-server {on <DEVICE-OR-DOMAIN-NAME>}

show wireless unsanctioned aps {detail|statistics} {(on <DEVICE-OR-DOMAIN-NAME>)}

show wireless wips [client-blacklist|event-history] {on <DEVICE-OR-DOMAIN-NAME>}

show wireless wlan {config|detail <WLAN>|on <DEVICE-OR-DOMAIN-NAME>|policy-
mappings|statistics|usage-mappings}

show wireless wlan {detail <WLAN>|on <DEVICE-OR-DOMAIN-NAME>|policy-
mappings|usage-mappings}

show wireless {config filter {device <DEVICE-NAME>|rf-domain <DOMAIN-NAME>}}

show wireless wlan statistics {<WLAN>|detail|traffic} {on <DEVICE-OR-DOMAIN-NAME>}
```

**Parameters**

- `show wireless ap {configured}`

| | |
|---|---|
| wireless | Displays wireless configuration parameters |
| ap | Displays managed access point information |
| configured | Optional. Displays configured AP information, such as name, MAC address, profile, RF Domain, and adoption status |

- `show wireless ap {detail} {<MAC/HOST-NAME>} {(on <DEVICE-OR-DOMAIN-NAME>)}`

| | |
|---|---|
| wireless | Displays wireless configuration parameters |
| ap | Displays managed access point information |
| detail <MAC/HOST-NAME> | Optional. Displays detailed information for all APs or a specified AP<br>• <MAC/HOST-NAME> – Optional. Displays information for a specified AP. Specify the AP's MAC address. |
| on <DEVICE-OR-DOMAIN-NAME> | The following keyword is recursive and common to the 'detail <MAC/HOST-NAME>' parameter:<br>• on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays information on a specified device or RF Domain<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |

- `show wireless ap {load-balancing} {client-capability|events|neighbors} {(on <DEVICE-NAME)}`

| | |
|---|---|
| wireless | Displays wireless configuration parameters |
| ap | Displays managed access point information |
| load-balancing {client-capability\| events\|neighbors} | Optional. Displays load balancing status. Use additional filters to view specific details.<br>• client-capability – Optional. Displays client band capability<br>• events – Optional. Displays client events<br>• neighbors – Optional. Displays neighboring clients |
| on <DEVICE-NAME> | The following keyword is recursive and common to the 'client-capability', 'events', and 'neighbors' parameters:<br>• on <DEVICE-NAME> – Optional. Displays load balancing information, based on the parameters passed, on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `show wireless bridge {candidate-ap} {<MAC/HOSTNAME> {<1-3>}} {(filter radio-mac <RADIO-MAC>)} {(on <DEVICE-OR-DOMAIN-NAME>)}`

| | |
|---|---|
| wireless | Displays wireless configuration statistics |
| bridge candidate-ap | Optional. Displays information about the candidate infrastructure access points as well as the infrastructure access point that the client-bridge radio has selected<br>**Note:** When enabled, the client-bridge radio scans its defined channels to locate the best candidate access point servicing the infrastructure WLAN. |
| <MAC/HOSTNAME> <1-3> | Optional. Specify the client-bridge access point's hostname or MAC address. Optionally append the radio interface's number to form client-bridge in the form of AA-BB-CC-DD-EE-FF:RX or HOSTNAME:RX.<br>• <1-3> – Optional. Radio interface index if not specified as part of mesh ID. |
| filter radio-mac <RADIO-MAC> | This is a recursive parameter and common to all of the above options.<br>• filter radio-mac – Optional. Provides additional filters to specifically identify the radio by its MAC address<br>• <RADIO-MAC> – Specify the radio's MAC address. |
| on <DEVICE-OR-DOMAIN-NAME> | This is a recursive parameter and common to all of the above options.<br>• on <DEVICE-OR-DOMAIN-NAME> – Optional. Executes the command on a specified device or devices within a specified RF Domain<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the AP, controller, service platform, or RF Domain name. |

- `show wireless bridge {certificate} status {on <DEVICE-NAME>}`

| | |
|---|---|
| wireless | Displays wireless configuration statistics |
| bridge certificate status | Optional. Displays all client bridges in configuration and the status of their PKCS#12 certificates |
| on <DEVICE-NAME> | Optional. Executes the command on a specified device<br>• <DEVICE-NAME> – Specify the AP, controller, service platform name. |

- `show wireless bridge {config}`

| | |
|---|---|
| wireless | Displays wireless configuration statistics |
| bridge config | Optional. Displays all client bridges in configuration<br>The output displays the configured client-bridges' hostname, MAC address, profile, RF Domain, SSID, band, encryption, authentication, and EAP username. |

- `show wireless bridge {hosts} {on <DEVICE-OR-DOMAIN-NAME>}`

| | |
|---|---|
| wireless | Displays wireless configuration statistics |
| bridge hosts | Optional. Displays the client bridge host information<br>The output displays the configured client-bridges' host's MAC Address, bridge MAC address, IPv4 address, bridging status, and activity<br>**Note:** The HOST MAC column displays real MAC addresses of wired hosts, while the BRIDGE MAC column displays the translated MAC addresses. The BRIDGE MAC column is based on the radio 2 base MAC address and increments by 1 for each wired host connected to the client bridges Ge1 port. |

| | |
|---|---|
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Executes the command on a specified device or devices within a specified RF Domain<br>• <DEVICE-OR-DOMAIN-NAME> – Optional. Specify the AP, controller, service platform, or Domain name. |

- `show wireless bridge {statistics} {rf|traffic} {(on <DEVICE-OR-DOMAIN-NAME>)}`

| | |
|---|---|
| wireless | Displays wireless configuration statistics |
| bridge statistics | Optional. Displays the client-bridge related statistics |
| rf | Optional. Displays the client-bridge related RF statistics<br>The output displays the signal, noise, SNR, TX/RX rates, retries, and errors. |
| traffic | Optional. Displays the client-bridge related traffic statistics<br>The output displays TX/RX bytes, TX/RX packets, TX/RX bits/second, and dropped packets. |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Executes the command on a specified device or devices within a specified RF Domain<br>• on <DEVICE-OR-DOMAIN-NAME> – Optional. Specify the AP, controller, service platform, or Domain name. |

- `show wireless client {association-history <MAC>} {on <DEVICE-OR-DOMAIN-NAME>}`

| | |
|---|---|
| wireless | Displays wireless configuration parameters |
| client | Displays client information based on the parameters passed |
| association-history <MAC> | Optional. Displays association history for a specified client<br>• <MAC> – Specify the MAC address of the client. |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Displays association history on a specified device or RF Domain<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |

- `show wireless client {detail <MAC>} {(on <DEVICE-OR-DOMAIN-NAME>)}`

| | |
|---|---|
| wireless | Displays wireless configuration parameters |
| client | Displays client information based on the parameters passed |
| detail <MAC> | Optional. Displays detailed wireless client(s) information<br>• <MAC> – Optional. Displays detailed information for a specified wireless client. Specify the MAC address of the client. |
| on <DEVICE-OR-DOMAIN-NAME> | The following keyword is recursive and common to the 'detail <MAC>' parameter:<br>• on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays detailed information on a specified device or RF Domain<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |

- `show wireless client {filter ip [<IP>|not <IP>]} {on <DEVICE-OR-DOMAIN-NAME>}`

| | |
|---|---|
| wireless | Displays wireless configuration parameters |
| client | Displays client information based on the parameters passed |

| | |
|---|---|
| filter IP [<IP>\|not <IP>] | Optional. Uses IP addresses to filter wireless clients<br>• <IP> – Selects clients with IP address matching the <IP> parameter<br>• not <IP> – Inverts the match selection |
| on <DEVICE-OR-DOMAIN-NAME> | The following keyword is common to the 'IP' and 'not IP' parameters:<br>• on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays selected wireless client information on a specified device or RF Domain<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |

- `show wireless client {filter} {state [data-ready|not [data-ready|roaming]|roaming]} {on <DEVICE-OR-DOMAIN-NAME>}`

| | |
|---|---|
| wireless | Displays wireless configuration parameters |
| client | Displays client information based on the parameters passed |
| filter state [data-ready\| not [data-ready\| roaming]\| roaming] | Optional. Filters clients based on their state<br>• data-ready – Selects wireless clients in the data-ready state<br>• not [data-ready\|roaming] – Inverts match selection. Selects wireless clients neither ready nor roaming<br>• Roaming – Selects roaming clients |
| on <DEVICE-OR-DOMAIN-NAME> | The following keyword is common to the 'ready', 'not', and 'roaming' parameters:<br>• on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays selected client details on a specified device or RF Domain<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |

- `show wireless client {filter} {wlan [<WLAN-NAME>|not <WLAN-NAME>]} {on <DEVICE-OR-DOMAIN-NAME>}`

| | |
|---|---|
| wireless | Displays wireless configuration parameters |
| client | Displays client information based on the parameters passed |
| filter wlan [<WLAN-NAME>\| not <WLAN-NAME>] | Optional. Filters clients on a specified WLAN<br>• <WLAN-NAME> – Specify the WLAN name.<br>• not <WLAN-NAME> – Inverts the match selection |
| on <DEVICE-OR-DOMAIN-NAME> | The following keyword is common to the 'WLAN and 'not' parameters:<br>• on <DEVICE-OR-DOMAIN-NAME> – Optional. Filters clients on a specified device or RF Domain<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |

- `show wireless client {statistics} {detail <MAC>|rf|window-data <MAC>} {(on <DEVICE-OR-DOMAIN-NAME>)}`

| | |
|---|---|
| wireless | Displays wireless configuration parameters |
| client | Displays client information based on the parameters passed |

| | |
|---|---|
| statistics {detail <MAC>\|rf\| window-data <MAC>} | Optional. Displays detailed client statistics. Use additional filters to view specific details.<br>• detail <MAC> – Optional. Displays detailed client statistics<br>• <MAC> – Optional. Displays detailed statistics for a specified client. Specify the client's MAC address.<br>• rf – Optional. Displays detailed client statistics on a specified device or RF Domain<br>• window-data <MAC> – Optional. Displays historical data, for a specified client<br>• <MAC> – Optional. Specify the client's MAC address |
| on <DEVICE-OR-DOMAIN-NAME> | The following keyword is recursive and common to the 'detail <MAC>', 'RF', and 'window-data <MAC>' parameters:<br>• on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays client statistics, based on the parameters passed, on a specified device or RF Domain<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |

- `show wireless client` *`{tspec} {<MAC>} {(on <DEVICE-OR-DOMAIN-NAME>)}`*

| | |
|---|---|
| wireless | Displays wireless configuration parameters |
| client | Displays client information based on the parameters passed |
| tspec <MAC> | Optional. Displays detailed *traffic specification* (TSPEC) information for all clients or a specified client<br>• <MAC> – Optional. Displays detailed TSPEC information for a specified client. Specify the MAC address of the client. |
| on <DEVICE-OR-DOMAIN-NAME> | The following keyword is recursive and common to the 'tspec <MAC>' parameter:<br>• on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays detailed TSPEC information for wireless clients on a specified device or RF Domain<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |

- `show wireless client` *`{include-ipv6} {detail <MAC>} {(on <DEVICE-OR-DOMAIN-NAME>)}`*

| | |
|---|---|
| wireless | Displays wireless configuration parameters |
| client | Displays client information based on the parameters passed |
| include-ipv6 | Includes IPv6 address (if known) of wireless clients |
| detail <MAC> | Optional. Displays detailed wireless client(s) information<br>• <MAC> – Optional. Displays detailed information for a specified wireless client. Specify the MAC address of the client. |
| on <DEVICE-OR-DOMAIN-NAME> | The following keyword is recursive and common to the 'detail <MAC>' parameter:<br>• on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays detailed information on a specified device or RF Domain<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |

- `show wireless client` *`{include-ipv6} {filter {ip|ipv6|state|wlan}}`*

| | |
|---|---|
| wireless | Displays wireless configuration parameters |
| client | Displays wireless client information based on the parameters passed |

| | |
|---|---|
| include-ipv6 {filter} | Optional. Includes IPv6 address (if known) of wireless clients<br>• filter – Optional. Defines additional filters. Use one of the following options to filter clients: ip, ipv6, state, and wlan<br>By default the system only displays the IPv4 address of clients. The include-ipv6 parameter includes the known IPv6 address of each client. |
| ip [<IPv4>\|not <IPv4>] | Optional. Displays wireless client information based on the IPv4 address passed<br>• <IPv4> – Displays information of the client identified by the <IPv4> parameter<br>• not <IPv4> – Inverts the match selection |
| ipv6 [<IPv6>\|<br>not <Pv6>] | Optional. Displays wireless client information based on the IPv6 address passed<br>• <IPv6> – Displays information of the client identified by the <IPv6> parameter<br>• not <IPv6> – Inverts the match selection |
| filter state [data-ready\|<br>not [data-ready\|<br>roaming]\|roaming] | Optional. Filters wireless client information based on their state<br>• data-ready – Displays information of wireless clients in the data-ready state<br>• not [data-ready\|roaming] – Inverts match selection. Displays information of wireless clients neither ready nor roaming<br>• Roaming – Displays information of roaming clients |
| wlan [<WLAN-NAME>\|<br>not <WLAN-NAME>] | Optional. Displays wireless client information based on the WLAN name passed<br>• <WLAN-NAME> – Specify the WLAN name.<br>• not <WLAN-NAME> – Inverts match selection |

- `show wireless coverage-hole-incidents` *`{detail} {filter [ap <MAC/HOSTNAME>|client-mac <MAC>]|summary} {(on <DOMAIN-NAME>)}`*

| | |
|---|---|
| wireless | Displays wireless configuration parameters. Use this option to view coverage-hole related incidents encountered by wireless clients and reported to associated access points. |
| coverage-hole-incidents | Displays coverage-hole related statistics |
| detail filters<br>[ap <MAC/HOSTNAME>\|<br>client-mac <MAC>] | Optional. Displays detailed coverage-hole related statistics<br>• filters – Optional. Displays detailed coverage-hole related statistics on a per access point or wireless-client basis<br>  • ap <MAC/HOSTNAME> – Displays detailed coverage-hole related statistics for a specified access point<br>  • <MAC/HOSTNAME> – Specify the access point's device name or MAC address.<br>  • client-mac <MAC> – Displays detailed coverage-hole related statistics encountered by a specified wireless client<br>  • <MAC> – Specify the wireless client's MAC address<br>**Note:** If the command is executed without any parameters being included, the system displays all coverage-hole related statistics. |
| summary | Optional. Displays a summary of coverage-hole related statistics |
| on <DOMAIN-NAME> | This parameter is recursive and is common to the 'detail' and 'summary' keywords:<br>• on <DOMAIN-NAME> – Optional. Displays detailed or summary coverage-hole related statistics on a specified RF Domain<br>  • <DOMAIN-NAME> – Specify the domain name. |

- `show wireless meshpoint {config} {filter [device <DEVICE-NAME>|rf-domain <DOMAIN-NAME>]}`

| | |
|---|---|
| wireless | Displays wireless configuration parameters. Use this option to view detailed statistics on each Mesh-capable client available within controller's adopted access point's radio coverage area.<br>A mesh network is where one where each node is able to communicate with other nodes and maintain more then one path to the other mesh nodes within the mesh network. A mesh network provides robust, reliable and redundant connectivity to all the members of the mesh network. When one member of the mesh network becomes unavailable, the other mesh nodes are still able to communicate with one another either directly or indirectly through intermediate nodes. |
| meshpoint | Displays meshpoint related information |
| config | Optional. Displays all meshpoint configuration |
| filters [device <DEVICE-NAME>\|rf-domain <DOMAIN-NAME>] | Optional. Provides additional filter options, such as device name and RF Domain name.<br>• device <DEVICE-NAME> – Displays meshpoints applied to a specified device<br>  • <DEVICE-NAME> – Specify the device name.<br>• rf-domain – <DOMAIN-NAME> – Displays meshpoints applied to a specified RF Domain<br>  • <DOMAIN-NAME> – Specify the domain name. |

- `show wireless meshpoint {detail} {<MESHPOINT-NAME>}`

| | |
|---|---|
| wireless | Displays wireless configuration parameters |
| meshpoint | Displays meshpoint related information. Use this option to view detailed statistics on each Mesh-capable client available within controller's adopted access point's radio coverage area.<br>A mesh network is where one where each node is able to communicate with other nodes and maintain more then one path to the other mesh nodes within the mesh network. A mesh network provides robust, reliable and redundant connectivity to all the members of the mesh network. When one member of the mesh network becomes unavailable, the other mesh nodes are still able to communicate with one another either directly or indirectly through intermediate nodes. |
| detail <MESHPOINT-NAME> | Optional. Displays detailed information for all meshpoints or a specified meshpoint<br>• <MESHPOINT-NAME> – Optional. Displays detailed information for a specified meshpoint. Specify the meshpoint name. |

- `show wireless meshpoint {multicast|path|proxy|root|security|statistics} [<MESHPOINT-NAME>|detail] {on <DEVICE-OR-DOMAIN-NAME>}`

| | |
|---|---|
| wireless | Displays wireless configuration parameters |

| | |
|---|---|
| meshpoint | Displays meshpoint related information. Use this option to view detailed statistics on each Mesh-capable client available within controller's adopted access point's radio coverage area.<br>A mesh network is where one where each node is able to communicate with other nodes and maintain more then one path to the other mesh nodes within the mesh network. A mesh network provides robust, reliable and redundant connectivity to all the members of the mesh network. When one member of the mesh network becomes unavailable, the other mesh nodes are still able to communicate with one another either directly or indirectly through intermediate nodes. |
| multicast | Optional. Displays meshpoint multicast information |
| path | Optional. Displays meshpoint path information |
| proxy | Optional. Displays meshpoint proxy information |
| root | Optional. Displays meshpoint root information |
| security | Optional. Displays meshpoint security information |
| statistics | Optional. Displays meshpoint statistics |
| [<MESHPOINT-NAME>\| detail] | The following keywords are common to all of the above parameters:<br>• <MESHPOINT-NAME> – Displays meshpoint related information for a specified meshpoint. Specify the meshpoint name.<br>• detail – Displays detailed multicast information for all meshpoints |
| on <DEVICE-OR-DOMAIN-NAME> | The following keyword is common to all of the above parameters:<br>• on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays detailed multicast information on a specified device or RF Domain.<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |

- `show wireless meshpoint` *`{neighbor}`* `[<MESHPOINT-NAME>|detail|statistics` *`{rf}`*`]` *`{on <DEVICE-OR-DOMAIN-NAME>}`*

| | |
|---|---|
| wireless | Displays wireless configuration parameters |
| meshpoint | Displays meshpoint related information. Use this option to view detailed statistics on each Mesh-capable client available within controller's adopted access point's radio coverage area.<br>A mesh network is where one where each node is able to communicate with other nodes and maintain more then one path to the other mesh nodes within the mesh network. A mesh network provides robust, reliable and redundant connectivity to all the members of the mesh network. When one member of the mesh network becomes unavailable, the other mesh nodes are still able to communicate with one another either directly or indirectly through intermediate nodes. |
| neighbor | Optional. Displays meshpoint neighbor information, based on the parameters passed |
| [<MESHPOINT-NAME>\|detail\| statistics {rf}] | Select one of the following parameter to view neighbor related information<br>• <MESHPOINT-NAME> – Displays detailed multicast information for a specified meshpoint. Specify the meshpoint name.<br>• detail – Displays detailed multicast information for all meshpoints<br>• statistics – Displays neighbors related statistics<br>• rf – Optional. Displays RF related statistics for neighbors |

| | |
|---|---|
| on <DEVICE-OR-DOMAIN-NAME> | The following keyword is common to all of the above parameters:<br>• on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays meshpoint neighbor information, based on the parameters passed, on a specified device or RF Domain.<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |

- `show wireless meshpoint {tree} {on <DEVICE-OR-DOMAIN-NAME>}`

| | |
|---|---|
| wireless | Displays wireless configuration parameters |
| meshpoint | Displays meshpoint related information<br>**Note:** The *show > wireless > meshpoint > tree* command can be executed only from a wireless controller. |
| tree | Optional. Displays meshpoint network tree |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Displays meshpoint network tree on a specified device or RF Domain<br>• <DEVICE-OR-DOMAIN-NAME> – Optional. Specify the name of AP, wireless controller, service platform, or RF Domain |

- `show wireless meshpoint {usage-mappings|on <DEVICE-OR-DOMAIN-NAME>}`

| | |
|---|---|
| wireless | Displays wireless configuration parameters |
| meshpoint | Displays meshpoint related information |
| usage-mappings | Optional. Lists all devices and profiles using the meshpoint |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Displays meshpoint applied to a specified device or RF Domain<br>• <DEVICE-OR-DOMAIN-NAME> – Optional. Specify the name of AP, wireless controller,service platform, or RF Domain |

- `show wireless mobility-database {on <DEVICE-NAME>}`

| | |
|---|---|
| wireless | Displays wireless configuration parameters |
| mobility-database | Displays controller-assisted mobility database |
| on <DEVICE-OR-DOMAIN-NAME> | The following keyword is recursive and common to the 'filter <RADIO-MAC>' parameter:<br>• on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays detailed radio operation status for all or a specified radio on a specified device or RF Domain.<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |

- `show wireless mint [client|detail] {portal-candidates {<DEVICE-NAME>|filter <RADIO-MAC>}|statistics} (on <DEVICE-OR-DOMAIN-NAME>)`

| | |
|---|---|
| wireless mint [client\|detail] | Displays radio MiNT-mesh related statistics<br>• client – Displays MiNT-mesh client related information. Use the 'client' option to view detailed statistics on each Mesh capable client available within the selected access point's radio coverage area.<br>• detail – Displays detailed MiNT-mesh related information |
| portal-candidates | Displays detailed information about portal candidates for a MiNT-mesh. Mesh points connected to an external network and forwarding traffic in and out are Mesh portals. Mesh points must find paths to a portal to access the Internet. When multiple portals exist, the mesh point must select one.<br>Use the additional filter option to view specific portal candidate details. |

| | |
|---|---|
| statistics | This option is common to the 'client' and 'detail' keyword.<br>Displays MiNT-mesh client statistical data |
| on <DEVICE-OR-DOMAIN-NAME> | This option is common to the 'client' and 'detail' keyword.<br>Displays MiNT-mesh client related information on a specific device or RF Domain<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the access point, controller, or RF Domain name. |

- `how wireless mint portal statistics` *`{on <DEVICE-OR-DOMAIN-NAME>}`*

| | |
|---|---|
| wireless mint | Displays radio MiNT-mesh related statistics |
| links | Displays MiNT-mesh links related information. MiNT Links are automatically created between controllers and access points during adoption using MLCP (*MiNT Link Creation Protocol*). They can also be manually created between a controller and access point (or) between access points. MiNT links are manually created between controllers while configuring a cluster.<br>Level 2 (or) remote MiNT links are controller aware links, and requires IP network for communication. This level 2 MiNT links at access points are intended for remote adaptive AP deployment and management from NOC. With Level2 MiNT links, access points are only aware of the controllers and not about other access points. Level 2 MiNT links also provide partitioning, between access points deployed at various remote sites. |
| on <DEVICE-OR-DOMAIN-NAME> | Displays MiNT-mesh links on a specific device or RF Domain<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the access point, controller, or RF Domain name. |

- `show wireless mint portal statistics` *`{on <DEVICE-OR-DOMAIN-NAME>}`*

| | |
|---|---|
| wireless mint | Displays radio MiNT-mesh related statistics |
| portal | Displays legacy client on MiNT-mesh portal |
| on <DEVICE-OR-DOMAIN-NAME> | Displays legacy client on MiNT-mesh portal on a specific device or RF Domain<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the access point, controller, or RF Domain name. |

- `show wireless radio` *`{detail} {<DEVICE-NAME> {<1-3>|filter|on}}`*

| | |
|---|---|
| wireless | Displays wireless configuration parameters |
| radio | Displays radio operation status and other related information. Use this option to view radio association data, including radio ID, connected APs, radio type, quality index and *Signal to Noise Ratio* (SNR). This data is reported to the managing controller or service platform from connected access point radios and should be refreshed periodically.<br>A radio's RF Mode displays as:<br>• 2.4GHz-wlan – If it is configured to provide 2.4 GHz WLAN service<br>• 5GHz-wlan – If it is configured to provide 5.0 GHz WLAN service<br>• bridge – If it is configured to provide client-bridge operation |
| detail | Optional. Displays detailed radio operation status |
| <DEVICE-NAME> | Optional. Displays detailed information for a specified radio. Specify the MAC address or hostname, or append the interface number to form the radio ID in the AA-BB-CC-DD-EE-FF:RX or HOSTNAME:RX format. |

| | |
|---|---|
| <1-3> | Optional. Specify the radio interface index from 1 - 3 (if not specified as part of the radio ID) |
| filter <RADIO-MAC> | Optional. Provides additional filters<br>• <RADIO-MAC> – Optional. Filters based on the radio MAC address |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. After specifying the radio MAC address, further refine the search by specifying a device or RF Domain.<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |

- `show wireless radio {detail} {filter <RADIO-MAC>} {(on <DEVICE-OR-DOMAIN-NAME>)}`

| | |
|---|---|
| wireless | Displays wireless configuration parameters |
| radio | Displays radio operation status and other related information. Use this option to view radio association data, including radio ID, connected APs, radio type, quality index and *Signal to Noise Ratio* (SNR). This data is reported to the managing controller or service platform from connected access point radios and should be refreshed periodically.<br>A radio's RF Mode displays as:<br>• 2.4GHz-wlan – If it is configured to provide 2.4 GHz WLAN service<br>• 5GHz-wlan – If it is configured to provide 5.0 GHz WLAN service<br>• bridge – If it is configured to provide client-bridge operation |
| detail | Optional. Displays detailed radio operation status |
| filter <RADIO-MAC> | Optional. Provides additional filter options<br>• <RADIO-MAC> – Uses MAC address to filter radios |
| on <DEVICE-OR-DOMAIN-NAME> | The following keyword is recursive and common to the 'filter <RADIO-MAC>' parameter:<br>• on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays detailed radio operation status for all or a specified radio on a specified device or RF Domain.<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |

- `show wireless radio {statistics} {on <DEVICE-OR-DOMAIN-NAME>|rf {on <DEVICE-OR-DOMAIN-NAME>}}`

| | |
|---|---|
| wireless | Displays wireless configuration parameters |
| radio | Displays radio operation status and other related information. Use this option to view radio association data, including radio ID, connected APs, radio type, quality index and SNR. This data is reported to the managing controller or service platform from connected access point radios and should be refreshed periodically.<br>A radio's RF Mode displays as:<br>• 2.4GHz-wlan – If it is configured to provide 2.4 GHz WLAN service<br>• 5GHz-wlan – If it is configured to provide 5.0 GHz WLAN service<br>• bridge – If it is configured to provide client-bridge operation |
| statistics | Optional. Displays radio traffic and RF statistics |

| | |
|---|---|
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Displays traffic and RF related statistics on a specified device or RF Domain<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |
| rf {on <DEVICE-OR-DOMAIN-NAME>} | Optional. Displays RF statistics on a specified device or RF Domain<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |

- `show wireless radio {statistics} {detail|window-data} {<DEVICE-NAME>} {<1-3>| filter <RADIO-MAC>} {(on <DEVICE-OR-DOMAIN-NAME>)}`

| | |
|---|---|
| wireless | Displays wireless configuration parameters |
| radio | Displays radio operation status and other related information. Use this option to view radio association data, including radio ID, connected APs, radio type, quality index and SNR. This data is reported to the managing controller or service platform from connected access point radios and should be refreshed periodically.<br>A radio's RF Mode displays as:<br>• 2.4GHz-wlan – If it is configured to provide 2.4 GHz WLAN service<br>• 5GHz-wlan – If it is configured to provide 5.0 GHz WLAN service<br>• bridge – If it is configured to provide client-bridge operation |
| statistics {detail\|window-data} | Optional. Displays radio traffic and RF statistics. Use additional filters to view specific details. The options are: are:<br>• detail – Displays detailed traffic and RF statistics of all radios<br>• window-data – Displays historical data over a time window |
| <DEVICE-NAME> | The following keywords are common to the 'detail' and 'window-data' parameters:<br>• <DEVICE-NAME> – Optional. Specify the MAC address or hostname, or append the interface number to form the radio ID in the AA-BB-CC-DD-EE-FF:RX or HOSTNAME:RX format. |
| <1-3> | Optional. Specify the radio interface index from 1- 3, if not specified as part of the radio ID using the preceding parameter. |
| filter <RADIO-MAC> | Optional. Provides additional filters<br>• <RADIO-MAC> – Optional. Filters based on the radio MAC address |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. After specifying the radio MAC address, further refine the search by specifying a device or RF Domain.<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |

- `show wireless radio {tspec} {<DEVICE-NAME>|filter|on <DEVICE-OR-DOMAIN-NAME>| option}`

| | |
|---|---|
| wireless | Displays wireless configuration parameters |

| | |
|---|---|
| radio | Displays radio operation status and other related information. Use this option to view radio association data, including radio ID, connected APs, radio type, quality index and *Signal to Noise Ratio* (SNR). This data is reported to the managing controller or service platform from connected access point radios and should be refreshed periodically.<br>A radio's RF Mode displays as:<br>• 2.4GHz-wlan – If it is configured to provide 2.4 GHz WLAN service<br>• 5GHz-wlan – If it is configured to provide 5.0 GHz WLAN service<br>• bridge – If it is configured to provide client-bridge operation |
| tspec | Optional.Displays TSPEC information on a radio |
| <DEVICE-NAME> | Optional. Specify the MAC address or hostname, or append the interface number to form the radio ID in the AA-BB-CC-DD-EE-FF:RX or HOSTNAME:RX format. |
| filter | Optional. Provides additional filters<br>• <RADIO-MAC> – Optional. Filters based on the radio MAC address |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. After specifying the radio MAC address, further refine the search by specifying a device or RF Domain.<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |

- `show wireless regulatory [channel-info <WORD>|county-code <WORD>]`

| | |
|---|---|
| wireless | Displays wireless configuration parameters |
| regulatory | Displays wireless regulatory information |
| channel-info <WORD> | Displays channel information<br>• <WORD> – Specify the channel number. |
| country-code <WORD> | Displays country code to country name information<br>• <WORD> – Specify the two letter ISO-3166 country code. |

- `show wireless regulatory device-type [ap6521|ap6522|ap6532|ap6562|ap7131|ap7161|ap7181|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap8132|ap8163|ap82xx|ap8432|ap8533|rfs4000] <WORD>`

| | |
|---|---|
| wireless | Displays wireless configuration parameters |
| regulatory | Displays wireless regulatory information |
| device-type <DEVICE-TYPE> <WORD> | Displays wireless regulatory information based on the device type selected. Select the device type. The options are:<br>AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8132, AP8163, AP8232, AP8432, AP8533 and RFS4000.<br>After specifying the device type, specify the country code.<br>• <WORD> – Specify the two letter ISO-3166 country code. |

- `show wireless rf-domain statistics` *`{detail} {(on <DEVICE-OR-DOMAIN-NAME>)}`*

| | |
|---|---|
| wireless | Displays wireless configuration parameters |
| rf-domain statistics | Displays RF Domain statistics |
| details | Optional. Displays detailed RF Domain statistics |

| | |
|---|---|
| on <DEVICE-OR-DOMAIN-NAME> | The following keyword is recursive and common to the 'detail' parameter:<br>• on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays RF Domain statistics on a specified device or RF Domain<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |

- `show wireless sensor-server` *`{on <DEVICE-OR-DOMAIN-NAME>}`*

| | |
|---|---|
| wireless | Displays wireless configuration parameters |
| sensor- server {on <DEVICE-OR-DOMAIN-NAME>} | Displays AirDefense sensor server configuration details<br>• on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays AirDefense sensor server configuration on a specified device or RF Domain |

- `show wireless unsanctioned aps` *`{detailed|statistics} {(on <DEVICE-OR-DOMAIN-NAME>)}`*

| | |
|---|---|
| wireless | Displays wireless configuration parameters |
| unsanctioned aps | Displays unauthorized APs. Use additional filters to view specific details. |
| detailed | Optional. Displays detailed unauthorized APs information |
| statistics | Optional. Displays channel statistics |
| on <DEVICE-OR-DOMAIN-NAME> | The following keyword is common to the 'detailed' and 'statistics' parameters:<br>• on <DEVICE-OR-DOMAIN-NAME> – Optional. Specify the name of the AP, wireless controller, service platform, or RF Domain.<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |

- `show wireless wips [client-blacklist|event-history]` *`{on <DEVICE-OR-DOMAIN-NAME>}`*

| | |
|---|---|
| wireless | Displays wireless configuration parameters |
| wips [client-blacklist\|event-history] | Displays the WIPS details<br>• client-blacklist – Displays blacklisted clients<br>• event-history – Displays event history |
| on <DEVICE-OR-DOMAIN-NAME> | The following keyword is common to the 'client-blacklist' and 'event-history' parameters:<br>• on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays the WIPS details on a specified device or RF Domain.<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |

- `show wlan` *`{detail <WLAN>|on <DEVICE-OR-DOMAIN-NAME>|policy-mappings|usage-mappings}`*

| | |
|---|---|
| wireless | Displays wireless configuration parameters |
| wlan | Displays WLAN related information based on the parameters passed |
| detail <WLAN> | Optional. Displays WLAN configuration<br>• <WLAN> – Specify the WLAN name. |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Displays WLAN configuration on a specified device or RF Domain<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |

| | |
|---|---|
| policy-mappings | Optional. Displays WLAN policy mappings |
| usage-mappings | Optional. Lists all devices and profiles using the WLAN |

- `show wlan {config filter {device <DEVICE-NAME>|rf-domain <DOMAIN-NAME>}`

| | |
|---|---|
| wireless | Displays wireless configuration parameters |
| wlan | Displays WLAN related information based on the parameters passed |
| config filter | Optional. Filters WLAN information based on the device name or RF Domain |
| device <DEVICE-NAME> | Optional. Filters WLAN information based on the device name<br>• <DEVICE-NAME> – Specify the device name. |
| rf-domain <DOMAIN-NAME> | Optional. Filters WLAN information based on the RF Domain<br>• <DOMAIN-NAME> – Specify the RF Domain name. |

- `show wlan {statistics {<WLAN>|detail} {(on <DEVICE-OR-DOMAIN-NAME>)}`

| | |
|---|---|
| wireless | Displays wireless configuration parameters |
| wlan | Displays WLAN related information based on the parameters passed |
| statistics {<WLAN>\|detail} | Optional. Displays WLAN statistics. Use additional filters to view specific details<br>• <WLAN> – Optional. Displays WLAN statistics. Specify the WLAN name.<br>• detail – Optional. Displays detailed WLAN statistics |
| on <DEVICE-OR-DOMAIN-NAME> | The following keyword is common to the 'WLAN' and 'detail' parameters:<br>• on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays WLAN statistics on a specified device or RF Domain<br>• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |

**Usage Guidelines**

The customize command enables you to customize the *show > wireless* command output.

```
rfs6000-81742D(config)#customize ?
  cdp-lldp-info-column-width                Customize cdp-lldp-info
                                            column width
  hostname-column-width                     Customize hostname column width
  show-adoption-offline                     Customize the output of (show
                                            adoption offline) command
  show-adoption-status                      Customize the output of (show
                                            adoption status) command
  show-wireless-bridge                      Customize the output of (show
                                            wireless bridge) command
  show-wireless-bridge-hosts                Customize the output of (show
                                            wireless bridge hosts)
                                            command
  show-wireless-bridge-stats                Customize the output of (show
                                            wireless bridge stats)
                                            command
  show-wireless-bridge-stats-rf             Customize the output of (show
                                            wireless bridge stats rf)
                                            command
  show-wireless-bridge-stats-traffic        Customize the output of (show
                                            wireless bridge stats)
                                            command
  show-wireless-client                      Customize the output of (show
                                            wireless client) command
  show-wireless-client-stats                Customize the output of (show
                                            wireless client stats) command
  show-wireless-client-stats-rf             Customize the output of (show
```

```
                                                    wireless client stats rf)
  show-wireless-legacy-mesh-client-stats            Customize the output of (show
                                                    wireless mint client stats)
                                                    command
  show-wireless-meshpoint                           Customize the output of (show
                                                    wireless meshpoint) command
  show-wireless-meshpoint-accelerated-multicast     Customize the output of (show
                                                    wireless meshpoint
                                                    accelerated-multicast)
                                                    command
  show-wireless-meshpoint-neighbor-stats            Customize the output of (show
                                                    wireless meshpoint neighbor
                                                    stats) command
  show-wireless-meshpoint-neighbor-stats-rf         Customize the output of (show
                                                   wireless meshpoint neighbor stats
                                                    rf) command
  show-wireless-mint-client                         Customize the output of (show
                                                    wireless mint client)
  show-wireless-mint-client-stats                   Customize the output of (show
                                                    wireless mint client stats)
                                                    command
  show-wireless-mint-client-stats-rf                Customize the output of (show
                                                    wireless mint client stats
                                                    rf) command
  show-wireless-mint-portal                         Customize the output of (show
                                                    wireless mint portal)
  show-wireless-mint-portal-stats                   Customize the output of (show
                                                    wireless mint portal stats)
                                                    command
  show-wireless-mint-portal-stats-rf                Customize the output of (show
                                                    wireless mint portal stats
                                                    rf) command
  show-wireless-radio                               Customize the output of (show
                                                    wireless radio) command
  show-wireless-radio-stats                         Customize the output of (show
                                                    wireless radio stats) command
  show-wireless-radio-stats-rf                      Customize the output of (show
                                                    wireless radio stats rf) command
rfs6000-81742D(config)#
```

The default setting for the *show > wireless > client* command is as follows:

```
rfs6000-81742D(config)#show wireless client
-------------------------------------------------------------------------------
-------
MAC         IPv4    VENDOR          RADIO-ID          WLAN             VLAN
STATE
-------------------------------------------------------------------------------
-------
-------------------------------------------------------------------------------
-------
Total number of wireless clients displayed: 0
rfs6000-81742D(config)#
```

The above output can be customized, using the customize > show-wireless-client command, as follows:

```
rfs6000-81742D(config)#customize show-wireless-client mac ip vendor vlan radio-id
state wlan location radio-alias radio-type
rfs6000-81742D(config)#commit

rfs6000-81742D(config)#show wireless client
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
--
MAC            IP   VENDOR          VLAN  RADIO-ID          STATE WLAN
AP-LOCATION     RADIO                RADIO-TYPE
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
--
```

```
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
--
Total number of wireless clients displayed: 0
rfs6000-81742D(config)#
```

**Example**

```
nx9500-6C8809(config)#show wireless wlan config
-------------------------------------------------------------------------------
  NAME   ENABLE   SSID   ENCRYPTION   AUTHENTICATION   VLAN     BRIDGING MODE
-------------------------------------------------------------------------------
  test   Y        test   wep64        none             1      local
-------------------------------------------------------------------------------
nx9500-6C8809(config)#

nx9500-6C8809(config)#show wireless wips client-blacklist
No wireless clients blacklisted
nx9500-6C8809(config)#

rfs6000-81742D#show wireless regulatory channel-info 36
Center frequency for channel 36 is 5180MHz
rfs6000-81742D#

nx9500-6C8809(config)#show wireless regulatory country-code
-------------------------------------------------------------------------------
            ISO CODE                                    NAME
-------------------------------------------------------------------------------
  gt                              Guatemala
  co                              Colombia
  cn                              China
  cm                              Cameroon
  cl                              Chile

--More--
nx9500-6C8809(config)#

nx9500-6C8809(config)#show wireless regulatory device-type ap7502 us
-------------------------------------------------------------------------------
--------------------
  #  Channel Set Power(mW) Power (dBm)    Placement        DFS      CAC(mins)
TPC
-------------------------------------------------------------------------------
--------------------

  1   1-11        4000      36          Indoor/Outdoor   NA             NA        NA
  2   36-48       4000      36          Indoor/Outdoor   Not Required   0         Not
Required
  3   52-64       500       27          Indoor/Outdoor   Required       1         Not
Required
  4   52-64      1000      30         Indoor/Outdoor   Required      1        Required
  5   100-140     500       27          Indoor/Outdoor   Required       1         Not
Required
  6   100-140    1000      30         Indoor/Outdoor   Required      1        Required
  7   149-165     4000      36          Indoor/Outdoor   Not Required   0         Not
Required

-------------------------------------------------------------------------------
--------------------
nx9500-6C8809(config)#
```

```
rfs6000-81742D#show wire ap detail

AP: 84-24-8D-84-A2-24
 AP Name               : ap7562-84A224
 Location              : Bangalore
 RF-Domain             : TechPubs
 Type                  : ap7562
 Model                 : AP-7562-67040-US
 IP                    : 192.168.13.29
 IPv6                  : ::
 Num of radios         : 2
 Num of clients        : 0
 Last Smart-RF time    : not done
 Stats update mode     : auto
 Stats interval        : 30
 Radio Modes           :
     radio-1           : wlan
     radio-2           : wlan
 Country-code          : not-set
 Site-Survivable       : True
 Last error          : in [India] not supported on hardware model AP-7562-67040-US
 Fault Detected        : False
 Power management information for ap7562:
--More--
rfs6000-81742D#

nx9500-6C8809#show wireless ap load-balancing on rfs6000-81742D
  Column Name Reference:
  Ap-Ld              : Load of the AP as reported by it.
  Avg-Ld             : Average AP load in the AP's neighborhood.
  2.4g-Ld            : 2.4GHz band load in the AP's neighborhood.
  5g-Ld              : 5GHz band load in the AP's neighborhood.
  Ap-2.4g-Ch-Ld      : Load in the AP's 2.4GHz channel in its neighborhood.
  Avg-2.4g-Ch-Ld     : Average load of a 2.4GHz channel in AP's neighborhood.
  Ap-5g-Ch-Ld        : Load in the AP's 5GHz channel in its neighborhood.
  Avg-5g-Ch-Ld       : Average load of a 5GHz channel in AP's neighborhood.
  Allow-2.4g-Req     : AP responds to client requests on 2.4ghz radio
  Allow-5g-Req       : AP responds to client requests on 5ghz radio
-------------------------------------------------------------------------------
-----------------------------------------------
  No.      Ap-Name           Ap-     Avg-    2.4g-   5g-     Band    Cfgd-   Ap-
Ap-     Avg-    Avg-    Allow    Allow
                             Load    Load    Load    Load    Ratio   Band    2.4g-
5g-     2.4g-   5g-     2.4g-    5g-
                                                                      Ratio   Ch-
Ld   Ch-Ld   Ch-Ld   Ch-Ld   Req      Req
-------------------------------------------------------------------------------
-----------------------------------------------
  1       rfs6000-81742D    0%      0%      0%      0%      0:0     0:1     182%
240%    0%      70%     yes     yes
-------------------------------------------------------------------------------
-----------------------------------------------
nx9500-6C8809#

nx9600-7F5124#show wireless meshpoint tree on PTP-AP
In progress .......
1:PTP-Radio2 [7 MPs(2 roots, 5 bound)]
|-ap7562-84A484-ROOT1
| |-ap7562-84A2CC-VMM
| |-ap7532-80C28C-NR
| |-ap7532-82CCA4-NR
| |-ap7562-84A22C-NR2
| |-ap7532-160114
|-ap7562-84A280-ROOT2

Total number of meshes displayed: 1
nx9600-7F5124#
```

```
ap6532-000001#show wireless meshpoint multicast detail
Multicast Paths @00-23-68-00-00-01 (ap6532-000001), mesh1 [00-23-68-2E-64-B2]
-------------------------------------------------------------------------------
      Group-Addr      Subscriber Name    Subscriber MPID     Timeout (mSecs)
-------------------------------------------------------------------------------
01-00-5E-01-01-01   ap6532-000001     00-23-68-2E-64-B2   N/A
-------------------------------------------------------------------------------

Total number of meshpoint displayed: 1
ap6532-000001#

ap6532-000001#show wireless meshpoint neighbor detail
Neighbors @00-23-68-00-00-01 (ap6532-000001), mesh1 [00-23-68-2E-64-B2]
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Neighbor Name          Neighbor MPID.IFID         Root Name     Root MPID     RMet
Hops  Type      Interface       Auth-State Resourced Rank LQ% LMet Age
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
              5C-0E-8B-21-76-22.5C-0E-8B-21-74-40          00-23-68-2E-97-60 115
1    Fixed 00-23-68-00-00-01:R2 Enabled    Yes       0    97  87   20
              00-23-68-30-F7-82.00-23-68-30-F8-F0          00-23-68-2E-97-60 99
1    Fixed 00-23-68-00-00-01:R2 Init       Yes       0    97  86   30
              00-23-68-30-F7-82.00-23-68-30-F7-82          00-23-68-2E-97-60 99
1    Fixed 00-23-68-00-00-01:R1 Enabled    Yes       0    96  94   0
              5C-0E-8B-21-76-22.5C-0E-8B-21-76-22          00-23-68-2E-97-60 115
1    Fixed 00-23-68-00-00-01:R1 Enabled    Yes       0    96  93   30
              00-23-68-2E-AB-50.00-23-68-2E-AB-50          00-23-68-2E-AB-50 0
0    Root  00-23-68-00-00-01:R2 Enabled    Yes       7    96  87   40
              00-23-68-2E-97-60.00-23-68-2E-97-60          00-23-68-2E-97-60 0
0    Root  00-23-68-00-00-01:R2 Enabled    Yes       8    94  90   10
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------

Total number of meshpoint displayed: 1
ap6532-000001#

ap6532-000001#show wireless meshpoint proxy detail
Proxies @00-23-68-00-00-01 (ap6532-000001), mesh1 [00-23-68-2E-64-B2]
-------------------------------------------------------------------------------
  Destination Addr   Owner Name      Owner MPID     Persist  VLAN      Age
-------------------------------------------------------------------------------
00-23-68-00-00-01 ap6532-000001 00-23-68-2E-64-B2 Permanent 101  180654310
00-1E-E5-A6-66-E2 ap6532-000001 00-23-68-2E-64-B2 Untimed   103  231920
-------------------------------------------------------------------------------

Total number of meshpoint displayed: 1
ap6532-000001#

ap6532-000001#show wireless meshpoint multicast mesh1
Multicast Paths @00-23-68-00-00-01 (ap6532-000001), mesh1 [00-23-68-2E-64-B2]
-------------------------------------------------------------------------------
      Group-Addr      Subscriber Name    Subscriber MPID     Timeout (mSecs)
-------------------------------------------------------------------------------
01-00-5E-01-01-01   ap6532-000001     00-23-68-2E-64-B2   -1
-------------------------------------------------------------------------------

Total number of meshpoint displayed: 1
ap6532-000001#
```

```
ap6532-000001#show wireless meshpoint path detail
Paths @00-23-68-00-00-01 (ap6532-000001), mesh1 [00-23-68-2E-64-B2]
------------------------------------------------------------------------------
-------------------------------------------------------------
Destination Name  Destination Addr Next Hop Name   Next Hop IFID   State Hops Type
Binding Metric Timeout Path-Timeout Sequence     MiNT ID
------------------------------------------------------------------------------
-------------------------------------------------------------
                  00-23-68-2E-AB-50              00-23-68-2E-AB-50 Valid 1    Root
Bound   89     8730    0           23847    68.31.19.58
                  00-23-68-2E-97-60              00-23-68-2E-97-60 Valid 1    Root
Unbound 92     5200    0           3481     68.31.1A.80
------------------------------------------------------------------------------
-------------------------------------------------------------
ap6532-000001#

rfs4000-22A24E#show wireless client
------------------------------------------------------------------------------
---------------------------------
Report start on RF-Domain: qs1
MAC                   IP    VENDOR           RADIO-ID           WLAN
VLAN     STATE
------------------------------------------------------------------------------
---------------------------------
Report end on RF-Domain: qs1
------------------------------------------------------------------------------
---------------------------------

------------------------------------------------------------------------------
---------------------------------
Report start on RF-Domain: Store-1
MAC                   IP    VENDOR           RADIO-ID           WLAN
VLAN         STATE
------------------------------------------------------------------------------
---------------------------------
00-01-02-03-04-10       2.3.4.16 3Com Corp         00-01-02-03-04-00:R1 sim-wlan-
1           1       Data-Ready
00-01-02-03-05-10       2.3.5.16 3Com Corp         00-01-02-03-04-00:R2 sim-wlan-
1           1       Data-Ready
Report end on RF-Domain: Store-1
------------------------------------------------------------------------------
---------------------------------

------------------------------------------------------------------------------
---------------------------------
Report start on RF-Domain: default
  database not available
Report end on RF-Domain: default
------------------------------------------------------------------------------
---------------------------------

Total number of clients displayed: 2
rfs4000-22A24E#
```

The following examples show client-bridge related information:

```
NX9500(config)#show adoption status
------------------------------------------------------------------------------
-------
DEVICE-NAME      VERSION    CFG-STAT  MSGS  ADOPTED-BY  LAST-ADOPTION      UPTIME
------------------------------------------------------------------------------
-------
ap6562-167598 5.9.1.0-017DB  configured   No    NX9500  0 days 00:01:59  0 days
00:03:22
------------------------------------------------------------------------------
-------
Total number of devices displayed: 1
NX9500(config)#
```

```
NX9500(config)#show wireless bridge on ap6562-167598
-------------------------------------------------------------------------------
-----------------
LOCAL RADIO      LOCAL BSSID     SELECTED AP    RF-BAND CHANNEL STATE    UP TIME
 ACTIVITY
 (sec ago)
-------------------------------------------------------------------------------
-----------------
ap6562-167598:R2 FC-0A-81-16-69-50  B4-C7-99-CA-A1-F0 5GHz   104  Selected 0 days
00:01:55   00:00:00
-------------------------------------------------------------------------------
-----------------
Total number of radios displayed: 1
NX9500(config)#


NX9500(config)#show wireless bridge config
-------------------------------------------------------------------------------
-------------------------------------------------------------
 IDX       NAME             MAC             PROFILE       RF-DOMAIN    SSID
BAND      ENCRYPTION    AUTHENTICATION    EAP-USERNAME
-------------------------------------------------------------------------------
-------------------------------------------------------------
  1   ap6562-167598   FC-0A-81-16-75-98   default-ap6562   default     inf_ap
2.4GHz/5GHz   ccmp         eap              hoabeo
-------------------------------------------------------------------------------
-------------------------------------------------------------
NX9500(config)#


NX9500(config)#show wireless bridge hosts
-------------------------------------------------------------------------------
HOST MAC             BRIDGE MAC         IP             BRIDGING STATUS ACTIVITY
                                                                    (sec ago)
-------------------------------------------------------------------------------
FC-0A-81-16-75-98    FC-0A-81-16-69-50 172.16.34.55    UP           00:00:00
-------------------------------------------------------------------------------
Total number of hosts displayed: 1
NX9500(config)#


NX9500(config)#show wireless bridge statistics
-------------------------------------------------------------------------------
-------
LOCAL RADIO         CONNECTED AP    SIGNAL   SNR TX-RATE RX-RATE    Tx     Rx  RETRY
                                    (dbm)    db  (Mbps)  (Mbps)    bps    bps   AVG
-------------------------------------------------------------------------------
-------
ap6562-167598:R2    B4-C7-99-CA-A1-F0   -52    50     53     36    1 k    3 k    10
-------------------------------------------------------------------------------
-------
Total number of radios displayed: 1
NX9500(config)#

NX9500(config)#show wireless bridge candidate-ap on ap6562-167598

 Client Bridge Candidate APs:
  AP-MAC             BAND    CHANNEL SIGNAL(dbm) STATUS
  B4-C7-99-CA-A1-F0  5 GHz   104     -39         selected

Total number of candidates displayed: 1
NX9500(config)#


NX9500(config)#show wireless bridge certificate status on ap6562-167598
Certificate Last Updated Status: Thu Jul 23 11:41:40 2017
NX9500(config)#
```

## 6.1.77 wwan

*show commands*

Displays wireless WAN status

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
show wwan [configuration|status] {on <DEVICE-OR-DOMAIN-NAME>}
```

**Parameters**

- `show wwan [configuration|status] {on <DEVICE-OR-DOMAIN-NAME>}`

| | |
|---|---|
| wwan | Displays wireless WAN configuration and status details |
| configuration | Displays wireless WAN configuration information |
| status | Displays wireless WAN status information |
| on <DEVICE-OR-DOMAIN-NAME> | The following keyword is common to the 'configuration' and 'status' parameters:<br>• on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays configuration or status details on a specified device or RF Domain<br><DEVICE-OR-DOMAIN-NAME> – Specify the AP, wireless controller, service platform, or RF Domain name. |

**Example**

```
rfs4000-229D58(config-device-00-23-68-22-9D-58)#show wwan configuration
>>> WWAN Configuration:
+-----------------------------------------
|  Access Port Name : isp.cingular
|  User Name        : testuser
|  Cryptomap        : map1
+-----------------------------------------
rfs4000-229D58(config-device-00-23-68-22-9D-58)#

rfs4000-229D58(config-device-00-23-68-22-9D-58)#show wwan status
>>> WWAN Status:
+-----------------------------------------
|  State : ACTIVE
|  DNS1  : 209.183.54.151
|  DNS2  : 209.183.54.151
+-----------------------------------------
rfs4000-229D58(config-device-00-23-68-22-9D-58)#
```

## 6.1.78 virtual-machine

*show commands*

Displays the *virtual-machine* (VM) configuration, logs, and statistics

**Supported in the following platforms:**

- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510

**Syntax**

```
show virtual-machine [configuration|debugging|export|statistics]

show virtual-machine [configuration|statistics] {<VM-NAME>|team-urc|team-rls|
team-vowlan} {(on <DEVICE-NAME>)}

show virtual-machine debugging {level|on}
show virtual-machine debugging {level [debug|error|info|warning]} {on <DEVICE-
NAME>}

show virtual-machine export <VM-NAME> {on <DEVICE-NAME>}

show virtual-machine [configuration|statistics] {<VM-NAME>|adsp|team-cmt}
```

**Parameters**

```
• show virtual-machine [configuration|statistics] {<VM-NAME>|team-urc|team-rls|
team-vowlan} {(on <DEVICE-NAME>)}
```

| | |
|---|---|
| virtual-machine | Displays the following VM-related information: configuration or statistics |
| configuration | Displays detailed VM configuration |
| statistics | Displays VM statistics |
| [<VM-NAME>\| team-urc\|team-rls\| team-vowlan] | The following keywords are common to the 'configuration' and 'statistics' parameters:<br>• <VM-NAME> – Optional. Displays VM configuration or statistics for the virtual machine identified by the <VM-NAME> keyword. Specify the VM name.<br>• team-urc – Optional. Displays TEAM-URC (IP-PBX) VM configuration/statistics<br>• team-rls – Optional. Displays TEAM-RLS (Radio Link Server) VM configuration/ statistics<br>• team-vowlan – Optional. Displays TEAM-VoWLAN (Voice over WLAN) VM configuration/statistics |
| on <DEVICE-NAME> | Optional. Specifies the name of the device on which the command is executed<br>• <DEVICE-NAME> – Specify the name of the service platform. |

```
• show virtual-machine [configuration|statistics] {<VM-NAME>|adsp|team-cmt}
{(on <DEVICE-NAME>)}
```

| | |
|---|---|
| virtual-machine | Displays the following VM-related information: configuration or statistics |
| configuration | Displays detailed VM configuration |
| statistics | Displays VM statistics |

| | |
|---|---|
| [<VM-NAME>\|adsp\| team-cmt] | The following keywords are common to the 'configuration' and 'statistics' parameters:<br>• <VM-NAME> – Optional. Displays VM configuration or statistics for the virtual machine identified by the <VM-NAME> keyword. Specify the VM name.<br>• adsp – Optional. Displays *Air-Defense Services Platform* (ADSP) VM configuration/ statistics<br>• team-cmt – Optional. Displays TEAM-CMT VM configuration/statistics<br>These keywords are specific to the NX9500 and NX9510 service platforms. |
| on <DEVICE-NAME> | Optional. Specifies the name of the device on which the command is executed<br>• <DEVICE-NAME> – Specify the name of the service platform. |

- `show virtual-machine debugging {level[debug|error|info|warning]} {on <DEVICE-NAME>}`

| | |
|---|---|
| virtual-machine | Displays the following VM-related information: configuration or statistics |
| debugging | Displays VM logs |
| level [debug\| error\|info\|warning] | Optional. Displays VM logs based on the level selected. The available options are:<br>• debug – Displays VM logs of level debug and above<br>• error – Displays VM logs of level error<br>• info – Displays VM logs of level Info and above<br>• warning – Displays logs of level warning and above<br>The NX9500 and NX9510 series service platforms will display ADSP and TEAM-CMT VM debugging logs. |
| on <DEVICE-NAME> | Optional. Specifies the name of the device on which the command is executed<br>• <DEVICE-NAME> – Specify the name of the service platform. |

- `show virtual-machine export <VM-NAME> {on <DEVICE-NAME>}`

| | |
|---|---|
| virtual-machine | Displays the following VM-related information: configuration or statistics |
| export | Displays VM configuration export related information |
| <VM-NAME> | Displays VM configuration export related information for the virtual machine identified by the <VM-NAME> keyword. Specify the VM name.<br>The NX9500 and NX9510 series service platforms will display ADSP and TEAM-CMT VM configuration export information |
| on <DEVICE-NAME> | Optional. Specifies the name of the device on which the command is executed<br>• <DEVICE-NAME> – Specify the name of the service platform. |

**Example**

```
nx9500-6C874D#show virtual-machine statistics
-------------------------------------------------------------------------------
       NAME         STATE   VCPUS MEM (MB)    BRIDGE-IF             IP
-------------------------------------------------------------------------------
  WiNG             -         -     18432    -               -
  adsp             Halted    -     -        unknown         -
  team-cmt         Halted    -     -        unknown         -
-------------------------------------------------------------------------------
nx9500-6C874D#

nx9500-6C874D#show virtual-machine configuration
-------------------------------------------------------------------------------
           NAME               AUTOSTART         MEMORY(MB)           VCPUS
-------------------------------------------------------------------------------
  WiNG                      -                 18432              -
  adsp                      ignore            12000              12
  team-cmt                  ignore            1024               1
-------------------------------------------------------------------------------

nx9500-6C874D#

nx9500-6C874D>show virtual-machine statistics adsp
 VM name: adsp
 Base Version    : unknown
 Install Status  : not_installed
nx9500-6C874D>
```

## 6.1.79 raid

*show commands*

Displays *Redundant Array of Independent Disks* (RAID) related information, such as array status, consistency check status, and RAID log.

Use this command to assess the RAID array's drive utilization and whether the drives are currently online. Since there is only one RAID array controller reporting status to the service platform, it is important to know if other drive s house hot spare drives as additional resources should one of the dedicated drives fail. This command also displays whether a physical within the RAID array has a drive installed, and whether the drive is currently online.

**Supported in the following platforms:**

- Service Platforms — NX9500

**Syntax**

```
show raid {on <DEVICE-NAME>}
```

**Parameters**

- `show raid {on <DEVICE-NAME>}`

| | |
|---|---|
| raid | Displays the RAID array status and statistics |
| on <DEVICE-NAME> | Optional. Displays RAID status and statistics on a specified device<br>• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

**Example**

```
nx9500-6C874D(config)#show raid
Logical drive info:
 Size 930 GB, State optimal
 Alarm enabled
 Last check: Sat Aug 10 02:56:54 2013
 Last check result: ending
Physical drive info:

Drive  0: online
Drive  1: online
Drive  2: not-installed
Drive  3: not-installed
Drive  4: not-installed
nx9500-6C874D(config)#
```

# 7 PROFILES

Profiles enable administrators to assign a common set of configuration parameters, policies, and WLANs to service platforms, controllers, and access points across a large, multi segment, site. The configuration parameters within a profile are based on the hardware model the profile was created to support.

The service platforms, wireless controllers, and access points support both default and user-defined profiles. Each default and user-defined profile contains policies and configurations that are applied to devices assigned to the profile. Changes made to these configurations are automatically inherited by the devices. The central benefit of a profile is its ability to update devices collectively without having to modify individual device configurations.

Default profiles are system maintained and are automatically applied to service platforms and wireless controllers. The default AP profile is automatically applied to a AP (discovered by a wireless controller or service platform), unless an AP auto-provisioning policy is defined specifically to assign APs to a user-defined profile. After adoption, changes made to a profile's parameters are reflected across all devices using the profile. Default profiles are ideal for single site deployments where service platforms, wireless controllers, and access points share a common configuration.

User-defined profiles, on the other hand, are manually created for each supported service platform, wireless controller, and access point model. User-defined profiles are recommended for larger deployments using centralized controllers and service platforms when groups of devices on different floors, buildings or sites share a common configuration. These user-defined profiles can be manually, or automatically assigned to through an auto provisioning policy. An auto provisioning policy provides the means to assign profiles to access points based on model, serial number, VLAN ID, DHCP options, IP address (subnet) and MAC address. For more information, see *AUTO-PROVISIONING-POLICY*.

Each default and user-defined profile contains policies and configuration parameters.

A user defined profile can be created for each of the following device type:

- AP6521 – Adds an AP6521 access point profile
- AP6522 – Adds an AP6522 access point profile
- AP6532 – Adds an AP6532 access point profile
- AP6562 – Adds an AP6562 access point profile
- AP7161 – Adds an AP7161 access point profile
- AP7502 – Adds an AP7502 access point profile
- AP7522 – Adds an AP7522 access point profile
- AP7532 – Adds an AP7532 access point profile
- AP7562 – Adds an AP7562 access point profile
- AP7602 – Adds an AP7602 access point profile
- AP7612 – Adds an AP7612 access point profile
- AP7622 – Adds an AP7622 access point profile
- AP7632 – Adds an AP7632 access point profile
- AP7662 – Adds an AP7662 access point profile
- AP81XX – Adds an AP81XX access point profile supporting the AP8132 and AP8163 models
- AP8232 – Adds an AP8232 access point profile
- AP8432 – Adds an AP8432 access point profile

- AP8533 – Adds an AP8533 access point profile
- EX3524 – Adds an EX3524 wireless controller profile
- EX3548 – Adds an EX3548 wireless controller profile
- RFS4000 – Adds an RFS4000 wireless controller profile
- RFS6000 – Adds an RFS6000 wireless controller profile
- NX5500 – Adds an NX5500 wireless controller profile
- NX7500 – Adds an NX75XX series service platform profile supporting the NX7510, NX7520, and NX7530 models
- NX9000 – Adds an NX95XX series service platform profile supporting the NX9500 and NX9510 models
- NX9600 – Adds an NX96XX series service platform profile supporting the NX9600 and NX9610 models. Supported only on an NX96XX model device.
- VX9000 – Adds a VX9000 wireless controller profile
- T5 – Adds a T5 controller profile

**NOTE:** A T5 profile can be created only on the following platforms: RFS4000, RFS6000, NX9500, NX9510, and NX9600.

Although profiles assign a common set of configuration parameters across devices, individual devices can still be assigned unique configuration parameters that follow the flat configuration model. As individual device updates are made, these devices no longer share the profile based configuration they originally supported. Therefore, changes made to a profile are not automatically inherited by devices who have had their configuration customized. These devices require careful administration, as they cannot be tracked as profile members. Their customized configurations overwrite their profile configurations until the profile is re-applied.

**NOTE:** The commands present under ‘Profiles’ are also available under the ‘Device mode’. The additional commands specific to the ‘Device mode’ are listed separately.

This chapter is organized into the following topics:

- *Profile Config Commands*
- *Device Config Commands*
- *T5 Profile Config Commands*
- *EX3524 & EX3548 Profile/Device Config Commands*

To view the list of device profiles supported, use the following command:

```
<DEVICE>(config)#profile ?
  anyap       Any access point profile
  ap650       AP650 access point profile
  ap6511      AP6511 access point profile
  ap6521      AP6521 access point profile
  ap6522      AP6522 access point profile
  ap6532      AP6532 access point profile
  ap6562      AP6562 access point profile
  ap71xx      AP7161 access point profile
  ap7502      AP7502 access point profile
  ap7522      AP7522 access point profile
  ap7532      AP7532 access point profile
  ap7562      AP7562 access point profile
```

```
  ap81xx      AP81XX access point profile
  ap82xx      AP8232 access point profile
  ap8432      AP8432 access point profile
  ap8533      AP8533 access point profile
  containing  Specify profiles that contain a sub-string in the profile name
  ex3524      EX3524 wireless controller profile
  ex3548      EX3548 wireless controller profile
  filter      Specify addition selection filter
  nx5500      NX5500 wireless controller profile
  nx75xx      NX75XX wireless controller profile
  nx9000      NX9000 wireless controller profile
  nx9600      NX9600 wireless controller profile
  rfs4000     RFS4000 wireless controller profile
  rfs6000     RFS6000 wireless controller profile
  rfs7000     RFS7000 wireless controller profile
  t5          T5 wireless controller profile
  vx9000      VX9000 wireless controller profile

<DEVICE>(config)#

rfs6000-37FABE(config)#profile rfs6000 default-rfs6000
rfs6000-37FABE(config-profile-default-rfs6000)#

rfs6000-37FABE(config)#profile ap71xx default-ap71xx
rfs6000-37FABE(config-profile-default-ap71xx)#

<DEVICE>(config)#profile <DEVICE-TYPE> <PROFILE-NAME>
<DEVICE>(config-profile-<PROFILE-NAME>)#

<DEVICE>(config-profile-<PROFILE-NAME>)#?
Profile Mode commands:
adopter-auto-provisioning-policy-lookup  Use centralized auto-provisioning
                                           policy when adopted by another
                                           controller
  adoption                                 Adoption configuration
  adoption-mode                            Configure the adoption mode for the
                                           access-points in this RF-Domain
  alias                                    Alias
  application-policy                       Application Poicy configuration
  area                                     Set name of area where the system
                                           is located
  arp                                      Address Resolution Protocol (ARP)
  auto-learn                               Auto learning
  autogen-uniqueid                         Autogenerate a unique id
  autoinstall                              Autoinstall settings
  bridge                                   Ethernet bridge
  captive-portal                           Captive portal
  cdp                                      Cisco Discovery Protocol
  cluster                                  Cluster configuration
  configuration-persistence                Enable persistence of configuration
                                           across reloads (startup config
                                           file)
  controller                               WLAN controller configuration
  critical-resource                        Critical Resource
  crypto                                   Encryption related commands
  database                                 Database command
  device-onboard                           Device-onboarding configuration
  device-upgrade                           Device firmware upgrade
  diag                                     Diagnosis of packets
  dot1x                                    802.1X
  dpi                                      Enable Deep-Packet-Inspection
                                           (Application Assurance)
  dscp-mapping                             Configure IP DSCP to 802.1p
                                           priority mapping for untagged
                                           frames
  eguest-server                            Enable ExtremeGuest Server
                                           functionality
  email-notification                       Email notification configuration
```

```
enforce-version                          Check the firmware versions of
                                         devices before interoperating
environmental-sensor                     Environmental Sensors Configuration
events                                   System event messages
export                                   Export a file
file-sync                                File sync between controller and
                                         adoptees
floor                                    Set the floor within a area where
                                         the system is located
gre                                      GRE protocol
http-analyze                             Specify HTTP-Analysis configuration
interface                                Select an interface to configure
ip                                       Internet Protocol (IP)
ipv6                                     Internet Protocol version 6 (IPv6)
l2tpv3                                   L2tpv3 protocol
l3e-lite-table                           L3e lite Table
led                                      Turn LEDs on/off on the device
led-timeout                              Configure the time for the led to
                                         turn off after the last radio state
                                         change
legacy-auto-downgrade                    Enable device firmware to auto
                                         downgrade when other legacy devices
                                         are detected
legacy-auto-update                       Auto upgrade of legacy devices
lldp                                     Link Layer Discovery Protocol
load-balancing                           Configure load balancing parameter
logging                                  Modify message logging facilities
mac-address-table                        MAC Address Table
mac-auth                                 802.1X
management-server                        Configure management server address
memory-profile                           Memory profile to be used on the
                                         device
meshpoint-device                         Configure meshpoint device
                                         parameters
meshpoint-monitor-interval               Configure meshpoint monitoring
                                         interval
min-misconfiguration-recovery-time       Time interval to check controller
                                         connectivity after configuration is
                                         received
mint                                     MiNT protocol
misconfiguration-recovery-time           Check controller connectivity after
                                         configuration is received
neighbor-inactivity-timeout              Configure neighbor inactivity
                                         timeout
neighbor-info-interval                   Configure neighbor information
                                         exchange interval
no                                       Negate a command or set its
                                         defaults
noc                                      Configure the noc related setting
nsight                                   NSight
ntp                                      Ntp server WORD
offline-duration                         Set duration for which a device
                                         remains unadopted before it
                                         generates offline event
otls                                     Omnitrail Location Server
power-config                             Configure power mode
preferred-controller-group               Controller group this system will
                                         prefer for adoption
preferred-tunnel-controller              Tunnel Controller Name this system
                                         will prefer for tunneling extended
                                         vlan traffic
radius                                   Configure device-level radius
                                         authentication parameters
raid                                     RAID
remote-debug                             Configure remote debug parameters
remove-override                          Remove configuration item override
                                         from the device (so profile value
                                         takes effect)
```

```
  rf-domain-manager                       RF Domain Manager
  router                                  Dynamic routing
  slot                                    PCI expansion Slot
  spanning-tree                           Spanning tree
  traffic-class-mapping                   Configure IPv6 traffic class to
                                          802.1p priority mapping for
                                          untagged frames
  traffic-shape                           Traffic shaping
  trustpoint                              Assign a trustpoint to a service
  tunnel-controller                       Tunnel Controller group this
                                          controller belongs to
  use                                     Set setting to use
  vrrp                                    VRRP configuration
  vrrp-state-check                        Publish interface via OSPF/BGP only
                                          if the interface VRRP state is not
                                          BACKUP
  wep-shared-key-auth                     Enable support for 802.11 WEP
                                          shared key authentication
  zone                                    Configure Zone name

  clrscr                                  Clears the display screen
  commit                                  Commit all changes made in this
                                          session
  do                                      Run commands from Exec mode
  end                                     End current mode and change to EXEC
                                          mode
  exit                                    End current mode and down to
                                          previous mode
  help                                    Description of the interactive help
                                          system
  revert                                  Revert changes
  service                                 Service Commands
  show                                    Show running system information
  write                                   Write running configuration to
                                          memory or terminal

<DEVICE>(config-profile-<PROFILE-NAME>)#

<DEVICE>(config-profile-<T5-PROFILE-NAME>)#?
T5 Profile Mode commands:
  cpe             T5 CPE configuration
  interface       Select an interface to configure
  ip              Internet Protocol (IP)
  no              Negate a command or set its defaults
  ntp             Configure NTP
  override-wlan   Configure RF Domain level overrides for wlan
  t5              T5 configuration
  t5-logging      Modify message logging facilities
  use             Set setting to use

  clrscr          Clears the display screen
  commit          Commit all changes made in this session
  do              Run commands from Exec mode
  end             End current mode and change to EXEC mode
  exit            End current mode and down to previous mode
  help            Description of the interactive help system
  revert          Revert changes
  service         Service Commands
  show            Show running system information
  write           Write running configuration to memory or terminal
<DEVICE>(config-profile-<T5-PROFILE-NAME>)#
```

```
<DEVICE>(config-profile-<EX3524/EX3548-PROFILE-NAME>)#?
EX3500 Profile Mode commands:
  interface  Select an interface to configure
  ip         Internet Protocol (IP)
  no         Negate a command or set its defaults
  power      Ex3500 Power over Ethernet Command
  upgrade    Configures upgrade option for ex3500 system
  use        Set setting to use

  clrscr     Clears the display screen
  commit     Commit all changes made in this session
  do         Run commands from Exec mode
  end        End current mode and change to EXEC mode
  exit       End current mode and down to previous mode
  help       Description of the interactive help system
  revert     Revert changes
  service    Service Commands
  show       Show running system information
  write      Write running configuration to memory or terminal
<DEVICE>(config-profile-<EX3524/EX3548-PROFILE-NAME>)#
```

**NOTE:** The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.

# 7.1 Profile Config Commands

*PROFILES*

The following table summarizes profile configuration mode commands:

| Command | Description | Reference |
|---|---|---|
| *adopter-auto-provisioning-policy-lookup* | Enables the use of a centralized auto provisioning policy on this profile | *page 7-11* |
| *adoption* | Configures a minimum and maximum delay time in the initiation of the device adoption process | *page 7-13* |
| *alias* | Creates various types of aliases, such as network, VLAN, network-group, network-service, encrypted-string, hashed -string, etc. at the profile level | *page 7-15* |
| *application-policy* | Associates a RADIUS server provided application policy with this profile. When associated, the application policy allows wireless clients (MUs) to always find the RADIUS-supplied application policy in the dataplane. | *page 7-22* |
| *area* | Sets the system's area of location (the area name) | *page 7-24* |
| *arp* | Configures static address resolution protocol | *page 7-25* |
| *auto-learn* | Enables controllers or service platforms to maintain a local configuration record of devices requesting adoption and provisioning. The command also enables learning of a device's host name via DHCP options. | *page 7-27* |
| *autogen-uniqueid* | Auto-generates a unique local ID for devices using this profile. When executed in the device configuration mode, this command generates a unique ID for the logged device. | *page 7-28* |
| *autoinstall* | Configures the automatic install feature | *page 7-30* |
| *bridge* | Configures bridge specific parameters | *page 7-31* |
| *captive-portal* | Configures captive portal advanced Web page upload on a device profile | *page 7-62* |
| *cdp* | Enables *Cisco Discovery Protocol* (CDP) on a device | *page 7-63* |
| *cluster* | Configures a cluster name | *page 7-64* |
| *configuration-persistence* | Enables persistence of configuration across reloads | *page 7-67* |
| *controller* | Configures a wireless controller or service platform | *page 7-68* |
| *critical-resource* | Monitors resources that are critical to the health of the service platform, wireless controller, or access point managed network. These critical resources are identified by their configured IP addresses. | *page 7-72* |
| *crypto* | Configures data encryption related protocols and settings | *page 7-80* |
| *database* | Backs up captive-portal and/or NSight database to a specified location and file and configures a low-disk-space threshold value | *page 7-143* |
| *device-onboard* | Configures the logo image file name and title displayed on the EGuest device-onboarding portal. This is the portal a vendor-admin user uses to onboard devices. | *page 7-144* |
| *device-upgrade* | Configures device firmware upgrade settings on this profile | *page 7-145* |
| *diag* | Enables looped packet logging | *page 7-147* |

| Command | Description | Reference |
|---|---|---|
| *dot1x* | Configures 802.1x standard authentication controls | *page 7-148* |
| *dpi* | Enables *Deep Packet Inspection* (DPI) on this profile | *page 7-150* |
| *dscp-mapping* | Configures an IP DSCP to 802.1p priority mapping for untagged frames | *page 7-153* |
| *eguest-server (VX9000 only)* | Enables the EGuest daemon when executed without the 'host' option | *page 7-154* |
| *eguest-server (NOC Only)* | Points to the EGuest server, when executed along with the 'host' option | *page 7-155* |
| *email-notification* | Configures e-mail notification settings | *page 7-156* |
| *enforce-version* | Enables checking of a device's firmware version before attempting adoption or clustering | *page 7-158* |
| *environmental-sensor* | Configures the environmental sensor settings on this profile (applicable to AP8132 model access point only) | *page 7-159* |
| *events* | Enables system event logging and message generation. This command also configures event message forwarding settings. | *page 7-161* |
| *export* | Enables export of startup.log file after every boot | *page 7-162* |
| *file-sync* | Configures parameters enabling synching of trustpoint and/or wireless-bridge certificate between the staging-controller and adopted access point | *page 7-163* |
| *floor* | Sets the floor name where the system is located | *page 7-164* |
| *gre* | Enables *Generic Routing Encapsulation* (GRE) tunneling on this profile | *page 7-165* |
| *http-analyze* | Configures HTTP analysis settings | *page 7-177* |
| *interface* | Configures an interface (VLAN, radio, GE, etc.) | *page 7-180* |
| *ip* | Configures IPv4 components | *page 7-348* |
| *ipv6* | Configures IPv6 components | *page 7-358* |
| *l2tpv3* | Defines the *Layer 2 Tunnel Protocol* (L2TP) protocol for tunneling layer 2 payloads using *Virtual Private Networks* (VPNs) | *page 7-362* |
| *l3e-lite-table* | Configures L3e Lite Table with this profile | *page 7-364* |
| *led* | Turns device LEDs on or off | *page 7-365* |
| *led-timeout* | Configures LED-timeout timer. This command is specific to the NX95XX series service platforms. | *page 7-366* |
| *legacy-auto-downgrade* | Auto downgrades a legacy device firmware | *page 7-368* |
| *legacy-auto-update* | Auto upgrades a legacy device firmware | *page 7-369* |
| *lldp* | Configures *Link Layer Discovery Protocol* (LLDP) | *page 7-370* |
| *load-balancing* | Configures load balancing parameters | *page 7-372* |
| *logging* | Modifies message logging settings | *page 7-377* |
| *mac-address-table* | Configures the MAC address table | *page 7-379* |
| *mac-auth* | Enables 802.1x user authentication protocol on this profile | *page 7-381* |

| Command | Description | Reference |
|---|---|---|
| *management-server* | Configures a management server with this profile | *page 7-384* |
| *memory-profile* | Configures the memory profile used on the device | *page 7-385* |
| *meshpoint-device* | Configures a meshpoint device parameters | *page 7-386* |
| *meshpoint-monitor-interval* | Configures meshpoint monitoring interval | *page 7-388* |
| *min-misconfiguration-recovery-time* | Configures the minimum device connectivity verification time | *page 7-389* |
| *mint* | Configures MiNT protocol settings | *page 7-390* |
| *misconfiguration-recovery-time* | Verifies device connectivity after a configuration is received | *page 7-397* |
| *neighbor-inactivity-timeout* | Configures neighbor inactivity timeout | *page 7-398* |
| *neighbor-info-interval* | Configures neighbor information exchange interval | *page 7-399* |
| *no* | Removes or reverts settings to their default. The no command, when used in the profile configuration mode, removes the selected profile's settings or reverts them to their default. | *page 7-400* |
| *noc* | Configures NOC settings | *page 7-402* |
| *nsight* | Configures NSight database related parameters | *page 7-403* |
| *ntp* | Configures NTP server settings | *page 7-408* |
| *otls* | Configures support for detection and forwarding of OmniTrail beacon tags | *page 7-411* |
| *offline-duration* | Sets the duration, in minutes, for which a device remains un-adopted before it generates offline event | *page 7-414* |
| *power-config* | Configures the power mode | *page 7-415* |
| *preferred-controller-group* | Specifies the wireless controller or service platform group preferred for adoption | *page 7-417* |
| *preferred-tunnel-controller* | Configures the tunnel wireless controller or service platform preferred by the system to tunnel extended VLAN traffic | *page 7-418* |
| *radius* | Configures device-level RADIUS authentication parameters | *page 7-419* |
| *raid* | Enables alarm on the array. This command is supported only on the NX9500 and NX9510 series service platform profile/device config modes. | *page 7-493* |
| *rf-domain-manager* | Enables devices using this profile to be elected as RF Domain manager. Also sets the priority value for devices using this profile in the RF Domain manager election process. | *page 7-420* |
| *router* | Configures dynamic router protocol settings | *page 7-421* |
| *spanning-tree* | Configures spanning tree related settings | *page 7-423* |
| *traffic-class-mapping* | Maps the IPv6 traffic class value of incoming IPv6 untagged packets to 802.1p priority | *page 7-426* |

| Command | Description | Reference |
|---|---|---|
| *traffic-shape* | Enables traffic shaping and configures traffic shaping parameters | *page 7-428* |
| *trustpoint (profile-config-mode)* | Configures the trustpoint assigned for validating a CMP auth Operator | *page 7-434* |
| *tunnel-controller* | Configures the name of tunneled WLAN (extended VLAN) wireless controller or service platform | *page 7-436* |
| *use* | Uses pre configured policies with this profile | *page 7-437* |
| *vrrp* | Configures *Virtual Router Redundancy Protocol* (VRRP) group settings | *page 7-443* |
| *vrrp-state-check* | Publishes interface via OSPF or BGP based on VRRP status | *page 7-447* |
| *virtual-controller* | Enables an access point as a *virtual-controller* (VC) or *dynamic virtual controller* (DVC). Note, DVC is supported only on the AP7522, AP7532, and AP7562 model access points. | *page 7-448* |
| *wep-shared-key-auth* | Enables support for 802.11 WEP shared key authentication | *page 7-450* |
| *service* | Service commands are used to view and manage configurations. The service commands and their corresponding parameters vary from mode to mode. | *page 7-451* |
| *zone* | Configures the zone for devices using this profile. The zone can also be configured on the device's self context. | *page 7-456* |

**NOTE:** For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see *COMMON COMMANDS*.

## 7.1.1 adopter-auto-provisioning-policy-lookup

*Profile Config Commands*

Enables the use of a centralized auto provisioning policy on this profile. When enabled, the auto-provisioning policy applied on the NOC gets precedence over the one applied at the site controller level. Optionally, use the '*evaluate-always*' option to set flag to run centralized auto-provisioning policy every time a device (access point/controller) is adopted. The device's previous adoption status is not taken into consideration.

This command is also applicable in the device configuration context.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
adopter-auto-provisioning-policy-lookup {evaluate-always}
```

**Parameters**

- `adopter-auto-provisioning-policy-lookup {evaluate-always}`

| | |
|---|---|
| adopter-auto-provisioning-policy-lookup {evaluate-always} | Enables the use of a centralized auto provisioning policy on this profile or device<br>• evaluate-always – Optional. Sets flag to run centralized auto-provisioning policy every time a device (access point/controller) is adopted. |

**Example**

```
rfs6000-81742D(config-profile-default-rfs6000)#adopter-auto-provisioning-policy-
lookup evaluate-always

rfs6000-81742D(config-profile-default-rfs6000)#show context
profile rfs6000 default-rfs6000
 autoinstall configuration
 autoinstall firmware
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 crypto remote-vpn-client
 interface me1
 interface up1
 interface ge1
 interface ge2
 interface ge3
 interface ge4
 interface ge5
 interface ge6
 interface ge7
 interface ge8
 interface wwan1
 interface pppoe1
 use firewall-policy default
```

```
 logging on
 service pm sys-restart
 adopter-auto-provisioning-policy-lookup
 router ospf
 router bgp
rfs6000-81742D(config-profile-default-rfs6000)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables the application of centralized auto provisioning policy on this profile or device |

## 7.1.2 adoption

*Profile Config Commands*

Configures a minimum and maximum delay time in the initiation of the device adoption process. When configured, devices do not attempt adoption immediately on coming up. The process is initiated after the lapse of a specified period of time (configured using this command as the *start-delay minimum* time).

Once configured and applied, this setting is applicable on all devices using this profile. This option is also available in the device-configuration mode.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
adoption start-delay min <0-30> max <0-30>
```

**Parameters**

- `adoption start-delay min <0-30> max <0-30>`

| | |
|---|---|
| adoption start-delay min <0-30> max <0-30> | Delays start of device adoption process<br>• min <0-30> – Configures the minimum time to lapse before a device attempts adoption. Specify a value from 0 - 30 seconds.<br>A device, on coming up, attempts adoption only after the lapse of the time specified here. The default is 5 seconds.<br>• max <0-30> – Configures the maximum time to lapse before a device attempts adoption. Specify a value from 0 - 30 seconds. The default is 20 seconds. |

**Example**

```
rfs6000-81742D(config-profile-default-rfs6000)#adoption start-delay min 10 max 30

rfs6000-81742D(config-profile-default-rfs6000)#show context
profile rfs6000 default-rfs6000
 autoinstall configuration
 autoinstall firmware
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 crypto remote-vpn-client
 interface me1
 interface up1
 interface ge1
 interface ge2
 interface ge3
 interface ge4
 interface ge5
 interface ge6
 interface ge7
 interface ge8
```

```
 interface wwan1
 interface pppoe1
 use firewall-policy default
 logging on
 service pm sys-restart
 adopter-auto-provisioning-policy-lookup
 router ospf
 router bgp
 adoption start-delay min 10 max 30
rfs6000-81742D(config-profile-default-rfs6000)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the configured minimum start-delay value. When removed, devices attempt adoption immediately on coming up. |

## 7.1.3 alias

*Profile Config Commands*

Configures network, VLAN, and service aliases. The aliases defined on this profile applies to all devices using this profile. Aliases can be also defined at the device level.

**NOTE:** You can apply overrides to aliases at the device level. Overrides applied at the device level take precedence. For more information on aliases, see *alias*.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
alias [address-range|encrypted-string|hashed-string|host|network|network-group|
network-service|number|string|vlan]

alias address-range <ADDRESS-RANGE-ALIAS-NAME> <STARTING-IP> to <ENDING-IP>

alias encrypted-string <ENCRYPTED-STRING-ALIAS-NAME> [0|2] <LINE>

alias hashed-string <HASHED-STRING-ALIAS-NAME> <LINE>

alias host <HOST-ALIAS-NAME> <HOST-IP>

alias network <NETWORK-ALIAS-NAME> <NETWORK-ADDRESS/MASK>

alias network-group <NETWORK-GROUP-ALIAS-NAME> [address-range|host|network]
alias network-group <NETWORK-GROUP-ALIAS-NAME> [address-range <STARTING-IP> to
<ENDING-IP> {<STARTING-IP> to <ENDING-IP>}|host <HOST-IP> {<HOST-IP>}|network
<NETWORK-ADDRESS/MASK> {<NETWORK-ADDRESS/MASK>}]

alias network-service <NETWORK-SERVICE-ALIAS-NAME> proto [<0-254>|<WORD>|eigrp|
gre|igmp|igp|ospf|vrrp] {(<1-65535>|<WORD>|bgp|dns|ftp|ftp-data|gopher|https|
ldap|nntp|ntp|pop3|proto|sip|smtp|sourceport|ssh|telnet|tftp|www)}

alias network-service <NETWORK-SERVICE-ALIAS-NAME> proto [<0-254>|<WORD>|eigrp|
gre|igmp|igp|ospf|vrrp] {(<1-65535>|<WORD>|bgp|dns|ftp|ftp-data|gopher|https|
ldap|nntp|ntp|pop3|proto|sip|smtp|sourceport [<1-65535>|<WORD>]|ssh|telnet|tftp|
www)}

alias number <NUMBER-ALIAS-NAME> <0-4294967295>

alias string <STRING-ALIAS-NAME> <LINE>

alias vlan <VLAN-ALIAS-NAME> <1-4094>
```

**Parameters**

- `alias address-range <ADDRESS-RANGE-ALIAS-NAME> <STARTING-IP> to <ENDING-IP>`

| | |
|---|---|
| address-range <ADDRESS-RANGE-ALIAS-NAME> | Creates a new address-range alias for this profile. Or associates an existing address-range alias with this profile. An address-range alias maps a name to a range of IP addresses. Use this option to create unique address-range aliases for different deployment scenarios.<br>Contd.. |

| | |
|---|---|
| | For example, if an ACL defines a pool of network addresses as 192.168.10.10 through 192.168.10.100 for an entire network, and a remote location's network range is 172.16.13.20 through 172.16.13.110, the remote location's ACL can be overridden using an alias. At the remote location, the ACL works with the 172.16.13.20-110 address range. A new ACL need not be created specifically for the remote deployment location.<br>• <ADDRESS-RANGE-ALIAS-NAME> – Specify the address range alias name.<br>**Note:** Alias name should begin with '$'. |
| <STARTING-IP> to <ENDING-IP> | Associates a range of IP addresses with this address range alias<br>• <STARTING-IP> – Specify the first IP address in the range.<br>• to <ENDING-IP> – Specify the last IP address in the range.<br>Aliases defined at any given level can be overridden at the next lower levels. For example, a global alias can be redefined on a selected set of RF Domains, profiles, or devices. Overrides applied at the device level take precedence. |

- `alias encrypted-string <ENCRYPTED-STRING-ALIAS-NAME> [0|2] <LINE>`

| | |
|---|---|
| encrypted-string <ENCRYPTED-STRING-ALIAS-NAME> | Creates an alias for an encrypted string. Use this alias for string configuration values that are encrypted when "password-encryption" is enabled. For example, in the management-policy, use it to define the SNMP community string. For more information, see *snmp-server*.<br>• <ENCRYPTED-STRING-ALIAS-NAME> – Specify the encrypted-string alias name.<br>Alias name should begin with '$'. |
| [0\|2] <LINE> | Configures the value associated with the alias name specified in the previous step<br>• [0\|2] <LINE> – Configures the alias value<br>Note, if password-encryption is enabled, in the *show > running-config* output, this clear text is displayed as an encrypted string, as shown below:<br>`nx9500-6C8809(config)#show running-config`<br>`!.............................`<br>`alias encrypted-string $enString 2`<br>`fABMK2is7UToNiZE3MQXbgAAAAxB0ZIysdqsEJwr6AH/Da//`<br>`!`<br>`--More--`<br>`nx9500-6C8809`<br>`In the above output, the '2' displayed before the encrypted-string alias value indicates that the displayed text is encrypted and not a clear text.`<br>`However, if password-encryption is disabled the clear text is displayed as is:`<br>`nx9500-6C8809(config)#show running-config`<br>`!.............................`<br>`!`<br>`alias encrypted-string $enString 0 test11223344`<br>`!`<br>`--More--`<br>`nx9500-6C8809`<br>For more information on enabling password-encryption, see *password-encryption*. |

- `alias hashed-string <HASHED-STRING-ALIAS-NAME> <LINE>`

| | |
|---|---|
| hashed-string <HASHED-STRING-ALIAS-NAME> | Creates an alias for a hashed string. Use this alias for configuration values that are hashed string, such as passwords. For example, in the management-policy, use it to define the privilege mode password. For more information, see *privilege-mode-password*.<br>• <HASHED-STRING-ALIAS-NAME> – Specify the hashed-string alias name.<br>Alias name should begin with '$'. |
| <LINE> | Configures the hashed-string value associated with this alias.<br>`nx9500-6C8809(config)#show running-config`<br>`!`<br>`alias encrypted-string $WRITE 2`<br>`sBqVCDAoxs3oByF5PCSuFAAAAAd7HT2+EiT/l/BXm9c4SBDv`<br>`!`<br>`alias hashed-string $PriMode 1`<br>`faffdde27cb49ad634ea20df4f7c8ef2685894d10ffcb1b2efba054112ec`<br>`fc75`<br>`--More--`<br>`nx9500-6C8809`<br>In the above *show > running-config* output, the '1' displayed before the hashed-string alias value indicates that the displayed text is hashed and not a clear text. |

- `alias host <HOST-ALIAS-NAME> <HOST-IP>`

| | |
|---|---|
| host <HOST-ALIAS-NAME> | Creates a new host alias for this profile. Or associates an existing host alias with this profile. A host alias configuration is for a particular host device's IP address. Use this option to create unique host aliases for different deployment scenarios. For example, if a central network DNS server is set a static IP address, and a remote location's local DNS server is defined, this host can be overridden at the remote location. At the remote location, the network is functional with a local DNS server, but uses the name set at the central network. A new host need not be created at the remote location. This simplifies creating and managing hosts and allows an administrator to better manage specific local requirements.<br>• <HOST-ALIAS-NAME> – Specify the host alias name.<br>Alias name should begin with '$'. |
| <HOST-IP> | Associates the network host's IP address with this host alias<br>• <HOST-IP> – Specify the network host's IP address.<br>Aliases defined at any given level can be overridden at the next lower levels. For example, a global alias can be redefined on a selected set of RF Domains, profiles, or devices. Overrides applied at the device level take precedence. |

- `alias network <NETWORK-ALIAS-NAME> <NETWORK-ADDRESS/MASK>`

| | |
|---|---|
| network <NETWORK-ALIAS-NAME> | Creates a new network alias for this profile. Or associates an existing network alias with this profile. A network alias configuration is utilized for an IP address on a particular network. Use this option to create unique Network aliases for different deployment scenarios. For example, if a central network ACL defines a network as 192.168.10.0/24, and a remote location's network range is 172.16.10.0/24, the ACL can be overridden at the remote location to suit their local (but remote) requirement.<br>At the remote location, the ACL functions with the 172.16.10.0/24 network. A new ACL need not be created specifically for the remote deployment. This simplifies ACL definition and allows an administrator to better manage specific local requirements.<br>• <NETWORK-ALIAS-NAME> – Specify the network alias name.<br>Alias name should begin with '$'. |

| | |
|---|---|
| <NETWORK-ADDRESS/MASK> | Associates a single network with this network alias<br>• <NETWORK-ADDRESS/MASK> – Specify the network's address and mask.<br>Aliases defined at any given level can be overridden at the next lower levels. For example, a global alias can be redefined on a selected set of RF Domains, profiles, or devices. Overrides applied at the device level take precedence. |

```
• alias network-group <NETWORK-GROUP-ALIAS-NAME> [address-range <STARTING-IP> to
<ENDING-IP> {<STARTING-IP> to <ENDING-IP>}|host <HOST-IP> {<HOST-IP>}|
network <NETWORK-ADDRESS/MASK> {<NETWORK-ADDRESS/MASK>}]
```

| | |
|---|---|
| network <NETWORK-GROUP-ALIAS-NAME> | Creates a new network-group alias for this profile. Or associates an existing network-group alias with this profile.<br>• <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name.<br>Alias name should begin with '$'.<br>The network-group aliases are used in ACLs, to define the network-specific components. ACLs using aliases can be used across sites by re-defining the network-group alias elements at the device or profile level.<br>After specifying the name, specify the following: a range of IP addresses, host addresses, or a range of network addresses.<br>Aliases defined at any given level can be overridden at the next lower levels. For example, a global alias can be redefined on a selected set of RF Domains, profiles, or devices. Overrides applied at the device level take precedence. |
| address-range <STARTING-IP> to <ENDING-IP> {<STARTING-IP> to <ENDING-IP>} | Associates a range of IP addresses with this network-group alias<br>• <STARTING-IP> – Specify the first IP address in the range.<br>• to <ENDING-IP> – Specify the last IP address in the range.<br>• <STARTING-IP> to <ENDING-IP> – Optional. Specifies more than one range of IP addresses. A maximum of eight (8) IP address ranges can be configured. |
| host <HOST-IP> {<HOST-IP>} | Associates a single or multiple hosts with this network-group alias<br>• <HOST-IP> – Specify the hosts' IP address.<br>• <HOST-IP> – Optional. Specifies more than one host. A maximum of eight (8) hosts can be configured. |
| network <NETWORK-ADDRESS/MASK> {<NETWORK-ADDRESS/MASK>} | Associates a single or multiple networks with this network-group alias<br>• <NETWORK-ADDRESS/MASK> – Specify the network's address and mask.<br>• <NETWORK-ADDRESS/MASK> – Optional. Specifies more than one network. A maximum of eight (8) networks can be configured. |

```
• alias network-service <NETWORK-SERVICE-ALIAS-NAME> proto [<0-254>|<WORD>|
eigrp|gre|igmp|igp|ospf|vrrp] {(<1-65535>|<WORD>|bgp|dns|ftp|ftp-data|gopher|
https|ldap|nntp|ntp|pop3|proto|sip|smtp|sourceport [<1-65535>|<WORD>]|ssh|
telnet|tftp|www)}
```

| | |
|---|---|
| alias network-service <NETWORK-SERVICE-ALIAS-NAME> | Creates a new network-service alias for this profile. Or associates an existing network-service alias with this profile. A network service alias is a set of configurations that consist of protocol and port mappings. Both source and destination ports are configurable. For each protocol, up to 2 source port ranges and up to 2 destination port ranges can be configured. A maximum of 4 protocol entries can be configured per network service alias.<br>• <NETWORK-SERVICE-ALIAS-NAME> – Specify a network-service alias name.<br>Alias name should begin with '$'.<br>Contd.. |

| | |
|---|---|
| | The network-service aliases are used in ACLs, to define the service-specific components. ACLs using aliases can be used across sites by re-defining the network-service alias elements at the device or profile level.<br>**Note:** Aliases defined at any given level can be overridden at the next lower levels. For example, a global alias can be redefined on a selected set of RF Domains, profiles, or devices. Overrides applied at the device level take precedence. |
| proto [<0-254>\|<WORD>\|eigrp\|gre\|igmp\|igp\|ospf\|vrrp] | Use one of the following options to associate an Internet protocol with this network-service alias:<br>• <0-254> – Identifies the protocol by its number. Specify the protocol number from 0 - 254. This is the number by which the protocol is identified in the *Protocol* field of the IPv4 header and the *Next Header* field of IPv6 header. For example, the *User Datagram Protocol's* (UDP) designated number is 17.<br>• <WORD> – Identifies the protocol by its name. Specify the protocol name.<br>• eigrp – Selects *Enhanced Interior Gateway Routing Protocol* (EIGRP). The protocol number 88.<br>• gre – Selects *Generic Routing Encapsulation* (GRE). The protocol number is 47.<br>• igmp – Selects *Internet Group Management Protocol* (IGMP). The protocol number is 2.<br>• igp – Selects *Interior Gateway Protocol* (IGP). The protocol number is 9.<br>• ospf – Selects *Open Shortest Path First* (OSPF). The protocol number is 89.<br>• vrrp – Selects *Virtual Router Redundancy Protocol* (VRRP). The protocol number is 112. |
| {(<1-65535>\|<WORD>\|bgp\|dns\|ftp\|ftp-data\|gopher\|https\|ldap\|nntp\|ntp\|pop3\|proto\|sip\|smtp\|sourceport [<1-65535>\|<WORD>]\|ssh\|telnet\|tftp\|www)} | After specifying the protocol, you may configure a destination port for this service. These keywords are recursive and you can configure multiple protocols and associate multiple destination and source ports.<br>• <1-65535> – Optional. Configures a destination port number from 1 - 65535<br>• <WORD> – Optional. Identifies the destination port by the service name provided. For example, the *secure shell* (SSH) service uses TCP port 22.<br>• bgp – Optional. Configures the default *Border Gateway Protocol* (BGP) services port (179)<br>• dns – Optional. Configures the default *Domain Name System* (DNS) services port (53)<br>• ftp – Optional. Configures the default *File Transfer Protocol* (FTP) control services port (21)<br>• ldap – Optional. Configures the default *Lightweight Directory Access Protocol* (LDAP) services port (389)<br>• ftp-data – Optional. Configures the default FTP data services port (20)<br>• gopher – Optional. Configures the default gopher services port (70)<br>• https – Optional. Configures the default HTTPS services port (443)<br>• nntp – Optional. Configures the default Newsgroup (NNTP) services port (119)<br>• ntp – Optional. Configures the default *Network Time Protocol* (NTP) services port (123)<br>• proto – Optional. Use this option to select another Internet protocol in addition to the one selected in the previous step.<br>• sip – Optional. Configures the default *Session Initiation Protocol* (SIP) services port (5060).<br>Contd.. |

| | |
|---|---|
| | • sourceport [<1-65535>\|<WORD>] – Optional. After specifying the destination port, you may specify a single or range of source ports.<br>• <1-65535> – Specify the source port from 1 - 65535.<br>• <WORD> – Specify the source port range, for example 1-10.<br>• ssh – Optional. Configures the default SSH services port (22)<br>• telnet – Optional. Configures the default Telnet services port (23)<br>• tftp – Optional. Configures the default *Trivial File Transfer Protocol* (TFTP) services port (69)<br>• www – Optional. Configures the default HTTP services port (80) |

• `alias number <NUMBER-ALIAS-NAME> <0-4294967295>`

| | |
|---|---|
| alias number <NUMBER-ALIAS-NAME> <0-4294967295> | Creates a number alias identified by the <NUMBER-ALIAS-NAME> keyword. Number aliases map a name to a numeric value. For example, 'alias number $NUMBER 100'<br>• The number alias name is: $NUMBER<br>• The value assigned is: 100<br>The value referenced by alias $NUMBER, wherever used, is 100.<br>• <NUMBER-ALIAS-NAME> – Specify the number alias name.<br>• <0-4294967295> – Specify the number, from 0 - 4294967295, assigned to the number alias created.<br>Alias name should begin with '$'. |

• `alias string <STRING-ALIAS-NAME> <LINE>`

| | |
|---|---|
| alias string <STRING-ALIAS-NAME> | Creates a new string alias for this profile. Or associates an existing string alias with this profile. String aliases map a name to an arbitrary string value. Use this option to create unique string aliases for different deployment scenarios. For example, if the main domain at a remote location is called loc1.domain.com and at another deployment location it is called loc2.domain.com, the alias can be overridden at the remote location to suit the local (but remote) requirement. At one remote location, the alias functions with the loc1.domain.com domain and at the other with the loc2.domain.com domain.<br>• <VLAN-ALIAS-NAME> – Specify the string alias name.<br>• <LINE> – Specify the string value.<br>Alias name should begin with '$'.<br>Aliases defined at any given level can be overridden at the next lower levels. For example, a global alias can be redefined on a selected set of RF Domains, profiles, or devices. Overrides applied at the device level take precedence. |

• `alias vlan <VLAN-ALIAS-NAME> <1-4094>`

| | |
|---|---|
| alias vlan <VLAN-ALIAS-NAME> | Creates a new VLAN alias for this profile. Or associates an existing VLAN alias with this profile. A VLAN alias maps a name to a VLAN ID. A VLAN alias is a configuration for optimal VLAN re-use and management for local and remote deployments. Use this option to create unique VLANs aliases for different deployment scenarios. For example, if a VLAN ID is set as 10 for the central network, and the VLAN is set as 26 at a remote location, the VLAN can be overridden at the remote location using an alias.<br>Contd.. |

| | |
|---|---|
| | At the remote location, the network is functional with an ID of 26, but utilizes the name defined at the central local network. A new VLAN need not be created specifically at the remote location.<br>• <VLAN-ALIAS-NAME> – Specify the VLAN alias name.<br>Alias name should begin with '$'. |
| <1-4094> | Maps the VLAN alias to a VLAN ID<br>• <1-4094> – Specify the VLAN ID from 1 - 4094.<br>Aliases defined at any given level can be overridden at the next lower levels. For example, a global alias can be redefined on a selected set of RF Domains, profiles, or devices. Overrides applied at the device level take precedence. |

**Example**

The following example shows the global aliases configured. Note the network-service alias '$kerberos' settings.

```
nx9500-6C8809(config)#show running-config | include alias
alias network-group $NetGrpAlias address-range 192.168.13.7 to 192.168.13.16
192.168.13.20 to 192.168.13.25
alias network-group $NetGrpAlias network 192.168.13.0/24 192.168.16.0/24
alias network $NetworkAlias 192.168.13.0/24
alias host $HostAlias 192.168.13.10
alias address-range $AddRanAlias 192.168.13.10 to 192.168.13.13
alias network-service $kerberos proto tcp 23 22 proto udp 25
alias vlan $VlanAlias 1
alias string $AREA Ecospace
alias string $IN-Blr-EcoSpace-Floor-4 IBEF4
alias encrypted-string $READ 2 CdO6glQ9w29hybKxfbd6JwAAAAa7lKMBMk9EiDQfFRf9kegO
alias hashed-string $PriMode 1
faffdde27cb49ad634ea20df4f7c8ef2685894d10ffcb1b2efba054112ecfc75
nx9500-6C8809(config)#
```

The following examples show the overrides applied to the network-service alias '$kerberos' at the profile level:

```
nx9500-6C8809(config-profile-testRFS4k)#alias network-service $kerberos proto tcp
88 proto udp 389
nx9500-6C8809(config-profile-testRFS4k)#
```

The following example shows the overrides applied to the network-service alias '$kerberos' at the profile level:

```
nx9500-6C8809(config-profile-testRFS4k)#show running-config | include alias
alias network-group $NetGrpAlias address-range 192.168.13.7 to 192.168.13.16
192.168.13.20 to 192.168.13.25
alias network-group $NetGrpAlias network 192.168.13.0/24 192.168.16.0/24
alias network $NetworkAlias 192.168.13.0/24
alias host $HostAlias 192.168.13.10
alias address-range $AddRanAlias 192.168.13.10 to 192.168.13.13
alias network-service $kerberos proto tcp 23 22 proto udp 25
alias vlan $VlanAlias 1
alias string $AREA Ecospace
alias string $IN-Blr-EcoSpace-Floor-4 IBEF4
alias encrypted-string $READ 2 /Mfbt1Et8XRhybKxfbd6JwAAAAZ9yrIYq7mNl4+gNNiiMIZI
alias hashed-string $PriMode 1
faffdde27cb49ad634ea20df4f7c8ef2685894d10ffcb1b2efba054112ecfc75
alias network-service $kerberos proto tcp 88 proto udp 389
nx9500-6C8809(config-profile-testRFS4k)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the use of centralized auto provisioning policy on this profile or device |

## 7.1.4 application-policy

*Profile Config Commands*

Associates a RADIUS server provided application policy with this profile. This command is also applicable to the device configuration mode. When associated, the application policy allows wireless clients (MUs) to always find the RADIUS-supplied application policy in the dataplane.

An application policy defines the actions executed on recognized HTTP (Facebook), enterprise (Webex) and peer-to-peer (gaming) applications or application-categories. The following are the actions that can be applied in an application policy:

- Allow - Allows packets for a specific application and its defined category type (for e.g., social networking)
- Deny - Denies (restricts) packets to a specific application and its defined category type
- Mark - Marks recognized packets with DSCP/8021p value
- Rate-limit - Rate limits packets from specific application type

For more information on configuring an application policy, see *application-policy*.

**Supported in the following platforms:**

- Access Points — AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8432, AP8533
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
application-policy radius <APP-POLICY-NAME>
```

**Parameters**

- `application-policy radius <APP-POLICY-NAME>`

| | |
|---|---|
| application-policy radius <APP-POLICY-NAME> | Associates a RADIUS server provided application policy with this profile<br>• <APP-POLICY-NAME> – Specify the application policy name (should be existing and configured). |

**Example**

```
nx9500-6C8809(config)#show context include-factory | include application-policy
application-policy Bing
  no use application-policy
  no use application-policy
  no use application-policy
 no use application-policy
 no use application-policy
 no use application-policy
 no use application-policy
 no use application-policy
  no use application-policy
nx9500-6C8809(config)#

nx9500-6C8809(config-profile-testNX9500)#application-policy radius Bing

nx9500-6C8809(config-profile-testNX9500)#show context include-factory | include
application-policy
 application-policy radius Bing
nx9500-6C8809(config-profile-testNX9500)#
```

```
nx9500-6C8809(config-application-Bing)#Show context
application Bing
 app-category streaming
 use url-list Bing
nx9500-6C8809(config-application-Bing)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the RADIUS-server provided application policy associated with this profile |

## 7.1.5 area

*Profile Config Commands*

Sets the system's area of location (the physical area of deployment)

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
area <WORD>
```

**Parameters**

- `area <WORD>`

| | |
|---|---|
| area <WORD> | Sets the system's area of location<br>• <WORD> – Specify the area name (should not exceed 64 characters). |

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000)#area Ecospace

rfs6000-37FABE(config-profile-default-rfs6000)#show context
profile rfs6000 default-rfs6000
 bridge vlan 1
  ip igmp snooping
  ip igmp snooping querier
 area Ecospace
 autoinstall configuration
 autoinstall firmware
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 interface me1
 interface ge1
--More--
rfs6000-37FABE(config-profile-default-rfs6000)#
```

**Related Commands**

| | |
|---|---|
| *no* | Resets the configured area name |

## 7.1.6 arp

*Profile Config Commands*

Adds a static *Address Resolution Protocol* (ARP) IP address in the ARP cache

The ARP protocol maps an IP address to a hardware MAC address recognized on the network. ARP provides protocol rules for making this correlation and providing address conversion in both directions.

When an incoming packet destined for a host arrives, ARP finds a physical host or MAC address that matches the IP address. ARP looks in its ARP cache and, if it finds the address, provides it so the packet can be converted to the right packet length, formatted, and sent to its destination. If no entry is found for the IP address, ARP broadcasts a request packet in a special format on the LAN to locate a device that recognizes the IP address. A device that recognizes the IP address as its own returns a reply indicating it. ARP updates the ARP cache for future reference and then sends the packet to the MAC address that replied.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
arp [<IP>|timeout]

arp <IP> <MAC> arpa [<L3-INTERFACE-NAME>|pppoe1|vlan <1-4094>|wwan1|serial <1-4>
<1-1> <1-1>] {dhcp-server|router}

arp timeout <15-86400>
```

**Parameters**

```
• arp <IP> <MAC> arpa [<L3-INTERFACE-NAME>|pppoe1|vlan <1-4094>|wwan1|serial <1-
4> <1-1> <1-1>] {dhcp-server|router}
```

| | |
|---|---|
| arp <IP> | Adds a static ARP IPv4 address in the ARP cache<br>• <IP> – Specify the static IP address. |
| <MAC> | Specify the MAC address associated with the IP and the *Switch Virtual Interface* (SVI). |
| arpa | Sets ARP encapsulation type to ARPA |
| <L3-INTERFACE-NAME> | Configures static ARP entry for a specified router interface<br>• <L3-INTERFACE-NAME> – Specify the router interface name. |
| pppoe1 | Configures static ARP entry for PPP over Ethernet interface |
| vlan <1-4094> | Configures static ARP entry for a VLAN interface<br>• <1-4094> – Specify a SVI VLAN ID from 1 - 4094. |
| wwan1 | Configures static ARP entry for Wireless WAN interface |
| {dhcp-server\|router} | The following keywords are common to all off the above interface types:<br>• dhcp-server – Optional. Sets ARP entries for a DHCP server<br>• router – Optional. Sets ARP entries for a router |

- `arp timeout <15-86400>`

| | |
|---|---|
| arp timeout <15-86400> | Sets ARP entry timeout<br>• <TIME> – Sets the ARP entry timeout in seconds. Specify a value from 15 - 86400 seconds. The default is 3600 seconds. |

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000)#arp timeout 2000

rfs6000-37FABE(config-profile-default-rfs6000)#show context
profile rfs6000 default-rfs6000
 bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
 arp timeout 2000
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 interface me1
 interface ge1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge2
  ip dhcp trust
--More--
rfs6000-37FABE(config-profile-default-rfs7000)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes an entry from the ARP cache |

## 7.1.7 auto-learn

*Profile Config Commands*

Enables controllers or service platforms to maintain a local configuration record of devices requesting adoption and provisioning. The command also enables learning of a device's host name via DHCP options.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
auto-learn [host-name-via-dhcp <WORD>|staging-config]
```

**Parameters**

- `auto-learn [host-name-via-dhcp <WORD>|staging-config]`

| | |
|---|---|
| auto-learn [host-name-via-dhcp <WORD>\| staging-config] | Enables auto-learning of:<br>• host-name-via-dhcp – A device's host name via DHCP option.<br>• <WORD> – Provide the optional template with substitution token. For example, 'outdoor-$DHCP[1:3]-ap', where the *$DHCP token* references DHCP Option value received by the adopting device. The $DHCP token should be present. This option is disabled by default.<br>• staging-config – The network configuration of devices requesting adoption. This option is enabled by default. For dependent access points that are pre-staged prior to deployment, it is recommended that the auto-learn-staging-config parameter remains enabled so that hostnames, VLAN and IP addressing configuration can be maintained upon initial adoption. However, if dependent access points are to be centrally managed and configured, it is recommended that the auto-learn-staging-config parameter be disabled. |

**Example**

```
nx9500-6C8809(config-profile-test)#auto-learn staging-config

nx9500-6C8809(config-profile-test)#show context include-factory | include auto-
learn
 auto-learn staging-config
 no auto-learn host-name-via-dhcp
nx9500-6C8809(config-profile-test)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables automatic recognition of devices' hostname and devices pending adoption |

## 7.1.8 autogen-uniqueid

*Profile Config Commands*

Auto-generates a unique ID for devices using this profile. When executed in the device configuration mode, this command generates a unique ID for the logged device. A device's unique ID is a combination of a user-defined string (prefix, suffix, or both) and a substitution token. The WiNG implementation provides two built-in substitution tokens: $SN and $MiNT-ID that represent the device's serial number and MiNT-ID respectively. The value referenced by these substitution tokens are internally retrieved and combined with the user-defined string to auto generate a unique identity for the device.

The general format of this command is: <PREFIX><SUBSTITUTION-TOKEN><SUFFIX>. You can provide both (prefix and suffix) or just a prefix or suffix.

For example, given the following set of inputs:

- user-defined prefix – TestAP6522
- substitution token – $SN

The unique ID is generated using TestAP6522$SN, where $SN is replaced with the device's serial number.

When executed on an AP6522 (having serial number B4C7996C8809), the autogen-uniqueid TestAP6522$SN command generates the unique ID: TestAP6522*B4C7996C8809*. When configured on an AP6522 profile, all AP6522s using the profile auto-generate a unique ID in which the device's serial number is preceded by the string 'TestAP6522'.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
autogen-uniqueid <WORD>
```

**Parameters**

- `autogen-uniqueid <WORD>`

| | |
|---|---|
| autogen-uniqueid <WORD> | Auto-generates a device's unique ID (not exceeding 64 characters in length)<br>The ID generated is a combination of the text provided and the value referenced through the substitution token $SN or $MiNT-ID. Where ever the autogen-uniqueid is used the device's serial number *OR* MiNT-ID is referenced depending on the substitution token used.<br>• <WORD> – Specify a auto generate unique ID format using one of the following substitution tokens:<br>Available tokens:<br>$SN - references SERIAL NUMBER of the device<br>$MINT-ID - references MINT-ID of the device<br>For example, Test-$SN-TechPubs. In this example 'Test' and 'TechPubs' represent the user-defined prefix and suffix respectively. And $SN is the substitution token. |

**Example**

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#autogen-uniqueid Test-$MiNT-ID-
TechPubs

nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#show context
nx9000 B4-C7-99-6C-88-09
 use profile default-nx9000
 use rf-domain TechPubs
 hostname nx9500-6C8809
 license AAP
66069c24b3bb1259b34ff016c723a9e299dd408f0ff891e7c5f7e279a382648397d6b3e975e356a1
 license HTANLT
66069c24b3bb1259eb36826cab3cc83999dd408f0ff891e74b62b2d3594f0b3dde7967f30e49e497
 timezone Asia/Calcutta
 use database-policy default
 use nsight-policy noc
 autogen-uniqueid Test-$MiNT-ID-TechPubs
 ip default-gateway 192.168.13.2
 device-upgrade auto rfs6000 ap81xx ap71xx ap7562 ap7532
 interface ge1
  switchport mode access
  switchport access vlan 1
 interface ge2
 --More--
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#
```

**Related Commands**

| | |
|---|---|
| *no* | When executed in the device configuration mode, removes the device's autogen-uniqueid. When executed in the profile configuration mode, removes the autogen-uniqueid on all devices using the profile. |

## 7.1.9 autoinstall

*Profile Config Commands*

Automatically installs firmware image and startup configuration parameters on to the selected device.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
autoinstall [configuration|firmware|start-interval <WORD>]
```

**Parameters**

- `autoinstall [configuration|firmware|start-interval <WORD>]`

| | |
|---|---|
| configuration | Autoinstalls startup configuration. Setup parameters are automatically configured on devices using this profile. This option is disabled by default. |
| firmware | Autoinstalls firmware image. Firmware images are automatically installed on devices using this profile. This option is disabled by default. |
| start-interval <WORD> | Configures the interval between system boot and start of autoinstall process (this is the time, from system boot, after which autoinstall should start)<br>• <WORD> – Specify the interval in minutes. The default is 10 minutes.<br>**Note:** Zero (0) implies firmware or startup configuration installation can start any time. |

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000)#autoinstall configuration

rfs6000-37FABE(config-profile-default-rfs6000)#autoinstall firmware

rfs7000-37FABE(config-profile-default-rfs6000)#show context
profile rfs6000 default-rfs6000
 bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
 arp timeout 2000
 autoinstall configuration
 autoinstall firmware
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 interface me1
 interface ge1
  ip dhcp trust
--More--
rfs6000-37FABE(config-profile-default-rfs6000)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables the auto install settings |

## 7.1.10 bridge

*Profile Config Commands*

The following table summarizes Ethernet bridge configuration commands:

| Command | Description | Reference |
|---|---|---|
| *bridge* | Enables Ethernet bridge configuration context | *page 7-32* |
| *bridge-vlan-mode commands* | Summarizes bridge VLAN configuration mode commands | *page 7-35* |

### 7.1.10.1 bridge

*bridge*

Configures VLAN Ethernet bridging parameters. Use this command to configure a Bridge NAT or Bridge VLAN settings

Configuring bridge *Network Address Translation* (NAT) parameters, allows management of Internet traffic originating at a remote site. In addition to traditional NAT functionality, bridge NAT provides a means of configuring NAT for bridged traffic through an access point. NAT rules are applied to bridged traffic through the access point, and matching packets are NATed to the WAN link instead of being bridged on their way to the router. Using bridge NAT, a tunneled VLAN (extended VLAN) is created between the NOC and a remote location. When a remote client needs to access the Internet, Internet traffic is routed to the NOC, and from there routed to the Internet. This increases the access time for the end user on the client. To resolve latency issues, bridge NAT identifies and segregates traffic heading towards the NOC and outwards towards the Internet. Traffic towards the NOC is allowed over the secure tunnel. Traffic towards the Internet is switched to a local WLAN link with access to the Internet.

A *Virtual LAN* (VLAN) is a separately administrated virtual network within the same physical managed network. VLANs are broadcast domains defined within wireless controllers or service platforms to allow control of broadcast, multicast, unicast, and unknown unicast within a layer 2 device. For example, say several computers are used in conference room X and some in conference Y. The systems in conference room X can communicate with one another, but not with the systems in conference room Y. The VLAN enables the systems in conference rooms X and Y to communicate with one another even though they are on separate physical subnets. The systems in conference rooms X and Y are managed by the same single wireless controller or service platform, but ignore the systems that are not using the same VLAN ID. Administrators often need to route traffic between different VLANs. Bridging VLANs are only for non-routable traffic, like tagged VLAN frames destined to some other device, which will untag it. When a data frame is received on a port, the VLAN bridge determines the associated VLAN based on the port of reception. Using forwarding database information, the bridge VLAN forwards the data frame on the appropriate port(s). VLANs are useful to set separate networks to isolate some computers from others, without actually having to have separate cabling and Ethernet switches. Controllers can do this on their own, without need for the computer or other gear to know itself what VLAN it is on (this is called port-based VLAN, since it is assigned by port of the switch). Another common use is to put specialized devices like VoIP Phones on a separate network for easier configuration, administration, security, or quality of service.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Switch Note:** For more information on the interface types and the devices supporting them, see *interface*.

**Syntax**

```
bridge [nat|vlan]

bridge nat source list <IP-ACCESS-LIST-NAME> precedence <1-500> interface
[<LAYER3-INTERFACE-NAME>|pppoe1|vlan <1-4094>|wwan1] [(address|interface|
overload|pool <NAT-POOL-NAME>)]

bridge vlan [<1-4094>|<VLAN-ALIAS-NAME>]
```

**Parameters**

- `bridge nat source list <IP-ACCESS-LIST-NAME> precedence <1-500> interface [<LAYER3-INTERFACE-NAME>|pppoe1|vlan <1-4094>|wwan1] [(address|interface|overload|pool <NAT-POOL-NAME>)]`

| | |
|---|---|
| nat | Configures bridge NAT parameters |
| source | Configures NAT source addresses |
| list <IP-ACCESS-LIST-NAME> precedence <1-500> | Associates an *access control list* (ACL) with this bridge NAT policy. The ACL specifies the IP address permit/deny rules applicable to this bridge NAT policy.<br>• <IP-ACCESS-LIST-NAME> – Specify access list name.<br>• precedence <1-500> – Specifies a precedence value for this bridge NAT policy. |
| interface [<LAYER3-INTERFACE-NAME>\| pppoe1\|vlan <1-4094>\| wwan1] | Selects one of the following as the primary interface (between the source and destination points):<br>• <LAYER3-INTERFACE-NAME> – A router interface. Specify interface name.<br>• pppoe1 – A PPP over Ethernet interface.<br>• vlan <1-4094> – A VLAN interface. Specify the VLAN interface index from 1 - 4094.<br>• wwan1 – A Wireless WAN interface. |
| [(address\|interface\| overload\|pool <NAT-POOL-NAME>)] | The following keywords are recursive and common to all interface types:<br>• address – Configures the interface IP address used for NAT<br>• interface – Configures the failover interface (default setting)<br>• overload – Enables use of one global address for multiple local addresses (terminates command)<br>• pool <NAT-POOLNAME> – Configures the NAT pool used with this bridge NAT policy. Specify the NAT pool name. For more information on configuring a NAT pool, see *nat-pool-config-instance*. |

- `bridge vlan [<1-4094>|<VLAN-ALIAS-NAME>]`

| | |
|---|---|
| vlan <1-4094> | Configures the numerical identifier for the Bridge VLAN when it was initially created.<br>• <1-4094> – Specify a VLAN index from 1 - 4094. |
| vlan <VLAN-ALIAS-NAME> | Configures the VLAN alias (should be existing and configured) identifying the bridge VLAN<br>• <VLAN-ALIAS-NAME> – Specify a VLAN alias name. |

**Usage Guidelines**

Creating customized filter schemes for bridged networks limits the amount of unnecessary traffic processed and distributed by the bridging equipment.

If a bridge does not hear *Bridge Protocol Data Units* (BPDUs) from the root bridge within the specified interval, defined in the max-age (seconds) parameter, assume the network has changed and recomputed the spanning-tree topology.

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000)#bridge vlan 1
rfs6000-37FABE(config-profile-default-rfs6000-bridge-vlan-1)#?
Bridge VLAN Mode commands:
  Bridge VLAN Mode commands:
  bridging-mode                                Configure how packets on this
                                               VLAN are bridged
  captive-portal                               Captive Portal
  captive-portal-enforcement                   Enable captive-portal enforcement
                                               on this extended VLAN
  description                                  Vlan description
  edge-vlan                                    Enable edge-VLAN mode
  firewall                                     Enable vlan firewall(IPv4)
  http-analyze                                 Forward URL and Data to
                                               controller
  ip                                           Internet Protocol (IP)
  ipv6                                         Internet Protocol version 6
                                               (IPv6)
  l2-tunnel-broadcast-optimization             Enable broadcast optimization
  l2-tunnel-forward-additional-packet-types    Forward additional packet types
                                               not normally forwarded by l2
                                               broadcast optimization
  mac-auth                                     Enable mac-auth for this bridge
                                               vlan
  no                                           Negate a command or set its
                                               defaults
  stateful-packet-inspection-l2                Enable stateful packet inspection
                                               in layer2 firewall
  tunnel                                       Vlan tunneling settings
  tunnel-over-level2                           Tunnel extended VLAN traffic over
                                               level 2 MiNT links
  use                                          Set setting to use

  clrscr                                       Clears the display screen
  commit                                       Commit all changes made in this
                                               session
  do                                           Run commands from Exec mode
  end                                          End current mode and change to
                                               EXEC mode
  exit                                         End current mode and down to
                                               previous mode
  help                                         Description of the interactive
                                               help system
  revert                                       Revert changes
  service                                      Service Commands
  show                                         Show running system information
  write                                        Write running configuration to
                                               memory or terminal

rfs6000-37FABE(config-profile-default-rfs6000-bridge-vlan-1)#
```

### 7.1.10.2 bridge-vlan-mode commands

- *bridge*

The following table summarizes bridge VLAN configuration mode commands:

| Command | Description | Reference |
|---|---|---|
| *bridging-mode* | Configures how packets on this VLAN are bridged | *page 7-36* |
| *captive-portal* | Enables IP packet snooping on wired captive portals, and also configures the subnet to snoop | *page 7-38* |
| *captive-portal-enforcement* | Enables auto-enforcement of captive portal rules on this extended VLAN interface | *page 7-39* |
| *description* | Configures VLAN bridge description | *page 7-40* |
| *edge-vlan* | Enables edge VLAN mode | *page 7-41* |
| *firewall* | Enables firewall on this bridge VLAN interface | *page 7-42* |
| *http-analyze* | Enables the analysis of URLs and data traffic on this Bridge VLAN | *page 7-43* |
| *ip* | Configures IP components | *page 7-44* |
| *ipv6* | Configures IPv6 components | *page 7-47* |
| *l2-tunnel-broadcast-optimization* | Enables broadcast optimization | *page 7-50* |
| *l2-tunnel-forward-additional-packet-types* | Enables forwarding of *Wireless Network Management Protocol* (WNMP) packets across L2 tunnels. These WNMP packets are normally not forwarded if L2 tunnel broadcast optimization is enabled. | *page 7-53* |
| *mac-auth* | Enables MAC authentication for Extended VLAN and Tunneled traffic | *page 7-51* |
| *no* | Negates a command or reverts settings to their default | *page 7-54* |
| *stateful-packet-inspection-l2* | Enables stateful packet inspection in the layer 2 fire wall | *page 7-56* |
| *tunnel* | Enables tunneling of unicast messages to unknown MAC destinations, on the selected VLAN bridge | *page 7-57* |
| *tunnel-over-level2* | Enables extended VLAN traffic over level 2 MiNT links | *page 7-59* |
| *use* | Associates a captive-portal, access control list (IP, IPv6, or MAC), and a URL filter with this bridge VLAN | *page 7-60* |

### 7.1.10.2.1 bridging-mode

*bridge-vlan-mode commands*

Configures how packets are bridged on the selected VLAN

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
bridging-mode [auto|isolated-tunnel|local|tunnel]
```

**Parameters**

- `bridging-mode [auto|isolated-tunnel|local|tunnel]`

| | |
|---|---|
| bridging-mode | Configures the VLAN bridging mode |
| auto | Automatically selects the bridging mode to match the WLAN, VLAN and bridging mode configurations. When selected, the controller or access point determines the best bridging mode for the VLAN. (default setting) |
| isolated-tunnel | Bridges packets between local Ethernet ports and local radios, and passes tunneled packets through without de-tunneling<br>Select this option for a dedicated tunnel for bridging VLAN traffic. |
| local | Bridges packets normally between local Ethernet ports and local radios (if any)<br>Local mode is typically configured in remote branch offices where traffic on remote private LAN segments need to be bridged locally. Local mode implies that traffic, wired and wireless, is to be bridged locally. |
| tunnel | Bridges packets between local Ethernet ports, local radios, and tunnels to other APs, wireless controllers, or service platforms<br>Select this option to use a shared tunnel for bridging VLAN traffic.<br>In tunnel mode, the traffic at the AP is always forwarded through the best path. The APs decide the best path to reach the destination and forward packets accordingly. Setting the VLAN to tunnel mode ensures packets are bridged between local Ethernet ports, any local radios, and tunnels to other APs, wireless controllers, and service platforms. |

**Usage Guidelines**

ACLs can only be used with tunnel or isolated-tunnel modes. They do not work with the local and automatic modes.

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-bridge-vlan-1)#bridging-mode
isolated-tunnel

rfs6000-37FABE(config-profile-default-rfs6000-bridge-vlan-1)#show context
 bridge vlan 1
 bridging-mode isolated-tunnel
 ip igmp snooping
 ip igmp snooping querier
rfs6000-37FABE(config-profile-default-rfs6000-bridge-vlan-1)#
```

**Related Commands**

| | |
|---|---|
| *no* | Resets bridging mode to auto |

### 7.1.10.2.2 captive-portal

*bridge-vlan-mode commands*

Enables IP (IPv4 and IPv6) packet snooping on wired captive portals, and also configures the subnet to snoop. When enabled, IP packets received from wired captive portal clients, on the specified subnet, are snooped to learn IP to MAC mapping.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
captive-portal [ipv4-snooping|ipv6-snooping] subnet <IPv4/M|IPv6/M> {excluded-address <IPv4|IPv6>}
```

**Parameters**

```
• captive-portal [ipv4-snooping|ipv6-snooping] subnet <IPv4/M|IPv6/M> {excluded-address <IPv4|IPv6>}
```

| | |
|---|---|
| captive-portal [ipv4-snooping\| ipv6-snooping] | Enables snooping of IPv4 or IPv6 packets (based on the option selected) for wired captive portal clients |
| subnet <IPv4/M\| IPv6/M> | Enables IPv4 or IPv6 packet snooping on a specified subnet<br>• <IPv4/M\|IPv6/M> – Specify the subnet address in the A.B.C.D/M or X:X::X:X/M format to identify an IPv4 or IPv6 subnet respectively. When specified, this is the IPv4/IPv6 subnet on which IP packets are to be snooped. |
| excluded-address <IPv4\|IPv6> | Optional. Configures the IPv4 or IPv6 address excluded from snooping within the specified IPv4\|IPv6 subnet.<br>• <IPv4\|IPv6> – Specify the IPv4 or IPv6 address. Use this parameter to configure the gateway's address. |

**Example**

```
nx9500-6C8809(config-profile NX9500Test-bridge-vlan-4)#captive-portal ip-snooping
subnet 192.168.13.0/24 excluded-address 192.168.13.7

nx9500-6C8809(config-profile NX9500Test-bridge-vlan-4)#show context
 bridge vlan 4
  captive-portal ip-snooping subnet 192.168.13.0/24 excluded-address 192.168.13.7
  ip igmp snooping
  ip igmp snooping querier
  ipv6 mld snooping
  ipv6 mld snooping querier
nx9500-6C8809(config-profile NX9500Test-bridge-vlan-4)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables IP packet snooping on wired captive portals |

### 7.1.10.2.3 captive-portal-enforcement

*bridge-vlan-mode commands*

Enables auto-enforcement of captive portal rules on this extended VLAN interface. This option is disabled by default.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
captive-portal-enforcement {fall-back}
```

**Parameters**

- `captive-portal-enforcement {fallback}`

| | |
|---|---|
| captive-portal-enforcement | Enables auto-enforcement of captive portal access permission rules to data transmitted over this extended VLAN interface. When enforced, wired network users can pass traffic through the captive portal without being redirected to an authentication page. Authentication instead takes place when the RADIUS server is queried against the wired user's MAC address. If the MAC address is in the RADIUS server's user database, the user is allowed access.<br>A captive portal is an access policy for providing temporary and restrictive access using a standard Web browser. Captive portals capture and re-direct a wired/wireless user's Web browser session to a captive portal login page where the user must enter valid credentials to access the network. |
| fall-back | Optional. If enabling source MAC authentication for Extended VLAN and tunneled traffic on this bridge VLAN, use this option to enforce captive-portal authentication as the fall-back mode of authentication in case MAC authentication fails. |

**Example**

```
nx9500-6C8809(config-profile testAP7602-bridge-vlan-20)#show context
 bridge vlan 20
  captive-portal-enforcement
  ip igmp snooping
  ip igmp snooping querier
  ipv6 mld snooping
  ipv6 mld snooping querier
nx9500-6C8809(config-profile testAP7602-bridge-vlan-20)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables auto-enforcement of captive portal rules on this extended VLAN interface |

### 7.1.10.2.4 description

*bridge-vlan-mode commands*

Configures this extended VLAN's description

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7632, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
description <WORD>
```

**Parameters**

- `description <WORD>`

| | |
|---|---|
| description <WORD> | Configures a description for this VLAN bridge<br>• <WORD> – Enter a description. The description should be unique to the VLAN's specific configuration to help differentiate it from other VLANs with similar configurations. |

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-bridge-vlan-1)#description "This is
a description for the bridged VLAN"

rfs6000-37FABE(config-profile-default-rfs6000-bridge-vlan-1)#show context
 bridge vlan 1
 description "This is a description for the bridged VLAN"
 bridging-mode isolated-tunnel
 ip igmp snooping
 ip igmp snooping querier
rfs6000-37FABE(config-profile-default-rfs6000-bridge-vlan-1)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes VLAN's description |

### 7.1.10.2.5 edge-vlan

*bridge-vlan-mode commands*

Enables the edge VLAN mode. In the edge VLAN mode, a protected port does not forward traffic to another protected port on the same wireless controller or service platform. This feature is enabled by default.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
edge-vlan
```

**Parameters**

None

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-bridge-vlan-1)#edge-vlan
rfs6000-37FABE(config-profile-default-rfs6000-bridge-vlan-1)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables the edge VLAN mode |

### 7.1.10.2.6 firewall

*bridge-vlan-mode commands*

Enables IPv4 firewall on this bridge VLAN interface. This feature is enabled by default.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
firewall
```

**Parameters**

None

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-bridge-vlan-1)#firewall
rfs6000-37FABE(config-profile-default-rfs6000-bridge-vlan-1)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables firewall on this bridge VLAN interface |

### 7.1.10.2.7 http-analyze

*bridge-vlan-mode commands*

Enables the analysis of URLs and data traffic on this Bridge VLAN. When enabled, URLs and data are forwarded to the controller running the HTTP analytics engine.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
http-analyze {filter [images|post|query-string]}
```

**Parameters**

- `http-analyze {filter [images|post|query-string]}`

| | |
|---|---|
| http-analyze filter [images\|post\|query-string] | Enables URL and HTTP data analysis. Optionally use the filter keyword to filter out specific URLs<br>• filter – Optional. Filters out specific URLs<br>  • images – Filters out URLs referring to images<br>  • post – Filters out URLs referring to POSTs<br>  • query-string – Filters out query strings received from URLs |

**Example**

```
rfs4000-229D58(config-device 00-23-68-22-9D-58-bridge-vlan-4)#http-analyze filter
images

rfs4000-229D58(config-device 00-23-68-22-9D-58-bridge-vlan-4)#show context
 bridge vlan 4
  http-analyze filter images
rfs4000-229D58(config-device 00-23-68-22-9D-58-bridge-vlan-4)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables forwarding of URLs and data to the controller running the HTTP analytics engine |

### 7.1.10.2.8 ip

*bridge-vlan-mode commands*

Configures VLAN bridge IP components

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ip [arp|dhcp|igmp]

ip [arp|dhcp] trust

ip igmp snooping {fast-leave|forward-unknown-multicast|last-member-query-count|
mrouter|querier}

ip igmp snooping {fast-leave|forward-unknown-multicast|last-member-query-count
<1-7>}

ip igmp snooping {mrouter [interface|learn]}
ip igmp snooping {mrouter [interface <INTERFACE-LIST>|learn pim-dvmrp]}

ip igmp snooping {querier} {address|max-response-time|timer|version}
ip igmp snooping {querier} {address <IP>|max-response-time <1-25>|timer expiry
<60-300>|version <1-3>}
```

**Parameters**

- `ip [arp|dhcp] trust`

| | |
|---|---|
| ip | Configures the VLAN bridge IP parameters |
| arp trust | Configures the ARP trust parameter. Trusted ARP packets are used to update the DHCP snoop table to prevent IP spoof and arp-cache poisoning attacks. This option is disabled by default.<br>• trust – Trusts ARP responses on the VLAN bridge |
| dhcp trust | Configures the DHCP trust parameter. Uses DHCP packets, from a DHCP server, as trusted and permissible within the access point, wireless controller, or service platform managed network. DHCP packets are used to update the DHCP snoop table to prevent IP spoof attacks. This feature is enabled by default.<br>• trust – Trusts DHCP responses on the VLAN bridge |

- `ip igmp snooping {fast-leave|forward-unknown-multicast|last-member-query-count <1-7>}`

| | |
|---|---|
| ip | Configures the VLAN bridge IP parameters |
| igmp snooping | Configures *Internet Group Management Protocol* (IGMP) snooping parameters. IGMP snooping is enabled by default.<br>IGMP establishes and maintains multicast group memberships for interested members. Multicasting allows a networked device to listen to IGMP network traffic and forward IGMP multicast packets to radios on which the interested hosts are connected. The device also maintains a map of the links that require multicast streams, there by reducing unnecessary flooding of the network with multicast traffic. |

| | |
|---|---|
| fast-leave | Optional. Enables fast leave processing. When enabled, layer 2 LAN interfaces are removed from the IGMP snooping forwarding table entry without initially sending IGMP group-specific queries to the interface. When receiving a group specific IGMPv2 leave message, IGMP snooping removes the interface from the Layer 2 forwarding table entry for that multicast group, unless a multicast router was learned on the port. Fast-leave processing enhances bandwidth management for all hosts on the network. This option is disabled by default.<br>This feature is supported only on the AP7502, AP8232, AP8533 model access points. |
| forward-unknown-multicast | Optional. Enables forwarding of multicast packets from unregistered multicast groups. If disabled, the unknown multicast forward feature is also disabled for individual VLANs. This option is enabled by default. |
| last-member-query-count <1-7> | Optional. Configures the last member query count used in determining the number of group-specific queries sent before removing the snoop entry<br>• <1-7> – Specify the count from 1 - 7. The default value is 2. |

- `ip igmp snooping {mrouter [interface <INTERFACE-LIST>|learn pim-dvmrp]}`

| | |
|---|---|
| ip | Configures the VLAN bridge IP parameters |
| igmp snooping | Configures the IGMP snooping parameters |
| mrouter | Optional. Configures the multicast router parameters |
| interface <INTERFACE-LIST> | Configures the multicast router interfaces. This option is disabled by default.<br>• <INTERFACE-LIST> – Specify a comma-separated list of interface names. |
| learn pim-dvmrp | Configures the multicast router learning protocols. This option is disabled by default.<br>• pim-dvmrp – Enables *Protocol-Independent Multicast* (PIM) and *Distance-Vector Multicast Routing Protocol* (DVMRP) snooping of packets |

- `ip igmp snooping {querier} {address <IP>|max-response-time <1-25>|timer expiry <60-300>|version <1-3>}`

| | |
|---|---|
| ip | Configures the VLAN bridge IP parameters |
| igmp snooping | Configures the IGMP snooping parameters |
| querier | Optional. Configures the IGMP querier parameters. This option is disabled by default.<br>Enables IGMP querier. IGMP snoop querier keeps host memberships alive. It is primarily used in a network where there is a multicast streaming server and hosts subscribed to the server and no IGMP querier present. The access point, wireless controller, or service platform performs the IGMP querier role. An IGMP querier sends out periodic IGMP query packets. Interested hosts reply with an IGMP report packet. IGMP snooping is only conducted on wireless radios. IGMP multicast packets are flooded on wired ports. IGMP multicast packet are not flooded on the wired port. IGMP membership is also learnt on it and only if present, then it is forwarded on that port. |
| address <IP> | Optional. Configures the IGMP querier source IP address. This address is used as the default VLAN querier IP address.<br>• <IP> – Specify the IGMP querier source IP address. |

| | |
|---|---|
| max-response-time <1-25> | Optional. Configures the IGMP querier maximum response time. This option is disabled by default.<br>• <1-25> – Specify the maximum response time from 1 - 25 seconds.<br>The access point, wireless controller, or service platform forwards multicast packets only to radios present in the snooping table. IGMP reports from wired ports are forwarded to the multicast router ports.<br>If no reports are received from a radio, it is removed from the snooping table. The radio then stops receiving multicast packets. |
| timer expiry <60-300> | Optional. Configures the IGMP querier expiry time. The value specified is used as the timeout interval for other querier resources. This option is disabled by default.<br>• expiry – Configures the IGMP querier timeout<br>  • <60-300> – Specify the IGMP querier timeout from 60 - 300 seconds. |
| version <1-3> | Optional. Configures the IGMP version. This option is disabled by default.<br>• <1-3> – Specify the IGMP version. The versions are 1- 3. |

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-bridge-vlan-1)#ip arp trust

rfs6000-37FABE(config-profile-default-rfs6000-bridge-vlan-1)#ip dhcp trust

rfs6000-37FABE(config-profile-default-rfs6000-bridge-vlan-1)#ip igmp snooping
mrouter interface ge1 ge2

rfs6000-37FABE(config-profile-default-rfs6000-bridge-vlan-1)#ip igmp snooping
mrouter learn pim-dvmrp

rfs6000-37FABE(config-profile-default-rfs6000-bridge-vlan-1)#ip igmp snooping
querier max-response-time 24

rfs6000-37FABE(config-profile-default-rfs6000-bridge-vlan-1)#ip igmp snooping
querier timer expiry 100

rfs6000-37FABE(config-profile-default-rfs6000-bridge-vlan-1)#ip igmp snooping
querier version 2

rfs6000-37FABE(config-profile-default-rfs6000-bridge-vlan-1)#show context
bridge vlan 1
  description "This is a description for the bridged VLAN"
  ip arp trust
  ip dhcp trust
  ip igmp snooping
  ip igmp snooping querier
  ip igmp snooping querier version 2
  ip igmp snooping querier max-response-time 24
  ip igmp snooping querier timer expiry 100
  ip igmp snooping mrouter interface ge2 ge1
rfs6000-37FABE(config-profile-default-rfs6000-bridge-vlan-1)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables or reverts the VLAN Ethernet bridge parameters |

### 7.1.10.2.9 ipv6

*bridge-vlan-mode commands*

Configures this VLAN bridge's IPv6 components

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ipv6 [dhcpv6|firewall|mld|nd]

ipv6 dhcpv6 trust

ipv6 firewall

ipv6 mld snooping {forward-unknown-multicast|mrouter|querier}

ipv6 mld snooping {forward-unknown-multicast}

ipv6 mld snooping {mrouter [interface|learn]}
ipv6 mld snooping {mrouter [interface <INTERFACE-LIST>|learn pim-dvmrp]}

ipv6 mld snooping {querier} {max-response-time|timer|version}
ipv6 mld snooping {querier} {max-response-time <1-25000>|timer expiry <60-300>|
version <1-2>}

ipv6 nd raguard
```

**Parameters**

- `ipv6 dhcpv6 trust`

| | |
|---|---|
| ipv6 | Configures the VLAN bridge IPv6 parameters |
| dhcpv6 trust | Enables the DHCPv6 trust option. When enabled all DHCPv6 responses are trusted on this bridge VLAN. This option is enabled by default.<br>• trust – Trusts DHCPv6 responses on this bridge VLAN |

- `ipv6 firewall`

| | |
|---|---|
| ipv6 | Configures the VLAN bridge IPv6 parameters |
| firewall | Enables IPv6 firewall on this bridge VLAN. This option is enabled by default.<br>Devices utilizing IPv6 addressing require firewall protection unique to IPv6 traffic.<br>IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the *neighbor discovery* (ND) protocol via ICMPv6 router discovery messages. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters. Routers respond to such a request with a *router advertisement* (RA) packet that contains Internet layer configuration parameters. |

- `ipv6 mld snooping {forward-unknown-multicast}`

| | |
|---|---|
| ipv6 | Configures the VLAN bridge IPv6 parameters |

| | |
|---|---|
| mld snooping | Configures *Multicast Listener Discovery Protocol* (MLD) snooping parameters<br>MLD snooping enables a access point, wireless controller, or service platform to examine MLD packets and make forwarding decisions based on the content. MLD is used by IPv6 devices to discover devices wanting to receive multicast packets destined for specific multicast addresses. MLD uses multicast listener queries and multicast listener reports to identify which multicast addresses have listeners and join multicast groups.<br>MLD snooping caps the flooding of IPv6 multicast traffic on controller, service platform or access point VLANs. When enabled, MLD messages between hosts and multicast routers are examined to identify the hosts receiving multicast group traffic. The access point, wireless controller, or service platform forward multicast traffic only to those interfaces connected to interested receivers instead of flooding traffic to all interfaces.<br>This option is enabled by default. |
| forward-unknown-multicast | Optional. Enables forwarding of multicast packets from unregistered multicast groups. If disabled, the unknown multicast forward feature is also disabled for individual VLANs. This option is enabled by default. |

- `ipv6 mld snooping {mrouter [interface <INTERFACE-LIST>|learn pim-dvmrp]}`

| | |
|---|---|
| ipv6 | Configures the VLAN bridge IPv6 parameters |
| mld snooping | Configures MLD snooping parameters. This option is enabled by default. |
| mrouter | Optional. Configures the multicast router parameters, such as interfaces and learning protocol used. |
| interface <INTERFACE-LIST> | Configures the multicast router interfaces. This option is disabled by default.<br>• <INTERFACE-LIST> – Specify a comma-separated list of interface names. |
| learn pim-dvmrp | Configures the multicast router learning protocols. This option is disabled by default.<br>• pim-dvmrp – Enables PIM and DVMRP snooping of packets |

- `ipv6 mld snooping {querier} {max-response-time <1-25000>|timer expiry <60-300>|version <1-2>}`

| | |
|---|---|
| ipv6 | Configures the VLAN bridge IPv6 parameters |
| mld snooping | Configures IPv6 MLD snooping parameters. This option is disabled by default. |
| querier | Optional. Enables and configures the MLD querier parameters. When enabled, the device (access point, wireless controller, and service platform) sends query messages to discover which network devices are members of a given multicast group. This option is disabled by default. |
| max-response-time <1-25000> | Optional. Configures the IPv6 MLD querier's maximum response time. This option is disabled by default.<br>• <1-25000> – Specify the maximum response time from 1 - 25000 milliseconds. |
| timer expiry <60-300> | Optional. Configures the IPv6 MLD other querier's timeout. This option is disabled by default.<br>• <60-300> – Specify the MLD other querier's timeout from 60 - 300 seconds. |
| version <1-2> | Optional. Configures the IPv6 MLD querier version. This option is disabled by default.<br>• <1-2> – Specify the MLD version. The versions are 1- 2. |

- `ipv6 nd raguard`

| | |
|---|---|
| ipv6 | Configures the VLAN bridge IPv6 parameters |
| nd raguard | Allows *router advertisement* (RA) or ICMPv6 redirects on this VLAN bridge. This option is enabled by default. |

**Example**

```
rfs7000-37FABE(config-profile test-bridge-vlan-2)#ipv6 dhcpv6 trust

rfs7000-37FABE(config-profile test-bridge-vlan-2)#ipv6 firewall

rfs7000-37FABE(config-profile test-bridge-vlan-2)#ipv6 mld snooping forward-
unknown-multicast

rfs7000-37FABE(config-profile test-bridge-vlan-2)#ipv6 mld snooping mrouter
interface ge1 ge2

rfs7000-37FABE(config-profile test-bridge-vlan-2)#ipv6 mld snooping mrouter learn
pim-dvmrp

rfs7000-37FABE(config-profile test-bridge-vlan-2)#ipv6 mld snooping querier max-
response-time 20000

rfs7000-37FABE(config-profile test-bridge-vlan-2)#ipv6 mld snooping querier timer
expiry 200

rfs7000-37FABE(config-profile test-bridge-vlan-2)#ipv6 mld snooping querier
version 2

rfs7000-37FABE(config-profile test-bridge-vlan-2)#show context
 bridge vlan 2
  ip igmp snooping
  ip igmp snooping querier
  ipv6 mld snooping
  ipv6 mld snooping querier
  ipv6 mld snooping mrouter interface ge2 ge1
  ipv6 mld snooping querier version 2
  ipv6 mld snooping querier max-response-time 20000
  ipv6 mld snooping querier timer expiry 200
rfs7000-37FABE(config-profile test-bridge-vlan-2)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables or reverts the VLAN Ethernet bridge IPV6 parameters |

### 7.1.10.2.10 l2-tunnel-broadcast-optimization

*bridge-vlan-mode commands*

Enables broadcast optimization on this bridge VLAN. L2 Tunnel Broadcast Optimization prevents flooding of ARP packets over the virtual interface. Based on the learned information, ARP packets are filtered at the wireless controller level.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
l2-tunnel-broadcast-optimization
```

**Parameters**

None

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-bridge-vlan-1)#l2-tunnel-broadcast
-optimization

rfs6000-37FABE(config-profile-default-rfs6000-bridge-vlan-1)#show context
 bridge vlan 1
  description "This is a description for the bridged VLAN"
  l2-tunnel-broadcast-optimization
  bridging-mode isolated-tunnel
  ip arp trust
  ip dhcp trust
  ip igmp snooping
  ip igmp snooping querier
  ip igmp snooping mrouter interface ge2 ge1
  ip igmp snooping querier version 2
  ip igmp snooping querier max-response-time 24
  ip igmp snooping querier timer expiry 100
rfs6000-37FABE(config-profile-default-rfs6000-bridge-vlan-1)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables L2 tunnel broadcast optimization |

### 7.1.10.2.11 mac-auth

*bridge-vlan-mode commands*

Enables source MAC authentication for Extended VLAN and tunneled traffic (MiNT and L2TPv3) on this bridge VLAN

**NOTE:** If enabling MAC authentication, ensure that an AAA policy is configured and for enforcing MAC Authentication.

**Supported in the following platforms:**

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
mac-auth {attempts <1-5>|throttle <0-255>}
```

**Parameters**

- `mac-auth {attempts <1-5>|throttle <0-255>}]`

| | |
|---|---|
| mac-auth | Enables MAC Authentication |
| attempts <1-5> | Optional. Configures the maximum number of retries allowed for MAC authentication requests.<br>• <1-5> – Specify the maximum allowed authentication retries from 1 - 5. The default is 3. |
| throttle <0-255> | Optional. Configures the throttle value for MAC authentication requests<br>• <0-255> – Specify the MAC authentication request throttle value from 0 -255. The default is 64. |

**Usage Guidelines Applying AAA Policy for MAC Authentication**

To enable MAC authentication,

- Create an AAA policy.
  nx9500-6C8809(config)#aaa-policy MAC-Auth
- Use the AAA policy on the device for MAC Authentication.
  nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#mac-auth use aaa-policy MAC-Auth
- In the bridge VLAN context, enable MAC Authentication,
  nx9500-6C8809(config-device B4-C7-99-6C-88-09-bridge-vlan-20)#mac-auth
- Optionally, configure the following MAC Authentication parameters. If not specified, default values are applied.
  nx9500-6C8809(config-device B4-C7-99-6C-88-09-bridge-vlan-20)#mac-auth attempts 2
  nx9500-6C8809(config-device B4-C7-99-6C-88-09-bridge-vlan-20)#mac-auth throttle 100

**Usage Guidelines Enabling Fall-back Captive Portal Authentication**

To enable fall-back captive-portal authentication on the bridge VLAN,

- apply a captive-portal policy to the bridge VLAN.
  nx9500-6C8809(config-device B4-C7-99-6C-88-09-bridge-vlan-20)#use captive-portal test

- enable captive-portal authentication as the fall-back authentication mode.
  nx9500-6C8809(config-device B4-C7-99-6C-88-09-bridge-vlan-20)#captive-portal-enforcement fall-back

**Example**

```
nx9500-6C8809(config-profile testNX9000-bridge-vlan-20)#mac-auth attempts 2

nx9500-6C8809(config-profile testNX9000-bridge-vlan-20)#mac-auth throttle 80

nx9500-6C8809(config-profile testNX9000-bridge-vlan-20)#show context
 bridge vlan 20
  mac-auth attempts 2
  mac-auth throttle 80
  ip igmp snooping
  ip igmp snooping querier
  ipv6 mld snooping
  ipv6 mld snooping querier
nx9500-6C8809(config-profile testNX9000-bridge-vlan-20)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables MAC authentication for Extended VLAN and Tunneled traffic on this bridge VLAN |

### 7.1.10.2.12 l2-tunnel-forward-additional-packet-types

*bridge-vlan-mode commands*

Enables forwarding of *Wireless Network Management Protocol* (WNMP) packets across L2 tunnels. Under normal circumstances, if L2 tunnel broadcast optimization is enabled. WNMP packets are not forwarded across the L2 tunnels. Use this option to enable the forwarding of only WNMP packets.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
l2-tunnel-forward-additional-packet-types wnmp
```

**Parameters**

None

**Example**

```
nx9500-6C8809(config-profile testNX9000-bridge-vlan-1)#l2-tunnel-forward-
additional-packet-types wnmp

nx9500-6C8809(config-profile testNX9000-bridge-vlan-1)#show context
 bridge vlan 1
  l2-tunnel-broadcast-optimization
  l2-tunnel-forward-additional-packet-types wnmp
  ip igmp snooping
  ip igmp snooping querier
  ipv6 mld snooping
  ipv6 mld snooping querier
nx9500-6C8809(config-profile testNX9000-bridge-vlan-1)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables WNMP packet forwarding across L2 tunnel |

### 7.1.10.2.13 no

*bridge-vlan-mode commands*

Negates a command or reverts settings to their default. The no command, when used in the bridge VLAN mode, negates the VLAN bridge settings or reverts them to their default.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
no [bridging-mode|captive-portal|captive-portal-enforcement|description|edge-
vlan|firewall|http-analyze|ip|ipv6|l2-tunnel-broadcast-optimization|l2-tunnel-
forward-additional-packet-types|mac-auth|stateful-packet-inspection-l2|tunnel|
tunnel-over-level2|use]

no [bridging-mode|captive-portal-enforcement|description|edge-vlan|firewall|
l2-tunnel-broadcast-optimization|l2-tunnel-forward-additional-packet-types|
mac-auth|stateful-packet-inspection-l2|tunnel-over-level2]

no captive-portal [ip-snooping|ipv6-snooping] subnet <IPv4/M|IPv6/M> {excluded-
address <IPv4|IPv6>}

no http-analyze {filter [images|post|query-string]}

no ip [arp|dhcp|igmp]

no ip [arp|dhcp] trust
no ip igmp snooping {fast-leave|forward-unknown-multicast|last-member-query-
count|mrouter|querier}
no ip igmp snooping {forward-unknown-multicast}
no ip igmp snooping {mrouter [interface <INTERFACE-LIST>|learn pin-dvmrp]}
no ip igmp snooping {querier} {address|max-response-time|timer expiry|version}

no ipv6 [dhcpv6|firewall|mld|nd]

no ipv6 dhcpv6 trust
no ipv6 firewall
no ipv6 mld snooping {forward-unknown-multicast}
no ipv6 mld snooping {mrouter [interface <INTERFACE-LIST>|learn pin-dvmrp]}
no ipv6 mld snooping {querier} {max-response-time|timer expiry|version}
no ipv6 nd raguard

no tunnel [rate-limit level2|unknown-unicast]

no use [application-policy|captive-portal|ip-access-list|ipv6-access-list|
mac-access-list|url-list] tunnel out
```

**Parameters**

- no <PARAMETERS>

| | |
|---|---|
| no <PARAMETERS> | Resets or reverts this bridge VLAN's settings based on the parameters passed |

**Example**

The following example displays bridge VLAN 20 settings before the ‘no’ commands are executed:

```
nx9500-6C8809(config-profile testNX9500-bridge-vlan-20)#show context
 bridge vlan 20
  ip igmp snooping
  ip igmp snooping querier
  ipv6 mld snooping
  ipv6 mld snooping querier
nx9500-6C8809(config-profile testNX9500-bridge-vlan-20)#

nx9500-6C8809(config-profile testNX9500-bridge-vlan-20)#no ip igmp snooping
nx9500-6C8809(config-profile testNX9500-bridge-vlan-20)#no ipv6 mld snooping
```

The following example displays bridge VLAN 20 settings after the ‘no’ commands are executed:

```
nx9500-6C8809(config-profile testNX9500-bridge-vlan-20)#show context
 bridge vlan 20
  no ip igmp snooping
  ip igmp snooping querier
  no ipv6 mld snooping
  ipv6 mld snooping querier
nx9500-6C8809(config-profile testNX9500-bridge-vlan-20)#


nx9500-6C8809(config-profile TestProfileNX9500-bridge-vlan-20)#show context
bridge vlan 20
  mac-auth attempts 2
  mac-auth throttle 80
  ip igmp snooping
  ip igmp snooping querier
  ipv6 mld snooping
  ipv6 mld snooping querier

nx9500-6C8809(config-profile TestProfileNX9500-bridge-vlan-20)#

nx9500-6C8809(config-profile TestProfileNX9500-bridge-vlan-20)#no mac-auth

nx9500-6C8809(config-profile TestProfileNX9500-bridge-vlan-20)#show context
 bridge vlan 20
  ip igmp snooping
  ip igmp snooping querier
  ipv6 mld snooping
  ipv6 mld snooping querier
nx9500-6C8809(config-profile TestProfileNX9500-bridge-vlan-20)#
```

### 7.1.10.2.14 stateful-packet-inspection-l2

*bridge-vlan-mode commands*

Enables a *stateful packet inspection* (SPI) at the layer 2 firewall. SPI, also referred to as dynamic packet filtering, is a security feature that tracks the operating state and characteristics of network connections traversing it. It distinguishes legitimate packets for different types of connections, and only allows packets matching a known active connection to pass.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
stateful-packet-inspection-l2
```

**Parameters**

None

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-bridge-vlan-1)#stateful-packet-ins
inspection-l2
rfs6000-37FABE(config-profile-default-rfs6000-bridge-vlan-1)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables stateful packet inspection at the layer 2 firewall |

### 7.1.10.2.15 tunnel

*bridge-vlan-mode commands*

Enables tunneling of unicast messages, to unknown MAC destinations, on the selected VLAN bridge

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
tunnel [rate-limit|unknown-unicast]

tunnel rate-limit level2 rate <50-1000000> max-burst-size <2-1024> {red-threshold
[background <0-100>|best-effort <0-100>|video <0-100>|voice <0-100>]}

tunnel unknown-unicast
```

**Parameters**

- `tunnel rate-limit level2 rate <50-1000000> max-burst-size <2-1024> {red-threshold [background <0-100>|best-effort <0-100>|video <0-100>|voice <0-100>]}`

| | |
|---|---|
| tunnel rate-limit level2 rate <50-1000000> max-burst-size <2-1024> | Configures a rate-limit parameters (max-burst-size and rate) for tunneled VLAN traffic over level 2 MiNT links<br>• rate – Optional. Configures the data rate, in kilobits per second, for the incoming and outgoing extended VLAN traffic tunneled over MiNT level 2 links<br>• <50-1000000> – Specify a value from 50 - 1000000 Kbps. The default is 5000 Kbps.<br>• max-burst-size – Optional. Configures the maximum burst size<br>• <2-1024> – Specify the maximum burst size from 2 - 1024 kbytes. The default is 320 kbytes.<br>After specifying the max-burst-size, optionally specify the red-threshold value for the different traffic types. The red-threshold is configured as a % of the specified max-burst-size.<br>• red-threshold – Optional. Configures the *random early detection* (red) threshold for the different traffic types<br>• background – Configures the red-threshold for low priority traffic from 0 - 100. The default is 50% of the specified max-burst-size.<br>• best-effort – Configures the red-threshold for normal priority traffic from 0 - 100. The default is 50% of the specified max-burst-size.<br>• video – Configures the red-threshold for video traffic from 0 - 100. The default is 25% of the specified max-burst-size.<br>• voice – Configures the red-threshold for voice traffic from 0 - 100. The default is 0% of the specified max-burst-size. |

- `tunnel unknown-unicast`

| | |
|---|---|
| tunnel unknown-unicast | Enables tunneling of unicast packets destined for unknown MAC addresses |

**Example**

```
rfs6000-37FABE(config-profile TestAP81xx-bridge-vlan-1)#tunnel unknown-unicast

rfs6000-37FABE(config-profile TestAP81xx-bridge-vlan-1)#no tunnel unknown-unicast

rfs6000-37FABE(config-profile TestAP81xx-bridge-vlan-1)#show context
 bridge vlan 1
  ip igmp snooping
  ip igmp snooping querier
  no tunnel unknown-unicast
rfs6000-37FABE(config-profile TestAP81xx-bridge-vlan-1)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables tunneling of unicast messages, to unknown MAC destinations, on the selected VLAN bridge |

### 7.1.10.2.16 tunnel-over-level2

*bridge-vlan-mode commands*

Enables extended VLAN (tunneled VLAN) traffic over level 2 MiNT links. This option is disabled by default.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
tunnel-over-level2
```

**Parameters**

None

**Example**

```
rfs4000-229D58(config-profile testRFS4000-bridge-vlan-1)#tunnel-over-level2

rfs4000-229D58(config-profile testRFS4000-bridge-vlan-1)#show context
 bridge vlan 1
  description "This is a description for the bridged VLAN"
  l2-tunnel-broadcast-optimization
  bridging-mode isolated-tunnel
  tunnel-over-level2
  ip arp trust
  ip dhcp trust
  ip igmp snooping
  ip igmp snooping querier
rfs4000-229D58(config-profile testRFS4000-bridge-vlan-1)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables extended VLAN traffic over level 2 MiNT links |

### 7.1.10.2.17 use

*bridge-vlan-mode commands*

Associates a captive-portal, access control list (IPv4, IPv6, or MAC), and/or a URL filter with this bridge VLAN

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
use [application-policy|captive-portal|ip-access-list|ipv6-access-list|mac-access-list|url-filter]

use application-policy <APP-POLICY-NAME>

use captive-portal <CAPTIVE-PORTAL-NAME>

use [ip-access-list|ipv6-access-list|mac-access-list] tunnel out <IP/ipv6/MAC-ACCESS-LIST-NAME>

use url-filter <URL-FILTER-NAME>
```

**Parameters**

- `use application-policy <APP-POLICY-NAME>`

| | |
|---|---|
| use application-policy <APP-POLICY-NAME> | Enforces application detection on this VLAN bridge<br>• <APP-POLICY-NAME> – Specify the application policy name (should be existing and configured).<br>• For more information on application definitions and application policies, see *application* and *application-policy*. |

- `use captive-portal <CAPTIVE-PORTAL-NAME>`

| | |
|---|---|
| use captive-portal | Applies an existing captive portal configuration to restrict access to the bridge VLAN configuration<br>A captive portal is an access policy for providing temporary and restrictive access using a standard Web browser. Captive portals provide authenticated access by capturing and re-directing a wireless user's Web browser session to a captive portal login page where the user must enter valid credentials to access to the network. Once logged into the captive portal, additional terms and agreement, welcome, fail, and no-service pages provide the administrator with a number of options on captive portal screen flow and user appearance.<br>• <CAPTIVE-PORTAL-NAME> – Specify the captive portal name. |

- `use [ip-access-list|ipv6-access-list|mac-access-list] tunnel out <IP/IPv6/MAC-ACCESS-LIST-NAME>`

| | |
|---|---|
| use | Sets this VLAN bridge policy to use an IPv4/IPv6 access list or a MAC access list |
| ip-access-list | Associates a pre-configured IPv4 access list with this VLAN-bridge interface |
| ipv6-access-list | Associates a pre-configured IPv6 access list with this VLAN-bridge interface |
| mac-access-list | Associates a pre-configured MAC access list with this VLAN- bridge interface |

| | |
|---|---|
| tunnel out <IP/IPv6/MAC-ACCESS-LIST-NAME> | The following keywords are common to the 'IPv4/IPv6 access list' and 'MAC access list' parameters:<br>• tunnel – Applies IPv4/IPv6 access list or MAC access list to all packets going into the tunnel<br>• out – Applies IPv4/IPv6 access list or MAC access list to all outgoing packets<br>• <IP/IPv6/MAC-ACCESS-LIST-NAME> – Specify the IP/IPv6 access list or MAC access list name. |

- `use url-filter <URL-FILTER-NAME>`

| | |
|---|---|
| use url-filter | Sets this VLAN bridge to use a URL filter |
| <URL-FILTER-NAME> | Specify the URL filter name. It should be existing and configured.<br>This option enforces URL filtering on the VLAN bridge. |

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-bridge-vlan-1)#use mac-access-list
tunnel out PERMIT-ARP-AND-IPv4

rfs6000-37FABE(config-profile-default-rfs6000-bridge-vlan-1)#show context
 bridge vlan 1
  ip igmp snooping
  ip igmp snooping querier
  use mac-access-list tunnel out PERMIT-ARP-AND-IPv4
rfs6000-37FABE(config-profile-default-rfs6000-bridge-vlan-1)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables or reverts VLAN Ethernet bridge settings |

## 7.1.11 captive-portal

*Profile Config Commands*

Configures captive portal advanced Web page uploads on this profile

A captive portal is a means of providing guests temporary and restrictive access to the controller managed wireless network. A captive portal provides secure authenticated controller access by capturing and re-directing a wireless user's Web browser session to a captive portal login page, where the user must enter valid credentials. Once the user is authenticated and logged into the controller managed network, additional agreement, welcome, and fail pages provide the administrator with options to control the captive portal's screen flow and user appearance.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
captive-portal page-upload count <1-20>
```

**Parameters**

- `captive-portal page-upload count <1-20>`

| | |
|---|---|
| page-upload | Enables captive portal advanced Web page upload |
| count <1-20> | Sets the maximum number of APs that can be uploaded concurrently<br>• <1-20> – Set a value from 1 - 20. The default is 10. |

**Example**

```
nx9500-6C8809(config-profile-testNX9500)#captive-portal page-upload count 15

nx9500-6C8809(config-profile-testNX9500)#show context include-factory | include
captive-portal
 captive-portal page-upload count 15
  no captive-portal-enforcement
  no captive-portal-enforcement
  no captive-portal-enforcement
  no captive-portal-enforcement
  no captive-portal-enforcement
  no captive-portal-enforcement
 service captive-portal-server connections-per-ip 3
nx9500-6C8809(config-profile-testNX9500)#
```

## 7.1.12 cdp

*Profile Config Commands*

Enables *Cisco Discovery Protocol* (CDP), a proprietary data link layer network protocol implemented in Cisco networking equipment and used to share network information amongst different vendor wireless devices

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
cdp [holdtime|run|timer]

cdp [holdtime <10-1800>|run|timer <5-900>]
```

**Parameters**

- `cdp [holdtime <10-1800>|run|timer <5-900>]`

| | |
|---|---|
| holdtime <10-1800> | Specifies the holdtime after which transmitted packets are discarded<br>• <10-1800> – Specify a value from 10 - 1800 seconds. The default is 180 seconds. |
| run | Enables CDP sniffing and transmit globally. This feature is enabled by default. |
| timer <5-900> | Specifies the interval, in seconds, between successive CDP packet transmission<br>• <5-900> – Specify a value from 5 - 900 seconds. The default is 60 seconds. |

**Example**

```
rfs6000-37FABE(config profile-default-rfs6000)#cdp run

rfs6000-37FABE(config profile-default-rfs6000)#cdp holdtime 1000

rfs7000-37FABE(config profile-default-rfs6000)#cdp timer 900

rfs6000-37FABE(config-profile-default-rfs6000)#show context
profile rfs6000 default-rfs6000
 bridge vlan 1
  no edge-vlan
  l2-tunnel-broadcast-optimization
 ..........................................................
  qos trust 802.1p
 interface pppoe1
 use firewall-policy default
 cdp holdtime 1000
 cdp timer 900
 service pm sys-restart
 router ospf
rfs6000-37FABE(config-profile-default-rfs6000)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables CDP on this profile |

## 7.1.13 cluster

*Profile Config Commands*

Sets the cluster configuration

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
cluster [force-configured-state|force-configured-state-delay|handle-stp|master-priority|member|mode|name|radius-counter-db-sync-time]

cluster [force-configured-state|force-configured-state-delay <3-1800>|handle-stp|master-priority <1-255>]

cluster member [ip|vlan]
cluster member [ip <IP> {level [1|2]}|vlan <1-4094>]

cluster mode [active|standby]

cluster name <CLUSTER-NAME>

cluster radius-counter-db-sync-time <1-1440>
```

**Parameters**

```
• cluster [force-configured-state|force-configured-state-delay <3-1800>|handle-stp|master-priority <1-255>]
```

| | |
|---|---|
| force-configured-state | Forces adopted APs to auto revert when a failed wireless controller or service platform (in a cluster) restarts<br>When an active controller (wireless controller, or service platform) fails, a standby controller in the cluster takes over APs adopted by the failed active controller. If the failed active controller were to restart, it starts a timer based on the 'force-configured-state-delay' interval specified. At the expiration of this interval, the standby controller releases all adopted APs and goes back to a monitoring mode. If the active controller fails during this interval, the 'force-configured-state-delay' timer is stopped. The timer restarts as soon as the active controller comes back up.<br>This feature is disabled by default. |
| force-configured-state-delay <3-1800> | Forces cluster transition to the configured state after a specified interval<br>• <3-1800> – Specify a delay from 3 - 1800 minutes. The default is 5 minutes.<br>This is the interval a standby controller waits before releasing adopted APs when a failed primary controller becomes active again. |
| handle-stp | Enables *Spanning Tree Protocol* (STP) convergence handling. This feature is disabled by default.<br>In layer 2 networks, this protocol is enabled to prevent network looping. If enabled, the network forwards data only after STP convergence. Enabling STP convergence delays the redundancy state machine execution until the STP convergence is completed (the standard protocol value for STP convergence is 50 seconds). Delaying the state machine is important to load balance APs at startup. |

| | |
|---|---|
| master-priority <1-255> | Configures cluster master priority<br>• <1-255> – Specifies cluster master election priority. Assign a value from 1 - 255. Higher the value higher is the precedence. The default is 128.<br>In a cluster environment one device from the cluster is elected as the cluster master. A device's master priority value decides the device's priority to become cluster master. |

- `cluster member [ip <IP> {level [1|2]}|vlan <1-4094>]`

| | |
|---|---|
| member | Adds a member to the cluster. It also configures the cluster VLAN where members can be reached. |
| ip <IP> level [1\|2] | Adds IP address of the new cluster member<br>• <IP> – Specify the IP address.<br>• level – Optional. Configures routing level for the new member. Select one of the following routing levels:<br>• 1 – Level 1, local routing<br>• 2 – Level 2, In-site routing |
| vlan <1-4094> | Configures the cluster VLAN where members can be reached<br>• <1-4094> – Specify the VLAN ID from 1- 4094. |

- `cluster mode [active|standby]`

| | |
|---|---|
| mode [active\|standby] | Configures cluster member's mode as active or standby<br>• active – Configures cluster mode as active. This is the default setting.<br>• standby – Configures cluster mode as standby<br>A member can be in either an Active or Standby mode. All active member controllers can adopt access points. Standby members only adopt access points when an active member has failed or sees an access point not adopted by a controller. |

- `cluster name <CLUSTER-NAME>`

| | |
|---|---|
| name <CLUSTER-NAME> | Configures the cluster name<br>• <CLUSTER-NAME> – Specify the cluster name. |

- `cluster radius-counter-db-sync-time <1-1440>`

| | |
|---|---|
| radius-counter-db-sync-time <1-1440> | Configures the interval, in minutes, at which the RADIUS counter database is synchronized with the dedicated NTP server resource.<br>• <1-1440> – Specify a value from 1 - 1440 minutes. The default is 5 minutes.<br>Use the *show > cluster > configuration* command to view RADIUS counter DB sync time. |

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000)#cluster name cluster1

rfs6000-37FABE(config-profile-default-rfs6000)#cluster member ip 172.16.10.3

rfs6000-37FABE(config-profile-default-rfs6000)#cluster mode active

rfs6000-37FABE(config-profile-default-rfs6000)#show context
profile rfs6000 default-rfs6000
 bridge vlan 1
  description Vlan1
.....................................................................
 cluster name cluster1
 cluster member ip 172.16.10.3
 cluster member vlan 1
rfs6000-37FABE(config-profile-default-rfs6000)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes cluster member |

## 7.1.14 configuration-persistence

*Profile Config Commands*

Enables configuration persistence across reloads. This option is enabled by default.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
configuration-persistence {auto|secure}
```

**Parameters**

- `configuration-persistence {auto|secure}`

| | |
|---|---|
| auto | Optional. Assigns default value based on the device type |
| secure | Optional. Ensures parts of a file that contain security information are not written during a reload |

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000)#configuration-persistence secure

rfs6000-37FABE(config-profile-default-rfs6000)#show context
profile rfs6000 default-rfs6000
 bridge vlan 1
  no edge-vlan
  ip igmp snooping
  no ip igmp snooping unknown-multicast-fwd
  no ip igmp snooping mrouter learn pim-dvmrp
  autoinstall configuration
 autoinstall firmware
 ..............................................................................
 cluster name cluster1
 cluster member ip 1.2.3.4 level 2
 cluster member ip 172.16.10.3
 cluster member vlan 4094
 cluster handle-stp
 cluster force-configured-state
  holdtime 1000
  timer 900
 configuration-persistence secure
rfs6000-37FABE(config-profile-default-rfs6000)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables automatic write up of startup configuration file |

## 7.1.15 controller

*Profile Config Commands*

Configures the WiNG controller (wireless controller or service platform) adoption settings

Adoption is the process a controller or service platform uses to discover available access points and/or peer controllers/service platforms, establish an association and provision the adopted device. Adoption settings are configurable and supported within a profile and applied to all devices supported by the profile.

Use this command to add a controller to a pool and group. This command also enables and disables adoption on controllers, and specifies the device types that can be adopted by a controller.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
controller [adopted-devices|adoption|group|hello-interval|vlan|host]

controller adopted-devices [aps {controllers}|controllers {aps}|external-devices|
external-devices-monitoring-only]hel

controller adoption

controller [group <CONTROLLER-GROUP-NAME>|vlan <1-4094>]

controller hello-interval <1-120> adjacency-hold-time <2-600>

controller host [<IPv4>|<IPv6>|<HOSTNAME>] {ipsec-secure|level|pool|remote-vpn-
client}

controller host [<IPv4>|<IPv6>|<HOSTNAME>] {ipsec-secure} {gw [<IP>|<HOSTNAME>]}

controller host [<IPv4>|<IPv6>|<HOSTNAME>] {level [1|2]|pool <1-2> level [1|2]}
{ipsec-secure {gw [<IP>|<HOSTNAME>]}|remote-vpn-client}

controller host [<IPv4>|<IPv6>|<HOSTNAME>] {remote-vpn-client}
```

**Parameters**

```
• controller adopted-devices [aps {controllers}|controllers {aps}|external-
devices|external-devices-monitoring-only]
```

| | |
|---|---|
| controller | Configures the WLAN's controller adoption settings |
| adopted-devices | Configures the types of device (AP/controller) this controller can adopt |
| aps {controllers} | Enables the adoption of network access points by this controller. This option is enabled by default.<br>• controllers – Optional. Enables the adoption of peer controllers by this controller<br>All adopted devices (referred to as adoptee) receive complete configuration from the adopting controller (referred to as adopter). |

| | |
|---|---|
| controllers {aps} | Enables the adoption of peer controllers by this controllers<br>• aps – Optional. Enables the adoption of network access points by this controller<br>A controller cannot be configured as an adoptee and an adopter simultaneously. In other words, an adopted controller (adoptee) cannot be configured to adopt another controller.<br>Use the *no > controller > adopted-devices* command to remove this setting. |
| external-devices | Enables adoption of external devices by this controller. This option is disabled by default.<br>When enabled, a WiNG controller can adopt and manage T5 controllers and EX3500 switches (using the IPX operating system) within a WiNG managed device subnet. This setting is disabled by default.<br>To disable T5 or EX3500 adoption, use the *no > controller > external-devices* command.<br>This feature is supported only on RFS4000, NX9500, NX9510, NX9600, and VX9000 platforms. |
| external-devices-monitoring-only | Enables only monitoring of external devices by this controller or service platform. This option is disabled by default. |

- `controller adoption`

| | |
|---|---|
| controller adoption | Enables the adoption of the logged device (wireless controller or service platform) by other controllers. This option is disabled by default.<br>Use the *no > controller > adoption* command to disable adoption. |

- `controller [group <CONTROLLER-GROUP-NAME>|vlan <1-4094>]`

| | |
|---|---|
| controller | Configures the WLAN's controller adoption settings |
| group <CONTROLLER-GROUP-NAME> | Configures the wireless controller or service platform group<br>• <CONTROLLER-GROUP-NAME> – Specify the wireless controller or service platform group name. |
| vlan <1-4094> | Configures the wireless controller or service platform VLAN<br>• <1-4094> – Specify the VLAN ID from 1 - 4094. |

- `controller hello-interval <1-120> adjacency-hold-time <2-600>`

| | |
|---|---|
| controller | Configures the WLAN's controller settings |
| hello-interval <1-120> | Configures the hello-interval in seconds. This is the interval between consecutive hello packets exchanged between AP and wireless controller or service platform.<br>• <1-120> – Specify a value from 1 - 120 seconds. |
| adjacency-hold-time <2-600> | Configures the adjacency hold time in seconds. This is the time since the last received hello packet, after which the adjacency between wireless controller or service platform and AP is lost, and the link is re-established.<br>• <2-600> – Specify a value from 2 - 600 seconds. |

- `controller host [<IPv4>|<IPv6>|<HOSTNAME>] {ipsec-secure} {gw [<IP>|<HOSTNAME>]}`

| | |
|---|---|
| controller | Configures the WLAN's controller adoption settings |

| | |
|---|---|
| host [<IPv4>\|<IPv6>\|<HOSTNAME>] | Configures wireless controller or service platform's IPv4/IPv6 address or hostname<br>• <IPv4> – Configures wireless controller or service platform's IPv4 address<br>• <IPv6> – Configures wireless controller or service platform's IPv6 address<br>• <HOSTNAME> – Configures wireless controller or service platform's hostname |
| ipsec-secure {gw [<IP>\|<HOSTNAME>]} | Optional. Enables Internet Protocol Security (IPSec) peer authentication on the connection (link) between the adopting devices. This option is disabled by default.<br>• gw – Optional. Specifies a IPSec gateway other than the wireless controller or service platform<br>• <IP> – Use this option to specify the IPSec gateway's IP address.<br>• <HOSTNAME> – Use this option to specify the IPSec gateway's hostname.<br>If the gateway's IP address or hostname is not specified, the system assumes the logged controller as the IPSec gateway. |

• `controller host [<IPv4>|<IPv6>|<HOSTNAME>] {level [1|2]|pool <1-2> level [1|2]} {ipsec-secure {gw [<IP>|<HOSTNAME>]}|remote-vpn-client}`

| | |
|---|---|
| controller | Configures the WLAN's controller adoption settings |
| host [<IPv4>\|<IPv6>\|<HOSTNAME>] | Configures wireless controller or service platform's IPv4/IPv6 address or name<br>• <IPv4> – Configures wireless controller or service platform's IPv4 address<br>• <IPv6> – Configures wireless controller or service platform's IPv6 address<br>• <HOSTNAME> – Configures wireless controller or service platform's name |
| level [1\|2] | The following keywords are common to the 'IP', 'IPv6', and 'hostname' parameters:<br>Optional. After providing the wireless controller or service platform's address, optionally select one of the following routing levels:<br>• 1 – Optional. Level 1, local routing<br>• 2 – Optional. Level 2, inter-site routing<br>**Note:** After specifying the routing level, you can, optionally enable IPSec Secure authentication and remote VPN client. |
| pool <1-2> level [1\|2] | The following keywords are common to the 'IP', 'IPv6', and 'hostname' parameters:<br>Optional. Sets the wireless controller or service platform's pool<br>• <1-2> – Select either 1 or 2 as the pool. The default is 1. After selecting the pool, optionally select one of the following two routing levels:<br>• 1 – Optional. Level 1, local routing<br>• 2 – Optional. Level 2, inter-site routing |
| {ipsec-secure {gw [<IP>\|<HOSTNAME>]}\|remote-vpn-client} | After specifying the routing level and or device's pool, you can optionally specify the following:<br>• ipsec-secure – Optional. Enables IPSec peer authentication on the connection (link) between the adopting devices. This option is disabled by default.<br>• gw – Optional. Specifies a IPSec gateway other than the wireless controller or service platform<br>• <IP> – Use this option to specify the IPSec gateway's IP address.<br>• <HOSTNAME> – Use this option to specify the IPSec gateway's hostname.<br>**Note:** If the gateway's IP address or hostname is not specified, the system assumes the logged controller as the IPSec gateway.<br>Contd.... |

| | |
|---|---|
| | • remote-vpn-client – Forces *MiNT link creation protocol* (MLCP) to use remote VPN connection on the controller<br>The controller uses remote VPN tunnel for this traffic. If multiple controller hosts are configured, either all the hosts should use remote-vpn-client or none.<br>When enabled, an MLCP connection is not initiated until remote VPN connection is UP and virtual IP, DNS server, source route, etc. are installed on the AP. |

- `controller host [<IPv4>|<IPv6>|<HOSTNAME>] {remote-vpn-client}`

| | |
|---|---|
| controller | Configures the WLAN's controller settings |
| host [<IPv4>\|<IPv6>\|<HOSTNAME>] | Configures wireless controller or service platform's IPv4/IPv6 address or hostname<br>• <IP> – Configures wireless controller or service platform's IPv4 address<br>• <IPv6> – Configures wireless controller or service platform's IPv6 address<br>• <HOSTNAME> – Configures wireless controller or service platform's name |
| remote-vpn-client | Forces MLCP to use remote VPN connection on the controller<br>The controller uses remote VPN tunnel for this traffic. If multiple controller hosts are configured, either all the hosts should use remote-vpn-client or none.<br>When enabled, an MLCP connection is not initiated until remote VPN connection is UP and virtual IP, DNS server, source route, etc. are installed on the AP. |

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000)controller group test

rfs6000-37FABE(config-profile-default-rfs6000)#controller host 1.2.3.4 pool 2

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs6000 default-rfs6000
 no autoinstall configuration
 no autoinstall firmware
 crypto isakmp policy default
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
.....................................................
 interface ge4
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 use firewall-policy default
 controller host 1.2.3.4 pool 2
 controller group test
 service pm sys-restart
--More--
rfs6000-37FABE(config-profile-default-rfs6000)#

rfs4000-229D58(config-profile-testRFS4000)#controller adopted-devices aps
controllers

rfs4000-229D58(config-profile-testRFS4000)#show context
profile rfs4000 testRFS4000
 autoinstall configuration
.............................................................
  logging on
 service pm sys-restart
 router ospf
 controller adopted-devices aps controllers
rfs4000-229D58(config-profile-testRFS4000)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables or reverts settings to their default |

## 7.1.16 critical-resource

*Profile Config Commands*

Enables monitoring of resources critical to the health of the service platform, wireless controller, or access point managed network. These critical resources are identified by their configured IP addresses. When enabled, the system monitors these devices regularly and logs their status. Use this command to create a *critical resource monitoring* (CRM) policy.

A critical resource can be a gateway, AAA server, WAN interface, any hardware, or a service on which the stability of the network depends. Monitoring these resources is therefore essential. When enabled, this feature pings critical resources regularly to ascertain their status. If there is a connectivity issue, an event is generated stating a critical resource is unavailable. By default, there is no enabled critical resource policy and one needs to be created and implemented.

Critical resources can be monitored directly through the interfaces on which they are discovered. For example, a critical resource on the same subnet as an AP8132 access point can be monitored by its IP address. However, a critical resource located on a VLAN must continue to be monitored on that VLAN.

Critical resource monitoring can be enabled on service platforms, wireless controllers, and access points through their respective device profiles.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
critical-resource [<CR-NAME>|monitor|retry-count]

critical-resource <CR-NAME> [monitor|monitor-using-flows]

critical-resource <CR-NAME> monitor [direct|via]

critical-resource <CR-NAME> monitor direct [all|any] [<IP/HOST-ALIAS-NAME>|sync-
adoptees] {<IP/HOST-ALIAS-NAME>|arp-only vlan [<1-4094>|<VLAN-ALIAS-NAME>]{<IP/
HOST-ALIAS-NAME>|port [<LAYER2-IF-NAME>|ge <1-4>|port-channel <1-2>]}}

critical-resource <CR-NAME> monitor via [<IP/HOST-ALIAS-NAME>|<LAYER3-INTERFACE-
NAME>|pppoe1|vlan|wwan1]

critical-resource <CR-NAME> monitor via [<IP/HOST-ALIAS-NAME>|<LAYER3-INTERFACE-
NAME>|pppoe1|vlan <1-4094>|wwan1] [all|any] [<IP/HOST-ALIAS-NAME>|
sync-adoptees] {<IP/HOST-ALIAS-NAME>|arp-only [vlan <1-4094>|<VLAN-ALIAS-NAME>]
{<IP/HOST-ALIAS-NAME>|port [<LAYER2-IF-NAME>|ge <1-4>|port-channel <1-2>]}}

critical-resource <CR-NAME> monitor-using-flows [all|any]
[criteria|dhcp|dns|sync-adoptees]

critical-resource <CR-NAME> monitor-using-flows [all|any] criteria [all|cluster-
master|rf-domain-manager] (dhcp [vlan <1-4094>|<VLAN-ALIAS-NAME>]|
dns <IP/HOST-ALIAS-NAME>) {dhcp vlan [<1-4094>|<VLAN-ALIAS-NAME>]|dns <IP/HOST-
ALIAS-NAME>}

critical-resource <CR-NAME> monitor-using-flows [all|any] dhcp vlan <1-4094> {dhcp
vlan [<1-4094>|<VLAN-ALIAS-NAME>]|dns <IP/HOST-ALIAS-NAME>}
```

```
critical-resource <CR-NAME> monitor-using-flows [all|any] dns <IP/HOST-ALIAS-NAME>
{dhcp [vlan <1-4094>|<VLAN-ALIAS-NAME>]|dns <IP/HOST-ALIAS-NAME>}

critical-resource <CR-NAME> monitor-using-flows [all|any] sync-adoptees criteria
[all|cluster-master|rf-domain-manager] (dhcp [vlan <1-4094>|<VLAN-ALIAS-
NAME>]|dns <IP/HOST-ALIAS-NAME>) {dhcp [vlan <1-4094>|
<VLAN-ALIAS-NAME>]|dns <IP/HOST-ALIAS-NAME>}

critical-resource monitor interval <5-86400>

critical-resource retry-count <0-10>
```

**Parameters**

```
• critical-resource <CR-NAME> monitor direct [all|any] [<IP/HOST-ALIAS-NAME>|sync-
adoptees] {<IP/HOST-ALIAS-NAME>|arp-only [vlan <1-4094>|<VLAN-ALIAS-NAME>] {<IP/
HOST-ALIAS-NAME>|port [<LAYER2-IF-NAME>|ge <1-4>|port-channel <1-2>]}}
```

| | |
|---|---|
| <CR-NAME> | Identifies the critical resource to be monitored. Provide the name of the critical resource. |
| monitor | Enables critical resource(s) monitoring |
| direct [all\|any] [<IP/HOST-ALIAS-NAME>\| sync-adoptees] | Monitors critical resources using the default routing engine<br>• all – Monitors all resources that are going down (generates an event when all specified critical resources are unreachable)<br>• any – Monitors any resource that is going down (generates an event when any one of the specified critical resource is unreachable)<br>• <IP/HOST-ALIAS-NAME> – Configures the IP address of the critical resource being monitored (for example, the DHCP or DNS server). Specify the IP address in the A.B.C.D format. You can use a host-alias to identify the critical resource. If using a host-alias, ensure that the host-alias is existing and configured.<br>• sync-adoptees – Syncs adopted access points with the controller. In the standalone AP scenario, where the CRM policy is running on the AP, the AP is directly intimated in case a critical resource goes down. On the other hand, when an AP is adopted to a controller (running the CRM policy), it is essential to enable the sync-adoptees option in order to sync the AP with the controller regarding the latest CRM status. |
| arp-only vlan [<1-4094>\|<VLAN-ALIAS-NAME>] {<IP/HOST-ALIAS-NAME>\| port [<LAYER2-IFNAME>\|ge\| port-channel]} | The following keywords are common to the 'all' and 'any' parameters:<br>• arp-only vlan <1-4094> – Optional. Uses ARP to determine if the IP address is reachable (use this option to monitor resources that do not have IP addresses). ARP is used to resolve hardware addresses when only the network layer address is known.<br>• vlan [<1-4094>\|<VLAN-ALIAS-NAME>] – Specifies the VLAN ID on which to send the probing ARP requests. Specify the VLAN ID from 1 - 4094. Alternately, use a vlan-alias to identify the VLAN. If using a vlan-alias, ensure that the alias is existing and configured.<br>• <IP/HOST-ALIAS-NAME> – Optional. Limits ARP to a device specified by the <IP> parameter. You can use a host-alias to specify the IP address. If using a host-alias, ensure that the host-alias is existing and configured.<br>• port [<LAYER2-IF-NAME>\|ge\|port-channel] – Optional. Limits ARP to a specified port |

- `critical-resource <CRM-POLICY-NAME> monitor via [<IP/HOST-ALIAS-NAME>|<LAYER3-INTERFACE-NAME>|pppoe1|vlan <1-4094>|wwan1] [all|any] [<IP/HOST-ALIAS-NAME>|sync-adoptees] {<IP/HOST-ALIAS-NAME>|arp-only vlan [<1-4094>|<VLAN-ALIAS-NAME>] {<IP>|port [<LAYER2-IFNAME>|ge|port-channel]}}`

| | |
|---|---|
| <CR-NAME> | Identifies the critical resource to be monitored. Provide the name of the critical resource. |
| monitor | Enables critical resource(s) monitoring |
| via | Specifies the interface or next-hop via which the ICMP pings should be sent.<br>Configures the interface or next-hop via which ICMP pings are sent. This does not apply to IP addresses configured for arp-only. For interfaces which learn the default-gateway dynamically (like DHCP clients and PPP interfaces), use an interface name for VIA, or use an IP address. |
| <IP/HOST-ALIAS-NAME> | Specify the IP address of the next-hop via which the critical resource(s) are monitored. Configures up to four IP addresses for monitoring. All the four IP addresses constitute critical resources. You can use a host-alias to specify the IP address. If using a host-alias, ensure that the host-alias is existing and configured. |
| <LAYER3-INTERFACE-NAME> | Specify the layer 3 Interface name (router interface) |
| pppoe1 | Specifies PPP over Ethernet interface |
| vlan [<1-4094>\|<VLAN-ALIAS-NAME>] | Specifies the wireless controller or service platform's VLAN interface. Specify VLAN ID from 1 - 4094. Alternately, use a vlan-alias to identify the VLAN. If using a vlan-alias, ensure that the alias is existing and configured. |
| wwan1 | Specifies Wireless WAN interface |
| [all\|any] [<IP/HOST-ALIAS-NAME>\| sync-adoptees] | Monitors critical resources using the default routing engine<br>• all – Monitors all resources that are going down (generates an event when all specified critical resource IP addresses are unreachable)<br>• any – Monitors any resource that is going down (generates an event when any one of the specified critical resource IP address is unreachable)<br>• <IP/HOST-ALIAS-NAME> – Configures the IP address of the critical resource being monitored (for example, the DHCP or DNS server). Specify the IP address in the A.B.C.D format. You can use a host-alias to specify the IP address. If using a host-alias, ensure that the host-alias is existing and configured.<br>• sync-adoptees – Syncs adopted access points with the controller. In the stand-alone AP scenario, where the CRM policy is running on the AP, the AP is directly intimated in case a critical resource goes down. On the other hand, when an AP is adopted to a controller (running the CRM policy), it is essential to enable the sync-adoptees option in order to sync the AP with the controller regarding the latest CRM status. |
| arp-only vlan [<1-4094>\|<VLAN-ALIAS-NAME>] {<IP/HOST-ALIAS-NAME>\| port [<LAYER2-IFNAME>\|ge\| port-channel]} | The following keywords are common to the 'all' and 'any' parameters:<br>• arp-only vlan <1-4094> – Optional. Uses ARP to determine if the IP address is reachable (use this option to monitor resources that do not have IP addresses). ARP is used to resolve hardware addresses when only the network layer address is known.<br>Contd.... |

| | |
|---|---|
| | • vlan [<1-4094>\|<VLAN-ALIAS-NAME>] – Specifies the VLAN ID to send the probing ARP requests. Specify the VLAN ID from 1 - 4094. Alternately, use a vlan-alias to identify the VLAN. If using a vlan-alias, ensure that the alias is existing and configured.<br>• <IP'HOST-ALIAS-NAME> – Optional. Limits ARP to a device specified by the <IP> parameter. You can use a host-alias to specify the IP address. If using a host-alias, ensure that the host-alias is existing and configured.<br>• port [<LAYER2-IF-NAME>\|ge\|port-channel] – Optional. Limits ARP to a specified port |

• `critical-resource <CRM-POLICY-NAME> monitor-using-flows [all|any] criteria [all|cluster-master|rf-domain-manager] (dhcp [vlan <1-4094>|<VLAN-ALIAS-NAME>]| dns <IP/HOST-ALIAS-NAME>)` *`{dhcp [vlan <1-4094>|<VLAN-ALIAS-NAME>]|dns <IP/HOST-ALIAS-NAME>}`*

| | |
|---|---|
| <CR-NAME> | Identifies the critical resource to be monitored. Provide the name of the critical resource. |
| monitor-using-flows | Enables critical resource(s) monitoring using message flows for DHCP or DNS (DHCP discover, DHCP offer, etc.) instead of ICMP or ARP packets in order to reduce the amount of traffic on the network. |
| [all\|any] | Configures how critical resource event messages are generated. Options include all and any.<br>• all – Monitors all resources that are going down (generates an event when all specified critical resources are unreachable)<br>• any – Monitors any resource that is going down (generates an event when any one of the specified critical resource is unreachable) |
| criteria [all\|cluster-master\| rf-domain-manager] | Configures the resource that will monitor critical resources and update the rest of the devices in a group. Options include all, rf-domain-manager, or cluster-master.<br>• all – Configures all devices within a group (cluster or RF Domain) as the monitoring resource<br>• cluster-master – Configures the cluster master as the monitoring resource<br>• rf-domain-manager – Configures the RF Domain manager as the monitoring resource |
| dhcp vlan [<1-4094>\| <VLAN-ALIAS-NAME>] | The following parameters are recursive and common to the 'all', 'cluster-master', and 'rf-domain-manager' keywords:<br>• dhcp – Configures DHCP as the mode of monitoring critical resources. When configured, DHCP message flows (DHCP Discover, DHCP Offer, etc.) are used instead of ICMP or ARP packets to confirm critical resource availability.<br>• vlan [<1-4094>\|<VLAN-ALIAS-NAME>] – Configures the VLAN on which the critical resource(s) is available. Specify the VLAN from 1 - 4094. Alternately, use a vlan-alias to identify the VLAN. If using a vlan-alias, ensure that the alias is existing and configured. |
| dns <IP/HOST-ALIAS-NAME> | The following parameters are recursive and common to the 'all', 'cluster-master', and 'rf-domain-manager' keywords:<br>• dns – Configures DNS as the mode of monitoring critical resources. When configured, DNS message flows are used instead of ICMP or ARP packets to confirm critical resource availability.<br>• <IP/HOST-ALIAS-NAME> – Configures the IPv4 address or host alias of the critical resource. Specify the IPv4 address or host alias name (should be existing and configured). |

| | |
|---|---|
| {dhcp [vlan <1-4094>\|<VLAN-ALIAS-NAME>]\| dns <IP/HOST-ALIAS-NAME>} | The 'dhcp' and 'dns' parameters are recursive and you can optionally configure multiple VLANs and critical resource IPv4 addresses (or host alias names).<br>• dhcp – Optional. Configures DHCP as the mode of monitoring critical resources. When configured, DHCP message flows (DHCP Discover, DHCP Offer, etc.) are used instead of ICMP or ARP packets to confirm critical resource availability.<br>• vlan [<1-4094>\|<VLAN-ALIAS-NAME>] – Configures the VLAN on which the critical resource(s) is available. Specify the VLAN from 1 - 4094. Alternately, use a vlan-alias to identify the VLAN. If using a vlan-alias, ensure that the alias is existing and configured.<br>• dns – Optional. Configures DNS as the mode of monitoring critical resources. When configured, DNS message flows are used instead of ICMP or ARP packets to confirm critical resource availability.<br>• <IP/HOST-ALIAS-NAME> – Configures the IPv4 address or host alias of the critical resource. Specify the IPv4 address or host alias name (should be existing and configured). |

• `critical-resource <CRM-POLICY-NAME> monitor-using-flows [all|any] dhcp vlan [<1-4094>|<VLAN-ALIAS-NAME>]` *`{dhcp vlan [<1-4094>|<VLAN-ALIAS-NAME>]|dns <IP/HOST-ALIAS-NAME>}`*

| | |
|---|---|
| <CR-NAME> | Identifies the critical resource to be monitored. Provide the name of the critical resource. |
| monitor-using-flows | Enables critical resource(s) monitoring using message flows for DHCP or DNS (DHCP Discover, DHCP Offer, etc.) instead of ICMP or ARP packets in order to reduce the amount of traffic on the network. |
| [all\|any] | Configures how critical resource event messages are generated. Options include *all* and *any*.<br>• all – Monitors all resources that are going down (generates an event when all specified critical resources are unreachable)<br>• any – Monitors any resource that is going down (generates an event when any one of the specified critical resource is unreachable) |
| dhcp vlan [<1-4094>\|<VLAN-ALIAS-NAME>] | Configures DHCP as the mode of monitoring critical resources. When configured, DHCP message flows (DHCP Discover, DHCP Offer, etc.) are used instead of ICMP or ARP packets to confirm critical resource availability.<br>• vlan [<1-4094>\|<VLAN-ALIAS-NAME>] – Configures the VLAN on which the critical resource(s) is available. Specify the VLAN from 1 - 4094. Alternately, use a vlan-alias to identify the VLAN. If using a vlan-alias, ensure that the alias is existing and configured. |
| {dhcp vlan [<1-4094>\|<VLAN-ALIAS-NAME>]\| dns <IP/HOST-ALIAS-NAME>} | The following parameters are recursive and optional. Use them to configure multiple VLANs and critical resource IPv4 addresses (or host alias names):<br>• dhcp – Optional. Configures DHCP as the mode of monitoring critical resources. When configured, DHCP message flows (DHCP Discover, DHCP Offer, etc.) are used instead of ICMP or ARP packets to confirm critical resource availability.<br>• vlan [<1-4094>\|<VLAN-ALIAS-NAME>] – Configures the VLAN on which the critical resource(s) is available. Specify the VLAN from 1 - 4094. Alternately, use a vlan-alias to identify the VLAN. If using a vlan-alias, ensure that the alias is existing and configured.<br>Contd... |

| | |
|---|---|
| | • dns – Optional. Configures DNS as the mode of monitoring critical resources. When configured, DNS message flows are used instead of ICMP or ARP packets to confirm critical resource availability.<br>• <IP/HOST-ALIAS-NAME> – Configures the IPv4 address or host alias of the critical resource. Specify the IPv4 address or host alias name (should be existing and configured). |

`• critical-resource <CRM-POLICY-NAME> monitor-using-flows [all|any] dns <IP/HOST-ALIAS-NAME> {dhcp vlan [<1-4094><VLAN-ALIAS-NAME>]|dns <IP/HOST-ALIAS-NAME>}`

| | |
|---|---|
| <CR-NAME> | Identifies the critical resource to be monitored. Provide the name of the critical resource. |
| monitor-using-flows | Enables critical resource(s) monitoring using message flows for DHCP or DNS (DHCP Discover, DHCP Offer, etc.) instead of ICMP or ARP packets in order to reduce the amount of traffic on the network. |
| [all\|any] | Configures how critical resource event messages are generated. Options include *all* and *any*.<br>• all – Monitors all resources that are going down (generates an event when all specified critical resources are unreachable)<br>• any – Monitors any resource that is going down (generates an event when any one of the specified critical resource is unreachable) |
| dns <IP/HOST-ALIAS-NAME> | Configures DNS as the mode of monitoring critical resources. When configured, DNS message flows are used instead of ICMP or ARP packets to confirm critical resource availability.<br>• <IP/HOST-ALIAS-NAME> – Configures the IPv4 address or host alias of the critical resource. Specify the IPv4 address or host alias name (should be existing and configured). |
| {dhcp vlan [<1-4094>\|<VLAN-ALIAS-NAME>\|dns <IP/HOST-ALIAS-NAME>} | The following parameters are recursive and optional. Use them to configure multiple VLANs and critical resource IPv4 addresses (or host alias names):<br>• dhcp – Optional. Configures DHCP as the mode of monitoring critical resources. When configured, DHCP message flows (DHCP Discover, DHCP Offer, etc.) are used instead of ICMP or ARP packets to confirm critical resource availability.<br>• vlan [<1-4094>\|<VLAN-ALIAS-NAME>] – Configures the VLAN on which the critical resource(s) is available. Specify the VLAN from 1 - 4094. Alternately, use a vlan-alias to identify the VLAN. If using a vlan-alias, ensure that the alias is existing and configured.<br>• dns – Optional. Configures DNS as the mode of monitoring critical resources. When configured, DNS message flows are used instead of ICMP or ARP packets to confirm critical resource availability.<br>• <IP/HOST-ALIAS-NAME> – Configures the IPv4 address or host alias of the critical resource. Specify the IPv4 address or host alias name (should be existing and configured). |

`• critical-resource <CRM-POLICY-NAME> monitor-using-flows [all|any] sync-adoptees criteria [all|cluster-master|rf-domain-manager] (dhcp vlan [<1-4094>|<VLAN-ALIAS-NAME>]|dns <IP/HOST-ALIAS-NAME>) {dhcp vlan [<1-4094>|<VLAN-ALIAS-NAME>]|dns <IP/HOST-ALIAS-NAME>}`

| | |
|---|---|
| <CR-NAME> | Identifies the critical resource to be monitored. Provide the name of the critical resource. |

| | |
|---|---|
| monitor-using-flows | Enables critical resource(s) monitoring using message flows for DHCP or DNS (DHCP Discover, DHCP Offer, etc.) instead of ICMP or ARP packets in order to reduce the amount of traffic on the network. |
| [all\|any] | Configures how critical resource event messages are generated. Options include *all* and *any*.<br>• all – Monitors all resources that are going down (generates an event when all specified critical resources are unreachable)<br>• any – Monitors any resource that is going down (generates an event when any one of the specified critical resource is unreachable) |
| syn-adoptees | Syncs adopted access points with the controller. In the stand-alone AP scenario, where the CRM policy is running on the AP, the AP is directly intimated in case a critical resource goes down. On the other hand, when an AP is adopted to a controller (running the CRM policy), it is essential to enable the sync-adoptees option in order to sync the AP with the controller regarding the latest CRM status. |
| criteria [all\|cluster-master\| rf-domain-manager] | Configures the resource that will monitor critical resources and update the rest of the devices in a group. Options include *all*, *rf-domain-manager*, or *cluster-master*.<br>• all – Configures all devices within a group (cluster or RF Domain) as the monitoring resource<br>• cluster-master – Configures the cluster master as the monitoring resource<br>• rf-domain-manager – Configures the RF Domain manager as the monitoring resource |
| dhcp vlan [<1-4094>\| <VLAN-ALIAS-NAME>] | The following parameters are recursive and common to the 'all', 'cluster-master', and 'rf-domain-manager' keywords:<br>• dhcp – Configures DHCP as the mode of monitoring critical resources. When configured, DHCP message flows (DHCP Discover, DHCP Offer, etc.) are used instead of ICMP or ARP packets to confirm critical resource availability.<br>• vlan [<1-4094>\|<VLAN-ALIAS-NAME>] – Configures the VLAN on which the critical resource(s) is available. Specify the VLAN from 1 - 4094. Alternately, use a vlan-alias to identify the VLAN. If using a vlan-alias, ensure that the alias is existing and configured. |
| dns <IP/HOST-ALIAS-NAME> | The following parameters are recursive and common to the 'all', 'cluster-master', and 'rf-domain-manager' keywords:<br>• dns – Configures DNS as the mode of monitoring critical resources. When configured, DNS message flows are used instead of ICMP or ARP packets to confirm critical resource availability.<br>• <IP/HOST-ALIAS-NAME> – Configures the IPv4 address or host alias of the critical resource. Specify the IPv4 address or host alias name (should be existing and configured). |
| {dhcp vlan {<1-4094>\| <VLAN-ALIAS-NAME>]\| dns <IP/HOST-ALIAS-NAME>} | The 'dhcp' and 'dns' parameters are recursive and you can optionally configure multiple VLANs and critical resource IPv4 addresses (or host alias names).<br>• dhcp – Optional. Configures DHCP as the mode of monitoring critical resources. When configured, DHCP message flows (DHCP Discover, DHCP Offer, etc.) are used instead of ICMP or ARP packets to confirm critical resource availability.<br>• vlan [<1-4094>\|<VLAN-ALIAS-NAME>] – Configures the VLAN on which the critical resource(s) is available. Specify the VLAN from 1 - 4094. Alternately, use a vlan-alias to identify the VLAN. If using a vlan-alias, ensure that the alias is existing and configured.<br>Contd... |

| | |
|---|---|
| | • dns – Optional. Configures DNS as the mode of monitoring critical resources. When configured, DNS message flows are used instead of ICMP or ARP packets to confirm critical resource availability.<br>• <IP/HOST-ALIAS-NAME> – Configures the IPv4 address or host alias of the critical resource. Specify the IPv4 address or host alias name (should be existing and configured). |

- `critical-resource monitor interval <5-86400>`

| | |
|---|---|
| monitor interval <5-86400> | Configures the critical resource monitoring frequency. This is the interval between two successive pings to the critical resource being monitored.<br>• <5-86400> – Specifies the frequency in seconds. Specify the time from 5 - 86400 seconds. The default is 30 seconds. |

- `critical-resource retry-count <0-10>`

| | |
|---|---|
| retry-count <0-10> | Configures the maximum number of failed attempts allowed to connect to a critical resource, using DHCP/DNS message flows, before marking it as down<br>• <0-10> – Specifies the maximum number of retries from 0 - 10. The default value is 3 attempts. |

**Example**

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#critical-resource test monitor
direct all 192.168.13.10 arp-only vlan 1
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#critical-resource monitor interval
40

nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#show context
rfs6000 B4-C7-99-6D-B5-D4
 use profile default-rfs6000
 use rf-domain default
 hostname rfs6000-6DB5D4
 license AP
6c781f42a3638757d8849c38268b4ea48e483e2f986ae392ebbcdd6a8f6f309443e93ad3123c3d76
 mint mlcp ip
 ip default-gateway 192.168.13.2
 interface vlan1
  ip address 192.168.13.16/24
  ip dhcp client request options all
 cluster mode standby
 cluster member ip 192.168.13.16 level 1
 controller host 192.168.13.13
 critical-resource monitor interval 40
 critical-resource test monitor direct all 192.168.13.10 arp-only vlan 1
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#
```

## 7.1.17 crypto

*Profile Config Commands*

Use the crypto command to define a system-level local ID for *Internet Security Association and Key Management Protocol* (ISAKMP) negotiation and to enter the ISAKMP policy, ISAKMP client, or ISAKMP peer command set.

The following table summarizes crypto configuration mode commands:

| Command | Description | Reference |
|---|---|---|
| *crypto* | Invokes commands used to configure ISAKMP policy, ISAKMP client, and ISAKMP peer | *page 7-81* |
| *crypto-auto-ipsec-tunnel commands* | Creates an auto IPSec VPN tunnel and enters its configuration mode | *page 7-87* |
| *crypto-ikev1/ikev2-policy commands* | Creates a crypto IKEv1/IKEv2 policy and enters its configuration mode | *page 7-94* |
| *crypto-ikev1/ikev2-peer commands* | Creates a IKEv1/IKEv2 peer and enters its configuration mode | *page 7-103* |
| *crypto-map-config-commands* | Creates a crypto map and enters its configuration mode | *page 7-111* |
| *crypto-remote-vpn-client commands* | Creates a remote VPN client and enters its configuration mode | *page 7-136* |

### 7.1.17.1 crypto

*crypto*

Use the crypto command to define a system-level local ID for ISAKMP negotiation and enter the ISAKMP policy, ISAKMP client, or ISAKMP peer configuration mode.

A crypto map entry is a single policy that describes how certain traffic is secured. There are two types of crypto map entries: ipsec-manual and ipsec-ike entries. Each entry is given an index (used to sort the ordered list).

When a non-secured packet arrives on an interface, the crypto map associated with that interface is processed (in order). If a crypto map entry matches the non-secured traffic, the traffic is discarded.

When a packet is transmitted on an interface, the crypto map associated with that interface is processed. The first crypto map entry that matches the packet is used to secure the packet. If a suitable *Security Association* (SA) exists, it is used for transmission. Otherwise, IKE is used to establish a SA with the peer. If no SA exists (and the crypto map entry is "respond only"), the packet is discarded.

When a secured packet arrives on an interface, its *Security Parameter Index* (SPI) is used to look up a SA. If a SA does not exist (or if the packet fails any of the security checks), it is discarded. If all checks pass, the packet is forwarded normally.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
crypto [auto-ipsec-secure|enable-ike-uniqueids|ike-version|ikev1|ikev2|ipsec|
load-management|map|pki|plain-text-deny-acl-scope|remote-vpn-client]

crypto [auto-ipsec-secure|enable-ike-uniqueids|load-management]

crypto ike-version [ikev1-only|ikev2-only]

crypto ikev1 [dpd-keepalive <10-3600>|dpd-retries <1-100>|nat-keepalive <10-
3600>|peer <IKEV1-PEER>|policy <IKEV1-POLICY-NAME>|remote-vpn]

crypto ikev2 [cookie-challenge-threshold <1-100>|dpd-keepalive <10-3600>|
dpd-retries <1-100>|nat-keepalive <10-3600>|peer <IKEV2-PEER>|policy <IKEV2-
POLICY-NAME>|remote-vpn]

crypto ipsec [df-bit|security-association|transform-set]
crypto ipsec df-bit [clear|copy|set]
crypto ipsec security-association lifetime [kilobytes <500-2147483646>|seconds
<120-86400>]
crypto ipsec transform-set <TRANSFORM-SET-TAG> [esp-3des|esp-aes|esp-aes-192|
esp-aes-256|esp-des|esp-null] [esp-aes-xcbc-mac|esp-md5-hmac|esp-sha-hmac|esp-
sha256-hmac]

crypto map <CRYPTO-MAP-TAG> <1-1000> [ipsec-isakmp {dynamic}|ipsec-manual]

crypto pki import crl <TRUSTPOINT-NAME> URL <1-168>

crypto plain-text-deny-acl-scope [global|interface]
```

```
crypto remote-vpn-client
```

**Parameters**

- `crypto [auto-ipsec-secure|enable-ike-uniqueids|load-management]`

| | |
|---|---|
| auto-ipsec-secure | Configures the Auto IPSec Secure parameter settings. For Auto IPSec tunnel configuration commands, see *crypto-auto-ipsec-tunnel commands*. |
| enable-ike-uniqueids | Enables *Internet Key Exchange* (IKE) unique ID check<br>For more information on IKE unique IDs, see *remotegw*. |
| load-management | Configures load management for platforms using software cryptography |

- `crypto ike-version [ikev1-only|ikev2-only]`

| | |
|---|---|
| ike-version [ikev1-only\|ikev2-only] | Selects and starts the IKE daemon<br>• ikev1-only – Enables support for IKEv1 tunnels only<br>• ikev2-only – Enables support for IKEv2 tunnels only |

- `crypto ikev1 [dpd-keepalive <10-3600>|dpd-retries <1-100>|nat-keepalive <10-3600>|peer <IKEV1-PEER>|policy <IKEV1-POLICY-NAME>|remote-vpn]`

| | |
|---|---|
| ikev1 | Configures the IKE version 1 parameters |
| dpd-keepalive <10-3600> | Sets the global *Dead Peer Detection* (DPD) keep alive interval from 10 - 3600 seconds. This is the interval between successive IKE keep alive messages sent to detect if a peer is dead or alive. The default is 30 seconds. |
| dpd-retries <1-1000> | Sets the global DPD retries count from 1 - 1000. This is the number of keep alive messages sent to a peer before the tunnel connection is declared as dead. The default is 5. |
| nat-keepalive <10-3600> | Sets the global NAT keep alive interval from 10 - 3600 seconds. This is the interval between successive NAT keep alive messages sent to detect if a peer is dead or alive. The default is 20 seconds. |
| peer <IKEV1-PEER> | Specify the name/Identifier for the IKEv1 peer. For IKEV1 peer configuration commands, see *crypto-ikev1/ikev2-peer commands*. |
| policy <IKEV1-POLICY-NAME> | Configures an ISKAMP policy. Specify the name of the policy.<br>The local IKE policy and the peer IKE policy must have matching group settings for successful negotiations.<br>For IKEV1 policy configuration commands, see *crypto-ikev1/ikev2-policy commands*. |
| remote-vpn | Specifies the IKEV1 remote-VPN server configuration (responder only) |

- `crypto ikev2 [cookie-challenge-threshold <1-100>|dpd-keepalive <10-3600>|dpd-retries <1-100>|nat-keepalive <10-3600>|peer <IKEV2-PEER>|policy <IKEV2-POLICY-NAME>|remote-vpn]`

| | |
|---|---|
| ikev2 | Configures the IKE version 2 parameters |
| cookie-challenge-threshold <1-100> | Starts the cookie challenge mechanism after the number of half open IKE SAs exceeds the specified limit. Specify the limit from 1 - 100. The default is 5. |
| dpd-keepalive <10-3600> | Sets the global DPD keepalive interval from 10 - 3600 seconds. The default is 30 seconds. |
| dpd-retries <1-100> | Sets the global DPD retries count from 1 - 100. The default is 5. |
| nat-keepalive <10-3600> | Sets the global NAT keepalive interval from 10 - 3600 seconds. The default is 20 seconds. |

| | |
|---|---|
| peer <IKEV2-PEER> | Specify the name/Identifier for the IKEv2 peer |
| policy <IKEV2-POLICY-NAME> | Configures an ISKAMP policy. Specify the policy name.<br>The local IKE policy and the peer IKE policy must have matching group settings for successful negotiations. |
| remote-vpn | Specifies an IKEv2 remote-VPN server configuration (responder only) |

- `crypto ipsec df-bit [clear|copy|set]`

| | |
|---|---|
| ipsec | Configures the IPSec policy parameters |
| df-bit [clear\|copy\|set] | Configures *Don't-Fragment* (DF) bit handling for encapsulating header. The options are:<br>• clear – Clears the DF bit in the outer header and ignores in the inner header<br>• copy – Copies the DF bit from the inner header to the outer header. This is the default setting.<br>• set – Sets the DF bit in the outer header |

- `crypto ipsec security-association lifetime [kilobytes <500-2147483646>|seconds <120-86400>]`

| | |
|---|---|
| ipsec | Configures the IPSec policy parameters |
| security-association | Configures the IPSec SAs parameters |
| lifetime [kilobyte \|seconds] | Defines the IPSec SAs lifetime (in kilobytes and/or seconds). Values can be entered in both kilobytes and seconds, which ever limit is reached first, ends the SA. When the SA lifetime ends it is renegotiated as a security measure.<br>• kilobytes – Specifies a volume-based key duration (minimum is 500 KB and maximum is 2147483646 KB)<br>• <500-2147483646> – Specify a value from 500 - 2147483646 KB. The default is 4608000 KB.<br>• seconds – Specifies a time-based key duration (minimum is 120 seconds and maximum is 86400 seconds)<br>• <120-86400> – Specify a value from 120 - 86400 seconds. The default is 3600 seconds.<br>The security association lifetime can be overridden under crypto maps. |

- `crypto ipsec transform-set <TRANSFORM-SET-TAG> [esp-3des|esp-aes|esp-aes-192|esp-aes-256|esp-des|esp-null] [esp-aes-xcbc-mac|esp-md5-hmac|esp-sha-hmac|esp-sha256-hmac]`

| | |
|---|---|
| ipsec | Configures the IPSec policy parameters |
| transform-set <TRANSFORM-SET-TAG> | Defines the transform set configuration (authentication and encryption) for securing data. A transform set is a combination of security protocols, algorithms and other settings applied to IPSec protected traffic.<br>• <TRANSFORM-SET-TAG> – Specify the transform set name.<br>After specifying the transform set used by the IPSec transport connection, set the encryption method and the authentication scheme used with the transform set.<br>The encryption methods are: DES, 3DES, AES, AES-192 and AES-256.<br>**Note:** The authentication schemes available are: esp-md5-hmac and esp-sha-hmac. |
| esp-3des | Configures the ESP transform using 3DES cipher (168 bits). The transform set is assigned to a crypto map using the map's *set > transform-set* command. |

| | |
|---|---|
| esp-aes | Configures the ESP transform using *Advanced Encryption Standard* (AES) cipher. The transform set is assigned to a crypto map using the map's *set > transform-set* command. |
| esp-aes-192 | Configures the ESP transform using AES cipher (192 bits). The transform set is assigned to a crypto map using the map's *set > transform-se*t command. |
| esp-aes-256 | Configures the ESP transform using AES cipher (256 bits). The transform set is assigned to a crypto map using the map's *set > transform-set* command. This is the default setting. |
| esp-des | Configures the ESP transform using *Data Encryption Standard* (DES) cipher (56 bits). The transform set is assigned to a crypto map using the map's *set > transform-set* command. |
| esp-null | Configures the ESP transform with no encryption |
| [esp-aes-xcbc-mac\| esp-md5-hmac\| esp-sha-hmac\| esp-sha256-hmac] | The following keywords are common to all of the above listed transform sets.<br>After specifying the transform set type, configure the authentication scheme used to validate identity credentials. The options are:<br>• esp-aes-xcbc-mac – Configures ESP transform using AES-XCBC authorization<br>• esp-md5-hmac – Configures ESP transform using HMAC-MD5 authorization<br>• esp-sha-hmac – Configures ESP transform using HMAC-SHA authorization. This is the default setting.<br>• esp-sha256-hmac – Configures ESP transform using HMAC-SHA256 authorization |

- `crypto map <CRYPTO-MAP-TAG> <1-1000> [ipsec-isakmp {dynamic}|ipsec-manual]`

| | |
|---|---|
| map <CRYPTO-MAP-TAG> | Configures the crypto map, a software configuration entity that selects data flows that require security processing. The crypto map also defines the policy for these data flows.<br>• <CRYPTO-MAP-TAG> – Specify a name for the crypto map. The name should not exceed 32 characters. For crypto map configuration commands, see *crypto-map-ipsec-manual-instance*. |
| <1-1000> | Defines the crypto map entry sequence. Each crypto map uses a list of entries, each entry having a specific sequence number. Specifying multiple sequence numbers within the same crypto map provides the flexibility to connect to multiple peers from the same interface. Specify a value from 1 - 1000. |
| ipsec-isakmp {dynamic} | Configures IPSEC w/ISAKMP.<br>• dynamic – Optional. Configures dynamic map entry (remote VPN configuration) for XAUTH with mode-config or ipsec-l2tp configuration |
| ipsec-manual | Configures IPSEC w/manual keying. Remote configuration is not allowed for manual crypto map. |

- `crypto pki import crl <TRUSTPOINT-NAME> <URL> <1-168>`

| | |
|---|---|
| pki | Configures certificate parameters. The *Public Key Infrastructure* (PKI) protocol creates encrypted public keys using digital certificates from certificate authorities. |
| import | Imports a trustpoint related configuration |

| | |
|---|---|
| crl <TRUSTPOINT-NAME> | Imports a *Certificate Revocation List* (CRL). Imports a trustpoint including either a private key and server certificate or a *certificate authority* (CA) certificate or both.<br>A CRL is a list of revoked certificates that are no longer valid. A certificate can be revoked if the CA had improperly issued a certificate, or if a private-key is compromised. The most common reason for revocation is the user no longer being in sole possession of the private key.<br>• <TRUSTPOINT-NAME> – Specify the trustpoint name. |
| <URL> | Specify the CRL source address in the following format. Both IPv4 and IPv6 address formats are supported.<br>tftp://<hostname\|IPv4 or IPv6>[:port]/path/file<br>ftp://<user>:<passwd>@<hostname\|IPv4 or IPv6>[:port]/path/file<br>sftp://<user>:<passwd>@<hostname\|IPv4 or IPv6>[:port]>/path/file<br>http://<hostname\|IPv4 or IPv6>[:port]/path/file<br>cf:/path/file<br>usb<n>:/path/file |
| <1-168> | Sets command replay duration from 1 - 168 hours. This is the interval (in hours) after which devices using this profile copy a CRL file from an external server and associate it with a trustpoint. |

- `crypto plain-text-deny-acl-scope [global|interface]`

| | |
|---|---|
| plain-text-deny-acl-scope | Configures plain-text-deny-acl-scope parameters |
| global | Applies the plain text deny ACL globally. This is the default setting. |
| interface | Applies the plain text deny ACL to the interface only |

- `crypto remote-vpn-client`

| | |
|---|---|
| remote-vpn-client | Configures remote VPN client settings. For more information, see *crypto-remote-vpn-client commands*. |

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000)#crypto ipsec transform-set tpsec-
tag1 esp-aes-256 esp-md5-hmac
rfs6000-37FABE(config-profile-default-rfs6000)#crypto map map1 10 ipsec-isakmp
dynamic
rfs6000-37FABE(config-profile-default-rfs6000)#crypto plain-text-deny-acl-scope
interface

rfs6000-37FABE(config-profile-default-rfs6000)#show context
profile rfs6000 default-rfs6000
  bridge vlan 1
  tunnel-over-level2
  ip igmp snooping
  ip igmp snooping querier
 no autoinstall configuration
 no autoinstall firmware
 device-upgrade persist-images
 crypto ikev1 dpd-retries 1
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ipsec transform-set tpsec-tag1 esp-aes-256 esp-md5-hmac
 crypto map map1 10 ipsec-isakmp dynamic
 crypto ikev1 remote-vpn
```

```
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 crypto plain-text-deny-acl-scope interface
 interface radio1
 interface radio2
 interface up
rfs6000-37FABE(config-profile-default-rfs6000)#

rfs6000-37FABE(config-profile-default-rfs6000)#crypto ipsec transform-set tag1
esp-null esp-md5-hmac

rfs6000-37FABE(config-profile-default-rfs6000-transform-set-tag1)#?
Crypto Ipsec Configuration commands:
  mode     Encapsulation mode (transport/tunnel)
  no       Negate a command or set its defaults

  clrscr   Clears the display screen
  commit   Commit all changes made in this session
  end      End current mode and change to EXEC mode
  exit     End current mode and down to previous mode
  help     Description of the interactive help system
  revert   Revert changes
  service  Service Commands
  show     Show running system information
  write    Write running configuration to memory or terminal

rfs6000-37FABE(config-profile-default-rfs6000-transform-set-tag1)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables or reverts settings to their default |

### 7.1.17.2 crypto-auto-ipsec-tunnel commands

*crypto*

Creates an auto IPSec VPN tunnel and changes the mode to auto-ipsec-secure mode for further configuration

Auto IPSec tunneling provides a secure tunnel between two networked peer controllers or service platforms and associated access points that are within a range of valid IP addresses. You can define which packets are sent within the tunnel, and how they are protected. When a tunneled peer sees a sensitive packet, it creates a secure tunnel and sends the packet through the tunnel to its remote peer destination or associated access point.

Tunnels are sets of SA between two peers. SAs define the protocols and algorithms applied to sensitive packets and specify the keying mechanisms used by tunneled peers. SAs are unidirectional and exist in both the inbound and outbound direction. SAs are established per the rules and conditions of defined security protocols (AH or ESP).

The IKE protocol is a key management protocol used in conjunction with IPSec. IKE enhances IPSec by providing additional features, flexibility, and configuration simplicity for the IPSec standard. IKE enables secure communications without time consuming manual pre-configuration for auto IPSec tunneling.

```
rfs7000-37FABE(config-profile-default-rfs7000)#crypto auto-ipsec-secure
rfs7000-37FABE(config-profile-default-rfs7000-crypto-auto-ipsec-secure)#?
Crypto Auto IPSEC Tunnel commands:
  groupid       Local/Remote identity and Authentication credentials for Auto
                IPSec Secure IKE negotiation
  ike-lifetime  Set lifetime for ISAKMP security association
  ikev2         IKEv2 configuration commands
  ip            Internet Protocol config commands
  no            Negate a command or set its defaults
  remotegw      Auto IPSec Secure Remote Peer IKE

  clrscr        Clears the display screen
  commit        Commit all changes made in this session
  do            Run commands from Exec mode
  end           End current mode and change to EXEC mode
  exit          End current mode and down to previous mode
  help          Description of the interactive help system
  revert        Revert changes
  service       Service Commands
  show          Show running system information
  write         Write running configuration to memory or terminal

rfs7000-37FABE(config-profile-default-rfs7000-crypto-auto-ipsec-secure)#
```

The following table summarizes the crypto IPSec auto tunnel configuration mode commands:

| Command | Description | Reference |
|---|---|---|
| *groupid* | Specifies the identity string used for IKE authentication | *page 7-88* |
| *ip* | Enables the controller or service platform to uniquely identify APs and the hosts present in the AP's subnet | *page 7-89* |
| *ike-lifetime* | Configures the IKE SA's key lifetime in seconds | *page 7-90* |
| *ikev2* | Enables the forced re-authentication of IKEv2 peer | *page 7-91* |
| *remotegw* | Defines the IKE version used for an auto IPSec tunnel using secure gateways | *page 7-92* |
| *no* | Removes or reverts the crypto auto IPSec tunnel settings | *page 7-93* |

### 7.1.17.2.1 groupid

*crypto-auto-ipsec-tunnel commands*

Specifies the identity string used for IKE authentication

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
groupid <WORD> [psk|rsa]
groupid <WORD> [psk [0 <WORD>|2 <WORD>|<WORD>]|rsa]
```

**Parameters**

- `groupid <WORD> [psk [0 <WORD>|2 <WORD>|<WORD>]|rsa]`

| | |
|---|---|
| <WORD> | Specify a string not exceeding 64 characters. This is the group identity used for IKE exchange for auto IPSec secure peers. After providing a group ID, specify the authentication method used to authenticate peers on the auto IPSec secure tunnel. The options are: psk and rsa. |
| psk [0 <WORD>\| 2 <WORD>\| <WORD>] | Configures the *pre-shared key* (PSK) as the authentication type for secure peer authentication on the auto IPSec secure tunnel<br>• 0 <WORD> – Configures a clear text key<br>• 2 <WORD> – Configures an encrypted key<br>• <WORD> – Specify a string value from 8 - 21 characters. |
| rsa | Configures the *Rivest-Shamir-Adleman* (RSA) key.<br>RSA is an algorithm for public key cryptography. It is the first algorithm known to be suitable for signing, as well as encryption. This is the default setting. |

**NOTE:** Only one group ID is supported on the controller or service platform. All APs, controllers, and service platform must use the same group ID.

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-crypto-auto-ipsec-secure)#groupid
 testgroup@123 rsa

rfs6000-37FABE(config-profile-default-rfs6000-crypto-auto-ipsec-secure)#show
context
 crypto auto-ipsec-secure
  groupid testgroup@123 rsa
rfs6000-37FABE(config-profile-default-rfs6000-crypto-auto-ipsec-secure)#
```

### 7.1.17.2.2 ip

*crypto-auto-ipsec-tunnel commands*

Enables the controller to uniquely identify APs and the hosts present in the AP's subnet. This allows the controller to correctly identify the destination host and create a dynamic site-to-site VPN tunnel between the host and the private network behind the controller.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ip nat crypto
```

**Parameters**

- `ip nat crypto`

| | |
|---|---|
| ip nat crypto | Enables unique identification of APs and the hosts present in each AP's subnet<br>Providing a unique ID enables the access point, wireless controller, or service platform to uniquely identify the destination device. This is essential in networks where there are multiple APs behind a router, or when two (or more) APs behind two (or more) different routers have the same IP address. Further, the same subnet exists behind these APs.<br>For example, let us consider a scenario where there are two APs (A and B) behind two routers (1 and 2). AP 'A' is behind router '1'. And AP 'B' is behind router '2'. Both these APs have the same IP address (192.168.13.8). The subnet behind APs A and B is also the same (100.1.1.0/24). In such a scenario the controller fails to uniquely identify the hosts present in either AP's subnet.<br>For more information, see *remotegw* and *crypto*. |

**Example**

```
rfs4000-229D58config-profile-testRFS4000-crypto-auto-ipsec-secure)#ip nat crypto

rfs4000-229D58config-profile-testRFS4000-crypto-auto-ipsec-secure)#show context
 crypto auto-ipsec-secure
  remotegw ike-version ikev2 uniqueid
  ip nat crypto
rfs4000-229D58config-profile-testRFS4000-crypto-auto-ipsec-secure)#
```

### 7.1.17.2.3 ike-lifetime

*crypto-auto-ipsec-tunnel commands*

Configures the IKE SA's key lifetime in seconds

The lifetime defines how long a connection (encryption/authentication keys) should last, from successful key negotiation to expiration. Two peers need not exactly agree on the lifetime, though if they do not, there is some clutter for a superseded connection on the peer defining the lifetime as longer.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ike-lifetime <600-86400>
```

**Parameters**

- `ike-lifetime <600-86400>`

| | |
|---|---|
| ike-lifetime <600-86400> | Sets the IKE SA's key lifetime in seconds<br>• <600-86400> – Specify a value fro m 600 - 86400 seconds. The default is 8600 seconds. |

**Example**

```
rfs4000-229D58(config-profile-testRFS4000-crypto-auto-ipsec-secure)#ike-lifetime
800

rfs4000-229D58(config-profile-testRFS4000-crypto-auto-ipsec-secure)#show context
crypto auto-ipsec-secure
  ike-lifetime 800
rfs4000-229D58(config-profile-testRFS4000-crypto-auto-ipsec-secure)#
```

#### 7.1.17.2.4 ikev2

*crypto-auto-ipsec-tunnel commands*

Enables the forced IKEv2 peer re-authentication. This option is disabled by default.

In most IPSec tunnel configurations, the lifetime of IKE SAs between peers is limited. Once the IKE SA key expires it is renegotiated. In such a scenario, the IKEv2 tunnel peers may or may not re-authenticate themselves. When enabled, IKE tunnel peers have to re-authenticate each time the IKE SA is renegotiated.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ikev2 peer reauth
```

**Parameters**

- `ikev2 peer reauth`

| | |
|---|---|
| ikev2 peer reauth | Enables IKEv2 peer re-authentication. When enabled, IKE tunnel peers are forced to re-authenticate each time the IKE key is renegotiated. |

**Example**

```
rfs4000-229D58(config-profile-testRFS4000-crypto-auto-ipsec-secure)#ikev2 peer
reauth
```

### 7.1.17.2.5 remotegw

*crypto-auto-ipsec-tunnel commands*

Defines the IKE version used for auto IPSEC tunnel negotiation with the IPSec remote gateway other than the controller

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
remotegw ike-version [ikev1-aggr|ikev1-main|ikev2] {uniqueid}
```

**Parameters**

- `remotegw ike-version [ikev1-aggr|ikev1-main|ikev2] {uniqueid}`

| | |
|---|---|
| remotegw ike-version | Configures the IKE version used for initiating auto IPSec tunnel with secure gateways other than the controller |
| ikev1-aggr | Aggregation mode is used by the auto IPSec tunnel initiator to set up the connection |
| ikev1-main | Main mode is used by the auto IPSec tunnel initiator to establish the connection |
| ikev2 | IKEv2 is the preferred method when wireless controller/AP only is used |
| uniqueid | This keyword is common to all of the above parameters.<br>• uniqueid – Optional. Enables the assigning of a unique ID to APs (using this profile) behind a router by prefixing the MAC address to the group ID<br>Providing a unique ID enables the access point, wireless controller, or service platform to uniquely identify the destination device. This is essential in networks where there are multiple APs behind a router, or when two (or more) APs behind two (or more) different routers have the same IP address. For example, let us consider a scenario where there are two APs (A and B) behind two routers (1 and 2). AP 'A' is behind router '1'. And AP 'B' is behind router '2'. Both these APs have the same IP address (192.168.13.8). In such a scenario, the controller fails to establish an Auto IPSec VPN tunnel to either APs, because it is unable to uniquely identify them.<br>After enabling unique ID assignment, enable IKE unique ID check. For more information, see *crypto*. |

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-crypto-auto-ipsec-secure)#remotegw
ike-version ikev2 uniqueid

rfs6000-37FABE(config-profile-default-rfs6000-crypto-auto-ipsec-secure)#show
context

 crypto auto-ipsec-secure
  remotegw ike-version ikev2 uniqueid
rfs6000-37FABE(config-profile-default-rfs6000-crypto-auto-ipsec-secure)#
```

### 7.1.17.2.6 no

*crypto-auto-ipsec-tunnel commands*

Removes or resets this auto IPSec tunnel settings

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
no [groupid|ike-lifetime|ikev2 peer reauth|ip nat crypto]
```

**Parameters**

- `no <PARAMETERS>`

| | |
|---|---|
| no <PARAMETERS> | Removes or resets this auto IPSec tunnel's settings based on the parameters passed |

**Example**

The following example shows the Auto IPSec VLAN bridge settings before the 'no' command is executed:

```
rfs6000-37FABE(config-profile-default-rfs6000-crypto-auto-ipsec-secure)#show
context
 crypto auto-ipsec-secure
  groupid testpassword@123 rsa
rfs6000-37FABE(config-profile-default-rfs6000-crypto-auto-ipsec-secure)#

rfs6000-37FABE(config-profile-default-rfs6000-crypto-auto-ipsec-secure)#no
groupid
```

The following example shows the Auto IPSec VLAN bridge settings after the 'no' command is executed:

```
rfs6000-37FABE(config-profile-default-rfs6000-crypto-auto-ipsec-secure)#show
context
 crypto auto-ipsec-secure
rfs6000-37FABE(config-profile-default-rfs6000-crypto-auto-ipsec-secure)#
```

### 7.1.17.3 crypto-ikev1/ikev2-policy commands

*crypto*

Defines crypto-IKEv1/IKEv2 commands in detail

IKE protocol is a key management protocol standard used in conjunction with IPSec. IKE enhances IPSec by providing additional features, flexibility, and configuration simplicity for the IPSec standard. IKE automatically negotiates IPSec SAs and enables secure communications without time consuming manual pre-configuration.

Use the (config) instance to configure IKEv1/IKEv2 policy configuration commands.

To navigate to the IKEv1/IKEv2 policy config instance, use the following commands:

```
<DEVICE>(config)#profile <DEVICE-TYPE> <PROFILE-NAME>
<DEVICE>(config-profile-<PROFILE-NAME>)#crypto ikev1/ikev2 policy <IKEV1/IKEV2-
POLICY-NAME>

rfs7000-37FABE(config-profile-default-rfs7000)#crypto ikev1 policy ikev1-
testpolicy
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-ikev1-testpolicy)#?
Crypto IKEv1 Policy Configuration commands:
  dpd-keepalive    Set Dead Peer Detection interval in seconds
  dpd-retries      Set Dead Peer Detection retries count
  isakmp-proposal  Configure ISAKMP Proposals
  lifetime         Set lifetime for ISAKMP security association
  mode             IKEv1 mode (main/aggressive)
  no               Negate a command or set its defaults

  clrscr           Clears the display screen
  commit           Commit all changes made in this session
  end              End current mode and change to EXEC mode
  exit             End current mode and down to previous mode
  help             Description of the interactive help system
  revert           Revert changes
  service          Service Commands
  show             Show running system information
  write            Write running configuration to memory or terminal

rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-ikev1-testpolicy)#

rfs7000-37FABE(config-profile-test-ikev2-policy-ikev2-testpolicy)#?
Crypto IKEv2 Policy Configuration commands:
  dpd-keepalive    Set Dead Peer Detection interval in seconds
  isakmp-proposal  Configure ISAKMP Proposals
  lifetime         Set lifetime for ISAKMP security association
  no               Negate a command or set its defaults
  sa-per-acl       Setup single SA for all rules in the ACL (ONLY APPLICABLE
                   FOR SITE-TO-SITE VPN)

  clrscr           Clears the display screen
  commit           Commit all changes made in this session
  do               Run commands from Exec mode
  end              End current mode and change to EXEC mode
  exit             End current mode and down to previous mode
  help             Description of the interactive help system
  revert           Revert changes
  service          Service Commands
  show             Show running system information
  write            Write running configuration to memory or terminal

rfs7000-37FABE(config-profile-test-ikev2-policy-ikev2-testpolicy)#
```

**NOTE:** IKEv2 being an improved version of the original IKEv1 design, is recommended in most deployments. IKEv2 provides enhanced cryptographic mechanisms, NAT and firewall traversal, attack resistance, etc.

The following table summarizes crypto IKEv1/iKEv2 configuration mode commands:

| Command | Description | Reference |
|---|---|---|
| *dpd-keepalive* | Sets DPD keep alive packet interval | *page 7-96* |
| *dpd-retries* | Sets the maximum number of attempts for sending DPD keep alive packets (applicable only to the IKEv1 policy) | *page 7-97* |
| *isakmp-proposal* | Configures ISAKMP proposals | *page 7-98* |
| *lifetime* | Specifies how long an IKE SA is valid before it expires | *page 7-100* |
| *mode* | Sets the mode of the tunnels (applicable only to the IKEv1 policy) | *page 7-101* |
| *no* | Removes or reverts IKEv1/IKEv2 policy settings | *page 7-102* |

#### 7.1.17.3.1 dpd-keepalive

*crypto-ikev1/ikev2-policy commands*

Sets the DPD keep-alive packet interval

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
dpd-keepalive <10-3600>
```

**Parameters**

- `dpd-keepalive <10-3600>`

| | |
|---|---|
| <10-3600> | Specifies the interval, in seconds, between successive DPD keep alive packets.The IKE keep alive message is used to detect a dead peer on the remote end of the IPSec VPN tunnel. Specify the time from 10 - 3600 seconds. The default is 30 seconds. |

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-ikev1-policy-ikev1-testpolicy)#
dpd-keepalive 11

rfs6000-37FABE(config-profile-default-rfs6000-ikev1-policy-testpolicy)#show
context
 crypto ikev1 policy testpolicy
  dpd-keepalive 11
  isakmp-proposal default encryption aes-256 group 2 hash sha
rfs6000-37FABE(config-profile-default-rfs6000-ikev1-policy-testpolicy)#
```

### 7.1.17.3.2 dpd-retries

*crypto-ikev1/ikev2-policy commands*

Sets the maximum number of times DPD keep-alive packets are sent to a peer. Once this value is exceeded, without a response from the peer, the VPN tunnel connection is declared dead. This option is available only for the IKEv1 policy.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
dpd-retries <1-100>
```

**Parameters**

- `dpd-retries <1-100>`

| | |
|---|---|
| <1-100> | Declares a peer dead after the specified number of retries. Specify a value from 1 - 100. The default is 5. |

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-ikev1-policy-ikev1-testpolicy)#
dpd-retries 10

rfs6000-37FABE(config-profile-default-rfs6000-ikev1-policy-ikev1-testpolicy)#
show context
 crypto ikev1 policy testpolicy
  dpd-keepalive 11
  dpd-retries 10
  isakmp-proposal default encryption aes-256 group 2 hash sha
rfs6000-37FABE(config-profile-default-rfs6000-ikev1-policy-ikev1-testpolicy)#
```

### 7.1.17.3.3 isakmp-proposal

*crypto-ikev1/ikev2-policy commands*

Configures ISAKMP proposals and their parameters

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
isakmp-proposal <WORD> encryption [3des|aes|aes-192|aes-256] group [14|2|5] hash
[aes-xcbc-mac|md5|sha|sha256]
```

**Parameters**

```
• isakmp-proposal <WORD> encryption [3des|aes|aes-192|aes-256] group [14|2|5] hash
[aes-xcbc-mac|md5|sha|sha256]
```

| | |
|---|---|
| <WORD> | Assigns the target peer (tunnel destination) a 32 character maximum name to distinguish it from others with a similar configuration. |
| encryption [3des\|aes\|aes-192\| aes-256] | Configures the encryption method used by the tunneled peers to securely inter-operate<br>• 3des – Configures triple data encryption standard<br>• aes – Configures AES (128 bit keys)<br>• aes-192 – Configures AES (192 bit keys)<br>• aes-256 – Configures AES (256 bit keys). This is the default setting. |
| group [14\|2\|5] | Specifies the *Diffie-Hellman* (DH) group identifier used by VPN peers to derive a shared secret password without having to transmit. DH groups determine the strength of the key used in key exchanges. The higher the group number, the stronger and more secure the key. Options include 2, 5 and 14.<br>• 14 – Configures DH group 14<br>• 2 – Configures DH group 2. This is the default setting.<br>• 5 – Configures DH group 5 |
| hash [maes-xcbc-mac\| md5\|sha\|sha256] | Specifies the hash algorithm used to authenticate data transmitted over the IKE SA. The hash algorithm specified here is used by VPN peers to exchange credential information.<br>• aes-xcbc-mac – Uses AES XCBC Auth hash algorithm. This option is applicable only to the IKEv2 policy configuration context.<br>• md5 – Uses *Message Digest 5* (MD5) hash algorithm<br>• sha – Uses *Secure Hash Authentication* (SHA) hash algorithm. This is the default setting.<br>• sha256 – Uses Secure Hash Standard 2 algorithm |

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-ikev1-policy-ikev1-testpolicy)#
isakmp-proposal testproposal encryption aes group 2 hash sha

rfs6000-37FABE(config-profile-default-rfs6000-ikev1-policy-ikev1-testpolicy)#
show context
 crypto ikev1 policy testpolicy
  dpd-keepalive 11
  dpd-retries 10
  isakmp-proposal default encryption aes-256 group 2 hash sha
  isakmp-proposal testpraposal encryption aes group 2 hash sha
rfs6000-37FABE(config-profile-default-rfs6000-ikev1-policy-ikev1-testpolicy)#
```

### 7.1.17.3.4 lifetime

*crypto-ikev1/ikev2-policy commands*

Specifies how long an IKE SA (encryption/authentication keys) is valid. The value specified is the validity period of the IKE SA from successful key negotiation to expiration.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
lifetime <600-86400>
```

**Parameters**

- `lifetime <600-86400>`

| | |
|---|---|
| lifetime <600-86400> | Specifies how many seconds an IKE SA lasts before it expires. Set a time stamp from 600 - 86400 seconds.<br>• <600-86400> – Specify a value from 600 - 86400 seconds. The default is 86400 seconds. |

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-ikev1-policy-ikev1-testpolicy)#
lifetime 655

rfs6000-37FABE(config-profile-default-rfs6000-ikev1-policy-ikev1-testpolicy)#
show context
 crypto ikev1 policy testpolicy
  dpd-keepalive 11
  dpd-retries 10
  lifetime 655
  isakmp-proposal default encryption aes-256 group 2 hash sha
  isakmp-proposal testpraposal encryption aes group 2 hash sha
rfs6000-37FABE(config-profile-default-rfs6000-ikev1-policy-ikev1-testpolicy)#
```

### 7.1.17.3.5 mode

*crypto-ikev1/ikev2-policy commands*

Configures the IPSec mode of operation for the IKEv1 policy. This option is not available for IKEv2 policy.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
mode [aggresive|main]
```

**Parameters**

- `mode [aggresive|main]`

| | |
|---|---|
| mode [aggresive\|main] | Sets the mode of the tunnels<br>• aggressive – Initiates the aggressive mode<br>• main – Initiates the main mode<br>If configuring the IKEv1 IPSec policy, define the IKE mode as either *main* or *aggressive*. In the aggressive mode, 3 messages are exchanged between the IPSec peers to setup the SA. On the other hand, in the main mode, 6 messages are exchanged. The default setting is main. |

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-ikev1-policy-ikev1-testpolicy)#
mode aggressive

rfs6000-37FABE(config-profile-default-rfs6000-ikev1-policy-ikev1-testpolicy)#
show context
 crypto ikev1 policy testpolicy
  dpd-keepalive 11
  dpd-retries 10
  lifetime 655
  isakmp-proposal default encryption aes-256 group 2 hash sha
  isakmp-proposal testpraposal encryption aes group 2 hash sha
  mode aggressive
rfs6000-37FABE(config-profile-default-rfs6000-ikev1-policy-ikev1-testpolicy)#
```

### 7.1.17.3.6 no

*crypto-ikev1/ikev2-policy commands*

Removes or reverts IKEv1/IKEv2 policy settings

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
no [dpd-keepalive|dpd-retries|isakmp-proposal <WORD>|lifetime|mode]
```

**Parameters**

- `no <PARAMETERS>`

| | |
|---|---|
| no <PARAMETERS> | Removes or reverts this IKEv1/IKEv2 policy settings based on parameters passed |

**Example**

The following example shows the IKEV1 Policy settings before the 'no' commands are executed:

```
rfs6000-37FABE(config-profile-default-rfs6000-ikev1-policy-ikev1-testpolicy)#
show context
 crypto ikev1 policy testpolicy
  dpd-keepalive 11
  dpd-retries 10
  lifetime 655
  isakmp-proposal default encryption aes-256 group 2 hash sha
  isakmp-proposal testpraposal encryption aes group 2 hash sha
  mode aggressive
rfs6000-37FABE(config-profile-default-rfs6000-ikev1-policy-ikev1-testpolicy)#

rfs6000-37FABE(config-profile-default-rfs6000-ikev1-policy-ikev1-testpolicy)#no
mode
rfs6000-37FABE(config-profile-default-rfs6000-ikev1-policy-ikev1-testpolicy)#no
dpd-keepalive
rfs6000-37FABE(config-profile-default-rfs6000-ikev1-policy-ikev1-testpolicy)#no
dpd-retries
```

The following example shows the IKEV1 Policy settings after the 'no' commands are executed:

```
rfs6000-37FABE(config-profile-default-rfs6000-ikev1-policy-ikev1-testpolicy)#
show context
 crypto ikev1 policy testpolicy
  lifetime 655
  isakmp-proposal default encryption aes-256 group 2 hash sha
  isakmp-proposal testpraposal encryption aes group 2 hash sha
rfs6000-37FABE(config-profile-default-rfs6000-ikev1-policy-ikev1-testpolicy)#
```

### 7.1.17.4 crypto-ikev1/ikev2-peer commands

*crypto*

Use the (config) instance to configure IKEv1/IKEv2 peer configuration commands. To navigate to the IKEv1/IKEv2 peer config instance, use the following commands:

```
<DEVICE>(config)#profile <DEVICE-TYPE> <PROFILE-NAME>
<DEVICE>(config-profile-<PROFILE-NAME>)#crypto ikev1/ikev2 peer <IKEV1/IKEV2-
PEER-NAME>

rfs7000-37FABE(config-profile-default-rfs7000)#crypto ikev1 peer peer1
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#?
Crypto IKEV1 Peer Configuration commands:
  authentication  Configure Authentication credentials
  ip              Configure peer address/fqdn
  localid         Set local identity
  no              Negate a command or set its defaults
  remoteid        Configure remote peer identity
  use             Set setting to use

  clrscr          Clears the display screen
  commit          Commit all changes made in this session
  end             End current mode and change to EXEC mode
  exit            End current mode and down to previous mode
  help            Description of the interactive help system
  revert          Revert changes
  service         Service Commands
  show            Show running system information
  write           Write running configuration to memory or terminal

rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#

rfs7000-37FABE(config-profile-default-rfs7000)#crypto ikev2 peer peer1
rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#?
Crypto IKEV2 Peer Configuration commands:
  authentication  Configure Authentication credentials
  ip              Configure peer address/fqdn
  localid         Set local identity
  no              Negate a command or set its defaults
  remoteid        Configure remote peer identity
  use             Set setting to use

  clrscr          Clears the display screen
  commit          Commit all changes made in this session
  do              Run commands from Exec mode
  end             End current mode and change to EXEC mode
  exit            End current mode and down to previous mode
  help            Description of the interactive help system
  revert          Revert changes
  service         Service Commands
  show            Show running system information
  write           Write running configuration to memory or terminal

rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#
```

The following table summarizes crypto IPSec IKEv1/IKEv2 peer configuration mode commands:

| Command | Description | Reference |
|---|---|---|
| *authentication* | Configures a peer's authentication mode and the pre-shared key | *page 7-105* |
| *ip* | Configures the peer's IP address | *page 7-106* |
| *localid* | Configures a peer's local identity details | *page 7-107* |
| *remoteid* | Configures a remote peer's identity details | *page 7-108* |
| *use* | Associates an IKEv1 policy and IKEv2 policy with the IKEv1 and IKEv2 peer respectively | *page 7-109* |
| *no* | Negates a command or reverts settings to their default. The no command, when used in the ISAKMP policy mode, defaults the ISAKMP protection suite settings. | *page 7-110* |

### 7.1.17.4.1 authentication

*crypto-ikev1/ikev2-peer commands*

Configures IKEv1/IKEv2 peer's authentication mode and the pre-shared key

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
authentication [psk|rsa]

authentication psk [0 <WORD>|2 <WORD>|<WORD>] {local|remote}

authentication rsa
```

**Parameters**

- `authentication psk [0 <WORD>|2 <WORD>|<WORD>] {local|remote}`

| | |
|---|---|
| psk [0 <WORD>\| 2 <WORD>\| <WORD>] *{local\|remote}* | Configures the authentication mode as *pre-shared key* (PSK). The PSK is a string, 8 - 12 characters long. It is shared by both ends of the VPN tunnel connection. If using IKEv2, both a local and remote string must be specified for handshake validation at both ends (local and remote) of the VPN connection.<br>• 0 <WORD> – Configures a clear text key<br>• 2 <WORD> – Configures an encrypted key<br>• <WORD> – Configures the pre-shared key<br>The following keywords are available only in the IKEv2 peer configuration mode:<br>• local – Optional. Uses the specified key for local peer authentication only<br>• remote – Optional. Uses the specified key for remote peer authentication only<br>**Note:** In case the peer type is not specified, this string is used for authenticating both local and remote peers. |

- `authentication rsa`

| | |
|---|---|
| rsa | Configures the authentication mode as *Rivest, Shamir, and Adleman* (RSA) This is the default setting (for both IKEv1 and IKEv2).<br>RSA is the first known public-key cryptography algorithm designed signing and encryption. If configuring the IKEv2 peer, the 'rsa' option allows you to enable authentication at both ends of the VPN connection (local and remote). |

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-ikev1-peer-peer1)#authentication
rsa

rfs6000-37FABE(config-profile-default-rfs6000-ikev2-peer-peer1)#authentication
psk 0 key@123456

rfs6000-37FABE(config-profile-default-rfs6000-ikev2-peer-peer1)#show context
 crypto ikev2 peer peer1
  authentication psk 0 key@123456 local
  authentication psk 0 key@123456 remote
rfs6000-37FABE(config-profile-default-rfs6000-ikev2-peer-peer1)#
```

### 7.1.17.4.2 ip

*crypto-ikev1/ikev2-peer commands*

Sets the IP address *or Fully Qualified Domain Name* (FQDN) of the IPSec VPN peer used in the tunnel setup

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ip [address <IP>|fqdn <WORD>]
```

**Parameters**

- `ip [address <IP>|fqdn <WORD>]`

| | |
|---|---|
| address <IP> | Specify the peer device's IP address. |
| fqdn <WORD> | Specify the peer device's FQDN hostname. |

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-ikev1-peer-peer1)#ip address
172.16.10.12

rfs6000-37FABE(config-profile-default-rfs6000-ikev1-peer-peer1)#show context
 crypto ikev1 peer peer1
  ip address 172.16.10.12
rfs6000-37FABE(config-profile-default-rfs6000-ikev1-peer-peer1)#

rfs6000-37FABE(config-profile-default-rfs6000-ikev2-peer-peer1)#ip address
192.168.10.6

rfs6000-37FABE(config-profile-default-rfs6000-ikev2-peer-peer1)#show context
 crypto ikev2 peer peer1
  ip address 192.168.10.6
  authentication psk 0 test@123456 local
  authentication psk 0 test@123456 remote
rfs6000-37FABE(config-profile-default-rfs6000-ikev2-peer-peer1)#
```

### 7.1.17.4.3 localid

*crypto-ikev1/ikev2-peer commands*

Sets a IKEv1/IKEv2 peer's local identity. This local identifier is used with this peer configuration for an IKE exchange with the target VPN IPSec peer.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
localid [address|autogen-uniqueid|dn|email|fqdn|string]

localid [address <IP>|autogen-uniqueid <WORD>|dn <WORD>|email <WORD>|fqdn <WORD>|
string <WORD>]
```

**Parameters**

- `localid [address <IP>|dn <WORD>|email <WORD>|fqdn <WORD>|string <WORD>]`

| | |
|---|---|
| address <IP> | Configures the peer's IP address. The IP address is used as local identity. |
| autogen-uniqueid <WORD> | Generates a localid using the device's unique identity. The system prefixes the device's unique identity to the string provided here. The device's unique identity should be existing and configured. For more information on configuring a device's unique identity, see *autogen-uniqueid*.<br>• <WORD> – Provide the string. |
| dn <WORD> | Configures the peer's distinguished name. (for example, "C=us ST=<state> L=<location> O=<organization> OU=<org unit>". The maximum length is 128 characters. |
| email <WORD> | Configures the peer's e-mail address. The maximum length is 128 characters. |
| fqdn <WORD> | Configures the peer's FQDN. The maximum length is 128 characters. |
| string <WORD> | Configures the peer's identity string. The maximum length is 128 characters. This is the default setting. |

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-ikev1-peer-peer1)#localid email
bob@examplecompany.com

rfs6000-37FABE(config-profile-default-rfs6000-ikev1-peer-peer1)#show context
 crypto ikev1 peer peer1
  ip address 172.16.10.12
  localid email bob@examplecompany.com
rfs6000-37FABE(config-profile-default-rfs6000-ikev1-peer-peer1)#
```

### 7.1.17.4.4 remoteid

*crypto-ikev1/ikev2-peer commands*

Configures a IKEv1/IKEV2 peer's remote identity. This remote identifier is used with this peer configuration for an IKE exchange with the target VPN IPSec peer.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
remoteid [address <IP>|dn <WORD>|email <WORD>|fqdn <WORD>|string <WORD>]
```

**Parameters**

- `remoteid [address <IP>|dn <WORD>|email <WORD>|fqdn <WORD>|string <WORD>`

| | |
|---|---|
| address <IP> | Configures the remote IKEv1/IKEV2 peer's IP address. The IP address is used as the peer's remote identity. |
| dn <WORD> | Configures the remote peer's distinguished name. For example, "C=us ST=<state> L=<location> O=<organization> OU=<org unit>". The maximum length is 128 characters. |
| email <WORD> | Configures the remote peer's e-mail address. The maximum length is 128 characters. |
| fqdn <WORD> | Configures a peer's FQDN. The maximum length is 128 characters. |
| string <WORD> | Configures a peer's identity string. The maximum length is 128 characters. |

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-ikev1-peer-peer1)#remoteid dn
SanJose

rfs6000-37FABE(config-profile-default-rfs6000-ikev1-peer-peer1)#show context
 crypto ikev1 peer peer1
  ip address 172.16.10.12
  remoteid dn SanJose
  localid email bob@examplecompany.com
rfs6000-37FABE(config-profile-default-rfs6000-ikev1-peer-peer1)#

rfs6000-37FABE(config-profile-default-rfs6000-ikev1-peer-peer1)#remoteid address
157.235.209.63

rfs6000-37FABE(config-profile-default-rfs6000-ikev2-peer-peer1)#show context
 crypto ikev2 peer peer1
  remoteid address 157.235.209.63
rfs6000-37FABE(config-profile-default-rfs6000-ikev2-peer-peer1)#
```

### 7.1.17.4.5 use

*crypto-ikev1/ikev2-peer commands*

Associates IKEv1/IKEv2 policy with the IKEv1/IKEv2 peer respectively

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
use ikev1-policy <IKEV1-POLICY-NAME>
use ikev2-policy <IKEV2-POLICY-NAME>
```

**Parameters**

- `use ikev1-policy <IKEV1-POLICY-NAME>`

| | |
|---|---|
| use ikev1-policy <IKEV1-POLICY-NAME> | Specify the IKEv1 policy name.<br>The local IKEv1 policy and the peer IKEv1 policy must have matching group settings for successful negotiations. |

- `use ikev2-policy <IKEV2-POLICY-NAME>`

| | |
|---|---|
| use ikev2-policy <IKEV2-POLICY-NAME> | Specify the IKEv2 policy name.<br>The local IKEv2 policy and the peer IKEv2 policy must have matching group settings for successful negotiations. |

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-ikev1-peer-peer1)#use ikev1-policy
test-ikev1policy

rfs6000-37FABE(config-profile-default-rfs6000-ikev1-peer-peer1)#show context
 crypto ikev1 peer peer1
  ip address 172.16.10.12
  remoteid dn SanJose
  localid email bob@examplecompany.com
  use ikev1-policy test-ikev1policy
rfs6000-37FABE(config-profile-default-rfs6000-ikev1-peer-peer1)#

rfs6000-37FABE(config-profile-default-rfs6000-ikev2-peer-peer1)#use ikev2-policy
test-ikev2policy

rfs6000-37FABE(config-profile-default-rfs6000-ikev2-peer-peer1)#show context
 crypto ikev2 peer peer1
  remoteid address 157.235.209.63
  use ikev2-policy test-ikev2policy
rfs6000-37FABE(config-profile-default-rfs6000-ikev2-peer-peer1)#
```

### 7.1.17.4.6 no

*crypto-ikev1/ikev2-peer commands*

Removes or reverts IKEv1/IKEv2 peer settings

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
no [authentication|ip|localid|remoteid|use <IKEv1/IKEv2-POLICY-NAME>]
```

**Parameters**

- `no <PARAMETERS>`

| | |
|---|---|
| no <PARAMETERS> | Removes or reverts IKEv1/IKEv2 peer settings based on the parameters passed |

**Example**

The following example shows the Crypto IKEV1 peer1 settings before the 'no' commands are executed:

```
rfs6000-37FABE(config-profile-default-rfs6000-ikev1-peer-peer1)#show context
 crypto ikev1 peer peer1
  ip address 172.16.10.12
  remoteid dn SanJose
  localid email bob@examplecompany.com
  use ikev1-policy test-ikev1policy
rfs6000-37FABE(config-profile-default-rfs6000-ikev1-peer-peer1)#

rfs6000-37FABE(config-profile-default-rfs6000-ikev1-peer-peer1)#no localid
rfs6000-37FABE(config-profile-default-rfs6000-ikev1-peer-peer1)#no remoteid
```

The following example shows the Crypto IKEV1 peer1 settings after the 'no' commands are executed:

```
rfs6000-37FABE(config-profile-default-rfs6000-ikev1-peer-peer1)#show context
 crypto ikev1 peer peer1
  ip address 172.16.10.12
  use ikev1-policy test-ikev1policy
rfs6000-37FABE(config-profile-default-rfs6000-ikev1-peer-peer1)#
```

The following example shows the Crypto IKEV2 peer1 settings before the 'no' commands are executed:

```
rfs6000-37FABE(config-profile-default-rfs6000-ikev2-peer-peer1)#show context
 crypto ikev2 peer peer1
  remoteid address 157.235.209.63
  use ikev2-policy test
rfs6000-37FABE(config-profile-default-rfs6000-ikev2-peer-peer1)#
```

The following example shows the Crypto IKEV2 peer1 settings after the 'no' commands are executed:

```
rfs6000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#no use ikev2-
policy

rfs6000-37FABE(config-profile-default-rfs6000-ikev2-peer-peer1)#show context
 crypto ikev2 peer peer1
  remoteid address 157.235.209.63
rfs6000-37FABE(config-profile-default-rfs6000-ikev2-peer-peer1)#
```

### 7.1.17.5 crypto-map-config-commands

*crypto*

This section explains crypto map configuration mode commands in detail.

A crypto map entry is a single policy that describes how certain traffic is secured. There are two types of crypto map entries: ipsec-manual and ipsec-ike. Each entry is given an index (used to sort the ordered list).

IPSec VPN provides a secure tunnel between two networked peers. Administrators can define which packets are sent within the tunnel, and how they're protected. When a tunneled peer sees a sensitive packet, it creates a secure tunnel and sends the packet through the tunnel to its remote peer destination.

Tunnels are sets of SA between two peers. SAs define the protocols and algorithms applied to sensitive packets and specify the keying mechanisms used by tunneled peers. SAs are unidirectional and exist in both the inbound and outbound direction. SAs are established per the rules and conditions of defined security protocols (AH or ESP).

IKE is a key management protocol standard used in conjunction with IPSec. IKE enhances IPSec by providing additional features, flexibility, and configuration simplicity for the IPSec standard. IKE automatically negotiates IPSec SAs, and enables secure communications without time consuming manual pre-configuration.

Use crypto maps to configure IPSec VPN SAs. Crypto maps combine the elements comprising IPSec SAs. Crypto maps also include transform sets. A transform set is a combination of security protocols, algorithms and other settings applied to IPSec protected traffic. One crypto map is utilized for each IPSec peer, however for remote VPN deployments one crypto map is used for all the remote IPSec peers.

Use the (config) instance to enter the crypto map configuration mode. To navigate to the crypto-map configuration instance, use the following commands:

```
In the device-config mode:
<DEVICE>(config-device-<DEVICE-MAC>)#crypto map <CRYPTO-MAP-TAG> <1-1000>
[ipsec-isakmp {dynamic}|ipsec-manual]

In the profile-config mode:
<DEVICE>(config-profile-<PROFILE-NAME>)#crypto map <CRYPTO-MAP-TAG> <1-1000>
[ipsec-isakmp {dynamic}|ipsec-manual]
```

There are three different configurations defined for each listed crypto map: site-to-site manual (ipsec-manual), site-to-site-auto tunnel (ipsec-isakmp), and remote VPN client (ipsec-isakmp dynamic). With site-to-site deployments, an IPSec tunnel is deployed between two gateways, each at the edge of two different remote networks. With remote VPN, an access point located at remote branch defines a tunnel with a security gateway. This facilitates the end points in the branch office to communicate with the destination endpoints (behind the security gateway) in a secure manner.

Each crypto map entry is given an index (used to sort the ordered list).

```
rfs6000-37FABE(config-profile-default-rfs6000)#crypto map map1 1 ipsec-manual
rfs6000-37FABE(config-profile-default-rfs6000-cryptomap-map1#1)#?
Manual Crypto Map Configuration commands:
  local-endpoint-ip     Use this IP as local tunnel endpoint address, instead
                        of the interface IP (Advanced Configuration)
  mode                  Set the tunnel mode
  no                    Negate a command or set its defaults
  peer                  Set peer
  security-association  Set security association parameters
  session-key           Set security session key parameters
  use                   Set setting to use

  clrscr                Clears the display screen
  commit                Commit all changes made in this session
  do                    Run commands from Exec mode
  end                   End current mode and change to EXEC mode
  exit                  End current mode and down to previous mode
  help                  Description of the interactive help system
  revert                Revert changes
  service               Service Commands
  show                  Show running system information
  write                 Write running configuration to memory or terminal

rfs6000-37FABE(config-profile-default-rfs6000-cryptomap-map1#1)#
```

The following table summarizes crypto map configuration mode commands:

| Command | Description | Reference |
|---|---|---|
| *crypto-map auto-vpn-tunnel/remote-vpn-client instance* | Configures an auto site-to-site VPN or remote VPN client | *page 7-113* |
| *crypto-map-ipsec-manual-instance* | Configures a manual site-to-site VPN | *page 7-127* |

#### 7.1.17.5.1 crypto-map auto-vpn-tunnel/remote-vpn-client instance

*crypto-map-config-commands*

To navigate to the auto site-to-site VPN tunnel configuration instance, use the following command:

In the device-config mode:

```
<DEVICE>(config-device-<DEVICE-MAC>)#crypto map <CRYPTO-MAP-TAG> <1-1000> ipsec-
isakmp
```

In the profile-config mode:

```
<DEVICE>(config-profile-<PROFILE-NAME>)#crypto map <CRYPTO-MAP-TAG> <1-1000>
ipsec-isakmp

rfs4000-229D58(config-device-00-23-68-22-9D-58)#crypto map test 1 ipsec-isakmp
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#?
Site to Site Crypto Map Configuration commands:
  ip                    Internet Protocol config commands
  local-endpoint-ip     Use this IP as local tunnel endpoint address, instead
                        of the interface IP (Advanced Configuration)
  no                    Negate a command or set its defaults
  peer                  Add a remote peer
  pfs                   Specify Perfect Forward Secrecy
  security-association  Security association parameters
  transform-set         Specify IPSec transform to use
  use                   Set setting to use

  clrscr                Clears the display screen
  commit                Commit all changes made in this session
  do                    Run commands from Exec mode
  end                   End current mode and change to EXEC mode
  exit                  End current mode and down to previous mode
  help                  Description of the interactive help system
  revert                Revert changes
  service               Service Commands
  show                  Show running system information
  write                 Write running configuration to memory or terminal

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#
```

To navigate to the remote VPN client configuration instance, use the following command:

```
In the device-config mode:
<DEVICE>(config-device-<DEVICE-MAC>)#crypto map <CRYPTO-MAP-TAG> <1-1000> ipsec-
isakmp {dynamic}

In the profile-config mode:
<DEVICE>(config-profile-<PROFILE-NAME>)#crypto map <CRYPTO-MAP-TAG> <1-1000>
ipsec-isakmp {dynamic}

rfs4000-229D58(config-device-00-23-68-22-9D-58)#crypto map test 2 ipsec-isakmp
dynamic
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#?
Dynamic Crypto Map Configuration commands:
  local-endpoint-ip     Use this IP as local tunnel endpoint address, instead
                        of the interface IP (Advanced Configuration)
  modeconfig            Set the mode config method
  no                    Negate a command or set its defaults
  peer                  Add a remote peer
  pfs                   Specify Perfect Forward Secrecy
  remote-type           Set the remote VPN client type
  security-association  Security association parameters
  transform-set         Specify IPSec transform to use
  use                   Set setting to use

  clrscr                Clears the display screen
  commit                Commit all changes made in this session
```

```
  do                    Run commands from Exec mode
  end                   End current mode and change to EXEC mode
  exit                  End current mode and down to previous mode
  help                  Description of the interactive help system
  revert                Revert changes
  service               Service Commands
  show                  Show running system information
  write                 Write running configuration to memory or terminal

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#
```

The following table lists the IPSec-Auto-VPN/Remote-VPN tunnel configuration commands:

| Command | Description | Reference |
|---|---|---|
| *ip* | Enables this setting to utilize IP/Port NAT on the VPN tunnel. This command is applicable only to the site-to-site VPN tunnel. | *page 7-115* |
| *local-endpoint-ip* | Uses the configured IP as local tunnel endpoint address, instead of the interface IP. This command is applicable to the site-to-site VPN tunnel and remote VPN client. | *page 7-116* |
| *modeconfig* | Configures the mode config method (pull or push) associated with the remote VPN client. This command is applicable only to the remote VPN client. | *page 7-117* |
| *peer* | Configures the IKEv1 or IKEv2 peer for the VPN tunnel. This command is applicable to the site-to-site VPN tunnel and remote VPN client. | *page 7-118* |
| *pfs* | Configures the *Perfect Forward Secrecy* (PFS) for the VPN tunnel. This command is applicable to the site-to-site VPN tunnel and remote VPN client. | *page 7-119* |
| *remote-type* | Configures the remote VPN client type as either None or XAuth. This command is applicable only to the remote VPN client. | *page 7-120* |
| *security-association* | Defines this automatic VPN tunnel's IPSec SA settings. This command is applicable to the site-to-site VPN tunnel and remote VPN client. | *page 7-121* |
| *transform-set* | Applies a transform set (encryption and hash algorithms) to the VPN tunnel. This command is applicable to the site-to-site VPN tunnel and remote VPN client. | *page 7-123* |
| *use* | Applies an existing and configured IP access list to the VPN tunnel. This command is applicable to the site-to-site VPN tunnel and remote VPN client. | *page 7-124* |
| *no* | Removes or reverts site-to-site VPN tunnel or remote VPN client settings | *page 7-125* |

### 7.1.17.5.2 ip

*crypto-map auto-vpn-tunnel/remote-vpn-client instance*

Enables this setting to utilize IP/Port NAT on this auto site-to-site VPN tunnel. This option is disabled by default.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ip nat crypto
```

**Parameters**

- `ip nat crypto`

| | |
|---|---|
| ip nat crypto | Enables this setting to utilize IP/Port NAT on the site-to-site VPN tunnel. This setting is disabled by default. |

**Example**

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#ip nat crypto

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#show context
 crypto map test 1 ipsec-isakmp
  ip nat crypto
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#
```

### 7.1.17.5.3 local-endpoint-ip

*crypto-map auto-vpn-tunnel/remote-vpn-client instance*

Uses the configured IP as local tunnel endpoint address, instead of the interface IP

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
local-endpoint-ip <IP>
```

**Parameters**

- `local-endpoint-ip <IP>`

| | |
|---|---|
| local-endpoint-ip <IP> | Configures the local VPN tunnel's (site-to-site VPN tunnel or remote VPN client) endpoint IP address<br>• <IP> – Specify the IP address. The specified IP address must be available on the interface. |

**Example**

```
Site-to-site VPN tunnel:

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#local-endpoint-
ip 192.168.13.10

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#show context
 crypto map test 1 ipsec-isakmp
  local-endpoint-ip 192.168.13.10
  ip nat crypto
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#

Remote VPN client:

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#local-endpoint-
ip 157.235.204.62

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#show context
 crypto map test 2 ipsec-isakmp dynamic
  local-endpoint-ip 157.235.204.62
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#
```

### 7.1.17.5.4 modeconfig

*crypto-map auto-vpn-tunnel/remote-vpn-client instance*

Configures the mode config method (pull or push) associated with the remote VPN client

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
modeconfig [pull|push]
```

**Parameters**

- `modeconfig [pull|push]`

| | |
|---|---|
| modeconfig [pull\|push] | Configures the mode config method associated with a remote VPN client. The options are: pull and push.<br>The mode (pull or push) defines the method used to assign a virtual IP. This setting is relevant for IKEv1 only, since IKEv2 always uses the configuration payload in pull mode. The default setting is push. |

**Example**

```
Remote VPN client:

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#modeconfig pull

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#show context
 crypto map test 2 ipsec-isakmp dynamic
  modeconfig pull
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)
```

### 7.1.17.5.5 peer

*crypto-map auto-vpn-tunnel/remote-vpn-client instance*

Configures the IKEv1 or IKEv2 peer for the auto site-to-site VPN tunnel or remote VPN client. The peer device can be specified either by its hostname or by its IP address. A maximum of three peers can be configured.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
peer <1-3> [ikev1|ikev2] <IKEv1/IKEv2-PEER-NAME>
```

**Parameters**

- `peer <1-3> [ikev1|ikev2] <IKEv1/IKEv2-PEER-NAME>`

| | |
|---|---|
| peer <1-3> | Creates a new peer and configures the peer's priority level. Peer '1' is the primary peer, and peer '3' is redundant. |
| ikev1 <IKEv1-PEER-NAME> | Configures an IKEv1 peer<br>• <IKEv1-PEER-NAME> – Specify the IKEv1 peer's name. |
| ikev2<IKEv2-PEER-NAME> | Configures an IKEv2 peer<br>• <IKEv2-PEER-NAME> – Specify the IKEv2 peer's name. |

**Example**

```
Site-to-site tunnel:

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#peer 1 ikev2
ikev2Peer1

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#show context
 crypto map test 1 ipsec-isakmp
  peer 1 ikev2 ikev2Peer1
  local-endpoint-ip 192.168.13.10
  ip nat crypto
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#

Remote VPN client:

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#peer 1 ikev1 Re
moteIKEv1Peer1

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#show context
 crypto map test 2 ipsec-isakmp dynamic
  peer 1 ikev1 RemoteIKEv1Peer1
  local-endpoint-ip 157.235.204.62
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#
```

### 7.1.17.5.6 pfs

*crypto-map auto-vpn-tunnel/remote-vpn-client instance*

Configures *Perfect Forward Secrecy* (PFS) for the auto site-to-site VPN tunnel or remote VPN client

PFS is the key-establishment protocol, used to secure VPN communications. If one encryption key is compromised, only data encrypted by that specific key is compromised. For PFS to exist, the key used to protect data transmissions must not be used to derive any additional keys. Options include 2, 5 and 14. This option is disabled by default.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
pfs [14|2|5]
```

**Parameters**

- `pfs [14|2|5]`

| | |
|---|---|
| pfs [14\|2\|5] | Configures PFS<br>• 14 – Configures D-H Group14 (2048-bit modp)<br>• 2 – Configures D-H Group2 (1024-bit modp)<br>• 5 – Configures D-H Group5 (1536-bit modp) |

**Example**

```
Site-to-site VPN tunnel:

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#pfs 5

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#show context
 crypto map test 1 ipsec-isakmp
  peer 1 ikev2 ikev2Peer1
  local-endpoint-ip 192.168.13.10
  pfs 5
  ip nat crypto
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#

Remote VPN client:

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#pfs 14

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#show context
 crypto map test 2 ipsec-isakmp dynamic
  peer 1 ikev1 RemoteIKEv1Peer1
  local-endpoint-ip 157.235.204.62
  pfs 14
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#
```

### 7.1.17.5.7 remote-type

*crypto-map auto-vpn-tunnel/remote-vpn-client instance*

Configures the remote VPN client type as either None or XAuth

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
remote-type [none|xauth]
```

**Parameters**

- `remote-type [none|xauth]`

| | |
|---|---|
| remote-type [none\|xauth] | Specify the remote VPN's client type<br>• none – Configures remote VPN client with No XAUTH<br>• xauth – Configures remote VPN client as using XAUTH (applicable only for IKEv1). This is the default setting.<br>XAuth (extended authentication) provides additional authentication validation by permitting an edge device to request extended authentication information from an IPSec host. This forces the host to respond with additional authentication credentials. The edge device respond with a failed or passed message. |

**Example**

```
Remote VPN client:

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#remote-type none

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#show context
 crypto map test 2 ipsec-isakmp dynamic
  peer 1 ikev1 RemoteIKEv1Peer1
  local-endpoint-ip 157.235.204.62
  pfs 14
  remote-type none
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#
```

### 7.1.17.5.8 security-association

*crypto-map auto-vpn-tunnel/remote-vpn-client instance*

Defines the IPSec SA's (created by this auto site-to-site VPN tunnel or remote VPN client) settings

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
security-association [inactivity-timeout|level|lifetime]

security-association [inactivity-timeout <120-86400>|level perhost]
security-association lifetime [kilobytes <500-2147483646>|seconds <120-86400>]
```

**Parameters**

- `security-association [inactivity-timeout <120-86400>|level perhost]`

| | |
|---|---|
| inactivity-timeout <120-86400> | Specifies an inactivity period, in seconds, for this IPSec VPN SA. Once the set value is exceeded, the association is timed out.<br>• <120-86400> – Specify a value from 120 - 86400 seconds. The default is 900 seconds. |
| level perhost | Specifies the granularity level for this IPSec VPN SA<br>• perhost – Sets the IPSec VPN SA's granularity to the host level |

- `security-association lifetime [kilobytes <500-2147483646>|seconds <120-86400>]`

| | |
|---|---|
| lifetime [kilobytes <500-2147483646>\| seconds <120-86400>] | Defines the IPSec SA's lifetime (in kilobytes and/or seconds). Values can be entered in both kilobytes and seconds. Which ever limit is reached first, ends the security association.<br>• kilobytes <500-2147483646> – Defines volume based key duration. Specify a value from 500 - 2147483646 kilobytes. Select this option to define a connection volume lifetime (in kilobytes) for the duration of the IPSec VPN SA. Once the set volume is exceeded, the association is timed out. This option is disabled by default.<br>• seconds <120-86400> – Defines time based key duration. Specify the time frame from 120 - 86400 seconds. Select this option to define a lifetime (in seconds) for the duration of the IPSec VPN SA. Once the set value is exceeded, the association is timed out. This option is disabled by default. |

**Example**

```
Site-to-site tunnel:

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#security-
association inactivity-timeout 200

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#security-
association level perhost

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#security-
association lifetime kilobytes 250000
```

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#show context
 crypto map test 1 ipsec-isakmp
  security-association level perhost
  peer 1 ikev2 ikev2Peer1
  local-endpoint-ip 192.168.13.10
  pfs 5
  security-association lifetime kilobytes 250000
  security-association inactivity-timeout 200
  ip nat crypto
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#

Remote VPN client:

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#security-
association lifetime seconds 10000

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#show context
 crypto map test 2 ipsec-isakmp dynamic
  peer 1 ikev1 RemoteIKEv1Peer1
  local-endpoint-ip 157.235.204.62
  pfs 14
  security-association lifetime seconds 10000
  remote-type none
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#
```

### 7.1.17.5.9 transform-set

*crypto-map auto-vpn-tunnel/remote-vpn-client instance*

Applies a transform set (encryption and hash algorithms) to site-to-site VPN tunnel or remote VPN client. This command allows you to provide customized data protection for each crypto map can be customized with its own data protection and peer authentication schemes.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
transform-set <TRANSFORM-SET-TAG> {<TRANSFORM-SET-TAG>}
```

**Parameters**

- `transform-set <TRANSFORM-SET-TAG> {<TRANSFORM-SET-TAG>}`

| | |
|---|---|
| transform-set <TRANSFORM-SET-TAG> <TRANSFORM-SET-TAG> | Applies a transform set. The transform set should be existing and configured.<br>• <TRANSFORM-SET-TAG> – Specify the transform set's name.<br>• <TRANSFORM-SET-TAG> – Optional. Specify a second transform set. You can provide multiple, space-separated, transform set tags. |

**Example**

```
Site-to-site VPN tunnel:

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#transform-set
AutoVPN

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#show context
 crypto map test 1 ipsec-isakmp
  security-association level perhost
  peer 1 ikev2 ikev2Peer1
  local-endpoint-ip 192.168.13.10
  pfs 5
  security-association lifetime kilobytes 250000
  security-association inactivity-timeout 200
  transform-set AutoVPN
  ip nat crypto
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#

Remote VPN client:

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#transform-set
RemoteVPN

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#show context
 crypto map test 2 ipsec-isakmp dynamic
  peer 1 ikev1 RemoteIKEv1Peer1
  local-endpoint-ip 157.235.204.62
  pfs 14
  security-association lifetime seconds 10000
  transform-set RemoteVPN
  remote-type none
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#
```

### 7.1.17.5.10 use

*crypto-map auto-vpn-tunnel/remote-vpn-client instance*

Applies an existing and configured IP access list to the auto site-to-site VPN tunnel or remote VPN client. Based on the IP access list's settings traffic is permitted or denied across the VPN tunnel.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
use ip-access-list <IP-ACCESS-LIST-NAME>
```

**Parameters**

```
• use ip-access-list <IP-ACCESS-LIST-NAME>
```

| | |
|---|---|
| ip-access-list <IP-ACCESS-LIST-NAME> | Specify the IP access list name. |

**Example**

```
Site-to-site VPN tunnel:

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#use ip-access-
list test

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#show context
 crypto map test 1 ipsec-isakmp
  use ip-access-list test
  security-association level perhost
  peer 1 ikev2 ikev2Peer1
  local-endpoint-ip 192.168.13.10
  pfs 5
  security-association lifetime kilobytes 250000
  security-association inactivity-timeout 200
  transform-set AutoVPN
  ip nat crypto
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#

Remote VPN client:

rrfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#use ip-access-
list test1

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#show context
' crypto map test 2 ipsec-isakmp dynamic
  use ip-access-list test1
  peer 1 ikev1 RemoteIKEv1Peer1
  local-endpoint-ip 157.235.204.62
  pfs 14
  security-association lifetime seconds 10000
  transform-set RemoteVPN
  remote-type none
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#
```

### 7.1.17.5.11 no

*crypto-map auto-vpn-tunnel/remote-vpn-client instance*

Removes or reverts the auto site-to-site VPN tunnel or remote VPN client settings

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
no [ip|local-endpoint-ip|modeconfig|peer|pfs|remote-type|security-association|
   transform-set|use]
```

**Parameters**

- `no <PARAMETERS>`

| | |
|---|---|
| no <PARAMETERS> | Removes or resets this auto site-to-site/remote VPN settings based on the parameters passed |

**Example**

The following example shows the IPSec site-to-site VPN tunnel 'test' settings before the 'no' commands are executed:

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#show context
 crypto map test 1 ipsec-isakmp
  use ip-access-list test
  security-association level perhost
  peer 1 ikev2 ikev2Peer1
  local-endpoint-ip 192.168.13.10
  pfs 5
  security-association lifetime kilobytes 250000
  security-association inactivity-timeout 200
  transform-set AutVPN
  ip nat crypto
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#no use ip-
access-list
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#no security-
association level perhost
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#no ip nat crypto
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#no pfs
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#no local-
endpoint-ip
```

The following example shows the IPSec site-to-site VPN tunnel 'test' settings after the 'no' commands are executed:

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#show context
 crypto map test 1 ipsec-isakmp
  peer 1 ikev2 ikev2Peer1
  security-association lifetime kilobytes 250000
  security-association inactivity-timeout 200
  transform-set AutoVPN
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#
```

The following example shows the IPSec remote VPN client ‘test’ settings before the ‘no’ commands are executed:

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#show context
 crypto map test 2 ipsec-isakmp dynamic
  use ip-access-list test2
  peer 1 ikev1 RemoteIKEv1Peer1
  local-endpoint-ip 157.235.204.62
  pfs 14
  security-association lifetime seconds 10000
  transform-set RemoteVPN
  remote-type none
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#no use ip-
access-list
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#no peer 1
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#no transform-set
```

The following example shows the IPSec remote VPN client ‘test’ settings after the ‘no’ commands are executed:

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#show context
 crypto map test 2 ipsec-isakmp dynamic
  local-endpoint-ip 157.235.204.62
  pfs 14
  security-association lifetime seconds 10000
  remote-type none
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#
```

### 7.1.17.5.12 crypto-map-ipsec-manual-instance

*crypto-map-config-commands*

To navigate to the automatic IPSec manual VPN tunnel configuration instance, use the following command:

In the device-config mode:

```
<DEVICE>(config-device-<DEVICE-MAC>)#crypto map <CRYPTO-MAP-TAG> <1-1000> ipsec-
manual
```

In the profile-config mode:

```
<DEVICE>(config-profile-<PROFILE-NAME>)#crypto map <CRYPTO-MAP-TAG> <1-1000>
ipsec-manual

rfs4000-229D58(config-device-00-23-68-22-9D-58)#crypto map test 3 ipsec-manual
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#3)#?
Manual Crypto Map Configuration commands:
  local-endpoint-ip     Use this IP as local tunnel endpoint address, instead
                        of the interface IP (Advanced Configuration)
  mode                  Set the tunnel mode
  no                    Negate a command or set its defaults
  peer                  Set peer
  security-association  Set security association parameters
  session-key           Set security session key parameters
  use                   Set setting to use

  clrscr                Clears the display screen
  commit                Commit all changes made in this session
  do                    Run commands from Exec mode
  end                   End current mode and change to EXEC mode
  exit                  End current mode and down to previous mode
  help                  Description of the interactive help system
  revert                Revert changes
  service               Service Commands
  show                  Show running system information
  write                 Write running configuration to memory or terminal

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#3)#
```

The following table summarizes IPSec manual VPN tunnel configuration mode commands:

| Command | Description | Reference |
|---|---|---|
| *local-endpoint-ip* | Uses the configured IP as local tunnel endpoint address, instead of the interface IP (Advanced Configuration) | *page 7-128* |
| *mode* | Sets the tunnel mode | *page 7-129* |
| *peer* | Sets the peer device's IP address | *page 7-130* |
| *security-association* | Defines the lifetime (in kilobytes and/or seconds) of IPSec SAs created by a crypto map | *page 7-131* |
| *session-key* | Defines encryption and authentication keys for a crypto map | *page 7-132* |
| *use* | Uses the configured IP access list | *page 7-134* |
| *no* | Removes or reverts crypto map IPSec manual settings | *page 7-135* |

### 7.1.17.5.13 local-endpoint-ip

*crypto-map-ipsec-manual-instance*

Uses the configured IP as local tunnel endpoint address, instead of the interface IP (Advanced Configuration)

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
local-endpoint-ip <IP>
```

**Parameters**

- `local-endpoint-ip <IP>`

| | |
|---|---|
| local-endpoint-ip <IP> | Uses the configured IP as local tunnel's endpoint address<br>• <IP> – Specify the IP address. The specified IP address must be available on the interface. |

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-cryptomap-map1#1)#local-endpoint-
ip 172.16.10.3
```

### 7.1.17.5.14 mode

*crypto-map-ipsec-manual-instance*

Sets the crypto map tunnel mode

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
mode [transport|tunnel]
```

**Parameters**

- `mode [transport|tunnel]`

| | |
|---|---|
| mode [transport\|tunnel] | Sets the mode of the tunnel for this crypto map<br>• transport – Initiates transport mode<br>• tunnel – Initiates tunnel mode (default setting) |

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-cryptomap-map1#1)#mode transport

rfs6000-37FABE(config-profile-default-rfs6000-cryptomap-map1#1)#show context
 crypto map map1 1 ipsec-manual
  mode transport
rfs6000-37FABE(config-profile-default-rfs6000-cryptomap-map1#1)#
```

### 7.1.17.5.15 peer

*crypto-map-ipsec-manual-instance*

Sets the peer device's IP address. This can be set for multiple remote peers. The remote peer can be an IP address.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
peer <IP>
```

**Parameters**

- `peer <IP>`

| | |
|---|---|
| peer <IP> | Enter the peer device's IP address. If not configured, it implies respond to any peer. |

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-cryptomap-map1#1)#peer 172.16.10.12

rfs6000-37FABE(config-profile-default-rfs6000-cryptomap-map1#1)#show context
 crypto map map1 1 ipsec-manual
  peer 172.16.10.12
rfs6000-37FABE(config-profile-default-rfs6000-cryptomap-map1#1)#
```

### 7.1.17.5.16 security-association

*crypto-map-ipsec-manual-instance*

Defines the lifetime (in kilobytes and/or seconds) of IPSec SAs created by this crypto map

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
security-association lifetime [kilobytes <500-2147483646>|seconds <120-86400>]
```

**Parameters**

- `security-association lifetime [kilobytes <500-2147483646>|seconds <120-86400>]`

| | |
|---|---|
| lifetime [kilobytes <500-2147483646>\| seconds <120-86400>] | Values can be entered in both kilobytes and seconds. Which ever limit is reached first, ends the security association.<br>• kilobytes <500-2147483646> – Defines volume based key duration. Specify a value from 500 - 2147483646 bytes.<br>• seconds <120-86400> – Defines time based key duration. Specify the time frame from 120 - 86400 seconds. |

**NOTE:** This command is not applicable to the ipsec-manual crypto map.

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-cryptomap-map2#2)#security-
association lifetime seconds 123

rfs6000-37FABE(config-profile-default-rfs6000-cryptomap-map2#2)#show context
 Command not applicable to this crypto map
rfs6000-37FABE(config-profile-default-rfs6000-cryptomap-map2#2)#
```

### 7.1.17.5.17 session-key

*crypto-map-ipsec-manual-instance*

Defines encryption and authentication keys for this crypto map

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
session-key [inbound|outbound] [ah|esp] <256-4294967295>
session-key [inbound|outbound] ah <256-4294967295> [0|2|authenticator [md5|sha]]
<WORD>
session-key [inbound|outbound] esp <256-4294967295> [0|2|cipher [3des|aes|aes-192|
aes-256|des|esp-null]] <WORD> authenticator [md5|sha] <WORD>
```

**Parameters**

- `session-key [inbound|outbound] ah <256-4294967295> [0|2|authenticator [md5|sha]] <WORD>`

| | |
|---|---|
| session-key [inbound\|outbound] | Defines the manual inbound and outbound security association key parameters |
| ah <256-4294967295> | Configures *authentication header* (AH) as the security protocol for the security session<br>• <256-4294967295> – Sets the SPI for the security association from 256 - 4294967295<br>The SPI (in combination with the destination IP address and security protocol) identifies the security association. |
| [0\|2\|authenticator [md5\|sha] <WORD>] | Specifies the key type<br>• 0 – Sets a clear text key<br>• 2 – Sets an encrypted key<br>• authenticator – Sets AH authenticator details<br>  • md5 <WORD> – AH with MD5 authentication<br>  • sha <WORD> – AH with SHA authentication<br>  • <WORD> – Sets security association key value. The following key lengths (in hex characters) are required (w/o leading 0x).AH-MD5: 32, AH-SHA: 40 |

- `session-key [inbound|outbound] esp <256-4294967295> [0|2|cipher [3des|aes|aes-192|aes-256|des|esp-null]] <WORD> authenticator [md5|sha] <WORD>`

| | |
|---|---|
| session-key [inbound\|outbound] | Defines the manual inbound and outbound security association key parameters |
| esp <256-4294967295> | Configures *Encapsulating Security Payloads* (ESP) as the security protocol for the security session. This is the default setting.<br>• <256-4294967295> – Sets the SPI for the security association from 256 - 4294967295<br>The SPI (in combination with the destination IP address and security protocol) identifies the security association. |

| | |
|---|---|
| [0\|2\|cipher [3des\|aes\|aes-192\| aes-256\|des\| esp-null]] | • 0 – Sets a clear text key<br>• 2 – Sets an encrypted key<br>• cipher – Sets encryption/decryption key details<br>  • 3des – ESP with 3DES encryption<br>  • aes – ESP with AES encryption<br>  • aes-192 – ESP with AES-192 encryption<br>  • aes-256 – ESP with AES-256 encryption<br>  • des – ESP with DES encryption<br>  • esp-null – ESP with no encryption<br>  • authenticator – Specify ESP authenticator details<br>  • md5 <WORD> – ESP with MD5 authentication<br>  • sha <WORD> – ESP with SHA authentication<br>  • <WORD> – Sets security association key value. The following key lengths (in hex characters) are required (w/o leading 0x).AH-MD5: 32, AH-SHA: 40 |

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-cryptomap-map1#1)#session-key
inbound esp 273 cipher esp-null authenticator sha 58768979

rfs6000-37FABE(config-profile-default-rfs6000-cryptomap-map1#1)#show context
 crypto map map1 1 ipsec-manual
  peer 172.16.10.2
  mode transport
  session-key inbound esp 273 0 cipher esp-null authenticator sha 58768979
rfs6000-37FABE(config-profile-default-rfs6000-cryptomap-map1#1)#
```

### 7.1.17.5.18 use

*crypto-map-ipsec-manual-instance*

Associates an existing IP access list with this crypto map. The ACL protects the VPN traffic.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
use ip-access-list <IP-ACCESS-LIST-NAME>
```

**Parameters**

- `use ip-access-list <IP-ACCESS-LIST-NAME>`

| | |
|---|---|
| ip-access-list <IP-ACCESS-LIST-NAME> | Specify the IP access list name. |

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-cryptomap-map1#1)#use ip-access-
list test

rfs6000-37FABE(config-profile-default-rfs6000-cryptomap-map1#1)#show context
 crypto map map1 1 ipsec-manual
  use ip-access-list test
  peer 172.16.10.12
  mode transport
  session-key inbound esp 273 0 cipher esp-null authenticator sha 5876897
rfs6000-37FABE(config-profile-default-rfs6000-cryptomap-map1#1)#
```

### 7.1.17.5.19 no

*crypto-map-ipsec-manual-instance*

Removes or resets this crypto map's settings

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
no [local-endpoint-ip|mode|peer|security-association|session-key|use]
```

**Parameters**

- `no <PARAMETERS>`

| | |
|---|---|
| no <PARAMETERS> | Removes or resets this crypto map settings based on the parameters passed |

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-cryptomap-map1#1)#show context
 crypto map map1 1 ipsec-manual
  use ip-access-list test
  peer 172.16.10.12
  mode transport
  session-key inbound esp 273 0 cipher esp-null authenticator sha 5876897
rfs6000-37FABE(config-profile-default-rfs6000-cryptomap-map1#1)#

rfs6000-37FABE(config-profile-default-rfs6000-cryptomap-map1#1)#no use ip-access-
list
rfs6000-37FABE(config-profile-default-rfs6000-cryptomap-map1#1)#no peer
rfs6000-37FABE(config-profile-default-rfs6000-cryptomap-map1#1)#no mode

rfs6000-37FABE(config-profile-default-rfs6000-cryptomap-map1#1)#show context
 crypto map map1 1 ipsec-manual
  session-key inbound esp 273 0 cipher esp-null authenticator sha 58768979
rfs6000-37FABE(config-profile-default-rfs6000-cryptomap-map1#1)#
```

### 7.1.17.6 crypto-remote-vpn-client commands

*crypto*

This section documents the IKEV2 remote VPN client configuration settings. Use this command to define the server resources used to secure (authenticate) a remote VPN connection with a target peer.

Use the profile-config instance to configure remote VPN client settings. To navigate to the remote-vpn-client configuration instance, use the following commands:

```
<DEVICE>(config)#profile <DEVICE-TYPE> <PROFILE-NAME>
<DEVICE>(config-profile-<PROFILE-NAME>)#crypto remote-vpn-client
<DEVICE>(config-profile-<PROFILE-NAME>-crypto-ikev2-remote-vpn-client)#
```

**NOTE:** To configure remote VPN client settings on a device, on the device's configuration mode, use the *crypto > remote-vpn-client* command.
For example: rfs4000-229D58(config-device-00-23-68-22-9D-58)#crypto remote-vpn-client

**NOTE:** The following configuration enables a access point to adopt to a controller over the remote VPN link:
On a profile: rfs4000-229D58(config-profile-testRFS4000)#controller host <HOST-IP> remote-vpn-client

On a device: rfs4000-229D58(config-00-23-68-22-9D-58)#controller host <HOST-IP> remote-vpn-client

```
rfs4000-229D58(config)#profile rfs4000 testRFS4000
rfs4000-229D58(config-profile-testRFS4000)#

rfs4000-229D58(config-profile-testRFS4000)#crypto remote-vpn-client
rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#?
Crypto IKEV2 Remote Vpn Client Config commands:
  dhcp-peer      Configure parameters for peers received via DHCP option
  no             Negate a command or set its defaults
  peer           Add a remote peer
  shutdown       Disable remote vpn client
  transform-set  Specify IPSec transform to use

  clrscr         Clears the display screen
  commit         Commit all changes made in this session
  do             Run commands from Exec mode
  end            End current mode and change to EXEC mode
  exit           End current mode and down to previous mode
  help           Description of the interactive help system
  revert         Revert changes
  service        Service Commands
  show           Show running system information
  write          Write running configuration to memory or terminal

rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#
```

The following table summarizes crypto remote VPN client configuration mode commands:

| Command | Description | Reference |
|---|---|---|
| *dhcp-peer* | Configures DHCP peer's local ID and authentication settings | *page 7-138* |
| *peer* | Adds a remote IKEv2 peer | *page 7-139* |
| *shutdown* | Disables the remote VPN client | *page 7-140* |
| *transform-set* | Associates an existing IPSec transform set with this remote VPN client | *page 7-141* |
| *no* | Removes the remote VPN client settings | *page 7-142* |

### 7.1.17.6.1 dhcp-peer

*crypto-remote-vpn-client commands*

Configures DHCP peer's local ID and authentication settings

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
dhcp-peer [authentication|localid]

dhcp-peer authentication [psk [0 <WORD>|2 <WORD>|<WORD>]|rsa]

dhcp-peer localid [autogen-uniqueid <WORD>|string <WORD>]
```

**Parameters**

- `dhcp-peer authentication [psk [0 <WORD>|2 <WORD>|<WORD>]|rsa]`

| | |
|---|---|
| dhcp-peer authentication psk [0 <WORD>\| 2 <WORD>\| <WORD>] | Configures the DHCP peer's authentication type as PSK<br>• 0 <WORD> – Configures a clear text authentication key<br>• 2 <WORD> – Configures an encrypted authentication key<br>• <WORD> – Provide a 8 - 21 character shared key password for DHCP peer authentication |
| dhcp-peer authentication rsa | Configures the DHCP peer's authentication type as RSA. This is the default setting. |

- `dhcp-peer localid [autogen-uniqueid <WORD>|string <WORD>]`

| | |
|---|---|
| dhcp-peer localid [autogen-uniqueid <WORD>\| string <WORD>] | Configures the DHCP peer's localid using one of the following options:<br>• autogen-uniqueid - Generates a localid using the device's unique identity. The system prefixes the device's unique identity to the string provided here. The device's unique identity should be existing and configured. For more information on configuring a device's unique identity, see *autogen-uniqueid*.<br>  • <WORD> – Provide the string.<br>• string - Uses the value provided here as the DHCP peer's localid.<br>  • <WORD> - Provide the string. |

**Example**

```
rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#dhcp-
peer authentication psk 0 @123testing

rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#show
context
 crypto remote-vpn-client
  dhcp-peer authentication psk 0 @123testing
rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#
```

### 7.1.17.6.2 peer

*crypto-remote-vpn-client commands*

Configures IKEv2 peers and assigns them priorities for utilization with remote VPN client connections. A maximum of three (3) peers can be added to support redundancy.

IKEv2 uses an initial handshake in which VPN peers negotiate cryptographic algorithms, mutually authenticate, and establish a session key, creating an IKE-SA. Additionally, a first IPSec SA is established during the initial SA creation. All IKEv2 messages are request/response pairs. It is the responsibility of the side sending the request to retransmit if it does not receive a timely response.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
peer <1-3> ikev2 <IKEV2-PEER-NAME>
```

**Parameters**

- `peer <1-3> ikev2 <IKEV2-PEER-NAME>`

| | |
|---|---|
| peer <1-3> | Adds a IKEv2 peer. You can add maximum of three (3) peers to achieve redundancy.<br>• <1-3> – Specify a priority level for the peer from 1 - 3 (1 = primary, 2 = secondary, and 3 = redundant). |
| ikev2 <IKEV2-PEER-NAME> | Specify the IKEv2 peer's name.<br>**Note:** The peer should be existing and configured. To configure an IKEv2 peer use the *crypto > ikev2 > peer > <IKEv2-PEER-NAME>* command. |

**Example**

```
rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#peer
1 ikev2 ikev2Peer1

rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#peer 2
 ikev2 ikev2Peer2

rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#show
context
 crypto remote-vpn-client
  peer 1 ikev2 ikev2Peer1
  peer 2 ikev2 ikev2Peer2
rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#
```

### 7.1.17.6.3 shutdown

*crypto-remote-vpn-client commands*

Disables remote-vpn-client on this profile or device. Remote VPN client feature is enabled by default.

To enable a disabled remote VPN client execute the *no > shutdown* command.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
shutdown
```

**Parameters**

None

**Example**

```
rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#
shutdown
rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#
```

### 7.1.17.6.4 transform-set

*crypto-remote-vpn-client commands*

Specifies the IPSec Transform set to use with this remote VPN client. A transform set is a combination of security protocols, algorithms, and other settings applied to IPSec protected client traffic.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
transform-set <IPSEC-XFORM-TAG> {<IPSEC-XFORM-TAG>}
```

**Parameters**

- `transform-set <IPSEC-XFORM-TAG> {<IPSEC-XFORM-TAG>}`

| | |
|---|---|
| transform-set <IPSEC-XFORM-TAG> <IPSEC-XFORM-TAG> | Associates an IPSec Transform (should be existing and configured) set with this remote VPN client. You can optionally associate more than one transform set with this remote VPN client configuration. List the transform set tags separated by a space.<br>**Note:** To configure a transform-set, use the *crypto > ipsec > transform-set* command in the profile or device configuration mode. |

**Example**

```
rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-
client)#transform-set TransformSet1

rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#show
context
 crypto remote-vpn-client
  peer 1 ikev2 ikev2Peer1
  transform-set TransformSet1
rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#
```

### 7.1.17.6.5 no

*crypto-remote-vpn-client commands*

Removes the remote VPN client settings

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
no [dhcp-peer|peer <1-3>|shutdown|transform-set]

no dhcp-peer [authentication|localid]

no peer <1-3>

no shutdown

no transform-set
```

**Parameters**

- no <PARAMETERS>

| | |
|---|---|
| no <PARAMETERS> | Removes or resets this remote VPN client settings based on the parameters passed |

**Example**

```
rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#show
context
 crypto remote-vpn-client
  peer 1 ikev2 peer5
rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#

rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#no peer
1

rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#show
context
 crypto remote-vpn-client
rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#
```

## 7.1.18 database

*Profile Config Commands*

Backs up captive-portal and/or NSight database to a specified location and file. When applied to devices, this profile will enable the back up of the specified database. This command also enables you to configures a low-disk-space threshold value.

These parameters can also be configured in the device configuration context of an NX95XX series service platform.

**Supported in the following platforms:**

- Service Platforms — NX9500, NX9510, NX9600, VX9000

**Syntax**

```
database [backup|low-disk-space-threshold]

database backup database [captive-portal|nsight] <URL>

database low-disk-space-threshold <10-50>
```

**Parameters**

- `database backup database [captive-portal|nsight] <URL>`

| | |
|---|---|
| database backup database [captive-portal\| nsight] | Backs up captive portal and/or NSight database to a specified location and file. Select the database to backup.<br>• database – Selects the database to backup<br>  • captive-portal – Backs up captive portal database<br>  • nsight – Backs up NSight database<br>After specifying the database type, configure the destination location and file name. |
| <URL> | Configures the destination location. The database is backed up at the specified location. Specify the location URL in one of the following formats:<br>ftp://<user>:<passwd>@<hostname\|IP>[:port]/path/file.tar.gz<br>sftp://<user>:<passwd>@<hostname\|IP>[:port]/path/file.tar.gz<br>tftp://<hostname\|IP>[:port]/path |

- `database low-disk-space-threshold <10-50>`

| | |
|---|---|
| database low-disk-space-threshold <10-50> | Configures the low disk space threshold for syslog warning. Once the threshold value configured here is reached a syslog warning is sent.<br>• <10-50> – Specify the threshold from 10 - 50. The default is 30. |

**Example**

```
nx9500-6C8809(config-profile-testNX9500)#database backup database nsight ftp://
anonymous:anonymous@192.168.13.10/backups/nsight/nsight.tar.gz
```

**Related Commands**

| | |
|---|---|
| *no* | Removes database backup configurations |

## 7.1.19 device-onboard

*Profile Config Commands*

Configures the logo image file name and title displayed on the EGuest device-onboarding portal. The EGuest UI can be accessed only by vendor-admin users.

**NOTE:** Vendor admin users are configured in the Management policy context. For more information, see *user*.

**Supported in the following platforms:**

- Service Platforms — NX9500, NX9510, NX9600, VX9000

**Syntax**

```
device-onboard [logo|title] <WORD>
```

**Parameters**

- `device-onboard [logo|title] <WORD>`

| | |
|---|---|
| device-onboard [logo\|title] <WORD> | Configures the logo and page title displayed on the device-onboarding portal<br>• logo – Specify the logo image file name. Note, logo image dimensions must not exceed 109 pixel and 52 pixel in width and height respectively.<br>• title – Specify the UI portal title. Note, the title should not exceed 32 characters in length.<br>The following keyword is common to both of the above parameters:<br>• <WORD> – Specify the logo image file name/page title. |

**Example**

```
Split-EG-Server(config-device-00-0C-29-09-3C-CC)#device-onboard logo
extremenetworks.png

Split-EG-Server(config-device-00-0C-29-09-3C-CC)#device-onboard title EXTREME
NETWORKS ONBOARDING UI

Split-EG-Server(config-device-00-0C-29-09-3C-CC)#show context include-factory |
include device-onboard
 device-onboard title EXTREME NETWORKS ONBOARDING UI
 device-onboard logo extremenetworks.png
Split-EG-Server(config-device-00-0C-29-09-3C-CC)#

Following example shows a Management Policy, vendor-admin user configuration:

EC-NOC(config-management-policy-EGuest)#show context include-factory | include
user
 user onboard-user password 1
1d5e9d60425bde727261b66b5e7eb0236058e7aae45225961ce7b872ea238240 role vendor-
admin group Samsung,Philips,Nest1,Orbit1
EC-NOC(config-management-policy-EGuest)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the device-onboarding UI portal's logo image file name and title configuration |

## 7.1.20 device-upgrade

*Profile Config Commands*

Configures device firmware upgrade settings on this profile

Administrators can customize profiles with unique device configuration file and firmware upgrade support. In a clustered environment, operations performed on one device are propagated to each member of the cluster and then onwards to devices managed by each cluster member. The number of concurrent device upgrades and their start times can be customized to ensure a sufficient number of devices remain in duty while upgrades are administered to others.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
device-upgrade [add-auto|auto|count|persist-images]

device-upgrade add-auto [(ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|
ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|
rfs4000|rfs6000|nx5500|nx75xx|nx9000|nx9600)]

device-upgrade auto {(ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|
ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|
rfs6000|nx5500|nx75xx|nx9000|nx9600)}

device-upgrade count <1-128>

device-upgrade persist-images
```

**Parameters**

```
• device-upgrade add-auto[(ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|
ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|
rfs4000|rfs6000|nx5500|nx75xx|nx9000|nx9600)]
```

| | |
|---|---|
| device-upgrade add-auto | Configures a list of devices types for automatic firmware upgrade<br>This command specifies the types of devices that can be automatically upgraded (if enabled). To enable automatic device firmware upgrade, use the 'auto' command. When enabled, access points, wireless controllers, and service platforms, using this profile, will automatically upgrade firmware on adopted devices that match the specified device types. |
| [<DEVICE-TYPE>] | Specifies the type of devices to be upgraded. Select the device type. The options are: AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533, RFS4000, RFS6000, NX5500, NX75XX, NX95XX, NX9600, VX9000.<br>**Note:** Multiple device types can be added to the add-auto list. |

- `device-upgrade auto {(ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|rfs6000|nx5500|nx75xx|nx9000|nx9600)}`

| | |
|---|---|
| device-upgrade auto | Enables automatic firmware upgrade on specified device types. When used along with the add-auto command, the auto command allows access points, wireless controllers, and service platforms to automatically upgrade firmware on adopted devices matching the specified device types. |
| <DEVICE-TYPE> | Optional. Specifies the type of device to be lined up for automatic firmware upgrade. The options are: AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533, RFS4000, RFS6000, NX5500, NX75XX, NX95XX, NX9600, VX9000.<br>**Note:** Multiple device types can be added to the auto list. |

- `device-upgrade count <1-128>`

| | |
|---|---|
| device-upgrade count <1-128> | Configures the maximum number of concurrent upgrades possible<br>• <1-128> – specify a value from 1 - 128. The default is 10. |

- `device-upgrade persist-images`

| | |
|---|---|
| device-upgrade | Configures parameters for automatic firmware upgrade of adopted devices. Use this command to select the device types and the maximum number of concurrent upgrades. |
| persist-images | Enables RF Domain manager to retain AP firmware image after upgrade, subject to availability of space. This option is enabled by default.<br>This option is enabled for all controllers and service platforms RF Domain managers with the flash memory capacity to store firmware images for the selected access point models they provision. This feature is disabled for access point RF Domain managers that do not typically have the flash memory capacity needed. |

**Example**

```
rfs4000-229D58(config-profile-default-rfs4000)#device-upgrade auto ap71xx

rfs4000-229D58config-profile-default-rfs4000)#show context
profile rfs4000 default-rfs4000
 autoinstall configuration
 autoinstall firmware
 device-upgrade auto ap71xx
 device-upgrade persist-ap-image
 crypto ikev1 policy ikev1-default
  qos trust 802.1p
--More--
rfs4000-229D58(config-profile-default-rfs4000)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes device firmware upgrade settings on this profile |
| *device-upgrade* (show commands) | Displays device upgrade details |

## 7.1.21 diag

*Profile Config Commands*

Enables looped packet logging. When enabled, devices, using this profile, start logging looped packets to a separate queue. This option is disabled by default.

Looped packet logging can also be enabled in the device configuration context.

**NOTE:** To view logged looped packets, execute the *service > show > diag > pkts* command. For more information, see *service*.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
diag pkts
```

**Parameters**

```
• diag pkts
```

| | |
|---|---|
| diag pkts | Enables looped packet logging |

**Example**

```
nx9500-6C8809(config-profile-default-nx75xx)#diag pkts

nx9500-6C8809(config-profile-default-nx75xx)#show context include-factory |
include diag
 diag pkts
nx9500-6C8809(config-profile-default-nx75xx)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables looped packet logging |

## 7.1.22 dot1x

*Profile Config Commands*

Configures 802.1x standard authentication controls

Dot1x (or 802.1x) is an IEEE standard for network authentication. It enables media-level (layer 2) access control, providing the capability to permit or deny connectivity based on user or device identity. Dot1x allows port-based access using authentication. An dot1x enabled port can be dynamically enabled or disabled depending on user identity or device connection.

Devices supporting dot1x allow the automatic provision and connection to the wireless network without launching a Web browser at login. When within range of a dot1x network, a device automatically connects and authenticates without needing to manually login.

Before authentication, the endpoint is unknown, and traffic is blocked. Upon authentication, the endpoint is known and traffic is allowed. The controller or service platform uses source MAC filtering to ensure only the authenticated endpoint is allowed to send traffic.

*Dot1x authentication capabilities is supported on the following platforms:*

**Supported in the following platforms:**

- Access Points — AP6511, AP6521, AP6522, AP6562, AP7161, AP7502, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432
- Wireless Controllers — RFS4000, RFS6000, NX5500, NX7500

*Dot1x supplicant capabilities is supported on the following platforms:*

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, NX5500, NX7500

**Syntax**

```
dot1x [guest-vlan|holdtime|system-auth-control|use]

dot1x holdtime <0-600>
dot1x system-auth-control
dot1x guest-vlan supplicant
dot1x use aaa-policy <AAA-POLICY-NAME>
```

**Parameters**

- `dot1x system-auth-control`

| | |
|---|---|
| system-auth-control | Enables system auth control. Enables dot1x authorization globally for the controller. This feature is disabled by default. |

- `dot1X holdtime <0-600>`

| | |
|---|---|
| holdtime <0-600> | Configures a holdtime value. This is the interval after which an authentication attempt is ignored or failed.<br>• <0-600> – Specify a value from 0 - 600 seconds. A value of '0' indicates no holdtime. The default is 600 seconds or 10 minutes.<br>Adding a hold time at startup allows time for the network to converge before receiving or transmitting 802.1x authentication packets. |

- `dot1x guest-vlan supplicant`

| | |
|---|---|
| guest-vlan | Configures guest VLAN and supplicant behavior<br>This feature is disabled by default. |
| supplicant | Allows 802.1x capable supplicant to enter guest VLAN. When enabled, this is the VLAN that supplicant's traffic is bridged on. |

- `dot1x use aaa-policy <AAA-POLICY-NAME>`

| | |
|---|---|
| use aaa-policy <AAA-POLICY-NAME> | Associates a specified 802.1x AAA policy (for MAC authentication) with this access point profile<br>• <AAA-POLICY-NAME> – Specify the AAA policy name. Once specified, this AAA policy is utilized for authenticating user requests. |

**Example**

```
nx9500-6C8809(config-profile-test-nx5500)#dot1x use aaa-policy OnBoarding

nx9500-6C8809(config-profile-test-nx5500)#dot1x system-auth-control

nx9500-6C8809(config-profile-test-nx5500)#show context
profile nx5500 test-nx5500
 no autoinstall configuration
 no autoinstall firmware
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 crypto load-management
 crypto remote-vpn-client
 interface ge1
 interface ge2
 interface ge3
 interface ge4
 interface ge5
 interface ge6
 interface pppoe1
 use firewall-policy default
 service pm sys-restart
 router ospf
 router bgp
 dot1x system-auth-control
 dot1x use aaa-policy OnBoarding
nx9500-6C8809(config-profile-test-nx5500)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables or reverts settings to their default |

## 7.1.23 dpi

*Profile Config Commands*

Enables *Deep Packet Inspection* (DPI) on this profile. DPI is an advanced packet analysis technique, which analyzes packet and packet content headers to determine the nature of network traffic. When enabled, DPI inspects packets of all flows to identify applications (such as, Netflix, Twitter, Facebook, etc.) and extract metadata (such as, host name, server name, TCP-RTT, etc.) for further use by the WiNG firewall.

This command is also available in the device configuration mode.

**Supported in the following platforms:**

- Access Points — AP7522, AP7532, AP7602, AP7612, AP7622, AP7632, AP7662
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

**Syntax**

```
dpi {custom-app|logging|metadata}

dpi {custom-app <CUSTOM-APP-NAME>}

dpi {logging [level [<0-7>|alerts|critical|debugging|emergencies|errors|
informational|notifications|warnings]|on]}

dpi {metadata [http|ssl|tcp-rtt|voice-video]}

dpi {metadata [http|ssl|voice-video]}

dpi {metadata tcp-rtt {app-group <APPLICATION-GROUP-NAME>}}
```

**Parameters**

- `dpi {custom-app <CUSTOM-APP-NAME>}`

| | |
|---|---|
| dpi | Enables DPI on this profile/device context and configures DPI settings. When enabled, all flow traffic is subjected to DPI for detection of applications, application categories, custom applications, and metadata extraction. |
| custom-app <CUSTOM-APP-NAME> | Optional. Adds custom application to this profile<br>• <CUSTOM-APP-NAME> – Specify custom application name (should be existing and configured)<br>If no custom application is specified, the system detects the PACE built-in applications.<br>**Note:** For more information on application categories and application detection, see *application*. |

- `dpi {logging [level [<0-7>|alerts|critical|debugging|emergencies|errors|informational|notifications|warnings]|on]}`

| | |
|---|---|
| dpi | Enables DPI on this profile/device context and configures DPI settings. When enabled, all flow traffic is subjected to DPI for detection of applications, application categories, custom applications, and metadata extraction. |

| | |
|---|---|
| logging [level [<0-7>\|alerts\|critical\|debugging\|emergencies\|errors\|informational\|notifications\|warnings]\|on] | Optional. Enables DPI logging and sets the logging level<br>• level – Configures the DPI logging level. Use one of the following options to specify the logging level:<br>• <0-7> Logging severity level<br>• alerts Immediate action needed (1)<br>• critical Critical conditions (2)<br>• debugging Debugging messages (7)<br>• emergencies System is unusable (0)<br>• errors Conditions (3)<br>• nformational Informational messages (6)<br>• notifications Normal but significant conditions (5) - Default setting<br>• warnings Warning conditions (4)<br>Either specify the logging level index (from 0 - 7) or the description. For example, to log all alerts either enter '1' or 'alerts'.<br>• on – Enables application detection event logging. DPI logging is disabled by default. |

- `dpi {metadata [http|ssl|voice-video]}`

| | |
|---|---|
| dpi | Enables DPI on this profile/device context and configures DPI settings. When enabled, all flow traffic is subjected to DPI for detection of applications, application categories, custom applications, and metadata extraction. |
| metadata [http\|ssl\|voice-video] | Optional. Enables metadata extraction from following flows:<br>• http – HTTP flows. This option is disabled by default.<br>• ssl – SSL flows. This option is disabled by default.<br>• voice-video – Voice and video classified flows. This option is disabled by default. |

- `dpi {metadata tcp-rtt {app-group <APPLICATION-GROUP-NAME>}}`

| | |
|---|---|
| dpi | Enables DPI on this profile/device context and configures DPI settings. When enabled, all flow traffic is subjected to DPI for detection of applications, application categories, custom applications, and metadata extraction. |
| metadata tcp-rtt {app-group <APPLICATION-GROUP-NAME>} | Optional. Enables *Transmission Control Protocol - Round Trip Time* (TCP-RTT) metadata collection for application groups. Before executing this command, ensure that you have created at least one application group.<br>Enable this option in the profile/device contexts of the AP7522, AP7532, AP7562, AP8432, AP8533 access point models, as only these APs support TCP-RTT metadata collection.<br>• app-group – Optional. Specifies the customized application-group name containing the applications for which TCP-RTT is to be collected<br>• <APPLICATION-GROUP-NAME> – Specify the app-group name (should be existing and configured). If not specified, the system collects TCP-RTT metadata for all the customized app-groups created. You can enable TCP-RTT metadata collection on eight (8) application groups at a time.<br>For more information on creating customized application-groups, see *application-group*.<br>The TCP-RTT metadata is viewable only on the NSight dashboard. Therefore, ensure the NSight server and database is up and NSight analytics data collection is enabled. |

**Example**

```
nx9500-6C8809(config-profile-testNX9500)#dpi logging on

nx9500-6C8809(config-profile-testNX9500)#dpi logging level 7

nx9500-6C8809(config-profile-testNX9500)#show context
profile nx9000 testNX9500
 bridge vlan 10
  ip igmp snooping
  ip igmp snooping querier
  ipv6 mld snooping
.....................................................
 router bgp
 dpi logging on
 dpi logging level debugging
nx9500-6C8809(config-profile-testNX9500)#

nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#dpi metadata tcp-rtt app-group
amazon
```

**Related Commands**

| | |
|---|---|
| *no* | Disables DPI (application assurance) on this profile |

## 7.1.24 dscp-mapping

*Profile Config Commands*

Configures IP *Differentiated Services Code Point* (DSCP) to 802.1p priority mapping for untagged frames

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
dscp-mapping <WORD> priority <0-7>
```

**Parameters**

- `dscp-mapping <word> priority <0-7>`

| | |
|---|---|
| <WORD> | Specifies the DSCP value of a received IP packet. This could be a single value or a list. For example, 10-20, 25, 30-35. |
| priority <0-7> | Specifies the 802.1p priority to use for a packet if untagged. The priority is set on a scale of 0 - 7. The priority values are:<br>• 0 – Best effort<br>• 1 – Background<br>• 2 – Spare<br>• 3 – Excellent effort<br>• 4 – Controlled load<br>• 5 – Video<br>• 6 – Voice<br>• 7 – Network control<br>**Note:** The specified 802.1p priority value is added as a 3-bit IP precedence value in the *Type of Service* (ToS) field of the IP header used to set the priority. Up to 64 entries are permitted. |

**Example**

```
rfs7000-37FABE(config-profile-default-rfs7000)#dscp-mapping 20 priority 7

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
 dscp-mapping 20 priority 7
 no autoinstall configuration
 no autoinstall firmware
 crypto isakmp policy default
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 interface me1
 interface ge1
 ip dhcp trust
 qos trust dscp
rfs7000-37FABE(config-profile-default-rfs7000)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables or reverts settings to their default |

## 7.1.25 eguest-server (VX9000 only)

*Profile Config Commands*

Enables the *ExtremeGuest* (EGuest) server

The WiNG EGuest solution is an independently installable VM/Server that provides integrated guest management and analytics. Use this command to enable the EGuest daemon on the EGuest server.

**NOTE:** EGuest being a licensed feature, ensure that the EGUEST-DEV license is applied on the EGuest server's self context. For more information, see *license*.

**Supported in the following platforms:**

- Service Platforms — VX9000

**NOTE:** For more information on configuring an EGuest captive-portal deployment, see *configuring ExtremeGuest captive-portal*.

**Syntax**

```
eguest-server
```

**Parameters**

- `eguest-server`

| | |
|---|---|
| eguest-server | Execute this command, without the 'host' option, on the EGuest server. When executed, the EGuest daemon is enabled on the host.<br>EGuest server can be hosted only a VX9000 platform. |

**Example**

On the EGuest server, execute the command without the 'host' option to enable the EGuest daemon.

```
EG-Server(config-device-02-EE-1A-7E-AE-5B)#eguest-server

EG-Server(config-device-02-EE-1A-7E-AE-5B)#show context include-factory | include
eguest-server
 eguest-server
EG-Server(config-device-02-EE-1A-7E-AE-5B)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables the EGuest server by stopping the EGuest daemon |

## 7.1.26 eguest-server (NOC Only)

*Profile Config Commands*

Points to the EGuest server when executed along with the 'host' option. The WiNG EGuest solution is an independently installable VM/Server that provides integrated guest management and analytics. Use this command to enable the EGuest daemon on the EGuest server.

**NOTE:** EGuest being a licensed feature, ensure that the EGUEST-DEV license is applied on the EGuest server's self context. For more information, see *license*.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**NOTE:** For more information on configuring an EGuest captive-portal deployment, see *configuring ExtremeGuest captive-portal*.

**Syntax**

```
eguest-server <1-3> host <IPv4/IPv6/HOSTNAME> {http|https}
```

**Parameters**

- `eguest-server <1-3> host <IPv4/IPv6/HOSTNAME> {http|https}`

| | |
|---|---|
| eguest-server <1-3> host <IPv4/IPv6/HOSTNAME> *{http/https}* | Configures the EGuest server details in the profile/device context of the NOC (access point/controller). When configured, the NOC posts registration requests and captive-portal related data directly to the specified EGuest server.<br>• <1-3> – Configures the EGuest server index number. A maximum of three EGuest servers can be configured.<br>• host <IPv4/IPv6/HOSTNAME> – Configures the EGuest server's IPv4/IPv6 address or hostname.<br>• {http\|https} – Optional. Configures the mode of connection as HTTP or HTTPS.<br>**Note:** HTTPS is recommended as it uses encryption for transmission and is therefore more secure. |

**Example**

On the NOC, execute along with the 'host' option to point to the EGuest server.

```
EG-NOC(config-device-74-67-F7-5C-64-4A)#eguest-server 1 host EG-Server https

EG-NOC(config-device-74-67-F7-5C-64-4A)#show context include-factory | include
eguest-server
 no eguest-server
 eguest-server 1 host EG-Server https
EG-NOC(config-device-74-67-F7-5C-64-4A)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the EGuest server IP address/hostname configuration |

## 7.1.27 email-notification

*Profile Config Commands*

Configures e-mail notification settings. When a system event occurs e-mail notifications are sent (provided message logging is enabled) based on the settings configured here. Use this option to configure the outgoing SMTP server settings.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
email-notification [host|recipient]

email-notification recipient <RECIPIENT-NAME>

email-notification host <SMTP-SERVER-IP/HOSTNAME> sender <SENDER-EMAIL>
[port|security|username]

email-notification host <SMTP-SERVER-IP/HOSTNAME> sender <SENDER-EMAIL> [(port <1-
65535>, security [none|ssl|starttls], username <SMTP-USERNAME> password [2 <WORD>|
<WORD>])]
```

**Parameters**

- `email-notification recipient <RECIPIENT-EMAIL>`

| | |
|---|---|
| recipient <RECIPIENT-EMAIL> | Defines the recipient's e-mail address. A maximum of 6 (six) e-mail addresses can the configured.<br>• <RECIPIENT-EMAIL> – Specify the recipient's e-mail address (should not exceed 64 characters in length). |

- `email-notification host <SMTP-SERVER-IP/HOSTNAME> sender <SENDER-EMAIL> [(port <1-65535>, security [none|ssl|starttls], username <SMTP-USERNAME> password [2 <WORD>|<WORD>])]`

| | |
|---|---|
| host <SMTP-SERVER-IP/ HOSTNAME> | Configures the host SMTP server's IP address or hostname<br>• <SMTP-SERVER-IP/HOSTNAME> – Specify the SMTP server's IP address or hostname. |
| sender <SENDER-EMAIL> | Defines the sender's e-mail address. This is the from address on notification e-mails.<br>• <SENDER-EMAIL> – Specify the sender's e-mail address (should not exceed 64 characters in length). Use the *email-notification > recipient > <EMAIL-ADDRESS>* command to configure the recipient's address. |
| port <1-65535> | This option is recursive and applicable to the 'security' and 'username' parameters.<br>Configures the SMTP server port. Use this option to configure a non-standard SMTP port on the outgoing SMTP server. The standard SMTP port is 25.<br>• <1-65535> – Specify the port from 1 - 65535. |

| | |
|---|---|
| security [none\|ssl\|starttls] | This option is recursive and applicable to the 'port' and 'username' parameters.<br>Configures the SMTP encryption type used<br>• none – No encryption used<br>• ssl – Uses *Secure Sockets Layer* (SSL) encryption between the SMTP server and the client<br>• starttls – Uses STARTTLS encryption between the SMTP server and the client |
| username <SMTP-USERNAME> password [2 <WORD>\| <WORD>] | This option is recursive and applicable to the 'port' and 'security' parameters.<br>Configures the SMTP sender's username. Many SMTP servers require users to authenticate with a username and password before sending e-mail through the server.<br>• <SMTP-USERNAME> – Specify the SMTP username (should not exceed 64 characters in length).<br>• password – Configures the SMTP server password. Specify the password associated with the username of the sender on the outgoing SMTP server.<br>• 2 <WORD> – Configures an encrypted password<br>• <WORD> – Specify the password (should not exceed 127 characters in length). |

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000)#email-notification recipient
test@examplecompany.com

rfs6000-37FABE(config-profile-default-rfs6000)#show context
profile rfs7000 default-rfs7000
 dscp-mapping 20 priority 7
 no autoinstall configuration
 no autoinstall firmware
 ..........................................................
 interface ge4
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 use firewall-policy default
 email-notification recipient test@examplecompany.com
 service pm sys-restart
rfs6000-37FABE(config-profile-default-rfs6000)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables or reverts settings to their default |

## 7.1.28 enforce-version

*Profile Config Commands*

Enables checking of a device's firmware version before attempting adoption or clustering

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
enforce-version [adoption|cluster] [full|major|minor|none|strict]
```

**Parameters**

- `enforce-version [adoption|cluster] [full|major|minor|none|strict]`

| | |
|---|---|
| adoption | Verifies firmware versions before adopting. This option is enabled by default. |
| cluster | Verifies firmware versions before clustering. This option is enabled by default. |
| full | Allows adoption or clustering when the first four octets of the firmware versions match (for example 5.8.6.0) |
| major | Allows adoption or clustering when the first two octets of the firmware versions match (for example 5.8) |
| minor | Allows adoption or clustering when the first three octets of the firmware versions match (for example 5.8.6) |
| none | Allows adoption or clustering between any firmware versions |
| strict | Allows adoption or clustering only when firmware versions exactly match (for example 5.8.6.0-008B). This is the default setting for both 'adoption' and 'cluster' options. |

**Example**

```
nx9500-6C8809(config-profile-test-nx5500)#enforce-version cluster full
nx9500-6C8809(config-profile-test-nx5500)#enforce-version adoption major

nx9500-6C8809(config-profile-test-nx5500)#show context
profile nx5500 test-nx5500
 no autoinstall configuration
 no autoinstall firmware
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 ..................................................
interface pppoe1
 use firewall-policy default
 enforce-version adoption major
 enforce-version cluster full
 service pm sys-restart
 router ospf
 router bgp
 dot1x system-auth-control
 dot1x use aaa-policy OnBoarding
nx9500-6C8809(config-profile-test-nx5500)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables or reverts settings to their default |

## 7.1.29 environmental-sensor

*Profile Config Commands*

Configures the environmental sensor settings

An AP8132 sensor module is a USB environmental sensor extension to an AP8132 model access point. It provides a variety of sensing mechanisms, allowing the monitoring and reporting of the AP8132's radio coverage area.

**Supported in the following platforms:**

- Access Points — AP8132

**Syntax**

```
environmental-sensor [humidity|light|motion|polling-interval|temperature]

environmental-sensor [humidity|motion|polling-interval <1-100>|temperature]

environmental-sensor light {holdtime|radio-shutdown|threshold}

environmental-sensor light {holdtime <10-201>|radio-shutdown [all|radio-1|radio-2]}

environmental-sensor light {threshold [high <100-10000>|low <0-1000>]}
```

**Parameters**

- `environmental-sensor [humidity|motion|polling-interval <1-100>|temperature]`

| | |
|---|---|
| environmental-sensor | Configures environmental sensor settings on this profile |
| humidity | Enables (turns on) humidity sensors. This setting is enabled by default. |
| motion | Enables (turns on) motion sensors.This setting is enabled by default. |
| polling-interval <1-100> | Configures polling interval, in seconds, on all sensors. This is the interval after which the sensor module polls its environment to assess the various parameters, such as light intensity.<br>• <1-100> – Specify a value from 1 - 100 seconds. The default is 5 seconds. |
| temperature | Enables (turns on) temperature sensors. This setting is enabled by default. |

- `environmental-sensor light {holdtime <10-201>|radio-shutdown [all|radio-1|radio-2]}`

| | |
|---|---|
| environmental-sensor | Configures environmental sensor settings on this profile |
| light | Enables (turns on) light sensors and specifies its settings<br>When enabled, the sensor module polls the environment to determine the light intensity. Based on the reading, the system determines whether the AP8132's deployment location has lights on or off. Light intensity also helps determine whether the access point's deployment location is currently populated with clients. |
| holdtime <10-201> | Optional. Configures a holdtime, in seconds, for the light sensor<br>• <10-201> – Specify a value from 10 - 201 seconds. The default value is 11 seconds. |

| | |
|---|---|
| radio-shutdown [all\|radio1\|radio2] | Optional. Shuts down the sensor's radios<br>• all – Shuts down all radios. This is the default setting.<br>• radio1 – Shuts down radio 1<br>• radio2 – Shuts down radio 2<br>AP8132's using this profile have their radios shut down, when the radio's power falls below the specified threshold. Use the *environmental-sensor > light > threshold > [high\|low]* command to set the threshold values. |

- `environmental-sensor light {threshold [high <100-10000>|low <0-1000>]}`

| | |
|---|---|
| environmental-sensor | Configures environmental sensor settings on this profile |
| light | Enables (turns on) light sensors and specifies its settings |
| threshold | Optional. Configures the upper and lower thresholds for the amount of light in the environment |
| high <100-10000> | Specifies the upper threshold from 100 - 10000 lux. This value determines whether lighting is on in the AP8132's deployment location. The radios are turned off if the average reading value is lower than the value set here. The default is 400 lux.<br>The light sensor triggers an event if the amount of light exceeds the specified value. |
| low <0-1000> | Specifies the lower threshold from 0 - 1000 lux. This value determines whether lighting is off in the AP8132's deployment location. The radios are turned on when the average value is higher than the value set here. The default is 200 lux.<br>The light sensor triggers an event if the amount of light drops below the specified value. |

**Example**

```
rfs4000-229D58(config-profile-testRFS4000)#environmental-sensor humidity
rfs4000-229D58(config-profile-testRFS4000)#environmental-sensor polling-interval
60
rfs4000-229D58(config-profile-testRFS4000)#environmental-sensor light radio-
shutdown all
rfs4000-229D58(config-profile-testRFS4000)#environmental-sensor light threshold
high 300
rfs4000-229D58(config-profile-testRFS4000)#environmental-sensor light threshold
low 100

rfs4000-229D58(config-profile-testRFS4000)#show context
profile rfs4000 testRFS4000
 bridge vlan 1
  tunnel-over-level2
  ip igmp snooping
  ip igmp snooping querier
 environmental-sensor polling-interval 60
 environmental-sensor light threshold high 300
 environmental-sensor light threshold low 100
 environmental-sensor light radio-shutdown all
 no autoinstall configuration
 no autoinstall firmware
 device-upgrade persist-images
--More--
rfs4000-229D58(config-profile-testRFS4000)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the environmental sensor's settings |

## 7.1.30 events

*Profile Config Commands*

Displays system event messages

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
events [forward on|on]
```

**Parameters**

- `events [forward on|on]`

| | |
|---|---|
| forward on | Forwards system event messages to the wireless controller, service platform, or cluster members. This feature is enabled by default.<br>• on – Enables forwarding of system events |
| on | Generates system events. This feature is enabled by default. |

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000)#events forward on
rfs6000-37FABE(config-profile-default-rfs6000)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables or reverts settings to their default |

## 7.1.31 export

*Profile Config Commands*

Enables export of startup.log file after every boot

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
export startup-log [max-retries|retry-interval|url]
export startup-log [max-retries <2-65535>|retry-interval <30-86400>|url <URL>]
```

**Parameters**

- `export startup-log [max-retries <2-65535>|retry-interval <30-86400>|url <URL>]`

| | |
|---|---|
| export startup-log | Enables export of the startup.log file after every boot. This option is disabled by default. |
| max-retries <2-65535> | Configures the maximum number of retries in case the export process fails<br>• <2-65535> – Specify a value from 2 - 65535. |
| retry-interval <30-86400> | Configures the interval between two consecutive retries<br>• <30-86400> – Specify a value from 30 - 86400 seconds. |
| url <URL> | Configures the destination URL in the following format:<br>tftp://<hostname\|IP>[:port]/path/file<br>ftp://<user>:<passwd>@<hostname\|IP>[:port]/path/file<br>sftp://<user>@<hostname\|IP>[:port]>/path/file |

**Example**

```
nx9500-6C8809(config-profile-test-nx5500)#export startup-log max-retries 10
retry-interval 30 url ftp://anonymous:anonymous@192.168.13.10/log/startup.log

nx9500-6C8809(config-profile-test-nx5500)#show context
profile nx5500 test-nx5500
 no autoinstall configuration
 no autoinstall firmware
 crypto ikev1 policy ikev1-default
  ....................................................
 interface ge5
 interface ge6
 interface pppoe1
 use firewall-policy default
 export startup-log max-retries 10 retry-interval 30 url ftp://
anonymous:anonymous@192.168.13.10/log/startup.log
 enforce-version adoption major
 enforce-version cluster full
 service pm sys-restart
--More--g
nx9500-6C8809(config-profile-test-nx5500)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables export of startup.log file |

## 7.1.32 file-sync

*Profile Config Commands*

Configures parameters enabling auto syncing of trustpoint/wireless-bridge certificate between the staging-controller and its adopted access points

This command is applicable to the access point's profile as well as device configuration modes.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

**Syntax**

```
file-sync [auto|count <1-20>]
```

**Parameters**

- `file-sync [auto|count <1-20>]`

| | |
|---|---|
| file-sync [auto\|count <1-20>] | Configures the following file-synching parameters:<br>• auto – Enables the staging controller to autoinstall trustpoint/wireless-bridge certificate on an access point when it comes up for the first time and adopts to the controller.<br>Prior to enabling file syncing, ensure that the wireless-bridge certificate is present on the staging controller. To upload the certificate on the controller, in the user or privilege executable modes, execute the following command: *file-sync > load-file > <URL>*.<br>• count <1-20> – Configures the maximum number of access points that can be concurrently auto-installed.<br>• <1-20> – Specify a value from 1 - 20. The default is 10 access points.<br>For the NX95XX service platforms the count-range is from 1 - 128. |

**Example**

```
nx9500-6C8809(config-profile-default-rfs6000)#file-sync auto

nx9500-6C8809(config-profile-default-rfs6000)#file-sync count 8

nx9500-6C8809(config-profile-default-rfs6000)#show context
profile rfs6000 default-rfs6000
 no autoinstall configuration
 no autoinstall firmware
 no device-upgrade auto
 file-sync count 8
 file-sync auto
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 --More--
nx9500-6C8809(config-profile-default-rfs6000)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables automatic file syncing between the staging-controller and its access points |

## 7.1.33 floor

*Profile Config Commands*

Sets the floor name where the target device (access point, wireless controller, or service platform using this profile) is physically located. Assigning a building floor name helps in grouping devices within the same general coverage area.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
floor <WORD> {<1-4094>}
```

**Parameters**

- `floor <WORD> {<1-4094>}`

| | |
|---|---|
| floor <WORD> {<1-4094>} | Sets the floor name where the target device is located<br>• <WORD> – Specify the floor name (should not exceed 64 characters in length).<br>• <1-4094> – Optional. Configures the floor number from 1 - 4094. The default is 1. |

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000)#floor fifth

rfs6000-37FABE(config-profile-default-rfs6000)#show context
profile rfs7000 default-rfs7000
 bridge vlan 1
  ip igmp snooping
  ip igmp snooping querier
 area Ecospace
 floor fifth
 autoinstall configuration
 autoinstall firmware
--More--
rfs6000-37FABE(config-profile-default-rfs6000)#
```

**Related Commands**

| | |
|---|---|
| *no* | Resets the configured floor name and number |

## 7.1.34 gre

*Profile Config Commands*

The following table summarizes commands that allow you to enter the GRE configuration mode:

| Command | Description | Reference |
|---|---|---|
| *gre* | Enables GRE tunneling on a profile/device This command also creates a GRE tunnel and enters its configuration mode. Use this command to modify an existing GRE tunnel's settings. | *page 7-166* |
| *gre-config-instance* | Summarizes GRE tunnel configuration mode commands | *page 7-168* |

### 7.1.34.1 gre

*gre*

Enables *Generic Routing Encapsulation* (GRE) tunneling on this profile, and creates a new GRE tunnel or modifies an existing GRE tunnel.

The GRE protocol allows encapsulation of one protocol over another. It is a tunneling protocol that transports any layer 3 protocol over an IP network. When enabled, a payload packet is first encapsulated in the GRE protocol. The GRE encapsulated payload is then encapsulated in another IP packet before being forwarded to the destination.

GRE tunneling can be configured to bridge Ethernet packets between WLANs and a remote WLAN gateway over an IPv4 GRE tunnel. The tunneling of 802.3 packets using GRE is an alternative to MiNT or L2TPv3. Related features like ACLs for extended VLANs are still available using layer 2 tunneling over GRE.

Using GRE, access points map one or more VLANs to a tunnel. The remote end point is a user-configured WLAN gateway IP address, with an optional secondary IP address should connectivity to the primary GRE peer be lost. VLAN traffic is expected in both directions in the GRE tunnel. A WLAN mapped to these VLANs can be either open or secure. Secure WLANs require authentication to a remote RADIUS server available within your deployment using standard RADIUS protocols. Access Points can reach both the GRE peer as well as the RADIUS server using IPv4.

The WiNG software now supports for both IPv4 or IPv6 tunnel endpoints. However, a tunnel needs to contain either IPv4 or IPv6 formatted device addresses and cannot be mixed. With the new IPv6 tunnel implementation, all outbound packets are encapsulated with the GRE header, then the IPv6 header. The header source IP address is the local address of the IPv6 address of tunnel interface, and the destination address peer address of the tunnel. All inbound packets are de-capsulated by removing the IPv6 and GRE header before sending it over to the IP stack.

**NOTE:** Only one GRE tunnel can be created for every profile.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
gre tunnel <GRE-TUNNEL-NAME>
```

**Parameters**

- `gre tunnel <GRE-TUNNEL-NAME>`

| | |
|---|---|
| gre tunnel <GRE-TUNNEL-NAME> | Creates a new GRE tunnel or modifies an existing GRE tunnel<br>• <GRE-TUNNEL-NAME> – If creating a new tunnel, specify a unique name for it. If modifying an existing tunnel, specify its name. |

**Example**

```
rfs4000-229D58(config-profile testRFS4000-gre-tunnel-testGREtunnel)#?
GRE Tunnel Mode commands:
  dscp                    Differentiated Services Code Point
  establishment-criteria  Set tunnel establishment criteria
  failover                L2gre tunnel failover
  mtu                     L2GRE tunnel endpoint maximum transmission unit(MTU)
  native                  Native trunking characteristics
  no                      Negate a command or set its defaults
  peer                    L2GRE peer
  tunneled-vlan           VLANs to tunnel

  clrscr                  Clears the display screen
  commit                  Commit all changes made in this session
  do                      Run commands from Exec mode
  end                     End current mode and change to EXEC mode
  exit                    End current mode and down to previous mode
  help                    Description of the interactive help system
  revert                  Revert changes
  service                 Service Commands
  show                    Show running system information
  write                   Write running configuration to memory or terminal

rfs4000-229D58(config-profile testRFS4000-gre-tunnel-testGREtunnel)#

rfs4000-229D58(config-profile testRFS4000-gre-tunnel-testGREtunnel)#peer 1 ip
192.168.13.8
rfs4000-229D58(config-profile testRFS4000-gre-tunnel-testGREtunnel)#peer 2 ip
192.168.13.10

rfs4000-229D58(config-profile testRFS4000-gre-tunnel-testGREtunnel)#show context
 gre tunnel testGREtunnel
  peer 1 ip 192.168.13.8
  peer 2 ip 192.168.13.10
rfs4000-229D58(config-profile testRFS4000-gre-tunnel-testGREtunnel)#

rfs4000-229D58(config-profile-testRFS4000)#show context
profile rfs4000 testRFS4000
 bridge vlan 1
  tunnel-over-level2
  ip igmp snooping
  ip igmp snooping querier
.....................................................................................
..
 use firewall-policy default
 service pm sys-restart
 router ospf
 gre tunnel testGREtunnel
  peer 1 ip 192.168.13.8
  peer 2 ip 192.168.13.10
rfs4000-229D58(config-profile-testRFS4000)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables GRE tunneling on this profile |

### 7.1.34.2 gre-config-instance

*gre*

The following table summarizes GRE tunnel configuration mode commands:

| Command | Description | Reference |
|---|---|---|
| *dscp* | Sets the GRE tunnel's *Differentiated Services Code Point* (DSCP) / 802.1q priority value | *page 7-169* |
| *establishment-criteria* | Configures the GRE tunnel establishment criteria | *page 7-169* |
| *failover* | Enables periodic pinging of the primary gateway to assess its availability, in case it is unreachable | *page 7-171* |
| *mtu* | Configures the *maximum transmission unit* (MTU) for IPv4/IPv6 L2GRE tunnel endpoints | *page 7-172* |
| *native* | Configures native trunking settings for this GRE tunnel | *page 7-173* |
| *no* | Removes the GRE tunnel settings based on the parameters passed | *page 7-174* |
| *peer* | Configures the GRE tunnel's end-point peers | *page 7-175* |
| *tunneled-vlan* | Defines the VLAN that connected clients use to route GRE-tunneled traffic within their respective WLANs | *page 7-176* |

### 7.1.34.2.1 dscp

*gre-config-instance*

Sets the GRE tunnel's DSCP / 802.1q priority value from encapsulated packets to the outer packet IPv4 header.

This option is disabled by default.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
dscp [<0-63>|reflect]
```

**Parameters**

- `dscp [<0-63>|reflect]`

| | |
|---|---|
| dscp <0-63> | Specifies the DSCP 802.1q priority value for outer packets from 0 - 63. The default is 1. |
| dscp reflect | Copies the DSCP 802.1q value from inner packets |

**Example**

```
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#dscp 20

rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#show
context
 gre tunnel testGRETunnel
  dscp 20
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the GRE tunnel settings based on the parameters passed |

### 7.1.34.2.2 establishment-criteria

*gre-config-instance*

Configures the GRE tunnel establishment criteria

In a multi-controller RF domain, it is always the master node that establishes the tunnel. The tunnel is created only if the tunnel device is designated as one of the following: vrrp-master, cluster-master, or rf-domain-manager.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
establishment-criteria [always|cluster-master|rf-domain-manager|vrrp-master <1-255>]
```

**Parameters**

```
• establishment-criteria [always|cluster-master|rf-domain-manager|vrrp-master <1-255>]
```

| | |
|---|---|
| establishment-criteria [always\| cluster-master\| rf-domain-manager\| vrrp-master <1-255>] | Configures the GRE tunnel establishment criteria. The options are:<br>• always – Always automatically establishes tunnel (default setting). The tunnel device need not be a cluster master, RF Domain manager, or VRRP master to establish the GRE tunnel. This is the default setting.<br>• cluster-master – Establishes tunnel only if the tunnel device is designated as the cluster master<br>• rf-domain-manager – Establishes tunnel only if the tunnel device is designated as the RF Domain manager<br>• vrrp-master <1-255> – Establishes tunnel only if the tunnel device is designated as the *Virtual Router Redundancy* (VRRP) master<br>• <1-255> – Configures the VRRP group ID from 1 - 255. A VRRP group enables the creation of a group of routers as a default gateway for redundancy. Clients can point to the IP address of the VRRP virtual router as their default gateway and utilize a different group member if a master becomes unavailable. |

**Example**

```
nx9500-6C8809(config-profile testNX9500-gre-tunnel-testGREtunnel)#establishment-criteria rf-domain-manager

nx9500-6C8809(config-profile testNX9500-gre-tunnel-testGREtunnel)#show context
 gre tunnel testGREtunnel
  establishment-criteria rf-domain-manager
nx9500-6C8809(config-profile testNX9500-gre-tunnel-testGREtunnel)#
```

### 7.1.34.2.3 failover

*gre-config-instance*

Enables periodic pinging of the primary gateway to assess its availability. When enabled, the system continues pinging, an unreachable gateway, for a specified number of times and at the specified interval.

This option is disabled by default.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
failover interval <1-250> retry <1-10>
```

**Parameters**

- `failover interval <1-250> retry <1-10>`

| | |
|---|---|
| failover interval <1-250> retry <1-10> | Specifies the interval, in seconds, between two successive pings to the primary gateway. If the primary gateway is unreachable, the system pings it at intervals specified here.<br>• <1-250> – Specify a value from 1 - 250 seconds.<br>• retry – Specifies the maximum number attempts made to ping the primary gateway before the session is terminated.<br>• <1-10> – Specify a value from 1 - 10. |

**Example**

```
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#failover
interval 200 retry 5

rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#show
context
 gre tunnel testGRETunnel
  dscp 20
  failover interval 200 retry 5
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the GRE tunnel settings based on the parameters passed |

### 7.1.34.2.4 mtu

*gre-config-instance*

Configures the MTU for IPv4/IPv6 L2GRE tunnel endpoints

The MTU is the largest physical packet size (in bytes) transmittable within the tunnel. Any messages larger than the configured MTU are divided into smaller packets before transmission. Larger the MTU greater is the efficiency because each packet carries more user data, while protocol overheads, such as headers or underlying per-packet delays remain fixed; the resulting higher efficiency means a slight improvement in bulk protocol throughput. A larger MTU results in the processing of fewer packets for the same amount of data.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
mtu [ipv4 <900-1476>|ipv6 <1236-1456>]
```

**Parameters**

- `mtu [ipv4 <900-1476>|ipv6 <1236-1456>]`

| | |
|---|---|
| mtu<br>[ipv4 <900-1476>\|<br>ipv6 <1236-1456>] | Configures the MTU for L2GRE tunnel endpoints<br>• ipv4 <900-1476> – Configures IPv4 L2GRE tunnel endpoint MTU from 900 - 1476. The default is 1476.<br>• ipv6 <1236-1456> – Configures IPv6 L2GRE tunnel endpoint MTU from 1236 - 1456. The default is 1456. |

**Example**

```
nx9500-6C8809(config-profile testNX9500-gre-tunnel-testGREtunnel)#mtu ipv4 1200

nx9500-6C8809(config-profile testNX9500-gre-tunnel-testGREtunnel)#mtu ipv6 1300

nx9500-6C8809(config-profile testNX9500-gre-tunnel-testGREtunnel)#show context
 gre tunnel testGREtunnel
  mtu ipv4 1200
  mtu ipv6 1300
  establishment-criteria rf-domain-manager
nx9500-6C8809(config-profile testNX9500-gre-tunnel-testGREtunnel)#
```

### 7.1.34.2.5 native

*gre-config-instance*

Configures native trunking settings for this GRE tunnel

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
native [tagged|vlan <1-4094>]
```

**Parameters**

- `native [tagged|vlan <1-4094>]`

| | |
|---|---|
| native tagged | Enables native VLAN tagging<br>The IEEE 802.1Q specification is supported for tagging frames and coordinating VLANs between devices. IEEE 802.1Q adds four bytes to each frame identifying the VLAN ID for upstream devices that the frame belongs. If the upstream Ethernet device does not support IEEE 802.1Q tagging, it does not interpret the tagged frames. When VLAN tagging is required between devices, both devices must support tagging and be configured to accept tagged VLANs. When a frame is tagged, the 12 bit frame VLAN ID is added to the 802.1Q header so upstream Ethernet devices know which VLAN ID the frame belongs to. The device reads the 12 bit VLAN ID and forwards the frame to the appropriate VLAN. When a frame is received with no 802.1Q header, the upstream device classifies the frame using the default or native VLAN assigned to the Trunk port. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. This feature is disabled by default. |
| native vlan <1-4094> | Specifies a numerical VLAN ID (1 - 4094) for the native VLAN<br>The native VLAN allows an Ethernet device to associate untagged frames to a VLAN, when no 802.1q frame is included in the frame. Additionally, the native VLAN is the VLAN untagged traffic is directed over when using a port in trunk mode. |

**Example**

```
nx9500-6C8809(config-profile testNX9500-gre-tunnel-testGREtunnel)#native tagged

nx9500-6C8809(config-profile testNX9500-gre-tunnel-testGREtunnel)#native vlan 20

nx9500-6C8809(config-profile testNX9500-gre-tunnel-testGREtunnel)#show context
 gre tunnel testGREtunnel
  native vlan 20
  native tagged
  mtu ipv4 1200
  mtu ipv6 1300
  establishment-criteria rf-domain-manager
nx9500-6C8809(config-profile testNX9500-gre-tunnel-testGREtunnel)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the GRE tunnel settings based on the parameters passed |

### 7.1.34.2.6 no

*gre-config-instance*

Removes or resets the GRE tunnel settings based on the parameters passed

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
no [dscp|establishment-criteria|failover|mtu|native|peer|tunneled-vlan]

no [dscp|establishment-criteria|failover|tunneled-vlan]

no mtu [ipv4|ipv6]

no native [tagged|vlan]

no peer <1-2>
```

**Parameters**

- no <PARAMETERS>

| | |
|---|---|
| no <PARAMETERS> | Removes or resets the GRE tunnel's settings based on the parameters passed |

**Example**

The following example shows the GRE tunnel 'testGRETunnel' settings before the no commands are executed:

```
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#show
context
 gre tunnel testGRETunnel
  peer 1 ip 192.168.13.6
  native vlan 1
  tunneled-vlan 1,10
  native tagged
  dscp 20
  failover interval 200 retry 5
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#

rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#no dscp
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#no
native vlan
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#no
tunneled-vlan
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#no
failover
```

The following example shows the GRE tunnel 'testGRETunnel' settings after the no commands are executed:

```
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#show
context
 gre tunnel testGRETunnel
  peer 1 ip 192.168.13.6
  native tagged
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#
```

### 7.1.34.2.7 peer

*gre-config-instance*

Adds the GRE tunnel's end-point peers. A maximum of two peers, representing the tunnel's end points, can be added for each GRE tunnel.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
peer <1-2> ip <IPv4/IPv6>
```

**Parameters**

- `peer <1-2> ip <IPv4/IPv6>`

| | |
|---|---|
| peer <1-2> ip <IPv4/IPv6> | Configures the tunnel's end-point peers<br>• <1-2> – Specify a numeric index for each peer to help differentiate the tunnel end points.<br>• ip – Specify the IP address (IPv4/IPv6) of the added GRE peer to serve as a network address identifier.<br>• <IPv4/IPv6> – Specify the peer's IPv4 or IPv6 address. |

**Example**

```
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#peer 1
ip 192.168.13.6

rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#show
context
 gre tunnel testGRETunnel
  peer 1 ip 192.168.13.6
  native tagged
  dscp 20
  failover interval 200 retry 5
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the GRE tunnel settings based on the parameters passed |

### 7.1.34.2.8 tunneled-vlan

*gre-config-instance*

Defines the VLAN that connected clients use to route GRE tunneled traffic within their respective WLANs

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
tunneled-vlan <VLAN-ID>
```

**Parameters**

- `tunneled-vlan <VLAN-ID>`

| | |
|---|---|
| tunneled-vlan <VLAN-ID> | Specifies the VLANs associated with this GRE tunnel<br>• <VLAN-ID> – Specify the VLAN IDs. Specify a comma-separated list of IDs, to specify multiple VLANs. For example, 1,10,12,16-20. |

**Example**

```
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#
tunneled-vlan 10

rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#show
context
 gre tunnel testGRETunnel
  peer 1 ip 192.168.13.6
  native vlan 1
  tunneled-vlan 1,10
  native tagged
  dscp 20
  failover interval 200 retry 5
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the GRE tunnel settings based on the parameters passed |

## 7.1.35 http-analyze

*Profile Config Commands*

Enables forwarding of HTTP request related data to the HTTP analytics engine

Wireless clients (MUs) connect to APs and route their HTTP requests through the APs. These APs extract and forward HTTP request packets, through MiNT, to the NX series controller. The NX series controller uses a new analytic daemon to cache, format, and forward information to the analytics engine. Currently the analytics daemon is supported only on the NX series service platform. Therefore, it is essential that all APs should use an NX series service platform as controller.

In a hierarchically organized network, HTTP analytics data forwarding is a simple and transparent process. The site controllers receive the HTTP data from adopted APs adopted. This data is compressed and forwarded to the *Network Operations Center* (NOC) controller. There is no need for a separate configuration to enable this feature.

Use this command to configure the mode and interval at which data is sent to the controller and the external analytics engine. This command also configures the external engine's details, such as URL, credentials, etc.

**NOTE:** The Analytics module helps gather data about customer behavior such as web sites visited, search terms used, mobile device types, number of new users vs. repeat users. This data provides a better understanding of pricing strategies and promotions being run by competitors.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
http-analyze [compress|external-server|update-interval <1-3600>]

http-analyze [compress|update-interval <1-3600>

http-analyze external-server [password <WORD>|proxy <URL>|update-interval <1-3600>|url <URL>|username <WORD>|validate-server-certificate]
```

**Parameters**

- `http-analyze [compress|update-interval <1-3600>]`

| | |
|---|---|
| http-analyze | Configures HTTP analysis related parameters |
| compress | Compresses update files before forwarding to the controller. This option is disabled by default. |
| update-interval <1-3600> | Configures the interval, in seconds, at which buffered packets are pushed to the controller<br>• <1-3600> – Specify the interval from 1 - 3600 seconds. The default is 60 seconds. |

- `http-analyze external-server [password <WORD>|proxy <URL>|update-interval|url|username|validate-server-certificate]`

| | |
|---|---|
| http-analyze external-server | Configures the external HTTP analytics engine's parameters |

| | |
|---|---|
| password <WORD> | Configures the external analytics engine's password<br>• <WORD> – Provide the login password. This is the password associated with the user name needed to access the external analytics engine. |
| proxy <URL> | Configures the proxy server's *uniform resource locator* (URL)<br>• <URL> – Specify the proxy server's URL in the following format: http://username:password@proxy-server:port. For example, http://mot:sym@wwwgate0.mot.com:1080 |
| update-interval <1-36000> | Configures the interval, in seconds, at which buffered packets are pushed to the external analytics engine<br>• <1-3600> – Specify the interval from 1 - 3600 seconds. The default is 60 seconds. |
| url <URl> | Configures the external analytics engine's IP address or URL<br>• <URL> – Provide the IP address or URL. |
| username <WORD> | Configures the user name needed to access the external analytics engine<br>• <WORD> – Provide the user name. |
| validate-server-certificate | Validates the external analytics engine's certificate, if it is using HTTPS as the mode of access |

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000)#http-analyze compress

rfs6000-37FABE(config-profile-default-rfs6000)#http-analyze update-interval 200

rfs6000-37FABE(config-profile-default-rfs6000)#show context
profile rfs7000 default-rfs7000
 bridge vlan 1

.................................................................
  qos trust 802.1p
 interface pppoe1
 use firewall-policy default
 http-analyze update-interval 200
 http-analyze compress
 service pm sys-restart
 router ospf
rfs6000-37FABE(config-profile-default-rfs6000)#

nx9500-6C8809(config-profile-test-nx5500)#http-analyze external-server username
anonymous
nx9500-6C8809(config-profile-test-nx5500)#http-analyze external-server password
anonymous
nx9500-6C8809(config-profile-test-nx5500)#http-analyze external-server validate-
server-certificate
nx9500-6C8809(config-profile-test-nx5500)#http-analyze external-server update-
interval 100
nx9500-6C8809(config-profile-test-nx5500)#http-analyze external-server url
https://192.168.13.10
```

```
nx9500-6C8809(config-profile-test-nx5500)#show context
profile nx5500 test-nx5500
 no autoinstall configuration
 no autoinstall firmware
 ..................................................
 interface ge5
 interface ge6
 interface pppoe1
 use firewall-policy default
 export startup-log max-retries 10 retry-interval 30 url ftp://
anonymous:anonymous@192.168.13.10/log/startup.log
 http-analyze external-server url https://192.168.13.10
 http-analyze external-server username anonymous
 http-analyze external-server password anonymous
 http-analyze external-server update-interval 100
 enforce-version adoption major
 enforce-version cluster full
--More--
nx9500-6C8809(config-profile-test-nx5500)#

nx9500-6C8809(config-profile-test-nx5500)#http-analyze external-server proxy
http://mot:sym@wwwgate0.mot.com:1080

nx9500-6C8809(config-profile-test-nx5500)#show context
profile nx5500 test-nx5500
 no autoinstall configuration
 no autoinstall firmware
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
.....................................................
 http-analyze external-server url https://192.168.13.10
 http-analyze external-server username anonymous
 http-analyze external-server password anonymous
 http-analyze external-server update-interval 100
 http-analyze external-server proxy http://mot:sym@wwwgate0.mot.com:1080
 enforce-version adoption major
 enforce-version cluster full
 service pm sys-restart
 router ospf
 router bgp
 dot1x system-auth-control
 dot1x use aaa-policy OnBoarding
nx9500-6C8809(config-profile-test-nx5500)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables HTTP analyze settings |

## 7.1.36 interface

*Profile Config Commands*

The following table summarizes interface configuration commands:

| Command | Description | Reference |
|---|---|---|
| *interface* | Selects an interface to configure | *page 7-181* |
| *interface-config-ge-instance* | Summarizes Ethernet interface (associated with the wireless controller or service platform) configuration commands | *page 7-184* |
| *interface-config-vlan-instance* | Summarizes VLAN interface configuration commands | *page 7-217* |
| *interface-config-port-channel-instance* | Summarizes port-channel interface configuration commands | *page 7-235* |
| *interface-config-radio-instance* | Summarizes radio interface configuration commands (applicable to devices with built-in radios) | *page 7-252* |
| *interface-config-wwan-instance* | Summarizes WWAN interface configuration commands | *page 7-327* |
| *interface-config-bluetooth-instance* | Summarizes the Bluetooth radio interface configuration commands (supported only on the AP8432 and AP8533 model access points | *page 7-337* |

### 7.1.36.1 interface

*interface*

Selects an interface to configure

A profile's interface configuration can be defined to support separate physical Ethernet configurations both unique and specific to RFS4000, RFS6000 controllers and NX7500 and NX95XX series service platforms. Ports vary depending on the platform, but controller or service platform models do have some of the same physical interfaces.

A controller or service platform requires its virtual interface be configured for layer 3 (IP) access or layer 3 service on a VLAN. A virtual interface defines which IP address is associated with each VLAN ID the controller or service platform is connected to.

If the profile is configured to support an access point radio, an additional radio interface is available, unique to the access point's radio configuration.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax Service Platforms**

```
interface [<INTERFACE-NAME>|fe <1-4>|ge <1-24>|me1|port-channel <1-4>|pppoe1|
radio [1|2|3]|serial <1-4>|t1e1 <1-4>|up <1-2>|vlan <1-4094>|wwan1|xge <1-4>]
```

**Syntax Access Points and Wireless Controllers**

```
interface [<INTERFACE-NAME>|bluetooth <1-1>|fe <1-4>|ge <1-8>|me1|port-channel <1-
4>|pppoe1|radio [1|2|3]|up1|vlan <1-4094>|wwan1|xge <1-4>]
```

**Parameters**

```
• interface [<INTERFACE-NAME>|bluetooth <1-1>|fe <1-4>|ge <1-8>|me1|port-channel
<1-4>|radio [1|2|3]|serial <1-4>|t1e1 <1-4>|up <1-2>|vlan <1-4094>|wwan1|xge <1-
4>]
```

| | |
|---|---|
| <INTERFACE-NAME> | Enters the configuration mode of the interface identified by the <INTERFACE-NAME> keyword |
| bluetooth <1-1> | Selects the Bluetooth radio interface<br>• <1-1> – Specify the Bluetooth radio interface index from 1 - 1. As of now only one Bluetooth radio interface is supported.<br>This interface is applicable only for the AP8432 and AP8533 model access points. |
| fe <1-4> | Selects a FastEthernet interface<br>• <1-4> – Specify the interface index from 1 - 4. |
| ge <1-24> | Selects a GigabitEthernet interface<br>• <1-24> – Specify the interface index from 1 - 24. (4 for RFS7000 and 8 for RFS6000). |

| | |
|---|---|
| me1 | Selects a management interface<br>Not applicable for RFS4000 model devices.<br>The management interface is applicable only for RFS6000 and RFS7000 model controllers. |
| port-channel <1-4> | Selects the port channel interface<br>• <1-4> – Specify the interface index from 1 - 4. |
| pppoe1 | Selects the PPP over Ethernet interface to configure |
| radio [1\|2\|3] | Selects a radio interface<br>• 1 – Selects radio interface 1<br>• 2 – Selects radio interface 2<br>• 3 – Selects radio interface 3<br>The radio interface is not available on wireless controllers or service platforms. |
| up1 | Selects the uplink GigabitEthernet interface |
| vlan <1-4094> | Selects a VLAN interface<br>• <1-4094> – Specify the SVI VLAN ID from 1 - 4094. |
| wwan1 | Selects a Wireless WAN interface<br>This interface is applicable only to AP7161, AP81XX, AP8232, RFS4000, RFS6000 model access points and controllers. |
| xge <1-4> | Selects a TenGigabitEthernet interface<br>• <1-2> – Specify the interface index from 1 - 4. |

**Usage Guidelines**

The ports available on a device vary depending on the model. For example, the following ports are available on RFS4000, RFS6000 and RFS7000 model wireless controllers:

- RFS4000 - ge1, ge2, ge3, ge4, ge5, up1
- RFS6000 - ge1, ge2, ge3, ge4, ge5, ge6, ge7, ge8, me1, up1

GE ports on are RJ-45 supporting 10/100/1000Mbps..

ME ports are available on RFS6000 platforms. ME ports are out-of-band management ports used to manage the controller via CLI or Web UI, even when the other ports on the controller are unreachable.

The ports available on service platforms also vary depending on the model. For example, the following ports are available on NX series service platforms:

- NX7500 - ge1-ge10, xge1-xge2
- NX95XX series - ge1, ge2, xge1-xge4
- EX3500 – ge1-1 to ge1-24
- EX3548 – ge1-1 to ge1-48

GE ports are available on devices, such as RFS4000 and RFS6000controllers. GE ports are RJ-45 supporting 10/100/1000Mbps.

ME ports are available on RFS6000 platforms. ME ports are out-of-band management ports used to manage the controller via CLI or Web UI, even when the other ports on the controller are unreachable.

UP ports are available on RFS4000 and RFS6000 platforms. A UP port is used to connect to the backbone network. UP ports are available on devices, such as RFS4000 and RFS6000 controllers. A UP port supports either RJ-45 or fiber. The UP port is the preferred means to connect to the backbone as it has a non-blocking 1gbps connection unlike the GE ports.

The following ports are available on access points:

- AP6511 - fe1, fe2, fe3, fe4, up1
- AP6521 - GE1/POE (LAN)
- AP6522 - GE1/POE (LAN)
- AP6532 - GE1/POE
- AP6562 - GE1/POE
- AP7161 - GE1/POE (LAN), GE2 (WAN)
- AP7502 - GE1 (THRU), fe1, fe2, fe3,
- AP7522 - GE1/POE (LAN)
- AP7532 - GE1/POE (LAN)
- AP81XX - GE1/POE (LAN), GE2 (WAN)
- AP82XX - GE1/POE (LAN), GE2 (WAN)

**NOTE:** For a NX7500 model service platform, there are options for either a 2 port or 4 port network management card. Either card can be managed using WiNG. If the 4 port card is used, ports ge7-ge10 are available. If the 2 port card is used, ports xge1-xge2 are available.

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-if-vlan44)#
rfs6000-37FABE(config-profile-default-rfs6000-if-vlan44)#?
SVI configuration commands:
  crypto                Encryption module
  description           Vlan description
  dhcp                  Dynamic Host Configuration Protocol (DHCP)
  dhcp-relay-incoming   Allow on-board DHCP server to respond to relayed DHCP
                        packets on this interface
  ip                    Interface Internet Protocol config commands
  ipv6                  Internet Protocol version 6 (IPv6)
  no                    Negate a command or set its defaults
  shutdown              Shutdown the selected interface
  use                   Set setting to use

  clrscr                Clears the display screen
  commit                Commit all changes made in this session
  do                    Run commands from Exec mode
  end                   End current mode and change to EXEC mode
  exit                  End current mode and down to previous mode
  help                  Description of the interactive help system
  revert                Revert changes
  service               Service Commands
  show                  Show running system information
  write                 Write running configuration to memory or terminal

rfs6000-37FABE(config-profile-default-rfs6000-if-vlan44)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the selected interface |

### 7.1.36.2 interface-config-ge-instance

*interface*

This section documents the GigabitEthernet configuration commands.

GE port placement and quantity varies depending on the controller, service platform, or access point model. Configure the GE interface either in the device's profile-config context or directly on a device.

The following example uses the config-profile-default-rfs7000 instance to configure a GigabitEthernet interface:

```
nx9500-6C8809(config-profile-testNX9000-if-ge2)#?
Interface configuration commands:
  captive-portal-enforcement  Enable captive-portal enforcement on this port
  cdp                         Cisco Discovery Protocol
  channel-group               Channel group commands
  description                 Interface specific description
  dot1x                       802.1X
  duplex                      Set duplex to interface
  ip                          Internet Protocol (IP)
  ipv6                        Internet Protocol version 6 (IPv6)
  lacp                        LACP commands
  lacp-channel-group          LACP channel commands
  lldp                        Link Local Discovery Protocol
  mac-auth                    Enable mac-auth for this port
  no                          Negate a command or set its defaults
  power                       PoE Command
  qos                         Quality of service
  remove-override             Remove configuration item override from the
                              device (so profile value takes effect)
  shutdown                    Shutdown the selected interface
  spanning-tree               Spanning tree commands
  speed                       Configure speed
  switchport                  Set switching mode characteristics
  use                         Set setting to use

  clrscr                      Clears the display screen
  commit                      Commit all changes made in this session
  do                          Run commands from Exec mode
  end                         End current mode and change to EXEC mode
  exit                        End current mode and down to previous mode
  help                        Description of the interactive help system
  revert                      Revert changes
  service                     Service Commands
  show                        Show running system information
  write                       Write running configuration to memory or
                              terminal

nx9500-6C8809(config-profile-testNX9000-if-ge2)#
```

The following table summarizes the interface configuration commands:

| Command | Description | Reference |
|---|---|---|
| *captive-portal-enforcement* | Enables captive-portal enforcement on this Ethernet port | *page 7-186* |
| *cdp* | Enables *Cisco Discovery Protocol* (CDP) on this Ethernet port | *page 7-187* |
| *channel-group* | Assigns this Ethernet port to a channel group | *page 7-188* |
| *description* | Configures a description for this Ethernet port | *page 7-189* |
| *dot1x (authenticator)* | Configures 802.1X authenticator settings | *page 7-190* |

| Command | Description | Reference |
|---|---|---|
| *dot1x (supplicant)* | Configures 802.1X supplicant settings | *page 7-193* |
| *duplex* | Specifies the duplex mode for the interface | *page 7-195* |
| *ip* | Sets the IP address for this Ethernet port | *page 7-196* |
| *ipv6* | Sets the DHCPv6 and ICMPv6 *neighbor discovery* (ND) components for this interface | *page 7-197* |
| *lacp* | Configures the selected GE port's *Link Aggregation Control Protocol* (LACP) port-priority value | *page 7-199* |
| *lacp-channel-group* | Configures the selected GE port as a member of a port-channel group (also referred as LAG) | *page 7-200* |
| *lldp* | Configures *Link Local Discovery Protocol* (LLDP) | *page 7-202* |
| *mac-auth* | Enables MAC-based authentication on this Ethernet port | *page 7-203* |
| *no* | Removes or reverts the selected Ethernet port settings | *page 7-204* |
| *power* | Configures *Power over Ethernet* (PoE) settings on this interface | *page 7-205* |
| *qos* | Enables QoS | *page 7-206* |
| *shutdown* | Disables the selected Ethernet port | *page 7-207* |
| *spanning-tree* | Configures spanning tree parameters | *page 7-208* |
| *speed* | Specifies the speed on this Ethernet port | *page 7-211* |
| *switchport* | Sets interface switching mode characteristics | *page 7-212* |
| *use* | Associates IPv4, IPv6, and/or MAC ACL with the selected Ethernet port | *page 7-215* |

### 7.1.36.2.1 captive-portal-enforcement

*interface-config-ge-instance*

Enables application of captive portal access permission rules to data transmitted over this specific Ethernet port. This setting is disabled by default.

Captive portal enforcement allows users on the wired network to pass traffic through the captive portal without being redirected to an authentication page. Authentication instead takes place when the RADIUS server is queried against the wired user's MAC address. If the MAC address is in the RADIUS server's user database, the user can pass traffic on the captive portal.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
captive-portal-enforcement {fall-back}
```

**Parameters**

- `captive-portal-enforcement {fall-back}`

| | |
|---|---|
| captive-portal-enforcement fall-back | Enables captive-portal enforcement on this Ethernet port<br>• fall-back – Optional. Enforces captive portal validation only if port authentication fails. When selected, captive portal policies are enforced only when RADIUS authentication of the client MAC address is not successful. If this option is not selected, captive portal policies are enforced regardless of the client's MAC address being in the RADIUS server's user database or not. |

**Example**

```
rfs6000-37FABE(config-device-B4-C7-99-6D-CD-4B-if-ge2)#captive-portal-
enforcement

rfs6000-37FABE(config-device-B4-C7-99-6D-CD-4B-if-ge2)#show context
 interface ge2
  captive-portal-enforcement
rfs6000-37FABE(config-device-B4-C7-99-6D-CD-4B-if-ge2)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables captive-portal enforcement on this interface |

### 7.1.36.2.2 cdp

*interface-config-ge-instance*

Enables CDP on the selected GE port

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
cdp [receive|transmit]
```

**Parameters**

- `cdp [receive|transmit]`

| | |
|---|---|
| receive | Enables CDP packet snooping on this interface. When enabled, the port receives periodic interface updates from a multicast address. This option is enabled by default. |
| transmit | Enables CDP packet transmission on this interface. When enabled, the port sends out periodic interface updates to a multicast address to advertise its presence to neighbors. This option is enabled by default. |

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-if-ge1)#cdp transmit
```

**Related Commands**

| | |
|---|---|
| *no* | Disables CDP packet snooping on the controller or service platform's selected GE ports |

### 7.1.36.2.3 channel-group

*interface-config-ge-instance*

Assigns this Ethernet port to a channel group. Ethernet ports can be aggregated to form a channel group. For example, an RFS7000 has four (4) Ethernet ports (1, 2, 3, & 4). These can be aggregated to form a minimum of one and maximum of two channel groups. A port can be a member of only one channel group at a time.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
channel-group <1-4>
```

**Parameters**

- `channel-group <1-4>`

| | |
|---|---|
| <1-4> | Specifies a channel group number from 1 - 4. The number of channel groups supported varies with the device type. For example:<br>RFS7000 – Supports two channel groups<br>RFS6000 – Supports four channel groups<br>RFS4000 – Supports three channel groups<br>NX5500 – Supports three channel groups<br>NX75XX – Supports four channel groups<br>NX95XX – Supports two channel groups |

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-if-ge1)#channel-group 1

rfs6000-37FABE(config-profile-default-rfs6000-if-ge1)#show context
 interface ge1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
  channel-group 1
rfs6000-37FABE(config-profile-default-rfs6000-if-ge1)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the channel group to which this port belongs |

### 7.1.36.2.4 description

*interface-config-ge-instance*

Configures a description for this Ethernet port

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
description [<LINE>|<WORD>]
```

**Parameters**

- `description [<LINE>|<WORD>]`

| | |
|---|---|
| <LINE> | Configures the maximum length (number of characters) of the interface description |
| <WORD> | Configures a unique description for this interface. The description should not exceed the length specified by the <LINE> parameter. |

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-if-ge1)#description "This is
GigabitEthernet interface for Royal King"

rfs6000-37FABE(config-profile-default-rfs6000-if-ge1)#show context
 interface ge1
  description "This is GigabitEthernet interface for Royal King"
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
  channel-group 1
rfs6000-37FABE(config-profile-default-rfs6000-if-ge1)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the interface description |

### 7.1.36.2.5 dot1x (authenticator)

*interface-config-ge-instance*

Configures 802.1X authenticator settings

Dot1x (or 802.1x) is an IEEE standard for network authentication. It enables media-level (layer 2) access control, providing the capability to permit or deny connectivity based on user or device identity. Dot1x allows port-based access using authentication. An dot1x enabled port can be dynamically enabled or disabled depending on user identity or device connection.

Devices supporting dot1x allow the automatic provision and connection to the wireless network without launching a Web browser at login. When within range of a dot1x network, a device automatically connects and authenticates without needing to manually login.

Before authentication, the endpoint is unknown, and traffic is blocked. Upon authentication, the endpoint is known and traffic is allowed. The controller or service platform uses source MAC filtering to ensure only the authenticated endpoint is allowed to send traffic.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6562, AP7161, AP7502, AP81XX, AP8232, AP8432
- Wireless Controllers — RFS4000, RFS6000, NX5500, NX7500

**Syntax**

```
dot1x authenticator [guest-vlan|host-mode|max-reauth-req|port-control|
reauthenticate|timeout]

dot1x authenticator [guest-vlan <1-4094>|host-mode [multi-host|single-host]|
max-reauth-req <1-10>|port-control [auto|force-authorized|force-unauthorized]|
reauthenticate|timeout [quiet-period|reauth-period] <1-65535>]
```

**NOTE:** The dot1x (802.1x) supplicant settings are documented in the next section.

**Parameters**

```
• dot1x authenticator [guest-vlan <1-4094>|host-mode [multi-host|single-host]|
max-reauth-req <1-10>|port-control [auto|force-authorized|force-unauthorized]|
reauthenticate|timeout [quiet-period|reauth-period]]
```

| | |
|---|---|
| dot1x authenticator | Configures 802.1x authenticator settings |
| guest-vlan <1-4094> | Configures the guest VLAN for this interface. This is the VLAN, traffic is bridged on if this port is unauthorized and the guest VLAN is globally enabled. Select the VLAN index from 1 - 4094. |
| host-mode [multi-host\| single-host] | Configures the host mode for this interface<br>• multi-host – Configures multiple host mode<br>• single-host – Configures single host mode. This is the default setting. |
| max-reauth-req <1-10> | Configures maximum number of re-authorization retries for the supplicant. This is the maximum number of re-authentication attempts made before this port is moved to unauthorized.<br>• <1-10> – Specify a value from 1 -10. The default is 2. |

| | |
|---|---|
| port-control [auto\| force-authorized\| force-unauthorized] | Configures port control state<br>• auto – Configures auto port state<br>• force-authorized – Configures authorized port state. This is the default setting.<br>• force-unauthorized – Configures unauthorized port state |
| reauthenticate | Enables re-authentication for this port. When enabled, clients are forced to re-authenticate on this port. The setting is disabled by default. Therefore, clients are not required to re-authenticate for connection over this port until this setting is enabled. |
| timeout [quiet-period\| reauth-period] <1-65535> | Configures timeout settings for this interface<br>• quiet-period – Configures the quiet period timeout in seconds. This is the interval, in seconds, between successive client authentication attempts.<br>• reauth-period – Configures the time after which re-authentication is initiated<br>The following option is common to 'quiet-period' and 'reauth-period' keywords:<br>• <1-65535> – Specify a 'quiet-period' or 'reauth-period' from 1 - 65535 seconds. |

**Example**

```
rfs4000-229D58(config-profile-testRFS4000-if-ge1)#dot1x authenticator guest-vlan
2

rfs4000-229D58(config-profile-testRFS4000-if-ge1)#dot1x authenticator host-mode
multi-host

rfs4000-229D58(config-profile-testRFS4000-if-ge1)#dot1x authenticator max-reauth-
req 6

rfs4000-229D58(config-profile-testRFS4000-if-ge1)#dot1x authenticator
reauthenticate

rfs4000-229D58(config-profile-testRFS4000-if-ge1)#show context
 interface ge1
  dot1x authenticator host-mode multi-host
  dot1x authenticator guest-vlan 2
  dot1x authenticator reauthenticate
  dot1x authenticator max-reauth-count 6
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
rfs4000-229D58(config-profile-testRFS4000-if-ge1)#
```

The following examples show the configurations made on an RFS6000 to enable it as a dot1X authenticator:

1 Configure AAA policy on the authenticator, and identify the authentication server as onboard (self):

```
rfs6000-817379(config-aaa-policy-aaa-wireddot1x)#show context
aaa-policy aaa-wireddot1x
authentication server 1 onboard controller
rfs6000-817379(config-aaa-policy-aaa-wireddot1x)#
```

This AAA policy is used in the authenticator's *self configuration* mode as shown in the last step.

2 Configure RADIUS user policy on the authenticator:

```
rfs6000-817379(config-radius-user-pool-wired-dot1x-users)#show con
radius-user-pool-policy wired-dot1x-users
user bob password 0 bob1234
rfs6000-817379(config-radius-user-pool-wired-dot1x-users)#
```

The user name and password configured here should match that of the supplicant. For more information, see the examples provided in the *dot1x (supplicant)* section.

3 Configure RADIUS server policy on the authenticator, and associate the RADIUS user policy created in the previous step:

```
rfs6000-817379(config-radius-server-policy-for-wired-dot1x)#show con
radius-server-policy for-wired-dot1x
use radius-user-pool-policy wired-dot1x-users
rfs6000-817379(config-radius-server-policy-for-wired-dot1x)#
```

4 In the authenticator's self configuration mode, associate the RADIUS server policy, created in the previous step, and configure other parameters (in bold) as shown in the following example:

```
rfs6000-817379(config-device-00-15-70-81-73-79)#use radius-server-policy for-
wired-dot1x
```

5 In the authenticator's *interface > ge* configuration mode, configure the following parameters:

```
rfs6000-817379(config-device-00-15-70-81-73-79-if-ge2)#dot1x authenticator
host-mode single-host
 rfs6000-817379(config-device-00-15-70-81-73-79-if-ge2)#dot1x authenticator
port-control auto
```

6 In the authenticator's *self* configuration mode, configure the following parameters:

```
rfs6000-817379(config-device-00-15-70-81-73-79)#dot1x system-auth-control
rfs6000-817379(config-device-00-15-70-81-73-79)#dot1x use aaa-policy aaa-
wireddot1x
```

Following example displays the above configured parameters:

```
rfs6000-817379(config-device-00-15-70-81-73-79)#show context
use profile default-rfs6000
use rf-domain default
hostname rfs6000-817379
 use radius-server-policy for-wired-dot1x
interface me1
  ip address 192.168.0.1/24
interface ge2
  dot1x authenticator host-mode single-host
  dot1x authenticator port-control auto
interface vlan1
  ip address dhcp
  ip dhcp client request options all
logging on
logging console debugging
dot1x system-auth-control
dot1x use aaa-policy aaa-wireddot1x
--More--
rfs6000-817379(config-device-00-15-70-81-73-79)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables or reverts interface settings to their default |

### 7.1.36.2.6 dot1x (supplicant)

*interface-config-ge-instance*

Configures 802.1X supplicant (client) settings

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, NX5500, NX7500

**Syntax**

```
dot1x supplicant username <USERNAME> password [0 <WORD>|2 <WORD>|<WORD>]
```

**Parameters**

- `dot1x supplicant username <USERNAME> password [0 <WORD>|2 <WORD>|<WORD>]`

| | |
|---|---|
| dot1x supplicant | Configures 802.1x suppliant settings |
| username <USERNAME> | Sets the username for authentication<br>• <USERNAME> – Specify the supplicant's username. |
| password [0 <WORD>\| 2 <WORD>\| <WORD>] | Sets the password associated with the supplicant's username. Select any one of the following options:<br>• 0 <WORD> – Sets a clear text password<br>• 2 <WORD> – Sets an encrypted password<br>• <WORD> – Specify the password. |

**Example**

```
rfs4000-229D58(config-profile-testRFS4000-if-ge1)#dot1x supplicant username bob
password 0 test@123

rfs4000-229D58(config-profile-testRFS4000-if-ge1)#show context
 interface ge1
  dot1x supplicant username bob password 0 test@123
  dot1x authenticator host-mode multi-host
  dot1x authenticator guest-vlan 2
  dot1x authenticator reauthenticate
  dot1x authenticator max-reauth-count 6
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
rfs4000-229D58(config-profile-testRFS4000-if-ge1)#
```

The following example shows the configuration made on an AP7522 to enable it as a dot1X supplicant:

```
ap7522-85B19C(config-device-84-24-8D-85-B1-9C-if-ge2)#dot1x supplicant username
bob password 0 bob1234
ap7522-85B19C(config-device-84-24-8D-85-B1-9C)#show context
use profile default-ap7522
use rf-domain default
hostname ap7522-85B19C
no adoption-mode
interface ge1
  switchport mode access
  switchport access vlan 1
  dot1x supplicant username bob password 0 bob1234
logging on
logging console debugging
--More--
ap7522-85B19C(config-device-84-24-8D-85-B1-9C
```

**Related Commands**

| | |
|---|---|
| *no* | Removes 802.1X supplicant (client) settings |

### 7.1.36.2.7 duplex

*interface-config-ge-instance*

Configures duplex mode (for the flow of packets) on this Ethernet port

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
duplex [auto|half|full]
```

**Parameters**

- `duplex [auto|half|full]`

| | |
|---|---|
| auto | Enables automatic duplexity on an interface port. The port automatically detects whether it should run in full or half-duplex mode. (default setting) |
| half | Sets the port to half-duplex mode. Allows communication in one direction only at any given time. When selected, data is sent over the port, then immediately data is received from the direction in which the data was transmitted. |
| full | Sets the port to full-duplex mode. Allows communication in both directions simultaneously. When selected, the port can send data while receiving data as well. |

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-if-ge1)#duplex full

rfs6000-37FABE(config-profile-default-rfs6000-if-ge1)#show context
 interface ge1
  description "This is GigabitEthernet interface for Royal King"
  duplex full
  dot1x supplicant username Bob password 0 test@123
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
  channel-group 1
rfs6000-37FABE(config-profile-default-rfs6000-if-ge1)#
```

**Related Commands**

| | |
|---|---|
| *no* | Reverts to default (auto) |

### 7.1.36.2.8 ip

*interface-config-ge-instance*

Sets the ARP and DHCP components for this Ethernet port

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ip [arp|dhcp]

ip [arp [header-mismatch-validation|trust]|dhcp trust]
```

**Parameters**

- `ip [arp [header-mismatch-validation|trust]|dhcp trust]`

| | |
|---|---|
| arp [header-mismatch-validation\| trust] | Configures ARP packet settings<br>• header-mismatch-validation – Enables matching of source MAC address in the ARP and Ethernet headers to check for mismatch. This option is disabled by default.<br>• trust – Enables trust state for ARP responses on this interface. When enabled, ARP packets received on this port are considered trusted and information from these packets is used to identify rogue devices within the network. This option is disabled by default. |
| dhcp trust | Enables trust state for DHCP responses on this interface. When enabled, only DHCP responses are trusted and forwarded on this port, and a DHCP server can be connected only to a DHCP trusted port. This option is enabled by default. |

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-if-ge1)#ip dhcp trust

rfs6000-37FABE(config-profile-default-rfs6000-if-ge1)#ip arp header-mismatch-
validation

rfs7000-37FABE(config-profile-default-rfs6000-if-ge1)#show context
 interface ge1
  description "This is GigabitEthernet interface for Royal King"
  duplex full
  dot1x supplicant username Bob password 0 test@123
  ip dhcp trust
  ip arp header-mismatch-validation
  qos trust dscp
  qos trust 802.1p
  channel-group 1
rfs6000-37FABE(config-profile-default-rfs6000-if-ge1)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the ARP and DHCP components configured for this interface |

### 7.1.36.2.9 ipv6

*interface-config-ge-instance*

Sets the DHCPv6 and ICMPv6 *neighbor discovery* (ND) components for this interface

The ICMPv6 ND protocol uses ICMP messages and solicited multicast addresses to track neighboring devices on the same local network. These messages are used to discover a neighbor's link layer address and to verify if a neighboring device is reachable.

The ICMP messages are *neighbor solicitation* (NS) and *neighbor advertisement* (NA) messages. When a destination host receives an NS message from a neighbor, it replies back with a NA. The NA contains the following information:

- Source address – This is the IPv6 address of the device sending the NA
- Destination address – This is the IPv6 address of the device from whom the NS message is received
- Data portion – Includes the link layer address of the device sending the NA

NS messages are used to verify a neighbor's (whose ink layer address is known) reachability. To confirm a neighbor's reachability a node sends an NS message in which the neighbor's unicast address is specified as the destination address. If the neighbor sends back an acknowledgment on receipt of the NS message it is considered reachable.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
ipv6 [dhcpv6|nd]

ipv6 dhcpv6 trust

ipv6 nd [header-mismatch-validation|raguard|trust]
```

**Parameters**

- `ipv6 dhcpv6 trust`

| | |
|---|---|
| ipv6 dhcpv6 trust | Enables trust state for DHCPv6 responses on this interface. When enabled, all DHCPv6 responses received on this port are trusted and forwarded. This option is enabled by default.<br>A DHCPv6 server can be connected to a DHCPv6 trusted port. |

- `ipv6 nd [header-mismatch-validation|raguard|trust]`

| | |
|---|---|
| ipv6 nd | Configures IPv6 ND settings |
| header-mismatch-validation | Enables matching of source MAC address in the ICMPv6 ND and Ethernet headers (link layer option) to check for mismatch. This option is disabled by default. |
| raguard | Allows redirection of *router advertisements* (RAs) and ICMPv6 packets originating on this interface. When selected, RAs are periodically sent to hosts or sent in response to neighbor solicitation requests. The advertisement includes IPv6 prefixes and other subnet and host information. This option is enabled by default. |

| | |
|---|---|
| trust | Enables trust state for IPv6 ND requests received on this interface. When enabled, IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the neighbor discovery protocol via ICMPv6 router discovery messages. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; routers respond to the request with a router advertisement packet containing Internet Layer configuration parameters. This option is disabled by default. |

**Example**

```
rfs6000-37FABE(config-device-B4-C7-99-6D-CD-4B-if-ge1)#ipv6 dhcpv6 trust

rfs6000-37FABE(config-device-B4-C7-99-6D-CD-4B-if-ge1)#ipv6 nd header-mismatch-
validation
rfs6000-37FABE(config-device-B4-C7-99-6D-CD-4B-if-ge1)#ipv6 nd trust

rfs6000-37FABE(config-device-B4-C7-99-6D-CD-4B-if-ge1)#show context
interface ge1
  switchport mode access
  switchport access vlan 1
  ipv6 nd trust
  ipv6 nd header-mismatch-validation
  ipv6 dhcpv6 trust
rfs6000-37FABE(config-device-B4-C7-99-6D-CD-4B-if-ge1)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes or reverts IPv6 settings on this interface |

### 7.1.36.2.10 lacp

*interface-config-ge-instance*

Configures the selected GE port's *Link Aggregation Control Protocol* (LACP) port-priority value. If LACP is enabled, and the selected port is a member of a *link aggregation group* (LAG), use this command to configure the port's priority within the LAG.

As per the IEEE 802.3ad standard, LACP enables aggregation of multiple physical links to form a single logical channel. Each aggregated group of physical links is a LAG. When enabled, LACP dynamically determines if link aggregation is possible between two peers, and automatically configures the aggregation. LACP also allows the switch to dynamically reconfigure the LAGs. The LAG is enabled only when LACP detects that the remote device is also using LACP and is able to join the LAG.

Enabling LACP provides automatic recovery in case one or more of the aggregated physical links fail.

**NOTE:** Use the *lacp-channel-group* command to configure this port as a LAG member.

**Supported in the following platforms:**

- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
lacp port-priority <1-65535>
```

**Parameters**

- `lacp port-priority <1-65535>`

| | |
|---|---|
| lacp port-priority <1-65535> | Configures the selected GE port's port-priority value. The selected port's actual priority within the LAG is determined by the port-priority value specified here along with the port's number. Higher the value, lower is the priority. Use this option to manipulate a port's priority. For example, in a LAG having five physical ports, four active and one standby, manually increasing the standby port's priority ensures that if one of the active port fails, the standby port is included in the LAG during re-negotiation.<br>• <1-65535> – Specify a value from 1 - 65535. The default value is 32768. |

**Example**

```
nx9500-6C8809(config-profile-testnx9000-if-ge1)#lacp port-priority 2

nx9500-6C8809(config-profile-testnx9000-if-ge1)#show context
 interface ge1
  lacp port-priority 2
nx9500-6C8809(config-profile-testnx9000-if-ge1)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the selected GE port's configured port-priority value |

### 7.1.36.2.11 lacp-channel-group

*interface-config-ge-instance*

Configures the selected GE port as a member of a port channel group (also referred as LAG)

As per the IEEE 802.3ad standard, LACP enables the aggregation of multiple physical links (ethernet ports) to form a single logical channel. When enabled, LACP dynamically determines if link aggregation is possible and then automatically configures the aggregation. LACP also allows the switch to dynamically reconfigure the LAGs. The LAG is enabled only when LACP detects that the remote device is also using LACP and is able to join the LAG.

**NOTE:** Successful aggregation of two or more physical links is feasible only if the aggregating physical links are configured identically. To ensure uniformity in configuration across LAG members, implement configuration changes (such as changes in the switching mode, speed, etc.) on the logical port (the port-channel) and not on the physical port. Changes made on the port-channel will cascade down to each member of the LAG thereby retaining uniformity.

**Supported in the following platforms:**

- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
lacp-channel-group <1-4> mode [active|passive]
```

**Parameters**

- `lacp-channel-group <1-4> mode [active|passive]`

| | |
|---|---|
| lacp-channel-group <1-4> | Associates this GE port with an existing port-channel group<br>• <1-4> – Specify a value from 1 - 4.<br>Use the *interface > port-channel > <1-4>* command to configure a port-channel group. For more information, see *interface-config-port-channel-instance*. |
| mode [active\|passive] | After configuring the selected port as a LAG member, specify whether the port is an active or passive member within the group. An active member initiates and participates in LACP negotiations.<br>• active – Configures the port as an active member. When set to active, the port always transmits LACPDU irrespective of the remote device's port mode.<br>• passive – Configures the port as passive member. When set to passive, the port will only respond to LACPDU received from its corresponding *Active* port.<br>At least one port within a LAG, on either of the two negotiating peers, should be in the active mode. LACP negotiations are not initiated if all LAG member ports are passive. Further, the peer-to-peer LACP negotiations are always initiated by the peer with the lower system-priority value. For more information on configuring the system-priority, see *lacp*. |

**Example**

```
nx9500-6C8809(config-profile-testnx9000-if-ge1)#lacp-channel-group 2 mode active

nx9500-6C8809(config-profile-test2nx9000-if-ge1)#show context
 interface ge1
  lacp-channel-group 2 mode active
  lacp port-priority 2
nx9500-6C8809(config-profile-test2nx900-if-ge1)#
```

To enable dynamic link aggregation on a device (service platform), execute the following steps:

1 Create a port-channel group on the device. Enter the port-channel configuration mode.

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#interface port-channel 1
```

a Set the switching mode to *access* or *trunk* as per requirement. In this example, the mode is set to 'access'.

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09-if-port-channel1)#switchport
mode
access
```

b Specify the VLAN to switch, commit changes and exit.

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09-if-port-channel1)#switchport
access vlan 1
nx9500-6C8809(config-device-B4-C7-99-6C-88-09-if-port-channel1)#commit
nx9500-6C8809(config-device-B4-C7-99-6C-88-09-if-port-channel1)#exit
```

2 Enable dynamic link aggregation on the device's physical port. Enter the GE port's configuration mode.

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#interface ge 2
```

a Enable link aggregation and associate the port with the port-channel group created in step 1.

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09-if-ge2)#lacp-channel-group 1
mode
active

Note, the mode can be set to passive. However, at least one of the aggregated
GE ports in the port-channel group should be active in order to initiate link
aggregation negotiations with other LACP-enabled peers.
```

b Specify the GE port's priority value.

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09-if-ge2)#lacp port-priority 2
```

**Related Commands**

| | |
|---|---|
| *no* | Removes the selected GE port's port-channel group membership |

### 7.1.36.2.12 lldp

*interface-config-ge-instance*

Configures *Link Local Discovery Protocol* (LLDP) parameters on this Ethernet port

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
lldp [receive|transmit]
```

**Parameters**

- `lldp [receive|transmit]`

| | |
|---|---|
| receive | Enables LLDP *Protocol Data Units* (PDUs) snooping. When enabled, the port receives periodic updates from a multicast address informing about presence of neighbors. This option is enabled by default. |
| transmit | Enables LLDP PDU transmission. When enabled, the port sends out periodic interface updates to a multicast address to advertise its presence to neighbors. This option is enabled by default. |

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-if-ge1)#lldp transmit
```

**Related Commands**

| | |
|---|---|
| *no* | Disables or reverts interface settings to their default |

### 7.1.36.2.13 mac-auth

*interface-config-ge-instance*

Enables authentication of MAC addresses on the selected wired port. When enabled, this feature authenticates the MAC address of a device, connecting to this interface, with a RADIUS server. When successfully authenticated, packets from the source are processed. Since only one MAC address is supported per wired port, packets from all other sources are dropped.

For more information on enabling this feature, see *mac-auth*.

Enable port MAC authentication in conjunction with Wired 802.1x settings to configure a MAC authentication AAA policy.

This option is also available in the device configuration mode.

**Supported in the following platforms:**

- Access Points — AP6522 AP6562, AP7161, AP7502, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
mac-auth
```

**Parameters**

None

**Example**

```
rfs4000-229D58(config-profile-testRFS4000-if-ge1)#mac-auth

rfs4000-229D58(config-profile-testRFS4000-if-ge1)#show context
 interface ge1
  mac-auth
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
  channel-group 1
rfs4000-229D58(config-profile-testRFS4000-if-ge1)#

rfs4000-229D58(config-profile-testRFS4000-if-ge5)#mac-auth

rfs4000-229D58(config-device-00-23-68-22-9D-58-if-ge5)#show context
 interface ge5
  switchport mode access
  switchport access vlan 1
  dot1x authenticator host-mode single-host
  dot1x authenticator guest-vlan 5
  dot1x authenticator port-control auto
  mac-auth
rfs4000-229D58(config-device-00-23-68-22-9D-58-if-ge5)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables authentication of MAC addresses on the selected wired port |

### 7.1.36.2.14 no

*interface-config-ge-instance*

Removes or reverts the selected Ethernet port settings

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
no [captive-portal-enforcement|cdp|channel-group|description|dot1x|duplex|ip|
ipv6|lacp|lacp-channel-group|lldp|mac-auth|power|qos|shutdown|spanning-tree|
speed|switchport|use]

no [captive-portal-enforcement|channel-group|description|duplex|mac-auth|
shutdown|speed]

no [cdp|lldp] [receive|transmit]

no dot1x [authenticator [guest-vlan|host-mode|max-reauth-req|port-control|
reauthentication|timeout [quiet-period|reauth-period]]|supplicant]

no ip [arp [header-mismatch-validation|trust]|dhcp trust]

no ipv6 [dhcpv6 trust|nd [header-mismatch-validation|raguard|trust]]

no [lacp port-priority|lacp-channel-group]

no power {best-effort|limit|priority}

no qos trust [802.1p|cos|dscp]

no spanning-tree [bpdufilter|bpduguard|force-version|guard|link-type|mst|
portfast]

no switchport [access vlan|mode|trunk native tagged]

no use [ip-access-list|ipv6-access-list|mac-access-list] in
```

**Parameters**

- no <PARAMETERS>

| | |
|---|---|
| no <PARAMETERS> | Removes or reverts this Ethernet port settings based on the parameters passed |

**Usage Guidelines**

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

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-if-ge1)#no cdp

rfs6000-37FABE(config-profile-default-rfs6000-if-ge1)#no duplex
```

### 7.1.36.2.15 power

*interface-config-ge-instance*

Configures *Power over Ethernet* (PoE) settings on this interface

When configured, this option allows the selected port to use Power over Ethernet. When enabled, the controller supports 802.3af PoE on each of its GE ports. PoE allows users to monitor port power consumption and configure power usage limits and priorities for each GE port.

**Supported in the following platforms:**

- Wireless Controllers — RFS4000, RFS6000

**Syntax**

```
power {best-effort|limit <0-40>|priority [critical|high|low]}
```

**Parameters**

- `power {best-effort|limit <0-40>|priority [critical|high|low]}`

| | |
|---|---|
| power | Configures power related thresholds for this interface |
| best-effort | Optional. Enables power when the device is not operating from an 802.3at class 4 power source |
| limit <0-40> | Optional. Configures the PoE power limit from 0 - 40 Watts. The default is 30 Watts. |
| priority [critical\|high\|low] | Optional. Configures the PoE power priority on this interface. This is the priority assigned to this port versus the power requirements of the other ports available on the controller.<br>• critical – Sets PoE priority as critical<br>• high – Sets PoE priority as high<br>• low – Sets PoE priority as low. This is the default setting. |

**Example**

```
rfs4000-229D58(config-profile-testRFS4000-if-ge1)#power limit 30

rfs4000-229D58(config-profile-testRFS4000-if-ge1)#power priority critical

rfs4000-229D58(config-profile-testRFS4000-if-ge1)#show context
 interface ge1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
  power limit 30
  power priority critical
rfs4000-229D58(config-profile-testRFS4000-if-ge1)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes PoE settings on this interface |

### 7.1.36.2.16 qos

*interface-config-ge-instance*

Defines *Quality of Service* (QoS) settings on this Ethernet port

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
qos trust [802.1p|cos|dscp]
```

**Parameters**

- `qos trust [802.1p|cos|dscp]`

| | |
|---|---|
| trust [802.1p\|cos\|dscp] | Trusts QoS values ingressing on this interface<br>• 802.1p – Trusts 802.1p COS values ingressing on this interface<br>• cos – Trusts 802.1p COS values ingressing on this interface. This option is enabled by default.<br>• dscp – Trusts IP DSCP QOS values ingressing on this interface. This option is enabled by default. |

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-if-ge1)#qos trust dscp

rfs6000-37FABE(config-profile-default-rfs6000-if-ge1)#qos trust 802.1p

rfs6000-37FABE(config-profile-default-rfs6000-if-ge1)#show context
 interface ge1
  description "This is GigabitEthernet interface for Royal King"
  duplex full
  dot1x supplicant username Bob password 0 test@123
  ip dhcp trust
  ip arp header-mismatch-validation
  qos trust dscp
  qos trust 802.1p
  channel-group 1
rfs6000-37FABE(config-profile-default-rfs6000-if-ge1)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes QoS settings on the selected interface |

### 7.1.36.2.17 shutdown

*interface-config-ge-instance*

Shuts down (disables) an interface. The interface is administratively enabled unless explicitly disabled using this command.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
shutdown
```

**Parameters**

None

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-if-ge1)#shutdown
```

**Related Commands**

| | |
|---|---|
| *no* | Disables or reverts interface settings to their default |

### 7.1.36.2.18 spanning-tree

*interface-config-ge-instance*

Configures spanning tree parameters

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
spanning-tree [bpdufilter|bpduguard|force-version|guard|link-type|mst|port-cisco-interoperability|portfast]

spanning-tree [force-version <0-3>|guard root|portfast]

spanning-tree [bpdufilter|bpduguard] [default|disable|enable]

spanning-tree link-type [point-to-point|shared]

spanning-tree mst <0-15> [cost <1-200000000>|port-priority <0-240>]

spanning-tree port-cisco-interoperability [disable|enable]
```

**Parameters**

- `spanning-tree [force-version <0-3>|guard root|portfast]`

| | |
|---|---|
| force-version <0-3> | Specifies the spanning tree force version. A version identifier of less than 2 enforces the spanning tree protocol. Select one of the following versions:<br>• 0 – *Spanning Tree Protocol* (STP)<br>• 1 – Not supported<br>• 2 – *Rapid Spanning tree Protocol* (RSTP)<br>• 3 – *Multiple Spanning Tree Protocol* (MSTP). This is the default setting |
| guard root | Enables Root Guard for the port<br>The Root Guard disables superior *Bridge Protocol Data Unit* (BPDU) reception. The Root Guard ensures the enabled port is a designated port. If the Root Guard enabled port receives a superior BPDU, it moves to a discarding state (root-inconsistent STP state). This state is equivalent to a listening state, and data is not forwarded across the port. Therefore, enabling the guard root enforces the root bridge position. Use the no parameter with this command to disable the Root Guard. |
| portfast | Enables rapid transitions. Enabling PortFast allows the port to bypass the listening and learning states. |

- `spanning-tree [bpdufilter|bpduguard] [default|disable|enable]`

| | |
|---|---|
| bpdufilter [default\|disable\|enable] | Sets a PortFast BPDU filter for the port<br>Use the no parameter with this command to revert the port BPDU filter to its default. The spanning tree protocol sends BPDUs from all ports. Enabling the BPDU filter ensures PortFast enabled ports do not transmit or receive BPDUs. |

| | |
|---|---|
| bpduguard [default\|disable\| enable] | Enables BPDU guard on a port<br>Use the no parameter with this command to set BPDU guard to its default.<br>When the BPDU guard is set for a bridge, all PortFast-enabled ports that have the BPDU guard set to default shut down upon receiving a BPDU. If this occurs, the BPDU is not processed. The port can be brought back either manually (using the no shutdown command), or by configuring the errdisable-timeout to enable the port after a specified interval. |

- `spanning-tree link-type [point-to-point|shared]`

| | |
|---|---|
| link-type [point-to-point\|shared] | Enables point-to-point or shared link types<br>• point-to-point – Enables rapid transition. This option indicates the port should be treated as connected to a point-to-point link. A port connected to a controller is a point-to-point link.<br>• shared – Disables rapid transition. This option indicates this port should be treated as having a shared connection. A port connected to a hub is on a shared link, |

- `spanning-tree mst <0-15> [cost <1-200000000>|port-priority <0-240>]`

| | |
|---|---|
| mst <0-15> | Configures MST on a spanning tree |
| cost <1-200000000> | Defines path cost for a port from 1 - 200000000. The default path cost depends on the speed of the port. The cost helps determine the role of the port in the MSTP network. The designated cost is the cost for a packet to travel from this port to the root in the MSTP configuration. The slower the media, the higher the cost. |
| port-priority <0-240> | Defines port priority for a bridge from 1 - 240. Lower the priority greater is the likelihood of the port becoming a designated port. Applying a higher value impacts the port's likelihood of becoming a designated port. |

- `spanning-tree port-cisco-interoperability [disable|enable]`

| | |
|---|---|
| port-cisco-interoperability | Enables interoperability with Cisco's version of MSTP (which is incompatible with standard MSTP) |
| enable | Enables CISCO Interoperability |
| disable | Disables CISCO Interoperability. The default is disabled. |

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-if-ge1)#spanning-tree bpdufilter
disable

rfs6000-37FABE(config-profile-default-rfs6000-if-ge1)#spanning-tree bpduguard
enable

rfs6000-37FABE(config-profile-default-rfs6000-if-ge1)#spanning-tree force-version
1

rfs6000-37FABE(config-profile-default-rfs6000-if-ge1)#spanning-tree guard root

rfs6000-37FABE(config-profile-default-rfs6000-if-ge1)#spanning-tree mst 2 port-
priority 10
```

```
rfs6000-37FABE(config-profile-default-rfs6000-if-ge1)#show context
 interface ge1
  description "This is GigabitEthernet interface for Royal King"
  duplex full
  spanning-tree bpduguard enable
  spanning-tree bpdufilter disable
  spanning-tree force-version 1
  spanning-tree guard root
  spanning-tree mst 2 port-priority 10
 --More--
rfs6000-37FABE(config-profile-default-rfs6000-if-ge1)#
```

**Related Commands**

| | |
|---|---|
| *no* | Removes spanning tree settings configured on this interface |

### 7.1.36.2.19 speed

*interface-config-ge-instance*

Specifies the speed of a FastEthernet (10/100) or GigabitEthernet (10/100/1000) port. This is the speed at which the port can receive and transmit the data.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
speed [10|100|1000|auto]
```

**Parameters**

- `speed [10|100|1000|auto]`

| | |
|---|---|
| 10 | Forces 10 Mbps operation |
| 100 | Forces 100 Mbps operation |
| 1000 | Forces 1000 Mbps operation |
| auto | Port automatically detects its operational speed based on the port at the other end of the link. Select this option to enable the port to automatically exchange information about data transmission speed and duplex capabilities. Auto negotiation is helpful when in an environment where different devices are connected and disconnected on a regular basis. |

**Usage Guidelines**

Set the interface speed to auto detect and use the fastest speed available. Speed detection is based on connected network hardware.

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-if-ge1)#speed 10

rfs6000-37FABE(config-profile-default-rfs6000-if-ge1)#show context
 interface ge1
  description "This is GigabitEthernet interface for Royal King"
  speed 10
  duplex full
  spanning-tree bpduguard enable
  spanning-tree bpdufilter disable
  spanning-tree force-version 1
  spanning-tree guard root
  spanning-tree mst 2 port-priority 10
  dot1x supplicant username Bob password 0 test@123
  ip dhcp trust
  ip arp header-mismatch-validation
  qos trust dscp
  qos trust 802.1p
  channel-group 1
rfs6000-37FABE(config-profile-default-rfs6000-if-ge1)#
```

**Related Commands**

| | |
|---|---|
| *no* | Resets speed to default (auto) |

### 7.1.36.2.20 switchport

*interface-config-ge-instance*

Sets switching mode characteristics for the selected interface

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
switchport [access|mode|trunk]

switchport access vlan [<1-4094>|<VLAN-ALIAS-NAME>]
switchport mode [access|trunk]
switchport trunk [allowed|native]
switchport trunk allowed vlan [<VLAN-ID>|add <VLAN-ID>|none|remove <VLAN-ID>]
switchport trunk native [tagged|vlan [<1-4094>|<VLAN-ALIAS-NAME>]]
```

**Parameters**

- `switchport access vlan [<1-4094>|<VLAN-ALIAS-NAME>]`

| | |
|---|---|
| access vlan [<1-4094>\| <VLAN-ALIAS-NAME>] | Sets the VLAN when interface is in the access mode. You can either directly specify the native VLAN ID or use a VLAN alias to identify the native VLAN.<br>• <1-4094> – Specify the SVI VLAN ID from 1 - 4094.<br>• <VLAN-ALIAS-NAME> – Specify the VLAN alias name (should be existing and configured).<br>An Ethernet port in the access mode accepts packets only from the native VLAN. Frames are forwarded out the port untagged with no 802.1Q header. All frames received on the port are expected as untagged and are mapped to the native VLAN. |

- `switchport mode [access|trunk]`

| | |
|---|---|
| mode [access\|trunk] | Sets the interface's switching mode to access or trunk (can only be used on physical - layer 2 - interfaces)<br>• access – If access mode is selected, the access VLAN is automatically set to VLAN1. In this mode, only untagged packets in the access VLAN (vlan1) are accepted on this port. All tagged packets are discarded.<br>• trunk – If trunk mode is selected, tagged VLAN packets are accepted. The native VLAN is automatically set to VLAN1. Untagged packets are placed in the native VLAN by the wireless controller or service platform. Outgoing packets in the native VLAN are sent untagged. The default mode for both ports is trunk. |

- `switchport trunk allowed vlan [<VLAN-ID>|add <VLAN-ID>|none|remove <VLAN-ID>]`

| | |
|---|---|
| trunk allowed | Sets trunking mode, allowed VLANs characteristics of the port. Use this option to add VLANs that exclusively send packets over the listed port. |

| | |
|---|---|
| vlan [<VLAN-ID>\| add <VLAN-ID>\| none\| remove <VLAN-ID> | Sets allowed VLAN options. The options are:<br>• <VLAN-ID> – Allows a group of VLAN IDs. Specify the VLAN IDs, can be either a range (55-60) or a comma-separated list (35, 41, etc.)<br>• none – Allows no VLANs to transmit or receive through the layer 2 interface<br>• add <VLAN-ID> – Adds VLANs to the current list<br>  • <VLAN-ID> – Specify the VLAN IDs. Can be either a range of VLAN (55-60) or a list of comma separated IDs (35, 41, etc.)<br>• remove <VLAN-ID> – Removes VLANs from the current list<br>  • <VLAN-ID> – Specify the VLAN IDs. Can be either a range of VLAN (55-60) or a list of comma separated IDs (35, 41, etc.)<br>Allowed VLANs are configured only when the switching mode is set to “trunk”. |

- `switchport trunk native [tagged|vlan [<1-4094>|<VLAN-ALIAS-NAME>]]`

| | |
|---|---|
| trunk | Sets trunking mode characteristics of the switchport |
| native [tagged\| vlan [<1-4094>\| <VLAN-ALIAS-NAME>]] | Configures the native VLAN ID for the trunk-mode port<br>The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. Additionally, the native VLAN is the VLAN untagged traffic is directed over when using a port in trunk mode.<br>• tagged – Tags the native VLAN. When a frame is tagged, the 12 bit frame VLAN ID is added to the 802.1Q header enabling upstream Ethernet devices to know which VLAN ID the frame belongs to. The device reads the 12 bit VLAN ID and forwards the frame to the appropriate VLAN. When a frame is received with no 802.1Q header, the upstream device classifies the frame using the default or native VLAN assigned to the Trunk port. A native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame.<br>• vlan [<1-4094>\|<VLAN-ALIAS-NAME>] – Sets the native VLAN for classifying untagged traffic when the interface is in trunking mode.<br>  • <1-4094> – Specify a value from 1 - 4094.<br>  • <VLAN-ALIAS-NAME> – Specify the VLAN alias name used to identify the VLANs. The VLAN alias should be existing and configured. |

**Usage Guidelines**

Interfaces ge1 - ge4 can be configured as trunk or in access mode. An interface configured as “trunk” allows packets (from the given list of VLANs) to be added to the trunk. An interface configured as “access” allows packets only from native VLANs.

Use the *[no] switchport (access|mode|trunk)* to undo switchport configurations.

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-if-ge1)#switchport trunk native
tagged

rfs6000-37FABE(config-profile-default-rfs6000-if-ge1)#switchport access vlan 1

rfs6000-37FABE(config-profile-default-rfs6000-if-ge1)#show context
 interface ge1
  description "This is GigabitEthernet interface for Royal King"
  speed 10
  duplex full
  switchport mode access
  switchport access vlan 1
  spanning-tree bpduguard enable
  spanning-tree bpdufilter disable
  --More--
rfs6000-37FABE(config-profile-default-rfs6000-if-ge1)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables or reverts interface settings to their default |

### 7.1.36.2.21 use

*interface-config-ge-instance*

Specifies the IP (IPv4 and IPv6) access list and MAC access list used with this Ethernet port. The associated ACL firewall inspects IP and MAC traffic flows and detects attacks typically not visible to traditional wired firewall appliances.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
use [ip-access-list in <IPv4-ACCESS-LIST-NAME>|ipv6-access-list <IPv6-ACCESS-LIST-NAME>|mac-access-list in <MAC-ACCESS-LIST-NAME>]
```

**Parameters**

```
• use [ip-access-list in <IPv4-ACCESS-LIST-NAME>|ipv6-access-list <IPv6-ACCESS-LIST-NAME>|mac-access-list in <MAC-ACCESS-LIST-NAME>]
```

| | |
|---|---|
| ip-access-list in <IPv4-ACCESS-LIST-NAME> | Associates an IPv4 access list with this Ethernet port. IPv4 is a connectionless protocol for packet switched networking. IPv4 operates as a best effort delivery method, as it does not guarantee delivery, and does not ensure proper sequencing or duplicate delivery (unlike (TCP). IPv4 hosts can use link local addressing to provide local connectivity.<br>• in – Applies the IPv4 ACL on incoming packets<br>• <IPv4-ACCESS-LIST-NAME> – Specify the IPv4 access list name (it should be an existing and configured). |
| ipv6-access-list in <IPv6-ACCESS-LIST-NAME> | Associates an IPv6 access list with this Ethernet port. IPv6 is the latest revision of the IP designed to replace IPv4. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.<br>• in – Applies the IPv6 ACL on incoming packets<br>• <IPv6-ACCESS-LIST-NAME> – Specify the IPv6 access list name (it should be an existing and configured). |
| mac-access-list in <MAC-ACCESS-LIST-NAME> | Associates a MAC access list with this Ethernet port. MAC ACLs filter/mark packets based on the MAC address from which they arrive, as opposed to filtering packets on layer 2 ports.<br>• in – Applies the MAC ACL on incoming packets<br>• <MAC-ACCESS-LIST-NAME> – Specify the MAC access list name (it should be an existing and configured). |

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-if-ge1)#use mac-access-list in test

rfs6000-37FABE(config-profile-default-rfs6000-if-ge1)#use ip-access-list in test

rfs6000-37FABE(config-profile-default-rfs6000-if-ge1)#show context
 interface ge1
  description "This is GigabitEthernet interface for Royal King"
  speed 10
  duplex full
  switchport mode accessi
  switchport access vlan 1
  use ip-access-list in test
  use mac-access-list in test
  spanning-tree bpduguard enable
  spanning-tree bpdufilter disable
  spanning-tree force-version 1
--More--
rfs6000-37FABE(config-profile-default-rfs6000-if-ge1)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disassociates the IP access list or MAC access list from the interface |

### 7.1.36.3 interface-config-vlan-instance

*interface*

Use the config-profile-<DEVICE-PROFILE-NAME> mode to configure Ethernet, VLAN and tunnel settings.

To switch to this mode, use the following commands:

```
<DEVICE>(config-profile-default-<DEVICE-TYPE>)#interface [<INTERFACE-NAME>|fe <1-
4>|ge <1-24>|me1|port-channel <1-4>|pppoe1|radio [1|2|3]|up1|vlan <1-4094>|wwan1|
xge <1-24>]
```

The following example uses the config-profile-default-rfs7000 instance to configure a VLAN interface:

```
rfs6000-37FABE(config-profile-default-rfs6000)#interface vlan 8
rfs6000-37FABE(config-profile-default-rfs6000-if-vlan8)#

rfs6000-37FABE(config-profile-default-rfs6000-if-vlan8)#?
SVI configuration commands:
  crypto                Encryption module
  description           Vlan description
  dhcp                  Dynamic Host Configuration Protocol (DHCP)
  dhcp-relay-incoming   Allow on-board DHCP server to respond to relayed DHCP
                        packets on this interface
  ip                    Interface Internet Protocol config commands
  ipv6                  Internet Protocol version 6 (IPv6)
  no                    Negate a command or set its defaults
  shutdown              Shutdown the selected interface
  use                   Set setting to use

  clrscr                Clears the display screen
  commit                Commit all changes made in this session
  do                    Run commands from Exec mode
  end                   End current mode and change to EXEC mode
  exit                  End current mode and down to previous mode
  help                  Description of the interactive help system
  revert                Revert changes
  service               Service Commands
  show                  Show running system information
  write                 Write running configuration to memory or terminal

rfs6000-37FABE(config-profile-default-rfs6000-if-vlan8)#
```

The following table summarizes interface VLAN configuration commands:

| Commands | Description | Reference |
|---|---|---|
| *crypto* | Defines the encryption module used with this VLAN interface | *page 7-218* |
| *description* | Defines the VLAN interface description | *page 7-219* |
| *dhcp* | Enables inclusion of optional fields (client identifier) in DHCP client requests | *page 7-220* |
| *dhcp-relay-incoming* | Allows an onboard DHCP server to respond to relayed DHCP packets on this interface | *page 7-221* |
| *ip* | Configures the VLAN interface's IP settings | *page 7-222* |
| *ipv6* | Configures the VLAN interface's IPv6 settings | *page 7-225* |
| *no* | Removes or reverts this VLAN interface's settings to default | *page 7-230* |
| *shutdown* | Shuts down this VLAN interface | *page 7-232* |
| *use* | Associates an IP (IPv4 and IPv6) access list, bonjour-gw-discovery policy, and an IPv6-route-advertisement policy with this VLAN interface | *page 7-233* |

### 7.1.36.3.1 crypto

*interface-config-vlan-instance*

Associates an existing and configured VPN crypto map with this VLAN interface.

Crypto map entries are sets of configuration parameters for encrypting packets that pass through the VPN tunnel. For more information on crypto maps, see *crypto-map-config-commands*.

**Supported in the following platforms:**

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
crypto map <CRYPTO-MAP-NAME>
```

**Parameters**

- `crypto map <CRYPTO-MAP-NAME>`

| | |
|---|---|
| map <CRYPTO-MAP-NAME> | Attaches a crypto map to the selected VLAN interface. The crypto map should be existing and configured.<br>• <CRYPTO-MAP-NAME> – Specify the crypto map name. |

**Example**

```
rfs6000-37FABE(config-profile-default-rfs6000-if-vlan8)#crypto map map1

rfs6000-37FABE(config-profile-default-rfs6000-if-vlan8)#show context
 interface vlan8
  crypto map map1
rfs6000-37FABE(config-profile-default-rfs6000-if-vlan8)#
```

**Related Commands**

| | |
|---|---|
| *no* | Disables or reverts interface VLAN settings to their default |