THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACcompanyING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (https://www.openssl.org/)

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2018–2019 Cisco Systems, Inc. All rights reserved.
# CONTENTS

## PREFACE
- Preface xxiii
  - Audience xxiii
  - Document Conventions xxiii
  - Related Documentation for Cisco Nexus 9000 Series Switches xxiv
  - Documentation Feedback xxiv
  - Communications, Services, and Additional Information xxiv

## CHAPTER 1
- New and Changed Information 1
  - New and Changed Information 1

## CHAPTER 2
- Overview 3
  - Software Image 3
  - Cisco NX-OS Device Configuration Methods 3
    - Configuring with CLI or XML Management Interface 4
    - Configuring with Cisco DCNM 4
  - Network Time Protocol 5
  - Cisco Discovery Protocol 5
  - Session Manager 5
  - Scheduler 5
  - SNMP 5
  - Online Diagnostics 5
  - Onboard Failure Logging 6
  - SPAN 6
  - ERSPAN 6
  - LLDP 6
  - MPLS Stripping 6
CHAPTER 3 Configuring Switch Profiles

About Switch Profiles

- Switch Profile Configuration Modes
  - Configuration Synchronization Mode
- Switch Profile Mode
- Switch Profile Import Mode
- Configuration Validation
  - Mutual Exclusion Checks
  - Merge Checks
- Software Upgrades and Downgrades with Switch Profiles

Licensing Requirements for Switch Profiles

Guidelines and Limitations for Switch Profiles

Configuring Switch Profiles

- Adding or Modifying Switch Profile Commands
- Importing a Switch Profile
- Importing Configurations in a vPC Topology
- Isolating a Peer Switch
- Deleting a Switch Profile
- Manually Correcting Mutex and Merge Failures

Verifying the Switch Profile Configuration

Configuration Examples for Switch Profiles

- Creating a Switch Profile on a Local and a Peer Switch
- Verifying the Synchronization Status
- Showing the Running Configuration
- Displaying the Switch Profile Synchronization Between the Local and the Peer Switch
- Displaying Verify and Commit on the Local and the Peer Switch
- Displaying the Successful and Unsuccessful Synchronization Between the Local and the Peer Switch
- Displaying the Switch Profile Buffer
Importing Configurations 28
Migrating to Cisco NX-OS Release 7.0(3)I2(1) or Higher in a Fabric Extender Straight-Through Topology 30
Replacing a Cisco Nexus 9000 Series Switch 30
Synchronizing Configurations 31
Synchronizing Configurations After a Cisco Nexus 9000 Series Switch Reboots 31
Synchronizing Configurations When the mgmt0 Interface Connectivity Is Lost 32
Reverting an Inadvertent Port Mode Change of Layer 2 to Layer 3 in Global Configuration Mode 32

CHAPTER 4

Configuring PTP 33
About PTP 33
PTP Device Types 34
Clocks 34
PTP Process 35
High Availability for PTP 36
Licensing Requirements for PTP 37
Guidelines and Limitations for PTP 37
Default Settings for PTP 39
Configuring PTP 39
Configuring PTP Globally 39
Configuring PTP on an Interface 41
Configuring PTP in Unicast Mode 44
Configuring Unicast Mode 44
Assigning Master Role 44
Assigning Slave Role 45
Configuring Unicast Source Address 45
Timestamp Tagging 46
Configuring Timestamp Tagging 46
Configuring the TTAG Marker Packets and Time Interval 47
Configuring a PTP Interface to Stay in a Master State 48
Verifying the PTP Configuration 49
Configuration Examples for PTP 50
Additional References 52
CHAPTER 5

Configuring NTP 53

About NTP 53
NTP Associations 54
NTP as a Time Server 54
Clock Manager 54
High Availability 54
Virtualization Support 54
Licensing Requirements for NTP 55
Prerequisites for NTP 55
Guidelines and Limitations for NTP 55
Default Settings for NTP 56
Configuring NTP 56
Enabling or Disabling NTP 56
Configuring the Device as an Authoritative NTP Server 57
Configuring an NTP Server and Peer 58
Configuring NTP Authentication 59
Configuring NTP Access Restrictions 61
Configuring the NTP Source IP Address 63
Configuring the NTP Source Interface 63
Configuring NTP Logging 64
Verifying the NTP Configuration 64
Configuration Examples for NTP 65
Additional References 66
Related Documents 66
MIBs 66

CHAPTER 6

Configuring CDP 67

About CDP 67
VTP Feature Support 68
High Availability 68
Virtualization Support 68
Licensing Requirements for CDP 69
CHAPTER 9

Configuring Session Manager  127
About Session Manager  127
High Availability  128
Licensing Requirements for Session Manager  128
Prerequisites for Session Manager  128
Guidelines and Limitations for Session Manager  128
Configuring Session Manager  129
Creating a Session  129
Configuring ACLs in a Session  129
Verifying a Session  130
Committing a Session  130
Saving a Session  130
Discarding a Session  131
Verifying the Session Manager Configuration  131
Configuration Example for Session Manager  131
Additional References  132
Related Documents  132

CHAPTER 10

Configuring the Scheduler  133
About the Scheduler  133
Remote User Authentication  134
Logs  134
High Availability  134
Licensing Requirements for the Scheduler  134
Prerequisites for the Scheduler  134
Guidelines and Limitations for the Scheduler  135
Default Settings for the Scheduler  135
Configuring the Scheduler  135
Enabling or Disabling the Scheduler  135
Defining the Scheduler Log File Size 136
Configuring Remote User Authentication 136
Defining a Job 137
Deleting a Job 138
Defining a Timetable 139
Clearing the Scheduler Log File 141
Verifying the Scheduler Configuration 141
Configuration Examples for the Scheduler 141
Creating a Scheduler Job 141
Scheduling a Scheduler Job 142
Displaying the Job Schedule 142
Displaying the Results of Running Scheduler Jobs 142

CHAPTER 11

Configuring SNMP 145
About SNMP 145
SNMP Functional Overview 145
SNMP Notifications 146
SNMPv3 147
  Security Models and Levels for SNMPv1, v2, v3 147
  User-Based Security Model 148
  CLI and SNMP User Synchronization 149
  Group-Based SNMP Access 150
SNMP and Embedded Event Manager 150
Multiple Instance Support 150
High Availability for SNMP 150
Virtualization Support for SNMP 150
Licensing Requirements for SNMP 151
Guidelines and Limitations for SNMP 151
Default Settings for SNMP 152
Configuring SNMP 152
  Configuring SNMP Users 152
  Enforcing SNMP Message Encryption 153
  Assigning SNMPv3 Users to Multiple Roles 153
  Creating SNMP Communities 154
CHAPTER 17 Configuring ERSPAN 249
   About ERSPAN 249
      ERSPAN Sources 249
      ERSPAN Sessions 250
         Localized ERSPAN Sessions 250
      ERSPAN Truncation 250
   Licensing Requirements for ERSPAN 250
   Prerequisites for ERSPAN 251
   Guidelines and Limitations for ERSPAN 251
   Default Settings 253
   Configuring ERSPAN 254
      Configuring an ERSPAN Source Session 254
      Shutting Down or Activating an ERSPAN Session 257
      Configuring an ERSPAN ACL 258
      Configuring UDF-Based ERSPAN 260
      Configuring ERSPAN Truncation 263
   Verifying the ERSPAN Configuration 264
   Configuration Examples for ERSPAN 265
      Configuration Example for a Unidirectional ERSPAN Session 265
      Configuration Example for an ERSPAN ACL 265
      Configuration Example for a Marker Packet 265
      Configuration Examples for UDF-Based ERSPAN 266
      Configuration Example for ERSPAN Truncation 267

CHAPTER 18 Configuring LLDP 269
   About LLDP 269
      About DCBXP 270
      High Availability 270
      Virtualization Support 271
   Licensing Requirements for LLDP 271
   Guidelines and Limitations for LLDP 271
   Default Settings for LLDP 271
   Configuring LLDP 272
Enabling or Disabling LLDP Globally 272
Enabling or Disabling LLDP on an Interface 273
Configuring the DCBXP Protocol Version 274
Configuring Optional LLDP Parameters 275
Verifying the LLDP Configuration 276
Configuration Example for LLDP 276

CHAPTER 19

Configuring NetFlow 279

About NetFlow 279
  Dual-Layer NetFlow Implementation 280
  Flow Records 280
  Flow Exporters 280
  Export Format 281
  Layer 2 NetFlow Keys 281
  Flow Monitors 281
  High Availability 281
Licensing Requirements for NetFlow 281
Prerequisites for NetFlow 282
Guidelines and Limitations for NetFlow 282
Configuring NetFlow 283
  Enabling the NetFlow Feature 284
  Creating a Flow Record 284
    Specifying the Match Parameters 285
    Specifying the Collect Parameters 286
  Creating a Flow Exporter 287
  Creating a Flow Monitor 288
  Applying a Flow Monitor to an Interface 289
Configuring Bridged NetFlow on a VLAN 290
Configuring Layer 2 NetFlow Keys 291
Configuring NetFlow Timeouts 292
Verifying the NetFlow Configuration 292
Monitoring NetFlow 293
Configuration Example for NetFlow 293
CHAPTER 20

Configuring sFlow 295

About sFlow 295

sFlow Agent 295

Licensing Requirements for sFlow 296

Prerequisites for sFlow 296

Guidelines and Limitations for sFlow 296

Default Settings for sFlow 297

Configuring sFlow 297

Enabling sFlow 297

Configuring the Sampling Rate 298

Configuring the Maximum Sampled Size 299

Configuring the Counter Poll Interval 299

Configuring the Maximum Datagram Size 300

Configuring the sFlow Collector Address 301

Configuring the sFlow Collector Port 302

Configuring the sFlow Agent Address 303

Configuring the sFlow Sampling Data Source 303

Verifying the sFlow Configuration 304

Monitoring and Clearing sFlow Statistics 304

Configuration Examples for sFlow 305

Additional References 305

Related Documents 305

CHAPTER 21

Configuring TAP Aggregation and MPLS Stripping 307

About TAP Aggregation 307

Network TAPs 307

TAP Aggregation 308

Licensing Requirements for TAP Aggregation 308

Guidelines and Limitations for TAP Aggregation 308

About MPLS Stripping 310

Licensing Requirements for MPLS Stripping 310

Guidelines and Limitations for MPLS Stripping 310

Configuring TAP Aggregation 311
Preface

This preface includes the following sections:

• Audience, on page xxiii
• Document Conventions, on page xxiii
• Related Documentation for Cisco Nexus 9000 Series Switches, on page xxiv
• Documentation Feedback, on page xxiv
• Communications, Services, and Additional Information, on page xxiv

Audience

This publication is for network administrators who install, configure, and maintain Cisco Nexus switches.

Document Conventions

Command descriptions use the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bold</strong></td>
<td>Bold text indicates the commands and keywords that you enter literally as shown.</td>
</tr>
<tr>
<td><em>Italic</em></td>
<td>Italic text indicates arguments for which you supply the values.</td>
</tr>
<tr>
<td>[x]</td>
<td>Square brackets enclose an optional element (keyword or argument).</td>
</tr>
<tr>
<td>[x</td>
<td>y]</td>
</tr>
<tr>
<td>{x</td>
<td>y}</td>
</tr>
<tr>
<td>[x {y</td>
<td>z}]</td>
</tr>
<tr>
<td>Convention</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>variable</td>
<td>Indicates a variable for which you supply values, in context where italics cannot be used.</td>
</tr>
<tr>
<td>string</td>
<td>A nonquoted set of characters. Do not use quotation marks around the string or the string includes the quotation marks.</td>
</tr>
</tbody>
</table>

Examples use the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>screen font</td>
<td>Terminal sessions and information the switch displays are in screen font.</td>
</tr>
<tr>
<td>boldface screen font</td>
<td>Information that you must enter is in boldface screen font.</td>
</tr>
<tr>
<td>italic screen font</td>
<td>Arguments for which you supply values are in italic screen font.</td>
</tr>
<tr>
<td>&lt;&gt;</td>
<td>Nonprinting characters, such as passwords, are in angle brackets.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Default responses to system prompts are in square brackets.</td>
</tr>
<tr>
<td>!, #</td>
<td>An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.</td>
</tr>
</tbody>
</table>

**Related Documentation for Cisco Nexus 9000 Series Switches**

The entire Cisco Nexus 9000 Series switch documentation set is available at the following URL:


**Documentation Feedback**

To provide technical feedback on this document, or to report an error or omission, please send your comments to nexus9k-docfeedback@cisco.com. We appreciate your feedback.

**Communications, Services, and Additional Information**

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you’re looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.
Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.
CHAPTER 1

New and Changed Information

This chapter provides release-specific information for each new and changed feature in the Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 9.2(x).

- New and Changed Information, on page 1

New and Changed Information

This table summarizes the new and changed features for the Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 9.2(x) and tells you where they are documented.

Table 1: New and Changed Features for Cisco NX-OS Release 9.2(x)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Changed in Release</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>PTP</td>
<td>Added supported on the N9K-C9504-FM-R</td>
<td>9.2(3)</td>
<td>Guidelines and Limitations for PTP, on page 37</td>
</tr>
<tr>
<td>Configuration Replace</td>
<td>Updates the <code>configure replace</code> command from maintenance mode to include a user-confirmation and a warning.</td>
<td>9.2(2)</td>
<td>Guidelines and Limitations for Configuration Replace, on page 363</td>
</tr>
<tr>
<td>NetFlow</td>
<td>Added support for Layer 2 FEX.</td>
<td>9.2(1)</td>
<td>Guidelines and Limitations for NetFlow, on page 282</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Changed in Release</td>
<td>Where Documented</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>--------------------------------------------------</td>
<td>--------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>sFlow</td>
<td>sFlow export over VXLAN is supported.</td>
<td>9.2(1)</td>
<td>Guidelines and Limitations for sFlow, on page 296</td>
</tr>
<tr>
<td>PTP</td>
<td>Updated support for IEEE 802.1AS.</td>
<td>9.2(1)</td>
<td>Guidelines and Limitations for PTP, on page 37</td>
</tr>
<tr>
<td>IEEE 802.1Qaz standards for DCBXP TLV</td>
<td>Added Support for the Cisco Nexus 9000 Series switches.</td>
<td>9.2(1)</td>
<td>About DCBXP, on page 270</td>
</tr>
<tr>
<td>LLDP</td>
<td>Introduced the <code>show qos dcbxp interface</code> command.</td>
<td>9.2(1)</td>
<td>Verifying the LLDP Configuration, on page 276</td>
</tr>
<tr>
<td>System message logging</td>
<td>Added support to send syslog messages to remote logging servers over secure TLS transport connection.</td>
<td>9.2(1)</td>
<td>Configuring System Message Logging, on page 73</td>
</tr>
<tr>
<td>TAP aggregation filters based on MPLS tags.</td>
<td>Introduced in this release.</td>
<td>9.2(1)</td>
<td>Guidelines and Limitations for TAP Aggregation, on page 308</td>
</tr>
</tbody>
</table>
CHAPTER 2

Overview

This chapter describes the system management features that you can use to monitor and manage Cisco NX-OS devices.

- Software Image, on page 3
- Cisco NX-OS Device Configuration Methods, on page 3
- Network Time Protocol, on page 5
- Cisco Discovery Protocol, on page 5
- Session Manager, on page 5
- Scheduler, on page 5
- SNMP, on page 5
- Online Diagnostics, on page 5
- Onboard Failure Logging, on page 6
- SPAN, on page 6
- ERSPAN, on page 6
- LLDP, on page 6
- MPLS Stripping, on page 6
- sFlow, on page 6
- SMUs, on page 6
- Virtual Device Contexts, on page 7
- Troubleshooting Features, on page 7

Software Image

The Cisco NX-OS software consists of one NXOS software image. This image runs on all Cisco Nexus 3400 Series switches.

Cisco NX-OS Device Configuration Methods

You can configure devices using direct network configuration methods or web services hosted on a Cisco Data Center Network Management (DCNM) server.

This figure shows the device configuration methods available to a network user.
Figure 1: Cisco NX-OS Device Configuration Methods

This table lists the configuration method and the document where you can find more information.

<table>
<thead>
<tr>
<th>Configuration Method</th>
<th>Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLI from a Secure Shell (SSH) session, a Telnet session,</td>
<td>Cisco Nexus 3400 Series NX-OS Fundamentals Configuration Guide</td>
</tr>
<tr>
<td>or the console port</td>
<td></td>
</tr>
<tr>
<td>Cisco DCNM client</td>
<td>Cisco DCNM Fundamentals Guide</td>
</tr>
</tbody>
</table>

Configuring with CLI or XML Management Interface

You can configure Cisco NX-OS devices using the command-line interface (CLI) or the XML management interface over Secure Shell (SSH) as follows:

- CLI from an SSH session, a Telnet session, or the console port—You can configure devices using the CLI from an SSH session, a Telnet session, or the console port. SSH provides a secure connection to the device. For more information, see the Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide.

- XML management interface over SSH—You can configure devices using the XML management interface, which is a programmatic method based on the NETCONF protocol that complements the CLI functionality. For more information, see the Cisco NX-OS XML Management Interface User Guide.

Configuring with Cisco DCNM

You can configure Cisco NX-OS devices using the Cisco DCNM client, which runs on your local PC and uses web services on the Cisco DCNM server. The Cisco DCNM server configures the device over the XML
Network Time Protocol

The Network Time Protocol (NTP) synchronizes the time of day among a set of distributed time servers and clients so that you can correlate time-specific information, such as system logs, received from the devices in your network.

Cisco Discovery Protocol

You can use the Cisco Discovery Protocol (CDP) to discover and view information about all Cisco equipment that is directly attached to your device. CDP runs on all Cisco-manufactured equipment including routers, bridges, access and communication servers, and switches. CDP is media and protocol independent, and gathers the protocol addresses of neighboring devices, discovering the platform of those devices. CDP runs over the data link layer only. Two systems that support different Layer 3 protocols can learn about each other.

Session Manager

Session Manager allows you to create a configuration and apply it in batch mode after the configuration is reviewed and verified for accuracy and completeness.

Scheduler

The scheduler allows you to create and manage jobs such as routinely backing up data or making quality of service (QoS) policy changes. The scheduler can start a job according to your needs—only once at a specified time or at periodic intervals.

SNMP

The Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network.

Online Diagnostics

Cisco Generic Online Diagnostics (GOLD) define a common framework for diagnostic operations across Cisco platforms. The online diagnostic framework specifies the platform-independent fault-detection architecture for centralized and distributed systems, including the common diagnostics CLI and the platform-independent fault-detection procedures for boot-up and run-time diagnostics. The platform-specific diagnostics provide hardware-specific fault-detection tests and allow you to take appropriate corrective action in response to diagnostic test results.
Onboard Failure Logging

You can configure a device to log failure data to persistent storage, which you can retrieve and display for analysis at a later time. This on-board failure logging (OBFL) feature stores failure and environmental information in nonvolatile memory on the module. This information is useful for analysis of failed modules.

SPAN

You can configure an Ethernet Switched Port Analyzer (SPAN) to monitor traffic in and out of your device. The SPAN features allow you to duplicate packets from source ports to destination ports.

ERSPAN

Encapsulated Remote Switched Port Analyzer (ERSPAN) is used to transport mirrored traffic in an IP network. ERSpan supports source ports, source VLANs, and destinations on different switches, which provide remote monitoring of multiple switches across your network.

To configure an ERS PAN source session, you associate a set of source ports or VLANs with a destination IP address, ERS PAN ID number, and virtual routing and forwarding (VRF) name.

LLDP

Link Layer Discovery Protocol (LLDP) is a vendor-neutral, one-way device discovery protocol that allows network devices to advertise information about themselves to other devices on the network. This protocol runs over the data-link layer, which allows two systems running different network layer protocols to learn about each other. You can enable LLDP globally or per interface.

MPLS Stripping

MPLS stripping provides the ability to strip MPLS labels from packets, enabling non-MPLS-capable network monitoring tools to monitor packets.

sFlow

Sampled flow (sFlow) allows you to monitor real-time traffic in data networks that contain switches and routers and to forward the sample data to a central data collector.

SMUs

A software maintenance upgrade (SMU) is a package file that contains fixes for a specific defect. SMUs are created to respond to immediate issues and do not include new features. SMUs are not an alternative to
maintenance releases. They provide a quick resolution of immediate issues. All defects fixed by SMUs are
integrated into the maintenance releases.

Virtual Device Contexts

Cisco NX-OS can segment operating system and hardware resources into virtual device contexts (VDCs) that
emulate virtual devices. The Cisco Nexus 9000 Series switches currently do not support multiple VDCs. All
switch resources are managed in the default VDC.

Troubleshooting Features

Cisco NX-OS provides troubleshooting tools such as ping, traceroute, Ethanalyzer, and the Blue Beacon
feature.

When a service fails, the system generates information that can be used to determine the cause of the failure.
The following sources of information are available:

- Every service restart generates a syslog message of level LOG_ERR.
- If the Smart Call Home service is enabled, every service restart generates a Smart Call Home event.
- If SNMP traps are enabled, the SNMP agent sends a trap when a service is restarted.
- When a service failure occurs on a local module, you can view a log of the event by entering the `show
  processes log` command in that module. The process logs are persistent across supervisor switchovers
  and resets.
- When a service fails, a system core image file is generated. You can view recent core images by entering
  the `show cores` command on the active supervisor. Core files are not persistent across supervisor
  switchovers and resets, but you can configure the system to export core files to an external server using
  the file transfer utility Trivial File Transfer Protocol (TFTP) by entering the `system cores` command.
- CISCO-SYSTEM-MIB contains a table for cores (cseSwCoresTable).
CHAPTER 3

Configuring Switch Profiles

This chapter describes how to configure switch profiles on the Cisco Nexus 9000 Series switches.

• About Switch Profiles, on page 9
• Licensing Requirements for Switch Profiles, on page 11
• Guidelines and Limitations for Switch Profiles, on page 11
• Configuring Switch Profiles, on page 13
• Adding or Modifying Switch Profile Commands, on page 15
• Importing a Switch Profile, on page 16
• Importing Configurations in a vPC Topology, on page 18
• Isolating a Peer Switch, on page 18
• Deleting a Switch Profile, on page 19
• Manually Correcting Mutex and Merge Failures, on page 20
• Verifying the Switch Profile Configuration, on page 20
• Configuration Examples for Switch Profiles, on page 21

About Switch Profiles

Several applications require consistent configuration across devices in the network. For example, with a virtual port channel (vPC), you must have identical configurations. Mismatched configurations can cause errors or misconfigurations that can result in service disruptions. The configuration synchronization (config-sync) feature allows you to configure one switch profile and have the configuration be automatically synchronized to the peer switch.

A switch profile provides the following benefits:

• Allows configurations to be synchronized between switches.
• Merges configurations when connectivity is established between two switches.
• Provides control of exactly which configuration gets synchronized.
• Ensures configuration consistency across peers through merge and mutual-exclusion checks.
• Provides verify and commit semantics.
• Allows for migrating existing vPC configurations to a switch profile.
Switch Profile Configuration Modes

The switch profile feature includes the following configuration modes:

- Configuration synchronization mode (config-sync)
- Switch profile mode (config-sync-sp)
- Switch profile import mode (config-sync-sp-import)

Configuration Synchronization Mode

The configuration synchronization mode (config-sync) allows you to create switch profiles.

Switch Profile Mode

The switch profile mode (config-sync-sp) allows you to add supported configuration commands to a switch profile temporary buffer that is later synchronized with a peer switch. Commands that you enter in the switch profile mode are not executed until you enter the commit command. Although the syntax of the commands are validated when you enter them, there is no guarantee that the commands will be successful when you enter the commit command.

Switch Profile Import Mode

The switch profile import mode (config-sync-sp-import) allows you to import existing switch configurations from the running configuration to a switch profile and specify which commands you want to include in that profile. This option is especially useful when you upgrade from a Cisco NX-OS release that does not support switch profiles to a release that does.

Cisco recommends that you import the necessary configurations from the running configuration using the switch profile import mode and commit the changes before making any additional changes in the switch profile or global configuration mode. Otherwise, you might jeopardize the import, requiring you to abandon the current import session and perform the process again. For more information, see Importing a Switch Profile, on page 16.

Configuration Validation

Two types of configuration validation checks can identify switch profile failures:

- Mutual exclusion checks
- Merge checks

Mutual Exclusion Checks

The mutual exclusion of configuration commands is enforced in order to avoid duplicate commands in the config-sync and global configuration modes. When you commit the configuration of a switch profile, mutual exclusion (mutex) checks are performed on the local switch as well as the peer switch (if configured). If no failures are reported on both switches, the commit is accepted and pushed into the running configuration.

A command that is included in a switch profile cannot be configured outside of the switch profile.

If a mutex check identifies errors, they are reported as mutex failures, and they must be manually corrected. For details, see Manually Correcting Mutex and Merge Failures, on page 20.
The following exceptions apply to the mutual exclusion policy:

- Interface configuration—An interface configuration can be partially present in a switch profile and partially present in the running configuration as long as there are no conflicts.
- Shutdown/no shutdown
- System QoS

Merge Checks

Merge checks are done on the peer switch that is receiving a configuration. The merge checks ensure that the received configuration does not conflict with the switch profile configuration that already exists on the receiving switch. The merge check occurs during the verify or commit process. Errors are reported as merge failures and must be manually corrected. For details, see Manually Correcting Mutex and Merge Failures, on page 20.

When one or both switches are reloaded and the configurations are synchronized for the first time, the merge check verifies that the switch profile configurations are identical on both switches. Differences in the switch profiles are reported as merge errors and must be manually corrected.

Software Upgrades and Downgrades with Switch Profiles

You must delete the switch profile when downgrading from a Cisco NX-OS release that supports switch profiles to a release that does not.

When you upgrade from an earlier release to a Cisco NX-OS release that supports switch profiles, you have the option to move some of the running-configuration commands to a switch profile. For details, see Switch Profile Import Mode, on page 10.

An upgrade can occur if there are buffered (uncommitted) configurations; however, the uncommitted configurations will be lost.

Licensing Requirements for Switch Profiles

<table>
<thead>
<tr>
<th>Product</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco NX-OS</td>
<td>Switch profiles do not require a license. Any feature not included in a license package is bundled with the nx-os image and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the Cisco NX-OS Licensing Guide.</td>
</tr>
</tbody>
</table>

Guidelines and Limitations for Switch Profiles

Switch profiles have the following configuration guidelines and limitations:

- Beginning with Cisco NX-OS Release 9.3(3), the mtu command is supported in the interface configuration mode through the switch-profiles configuration mode.
• Switch profiles are supported only on Cisco Nexus 9300 Series switches. Cisco Nexus 9500 Series switches do not support switch profiles.

• You can only enable configuration synchronization using the mgmt0 interface.

• When using config-sync in a virtual peer-link environment, note the following limitations:
  • To initiate a config-sync session with a virtual peer link, be sure to configure a loopback IP address instead of a management IP address between the peer switches.
  • You cannot perform a configuration synchronization between a multichassis EtherChannel trunk (MCT) configuration and a virtual peer-link configuration. This config-sync operation is not supported.

• You must configure synchronized peers with the same switch profile name.

• Commands that are qualified for a switch profile configuration are allowed to be configured in the configuration switch profile mode (config-sync-sp).

• Supported switch profile commands relate to vPC commands.

• Only one switch profile session can be in progress at a time. Attempts to start another session will fail.

• Command changes made from the global configuration mode are blocked when a switch profile session is in progress.

• When you enter the `commit` command and a peer switch is reachable, the configuration is applied to both peer switches or neither switch. If a commit failure occurs, the commands remain in the switch profile buffer. You can then make necessary corrections and try the commit again.

• The configuration synchronization (config-sync) mode is an L2 mode parallel to the config-terminal mode (config t). Config-sync uses the switch-profile to update config t mode in the same switch as well as the peer switch. To prevent sync issues in switch-profile mode, Cisco recommends that you perform a commit action after each CLI command before overriding, or replacing the current CLI command.

For example, if you want to overwrite CLI_command_A and change it to CLI_command_B, commit CLI_command_A first, then configure CLI_command_B and perform another commit action.

```
switch# conf sync
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-sync)# switch-profile test
Resyncing db before starting Switch-profile. Re-synchronization of switch-profile db takes a few minutes...
Re-synchronize switch-profile db completed successfully.
Switch-Profile started, Profile ID is 1
switch(config-sync-sp-#)
switch(config-sync-sp)# int e 1/3
switch(config-sync-sp-if)# switchport trunk allowed vlan 100-150
switch(config-sync-sp-if)# commit
Verification successful...
Proceeding to apply configuration. This might take a while depending on amount of configuration in buffer.
Please avoid other configuration changes during this time.
Commit Successful.
switch(config-sync-#)
switch(config-sync)# switch-profile test
Resyncing db before starting Switch-profile. Re-synchronization of switch-profile db takes a few minutes...
Re-synchronize switch-profile db completed successfully.
Switch-Profile started, Profile ID is 1
switch(config-sync-sp)#
```

• Layer 3 commands are not supported.

### Configuring Switch Profiles

You can create and configure a switch profile on the local switch and then add a second switch that will be included in the synchronization.

You must create the switch profile with the same name on each switch, and the switches must configure each other as a peer. When connectivity is established between switches with the same active switch profile, the switch profiles are synchronized.

#### Procedure

**Step 1**
**configure terminal**

**Example:**

```plaintext
switch# configure terminal
switch(config)#
```

Enters global configuration mode.

**Step 2**
Required: `cfs ipv4 distribute`

**Example:**

```plaintext
switch(config)# cfs ipv4 distribute
```

Enables Cisco Fabric Services (CFS) distribution between the peer switches.

**Step 3**
Required: `config sync`

**Example:**

```plaintext
switch(config)# config sync
switch(config-sync)#
```

Enters the configuration synchronization mode.

**Step 4**
Required: `switch-profile name`

**Example:**

```plaintext
switch(config-sync)# switch-profile abc
switch(config-sync-sp)#
```

Configures the switch profile, names the switch profile, and enters the switch profile configuration mode.

**Step 5**
Required: `[no] sync-peers destination ip-address`
Example:
switch(config-sync-sp)# sync-peers destination 10.1.1.1

Adds a switch to the switch profile. The destination IP address is the IP address of the switch that you want to synchronize.

The no form of this command removes the specified switch from the switch profile.

Note You need to wait for peer switches to show the switch-profile status of "In sync" before any commit is done.

Step 6 Required: For Cisco Nexus 3164Q switches only, follow these steps:

a) interface type slot/port

Example:
switch(config-sync-sp)# interface ethernet 1/1
switch(config-sync-sp-if)#

Enters the switch profile interface configuration mode.

b) switchport

Example:
switch(config-sync-sp-if)# switchport

Changes a Layer 3 interface into a Layer 2 interface.

c) exit

Example:
switch(config-sync-sp-if)# exit
switch(config-sync-sp)#

Exits the switch profile interface configuration mode.

d) commit

Example:
switch(config-sync-sp)# commit

Commits the current configuration.

Note Verify that the switch-profile status shows as "In sync" before any commit is done.

Step 7 (Optional) end

Example:
switch(config-sync-sp)# end
switch#

Exits the switch profile configuration mode and returns to EXEC mode.

Step 8 (Optional) show switch-profile name status

Example:
switch# show switch-profile abc status

Displays the switch profile on the local switch and the peer switch information.

Step 9 (Optional) show switch-profile name peer ip-address
Example:
switch# show switch-profile abc peer 10.1.1.1
Displays the switch profile peer configuration.

Step 10  (Optional) copy running-config startup-config
Example:
switch# copy running-config startup-config
Copies the running configuration to the startup configuration.

Adding or Modifying Switch Profile Commands

After you configure a switch profile on the local and the peer switch, you must add and commit the supported commands to the switch profile.

Commands that are added or modified are buffered until you enter the commit command. Commands are executed in the same order in which they are buffered. If there is an order dependency for certain commands (for example, a QoS policy must be defined before being applied), you must maintain that order; otherwise, the commit might fail. You can use utility commands, such as the show switch-profile name buffer command, the buffer-delete command, and the buffer-move command, to change the buffer and correct the order of already entered commands.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Required: config sync</td>
</tr>
<tr>
<td>Example:</td>
<td>switch# config sync</td>
</tr>
<tr>
<td></td>
<td>switch(config-sync)#</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Required: switch-profile name</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config-sync)# switch-profile abc</td>
</tr>
<tr>
<td></td>
<td>switch(config-sync-sp)#</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Required: command</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config-sync-sp)# interface Port-channel100</td>
</tr>
<tr>
<td></td>
<td>switch(config-sync-sp-if)# speed 1000</td>
</tr>
<tr>
<td></td>
<td>switch(config-sync-sp-if)# interface Ethernet1/1</td>
</tr>
<tr>
<td></td>
<td>switch(config-sync-sp-if)# speed 1000</td>
</tr>
<tr>
<td></td>
<td>switch(config-sync-sp-if)# channel-group 100</td>
</tr>
<tr>
<td></td>
<td>switch(config-sync-sp-if)# exit</td>
</tr>
<tr>
<td></td>
<td>switch(config-sync-sp)#</td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td>4</td>
<td>(Optional) <code>show switch-profile name buffer</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td><code>switch(config-sync-sp)# show</code></td>
</tr>
<tr>
<td></td>
<td><code>switch-profile abc buffer</code></td>
</tr>
<tr>
<td>5</td>
<td>Required: <code>verify</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td><code>switch(config-sync-sp)# verify</code></td>
</tr>
<tr>
<td>6</td>
<td>Required: <code>commit</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td><code>switch(config-sync-sp)# commit</code></td>
</tr>
<tr>
<td></td>
<td>- Triggers the mutex check and the merge check to verify the synchronization.</td>
</tr>
<tr>
<td></td>
<td>- Creates a checkpoint with a rollback infrastructure.</td>
</tr>
<tr>
<td></td>
<td>- Executes a rollback on all switches if an application failure occurs on any of the switches in the switch profile.</td>
</tr>
<tr>
<td></td>
<td>- Deletes the checkpoint.</td>
</tr>
<tr>
<td>7</td>
<td>(Optional) <code>end</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td><code>switch(config-sync-sp)# end switch#</code></td>
</tr>
<tr>
<td>8</td>
<td>(Optional) <code>show switch-profile name status</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td><code>switch# show switch-profile abc status</code></td>
</tr>
<tr>
<td>9</td>
<td>(Optional) <code>copy running-config startup-config</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td><code>switch# copy running-config startup-config</code></td>
</tr>
</tbody>
</table>

### Importing a Switch Profile

You can import a switch profile based on the set of commands that you want to import.

**Before you begin**

Make sure that the switch profile buffer is empty before you import commands to a switch profile.
## Configuring Switch Profiles

### Importing a Switch Profile

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | (Optional) Configure the interface that will be imported in Step 4. **Example:**

```
switch(config)# interface ethernet 1/2
switch(config-if)# switchport
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk
allowed vlan 12
switch(config-if)# speed 10000
switch(config-if)# spanning-tree port
  type edge trunk
switch(config)# end
```

Enters configuration synchronization mode.

| **Step 2** | `config sync` **Example:**

```
switch# config sync
```

Enters configuration synchronization mode.

| **Step 3** | Required: `switch-profile name` **Example:**

```
switch(config-sync)# switch-profile abc
```

Configures the switch profile, names the switch profile, and enters the switch profile configuration mode.

| **Step 4** | Required: `import [interface interface port/slot | running-config]` **Example:**

```
switch(config-sync-sp)# import interface ethernet 1/2
```

Identifies the commands that you want to import and enters the switch profile import mode. The following options are available:

- Entering the `import` command without any options adds the selected commands to the switch profile.
- The `import interface` option adds the supported commands for a specified interface.
- The `running-config` option adds supported system-level commands.

**Note** If new commands are added during the import, the switch profile remains unsaved, and the switch remains in the switch profile import mode.

| **Step 5** | Required: `commit` **Example:**

```
switch(config-sync-sp-import)# commit
```

Imports the commands and saves the commands to the switch profile.
### Command or Action | Purpose
--- | ---
**Step 6** (Optional) **abort**  
*Example:*  
switch(config-sync-sp-import)# abort | aborts the import process.

**Step 7** (Optional) **end**  
*Example:*  
switch(config-sync-sp-import)# end  
switch# | Exits the switch profile import mode and returns to EXEC mode.

**Step 8** (Optional) **show switch-profile**  
*Example:*  
switch# show switch-profile | Displays the switch profile configuration.

**Step 9** (Optional) **copy running-config startup-config**  
*Example:*  
switch# copy running-config startup-config | Copies the running configuration to the startup configuration.

### Importing Configurations in a vPC Topology

You can import configurations in a two-switch vPC topology.

**Note**
For specific information on the following steps, see the appropriate sections in this chapter.

1. Configure the switch profile with the same name on both switches.
2. Import the configurations to both switches independently.

**Note**
Make sure that the configuration moved to the switch profile on both switches is identical; otherwise, a merge-check failure might occur.

3. Configure the switches by entering the `sync-peers destination` command.
4. Verify that the switch profiles are the same by entering the appropriate `show` commands.

### Isolating a Peer Switch

You can isolate a peer switch in order to make changes to a switch profile. This process can be used when you want to block configuration synchronization, debug configurations, or recover from a situation when the config-sync feature becomes out of sync.
Isolating a peer switch requires that you break the peer connection from the switch profile and then add the peer switch back to the switch profile.

### Note
For specific information on the following steps, see the appropriate sections in this chapter.

1. Remove the peer switch from the switch profile on both switches.
2. Add the `no sync-peers destination` command to the switch profile and commit the changes on both switches.
3. Add any necessary troubleshooting configurations.
4. Verify that the show running switch-profile is identical on both switches.
5. Add the `sync-peers destination ip-address` command to both switches and commit the changes.
6. Verify that the peers are in sync.

## Deleting a Switch Profile

You can delete a switch profile.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>config sync</td>
<td>Enters configuration synchronization mode.</td>
</tr>
</tbody>
</table>
| Example: | switch# config sync  
switch(config-sync)# |  |
| Step 2 | Required: `no switch-profile name {all-config  
local-config}` | Deletes the switch profile as follows: |
| Example: | switch(config-sync)# no switch-profile  
abc local-config  
switch(config-sync-sp)# |  |
| Step 3 | (Optional) `end` | Exits the switch profile configuration mode and returns to EXEC mode. |
| | Example: | |

### Note
It is recommended that you execute `resync-database` prior to deleting a switch-profile:

```
switch(config-sync)# resync-database
```
### Configuring Switch Profiles

#### Manually Correcting Mutex and Merge Failures

You can manually correct mutex and merge failures when they occur.

**Note**

If the conflict is on the peer switch, follow the steps in *Isolating a Peer Switch, on page 18* to correct the problem on that switch.

1. Import the offending command into the switch profile using the switch profile import mode.
2. Change the behavior as desired.

#### Verifying the Switch Profile Configuration

To display information about a switch profile, perform one of the following tasks:

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show switch-profile name</code></td>
<td>Displays the commands in a switch profile.</td>
</tr>
<tr>
<td><code>show switch-profile name buffer</code></td>
<td>Displays the uncommitted commands in a switch profile, the commands that were moved, and the commands that were deleted.</td>
</tr>
<tr>
<td><code>show switch-profile name peer ip-address</code></td>
<td>Displays the synchronization status for a peer switch.</td>
</tr>
<tr>
<td><code>show switch-profile name session-history</code></td>
<td>Displays the status of the last 20 switch profile sessions.</td>
</tr>
<tr>
<td><code>show switch-profile name status</code></td>
<td>Displays the configuration synchronization status of a peer switch.</td>
</tr>
<tr>
<td><code>show running-config switch-profile</code></td>
<td>Displays the running configuration for the switch profile on the local switch.</td>
</tr>
<tr>
<td><code>show startup-config switch-profile</code></td>
<td>Displays the startup configuration for the switch profile on the local switch.</td>
</tr>
</tbody>
</table>
Configuration Examples for Switch Profiles

Creating a Switch Profile on a Local and a Peer Switch

The following example shows how to create a successful switch profile configuration on a local and a peer switch, including configuring QoS policies, a vPC peer link, and a vPC in a switch profile.

1. Enable CFS distribution on the local and the peer switch and configure the destination IP address of the switch that you want to synchronize with, such as the management interface on the switch.

   ```
   --Local switch-1#---
   switch-1# configure terminal
   switch-1(config)# cfs ipv4 distribute
   switch-1(config)# interface mgmt 0
   switch-1(config-if)# ip address 30.0.0.81/8
   
   --Peer switch-2#--
   switch-2# configure terminal
   switch-2(config)# cfs ipv4 distribute
   switch-2(config)# interface mgmt 0
   switch-2(config-if)# ip address 30.0.0.82/8
   ```

2. Create a new switch profile on the local and the peer switch.

   ```
   --Local switch-1#---
   switch-1# config sync
   switch-1(config-sync)# switch-profile A
   Switch-Profile started, Profile ID is 1
   switch-1(config-sync-sp)# sync-peers destination 30.0.0.82
   switch-1(config-sync-sp)# end
   
   --Peer switch-2#--
   switch-1# config sync
   switch-1(config-sync)# switch-profile A
   Switch-Profile started, Profile ID is 1
   switch-1(config-sync-sp)# sync-peers destination 30.0.0.81
   switch-1(config-sync-sp)# end
   ```

3. Verify that the switch profiles are the same on the local and the peer switch.

   ```
   switch-1(config-sync-sp)# show switch-profile status
   switch-profile : A
   ------------------------------------------
   Start-time: 843992 usecs after Wed Aug 19 17:00:01 2015
   End-time: 770051 usecs after Wed Aug 19 17:00:03 2015
   Profile-Revision: 1
   Session-type: Initial-Exchange
   Session-subtype: Init-Exchange-All
   Peer-triggered: Yes
   Profile-status: Sync Success
   Local information:
   ----------------
   Status: Commit Success
   Error(s):
   ```
4. Add the configuration commands to the switch profile on the local switch. The commands will be applied to the peer switch when the commands are committed.

```
switch-1# config sync
switch-1(config-sync)# switch-profile A
Switch-Profile started, Profile ID is 1
switch-1(config-sync-sp)# interface port-channel 10
switch-1(config-sync-sp-if)# switchport
switch-1(config-sync-sp-if)# commit
Verification successful...
Proceeding to apply configuration. This might take a while depending on amount of configuration in buffer.
Please avoid other configuration changes during this time.
Commit Successful
```

```
switch-1(config-sync)# switch-profile A
Switch-Profile started, Profile ID is 1
switch-1(config-sync-sp)# interface port-channel 10
switch-1(config-sync-sp-if)# switchport mode trunk
switch-1(config-sync-sp-if)# switchport trunk allowed vlan 10
switch-1(config-sync-sp-if)# spanning-tree port type network
switch-1(config-sync-sp-if)# vpc peer-link
switch-1(config-sync-sp-if)# switch-profile switching-mode switchname
switch-1(config-sync-sp-if)# show switch-profile buffer
```

```
switch-profile : A
========================================================================
Seq-no Command
========================================================================
1 interface port-channel10
1.1 switchport mode trunk
1.2 switchport trunk allowed vlan 10
1.3 spanning-tree port type network
1.4 vpc peer-link
```

```
switch-1(config-sync-sp-if)# commit
Verification successful...
Proceeding to apply configuration. This might take a while depending on amount of configuration in buffer.
Please avoid other configuration changes during this time.
Commit Successful
```

```
switch-1(config-sync)# switch-profile A
Switch-Profile started, Profile ID is 1
switch-1(config-sync-sp)# interface ethernet 2/1
switch-1(config-sync-sp-if)# switchport mode trunk
switch-1(config-sync-sp-if)# switchport trunk allowed vlan 10
switch-1(config-sync-sp-if)# spanning-tree port type network
switch-1(config-sync-sp-if)# channel-group 10 mode active
```

5. View the buffered commands.

```
switch-1(config-sync-sp-if)# show switch-profile buffer
```

```
switch-profile : A
========================================================================
```
6. Verify the commands in the switch profile.

   switch-1(config-sync-sp-if)# verify
   Verification Successful

7. Apply the commands to the switch profile and synchronize the configurations between the local and the peer switch.

   -Local switch-2#--
   switch-1(config-sync-sp)# commit
   Verification successful...
   Proceeding to apply configuration. This might take a while depending on amount of configuration in buffer.
   Please avoid other configuration changes during this time.
   Commit Successful
   switch-1(config-sync)# end

   switch-1# show running-config switch-profile
   switch-profile A
   sync-peers destination 30.0.0.82
   interface port-channel10
   switchport mode trunk
   switchport trunk allowed vlan 10
   spanning-tree port type network
   vpc peer-link
   interface Ethernet2/1
   switchport mode trunk
   switchport trunk allowed vlan 10
   spanning-tree port type network
   channel-group 10 mode active

   -Peer switch-2#--
   switch-2# show running-config switch-profile
   switch-profile A
   sync-peers destination 30.0.0.81
   interface port-channel10
   switchport mode trunk
   switchport trunk allowed vlan 10
   spanning-tree port type network
   vpc peer-link
   interface Ethernet2/1
   switchport mode trunk
   switchport trunk allowed vlan 10
   spanning-tree port type network
   channel-group 10 mode active
Verifying the Synchronization Status

The following example shows how to verify the synchronization status between the local and the peer switch:

```
switch-1# show switch-profile status

switch-profile : A
-----------------switch-1---------------------------------------------

Start-time: 912776 usecs after Wed Aug 19 17:03:43 2015
End-time: 868379 usecs after Wed Aug 19 17:03:48 2015

Profile-Revision: 4
Session-type: Commit
Session-subtype: -
Peer-triggered: No
Profile-status: Sync Success

Local information:
-------------------
Status: Commit Success
Error(s):

Peer information:
-----------------
IP-address: 30.0.0.82
Sync-status: In sync
Status: Commit Success
Error(s):
```

Showing the Running Configuration

The following example shows the running configuration of the switch profile on the local switch:

```
——— PEER SWITCH-1 ———
switch-1# show running-config switch-profile

switch-profile A
sync-peers destination 30.0.0.82

interface port-channel10
switchport mode trunk
switchport trunk allowed vlan 10
spanning-tree port type network
vpc peer-link

interface Ethernet2/1
switchport mode trunk
switchport trunk allowed vlan 10
spanning-tree port type network
channel-group 10 mode active

switch-1#

——— PEER SWITCH-2 ———
switch-2# show running-config switch-profile

switch-profile A
sync-peers destination 30.0.0.81

interface port-channel10
switchport mode trunk
```
switchport trunk allowed vlan 10
spanning-tree port type network
vpc peer-link
interface Ethernet2/1
switchport mode trunk
switchport trunk allowed vlan 10
spanning-tree port type network
channel-group 10 mode active
switch-2#

Displaying the Switch Profile Synchronization Between the Local and the Peer Switch

The following example shows how to display the initial successful synchronization between the two peers:

switch1# show switch-profile sp status
Start-time: 491815 usecs after Mon Jul 20 11:54:51 2015
End-time: 449475 usecs after Mon Jul 20 11:54:58 2015
Profile-Revision: 1
Session-type: Initial-Exchange
Peer-triggered: No
Profile-status: Sync Success

Local information:
----------------
Status: Commit Success
Error(s):

Peer information:
---------------
IP-address: 10.193.194.52
Sync-status: In Sync.
Status: Commit Success
Error(s):

switch2# show switch-profile sp status
Start-time: 503194 usecs after Mon Jul 20 11:54:51 2015
End-time: 532989 usecs after Mon Jul 20 11:54:58 2015
Profile-Revision: 1
Session-type: Initial-Exchange
Peer-triggered: Yes
Profile-status: Sync Success

Local information:
----------------
Status: Commit Success
Error(s):

Peer information:
---------------
IP-address: 10.193.194.51
Sync-status: In Sync.
Status: Commit Success
Error(s):
Displaying Verify and Commit on the Local and the Peer Switch

The following example shows how to perform a successful verify and commit of the local and the peer switch:

```
switch1# config sync
switch1(config-sync)# switch-profile sp
Switch-Profile started, Profile ID is 1
switch1(config-sync-sp)# interface Ethernet1/1
switch1(config-sync-sp-if)# description foo
switch1(config-sync-sp-if)# exit
switch1(config-sync-sp)# verify
Verification Successful
switch1(config-sync-sp)# commit
Commit Successful
switch1(config-sync)# show running-config switch-profile
switch-profile sp
  sync-peers destination 10.193.194.52
  interface Ethernet1/1
description foo
switch1(config-sync)# show switch-profile sp status
End-time: 676451 usecs after Wed Jul 20 17:51:43 2015
Profile-Revision: 3
Session-type: Commit
Peer-triggered: No
Profile-status: Sync Success
Local information:
----------------
Status: Commit Success
Error(s):
Peer information:
--------------
IP-address: 10.193.194.52
Sync-status: In Sync.
Status: Commit Success
Error(s):

switch2# show running-config switch-profile
switch-profile sp
  sync-peers destination 10.193.194.51
  interface Ethernet1/1
description foo
switch2# show switch-profile sp status
End-time: 734702 usecs after Mon Jul 20 16:51:43 2015
Profile-Revision: 3
Session-type: Commit
Peer-triggered: Yes
Profile-status: Sync Success
Local information:
----------------
Status: Commit Success
Error(s):
```
Configuring Switch Profiles

Displaying the Successful and Unsuccessful Synchronization Between the Local and the Peer Switch

The following example shows how to configure the synchronization status of the switch profile on the peer switch. The first example shows a successful synchronization, and the second example shows a peer-not-reachable status.

switch1# show switch-profile sp peer

switch1# show switch-profile sp peer 10.193.194.52
Peer-sync-status : In Sync.
Peer-status : Commit Success
Peer-error(s) :

switch1# show switch-profile sp peer 10.193.194.52
Peer-sync-status : Not yet merged. pending-merge:1 received_merge:0
Peer-status : Peer not reachable
Peer-error(s) :

Displaying the Switch Profile Buffer

The following example shows how to configure the switch profile buffer, the buffer-move configuration, and the buffer-delete configuration:

switch1# config sync
switch1(config-sync)# switch-profile sp
Switch-Profile started, Profile ID is 1
switch1(config-sync-sp)# vlan 101
switch1(config-sync-sp-vlan)# ip igmp snooping querier 10.101.1.1
switch1(config-sync-sp-vlan)# exit
switch1(config-sync-sp)# mac address-table static 0000.0000.0001 vlan 101 drop
switch1(config-sync-sp)# interface Ethernet1/2
switch1(config-sync-sp-if)# switchport mode trunk
switch1(config-sync-sp-if)# switchport trunk allowed vlan 101
switch1(config-sync-sp-if)# exit
switch1(config-sync-sp)# show switch-profile sp buffer
------------------------------
Seq-no Command
------------------------------
1 vlan 101
1.1 ip igmp snooping querier 10.101.1.1
2 mac address-table static 0000.0000.0001 vlan 101 drop
3 interface Ethernet1/2
3.1 switchport mode trunk
3.2 switchport trunk allowed vlan 101

switch1(config-sync-sp)# buffer-move 3 1
Importing Configurations

The following example shows how to import an interface configuration:

```
switch# show running-config interface Ethernet1/3

!Command: show running-config interface Ethernet1/3

version 7.0(3)I2(1)

interface Ethernet1/3
    switchport mode trunk
    switchport trunk allowed vlan 1-100

switch# config sync
switch(config-sync)# switch-profile sp
Switch-Profile started, Profile ID is 1

switch(config-sync-sp)# import interface Ethernet1/3
switch(config-sync-sp-import)# show switch-profile sp buffer

Seq-no Command
--------------------------------------------------------------------------
1  interface Ethernet1/3
1.1  switchport mode trunk
1.2  switchport trunk allowed vlan 1-100

switch(config-sync-sp-import)# verify
Verification Successful
switch(config-sync-sp-import)# commit
Commit Successful
```

The following example shows how to import the supported commands in a running configuration:

```
switch(config-sync)# switch-profile sp
Switch-Profile started, Profile ID is 1
switch(config-sync-sp)# import running-config
```
switch(config-sync-sp-import)# show switch-profile sp buffer
----------------------------------------------------------
Seq-no Command
----------------------------------------------------------
1 logging event link-status default
2 vlan 1
3 interface port-channel 3
3.1 switchport mode trunk
3.2 vpc peer-link
3.3 spanning-tree port type network
4 interface port-channel 30
4.1 switchport mode trunk
4.2 vpc 30
4.3 switchport trunk allowed vlan 2-10
5 interface port-channel 31
5.1 switchport mode trunk
5.2 vpc 31
5.3 switchport trunk allowed vlan 11-20
6 interface port-channel 101
6.1 switchport mode fex-fabric
6.2 fex associate 101
7 interface port-channel 102
7.1 switchport mode fex-fabric
7.2 vpc 102
7.3 fex associate 102
8 interface port-channel 103
8.1 switchport mode fex-fabric
8.2 vpc 103
8.3 fex associate 103
9 interface Ethernet1/1
10 interface Ethernet1/2
11 interface Ethernet1/3
12 interface Ethernet1/4
12.1 switchport mode trunk
12.2 channel-group 3
13 interface Ethernet1/5
13.1 switchport mode trunk
13.2 channel-group 3
14 interface Ethernet1/6
14.1 switchport mode trunk
14.2 channel-group 3
15 interface Ethernet1/7
15.1 switchport mode trunk
15.2 channel-group 3
16 interface Ethernet1/8
17 interface Ethernet1/9
17.1 switchport mode trunk
17.2 switchport trunk allowed vlan 11-20
17.3 channel-group 31 mode active
18 interface Ethernet1/10
18.1 switchport mode trunk
18.2 switchport trunk allowed vlan 11-20
18.3 channel-group 31 mode active
19 interface Ethernet1/11
20 interface Ethernet1/12
...
45 interface Ethernet2/4
45.1 fex associate 101
45.2 switchport mode fex-fabric
45.3 channel-group 101
46 interface Ethernet2/5
46.1 fex associate 101
46.2 switchport mode fex-fabric
46.3 channel-group 101
Migrating to Cisco NX-OS Release 7.0(3)I2(1) or Higher in a Fabric Extender Straight-Through Topology

This example shows the tasks used to migrate to Cisco NX-OS Release 7.0(3)I2(1) or higher in a Fabric Extender active/active or straight-through topology. For details on the tasks, see the appropriate sections in this chapter.

1. Make sure configurations are the same on both switches.
2. Configure the switch profile with the same name on both switches.
3. Enter the `import interface port-channel x-y, port-channel z` command for all vPC port channels on both switches.
4. Enter the `show switch-profile name buffer` command to ensure all configurations are correctly imported on both switches.
5. Remove unwanted configuration settings by editing the buffer.
6. Enter the `commit` command on both switches.
7. Enter the `sync-peers destination ip-address` command to configure the peer switch on both switches.
8. Enter the `show switch-profile name status` command to ensure both switches are synchronized.

Replacing a Cisco Nexus 9000 Series Switch

When a Cisco Nexus 9000 Series switch has been replaced, perform the following configuration steps on the replacement switch to synchronize it with the existing Cisco Nexus 9000 Series switch. This procedure can be done in a hybrid Fabric Extender active/active topology and Fabric Extender straight-through topology.

1. Do not connect any peer link, vPC, active/active, or straight-through topology fabric ports to the replacement switch.
2. Boot the replacement switch. The switch comes up with no configuration.
3. Configure the replacement switch:
• If the running configuration was saved offline, follow Steps 4 through 8 to apply the configuration.

• If the running configuration was not saved offline, you can obtain it from the peer switch if the configuration synchronization feature is enabled. (See Steps 1 and 2 in Creating a Switch Profile on a Local and a Peer Switch, on page 21; then begin with Step 9 below).

• If neither condition is met, manually add the configuration and then begin with Step 9 below.

4. Edit the configuration file to remove the sync-peer command if you are using the configuration synchronization feature.

5. Configure the mgmt port IP address and download the configuration file.

6. Copy the saved configuration file to the running configuration.

7. Verify that the configuration is correct by entering the show running-config command.

8. If the switch profile configuration changes were made on the peer switch while the replacement switch was out of service, apply those configurations in the switch profile and then enter the commit command.

9. Shut down all Fabric Extender straight-through topology ports that are included in a vPC topology.


11. Wait for the Fabric Extender straight-through topology switches to come online.

12. Make sure that the vPC role priority of the existing switch is better than the replacement switch.

13. Connect the peer-link ports to the peer switch.

14. Connect the switch vPC ports.

15. Enter the no shutdown command on all Fabric Extender straight-through vPC ports.

16. Verify that all vPC switches and the Fabric Extenders on the replacement switch come online and that there is no disruption in traffic.

17. If you are using the configuration synchronization feature, add the sync-peer configuration to the switch profile if it was not enabled in Step 3.

18. If you are using the configuration synchronization feature, enter the show switch-profile name status command to ensure both switches are synchronized.

### Synchronizing Configurations

#### Synchronizing Configurations After a Cisco Nexus 9000 Series Switch Reboots

If a Cisco Nexus 9000 Series switch reboots while a new configuration is committed on a peer switch using a switch profile, follow these steps to synchronize the peer switches after the reload:

1. Remove the peer switch from the switch profile on both switches.

2. Add the no sync-peers destination command to the switch profile and commit the changes on both switches.

3. Add any missing or changed commands.
4. Verify that the show running switch-profile is identical on both switches.
5. Add the `sync-peers destination ip-address` command to both switches and commit the changes.
6. Verify that the peers are in sync.

**Synchronizing Configurations When the mgmt0 Interface Connectivity Is Lost**

When the mgmt0 interface connectivity is lost and configuration changes are required, apply the configuration changes on both switches using the switch profile. When connectivity to the mgmt0 interface is restored, both switches are synchronized.

If a configuration change is made on only one switch in this scenario, a merge will succeed when the mgmt0 interface comes up and the configuration gets applied on the other switch.

**Reverting an Inadvertent Port Mode Change of Layer 2 to Layer 3 in Global Configuration Mode**

The configurations related to a port imported in config-sync mode should never be configured in the global configuration mode. Normally any attempt to do so will be denied by the config-sync feature, and a mutex warning will appear. However, due to limitations in mutex checks, if a port configured as Layer 2 in the config-sync mode is changed to Layer 3 (no switchport) in the global configuration mode, the config-sync feature is unable to detect and prevent it. As a result, the config-sync mode might become out of sync with the global configuration mode. In this case, follow these steps to revert the change:

1. Remove the peer switch from the switch profile on both switches.
2. Add the `no sync-peers destination` command to the switch profile and commit the changes on both switches.
3. Import the current interface configuration.
4. Make any necessary changes and commit them.
5. Verify that the show running switch-profile is identical on both switches.
6. Add the `sync-peers destination ip-address` command to both switches and commit the changes.
7. Verify that the peers are in sync.
CHAPTER 4

Configuring PTP

This chapter describes how to configure the Precision Time Protocol (PTP) on Cisco NX-OS devices.

This chapter includes the following sections:

• About PTP, on page 33
• Licensing Requirements for PTP, on page 37
• Guidelines and Limitations for PTP, on page 37
• Default Settings for PTP, on page 39
• Configuring PTP, on page 39
• Timestamp Tagging, on page 46
• Configuring Timestamp Tagging, on page 46
• Configuring the TTAG Marker Packets and Time Interval, on page 47
• Configuring a PTP Interface to Stay in a Master State, on page 48
• Verifying the PTP Configuration, on page 49
• Configuration Examples for PTP, on page 50
• Additional References, on page 52

About PTP

PTP is a time synchronization protocol defined in IEEE 1588 for nodes distributed across a network. With PTP, it is possible to synchronize distributed clocks with an accuracy of less than 1 microsecond via Ethernet networks. In addition, PTP's hardware timestamping feature provides timestamp information in the ERSPAN Type III header that can be used to calculate packet latency among edge, aggregate, and core switches.

A PTP system can consist of a combination of PTP and non-PTP devices. PTP devices include ordinary clocks, boundary clocks, and transparent clocks. Non-PTP devices include ordinary network switches, routers, and other infrastructure devices.

PTP is a distributed protocol that specifies how real-time PTP clocks in the system synchronize with each other. These clocks are organized into a master-slave synchronization hierarchy with the grandmaster clock, which is the clock at the top of the hierarchy, determining the reference time for the entire system. Synchronization is achieved by exchanging PTP timing messages, with the members using the timing information to adjust their clocks to the time of their master in the hierarchy. PTP operates within a logical scope called a PTP domain.

PTP supports the following functionality:
• Multicast and unicast PTP transport—In the multicast transport mode, PTP uses multicast destination IP address 224.0.1.129 as per IEEE 1588 standards for communication between devices. For the source IP address, it uses the user configurable global IP address under the PTP domain. In the unicast transport mode, PTP uses configurable unicast source and destination IP addresses that can be configured under an interface. In both, the unicast and the multicast modes, PTP uses UDP ports, 319 for event messages and 320 for general messages communication between devices.

• PTP multicast configuration is supported only under physical interface for L2 or L3. Unicast PTP configuration supported only under L3 physical interface. PTP is not supported for virtual interfaces such as Port-channel, SVI, and tunnel.

• PTP encapsulation over UDP over IP—PTP uses UDP as the transport protocol over IP. In both, the unicast and multicast modes, PTP uses UDP ports 319 for event messages and 320 for general messages communication between devices. L2 encapsulation mode is not supported.

• PTP profiles—PTP supports default (1588), AES67, and SMPTE 2059-2 profiles. They all have different ranges of sync and delay request intervals. For information on the default profile, refer to IEEE 1588. For more information on AES67 and SMPTE 2059-2, refer to the respective specifications.

• Path delay measurement—We support delay request and response mechanism to measure the delay between the master and slave devices. Peer delay request and response mechanism is not supported.

• Message intervals—You can configure the interval at which the announce, sync, and delay request messages needs to be sent between devices.

• Best master clock (BMC) selection—BMC algorithm is used to select master, slave, and passive states of the PTP enabled interfaces based on the Announce message received as per 1588 specification.

PTP Device Types

The PTP device type is configurable and can be used to set the clock type.

Clocks

The following clocks are common PTP devices:

Ordinary clock

Communicates with the network based on a single physical port, similar to an end host. An ordinary clock can function as a grandmaster clock.

Boundary clock

Typically has several physical ports, with each port behaving like a port of an ordinary clock. However, each port shares the local clock, and the clock data sets are common to all ports. Each port decides its individual state, either master (synchronizing other ports connected to it) or slave (synchronizing to a downstream port), based on the best clock available to it through all of the other ports on the boundary clock. Messages related to synchronization and establishing the master-slave hierarchy terminate in the protocol engine of a boundary clock and are not forwarded.

Transparent clock

Forwards all PTP messages like an ordinary switch or router but measures the residence time of a packet in the switch (the time that the packet takes to traverse the transparent clock) and in some cases the link delay of the ingress port for the packet. The ports have no state because the transparent clock does not need to synchronize to the grandmaster clock.
There are two kinds of transparent clocks:

**End-to-end transparent clock**

Measures the residence time of a PTP message and accumulates the times in the correction field of the PTP message or an associated follow-up message.

**Peer-to-peer transparent clock**

Measures the residence time of a PTP message and computes the link delay between each port and a similarly equipped port on another node that shares the link. For a packet, this incoming link delay is added to the residence time in the correction field of the PTP message or an associated follow-up message.

---

**Note**

PTP operates only in boundary clock mode. Cisco recommends deployment of a Grand Master Clock (10 MHz) upstream, with servers containing clocks requiring synchronization connected to the switch.

End-to-end transparent clock and peer-to-peer transparent clock modes are not supported.

---

**Clock Modes**

The IEEE 1588 standard specifies two clock modes for the PTP supporting devices to operate in: one-step and two-step.

**One-Step Mode:**

In one-step mode the clock synchronization messages include the time at which the master port sends the message. The ASIC adds the timestamp to the synchronization message as it leaves the port. The master port operating in one-step mode for N9K-C9508-FM-R and N9K-C9504-FM-R fabric modules and N9K-X9636C-R, N9K-X9636Q-R, and N9K-X9636C-RX line cards.

The slave port uses the timestamp that comes as part of the synchronization messages.

**Two-Step Mode:**

In two-step mode the time at which the synchronization message leaves the port is sent in a subsequent follow-up message. This is the default mode.

---

**PTP Process**

The PTP process consists of two phases: establishing the master-slave hierarchy and synchronizing the clocks.

Within a PTP domain, each port of an ordinary or boundary clock follows this process to determine its state:

- Examines the contents of all received announce messages (issued by ports in the master state)
- Compares the data sets of the foreign master (in the announce message) and the local clock for priority, clock class, accuracy, and so on
- Determines its own state as either master or slave

The ordinary and boundary clocks use **Sync, Delay_Req, Follow_Up, Delay_Resp** event messages to generate and communicate timing information.

These messages are sent in the following sequence:
1. The master sends a Sync message to the slave and notes the time, $t_1$ at which it was sent. For one-step Sync message carries the time when the message leaves the master and for two-step this time is sent in the subsequent Follow-Up event message.

2. The slave receives the Sync message and notes the time of reception, $t_2$.

3. The master conveys to the slave the timestamp, $t_1$ by embedding the timestamp in a Follow_Up event message.

4. The slave sends a Delay_Req message to the master and notes the time, $t_3$ at which it was sent.

5. The master receives the Delay_Req message and notes the time of reception, $t_4$.

6. The master conveys to the slave the timestamp, $t_4$ by embedding it in a Delay_Resp message.

7. After this sequence, the slave possesses all four timestamps. These timestamps can be used to compute the offset of the slave clock relative to the master, and the mean propagation time of messages between the two clocks.

The following figure describes the event messages in the PTP process that generate and communicate timing information.

*Figure 2: PTP Process*

---

**High Availability for PTP**

Stateful restarts are not supported for PTP. After a reboot or a supervisor switchover, the running configuration is applied. For more information on high availability, see the Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide.
Licensing Requirements for PTP

<table>
<thead>
<tr>
<th>Product</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco NX-OS</td>
<td>PTP requires no license. Any feature not included in a license package is bundled with the nx-os image and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the Cisco NX-OS Licensing Guide.</td>
</tr>
</tbody>
</table>

Guidelines and Limitations for PTP

The following are the guidelines and limitations for Cisco Nexus 9000 series switches for PTP:

- For optimal PTP performance, it is recommended to use the latest SUP and LC FPGA versions for the release.
- PTP domain is limited to a single domain per network.
- PTP transport over User Datagram Protocol (UDP) is supported. Transport over Ethernet is not supported.
- PTP supports multicast communication. PTP also supports unicast communication and the unicast mode is optional.
- PTP supports boundary clock mode. End-to-end transparent clock and peer-to-peer transparent clock modes are not supported.
- It is recommended that the PTP device can either have multicast or unicast PTP mode configured, but not both multicast and unicast mode together.
- PTP can be enabled on port-channel member ports.
- All management messages received on a Slave port is forwarded on all PTP enabled ports. Handling management messages is not supported.
- To match PTP control packets using RACL, enable PIM on the L3 interface.
- When PTP is configured on a Cisco Nexus 9000 series switches, set the clock protocol to use PTP through the clock protocol ptp vdc 1 command. NTP cannot coexist with PTP on a Cisco Nexus 9000 series switch.
- PTP is supported for all Cisco Nexus 9000 Series and 3164Q hardware except for the 100G 9408PC line card and the 100G M4PC generic expansion module (GEM).
- Beginning with Cisco NX-OS Release 9.2(3), PTP is supported on the N9K-C9504-FM-R.
- For Cisco Nexus 31108PC-V and 31108TC-V switches, PTP is not supported on ports running at 100G speed.
- For Cisco Nexus 9300 and 9500 Series switches, PTP clock correction is expected to be in the 3-digit range, from 100 to 999 nanoseconds. For Cisco Nexus 9200 and 9300-EX Series switches, PTP clock correction is expected to be in the 1-digit to 2-digit range, from 1 to 99 nanoseconds.
Cisco Nexus 9000 series switches support mixed non-negotiated mode of operation on master PTP ports. That means when a slave client sends unicast delay request PTP packet, the Cisco Nexus 9000 responds with an unicast delay response packet. And, if the slave client sends multicast delay request PTP packet, the Cisco Nexus 9000 responds with a multicast delay response packet. For mixed non-negotiated mode to work, the source IP address used in the ptp source IP address configuration on the BC device must also be configured on any physical or logical interface of the BC device. The recommended best practice is to use the loopback interface of the device.

Cisco Nexus 9000 series switches support mixed non-negotiated mode of operation on master PTP ports. Meaning that when a slave client sends unicast delay request PTP packet, the Cisco Nexus 9000 responds with an unicast delay response packet. And, if the slave client sends multicast delay request PTP packet, the Cisco Nexus 9000 responds with a multicast delay response packet.


PTP offload is not supported on the Cisco Nexus 9508 switch with an -R series line card.

PTP is not supported on the Cisco Nexus 9504 switch with an -R series line card.

PTP offload is not supported on the Cisco N3K-C36180YC-R and N3K-C3636C-R line cards.

Beginning with Cisco NX-OS Release 9.2(1), Cisco N9K-X9636C-RX, N9K-X9636C-R, and N9K-X9636Q-R line cards support IEEE 802.1AS. IEEE 802.1AS is not supported on the Cisco N9K-X96136YC-R line card or the Cisco Nexus 9504.

PTP is not supported on the Cisco N9K-X96136YC-R line card.

Cisco Nexus 93108TC-EX and 93180YC-EX switches support PTP mixed mode and unicast mode. The Cisco Nexus 9396 switch supports PTP mixed mode.

PTP is supported with sync interval -3 only on Cisco Nexus 9508-R family line cards. Higher sync intervals are not supported.

PTP unicast is supported only on the default vrf.


PTP unicast mode on the Layer2 SVI interfaces is not supported on Cisco Nexus 9508 switches with N9K-X9636C-R, N9K-X9636C-RX, and N9K-X9636Q-R line cards.

PTP configuration with UC and MC on either side is not supported on Cisco Nexus 9508 switches with N9K-X9636C-R and N9K-X9636Q-R line cards.

PTP is not supported on FEX interfaces.

PTP-capable ports do not identify PTP packets and do not time-stamp or redirect those packets unless you enable PTP on those ports.

Cisco Nexus 9500 platform switches with N9K-X9700-EX line cards support timestamp tagging.

Mix of PTP profiles between the default 1588 and SMPTE-2059-2/aes67 is supported, but mix of PTP profiles between SMPTE-20159-2 and AES67 is not supported.
Default Settings for PTP

The following table lists the default settings for PTP parameters.

**Table 3: Default PTP Parameters**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>PTP</td>
<td>Disabled</td>
</tr>
<tr>
<td>PTP version</td>
<td>2</td>
</tr>
<tr>
<td>PTP domain</td>
<td>0</td>
</tr>
<tr>
<td>PTP priority 1 value when advertising the clock</td>
<td>255</td>
</tr>
<tr>
<td>PTP priority 2 value when advertising the clock</td>
<td>255</td>
</tr>
<tr>
<td>PTP announce interval</td>
<td>1 log second</td>
</tr>
<tr>
<td>PTP announce timeout</td>
<td>3 announce intervals</td>
</tr>
<tr>
<td>PTP delay-request interval</td>
<td>• 0 log seconds</td>
</tr>
<tr>
<td></td>
<td>• -1 log seconds for Cisco Nexus 3232C, 3264Q, and 9500 platform switches</td>
</tr>
<tr>
<td>PTP sync interval</td>
<td>• -2 log seconds</td>
</tr>
<tr>
<td></td>
<td>• -3 log seconds for Cisco Nexus 3232C, 3264Q, and 9500 platform switches</td>
</tr>
<tr>
<td>PTP VLAN</td>
<td>gPTP supports only default vlan 1, and no other user configured VLANs.</td>
</tr>
</tbody>
</table>

Configuring PTP

Configuring PTP Globally

You can enable or disable PTP globally on a device. You can also configure various PTP clock parameters to help determine which clock in the network has the highest priority to be selected as the grandmaster.

**Note**

You must always set the clock protocol ptp vdc1 for the local clock to be updated by the PTP protocol, irrespective of the one-step or the two-step mode. You can verify the configuration using the **show running-config clock_manager** command.
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>switch# configure terminal                                                                                                                                  switch(config)#</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>[no] feature ptp</code></td>
<td>Enables or disables PTP on the device.  <strong>Note</strong> Enabling PTP on the switch does not enable PTP on each interface.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>switch(config)# feature ptp</td>
</tr>
<tr>
<td>Step 3</td>
<td>`[no] ptp device-type [generalized-ptp</td>
<td>boundary-clock]`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>switch(config)# ptp device-type generalized-ptp</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>[no] ptp source ip-address</code></td>
<td>Configures the source IPv4 address for all the PTP packets in the multicast PTP mode.                                                                           switch(config)# ptp source 10.10.10.1</td>
</tr>
<tr>
<td>Step 5</td>
<td><em>(Optional) [no] ptp domain number</em></td>
<td>Configures the domain number to use for this clock. PTP domains allow you to use multiple independent PTP clocking subdomains on a single network.                                                 switch(config)# ptp domain 1</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td><em>(Optional) [no] ptp priority1 value</em></td>
<td>Configures the priority1 value to use when advertising this clock. This value overrides the default criteria (clock quality, clock class, etc.) for best master clock selection. Lower values take precedence.                                switch(config)# ptp priority1 1</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td><em>(Optional) [no] ptp priority2 value</em></td>
<td>Configures the priority2 value to use when advertising this clock. This value is used to decide between two devices that are otherwise equally matched in the default criteria. For example, you can use the priority2 value to give a specific switch priority over other identical switches. The range for the <code>value</code> is from 0 to 255. switch(config)# ptp priority2 1</td>
</tr>
<tr>
<td>Step 8</td>
<td><em>(Optional) copy running-config startup-config</em></td>
<td>Copies the running configuration to the startup configuration.                                                                                                                                  switch(config)# copy running-config startup-config</td>
</tr>
</tbody>
</table>
Configuring PTP on an Interface

After you globally enable PTP, it is not enabled on all supported interfaces by default. You must enable PTP interfaces individually.

Before you begin

Make sure that you have globally enabled PTP on the switch and configured the source IP address for PTP communication.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2**        | Specifies the interface on which you are enabling PTP and enters the interface configuration mode. |
| interface ethernet slot/port | |
| **Example:**      |         |
| switch(config)# interface ethernet 2/1 |         |
| switch(config-if)# |         |

| **Step 3**        | Enables or disables PTP on an interface in a multicast mode. |
| [no] ptp          |         |
| **Example:**      |         |
| switch(config-if)# ptp |         |

| **Step 4**        | Enables PTP on the interface in an unicast mode (PTP master use). |
| Required: interface ethernet slot/port {ptp transport ipv4 ucast masterslave ipv4[/slave-ipv4] ptp ucast-source [interface-ip]} | |
| **Example:**      |         |
| switch(config)# interface ethernet 2/1 |         |

| **Step 5**        | Enables PTP on the interface in an unicast mode (PTP slave use). |
| Required: interface ethernet slot/port {ptp transport ipv4 ucast slavemaster ipv4[/master-ipv4] ptp ucast-source [interface-ip]} | |
| **Example:**      |         |
| switch(config)# interface ethernet 2/1 |         |

| **Step 6**        | Configures the interval between PTP announce messages on an interface or the number of PTP intervals before a timeout occurs on an interface. |
| (Optional) [no] ptp announce {interval log-seconds | timeout count} | |
| **Example:**      |         |
| switch(config-if)# ptp announce interval 3 |         |

The range for the PTP announcement interval is from 0 to 4 log seconds, and the range for the interval timeout is from 2 to 4 intervals.
### Configuring PTP on an Interface

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 7</strong></td>
<td>(Optional) <code>[no]</code> <strong>ptp announce interval</strong> `[aes67</td>
<td>smpte-2059] log-seconds`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>switch(config-if)# ptp announce interval aes67 3</code></td>
<td></td>
</tr>
</tbody>
</table>

**Table 4: PTP Announcement Interval Range and Default Values**

<table>
<thead>
<tr>
<th>Option</th>
<th>Range</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>aes67-2015</td>
<td>0 to 4 log seconds</td>
<td>1 log second</td>
</tr>
<tr>
<td>smpte-2059-2</td>
<td>–3 to 1 log seconds</td>
<td>1 log second</td>
</tr>
<tr>
<td>Without the aes67 or smpte-2059 option</td>
<td>0 to 4 log seconds</td>
<td>1 log second</td>
</tr>
</tbody>
</table>

| **Step 8** | (Optional) `[no]` **ptp delay-request minimum interval** `log-seconds` | Configures the minimum interval allowed between PTP delay messages when the port is in the master state. |
| **Example:** | `switch(config-if)# ptp delay-request minimum interval -1` | The range is from \(\log(-1)\) to \(\log(6)\) seconds, where \(\log(-1) = 2\) frames every second. |

**Table 5: PTP Delay-Request Minimum Interval Range and Default Values**

<table>
<thead>
<tr>
<th>Option</th>
<th>Range</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>aes67-2015</td>
<td>–4 to 5 log seconds</td>
<td>0 log seconds</td>
</tr>
<tr>
<td>smpte-2059-2</td>
<td>–4 to 5 log seconds</td>
<td>0 log seconds</td>
</tr>
<tr>
<td>Without the aes67-2015 or smpte-2059-2 option</td>
<td>–1 to 6 log seconds (where (\log(-1) = 2) frames every second)</td>
<td>0 log seconds</td>
</tr>
</tbody>
</table>

| **Step 9** | (Optional) `[no]` **ptp delay-request minimum interval** `[aes67-2015 | smpte-2059-2] log-seconds` | Configures the minimum interval allowed between PTP delay messages when the port is in the master state. |
| **Example:** | `switch(config-if)# ptp delay-request minimum interval aes67-2015-1` | |

| **Step 10** | (Optional) `[no]` **ptp sync interval** `log-seconds` | Configures the interval between PTP synchronization messages on an interface. |
| **Example:** | `switch(config-if)# ptp sync interval 1` | The range is from \(\log(-3)\) to \(\log(1)\) seconds. For the media-related profile information, see |
### Command or Action

|---------|--------------------------------------------------------------------------------|

**Example:**

```bash
switch(config-if)# ptp sync interval aes67 1
```

### Purpose

- **the Cisco NX-OS IP Fabric for Medial Solution Guide** when configuring PTP for media.
- Configures the interval between PTP synchronization messages on an interface.

### Table 6: PTP Synchronization Interval Range and Default Values

<table>
<thead>
<tr>
<th>Option</th>
<th>Range</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>aes67-2015</td>
<td>–4 to 1 log seconds</td>
<td>–2 log seconds</td>
</tr>
<tr>
<td>smpte-2059-2</td>
<td>–4 to –1 log seconds</td>
<td>–2 log seconds</td>
</tr>
<tr>
<td>Without the aes67-2015 or smpte-2059-2 option</td>
<td>–3 to 1 log seconds</td>
<td>–2 log seconds</td>
</tr>
</tbody>
</table>

### Step 12

<table>
<thead>
<tr>
<th>(Optional) [no] ptp vlan vlan-id</th>
</tr>
</thead>
</table>

**Example:**

```bash
switch(config-if)# ptp vlan 1
```

### Purpose

- Specifies the VLAN for the interface where PTP is being enabled. You can only enable PTP on one VLAN on an interface.
- The range is from 1 to 4094.

### Step 13

<table>
<thead>
<tr>
<th>(Optional) show ptp brief</th>
</tr>
</thead>
</table>

**Example:**

```bash
switch(config-if)# show ptp brief
```

### Purpose

- Displays the PTP status.

### Step 14

<table>
<thead>
<tr>
<th>(Optional) show ptp port interface interface slot/port</th>
</tr>
</thead>
</table>

**Example:**

```bash
switch(config-if)# show ptp port interface ethernet 2/1
```

### Purpose

- Displays the status of the PTP port.

### Step 15

<table>
<thead>
<tr>
<th>(Optional) copy running-config startup-config</th>
</tr>
</thead>
</table>

**Example:**

```bash
switch(config-if)# copy running-config startup-config
```

### Purpose

- Copies the running configuration to the startup configuration.
Configuring PTP in Unicast Mode

Configuring Unicast Mode

Traditional PTP messages are delivered to the nodes that are capable of receiving PTP multicast messages. (For example, announce, sync, delay_req, delay_resp and follow_up). In Unicast mode, all PTP messages are delivered only to a particular PTP node. Multicast address is not used. In unicast mode, you can configure master/slave role and assign corresponding peer slave/master IP addresses.

Up to 8 master IPs can be configured for a slave unicast port and 64 slave IPs can be configured for a master port with a maximum 256 slave IP total for all ports. The following commands are used to configure the unicast slave IPs and unicast master IPs. Unicast packets are only sent to and received from these IPs. Packets received from other IPs are ignored.

```
switch(config-if)# ptp transport ipv4 ucast master
switch(config-if-ptp-master)# slave ipv4 10.10.10.2
```

```
switch(config-if)# ptp transport ipv4 ucast slave
switch(config-if-ptp-slave)# master ipv4 10.10.10.1
```

Assigning Master Role

Complete the following steps to assign a master role:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch# configure terminal switch(config)#</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>interface ethernet slot/port</td>
<td>Specifies the interface on which you are enabling PTP and enters the interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# interface ethernet 2/1 switch(config-if)#</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>[no] ptp transport ipv4 ucast master</td>
<td>Enables PTP master on a particular port (Layer 3 interface). In the master sub-mode, you can enter the slave IPv4 addresses.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config-if)# ptp transport ipv4 ucast master switch(config-if-ptp-master)#</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>slave ipv4 <code>&lt;IP_address&gt;</code></td>
<td>Enters the slave IPv4 addresses. Maximum of 64 IP addresses are allowed per master, but this number varies and it depends on the sync interval configuration. The master sends announce, sync, follow-up, and delayResp only to these slave addresses. You have to make sure that the slave IP is reachable.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch-1(config)# interface ethernet 1/1 switch-1(config-if)# ptp transport ipv4 ucast master switch-1(config-if-ptp-master)# slave ipv4 1.2.3.1 switch-1(config-if-ptp-master)# slave ipv4 1.2.3.2</td>
<td></td>
</tr>
</tbody>
</table>
### Assigning Slave Role

Complete the following steps to assign a slave role:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>switch# configure terminal</code> <code>switch(config)#</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>interface ethernet slot/port</code></td>
<td>Specifies the interface on which you are enabling PTP and enters the interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>switch(config)# interface ethernet 2/1</code> <code>switch(config-if)#</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>[no] ptp transport ipv4 ucast slave</code></td>
<td>Enables PTP slave on a particular port (Layer 3 interface). In the slave sub-mode, you can enter the master IPv4 addresses.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>switch(config-if)# ptp transport ipv4 ucast slave</code> <code>switch(config-if-ptp-slave)#</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>master ipv4 &lt;IP_address&gt;</code></td>
<td>Enters the master IPv4 addresses. Maximum of 64 IP addresses are allowed per master, but this number varies and it depends on the sync interval configuration. The master sends announce, sync, follow-up, and delay_respond only to these slave addresses. You have to make sure that the slave IP is reachable. Maximum of 8 IP addresses are allowed per slave. The announce, sync, and follow-up messages are received only from the configured master and all other are rejected. This slave sends a delay request to the best master among the configured masters. You have to make sure that the master IP is reachable.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>switch-1(config)# interface ethernet 1/1</code> <code>switch-1(config-if)# ptp transport ipv4 ucast slave</code> <code>switch-1(config-if-ptp-slave)# master ipv4 4.4.4.1</code> <code>switch-1(config-if-ptp-slave)# master ipv4 4.4.4.2</code> <code>switch-1(config-if-ptp-slave)# master ipv4 4.4.4.3</code></td>
<td></td>
</tr>
</tbody>
</table>

### Configuring Unicast Source Address

Complete the following steps to configure unicast source address:
## Configuring PTP

The timestamp tagging feature provides precision time information to track in real time when packets arrive at remote devices. Packets are truncated and timestamped using PTP with nanosecond accuracy. Using the TAP aggregation functionality on the switch, along with the Cisco Nexus Data Broker, you can copy the network traffic using SPAN, filter and timestamp the traffic, and send it for recording and analysis.

### Configuring Timestamp Tagging

You can configure timestamp tagging for Cisco Nexus 9200 and 9300-EX Series switches

**Note**

Configuring timestamp tagging is not supported on Cisco Nexus 9508 switches with N9K-X9636C-R, N9K-X9636C-RX, and N9K-X9636Q-R line cards.

**Before you begin**

Make sure that you have globally enabled PTP offloading.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

---

## Procedure

### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

---

### Example

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch(config-if)# ptp ucast-source A.B.C.D IPv4 address (A.B.C.D) of source</td>
<td>You can configure PTP source address per interface level. This IP address is used only for unicast PTP messages. You have to make sure that the PTP unicast source IP address is reachable.</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `switch# configure terminal`  
`switch(config)#` | |
| **Step 2**  
`interface type slot/port`  
**Example:**  
`switch(config)# interface ethernet 2/2`  
`switch(config-if)#` | Enters interface configuration mode for the specified interface. |
| **Step 3**  
`[no] ttag`  
**Example:**  
`switch(config-if)# ttag` | Configures timestamp tagging on the Layer 2 or Layer 3 egress interface. |

## Configuring the TTAG Marker Packets and Time Interval

You can configure timestamp tagging for Cisco Nexus 9200 and 9300-EX Series switches.

The ttag timestamp field attaches a 48-bit timestamp on the marker packet. This 48-bit timestamp is not a human familiar ASCII based timestamp. To make this 48-bit timestamp human readable, the ttag marker packet can be used to provide additional information to decode the 48-bit timestamp information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Position (byte:bit)</th>
<th>Length</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Magic</td>
<td></td>
<td>64</td>
<td>By default, this field displays A6A6A6A6A6A6A6A6A6A6. This enables to identify ttag-marker packets on the packet stream.</td>
</tr>
<tr>
<td>Version</td>
<td></td>
<td>8</td>
<td>Version number. The default version is 1.</td>
</tr>
<tr>
<td>Granularity</td>
<td></td>
<td>8</td>
<td>This field is 32-bit based hardware timestamp value of the switch. By default, the value is 0, which is 100 picoseconds or 0.1 nanoseconds.</td>
</tr>
<tr>
<td>UTC_offset</td>
<td></td>
<td>8</td>
<td>The utc_offset between the ASIC and the UTC clocks. The default value is 0.</td>
</tr>
<tr>
<td>Timestamp_hi</td>
<td></td>
<td>32</td>
<td>The high 16-bit of 48-bit ASIC hardware timestamp.</td>
</tr>
<tr>
<td>Timestamp_lo</td>
<td></td>
<td>32</td>
<td>The low 32-bit of 48-bit ASIC hardware timestamp.</td>
</tr>
<tr>
<td>UTC sec</td>
<td></td>
<td>32</td>
<td>The seconds part of UTC timestamp from the CPU clock of the Cisco Nexus 9000 Series switch.</td>
</tr>
</tbody>
</table>
### Configuring PTP Interface to Stay in a Master State

This procedure describes how to prevent an endpoint from causing a port to transition to a slave state.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> interface type slot/port</td>
<td>Enters interface configuration mode for the specified interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# interface ethernet 2/2</td>
<td></td>
</tr>
<tr>
<td>switch(config-if)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> [no] ttag-marker enable</td>
<td>Sends the ttag-marker packets to the outgoing port.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config-if)# ttag-marker enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ttag-marker-interval 90</td>
<td>Configures the seconds that a switch will take to send a ttag-marker packet to the outgoing ports. This is a global to the switch. By default, it sends a ttag-marker packet every 60 seconds.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config-if)# ttag-marker enable</td>
<td></td>
</tr>
</tbody>
</table>

### Before you begin

Make sure that you have globally enabled PTP offloading.

#### Procedure

**UTC usec** | 32 | The microsecond part of UTC timestamp from the CPU clock of the Cisco Nexus 9000 Series switch.  
Reserved | 32 | Reserved for future use.  
Signature | 32 | The default value is 0xA5A5A5A5A5. This allows a forward search of marker packet and provide references to the UTC timestamp, so the client software can use that reference UTC to recover the 32-bit hardware timestamp in each packet header.  
Pad | 8 | This is align byte to convert the ttag-marker align to 4 byte boundary.
Before you begin

- Make sure that you have globally enabled PTP on the switch and configured the source IP address for PTP communication.
- After you globally enable PTP, it is not enabled on all supported interfaces by default. You must enable PTP interfaces individually.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>switch # configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>switch(config) # interface ethernet slot/port</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>switch(config-if) # [no] feature ptp</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>switch(config-if) # ptp multicast master-only</td>
</tr>
</tbody>
</table>

Example

This example shows how to configure PTP on an interface and configure the interface to maintain the Master state:

```
switch(config)# show ptp brief

PTP port status
----------------------------------
Port State
------------------ ------------
Eth1/1 Slave
```

```
switch(config)# show ptp brief

Port State
------------------ ------------
Eth1/1 Slave
```

```
switch(config)# interface ethernet 1/1
switch(config-if)# ptp multicast master-only
```

```
2001 Jan 7 07:50:03 A3-MTC-CR-1 % VDC-1 % %PTP-2-PTP GM CHANGE: Grandmaster clock has changed from 60:73:5c:ff:fe:62:a1:41 to 58:97:bd:ff:fe:0d:54:01 for the PTP protocol
2001 Jan 7 07:50:03 A3-MTC-CR-1 % VDC-1 % %PTP-2-PTP STATE_CHANGE: Interface Eth1/1 change from PTP_BMC_STATE_SLAVE to PTP_BMC_STATE_PRE_MASTER
2001 Jan 7 07:50:03 A3-MTC-CR-1 % VDC-1 % %PTP-2-PTP TIME_SYNC_LOST: Lost sync with master clock
2001 Jan 7 07:50:03 A3-MTC-CR-1 % VDC-1 % %PTP-2-PTP STATE_CHANGE: Interface Eth1/1 change from PTP_BMC_STATE_PRE_MASTER to PTP_BMC_STATE_MASTER
```

Verifying the PTP Configuration

Use one of the following commands to verify the configuration:

Table 7: PTP Show Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ptp brief</td>
<td>Displays the PTP status.</td>
</tr>
</tbody>
</table>
### Command Purpose

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ptp clock</td>
<td>Displays the properties of the local clock, including clock identity.</td>
</tr>
<tr>
<td>show ptp clock foreign-masters-record</td>
<td>Displays the state of foreign masters known to the PTP process. For each foreign master, the output displays the clock identity, basic clock properties, and whether the clock is being used as a grandmaster.</td>
</tr>
<tr>
<td>show ptp corrections</td>
<td>Displays the last few PTP corrections.</td>
</tr>
<tr>
<td>show ptp counters [all</td>
<td>interface ethernet slot/port]</td>
</tr>
<tr>
<td>show ptp parent</td>
<td>Displays the properties of the PTP parent.</td>
</tr>
<tr>
<td>show ptp port interface ethernet slot/port</td>
<td>Displays the status of the PTP port on the switch.</td>
</tr>
<tr>
<td>show ptp time-property</td>
<td>Displays the PTP clock properties.</td>
</tr>
<tr>
<td>show ttag brief</td>
<td>Displays the status of the timestamp tagging configuration. Note: Timestamp tagging configuration is not supported on Cisco Nexus 9508 switches with N9K-X9636C-R, N9K-X9636C-RX, and N9K-X9636Q-R line cards.</td>
</tr>
<tr>
<td>show running-config ptp [all]</td>
<td>Displays the running configuration for PTP.</td>
</tr>
<tr>
<td>clear ptp counters [all</td>
<td>interface ethernet slot/port]</td>
</tr>
<tr>
<td>clear ptp corrections</td>
<td>Clears the history of the PTP corrections.</td>
</tr>
</tbody>
</table>

### Configuration Examples for PTP

This example shows how to configure PTP globally on the device, specify the source IP address for PTP communications, and configure a preference level for the clock:

```
switch# configure terminal
switch(config)# feature ptp
switch(config)# ptp source 10.10.10.1
switch(config)# ptp priority1 1
switch(config)# ptp priority2 1
switch(config)# show ptp brief
PTP port status
-------------------------------
Port State  -------------------
switch(config)# show ptp clock
PTP Device Type: Boundary clock
```
This example shows how to configure PTP on an interface and configure the intervals for the announce, delay-request, and synchronization messages:

```bash
switch# configure terminal
switch(config)# interface Ethernet 1/1
switch(config-if)# ptp
switch(config-if)# ptp announce interval 3
switch(config-if)# ptp announce timeout 2
switch(config-if)# ptp delay-request minimum interval smpte-2059-2 -3
switch(config-if)# ptp sync interval smpte-2059-2 -3
switch(config-if)# no shutdown
switch(config-if)# show ptp brief
```

PTP Port status
-----------------------
Port State
------- --------------
Eth2/1 Master

```bash
switch(config-if)# show ptp port interface ethernet 2/1
```

PTP Port Dataset: Eth2/1
Port identity: port number: 1028
Port state: Master
Delay request interval(log mean): 4
Announce receipt time out: 2
Peer mean path delay: 0
Announce interval(log mean): 3
Sync interval(log mean): 1
Delay Mechanism: End to End
Peer delay request interval(log mean): 0

This example shows how to configure master/slave role and assign corresponding peer slave/master IP addresses.

```bash
switch-1(config)# interface ethernet 1/1
switch-1(config-if)# ptp transport ipv4 ucast master
switch-1(config-if-ptp-master)# slave ipv4 1.2.3.1
switch-1(config-if-ptp-master)# slave ipv4 1.2.3.2
switch-1(config-if-ptp-master)# slave ipv4 1.2.3.3
switch-1(config-if-ptp-master)# slave ipv4 1.2.3.4

switch-1(config-if)# ptp transport ipv4 ucast slave
switch-1(config-if-ptp-slave)# master ipv4 4.4.4.1
switch-1(config-if-ptp-slave)# master ipv4 4.4.4.2
switch-1(config-if-ptp-slave)# master ipv4 4.4.4.3
```
switch-1(config-if-tp-slave)# ptp ucast-source 9.9.9.9

switch-1(config-if)# sh running-config ptp

!Command: show running-config ptp
!Time: Tue Feb 7 17:37:09 2017

version 7.0(3)I4(6)
feature ptp

ptp source 1.1.1.1

interface Ethernet1/1
  ptp transport ipv4 ucast master
  slave ipv4 1.2.3.1
  slave ipv4 1.2.3.2
  slave ipv4 1.2.3.3
  slave ipv4 1.2.3.4

interface Ethernet1/2
  ptp transport ipv4 ucast slave
  master ipv4 4.4.4.1
  master ipv4 4.4.4.2
  master ipv4 4.4.4.3
  ptp ucast-source 9.9.9.9

switch-1(config-if)#

Additional References

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1588 IEEE</td>
<td>1588 IEEE standards and https: <a href="http://www.smpte.org">www.smpte.org</a> <a href="http://www.aes.org">www.aes.org</a></td>
</tr>
</tbody>
</table>
CHAPTER 5

Configuring NTP

This chapter describes how to configure the Network Time Protocol (NTP) on Cisco NX-OS devices. This chapter includes the following sections:

- About NTP, on page 53
- Licensing Requirements for NTP, on page 55
- Prerequisites for NTP, on page 55
- Guidelines and Limitations for NTP, on page 55
- Default Settings for NTP, on page 56
- Configuring NTP, on page 56
- Verifying the NTP Configuration, on page 64
- Configuration Examples for NTP, on page 65
- Additional References, on page 66

About NTP

The Network Time Protocol (NTP) synchronizes the time of day among a set of distributed time servers and clients so that you can correlate events when you receive system logs and other time-specific events from multiple network devices. NTP uses the User Datagram Protocol (UDP) as its transport protocol. All NTP communications use Coordinated Universal Time (UTC).

An NTP server usually receives its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server, and then distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two machines to within a millisecond of each other.

NTP uses a stratum to describe the distance between a network device and an authoritative time source:

- A stratum 1 time server is directly attached to an authoritative time source (such as a radio or atomic clock or a GPS time source).
- A stratum 2 NTP server receives its time through NTP from a stratum 1 time server.

Before synchronizing, NTP compares the time reported by several network devices and does not synchronize with one that is significantly different, even if it is a stratum 1. Because Cisco NX-OS cannot connect to a radio or atomic clock and act as a stratum 1 server, we recommend that you use the public NTP servers available on the Internet. If the network is isolated from the Internet, Cisco NX-OS allows you to configure the time as though it were synchronized through NTP, even though it was not.
You can create NTP peer relationships to designate the time-serving hosts that you want your network device to consider synchronizing with and to keep accurate time if a server failure occurs.

The time kept on a device is a critical resource, so we strongly recommend that you use the security features of NTP to avoid the accidental or malicious setting of incorrect time. Two mechanisms are available: an access list-based restriction scheme and an encrypted authentication mechanism.

**NTP Associations**

An NTP association can be one of the following:

- A peer association—The device can either synchronize to another device or allow another device to synchronize to it.
- A server association—The device synchronizes to a server.

You need to configure only one end of an association. The other device can automatically establish the association.

**NTP as a Time Server**

The Cisco NX-OS device can use NTP to distribute time. Other devices can configure it as a time server. You can also configure the device to act as an authoritative NTP server, enabling it to distribute time even when it is not synchronized to an outside time source.

**Clock Manager**

Clocks are resources that need to be shared across different processes. Multiple time synchronization protocols, such as NTP, might be running in the system.

The clock manager allows you to specify the protocol to control the various clocks in the system. Once you specify the protocol, the system clock starts updating. For information on configuring the clock manager, see the Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide.

**High Availability**

Stateless restarts are supported for NTP. After a reboot or a supervisor switchover, the running configuration is applied. For more information on high availability, see the Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide.

You can configure NTP peers to provide redundancy in case an NTP server fails.

**Virtualization Support**

NTP recognizes virtual routing and forwarding (VRF) instances. NTP uses the default VRF if you do not configure a specific VRF for the NTP server and NTP peer. See the Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide for more information about VRFs.
Licensing Requirements for NTP

<table>
<thead>
<tr>
<th>Product</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco NX-OS</td>
<td>NTP requires no license. Any feature not included in a license package is bundled with the nx-os image and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the Cisco NX-OS Licensing Guide.</td>
</tr>
</tbody>
</table>

Prerequisites for NTP

NTP has the following prerequisites:

- To configure NTP, you must have connectivity to at least one server that is running NTP.

Guidelines and Limitations for NTP

NTP has the following configuration guidelines and limitations:

- NTP server functionality is supported.

- We recommend that you configure a peer association with another device only when you are sure that your clock is reliable (which means that you are a client of a reliable NTP server).

- A peer that is configured alone takes on the role of a server and should be used as a backup. If you have two servers, you can configure several devices to point to one server and the remaining devices to point to the other server. You can then configure a peer association between these two servers to create a more reliable NTP configuration.

- If you have only one server, we recommend that you configure all the devices as clients to that server.

- You can configure up to 64 NTP entities (servers and peers).

- If you configure NTP in a VRF, ensure that the NTP server and peers can reach each other through the configured VRFs.

- Manually distribute NTP authentication keys on the NTP server and Cisco NX-OS devices across the network.

- If you are using the switch as an edge device and want to use NTP, we recommend using the ntp access-group command and filtering NTP only to the required edge devices.

- If the system has been configured with the ntp passive, ntp broadcast client, or ntp multicast client commands, when NTP receives an incoming symmetric active, broadcast, or multicast packet, it can set up an ephemeral peer association in order to synchronize with the sender.
Make sure that you specify `ntp authenticate` before enabling any of the preceding commands. Failure to do so will allow your device to synchronize with any device that sends one of the preceding packet types, including malicious attacker-controlled devices.

- If you specify the `ntp authenticate` command, when a symmetric active, broadcast, or multicast packet is received, the system does not synchronize to the peer unless the packet carries one of the authentication keys that are specified in the `ntp trusted-key` global configuration command.

- To prevent synchronization with unauthorized network hosts, the `ntp authenticate` command should be specified any time the `ntp passive`, `ntp broadcast client`, or `ntp multicast client` command has been specified unless other measures, such as the `ntp access-group` command, have been taken to prevent unauthorized hosts from communicating with the NTP service on the device.

- The `ntp authenticate` command does not authenticate peer associations that are configured via the `ntp server` and `ntp peer` configuration commands. To authenticate the `ntp server` and `ntp peer` associations, specify the `key` keyword.

- A maximum of four IP ACLs can be configured for a single NTP access group. IPv4 and IPv6 ACLs are supported.

## Default Settings for NTP

The following table lists the default settings for NTP parameters.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP</td>
<td>Enabled</td>
</tr>
<tr>
<td>NTP authentication</td>
<td>Disabled</td>
</tr>
<tr>
<td>NTP access</td>
<td>Enabled</td>
</tr>
<tr>
<td>NTP access group match all</td>
<td>Disabled</td>
</tr>
<tr>
<td>NTP logging</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

## Configuring NTP

Be aware that the Cisco NX-OS commands for this feature may differ from those commands used in Cisco IOS.

## Enabling or Disabling NTP

You can enable or disable NTP. NTP is enabled by default.
### Configuring NTP

#### Procedure

| Step 1 | configure terminal
Example:
`switch# configure terminal
switch(config)#` | Enters global configuration mode. |
|--------|-------------------------------------------------|---------------------------------|
| Step 2 | `[no] feature ntp
Example:
`switch(config)# feature ntp` | Enables or disables NTP. |
| Step 3 | `(Optional) copy running-config startup-config
Example:
`switch(config)# copy running-config startup-config` | Copies the running configuration to the startup configuration. |

#### Configuring the Device as an Authoritative NTP Server

You can configure the device to act as an authoritative NTP server, enabling it to distribute time even when it is not synchronized to an existing time server.

**Procedure**

| Step 1 | configure terminal
Example:
`switch# configure terminal
switch(config)#` | Enters global configuration mode. |
|--------|-------------------------------------------------|---------------------------------|
| Step 2 | `[no] ntp master [stratum]
Example:
`switch(config)# ntp master` | Configures the device as an authoritative NTP server.
- You can specify a different stratum level from which NTP clients get their time synchronized.
  - The range is from 1 to 15. |
| Step 3 | `(Optional) show running-config ntp
Example:
`switch(config)# show running-config ntp` | Displays the NTP configuration. |
| Step 4 | `(Optional) copy running-config startup-config
Example:
`switch(config)# copy running-config startup-config` | Copies the running configuration to the startup configuration. |
Configuring an NTP Server and Peer

You can configure an NTP server and peer.

Before you begin

Make sure you know the IP address or Domain Name System (DNS) names of your NTP server and its peers.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: switch# configure terminal switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> [no] ntp server {ip-address</td>
<td>ipv6-address</td>
</tr>
<tr>
<td>Example: switch(config)# ntp server 192.0.2.10</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> [no] ntp peer {ip-address</td>
<td>ipv6-address</td>
</tr>
<tr>
<td>Example: switch(config)# ntp peer 2001:0db8::4101</td>
<td></td>
</tr>
</tbody>
</table>
Purpose

Use the `maxpoll` and `minpoll` keywords to configure the maximum and minimum intervals in which to poll a server. The range for the `max-poll` and `min-poll` arguments is from 4 to 17 (configured as powers of 2, so effectively 16 to 131072 seconds), and the default values are 6 and 4, respectively (`maxpoll` default = 64 seconds, `minpoll` default = 16 seconds).

Use the `prefer` keyword to make this peer the preferred NTP peer for the device.

Use the `use-vrf` keyword to configure the NTP peer to communicate over the specified VRF. The `vrf-name` argument can be `default`, `management`, or any case-sensitive, alphanumeric string up to 32 characters.

Step 4

*(Optional)*  `show ntp peers`

*Example:*

```
switch(config)# show ntp peers
```

*Purpose*

Displays the configured server and peers.

*Note*

A domain name is resolved only when you have a DNS server configured.

Step 5

*(Optional)*  `copy running-config startup-config`

*Example:*

```
switch(config)# copy running-config startup-config
```

*Purpose*

Copies the running configuration to the startup configuration.

Configuring NTP Authentication

You can configure the device to authenticate the time sources to which the local clock is synchronized. When you enable NTP authentication, the device synchronizes to a time source only if the source carries one of the authentication keys specified by the `ntp trusted-key` command. The device drops any packets that fail the authentication check and prevents them from updating the local clock. NTP authentication is disabled by default.

Before you begin

Make sure that you configured the NTP server with the authentication keys that you plan to specify in this procedure.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong>  <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

Configuring NTP Authentication

You can configure the device to authenticate the time sources to which the local clock is synchronized. When you enable NTP authentication, the device synchronizes to a time source only if the source carries one of the authentication keys specified by the `ntp trusted-key` command. The device drops any packets that fail the authentication check and prevents them from updating the local clock. NTP authentication is disabled by default.

Before you begin

Make sure that you configured the NTP server with the authentication keys that you plan to specify in this procedure.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong>  <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><code>switch# configure terminal</code>&lt;br&gt;<code>switch(config)#</code></td>
<td>Defines the authentication keys. The device does not synchronize to a time source unless the source has one of these authentication keys and the key number is specified by the <code>ntp trusted-key number</code> command. The range for authentication keys is from 1 to 65535. For the MD5 string, you can enter up to eight alphanumeric characters.</td>
</tr>
</tbody>
</table>
| **Step 2** `[no] ntp authentication-key number md5 md5-string`<br>**Example:**<br>`switch(config)# ntp authentication-key 42 md5 aNiceKey` | Forms an association with a server. Use the `key` keyword to configure a key to be used while communicating with the NTP server. The range for the `key-id` argument is from 1 to 65535.
To require authentication, the `key` keyword must be used. Any `ntp server` or `ntp peer` commands that do not specify the `key` keyword will continue to operate without authentication. |
| **Step 3** `ntp server ip-address key key-id`<br>**Example:**<br>`switch(config)# ntp server 192.0.2.1 key 1001` | Specifies one or more keys (defined in Step 2) that an unconfigured remote symmetric, broadcast, and multicast time source must provide in its NTP packets in order for the device to synchronize to it. The range for trusted keys is from 1 to 65535.
This command provides protection against accidentally synchronizing the device to a time source that is not trusted. |
| **Step 4** *(Optional)* `show ntp authentication-keys`<br>**Example:**<br>`switch(config)# show ntp authentication-keys` | Enables or disables authentication for ntp passive, ntp broadcast client, and ntp multicast. NTP authentication is disabled by default. |
| **Step 5** `[no] ntp trusted-key number`<br>**Example:**<br>`switch(config)# ntp trusted-key 42` | Displays the configured NTP trusted keys. |
| **Step 6** *(Optional)* `show ntp trusted-keys`<br>**Example:**<br>`switch(config)# show ntp trusted-keys` | Displays the status of NTP authentication. |
| **Step 7** `[no] ntp authenticate`<br>**Example:**<br>`switch(config)# ntp authenticate` | Displays the configured NTP authentication keys. |
Configuring NTP Access Restrictions

You can control access to NTP services by using access groups. Specifically, you can specify the types of requests that the device allows and the servers from which it accepts responses.

If you do not configure any access groups, NTP access is granted to all devices. If you configure any access groups, NTP access is granted only to the remote device whose source IP address passes the access list criteria.

Beginning with Cisco NX-OS Release 7.0(3)I7(3), access groups are evaluated in the following method:

- Without the `match-all` keyword, the packet gets evaluated against the access groups (in the order mentioned below) until it finds a permit. If a permit is not found, the packet is dropped.
- With `match-all` keyword, the packet gets evaluated against all the access groups (in the order mentioned below) and the action is taken based on the last successful evaluation (the last access group where an ACL is configured).

The mapping of the access group to the type of packet is as follows:

- peer—process client, symmetric active, symmetric passive, serve, control, and private packets (all types)
- serve—process client, control, and private packets
- serve-only—process client packets only
- query-only—process control and private packets only

The access groups are evaluated in the following descending order:

1. peer (all packet types)
2. serve (client, control, and private packets)
3. query only (client packets) or query-only (control and private packets)

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

Example:

```
switch# configure terminal
switch(config)#
```
### Purpose

Command or Action | Purpose
--- | ---
### Step 2 | Creates or removes an access group to control NTP access and applies a basic IP access list.

ACL processing stops and does not continue to the next access group option if NTP matches a deny ACL rule in a configured peer.

- The **peer** keyword enables the device to receive time requests and NTP control queries and to synchronize itself to the servers specified in the access list.

- The **serve** keyword enables the device to receive only time requests from the servers specified in the access list but not to synchronize itself to the specified servers.

- The **serve-only** keyword enables the device to receive only time requests from servers specified in the access list.

- The **query-only** keyword enables the device to receive only NTP control queries from the servers specified in the access list.

- The **match-all** keyword enables the access group options to be scanned in the following order, from least restrictive to most restrictive: peer, serve, serve-only, query-only. If the incoming packet does not match the ACL in the peer access group, it goes to the serve access group to be processed. If the packet does not match the ACL in the serve access group, it goes to the serve-only access group, and so on.

#### Note

The **match-all** keyword is available beginning with Cisco NX-OS Release 7.0(3)I6(1) and is supported on Cisco Nexus 9000 Series switches and the Cisco Nexus 3164Q, 31128PQ, 3232C, and 3264Q switches.

- The **access-list-name** variable is the name of the NTP access group. The name can be an alphanumeric string up to 64 characters, including special characters.

Example:

- **switch(config)# ntp access-group match-all {peer | serve | serve-only | query-only}
  
- **access-list-name**

Example:

- **switch(config)# ntp access-group peer peer-acl
- **switch(config)# ntp access-group serve serve-acl**
Configuring NTP

Configuring the NTP Source IP Address

NTP sets the source IP address for all NTP packets based on the address of the interface through which the NTP packets are sent. You can configure NTP to use a specific source IP address.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> [no] ntp source ip-address</td>
<td>Configures the source IP address for all NTP packets. The <em>ip-address</em> can be in IPv4 or IPv6 format.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td>ntp source 192.0.2.1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> (Optional) copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

Configuring the NTP Source Interface

You can configure NTP to use a specific interface.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
</tbody>
</table>
Configuring NTP Logging

You can configure NTP logging in order to generate system logs with significant NTP events. NTP logging is disabled by default.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch# configure terminal switch(config)#</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>[no] ntp logging</td>
<td>Enables or disables system logs to be generated with significant NTP events. NTP logging is disabled by default.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# ntp logging</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>(Optional) show ntp logging-status</td>
<td>Displays the NTP logging configuration status.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# show ntp logging-status</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>(Optional) copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

Verifying the NTP Configuration

To display the NTP configuration, perform one of the following tasks:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ntp access-groups</td>
<td>Displays the NTP access group configuration.</td>
</tr>
<tr>
<td>show ntp authentication-keys</td>
<td>Displays the configured NTP authentication keys.</td>
</tr>
<tr>
<td>Command</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>show ntp authentication-status</td>
<td>Displays the status of NTP authentication.</td>
</tr>
<tr>
<td>show ntp logging-status</td>
<td>Displays the NTP logging status.</td>
</tr>
<tr>
<td>show ntp peer-status</td>
<td>Displays the status for all NTP servers and peers.</td>
</tr>
<tr>
<td>show ntp peers</td>
<td>Displays all the NTP peers.</td>
</tr>
<tr>
<td>show ntp rts-update</td>
<td>Displays the RTS update status.</td>
</tr>
<tr>
<td>show ntp source</td>
<td>Displays the configured NTP source IP address.</td>
</tr>
<tr>
<td>show ntp source-interface</td>
<td>Displays the configured NTP source interface.</td>
</tr>
<tr>
<td>show ntp statistics</td>
<td>Displays the NTP statistics.</td>
</tr>
<tr>
<td>show ntp trusted-keys</td>
<td>Displays the configured NTP trusted keys.</td>
</tr>
<tr>
<td>show running-config ntp</td>
<td>Displays NTP information.</td>
</tr>
</tbody>
</table>

Use the `clear ntp session` command to clear the NTP sessions.

Use the `clear ntp statistics` command to clear the NTP statistics.

**Configuration Examples for NTP**

This example shows how to configure the device to synchronize only to time sources that provide authentication key 42 in their NTP packets:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ntp authentication-key 42 md5 aNiceKey
switch(config)# ntp server 192.0.2.105 key 42
switch(config)# ntp trusted-key 42
switch(config)# ntp authenticate
switch(config)# copy running-config startup-config
[########################################] 100%
switch(config)#
```

This example shows an NTP access group configuration with the following restrictions:

- Peer restrictions are applied to IP addresses that pass the criteria of the access list named “peer-acl.”
- Serve restrictions are applied to IP addresses that pass the criteria of the access list named “serve-acl.”
- Serve-only restrictions are applied to IP addresses that pass the criteria of the access list named “serve-only-acl.”
- Query-only restrictions are applied to IP addresses that pass the criteria of the access list named “query-only-acl.”

```
switch# configure terminal
switch(config)# ntp peer 10.1.1.1
switch(config)# ntp peer 10.2.2.2
switch(config)# ntp peer 10.3.3.3
switch(config)# ntp peer 10.4.4.4
```
switch(config)# ntp peer 10.5.5.5
switch(config)# ntp peer 10.6.6.6
switch(config)# ntp peer 10.7.7.7
switch(config)# ntp peer 10.8.8.8
switch(config)# ntp access-group peer peer-acl
switch(config)# ntp access-group serve serve-acl
switch(config)# ntp access-group serve-only serve-only-acl
switch(config)# ntp access-group query-only query-only-acl
switch(config)# ip access-list peer-acl
switch(config-acl)# 10 permit ip host 10.1.1.1 any
switch(config-acl)# 20 permit ip host 10.8.8.8 any
switch(config)# ip access-list serve-acl
switch(config-acl)# 10 permit ip host 10.4.4.4 any
switch(config-acl)# 20 permit ip host 10.5.5.5 any
switch(config)# ip access-list serve-only-acl
switch(config-acl)# 10 permit ip host 10.6.6.6 any
switch(config-acl)# 20 permit ip host 10.7.7.7 any
switch(config)# ip access-list query-only-acl
switch(config-acl)# 10 permit ip host 10.2.2.2 any
switch(config-acl)# 20 permit ip host 10.3.3.3 any

## Additional References

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clock manager</td>
<td>Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide</td>
</tr>
</tbody>
</table>

## MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIBs related to NTP</td>
<td>To locate and download supported MIBs, go to the following URL:</td>
</tr>
<tr>
<td></td>
<td>Nexus9000MIBSupportList.html</td>
</tr>
</tbody>
</table>
CHAPTER 6

Configuring CDP

This chapter describes how to configure the Cisco Discovery Protocol (CDP) on Cisco NX-OS devices. This chapter includes the following sections:

- About CDP, on page 67
- Licensing Requirements for CDP, on page 69
- Guidelines and Limitations for CDP, on page 69
- Default Settings for CDP, on page 69
- Configuring CDP, on page 69
- Verifying the CDP Configuration, on page 72
- Configuration Example for CDP, on page 72

About CDP

The Cisco Discovery Protocol (CDP) is a media-independent and protocol-independent protocol that runs on all Cisco-manufactured equipment including routers, bridges, access and communication servers, and switches. You can use CDP to discover and view information about all the Cisco devices that are directly attached to the device.

CDP gathers protocol addresses of neighboring devices and discovers the platform of those devices. CDP runs over the data link layer only. Two systems that support different Layer 3 protocols can learn about each other.

Each device that you configure for CDP sends periodic advertisements to a multicast address. Each device advertises at least one address at which it can receive SNMP messages. The advertisements also contain hold-time information, which indicates the length of time that a receiving device should hold CDP information before removing it. You can configure the advertisement or refresh timer and the hold timer.

CDP Version-2 (CDPv2) allows you to track instances where the native VLAN ID or port duplex states do not match between connecting devices.

CDP advertises the following type-length-value fields (TLVs):

- Device ID
- Address
- Port ID
- Capabilities
• Version
• Platform
• Native VLAN
• Full or Half Duplex
• MTU
• SysName
• SysObjectID
• Management Address
• Physical Location
• VTP

All CDP packets include a VLAN ID. If you configure CDP on a Layer 2 access port, the CDP packets sent from that access port include the access port VLAN ID. If you configure CDP on a Layer 2 trunk port, the CDP packets sent from that trunk port include the lowest configured VLAN ID allowed on that trunk port. The trunk port can receive CDP packets that include any VLAN ID in the allowed VLAN list for that trunk port. For more information on VLANs, see the Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide.

VTP Feature Support

CDP sends the VLAN Trunking Protocol (VTP) type-length-value field (TLV) if the following conditions are met:

• CDP Version 2 is enabled.
• The VTP feature is enabled.
• A VTP domain name is configured.

You can view the VTP information with the show cdp neighbors detail command.

High Availability

Cisco NX-OS supports both stateful and stateless restarts and switchover for CDP. For more information on high availability, see the Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide.

Virtualization Support

Cisco NX-OS supports one instance of CDP.
Licensing Requirements for CDP

<table>
<thead>
<tr>
<th>Product</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco NX-OS</td>
<td>CDP requires no license. Any feature not included in a license package is bundled with the nx-os image and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the <em>Cisco NX-OS Licensing Guide</em>.</td>
</tr>
</tbody>
</table>

Guidelines and Limitations for CDP

CDP has the following configuration guidelines and limitations:

- CDP can discover up to 256 neighbors per port if the port is connected to a hub with 256 connections.
- CDP must be enabled on the device or you cannot enable it on any interfaces.
- You can configure CDP on physical interfaces and port channels only.

Default Settings for CDP

This table lists the default settings for CDP parameters.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDP</td>
<td>Enabled globally and on all interfaces</td>
</tr>
<tr>
<td>CDP version</td>
<td>Version 2</td>
</tr>
<tr>
<td>CDP device ID</td>
<td>Serial number</td>
</tr>
<tr>
<td>CDP timer</td>
<td>60 seconds</td>
</tr>
<tr>
<td>CDP hold timer</td>
<td>180 seconds</td>
</tr>
</tbody>
</table>

Configuring CDP

**Note**

The Cisco NX-OS commands for this feature may differ from those commands that are used in Cisco IOS.

Enabling or Disabling CDP Globally

CDP is enabled by default. You can disable CDP and then reenable it.
You must enable CDP on the device before you enable CDP on any interfaces. If CDP is disabled globally and you enable CDP on specified interfaces, CDP will not be active on those interfaces; the system does not return an error message.

### Enabling or Disabling CDP on an Interface

CDP is enabled by default on an interface. You can disable CDP on an interface.

If CDP is disabled globally and you enable CDP on specified interfaces, CDP will not be active on those interfaces; the system does not return an error message.

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>switch# configure terminal</code> <code>switch(config)#</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>[no] cdp enable</code></td>
<td>Enables or disables the CDP feature on the entire device. It is enabled by default.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>switch(config)# cdp enable</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>(Optional) copy running-config startup-config</code></td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>switch(config)# copy running-config startup-config</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>(Optional) show cdp interface interface slot/port</code></td>
<td>Displays CDP information for an interface.</td>
</tr>
</tbody>
</table>
Configuring CDP

You can use the optional commands in this procedure to modify CDP.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: switch(config)# configure terminal switch(config)#</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2** (Optional) cdp advertise {v1 | v2} | Sets the CDP version that is supported by the device. The default is v2. |
| Example: switch(config)# cdp advertise v1 | |

| **Step 3** (Optional) cdp format device-id {mac-address | serial-number | system-name} | Sets the CDP device ID. The options are as follows: |
| Example: switch(config)# cdp format device-id mac-address | • mac-address—The MAC address of the chassis. |
| | • serial-number—The chassis serial number/Organizationally Unique Identifier (OUI). |
| | • system-name—The system name or fully qualified domain name. The default is system-name. |

| **Step 4** (Optional) cdp holdtime seconds | Sets the time that CDP holds onto neighbor information before removing it. The range is from 10 to 255 seconds. The default is 180 seconds. |
| Example: switch(config)# cdp holdtime 150 | |

| **Step 5** (Optional) cdp timer seconds | Sets the refresh time when CDP sends advertisements to neighbors. The range is from 5 to 254 seconds. The default is 60 seconds. |
| Example: switch(config)# cdp timer 50 | |
### Configuring CDP

#### Verifying the CDP Configuration

To display the CDP configuration, perform one of the following tasks:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show cdp all</td>
<td>Displays all interfaces that have CDP enabled.</td>
</tr>
<tr>
<td>show cdp entry {all</td>
<td>name entry-name}</td>
</tr>
<tr>
<td>show cdp global</td>
<td>Displays the CDP global parameters.</td>
</tr>
<tr>
<td>show cdp interface interface slot/port</td>
<td>Displays the CDP interface status.</td>
</tr>
<tr>
<td>show cdp neighbors {device-id</td>
<td>interface interface slot/port} [detail]</td>
</tr>
<tr>
<td>show cdp interface interface slot/port</td>
<td>Displays the CDP traffic statistics on an interface.</td>
</tr>
</tbody>
</table>

Use the `clear cdp counters` command to clear CDP statistics on an interface.

Use the `clear cdp table` command to clear the CDP cache for one or all interfaces.

#### Configuration Example for CDP

This example shows how to enable the CDP feature and configure the refresh and hold timers:

```
configure terminal
cdp enable
cdp timer 50
cdp holdtime 100
```
CHAPTER 7

Configuring System Message Logging

This chapter describes how to configure system message logging on Cisco NX-OS devices.

This chapter contains the following sections:

- About System Message Logging, on page 73
- Licensing Requirements for System Message Logging, on page 75
- Guidelines and Limitations for System Message Logging, on page 75
- Default Settings for System Message Logging, on page 75
- Configuring System Message Logging, on page 76
- Verifying the System Message Logging Configuration, on page 88
- Configuration Example for System Message Logging, on page 89
- Additional References, on page 89

About System Message Logging

You can use system message logging to control the destination and to filter the severity level of messages that system processes generate. You can configure logging to terminal sessions, a log file, and syslog servers on remote systems.

For more information about the system message format and the messages that the device generates, see the Cisco NX-OS System Messages Reference.

By default, the device outputs messages to terminal sessions and logs system messages to a log file.

The following table describes the severity levels used in system messages. When you configure the severity level, the system outputs messages at that level and lower.

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 – emergency</td>
<td>System unusable</td>
</tr>
<tr>
<td>1 – alert</td>
<td>Immediate action needed</td>
</tr>
<tr>
<td>2 – critical</td>
<td>Critical condition</td>
</tr>
<tr>
<td>3 – error</td>
<td>Error condition</td>
</tr>
<tr>
<td>Level</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td>4 – warning</td>
<td>Warning condition</td>
</tr>
<tr>
<td>5 – notification</td>
<td>Normal but significant condition</td>
</tr>
<tr>
<td>6 – informational</td>
<td>Informational message only</td>
</tr>
<tr>
<td>7 – debugging</td>
<td>Appears during debugging only</td>
</tr>
</tbody>
</table>

The device logs the most recent 100 messages of severity 0, 1, or 2 to the NVRAM log. You cannot configure logging to the NVRAM.

You can configure which system messages should be logged based on the facility that generated the message and its severity level.

**Syslog Servers**

The syslog servers run on remote systems that log system messages based on the syslog protocol. You can configure up to eight IPv4 or IPv6 syslog servers.

To support the same configuration of syslog servers on all switches in a fabric, you can use Cisco Fabric Services (CFS) to distribute the syslog server configuration.

**Note**

When the device first initializes, messages are sent to syslog servers only after the network is initialized.

**Secure Syslog Servers**

Beginning with Cisco NX-OS Release 9.2(1), you can configure the syslog server with support for a secure TLS transport connectivity to remote logging servers. Additionally, you can enforce the NX-OS switches (client) identity via the mutual authentication configuration. For NX-OS switches, this feature supports TLSv1.1 and TLSv1.2.

The Secure syslog server feature uses the TCP/TLS transport and security protocols to provide device authentication and encryption. This feature enables a Cisco NX-OS device (acting as a client) to make a secure, encrypted outbound connection to remote syslog servers (acting as a server) supporting secure connectivity for logging. With authentication and encryption, this feature allows for a secure communication over an insecure network.
Licensing Requirements for System Message Logging

<table>
<thead>
<tr>
<th>Product</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco NX-OS</td>
<td>System message logging requires no license. Any feature not included in a license package is bundled with the nx-os image and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the Cisco NX-OS Licensing Guide.</td>
</tr>
</tbody>
</table>

Guidelines and Limitations for System Message Logging

System message logging has the following configuration guidelines and limitations:

- System messages are logged to the console and the log file by default.
- Any system messages that are printed before the syslog server is reachable (such as supervisor active or online messages) cannot be sent to the syslog server.
- Beginning with Cisco NX-OS Release 9.2(1), you can configure the syslog server with support for a secure TLS transport connectivity to remote logging servers. This feature supports TLSv1.1 and TLSv1.2.
- For the secure syslog server(s) to be reachable over an in-band (nonmanagement) interface, the CoPP profile may need tweaks. Especially when multiple logging servers are configured and when many syslogs are generated in a short time (such as, boot up and config application).

Default Settings for System Message Logging

The following table lists the default settings for the system message logging parameters.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console logging</td>
<td>Enabled at severity level 2</td>
</tr>
<tr>
<td>Monitor logging</td>
<td>Enabled at severity level 5</td>
</tr>
<tr>
<td>Log file logging</td>
<td>Enabled to log messages at severity level 5</td>
</tr>
<tr>
<td>Module logging</td>
<td>Enabled at severity level 5</td>
</tr>
<tr>
<td>Facility logging</td>
<td>Enabled</td>
</tr>
<tr>
<td>Time-stamp units</td>
<td>Seconds</td>
</tr>
<tr>
<td>Syslog server logging</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
**Configuring System Message Logging**

*Note* Be aware that the Cisco NX-OS commands for this feature might differ from those commands used in Cisco IOS.

**Configuring System Message Logging to Terminal Sessions**

You can configure the device to log messages by their severity level to console, Telnet, and SSH sessions. By default, logging is enabled for terminal sessions.

*Note* The current critical (default) logging level is maintained if the console baud speed is 9600 baud (default). All attempts to change the console logging level will generate an error message. To increase the logging level (above critical), you must change the console baud speed to 38400 baud.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>terminal monitor</td>
<td>Enables the device to log messages to the console.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch# terminal monitor</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch# configure terminal switch(config)#</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>[no] logging console [severity-level]</td>
<td>Configures the device to log messages to the console session based on a specified severity level or higher. A lower number indicates a higher severity level. Severity levels range from 0 to 7:</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# logging console 3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 0 – emergency</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1 – alert</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2 – critical</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 3 – error</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
</tbody>
</table>
|                   | • 4 – warning  
|                   | • 5 – notification  
|                   | • 6 – informational  
|                   | • 7 – debugging  

If the severity level is not specified, the default of 2 is used. The no option disables the device’s ability to log messages to the console.

**Step 4** *(Optional)* show logging console  
**Example:**  
switch(config)# show logging console  

Displays the console logging configuration.

**Step 5** [no] logging monitor [severity-level]  
**Example:**  
switch(config)# logging monitor 3  

Enables the device to log messages to the monitor based on a specified severity level or higher. A lower number indicates a higher severity level. Severity levels range from 0 to 7:

- • 0 – emergency  
- • 1 – alert  
- • 2 – critical  
- • 3 – error  
- • 4 – warning  
- • 5 – notification  
- • 6 – informational  
- • 7 – debugging  

The configuration applies to Telnet and SSH sessions.

If the severity level is not specified, the default of 2 is used. The no option disables the device’s ability to log messages to the Telnet and SSH sessions.

**Step 6** *(Optional)* show logging monitor  
**Example:**  
switch(config)# show logging monitor  

Displays the monitor logging configuration.

**Step 7** [no] logging message interface type ethernet description  
**Example:**  

Enables you to add the description for physical Ethernet interfaces and subinterfaces in the system message log. The description is the same description that was configured on the interface.
Purpose

Command or Action

switch(config)# logging message interface
type ethernet description

Purpose

The **no** option disables the printing of the interface description in the system message log for physical Ethernet interfaces.

<table>
<thead>
<tr>
<th>Step 8</th>
<th>(Optional) copy running-config startup-config</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>switch(config)# copy running-config startup-config</td>
</tr>
</tbody>
</table>

Copies the running configuration to the startup configuration.

---

## Configuring the Origin ID for Syslog Messages

You can configure Cisco NX-OS to append the hostname, an IP address, or a text string to syslog messages that are sent to remote syslog servers.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch# configure terminal switch(config)#</td>
</tr>
<tr>
<td><strong>Step 2</strong> Required: `logging origin-id {hostname</td>
<td>ip ip-address</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# logging origin-id string n9k-switch-abc</td>
</tr>
<tr>
<td><strong>Step 3</strong> (Optional) <code>show logging origin-id</code></td>
<td>Displays the configured hostname, IP address, or text string that is appended to syslog messages that are sent to remote syslog servers.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# show logging origin-id Logging origin_id : enabled (string: n9k-switch-abc)</td>
</tr>
<tr>
<td><strong>Step 4</strong> (Optional) <code>copy running-config startup-config</code></td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# copy running-config startup-config</td>
</tr>
</tbody>
</table>

---

## Logging System Messages to a File

You can configure the device to log system messages to a file. By default, system messages are logged to the file `log:messages`.

---
### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
| Example: | switch# configure terminal  
switch(config)# | |

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| [no] logging logfile logfile-name severity-level | Configures the name of the log file used to store system messages and the minimum severity level to log. A lower number indicates a higher severity level. Severity levels range from 0 to 7:  
- 0 – emergency  
- 1 – alert  
- 2 – critical  
- 3 – error  
- 4 – warning  
- 5 – notification  
- 6 – informational  
- 7 – debugging  | |
| [size bytes] | You can optionally specify a maximum file size. The default severity level is 5, and the file size is from 4096 to 4194304 bytes. | |
| Example: | switch(config)# logging logfile my_log 6 | |

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>logging event {link-status</td>
<td>trunk-status</td>
<td></td>
</tr>
</tbody>
</table>
{enable | default} | Logs interface events.  
- link-status—Logs all UP/DOWN and CHANGE messages.  
- trunk-status—Logs all TRUNK status messages.  
- enable—Specifies to enable logging to override the port level configuration.  
- default—Specifies that the default logging configuration is used by interfaces not explicitly configured. | |
| Example: | switch(config)# logging event link-status default | |

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Optional) show logging info</td>
<td>Displays the logging configuration.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# show logging info</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Module and Facility Messages Logging

You can configure the severity level and time-stamp units of messages logged by modules and facilities.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><code>switch(config)#</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enables module log messages that have the specified severity level or higher. Severity levels range from 0 to 7:</td>
</tr>
<tr>
<td><code>[no] logging module [severity-level]</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>switch(config)# logging module 3</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Displays the module logging configuration.</td>
</tr>
<tr>
<td><code>(Optional) show logging module</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>switch(config)# show logging module</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Enables logging messages from the specified facility that have the specified severity level or higher. Severity levels range from 0 to 7:</td>
</tr>
<tr>
<td><code>[no] logging level facility severity-level</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>switch(config)# logging level aaa 2</code></td>
<td></td>
</tr>
</tbody>
</table>

#### Example:

```
switch(config)# copy running-config startup-config
```

```
switch# configure terminal
switch(config)#
```

```
switch(config)# logging module 3
```

```
switch(config)# show logging module
```

```
switch(config)# logging level aaa 2
```

```
switch(config)#
```

---

*(Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 9.2(x)*)
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 1 – alert</td>
<td></td>
</tr>
<tr>
<td>• 2 – critical</td>
<td></td>
</tr>
<tr>
<td>• 3 – error</td>
<td></td>
</tr>
<tr>
<td>• 4 – warning</td>
<td></td>
</tr>
<tr>
<td>• 5 – notification</td>
<td></td>
</tr>
<tr>
<td>• 6 – informational</td>
<td></td>
</tr>
<tr>
<td>• 7 – debugging</td>
<td></td>
</tr>
</tbody>
</table>

To apply the same severity level to all facilities, use the **all** facility. For defaults, see the **show logging level** command.

The **no** option resets the logging severity level for the specified facility to its default level. If you do not specify a facility and severity level, the device resets all facilities to their default levels.

#### Step 5

(Optional) **show logging level** [*facility]*

**Example:**

```
switch(config)# show logging level aaa
```

Display the logging level configuration and the system default level by facility. If you do not specify a facility, the device displays levels for all facilities.

#### Step 6

(Optional) **[no]** **logging level** *ethpm*

**Example:**

```
switch(config)# logging level ethpm link-down ?
<0-7>
0-emerg;1-alert;2-crit;3-err;4-warn;5-notif;6-inform;7-debug
```

Enables logging of the Ethernet Port Manager link-up/link-down syslog messages at level 3.

Use the **no** option to use the default logging level for Ethernet Port Manager syslog messages.
### Configuring Syslog Servers

You can configure up to eight syslog servers that reference remote systems where you want to log system messages.

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>[no] logging server host [severity-level [use-vrf vrf-name]]</td>
<td>Configures a syslog server at the specified hostname or IPv4 or IPv6 address. You can</td>
</tr>
</tbody>
</table>

**Note**

Cisco recommends that you configure the syslog server to use the management virtual routing and forwarding (VRF) instance. For more information on VRFs, see Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide.

---

### Configuring System Message Logging

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch(config)#logging level ethpm link-up ?</td>
<td></td>
</tr>
<tr>
<td>error  ERRORS</td>
<td></td>
</tr>
<tr>
<td>notif NOTICE</td>
<td></td>
</tr>
<tr>
<td>(config)# logging level ethpm link-up error ?</td>
<td></td>
</tr>
<tr>
<td>&lt;CR&gt;</td>
<td></td>
</tr>
<tr>
<td>(config)# logging level ethpm link-up notif ?</td>
<td></td>
</tr>
<tr>
<td>&lt;CR&gt;</td>
<td></td>
</tr>
</tbody>
</table>

Step 7

**[no]** logging timestamp [microseconds | milliseconds | seconds]

**Example:**

switch(config)# logging timestamp milliseconds

Sets the logging time-stamp units. By default, the units are seconds.

**Note**

This command applies to logs that are kept in the switch. It does not apply to the external logging server.

Step 8

(Optional) **show logging timestamp**

**Example:**

switch(config)# show logging timestamp

Displays the logging time-stamp units configured.

Step 9

(Optional) **copy running-config startup-config**

**Example:**

switch(config)# copy running-config startup-config

Copies the running configuration to the startup configuration.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong> switch(config)# logging server 192.0.2.253</td>
<td>limit logging of messages to a particular VRF by using the <code>use-vrf</code> keyword. Severity levels range from 0 to 7:</td>
</tr>
<tr>
<td><strong>Example:</strong> switch(config)# logging server 2001::)db*::3 5 use-vrf red</td>
<td>• 0 – emergency</td>
</tr>
<tr>
<td></td>
<td>• 1 – alert</td>
</tr>
<tr>
<td></td>
<td>• 2 – critical</td>
</tr>
<tr>
<td></td>
<td>• 3 – error</td>
</tr>
<tr>
<td></td>
<td>• 4 – warning</td>
</tr>
<tr>
<td></td>
<td>• 5 – notification</td>
</tr>
<tr>
<td></td>
<td>• 6 – informational</td>
</tr>
<tr>
<td></td>
<td>• 7 – debugging</td>
</tr>
<tr>
<td></td>
<td>The default outgoing facility is local7.</td>
</tr>
<tr>
<td></td>
<td>The no option removes the logging server for the specified host.</td>
</tr>
<tr>
<td></td>
<td>The first example forwards all messages on facility local 7. The second example forwards messages with severity level 5 or lower for VRF red.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Required:</strong> <code>logging source-interface loopback virtual-interface</code></td>
</tr>
<tr>
<td><strong>Example:</strong> switch(config)# logging source-interface loopback 5</td>
<td>Enables a source interface for the remote syslog server. The range for the <code>virtual-interface</code> argument is from 0 to 1023.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>(Optional) show logging server</strong></td>
</tr>
<tr>
<td><strong>Example:</strong> switch(config)# show logging server</td>
<td>Displays the syslog server configuration.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>(Optional) copy running-config startup-config</strong></td>
</tr>
<tr>
<td><strong>Example:</strong> switch(config)# copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>
## Configuring Secure Syslog Servers

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch# configure terminal switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>[no] logging server host [severity-level [port port-number]] [secure [trustpoint client-identity trustpoint-name]] [use-vrf vrf-name]]</code></td>
<td>Configures a syslog server at the specified hostname or IPv4 or IPv6 address. Optionally, you can enforce mutual authentication by installing the client identity certificate that is signed by any CA and using the trustpoint client-identity option. The default destination port for a secure TLS connection is 6514.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config)# logging server 192.0.2.253 secure</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config)# logging server 2001::3 5 secure trustpoint client-identity myCA use-vrf red</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>(Optional) logging source-interface interface name</code></td>
<td>Enables a source interface for the remote syslog server.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config)# logging source-interface lo0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>(Optional) show logging server</code></td>
<td>Displays the syslog server configuration. If the secure option is configured, the output will have an entry with the transport information. By default, the transport is UDP if the secure option is not configured.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config)# show logging server</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>(Optional) copy running-config startup-config</code></td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config)# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring the CA Certificate

For the secure syslog feature support, the remote servers must be authenticated via a trustpoint configuration.
Enrolling the CA Certificate

For mutual authentication, where the remote server wants the NX-OS switch (the client) to identify, that the peer authentication is mandatory, this is an additional configuration to enroll the certificate on the switch.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: switch# configure terminal switch(config)#</td>
<td></td>
</tr>
<tr>
<td>[no] crypto ca trustpoint trustpoint-name</td>
<td>Configures a trustpoint.</td>
</tr>
<tr>
<td>Example: switch(config)# crypto ca trustpoint winca switch(config-trustpoint)#</td>
<td>Note: You must configure the ip domain-name before the trustpoint configuration.</td>
</tr>
<tr>
<td>Required: crypto ca authenticate trustpoint-name</td>
<td>Configures a CA certificate for the trustpoint.</td>
</tr>
<tr>
<td>Example: switch(config-trustpoint)# crypto ca authenticate winca</td>
<td></td>
</tr>
<tr>
<td>(Optional) show crypto ca certificate</td>
<td>Displays the configured certificate/chain and the associated trustpoint.</td>
</tr>
<tr>
<td>Example: switch(config)# show crypto ca certificates</td>
<td></td>
</tr>
<tr>
<td>(Optional) copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration so that the trustpoint is persistent across the reload of the device.</td>
</tr>
<tr>
<td>Example: switch(config)# copy running-config startup-config</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td><code>switch(config-trustpoint)# crypto key generate rsa label myKey exportable modulus 2048</code></td>
<td>Configures a trustpoint.</td>
</tr>
</tbody>
</table>

**Step 3**

**Example:**

```
switch(config)# crypto ca trustpoint myCA
switch(config-trustpoint)#
```

*Note:* You must configure the ip domain-name before the trustpoint configuration.

**Step 4**

**Required:** `rsakeypair key-name`

**Example:**

```
switch(config-trustpoint)# rsakeypair myKey
```

Associates the keypair generated to the trustpoint CA.

**Step 5**

**Example:**

```
switch(config)# crypto ca authenticate myCA
```

Configures a CA certificate for the trustpoint.

**Step 6**

**Example:**

```
switch(config)# crypto ca enroll myCA
```

Generate an identity certificate of the switch to enroll it to a CA.

**Step 7**

**Example:**

```
switch(config-trustpoint)# crypto ca import myCA certificate
```

Imports the identity certificate signed by the CA to the switch.

**Step 8**

(Optional) **Example:**

```
switch# show crypto ca certificates
```

Displays the configured certificate or chain and the associated trustpoint.

**Step 9**

**Required:** `copy running-config startup-config`

**Example:**

```
switch# copy running-config startup-config
```

Copies the running configuration to the startup configuration.

---

**Configuring Syslog Servers on a UNIX or Linux System**

You can configure a syslog server on a UNIX or Linux system by adding the following line to the `/etc/syslog.conf` file:

```
facility.level <five tab characters> action
```

The following table describes the syslog fields that you can configure.
### Table 10: Syslog fields in syslog.conf

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facility</td>
<td>Creator of the message, which can be auth, authpriv, cron, daemon, kern, lpr, mail, mark, news, syslog, user, local0 through local7, or an asterisk (*) for all. These facility designators allow you to control the destination of messages based on their origin.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Check your configuration before using a local facility.</td>
</tr>
<tr>
<td>Level</td>
<td>Minimum severity level at which messages are logged, which can be debug, info, notice, warning, err, crit, alert, emerg, or an asterisk (*) for all. You can use none to disable a facility.</td>
</tr>
<tr>
<td>Action</td>
<td>Destination for messages, which can be a filename, a hostname preceded by the at sign (@), a comma-separated list of users, or an asterisk (*) for all logged-in users.</td>
</tr>
</tbody>
</table>

#### Procedure

**Step 1**  
Log debug messages with the local7 facility in the file `/var/log/myfile.log` by adding the following line to the `/etc/syslog.conf` file:

**Example:**

debug.local7 var/log/myfile.log

**Step 2**  
Create the log file by entering these commands at the shell prompt:

**Example:**

```
$ touch /var/log/myfile.log
$ chmod 666 /var/log/myfile.log
```

**Step 3**  
Make sure the system message logging daemon reads the new changes by checking `myfile.log` after entering this command:

**Example:**

```
$ kill -HUP ~cat /etc/syslog.pid~
```

### Displaying and Clearing Log Files

You can display or clear messages in the log file and the NVRAM.
Verifying the System Message Logging Configuration

To display system message logging configuration information, perform one of the following tasks:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show logging console</td>
<td>Displays the console logging configuration.</td>
</tr>
<tr>
<td>show logging info</td>
<td>Displays the logging configuration.</td>
</tr>
<tr>
<td>show logging last number-lines</td>
<td>Displays the last number of lines of the log file.</td>
</tr>
<tr>
<td>show logging level [facility]</td>
<td>Displays the facility logging severity level configuration.</td>
</tr>
<tr>
<td>show logging logfile [start-time yyyy mmm dd hh:mm:ss] [end-time yyyy mmm dd hh:mm:ss]</td>
<td>Displays the messages in the log file.</td>
</tr>
<tr>
<td>show logging module</td>
<td>Displays the module logging configuration.</td>
</tr>
<tr>
<td>show logging monitor</td>
<td>Displays the monitor logging configuration.</td>
</tr>
<tr>
<td>show logging nvram [last number-lines]</td>
<td>Displays the messages in the NVRAM log.</td>
</tr>
</tbody>
</table>
### Command Table

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show logging origin-id</td>
<td>Displays the configured hostname, IP address, or text string that is appended to syslog messages that are sent to remote syslog servers.</td>
</tr>
<tr>
<td>show logging server</td>
<td>Displays the syslog server configuration.</td>
</tr>
<tr>
<td>show logging timestamp</td>
<td>Displays the logging time-stamp units configuration.</td>
</tr>
</tbody>
</table>

### Configuration Example for System Message Logging

This example shows how to configure system message logging:

```
configure terminal
logging console 3
logging monitor 3
logging logfile my_log 6
logging module 3
logging level aaa 2
logging timestamp milliseconds
logging server 172.28.254.253
logging server 172.28.254.254 5 facility local3
copy running-config startup-config
```

### Additional References

#### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>System messages</td>
<td><em>Cisco NX-OS System Messages Reference</em></td>
</tr>
</tbody>
</table>
Configuring Smart Call Home

This chapter describes how to configure the Smart Call Home feature of the Cisco NX-OS devices.

This chapter contains the following sections:

- About Smart Call Home, on page 91
- Licensing Requirements for Smart Call Home, on page 97
- Prerequisites for Smart Call Home, on page 97
- Guidelines and Limitations for Smart Call Home, on page 98
- Default Settings for Smart Call Home, on page 98
- Configuring Smart Call Home, on page 99
- Verifying the Smart Call Home Configuration, on page 112
- Configuration Examples for Smart Call Home, on page 113
- Additional References, on page 114

About Smart Call Home

Smart Call Home provides an email-based notification for critical system policies. A range of message formats are available for compatibility with pager services, standard email, or XML-based automated parsing applications. You can use this feature to page a network support engineer, email a Network Operations Center, or use Cisco Smart Call Home services to automatically generate a case with the Technical Assistance Center.

Smart Call Home offers the following features:

- Automatic execution and attachment of relevant CLI command output.
- Multiple message format options such as the following:
  - Short Text—Suitable for pagers or printed reports.
  - Full Text—Fully formatted message information suitable for human reading.
  - XML—Machine-readable format that uses Extensible Markup Language (XML) and Adaptive Messaging Language (AML) XML schema definition (XSD). The AML XSD is published on the Cisco.com website. The XML format enables communication with the Technical Assistance Center.
- Multiple concurrent message destinations. You can configure up to 50 email destination addresses for each destination profile.
Destination Profiles

A destination profile includes the following information:

- One or more alert groups—The group of alerts that trigger a specific Smart Call Home message if the alert occurs.
- One or more email destinations—The list of recipients for the Smart Call Home messages generated by alert groups assigned to this destination profile.
- Message format—The format for the Smart Call Home message (short text, full text, or XML).
- Message severity level—The Smart Call Home severity level that the alert must meet before Cisco NX-OS generates a Smart Call Home message to all email addresses in the destination profile. Cisco NX-OS does not generate an alert if the Smart Call Home severity level of the alert is lower than the message severity level set for the destination profile.

You can also configure a destination profile to allow periodic inventory update messages by using the inventory alert group that will send out periodic messages daily, weekly, or monthly.

Cisco NX-OS supports the following predefined destination profiles:

- CiscoTAC-1—Supports the Cisco-TAC alert group in XML message format. This profile is preconfigured with the callhome@cisco.com email contact, maximum message size, and message severity level 0. You cannot change any of the default information for this profile.
- full-text-destination—Supports the full text message format.
- short-text-destination—Supports the short text message format.

Smart Call Home Alert Groups

An alert group is a predefined subset of Smart Call Home alerts that are supported in all Cisco Nexus devices. Alert groups allow you to select the set of Smart Call Home alerts that you want to send to a predefined or custom destination profile. The device sends Smart Call Home alerts to email destinations in a destination profile only if that Smart Call Home alert belongs to one of the alert groups associated with that destination profile and if the alert has a Smart Call Home message severity at or above the message severity set in the destination profile.

The following table lists the supported alert groups and the default CLI command output included in Smart Call Home messages generated for the alert group.

<table>
<thead>
<tr>
<th>Alert Group</th>
<th>Description</th>
<th>Executed Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco-TAC</td>
<td>All critical alerts from the other alert groups destined for Smart Call Home.</td>
<td>Execute commands based on the alert group that originates the alert.</td>
</tr>
</tbody>
</table>
| Configuration | Periodic events related to configuration. | `show module`  
`show version` |
<table>
<thead>
<tr>
<th>Alert Group</th>
<th>Description</th>
<th>Executed Commands</th>
</tr>
</thead>
</table>
| Diagnostic      | Events generated by diagnostics.                                            | `show diagnostic result module all detail`
|                 |                                                                             | `show diagnostic result module `number` detail`                                    |
|                 |                                                                             | `show hardware`                                                                    |
|                 |                                                                             | `show logging last 200`                                                           |
|                 |                                                                             | `show module`                                                                      |
|                 |                                                                             | `show sprom all`                                                                   |
|                 |                                                                             | `show tech-support gold`                                                           |
|                 |                                                                             | `show tech-support ha`                                                             |
|                 |                                                                             | `show tech-support platform`                                                       |
|                 |                                                                             | `show version`                                                                     |
| EEM             | Events generated by EEM.                                                    | `show diagnostic result module all detail`
<p>|                 |                                                                             | <code>show diagnostic result module </code>number<code> detail</code>                                    |
|                 |                                                                             | <code>show module</code>                                                                      |
|                 |                                                                             | <code>show sprom all</code>                                                                   |
|                 |                                                                             | <code>show tech-support gold</code>                                                           |
|                 |                                                                             | <code>show tech-support ha</code>                                                             |
|                 |                                                                             | <code>show tech-support platform</code>                                                       |
| Environmental   | Events related to power, fan, and environment-sensing elements such as      | <code>show environment</code>                                                                 |
|                 | temperature alarms.                                                        | <code>show logging last 200</code>                                                           |
|                 |                                                                             | <code>show module</code>                                                                      |
|                 |                                                                             | <code>show version</code>                                                                     |
| Inventory       | Inventory status that is provided whenever a unit is cold booted or when    | <code>show inventory</code>                                                                   |
|                 | FRUs are inserted or removed. This alert is considered a noncritical event, | <code>show license usage</code>                                                               |
|                 | and the information is used for status and entitlement.                    | <code>show module</code>                                                                      |
|                 |                                                                             | <code>show sprom all</code>                                                                   |
|                 |                                                                             | <code>show system uptime</code>                                                               |
|                 |                                                                             | <code>show version</code>                                                                     |
| License         | Events related to licensing and license violations.                        | <code>show logging last 200</code>                                                           |</p>
<table>
<thead>
<tr>
<th>Alert Group</th>
<th>Description</th>
<th>Executed Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linecard hardware</td>
<td>Events related to standard or intelligent switching modules.</td>
<td>show diagnostic result module all detail &lt;br&gt;show diagnostic result module <em>number</em> detail &lt;br&gt;show hardware &lt;br&gt;show logging last 200 &lt;br&gt;show module &lt;br&gt;show sprom all &lt;br&gt;show tech-support ethpm &lt;br&gt;show tech-support gold &lt;br&gt;show tech-support ha &lt;br&gt;show tech-support platform &lt;br&gt;show version</td>
</tr>
<tr>
<td>Supervisor hardware</td>
<td>Events related to supervisor modules.</td>
<td>show diagnostic result module all detail &lt;br&gt;show hardware &lt;br&gt;show logging last 200 &lt;br&gt;show module &lt;br&gt;show sprom all &lt;br&gt;show tech-support ethpm &lt;br&gt;show tech-support gold &lt;br&gt;show tech-support ha &lt;br&gt;show tech-support platform &lt;br&gt;show version</td>
</tr>
<tr>
<td>Syslog port group</td>
<td>Events generated by the syslog PORT facility.</td>
<td>show license usage &lt;br&gt;show logging last 200</td>
</tr>
</tbody>
</table>
## Executed Commands

<table>
<thead>
<tr>
<th>Alert Group</th>
<th>Description</th>
<th>Executed Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>Events generated by failure of a software system that is critical to unit operation.</td>
<td>show diagnostic result module all detail show hardware show logging last 200 show module show sprom all show tech-support ethpm show tech-support gold show tech-support ha show tech-support platform</td>
</tr>
<tr>
<td>Test</td>
<td>User-generated test message.</td>
<td>show module show version</td>
</tr>
</tbody>
</table>

Smart Call Home maps the syslog severity level to the corresponding Smart Call Home severity level for syslog port group messages.

You can customize predefined alert groups to execute additional CLI `show` commands when specific events occur and send that `show` output with the Smart Call Home message.

You can add `show` commands only to full text and XML destination profiles. Short text destination profiles do not support additional `show` commands because they only allow 128 bytes of text.

### Smart Call Home Message Levels

Smart Call Home allows you to filter messages based on their level of urgency. You can associate each predefined or user-defined destination profile with a Smart Call Home threshold from 0 (least urgent) to 9 (most urgent). The default is 0 (all messages are sent).

Syslog severity levels are mapped to the Smart Call Home message level.

---

**Note**

Smart Call Home does not change the syslog message level in the message text.

The following table lists each Smart Call Home message level keyword and the corresponding syslog level for the syslog port alert group.

### Table 12: Severity and Syslog Level Mapping

<table>
<thead>
<tr>
<th>Smart Call Home Level</th>
<th>Keyword</th>
<th>Syslog Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>Catastrophic</td>
<td>N/A</td>
<td>Network-wide catastrophic failure.</td>
</tr>
</tbody>
</table>
### Obtaining Smart Call Home

If you have a service contract directly with Cisco, you can register for the Smart Call Home service. Smart Call Home analyzes Smart Call Home messages and provides background information and recommendations. For known issues, particularly online diagnostics failures, Automatic Service Requests are generated with the Cisco TAC.

Smart Call Home offers the following features:

- Continuous device health monitoring and real-time diagnostic alerts.
- Analysis of Smart Call Home messages and, if needed, Automatic Service Request generation, routed to the correct TAC team, including detailed diagnostic information to speed problem resolution.
- Secure message transport directly from your device, through an HTTP proxy server, or a downloadable Transport Gateway (TG). You can use a TG aggregation point to support multiple devices or in cases where security dictates that your devices may not be connected directly to the Internet.
- Web-based access to Smart Call Home messages and recommendations, inventory, and configuration information for all Smart Call Home devices. This feature provides access to associated field notices, security advisories, and end-of-life information.

You need the following information to register:

- The SMARTnet contract number for your device
- Your email address
- Your Cisco.com ID
Database Merge Guidelines

When you merge two Smart Call Home databases, the following guidelines apply:

- The merged database contains the following information:
  - A superset of all the destination profiles from the merging devices.
  - The destination profile email addresses and alert groups.
  - Other configuration information (for example, message throttling, or periodic inventory) present in the managing device.

- Destination profile names cannot be duplicated within the merging devices—even though the configurations are different, the names cannot be duplicated. If a profile name is duplicated, one of the duplicate profiles must first be deleted or the merger fails.

High Availability

Both stateful and stateless restarts are supported for Smart Call Home.

Virtualization Support

One instance of Smart Call Home is supported. You can register your contact information at the Smart Call Home web site at the following URL: https://supportforums.cisco.com/community/netpro/solutions/smart_services/smartcallhome

You can test Smart Call Home using the `callhome send` and `callhome test` commands.

Smart Call Home is virtual routing and forwarding (VRF) aware. You can configure Smart Call Home to use a particular VRF to reach the Smart Call Home SMTP server.

Licensing Requirements for Smart Call Home

<table>
<thead>
<tr>
<th>Product</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco NX-OS</td>
<td>Smart Call Home requires no license. Any feature not included in a license package is bundled with the nx-os image and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the Cisco NX-OS Licensing Guide.</td>
</tr>
</tbody>
</table>

Prerequisites for Smart Call Home

Smart Call Home has the following prerequisites:
• To send messages to an email address, you must first configure an email server. To send messages using HTTP, you must have access to an HTTPS server and have a valid certificate installed on the Cisco Nexus device.

• Your device must have IP connectivity to an email server or HTTPS server.

• You must first configure the contact name (SNMP server contact), phone, and street address information. This step is required to determine the origin of messages received.

• If you use Smart Call Home, you need an active service contract for the device that you are configuring.

### Guidelines and Limitations for Smart Call Home

Smart Call Home has the following configuration guidelines and limitations:

• If there is no IP connectivity or if the interface in the virtual routing and forwarding (VRF) instance to the profile destination is down, the device cannot send Smart Call Home messages.

• Smart Call Home operates with any SMTP server.

• You can configure up to five SMTP servers for Smart Call Home.

• Link up/down syslog messages do not trigger Smart Call Home messages or alert notifications.

### Default Settings for Smart Call Home

This table lists the default settings for Smart Call Home parameters.

**Table 13: Default Smart Call Home Parameters**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination message size for a message sent in full text format</td>
<td>2,500,000</td>
</tr>
<tr>
<td>Destination message size for a message sent in XML format</td>
<td>2,500,000</td>
</tr>
<tr>
<td>Destination message size for a message sent in short text format</td>
<td>4000</td>
</tr>
<tr>
<td>SMTP server port number if no port is specified</td>
<td>25</td>
</tr>
<tr>
<td>SMTP server priority if no priority is specified</td>
<td>50</td>
</tr>
<tr>
<td>Alert group association with profile</td>
<td>All for full-text-destination and short-text-destination profiles. The cisco-tac alert group for the CiscoTAC-1 destination profile.</td>
</tr>
<tr>
<td>Format type</td>
<td>XML</td>
</tr>
<tr>
<td>Smart Call Home message level</td>
<td>0 (zero)</td>
</tr>
</tbody>
</table>
Configuring Smart Call Home

Be aware that the Cisco NX-OS commands may differ from the Cisco IOS commands.

We recommend that you complete the Smart Call Home configuration procedures in the following sequence:

1. Configuring Contact Information, on page 99
2. Creating a Destination Profile, on page 101
3. Associating an Alert Group with a Destination Profile, on page 104
4. (Optional) Adding Show Commands to an Alert Group, on page 105
5. Enabling or Disabling Smart Call Home, on page 111
6. (Optional) Testing the Smart Call Home Configuration, on page 112

Configuring Contact Information

You must configure the email, phone, and street address information for Smart Call Home. You can optionally configure the contract ID, customer ID, site ID, and switch priority information.

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>switch# configure terminal</code> <code>switch(config)#</code></td>
<td></td>
</tr>
</tbody>
</table>

| Step 2    | `snmp-server contact sys-contact`  | Configures the SNMP sysContact. |
|           | Example: `switch(config)# snmp-server contact personname@companyname.com` |

| Step 3    | `callhome`  | Enters Smart Call Home configuration mode. |
|           | Example: `switch(config)# callhome` `switch(config-callhome)#` |

| Step 4    | `email-contact email-address`  | Configures the email address for the person primarily responsible for the device. |
|           | Example: |

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP proxy server use</td>
<td>Disabled and no proxy server configured</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>switch(config-callhome)# email-contact <a href="mailto:admin@Mycompany.com">admin@Mycompany.com</a></td>
<td>The <em>email-address</em> can be up to 255 alphanumeric characters in email address format.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> You can use any valid email address. The address cannot contain spaces.</td>
</tr>
<tr>
<td><em>Step 5</em> switch(config-callhome)# phone-contact</td>
<td>Configures the phone number in international phone number format for the person primarily responsible for the device. The <em>international-phone-number</em> can be up to 17 alphanumeric characters and must be in international phone number format.</td>
</tr>
<tr>
<td><em>Example:</em> switch(config-callhome)# phone-contact +1-800-123-4567</td>
<td><strong>Note</strong> The phone number cannot contain spaces. Use the plus (+) prefix before the number.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><em>Step 6</em> switch(config-callhome)# streetaddress 123 Anystreet st. Anytown,AnyWhere</td>
<td>Configures the street address as an alphanumeric string with white spaces for the person primarily responsible for the device. The <em>address</em> can be up to 255 alphanumeric characters. Spaces are accepted.</td>
</tr>
<tr>
<td><em>Example:</em> switch(config-callhome)# streetaddress 123 Anystreet st. Anytown,AnyWhere</td>
<td></td>
</tr>
<tr>
<td><em>Step 7</em> switch(config-callhome)# contract-id Contract5678</td>
<td>Configures the contract number for this device from the service agreement. The <em>contract-number</em> can be up to 255 alphanumeric characters in free format.</td>
</tr>
<tr>
<td><em>Example:</em> switch(config-callhome)# contract-id Contract5678</td>
<td></td>
</tr>
<tr>
<td><em>Step 8</em> switch(config-callhome)# customer-id Customer123456</td>
<td>Configures the customer number for this device from the service agreement. The <em>customer-number</em> can be up to 255 alphanumeric characters in free format.</td>
</tr>
<tr>
<td><em>Example:</em> switch(config-callhome)# customer-id Customer123456</td>
<td></td>
</tr>
<tr>
<td><em>Step 9</em> switch(config-callhome)# site-id Site1</td>
<td>Configures the site number for this device. The <em>site-number</em> can be up to 255 alphanumeric characters in free format.</td>
</tr>
<tr>
<td><em>Example:</em> switch(config-callhome)# site-id Site1</td>
<td></td>
</tr>
<tr>
<td><em>Step 10</em> switch(config-callhome)# switch-priority 3</td>
<td>Configures the switch priority for this device. The range is from 0 to 7, with 0 being the highest priority and 7 the lowest. The default is 7.</td>
</tr>
<tr>
<td><em>Example:</em> switch(config-callhome)# switch-priority 3</td>
<td></td>
</tr>
<tr>
<td><em>Step 11</em> switch(config-callhome)# commit</td>
<td>Commits the Smart Call Home configuration commands.</td>
</tr>
<tr>
<td><em>Example:</em> switch(config-callhome)# commit</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Smart Call Home

**Purpose**

- Displays a summary of the Smart Call Home configuration.

**Command or Action**

<table>
<thead>
<tr>
<th>Step 12</th>
<th>(Optional) <code>show callhome</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config-callhome)# show callhome</td>
<td></td>
</tr>
</tbody>
</table>

**Purpose**

- Copies the running configuration to the startup configuration.

**Command or Action**

<table>
<thead>
<tr>
<th>Step 13</th>
<th>(Optional) <code>copy running-config startup-config</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

### What to do next

Create a destination profile.

## Creating a Destination Profile

You can create a user-defined destination profile and configure its message format.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>switch# configure terminal</td>
</tr>
<tr>
<td></td>
<td>switch(config)#</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>callhome</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# callhome</td>
</tr>
<tr>
<td></td>
<td>switch(config-callhome)#</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>destination-profile name</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config-callhome)#</td>
</tr>
<tr>
<td></td>
<td>destination-profile Noc101</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>destination-profile name format {XML</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config-callhome)#</td>
</tr>
<tr>
<td></td>
<td>destination-profile Noc101 format full-txt</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>commit</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>

Sets the message format for the profile. The name can be any alphanumeric string up to 31 characters.

Commits the Smart Call Home configuration commands.
## Modifying a Destination Profile

You can modify the following attributes for a predefined or user-defined destination profile:

- **Destination email address**—The actual address, pertinent to the transport mechanism, to which the alert should be sent.
- **Destination URL**—The HTTP or HTTPS URL that defines where alerts should be sent.
- **Transport method**—The email or HTTP transport that determines which type of destination addresses are used.
- **Message formatting**—The message format used for sending the alert (full text, short text, or XML).
- **Message level**—The Smart Call Home message severity level for this destination profile.
- **Message size**—The allowed length of a Smart Call Home message sent to the email addresses in this destination profile.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>callhome</td>
<td>Enters Smart Call Home configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# callhome</td>
<td></td>
</tr>
<tr>
<td>switch(config-callhome)#</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
</tbody>
</table>
| 3    | **destination-profile** `{name | CiscoTAC-1 | full-txt-destination | short-txt-destination; email-addr address` | Configures an email address for a user-defined or predefined destination profile. You can configure up to 50 email addresses in a destination profile.  
   **Example:**  
   ```plaintext```switch(config-callhome)# destination-profile full-txt-destination email-addr person@place.com```plaintext``` |
| 4    | **destination-profile** `{name | CiscoTAC-1 | full-txt-destination | short-txt-destination; http address` | Configures an HTTP or HTTPS URL for a user-defined or predefined destination profile. The URL can be up to 255 characters.  
   **Example:**  
   ```plaintext```switch(config-callhome)# destination-profile CiscoTAC-1 http http://site.com/service/callhome```plaintext``` |
| 5    | **destination-profile** `{name | CiscoTAC-1 | full-txt-destination | short-txt-destination; transport-method {email | http}` | Configures an email or HTTP transport method for a user-defined or predefined destination profile. The type of transport method that you choose determines the configured destination addresses of that type.  
   **Example:**  
   ```plaintext```switch(config-callhome)# destination-profile CiscoTAC-1 transport-method http```plaintext``` |
| 6    | **destination-profile** `{name | CiscoTAC-1 | full-txt-destination | short-txt-destination; message-level number` | Configures the Smart Call Home message severity level for this destination profile. Cisco NX-OS sends only alerts that have a matching or higher Smart Call Home severity level to destinations in this profile. The range is from 0 to 9, where 9 is the highest severity level.  
   **Example:**  
   ```plaintext```switch(config-callhome)# destination-profile full-txt-destination message-level 5```plaintext``` |
| 7    | **destination-profile** `{name | CiscoTAC-1 | full-txt-destination | short-txt-destination; message-size number` | Configures the maximum message size for this destination profile. The range is from 0 to 5000000. The default is 2500000.  
   **Example:**  
   ```plaintext```switch(config-callhome)# destination-profile full-txt-destination message-size 100000```plaintext``` |
| 8    | **commit** | Commits the Smart Call Home configuration commands.  
   **Example:**  
   ```plaintext```switch(config-callhome)# commit```plaintext``` |
| 9    | (Optional) **show callhome destination-profile** [profile name] | Displays information about one or more destination profiles.  
   **Example:** |
Associating an Alert Group with a Destination Profile

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch(config-callhome)# show callhome</td>
<td></td>
</tr>
<tr>
<td>destination-profile profile</td>
<td></td>
</tr>
<tr>
<td>full-text-destination</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td></td>
</tr>
<tr>
<td>(Optional) copy running-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td>startup-config</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config)# copy running-config</td>
<td></td>
</tr>
<tr>
<td>startup-config</td>
<td></td>
</tr>
</tbody>
</table>

**What to do next**

Associate one or more alert groups with a destination profile.

**Example:**

- `copy running-config startup-config`
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show callhome</code></td>
<td></td>
</tr>
</tbody>
</table>

### Step 6

(Optional) `copy running-config startup-config`  

**Example:**

```plaintext
switch(config)# copy running-config startup-config
```

Copies the running configuration to the startup configuration.

---

### What to do next

Optionally add `show` commands to an alert group and then configure the SMTP email server.

---

### Adding Show Commands to an Alert Group

You can assign a maximum of five user-defined CLI `show` commands to an alert group.

#### Note

You cannot add user-defined CLI `show` commands to the CiscoTAC-1 destination profile.

---

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
| **Example:**

```
switch# configure terminal
switch(config)#
```

<table>
<thead>
<tr>
<th>Step 2</th>
<th><code>callhome</code></th>
<th>Enters Smart Call Home configuration mode.</th>
</tr>
</thead>
</table>
| **Example:**

```
switch(config)# callhome
switch(config-callhome)#
```

| Step 3 | `alert-group` {Configuration | Diagnostic | EEM | Environmental | Inventory | License | Supervisor-Hardware | Syslog-group-port | System | Test} user-def-cmd `show-cmd`  

**Example:**

```
switch(config-callhome)# alert-group Configuration user-def-cmd show-cmd show ip route
```

Adds the `show` command output to any Smart Call Home messages sent for this alert group. Only valid `show` commands are accepted.

| Step 4 | `commit`  
|--------|----------|
| **Example:**

```
switch(config-callhome)# commit
```

Commits the Smart Call Home configuration commands.
### Configuring the Email Server

You must configure the SMTP server address for the Smart Call Home functionality to work. You can also configure the from and reply-to email addresses.

You can configure up to five SMTP servers for Smart Call Home. The servers are tried based on their priority. The highest priority server is tried first. If the message fails to be sent, the next server in the list is tried until the limit is exhausted. If two servers have equal priority, the one that was configured earlier is tried first.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> callhome</td>
<td>Enters Smart Call Home configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# callhome</td>
<td></td>
</tr>
<tr>
<td>switch(config-callhome)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> transport email mail-server ip-address [port number] [priority number] [use-vrf vrf-name]</td>
<td>Configures the SMTP server as the domain name server (DNS) name, IPv4 address, or IPv6 address. Optionally configures the port number. The port range is from 1 to 65535. The default port number is 25. Also optionally configures the priority of the SMTP server. The priority range is from 1 to 100, with 1 being the highest priority and 100 the lowest. If you do not specify a priority, the default value of 50 is used.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config-callhome)# transport email mail-server 192.0.2.1 use-vrf Red</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step 4</th>
<th>(Optional) transport email from email-address</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config-callhome)# transport email from <a href="mailto:person@company.com">person@company.com</a></td>
</tr>
</tbody>
</table>

Configures the email from field for Smart Call Home messages.

<table>
<thead>
<tr>
<th>Step 5</th>
<th>(Optional) transport email reply-to email-address</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config-callhome)# transport email reply-to <a href="mailto:person@company.com">person@company.com</a></td>
</tr>
</tbody>
</table>

Configures the email reply-to field for Smart Call Home messages.

<table>
<thead>
<tr>
<th>Step 6</th>
<th>commit</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config-callhome)# commit</td>
</tr>
</tbody>
</table>

Commits the Smart Call Home configuration commands.

<table>
<thead>
<tr>
<th>Step 7</th>
<th>(Optional) show callhome transport</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config-callhome)# show callhome transport</td>
</tr>
</tbody>
</table>

Displays the transport-related configuration for Smart Call Home.

<table>
<thead>
<tr>
<th>Step 8</th>
<th>(Optional) copy running-config startup-config</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config)# copy running-config startup-config</td>
</tr>
</tbody>
</table>

Copies the running configuration to the startup configuration.

### What to do next

Optionally use VRFs to send Smart Call Home messages over HTTP.

### Configuring VRFs To Send Messages Using HTTP

You can use VRFs to send Smart Call Home messages over HTTP. If HTTP VRFs are not configured, the default VRF is used to transport messages over HTTP.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
| **Example:** | switch# configure terminal  
switch(config)# |
### Configuring Smart Call Home

**Purpose**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2 callhome</td>
<td>Enters Smart Call Home configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# callhome</td>
<td></td>
</tr>
<tr>
<td>switch(config-callhome)#</td>
<td></td>
</tr>
<tr>
<td>Step 3 transport http use-vrf vrf-name</td>
<td>Configures the VRF used to send email and other Smart Call Home messages over HTTP.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config-callhome)# transport http use-vrf Blue</td>
<td></td>
</tr>
<tr>
<td>Step 4 commit</td>
<td>Commits the Smart Call Home configuration commands.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config-callhome)# commit</td>
<td></td>
</tr>
<tr>
<td>Step 5 (Optional) show callhome</td>
<td>Displays information about Smart Call Home.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config-callhome)# show callhome</td>
<td></td>
</tr>
<tr>
<td>Step 6 (Optional) copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

**What to do next**

Optionally configure Smart Call Home to send HTTP messages through an HTTP proxy server.

### Configuring an HTTP Proxy Server

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td>Step 2 callhome</td>
<td>Enters Smart Call Home configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# callhome</td>
<td></td>
</tr>
<tr>
<td>switch(config-callhome)#</td>
<td></td>
</tr>
<tr>
<td>Step 3 transport http proxy server ip-address [port number]</td>
<td>Configures the HTTP proxy server domain name server (DNS) name, IPv4 address, or IPv6 address. Optionally configures the port number.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Periodic Inventory Notifications

You can configure the device to periodically send a message with an inventory of all software services currently enabled and running on the device along with hardware inventory information. The device generates two Smart Call Home notifications: periodic configuration messages and periodic inventory messages.

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

**What to do next**

Optionally configure your device to periodically send inventory notifications.
### Configuring Smart Call Home

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Command or Action</strong></td>
</tr>
<tr>
<td><strong>callhome</strong></td>
<td>Enters Smart Call Home configuration mode.</td>
</tr>
</tbody>
</table>
| **Example:** | switch(config)# callhome  
switch(config-callhome)# |
| **Step 3** | **Command or Action** | **Purpose** |
| **periodic-inventory notification [interval **days**] [timeofday **time**]** | Configures periodic inventory messages. The interval range is from 1 to 30 days, and the default is 7 days. The **time** argument is in HH:MM format. It defines at what time of the day every **X** days an update is sent (where **X** is the update interval). |
| **Example:** | switch(config-callhome)# periodic-inventory notification interval 20 |
| **Step 4** | **Command or Action** | **Purpose** |
| **commit** | Commits the Smart Call Home configuration commands. |
| **Example:** | switch(config-callhome)# commit |
| **Step 5** | **Command or Action** | **Purpose** |
| **(Optional) show callhome** | Displays information about Smart Call Home. |
| **Example:** | switch(config-callhome)# show callhome |
| **Step 6** | **Command or Action** | **Purpose** |
| **(Optional) copy running-config startup-config** | Copies the running configuration to the startup configuration. |
| **Example:** | switch(config)# copy running-config startup-config |

### What to do next

Optionally disable duplicate message throttling.

### Disabling Duplicate Message Throttling

You can limit the number of duplicate messages received for the same event. By default, the device limits the number of duplicate messages received for the same event. If the number of duplicate messages sent exceeds 30 messages within a 2-hour time frame, the device discards further messages for that alert type.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Command or Action</strong></td>
</tr>
<tr>
<td><strong>configure terminal</strong></td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
| **Example:** | switch# configure terminal  
switch(config)# |
| **Step 2** | **Command or Action** | **Purpose** |
| **callhome** | Enters Smart Call Home configuration mode. |
| **Example:** | switch(config)# callhome  
switch(config-callhome)# |
### Enabling or Disabling Smart Call Home

Once you have configured the contact information, you can enable the Smart Call Home function.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
configure terminal
Example:
switch# configure terminal
switch(config)# | Enters global configuration mode. |
| **Step 2**
callhome
Example:
switch(config)# callhome
switch(config-callhome)# | Enters Smart Call Home configuration mode. |
| **Step 3**
[no] enable
Example:
switch(config-callhome)# enable | Enables or disables Smart Call Home.
Smart Call Home is disabled by default. |
| **Step 4**
commit
Example:
switch(config-callhome)# commit | Commits the Smart Call Home configuration commands. |
Testing the Smart Call Home Configuration

You can generate a test message to test your Smart Call Home communications.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

**Step 5**

(Optional) copy running-config startup-config

Example:

```
switch(config)# copy running-config startup-config
```

What to do next

Optionally generate a test message.

Verifying the Smart Call Home Configuration

To display Smart Call Home configuration information, perform one of the following tasks:
### Configuration Examples for Smart Call Home

This example shows how to create a destination profile called Noc101, associate the Configuration alert group to that profile, configure contact and email information, and specify the VRF used to send Smart Call Home messages over HTTP:

```con
configure terminal
callhome
distribute
snmp-server contact person@company.com
destination-profile Noc101 format full-txt
destination-profile full-text-destination email-addr person@company.com
destination-profile full-text-destination message-level 5
destination-profile Noc101 alert-group Configuration
alert-group Configuration user-def-cmds show ip route
transport email mail-server 192.0.2.10 priority 1
transport http use-vrf Blue
enable
commit
```

This example shows how to configure multiple SMTP servers for Smart Call Home messages:

```con
configure terminal
callhome
distribute
transport email mail-server 192.0.2.10 priority 4
transport email mail-server 172.21.34.193
transport email smtp-server 10.1.1.174
transport email mail-server 64.72.101.213 priority 60
transport email from person@company.com
transport email reply-to person@company.com
enable
commit
```

Based on the configuration above, the SMTP servers would be tried in this order:

- 10.1.1.174 (priority 0)
- 192.0.2.10 (priority 4)

### Table: Commands and Purposes

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show callhome</td>
<td>Displays the Smart Call Home configuration.</td>
</tr>
<tr>
<td>show callhome destination-profile name</td>
<td>Displays one or more Smart Call Home destination profiles.</td>
</tr>
<tr>
<td>show callhome transport</td>
<td>Displays the transport-related configuration for Smart Call Home.</td>
</tr>
<tr>
<td>show callhome user-def-cmds</td>
<td>Displays CLI commands added to any alert groups.</td>
</tr>
<tr>
<td>show running-config callhome [all]</td>
<td>Displays the running configuration for Smart Call Home.</td>
</tr>
<tr>
<td>show startup-config callhome</td>
<td>Displays the startup configuration for Smart Call Home.</td>
</tr>
<tr>
<td>show tech-support callhome</td>
<td>Displays the technical support output for Smart Call Home.</td>
</tr>
</tbody>
</table>
172.21.34.193 (priority 50, which is the default)
64.72.101.213 (priority 60)

The `transport email smtp-server` command has a priority of 0, which is the highest. The server specified by this command is tried first followed by the servers specified by the `transport email mail-server` commands in order of priority.

This example shows how to configure Smart Call Home to send HTTP messages through an HTTP proxy server:

```
configure terminal
callhome
transport http proxy server 10.10.10.1 port 4
transport http proxy enable
commit
```

### Additional References

#### Event Triggers

The following table lists the event triggers and their Smart Call Home message severity levels.

<table>
<thead>
<tr>
<th>Alert Group</th>
<th>Event Name</th>
<th>Description</th>
<th>Smart Call Home Severity Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration</td>
<td>PERIODIC_CONFIGURATION</td>
<td>Periodic configuration update message.</td>
<td>2</td>
</tr>
<tr>
<td>Diagnostic</td>
<td>DIAGNOSTIC_MAJOR_ALERT</td>
<td>GOLD generated a major alert.</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>DIAGNOSTIC_MINOR_ALERT</td>
<td>GOLD generated a minor alert.</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>DIAGNOSTIC_NORMAL_ALERT</td>
<td>Smart Call Home generated a normal diagnostic alert.</td>
<td>2</td>
</tr>
<tr>
<td>Environmental and CISCO_TAC</td>
<td>FAN_FAILURE</td>
<td>Cooling fan has failed.</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>POWER_SUPPLY_ALERT</td>
<td>Power supply warning has occurred.</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>POWER_SUPPLY_FAILURE</td>
<td>Power supply has failed.</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>POWER_SUPPLY_SHUTDOWN</td>
<td>Power supply has shut down.</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>TEMPERATURE_ALARM</td>
<td>Thermal sensor going bad.</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>TEMPERATURE_MAJOR_ALARM</td>
<td>Thermal sensor indicates temperature has reached operating major threshold.</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>TEMPERATURE_MINOR_ALARM</td>
<td>Thermal sensor indicates temperature has reached operating minor threshold.</td>
<td>4</td>
</tr>
</tbody>
</table>
## Event Triggers

<table>
<thead>
<tr>
<th>Alert Group</th>
<th>Event Name</th>
<th>Description</th>
<th>Smart Call Home Severity Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory and CISCO_TAC</td>
<td>COLD_BOOT</td>
<td>Switch is powered up and reset to a cold boot sequence.</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>HARDWARE_INSERTION</td>
<td>New piece of hardware has been inserted into the chassis.</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>HARDWARE_REMOVAL</td>
<td>Hardware has been removed from the chassis.</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>PERIODIC_INVENTORY</td>
<td>Periodic inventory message has been generated.</td>
<td>2</td>
</tr>
<tr>
<td>License</td>
<td>LICENSE_VIOLATION</td>
<td>Feature in use is not licensed and is turned off after grace period expiration.</td>
<td>6</td>
</tr>
<tr>
<td>Line module Hardware and</td>
<td>LINE module_FAILURE</td>
<td>Module operation has failed.</td>
<td>7</td>
</tr>
<tr>
<td>CISCO_TAC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supervisor Hardware and</td>
<td>SUP_FAILURE</td>
<td>Supervisor module operation has failed.</td>
<td>7</td>
</tr>
<tr>
<td>CISCO_TAC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Syslog-group-port</td>
<td>PORT_FAILURE</td>
<td>syslog message that corresponds to the port facility has been generated.</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>SYSLOG_ALERT</td>
<td>syslog alert message has been generated.</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> Link up/down syslog messages do not trigger Smart Call Home messages or alert notifications.</td>
<td></td>
</tr>
<tr>
<td>System and CISCO_TAC</td>
<td>SW_CRASH</td>
<td>Software process has failed with a stateless restart, indicating an interruption of a service. Messages are sent for process crashes on supervisor modules.</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>SW_SYSTEM_INCONSISTENT</td>
<td>Inconsistency has been detected in software or file system.</td>
<td>5</td>
</tr>
<tr>
<td>Test and CISCO_TAC</td>
<td>TEST</td>
<td>User generated test has occurred.</td>
<td>2</td>
</tr>
</tbody>
</table>
# Message Formats

Smart Call Home supports the following message formats:

## Short Text Message Format

The following table describes the short text formatting option for all message types.

<table>
<thead>
<tr>
<th>Data Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device identification</td>
<td>Configured device name</td>
</tr>
<tr>
<td>Date/time stamp</td>
<td>Time stamp of the triggering event</td>
</tr>
<tr>
<td>Error isolation message</td>
<td>Plain English description of triggering event</td>
</tr>
<tr>
<td>Alarm urgency level</td>
<td>Error level such as that applied to system message</td>
</tr>
</tbody>
</table>

## Common Event Message Fields

The following table describes the first set of common event message fields for full text or XML messages.

<table>
<thead>
<tr>
<th>Data Item (Plain Text and XML)</th>
<th>Description (Plain Text and XML)</th>
<th>XML Tag (XML Only)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timestamp</td>
<td>Date and time stamp of event in ISO time notation: YYYY-MM-DD HH:MM:SS GMT+HH:MM.</td>
<td>/aml/header/time</td>
</tr>
<tr>
<td>Message name</td>
<td>Name of message.</td>
<td>/aml/header/name</td>
</tr>
<tr>
<td>Message type</td>
<td>Name of message type, such as reactive or proactive.</td>
<td>/aml/header/type</td>
</tr>
<tr>
<td>Message group</td>
<td>Name of alert group, such as syslog.</td>
<td>/aml/header/group</td>
</tr>
<tr>
<td>Severity level</td>
<td>Severity level of message.</td>
<td>/aml/header/level</td>
</tr>
<tr>
<td>Source ID</td>
<td>Product type for routing, such as the Cisco Nexus 9000 Series switch.</td>
<td>/aml/header/source</td>
</tr>
</tbody>
</table>
### Data Item (Plain Text and XML) | Description (Plain Text and XML) | XML Tag (XML Only)
---|---|---
Device ID | Unique device identifier (UDI) for the end device that generated the message. This field should be empty if the message is nonspecific to a device. The format is type@Sid@serial.  
• *type* is the product model number from the backplane IDPROM.  
• *@* is a separator character.  
• *Sid* is C, identifying the serial ID as a chassis serial number.  
• *serial* is the number identified by the Sid field.  
   An example is N9K-C9508@C@12345678. | /aml/ header/deviceId
Customer ID | Optional user-configurable field used for contract information or other ID by any support service. | /aml/ header/customerID
Contract ID | Optional user-configurable field used for contract information or other ID by any support service. | /aml/ header /contractId
Site ID | Optional user-configurable field used for Cisco-supplied site ID or other data meaningful to alternate support service. | /aml/ header/siteId
Server ID | If the message is generated from the device, this ID is the unique device identifier (UDI) of the device. The format is type@Sid@serial.  
• *type* is the product model number from the backplane IDPROM.  
• *@* is a separator character.  
• *Sid* is C, identifying the serial ID as a chassis serial number.  
• *serial* is the number identified by the Sid field.  
   An example is N9K-C9508@C@12345678. | /aml/ header/serverId
Message description | Short text that describes the error. | /aml/body/msgDesc
### Alert Group Message Fields

The following table describes the fields specific to alert group messages for full text and XML. These fields may be repeated if multiple CLI commands are executed for an alert group.

<table>
<thead>
<tr>
<th>Data Item (Plain Text and XML)</th>
<th>Description (Plain Text and XML)</th>
<th>XML Tag (XML Only)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command output name</td>
<td>Exact name of the issued CLI command.</td>
<td>/aml/attachments/attachment/name</td>
</tr>
<tr>
<td>Attachment type</td>
<td>Specific command output.</td>
<td>/aml/attachments/attachment/type</td>
</tr>
<tr>
<td>MIME type</td>
<td>Either plain text or encoding type.</td>
<td>/aml/attachments/attachment/mime</td>
</tr>
<tr>
<td>Command output text</td>
<td>Output of command automatically executed.</td>
<td>/aml/attachments/attachment/ataData</td>
</tr>
</tbody>
</table>

### Fields for Reactive and Proactive Event Messages

The following table describes the reactive and proactive event message format for full text or XML messages.

<table>
<thead>
<tr>
<th>Data Item (Plain Text and XML)</th>
<th>Description (Plain Text and XML)</th>
<th>XML Tag (XML Only)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis hardware version</td>
<td>Hardware version of chassis.</td>
<td>/aml/body/chassis/hwVersion</td>
</tr>
<tr>
<td>Supervisor module software version</td>
<td>Top-level software version.</td>
<td>/aml/body/chassis/swVersion</td>
</tr>
</tbody>
</table>
The following table describes the inventory event message format for full text or XML messages.

<table>
<thead>
<tr>
<th>Data Item (Plain Text and XML)</th>
<th>Description (Plain Text and XML)</th>
<th>XML Tag (XML Only)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected FRU name</td>
<td>Name of the affected FRU that is generating the event message.</td>
<td>/aml/body/fru/name</td>
</tr>
<tr>
<td>Affected FRU serial number</td>
<td>Serial number of the affected FRU.</td>
<td>/aml/body/fru/serialNo</td>
</tr>
<tr>
<td>Affected FRU part number</td>
<td>Part number of the affected FRU.</td>
<td>/aml/body/fru/partNo</td>
</tr>
<tr>
<td>FRU slot</td>
<td>Slot number of the FRU that is generating the event message.</td>
<td>/aml/body/fru/slot</td>
</tr>
<tr>
<td>FRU hardware version</td>
<td>Hardware version of the affected FRU.</td>
<td>/aml/body/fru/hwVersion</td>
</tr>
<tr>
<td>FRU software version</td>
<td>Software version(s) that is running on the affected FRU.</td>
<td>/aml/body/fru/swVersion</td>
</tr>
</tbody>
</table>

The following table describes the user-generated test message format for full text or XML.

<table>
<thead>
<tr>
<th>Data Item (Plain Text and XML)</th>
<th>Description (Plain Text and XML)</th>
<th>XML Tag (XML Only)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process ID</td>
<td>Unique process ID.</td>
<td>/aml/body/process/id</td>
</tr>
<tr>
<td>Process state</td>
<td>State of process (for example, running or halted).</td>
<td>/aml/body/process/processState</td>
</tr>
<tr>
<td>Process exception</td>
<td>Exception or reason code.</td>
<td>/aml/body/process/processException</td>
</tr>
</tbody>
</table>

Fields for Inventory Event Messages

Fields for User-Generated Test Messages
Sample Syslog Alert Notification in Full-Text Format

This sample shows the full-text format for a syslog port alert-group notification:

Severity Level: 5
Series: Nexus9000
Switch Priority: 0
Device Id: N9K-C9508@C@TXX12345678
Server Id: N9K-C9508@C@TXX12345678
Time of Event: 2013-05-17 16:31:33 GMT+0000 Message Name: syslog
System Name: dc3-test
Contact Name: Jay Tester
Contact Email: contact@example.com
Contact Phone: +91-80-1234-5678
Street Address: #1 Any Street
Event Description: SYSLOG_ALERT 2013 May 17 16:31:33 dc3-test %ETHPORT-2-IF_SEQ_ERROR: Error (0x20) while communicating with component MTS_SAP_ELTM opcode: MTS_OPC_ETHPM_PORT_PHY_CLEANUP (for: RID_PORT: Ethernet3/1)

syslog_facility: ETHPORT
start chassis information:
Affected Chassis: N9K-C9508
Affected Chassis Serial Number: TXX12345678
Affected Chassis Hardware Version: 0.405
Affected Chassis Software Version: 6.1(2)
Affected Chassis Part No: 11-11111-11
end chassis information:
start attachment
name: show logging logfile | tail -n 200
type: text
data:
2013 May 17 10:57:51 dc3-test %SYSLOG-1-SYSTEM_MSG: Logging logfile (messages) cleared by user
2013 May 17 10:57:53 dc3-test %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from /dev/ttySO /dev/ttySO_console
2013 May 17 10:58:35 dc3-test %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from /dev/ttySO /dev/ttySO_console
2013 May 17 10:59:00 dc3-test %DAEMON-3-SYSTEM_MSG: error: setsockopt IP_TOS 16: Invalid argument: - sshd[14484]
2013 May 17 10:59:05 dc3-test %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from /dev/ttySO /dev/ttySO_console
2013 May 17 12:11:18 dc3-test %SYSMGR-3-BASIC_TRACE: core_copy: PID 2579 with message Core not generated by system for eltm(0). WCOREDUMP(9) returned zero
2013 May 17 16:28:03 dc3-test %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from /dev/ttySO /dev/ttySO_console
2013 May 17 16:28:44 dc3-test %SYSMGR-3-BASIC_TRACE: core_copy: PID 2579 with message Core not generated by system for eltm(0). WCOREDUMP(9) returned zero
2013 May 17 16:28:44 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID 3504) hasn't caught signal 9 (no core).
2013 May 17 16:29:08 dc3-test %SYSMGR-3-BASIC_TRACE: core_copy: PID 2579 with message Core not generated by system for eltm(0). WCOREDUMP(9) returned zero
2013 May 17 16:29:08 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID 23210) hasn't caught signal 9 (no core).
2013 May 17 16:29:25 dc3-test %SYSMGR-2-HASWITCHOVER_PRE_START: This supervisor is becoming active (pre-start phase).
2013 May 17 16:29:25 dc3-test %SYSMGR-2-HASWITCHOVER_START: This supervisor is becoming active.
2013 May 17 16:29:26 dc3-test %USER-3-SYSTEM_MSG: crdcfg_get_srvinfo: mts_send failed - device test
2013 May 17 16:29:27 dc3-test %NETSTACK-3-IP_UNK_MSG_MAJOR: netstack [4336] Unrecognized message from MRIB. Major type 1807

2013 May 17 16:29:27 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is DOWN
2013 May 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:socket family : 2 - ntpd[19045]
2013 May 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:socket family : 10 - ntpd[19045]

2013 May 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:ipv6 only defined - ntpd[19045]
2013 May 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:bindv6 only defined - ntpd[19045]

recovery failed (0)
recovery failed (0)
2013 May 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ssh disabled, removing - dcos-xinetd[19077]
2013 May 17 16:29:29 dc3-test %DAEMON-3-SYSTEM_MSG: Telnet disabled, removing - dcos-xinetd[19077]
2013 May 17 16:29:31 dc3-test %DAEMON-3-SYSTEM_MSG: Telnet disabled, removing - dcos-xinetd[19078]
2013 May 17 16:29:32 dc3-test %DAEMON-3-SYSTEM_MSG: ssh disabled, removing - dcos-xinetd[19078]
2013 May 17 16:29:34 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is UP

2013 May 17 16:29:46 dc3-test vsh[19166]: CLIC-3-FAILED_EXEC: Can not exec command <more>
return code <14>
2013 May 17 16:30:24 dc3-test vsh[23810]: CLIC-3-FAILED_EXEC: Can not exec command <more>
return code <14>
2013 May 17 16:30:24 dc3-test vsh[23803]: CLIC-3-FAILED_EXEC: Can not exec command <more>
return code <14>
2013 May 17 16:30:24 dc3-test vsh[23818]: CLIC-3-FAILED_EXEC: Can not exec command <more>
return code <14>
2013 May 17 16:30:47 dc3-test %SYSMGR-3-BASIC_TRACE: core_copy: PID 2630 with message
Core not generated by system for eltm(0). WCOREDUMP(9) returned zero .
2013 May 17 16:30:47 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID 4820) hasn't
captured signal 9 (no core).
2013 May 17 16:31:02 dc3-test %SYSMGR-3-BASIC_TRACE: core_copy: PID 2630 with message
Core not generated by system for eltm(0). WCOREDUMP(9) returned zero .
2013 May 17 16:31:02 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID 24239)
hasn't captured signal 9 (no core).
2013 May 17 16:31:14 dc3-test %SYSMGR-3-BASIC_TRACE: core_copy: PID 2630 with message
Core not generated by system for eltm(0). WCOREDUMP(9) returned zero .
2013 May 17 16:31:14 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID 24401)
hasn't captured signal 9 (no core).
2013 May 17 16:31:23 dc3-test %CALLHOME-2-EVENT: SW CRASH alert for service: eltm
2013 May 17 16:31:23 dc3-test %SYSMGR-3-BASIC_TRACE: core_copy: PID 2630 with message
Core not generated by system for eltm(0). WCOREDUMP(9) returned zero .
2013 May 17 16:31:23 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID 24407)
hasn't captured signal 9 (no core).
2013 May 17 16:31:24 dc3-test vsh[24532]: CLIC-3-FAILED_EXEC: Can not exec command <more>
return code <14>
2013 May 17 16:31:24 dc3-test vsh[24548]: CLIC-3-FAILED_EXEC: Can not exec command <more>
return code <14>
Sample Syslog Alert Notification in XML Format

This sample shows the XML format for a syslog port alert-group notification:

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<soap-env:Envelope xmlns:soap-env="http://www.w3.org/2003/05/soap-envelope">
  <soap-env:Header>
      soap-env:mustUnderstand="true"
      soap-env:role="http://www.w3.org/2003/05/soap-envelope/role/next">
      <aml-session:To>http://tools.cisco.com/neddce/services/DDCEService</aml-session:To>
      <aml-session:Path>
        <aml-session:Via>http://www.cisco.com/appliance/uri</aml-session:Via>
      </aml-session:Path>
      <aml-session:MessageId>1004:TXX12345678:478F82E6</aml-session:MessageId>
    </aml-session:Session>
  </soap-env:Header>
  <soap-env:Body>
      <aml-block:Header>
        <aml-block:Name>show license usage</aml-block:Name>
        <aml-block:data>
          Feature Ins Lic Status Expiry Date Comments
          Count
          -------------------------------------------
          LAN_ENTERPRISE_SERVICES_PKG Yes - Unused Never -
          -------------------------------------------
        </aml-block:data>
      </aml-block:Header>
    </aml-block:Block>
  </soap-env:Body>
</soap-env:Envelope>
```
<xml version="1.0" encoding="UTF-8">
<ch:CallHome xmlns:ch="http://www.cisco.com/2005/05/callhome" version="1.0">
  <ch:MessageDescription>SYSLOG_ALERT
  2013 May 17 16:31:33 dc3-test %ETHPORT-2-IF_SEQ_ERROR: Error (0x20) while communicating
  with component MTS_SAP_ELTM opcode:MTS_OPC_ETHPM_PORT_PHY_CLEANUP (for:RID_PORT: Ethernet3/1)
  </ch:MessageDescription>
  <ch:Event> <ch:Type>syslog</ch:Type> <ch:SubType></ch:SubType> <ch:Brand>Cisco</ch:Brand>
  <ch:Email>contact@example.com</ch:Email>
  <ch:ContractData>
    <ch:DeviceId>N9K-C9508@C@TXX12345678</ch:DeviceId>
  </ch:ContractData>
  <ch:SystemInfo>
    <ch:Name>dc3-test</ch:Name>
    <ch:Contact>Jay Tester</ch:Contact> <ch:ContactEmail>contact@example.com</ch:ContactEmail>
    <ch:ContactPhoneNumber>+91-80-1234-5678</ch:ContactPhoneNumber>
    <ch:StreetAddress>#1, Any Street</ch:StreetAddress> </ch:SystemInfo> </ch:CustomerData>
  <ch:Device> <rme:Chassis xmlns:rme="http://www.cisco.com/rme/4.1">
    <rme:Model>N9K-C9508</rme:Model>
    <rme:HardwareVersion>0.405</rme:HardwareVersion>
    <rme:SerialNumber>TXX12345678</rme:SerialNumber>
  </rme:Chassis> </ch:Device>
</xml>
not generated by system for eltm(0). WCOREDUMP(9) returned zero.
2013 May 17 16:29:08 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID 23210) has&apos;rt caught signal 9 (no core).
2013 May 17 16:29:17 dc3-test %SYSMGR-3-BASIC_TRACE: core_copy: PID 2579 with message Core not generated by system for eltm(0). WCOREDUMP(9) returned zero.
2013 May 17 16:29:17 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID 23294) has&apos;rt caught signal 9 (no core).
2013 May 17 16:29:25 dc3-test %SYSMGR-2-HASWITCHOVER_PRE_START: This supervisor is becoming active (pre-start phase).
2013 May 17 16:29:25 dc3-test %SYSMGR-2-HASWITCHOVER_START: This supervisor is becoming active.
2013 May 17 16:29:26 dc3-test %USER-3-SYSTEM_MSG: crdcfg_get_srvinfo: mts_send failed - device_test
2013 May 17 16:29:27 dc3-test %NETSTACK-3-IP_UNK_MSG_MAJOR: netstack [4336] Unrecognized message from MRIB. Major type 1807
2013 May 17 16:29:28 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is DOWN
2013 May 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:socket family : 2 - ntpd[19045]
2013 May 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:socket family : 10 - ntpd[19045]
2013 May 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:ipv6 only defined - ntpd[19045]
2013 May 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:bindv6 only defined - ntpd[19045]
2013 May 17 16:29:28 dc3-test %NETSTACK-3-CLIENT_GET: netstack [4336] HA client filter recovery failed (0)
2013 May 17 16:29:28 dc3-test %NETSTACK-3-CLIENT_GET: netstack [4336] HA client filter recovery failed (0)
2013 May 17 16:29:29 dc3-test %DAEMON-3-SYSTEM_MSG: ssh disabled, removing - dcos-xinetd(19072)
2013 May 17 16:29:29 dc3-test %DAEMON-3-SYSTEM_MSG: Telnet disabled, removing - dcos-xinetd(19072)
2013 May 17 16:29:31 dc3-test %DAEMON-3-SYSTEM_MSG: Telnet disabled, removing - dcos-xinetd(19073)
2013 May 17 16:29:32 dc3-test %DAEMON-3-SYSTEM_MSG: ssh disabled, removing - dcos-xinetd(19079)
2013 May 17 16:29:32 dc3-test %DAEMON-3-SYSTEM_MSG: Telnet disabled, removing - dcos-xinetd(19079)
2013 May 17 16:29:34 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is UP
2013 May 17 16:29:34 dc3-test %DAEMON-3-SYSTEM_MSG: ssh disabled, removing - dcos-xinetd(19105)
2013 May 17 16:29:34 dc3-test %DAEMON-3-SYSTEM_MSG: Telnet disabled, removing - dcos-xinetd(19105)
2013 May 17 16:29:35 dc3-test %PLATFORM-2-PS_AC_IN_MISSING: Power supply 2 present but all AC inputs are not connected, ac-redundancy might be affected
2013 May 17 16:29:35 dc3-test %PLATFORM-2-PS_AC_IN_MISSING: Power supply 3 present but all AC inputs are not connected, ac-redundancy might be affected
2013 May 17 16:29:38 dc3-test %CALLHOME-2-EVENT: SUP_FAILURE
2013 May 17 16:29:46 dc3-test vsh[19166]: CLIC-3-FAILED_EXEC: Can not exec command &lt;more&gt; return code &lt;14&gt;
2013 May 17 16:30:24 dc3-test vsh[23810]: CLIC-3-FAILED_EXEC: Can not exec command &lt;more&gt; return code &lt;14&gt;
2013 May 17 16:30:24 dc3-test vsh[23803]: CLIC-3-FAILED_EXEC: Can not exec command &lt;more&gt; return code &lt;14&gt;
2013 May 17 16:30:24 dc3-test vsh[23818]: CLIC-3-FAILED_EXEC: Can not exec command &lt;more&gt; return code &lt;14&gt;
2013 May 17 16:30:47 dc3-test %SYSMGR-3-BASIC_TRACE: core_copy: PID 2630 with message Core not generated by system for eltm(0). WCOREDUMP(9) returned zero.
2013 May 17 16:30:47 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID 4820) has&apos;rt caught signal 9 (no core).
2013 May 17 16:31:02 dc3-test %SYSMGR-3-BASIC_TRACE: core_copy: PID 2630 with message Core not generated by system for eltm(0). WCOREDUMP(9) returned zero.
2013 May 17 16:31:02 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID 24239) has&apos;rt caught signal 9 (no core).
2013 May 17 16:31:14 dc3-test %SYSMGR-3-BASIC_TRACE: core_copy: PID 2630 with message Core not generated by system for eltm(0). WCOREDUMP(9) returned zero.
2013 May 17 16:31:14 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID 24401) has not caught signal 9 (no core).
2013 May 17 16:31:23 dc3-test %CALLHOME-2-EVENT: SW_CRASH alert for service: eltm
2013 May 17 16:31:23 dc3-test %SYSMGR-3-BASIC_TRACE: core_copy: PID 2630 with message Core not generated by system for eltm(0). WCOREDUMP(9) returned zero.
2013 May 17 16:31:23 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID 24407) has not caught signal 9 (no core).
2013 May 17 16:31:24 dc3-test vsh[24532]: CLIC-3-FAILED_EXEC: Can not exec command &lt;more&gt; return code &lt;14&gt;
2013 May 17 16:31:24 dc3-test vsh[24548]: CLIC-3-FAILED_EXEC: Can not exec command &lt;more&gt; return code &lt;14&gt;
2013 May 17 16:31:24 dc3-test vsh[24535]: CLIC-3-FAILED_EXEC: Can not exec command &lt;more&gt; return code &lt;14&gt;
2013 May 17 16:31:33 dc3-test %NETSTACK-3-INTERNAL_ERROR: netstack [4336] (null)
2013 May 17 16:31:33 dc3-test %ETHPORT-2-IF_SEQ_ERROR: Error (0x20) while communicating with component MTS_SAP_ELTM opcode:MTS_OPC_ETHPM_PORT_PHY_CLEANUP (for:RID_PORT:Ethernet3/1)
</aml-block:Data> </aml-block:Attachment> <aml-block:Attachment type="inline"> <aml-block:Name>show license usage</aml-block:Name> <aml-block:Data encoding="plain"><![CDATA[Feature Ins Lic Status Expiry Date Comments Count
--------------------------------------------------------------------------------
LAN_ENTERPRISE_SERVICES_PKG Yes - Unused Never -
--------------------------------------------------------------------------------]]>
</aml-block:Data>
</aml-block:Attachment>
</soap-env:Envelope>
### MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIBs related to Smart Call Home</td>
<td>To locate and download supported MIBs, go to the following URL:</td>
</tr>
<tr>
<td></td>
<td>Nexus9000MIBSupportList.html</td>
</tr>
</tbody>
</table>
Configuring Session Manager

This chapter describes how to configure Session Manager on Cisco NX-OS devices.

This chapter contains the following sections:

• About Session Manager, on page 127
• Licensing Requirements for Session Manager, on page 128
• Prerequisites for Session Manager, on page 128
• Guidelines and Limitations for Session Manager, on page 128
• Configuring Session Manager, on page 129
• Verifying the Session Manager Configuration, on page 131
• Configuration Example for Session Manager, on page 131
• Additional References, on page 132

About Session Manager

Session Manager allows you to implement your configuration changes in batch mode. Session Manager works in the following phases:

• Configuration session—Creates a list of commands that you want to implement in Session Manager mode.

• Validation—Provides a basic semantic check on your configuration. Cisco NX-OS returns an error if the semantic check fails on any part of the configuration.

• Verification—Verifies the configuration as a whole, based on the existing hardware and software configuration and resources. Cisco NX-OS returns an error if the configuration does not pass this verification phase.

• Commit—Cisco NX-OS verifies the complete configuration and applies the changes to the device. If a failure occurs, Cisco NX-OS reverts to the original configuration.

• Abort—Discards the configuration changes before implementation.

You can optionally end a configuration session without committing the changes. You can also save a configuration session.
High Availability

Session Manager sessions remain available after a supervisor switchover. Sessions are not persistent across a software reload.

Licensing Requirements for Session Manager

<table>
<thead>
<tr>
<th>Product</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco NX-OS</td>
<td>Session Manager requires no license. Any feature not included in a license package is bundled with the nx-os image and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the Cisco NX-OS Licensing Guide.</td>
</tr>
</tbody>
</table>

Prerequisites for Session Manager

Make sure that you have the privilege level required to support the Session Manager commands that you plan to use.

Guidelines and Limitations for Session Manager

Session Manager has the following configuration guidelines and limitations:

- Configuration for only one service access point (SAP) can be performed using one session.
- Configuration sessions are not persistent across reloads.
- Session Manager supports only access control list (ACL) and quality of service (QoS) features.
- You can create up to 32 configuration sessions.
- You can configure a maximum of 20,000 commands across all sessions.
- You cannot simultaneously execute configuration commands in more than one configuration session or configuration terminal mode. Parallel configurations (for example, one configuration session and one configuration terminal) could cause validation or verification failures in the configuration session.
- If an interface reloads while you are configuring it in a configuration session, Session Manager can accept the commands even if the interface is not present in the device.
Configuring Session Manager

Be aware that the Cisco NX-OS commands might differ from Cisco IOS commands.

Creating a Session

You can create up to 32 configuration sessions.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure session <em>name</em></td>
<td>Creates a configuration session and enters session configuration mode. The name can be any alphanumeric string.</td>
</tr>
<tr>
<td><strong>Example:</strong> switch# configure session myACLs switch(config-s)#</td>
<td>Displays the contents of the session.</td>
</tr>
<tr>
<td><strong>Step 2</strong> (Optional) show configuration session [<em>name</em>]</td>
<td>Displays the contents of the session.</td>
</tr>
<tr>
<td><strong>Example:</strong> switch(config-s)# show configuration session myACLs</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> (Optional) save <em>location</em></td>
<td>Saves the session to a file. The location can be in bootflash:, slot0:, or volatile:.</td>
</tr>
<tr>
<td><strong>Example:</strong> switch(config-s)# save bootflash:sessions/myACLs</td>
<td></td>
</tr>
</tbody>
</table>

Configuring ACLs in a Session

You can configure ACLs within a configuration session.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure session <em>name</em></td>
<td>Creates a configuration session and enters session configuration mode. The name can be any alphanumeric string.</td>
</tr>
<tr>
<td><strong>Example:</strong> switch# configure session myacls switch(config-s)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> ip access-list <em>name</em></td>
<td>Creates an ACL and enters a configuration mode for that ACL.</td>
</tr>
<tr>
<td><strong>Example:</strong> switch(config-s)# ip access-list acl1 switch(config-s-acl)#</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Session Manager

#### Verifying a Session

Use the following command in session mode to verify a session:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>verify [verbose]</td>
<td>Verifies the configuration as a whole, based on the existing hardware and software configuration and resources. Cisco NX-OS returns an error if the configuration does not pass this verification.</td>
</tr>
</tbody>
</table>

**Example:**

```
switch(config-s)# verify
```

#### Committing a Session

Use the following command in session mode to commit a session:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>commit [verbose]</td>
<td>Validates the configuration changes made in the current session and applies valid changes to the device. If the validation fails, Cisco NX-OS reverts to the original configuration.</td>
</tr>
</tbody>
</table>

**Example:**

```
switch(config-s)# commit
```

#### Saving a Session

Use the following command in session mode to save a session:

```
```
### Discarding a Session

Use the following command in session mode to discard a session:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>abort</code></td>
<td>Discards the configuration session without applying the changes.</td>
</tr>
</tbody>
</table>

#### Verify Example

```bash
switch(config-s)# abort
switch#
```

---

### Verifying the Session Manager Configuration

To display the Session Manager configuration information, perform one of the following tasks:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show configuration session [name]</code></td>
<td>Displays the contents of the configuration session.</td>
</tr>
<tr>
<td><code>show configuration session status [name]</code></td>
<td>Displays the status of the configuration session.</td>
</tr>
<tr>
<td><code>show configuration session summary</code></td>
<td>Displays a summary of all the configuration sessions.</td>
</tr>
</tbody>
</table>

---

### Configuration Example for Session Manager

This example shows how to create and commit an ACL configuration using Session Manager:

```bash
switch# configure session ACL_tcp_in
Config Session started, Session ID is 1
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-s)# ip access-list ACL1
switch(config-s-acl)# permit tcp any any
switch(config)# interface e 7/1
switch(config-if)# ip access-group ACL1 in
switch(config-if)# exit
switch(config)# exit
switch# configure session ACL_tcp_in
Config Session started, Session ID is 1
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-s)# verify
Verification Successful
switch(config-s)# commit
Commit Successful
```
Additional References

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration files</td>
<td>Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide</td>
</tr>
</tbody>
</table>
CHAPTER 10

Configuring the Scheduler

This chapter describes how to configure the scheduler on Cisco NX-OS devices.

This chapter includes the following sections:

- About the Scheduler, on page 133
- Licensing Requirements for the Scheduler, on page 134
- Prerequisites for the Scheduler, on page 134
- Guidelines and Limitations for the Scheduler, on page 135
- Default Settings for the Scheduler, on page 135
- Configuring the Scheduler, on page 135
- Verifying the Scheduler Configuration, on page 141
- Configuration Examples for the Scheduler, on page 141

About the Scheduler

The scheduler allows you to define and set a timetable for maintenance activities such as the following:

- Quality of service (QoS) policy changes
- Data backup
- Saving a configuration

Jobs consist of a single command or multiple commands that define routine activities. Jobs can be scheduled one time or at periodic intervals.

The scheduler defines a job and its timetable as follows:

- Job—A routine task or tasks defined as a command list and completed according to a specified schedule.
- Schedule—The timetable for completing a job. You can assign multiple jobs to a schedule. A schedule is defined as either periodic or one-time only:
  - Periodic mode—A recurring interval that continues until you delete the job. You can configure the following types of intervals:
    - Daily—A job is completed once a day.
    - Weekly—A job is completed once a week.
    - Monthly—A job is completed once a month.
Remote User Authentication

Before starting a job, the scheduler authenticates the user who created the job. Since user credentials from a remote authentication are not retained long enough to support a scheduled job, you need to locally configure the authentication passwords for users who create jobs. These passwords are part of the scheduler configuration and are not considered a locally configured user.

Before starting the job, the scheduler validates the local password against the password from the remote authentication server.

Logs

The scheduler maintains a log file containing the job output. If the size of the job output is greater than the size of the log file, the output is truncated.

High Availability

Scheduled jobs remain available after a supervisor switchover or a software reload.

Licensing Requirements for the Scheduler

<table>
<thead>
<tr>
<th>Product</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco NX-OS</td>
<td>The scheduler requires no license. Any feature not included in a license package is bundled with the nx-os image and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the Cisco NX-OS Licensing Guide.</td>
</tr>
</tbody>
</table>

Prerequisites for the Scheduler

The scheduler has the following prerequisites:

- You must enable any conditional features before you can configure those features in a job.
- You must have a valid license installed for any licensed features that you want to configure in the job.
- You must have network-admin user privileges to configure a scheduled job.
Guidelines and Limitations for the Scheduler

The scheduler has the following configuration guidelines and limitations:

- The scheduler can fail if it encounters one of the following while performing a job:
  - Verify that you have configured the time. The scheduler does not apply a default timetable. If you create a schedule and assign jobs and do not configure the time, the job is not started.
  - While defining a job, verify that no interactive or disruptive commands (for example, `copy bootflash: file ftp: URI`, `write erase`, and other similar commands) are specified because the job is started and conducted noninteractively.
  - The scheduler accepts `start_time` in the past for any schedule with a repeat option in the time command under schedule mode configuration. It then throws a warning that the entered start time is in the past. The `start_time` of any schedule will always remain the same as it was in the beginning, across reboot, and even after re-applying the previous saved configuration.

Default Settings for the Scheduler

This table lists the scheduler default settings.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduler state</td>
<td>Disabled</td>
</tr>
<tr>
<td>Log file size</td>
<td>16 KB</td>
</tr>
</tbody>
</table>

Configuring the Scheduler

Enabling or Disabling the Scheduler

You can enable the scheduler feature so that you can configure and schedule jobs, or you can disable the scheduler feature after it has been enabled.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><code>switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)#</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>[no] feature scheduler</code></td>
<td>Enables or disables the scheduler.</td>
</tr>
<tr>
<td></td>
<td><code>switch(config)# feature scheduler</code></td>
<td></td>
</tr>
</tbody>
</table>
Defining the Scheduler Log File Size

You can configure the log file size for capturing jobs, schedules, and job output.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td>switch(config)# configure terminal</td>
</tr>
<tr>
<td></td>
<td>switch# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>scheduler logfile size value</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td>switch(config)# scheduler logfile size 1024</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If the size of the job output is greater than the size of the log file, then the output is truncated.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>(Optional) copy running-config startup-config</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td>switch(config)# copy running-config startup-config</td>
</tr>
</tbody>
</table>

Configuring Remote User Authentication

You can configure the scheduler to use remote authentication for users who want to configure and schedule jobs.

*Note* Remote users must authenticate with their clear text password before creating and configuring jobs.
Remote user passwords are always shown in encrypted form in the output of the `show running-config` command. The encrypted option (7) in the command supports the ASCII device configuration.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
|      | Example: `switch# configure terminal
switch(config)#` | |
| Step 2 | `scheduler aaa-authentication password [0 | 7] password` | Configures a cleartext password for the user who is currently logged in. |
|      | Example: `switch(config)# scheduler aaa-authentication password X12y34Z56a` | |
| Step 3 | `scheduler aaa-authentication username name password [0 | 7] password` | Configures a cleartext password for a remote user. |
|      | Example: `switch(config)# scheduler aaa-authentication username newuser password Z98y76X54b` | |
| Step 4 | `(Optional) show running-config | include “scheduler aaa-authentication”` | Displays the scheduler password information. |
|      | Example: `switch(config)# show running-config | include “scheduler aaa-authentication”` | |
| Step 5 | `(Optional) copy running-config startup-config` | Copies the running configuration to the startup configuration. |
|      | Example: `switch(config)# copy running-config startup-config` | |

### Defining a Job

You can define a job including the job name and the command sequence.

⚠️ **Caution**

After you define a job, you cannot modify or remove commands. To change the job, you must delete it and create a new one.
### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>scheduler job name string</td>
<td>Creates a job and enters the job configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# scheduler job name backup-cfg</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config-job)</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>command1 ; [command2 ; command3 ; ...]</td>
<td>Defines the sequence of commands for the specified job. Separate commands with spaces and semicolons (for example, &quot; ; &quot;).</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config-job)# copy running-config tftp://1.2.3.4/$(SWITCHNAME)-cfg.$(TIMESTAMP) vrf management switch(config-job)#</td>
<td>This example creates a scheduler job that saves the running configuration to a file in the bootflash. The job then copies the file from the bootflash to a TFTP server and creates the filename using the current timestamp and switch name.</td>
</tr>
<tr>
<td>4</td>
<td>(Optional) show scheduler job [name name]</td>
<td>Displays the job information.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config-job)# show scheduler job</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>(Optional) copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

### Deleting a Job

You can delete a job from the scheduler.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>no scheduler job name string</td>
<td>Deletes the specified job and all commands defined within it.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Defining a Timetable

You can define a timetable in the scheduler to be used with one or more jobs.

If you do not specify the time for the `time` commands, the scheduler assumes the current time. For example, if the current time is March 24, 2013, 22:00 hours, jobs are started as follows:

- For the `time start 23:00 repeat 4:00:00` command, the scheduler assumes a start time of March 24, 2013, 23:00 hours.
- For the `time daily 55` command, the scheduler assumes a start time every day at 22:55 hours.
- For the `time weekly 23:00` command, the scheduler assumes a start time every Friday at 23:00 hours.
- For the `time monthly 23:00` command, the scheduler assumes a start time on the 24th of every month at 23:00 hours.

---

**Note**

The scheduler will not begin the next occurrence of a job before the last one completes. For example, you have scheduled a job to be completed at one-minute intervals beginning at 22:00; but the job requires two minutes to complete. The scheduler starts the first job at 22:00, completes it at 22:02, and then observes a one-minute interval before starting the next job at 22:03.

---

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
| Example: | switch# configure terminal  
switch(config)# | |
| **Step 2** | `scheduler schedule name string` | Creates a new schedule and places you in schedule configuration mode for that schedule. |
| Example: | switch(config)# scheduler schedule name weekendbackupqos  
switch(config-schedule)# | |
### Defining a Timetable

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 3** | job name *string*  
**Example:**  
switch(config-schedule)# job name  
offpeakZoning | Associates a job with this schedule. You can add multiple jobs to a schedule. |
| **Step 4** | time daily *time*  
**Example:**  
switch(config-schedule)# time daily 23:00 | Indicates the job starts every day at a designated time specified as HH:MM. |
| **Step 5** | time weekly *[dow:]HH:MM*  
**Example:**  
switch(config-schedule)# time weekly  
Sun:23:00 | Indicates that the job starts on a specified day of the week.  
Day of the week (dow) specified as one of the following:  
- An integer such as 1 = Sunday, 2 = Monday, and so on.  
- An abbreviation such as Sun = Sunday.  
The maximum length for the entire argument is 10. |
| **Step 6** | time monthly *[dm:]HH:MM*  
**Example:**  
switch(config-schedule)# time monthly  
28:23:00 | Indicates the job starts on a specified day each month (dm). If you specify either 29, 30, or 31, the job is started on the last day of each month. |
| **Step 7** | time start {now repeat repeat-interval | delta-time [repeat repeat-interval]}  
**Example:**  
switch(config-schedule)# time start now  
repeat 48:00 | Indicates the job starts periodically.  
The start-time format is [[[yyyy:]mmm:]dd:]HH:MM.  
- *delta-time*—Specifies the amount of time to wait after the schedule is configured before starting a job.  
- *now*—Specifies that the job starts now.  
- *repeat repeat-interval*—Specifies the frequency at which the job is repeated.  
In this example, the job starts immediately and repeats every 48 hours. |
| **Step 8** | (Optional) show scheduler config  
**Example:**  
switch(config)# show scheduler config | Displays the scheduler configuration. |
Clearing the Scheduler Log File

You can clear the scheduler log file.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>clear scheduler logfile</td>
<td>Clears the scheduler log file.</td>
</tr>
</tbody>
</table>

Verifying the Scheduler Configuration

To display the scheduler configuration information, perform one of the following tasks:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show scheduler config</td>
<td>Displays the scheduler configuration.</td>
</tr>
<tr>
<td>show scheduler job [name string]</td>
<td>Displays the jobs configured.</td>
</tr>
<tr>
<td>show scheduler logfile</td>
<td>Displays the contents of the scheduler log file.</td>
</tr>
<tr>
<td>show scheduler schedule [name string]</td>
<td>Displays the schedules configured.</td>
</tr>
</tbody>
</table>

Configuration Examples for the Scheduler

Creating a Scheduler Job

This example shows how to create a scheduler job that saves the running configuration to a file in the bootflash. The job then copies the file from the bootflash to a TFTP server (creates the filename using the current timestamp and switch name):
Scheduling a Scheduler Job

This example shows how to schedule a scheduler job called backup-cfg to run daily at 1 a.m.:

```
switch# configure terminal
switch(config)# scheduler job name backup-cfg
switch(config-job)# copy running-config
 tftp://1.2.3.4/$(SWITCHNAME)-cfg.$(TIMESTAMP) vrf management
switch(config-job)# end
switch(config)#
```

Displaying the Job Schedule

This example shows how to display the job schedule:

```
switch# show scheduler schedule
Schedule Name : daily
-----------------------------
User Name : admin
Schedule Type : Run every day at 1 Hrs 00 Mins
Last Execution Time : Fri Jan 2 1:00:00 2013
Last Completion Time: Fri Jan 2 1:00:01 2013
Execution count : 2
-----------------------------
Job Name Last Execution Status
-----------------------------
back-cfg Success (0)
switch#
```

Displaying the Results of Running Scheduler Jobs

This example shows how to display the results of scheduler jobs that have been executed by the scheduler:

```
switch# show scheduler logfile
Job Name : back-cfg Job Status: Failed (1)
Schedule Name : daily User Name : admin
Completion time: Fri Jan 1 1:00:01 2013
----------------------------- Job Output -----------------------------
copy: cannot access file '/bootflash/switch-cfg.2013-01-01-01.00.00'
==============================================================================
Job Name : back-cfg Job Status: Success (0)
Schedule Name : daily User Name : admin
Completion time: Fri Jan 2 1:00:01 2013
----------------------------- Job Output -----------------------------
copy running-config bootflash:/switch-cfg.2013-01-02-01.00.00
'copy bootflash:/switch-cfg.2013-01-02-01.00.00 tftp://1.2.3.4/ vrf management
'copy bootflash:/switch-cfg.2013-01-02-01.00.00 tftp://1.2.3.4/ vrf management
```
Connection to Server Established.
[ ] 0.50KB Trying to connect to tftp server......
[#] 24.50KB
TFTP put operation was successful
switch#
Displaying the Results of Running Scheduler Jobs
CHAPTER 11

Configuring SNMP

This chapter describes how to configure the SNMP feature on Cisco NX-OS devices.

This chapter contains the following sections:

- About SNMP, on page 145
- Licensing Requirements for SNMP, on page 151
- Guidelines and Limitations for SNMP, on page 151
- Default Settings for SNMP, on page 152
- Configuring SNMP, on page 152
- Configuring the SNMP Local Engine ID, on page 174
- Verifying SNMP Configuration, on page 175
- Configuration Examples for SNMP, on page 176
- Additional References, on page 177

About SNMP

The Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network.

SNMP Functional Overview

The SNMP framework consists of three parts:

- An SNMP manager—The system used to control and monitor the activities of network devices using SNMP.

- An SNMP agent—The software component within the managed device that maintains the data for the device and reports these data, as needed, to managing systems. The Cisco Nexus device supports the agent and MIB. To enable the SNMP agent, you must define the relationship between the manager and the agent.

- A managed information base (MIB)—The collection of managed objects on the SNMP agent

SNMP is defined in RFCs 3411 to 3418.
The device supports SNMPv1, SNMPv2c, and SNMPv3. Both SNMPv1 and SNMPv2c use a community-based form of security.

Cisco NX-OS supports SNMP over IPv6.

### SNMP Notifications

A key feature of SNMP is the ability to generate notifications from an SNMP agent. These notifications do not require that requests be sent from the SNMP manager. Notifications can indicate improper user authentication, restarts, the closing of a connection, loss of connection to a neighbor router, or other significant events.

Cisco NX-OS generates SNMP notifications as either traps or informs. A trap is an asynchronous, unacknowledged message sent from the agent to the SNMP managers listed in the host receiver table. Informs are asynchronous messages sent from the SNMP agent to the SNMP manager which the manager must acknowledge receipt of.

Traps are less reliable than informs because the SNMP manager does not send any acknowledgment when it receives a trap. The device cannot determine if the trap was received. An SNMP manager that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the device never receives a response, it can send the inform request again.

You can configure Cisco NX-OS to send notifications to multiple host receivers.

The following table lists the SNMP traps that are enabled by default.

<table>
<thead>
<tr>
<th>Trap Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>generic</td>
<td>: coldStart</td>
</tr>
<tr>
<td>entity</td>
<td>: entity_fan_status_change</td>
</tr>
<tr>
<td>entity</td>
<td>: entity_mib_change</td>
</tr>
<tr>
<td>entity</td>
<td>: entity_module_status_change</td>
</tr>
<tr>
<td>entity</td>
<td>: entity_module_inserted</td>
</tr>
<tr>
<td>entity</td>
<td>: entity_module_removed</td>
</tr>
<tr>
<td>entity</td>
<td>: entity_power_out_change</td>
</tr>
<tr>
<td>entity</td>
<td>: entity_power_status_change</td>
</tr>
<tr>
<td>entity</td>
<td>: entity_unrecognised_module</td>
</tr>
<tr>
<td>link</td>
<td>: cErrDisableInterfaceEventRev1</td>
</tr>
<tr>
<td>link</td>
<td>: cieLinkDown</td>
</tr>
<tr>
<td>link</td>
<td>: cieLinkUp</td>
</tr>
<tr>
<td>link</td>
<td>: cmn-mac-move-notification</td>
</tr>
<tr>
<td>link</td>
<td>: delayed-link-state-change</td>
</tr>
<tr>
<td>link</td>
<td>: extended-linkDown</td>
</tr>
<tr>
<td>link</td>
<td>: extended-linkUp</td>
</tr>
<tr>
<td>link</td>
<td>: linkDown</td>
</tr>
</tbody>
</table>
SNMPv3

SNMPv3 provides secure access to devices by a combination of authenticating and encrypting frames over the network. The security features provided in SNMPv3 are the following:

- Message integrity—Ensures that a packet has not been tampered with in-transit.
- Authentication—Determines the message is from a valid source.
- Encryption—Scrambles the packet contents to prevent it from being seen by unauthorized sources.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.

Security Models and Levels for SNMPv1, v2, v3

The security level determines if an SNMP message needs to be protected from disclosure and if the message needs to be authenticated. The various security levels that exist within a security model are as follows:

- noAuthNoPriv—Security level that does not provide authentication or encryption. This level is not supported for SNMPv3.
- authNoPriv—Security level that provides authentication but does not provide encryption.
- authPriv—Security level that provides both authentication and encryption.

Three security models are available: SNMPv1, SNMPv2c, and SNMPv3. The security model combined with the security level determine the security mechanism applied when the SNMP message is processed. The following table identifies what the combinations of security models and levels mean.

<table>
<thead>
<tr>
<th>Trap Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>link</td>
<td>: linkUp</td>
</tr>
<tr>
<td>rf</td>
<td>: redundancy_framework</td>
</tr>
<tr>
<td>license</td>
<td>: notify-license-expiry</td>
</tr>
<tr>
<td>license</td>
<td>: notify-no-license-for-feature</td>
</tr>
<tr>
<td>license</td>
<td>: notify-licensefile-missing</td>
</tr>
<tr>
<td>license</td>
<td>: notify-license-expiry-warning</td>
</tr>
<tr>
<td>upgrade</td>
<td>: UpgradeOpNotifyOnCompletion</td>
</tr>
<tr>
<td>upgrade</td>
<td>: UpgradeJobStatusNotify</td>
</tr>
<tr>
<td>entity</td>
<td>: entity_sensor</td>
</tr>
<tr>
<td>rmon</td>
<td>: fallingAlarm</td>
</tr>
<tr>
<td>rmon</td>
<td>: hcRisingAlarm</td>
</tr>
<tr>
<td>rmon</td>
<td>: hcFallingAlarm</td>
</tr>
<tr>
<td>rmon</td>
<td>: risingAlarm</td>
</tr>
</tbody>
</table>
Table 14: SNMP Security Models and Levels

<table>
<thead>
<tr>
<th>Model</th>
<th>Level</th>
<th>Authentication</th>
<th>Encryption</th>
<th>What Happens</th>
</tr>
</thead>
<tbody>
<tr>
<td>v1</td>
<td>noAuthNoPriv</td>
<td>Community string</td>
<td>No</td>
<td>Uses a community string match for authentication.</td>
</tr>
<tr>
<td>v2c</td>
<td>noAuthNoPriv</td>
<td>Community string</td>
<td>No</td>
<td>Uses a community string match for authentication.</td>
</tr>
<tr>
<td>v3</td>
<td>authNoPriv</td>
<td>HMAC-MD5 or HMAC-SHA</td>
<td>No</td>
<td>Provides authentication based on the Hash-Based Message Authentication Code (HMAC) Message Digest 5 (MD5) algorithm or the HMAC Secure Hash Algorithm (SHA).</td>
</tr>
<tr>
<td>v3</td>
<td>authPriv</td>
<td>HMAC-MD5 or HMAC-SHA</td>
<td>DES</td>
<td>Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard.</td>
</tr>
</tbody>
</table>

User-Based Security Model

The SNMPv3 User-Based Security Model (USM) refers to SNMP message-level security and offers the following services:

- **Message integrity**—Ensures that messages have not been altered or destroyed in an unauthorized manner and that data sequences have not been altered to an extent greater than can occur nonmaliciously.

- **Message origin authentication**—Ensures that the claimed identity of the user on whose behalf received data was originated is confirmed.

- **Message confidentiality**—Ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes.

SNMPv3 authorizes management operations only by configured users and encrypts SNMP messages.
Cisco NX-OS uses two authentication protocols for SNMPv3:

- HMAC-MD5-96 authentication protocol
- HMAC-SHA-96 authentication protocol

Cisco NX-OS uses Advanced Encryption Standard (AES) as one of the privacy protocols for SNMPv3 message encryption and conforms with RFC 3826.

The `priv` option offers a choice of DES or 128-bit AES encryption for SNMP security encryption. The `priv` option and the `aes-128` token indicate that this privacy password is for generating a 128-bit AES key. The AES priv password can have a minimum of eight characters. If the passphrases are specified in clear text, you can specify a maximum of 64 case-sensitive, alphanumeric characters. If you use the localized key, you can specify a maximum of 130 characters.

For an SNMPv3 operation using the external AAA server, you must use AES for the privacy protocol in the user configuration on the external AAA server.

**CLI and SNMP User Synchronization**

SNMPv3 user management can be centralized at the Access Authentication and Accounting (AAA) server level. This centralized user management allows the SNMP agent in Cisco NX-OS to leverage the user authentication service of the AAA server. Once user authentication is verified, the SNMP PDUs are processed further. Additionally, the AAA server is also used to store user group names. SNMP uses the group names to apply the access/role policy that is locally available in the switch.

Any configuration changes made to the user group, role, or password results in database synchronization for both SNMP and AAA.

Cisco NX-OS synchronizes the user configuration in the following ways:

- The authentication passphrase specified in the `snmp-server user` command becomes the password for the CLI user.
- The password specified in the `username` command becomes the authentication and privacy passphrases for the SNMP user.
- If you create or delete a user using either SNMP or the CLI, the user is created or deleted for both SNMP and the CLI.
- User-role mapping changes are synchronized in SNMP and the CLI.
- Role changes (deletions or modifications) from the CLI are synchronized to SNMP.

When you configure a passphrase/password in localized key/encrypted format, Cisco NX-OS does not synchronize the user information (passwords, roles, and so on).

Cisco NX-OS holds the synchronized user configuration for 60 minutes by default.
Group-Based SNMP Access

Because *group* is a standard SNMP term used industry-wide, we refer to roles as groups in this SNMP section.

SNMP access rights are organized by groups. Each group in SNMP is similar to a role through the CLI. Each group is defined with read access or read-write access.

You can begin communicating with the agent once your username is created, your roles are set up by your administrator, and you are added to the roles.

SNMP and Embedded Event Manager

The Embedded Event Manager (EEM) feature monitors events, including SNMP MIB objects, and triggers an action based on these events. One of the actions could be to send an SNMP notification. EEM sends the cEventMgrPolicyEvent of CISCO-EMBEDDED-EVENT-MGR-MIB as the SNMP notification.

Multiple Instance Support

A device can support multiple instances of a logical network entity, such as protocol instances or virtual routing and forwarding (VRF) instances. Most existing MIBs cannot distinguish between these multiple logical network entities. For example, the original OSPF-MIB assumes a single protocol instance on a device, but you can now configure multiple OSPF instances on a device.

SNMPv3 uses contexts to distinguish between these multiple instances. An SNMP context is a collection of management information that you can access through the SNMP agent. A device can support multiple contexts for different logical network entities. An SNMP context allows the SNMP manager to access one of the multiple instances of a MIB module supported on the device for the different logical network entities.

Cisco NX-OS supports the CISCO-CONTEXT-MAPPING-MIB to map between SNMP contexts and logical network entities. You can associate an SNMP context to a VRF, protocol instance, or topology.

SNMPv3 supports contexts with the contextName field of the SNMPv3 PDU. You can map this contextName field to a particular protocol instance or VRF.

For SNMPv2c, you can map the SNMP community to a context using the snmpCommunityContextName MIB object in the SNMP-COMMUNITY-MIB (RFC 3584). You can then map this snmpCommunityContextName to a particular protocol instance or VRF using the CISCO-CONTEXT-MAPPING-MIB or the CLI.

High Availability for SNMP

Cisco NX-OS supports stateless restarts for SNMP. After a reboot or supervisor switchover, Cisco NX-OS applies the running configuration.

Virtualization Support for SNMP

Cisco NX-OS supports one instance of the SNMP. SNMP supports multiple MIB module instances and maps them to logical network entities.
SNMP is also VRF aware. You can configure SNMP to use a particular VRF to reach the SNMP notification host receiver. You can also configure SNMP to filter notifications to an SNMP host receiver based on the VRF where the notification occurred.

### Licensing Requirements for SNMP

<table>
<thead>
<tr>
<th>Product</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco NX-OS</td>
<td>SNMP requires no license. Any feature not included in a license package is bundled with the nx-os image and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the Cisco NX-OS Licensing Guide.</td>
</tr>
</tbody>
</table>

### Guidelines and Limitations for SNMP

SNMP has the following configuration guidelines and limitations:

- Access control list (ACLs) can be applied only to local SNMPv3 users configured on the switch. ACLs cannot be applied to remote SNMPv3 users stored on Authentication, Authorization, and Accounting (AAA) servers.

- Cisco NX-OS supports read-only access to some SNMP MIBs. See the Cisco NX-OS MIB support list at the following URL for more information: ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html

- Cisco NX-OS does not support the SNMPv3 noAuthNoPriv security level.

- Cisco Nexus 9000 Series switches and the Cisco Nexus 3164Q, 31128PQ, 3232C, and 3264Q switches support the configuration of the SNMP local engine ID.

- For a nondisruptive downgrade path to an earlier release, if a local engine ID has been configured, then you must unconfigure the local engine ID, and then reconfigure the SNMP users and the community strings.

- The default SNMP PDU value is 1500 bytes. The SNMP agent drops any response PDU that is greater than 1500 bytes, causing the SNMP request to fail. To receive MIB data values larger than 1500 bytes, use the `snmp-server packetsize <byte-count>` command to reconfigure the packet size. The valid byte-count range is from 484 to 17382. When a GETBULK response exceeds the packet size, the data can get truncated.

- You must use either the CLI or SNMP to configure a feature on your switch. Do not configure a feature using both interfaces to the switch.

- Using cefcFanTrayOperStatus snmpwalk on an individual fan OID tree where the fan is not populated in chassis, can return a response for next OID entry in the tree. To prevent this behavior, use the -CI option in snmpwalk.

The behavior is not seen when polling parent OID, or when using getmany.
Default Settings for SNMP

The following table lists the default settings for SNMP parameters.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>License notifications</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Configuring SNMP

Be aware that the Cisco NX-OS commands for this feature may differ from those commands used in Cisco IOS.

Configuring SNMP Users

You can configure a user for SNMP.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>configure terminal</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)#</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><strong>snmp-server user name</strong></td>
<td>Configures an SNMP user with authentication and privacy parameters.</td>
</tr>
<tr>
<td></td>
<td>**[auth {md5</td>
<td>sha} passphrase [auto] [priv {aes-128} passphrase] [engineID id] [localizedkey]]**</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)# snmp-server user Admin auth sha abcd1234 priv abcdefgh</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><strong>(Optional) show snmp user</strong></td>
<td>Displays information about one or more SNMP users.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)# show snmp user</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><strong>(Optional) copy running-config</strong></td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td></td>
<td><strong>startup-config</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)# copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>
Enforcing SNMP Message Encryption

You can configure SNMP to require authentication or encryption for incoming requests. By default, the SNMP agent accepts SNMPv3 messages without authentication and encryption. When you enforce privacy, Cisco NX-OS responds with an authorization error for any SNMPv3 PDU request using a security level parameter of either noAuthNoPriv or authNoPriv.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> snmp-server user name enforcePriv</td>
<td>Enforces SNMP message encryption for this user.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# snmp-server user Admin enforcePriv</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> snmp-server globalEnforcePriv</td>
<td>Enforces SNMP message encryption for all users.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# snmp-server globalEnforcePriv</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> (Optional) copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

**Assigning SNMPv3 Users to Multiple Roles**

After you configure an SNMP user, you can assign multiple roles for the user.

**Note**

Only users belonging to a network-admin role can assign roles to other users.
Creating SNMP Communities

You can create SNMP communities for SNMPv1 or SNMPv2c.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><code>switch(config)#</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>snmp-server user name group</code></td>
<td>Associates this SNMP user with the configured user role.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>switch(config)# snmp-server user Admin superuser</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>(Optional) copy running-config startup-config</code></td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>switch(config)# copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>

Filtering SNMP Requests

You can assign an access control list (ACL) to an SNMPv2 community or SNMPv3 user to filter SNMP requests. If the assigned ACL allows the incoming request packet, SNMP processes the request. If the ACL denies the request, SNMP drops the request and sends a system message.
Create the ACL with the following parameters:

- Source IP address
- Destination IP address
- Source port
- Destination port
- Protocol (UDP or TCP)

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>switch# configure terminal</code> <code>switch(config)#</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>`snmp-server community name [use-ipv4acl acl-name</td>
<td>use-ipv6acl acl-name]`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>switch(config)# snmp-server community public use-ipv4acl myacl</code></td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>IPv6 ACLs are supported for SNMPv2 communities beginning with Cisco NX-OS Release 7.0(3)I4(1).</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>In releases prior to Cisco NX-OS Release 7.0(3)I4(1), this CLI command includes <code>use-acl</code> rather than <code>use-ipv4acl</code>.</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>`snmp-server user username [use-ipv4acl acl-name</td>
<td>use-ipv6acl acl-name]`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>switch(config)# snmp-server user user1 use-ipv4acl myacl</code></td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>IPv6 ACLs are supported for SNMPv3 users beginning with Cisco NX-OS Release 7.0(3)I4(1).</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>In releases prior to Cisco NX-OS Release 7.0(3)I4(1), this CLI command includes <code>use-acl</code> rather than <code>use-ipv4acl</code>.</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><em>(Optional)</em> <code>copy running-config startup-config</code></td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>switch(config)# copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>
Configuring SNMP Notification Receivers

You can configure Cisco NX-OS to generate SNMP notifications to multiple host receivers.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> snmp-server host ip-address traps version 1</td>
<td>Configures a host receiver for SNMPv1 traps.</td>
</tr>
<tr>
<td>community [udp_port number]</td>
<td>The ip-address can be an IPv4 or IPv6 address.</td>
</tr>
<tr>
<td>Example:</td>
<td>The community can be any alphanumeric string up to 255 characters.</td>
</tr>
<tr>
<td>switch(config)# snmp-server host</td>
<td>The UDP port number range is from 0 to 65535.</td>
</tr>
<tr>
<td>192.0.2.1 traps version 1 public</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> snmp-server host ip-address [traps</td>
<td>informs] version 2c</td>
</tr>
<tr>
<td>community [udp_port number]</td>
<td>The ip-address can be an IPv4 or IPv6 address.</td>
</tr>
<tr>
<td>Example:</td>
<td>The community can be any alphanumeric string up to 255 characters.</td>
</tr>
<tr>
<td>switch(config)# snmp-server host</td>
<td>The UDP port number range is from 0 to 65535.</td>
</tr>
<tr>
<td>192.0.2.1 informs version 2c public</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> snmp-server host ip-address [traps</td>
<td>informs] version 3</td>
</tr>
<tr>
<td>{auth</td>
<td>noauth</td>
</tr>
<tr>
<td>Example:</td>
<td>The username can be any alphanumeric string up to 255 characters.</td>
</tr>
<tr>
<td>switch(config)# snmp-server host</td>
<td>The UDP port number range is from 0 to 65535.</td>
</tr>
<tr>
<td>192.0.2.1 informs version 3 auth NMS</td>
<td>Note</td>
</tr>
<tr>
<td><strong>Step 5</strong> (Optional) copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

Configuring a Source Interface for SNMP Notifications

You can configure SNMP to use the IP address of an interface as the source IP address for notifications. When a notification is generated, its source IP address is based on the IP address of this configured interface.

You can configure a source interface as follows:

- All notifications sent to all SNMP notification receivers.
• All notifications sent to a specific SNMP notification receiver. This configuration overrides the global source interface configuration.

**Note**
Configuring the source interface IP address for outgoing trap packets does not guarantee that the device will use the same interface to send the trap. The source interface IP address defines the source address inside of the SNMP trap, and the connection is opened with the address of the egress interface as source.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>
| **Example:** | switch# configure terminal  
switch(config)# |
| **Step 2** | (Optional) Send Traps messages to this host.  
The traps version is the SNMP version to use for notification messages. 2c indicates that SNMPv2c is to be used. |
| `snmp-server host ip-address source-interface if-type if-number traps version 2c name` | |
| **Example:** | snmp-server host 192.0.2.1  
source-interface ethernet 2/1 traps version 2c public |
| **Step 3** | Configures SNMP to use the selected VRF to communicate with the host receiver. The ip-address can be an IPv4 or IPv6 address. The VRF name can be any alphanumeric string up to 32 characters. |
| `snmp-server host ip-address source-interface if-type if-number use-vrf vrf-name` | |
| **Example:** | snmp-server host 192.0.2.1  
source-interface ethernet 2/1 use-vrf default |
| **Note** | This command does not remove the host configuration. |
| **Step 4** | Configures a host receiver for SNMPv2c traps or informs. The ip-address can be an IPv4 or IPv6 address. Use ? to determine the supported interface types. The UDP port number range is from 0 to 65535.  
This configuration overrides the global source interface configuration. |
| `snmp-server host ip-address source-interface if-type if-number [udp_port number]` | |
| **Example:** | switch(config)# snmp-server host  
192.0.2.1 source-interface ethernet 2/1 |
| **Step 5** | Configures a source interface for sending out SNMPv2c traps or informs. Use ? to determine the supported interface types. |
| `snmp-server source-interface {traps | informs} if-type if-number` | |
| **Example:** | switch(config)# snmp-server  
source-interface traps ethernet 2/1 |
| **Step 6** | Displays information about configured source interfaces. |
| `show snmp source-interface` | |
Configuring the Notification Target User

You must configure a notification target user on the device to send SNMPv3 inform notifications to a notification host receiver.

Cisco NX-OS uses the credentials of the notification target user to encrypt the SNMPv3 inform notification messages to the configured notification host receiver.

**Note**
For authenticating and decrypting the received inform PDU, the notification host receiver should have the same user credentials as configured in Cisco NX-OS to authenticate and decrypt the informs.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>switch# configure terminal switch(config)#</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configures the notification target user with the specified engine ID for the notification host receiver. The engine ID format is a 12-digit colon-separated decimal number.</td>
</tr>
<tr>
<td>`snmp-server user name [auth {md5</td>
<td>sha}] passphrase [auto] [priv {aes-128}] passphrase [engineID id]`</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# snmp-server user NMS auth sha abcd1234 priv abcdefgh engineID 00:00:00:63:00:01:00:10:20:15:10:03</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td>(Optional) <code>copy running-config startup-config</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# copy running-config startup-config</td>
</tr>
</tbody>
</table>

Configuring SNMP Notification Receivers with VRFs

SNMP adds entries into the eExtSnmpTargetVrfTable of the CISCO-SNMP-TARGET-EXT-MIB when you configure the VRF reachability and filtering options for an SNMP notification receiver.

**Note**
You must configure the host before configuring the VRF reachability or filtering options.
You can configure Cisco NX-OS to use a configured VRF to reach the host receiver or to filter notifications based on the VRF in which the notification occurred.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>configure terminal</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>[no] snmp-server host ip-address use-vrf vrf-name [udp_port number]</td>
<td>Configures SNMP to use the selected VRF to communicate with the host receiver. The ip-address can be an IPv4 or IPv6 address. The VRF name can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535. This command adds an entry into the ExtSnmpTargetVrfTable of the CISCO-SNMP-TARGET-EXT-MB. The no form of this command removes the VRF reachability information for the configured host and removes the entry from the ExtSnmpTargetVrfTable of the CISCO-SNMP-TARGET-EXT-MB. This command does not remove the host configuration.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# snmp-server host 192.0.2.1 use-vrf Blue</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>[no] snmp-server host ip-address filter-vrf vrf-name [udp_port number]</td>
<td>Filters notifications to the notification host receiver based on the configured VRF. The ip-address can be an IPv4 or IPv6 address. The VRF name can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535. This command adds an entry into the ExtSnmpTargetVrfTable of the CISCO-SNMP-TARGET-EXT-MB. The no form of this command removes the VRF filter information for the configured host and removes the entry from the ExtSnmpTargetVrfTable of the CISCO-SNMP-TARGET-EXT-MB. This command does not remove the host configuration.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# snmp-server host 192.0.2.1 filter-vrf Red</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>(Optional) <strong>copy running-config startup-config</strong></td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
Configuring SNMP to Send Traps Using an Inband Port

You can configure SNMP to send traps using an inband port. To do so, you must configure the source interface (at the global or host level) and the VRF used to send the traps.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>snmp-server source-interface traps if-type if-number</td>
<td>Globally configures a source interface for sending out SNMP traps. Use ? to determine the supported interface types.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# snmp-server source-interface traps ethernet 1/2</td>
<td>You can configure the source interface at the global level or at a host level. When the source interface is configured globally, any new host configuration uses the global configuration to send the traps.</td>
</tr>
<tr>
<td>Note</td>
<td>To configure a source interface at the host level, use the snmp-server host ip-address source-interface if-type if-number command.</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>(Optional) show snmp source-interface</td>
<td>Displays information about configured source interfaces.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# show snmp source-interface</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>snmp-server host ip-address use-vrf vrf-name [udp_port number]</td>
<td>Configures SNMP to use the selected VRF to communicate with the host receiver. The ip-address can be an IPv4 or IPv6 address. The VRF name can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535. This command adds an entry into the ExtSnmpTargetVrfTable of the CISCO-SNMP-TARGET-EXT-MB.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# snmp-server host 171.71.48.164 use-vrf default</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>By default, SNMP sends the traps using the management VRF. If you do not want to use the management VRF, you must use this command to specify the desired VRF.</td>
<td></td>
</tr>
</tbody>
</table>
Enabling SNMP Notifications

You can enable or disable notifications. If you do not specify a notification name, Cisco NX-OS enables all notifications except BGP, EIGRP, and OSPF notifications.

The `snmp-server enable traps` command enables both traps and informs, depending on the configured notification host receivers.

The following table lists the commands that enable the notifications for Cisco NX-OS MIBs.

**Table 15: Enabling SNMP Notifications**

<table>
<thead>
<tr>
<th>MIB</th>
<th>Related Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>All notifications (except BGP, EIGRP, and OSPF)</td>
<td><code>snmp-server enable traps</code></td>
</tr>
<tr>
<td>CISCO-AAA-SERVER-MIB</td>
<td><code>snmp-server enable traps aaa</code></td>
</tr>
<tr>
<td></td>
<td><code>snmp-server enable traps aaa server-state-change</code></td>
</tr>
<tr>
<td>CISCO-BGP4-MIB</td>
<td><code>snmp-server enable traps bgp</code></td>
</tr>
<tr>
<td>CISCO-CALLHOME-MIB</td>
<td><code>snmp-server enable traps callhome</code></td>
</tr>
<tr>
<td></td>
<td><code>snmp-server enable traps callhome event-notify</code></td>
</tr>
<tr>
<td></td>
<td><code>snmp-server enable traps callhome smtp-send-fail</code></td>
</tr>
<tr>
<td>CISCO-CONFIG-MAN-MIB</td>
<td><code>snmp-server enable traps config</code></td>
</tr>
<tr>
<td></td>
<td><code>snmp-server enable traps config ccmCLIRunningConfigChanged</code></td>
</tr>
<tr>
<td>CISCO-EIGRP-MIB</td>
<td><code>snmp-server enable traps eigrp [tag]</code></td>
</tr>
<tr>
<td>CISCO-ERR-DISABLE-MIB</td>
<td><code>snmp-server enable traps link cerrDisableInterfaceEventRev1</code></td>
</tr>
<tr>
<td>MIB</td>
<td>Related Commands</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>------------------------------------------------------------</td>
</tr>
<tr>
<td>ENTITY-MIB, CISCO-ENTITY-SENSOR-MIB</td>
<td>snmp-server enable traps entity</td>
</tr>
<tr>
<td></td>
<td>snmp-server enable traps entity</td>
</tr>
<tr>
<td></td>
<td>entity_fan_status_change</td>
</tr>
<tr>
<td></td>
<td>snmp-server enable traps entity</td>
</tr>
<tr>
<td></td>
<td>entity_mib_change</td>
</tr>
<tr>
<td></td>
<td>snmp-server enable traps entity</td>
</tr>
<tr>
<td></td>
<td>entity_module_inserted</td>
</tr>
<tr>
<td></td>
<td>snmp-server enable traps entity</td>
</tr>
<tr>
<td></td>
<td>entity_module_removed</td>
</tr>
<tr>
<td></td>
<td>snmp-server enable traps entity</td>
</tr>
<tr>
<td></td>
<td>entity_module_status_change</td>
</tr>
<tr>
<td></td>
<td>snmp-server enable traps entity</td>
</tr>
<tr>
<td></td>
<td>entity_power_out_change</td>
</tr>
<tr>
<td></td>
<td>snmp-server enable traps entity</td>
</tr>
<tr>
<td></td>
<td>entity_power_status_change</td>
</tr>
<tr>
<td></td>
<td>snmp-server enable traps entity</td>
</tr>
<tr>
<td></td>
<td>entity_unrecognised_module</td>
</tr>
<tr>
<td>CISCO-FEATURE-CONTROL-MIB</td>
<td>snmp-server enable traps feature-control</td>
</tr>
<tr>
<td></td>
<td>snmp-server enable traps feature-control</td>
</tr>
<tr>
<td></td>
<td>FeatureOpStatusChange</td>
</tr>
<tr>
<td>CISCO-HSRP-MIB</td>
<td>snmp-server enable traps hsrp</td>
</tr>
<tr>
<td></td>
<td>snmp-server enable traps hsrp state-change</td>
</tr>
<tr>
<td>CISCO-LICENSE-MGR-MIB</td>
<td>snmp-server enable traps license</td>
</tr>
<tr>
<td></td>
<td>snmp-server enable traps license</td>
</tr>
<tr>
<td></td>
<td>notify-license-expiry</td>
</tr>
<tr>
<td></td>
<td>snmp-server enable traps license</td>
</tr>
<tr>
<td></td>
<td>notify-license-expiry-warning</td>
</tr>
<tr>
<td></td>
<td>snmp-server enable traps license</td>
</tr>
<tr>
<td></td>
<td>notify-licensefile-missing</td>
</tr>
<tr>
<td></td>
<td>snmp-server enable traps license</td>
</tr>
<tr>
<td></td>
<td>notify-no-license-for-feature</td>
</tr>
</tbody>
</table>

Enabling SNMP Notifications

Configuring SNMP
<table>
<thead>
<tr>
<th>MIB</th>
<th>Related Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>IF-MIB</td>
<td>snmp-server enable traps link</td>
</tr>
<tr>
<td></td>
<td>snmp-server enable traps link</td>
</tr>
<tr>
<td></td>
<td>IETF-extended-linkDown</td>
</tr>
<tr>
<td></td>
<td>snmp-server enable traps link</td>
</tr>
<tr>
<td></td>
<td>IETF-extended-linkUp</td>
</tr>
<tr>
<td></td>
<td>snmp-server enable traps link</td>
</tr>
<tr>
<td></td>
<td>cisco-extended-linkDown</td>
</tr>
<tr>
<td></td>
<td>snmp-server enable traps link</td>
</tr>
<tr>
<td></td>
<td>cisco-extended-linkUp</td>
</tr>
<tr>
<td></td>
<td>snmp-server enable traps link linkDown</td>
</tr>
<tr>
<td></td>
<td>snmp-server enable traps link Up</td>
</tr>
<tr>
<td>OSPF-MIB, OSPF-TRAP-MIB</td>
<td>snmp-server enable traps ospf [tag]</td>
</tr>
<tr>
<td></td>
<td>snmp-server enable traps ospf lsa</td>
</tr>
<tr>
<td></td>
<td>snmp-server enable traps ospf rate-limit <em>rate</em></td>
</tr>
<tr>
<td>CISCO-RF-MIB</td>
<td>snmp-server enable traps rf</td>
</tr>
<tr>
<td></td>
<td>snmp-server enable traps rf</td>
</tr>
<tr>
<td></td>
<td>redundancy.Framework</td>
</tr>
<tr>
<td>CISCO-RMON-MIB</td>
<td>snmp-server enable traps rmon</td>
</tr>
<tr>
<td></td>
<td>snmp-server enable traps rmon fallingAlarm</td>
</tr>
<tr>
<td></td>
<td>snmp-server enable traps rmon hcFallingAlarm</td>
</tr>
<tr>
<td></td>
<td>snmp-server enable traps rmon hcRisingAlarm</td>
</tr>
<tr>
<td></td>
<td>snmp-server enable traps rmon risingAlarm</td>
</tr>
<tr>
<td>SNMPv2-MIB</td>
<td>snmp-server enable traps snmp</td>
</tr>
<tr>
<td></td>
<td>snmp-server enable traps snmp authentication</td>
</tr>
<tr>
<td>CISCO-MAC-NOTIFICATION-MIB</td>
<td>snmp-server enable trap link</td>
</tr>
<tr>
<td></td>
<td>cmn-mac-move-notification</td>
</tr>
<tr>
<td>CISCO-PORT-STORM-CONTROL-MIB</td>
<td>storm-control action trap</td>
</tr>
<tr>
<td>CISCO-STP-EXTENSIONS-MIB</td>
<td>snmp-server enable traps stpx</td>
</tr>
<tr>
<td></td>
<td>stpxMstInconsistencyUpdate</td>
</tr>
<tr>
<td>CISCO-STP-BRIDGE-MIB</td>
<td>snmp-server enable traps bridge</td>
</tr>
<tr>
<td></td>
<td>snmp-server enable traps bridge newroot</td>
</tr>
<tr>
<td></td>
<td>snmp-server enable traps bridge topologychange</td>
</tr>
</tbody>
</table>
### Enabling SNMP Notifications

<table>
<thead>
<tr>
<th>MIB</th>
<th>Related Commands</th>
</tr>
</thead>
</table>
| CISCO-STPX-MIB | `snmp-server enable traps stpx`  
`snmp-server enable traps stpx inconsistency`  
`snmp-server enable traps stpx loop-inconsistency`  
`snmp-server enable traps stpx root-inconsistency` |
| CISCO-SYSTEM-EXT-MIB | `snmp-server enable traps sysmgr`  
`snmp-server enable traps sysmgr cseFailSwCoreNotifyExtended` |
| UPGRADE-MIB | `snmp-server enable traps upgrade`  
`snmp-server enable traps upgrade UpgradeJobStatusNotify`  
`snmp-server enable traps upgrade UpgradeOpNotifyOnCompletion` |
| VTP-MIB | `snmp-server enable traps vtp`  
`snmp-server enable traps vtp notifs`  
`snmp-server enable traps vtp vlancreate`  
`snmp-server enable traps vtp vlannedelete` |

Use the following commands in the configuration mode shown to enable the specified notification:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>snmp-server enable traps</code></td>
<td>Enables all SNMP notifications.</td>
</tr>
</tbody>
</table>
| **Example:**  
`switch(config)# snmp-server enable traps` |  |
| `snmp-server enable traps aaa [server-state-change]` | Enables the AAA SNMP notifications. Optionally, enables the following specific notifications:  
• `server-state-change`—Enables AAA server state-change notifications. |
| **Example:**  
`switch(config)# snmp-server enable traps aaa` |  |
| `snmp-server enable traps bgp` | Enables Border Gateway Protocol (BGP) SNMP notifications. |
| **Example:**  
`switch(config)# snmp-server enable traps bgp` |  |
| `snmp-server enable traps bridge [newroot] [topologychange]` | Enables STP bridge SNMP notifications. Optionally, enables the following specific notifications:  
• `newroot`—Enables STP new root bridge notifications.  
• `topologychange`—Enables STP bridge topology-change notifications. |
| **Example:**  
`switch(config)# snmp-server enable traps bridge bridge` |  |
<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **snmp-server enable traps callhome** [event-notify] [smtp-send-fail] | Enables Call Home notifications. Optionally, enables the following specific notifications:  
  - **event-notify**—Enables Call Home external event notifications.  
  - **smtp-send-fail**—Enables Simple Mail Transfer Protocol (SMTP) message send fail notifications. |
| **Example:**  
  switch(config)# snmp-server enable traps callhome | |
| **snmp-server enable traps config** [ccmCLIRunningConfigChanged] | Enables SNMP notifications for configuration changes.  
  - **ccmCLIRunningConfigChanged**—Enables SNMP notifications for configuration changes in the running or startup configuration. |
| **Example:**  
  switch(config)# snmp-server enable traps config | |
| **snmp-server enable traps eigrp** [tag] | Enables CISCO-EIGRP-MIB SNMP notifications. |
| **Example:**  
  switch(config)# snmp-server enable traps eigrp | |
| **snmp-server enable traps entity** [entity_fan_status_change] [entity_mib_change] [entity_module_inserted] [entity_module_removed] [entity_module_status_change] [entity_power_out_change] [entity_power_status_change] [entity_unrecognised_module] | Enables ENTITY-MIB SNMP notifications. Optionally, enables the following specific notifications:  
  - **entity_fan_status_change**—Enables entity fan status-change notifications.  
  - **entity_mib_change**—Enables entity MIB change notifications.  
  - **entity_module_inserted**—Enables entity module inserted notifications.  
  - **entity_module_removed**—Enables entity module removed notifications.  
  - **entity_module_status_change**—Enables entity module status-change notifications.  
  - **entity_power_out_change**—Enables entity power-out change notifications.  
  - **entity_power_status_change**—Enables entity power status-change notifications.  
  - **entity_unrecognised_module**—Enables entity unrecognized module notifications. |
| **Example:**  
  switch(config)# snmp-server enable traps entity | |
### Enabling SNMP Notifications

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **snmp-server enable traps feature-control [FeatureOpStatusChange]** | Enables feature-control SNMP notifications. Optionally, enables the following specific notifications:  
  - **FeatureOpStatusChange**—Enables feature operation status-change notifications. |
| **snmp-server enable traps hsrp state-change** | Enables CISCO-HSRP-MIB SNMP notifications. Optionally, enables the following specific notifications:  
  - **state-change**—Enables HSRP state-change notifications. |
| **snmp-server enable traps license [notify-license-expiry] [notify-license-expiry-warning] [notify-licensefile-missing] [notify-no-license-for-feature]** | Enables ENTITY-MIB SNMP notifications. Optionally, enables the following specific notifications:  
  - **notify-license-expiry**—Enables license expiry notifications.  
  - **notify-license-expiry-warning**—Enables license expiry warning notifications.  
  - **notify-licensefile-missing**—Enables license file-missing notifications.  
  - **notify-no-license-for-feature**—Enables no-license-installed-for-feature notifications. |

**Example:**

```bash
switch(config)# snmp-server enable traps feature-control
```

```bash
switch(config)# snmp-server enable traps hsrp state-change
```

```bash
switch(config)# snmp-server enable traps license
```

```bash
switch(config)# snmp-server enable traps
```
### Enabling SNMP Notifications

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `snmp-server enable traps link [cieLinkDown] [cieLinkUp] [cmn-mac-move-notification] [IETF-extended-linkDown] [IETF-extended-linkUp] [cisco-extended-linkDown] [cisco-extended-linkUp] [linkDown] [linkUp]` | Enables IF-MIB link notifications. Optionally, enables the following specific notifications:  
- **IETF-extended-linkDown**—Enables Cisco extended link state down notifications.  
- **IETF-extended-linkUp**—Enables Cisco extended link state up notifications.  
- **cmn-mac-move-notification**—Enables MAC address move notifications.  
- **cisco-extended-linkDown**—Enables Internet Engineering Task Force (IETF) extended link state down notifications.  
- **cisco-extended-linkUp**—Enables Internet Engineering Task Force (IETF) extended link state up notifications.  
- **linkDown**—Enables IETF link state down notifications.  
- **linkUp**—Enables IETF link state up notifications.  |
| `snmp-server enable traps ospf [tag] [lsa]` | Enables Open Shortest Path First (OSPF) notifications. Optionally, enables the following specific notifications:  
- **lsa**—Enables OSPF link state advertisement (LSA) notifications.  |
| `snmp-server enable traps rf [redundancy-framework]` | Enables redundancy framework (RF) SNMP notifications. Optionally, enables the following specific notifications:  
- **redundancy-framework**—Enables RF supervisor switchover MIB notifications.  |
### Enabling SNMP Notifications

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `snmp-server enable traps rmon [fallingAlarm] [hcFallingAlarm] [hcRisingAlarm] [risingAlarm]` | Enables remote monitoring (RMON) SNMP notifications. Optionally, enables the following specific notifications:  
  - `fallingAlarm`—Enables RMON falling alarm notifications.  
  - `hcFallingAlarm`—Enables RMON high-capacity falling alarm notifications.  
  - `hcRisingAlarm`—Enables RMON high-capacity rising alarm notifications.  
  - `risingAlarm`—Enables RMON rising alarm notifications.  
  
  Example:  
  `switch(config)# snmp-server enable traps rmon`

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `snmp-server enable traps snmp [authentication]` | Enables general SNMP notifications. Optionally, enables the following specific notifications:  
  - `authentication`—Enables SNMP authentication notifications.  
  
  Example:  
  `switch(config)# snmp-server enable traps snmp`

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `snmp-server enable traps stpx [inconsistency] [loop-inconsistency] [root-inconsistency]` | Enables remote monitoring (RMON) SNMP notifications. Optionally, enables the following specific notifications:  
  - `inconsistency`—Enables SNMP STP X MIB inconsistency update notifications.  
  - `loop-inconsistency`—Enables SNMP STP X MIB loop-inconsistency update notifications.  
  - `root-inconsistency`—Enables SNMP STP X MIB root-inconsistency update notifications.  
  
  Example:  
  `switch(config)# snmp-server enable traps stpx`

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `snmp-server enable traps syslog [message-generated]` | Sends syslog messages as traps to the defined SNMP host. Optionally, enables the following specific notifications:  
  - `message-generated`—Enables software log message generated notifications.  
  
  Example:  
  `switch(config)# snmp-server enable traps syslog`

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `snmp-server enable traps sysmgr [cseFailSwCoreNotifyExtended]` | Enables software change notifications. Optionally, enables the following specific notifications:  
  - `cseFailSwCoreNotifyExtended`—Enables software core notifications.  
  
  Example:  
  `switch(config)# snmp-server enable traps sysmgr`
Disabling Link Notifications on an Interface

You can disable linkUp and linkDown notifications on an individual interface. You can use this limit notifications on flapping interface (an interface that transitions between up and down repeatedly).

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch# configure terminal switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface type slot/port</td>
<td>Disables SNMP link-state traps for the interface. This command is enabled by default.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config)# interface ethernet 2/2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>no snmp trap link-status</td>
<td>Disables SNMP link-state traps for the interface. This command is enabled by default.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config-if)# no snmp trap link-status</td>
<td></td>
</tr>
</tbody>
</table>
Displaying SNMP ifIndex for an Interface

The SNMP ifIndex is used across multiple SNMP MIBs to link related interface information.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> show interface snmp-ifindex</td>
<td>Displays the persistent SNMP ifIndex value from the IF-MIB for all interfaces. Optionally, use the</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch# show interface snmp-ifindex</td>
<td></td>
</tr>
<tr>
<td>grep -i Eth12/1</td>
<td>Eth12/1 441974784 (0x1a580000)</td>
</tr>
</tbody>
</table>

Enabling a One-Time Authentication for SNMP over TCP

You can enable a one-time authentication for SNMP over a TCP session.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> snmp-server tcp-session [auth]</td>
<td>Enables a one-time authentication for SNMP over a TCP session. The default is disabled.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config)# snmp-server tcp-session</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> (Optional) copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config)# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

Assigning SNMP Device Contact and Location Information

You can assign the device contact information, which is limited to 32 characters (without spaces) and the device location.
Configuring SNMP

### Configuring the Context to Network Entity Mapping

You can configure an SNMP context to map to a logical network entity, such as a protocol instance or VRF.

#### Before you begin

Determine the logical network entity instance. For more information on VRFs and protocol instances, see the Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide or the Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><code>switch(config)#</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> snmp-server contact name</td>
<td>Configures sysContact, which is the SNMP contact name.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>switch(config)# snmp-server contact Admin</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> snmp-server location name</td>
<td>Configures sysLocation, which is the SNMP location.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>switch(config)# snmp-server location Lab-7</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> (Optional) show snmp</td>
<td>Displays information about one or more destination profiles.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>switch(config)# show snmp</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> (Optional) copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>switch(config)# copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Command or Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong>&lt;br&gt;switch(config)# snmp-server context public1 vrf red</td>
<td>The <strong>no</strong> option deletes the mapping between an SNMP context and a protocol instance, VRF, or topology. <strong>Note</strong> Do not enter an instance, VRF, or topology to delete a context mapping. If you use the instance, VRF, or topology keywords, you configure a mapping between the context and a zero-length string.</td>
</tr>
<tr>
<td><strong>Step 3</strong>&lt;br&gt;(Optional) <strong>snmp-server mib community-map</strong>&lt;br&gt;community-name context context-name</td>
<td>Maps an SNMPv2c community to an SNMP context. The names can be any alphanumeric string up to 32 characters.</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;switch(config)# snmp-server mib community-map public context public1</td>
<td>Displays information about one or more SNMP contexts.</td>
</tr>
<tr>
<td><strong>Step 4</strong>&lt;br&gt;(Optional) <strong>show snmp context</strong></td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;switch(config)# show snmp context</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong>&lt;br&gt;(Optional) <strong>copy running-config startup-config</strong></td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;switch(config)# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

### Disabling SNMP

You can disable SNMP on the device.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong>&lt;br&gt;<strong>configure terminal</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;switch# configure terminal&lt;br&gt;switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong>&lt;br&gt;<strong>no snmp-server protocol enable</strong></td>
<td>Disables SNMP. SNMP is enabled by default.</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;switch(config)# no snmp-server protocol enable</td>
<td></td>
</tr>
</tbody>
</table>

### Managing the SNMP Server Counter Cache Update Timer

You can modify how long, in seconds Cisco NX-OS holds the cache port state.
### Configuring SNMP

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> snmp-server counter cache timeout seconds</td>
<td>Defines how long in seconds, the port states are held in the local cache. The counter cache is enabled by default, and the default cache timeout value is 10 seconds. When disabled, the default cache timeout value is 50 seconds. The range is 1-3600.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# snmp-server counter cache</td>
<td></td>
</tr>
<tr>
<td>timeout 1200</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>For end of row (EoR) switching - The range is from 1 to 3600.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> (Optional) show running-config snmp all</td>
<td>Displays the configured SNMP-server counter cache update timeout value.</td>
</tr>
<tr>
<td>i cac</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# copy running-config snmp all</td>
<td></td>
</tr>
<tr>
<td>i cac</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> no snmp-server counter cache enable</td>
<td>Disables the counter cache update.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# no snmp-server counter cache enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Modifying the AAA Synchronization Time

You can modify how long Cisco NX-OS holds the synchronized user configuration.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> snmp-server aaa-user cache-timeout seconds</td>
<td>Configures how long the AAA synchronized user configuration stays in the local cache. The range is from 1 to 86400 seconds. The default is 3600.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# snmp-server aaa-user cache-timeout 1200</td>
<td></td>
</tr>
</tbody>
</table>
Configuring the SNMP Local Engine ID

Beginning with Cisco NX-OS Release 7.0(3)I6(1), you can configure the engine ID on a local device.

Note

After you configure the SNMP local engine ID, you must reconfigure all SNMP users, any host configured with the V3 users, and the community strings. Beginning with Cisco NX-OS Release 7.0(3)I7(1), you need to reconfigure only the SNMP users and community strings.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch# configure terminal switch(config)#</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>snmp-server engineID local engineid-string</td>
<td>Changes the SNMP engine ID of the local device.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# snmp-server engineID local AA:BB:CC:1A:2C:10</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>show snmp engineID</td>
<td>Displays the identification of the configured SNMP engine.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# show snmp engineID</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>[no] snmp-server engineID local engineid-string</td>
<td>Disables the local engine ID and the default auto-generated engine ID is configured.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# no snmp-server engineID local AA:BB:CC:1A:2C:10</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>Required: copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Verifying SNMP Configuration

To display SNMP configuration information, perform one of the following tasks:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interface snmp-ifindex</td>
<td>Displays the SNMP ifIndex value for all interfaces (from IF-MIB).</td>
</tr>
<tr>
<td>show running-config snmp [all]</td>
<td>Displays the SNMP running configuration.</td>
</tr>
<tr>
<td>show snmp</td>
<td>Displays the SNMP status.</td>
</tr>
<tr>
<td>show snmp community</td>
<td>Displays the SNMP community strings. <strong>Note</strong> If the name of the SNMP context in the snmp-server mib community-map command is more than 11 characters, the output of the show snmp community command is displayed in a vertical format instead of a tabular format.</td>
</tr>
<tr>
<td>show snmp context</td>
<td>Displays the SNMP context mapping.</td>
</tr>
<tr>
<td>show snmp engineID</td>
<td>Displays the SNMP engineID.</td>
</tr>
<tr>
<td>show snmp group</td>
<td>Displays SNMP roles.</td>
</tr>
<tr>
<td>show snmp host</td>
<td>Displays information about configured SNMP hosts.</td>
</tr>
<tr>
<td>show snmp session</td>
<td>Displays SNMP sessions.</td>
</tr>
<tr>
<td>show snmp source-interface</td>
<td>Displays information about configured source interfaces.</td>
</tr>
<tr>
<td>show snmp trap</td>
<td>Displays the SNMP notifications enabled or disabled.</td>
</tr>
<tr>
<td>show snmp user</td>
<td>Displays SNMPv3 users.</td>
</tr>
</tbody>
</table>
Configuration Examples for SNMP

This example shows how to configure Cisco NX-OS to send the Cisco linkUp or Down notifications to one notification host receiver using the Blue VRF and defines two SNMP users, Admin and NMS:

```plaintext
configure terminal
snmp-server contact Admin@company.com
snmp-server user Admin auth sha abcd1234 priv abcdefgh
snmp-server user NMS auth sha abcd1234 priv abcdefgh engineID 00:00:00:63:00:01:00:22:32:15:10:03
snmp-server host 192.0.2.1 informs version 3 auth NMS
snmp-server host 192.0.2.1 use-vrf Blue
snmp-server enable traps link cisco
```

This example shows how to configure SNMP to send traps using an inband port configured at the host level:

```plaintext
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# snmp-server host 171.71.48.164 version 2c public
switch(config)# snmp-server host 171.71.48.164 source-interface ethernet 1/2
```

This example shows how to configure SNMP to send traps using a globally configured inband port:

```plaintext
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# snmp-server source-interface traps ethernet 1/2
```

This example shows how to map VRF red to the SNMPv2c public community string:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# vrf context red
switch(config-vrf)# exit
switch(config)# snmp-server context public1 vrf red
switch(config)# snmp-server mib community-map public context public1
```

This example shows how to map OSPF instance Enterprise to the same SNMPv2c public community string:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# feature ospf
switch(config)# router ospf Enterprise
switch(config-router)# exit
switch(config)# snmp-server context public1 instance Enterprise
switch(config)# snmp-server mib community-map public context public1
```

### Additional References

#### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP ACLs and AAA</td>
<td><em>Cisco Nexus 9000 Series NX-OS Security Configuration Guide</em></td>
</tr>
<tr>
<td>MIBs</td>
<td><em>Cisco Nexus 7000 Series and 9000 Series NX-OS MIB Quick Reference</em></td>
</tr>
</tbody>
</table>

#### RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 3414</td>
<td><em>User-based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3)</em></td>
</tr>
<tr>
<td>RFC 3415</td>
<td><em>View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)</em></td>
</tr>
</tbody>
</table>

#### MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIBs related to SNMP</td>
<td>To locate and download supported MIBs, go to the following URL:</td>
</tr>
<tr>
<td></td>
<td>Nexus9000MIBSupportList.html</td>
</tr>
</tbody>
</table>
Configuring SNMP

MIBs
CHAPTER 12

Configuring RMON

This chapter describes how to configure the remote monitoring (RMON) feature on Cisco NX-OS devices.

This chapter contains the following sections:

• About RMON, on page 179
• Licensing Requirements for RMON, on page 181
• Guidelines and Limitations for RMON, on page 181
• Default Settings for RMON, on page 181
• Configuring RMON, on page 181
• Verifying the RMON Configuration, on page 183
• Configuration Examples for RMON, on page 184
• Additional References, on page 184

About RMON

RMON is a Simple Network Management Protocol (SNMP) Internet Engineering Task Force (IETF) standard monitoring specification that allows various network agents and console systems to exchange network monitoring data. Cisco NX-OS supports RMON alarms, events, and logs to monitor Cisco NX-OS devices.

An RMON alarm monitors a specific management information base (MIB) object for a specified interval, triggers an alarm at a specified threshold value (threshold), and resets the alarm at another threshold value. You can use alarms with RMON events to generate a log entry or an SNMP notification when the RMON alarm triggers.

RMON is enabled by default, but no alarms are configured in Cisco NX-OS. You can configure RMON alarms by using the CLI or an SNMP-compatible network management station.

RMON Alarms

You can set an alarm on any MIB object that resolves into an SNMP INTEGER type. The specified object must be an existing SNMP MIB object in standard dot notation (for example, 1.3.6.1.2.1.2.2.1.14 represents ifInOctets.14).

When you create an alarm, you specify the following parameters:

• MIB object to monitor.

• Sampling interval—The interval that the device uses to collect a sample value of the MIB object.
• Sample type—Absolute samples take the current snapshot of the MIB object value. Delta samples take two consecutive samples and calculate the difference between them.

• Rising threshold—The value at which the device triggers a rising alarm or resets a falling alarm.

• Falling threshold—The value at which the device triggers a falling alarm or resets a rising alarm.

• Events—The action that the device takes when an alarm (rising or falling) triggers.

---

**Note**

Use the halarms option to set an alarm on a 64-bit integer MIB object.

For example, you can set a delta type rising alarm on an error counter MIB object. If the error counter delta exceeds this value, you can trigger an event that sends an SNMP notification and logs the rising alarm event. This rising alarm will not occur again until the delta sample for the error counter drops below the falling threshold.

---

**Note**

The falling threshold must be less than the rising threshold.

---

**RMON Events**

You can associate a particular event to each RMON alarm. RMON supports the following event types:

• SNMP notification—Sends an SNMP risingAlarm or fallingAlarm notification when the associated alarm triggers.

• Log—Adds an entry in the RMON log table when the associated alarm triggers.

• Both—Sends an SNMP notification and adds an entry in the RMON log table when the associated alarm triggers.

You can specify a different even for a falling alarm and a rising alarm.

---

**Note**

You may choose to use the default RMON events template configuration or you can delete these entries and create new RMON events. Until you create RMON alarm configurations, no alarms will be triggered by these configurations.

---

**High Availability for RMON**

Cisco NX-OS supports stateless restarts for RMON. After a reboot or supervisor switchover, Cisco NX-OS applies the running configuration.

**Virtualization Support for RMON**

Cisco NX-OS supports one instance of RMON.
RMON is virtual routing and forwarding (VRF) aware. You can configure RMON to use a particular VRF to reach the RMON SMTP server.

**Licensing Requirements for RMON**

<table>
<thead>
<tr>
<th>Product</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco NX-OS</td>
<td>RMON requires no license. Any feature not included in a license package is bundled with the nx-os image and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the Cisco NX-OS Licensing Guide.</td>
</tr>
</tbody>
</table>

**Guidelines and Limitations for RMON**

RMON has the following configuration guidelines and limitations:

- You must configure an SNMP user and a notification receiver to use the SNMP notification event type.
- You can configure an RMON alarm only on a MIB object that resolves to an integer.
- When you configure an RMON alarm, the object identifier must be complete with its index so that it refers to only one object. For example, 1.3.6.1.2.1.2.2.1.14 corresponds to cpmCPUTotal5minRev, and .1 corresponds to index cpmCPUTotalIndex, which creates object identifier 1.3.6.1.2.1.2.2.1.14.1.

**Default Settings for RMON**

The following table lists the default settings for RMON parameters.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>RMON</td>
<td>Enabled</td>
</tr>
<tr>
<td>Alarms</td>
<td>None configured</td>
</tr>
</tbody>
</table>

**Configuring RMON**

Be aware that the Cisco NX-OS commands for this feature may differ from those commands used in Cisco IOS.
Configuring RMON Alarms

You can configure RMON alarms on any integer-based SNMP MIB object. You can optionally specify the following parameters:

- The event number to trigger if the rising or falling threshold exceeds the specified limit.
- The owner of the alarm.

Ensure you have configured an SNMP user and enabled SNMP notifications.

Before you begin
Make sure that you have configured an SNMP user and enabled SNMP notifications.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: switch# configure terminal switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> rmon alarm index mib-object sample-interval {absolute</td>
<td>delta} rising-threshold value [event-index] falling-threshold value [event-index] [owner name]</td>
</tr>
<tr>
<td>Example: switch(config)# rmon alarm 20 1.3.6.1.2.1.2.1.4.1 2900 delta rising-threshold 1500 1 falling-threshold 0 owner test</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> rmon hcalarm index mib-object sample-interval {absolute</td>
<td>delta} rising-threshold-high value rising-threshold-low value [event-index] falling-threshold-high value falling-threshold-low value [event-index] [owner name] [storagetype type]</td>
</tr>
<tr>
<td>Example: switch(config)# rmon alarm 20 1.3.6.1.2.1.2.1.14.1.16777216 2900 delta rising-threshold-high 15 rising-threshold-low 151 falling-threshold-high 0 falling-threshold-low 0 owner test</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> (Optional) show rmon {alarms</td>
<td>hcalarms}</td>
</tr>
<tr>
<td>Example: switch(config)# show rmon alarms</td>
<td></td>
</tr>
</tbody>
</table>
Configuring RMON

Configuring RMON Events

You can configure RMON events to associate with RMON alarms. You can reuse the same event with multiple RMON alarms.

Before you begin

Make sure you have configured an SNMP user and enabled SNMP notifications.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>rmon event index [description string] [log] [trap string] [owner name]</td>
<td>Configures an RMON event. The description string, trap string, and owner name can be any alphanumeric string.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# rmon event 1 trap trap1</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>(Optional) show rmon events</td>
<td>Displays information about RMON events.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# show rmon events</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>(Optional) copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

Verifying the RMON Configuration

To display RMON configuration information, perform one of the following tasks:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show rmon alarms</td>
<td>Displays information about RMON alarms.</td>
</tr>
<tr>
<td>show rmon events</td>
<td>Displays information about RMON events.</td>
</tr>
<tr>
<td>Command</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>show rmon hcalarms</td>
<td>Displays information about RMON high-capacity alarms.</td>
</tr>
<tr>
<td>show rmon logs</td>
<td>Displays information about RMON logs.</td>
</tr>
</tbody>
</table>

**Configuration Examples for RMON**

This example shows how to create a delta rising alarm on ifInOctets.14 and associates a notification event with this alarm:

```
configure terminal
rmon alarm 20 1.3.6.1.2.1.2.2.1.14.1 2900 delta rising-threshold 1500 1 falling-threshold 0 owner test
rmon event 1 trap trap1
```

**Additional References**

**MIBs**

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIBs related to RMON</td>
<td>To locate and download supported MIBs, go to the following URL:</td>
</tr>
<tr>
<td></td>
<td>Nexus9000MIBSupportList.html</td>
</tr>
</tbody>
</table>
CHAPTER 13

Configuring Online Diagnostics

This chapter describes how to configure the generic online diagnostics (GOLD) feature on Cisco NX-OS devices.

This chapter contains the following sections:

- About Online Diagnostics, on page 185
- Licensing Requirements for Online Diagnostics, on page 188
- Guidelines and Limitations for Online Diagnostics, on page 189
- Default Settings for Online Diagnostics, on page 189
- Configuring Online Diagnostics, on page 190
- Verifying the Online Diagnostics Configuration, on page 193
- Configuration Examples for Online Diagnostics, on page 194

About Online Diagnostics

With online diagnostics, you can test and verify the hardware functionality of the device while the device is connected to a live network.

The online diagnostics contain tests that check different hardware components and verify the data path and control signals. Disruptive online diagnostic tests (such as the disruptive loopback test) and nondisruptive online diagnostic tests (such as the ASIC register check) run during bootup, line module online insertion and removal (OIR), and system reset. The nondisruptive online diagnostic tests run as part of the background health monitoring, and you can run these tests on demand.

Online diagnostics are categorized as bootup, runtime or health-monitoring diagnostics, and on-demand diagnostics. Bootup diagnostics run during bootup, health-monitoring tests run in the background, and on-demand diagnostics run once or at user-designated intervals when the device is connected to a live network.

Bootup Diagnostics

Bootup diagnostics run during bootup and detect faulty hardware before Cisco NX-OS brings a module online. For example, if you insert a faulty module in the device, bootup diagnostics test the module and take it offline before the device uses the module to forward traffic.

Bootup diagnostics also check the connectivity between the supervisor and module hardware and the data and control paths for all the ASICs. The following table describes the bootup diagnostic tests for a module and a supervisor.
Bootup diagnostics log failures to onboard failure logging (OBFL) and syslog and trigger a diagnostic LED indication (on, off, pass, or fail).

You can configure the device to either bypass the bootup diagnostics or run the complete set of bootup diagnostics.

### Runtime or Health Monitoring Diagnostics

Runtime diagnostics are also called health monitoring (HM) diagnostics. These diagnostics provide information about the health of a live device. They detect runtime hardware errors, memory errors, the degradation of hardware modules over time, software faults, and resource exhaustion.

Health monitoring diagnostics are nondisruptive and run in the background to ensure the health of a device that is processing live network traffic. You can enable or disable health monitoring tests or change their runtime interval.

The following table describes the health monitoring diagnostics and test IDs for a module and a supervisor.

<table>
<thead>
<tr>
<th>Diagnostic</th>
<th>Default Interval</th>
<th>Default Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACT2</td>
<td>30 minutes</td>
<td>active</td>
<td>Verifies the integrity of the security device on the module.</td>
</tr>
<tr>
<td>ASICRegisterCheck</td>
<td>1 minute</td>
<td>active</td>
<td>Checks read/write access to scratch registers for the ASICs on a module.</td>
</tr>
<tr>
<td>PrimaryBootROM</td>
<td>30 minutes</td>
<td>active</td>
<td>Verifies the integrity of the primary boot device on a module.</td>
</tr>
<tr>
<td>SecondaryBootROM</td>
<td>30 minutes</td>
<td>active</td>
<td>Verifies the integrity of the secondary boot device on a module.</td>
</tr>
<tr>
<td>Diagnostic</td>
<td>Default Interval</td>
<td>Default Setting</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------</td>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Module</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PortLoopback</td>
<td>On demand [for releases prior to Cisco NX-OS 7.0(3)I1(2)] 30 minutes [starting with Cisco NX-OS Release 7.0(3)I1(2)]</td>
<td>active</td>
<td>Checks diagnostics on a per-port basis on all admin down ports.</td>
</tr>
<tr>
<td>RewriteEngineLoopback</td>
<td>1 minute</td>
<td>active</td>
<td>Verifies the integrity of the nondisruptive loopback for all ports up to the 1 Engine ASIC device.</td>
</tr>
<tr>
<td>AsicMemory</td>
<td>Only on boot up</td>
<td>Only on boot up - inactive</td>
<td>Checks if the AsicMemory is consistent using the Mbist bit in the ASIC.</td>
</tr>
<tr>
<td>FpgaRegTest</td>
<td>30 seconds</td>
<td>Health monitoring test - every 30 seconds - active</td>
<td>Test the FPGA status by read/write to FPGA.</td>
</tr>
<tr>
<td><strong>Supervisor</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NVRAM</td>
<td>5 minutes</td>
<td>active</td>
<td>Verifies the sanity of the NVRAM blocks on a supervisor.</td>
</tr>
<tr>
<td>RealTimeClock</td>
<td>5 minutes</td>
<td>active</td>
<td>Verifies that the real-time clock on the supervisor is ticking.</td>
</tr>
<tr>
<td>PrimaryBootROM</td>
<td>30 minutes</td>
<td>active</td>
<td>Verifies the integrity of the primary boot device on the supervisor.</td>
</tr>
<tr>
<td>SecondaryBootROM</td>
<td>30 minutes</td>
<td>active</td>
<td>Verifies the integrity of the secondary boot device on the supervisor.</td>
</tr>
<tr>
<td>BootFlash</td>
<td>30 minutes</td>
<td>active</td>
<td>Verifies access to the bootflash devices.</td>
</tr>
<tr>
<td>USB</td>
<td>30 minutes</td>
<td>active</td>
<td>Verifies access to the USB devices.</td>
</tr>
<tr>
<td>SystemMgmtBus</td>
<td>30 seconds</td>
<td>active</td>
<td>Verifies the availability of the system management bus.</td>
</tr>
<tr>
<td>Mce</td>
<td>30 minutes</td>
<td>Health monitoring test - 30 minutes - active</td>
<td>This test uses the mcd_dameon and reports any machine check error reported by the Kernel.</td>
</tr>
<tr>
<td>Pcie</td>
<td>Only on boot up</td>
<td>Only on boot up - inactive</td>
<td>Reads PCIe status registers and check for any error on the PCIe device.</td>
</tr>
</tbody>
</table>
### On-Demand Diagnostics

On-demand tests help localize faults and are usually needed in one of the following situations:

- To respond to an event that has occurred, such as isolating a fault.
- In anticipation of an event that may occur, such as a resource exceeding its utilization limit.

You can run all the health monitoring tests on demand. You can schedule on-demand diagnostics to run immediately.

You can also modify the default interval for a health monitoring test.

### High Availability

A key part of high availability is detecting hardware failures and taking corrective action while the device runs in a live network. Online diagnostics in high availability detect hardware failures and provide feedback to high availability software components to make switchover decisions.

Cisco NX-OS supports stateless restarts for online diagnostics. After a reboot or supervisor switchover, Cisco NX-OS applies the running configuration.

### Virtualization Support

Online diagnostics are virtual routing and forwarding (VRF) aware. You can configure online diagnostics to use a particular VRF to reach the online diagnostics SMTP server.

### Licensing Requirements for Online Diagnostics

<table>
<thead>
<tr>
<th>Product</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco NX-OS</td>
<td>Online diagnostics require no license. Any feature not included in a license package is bundled with the nx-os image and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the Cisco NX-OS Licensing Guide.</td>
</tr>
</tbody>
</table>
Guidelines and Limitations for Online Diagnostics

Online diagnostics has the following configuration guidelines and limitations:

- The following Cisco Nexus platform switches and line cards do not support the run-time PortLoopback test but do support the Bootup PortLoopback test:
  - N9K-C92160YC-X
  - N9K-C92304QC
  - N9K-C9264PQ
  - N9K-C9272Q
  - N9K-C9232C
  - N9K-C9236C
  - N9K-C9256PV
  - N9K-C92300YC
  - N9K-C93108TC-EX
  - N9K-C93108TC-EX-24
  - N9K-C93180LC-EX
  - N9K-C93180YC-EX
  - N9K-C93180YC-EXU
  - N9K-C93180YC-EX-24
  - N9K-C93180YC-FX3S
  - N9K-X9736C-EX line card
  - N9K-X97160YC-EX line card
  - N9K-X9732C-EX line card
  - N9K-X9732C-EXM line card

- You cannot run disruptive online diagnostic tests on demand.

- Interface Rx and Tx packet counters are incremented (approximately four packets every 15 minutes) for ports in the shutdown state.

- The PortLoopback test is periodic, so the packet counter is incremented on admin down ports every 30 minutes. The test runs only on admin down ports. When a port is unshut, the counters are not affected.

Default Settings for Online Diagnostics

The following table lists the default settings for online diagnostic parameters.
Be aware that the Cisco NX-OS commands for this feature may differ from those commands used in Cisco IOS.

Note

Setting the Bootup Diagnostic Level

You can configure the bootup diagnostics to run the complete set of tests, or you can bypass all bootup diagnostic tests for a faster module bootup time.

Note

We recommend that you set the bootup online diagnostics level to complete. We do not recommend bypassing the bootup online diagnostics.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: switch# configure terminal switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> diagnostic bootup level {complete</td>
<td>minimal</td>
</tr>
<tr>
<td>Example: switch(config)# diagnostic bootup level complete</td>
<td>• complete—Perform a complete set of bootup diagnostics. The default is complete.</td>
</tr>
<tr>
<td></td>
<td>• minimal—Perform a minimal set of bootup diagnostics for the supervisor engine and bootup port loopback tests.</td>
</tr>
<tr>
<td></td>
<td>• bypass—Do not perform any bootup diagnostics.</td>
</tr>
<tr>
<td><strong>Step 3</strong> (Optional) show diagnostic bootup level</td>
<td>Displays the bootup diagnostic level (bypass or complete) that is currently in place on the device.</td>
</tr>
<tr>
<td>Example: switch(config)# show diagnostic bootup level</td>
<td></td>
</tr>
</tbody>
</table>
### Activating a Diagnostic Test

You can set a diagnostic test as active and optionally modify the interval (in hours, minutes, and seconds) at which the test runs.

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
| Example: | `switch# configure terminal
switch(config)#` | |
| **Step 2** | `diagnostic monitor interval module slot test [test-id | name | all] hour hour minute second second` | Configures the interval at which the specified test is run. If no interval is set, the test runs at the interval set previously, or the default interval. The argument ranges are as follows: |
| Example: | `switch(config)# diagnostic monitor interval module 6 test 3 hour 1 min 0 second 0` | |
| **Step 3** | `[no] diagnostic monitor module slot test [test-id | name | all]` | Activates the specified test. The argument ranges are as follows: |
| Example: | `switch(config)# diagnostic monitor interval module 6 test 3` | |
| | | |

The `[no]` form of this command inactivates the specified test. Inactive tests keep their current configuration but do not run at the scheduled interval.
## Starting or Stopping an On-Demand Diagnostic Test

You can start or stop an on-demand diagnostic test. You can optionally modify the number of iterations to repeat this test, and the action to take if the test fails.

We recommend that you only manually start a disruptive diagnostic test during a scheduled network maintenance time.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>(Optional) <code>diagnostic ondemand iteration number</code></td>
<td>Configures the number of times that the on-demand test runs. The range is from 1 to 999. The default is 1.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>switch# diagnostic ondemand iteration 5</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>(Optional) `diagnostic ondemand action-on-failure {continue failure-count num-fails</td>
<td>stop}`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>switch# diagnostic ondemand action-on-failure stop</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Required: `diagnostic start module slot test [test-id</td>
<td>name</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>switch# diagnostic start module 6 test all</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Required: `diagnostic stop module slot test [test-id</td>
<td>name</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>switch# diagnostic stop module 6 test all</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>(Optional) <code>show diagnostic status module slot</code></td>
<td>Verifies that the diagnostic has been scheduled.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>switch# show diagnostic status module 6</code></td>
<td></td>
</tr>
</tbody>
</table>
Simulating Diagnostic Results

You can simulate a diagnostic test result.

### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>diagnostic test simulation module slot test test-id {fail</td>
<td>random-fail</td>
</tr>
<tr>
<td>Example:</td>
<td>switch# diagnostic test simulation module 2 test 2 fail</td>
<td></td>
</tr>
</tbody>
</table>

Clearing Diagnostic Results

You can clear diagnostic test results.

### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>diagnostic clear result module [slot</td>
<td>all] test test-id {all}</td>
</tr>
<tr>
<td>Example:</td>
<td>switch# diagnostic clear result module 2 test all</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>diagnostic test simulation module slot test test-id clear</td>
<td>Clears the simulated test result. The test-id range is from 1 to 14.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch# diagnostic test simulation module 2 test 2 clear</td>
<td></td>
</tr>
</tbody>
</table>

Verifying the Online Diagnostics Configuration

To display online diagnostics configuration information, perform one of the following tasks:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show diagnostic bootup level</td>
<td>Displays information about bootup diagnostics.</td>
</tr>
<tr>
<td>show diagnostic content module {slot</td>
<td>all}</td>
</tr>
<tr>
<td>show diagnostic description module slot test [test-name</td>
<td>all]</td>
</tr>
<tr>
<td>Command</td>
<td>Purpose</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>`show diagnostic events [error</td>
<td>info]`</td>
</tr>
<tr>
<td><code>show diagnostic ondemand setting</code></td>
<td>Displays information about on-demand diagnostics.</td>
</tr>
<tr>
<td>`show diagnostic result module slot [test [test-name</td>
<td>all]] [detail]`</td>
</tr>
<tr>
<td><code>show diagnostic simulation module slot</code></td>
<td>Displays information about a simulated diagnostic.</td>
</tr>
<tr>
<td><code>show diagnostic status module slot</code></td>
<td>Displays the test status for all tests on a module.</td>
</tr>
<tr>
<td>`show hardware capacity [eobc</td>
<td>forwarding</td>
</tr>
<tr>
<td><code>show module</code></td>
<td>Displays module information including the online diagnostic test status.</td>
</tr>
</tbody>
</table>

### Configuration Examples for Online Diagnostics

This example shows how to start all on-demand tests on module 6:
```
diagnostic start module 6 test all
```

This example shows how to activate test 2 and set the test interval on module 6:
```
configure terminal
diagnostic monitor module 6 test 2
diagnostic monitor interval module 6 test 2 hour 3 min 30 sec 0
```
Configuring the Embedded Event Manager

This chapter describes how to configure the Embedded Event Manager (EEM) to detect and handle critical events on Cisco NX-OS devices.

This chapter contains the following sections:

- About EEM, on page 195
- Licensing Requirements for EEM, on page 199
- Prerequisites for EEM, on page 199
- Guidelines and Limitations for EEM, on page 199
- Default Settings for EEM, on page 200
- Configuring EEM, on page 200
- Verifying the EEM Configuration, on page 214
- Configuration Examples for EEM, on page 215

About EEM

EEM monitors events that occur on your device and takes action to recover or troubleshoot these events, based on your configuration.

EEM consists of three major components:

- Event statements—Events to monitor from another Cisco NX-OS component that may require some action, workaround, or notification.

- Action statements—An action that EEM can take, such as executing CLI commands, sending an email through the use of Smart Call Home feature, and disabling an interface to recover from an event.

- Policies—An event that is paired with one or more actions to troubleshoot or recover from the event.

Policies

An EEM policy consists of an event statement and one or more action statements. The event statement defines the event to look for as well as the filtering characteristics for the event. The action statement defines the action EEM takes when the event occurs.

This figure shows the two basic statements in an EEM policy.
You can configure EEM policies using the command-line interface (CLI) or a VSH script.

EEM gives you a device-wide view of policy management. You configure EEM policies on the supervisor, and EEM pushes the policy to the correct module based on the event type. EEM takes any actions for a triggered event either locally on the module or on the supervisor (the default option).

EEM maintains event logs on the supervisor.

Cisco NX-OS has a number of preconfigured system policies. These system policies define many common events and actions for the device. System policy names begin with two underscore characters (_).

You can create user policies to suit your network. If you create a user policy, any actions in your policy occur after EEM triggers any system policy actions that are related to the same event as your policy.

You can also override some system policies. The overrides that you configure take the place of the system policy. You can override the event or the actions.

Use the `show event manager system-policy` command to view the preconfigured system policies and determine which policies that you can override.

---

**Note**

You should use the `show running-config eem` command to check the configuration of each policy. An override policy that consists of an event statement and no action statement triggers no action and no notification of failures.

---

**Note**

Your override policy should always include an event statement. An override policy without an event statement overrides all possible events in the system policy.

---

### Event Statements

An event is any device activity for which some action, such as a workaround or a notification, should be taken. In many cases, these events are related to faults in the device such as when an interface or a fan malfunctions.

EEM defines event filters so only critical events or multiple occurrences of an event within a specified time period trigger an associated action.

This figure shows events that are handled by EEM.
Event statements specify the event that triggers a policy to run. You can configure multiple event triggers. EEM schedules and runs policies on the basis of event statements. EEM examines the event and action commands and runs them as defined.

**Note**

If you want to allow the triggered event to process any default actions, you must configure the EEM policy to allow the event default action statement.

### Action Statements

Action statements describe the action triggered by a policy. Each policy can have multiple action statements. If no action is associated with a policy, EEM still observes events but takes no actions.

EEM supports the following actions in action statements:

- Execute any CLI commands.
- Update a counter.
- Log an exception.
- Force the shutdown of any module.
- Reload the device.
- Shut down specified modules because the power is over budget.
- Generate a syslog message.
• Generate a Call Home event.
• Generate an SNMP notification.
• Use the default action for the system policy.

Note: EEM can only process a complete action cli list of up to 1024 characters in total. If more actions are required, you must define them as a new redundant applet with same trigger.

Note: If you want to allow the triggered event to process any default actions, you must configure the EEM policy to allow the default action. For example, if you match a CLI command in a match statement, you must add the event-default action statement to the EEM policy or EEM will not allow the CLI command to execute.

Note: Verify that your action statements within your user policy or overriding policy do not negate each other or adversely affect the associated system policy.

VSH Script Policies
You can also write policies in a VSH script, using a text editor. These policies have an event statement and action statement(s) just as other policies, and these policies can either augment or override system policies. After you write your VSH script policy, copy it to the device and activate it.

Environment Variables
You can define environment variables for EEM that are available for all policies. Environment variables are useful for configuring common values that you can use in multiple policies. For example, you can create an environment variable for the IP address of an external email server.

You can use an environment variable in action statements by using the parameter substitution format.

This example shows a sample action statement to force a module 1 shutdown, with a reset reason of “EEM action.”

```
switch (config-eem-policy)# action 1.0 forceshut module 1 reset-reason "EEM action."
```

If you define an environment variable for the shutdown reason, called default-reason, you can replace that reset reason with the environment variable, as shown in the following example.

```
switch (config-eem-policy)# action 1.0 forceshut module 1 reset-reason $default-reason
```

You can reuse this environment variable in any policy.
EEM Event Correlation

You can trigger an EEM policy based on a combination of events. First, you use the tag keyword to create and differentiate multiple events in the EEM policy. Then, using a set of boolean operators (and, or, andnot), along with the count and time, you can define a combination of these events to trigger a custom action.

High Availability

Cisco NX-OS supports stateless restarts for EEM. After a reboot or supervisor switchover, Cisco NX-OS applies the running configuration.

Virtualization Support

Not all actions or events are visible. You must have network-admin privileges to configure policies.

Licensing Requirements for EEM

<table>
<thead>
<tr>
<th>Product</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco NX-OS</td>
<td>EEM requires no license. Any feature not included in a license package is bundled with the nx-os image and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the Cisco NX-OS Licensing Guide.</td>
</tr>
</tbody>
</table>

Prerequisites for EEM

EEM has the following prerequisites:

• You must have network-admin user privileges to configure EEM.

Guidelines and Limitations for EEM

EEM has the following configuration guidelines and limitations:

• The maximum number of configurable EEM policies is 500.

• Action statements within your user policy or overriding policy should not negate each other or adversely affect the associated system policy.

• To allow a triggered event to process any default actions, you must configure the EEM policy to allow the default action. For example, if you match a CLI command in a match statement, you must add the event-default action statement to the EEM policy or EEM will not allow the CLI command to execute.

• When you configure an EEM policy action to collect show tech commands, make sure to allocate enough time for the show tech commands to complete before the same action is called again.
• Note the following about override policies:
  • An override policy that consists of an event statement without an action statement triggers no action and no notification of failures.
  • An override policy without an event statement overrides all possible events in the system policy.

• The following rules apply to regular command expressions:
  • All keywords must be expanded.
  • only the * symbol can be used for argument replacement.

• Note the following about EEM event correlation:
  • EEM event correlation is supported only on the supervisor module.
  • EEM event correlation is not supported across different modules within a single policy.
  • EEM event correlation supports up to four event statements in a single policy. The event types can be the same or different, but only these event types are supported: cli, counter, module, module-failure, oir, snmp, and syslog.
  • EEM event correlation does not override the system default policies.

• When more than one event statement is included in an EEM policy, each event statement must have a tag keyword with a unique tag argument.

• Default action execution is not supported for policies that are configured with tagged events.

• You can invoke EEM from Python. For more information about Python, see the Cisco Nexus 9000 Series NX-OS Programmability Guide.

Default Settings for EEM

This table lists the default settings for EEM parameters.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>System policies</td>
<td>Active</td>
</tr>
</tbody>
</table>

Configuring EEM

You can create policies that contain actions to take based on system policies. To display information about the system policies, use the `show event manager system-policy` command.

Defining an Environment Variable

You can define a variable to serve as a parameter in an EEM policy.
## Defining a User Policy Using the CLI

You can define a user policy using the CLI to the device.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> event manager applet applet-name</td>
<td>Registers the applet with EEM and enters applet configuration mode. The applet-name can be any case-sensitive, alphanumeric string up to 29 characters.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# event manager applet</td>
<td></td>
</tr>
<tr>
<td>monitor Shutdown</td>
<td></td>
</tr>
<tr>
<td>switch(config-applet)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> (Optional) description policy-description</td>
<td>Configures a descriptive string for the policy. The string can be any alphanumeric string up to 80 characters. Enclose the string in quotation marks.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config-applet)# description</td>
<td></td>
</tr>
<tr>
<td>“Monitors interface shutdown.”</td>
<td></td>
</tr>
</tbody>
</table>
## Configuring Event Statements

Use one of the following commands in applet configuration mode to configure an event statement:

### Command

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>event application {tag} sub-system sub-system-id type event-type</td>
<td>Triggers an event when an event specification matches the subsystem ID and application event type. The range for the <code>sub-system-id</code> and for the <code>event-type</code> is from 1 to 4294967295. The <code>tag</code> keyword-argument pair identifies this specific event when multiple events are included in the policy. <strong>Note: To use this command, you must first enable the <code>feature evmed</code> command to enable generic event detectors.</strong></td>
</tr>
</tbody>
</table>

### Example:

```
switch(config-applet)# event application "conf t ; interface * ; shutdown"
```

---

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>event event-statement</strong></td>
<td>Configures the event statement for the policy. Repeat this step for multiple event statements. See Configuring Event Statements, on page 202.</td>
</tr>
</tbody>
</table>

**Example:**

```
switch(config-applet)# event cli match "conf t ; interface * ; shutdown"
```

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>(Optional)</em> tag {and</td>
<td>andnot</td>
</tr>
</tbody>
</table>

**Example:**

```
switch(config-applet)# tag one or two happens 1 in 10000
```

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>action number[.number2] action-statement</td>
<td>Configures an action statement for the policy. Repeat this step for multiple action statements. See Configuring Action Statements, on page 207.</td>
</tr>
</tbody>
</table>

**Example:**

```
switch(config-applet)# action 1.0 cli show interface e 3/1
```

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>(Optional)</em> show event manager policy-state name {module module-id}</td>
<td>Displays information about the status of the configured policy.</td>
</tr>
</tbody>
</table>

**Example:**

```
switch(config-applet)# show event manager policy-state monitor Shutdown
```

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>(Optional)</em> copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

**Example:**

```
switch(config)# copy running-config startup-config
```
### Command

**event cli [tag tag] match expression [count repeats | time seconds]**

**Example:**
```
switch(config-applet)# event cli match "conf t ; interface * ; shutdown"
```

**Purpose**
Triggers an event if you enter a command that matches the regular expression.

The `tag tag` keyword-argument pair identifies this specific event when multiple events are included in the policy.

The `repeats` range is from 1 to 65000. The time range, in seconds, is from 0 to 4294967295, where 0 indicates no time limit.

---

**event counter [tag tag] name counter entry-val entry-op {eq | ge | gt | le | lt | ne} [exit-val exit-op {eq | ge | gt | le | lt | ne}]

**Example:**
```
switch(config-applet)# event counter name mycounter entry-val 20 gt
```

**Purpose**
Triggers an event if the counter crosses the entry threshold based on the entry operation. The event resets immediately. Optionally, you can configure the event to reset after the counter passes the exit threshold.

The `tag tag` keyword-argument pair identifies this specific event when multiple events are included in the policy.

The `counter name` can be any case-sensitive, alphanumeric string up to 28 characters. The `entry` and `exit` value ranges are from 0 to 2147483647.

---

**event fanabsent [fan number] time seconds**

**Example:**
```
switch(config-applet)# event fanabsent time 300
```

**Purpose**
Triggers an event if a fan is removed from the device for more than the configured time, in seconds. The `number` range is module-dependent. The `seconds` range is from 10 to 64000.

---

**event fanbad [fan number] time seconds**

**Example:**
```
switch(config-applet)# event fanbad time 3000
```

**Purpose**
Triggers an event if a fan fails for more than the configured time, in seconds. The `number` range is module-dependent. The `seconds` range is from 10 to 64000.

---

**event fib {adjacency extra | resource tcam usage | route {extra | inconsistent | missing}}**

**Example:**
```
switch(config-applet)# event fib adjacency extra
```

**Purpose**
Triggers an event for one of the following:

- **adjacency extra**—If there is an extra route in the unicast FIB.
- **resource tcam usage**—Each time the TCAM utilization percentage becomes a multiple of 5, in either direction.
- **route {extra | inconsistent | missing}**—If a route is added, changed, or deleted in the unicast FIB.
### Command

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`event gold module {slot</td>
<td>all} test test-name [severity {major</td>
</tr>
<tr>
<td><code>event interface [tag tag] {name interface slot/port parameter}</code></td>
<td>Triggers an event if the counter is exceeded for the specified interface. The <code>tag tag</code> keyword-argument pair identifies this specific event when multiple events are included in the policy. <strong>Note</strong> To use this command, you must first enable the <code>feature evmed</code> command to enable generic event detectors.</td>
</tr>
<tr>
<td>`event memory {critical</td>
<td>minor</td>
</tr>
<tr>
<td>`event module [tag tag] status {online</td>
<td>offline</td>
</tr>
<tr>
<td>`event module-failure [tag tag] type failure-type module {slot</td>
<td>all} count repeats [time seconds]`</td>
</tr>
<tr>
<td><code>event none</code></td>
<td>Manually runs the policy event without any events specified. <strong>Note</strong> To use this command, you must first enable the <code>feature evmed</code> command to enable generic event detectors.</td>
</tr>
<tr>
<td>Command</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| event oir [tag tag] {fan | module | powersupply} | Triggers an event if the configured device element (fan, module, or power supply) is inserted or removed from the device. The **tag** keyword-argument pair identifies this specific event when multiple events are included in the policy. You can optionally configure a specific fan, module, or power supply number. The **number** range is as follows:
  * Fan number—Module dependent.
  * Module number—Device dependent.
  * Power supply number—The range is from 1 to 3. |
<p>|          | Example: |
| switch(config-applet)# event oir fan remove 4 | |
| event policy-default count repeats [time seconds] | Uses the event configured in the system policy. Use this option for overriding policies. The <strong>repeats</strong> range is from 1 to 65000. The <strong>seconds</strong> range is from 0 to 4294967295, where 0 indicates no time limit. |
|          | Example: |
| switch(config-applet)# event policy-default count 3 | |
| event poweroverbudget | Triggers an event if the power budget exceeds the capacity of the configured power supplies. |
|          | Example: |
| switch(config-applet)# event poweroverbudget | |
| event snmp [tag tag] oid oid get-type {exact | next} | Triggers an event if the SNMP OID crosses the entry threshold based on the entry operation. The event resets immediately, or optionally you can configure the event to reset after the counter passes the exit threshold. The OID is in dotted decimal notation. The <strong>tag</strong> keyword-argument pair identifies this specific event when multiple events are included in the policy. The <strong>entry</strong> and <strong>exit</strong> value ranges are from 0 to 18446744073709551615. The time, in seconds, is from 0 to 2147483647. The interval, in seconds, is from 1 to 2147483647. |
| entry-op {eq | ge | gt | le | lt | ne} entry-val entry | |
| exit-comb {and | or} | |
| exit-op {eq | ge | gt | le | lt | ne} exit-val exit | |
| exit-time time polling-interval interval | |
|          | Example: |
| switch(config-applet)# event snmp oid 1.3.6.1.2.1.31.1.1.1.6 get-type next entry-op lt 300 entry-val 0 exit-op eq 400 exit-time 30 polling-interval 300 | |
| event storm-control | Triggers an event if traffic on a port exceeds the configured storm control threshold. |
|          | Example: |
| switch(config-applet)# event storm-control | |</p>
<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `event syslog [occurs count] {pattern string | period time | priority level | tag tag}` | Triggers an event if the specified syslog threshold is exceeded. The range for the count is from 1 to 65000, and the range for the time is from 1 to 4294967295. The priority range is from 0 to 7. The `tag tag` keyword-argument pair identifies this specific event when multiple events are included in the policy. **Example:**

```
switch(config-applet)# event syslog period 500
```

| `event sysmgr memory [module module-num] major major-percent minor minor-percent clear clear-percent` | Triggers an event if the specified system manager memory threshold is exceeded. The range for the percentage is from 1 to 99. **Example:**

```
switch(config-applet)# event sysmgr memory minor 80
```

| `event sysmgr switchover count count time interval` | Triggers an event if the specified switchover count is exceeded within the time interval specified. The switchover count is from 1 to 65000. The time interval is from 0 to 2147483647. **Example:**

```
switch(config-applet)# event sysmgr switchover count 10 time 1000
```

| `event temperature [module slot] [sensor-number] threshold {any | major | minor}` | Triggers an event if the temperature sensor exceeds the configured threshold. The sensor range is from 1 to 18. **Example:**

```
switch(config-applet)# event temperature module 2 threshold any
```
### Configuring Action Statements

Use the following commands in EEM configuration mode to configure action statements:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>action number{number2} cli command1 [command2...][local]</strong></td>
<td>Runs the configured CLI commands. You can optionally run the commands on the module where the event occurred. The action label is in the format number1.number2. <em>number</em> can be any number up to 16 digits. The range for number2 is from 0 to 9.</td>
</tr>
</tbody>
</table>

---

### Configuring the Embedded Event Manager

The **event timer** command triggers an event if the specified time is reached. The range for the time is from 1 to 4294967295.

- **absolute time**—Triggers an event when the specified absolute time of day occurs.
- **countdown time**—Triggers an event when the specified time counts down to zero. The timer does not reset.
- **cron cronentry**—Triggers an event when the CRON string specification matches the current time.
- **watchdog time**—Triggers an event when the specified time counts down to zero. The timer automatically resets to the initial value and continues to count down.

The **tag** keyword-argument pair identifies this specific event when multiple events are included in the policy.

**Note**

To use this command, you must first enable the **feature evmed** command to enable generic event detectors.

---

### Event Timer Example

```
example:
switch(config-applet)# event timer absolute 
time 100 name abtimer
```

---

### Event Track Example

```
example:
switch(config-applet)# event track 1 state 
down
```

---

### Configuring Action Statements

**Purpose**

- **Triggers an event if the specified time is reached. The range for the time is from 1 to 4294967295.**
  - **absolute time**—Triggers an event when the specified absolute time of day occurs.
  - **countdown time**—Triggers an event when the specified time counts down to zero. The timer does not reset.
  - **cron cronentry**—Triggers an event when the CRON string specification matches the current time.
  - **watchdog time**—Triggers an event when the specified time counts down to zero. The timer automatically resets to the initial value and continues to count down.

The **tag** keyword-argument pair identifies this specific event when multiple events are included in the policy.

**Note**

To use this command, you must first enable the **feature evmed** command to enable generic event detectors.

---

### Event Track Example

```
example:
switch(config-applet)# event track 1 state 
down
```

---

### Configuring Action Statements

**Purpose**

- **Triggers an event if the tracked object is in the configured state.**

The **tag** keyword-argument pair identifies this specific event when multiple events are included in the policy.

The **object-number** range is from 1 to 500.
<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`action number[.number2] counter name counter value val op {dec</td>
<td>inc</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch{config-applet)# action 2.0 counter name mycounter value 20 op inc</td>
</tr>
<tr>
<td><code>action number[.number2] event-default</code></td>
<td>Executes the default action for the associated event. The action label is in the format number1.number2. number can be any number up to 16 digits. The range for number2 is from 0 to 9.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch{config-applet)# action 1.0 event-default</td>
</tr>
<tr>
<td>`action number[.number2] forshut [module slot</td>
<td>xbar xbar-number] reset-reason seconds`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch{config-applet)# action 1.0 forshut module 2 reset-reason “flapping links”</td>
</tr>
<tr>
<td><code>action number[.number2] overbudgetshut [module slot[-slot]]</code></td>
<td>Forces one or more modules or the entire system to shut down because of a power overbudget issue. number can be any number up to 16 digits. The range for number2 is from 0 to 9.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch{config-applet)# action 1.0 overbudgetshut module 3-5</td>
</tr>
<tr>
<td><code>action number[.number2] policy-default</code></td>
<td>Executes the default action for the policy that you are overriding. The action label is in the format number1.number2. number can be any number up to 16 digits. The range for number2 is from 0 to 9.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch{config-applet)# action 1.0 policy-default</td>
</tr>
<tr>
<td><code>action number[.number2] publish-event</code></td>
<td>Forces the publication of an application-specific event. The action label is in the format number1.number2. number can be any number up to 16 digits. The range for number2 is from 0 to 9.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch{config-applet)# action 1.0 publish-event</td>
</tr>
<tr>
<td><code>action number[.number2] reload [module slot[-slot]]</code></td>
<td>Forces one or more modules or the entire system to reload. number can be any number up to 16 digits. The range for number2 is from 0 to 9.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch{config-applet)# action 1.0 reload module 3-5</td>
</tr>
</tbody>
</table>
Defining a Policy Using a VSH Script

You can define a policy using a VSH script.

**Before you begin**

Ensure that you are logged in with administrator privileges.

Ensure that your script name is the same name as the script filename.

**Procedure**

**Step 1** In a text editor, list the commands that define the policy.

**Step 2** Name the text file and save it.

**Step 3** Copy the file to the following system directory: bootflash://eem/user_script_policies.

**Defining a Policy Using a VSH Script**

You can define a policy using a VSH script.

**Before you begin**

Ensure that you are logged in with administrator privileges.

Ensure that your script name is the same name as the script filename.

**Procedure**

**Step 1** In a text editor, list the commands that define the policy.

**Step 2** Name the text file and save it.

**Step 3** Copy the file to the following system directory: bootflash://eem/user_script_policies.

**Registering and Activating a VSH Script Policy**

You can register and activate a policy defined in a VSH script.
## Overriding a Policy

You can override a system policy.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2** | Registers and activates an EEM script policy. The *policy-script* can be any case-sensitive alphanumeric string up to 29 characters. |
| event manager policy *policy-script* | |
| **Example:** | |
| switch(config)# event manager policy moduleScript | |

| **Step 3** | Copies the running configuration to the startup configuration. |
| (Optional) copy running-config startup-config | |
| **Example:** | |
| switch(config)# copy running-config startup-config | |
### Configuring Memory Thresholds

You can set the memory thresholds that are used to trigger events and set whether the operating system should kill processes if it cannot allocate memory.

**Before you begin**

Ensure that you are logged in with administrator privileges.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1  <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><code>switch(config)#</code></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configures the system memory thresholds that generate EEM memory events. The default values are as follows:</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>When these memory thresholds are exceeded, the system generates the following sylogs:</td>
</tr>
<tr>
<td><code>system memory-thresholds minor 60 severe 70 critical 80</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Minor-85</td>
</tr>
<tr>
<td></td>
<td>• Severe-90</td>
</tr>
<tr>
<td></td>
<td>• Critical-95</td>
</tr>
<tr>
<td></td>
<td>• 2013 May 7 17:06:30 switch %$ %PLATFORM-2-MEMORY_ALERT: Memory Status Alert : MINOR</td>
</tr>
<tr>
<td></td>
<td>• 2013 May 7 17:06:30 switch %$ %PLATFORM-2-MEMORY_ALERT: Memory Status Alert : SEVERE</td>
</tr>
<tr>
<td></td>
<td>• 2013 May 7 17:06:30 switch %$ %PLATFORM-2-MEMORY_ALERT: Memory Status Alert : CRITICAL</td>
</tr>
<tr>
<td></td>
<td>• 2013 May 7 17:06:35 switch %$ %PLATFORM-2-MEMORY_ALERT: Memory Status Alert : MINOR ALERT RECOVERED</td>
</tr>
<tr>
<td></td>
<td>• 2013 May 7 17:06:35 switch %$ %PLATFORM-2-MEMORY_ALERT: Memory Status Alert : SEVERE ALERT RECOVERED</td>
</tr>
<tr>
<td></td>
<td>• 2013 May 7 17:06:35 switch %$ %PLATFORM-2-MEMORY_ALERT: Memory Status Alert : CRITICAL ALERT RECOVERED</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configures the system to not kill processes when the memory cannot be allocated. The default value is to allow the system to kill processes, starting with the one that consumes the most memory.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>system memory-thresholds threshold critical no-process-kill</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Displays information about the system memory configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>`(Optional) show running-config</td>
<td>include &quot;system memory&quot;`</td>
</tr>
</tbody>
</table>
### Configuring Syslog as EEM Publisher

You can monitor syslog messages from the switch.

**Note**

The maximum number of searchable strings to monitor syslog messages is 10.

**Before you begin**

EEM should be available for registration by syslog. The syslog daemon must be configured and executed.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>[ switch# configure terminal ] switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> event manager applet applet-name</td>
<td>Registers an applet with EEM and enters applet configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>[ switch(config)# event manager applet abc ] switch(config-applet)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> event syslog [tag tag] {occurs number</td>
<td>period seconds</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>[ switch(config-applet)# event syslog occurs 10 ]</td>
<td></td>
</tr>
</tbody>
</table>

- The **tag tag** keyword-argument pair identifies this specific event when multiple events are included in the policy.
- The **occurs number** keyword-argument pair specifies the number of occurrences. The range is from 1 to 65000.
- The **period seconds** keyword-argument pair specifies the interval during which the event occurs. The range is from 1 to 4294967295.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• The pattern <code>msg-text</code> keyword-argument pair specifies the matching regular expression. The pattern can contain character text, an environment variable, or a combination of the two. If the string contains embedded blanks, it is enclosed in quotation marks.</td>
<td></td>
</tr>
<tr>
<td>• The priority <code>priority</code> keyword-argument pair specifies the priority of the syslog messages. If this keyword is not selected, all syslog messages are set at the informational priority level.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 4** (Optional) `copy running-config startup-config`  
**Example:**  
```
switch(config)# copy running-config startup-config
```  
Copies the running configuration to the startup configuration.

---

## Verifying the EEM Configuration

To display EEM configuration information, perform one of the following tasks:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`show event manager environment [variable-name</td>
<td>all]`</td>
</tr>
<tr>
<td>`show event manager event-types [event</td>
<td>all</td>
</tr>
<tr>
<td>`show event manager history events [detail] [maximum num-events] [severity {catastrophic</td>
<td>minor</td>
</tr>
<tr>
<td><code>show event manager policy-state policy-name</code></td>
<td>Displays information about the policy state, including thresholds.</td>
</tr>
<tr>
<td>`show event manager script system [policy-name</td>
<td>all]`</td>
</tr>
<tr>
<td><code>show event manager system-policy [all]</code></td>
<td>Displays information about the predefined system policies.</td>
</tr>
<tr>
<td><code>show running-config eem</code></td>
<td>Displays information about the running configuration for EEM.</td>
</tr>
<tr>
<td><code>show startup-config eem</code></td>
<td>Displays information about the startup configuration for EEM.</td>
</tr>
</tbody>
</table>
Configuration Examples for EEM

This example shows how to override the __lcm_module_failure system policy by changing the threshold for just module 3 hitless upgrade failures. This example also sends a syslog message. The settings in the system policy, __lcm_module_failure, apply in all other cases.

```bash
event manager applet example2 override __lcm_module_failure
event module-failure type hitless-upgrade-failure module 3 count 2
action 1 syslog priority errors msg module 3 "upgrade is not a hitless upgrade!"
action 2 policy-default
```

This example shows how to override the __ethpm_link_flap system policy and shuts down the interface:

```bash
event manager applet ethport override __ethpm_link_flap
event policy-default count 2 time 1000
action 1 cli conf t
action 2 cli int et1/1
action 3 cli no shut
```

This example creates an EEM policy that allows the CLI command to execute but triggers an SNMP notification when a user enters configuration mode on the device:

```bash
event manager applet TEST
event cli match "conf t"
action 1.0 snmp-trap strdata "Configuration change"
action 2.0 event-default
```

You must add the event-default action statement to the EEM policy or EEM will not allow the CLI command to execute.

This example shows how to correlate multiple events in an EEM policy and execute the policy based on a combination of the event triggers. In this example, the EEM policy is triggered if one of the specified syslog patterns occurs within 120 seconds.

```bash
event manager applet eem-correlate
event syslog tag one pattern "copy bootflash::.* running-config.*"
event syslog tag two pattern "copy run start"
event syslog tag three pattern "hello"
tag one or two or three happens 1 in 120
action 1.0 reload module 1
```

For additional EEM configuration examples, see Embedded Event Manager System Events and Configuration Examples, on page 379.
CHAPTER 15

Configuring Onboard Failure Logging

This chapter describes how to configure the onboard failure logging (OBFL) features on Cisco NX-OS devices.

This chapter includes the following sections:

• About OBFL, on page 217
• Licensing Requirements for OBFL, on page 218
• Prerequisites for OBFL, on page 218
• Guidelines and Limitations for OBFL, on page 218
• Default Settings for OBFL, on page 218
• Configuring OBFL, on page 219
• Verifying the OBFL Configuration, on page 221
• Configuration Example for OBFL, on page 222
• Additional References, on page 223

About OBFL

Cisco NX-OS provides the ability to log failure data to persistent storage, which you can retrieve and display for analysis at a later time. This onboard failure logging (OBFL) feature stores failure and environmental information in nonvolatile memory on the module. The information will help analyze failed modules.

OBFL stores the following types of data:

• Time of initial power-on
• Slot number of the module in the chassis
• Initial temperature of the module
• Firmware, BIOS, FPGA, and ASIC versions
• Serial number of the module
• Stack trace for crashes
• CPU hog information
• Memory leak information
• Software error messages
• Hardware exception logs
Licensing Requirements for OBFL

<table>
<thead>
<tr>
<th>Product</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco NX-OS</td>
<td>OBFL requires no license. Any feature not included in a license package is bundled with the nx-os image and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the Cisco NX-OS Licensing Guide.</td>
</tr>
</tbody>
</table>

Prerequisites for OBFL

You must have network-admin user privileges.

Guidelines and Limitations for OBFL

OBFL has the following guidelines and limitations:

- OBFL is enabled by default.
- OBFL flash supports a limited number of writes and erases. The more logging that you enable, the faster you use up this number of writes and erases.

Note

Be aware that the Cisco NX-OS commands for this feature may differ from those commands that are used in Cisco IOS.

Default Settings for OBFL

The following table lists the default settings for OBFL parameters.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>OBFL</td>
<td>All features enabled</td>
</tr>
</tbody>
</table>
Configuring OBFL

You can configure the OBFL features on Cisco NX-OS devices.

Before you begin
Make sure that you are in global configuration mode.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)#</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>hw-module logging onboard</code></td>
<td>Enables all OBFL features.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)# hw-module logging onboard</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Module: 7 Enabling ... was successful.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Module: 10 Enabling ... was successful.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Module: 12 Enabling ... was successful.</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>hw-module logging onboard counter-stats</code></td>
<td>Enables the OBFL counter statistics.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)# hw-module logging onboard counter-stats</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Module: 7 Enabling counter-stats ... was successful.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Module: 10 Enabling counter-stats ... was successful.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Module: 12 Enabling counter-stats ... was successful.</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>hw-module logging onboard cpuhog</code></td>
<td>Enables the OBFL CPU hog events.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)# hw-module logging onboard cpuhog</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Module: 7 Enabling cpu-hog ... was successful.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Module: 10 Enabling cpu-hog ... was successful.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Module: 12 Enabling cpu-hog ... was successful.</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>hw-module logging onboard environmental-history</code></td>
<td>Enables the OBFL environmental history.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>-------------------------------</td>
<td></td>
</tr>
<tr>
<td>switch(config)# hw-module logging onboard environmental-history Module: 7 Enabling environmental-history ... was successful. Module: 10 Enabling environmental-history ... was successful. Module: 12 Enabling environmental-history ... was successful.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> hw-module logging onboard error-stats</td>
<td>Enables the OBFL error statistics.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>switch(config)# hw-module logging onboard error-stats</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Module: 7 Enabling error-stats ... was successful.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Module: 10 Enabling error-stats ... was successful.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Module: 12 Enabling error-stats ... was successful.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> hw-module logging onboard interrupt-stats</td>
<td>Enables the OBFL interrupt statistics.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>switch(config)# hw-module logging onboard interrupt-stats</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Module: 7 Enabling interrupt-stats ... was successful.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Module: 10 Enabling interrupt-stats ... was successful.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Module: 12 Enabling interrupt-stats ... was successful.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> hw-module logging onboard module slot</td>
<td>Enables the OBFL information for a module.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>switch(config)# hw-module logging onboard module 7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Module: 7 Enabling ... was successful.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> hw-module logging onboard obfl-logs</td>
<td>Enables the boot uptime, device version, and OBFL history.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>switch(config)# hw-module logging onboard obfl-logs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Module: 7 Enabling obfl-log ... was successful.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Module: 10 Enabling obfl-log ... was successful.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Module: 12 Enabling obfl-log ... was successful.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Verifying the OBFL Configuration

To display OBFL information stored in flash on a module, perform one of the following tasks:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show logging onboard boot-uptime</td>
<td>Displays the boot and uptime information.</td>
</tr>
<tr>
<td>show logging onboard counter-stats</td>
<td>Displays statistics on all ASIC counters.</td>
</tr>
<tr>
<td>show logging onboard credit-loss</td>
<td>Displays OBFL credit loss logs.</td>
</tr>
<tr>
<td>show logging onboard device-version</td>
<td>Displays device version information.</td>
</tr>
<tr>
<td>show logging onboard endtime</td>
<td>Displays OBFL logs to a specified end time.</td>
</tr>
<tr>
<td>show logging onboard environmental-history</td>
<td>Displays environmental history.</td>
</tr>
<tr>
<td>show logging onboard error-stats</td>
<td>Displays error statistics.</td>
</tr>
<tr>
<td>show logging onboard exception-log</td>
<td>Displays exception log information.</td>
</tr>
<tr>
<td>show logging onboard interrupt-stats</td>
<td>Displays interrupt statistics.</td>
</tr>
<tr>
<td>show logging onboard module slot internal reset-reason</td>
<td>Displays OBFL information for a specific module.</td>
</tr>
<tr>
<td>show logging onboard obfl-history</td>
<td>Displays history information.</td>
</tr>
<tr>
<td>show logging onboard obfl-logs</td>
<td>Displays log information.</td>
</tr>
<tr>
<td>show logging onboard stack-trace</td>
<td>Displays kernel stack trace information.</td>
</tr>
</tbody>
</table>

**Note**: If you specify `internal reset-reason` and you are operating in a redundant supervisor configuration, checking the persistent log on the standby supervisor after a system reset occurs will display a relevant reset reason. The reset reason is recorded on the on-board flash for both the active and standby supervisor.
<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show logging onboard starttime</strong></td>
<td>Displays OBFL logs from a specified start time.</td>
</tr>
<tr>
<td><strong>show logging onboard status</strong></td>
<td>Displays OBFL status information.</td>
</tr>
</tbody>
</table>

Use the **show logging onboard status** command to display the configuration status of OBFL.

```
switch# show logging onboard status
-----------------------------
OBFL Status
-----------------------------
Switch OBFL Log: Enabled
Module: 4 OBFL Log: Enabled
    cpu-hog Enabled
    credit-loss Enabled
    environmental-history Enabled
    error-stats Enabled
    exception-log Enabled
    interrupt-stats Enabled
    mem-leak Enabled
    miscellaneous-error Enabled
    obfl-log (boot-upptime/device-version/obfl-history) Enabled
    register-log Enabled
    request-timeout Enabled
    stack-trace Enabled
    system-health Enabled
    timeout-drops Enabled
    stack-trace Enabled
Module: 22 OBFL Log: Enabled
    cpu-hog Enabled
    credit-loss Enabled
    environmental-history Enabled
    error-stats Enabled
    exception-log Enabled
    interrupt-stats Enabled
    mem-leak Enabled
    miscellaneous-error Enabled
    obfl-log (boot-upptime/device-version/obfl-history) Enabled
    register-log Enabled
    request-timeout Enabled
    stack-trace Enabled
    system-health Enabled
    timeout-drops Enabled
    stack-trace Enabled
```

Use the **clear logging onboard** command to clear the OBFL information for each of the **show** command options listed.

### Configuration Example for OBFL

This example shows how to enable OBFL on module 2 for environmental information:

```
switch# configure terminal
switch(config)# hw-module logging onboard module 2 environmental-history
```
Additional References

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration files</td>
<td><em>Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide</em></td>
</tr>
</tbody>
</table>
CHAPTER 16

Configuring SPAN

This chapter describes how to configure an Ethernet switched port analyzer (SPAN) to analyze traffic between ports on Cisco NX-OS devices.

This chapter contains the following sections:

• About SPAN, on page 225
• Licensing Requirements for SPAN, on page 228
• Prerequisites for SPAN, on page 229
• Guidelines and Limitations for SPAN, on page 229
• Default Settings for SPAN, on page 235
• Configuring SPAN, on page 235
• Verifying the SPAN Configuration, on page 243
• Configuration Examples for SPAN, on page 243
• Additional References, on page 248

About SPAN

SPAN analyzes all traffic between source ports by directing the SPAN session traffic to a destination port with an external analyzer attached to it.

You can define the sources and destinations to monitor in a SPAN session on the local device.

SPAN Sources

The interfaces from which traffic can be monitored are called SPAN sources. Sources designate the traffic to monitor and whether to copy ingress (Rx), egress (Tx), or both directions of traffic. SPAN sources include the following:

• Ethernet ports (but not subinterfaces)
• The inband interface to the control plane CPU

Note

When you specify the supervisor inband interface as a SPAN source, the device monitors all packets that are sent by the Supervisor CPU.
Characteristics of Source Ports

SPAN source ports have the following characteristics:

- A port configured as a source port cannot also be configured as a destination port.
- If you use the supervisor inband interface as a SPAN source, the following packets are monitored:
  - All packets that arrive on the supervisor hardware (ingress)
  - All packets generated by the supervisor hardware (egress)

SPAN Destinations

SPAN destinations refer to the interfaces that monitor source ports. Destination ports receive the copied traffic from SPAN sources. SPAN destinations include the following:

- Ethernet ports in either access or trunk mode
- Port channels in either access or trunk mode
• Uplink ports on Cisco Nexus 9300 Series switches

FEX ports are not supported as SPAN destination ports.

**Characteristics of Destination Ports**

SPAN destination ports have the following characteristics:

• A port configured as a destination port cannot also be configured as a source port.
• A destination port can be configured in only one SPAN session at a time.
• Destination ports do not participate in any spanning tree instance. SPAN output includes bridge protocol data unit (BPDU) Spanning Tree Protocol hello packets.

**SPAN Sessions**

You can create SPAN sessions to designate sources and destinations to monitor.

See the *Cisco Nexus 9000 Series NX-OS Verified Scalability Guide* for information on the number of supported SPAN sessions.

This figure shows a SPAN configuration. Packets on three Ethernet ports are copied to destination port Ethernet 2/5. Only traffic in the direction specified is copied.

*Figure 5: SPAN Configuration*

<table>
<thead>
<tr>
<th>Source Port</th>
<th>Direction</th>
<th>Destination Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>E 2/1</td>
<td>Rx</td>
<td>E 2/5</td>
</tr>
<tr>
<td>E 2/2</td>
<td>Rx, Tx</td>
<td></td>
</tr>
<tr>
<td>E 2/3</td>
<td>Tx</td>
<td></td>
</tr>
</tbody>
</table>

**Localized SPAN Sessions**

A SPAN session is localized when all of the source interfaces are on the same line card. A session destination interface can be on any line card.

A SPAN session with a VLAN source is not localized.

**SPAN Truncation**

Beginning with Cisco NX-OS Release 7.0(3)I7(1), you can configure the truncation of source packets for each SPAN session based on the size of the MTU. Truncation helps to decrease SPAN bandwidth by reducing the size of monitored packets. Any SPAN packet that is larger than the configured MTU size is truncated to
the given size. For example, if you configure the MTU as 300 bytes, the packets with greater than 300 bytes are truncated to 300 bytes.

SPAN truncation is disabled by default. To use truncation, you must enable it for each SPAN session.

**Multicast Tx SPAN Across Different Slices**

In this example, Eth1/15, Eth1/16, and Eth1/17 are ports on slice 0 of the LSE, and Eth1/27 is a port on slice 1 of the LSE.

![Figure 6: Multicast Tx SPAN Across Different LSE Slices](image)

Eth1/15 can receive multicast traffic with a receiver on Eth1/16, and traffic egressing Eth1/16 can be spanned across to Eth1/17 because these ports are all on the same slice. With multicast Tx SPAN enabled, Eth1/27 (which is on a different slice) can be the SPAN destination for multicast Tx traffic with Eth1/16 as the SPAN source.

**ACL TCAM Regions**

You can change the size of the ACL ternary content addressable memory (TCAM) regions in the hardware. For information on the TCAM regions used by SPAN sessions, see the Configuring IP ACLs chapter of the Cisco Nexus 9000 Series NX-OS Security Configuration Guide.

**High Availability**

The SPAN feature supports stateless and stateful restarts. After a reboot or supervisor switchover, the running configuration is applied. For more information on high availability, see the Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide.

**Licensing Requirements for SPAN**

<table>
<thead>
<tr>
<th>Product</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco NX-OS</td>
<td>SPAN requires no license. Any feature not included in a license package is bundled with the nx-os image and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the Cisco NX-OS Licensing Guide.</td>
</tr>
</tbody>
</table>
Prerequisites for SPAN

SPAN has the following prerequisites:

- You must first configure the ports on each device to support the desired SPAN configuration. For more information, see the Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide.

Guidelines and Limitations for SPAN

SPAN has the following configuration guidelines and limitations:

- Traffic that is denied by an ACL may still reach the SPAN destination port because SPAN replication is performed on the ingress side prior to the ACL enforcement (ACL dropping traffic).
- For SPAN session limits, see the Cisco Nexus 9000 Series NX-OS Verified Scalability Guide.
- All SPAN replication is performed in the hardware. The supervisor CPU is not involved.
- You can configure a SPAN session on the local device only.
- Configuring two SPAN or ERSPAN sessions on the same source interface, with only one filter is not supported.
- You can configure only one destination port in a SPAN session.
- A destination port can be configured in only one SPAN session at a time.
- You cannot configure a port as both a source and destination port.
- Enabling UniDirectional Link Detection (UDLD) on the SPAN source and destination ports simultaneously is not supported. If UDLD frames are expected to be captured on the source port of such SPAN session, disable UDLD on the destination port of the SPAN session.
- SPAN is not supported for management ports.
- Statistics are not support for the filter access group.
- SPAN is supported in Layer 3 mode; however, SPAN is not supported on Layer 3 subinterfaces or Layer 3 port-channel subinterfaces.
- When a SPAN session contains source ports that are monitored in the transmit or transmit and receive direction, packets that these ports receive might be replicated to the SPAN destination port even though the packets are not actually transmitted on the source ports. Some examples of this behavior on source ports are as follows:
  - Traffic that results from flooding
  - Broadcast and multicast traffic
- SPAN sessions cannot capture packets with broadcast or multicast MAC addresses that reach the supervisor, such as ARP requests and Open Shortest Path First (OSPF) protocol hello packets, if the source of the session is the supervisor Ethernet in-band interface. To capture these packets, you must use the physical interface as the source in the SPAN sessions.
• VLAN SPAN monitors only the traffic that enters Layer 2 ports in the VLAN.
• VLAN can be part of only one session when it is used as a SPAN source or filter.
• VLAN ACL redirects to SPAN destination ports are not supported.
• When using a VLAN ACL to filter a SPAN, only action forward is supported; action drop and action redirect are not supported.
• The combination of VLAN source session and port source session is not supported. If the traffic stream matches the VLAN source session as well as the port source session, two copies are needed at two destination ports. Due to the hardware limitation, only the VLAN source SPAN and the specific destination port receive the SPAN packets.
• This limitation applies to the following Cisco devices:

Table 18: Table 1. Cisco Nexus 9000 Series Switches

<table>
<thead>
<tr>
<th>Cisco Nexus 93120TX</th>
<th>Cisco Nexus 93128TX</th>
<th>Cisco Nexus 9332PQ</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Nexus 9372PX</td>
<td>Cisco Nexus 9372PX-E</td>
<td>Cisco Nexus 9372TX</td>
</tr>
<tr>
<td>Cisco Nexus 9396PX</td>
<td>Cisco Nexus 9372TX-E</td>
<td>Cisco Nexus 9396TX</td>
</tr>
</tbody>
</table>

Table 19: Table 2. Cisco Nexus 9000 Series Line Cards, Fabric Modules, and GEM Modules

<table>
<thead>
<tr>
<th>N9K-X9408PC-CFP2</th>
<th>N9K-X9563PQ</th>
<th>N9K-C9508-FM</th>
</tr>
</thead>
<tbody>
<tr>
<td>N9K-X9432PQ</td>
<td>N9K-X9564PX</td>
<td>N9K-C9504-FM</td>
</tr>
<tr>
<td>N9K-X9464PX</td>
<td>N9K-X9564TX</td>
<td>N9K-C9516-FM</td>
</tr>
<tr>
<td>N9K-X9464TX</td>
<td>N9K-X9636PQ</td>
<td>N9K-M4PC-CFP2</td>
</tr>
</tbody>
</table>

• The number of SPAN sessions per line card reduces to two if the same interface is configured as a bidirectional source in more than one session. This guideline does not apply for Cisco Nexus 9508 switches with N9K-X9636C-R and N9K-X9636Q-R line cards.
• An access-group filter in a SPAN session must be configured as vlan-accessmap. This guideline does not apply for Cisco Nexus 9508 switches with N9K-X9636C-R and N9K-X9636Q-R line cards.
• Supervisor-generated stream of bytes module header (SOBMH) packets have all the information to go out on an interface and can bypass all forwarding lookups in the hardware, including SPAN and ERSPAN. CPU-generated frames for Layer 3 interfaces and the Bridge Protocol Data Unit (BPDU) class of packets are sent using SOBMH. This guideline does not apply for Cisco Nexus 9508 switches with N9K-X9636C-R and N9K-X9636Q-R line cards. The Cisco Nexus N9K-X9636C-R and N9K-X9636Q-R both support inband SPAN and local SPAN.
• Cisco NX-OS does not span Link Layer Discovery Protocol (LLDP) or Link Aggregation Control Protocol (LACP) packets when the source interface is not a host interface port channel.
• SPAN copies for multicast packets are made before rewrite. Therefore, the TTL, VLAN ID, any remarking due to egress policy, and so on, are not captured in the SPAN copy.
• If SPAN is mirroring the traffic which ingresses on an interface in an ASIC instance and egresses on a Layer 3 interface (SPAN Source) on a different ASIC instance, then TX mirrored packet has a VLAN ID 4095 on Cisco Nexus 9000 platform modular switches using non-EX line cards.

• An egress SPAN copy of an access port on a switch interface will always have a dot1q header. This guideline does not apply for Cisco Nexus 9508 switches with N9K-X9636C-R and N9K-X9636Q-R line cards.

• The flows for post-routed unknown unicast flooded packets are in the SPAN session, even if the SPAN session is configured not to monitor the ports on which this flow is forwarded. This limitation applies to Network Forwarding Engine (NFE) and NFE2-enabled EOR switches and SPAN sessions that have Tx port sources.

• VLAN sources are spanned only in the Rx direction. This guideline does not apply for Cisco Nexus 9508 switches with N9K-X9636C-R and N9K-X9636Q-R line cards.

• Session filtering functionality (VLAN or ACL filters) is supported only for Rx sources. This guideline does not apply for Cisco Nexus 9508 switches with N9K-X9636C-R and N9K-X9636Q-R line cards.

• The FEX NIF interfaces or port-channels cannot be used as a SPAN source or SPAN destination. If the FEX NIF interfaces or port-channels are specified as a SPAN source or SPAN destination, the software displays an unsupported error.

• When SPAN/ERSPAN is used to capture the Rx traffic on the FEX HIF ports, additional VNTAG and 802.1Q tags are present in the captured traffic.

• VLAN and ACL filters are not supported for FEX ports.

• If the sources used in bidirectional SPAN sessions are from the same FEX, the hardware resources are limited to two SPAN sessions.

• SPAN source or destination is supported on any port.

• Rx SPAN is supported. Tx or both (Tx and Rx) are not supported.

• Truncation is supported only for local and SPAN source sessions. It is not supported for SPAN destination sessions.

• Configuring MTU on a SPAN session truncates all of the packets egressing on the SPAN destination (for that session) to the MTU value specified.

• The cyclic redundancy check (CRC) is recalculated for the truncated packet.

• The bytes specified are retained starting from the header of the packets. The rest are truncated if the packet is longer than the MTU.

• The bytes specified are retained starting from the header of the packets. The rest are truncated if the packet is longer than the MTU.

### SPAN Limitations for the Cisco Nexus 3000 Platform Switches

The following guidelines and limitations apply only the Nexus 3000 Series switches running Cisco Nexus 9000 code:

• The Cisco Nexus 3232C and 3264Q switches do not support SPAN on CPU as destination.
SPAN Limitations for the Cisco Nexus 9200 Platform Switches

The following guidelines and limitations apply only the Cisco Nexus 9200 platform switches:

- For Cisco Nexus 9200 platform switches, Rx SPAN is not supported for multicast without a forwarding interface on the same slice as the SPAN destination port.
- Tx SPAN for multicast, unknown multicast, and broadcast traffic are not supported on the Cisco Nexus 9200 platform switches.
- Tx SPAN of CPU-generated packets is not supported on Cisco Nexus 9200 platform switches.
- UDF-based SPAN is supported on the Cisco Nexus 9200 platform switches.
- The Cisco Nexus 9200 platform switches do not support Multiple ACL filters on the same source.
- When multiple egress ports on the same slice are congested by egressing SPAN traffic, those egress ports will not get the line rate on the Cisco Nexus 9200 platform switches.
- Using the ACL filter to span subinterface traffic on the parent interface is not supported on the Cisco Nexus 9200 platform switches.
- On the Cisco Nexus 9200 platform switches, the CPU SPAN source can be added only for the Rx direction (SPAN packets coming from the CPU).
- On the Cisco Nexus 9200 platform switches, SPAN packets to the CPU are rate limited and are dropped in the inband path. You can change the rate limit using the `hardware rate-limiter span` command. You can analyze SPAN copies on the supervisor using the `ethanalyzer local interface inband mirror detail` command.

SPAN Limitations for the Cisco Nexus 9300 Platform Switches

The following guidelines and limitations apply only the Cisco Nexus 9300 platform switches:

- The following limitations apply to egress (Tx) SPAN on Cisco Nexus 9300-EX and -FX platform switches:
  - ACL filtering is not supported (applies to both unicast and Broadcast, Unknown Unicast and Multicast (BUM) traffic)
  - VLAN filtering is supported, but only for unicast traffic
  - VLAN filtering is not supported for BUM traffic
- On Cisco Nexus 9300-EX/FX platform switches, SPAN and sFlow cannot both be enabled simultaneously. If one is active, the other cannot be enabled. However, on the Cisco Nexus 9300-EX/FX/FX2, both NetFlow and SPAN can both be enabled simultaneously, providing a viable alternative to using sFlow and SPAN.

**Note**

Cisco Nexus 9300-FX2 switches support sFlow and SPAN co-existence.

- Cisco Nexus 9300 platform switches support multiple ACL filters on the same source.
• A single forwarding engine instance supports four SPAN sessions. For Cisco Nexus 9300 platform switches, if the first three sessions have bidirectional sources, the fourth session has hardware resources only for Rx sources.

• Cisco Nexus 9300-EX/FX2/FX3/FXP platform switches support FEX ports as SPAN sources only in the ingress direction.

• Cisco Nexus 9300 platform switches (excluding Cisco Nexus 9300-EX/FX2/FX3/FXP switches) support FEX ports as SPAN sources in the ingress direction for all traffic and in the egress direction only for known Layer 2 unicast traffic flows through the switch and FEX. Routed traffic might not be seen on FEX HIF egress SPAN.

• Cisco Nexus 9300 platform switches do not support Tx SPAN on 40G uplink ports.

  **Note**  
  This limitation does not apply to Nexus 9300-EX/FX/FX2 switches that have the 100G interfaces.

• Tx SPAN of CPU-generated packets is not supported on Cisco Nexus 9300-EX/-FX/-FXP platform switches.

• NetFlow and SPAN functionality is supported on Cisco Nexus 9336C-FX2 and Cisco Nexus 93240Y-C-FX2 switches.

• Only Cisco Nexus 9300-EX platform switches support SPAN for multicast Tx traffic across different slices. The slices must be on the same leaf spine engine (LSE).

• For Tx interface SPAN with Layer 2 switch port and port-channel sources on Cisco Nexus 9300-EX platform switches, only one copy is made per receiver unit regardless of how many Layer 2 members are receiving the stream in the same VLAN. For example, if e1/1-8 are all Tx direction SPAN sources and all are joined to the same group, the SPAN destination port sees one pre-rewrite copy of the stream, not eight copies. In addition, if for any reason one or more of those ports drops the packets on egress (for example, due to congestion), the packets may still reach the SPAN destination port. For the N9K-X9732C-EX line card, one copy is made per unit that has members. For port-channel sources, the Layer 2 member that will SPAN is the first port-channel member.

• SPAN Tx broadcast and SPAN Tx multicast are supported for Layer 2 port and port-channel sources across slices on Cisco Nexus 9300-EX platform switches and the Cisco Nexus N9K-X9732C-EX line card but only when IGMP snooping is disabled. (Otherwise, the slice limitation still applies.) These features are not supported for Layer 3 port sources, FEX ports (with unicast or multicast traffic), and VLAN sources.

• A SPAN copy of Cisco Nexus 9300 platform switch 40G uplink interfaces will miss the dot1q information when spanned in the Rx direction.

  **Note**  
  This limitation does not apply to Nexus 9300-EX/FX/FX2 switches that have the 100G interfaces.

• UDF-based SPAN is supported on the Cisco Nexus 9300-EX platform switches.

• The Cisco Nexus 9300-EX platform switches do not support Multiple ACL filters on the same source.
• When multiple egress ports on the same slice are congested by egressing SPAN traffic, those egress ports will not get the line rate on the Cisco Nexus 9300-EX platform switches.

• Using the ACL filter to span subinterface traffic on the parent interface is not supported on the Cisco Nexus 9300-EX platform switches.

• On the Cisco Nexus 9200 and 9300-EX platform switches, the CPU SPAN source can be added only for the Rx direction (SPAN packets coming from the CPU).

• On the Cisco Nexus 9300-EX platform switches, SPAN packets to the CPU are rate limited and are dropped in the inband path. You can change the rate limit using the `hardware rate-limiter span` command. You can analyze SPAN copies on the supervisor using the `ethanalyzer local interface inband mirror detail` command.

• The following Cisco Nexus switches support sFlow and SPAN together:

### SPAN Limitations for the Cisco Nexus 9500 Platform Switches

The following guidelines and limitations apply only the Cisco Nexus 9500 platform switches:

• The following limitations apply to egress (Tx) SPAN on 9500-EX, -FX and -FXP platform switches:
  • ACL filtering is not supported (applies to both unicast and Broadcast, Unknown Unicast and Multicast (BUM) traffic)
  • VLAN filtering is supported, but only for unicast traffic
  • VLAN filtering is not supported for BUM traffic

• FEX and SPAN port-channel destinations are not supported on the Cisco Nexus 9500 platform switches with an -EX or -FX type line card.

• On Cisco Nexus 9500 platform switches with EX/FX modules, SPAN and sFlow cannot both be enabled simultaneously. If one is active, the other cannot be enabled. However, on the Cisco Nexus 9500 platform switches with EX modules, both NetFlow and SPAN can both be enabled simultaneously, providing a viable alternative to using sFlow and SPAN.

• Cisco Nexus 9500 platform switches support multiple ACL filters on the same source.

• Tx SPAN of CPU-generated packets is not supported on Cisco Nexus 9500 platform switches with EX-based line cards.

• On the Cisco Nexus 9500 platform switches, depending on the SPAN source's forwarding engine instance mappings, a single forwarding engine instance may support four SPAN sessions. This guideline does not apply for Cisco Nexus 9508 switches with N9K-X9636C-R and N9K-X9636Q-R line cards.

• Multiple ACL filters are not supported on the same source.

• Cisco Nexus 9500 platform switches support FEX ports as SPAN sources in the ingress direction for all traffic and in the egress direction only for known Layer 2 unicast traffic flows through the switch and FEX. Routed traffic might not be seen on FEX HIF egress SPAN.

• SPAN does not support destinations on N9K-X9408PC-CFP2 line card ports.
SPAN Limitations for the Cisco Nexus 9508 Switches

The following guidelines and limitations apply only to the Cisco Nexus 9508 platform switches:

- VLANs can be SPAN sources in the ingress and egress direction on Cisco Nexus 9508 switches with N9K-X9636C-R and N9K-X9636Q-R line cards. For all other switches, VLANs are supported as SPAN sources only in the ingress direction.

Default Settings for SPAN

The following table lists the default settings for SPAN parameters.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPAN sessions</td>
<td>Created in the shut state</td>
</tr>
</tbody>
</table>

Configuring SPAN

Cisco NX-OS commands for this feature may differ from those in Cisco IOS.

Configuring a SPAN Session

You can configure a SPAN session on the local device only. By default, SPAN sessions are created in the shut state.

Note

For bidirectional traditional sessions, you can configure the sessions without specifying the direction of the traffic.

Before you begin

You must configure the destination ports in access or trunk mode. For more information, see the Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)#</code></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring a SPAN Session

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters interface configuration mode on the selected slot and port.</td>
</tr>
</tbody>
</table>
| `interface interface slot/port` | **Example:**
  - `switch(config)# interface ethernet 2/5`
  - `switch(config-if)#` |
| **Step 3** | Configures switchport parameters for the selected slot and port or range of ports. |
| `switchport` | **Example:**
  - `switch(config-if)# switchport` |
| **Step 4** | Configures the switchport interface as a SPAN destination. |
| `switchport monitor` | **Example:**
  - `switch(config-if)# switchport monitor` |
| **Step 5** | (Optional) Repeat Steps 2 through 4 to configure monitoring on additional SPAN destinations. |
| `no monitor session session-number` | **Example:**
  - `switch(config)# no monitor session 3` |
| **Step 6** | Clears the configuration of the specified SPAN session. The new session configuration is added to the existing session configuration. |
| `monitor session session-number [rx | tx] [shut]` | **Example:**
  - `switch(config)# monitor session 3 rx`  
  - `switch(config-monitor)#`
  - `Example:`
  - `switch(config)# monitor session 3 tx`  
  - `switch(config-monitor)#`
  - `Example:`
  - `switch(config)# monitor session 3 shut`  
  - `switch(config-monitor)#` |
| **Step 7** | Enters the monitor configuration mode. The new session configuration is added to the existing session configuration. By default, the session is created in the shut state, and the session is a local SPAN session. The optional keyword shut specifies a shut state for the selected session. |
| `description description` | **Example:**
  - `switch(config-monitor)# description my_span_session_3` |
| **Step 8** | Configures a description for the session. By default, no description is defined. The description can be up to 32 alphanumeric characters. |
| `source {interface type [rx | tx | both] | [vlan number | range] [rx]}` | **Example:**
  - `switch(config-monitor)# source interface ethernet 2/1-3, ethernet 3/1 rx`
  - `Example:`
  - `switch(config-monitor)# source interface port-channel 2` |
| **Step 9** | Configures sources and the traffic direction in which to copy packets. You can enter a range of Ethernet ports, a port channel, an inband interface, a range of VLANs, or a satellite port or host interface port channel on the Cisco Nexus 2000 Series Fabric Extender (FEX). You can configure one or more sources, as either a series of comma-separated entries or a range of numbers. |
### Configuring SPAN

#### Example:

```
switch(config-monitor)# source interface sup-eth 0 both
```

#### Source VLANs are supported only in the ingress direction. Source FEX ports are supported in the ingress direction for all traffic and in the egress direction only for known Layer 2 unicast traffic.

#### Note

```
switch(config-monitor)# source interface ethernet 101/1/1-3
```

For a unidirectional session, the direction of the source must match the direction specified in the session.

### Step 10
(Optional) Repeat Step 9 to configure all SPAN sources.

### Step 11
```
filter vlan {number | range}
```

- Example:
  
  ```
  switch(config-monitor)# filter vlan 3-5, 7
  ```

#### Configures which VLANs to select from the configured sources. You can configure one or more VLANs, as either a series of comma-separated entries or a range of numbers.

#### Note

```
switch(config-monitor)# filter access-group acl-filter
```

- Example:
  
  ```
  switch(config-monitor)# filter access-group ACL1
  ```

#### Associates an ACL with the SPAN session.

### Step 13
(Optional) Repeat Step 11 to configure all source VLANs to filter.

### Step 14
```
Required: destination interface type slot/port
```

- Example:
  
  ```
  switch(config-monitor)# destination interface ethernet 2/5
  ```

#### Configures a destination for copied source packets.

#### Note

- The SPAN destination port must be either an access port or a trunk port.
- You must enable monitor mode on the destination port.

#### You can configure the CPU as the SPAN destination for Cisco Nexus 9200 Series switches, beginning with Cisco NX-OS Release 7.0(3)14(1), and Cisco Nexus 9300-EX Series switches, beginning with Cisco NX-OS Release 7.0(3)14(2). To do so, enter `sup-eth 0` for the interface type.

### Step 15
```
Required: no shut
```

- Example:
  
  ```
  ```

#### Enables the SPAN session. By default, the session is created in the shut state.
Configuring UDF-Based SPAN

You can configure the device to match on user-defined fields (UDFs) of the outer or inner packet fields (header or payload) and to send the matching packets to the SPAN destination. Doing so can help you to analyze and isolate packet drops in the network.

Before you begin

Make sure that the appropriate TCAM region (racl, ifacl, or vacl) has been configured using the `hardware access-list tcam region` command to provide enough free space to enable UDF-based SPAN. For information, see the "Configuring ACL TCAM Region Sizes" section in the Cisco Nexus 9000 Series NX-OS Security Configuration Guide.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><code>switch(config)#</code></td>
<td></td>
</tr>
<tr>
<td><code>switch(config)# udf udf-name offset-base offset length</code></td>
<td>Defines the UDF as follows:</td>
</tr>
<tr>
<td><code>switch(config)# udf udf-x packet-start 12 1</code></td>
<td></td>
</tr>
<tr>
<td><code>switch(config)# udf udf-y header outer 13 20 2</code></td>
<td></td>
</tr>
</tbody>
</table>

**Configuring UDF-Based SPAN**

You can configure the device to match on user-defined fields (UDFs) of the outer or inner packet fields (header or payload) and to send the matching packets to the SPAN destination. Doing so can help you to analyze and isolate packet drops in the network.

**Before you begin**

Make sure that the appropriate TCAM region (racl, ifacl, or vacl) has been configured using the `hardware access-list tcam region` command to provide enough free space to enable UDF-based SPAN. For information, see the "Configuring ACL TCAM Region Sizes" section in the Cisco Nexus 9000 Series NX-OS Security Configuration Guide.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><code>switch(config)#</code></td>
<td></td>
</tr>
<tr>
<td><code>switch(config)# udf udf-name offset-base offset length</code></td>
<td>Defines the UDF as follows:</td>
</tr>
<tr>
<td><code>switch(config)# udf udf-x packet-start 12 1</code></td>
<td></td>
</tr>
<tr>
<td><code>switch(config)# udf udf-y header outer 13 20 2</code></td>
<td></td>
</tr>
</tbody>
</table>

**Configuring UDF-Based SPAN**

You can configure the device to match on user-defined fields (UDFs) of the outer or inner packet fields (header or payload) and to send the matching packets to the SPAN destination. Doing so can help you to analyze and isolate packet drops in the network.

**Before you begin**

Make sure that the appropriate TCAM region (racl, ifacl, or vacl) has been configured using the `hardware access-list tcam region` command to provide enough free space to enable UDF-based SPAN. For information, see the "Configuring ACL TCAM Region Sizes" section in the Cisco Nexus 9000 Series NX-OS Security Configuration Guide.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><code>switch(config)#</code></td>
<td></td>
</tr>
<tr>
<td><code>switch(config)# udf udf-name offset-base offset length</code></td>
<td>Defines the UDF as follows:</td>
</tr>
<tr>
<td><code>switch(config)# udf udf-x packet-start 12 1</code></td>
<td></td>
</tr>
<tr>
<td><code>switch(config)# udf udf-y header outer 13 20 2</code></td>
<td></td>
</tr>
</tbody>
</table>

**Configuring UDF-Based SPAN**

You can configure the device to match on user-defined fields (UDFs) of the outer or inner packet fields (header or payload) and to send the matching packets to the SPAN destination. Doing so can help you to analyze and isolate packet drops in the network.

**Before you begin**

Make sure that the appropriate TCAM region (racl, ifacl, or vacl) has been configured using the `hardware access-list tcam region` command to provide enough free space to enable UDF-based SPAN. For information, see the "Configuring ACL TCAM Region Sizes" section in the Cisco Nexus 9000 Series NX-OS Security Configuration Guide.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><code>switch(config)#</code></td>
<td></td>
</tr>
<tr>
<td><code>switch(config)# udf udf-name offset-base offset length</code></td>
<td>Defines the UDF as follows:</td>
</tr>
<tr>
<td><code>switch(config)# udf udf-x packet-start 12 1</code></td>
<td></td>
</tr>
<tr>
<td><code>switch(config)# udf udf-y header outer 13 20 2</code></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>first byte from the offset base (Layer 3/Layer 4 header), configure the offset as 0.</td>
<td></td>
</tr>
<tr>
<td>• length—Specifies the number of bytes from the offset. Only 1 or 2 bytes are supported. To match additional bytes, you must define multiple UDFs.</td>
<td></td>
</tr>
<tr>
<td>You can define multiple UDFs, but Cisco recommends defining only required UDFs.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Step 3</strong> hardware access-list tcam region {racl</td>
</tr>
<tr>
<td></td>
<td>switch(config)# hardware access-list tcam region racl qualify udf udf-x udf-y</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>You can attach up to 8 UDFs to a TCAM region.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>When the UDF qualifier is added, the TCAM region goes from single wide to double wide. Make sure enough free space is available; otherwise, this command will be rejected. If necessary, you can reduce the TCAM space from unused regions and then re-enter this command. For more information, see the &quot;Configuring ACL TCAM Region Sizes&quot; section in the Cisco Nexus 9000 Series NX-OS Security Configuration Guide.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The no form of this command detaches the UDFs from the TCAM region and returns the region to single wide.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Required: copy running-config startup-config</td>
</tr>
<tr>
<td></td>
<td>switch(config)# copy running-config startup-config</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Required: reload</td>
</tr>
<tr>
<td></td>
<td>switch(config)# reload</td>
</tr>
</tbody>
</table>
Configuring SPAN Truncation

You can configure truncation for local and SPAN source sessions only.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
</tbody>
</table>

<p>| <strong>Step 2</strong> | Enters monitor configuration mode for the specified SPAN session. |
| monitor session <em>session number</em> | |
| Example: | |
| switch(config)# monitor session 5 | |
| switch(config-monitor)# | |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Configure the source interface.</strong></td>
</tr>
<tr>
<td>source interface type slot/port [rx</td>
<td>tx</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config-monitor)# source interface ethernet 1/5 both</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 4** | **Configure the MTU size for truncation.** |
| mtu size | Any SPAN packet that is larger than the configured MTU size is truncated to the configured size. |
| Example: | |
| switch(config-monitor)# mtu 320 | |
| Example: | |
| switch(config-monitor)# mtu ? | |
| <320-1518> Enter the value of MTU truncation size for SPAN packets | |

| **Step 5** | **Configure the Ethernet SPAN destination port.** |
| destination interface type slot/port | |
| Example: | |
| switch(config-monitor)# destination interface Ethernet 1/39 | |

| **Step 6** | **Enable the SPAN session.** |
| no shut | By default, the session is created in the shut state. |
| Example: | |
| switch(config-monitor)# no shut | |

| **Step 7** | **Display the SPAN configuration.** |
| (Optional) show monitor session session | |
| Example: | |
| switch(config-monitor)# show monitor session 5 | |

| **Step 8** | **Copy the running configuration.** |
| copy running-config startup-config | |
| Example: | |
| switch(config-monitor)# copy running-config startup-config | |

---

**Configuring SPAN for Multicast Tx Traffic Across Different LSE Slices**

Beginning with Cisco NX-OS Release 7.0(3)I7(1), you can configure SPAN for multicast Tx traffic across different leaf spine engine (LSE) slices on Cisco Nexus 9300-EX platform switches.
### Configuring SPAN

#### Shutting Down or Resuming a SPAN Session

You can shut down SPAN sessions to discontinue the copying of packets from sources to destinations. You can shut down one session in order to free hardware resources to enable another session. By default, SPAN sessions are created in the shut state.

You can resume (enable) SPAN sessions to resume the copying of packets from sources to destinations. In order to enable a SPAN session that is already enabled but operationally down, you must first shut it down and then enable it.

You can configure the shut and enabled SPAN session states with either a global or monitor configuration mode command.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> [no] hardware multicast global-tx-span</td>
<td>Configures SPAN for multicast Tx traffic across different leaf spine engine (LSE) slices.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td>hardware multicast global-tx-span</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> reload</td>
<td>Reloads the device.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td>reload</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring SPAN

#### Verifying the SPAN Configuration

To display the SPAN configuration, perform one of the following tasks:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`show monitor session all</td>
<td>Displays the SPAN session configuration.</td>
</tr>
<tr>
<td><code>session-number</code></td>
<td></td>
</tr>
<tr>
<td><code>range session-range</code></td>
<td></td>
</tr>
<tr>
<td>`</td>
<td>brief`</td>
</tr>
</tbody>
</table>

#### Configuration Examples for SPAN

#### Configuration Example for a SPAN Session

To configure a SPAN session, follow these steps:

1. **Step 3**
   - **monitor session** `session-number`
   - **Example:**
     ```
     switch(config)# monitor session 3
     switch(config-monitor)#
     ```

   - **Note:** Enters the monitor configuration mode. The new session configuration is added to the existing session configuration.

2. **Step 4**
   - **[no]** shut
   - **Example:**
     ```
     switch(config-monitor)# shut
     ```

   - **Step 5**
     - **(Optional) show monitor**
     - **Example:**
       ```
       switch(config-monitor)# show monitor
       ```

   - **Step 6**
     - **(Optional) copy running-config startup-config**
     - **Example:**
       ```
       switch(config)# copy running-config startup-config
       ```
Configuration Example for a Unidirectional SPAN Session

To configure a unidirectional SPAN session, follow these steps:

Procedure

Step 1  Configure destination ports in access mode and enable SPAN monitoring.

Example:

```
switch# configure terminal
switch(config)# interface ethernet 2/5
switch(config-if)# switchport
switch(config-if)# switchport monitor
switch(config-if)# no shut
switch(config-if)# exit
switch(config)#
```

Step 2  Configure a SPAN session.

Example:

```
switch(config)# no monitor session 3
switch(config)# monitor session 3
switch(config-monitor)# source interface ethernet 2/1-3, ethernet 3/1 rx
switch(config-monitor)# source interface port-channel 2
switch(config-monitor)# source interface sup-eth 0 both
switch(config-monitor)# source interface vlan 3, 6-8 rx
switch(config-monitor)# source interface ethernet 101/1/1-3
switch(config-monitor)# filter vlan 3-5, 7
switch(config-monitor)# destination interface ethernet 2/5
switch(config-monitor)# no shut
switch(config-monitor)# exit
switch(config)# show monitor session 3
switch(config)# copy running-config startup-config
```
switch(config)# no monitor session 3
switch(config)# monitor session 3 rx
switch(config-monitor)# source interface ethernet 2/1-3, ethernet 3/1 rx
switch(config-monitor)# filter vlan 3-5, 7
switch(config-monitor)# destination interface ethernet 2/5
switch(config-monitor)# no shut
switch(config-monitor)# exit
switch(config)# show monitor session 3
switch(config)# copy running-config startup-config

### Configuration Example for a SPAN ACL

This example shows how to configure a SPAN ACL:

```
switch# configure terminal
switch(config)# ip access-list match_11_pkts
switch(config-acl)# permit ip 11.0.0.0 0.255.255.255 any
switch(config-acl)# exit
switch(config)# ip access-list match_12_pkts
switch(config-acl)# permit ip 12.0.0.0 0.255.255.255 any
switch(config-acl)# exit
switch(config)# vlan access-map span_filter 5
switch(config-access-map)# match ip address match_11_pkts
switch(config-access-map)# action forward
switch(config-access-map)# exit
switch(config)# vlan access-map span_filter 10
switch(config-access-map)# match ip address match_12Pkts
switch(config-access-map)# action forward
switch(config-access-map)# exit
switch(config)# monitor session 1
switch(config-erspan-src)# filter access-group span_filter
```

### Configuration Examples for UDF-Based SPAN

This example shows how to configure UDF-based SPAN to match on the inner TCP flags of an encapsulated IP-in-IP packet using the following match criteria:

- **Outer source IP address**: 10.0.0.2
- **Inner TCP flags**: Urgent TCP flag is set
- **Bytes**: EthHdr (14) + Outer IP (20) + Inner IP (20) + Inner TCP (20, but TCP flags at 13th byte)
- **Offset from packet-start**: $14 + 20 + 20 + 13 = 67$
- **UDF match value**: 0x20
- **UDF mask**: 0xFF

```
udf udf_tcpflags packet-start 67 1
hardware access-list tcam region racl qualify udf udf_tcpflags
copy running-config startup-config
reload
ip access-list acl-udf
permit ip 10.0.0.2/32 any udf udf_tcpflags 0x20 0xff
monitor session 1
source interface Ethernet 1/1
filter access-group acl-udf
```
This example shows how to configure UDF-based SPAN to match regular IP packets with a packet signature (DEADBEEF) at 6 bytes after a Layer 4 header start using the following match criteria:

- Outer source IP address: 10.0.0.2
- Inner TCP flags: Urgent TCP flag is set
- Bytes: EthHdr (14) + IP (20) + TCP (20) + Payload: 112233445566DEADBEEF7788
- Offset from Layer 4 header start: 20 + 6 = 26
- UDF match value: 0xDEADBEEF (split into two-byte chunks and two UDFs)
- UDF mask: 0xFFFFFFFF

```
udf udf_pktsig_msb header outer l3 26 2
udf udf_pktsig_lsb header outer l3 28 2
hardware access-list tcam region racl qualify udf udf_pktsig_msb udf_pktsig_lab
copy running-config startup-config
reload
ip access-list acl-udf-pktsig
permit udf udf_pktsig_msb 0xDEAD 0xFFFF udf udf_pktsig_lsb 0xBEEF 0xFFFF
monitor session 1
source interface Ethernet 1/1
filter access-group acl-udf-pktsig
```

Configuration Example for SPAN Truncation

This example shows how to configure SPAN truncation for use with MPLS stripping:

```
mpls strip
ip access-list mpls
statistics per-entry
20 permit ip any any redirect Ethernet1/5
interface Ethernet1/5
switchport
switchport mode trunk
mtu 9216
no shutdown
monitor session 1
source interface Ethernet1/5 tx
mtu 64
destination interface Ethernet1/6
no shut
```

Configuration Examples for Multicast Tx SPAN Across LSE Slices

This example shows how to configure multicast Tx SPAN across LSE slices for Cisco Nexus 9300-EX platform switches. It also shows sample output before and after multicast Tx SPAN is configured.

**Before Multicast Tx SPAN Is Configured**

```
switch# show interface eth1/15-16, ethernet 1/27 counters
```

<table>
<thead>
<tr>
<th>Port</th>
<th>InOctets</th>
<th>InUcastPkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth1/15</td>
<td>580928</td>
<td>0</td>
</tr>
<tr>
<td>Eth1/16</td>
<td>239</td>
<td>0</td>
</tr>
</tbody>
</table>
### Configuring Multicast Tx SPAN

```
switch(config)# hardware multicast global-tx-span
Warning: Global Tx SPAN setting changed, please save config and reload
switch(config)# copy running-config start-up config
[########################################] 100%
Copy complete.
switch(config)# reload
This command will reboot the system. (y/n)? [n] y
```

### After Multicast Tx SPAN Is Configured

```
switch# show interface eth1/15-16, eth1/27 counters
```

<table>
<thead>
<tr>
<th>Port</th>
<th>InOctets</th>
<th>InUcastPkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth1/15</td>
<td>392576</td>
<td>0</td>
</tr>
<tr>
<td>Eth1/16</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Eth1/27</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>InMcastPkts</th>
<th>InBcastPkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth1/15</td>
<td>6134</td>
<td>0</td>
</tr>
<tr>
<td>Eth1/16</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Eth1/27</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>OutOctets</th>
<th>OutUcastPkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth1/15</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Eth1/16</td>
<td>392644</td>
<td>0</td>
</tr>
<tr>
<td>Eth1/27</td>
<td>417112</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>OutMcastPkts</th>
<th>OutBcastPkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth1/15</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Eth1/16</td>
<td>6135</td>
<td>0</td>
</tr>
</tbody>
</table>
# Additional References

## Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL TCAM regions</td>
<td><em>Cisco Nexus 9000 Series NX-OS Security Configuration Guide</em></td>
</tr>
<tr>
<td>FEX</td>
<td><em>Cisco Nexus 2000 Series NX-OS Fabric Extender Software Configuration Guide for Cisco Nexus 9000 Series Switches</em></td>
</tr>
</tbody>
</table>
CHAPTER 17

Configuring ERSPAN

This chapter describes how to configure an encapsulated remote switched port analyzer (ERSPAN) to transport mirrored traffic in an IP network on Cisco NX-OS devices.

• About ERSPAN, on page 249
• Licensing Requirements for ERSPAN, on page 250
• Prerequisites for ERSPAN, on page 251
• Guidelines and Limitations for ERSPAN, on page 251
• Default Settings, on page 253
• Configuring ERSPAN, on page 254
• Verifying the ERSPAN Configuration, on page 264
• Configuration Examples for ERSPAN, on page 265

About ERSPAN

ERSPAN transports mirrored traffic over an IP network, which provides remote monitoring of multiple switches across your network. The traffic is encapsulated at the source router and is transferred across the network. The packet is decapsulated at the destination router and then sent to the destination interface.

ERSPAN Sources

The interfaces from which traffic can be monitored are called ERSPAN sources. Sources designate the traffic to monitor and whether to copy ingress, egress, or both directions of traffic. ERSPAN sources include the following:

• Ethernet ports (but not subinterfaces)
• Port channels
• The inband interface to the control plane CPU
• VLANs

Note

When a VLAN is specified as an ERSPAN source, all supported interfaces in the VLAN are ERSPAN sources.
ERSPAN Sessions

You can create ERSPAN sessions that designate sources to monitor.

Localized ERSPAN Sessions

An ERSPAN session is localized when all of the source interfaces are on the same line card.

Note
An ERSPAN session with a VLAN source is not localized

ERSPAN Truncation

Beginning with Cisco NX-OS Release 7.0(3)I7(1), you can configure the truncation of source packets for each ERSPAN session based on the size of the MTU. Truncation helps to decrease ERSPAN bandwidth by reducing the size of monitored packets. Any ERSPAN packet that is larger than the configured MTU size is truncated to the given size. For ERSPAN, an additional ERSPAN header is added to the truncated packet from 54 to 166 bytes depending on the ERSPAN header type. For example, if you configure the MTU as 300 bytes, the packets are replicated with an ERSPAN header size from 354 to 466 bytes depending on the ERSPAN header type configuration.

ERSPAN truncation is disabled by default. To use truncation, you must enable it for each ERSPAN session.

Licensing Requirements for ERSPAN

The following table shows the licensing requirements for this feature:

<table>
<thead>
<tr>
<th>Product</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco NX-OS</td>
<td>ERSPAN requires no license. Any feature not included in a license package is bundled with the nx-os image and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the Cisco NX-OS Licensing Guide.</td>
</tr>
</tbody>
</table>
Prerequisites for ERSPAN

ERSPAN has the following prerequisites:

- You must first configure the ports on each device to support the desired ERSPAN configuration. For more information, see the Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide.

Guidelines and Limitations for ERSPAN

ERSPAN has the following configuration guidelines and limitations:

- ERSPAN destination handles jumbo frames for MTU differently based on the platform. For the following Cisco Nexus 9300-series switches (and supporting line cards), ERSPAN destination drops the jumbo frames:
  - N9K-C9332PQ
  - N9K-C9372PX
  - N9K-C9372PX-E
  - N9K-C9372TX
  - N9K-C9372TX-E
  - N9K-C93120TX
  - N9K-X9564PX
  - N9K-X9464TX
  - N9K-X9464TX2
  - N9K-X9564TX
  - N9K-X9464PX
  - N9K-X9536PQ
  - N9K-X9636PQ
  - N9K-X9432PQ
  For the following Cisco Nexus 9200-series switches (and supporting line cards), ERSPAN truncates the packets at port MTU, and issues a TX Output error:
  - N9K-C92160YCX-X
  - N9K-C92304QC
  - N9K-C9272Q
  - N9K-C9232C
  - N9K-C9236C
• For ERSPAN session limits, see theCisco Nexus 9000 Series NX-OS Verified Scalability Guide.

• The number of ERSPAN sessions per line card reduces to two if the same interface is configured as a bidirectional source in more than one session.

• Only ERSPAN source sessions are supported. Destination sessions are not supported.

• Configuring two SPAN or ERSPAN sessions on the same source interface, with only one filter is not supported.

• Statistics are not supported for the filter access group.

• An access-group filter in an ERSPAN session must be configured as vlan-accessmap.

• Control plane packets that are generated by the supervisor cannot be ERSPAN encapsulated or filtered by an ERSPAN access control list (ACL).

• ERSPAN is not supported for management ports.

• ERSPAN does not support destinations on Layer 3 port-channel subinterfaces.

• A VLAN can be part of only one session when it is used as an ERSPAN source or filter.

• VLAN ERSPAN monitors only the traffic that leaves or enters Layer 2 ports in the VLAN.

• If you enable ERSPAN on a vPC and ERSPAN packets must be routed to the destination through the vPC, packets that come through the vPC peer link cannot be captured.

• ERSPAN is not supported over a VXLAN overlay.

• ERSPAN copies for multicast packets are made before rewrite. Therefore, the TTL, VLAN ID, any remarking due to egress policy, and so on, are not captured in the ERSPAN copy.

• The timestamp granularity of ERSPAN Type III sessions is not configurable through the CLI. It is 100 picoseconds and driven through PTP.

• ERSPAN works on default and nondefault VRFs, but ERSPAN marker packets work only on the default VRF.

• The same source can be part of multiple sessions.

The following guidelines and limitations apply to egress (Tx) ERSPAN:
• The flows for post-routed unknown unicast flooded packets are in the ERSPAN session, even if the ERSPAN session is configured to not monitor the ports on which this flow is forwarded. This limitation applies to Network Forwarding Engine (NFE) and NFE2-enabled EOR switches and ERSPAN sessions that have TX port sources.

• The following guidelines and limitations apply to ingress (Rx) ERSPAN:
  - VLAN sources are spanned only in the Rx direction.
  - Session filtering functionality (VLAN or ACL filters) is supported only for Rx sources.
  - VLANs are supported as ERSPAN sources only in the ingress direction.

• The following guidelines and limitations apply to FEX ports:
  - If the sources used in bidirectional ERSPAN sessions are from the same FEX, the hardware resources are limited to two ERSPAN sessions.
  - FEX ports are supported as ERSPAN sources in the ingress direction for all traffic and in the egress direction only for known Layer 2 unicast traffic.
  - The Cisco Nexus 9300Series does not support ERSPAN destination being connected on aFEX interface. The ERSPAN destination must be connected to a front panel port.
  - VLAN and ACL filters are not supported for FEX ports.
    - It cannot co-exist with filters.
    - FEX ports are supported as ERSPAN sources in the ingress direction for all traffic and in the egress direction only for known Layer 2 unicast traffic.
    - The Cisco Nexus 9300Series does not support ERSPAN destination being connected on aFEX interface. The ERSPAN destination must be connected to a front panel port.
    - VLAN and ACL filters are not supported for FEX ports.

• Priority flow control (PFC) ERSPAN has the following guidelines and limitations:
  - It cannot co-exist with filters
  - It is supported only in the Rx direction on physical or port-channel interfaces. It is not supported in the Rx direction on VLAN interfaces or in the Tx direction.

### Default Settings

The following table lists the default settings for ERSPAN parameters.

#### Table 20: Default ERSPAN Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERSPAN sessions</td>
<td>Created in the shut state</td>
</tr>
<tr>
<td>ERSPAN marker packet interval</td>
<td>100 milliseconds</td>
</tr>
</tbody>
</table>
Configuring ERSPAN

Note
Be aware that the Cisco NX-OS commands for this feature may differ from those commands used in Cisco IOS.

Configuring an ERSPAN Source Session

You can configure an ERSPAN session on the local device only. By default, ERSPAN sessions are created in the shut state.

Note
ERSPAN does not monitor any packets that are generated by the supervisor, regardless of their source.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)#</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>monitor erspan origin ip-address ip-address global</code></td>
<td>Configures the ERSPAN global origin IP address.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)# monitor erspan origin ip-address 10.0.0.1 global</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>`no monitor session {session-number</td>
<td>Clears the configuration of the specified ERSPAN session. The new session configuration is added to the existing session configuration.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>all}`</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)# no monitor session 3</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>`monitor session {session-number</td>
<td>Configures an ERSPAN Type II source session. By default the session is bidirectional. The optional keyword shut specifies a shut state for the selected session.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>all} type erspan-source [shut]`</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)# monitor session 3 type erspan-source</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config-erspan-src)#</code></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring an ERSPAN Source Session

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong></td>
<td><code>description description</code></td>
<td>Configures a description for the session. By default, no description is defined. The description can be up to 32 alphanumeric characters.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config-erspan-src)# description erspan_src_session_3</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>`source {interface type [ tx</td>
<td>rx</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config-erspan-src)# source interface ethernet 2/1-3, ethernet 3/1 rx</td>
<td>You can configure one or more sources, as either a series of comma-separated entries or a range of numbers. You can specify the traffic direction to copy as ingress, egress, or both.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config-erspan-src)# source interface port-channel 2</td>
<td>For a unidirectional session, the direction of the source must match the direction specified in the session.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config-erspan-src)# source interface sup-eth 0 both</td>
<td><strong>Note</strong> Source VLANs are supported only in the ingress direction. Source FEX ports are supported in the ingress direction for all traffic and in the egress direction only for known Layer 2 unicast traffic.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><em>(Optional)</em> Repeat Step 7 to configure all ERSPAN sources.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>`filter vlan {number</td>
<td>range}`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config-erspan-src)# filter vlan 3-5, 7</td>
<td><strong>Note</strong> A FEX port that is configured as an ERSPAN source does not support VLAN filters.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><em>(Optional)</em> Repeat Step 9 to configure all source VLANs — to filter.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td><code>filter access-group acl-filter</code></td>
<td>Associates an ACL with the ERSPAN session. (You can create an ACL using the standard ACL configuration process. For more</td>
</tr>
</tbody>
</table>
### Configuring an ERSPAN Source Session

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>switch(config-erspan-src)# filter access-group ACL1</strong>&lt;br&gt;<strong>Example:</strong></td>
<td>information, see the Cisco Nexus 9000 Series NX-OS Security Configuration Guide.)</td>
</tr>
<tr>
<td><strong>Step 11</strong>&lt;br&gt;<strong>destination ip ip-address</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;switch(config-erspan-src)# destination ip 10.1.1.1</td>
<td>Configures the destination IP address in the ERSPAN session. Only one destination IP address is supported per ERSPAN source session.</td>
</tr>
<tr>
<td><strong>Step 12</strong>&lt;br&gt;<strong>erspan-id erspan-id</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;switch(config-erspan-src)# erspan-id 5</td>
<td>Configures the ERSPAN ID for the ERSPAN source session. The ERSPAN range is from 1 to 1023.</td>
</tr>
<tr>
<td><strong>Step 13</strong>&lt;br&gt;<strong>vrf vrf-name</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;switch(config-erspan-src)# vrf default</td>
<td>Configures the virtual routing and forwarding (VRF) instance that the ERSPAN source session uses for traffic forwarding. The VRF name can be any case-sensitive, alphanumeric string up to 32 characters.</td>
</tr>
<tr>
<td><strong>Step 14</strong>&lt;br&gt;<strong>(Optional) ip ttl ttl-number</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;switch(config-erspan-src)# ip ttl 25</td>
<td>Configures the IP time-to-live (TTL) value for the ERSPAN traffic. The range is from 1 to 255.</td>
</tr>
<tr>
<td><strong>Step 15</strong>&lt;br&gt;<strong>(Optional) ip dscp dscp-number</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;switch(config-erspan-src)# ip dscp 42</td>
<td>Configures the differentiated services code point (DSCP) value of the packets in the ERSPAN traffic. The range is from 0 to 63.</td>
</tr>
<tr>
<td><strong>Step 16</strong>&lt;br&gt;<strong>(Optional) [no] marker-packet milliseconds</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;switch(config-erspan-src)# marker-packet 100</td>
<td>Enables the ERSPAN marker packet for a session in order to recover the real value of the ERSPAN timestamp. The interval can range from 100 to 1000 milliseconds. The no form of this command disables the marker packet for the session.</td>
</tr>
<tr>
<td><strong>Step 17</strong>&lt;br&gt;<strong>no shut</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;switch(config-erspan-src)# no shut</td>
<td>Enables the ERSPAN source session. By default, the session is created in the shut state.</td>
</tr>
<tr>
<td><strong>Step 18</strong>&lt;br&gt;<strong>exit</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;switch(config-erspan-src)# exit&lt;br&gt;switch(config)#</td>
<td>Exits the monitor configuration mode.</td>
</tr>
<tr>
<td><strong>Step 19</strong>&lt;br&gt;**(Optional) show monitor session {all</td>
<td>session-number [range session-range]} [brief]**&lt;br&gt;<strong>Example:</strong>&lt;br&gt;switch(config)# show monitor session 3</td>
</tr>
</tbody>
</table>
Purpose
Command or Action | Purpose
--- | ---
Step 20 | (Optional) show running-config monitor
Example:
switch(config)# show running-config monitor | Displays the running ERSPAN configuration.
Step 21 | (Optional) show startup-config monitor
Example:
switch(config)# show startup-config monitor | Displays the ERSPAN startup configuration.
Step 22 | (Optional) copy running-config startup-config
Example:
switch(config)# copy running-config startup-config | Copies the running configuration to the startup configuration.

## Shutting Down or Activating an ERSPAN Session

You can shut down ERSPAN sessions to discontinue the copying of packets from sources to destinations. You can shut down one session in order to free hardware resources to enable another session. By default, ERSPAN sessions are created in the shut state.

You can enable ERSPAN sessions to activate the copying of packets from sources to destinations. To enable an ERSPAN session that is already enabled but operationally down, you must first shut it down and then enable it. You can shut down and enable the ERSPAN session states with either a global or monitor configuration mode command.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | configure terminal
Example:
switch# configure terminal
switch(config)# |
| Enters global configuration mode. |
| **Step 2** | monitor session {session-range | all} shut
Example:
switch(config)# monitor session 3 shut |
| Shuts down the specified ERSPAN sessions. By default, sessions are created in the shut state. |
| **Step 3** | no monitor session {session-range | all} shut
Example:
switch(config)# no monitor session 3 shut |
| Resumes (enables) the specified ERSPAN sessions. By default, sessions are created in the shut state.
If a monitor session is enabled but its operational status is down, then to enable the session, you must first specify the monitor... |
### Configuring an ERSPAN ACL

You can create an IPv4 ERSPAN ACL on the device and add rules to it.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>session shut</td>
<td>session shut command followed by the no monitor session shut command.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>monitor session session-number type erspan-source</td>
<td>Enters the monitor configuration mode for the ERSPAN source type. The new session configuration is added to the existing session configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# monitor session 3 type erspan-source</td>
<td></td>
</tr>
<tr>
<td>switch(config-erspan-src)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>shut</td>
<td>Shuts down the ERSPAN session. By default, the session is created in the shut state.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config-erspan-src)# shut</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td>no shut</td>
<td>Enables the ERSPAN session. By default, the session is created in the shut state.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config-erspan-src)# no shut</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td>Exits the monitor configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config-erspan-src)# exit</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td></td>
</tr>
<tr>
<td>(Optional) show monitor session all</td>
<td>Displays the status of ERSPAN sessions.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# show monitor session all</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td></td>
</tr>
<tr>
<td>(Optional) show running-config monitor</td>
<td>Displays the ERSPAN running configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# show running-config monitor</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td></td>
</tr>
<tr>
<td>(Optional) show startup-config monitor</td>
<td>Displays the ERSPAN startup configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# show startup-config monitor</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td></td>
</tr>
<tr>
<td>(Optional) copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>
Before you begin

To modify the DSCP value or the GRE protocol, you need to allocate a new destination monitor session. A maximum of four destination monitor sessions are supported.

### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)#</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ip access-list acl-name</td>
<td>Creates the ERSPAN ACL and enters IP ACL configuration mode. The acl-name argument can be up to 64 characters.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# ip access-list erSPAN-acl</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config-acl)#</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>[sequence-number] {permit</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Example:</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch(config-acl)# permit ip 192.168.2.0/24 any</td>
</tr>
<tr>
<td>set-erspan-dscp 40 set-erspan-greproto 5555</td>
</tr>
</tbody>
</table>

The `permit` and `deny` commands support many ways of identifying traffic. The `sequence-number` argument can be a whole number between 1 and 4294967295.}

The `set-erspan-dscp` option sets the DSCP value in the ERSPAN outer IP header. The range for the DSCP value is from 0 to 63. The DSCP value configured in the ERSPAN ACL overrides the value configured in the monitor session. If you do not include this option in the ERSPAN ACL, 0 or the DSCP value configured in the monitor session will be set.

The `set-erspan-greproto` option sets the protocol value in the ERSPAN GRE header. The range for the protocol value is from 0 to 65535. If you do not include this option in the ERSPAN ACL, the default value of 0x88be will be set as the protocol in the GRE header for ERSPAN-encapsulated packets.

Each access control entry (ACE) with the `set-erspan-greproto` or `set-erspan-dscp` action consumes one destination monitor session. A maximum of three ACEs with one of these actions is supported per ERSPAN ACL. For example, you can configure one of the following:

- One ERSPAN session with an ACL having a maximum of three ACEs with the
### Configuring ERSPAN

You can configure the device to match on user-defined fields (UDFs) of the outer or inner packet fields (header or payload) and to send the matching packets to the ERSPAN destination. Doing so can help you to analyze and isolate packet drops in the network.

#### Before you begin

Make sure that the appropriate TCAM region (racl, ifacl, or vacl) has been configured using the `hardware access-list tcam region` command to provide enough free space to enable UDF-based ERSPAN. For information, see the "Configuring ACL TCAM Region Sizes" section in the Cisco Nexus 9000 Series NX-OS Security Configuration Guide.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

### Configuring UDF-Based ERSPAN

You can configure the device to match on user-defined fields (UDFs) of the outer or inner packet fields (header or payload) and to send the matching packets to the ERSPAN destination. Doing so can help you to analyze and isolate packet drops in the network.

#### Before you begin

Make sure that the appropriate TCAM region (racl, ifacl, or vacl) has been configured using the `hardware access-list tcam region` command to provide enough free space to enable UDF-based ERSPAN. For information, see the "Configuring ACL TCAM Region Sizes" section in the Cisco Nexus 9000 Series NX-OS Security Configuration Guide.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td>(Optional) <code>show ip access-lists name</code></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>switch(config-acl)# show ip access-lists erpsan-acl</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>(Optional) `show monitor session {all</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>switch(config-acl)# show monitor session 1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>(Optional) <code>copy running-config startup-config</code></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>switch(config-acl)# copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring UDF-Based ERSPAN

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| switch# configure terminal  
switch(config)# | Defines the UDF as follows:  
• **udf-name**—Specifies the name of the UDF. You can enter up to 16 alphanumeric characters for the name.  
• **offset-base**—Specifies the UDF offset base as follows, where **header** is the packet header to consider for the offset:  
  - **packet-start**  
  - **header**  
    - **outer**  
    - **inner**  
    - **l3**  
    - **l4**  
• **offset**—Specifies the number of bytes offset from the offset base. To match the first byte from the offset base (Layer 3/Layer 4 header), configure the offset as 0.  
• **length**—Specifies the number of bytes from the offset. Only 1 or 2 bytes are supported. To match additional bytes, you must define multiple UDFs.  
You can define multiple UDFs, but Cisco recommends defining only required UDFs. |
| **Step 2**  
**udf udf-name offset-base offset length**  
**Example:**  
switch(config)# udf udf-x packet-start  
12 1  
switch(config)# udf udf-y header outer  
13 20 2 | |
| **Step 3**  
**hardware access-list tcam region**  
{ **racl** | **ifacl**  
| **vacl** } qualify **udf**  
**udf-names**  
**Example:**  
switch(config)# hardware access-list tcam region  
racl qualify udf udf-x udf-y | Attaches the UDFs to one of the following TCAM regions:  
• **racl**—Applies to Layer 3 ports.—Applies to layer 2 and Layer 3 ports.  
• **ifacl**—Applies to Layer 2 ports.  
• **vacl**—Applies to source VLANs.  
You can attach up to 8 UDFs to a TCAM region. |
### Configuring UDF-Based ERSPAN

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td>Required: <code>copy running-config startup-config</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;<code>switch(config)# copy running-config startup-config</code>&lt;br&gt;Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Required: <code>reload</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;<code>switch(config)# reload</code>&lt;br&gt;Reloads the device.&lt;br&gt;<strong>Note</strong> Your UDF configuration is effective only after you enter <code>copy running-config startup-config + reload</code>.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>ip access-list erspan-acl</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;<code>switch(config)# ip access-list erspan-acl udf-only</code>&lt;br&gt;<code>switch(config-acl)#</code>&lt;br&gt;Creates an IPv4 access control list (ACL) and enters IP access list configuration mode.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Enter one of the following commands:&lt;br&gt;• <code>permit udf udf-name value mask</code>&lt;br&gt;• <code>permit ip source destination udf udf-name value mask</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;<code>switch(config-acl)# permit udf udf-x 0x40 0xF0 udf-y 0x1001 0xF00F</code>&lt;br&gt;<code>switch(config-acl)# permit ip 10.0.0./24 any udf udf-x 0x02 0x0F udf-y 0x1001 0xF00F</code>&lt;br&gt;Configures the ACL to match only on UDFs (example 1) or to match on UDFs along with the current access control entries (ACEs) for the outer packet fields (example 2).&lt;br&gt;A single ACL can have ACEs with and without UDFs together. Each ACE can have different UDF fields to match, or all ACEs can match for the same list of UDFs.</td>
</tr>
</tbody>
</table>
**Configuring ERSPAN Truncation**

You can configure truncation for local and ERSPAN source sessions only.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)#</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>monitor session session-number type erspan-source</code></td>
<td>Enters monitor configuration mode for the specified ERSPAN session.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)# monitor session 10 type erspan-source</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config-erspan-src)#</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>`source interface type slot/port [rx</td>
<td>tx</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config-erspan-src)# source interface ethernet 1/5 both</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>mtu size</code></td>
<td>Configures the MTU size for truncation. Any ERSPAN packet that is larger than the configured MTU size is truncated to the configured size. The MTU ranges for ERSPAN packet truncation are:</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config-erspan-src)# mtu 512</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config-erspan-src)# mtu ?</code></td>
<td>&lt;512-1518&gt; Enter the value of MTU truncation size for ERSPAN packets (erspan header + truncated original packet)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The MTU size range is 512 to 1518 bytes for Cisco Nexus 9300-EX platform switches.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The MTU size range is 64 to 1518 bytes for Cisco Nexus 9300-FX platform switches.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>destination interface type slot/port</code></td>
<td>Configures the Ethernet ERSPAN destination port.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config-erspan-src)# destination interface Ethernet 1/39</code></td>
<td></td>
</tr>
</tbody>
</table>

**Step 8**

(Optional) `copy running-config startup-config`

**Example:**

```
switch(config)# copy running-config startup-config
```
### Configuring ERSPAN

#### Verifying the ERSPAN Configuration

To display the ERSPAN configuration, perform one of the following tasks:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip access-lists name</code></td>
<td>Displays the ERSPAN ACL configuration.</td>
</tr>
</tbody>
</table>
| `show monitor session {all | session-number | range session-range} [brief]` | Displays the ERSPAN session configuration. The output includes the egress interface that is used to send the ERSPAN packets. The output varies depending on the type of egress interface used:  
  - Physical Layer 3 interface—Displays the interface name.  
  - SVI interface—Displays the member interface through which the route was learned.  
  - Layer 3 port channel—Displays the port-channel interface name.  
  - Layer 3 subinterface—Displays the parent interface name.  
  - ECMP path—Displays the name of one of the equal-cost multipath (ECMP) member interfaces. Only the interface that is displayed will be used for mirroring the traffic even though the route is ECMP.  
  - PFC on interfaces—Displays the priority flow control (PFC) status on the interface. |
| `show running-config monitor` | Displays the running ERSPAN configuration. |
**Configuration Examples for ERSPAN**

**Configuration Example for a Unidirectional ERSPAN Session**

This example shows how to configure a unidirectional ERSPAN session:

```
switch# configure terminal
switch(config)# interface ethernet 14/30
switch(config-if)# no shut
switch(config-if)# exit
switch(config)# no monitor session 3
switch(config)# monitor session 3 rx
switch(config-erspan-src)# source interface ethernet 2/1-3 rx
switch(config-erspan-src)# erspan-id 1
switch(config-erspan-src)# ip ttl 16
switch(config-erspan-src)# ip dscp 5
switch(config-erspan-src)# vrf default
switch(config-erspan-src)# destination ip 9.1.1.2
switch(config-erspan-src)# no shut
switch(config-erspan-src)# exit
switch(config)# show monitor session 1
```

**Configuration Example for an ERSPAN ACL**

This example shows how to configure an ERSPAN ACL:

```
switch# configure terminal
switch(config)# ip access-list match_11_pkts
switch(config-acl)# permit ip 11.0.0.0 0.255.255.255 any
switch(config-acl)# exit
switch(config)# ip access-list match_12_pkts
switch(config-acl)# permit ip 12.0.0.0 0.255.255.255 any
switch(config-acl)# exit
switch(config)# vlan access-map erspan_filter 5
switch(config-access-map)# match ip address match_11_pkts
switch(config-access-map)# action forward
switch(config-access-map)# exit
switch(config)# vlan access-map erspan_filter 10
switch(config-access-map)# match ip address match_12_pkts
switch(config-access-map)# action forward
switch(config-access-map)# exit
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# filter access_group erspan_filter
```

**Configuration Example for a Marker Packet**

This example shows how to enable the ERSPAN marker packet with an interval of 2 seconds:

```
switch# configure terminal
switch(config)# monitor erspan origin ip-address 172.28.15.250 global
switch(config)# monitor session 1 type erspan-source
```

---

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show startup-config monitor</td>
<td>Displays the ERSPAN startup configuration.</td>
</tr>
</tbody>
</table>
switch(config-erspan-src)# header-type 3
switch(config-erspan-src)# erspan-id 1
switch(config-erspan-src)# ip ttl 16
switch(config-erspan-src)# ip dscp 5
switch(config-erspan-src)# vrf default
switch(config-erspan-src)# destination ip 9.1.1.2
switch(config-erspan-src)# source interface ethernet 1/15 both
switch(config-erspan-src)# marker-packet 100
switch(config-erspan-src)# no shut
switch(config-erspan-src)# show monitor session 1

---------------
type : erspan-source
state : up
granularity : nanoseconds
erspan-id : 1
vrf-name : default
destination-ip : 9.1.1.2
ip-ttl : 16
ip-dscp : 5
header-type : 3
origin-ip : 172.28.15.250 (global)
source intf :
    rx : Eth1/15
tx : Eth1/15
both : Eth1/15
    rx :
marker-packet : enabled
packet interval : 100
packet sent : 25
packet failed : 0
egress-intf :

Configuration Examples for UDF-Based ERSPAN

This example shows how to configure UDF-based ERSPAN to match on the inner TCP flags of an encapsulated IP-in-IP packet using the following match criteria:

- Outer source IP address: 10.0.0.2
- Inner TCP flags: Urgent TCP flag is set
- Bytes: EthHdr (14) + Outer IP (20) + Inner IP (20) + Inner TCP (20) + Inner TCP flags at 13th byte
- Offset from packet-start: 14 + 20 + 20 + 13 = 67
- UDF match value: 0x20
- UDF mask: 0xFF

udf udf_tcpflags packet-start 67 1
hardware access-list tcam region racl qualify udf udf_tcpflags
copy running-config startup-config
reload
ip access-list acl-udf
permit ip 10.0.0.2/32 any udf udf_tcpflags 0x20 0xff
monitor session 1 type erspan-source
source interface Ethernet 1/1
filter access-group acl-udf
This example shows how to configure UDF-based ERSPAN to match regular IP packets with a packet signature (DEADBEEF) at 6 bytes after a Layer 4 header start using the following match criteria:

- Outer source IP address: 10.0.0.2
- Inner TCP flags: Urgent TCP flag is set
- Bytes: Eth Hdr (14) + IP (20) + TCP (20) + Payload: 11223445566DEADBEEF7788
- Offset from Layer 4 header start: 20 + 6 = 26
- UDF match value: 0xDEADBEEF (split into two-byte chunks and two UDFs)
- UDF mask: 0xFFFFFFFF

```
udf udf_pktsig_msb header outer l3 26 2
udf udf_pktsig_lsb header outer l3 28 2
hardware access-list tcam region racl qualify udf udf_pktsig_msb udf_pktsig_lsb
copy running-config startup-config
reload
ip access-list acl-udf-pktsig
permit udf udf_pktsig_msb 0xDEAD 0xFFFF udf udf_pktsig_lsb 0xBEEF 0xFFFF
monitor session 1 type erspan-source
source interface Ethernet 1/1
filter access-group acl-udf-pktsig
```

### Configuration Example for ERSPAN Truncation

This example shows how to configure ERSPAN truncation for use with MPLS stripping:

```
mpls strip
ip access-list mpls
   statistics per-entry
   20 permit ip any any redirect Ethernet1/5

interface Ethernet1/5
   switchport
   switchport mode trunk
   mtu 9216
   no shutdown

monitor session 1
   source interface Ethernet1/5 tx
   mtu 64
   destination interface Ethernet1/6
   no shut
monitor session 21 type erspan-source
   description "ERSPAN Session 21"
   header-type 3
   erspan-id 21
   vrf default
   destination ip 19.1.1.2
   source interface Ethernet1/5 tx
   mtu 64
   no shut
monitor session 22 type erspan-source
   description "ERSPAN Session 22"
   erspan-id 22
   vrf default
   destination ip 19.2.1.2
   source interface Ethernet1/5 tx
```

mtu 750
no shut
monitor session 23 type erspan-source
description "ERSPAN Session 23"
header-type 3
marker-packet 1000
erspan-id 23
vrf default
destination ip 19.3.1.2
source interface Ethernet1/5 tx
mtu 1000
no shut
About LLDP

The Cisco Discovery Protocol (CDP) is a device discovery protocol that allows network management applications to automatically discover and learn about other Cisco devices that are connected to the network. To permit the discovery of non-Cisco devices, the switch also supports the Link Layer Discovery Protocol (LLDP), a vendor-neutral device discovery protocol that is defined in the IEEE 802.1ab standard. LLDP allows network devices to advertise information about themselves to other devices on the network. This protocol runs over the data-link layer, which allows two systems running different network layer protocols to learn about each other.

LLDP is a one-way protocol that transmits information about the capabilities and current status of a device and its interfaces. LLDP devices use the protocol to solicit information only from other LLDP devices.

LLDP supports a set of attributes that it uses to discover other devices. These attributes contain type, length, and value (TLV) descriptions. LLDP devices can use TLVs to send and receive information to other devices on the network. Details such as configuration information, device capabilities, and device identity can be advertised using this protocol.

LLDP advertises the following TLVs by default:

- DCBXP
- Management address
- Port description
About DCBXP

The Data Center Bridging Exchange Protocol (DCBXP) is an extension of LLDP. It is used to announce, exchange, and negotiate node parameters between peers. DCBXP parameters are packaged as DCBXP TLVs in the LLDP packet. If CEE is used, DCBXP will use an acknowledgment mechanism over LLDP. When the port comes up, DCBX TLVs are sent and any DCBX TLVs received are processed. By default, the DCBX protocol is set to auto-detect, and the latest protocol version supported by both the peers is used.

Features that need to exchange and negotiate parameters with peer nodes using DCBXP are as follows:

- **Priority-based Flow Control (PFC)**—PFC is an enhancement to the existing Pause mechanism in Ethernet. It enables Pause based on user priorities or classes of service. A physical link that is divided into eight virtual links with PFC provides the capability to use Pause on a single virtual link without affecting traffic on the other virtual links. Enabling Pause on a per-user-priority basis allows administrators to create lossless links for traffic requiring no-drop service while retaining packet-drop congestion management for IP traffic.

- **Enhanced Transmission Selection (ETS)**—ETS enables optimal bandwidth management of virtual links. ETS is also called priority grouping. It enables differentiated treatments within the same priority classes of PFC. ETS provides prioritized processing based on bandwidth allocation, low latency, or best effort, resulting in per-group traffic class allocation. For example, an Ethernet class of traffic may have a high-priority designation and a best effort within that same class. ETS allows differentiation between traffic of the same priority class, thus creating priority groups.

- **Application Priority Configuration**—Carries information about the priorities that are assigned to specific protocols.

- **Priority to DSCP Mapping**—The mapping of the DSCP and COS values configured in the QOS policy are sent in the Application Priority TLV.

For information on the quality of service (QoS) features, see the Cisco Nexus 9000 Series NX-OS Quality of Service Configuration Guide.

DCBXP is enabled by default, provided LLDP is enabled. When LLDP is enabled, DCBXP can be enabled or disabled using the [no] `lldp tlv-select dcbxp` command. DCBXP is disabled on ports where LLDP transmit or receive is disabled.

**High Availability**

The LLDP feature supports stateless and stateful restarts. After a reboot or supervisor switchover, the running configuration is applied.
For more information on high availability, see the *Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide*.

**Virtualization Support**

One instance of LLDP is supported.

**Licensing Requirements for LLDP**

<table>
<thead>
<tr>
<th>Product</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco NX-OS</td>
<td>LLDP requires no license. Any feature not included in a license package is bundled with the nx-os image and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the <em>Cisco NX-OS Licensing Guide</em>.</td>
</tr>
</tbody>
</table>

**Guidelines and Limitations for LLDP**

LLDP has the following configuration guidelines and limitations:

- LLDP must be enabled on the device before you can enable or disable it on any interfaces.
- LLDP is supported only on physical interfaces.
- LLDP can discover up to one device per port.
- DCBXP is supported on the following platforms:
  - Cisco Nexus 9200, 9300-EX, 9300-FX, and 9300-FX2 Series switches
  - Cisco Nexus 9332C, 9332PQ, 9364C, 9372PX, 9372PX-E, and 9396PX switches
  - Cisco Nexus 9504 and 9508 switches with X9432PQ, X9464PX, X9536PQ, X9564PX, X9636PQ, X9732C-EX, and X9736C-FX, line cards
- The Cisco Nexus 3232C and 3264Q switches do not support DCBXP.
- DCBXP incompatibility messages might appear when you change the network QoS policy if a physical loopback connection is in the device. The incompatibility exists for only a short time and then clears.
- DCBX TLVs are sent only when the input queuing is configured and applied at the system level.
- PFC TLV are sent when pause is enabled for at least one COS value in network-qos policy and priority-flow-control mode should be auto in the Interface level.

**Default Settings for LLDP**

This table lists the LLDP default settings.
## Configuring LLDP

### Note

Cisco NX-OS commands for this feature may differ from Cisco IOS commands for a similar feature.

### Enabling or Disabling LLDP Globally

You can enable or disable LLDP globally on a device. You must enable LLDP globally to allow a device to send and receive LLDP packets.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code>&lt;br&gt;<code>Example:</code>&lt;br&gt;switch# configure terminal&lt;br&gt;switch(config)#</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>[no] feature lldp</code>&lt;br&gt;<code>Example:</code>&lt;br&gt;switch(config)# feature lldp</td>
<td>Enables or disables LLDP on the device. LLDP is disabled by default.</td>
</tr>
<tr>
<td>Step 3</td>
<td><em>(Optional)</em> <code>show running-config lldp</code>&lt;br&gt;<code>Example:</code>&lt;br&gt;switch(config)# show running-config lldp</td>
<td>Displays the global LLDP configuration. If LLDP is enabled, it shows &quot;feature lldp.&quot; If LLDP is disabled, it shows an &quot;Invalid command&quot; error.</td>
</tr>
</tbody>
</table>
### Enabling or Disabling LLDP on an Interface

After you globally enable LLDP, it is enabled on all supported interfaces by default. However, you can enable or disable LLDP on individual interfaces or selectively configure an interface to only send or only receive LLDP packets.

#### Before you begin

Make sure that you have globally enabled LLDP on the device.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><code>switch(config)#</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Specifies the interface on which you are enabling LLDP and enters the interface configuration mode.</td>
</tr>
<tr>
<td><code>interface interface slot/port</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>switch(config)# interface ethernet 7/1</code></td>
<td></td>
</tr>
<tr>
<td><code>switch(config-if)#</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enables or disables the transmission of LLDP packets on an interface. After you globally enable LLDP, it is enabled on all supported interfaces by default.</td>
</tr>
<tr>
<td><code>[no] lldp transmit</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>switch(config-if)# lldp transmit</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Enables or disables the reception of LLDP packets on an interface. After you globally enable LLDP, it is enabled on all supported interfaces by default.</td>
</tr>
<tr>
<td><code>[no] lldp receive</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>switch(config-if)# lldp receive</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Displays the LLDP configuration on the interface.</td>
</tr>
<tr>
<td><code>(Optional) show lldp interface interface slot/port</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>switch(config-if)# show lldp interface ethernet 7/1</code></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring the DCBXP Protocol Version

You can specify the protocol version in which the DCBX TLVs are sent.

**Note**

If the peers are not running the same version, DCBX parameters may not converge for the link. You may need to reset the link for the new protocol version to take effect.

**Before you begin**

Make sure that you have globally enabled LLDP on the device.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>switch# configure terminal</code>&lt;br&gt;<code>switch(config)#</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>interface interface slot/port</code></td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>switch(config)# interface ethernet 1/25</code>&lt;br&gt;<code>switch(config-if)#</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>lldp dcbx version cee/ieee/auto</code></td>
<td>Specifies the protocol version mode sent.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>switch(config-if)#lldp dcbx version cee</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The <code>cee</code> variable sets the port to only send TLVs in Converged Enhanced Ethernet (CEE) protocol version.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The <code>ieee</code> variable sets the port to only send TLVs in IEEE 802.1Qaz protocol version.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The <code>auto</code> variable sets the port to send TLVs in the latest protocol version supported by both the peers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default is set to <code>auto</code>.</td>
</tr>
</tbody>
</table>
### Configuring Optional LLDP Parameters

You can configure the frequency of LLDP updates, the amount of time for a receiving device to hold the information before discarding it, and the initialization delay time. You can also select the TLVs to include in LLDP packets.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
| **Example:** | `switch# configure terminal
switch(config)#` | |

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td><code>(Optional) [no] lldp holdtime seconds</code></td>
<td>Specifies the amount of time in seconds that a receiving device should hold the information that is sent by your device before discarding it. The range is 10 to 255 seconds; the default is 120 seconds.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>switch(config)# lldp holdtime 200</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td><code>(Optional) [no] lldp reinit seconds</code></td>
<td>Specifies the delay time in seconds for LLDP to initialize on any interface. The range is 1 to 10 seconds; the default is 2 seconds.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>switch(config)# lldp reinit 5</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td><code>(Optional) [no] lldp timer seconds</code></td>
<td>Specifies the transmission frequency of LLDP updates in seconds. The range is 5 to 254 seconds; the default is 30 seconds.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>switch(config)# lldp timer 50</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong></td>
<td><code>(Optional) show lldp timers</code></td>
<td>Displays the LLDP hold time, delay time, and update frequency configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>switch(config)# show lldp timers</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong></td>
<td><code>(Optional) [no] lldp tlv-select tlv</code></td>
<td>Specifies the TLVs to send and receive in LLDP packets. The available TLVs are dcbxp, management-address, port-description, port-vlan, system-capabilities, system-description, and system-name. All available TLVs are enabled by default.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>switch(config)# lldp tlv-select system-name</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 7</strong></td>
<td><code>(Optional) show lldp tlv-select</code></td>
<td>Displays the LLDP TLV configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>switch(config)# show lldp tlv-select</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 8</strong></td>
<td><code>(Optional) copy running-config startup-config</code></td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Verifying the LLDP Configuration

To display the LLDP configuration, perform one of the following tasks:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show running-config lldp</code></td>
<td>Displays the global LLDP configuration.</td>
</tr>
<tr>
<td><code>show lldp all</code></td>
<td>Displays the LLDP DCBXP, transmit and receive configuration for all interfaces.</td>
</tr>
<tr>
<td><code>show lldp interface slot/port</code></td>
<td>Displays the LLDP interface configuration.</td>
</tr>
<tr>
<td><code>show lldp timers</code></td>
<td>Displays the LLDP hold time, delay time, and update frequency configuration.</td>
</tr>
<tr>
<td><code>show lldp tlv-select</code></td>
<td>Displays the LLDP TLV configuration.</td>
</tr>
<tr>
<td><code>show lldp dcbx interface slot/port</code></td>
<td>Displays DCBXP TLV information for a specific interface.</td>
</tr>
<tr>
<td>`show lldp neighbors {detail</td>
<td>interface slot/port}`</td>
</tr>
<tr>
<td><code>show lldp traffic</code></td>
<td>Displays the LLDP counters, including the number of LLDP packets sent and received by the device, the number of discarded packets, and the number of unrecognized TLVs.</td>
</tr>
<tr>
<td><code>show lldp traffic interface slot/port</code></td>
<td>Displays the number of LLDP packets sent and received on the interface.</td>
</tr>
<tr>
<td><code>show qos dcbxp interface slot/port</code></td>
<td>Displays DCBXP information for a specific interface.</td>
</tr>
</tbody>
</table>

Use the `clear lldp counters` command to clear the LLDP statistics.

Configuration Example for LLDP

This example shows how to enable LLDP on a device; disable LLDP on some interfaces; configure optional parameters such as hold time, delay time, and update frequency; and disable several LLDP TLVs:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# feature lldp
switch(config)# interface ethernet 7/9
switch(config-if)# no lldp transmit
switch(config-if)# no lldp receive
switch(config-if)# exit
switch(config)# interface ethernet 7/10
switch(config-if)# no lldp transmit
switch(config-if)# no lldp receive
```
switch(config-if)# exit
switch(config)# lldp holdtime 200
switch(config)# lldp reinit 5
switch(config)# lldp timer 50
switch(config)# no lldp tlv-select port-vlan
switch(config)# no lldp tlv-select system-name
CHAPTER 19

Configuring NetFlow

This chapter describes how to configure the NetFlow feature on Cisco NX-OS devices.

This chapter contains the following sections:

- About NetFlow, on page 279
- Licensing Requirements for NetFlow, on page 281
- Prerequisites for NetFlow, on page 282
- Guidelines and Limitations for NetFlow, on page 282
- Configuring NetFlow, on page 283
- Verifying the NetFlow Configuration, on page 292
- Monitoring NetFlow, on page 293
- Configuration Example for NetFlow, on page 293

About NetFlow

NetFlow identifies packet flows for ingress IP packets and provides statistics based on these packet flows. NetFlow does not require any change to either the packets themselves or to any networking device.

NetFlow uses flows to provide statistics for accounting, network monitoring, and network planning. A flow is a unidirectional stream of packets that arrives on a source interface (or VLAN) and has the same values for the keys. A key is an identified value for a field within the packet. You create a flow using a flow record to define the unique keys for your flow.

Cisco NX-OS supports the flexible NetFlow feature that enables enhanced network anomalies and security detection. Flexible NetFlow allows you to define an optimal flow record for a particular application by selecting the keys from a large collection of predefined fields.

All key values must match for the packet to count in a given flow. A flow might gather other fields of interest, depending on the export record version that you configure. Flows are stored in the NetFlow cache.

You can export the data that NetFlow gathers for your flow by using a flow exporter and export this data to a remote NetFlow Collector, such as Cisco Stealthwatch. Cisco NX-OS exports a flow as part of a NetFlow export User Datagram Protocol (UDP) datagram under the following circumstances:

- Flows are exported periodically as per the flow timeout value, which defaults to 10 seconds if not configured.
- You have forced the flow to export.
The flow record determines the size of the data to be collected for a flow. The flow monitor combines the flow record and flow exporter with the NetFlow cache information.

Cisco NX-OS can gather NetFlow statistics and analyze all packets on the interface or subinterface.

**Dual-Layer NetFlow Implementation**

Unlike other Cisco Nexus platforms, Cisco Nexus 9000 Series switches separate NetFlow processing into two layers:

- The first layer supports per-packet visibility for line-rate traffic. Packets do not need to be sampled and statistically analyzed. Instead, the packets can be processed and aggregated at line rate.
- The second layer enables the gathering of flows at scale. It can maintain hundreds of thousands of flows without losing any flows and periodically exports them to an external collector.

**Flow Records**

A flow record defines the keys that NetFlow uses to identify packets and other fields of interest that NetFlow gathers for the flow. You can define a flow record with any combination of keys and fields of interest. Cisco NX-OS supports a rich set of keys. A flow record also defines the types of counters gathered per flow. You can configure 32- or 64-bit packet or byte counters.

The key fields are specified with the `match` keyword. The fields of interest and counters are specified under the `collect` keyword.

Cisco NX-OS enables the following match fields as the defaults when you create a flow record:

- match interface input
- match flow direction

**Flow Exporters**

A flow exporter contains network layer and transport layer details for the NetFlow export packet. You can configure the following information in a flow exporter:

- Export destination IP address
- Source interface
- UDP port number (where the NetFlow Collector is listening for NetFlow packets)—The default value is 9995.

---

**Note**

NetFlow export packets use the IP address that is assigned to the source interface. If the source interface does not have an IP address assigned to it, the flow exporter drops flows that were meant to be exported.

Cisco NX-OS exports data to the NetFlow Collector whenever a timeout occurs. You can configure a flush cache timeout (using the `flow timeout` command) to flush the cache and force a flow export.
Export Format

Cisco NX-OS supports the Version 9 export format. This format supports a more efficient network utilization than the older Version 5 export format and supports IPv6 and Layer 2 fields. In addition, the Version 9 export format supports the full 32-bit SNMP ifIndex values at the NetFlow Collector.

Layer 2 NetFlow Keys

You can define Layer 2 keys in flexible NetFlow records that you can use to capture flows in Layer 2 interfaces. The Layer 2 keys are as follows:

- Source and destination MAC addresses
- Source VLAN ID
- EtherType from the Ethernet frame

You can apply Layer 2 NetFlow to the following interfaces for the ingress direction:

- Switch ports in access mode
- Switch ports in trunk mode
- Layer 2 port channels

Note

You cannot apply Layer 2 NetFlow to VLANs, egress interfaces, or Layer 3 interfaces such as VLAN interfaces.

Flow Monitors

A flow monitor references the flow record and flow exporter. You apply a flow monitor to an interface.

High Availability

Cisco NX-OS supports stateful restarts for NetFlow. After a reboot, Cisco NX-OS applies the running configuration.

The flow cache is not preserved across restarts, and packets that come to the software during restarts cannot be processed.

Licensing Requirements for NetFlow

<table>
<thead>
<tr>
<th>Product</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco NX-OS</td>
<td>NetFlow requires no license. Any feature not included in a license package is bundled with the nx-os image and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the Cisco NX-OS Licensing Guide.</td>
</tr>
</tbody>
</table>
Prerequisites for NetFlow

NetFlow has the following prerequisites:

- Make sure that you understand the resources required on your device because NetFlow consumes memory and CPU resources.

- In order to provide enough free space to monitor flows, the ing-netflow TCAM region is carved to 512 by default on Cisco Nexus 9300-FX platform switches. If more space is required, use the **hardware access-list tcam region ing-netflow size** command to modify the size of this TCAM region, using a multiple of 512. For more information, see the "Configuring ACL TCAM Region Sizes" section in the Cisco Nexus 9000 Series NX-OS Security Configuration Guide.

Guidelines and Limitations for NetFlow

NetFlow has the following configuration guidelines and limitations:

- Beginning with Cisco NX-OS Release 9.2(2), the Cisco Nexus 9300-FX switch supports collecting the OUTPUT_SNMP field for NetFlow Data Export (NDE). No other Cisco Nexus 9000 platform switch or Cisco Nexus line card supports collecting the OUTPUT_SNMP field.

- For Cisco Nexus 9300-FX platform switches only, if you add a member to a port channel that is already configured for Layer 2 NetFlow, its NetFlow configuration is removed and the Layer 2 configuration of the port channel is added to it.

- NetFlow is not supported on tunnel interfaces.

- NetFlow is not supported for CPU-transmitted packets.

- Only ingress NetFlow is supported. Egress NetFlow is not supported.

- Flow cache can be cleared per flow type, such as Layer 2, IPv4, and IPv6. It cannot be cleared per flow monitor.

- Flow collection is not performed for ARP traffic.

- You must configure a source interface for the NetFlow Data Export (NDE). If you do not configure a source interface, the flow exporter drops flows that were meant to be exported.

- Layer 2 switched flow monitors are applied only to Layer 2 interfaces. IP and IPv6 flow monitors can be applied to VLANs, SVIs, Layer 3 routed interfaces, or subinterfaces.

- If you change a Layer 2 interface to a Layer 3 interface, or a Layer 3 interface to a Layer 2 interface, the software removes the Layer 2 NetFlow configuration from the interface.

- The same flow monitor cannot be shared with a VLAN and Layer 3 interfaces (for example, physical Layer 3 interface, SVI interface, or Layer 3 subinterface). You must distinguish a VLAN and Layer 3 interface since the ACL is different and cannot be shared. They must be treated as two different profiles.

- A rollback fails if you try to modify a record that is programmed in the hardware during a rollback.

- Beginning with Cisco NX-OS Release 9.2(1):
• NetFlow for FEX Layer 3 ports is supported on Cisco Nexus 9300-EX and 9300-FX platform switches.

• NetFlow CE is supported on the Cisco Nexus 9300-EX platform switches.

Note

All -EX type platform switches, including the N9K-X9700-FX line cards, CE NetFlow only captures CE flow records for non-IPv4 and IPv6 traffic flows. Whereas for -FX and -FX2 type platform switches and line cards, we can capture CE flow data for IP flows as long as **mac packet-classify** is applied on the interface.

• For Cisco Nexus 9300-EX platform switches, a flow monitor applied on a VLAN or SVI can collect flows for both switched and routed traffic. For Cisco Nexus 9300-FX platform switches, NetFlow VLANs are supported for switched traffic only, and NetFlow SVIs are supported for routed traffic only.

• The Cisco Nexus 9300-EX platform switch supports NetFlow and SPAN on the same interface at the same time. This functionality is a viable alternative to using SPAN and sFlow.

• On Cisco Nexus 9300-EX/FX platform switches, and Cisco Nexus 9500 platform switches with EX/FX modules, SPAN, and sFlow cannot both be enabled simultaneously. If one is active, the other cannot be enabled. However, on the Cisco Nexus 9300-EX/FX/FX2 and the Cisco Nexus 9500 platform switches with EX modules, both NetFlow and SPAN can both be enabled simultaneously, providing a viable alternative to using sFlow and SPAN.

Note

Cisco Nexus 9300-FX2 switches support sFlow and SPAN co-existence.

• For Cisco Nexus 9300-EX platform switches, the same flow monitor cannot be attached to a VLAN and an SVI at the same time.

• The Cisco Nexus 9300-EX platform switches have dedicated TCAM and do not require carving.

• The ToS field is not exported for Cisco Nexus 9300-EX platform switches.

• The Cisco Nexus 3232C and 3264Q switches do not support NetFlow.

• Enable NetFlow only on platforms that support this feature.

Note

For verified NetFlow scalability numbers, see the [Cisco Nexus 9000 Series NX-OS Verified Scalability Guide](#).

**Configuring NetFlow**

Follow these steps to configure NetFlow:

---

For verified NetFlow scalability numbers, see the [Cisco Nexus 9000 Series NX-OS Verified Scalability Guide](#).
Enabling the NetFlow Feature

You must globally enable NetFlow before you can configure any flows.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code>&lt;br&gt;Example: <code>switch# configure terminal&lt;br&gt;switch(config)#</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>[no] feature netflow</code>&lt;br&gt;Example: <code>switch(config)# feature netflow</code></td>
<td>Enables or disables the NetFlow feature. The default is disabled.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>(Optional) copy running-config startup-config</code>&lt;br&gt;Example: <code>switch(config)# copy running-config startup-config</code></td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

Creating a Flow Record

You can create a flow record and add keys to match on and nonkey fields to collect in the flow.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code>&lt;br&gt;Example: <code>switch# configure terminal&lt;br&gt;switch(config)#</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>flow record name</code>&lt;br&gt;Example: <code>switch(config)# flow record name</code></td>
<td>Creates a flow record and enters flow record configuration mode. You can enter up to 63</td>
</tr>
</tbody>
</table>
### Specifying the Match Parameters

You must configure at least one of the following match parameters for flow records:

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `switch(config)# flow record Test`  
`switch(config-flow-record)#`                                                      | alphanumeric characters for the flow record name. |
| **Step 3** *(Optional) description string*                                          | Describes this flow record as a maximum 63-character string. |
| **Example:** *switch(config-flow-record)# description IPv4Flow*                    |                                                   |
| **Step 4** *(Optional) match type*                                                 | Specifies a match key. For more information, see *Specifying the Match Parameters*, on page 285. |
| **Note** *The match transport destination-port and match ip protocol commands are required to export Layer 4 port data.* |                                                   |
| **Example:** *switch(config-flow-record)# match transport destination-port*        |                                                   |
| **Step 5** *(Optional) collect type*                                               | Specifies the collection field. For more information, see *Specifying the Collect Parameters*, on page 286. |
| **Example:** *switch(config-flow-record)# collect counter packets*                 |                                                   |
| **Step 6** *(Optional) show flow record [name] [record-name] [netflow-original | Displays information about NetFlow flow records. You can enter up to 63 alphanumeric characters for the flow record name. |
| [netflow-protocol-port] [netflow ipv4 | ipv6] [original-input | original-output] }                      |                                                   |
| **Example:** *switch(config-flow-record)# show flow record netflow protocol-port* |                                                   |
| **Step 7** *(Optional) copy running-config startup-config*                         | Copies the running configuration to the startup configuration. |
| **Example:** *switch(config-flow-record)# copy running-config startup-config*       |                                                   |

---

### Specifying the Collect Parameters

You must configure at least one of the following collect parameters for flow records:

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>switch(config)# collect counter packets</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> <em>(Optional) collect type</em></td>
<td>Specifies the collection field. For more information, see <em>Specifying the Collect Parameters</em>, on page 286.</td>
</tr>
<tr>
<td><strong>Example:</strong> <em>switch(config-flow-record)# collect counter packets</em></td>
<td></td>
</tr>
</tbody>
</table>

---

### Specifying the Protocol Parameters

You must configure at least one of the following protocol parameters for flow records:

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>switch(config)# protocol transport transport-protocol-port</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> <em>(Optional) match type</em></td>
<td>Specifies a match key. For more information, see <em>Specifying the Match Parameters</em>, on page 285.</td>
</tr>
<tr>
<td><strong>Note</strong> <em>The match transport destination-port and match ip protocol commands are required to export Layer 4 port data.</em></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> <em>switch(config-flow-record)# match transport destination-port</em></td>
<td></td>
</tr>
</tbody>
</table>

---

### Specifying the Transport Parameters

You must configure at least one of the following transport parameters for flow records:

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>switch(config)# transport transport-protocol-port</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> <em>(Optional) match type</em></td>
<td>Specifies a match key. For more information, see <em>Specifying the Match Parameters</em>, on page 285.</td>
</tr>
<tr>
<td><strong>Note</strong> <em>The match transport destination-port and match ip protocol commands are required to export Layer 4 port data.</em></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> <em>switch(config-flow-record)# match transport destination-port</em></td>
<td></td>
</tr>
</tbody>
</table>

---

### Specifying the Source Parameters

You must configure at least one of the following source parameters for flow records:

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>switch(config)# source source-address</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <em>(Optional) description string</em></td>
<td>Describes this flow record as a maximum 63-character string.</td>
</tr>
<tr>
<td><strong>Example:</strong> <em>switch(config-flow-record)# description IPv4Flow</em></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> <em>(Optional) match type</em></td>
<td>Specifies a match key. For more information, see <em>Specifying the Match Parameters</em>, on page 285.</td>
</tr>
<tr>
<td><strong>Note</strong> <em>The match transport destination-port and match ip protocol commands are required to export Layer 4 port data.</em></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> <em>switch(config-flow-record)# match transport destination-port</em></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> <em>(Optional) collect type</em></td>
<td>Specifies the collection field. For more information, see <em>Specifying the Collect Parameters</em>, on page 286.</td>
</tr>
<tr>
<td><strong>Example:</strong> <em>switch(config-flow-record)# collect counter packets</em></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> *(Optional) show flow record [name] [record-name] [netflow-original</td>
<td>Displays information about NetFlow flow records. You can enter up to 63 alphanumeric characters for the flow record name.</td>
</tr>
<tr>
<td>[netflow-protocol-port] [netflow ipv4</td>
<td>ipv6] [original-input</td>
</tr>
<tr>
<td><strong>Example:</strong> <em>switch(config-flow-record)# show flow record netflow protocol-port</em></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> <em>(Optional) copy running-config startup-config</em></td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong> <em>switch(config-flow-record)# copy running-config startup-config</em></td>
<td></td>
</tr>
</tbody>
</table>
### Specifying the Collect Parameters

You must configure at least one of the following collect parameters for flow records:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>collect counter {bytes</td>
<td>packets} [long]</td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>collect ip version</strong></td>
<td>Collects the IP version for the flow.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>switch(config-flow-record)# collect ip version</code></td>
<td></td>
</tr>
<tr>
<td><strong>collect timestamp sys-uptime</strong></td>
<td>Collects the system up time for the first or last packet in the flow.</td>
</tr>
<tr>
<td>`{first</td>
<td>last}`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>switch(config-flow-record)# collect timestamp sys-uptime last</code></td>
<td></td>
</tr>
<tr>
<td><strong>collect transport tcp flags</strong></td>
<td>Collects the TCP transport layer flags for the packets in the flow.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>switch(config-flow-record)# collect transport tcp flags</code></td>
<td></td>
</tr>
</tbody>
</table>

### Creating a Flow Exporter

The flow exporter configuration defines the export parameters for a flow and specifies reachability information for the remote NetFlow Collector.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>configure terminal</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)#</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>flow exporter name</strong></td>
<td>Creates a flow exporter and enters flow exporter configuration mode. You can enter up to 63 alphanumeric characters for the flow exporter name.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)# flow exporter flow-exporter-one</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config-flow-exporter)#</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>destination</strong></td>
<td>Sets the destination IPv4 or IPv6 address for this flow exporter. You can optionally configure the VRF to use to reach the NetFlow Collector. You can enter up to 32 alphanumeric characters for the VRF name.</td>
</tr>
<tr>
<td></td>
<td>`{ipv4-address</td>
<td>ipv6-address} [use-vrf name]`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config-flow-exporter)# destination 192.0.2.1</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>source</strong></td>
<td>Specifies the interface to use to reach the NetFlow Collector at the configured destination.</td>
</tr>
<tr>
<td></td>
<td><strong>interface-type name/port</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config-flow-exporter)# source ethernet 2/1</code></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Describes this flow exporter. You can enter up to 63 alphanumeric characters for the description.</td>
<td></td>
</tr>
<tr>
<td>(Optional) <strong>description string</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>switch(config-flow-exporter)# description exportversion9</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| **Step 6** | Specifies the differentiated services codepoint value. The range is from 0 to 63. |
| (Optional) **dscp value** | |
| **Example:** | |
| switch(config-flow-exporter)# dscp 0 | |

| **Step 7** | Specifies the UDP port to use to reach the NetFlow Collector. The range is from 0 to 65535. |
| (Optional) **transport udp port** | |
| **Example:** | |
| switch(config-flow-exporter)# transport udp 200 | |

| Note | If you do not specify the UDP port, 9995 is selected as the default. |

| **Step 8** | Specifies the NetFlow export version. Choose version 9 to enter the flow exporter version 9 configuration submode. |
| **version 9** | |
| **Example:** | |
| switch(config-flow-exporter)# version 9 | |
| switch(config-flow-exporter-version-9)# | |

| **Step 9** | Sets the flow exporter statistics resend timer. The range is from 1 to 86400 seconds. |
| (Optional) **option {exporter-stats | interface-table} timeout seconds** | |
| **Example:** | |
| switch(config-flow-exporter-version-9)# option exporter-stats timeout 1200 | |

| **Step 10** | Sets the template data resend timer. The range is from 1 to 86400 seconds. |
| (Optional) **template data timeout seconds** | |
| **Example:** | |
| switch(config-flow-exporter-version-9)# template data timeout 1200 | |

| **Step 11** | Copies the running configuration to the startup configuration. |
| (Optional) **copy running-config startup-config** | |
| **Example:** | |
| switch(config-flow-exporter-version-9)# copy running-config startup-config | |

### Creating a Flow Monitor

You can create a flow monitor and associate it with a flow record and a flow exporter. All of the flows that belong to a monitor use the associated flow record to match on the different fields, and the data is exported to the specified flow exporter.
Configuring NetFlow

Applying a Flow Monitor to an Interface

You can apply a flow monitor to an ingress interface. Egress Netflow is not supported.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

Step 1

Enters global configuration mode.

Example:

```
switch# configure terminal
switch(config)#
```

Step 2

Creates a flow monitor and enters flow monitor configuration mode. You can enter up to 63 alphanumeric characters for the flow monitor name.

**Example:**

```
Step 2
switch(config)# flow monitor name
```

Step 3

Describes this flow monitor. You can enter up to 63 alphanumeric characters for the description.

**Example:**

```
(Optional) description string
switch(config-flow-monitor)# description IPv4Monitor
```

Step 4

Associates a flow exporter with this flow monitor. You can enter up to 63 alphanumeric characters for the exporter name.

**Example:**

```
(Optional) exporter name
switch(config-flow-monitor)# export v9
```

Step 5

Associates a flow record with the specified flow monitor. You can enter up to 63 alphanumeric characters for the record name.

**Example:**

```
record name [netflow-original | netflow protocol-port | netflow ipv4 | ipv6] {original-input | original-output}
switch(config-flow-monitor)# record IPv4Flow
```

Step 6

Copies the running configuration to the startup configuration.

**Example:**

```
(Optional) copy running-config startup-config
switch(config-flow-monitor)# copy running-config startup-config
```

Applying a Flow Monitor to an Interface

You can apply a flow monitor to an ingress interface. Egress Netflow is not supported.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

Step 1

Enters global configuration mode.

Example:

```
switch# configure terminal
switch(config)#
```
## Configuring Bridged NetFlow on a VLAN

You can apply a flow monitor to a VLAN in order to gather Layer 3 data over Layer 2 switched packets in a VLAN.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch# configure terminal switch(config)#</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>vlan configuration vlan-id</td>
<td>Enters VLAN configuration mode. The VLAN ID range is from 1 to 3967 or from 4048 to 4093.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# vlan configuration 30 switch(config-vlan-config)#</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>{ip</td>
<td>ipv6} flow monitor name</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config-vlan-config)# {ip</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>(Optional) copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config-vlan-config)# copy running-config startup-config</td>
</tr>
</tbody>
</table>
### Configuring Layer 2 NetFlow Keys

You can define Layer 2 keys in flexible NetFlow records that you can use to capture flows in Layer 2 interfaces.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# configure terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>flow record name</td>
<td>Enters flow record configuration mode. For more information about configuring flow records, see Creating a Flow Record, on page 284.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# flow record L2_record</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config-flow-record)#</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>match datalink {mac source-address</td>
<td>Specifies the Layer 2 attribute as a key.</td>
</tr>
<tr>
<td></td>
<td>mac destination-address</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ethertype</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Purpose

You must use this command to capture flows.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>layer2-switched flow monitor flow-name</td>
<td>Associates a flow monitor to the switch port input packets. You can enter up to 63 alphanumeric characters for the flow monitor name.</td>
</tr>
</tbody>
</table>

Step 8

Example:
```
switch(config-if)# layer2-switched flow monitor L2_monitor
```

Step 9

(Optional) show flow record netflow layer2-switched input

Example:
```
switch(config-if)# show flow record netflow layer2-switched input
```

Step 10

(Optional) copy running-config startup-config

Example:
```
switch(config-if)# copy running-config startup-config
```

Configuring NetFlow Timeouts

You can optionally configure global NetFlow timeouts that apply to all flows in the system.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

Example:
```
switch# configure terminal
switch(config)#
```

Step 2

flow timeout seconds

Example:
```
switch(config)# flow timeout 30
```

Sets the flush timeout value in seconds. The range is from 5 to 60 seconds. The default value is 10 seconds.

Step 3

(Optional) copy running-config startup-config

Example:
```
switch(config)# copy running-config startup-config
```

Copies the running configuration to the startup configuration.

Verifying the NetFlow Configuration

To display the NetFlow configuration, perform one of the following tasks:
### Monitoring NetFlow

Use the `show flow exporter` command to display NetFlow statistics. Use the `clear flow exporter` command to clear NetFlow flow exporter statistics.

### Configuration Example for NetFlow

This example shows how to configure a NetFlow exporter configuration for IPv4:

```
feature netflow
flow exporter ee
  destination 171.70.242.48 use-vrf management
  source mgmt0
  version 9
  template data timeout 20
flow record rr
  match ipv4 source address
  match ipv4 destination address
  collect counter bytes
  collect counter packets
flow monitor foo
  record rr
exporter ee
interface Ethernet2/45
  ip flow monitor foo input
  ip address 10.20.1.1/24
no shutdown
```
Configuring sFlow

This chapter describes how to configure sFlow on Cisco NX-OS devices.

This chapter includes the following sections:

- About sFlow, on page 295
- Licensing Requirements for sFlow, on page 296
- Prerequisites for sFlow, on page 296
- Guidelines and Limitations for sFlow, on page 296
- Default Settings for sFlow, on page 297
- Configuring sFlow, on page 297
- Verifying the sFlow Configuration, on page 304
- Monitoring and Clearing sFlow Statistics, on page 304
- Configuration Examples for sFlow, on page 305
- Additional References, on page 305

About sFlow

Sampled flow (sFlow) allows you to monitor real-time traffic in data networks that contain switches and routers. It uses the sampling mechanism in the sFlow agent software on switches and routers to monitor traffic and to forward the sample data to the central data collector.

For more information about sFlow, see RFC 3176.

sFlow Agent

The sFlow agent, which is embedded in the Cisco NX-OS software, periodically samples or polls the interface counters that are associated with a data source of the sampled packets. The data source can be an Ethernet interface, an EtherChannel interface, or a range of Ethernet interfaces. The sFlow agent queries the Ethernet port manager for the respective EtherChannel membership information and also receives notifications from the Ethernet port manager for membership changes.

When you enable sFlow sampling, based on the sampling rate and the hardware internal random number, the ingress packets and egress packets are sent to the CPU as an sFlow-sampled packet. The sFlow agent processes the sampled packets and sends an sFlow datagram to the sFlow analyzer. In addition to the original sampled packet, an sFlow datagram includes information about the ingress port, the egress port, and the original packet length. An sFlow datagram can have multiple sFlow samples.
Licensing Requirements for sFlow

<table>
<thead>
<tr>
<th>Product</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco NX-OS</td>
<td>sFlow requires no license. Any feature not included in a license package is bundled with the nx-os image and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the Cisco NX-OS Licensing Guide.</td>
</tr>
</tbody>
</table>

Prerequisites for sFlow

sFlow has the following prerequisites:

- For Cisco Nexus 9332PQ, 9372PX, 9372TX, and 93120TX switches and for Cisco Nexus 9396PX, 9396TX, and 93128TX switches with the N9K-M6PQ or N9K-M12PQ generic expansion module (GEM), you must configure the sFlow and SPAN ACL TCAM region sizes for any uplink ports that are to be configured as an sFlow data source. To do so, use the hardware access-list tcam region sflow and hardware access-list tcam region span commands. See Configuring ACL TCAM Region Sizes for more information.

Note

By default, the sflow region size is zero, and the span region size is non-zero. You need to configure the sflow region to 256 and allocate enough entries to the span region in order to configure the port as an sFlow data source.

- Egress sFlow of multicast traffic requires hardware multicast global-tx-span configuration

Guidelines and Limitations for sFlow

sFlow has the following guidelines and limitations:

- If at least one sFlow data source is configured, the SPAN sessions cannot be brought up.
  - If at least one SPAN session is configured as no shut, sFlow data sources cannot be added.
  - The sampling mode that is used for sFlow is based on an algorithm that is known as LFSR. Due to the use of LFSR, it is not guaranteed that one in every few packets are sampled with the sampling rate of n. However, the number of packets that are sampled is equal to the total packets over a period of time.

- sFlow is a software driven feature, hardware only sends copies of traffic from the sFlow source interfaces to the CPU for further processing. Elevated CPU usage is expected. sFlow traffic sent to the CPU by hardware is rate-limited to protect the CPU.

- When you enable sFlow for an interface, it is enabled for both ingress and egress. You cannot enable sFlow for only ingress or only egress.
- sFlow is not supported on the SVIs.
- Subinterfaces are not supported for sFlow.
- We recommend you configure the sampling rate based on the sFlow configuration and traffic in the system.
- The switch supports only one sFlow collector.
- sFlow and Network Address Translation (NAT) are not supported on the same port.
- sFlow supports sampling IPv6 traffic but only on IPv4 collector ports.
- sFlow counters increment even for control packets that ingress on the sFlow data-source interfaces. These packets may be sampled and send out as sFlow datagrams (similar to data plane traffic).
- The following Cisco Nexus switches support sFlow and SPAN together:

**Default Settings for sFlow**

The following table lists the default settings for sFlow parameters.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>sFlow sampling rate</td>
<td>4096</td>
</tr>
<tr>
<td>sFlow sampling size</td>
<td>128</td>
</tr>
<tr>
<td>sFlow counter poll interval</td>
<td>20</td>
</tr>
<tr>
<td>sFlow maximum datagram size</td>
<td>1400</td>
</tr>
<tr>
<td>sFlow collector IP address</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>sFlow collector port</td>
<td>6343</td>
</tr>
<tr>
<td>sFlow agent IP address</td>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>

**Configuring sFlow**

**Enabling sFlow**

You must enable the sFlow feature before you can configure sFlow settings on the switch.
**Configuring the Sampling Rate**

You can configure the sampling rate for sFlow.

**Before you begin**

Make sure that you have enabled sFlow.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> [no] feature sflow</td>
<td>Enables or disables sFlow.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config)# feature sflow</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> (Optional) show feature</td>
<td>Displays the enabled and disabled features.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config)# show feature</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> (Optional) copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config)# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>
Configuring sFlow

Configuring the Maximum Sampled Size

You can configure the maximum number of bytes that should be copied from a sampled packet.

Before you begin

Make sure that you have enabled sFlow.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>[no] sflow max-sampled-size sampling-size</td>
<td>Configures the sFlow maximum sampling size. The range for the sampling-size is from 64 to 256 bytes.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# sflow max-sampled-size 200</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>(Optional) show sflow</td>
<td>Displays the sFlow configuration.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# show sflow</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>(Optional) copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

Configuring the Counter Poll Interval

You can configure the maximum number of seconds between successive samples of the counters that are associated with the data source. A sampling interval of 0 disables counter sampling.

Before you begin

Make sure that you have enabled sFlow.
Configuring sFlow

Configuring the Maximum Datagram Size

You can configure the maximum number of data bytes that can be sent in a single sample datagram.

Before you begin

Make sure that you have enabled sFlow.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>configure terminal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>[no] sflow max-datagram-size datagram-size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example</td>
<td>switch(config)# sflow max-datagram-size 2000</td>
</tr>
<tr>
<td>Purpose</td>
<td>Configures the sFlow maximum datagram size. The range for the datagram-size is from 200 to 9000 bytes.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>(Optional) show sflow</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example</td>
<td>switch(config)# show sflow</td>
</tr>
<tr>
<td>Purpose</td>
<td>Displays the sFlow configuration.</td>
</tr>
</tbody>
</table>
### Configuring the sFlow Collector Address

You can configure the IPv4 address of the sFlow data collector that is connected to the management port.

**Before you begin**

Make sure that you have enabled sFlow.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# configure terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)#</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>[no] sflow collector-ip ip-address vrf vrf [source ip-address]</td>
<td>Configures the IPv4 address for the sFlow collector. If the IP address is set to 0.0.0.0, all sampling is disabled.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# sflow collector-ip 192.0.2.5 vrf management</td>
<td></td>
</tr>
</tbody>
</table>

The `vrf` can be one of the following:

- A user-defined VRF name—You can specify a maximum of 32 alphanumeric characters.
- `vrf management`—You must use this option if the sFlow data collector is on the network connected to the management port.
- `vrf default`—You must use this option if the sFlow data collector is on the network connected to the front-panel ports.

The `source ip-address` option causes the sent sFlow datagram to use the source IP address as the IP packet source address. The source IP address has to be already configured on one of the switch local interfaces; otherwise, an error message appears. If the interface with the source IP address is changed or removed after this option is configured, the sFlow datagram will no longer be sent out, and an event history error
### Configuring the sFlow Collector Port

You can configure the destination port for sFlow datagrams.

**Before you begin**

Make sure that you have enabled sFlow.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>switch# configure terminal</code> <code>switch(config)#</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configures the UDP port of the sFlow collector.</td>
</tr>
<tr>
<td><code>[no] sflow collector-port collector-port</code></td>
<td>The range for the <code>collector-port</code> is from 1 to 65535.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>switch(config)# sflow collector-port 7000</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Displays the sFlow configuration.</td>
</tr>
<tr>
<td><code>(Optional) show sflow</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>switch(config)# show sflow</code></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td><code>(Optional) copy running-config startup-config</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>switch(config)# copy running-config startup-config</code></td>
</tr>
</tbody>
</table>
Configuring the sFlow Agent Address

You can configure the IPv4 address of the sFlow agent.

Before you begin
Make sure that you have enabled sFlow.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>[no] sflow agent-ip ip-address</td>
<td>Configures the IPv4 address of the sFlow agent.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# sflow agent-ip 192.0.2.3</td>
<td>The default IP address is 0.0.0.0, which means that all sampling is disabled on the switch. You must specify a valid IP address to enable sFlow functionality.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: This IP address is not necessarily the source IP address for sending the sFlow datagram to the collector.</td>
</tr>
<tr>
<td>Step 3</td>
<td>(Optional) show sflow</td>
<td>Displays the sFlow configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# show sflow</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>(Optional) copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

Configuring the sFlow Sampling Data Source

You can configure the source of the data for the sFlow sampler as an Ethernet port, a range of Ethernet ports, or a port channel.

Before you begin
Make sure that you have enabled sFlow.

If you want to use a port channel as the data source, make sure that you have already configured the port channel and you know the port channel number.

Make sure that the sFlow and SPAN ACL TCAM region sizes are configured for any uplink ports that are to be configured as an sFlow data source on the following devices: Cisco Nexus 9332PQ, 9372PX, 9372TX,
and 93120TX switches and Cisco Nexus 9396PX, 9396TX, and 93128TX switches with the N9K-M6PQ or N9K-M12PQ generic expansion module (GEM).

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)#</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>[no] sflow data-source interface [ethernet slot[/port[-port]]</td>
<td>Configures the sFlow sampling data source.</td>
</tr>
<tr>
<td></td>
<td>port-channel channel-number</td>
<td>For an Ethernet data source, slot is the slot number, and port can be either a single port number or a range of ports designated as port-port.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# sflow data-source interface ethernet 1/5-12</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(Optional) show sflow</td>
<td>Displays the sFlow configuration.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# show sflow</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(Optional) copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

**Verifying the sFlow Configuration**

Use these commands to display the sFlow configuration.

**Table 23: sFlow Show Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show sflow</td>
<td>Displays all the data sources of the sFlow samplers and the sFlow agent configuration.</td>
</tr>
<tr>
<td>show process</td>
<td>Verifies whether the sFlow process is running.</td>
</tr>
<tr>
<td>show running-config sflow [all]</td>
<td>Displays the current sFlow running configuration.</td>
</tr>
</tbody>
</table>

**Monitoring and Clearing sFlow Statistics**

Use the `show sflow statistics` command to display the sFlow statistics.

Use the following commands to clear the sFlow statistics:
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear sflow statistics</td>
<td>Clears most of the sFlow statistics from the <code>show sflow statistics</code> command.</td>
</tr>
<tr>
<td>clear counters interface all</td>
<td>Clears the Total Packets field from the <code>show sflow statistics</code> command.</td>
</tr>
<tr>
<td>clear hardware rate-limiter sflow</td>
<td>Clears the Total Samples field from the <code>show sflow statistics</code> command.</td>
</tr>
</tbody>
</table>

**Configuration Examples for sFlow**

This example shows how to configure sFlow:

```plaintext
feature sflow
sflow sampling-rate 5000
sflow max-sampled-size 200
sflow counter-poll-interval 100
sflow max-datagram-size 2000
sflow collector-ip 192.0.2.5 vrf management
sflow collector-port 7000
sflow agent-ip 192.0.2.3
sflow data-source interface ethernet 1/5
```

**Additional References**

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL TCAM regions</td>
<td>Configuring IP ACLs</td>
</tr>
</tbody>
</table>
Configuring TAP Aggregation and MPLS Stripping

This chapter describes how to configure TAP aggregation and MPLS stripping on Cisco NX-OS devices.

This chapter contains the following sections:

• About TAP Aggregation, on page 307
• About MPLS Stripping, on page 310
• Configuring TAP Aggregation, on page 311
• Verifying the TAP Aggregation Configuration, on page 315
• Configuration Example for TAP Aggregation, on page 315
• Configuring MPLS Stripping, on page 316
• Verifying the MPLS Stripping Configuration, on page 319
• Clearing MPLS Stripping Counters and Label Entries, on page 321
• Configuration Examples for MPLS Stripping, on page 321
• Additional References, on page 322

About TAP Aggregation

Network TAPs

You can use various methods to monitor packets. One method uses physical hardware test access points (TAPs).

Network TAPs can be extremely useful in monitoring traffic because they provide direct inline access to data that flows through the network. In many cases, a third party monitors the traffic between two points in the network. If the network between points A and B consists of a physical cable, a network TAP might be the best way to accomplish this monitoring. The network TAP has at least three ports: an A port, a B port, and a monitor port. A TAP inserted between the A and B ports passes all traffic through unimpeded, but it also copies that same data to its monitor port, which could enable a third party to listen.

TAPs have the following benefits:

• They can handle full-duplex data transmission.

• They are unobtrusive and not detectable by the network (with no physical or logical addressing).

• Some TAPs support full inline power with the capability to build a distributed TAP.
If you are trying to gain visibility into the server-to-server data communication at the edge or virtual edge of your network or to provide a copy of traffic to the Intrusion Prevention System (IPS) appliance at the Internet edge of your network, you can use network TAPs nearly anywhere in the environment. However, this deployment can add significant costs, operation complexities, and cabling challenges in a large-scale environment.

**TAP Aggregation**

TAP aggregation is an alternative solution to help with monitoring and troubleshooting tasks in the data center. It works by designating a device to allow the aggregation of multiple test access points (TAPs) and to connect to multiple monitoring systems. TAP aggregation switches link all of the monitoring devices to specific points in the network fabric that handle the packets that need to be observed.

In the TAP aggregation switch solution, a Cisco Nexus 9000 Series switch is connected to various points in the network at which packet monitoring is advantageous. From each network element, you can use switched port analyzer (SPAN) ports or optical TAPs to send traffic flows directly to this TAP aggregation switch. The TAP aggregation switch is directly connected to all of the analysis tools used to monitor the events in the network fabric. These monitoring devices include remote monitor (RMON) probes, application firewalls, IPS devices, and packet sniffer tools.

You can configure the TAP aggregation switch to filter specific traffic and redirect it to one or more tools. In order to redirect the traffic to multiple interfaces, a multicast group is created internally on the switch, and the interfaces that are part of the redirect list are added as member ports. When an access control list (ACL) policy with the redirect action is applied to an interface, the traffic matching the ACL rule is redirected to the internal multicast group that is created.

**Licensing Requirements for TAP Aggregation**

The following table shows the licensing requirements for this feature:

<table>
<thead>
<tr>
<th>Product</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco NX-OS</td>
<td>TAP aggregation requires no license. Any feature not included in a license package is bundled with the nx-os image and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the <em>Cisco NX-OS Licensing Guide</em>.</td>
</tr>
</tbody>
</table>

**Guidelines and Limitations for TAP Aggregation**

TAP aggregation has the following guidelines and limitations:

- **TAP aggregation:**
  - Supported on all Cisco Nexus 9000 Series switches and the 3164Q, 31128PQ, 3232C, and 3264Q switches.
  - Supported on 100G ports.
  - Supports only on switch ports and only in the ingress direction.
- Supports IPv4 ACLs with UDF-based match for Cisco Nexus 9200, 9300, and 9300-EX Series switches.

- Beginning with Cisco NX-OS Release 9.2(1), TAP aggregation filters on MPLS tags are supported on the following Cisco Nexus platform switches:
  - Cisco Nexus 9000 platform switches, including the N9K-X9700-EX and N9K-X9700-FX line cards.
  - Cisco Nexus 9200 platform switches.
  - Cisco Nexus 9300 platform switches.
  - Cisco Nexus 9500 switches.

- TAP aggregation filters on MPLS tags are not supported on the following Cisco Nexus Series switches, line cards, and fabric modules:

<table>
<thead>
<tr>
<th>Table 24: Cisco Nexus 9000 Series Switches</th>
</tr>
</thead>
<tbody>
<tr>
<td>N3K-C3164Q-40GE</td>
</tr>
<tr>
<td>N9K-C9372TX</td>
</tr>
<tr>
<td>N3K-C3232C</td>
</tr>
<tr>
<td>N3K-C3264Q-S</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 25: Cisco Nexus 9000 Series Line Cards and Fabric Modules</th>
</tr>
</thead>
<tbody>
<tr>
<td>N9K-X9564PX</td>
</tr>
<tr>
<td>N9K-M12PQ</td>
</tr>
<tr>
<td>N9K-C9396TX</td>
</tr>
<tr>
<td>N9K-X9432PQ</td>
</tr>
<tr>
<td>N9K-X9464TX2</td>
</tr>
<tr>
<td>N9K-M6PQ</td>
</tr>
</tbody>
</table>

- Cisco Nexus N9K-X9700-EX and N9K-X9700-FX line cards support TAP aggregation with IPv4, IPv6, and MAC ACLs.

- Only Layer 2 interfaces support the TAP aggregation policy. You can apply the policy to a Layer 3 interface, but the policy becomes nonfunctional.

- The redirect port must be part of the same VLAN as the source (TAP) port.

- Each rule must be associated with only one unique match criterion.

- When you enter a list of interfaces for the TAP aggregation policy, you must separate them with commas but no spaces. For example, port-channel50, ethernet1/12, port-channel20.
About MPLS Stripping

The ingress ports of Cisco Nexus 9000 Series switches receive various Multiprotocol Label Switching (MPLS) packet types. Each data packet in an MPLS network has one or more label headers. These packets are redirected on the basis of a redirect access control list (ACL).

A label is a short, four-byte, fixed-length, locally significant identifier that is used to identify a Forwarding Equivalence Class (FEC). The label that is put on a particular packet represents the FEC to which that packet is assigned. It has the following components:

- **Label**—Label value (unstructured), 20 bits
- **Exp**—Experimental use, 3 bits; currently used as a class of service (CoS) field
- **S**—Bottom of stack, 1 bit
- **TTL**—Time to live, 8 bits

Some MPLS labels are imposed between the Layer 2 header and the Layer 3 header. For these labels, the headers and data are not located at the standard byte offset. Standard network monitoring tools cannot monitor and analyze this traffic. To enable standard network monitoring tools to monitor this traffic, single-labeled packets are stripped off their MPLS label headers and redirected to T-cache devices.

MPLS packets with multiple label headers are sent to deep packet inspection (DPI) devices without stripping their MPLS headers.

Beginning Cisco NX-OS Release 7.0(3)I7(3), for Cisco Nexus 9300-EX switches, a VLAN tag can be applied to packets going out of redirect ports. You can pop 1-5 labels with the MPLS strip.

Licensing Requirements for MPLS Stripping

The following table shows the licensing requirements for this feature:

<table>
<thead>
<tr>
<th>Product</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco NX-OS</td>
<td>MPLS stripping requires no license. Any feature not included in a license package is bundled with the nx-os image and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the Cisco NX-OS Licensing Guide.</td>
</tr>
</tbody>
</table>

Guidelines and Limitations for MPLS Stripping

MPLS stripping has the following guidelines and limitations:

- Cisco Nexus N9K-X9700-EX and N9K-X9700-FX line cards do not support MPLS stripping.
• Disable all Layer 3 and vPC features before you enable MPLS stripping.

• Static MPLS, MPLS segment routing, and MPLS stripping cannot be enabled at the same time.

• Only the ingress interfaces involved in MPLS stripping must have TAP aggregation enabled.

• You must configure the TAP aggregation ACL with a redirect action on the ingress interface to forward the packet to the desired destination.

• Only one TAP ACL is supported on the system.

• The egress interface where stripped packets will exit must be an interface that has VLAN 1 as an allowed VLAN. We recommend that you configure the egress interface as a trunk with all VLANs allowed by default.

• Port-channel load balancing is supported for MPLS stripped packets.

• Layer 3 header-based hashing and Layer 4 header-based hashing are supported, but Layer 2 header-based hashing is not supported.

• During MPLS stripping, the incoming VLAN is not preserved.

• Cisco Nexus 9200, 9300-EX, and 9300-FX platform switches support tagging of VLANs to packets going out of redirect ports. The ingress/egress ports can either be ethernet or port channel. The VLAN tag is derived from the incoming port configuration. The new ACL on the ingress interface should not be associated with a VLAN value different from the interface VLAN value.

• For every ACE (under an ACL associated with a particular VLAN) with a unique redirect port list, we allocate a hardware entry. The current hardware limit for the number of ACEs is 50 and you cannot configure more than 50 such ACEs.

## Configuring TAP Aggregation

### Enabling TAP Aggregation for Line Cards

Beginning with Cisco NX-OS Release 7.0(3)I7(2), you can enable TAP aggregation for Cisco Nexus 9500 platform switches with N9K-X9700-EX and N9K-X9700-FX line cards.

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# hardware acl tap-agg</td>
<td></td>
</tr>
</tbody>
</table>
Configuring a TAP Aggregation Policy

You can configure a TAP aggregation policy on an IP access control list (ACL) or on a MAC ACL.

Before you begin

You must configure the ACL TCAM region size for IPv4 port ACLs or MAC port ACLs using the `hardware access-list team region {ifacl | mac-ifacl}` command. Configure the ACL TCAM region size for IPv6 port ACLs using the command, `hardware access-list team region ipv6-ifacl`.

For information, see the "Configuring ACL TCAM Region Sizes" in the Cisco Nexus 9000 Series NX-OS Security Configuration Guide.

Note

By default the region size for both ifacl and mac-ifacl is zero. You need to allocate enough entries to the ifacl or mac-ifacl region to support TAP aggregation.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter one of the following commands:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <code>ip access-list access-list-name</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <code>mac access-list access-list-name</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| switch(config)# ip access-list test | Beginning with Cisco NX-OS Release 7.0(3)15(1), support for IPv6 ACLs is added for Cisco Nexus 9000 Series switches. The redirect action is supported in IPv6 ACLs. All the match options that are currently supported for IPv6 PACLs are now supported with the redirect action. 

Create an IPACL and enters IP access list configuration mode or creates a MAC ACL and enters MAC access list configuration mode. | |
<p>| switch(config-acl)# | | |
| switch(config)# mac access-list mactap1 | | |
| switch(config-mac-acl)# | | |
| switch(config)# ipv6 access-list testv6 | | |
| switch# sh running-config aclmgr | | |
| !Command: show running-config aclmgr | | |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `version 7.0(3)I5(1)`<br>`ipv6 access-list testv6`
|**Enters global configuration mode.**<br>Configures the system to use version 7.0 for `I5` protocols and access-list for `testv6`.
| | |
| `10 permit ipv6 any any redirect Ethernet2/1`<br>`interface Ethernet6/6`
| | |
| `ipv6 port traffic-filter testv6 in`<br>Starts recording statistics for how many packets are permitted or denied by each entry. |

### Step 3
(Optional) `statistics per-entry`<br>Example:  
switch(config-acl)# statistics per-entry

### Step 4
[no] `permit protocol source destination redirect interfaces`<br>Example:  
switch(config-acl)# permit ip any any redirect ethernet1/8

**Note** When you enter an interface for the TAP aggregation policy, do not abbreviate it. When you enter a list of interfaces, separate them with commas but no spaces.

### Step 5
(Optional) Enter one of the following commands:<br>• `show ip access-lists [access-list-name]`
• `show mac access-lists [access-list-name]`<br>Example:  
switch(config-acl)# show ip access-lists test
switch(config-mac-acl)# show mac access-lists mactap1

### Step 6
(Optional) `copy running-config startup-config`<br>Example:  
switch(config-acl)# copy running-config startup-config

Copies the running configuration to the startup configuration.

---

## Attaching a TAP Aggregation Policy to an Interface

You can apply an ACL configured with TAP aggregation to a Layer 2 interface.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure terminal</code>&lt;br&gt;<strong>Enters global configuration mode.</strong>&lt;br&gt;A command required to configure the system.</td>
<td></td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> interface type slot/port</td>
<td>Enters interface configuration mode for the specified interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config)# interface ethernet 2/2</td>
<td></td>
</tr>
<tr>
<td>switch(config-if)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> switchport</td>
<td>Changes a Layer 3 interface to a Layer 2 interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config-if)# switchport</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> Make sure that the interface is a Layer 2 interface.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> Enter one of the following commands:</td>
<td>Applies an IPv4 or MAC ACL configured with TAP aggregation to the interface. The no form of this command removes the ACL from the interface.</td>
</tr>
<tr>
<td>• [no] ip port access-group access-list-name in</td>
<td></td>
</tr>
<tr>
<td>• [no] mac port access-group access-list-name in</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config-if)# ip port access-group test in</td>
<td></td>
</tr>
<tr>
<td>switch(config-if)# mac port access-group test in</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> (Optional) mode tap-aggregation</td>
<td>Allows the attachment of an ACL with the tap aggregation policy to the interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config-if)# mode tap-aggregation</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> This command is introduced in Cisco NX-OS Release 7.0(3)I2(1) for use with MPLS stripping. This command is required for MPLS stripping to work on ingress Layer 2 interfaces and port channels. For Layer 2 port channels, this command is required only on the parent interface and not on the channel group member interface.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> (Optional) copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config-if)# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>
Verifying the TAP Aggregation Configuration

To display the TAP aggregation configuration information, perform one of the following tasks.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip access-lists [access-list-name]</code></td>
<td>Displays all IPv4 ACLs or a specific IPv4 ACL.</td>
</tr>
<tr>
<td><code>show mac access-lists [access-list-name]</code></td>
<td>Displays all MAC ACLs or a specific MAC ACL.</td>
</tr>
</tbody>
</table>

Configuration Example for TAP Aggregation

This example shows how to configure a TAP aggregation policy on an IPv4 ACL:

```
switch# configure terminal
switch(config)# ip access-list test
switch(config-acl)# 10 deny ip 100.1.1/24 any
switch(config-acl)# 20 permit tcp any eq www any redirect port-channel4
switch(config-acl)# 30 permit ip any any redirect Ethernet1/1, Ethernet1/2, port-channel7, port-channel8, Ethernet1/12, Ethernet1/13
switch(config-acl)# show ip access-lists test
IP access list test
   10 deny ip 100.1.1/24 any
   20 permit tcp any eq www any redirect port-channel4
   30 permit ip any any redirect Ethernet1/1, Ethernet1/2, port-channel7, port-channel8, Ethernet1/12, Ethernet1/13
```

This example shows how to apply a TAP aggregation policy to an IPv4 ACL with UDF–based match.

```
switch# configure terminal
switch(config)# ip access-list tap_agg
switch(config-acl)# 10 permit ip any any redirect Ethernet1/4
switch(config-acl)# 20 deny ip any any
switch# configure terminal
switch(config)# interface Ethernet1/4
switch(config-if)# ip port access-group tap_agg in
switch(config-if)# switchport
switch(config-if)# no shutdown
```

This example shows how to configure a TAP aggregation policy on a MAC ACL:

```
switch# configure terminal
switch(config)# mac access-list mactap1
switch(config-mac-acl)# 10 permit any any 0x86dd redirect port-channel1
switch(config-mac-acl)# show mac access-lists mactap1
MAC access list mactap1
   10 permit any any 0x86dd redirect port-channel1
```

This example shows how to attach a TAP aggregation policy to a Layer 2 interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# ip port access-group test in
```
Configuring MPLS Stripping

Enabling MPLS Stripping

You can enable MPLS stripping globally.

Before you begin

Disable all Layer 3 and vPC features before you enable MPLS stripping.

Attach an ACL with the tap aggregation policy to the Layer 2 interface or port channel using the `mode tap-aggregation` command. For more information, see Attaching a TAP Aggregation Policy to an Interface, on page 313.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)#</code></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><code>[no] mpls strip</code></td>
<td>Globally enables MPLS stripping. The <code>no</code> form of this command disables MPLS stripping.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)# mpls strip</code></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><code>[no] mpls strip mode dot1q</code></td>
<td>Enables VLAN tagging on the packets coming from the redirect port. The VLAN that needs to be tagged must be specified in the ingress port.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)# mpls strip mode dot1q</code></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Required: <code>copy running-config startup-config</code></td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)# copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>

Configuring the Incoming Port for the VLAN Tag

The VLAN tag is derived from the incoming port configuration. The ingress/egress ports can either be ethernet or port channel.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
</tbody>
</table>
| switch# configure terminal  
switch(config)# | Enters interface configuration mode for the specified interface. |

**Step 2**

**Interface Type**  
`interface type slot/port`  
**Example:**  
`switch(config)# interface ethernet 1/26`  
**Note** Make sure the interface is a Layer 2 interface.

**Step 3**

**Switchport**  
`switchport`  
**Example:**  
`switch(config-if)# switchport`  
**Note** Make sure the interface is a Layer 2 interface.

**Step 4**

Enter one of the following commands:  
- `[no] ip port access-group access-list-name in`  
- `[no] mac port access-group access-list-name in`  
**Example:**  
`switch(config-if)# ip port access-group test in`  
`switch(config-if)# mac port access-group test in`

Applies an IPv4 or MAC ACL configured with TAP aggregation to the interface. The `no` form of this command removes the ACL from the interface.

**Step 5**

Enter one of the following commands:  
- `[no] ip port access-group access-list-name in`  
- `[no] mac port access-group access-list-name in`  
**Example:**  
`switch(config-if)# ip port access-group test in`  
`switch(config-if)# mac port access-group test in`

Applies an IPv4 or MAC ACL configured with TAP aggregation to the interface. The `no` form of this command removes the ACL from the interface.

**Step 6**

**Required:** `mode tap-aggregation vlan vlan_id`  
**Example:**  
`switch(config-if)# mode tap-aggregation vlan 26`

Configures the value of the VLAN that will be tagged to the packets coming from the redirect ports.

**Step 7**

**Optional:** `copy running-config startup-config`  
**Example:**  
`switch(config-if)# copy running-config startup-config`

Copies the running configuration to the startup configuration.
Adding and Deleting MPLS Labels

The device can learn the labels dynamically whenever a frame is received with an unknown label on a TAP interface. You can also add or delete static MPLS labels.

Before you begin

Configure a TAP aggregation policy and attach the policy to an interface. For more information, see the *Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*.

You must configure the TAP aggregation ACL with a redirect action on the ingress interface to forward the packet to the desired destination.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

**Example:**

```
switch# configure terminal
switch(config)#
```

| Step 2 | `mpls strip label label`                   | Adds the specified static MPLS label. The 20-bit value of the label can range from 1 to 1048575. The `[no] mpls strip label {label | all}` command deletes the specified static MPLS label. The `all` option deletes all static MPLS labels. |
|--------|--------------------------------------------|-------------------------------------------------------------------------|

**Example:**

```
switch(config)# mpls strip label 100
```

<table>
<thead>
<tr>
<th>Step 3</th>
<th><em>(Optional)</em> <code>copy running-config startup-config</code></th>
<th>Copies the running configuration to the startup configuration.</th>
</tr>
</thead>
</table>

**Example:**

```
switch(config)# copy running-config startup-config
```

Configuring Destination MAC Addresses

You can configure the destination MAC address for stripped egress frames.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th><code>configure terminal</code></th>
<th>Enters global configuration mode.</th>
</tr>
</thead>
</table>

**Example:**

```
switch# configure terminal
switch(config)#
```

<table>
<thead>
<tr>
<th>Step 2</th>
<th><code>mpls strip dest-mac mac-address</code></th>
<th>Specifies the destination MAC address for egress frames that are stripped of their headers.</th>
</tr>
</thead>
</table>

**Example:**

```
```
Purpose

Command or Action

The MAC address can be specified in one of the following four formats:
- E.E.E
- EE-EE-EE-EE-EE-EE
- EE:EE:EE:EE:EE:EE
- EEEE.EEEE.EEEE

Step 3
(Optional) copy running-config startup-config

Example:
switch(config)# copy running-config startup-config

Copies the running configuration to the startup configuration.

Configuring MPLS Label Aging

You can define the amount of time after which dynamic MPLS labels will age out, if unused.

Procedure

Command or Action | Purpose
--- | ---
Step 1 | Enters global configuration mode.
configure terminal
Example:
switch# configure terminal
switch(config)#

Step 2 | Specifies the amount of time in seconds after which dynamic MPLS labels age out. The range is from 61 to 31622400.
mpsl strip label-age age
Example:
switch(config)# mpls strip label-age 300

Step 3 | Copies the running configuration to the startup configuration.
(Optional) copy running-config startup-config
Example:
switch(config)# copy running-config startup-config

Verifying the MPLS Stripping Configuration

To display the MPLS stripping configuration, perform one of the following tasks:
### Command

**show mpls strip labels [label | all | dynamic | static]**

**Purpose**
Displays information about MPLS labels. You can specify the following options:

- **label**—Label to be displayed.
- **all**—Specifies that all labels must be displayed. This is the default option.
- **dynamic**—Specifies that only dynamic labels must be displayed.
- **static**—Specifies that only static labels must be displayed.

---

This example shows how to display all MPLS labels:

```
switch# show mpls strip labels
MPLS Strip Labels:
   Total : 3005
   Static : 5
Legend:  * - Static Label
   Interface - where label was first learned
   Idle-Age - Seconds since last use
   SW-Counter- Packets received in Software
   HW-Counter- Packets switched in Hardware
```

<table>
<thead>
<tr>
<th>Label</th>
<th>Interface</th>
<th>Idle-Age</th>
<th>SW-Counter</th>
<th>HW-Counter</th>
</tr>
</thead>
<tbody>
<tr>
<td>4096</td>
<td>Eth1/53/1</td>
<td>15</td>
<td>1</td>
<td>210</td>
</tr>
<tr>
<td>4097</td>
<td>Eth1/53/1</td>
<td>15</td>
<td>1</td>
<td>210</td>
</tr>
<tr>
<td>4098</td>
<td>Eth1/53/1</td>
<td>15</td>
<td>1</td>
<td>210</td>
</tr>
<tr>
<td>4099</td>
<td>Eth1/53/1</td>
<td>7</td>
<td>2</td>
<td>219</td>
</tr>
<tr>
<td>4100</td>
<td>Eth1/53/1</td>
<td>7</td>
<td>2</td>
<td>219</td>
</tr>
<tr>
<td>4101</td>
<td>Eth1/53/1</td>
<td>7</td>
<td>2</td>
<td>219</td>
</tr>
<tr>
<td>4102</td>
<td>Eth1/53/1</td>
<td>39</td>
<td>1</td>
<td>206</td>
</tr>
<tr>
<td>4103</td>
<td>Eth1/53/1</td>
<td>39</td>
<td>1</td>
<td>206</td>
</tr>
<tr>
<td>4104</td>
<td>Eth1/53/1</td>
<td>39</td>
<td>1</td>
<td>206</td>
</tr>
<tr>
<td>4105</td>
<td>Eth1/53/1</td>
<td>1</td>
<td>1</td>
<td>217</td>
</tr>
<tr>
<td>4106</td>
<td>Eth1/53/1</td>
<td>1</td>
<td>1</td>
<td>217</td>
</tr>
<tr>
<td>4107</td>
<td>Eth1/53/1</td>
<td>1</td>
<td>1</td>
<td>217</td>
</tr>
<tr>
<td>4108</td>
<td>Eth1/53/1</td>
<td>15</td>
<td>1</td>
<td>210</td>
</tr>
<tr>
<td>* 25000 None &lt;User&gt;</td>
<td>39</td>
<td>1</td>
<td>206</td>
<td></td>
</tr>
<tr>
<td>* 20000 None &lt;User&gt;</td>
<td>39</td>
<td>1</td>
<td>206</td>
<td></td>
</tr>
<tr>
<td>* 21000 None &lt;User&gt;</td>
<td>1</td>
<td>1</td>
<td>217</td>
<td></td>
</tr>
</tbody>
</table>

This example shows how to display only static MPLS labels:

```
switch(config)# show mpls strip labels static
MPLS Strip Labels:
   Total : 3005
   Static : 5
Legend:  * - Static Label
   Interface - where label was first learned
   Idle-Age - Seconds since last use
   SW-Counter- Packets received in Software
   HW-Counter- Packets switched in Hardware
```

<table>
<thead>
<tr>
<th>Label</th>
<th>Interface</th>
<th>Idle-Age</th>
<th>SW-Counter</th>
<th>HW-Counter</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Clearing MPLS Stripping Counters and Label Entries

To clear the MPLS stripping counters and label entries, perform these tasks:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear mpls strip label dynamic</td>
<td>Clears dynamic label entries from the MPLS label table.</td>
</tr>
<tr>
<td>clear counters mpls strip</td>
<td>Clears all MPLS stripping counters.</td>
</tr>
</tbody>
</table>

The following example shows how to clear all MPLS stripping counters:

```
switch# clear counters mpls strip
switch# show mpls strip labels
MPLS Strip Labels:
  Total : 15000
  Static : 2
Legend: * - Static Label
Interface = where label was first learned
Idle-Age = Seconds since last use
SW-Counter = Packets received in Software
HW-Counter = Packets switched in Hardware

<table>
<thead>
<tr>
<th>Label</th>
<th>Interface</th>
<th>Idle-Age</th>
<th>SW-Counter</th>
<th>HW-Counter</th>
</tr>
</thead>
<tbody>
<tr>
<td>4096</td>
<td>Eth1/44</td>
<td>15</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>8192</td>
<td>Eth1/44</td>
<td>17</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>12288</td>
<td>Eth1/44</td>
<td>15</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>16384</td>
<td>Eth1/44</td>
<td>39</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>20480</td>
<td>Eth1/44</td>
<td>47</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>24576</td>
<td>Eth1/44</td>
<td>7</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>28672</td>
<td>Eth1/44</td>
<td>5</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>36864</td>
<td>Eth1/44</td>
<td>7</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>40960</td>
<td>Eth1/44</td>
<td>19</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>45056</td>
<td>Eth1/44</td>
<td>9</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>49152</td>
<td>Eth1/44</td>
<td>45</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>53248</td>
<td>Eth1/44</td>
<td>9</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

Configuration Examples for MPLS Stripping

This example shows how to add static MPLS labels:

```
switch# configure terminal
switch(config)# mpls strip label 100
switch(config)# mpls strip label 200
switch(config)# mpls strip label 300
```
## Additional References

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP ACLs</td>
<td><em>Cisco Nexus 9000 Series NX-OS Security Configuration Guide</em></td>
</tr>
<tr>
<td>MAC ACLs</td>
<td><em>Cisco Nexus 9000 Series NX-OS Security Configuration Guide</em></td>
</tr>
<tr>
<td>Port-channel symmetric hashing</td>
<td><em>Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide</em></td>
</tr>
<tr>
<td>Remote monitoring (RMON)</td>
<td>Configuring RMON, on page 179</td>
</tr>
<tr>
<td>Switched port analyzer (SPAN)</td>
<td>Configuring SPAN, on page 225</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td><em>Cisco Nexus 9000 Series NX-OS Troubleshooting Guide</em></td>
</tr>
</tbody>
</table>
CHAPTER 22

Configuring Graceful Insertion and Removal

This chapter describes how to configure graceful insertion and removal (GIR) on the Cisco Nexus 9000 Series switches.

This chapter contains the following sections:

• About Graceful Insertion and Removal, on page 323
• Licensing Requirements for GIR, on page 325
• Guidelines and Limitations for GIR, on page 325
• GIR Workflow, on page 326
• Configuring the Maintenance-Mode Profile, on page 327
• Configuring the Normal-Mode Profile, on page 328
• Creating a Snapshot, on page 329
• Adding Show Commands to Snapshots, on page 331
• Triggering Graceful Removal, on page 333
• Triggering Graceful Insertion, on page 335
• Maintenance Mode Enhancements, on page 336
• Verifying the GIR Configuration, on page 337
• Configuration Examples for GIR, on page 338

About Graceful Insertion and Removal

You can use graceful insertion and removal to gracefully eject a switch and isolate it from the network in order to perform debugging or upgrade operations. The switch is removed from the regular forwarding path with minimal traffic disruption. When you are finished performing debugging or upgrade operations, you can use graceful insertion to return the switch to its fully operational (normal) mode.

When you place the switch in maintenance mode, all configured Layer 3 control-plane protocols are isolated from the network. Directly connected routes are not withdrawn or modified during this state. When normal mode is restored, the advertisement of all routes is restored.

In graceful removal, all protocols and vPC domains are gracefully brought down and the switch is isolated from the network. In graceful insertion, all protocols and vPC domains are restored.

The following protocols are supported (for both IPv4 and IPv6 address families):

• Border Gateway Protocol (BGP)
• Enhanced Interior Gateway Routing Protocol (EIGRP)
• Intermediate System-to-Intermediate System (ISIS)
• Open Shortest Path First (OSPF)
• Protocol Independent Multicast (PIM)
• Routing Information Protocol (RIP)

For graceful insertion and removal, the PIM protocol is applicable only to vPC environments. During graceful removal, the vPC forwarding role is transferred to the vPC peer for all northbound sources of multicast traffic.

**Profiles**

By default, the system isolates all enabled protocols during graceful removal and restores them during graceful insertion. The protocols are isolated and restored in a predefined order.

If you want to isolate, shut down, or restore the protocols individually (or perform additional configurations), you can create a profile with configuration commands that can be applied during graceful removal or graceful insertion. However, you need to make sure that the order of the protocols is correct and any dependencies are considered.

The switch supports the following profiles:

- Maintenance-mode profile—Contains all the commands that will be executed during graceful removal, when the switch enters maintenance mode.
- Normal-mode profile—Contains all the commands that will be executed during graceful insertion, when the switch returns to normal mode.

The following commands (along with any configuration commands) are supported in the profiles.

**Note** The `shutdown` command takes precedence when both `shutdown` and `isolate` are configured under a routing protocol instance or maintenance-mode profile.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>isolate</code></td>
<td>Isolates the protocol from the switch and puts the protocol in maintenance mode.</td>
</tr>
<tr>
<td><code>no isolate</code></td>
<td>Restores the protocol and puts the protocol in normal mode.</td>
</tr>
<tr>
<td><code>shutdown</code></td>
<td>Shuts down the protocol or vPC domain.</td>
</tr>
<tr>
<td><code>no shutdown</code></td>
<td>Brings up the protocol or vPC domain.</td>
</tr>
<tr>
<td><code>system interface shutdown [exclude fex-fabric]</code></td>
<td>Shuts down the system interfaces (except the management interface).</td>
</tr>
<tr>
<td><code>no system interface shutdown [exclude fex-fabric]</code></td>
<td>Brings up the system interfaces.</td>
</tr>
</tbody>
</table>
Snapshots

In Cisco NX-OS, a snapshot is the process of capturing the running states of selected features and storing them on persistent storage media.

Snapshots are useful to compare the state of a switch before graceful removal and after graceful insertion. The snapshot process consists of three parts:

- Creating a snapshot of the states of a few preselected features on the switch and storing them on the persistent storage media
- Listing the snapshots taken at various time intervals and managing them
- Comparing snapshots and showing the differences between features

Licensing Requirements for GIR

<table>
<thead>
<tr>
<th>Product</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco NX-OS</td>
<td>Graceful insertion and removal (GIR) requires no license. Any feature not included in a license package is bundled with the nx-os image and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the Cisco NX-OS Licensing Guide.</td>
</tr>
</tbody>
</table>

Guidelines and Limitations for GIR

Graceful Insertion and Replacement have the following configuration guidelines and limitations:
• Beginning with Cisco NX-OS Release 9.2(1), L2 Graceful Insertion and Replacement is supported. When moving from normal to maintenance mode, MCT goes down resulting in north to south traffic convergence. Zero packet loss is not supported. The following table provides an example of traffic convergence of 10 vPCs with 2 port member on each VPC port and 60k mac scale.

<table>
<thead>
<tr>
<th>Trigger</th>
<th>Role</th>
<th>North to South Traffic</th>
<th>South to North Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal to maintenance mode</td>
<td>Primary</td>
<td>760 ms</td>
<td>1320 ms</td>
</tr>
<tr>
<td>Maintenance mode to normal</td>
<td>Primary</td>
<td>13155 ms</td>
<td>27980 ms</td>
</tr>
<tr>
<td>Normal to maintenance mode</td>
<td>Secondary</td>
<td>300 ms</td>
<td>1375 ms</td>
</tr>
<tr>
<td>Maintenance mode to normal</td>
<td>Secondary</td>
<td>15905 ms</td>
<td>23350 ms</td>
</tr>
</tbody>
</table>

• Beginning with Cisco NX-OS Release 9.2(1), if you configure the isolate option for OSPF, direct routes and stub routes are advertised as max-metric routes. As a result, north-to-south traffic to the SVI hosts goes through the vPC peer when only one vPC switch is isolated.

• Remove all existing custom profiles before creating new custom profiles for normal-mode and maintenance-mode.

GIR Workflow

Follow these steps to complete the graceful insertion and removal (GIR) workflow:

1. (Optional) Create the maintenance-mode profile. (See Configuring the Maintenance-Mode Profile, on page 327.)

2. (Optional) Create the normal-mode profile. (See Configuring the Normal-Mode Profile, on page 328.)

3. Take a snapshot before triggering graceful removal. (See Creating a Snapshot, on page 329.)

4. Trigger graceful removal to put the switch in maintenance mode. (See Triggering Graceful Removal, on page 333.)

5. Trigger graceful insertion to return the switch to normal mode. (See Triggering Graceful Insertion, on page 335.)

6. Take a snapshot after triggering graceful insertion. (See Creating a Snapshot, on page 329.)

7. Use the show snapshots compare command to compare the operational data before and after the graceful removal and insertion of the switch to make sure that everything is running as expected. (See Verifying the GIR Configuration, on page 337.)
Configuring the Maintenance-Mode Profile

You can create a maintenance-mode profile with configuration commands that can be applied during graceful removal or graceful insertion.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters a configuration session for the maintenance-mode profile. The no option deletes the maintenance profile maintenance-mode. Depending on which protocols you have configured, you must now enter the appropriate commands to bring down the protocols. For a list of supported commands, see Profiles, on page 324.</td>
</tr>
</tbody>
</table>
| [no] configure maintenance profile maintenance-mode | **Example:**
switch# configure maintenance profile maintenance-mode
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-mm-profile)# |
| **Step 2** | Closes the maintenance-mode profile. |
| end | **Example:**
switch(config-mm-profile)# end
switch# |
| **Step 3** | Displays the details of the maintenance-mode profile. |
| show maintenance profile maintenance-mode | **Example:**
switch# show maintenance profile maintenance-mode |

Example

This example shows how to create a maintenance-mode profile:

```
switch# configure maintenance profile maintenance-mode
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-mm-profile)# ip pim isolate
switch(config-mm-profile)# vpc domain 10
switch(config-mm-profile-config-vpc-domain)# shutdown
switch(config-mm-profile)# router bgp 100
switch(config-mm-profile-router)# shutdown
switch(config-mm-profile-router)# router eigrp 10
switch(config-mm-profile-router)# shutdown
switch(config-mm-profile-router)# address-family ipv6 unicast
switch(config-mm-profile-router-af)# shutdown
switch(config-mm-profile)# system interface shutdown
switch(config-mm-profile)# end
Exit maintenance profile mode.
switch# show maintenance profile maintenance-mode
[Maintenance Mode]
ip pim isolate
vpc domain 10
```
shutdown
router bgp 100
shutdown
router eigrp 10
shutdown
  address-family ipv6 unicast
shutdown
system interface shutdown

This example shows how to configure sleep instance in a custom profile to add a delay before the next protocol change.

```bash
switch# configure maintenance profile maintenance-mode
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-mm-profile)# router bgp 65001
switch(config-mm-profile-router)# isolate
switch(config-mm-profile-router)# sleep instance 1 10
switch(config-mm-profile-router)# isolate
switch(config-mm-profile-router)# sleep instance 2 15
switch(config-mm-profile-router)# isolate
switch(config-mm-profile-router)# sleep instance 3 20
switch(config-mm-profile-router)# isolate
switch(config-mm-profile-router)# sleep instance 4 5
switch(config-mm-profile-router)# isolate
switch(config-mm-profile-router)# isolate
switch(config-mm-profile-router)# isolate
switch(config-mm-profile-router)# end
Exit maintenance profile mode.
switch#
```

**Note**

If you need to run exec commands or add a dynamic delay while the maintenance mode profile is applied, use the `python instance instance-number uri [python-arguments]` script.

---

**Configuring the Normal-Mode Profile**

You can create a normal-mode profile with configuration commands that can be applied during graceful removal or graceful insertion.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>[no] configure maintenance profile normal-mode</code></td>
<td>Enters a configuration session for the normal-mode profile. The <code>no</code> version removes the maintenance profile normal-mode. Depending on which protocols you have configured, you must now enter the appropriate commands to bring up the protocols. For a list of supported commands, see Profiles, on page 324.</td>
</tr>
</tbody>
</table>
### Creating a Snapshot

You can create a snapshot of the running states of selected features. When you create a snapshot, a predefined set of `show` commands are run and the outputs are saved.

---

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Command or Action</th>
</tr>
</thead>
</table>
| Closes the normal-mode profile. | **Step 2**  
Example:  
switch(config-mm-profile)# end  
switch# |
| Displays the details of the normal-mode profile. | **Step 3**  
Example:  
switch# show maintenance profile normal-mode |

---

---

### Creating a Snapshot

You can create a snapshot of the running states of selected features. When you create a snapshot, a predefined set of `show` commands are run and the outputs are saved.

---

---

### Creating a Snapshot

You can create a snapshot of the running states of selected features. When you create a snapshot, a predefined set of `show` commands are run and the outputs are saved.

---

---

### Creating a Snapshot

You can create a snapshot of the running states of selected features. When you create a snapshot, a predefined set of `show` commands are run and the outputs are saved.

---

---

### Creating a Snapshot

You can create a snapshot of the running states of selected features. When you create a snapshot, a predefined set of `show` commands are run and the outputs are saved.

---

---

### Creating a Snapshot

You can create a snapshot of the running states of selected features. When you create a snapshot, a predefined set of `show` commands are run and the outputs are saved.

---

---

### Creating a Snapshot

You can create a snapshot of the running states of selected features. When you create a snapshot, a predefined set of `show` commands are run and the outputs are saved.

---

---

### Creating a Snapshot

You can create a snapshot of the running states of selected features. When you create a snapshot, a predefined set of `show` commands are run and the outputs are saved.

---

---

### Creating a Snapshot

You can create a snapshot of the running states of selected features. When you create a snapshot, a predefined set of `show` commands are run and the outputs are saved.

---

---

### Creating a Snapshot

You can create a snapshot of the running states of selected features. When you create a snapshot, a predefined set of `show` commands are run and the outputs are saved.

---

---

### Creating a Snapshot

You can create a snapshot of the running states of selected features. When you create a snapshot, a predefined set of `show` commands are run and the outputs are saved.

---

---

### Creating a Snapshot

You can create a snapshot of the running states of selected features. When you create a snapshot, a predefined set of `show` commands are run and the outputs are saved.

---

---

### Creating a Snapshot

You can create a snapshot of the running states of selected features. When you create a snapshot, a predefined set of `show` commands are run and the outputs are saved.

---

---

### Creating a Snapshot

You can create a snapshot of the running states of selected features. When you create a snapshot, a predefined set of `show` commands are run and the outputs are saved.

---

---

### Creating a Snapshot

You can create a snapshot of the running states of selected features. When you create a snapshot, a predefined set of `show` commands are run and the outputs are saved.

---

---

### Creating a Snapshot

You can create a snapshot of the running states of selected features. When you create a snapshot, a predefined set of `show` commands are run and the outputs are saved.

---

---

### Creating a Snapshot

You can create a snapshot of the running states of selected features. When you create a snapshot, a predefined set of `show` commands are run and the outputs are saved.

---

---

### Creating a Snapshot

You can create a snapshot of the running states of selected features. When you create a snapshot, a predefined set of `show` commands are run and the outputs are saved.

---

---

### Creating a Snapshot

You can create a snapshot of the running states of selected features. When you create a snapshot, a predefined set of `show` commands are run and the outputs are saved.

---

---

### Creating a Snapshot

You can create a snapshot of the running states of selected features. When you create a snapshot, a predefined set of `show` commands are run and the outputs are saved.

---

---

### Creating a Snapshot

You can create a snapshot of the running states of selected features. When you create a snapshot, a predefined set of `show` commands are run and the outputs are saved.

---

---

### Creating a Snapshot

You can create a snapshot of the running states of selected features. When you create a snapshot, a predefined set of `show` commands are run and the outputs are saved.

---

---

### Creating a Snapshot

You can create a snapshot of the running states of selected features. When you create a snapshot, a predefined set of `show` commands are run and the outputs are saved.

---

---

### Creating a Snapshot

You can create a snapshot of the running states of selected features. When you create a snapshot, a predefined set of `show` commands are run and the outputs are saved.

---

---

### Creating a Snapshot

You can create a snapshot of the running states of selected features. When you create a snapshot, a predefined set of `show` commands are run and the outputs are saved.

---

---

### Creating a Snapshot

You can create a snapshot of the running states of selected features. When you create a snapshot, a predefined set of `show` commands are run and the outputs are saved.

---

---

### Creating a Snapshot

You can create a snapshot of the running states of selected features. When you create a snapshot, a predefined set of `show` commands are run and the outputs are saved.

---

---

### Creating a Snapshot

You can create a snapshot of the running states of selected features. When you create a snapshot, a predefined set of `show` commands are run and the outputs are saved.

---

---

### Creating a Snapshot

You can create a snapshot of the running states of selected features. When you create a snapshot, a predefined set of `show` commands are run and the outputs are saved.

---

---

### Creating a Snapshot

You can create a snapshot of the running states of selected features. When you create a snapshot, a predefined set of `show` commands are run and the outputs are saved.

---

---

### Creating a Snapshot

You can create a snapshot of the running states of selected features. When you create a snapshot, a predefined set of `show` commands are run and the outputs are saved.
## Creating a Snapshot

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>snapshot create snapshot-name description</strong></td>
<td>Captures the running state or operational data of selected features and stores the data on persistent storage media. You can enter a maximum of 64 alphanumeric chapters for the snapshot name and a maximum of 254 alphanumeric characters for the description. Use the <code>snapshot delete</code> {all</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch# snapshot create snap_before_maintenance Taken before maintenance Executing 'show interface'... Done Executing 'show ip route summary vrf all'... Done Executing 'show ipv6 route summary vrf all'... Done Executing 'show bgp sessions vrf all'... Done Executing 'show ip eigrp topology summary'... Done Executing 'show ipv6 eigrp topology summary'... Done Feature 'vpc' not enabled, skipping... Executing 'show ip ospf vrf all'... Done Feature 'ospfv3' not enabled, skipping... Feature 'isis' not enabled, skipping... Feature 'rip' not enabled, skipping... Snapshot 'snap_before_maintenance' created</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>show snapshots</strong></td>
<td>Displays snapshots present on the switch.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch# show snapshots Snapshot Name Time Description snap_before_maintenance Wed Aug 19 13:53:28 2015 Taken before maintenance</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>show snapshots compare snapshot-name-1 snapshot-name-2</strong> {summary</td>
<td>ipv4routes</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch# show snapshots compare snap_before_maintenance snap_after_maintenance</td>
<td></td>
</tr>
</tbody>
</table>

### Example

The following example shows a summary of the changes between two snapshots:

```
switch# show snapshots compare snapshot1 snapshot2 summary

feature snapshot1 snapshot2 changed
basic summary
  # of interfaces 16 12 *
  # of vlans 10 4 *
  # of ipv4 routes 33 3 *
```

---

The following example shows the changes in IPv4 routes between two snapshots:

```
switch# show snapshots compare snapshot1 snapshot2 ipv4routes
metric       snapshot1  snapshot2  changed
# of routes     33      3      *  
# of adjacencies 10      4      *  
Prefix       Changed Attribute
---------    -------------------
  23.0.0.0/8  not in snapshot2
  10.10.10/32 not in snapshot2
  21.1.2.3/8  adjacency index has changed from 29 (snapshot1) to 38 (snapshot2)
```

There were 28 attribute changes detected

### Adding Show Commands to Snapshots

You can specify additional `show` commands to be captured in snapshots. These `show` commands are defined in user-specified snapshot sections.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> snapshot section add &quot;show-command&quot; row-id element-key1 [element-key2]</td>
<td>Adds a user-specified section to snapshots. The section is used to name the show command output. You can use any word to name the section. The show command must be enclosed in quotation marks. Non-show commands will not be accepted. The row-id argument specifies the tag of each row entry of the show command’s XML output. The element-key1 and element-key2 arguments specify the tags used to distinguish among row entries. In most cases, only the element-key1 argument needs to be specified to be able to distinguish among row entries.</td>
</tr>
</tbody>
</table>
| Example:

```
switch# snapshot section add myshow "show ip interface brief" ROW_intf intf-name
``` |
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Note</strong> To delete a user-specified section from snapshots, use the <code>snapshot section delete section</code> command.</td>
</tr>
<tr>
<td><code>show snapshots sections</code></td>
<td>Displays the user-specified snapshot sections.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Displays a comparison of two snapshots.</td>
</tr>
<tr>
<td>`show snapshots compare snapshot-name-1 snapshot-name-2 [summary</td>
<td>ipv4routes</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>The <code>ipv4routes</code> and <code>ipv6routes</code> options display the changes in IPv4 and IPv6 routes between the two snapshots.</td>
</tr>
<tr>
<td><code>switch# show snapshots compare snap1 snap2</code></td>
<td></td>
</tr>
</tbody>
</table>

**Example**

The following example adds the `show ip interface brief` command to the `myshow` snapshot section. It also compares two snapshots (snap1 and snap2) and shows the user-specified sections in both snapshots.

```
switch# snapshot section add myshow "show ip interface brief" ROW_intf intf-name
switch# show snapshots sections
user-specified snapshot sections
--------------------------------
[myshow]
  cmd: show ip interface brief
  row: ROW_intf
  key1: intf-name
  key2: -

[sect2]
  cmd: show ip ospf vrf all
  row: ROW_ctx
  key1: instance_number
  key2: cname
```

```
switch# show snapshots compare snap1 snap2
============================================================================= Feature Tag snap1 snap2
============================================================================= 
[bgp]
----------------------------------------------------------------------------
...........

[interface]
----------------------------------------------------------------------------
[interface:mgmt0]
  vdc_lvl_in_pkts 692310 **692317**
  vdc_lvl_in_mcast 575281 **575287**
  vdc_lvl_in_bcast 77209 **77210**
```
Triggering Graceful Removal

In order to perform debugging or upgrade operations, you can trigger a graceful removal of the switch, which will eject the switch and isolate it from the network.

Before you begin

If you want the system to use a maintenance-mode profile that you create, see Configuring the Maintenance-Mode Profile, on page 327.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> system mode maintenance</td>
<td>Puts all enabled protocols in maintenance mode (using the isolate command).</td>
</tr>
<tr>
<td>[dont-generate-profile</td>
<td>timeout value</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# system mode maintenance</td>
<td></td>
</tr>
<tr>
<td>Following configuration will be applied:</td>
<td></td>
</tr>
<tr>
<td>ip pim isolate</td>
<td></td>
</tr>
<tr>
<td>router bgp 65502</td>
<td></td>
</tr>
<tr>
<td>isolate</td>
<td></td>
</tr>
<tr>
<td>router ospf p1</td>
<td></td>
</tr>
<tr>
<td>isolate</td>
<td></td>
</tr>
<tr>
<td>router ospfv3 p1</td>
<td></td>
</tr>
<tr>
<td>isolate</td>
<td></td>
</tr>
<tr>
<td>Do you want to continue (y/n)? [no] y</td>
<td></td>
</tr>
</tbody>
</table>

Triggering Graceful Insertion and Removal
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generating a snapshot before going into maintenance mode</td>
<td>The no system mode maintenance timeout command disables the timer.</td>
</tr>
<tr>
<td>Starting to apply commands...</td>
<td>• shutdown—Shuts down all protocols, vPC domains, and interfaces except the management interface (using the shutdown command). This option is disruptive while the default (which uses the isolate command) is not.</td>
</tr>
<tr>
<td>Applying : ip pim isolate</td>
<td>• on-reload reset-reason reason—Boots the switch into maintenance mode automatically in the event of a specified system crash. The no system mode maintenance on-reload reset-reason command prevents the switch from being brought up in maintenance mode in the event of a system crash.</td>
</tr>
<tr>
<td>Applying : router bgp 65502</td>
<td>The maintenance mode reset reasons are as follows:</td>
</tr>
<tr>
<td>Applying : isolate</td>
<td>• HW_ERROR—Hardware error</td>
</tr>
<tr>
<td>Applying : router ospf p1</td>
<td>• SVC_FAILURE—Critical service failure</td>
</tr>
<tr>
<td>Applying : isolate</td>
<td>• KERN_FAILURE—Kernel panic</td>
</tr>
<tr>
<td>Applying : router ospfv3 p1</td>
<td>• WDOG_TIMEOUT—Watchdog timeout</td>
</tr>
<tr>
<td>Applying : isolate</td>
<td>• FATAL_ERROR—Fatal error</td>
</tr>
<tr>
<td>Maintenance mode operation successful.</td>
<td>• LC_FAILURE—Line card failure</td>
</tr>
<tr>
<td></td>
<td>• MATCH_ANY—Any of the above reasons</td>
</tr>
</tbody>
</table>

The system prompts you to continue. Enter y to continue or n to terminate the process.

### Step 3  (Optional) show system mode

**Example:**

```bash
switch(config)# show system mode
System Mode: Maintenance
```

Displays the current system mode.

The switch is in maintenance mode. You can now perform any desired debugging or upgrade operations on the switch.

### Step 4  (Optional) copy running-config startup-config

**Example:**

```bash
switch(config)# copy running-config startup-config
```

Copies the running configuration to the startup configuration. This command is required if you want to preserve maintenance mode following a reboot.
**Example**

This example shows how to shut down all protocols, vPC domains, and interfaces on the switch:

```
switch(config)# system mode maintenance shutdown
```

Following configuration will be applied:

```
vpc domain 10
    shutdown
router bgp 65502
    shutdown
router ospf p1
    shutdown
router ospfv3 p1
    shutdown
system interface shutdown
```

Do you want to continue (y/n)? [no] y

Generating a snapshot before going into maintenance mode

Starting to apply commands...

Applying: vpc domain 10
Applying: shutdown
Applying: router bgp 65502
Applying: shutdown
Applying: router ospf p1
Applying: shutdown
Applying: router ospfv3 p1
Applying: shutdown

Maintenance mode operation successful.

This example shows how to automatically boot the switch into maintenance mode if a fatal error occurs:

```
switch(config)# system mode maintenance on-reload reset-reason fatal_error
```

---

**Triggering Graceful Insertion**

When you finish performing any debugging or upgrade operations, you can trigger a graceful insertion to restore all protocols.

**Before you begin**

If you want the system to use a normal-mode profile that you create, see Configuring the Maintenance-Mode Profile, on page 327.
### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><strong>configure terminal</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><strong>no system mode maintenance</strong></td>
<td>Puts all enabled protocols in normal mode</td>
</tr>
<tr>
<td><strong>[dont-generate-profile]</strong></td>
<td>(using the <strong>no isolate</strong> command).</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config)# no system mode</td>
<td></td>
</tr>
<tr>
<td>maintenance dont-generate-profile</td>
<td></td>
</tr>
<tr>
<td>Following configuration will be applied:</td>
<td></td>
</tr>
<tr>
<td>no ip pim isolate</td>
<td></td>
</tr>
<tr>
<td>router bgp 65502</td>
<td></td>
</tr>
<tr>
<td>no isolate</td>
<td></td>
</tr>
<tr>
<td>router ospf p1</td>
<td></td>
</tr>
<tr>
<td>no isolate</td>
<td></td>
</tr>
<tr>
<td>router ospfv3 p1</td>
<td></td>
</tr>
<tr>
<td>no isolate</td>
<td></td>
</tr>
<tr>
<td>Do you want to continue (y/n)? [no]</td>
<td></td>
</tr>
<tr>
<td>y</td>
<td></td>
</tr>
<tr>
<td>Starting to apply commands...</td>
<td></td>
</tr>
<tr>
<td>Applying : no ip pim isolate</td>
<td></td>
</tr>
<tr>
<td>Applying : router bgp 65502</td>
<td></td>
</tr>
<tr>
<td>Applying : no isolate</td>
<td></td>
</tr>
<tr>
<td>Applying : router ospf p1</td>
<td></td>
</tr>
<tr>
<td>Applying : no isolate</td>
<td></td>
</tr>
<tr>
<td>Applying : router ospfv3 p1</td>
<td></td>
</tr>
<tr>
<td>Applying : no isolate</td>
<td></td>
</tr>
<tr>
<td>Maintenance mode operation successful.</td>
<td></td>
</tr>
<tr>
<td>Generating Current Snapshot</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><em>(Optional)</em> <strong>show system mode</strong></td>
<td>Displays the current system mode. The switch</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>is now in normal mode and is fully operational.</td>
</tr>
<tr>
<td>switch(config)# show system mode</td>
<td></td>
</tr>
<tr>
<td>System Mode: Normal</td>
<td></td>
</tr>
</tbody>
</table>

### Maintenance Mode Enhancements

Starting with Release 7.0(3)i5(1), the following maintenance mode enhancements have been added to Cisco Nexus 9000 Series switches:

- In the system maintenance shutdown mode, the following message is added:

  **NOTE:** The command system interface shutdown will shutdown all interfaces excluding mgmt 0.
• Entering the CLI command, **system mode maintenance** checks and sends alerts for the orphan ports.

• In isolate mode, when the vPC is configured, the following message is added:

  NOTE: If you have vPC orphan interfaces, please ensure vpc orphan-port suspend is configured under them, before proceeding further.

• Custom Profile Configuration: A new CLI command, **system mode maintenance always-use-custom-profile** is added for custom profile configuration. A new CLI command, **system mode maintenance non-interactive** is added for Cisco Nexus 9000 Series switches only. It provides a way to facilitate the transition to maintenance mode or normal mode without confirmation being done or each step being printed on the CLI session.

When you create a custom profile (in maintenance or normal mode), it displays the following message:

  Please use the command **system mode maintenance always-use-custom-profile** if you want to always use the custom profile.

• A delay has been added before the after_maintenance snapshot is taken. The **no system mode maintenance** command exits once all the configuration for the normal mode has been applied, the mode has been changed to normal mode, and a timer has been started to take the after_maintenance snapshot. Once the timer expires, the after_maintenance snapshot is taken in the background and a new warning syslog, MODE_SNAPSHOT_DONE is sent once the snapshot is complete.

  The final output of the CLI command **no system mode maintenance** indicates when the after_maintenance snapshot is generated:

  The after_maintenance snapshot will be generated in <delay> seconds. After that time, please use show snapshots compare before_maintenance after_maintenance to check the health of the system. The timer delay for the after_maintenance snapshot is defaulted to 120 seconds but it can be changed by a new configuration command.

  The new configuration command to change the timer delay for the after_maintenance snapshot is **system mode maintenance snapshot-delay <seconds>**. This configuration overrides the default setting of 120 seconds to any value between 0 and 65535 and it is displayed in the ASCII configuration.

  A new show command, **show maintenance snapshot-delay** has also been added to display the current snapshot-delay value. This new show command supports the XML output.

• A visible CLI indicator has been added to display when the system is in the maintenance mode, for example, switch (maint-mode) #.

• Support for the SNMP traps has been added when the device moves from the maintenance mode to the normal mode and vice-versa through CLI reload, or system reset. The **snmp-server enable traps mmode cseMaintModeChangeNotify** trap is added to enable changing to the maintenance mode trap notification. The **snmp-server enable traps mmode cseNormalModeChangeNotify** is added to enable changing to the normal mode trap notification. Both the traps are disabled by default.

## Verifying the GIR Configuration

To display the GIR configuration, perform one of the following tasks:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interface brief</td>
<td>Displays abbreviated interface information.</td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show maintenance on-reload reset-reasons</code></td>
<td>Displays the reset reasons for which the switch comes up in maintenance mode. For a description of the maintenance mode reset reasons, see Triggering Graceful Removal, on page 333.</td>
</tr>
<tr>
<td>`show maintenance profile [maintenance-mode</td>
<td>normal-mode]`</td>
</tr>
<tr>
<td><code>show maintenance timeout</code></td>
<td>Displays the maintenance-mode timeout period, after which the switch automatically returns to normal mode.</td>
</tr>
<tr>
<td>`show {running-config</td>
<td>startup-config} mmode [all]`</td>
</tr>
<tr>
<td><code>show snapshots</code></td>
<td>Displays snapshots present on the switch.</td>
</tr>
<tr>
<td>`show snapshots compare snapshot-name-1 snapshot-name-2 [summary</td>
<td>ipv4routes</td>
</tr>
<tr>
<td><code>show snapshots dump snapshot-name</code></td>
<td>Displays the content of each file that was generated when the snapshot was taken.</td>
</tr>
<tr>
<td><code>show snapshots sections</code></td>
<td>Displays the user-specified snapshot sections.</td>
</tr>
<tr>
<td><code>show system mode</code></td>
<td>Displays the current system mode.</td>
</tr>
</tbody>
</table>

### Configuration Examples for GIR

The `redistribute direct` configuration under Border Gateway Protocol (BGP) will attract traffic as the BGP isolate mode does not withdraw direct routes. This example shows how to use the `route-map` command to enable BGP to withdraw direct routes in isolate mode.

#### Policy Configuration

Use the `route-map my-rmap-deny` command in maintenance mode to exclude SVIs with a tag 200 configuration.

```shell
switch(config)# route-map my-rmap-deny deny 10
switch(config-route-map)# match tag 200
switch(config-route-map)# exit
switch(config)# route-map my-rmap-deny permit 20
```

Use the `route-map my-rmap-permit` command in normal mode to include SVIs with a tag 200 configuration.

```shell
```
switch(config)# route-map my-rmap-permit permit 10
switch(config-route-map)# match tag 200
switch(config-route-map)# exit
switch(config)# route-map my-rmap-permit permit 20

Virtual IP (vIP)/Switch Virtual Interface (SVI) Configuration

switch(config)# interface loopback 200
switch(config-if)# ip address 192.0.2.100/8 tag 200
switch(config)# interface vlan 2
switch(config-if)# ip address 192.0.2.108/8 tag 200
....
switch(config)# interface vlan 3
switch(config-if)# ip address 192.0.2.102/8 tag 200

BGP Configuration

switch(config)# feature bgp
switch(config)# router bgp 100
switch(config-router)# neighbor 192.0.2.100
....

Maintenance Mode Profile

switch# configure maintenance profile maintenance-mode
switch(config-mm-profile)# router bgp 200
switch(config-mm-profile-router)# address-family ipv4 unicast
switch(config-mm-profile-router-af)# redistribute direct route-map my-rmap-deny
switch(config-mm-profile-router-af)# exit
switch(config-mm-profile)# sleep instance 1 10

Normal Mode Profile

switch# configure maintenance profile normal-mode
switch(config-mm-profile)# router bgp 100
switch(config-mm-profile-router)# address-family ipv4 unicast
switch(config-mm-profile-router-af)# redistribute direct route-map my-rmap-permit
switch(config-mm-profile-router-af)# exit
switch(config-mm-profile)# sleep instance 1 20
Configuration Examples for GIR
Performing Software Maintenance Upgrades

This chapter describes how to perform software maintenance upgrades (SMUs) on Cisco NX-OS devices.

This chapter includes the following sections:

• About SMUs, on page 341
• Prerequisites for SMUs, on page 343
• Guidelines and Limitations for SMUs, on page 343
• Performing a Software Maintenance Upgrade for Cisco NX-OS, on page 344
• Performing a Software Maintenance Upgrade for Guest Shell Bash, on page 357
• Additional References, on page 359
• SMU History, on page 359

About SMUs

A software maintenance upgrade (SMU) is a package file that contains fixes for a specific defect. SMUs are created to respond to immediate issues and do not include new features. Typically, SMUs do not have a large impact on device operations. SMU versions are synchronized to the package major, minor, and maintenance versions they upgrade.

The effect of an SMU depends on its type:

• Process restart SMU-Causes a process or group of processes to restart on activation.
• Reload SMU-Causes a parallel reload of supervisors and line cards.

SMUs are not an alternative to maintenance releases. They provide a quick resolution of immediate issues. All defects fixed by SMUs are integrated into the maintenance releases.

For information on upgrading your device to a new feature or maintenance release, see the Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide.

For information on Cisco NX-OS optionality feature, see the Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide.

Activating an SMU does not cause any earlier SMUs, or the package to which the SMU applies, to be automatically deactivated.
Beginning with Cisco NX-OS Release 7.0(3)I2(1), SMU package files have an .rpm extension. Earlier files have a .bin extension.

Package Management

The general procedure for adding and activating SMU packages on the device is as follows:

1. Copy the package file or files to a local storage device or file server.
2. Add the package or packages on the device using the install add command.
3. Activate the package or packages on the device using the install activate command.
4. Commit the current set of packages using the install commit command.
5. (Optional) Deactivate and remove the package, when desired.

The following figure illustrates the key steps in the package management process.

Figure 7: Process to Add, Activate, and Commit SMU Packages

Impact of Package Activation and Deactivation

The activation or deactivation of an SMU package can have an immediate impact on the system. The system can be affected in the following ways:

- New processes might be started.
- Running processes might be stopped or restarted.
- All processes in the line cards might be restarted. Restarting processes in the line cards is equivalent to a soft reset.
- The line cards might reload.
- No processes in the line cards might be affected.

You must address any issues that result from the revised configuration and reapply the configuration, if necessary.
Prerequisites for SMUs

These prerequisites must be met for a package to be activated or deactivated:

- You must be in a user group associated with a task group that includes the proper task IDs. If you suspect a user group assignment is preventing you from using a command, contact your AAA administrator for assistance.
- Verify that all line cards are installed and operating properly. For example, do not activate or deactivate packages while line cards are booting, while line cards are being upgraded or replaced, or when you anticipate an automatic switchover activity.

Guidelines and Limitations for SMUs

SMUs have the following guidelines and limitations:

- Some packages require the activation or deactivation of other packages. If the SMUs have dependencies on each other, you cannot activate them without first activating the previous ones.
- The package being activated must be compatible with the current active software set.
- Activation is performed only after the package compatibility checks have been passed. If a conflict is found, an error message displays.
- You can activate or deactivate multiple SMUs with a tarball SMU.
- While a software package is being activated, other requests are not allowed to run on any of the impacted nodes. Package activation is completed when a message similar to this one appears:
  
  Install operation 1 completed successfully at Thu Jan 9 01:19:24 2014

- Each CLI install request is assigned a request ID, which can be used later to review the events.
- If you perform a software maintenance upgrade and later upgrade your device to a new Cisco NX-OS software release, the new image will overwrite both the previous Cisco NX-OS release and the SMU package file.
- The SMU package file is named nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.i5.1.lib32_n9000.rpm, which support both n9k_EOR and n9k_TOR platforms.
- For the "Unable to remove MAC ACE using sequence number in 7.0(3)I7(2)" issue, if you are going to apply the patch that resolves it, you must make sure that the ACL is deleted before applying the patch. Otherwise, the issue will be seen again. This issue applies only to the ACL which has the redirect keyword in it.
Performing a Software Maintenance Upgrade for Cisco NX-OS

Preparing for Package Installation

You should use several `show` commands to gather information in preparation for the SMU package installation.

**Before you begin**

Determine if a software change is required.

Verify that the new package is supported on your system. Some software packages require that other packages or package versions be activated, and some packages support only specific line cards.

Review the release notes for important information related to that release and to help determine the package compatibility with your device configuration.

Verify that the system is up, stable, and prepared for the software changes.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>`show logging logfile</td>
<td>grep -i &quot;System ready&quot;`</td>
</tr>
<tr>
<td>Example:</td>
<td>`switch# show logging logfile</td>
<td>grep -i &quot;System ready&quot;`</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>show install active</code></td>
<td>Displays the active software on the device. Use this command to determine what software should be added on the device and to compare to the active software report after installation operations are complete.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>switch# show install active</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>show module</code></td>
<td>Confirms that all modules are in the stable state.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>switch# show module</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>show clock</code></td>
<td>Verifies that the system clock is correct. Software operations use certificates based on device clock times.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>switch# show clock</code></td>
<td></td>
</tr>
</tbody>
</table>

**Example**

This example shows how to verify that the system is up. A "System ready" response indicates that the system is ready for SMU package installation.
switch# show logging logfile | grep -i "System ready"

This example shows how to display the active packages for the entire system. Use this information to determine if a software change is required.

switch# show install active
Boot Image:
   NXOS Image: bootflash:///nxos.7.0.3.I7.3.1.bin

Active Packages:

switch#

This example shows how to display the current system clock setting:

switch# show clock
02:14:51.474 PST Wed Jan 04 2014

---

**Downloading the SMU Package File from Cisco.com**

Follow these steps to download the SMU package file:

**Procedure**

**Step 1** Log in to Cisco.com.
**Step 2** Go to the Download Software page at this URL: [http://software.cisco.com/download/navigator.html](http://software.cisco.com/download/navigator.html)
**Step 3** In the Select a Product list, choose *Switches* > *Data Center Switches* > *Cisco Nexus 9000 Series Switches* > *model*.
**Step 4** Choose the appropriate SMU file for your device and click *Download*.

---

**Copying the Package File to a Local Storage Device or Network Server**

You must copy the SMU package file to a local storage device or a network file server to which the device has access. After this task is done, the package can be added and activated on the device.

If you need to store package files on the device, we recommend that you store the files on the hard disk. The boot device is the local disk from which the package is added and activated. The default boot device is bootflash:

---

**Tip**

Before you copy package files to a local storage device, use the `dir` command to determine if the required package files are already on the device.

If the SMU package files are located on a remote TFTP, FTP, or SFTP server, you can copy the files to a local storage device. After the files are located on the local storage device, the package can be added and activated on the device from that storage device. The following server protocols are supported:
• Trivial File Transfer Protocol—TFTP allows files to be transferred from one computer to another over a network, usually without the use of client authentication (for example, username and password). It is a simplified version of FTP.

Note
Some package files might be larger than 32 MB, and the TFTP services provided by some vendors might not support a file this large. If you do not have access to a TFTP server that supports files larger than 32 MB, download the file using FTP.

• File Transfer Protocol—FTP is part of the TCP/IP protocol stack and requires a username and password.

• SSH File Transfer Protocol—SFTP is part of the SSHv2 feature in the security package and provides for secure file transfers. For more information, see the Cisco Nexus 9000 Series NX-OS Security Configuration Guide.

Note
Consult your system administrator for the location and availability of your network server.

Use the commands in the following table to copy the SMU package file from the server to your device using the file transfer protocols.

Table 27: Commands for Copying SMU Package Files to the Device

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `copy tftp://hostname-or-ipaddress/directory-path/filename bootflash:` | Copies the package file from the TFTP server to the bootflash:.
  • `hostname-or-ipaddress`—The hostname or IP address of the network file server.
  • `directory-path`—The network file server path that leads to the package file to be added.
  • `filename`—The name of the package file that you want to add. |
<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**copy**
ftp://username:password@hostname-or-ipaddress/directory-path/filename
bootflash: |

Copies the package file from the FTP server to the bootflash:.

- **username**—The username of the user who has access privileges to the directory in which the package file is stored.
- **password**—The password associated with the username of the user who has access privileges to the directory in which the package file is stored. If a password is not provided, the networking device accepts anonymous FTP.
- **hostname-or-ipaddress**—The hostname or IP address of the network file server.
- **directory-path**—The network file server path that leads to the package file to be added. The specified directory should be a directory under the home directory of the user. In this example, the file being downloaded is in a subdirectory called "images" in the home directory of the user "john."

**Note** For FTP services, **directory-path** is the directory relative to the **username** home directory. If you want to specify an absolute path for the directory, you must add a "/" following the server address.

- **filename**—The name of the package file that you want to add.
Adding and Activating Packages

You can add SMU package files that are stored on a local storage device or on a remote TFTP, FTP, or SFTP server to your device.

Note

This procedure uses Cisco NX-OS CLI commands to add and activate RPM package files. If you would prefer to use YUM commands, follow the instructions in the "Installing RPMs from Bash" section of the Cisco Nexus 9000 Series NX-OS Programmability Guide.

Note

The SMU package being activated must be compatible with the currently active software to operate. When an activation is attempted, the system runs an automatic compatibility check to ensure that the package is compatible with the other active software on the device. If a conflict is found, an error message displays. The activation is performed only after all compatibility checks have been passed.

Note

Activating an SMU does not cause any earlier SMUs or the package to which the SMU applies to be automatically deactivated.

Before you begin

Make sure that all packages to be added are present on a local storage device or a network file server.
Make sure that you meet all of the prerequisites for the activation of packages.
Complete the procedure described in Copying the Package File to a Local Storage Device or Network Server, on page 345.
### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Connect to the console port and log in.</td>
<td>Establishes a CLI management session to the console port.</td>
</tr>
</tbody>
</table>
| Step 2 | (Optional) `dir bootflash:` | Displays the package files that are available to be added.  
**Note** Only SMU package files can be added and activated using this procedure. |
| Step 3 | `install add filename [activate]`  
**Example:**  
switch# install add bootflash: nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.I5.1.1ib32_n9000.rpm | Unpacks the package software files from the local storage device or network server and adds them to the bootflash: and all active and standby supervisors installed on the device.  
The `filename` argument can take any of these formats:  
- `bootflash:filename`  
- `ftp://hostname-or-ipaddress/directory-path/filename`  
- `ftp://username:password@hostname-or-ipaddress/directory-path/filename`  
- `usb1:filename`  
- `usb2:filename`  
For all SMU packages except the CSCur02700 SMU package, you can use the optional `activate` keyword to automatically activate the package after it is added successfully.  
**Note** For the CSCur02700 SMU package, use the `install activate` command in Step 5 to activate the package. Do not use the optional `activate` keyword with the `install add` command as the package might fail and require a reboot.  
**Note** Multiple versions of an SMU package can be added to the storage device without impacting the running configuration, but only one version of a package can be activated for a line card.  
**Note** Press ? after a partial package name to display all possible matches available for activation. If there is only one match, press the Tab key to fill in the rest of the package name. |
Adding and Activating Packages

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>You can use the <strong>install add</strong> command with a tarball SMU to install multiple SMUs at the same time.</td>
<td></td>
</tr>
</tbody>
</table>

### Step 4
(Optional) **show install inactive**

**Example:**

```
switch# show install inactive
```

Displays the inactive packages on the device. Verify that the package added in the previous step appears in the display.

### Step 5
Required: **install activate filename**

**Example:**

```
switch# install activate
nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.I5.1.lib32_n9000.rpm
```

**Example:**

```
switch# install activate
nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.I5.1.lib32_n9000.rpm
Install operation 18 !!WARNING!! This patch will get activated only after a reload of the switch. at Wed Jun 22 00:42:12 2016
```

**Activates a package that was added to the device. SMU packages remain inactive until activated. (Skip this step if the package was activated earlier with the **install add activate** command.)**

**Tip**

After the activation process finishes, enter the **show install log** command to display the process results.

### Step 6
Repeat Step 5 until all packages are activated.

**Activates additional packages as required.**

### Step 7
(Optional) **show install active**

**Example:**

```
switch# show install active
```

**Displays all active packages. Use this command to determine if the correct packages are active.**

### Example

This example shows how to add multiple SMU package files with a tarball and then verify the added package files.

```
switch# install add bootflash:nxos.CSC123456-n9k_ALL-1.0.0-7.0.3.I7.3.lib32_n9000.tar
[####################] 100%
Install operation 882 completed successfully at Tue Mar 6 17:30:31 2018
```

```
switch#
```

```
switch# show install inactive
Boot Image: 
NXOS Image: bootflash:///nxos.7.0.3.I7.3.bin-219-CCO

Inactive Packages:
nxos.CSC123456_core-n9k_ALL-1.0.0-7.0.3.I7.3.lib32_n9000
nxos.CSC123456_eth-n9k_ALL-1.0.0-7.0.3.I7.3.lib32_n9000

Inactive Base Packages:
```

```
switch#
```
Committing the Active Package Set

When an SMU package is activated on the device, it becomes part of the current running configuration. To make the package activation persistent across system-wide reloads, you must commit the package on the device.

On startup, the device loads the committed package set. If the system is reloaded before the current active package is committed, the previously committed package set is used.

**Before you begin**

Before you commit a package set, verify that the device is operating correctly and is forwarding packets as expected.

Complete the procedure described in *Adding and Activating Packages, on page 348.*

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Commit the current set of packages so that these packages are used if the device is restarted.</td>
</tr>
<tr>
<td>install commit <em>filename</em></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch# install commit nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.I5.1.lib32_n9000.rpm</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2** | Displays which packages are committed. |
| (Optional) show install committed | |
| **Example:** | |
| switch# show install committed | |

**Example**

This example shows how to commit active SMU packages on the device and then verify the committed packages:

```
switch# install commit nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.I5.1.lib32_n9000.rpm
Install operation 2 completed successfully at Wed Jun 22 01:20:46 2016

switch# show install committed
Committed Packages:
    nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.I5.1.lib32_n9000.rpm
```

Deactivating and Removing Packages

When a package is deactivated, it is no longer active on the device, but the package files remain on the boot disk. The package files can be reactivated later, or they can be removed from the disk.

The Cisco NX-OS software also provides the flexibility to roll back the selected package set to a previously saved package set. If you find that you prefer a previous package set over the currently active package set,
you can use the **install deactivate** and **install commit** commands to make a previously active package set active again.

**Note**

This procedure uses Cisco NX-OS CLI commands to deactivate and remove RPM package files. If you would prefer to use YUM commands, follow the instructions in the "Erasing an RPM" section of the Cisco Nexus 9000 Series NX-OS Programmability Guide.

**Before you begin**

You cannot deactivate a package if it is required by another active package. When you attempt to deactivate a package, the system runs an automatic check to ensure that the package is not required by other active packages. The deactivation is performed only after all compatibility checks have been passed.

You cannot delete a package if it is part of the running or committed software of the device.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Connect to the console port and log in. Establishes a CLI management session to the console port.</td>
</tr>
</tbody>
</table>
| **Step 2** | **install deactivate** *filename*
  **Example:**
  `switch# install deactivate`
  `nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.15.1.lib32_n9000.rpm`
  Deactivates a package that was added to the device and turns off the package features for the line card. |
| **Step 3** | (Optional) **show install inactive**
  **Example:**
  `switch# show install inactive`
  Displays the inactive packages on the device. |
| **Step 4** | (Optional) **install commit**
  **Example:**
  `switch# install commit`
  Commits the current set of packages so that these packages are used if the device is restarted. **Note** Packages can be removed only if the deactivation operation is committed. |
| **Step 5** | (Optional) **install remove** {*filename | inactive*}
  **Example:**
  `switch# install remove`
  `nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.15.1.lib32_n9000.rpm`
  `Proceed with removing? (y/n)? [n] y`
  `nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.15.1.lib32_n9000.rpm? (y/n)? [n] y`
  Removes the inactive package. **Note**
  - Only inactive packages can be removed.
  - Packages can be removed only if they are deactivated from all line cards in the device.
  - The package deactivation must be committed.
  - To remove a specific inactive package from a storage device, use the **install**
Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>remove command with the <code>filename</code> argument.</td>
<td></td>
</tr>
<tr>
<td>To remove all inactive packages from all nodes in the system, use the <code>install remove</code> command with the <code>inactive</code> keyword.</td>
<td></td>
</tr>
</tbody>
</table>

Example

This example shows how to deactivate a package, commit the changes, and remove the inactive package from the device:

```
switch# install deactivate nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.I5.1.lib32_n9000.rpm
Install operation 3 completed successfully at Wed Jun 22 01:20:36 2016

switch# show install inactive
Inactive Packages:
nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.I5.1.lib32_n9000.rpm

switch# install commit
Install operation 4 completed successfully at Wed Jun 22 01:20:46 2016

switch# install remove nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.I5.1.lib32_n9000.rpm
Proceed with removing nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.I5.1.lib32_n9000.rpm? (y/n)? [n] y
Install operation 5 completed successfully at Wed Jun 22 01:20:57 2016
```

This example shows how to deactivate multiple packages with one command, remove the inactive packages from the device, and verify the package removal:

```
switch# install deactivate nxos.CSC123456_core-n9k_ALL-1.0.0-7.0.3.I7.3.lib32_n9000 nxos.CSC123456_eth-n9k_ALL-1.0.0-7.0.3.I7.3.lib32_n9000
[####################] 100%
Install operation 884 completed successfully at Tue Mar 6 17:34:02 2018

switch#
switch# show install inactive
Boot Image:
  NXOS Image: bootflash://nxos.7.0.3.I7.3.bin-219-CCO

Inactive Packages:
nxos.CSC123456_core-n9k_ALL-1.0.0-7.0.3.I7.3.lib32_n9000
nxos.CSC123456_eth-n9k_ALL-1.0.0-7.0.3.I7.3.lib32_n9000

Inactive Base Packages:

switch#
switch# install remove nxos.CSC123456_core-n9k_ALL-1.0.0-7.0.3.I7.3.lib32_n9000
Proceed with removing nxos.CSC123456_core-n9k_ALL-1.0.0-7.0.3.I7.3.lib32_n9000? (y/n)? [n] y
[####################] 100%
Install operation 885 completed successfully at Tue Mar 6 17:34:56 2018

switch# install remove nxos.CSC123456_eth-n9k_ALL-1.0.0-7.0.3.I7.3.lib32_n9000
Proceed with removing nxos.CSC123456_eth-n9k_ALL-1.0.0-7.0.3.I7.3.lib32_n9000? (y/n)? [n] y
```
Install operation 886 completed successfully at Tue Mar 6 17:35:14 2018

switch#

switch# show install inactive

Boot Image:
NXOS Image: bootflash:///nxos.7.0.3.I7.3.bin-219-CCO

Inactive Packages:

Inactive Base Packages:

switch#

## Downgrading Feature RPMs

Follow this procedure to downgrade an installed feature RPM to the base feature RPM.

---

### Note

This procedure uses Cisco NX-OS CLI commands to downgrade feature RPMs. If you would prefer to use YUM commands, follow the instructions in the "Downgrading an RPM" section of the *Cisco Nexus 9000 Series NX-OS Programmability Guide*.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>(Optional) <strong>show install packages</strong></td>
<td>Displays the feature RPM packages on the device.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>switch# show install packages</code></td>
<td></td>
</tr>
<tr>
<td><code>ntp.lib32_n9000 1.0.1-7.0.3.I2.2e installed</code></td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2**        |         |
| Required: **run bash** | Loads Bash. |
| **Example:**      |         |
| `switch# run bash` |         |
| `bash-4.2$` |         |

| **Step 3**        |         |
| Required: **cd /rpms** | Changes to the RPMs folder in Bash. |
| **Example:**      |         |
| `bash-4.2$ cd /rpms` |         |

| **Step 4**        |         |
| Required: **ls *feature*** | Lists the RPM for the specified feature. |
| **Example:**      |         |
| `bash-4.2$ ls *ntp*` |         |
| `ntp-1.0.0-7.0.3.I2.2e.lib32_n9000.rpm` |         |

| **Step 5**        |         |
| Required: **cp filename /bootflash** | Copies the base feature RPM to the bootflash. |
| **Example:**      |         |

---

Performing Software Maintenance Upgrades

Displaying Installation Log Information

The installation log provides information on the history of the installation operations. Each time an installation operation is run, a number is assigned to that operation.

- Use the `show install log` command to display information about both successful and failed installation operations.
• Use the `show install log` command with no arguments to display a summary of all installation operations. Specify the `request-id` argument to display information specific to an operation. Use the `detail` keyword to display details for a specific operation, including file changes, nodes that could not be reloaded, and any impact to processes.

This example shows how to display information for all installation requests:

```
switch# show install log
Wed Jun 22 01:26:09 2016
Install operation 1 by user 'admin' at Wed Jun 22 01:19:19 2016
Install add bootflash:nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.15.1.lib32_n9000.rpm
Install operation 1 completed successfully at Wed Jun 22 01:19:24 2016
-------------------------------------------------------------
Install operation 2 by user 'admin' at Wed Jun 22 01:19:29 2016
Install activate nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.15.1.lib32_n9000.rpm
Install operation 2 completed successfully at Wed Jun 22 01:19:45 2016
-------------------------------------------------------------
Install operation 3 by user 'admin' at Wed Jun 22 01:20:05 2016
Install commit nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.15.1.lib32_n9000.rpm
Install operation 3 completed successfully at Wed Jun 22 01:20:08 2016
-------------------------------------------------------------
Install operation 4 by user 'admin' at Wed Jun 22 01:20:21 2016
Install deactivate nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.15.1.lib32_n9000.rpm
Install operation 4 completed successfully at Wed Jun 22 01:20:36 2016
-------------------------------------------------------------
Install operation 5 by user 'admin' at Wed Jun 22 01:20:43 2016
Install commit nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.15.1.lib32_n9000.rpm
Install operation 5 completed successfully at Wed Jun 22 01:20:46 2016
-------------------------------------------------------------
Install operation 6 by user 'admin' at Wed Jun 22 01:20:55 2016
Install remove nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.15.1.lib32_n9000.rpm
Install operation 6 completed successfully at Wed Jun 22 01:20:57 2016
-------------------------------------------------------------
Install operation 7 by user 'admin' at Wed Jun 22 01:21:07 2016
Install remove
Install operation 7 completed successfully at Wed Jun 22 01:21:10 2016
```

This example shows how to display additional information, including any impact to nodes and processes:

```
switch# show install log detail
Wed Jun 22 01:24:03 2016
Install operation 1 by user 'admin' at Wed Jun 22 01:19:19 2016
Installer started downloading the package:
/nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.15.1.lib32_n9000.rpm
via bootflash
Install add bootflash:nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.15.1.lib32_n9000.rpm
Copying file at Wed Jun 22 01:19:20 2016
Download success, 238545 bytes received
Verifying package
Checking MD5 at Wed Jun 22 01:19:21 2016
MD5 checksum OK
Checking HW platform at Wed Jun 22 01:19:22 2016
Checking SW platform at Wed Jun 22 01:19:23 2016
Package verified successfully
Sending patch file to plugin manager at Wed Jun 22 01:19:23 2016
The following package is now available to be activated: nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.15.1.lib32_n9000.rpm
Install operation 1 completed successfully at Wed Jun 22 01:19:24 2016
-------------------------------------------------------------
Install operation 2 by user 'admin' at Wed Jun 22 01:19:29 2016
Install activate nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.15.1.lib32_n9000.rpm
Install activate action started
The software will be activated with process restart
```
This example shows the output after an SMU package has been activated but before the switch has been reloaded:

```
switch# show install log detail
Install operation 18 by user 'admin' at Wed Jun 22 00:42:10 2016
Install activate nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.15.1.1lib32_n9000.rpm
Install activate action started
The software will be activated with system reload
Install operation 18 !!WARNING!! This patch will get activated only after a reload of the switch. at Wed Jun 22 00:42:12 2016
```

**Performing a Software Maintenance Upgrade for Guest Shell Bash**

You can perform a software maintenance upgrade for Bash in the Guest Shell.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Download the SMU package file for Guest Shell Bash from Cisco.com.</td>
<td>Obtains the package file from Cisco.com. For instructions, see Downloading the SMU Package File from Cisco.com, on page 345.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>--------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td>Copy the SMU package file to the bootflash: of the switch.</td>
<td>Copies the package file to the device. For instructions, see Copying the Package File to a Local Storage Device or Network Server, on page 345.</td>
</tr>
</tbody>
</table>

**Step 3**

**Example:**

```bash
switch# guestshell
guestshell:~$
```

Accesses the Guest Shell.

**Step 4**

**Example:**

```bash
guestshell:~$ sudo rpm -Uvh /bootflash/filename
```

Upgrades the existing Bash file in the Guest Shell.

**Step 5**

**Example:**

```bash
guestshell:~$ rpm -qa | grep bash
bash-4.2-r8.x86_64
```

Verifies that the new version of the Bash file was installed successfully.

**Step 6**

**Example:**

```bash
switch# guestshell sync
```

On a dual-supervisors system, synchronizes the rootfs with the Bash SMU version to the standby supervisor before doing a switchover. If you do not run this command, you will need to repeat this procedure after a supervisor switchover.

**Note**

The new Bash file is preserved after a Guest Shell reboot or Guest Shell disable+enable. However, you need to reinstall the Guest Shell Bash SMU package file after a Guest Shell destroy+enable.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>virtual service 'guestshell+'</td>
<td>Successfully activated virtual service 'guestshell+'</td>
</tr>
</tbody>
</table>

**Additional References**

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software upgrades</td>
<td><em>Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide</em></td>
</tr>
</tbody>
</table>

**SMU History**

This table lists the release history for SMU package files.

<table>
<thead>
<tr>
<th>SMU Package File</th>
<th>Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bash-4.2-r8.x86_64.rpm</td>
<td>6.1(2)I3(1)</td>
<td>Guest Shell Bash SMU for Bash vulnerabilities CVE-2014-6277, CVE-2014-6278, CVE-2014-7186, and CVE-2014-7187</td>
</tr>
<tr>
<td>n9000-dk9.6.1.2.I3.1.CSCur02700.bin</td>
<td>6.1(2)I3(1) and all 6.1(2)I2(x) releases</td>
<td>Cisco NX-OS SMU for CSCur02700 (Bash vulnerabilities CVE-2014-6277, CVE-2014-6278, CVE-2014-7186, and CVE-2014-7187)</td>
</tr>
<tr>
<td>n9000-dk9.6.1.2.I2.1.CSCup81353.bin</td>
<td>6.1(2)I2(1), 6.1(2)I2(2), 6.1(2)I2(2a), and 6.1(2)I2(3)</td>
<td>Cisco NX-OS SMU for CSCup81353</td>
</tr>
</tbody>
</table>
Performing Configuration Replace

This chapter includes the following sections:

• About Configuration Replace and Commit-timeout, on page 361
• Overview, on page 361
• Guidelines and Limitations for Configuration Replace, on page 363
• Recommended Workflow for Configuration Replace, on page 365
• Performing a Configuration Replace, on page 365
• Verifying Configuration Replace, on page 365
• Examples for Configuration Replace, on page 365

About Configuration Replace and Commit-timeout

The configuration replace feature enables you to replace the running configuration of the Cisco Nexus switch with the user provided configuration without reloading the device. The device reload may be required only when a configuration itself requires a reload. The running configuration file that is provided by the user should be taken using copy running file. Unlike copy file: to running, the configuration replace feature is not a merge operation. This feature replaces the entire running configuration with a new configuration that is provided by the user. If there is a failure in the configuration replace, the original configuration is restored in the switch. From Cisco NX-OS Release 9.3(1), best-effort option is introduced. This option enables the configuration replace to execute the full patch despite any error in the commands and the original configuration is not restored in the switch.

The commit-timeout feature enables you to rollback to the previous configuration after successfully performing the configuration replace operation. If the commit timer expires, the rollback operation is automatically initiated.

Note

• You must provide a valid running configuration that has been received with the Cisco NX-OS device. It should not be a partial configuration.

Overview

The configuration replace feature has the following operation steps:
• Configuration replace intelligently calculates the difference between the current running-configuration and the user-provided configuration in the Cisco Nexus switch and generates a patch file which is the difference between the two files. You can view this patch file which includes a set of configuration commands.

• Configuration replace applies the configuration commands from the patch file similarly to executing commands.

• The configuration rolls back to or restores the previous running configuration under the following situations:
  • If there is a mismatch in the configuration after the patch file has been applied.
  • If you perform the configuration operation with a commit timeout and the commit timer expires.

• The configuration does not roll back to or does not restore the previous running configuration when the best-effort option is used. This option enables the configuration replace to execute the full patch despite any error in the commands and will not roll back to the previous configuration.

• You can view the exact configuration that caused a failure using the `show config-replace log exec` command.

• Restore operations that fail while restoring the switch to the original configuration, are not interrupted. The restore operation continues with the remaining configuration. Use the `show config-replace log exec` command to list the commands that failed during the restore operation.

• If you enter the `configure replace commit` command before the timer expires, the commit timer stops and the switch runs on the user provided configuration that has been applied through the configuration replace feature.

• If the commit timer expires, roll back to the previous configuration is initiated automatically.

• In Cisco NX-OS Release 9.3(1), semantic validation support is added for the configuration replace. This semantic validation is done as part of the precheck in configuration replace. The patch gets applied only when the semantic validation is successful. After applying the patch file, configuration replace triggers the verification process. The configuration replace compares the running-configuration with the user configuration file during the verification process. If there is a mismatch, it restores the device to the original configuration.

The differences between configuration replace and copying a file to the running-configuration are as follows:

<table>
<thead>
<tr>
<th>Configuration Replace</th>
<th>Copying a file</th>
</tr>
</thead>
<tbody>
<tr>
<td>The <code>configure replace &lt;target-url&gt;</code> command removes the commands from the current running-configuration that are not present in the replacement file. It also adds commands that need to be added to the current running-configuration.</td>
<td>The <code>copy &lt;source-url&gt; running-config</code> command is a merge operation which preserves all the commands from, both the source file and the current running-configuration. This command does not remove the commands from the current running-configuration that are not present in the source file.</td>
</tr>
<tr>
<td>You must use a complete Cisco NX-OS configuration file as the replacement file for the <code>configure replace &lt;target-url&gt;</code> command.</td>
<td>You can use a partial configuration file as a source file for the <code>copy &lt;source-url&gt; running-config</code> command.</td>
</tr>
</tbody>
</table>
Benefits of Configuration Replace

The benefits of configuration replace are:

- You can replace the current running-configuration file with the user-provided configuration file without having to reload the switch or manually undo CLI changes to the running-configuration file. As a result, the system downtime is reduced.

- You can revert to the saved Cisco NX-OS configuration state.

- It simplifies the configuration changes by allowing you to apply a complete configuration file to the device, where only the commands that need to be added or removed are affected. The other service and configurations that are not modified remain untouched.

- If you configure the commit-timeout feature, you can rollback to the previous configuration even when the configuration replace operation has been successful.

Guidelines and Limitations for Configuration Replace

The configuration replace feature has the following configuration guidelines and limitations:

- The configuration replace feature is supported on Cisco Nexus 3000 Series and Cisco Nexus 9000 Series switches.

- Only one user can perform the configuration replace, checkpoint, and rollback operations, or copy the running-configuration to the startup configuration at the same time. Parallel operations such as operations via multiple Telnet/SSH or NX-API sessions are not supported. The multiple configuration replace or rollback request is serialized, for example, only after the first request is completed, processing of the second request begins.

- You are not allowed to initiate another configuration replace operation when the commit timer is running. You must either stop the timer by using the `configure replace commit` command or wait until the commit timer expires before you initiate another configuration replace operation.

- The commit-timeout feature is initiated only if you perform the configuration replace operation with the commit-timeout. The timer value range is between 30-3600 seconds.

- The user provided configuration file must be the valid show running-configuration output that is taken from the Cisco NX-OS device (copy run file). This cannot be a partial configuration and should include mandated commands, such as user admin and so on.

- We do not recommend a configuration replace operation performed on the configuration file that is generated across the software version because this operation could fail. A new configuration file must be regenerated whenever there is change in the software version.

- The configuration replace operation is not supported if you attempt to replace a multichassis EtherChannel trunk (MCT) configuration with a virtual peer-link configuration. This operation is not allowed because the physical MCT uses the CFS distribution over Ethernet mode and the virtual peer-link use the CFS distribution over IP mode.

- We recommend that you do not change any configuration from others sessions if the configuration replace operation is in progress because it could cause the operation to fail.

- Note the following about the configuration replace feature:
• The configuration replace feature is not supported on switches that include FEX line cards.

• The configuration replace feature is not supported on Cisco Nexus 9500 platform switches with -R line cards.

• The configuration replace feature is not supported on port profiles that are inherited on the switch interfaces.

• The configuration replace feature is not supported on the hardware profile portmode feature on Cisco Nexus C92160YC-X (N9K-C92160YC-X) and Cisco Nexus -C93180LC-EX (N9K-C93180LC-EX) switches.

• The configuration replace feature is supported only for the configure terminal mode commands. The configure profile, configure jobs, and any other modes are not supported.

• The configuration replace feature is not supported for breakout interface configurations.

• The configuration replace feature could fail if the running configuration includes the feature-set mpls or the mpls static range commands and tries to move to a configuration without MPLS or modifies the label range.

• The configuration replace feature does not support auto configurations.

• If the line card to which the configuration replace feature is applied is offline, the configuration replace operation fails.

• Entering maintenance mode from user configuration is not supported.

• Using the configure replace command from maintenance mode asks for a user-confirmation with following warning:

  Warning: System is in maintenance mode. Please ensure user config won't inadvertently revert back config in maintenance mode profile.
  Do you wish to proceed anyway? (y/n) [n]

• Using the configure replace command from maintenance mode with a <non-interactive> option is supported. It takes the yes user-confirmation by default and proceeds.

• If your configurations demand reloading the Cisco NX-OS device in order to apply the configuration, then you must reload these configurations after the configuration replace operation.

• The order of the commands in the user provided configuration file must be the same as that in the running configuration of the Cisco Nexus switch.

• The user configuration file to which you need to replace the running configuration on the switch using CR should be generated from the running-config of the switch after configuring the new commands. The user configuration file should not be manually edited with the CLI commands and the sequence of the configuration commands should not be altered.

• The semantic validation is not supported in 4-Gig memory platforms.

• When different versions of a feature are present in the running configuration and user configuration (for example: VRRPv2 and VRRPv3), semantic validation option does not work as expected. This is a known limitation.
Recommended Workflow for Configuration Replace

The following workflow is the recommended workflow for configuration replace:

Performing a Configuration Replace

To perform configuration replace, do the following:

Verifying Configuration Replace

To check and verify configuration replace and its status, use the commands that are outlined in the table:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure replace [bootflash/scp/sftp]&lt;user-configuration-file&gt; show-patch</td>
<td>Displays the difference between the running-configurations and user-provided configurations.</td>
</tr>
<tr>
<td>show config-replace log exec</td>
<td>Displays a log of all the configurations executed and those that failed. In case of an error, it displays an error message against that configuration.</td>
</tr>
<tr>
<td>show config-replace log verify</td>
<td>Displays the configurations that failed, along with an error message. It does not display configurations that were successful.</td>
</tr>
<tr>
<td>show config-replace status</td>
<td>Displays the status of the configuration replace operations, including in-progress, successful, and failure. If you have configured the commit-timeout feature, the commit and timer status and the commit timeout time remaining is also displayed.</td>
</tr>
</tbody>
</table>

Examples for Configuration Replace

See the following configuration examples for configuration replace:

- Use the `configure replace bootflash: <file> show-patch` CLI command to display the difference between the running-configurations and user-provided configurations.

```
switch(config)# configure replace bootflash:<file> show-patch
Collecting Running-Config
Converting to checkpoint file
#Generating Rollback Patch
!!
no role name abc
```
• Use the `configure replace bootflash: <file> verbose` CLI command to replace the entire running-configuration in the switch with the user-configuration.

```
switch(config)# configure replace bootflash:<file> verbose
Collecting Running-Config
Generating Rollback patch for switch profile
Rollback Patch is Empty
Note: Applying config parallelly may fail Rollback verification
Collecting Running-Config
#Generating Rollback Patch
Executing Rollback Patch

========================================================
config t
no role name abc

Generating Running-config for verification
Generating Patch for verification

Rollback completed successfully.
```

Sample Example with adding of BGP configurations.
```
switch(config)# sh run | section bgp
switch(config)# sh file bootflash:file | section bgp
feature bgp
router bgp 1
  address-family ipv4 unicast
  neighbor 1.1.1.1
switch(config)#
switch(config)# configure replace bootflash:file verbose
Collecting Running-Config
Generating Rollback patch for switch profile
Rollback Patch is Empty
Note: Applying config parallelly may fail Rollback verification
Collecting Running-Config
#Generating Rollback Patch
Executing Rollback Patch

========================================================
```
```
feature bgp
router bgp 1
  address-family ipv4 unicast
  neighbor 1.1.1.1
```
```
Generating Running-config for verification
Generating Patch for verification

Rollback completed successfully.
```
```
switch(config)# sh run | section bgp
feature bgp
router bgp 1
  address-family ipv4 unicast
  neighbor 1.1.1.1
```
```
Sample Example with ACL
switch(config)# configure replace bootflash:run_1.txt
Collecting Running-Config
Generating Rollback patch for switch profile
Rollback Patch is Empty
Note: Applying config parallelly may fail Rollback verification
Collecting Running-Config
#Generating Rollback Patch
Executing Rollback Patch

 Generating Running-config for verification
Generating Patch for verification

Rollback completed successfully.
```
```
switch(config)# sh run | section bgp
feature bgp
router bgp 1
  address-family ipv4 unicast
  neighbor 1.1.1.1
```
```
Sample Example with ACL
switch(config)# configure replace bootflash:run_1.txt
Collecting Running-Config
Generating Rollback patch for switch profile
Rollback Patch is Empty
Note: Applying config parallelly may fail Rollback verification
Collecting Running-Config
#Generating Rollback Patch
Executing Rollback Patch

 Generating Running-config for verification
Generating Patch for verification

Rollback completed successfully.
```
```
switch(config)# sh run | section bgp
feature bgp
router bgp 1
  address-family ipv4 unicast
  neighbor 1.1.1.1
```
config t
no ip access-list nexus-50-new-xyz
ip access-list nexus-50-new-xyz-jkl-abc
10 remark Newark
20 permit ip 17.31.5.0/28 any
30 permit ip 17.34.146.193/32 any
40 permit ip 17.128.199.0/27 any
50 permit ip 17.150.128.0/22 any

Generating Running-config for verification
Generating Patch for verification
Rollback completed successfully.

switch(config)#

switch(config)# show run aclmgr | sec nexus-50-new-xyz-jkl-abc
ip access-list nexus-50-new-xyz-jkl-abc
10 remark Newark
20 permit ip 17.31.5.0/28 any
30 permit ip 17.34.146.193/32 any
40 permit ip 17.128.199.0/27 any
50 permit ip 17.150.128.0/22 any

• Use the configure replace bootflash:user-config.cfg verify-only CLI command to generate and verify the patch semantically.

switch(config)# configure replace bootflash:user-config.cfg verify-only

Version match between user file and running configuration.
Pre-check for User config PASSED
Collecting Running-Config
Converting to checkpoint file
Generating Rollback Patch
Validating Patch

'config t'
'interface Ethernet1/1'
'shutdown'
'no switchport trunk allowed vlan'
'no switchport mode'
'no switchport'
'exit'
Skip non dme command for CR validation
'interface Vlan1'
'shutdown'
'interface Ethernet1/1'
'shutdown'
'no switchport'
'ip address 1.1.1.1/24'
'exit'
Skip non dme command for CR validation

Patch validation completed successful
switch(config)#

• Use the configure replace bootflash:user-config.cfg best-effort verify-and-commit CLI command to replace the switch running configuration with the given user configuration after performing the semantic validation on patch.

switch(config)# configure replace bootflash:user-config.cfg best-effort verify-and-commit
Performing Configuration Replace

Version match between user file and running configuration.
Pre-check for User config PASSED
ADVISORY: Config Replace operation started...
Modifying running configuration from another VSH terminal in parallel
is not recommended, as this may lead to Config Replace failure.

Collecting Running-Config
Generating Rollback patch for switch profile
Rollback Patch is Empty
Collecting Running-Config
Generating Rollback Patch

Validating Patch
Patch validation completed successful
Executing Rollback Patch
During CR operation, will retain L3 configuration
when vrf member change on interface
Generating Running-config for verification
Generating Rollback Patch

Configure replace completed successfully. Please run 'show config-replace log exec' to
see if there is any configuration that requires reload to take effect.

switch(config)#

• Use the show config-replace log exec CLI command to check all the configuration that is executed and
  failures if any.

switch(config)# show config-replace log exec
Operation : Rollback to Checkpoint File
Checkpoint file name : .replace_tmp_28081
Scheme : tmp
Rollback done By : admin
Rollback mode : atomic
Verbose : enabled
Start Time : Wed, 06:39:34 25 Jan 2017

--------------------------------------------------------------------------------
time: Wed, 06:39:47 25 Jan 2017
Status: SUCCESS
Rollback Status : Success

Executing Patch:
----------------
switch#config t
switch#no role name abc

• Use the show config-replace log verify CLI command to check the failed configuration if any.

switch(config)# show config-replace log verify
Operation : Rollback to Checkpoint File
Checkpoint file name : .replace_tmp_28081
Scheme : tmp
Rollback done By : admin
Rollback mode : atomic
Verbose : enabled
Start Time : Wed, 06:39:34 25 Jan 2017
Status : Success

Verification patch contains the following commands:
---------------------------------------------------
!!
! No changes
* Use the `show config-replace status` CLI command to check the status of configuration replace.

```bash
switch(config)# show config-replace status
Last operation : Rollback to file
Details:
  Rollback type: atomic replace_tmp_28081
  Operation Status: Success
switch(config)#
```
CHAPTER 25

Configuring Rollback

This chapter describes how to configure rollback on Cisco NX-OS devices.

This chapter contains the following sections:

• About Rollbacks, on page 371
• Licensing Requirements for Rollbacks, on page 373
• Prerequisites for Rollbacks, on page 373
• Guidelines and Limitations for Rollbacks, on page 373
• Default Settings for Rollbacks, on page 374
• Configuring Rollbacks, on page 374
• Verifying the Rollback Configuration, on page 375
• Configuration Example for Rollback, on page 376
• Additional References, on page 376

About Rollbacks

A rollback allows you to take a snapshot, or user checkpoint, of the Cisco NX-OS configuration and then reapply that configuration to your device at any point without having to reload the device. A rollback allows any authorized administrator to apply this checkpoint configuration without requiring expert knowledge of the features configured in the checkpoint.

Cisco NX-OS automatically creates system checkpoints. You can use either a user or system checkpoint to perform a rollback.

You can create a checkpoint copy of the current running configuration at any time. Cisco NX-OS saves this checkpoint as an ASCII file which you can use to roll back the running configuration to the checkpoint configuration at a future time. You can create multiple checkpoints to save different versions of your running configuration.

When you roll back the running configuration, you can trigger the following rollback types:

• atomic—Implement a rollback only if no errors occur.
• best-effort—Implement a rollback and skip any errors.
• stop-at-first-failure—Implement a rollback that stops if an error occurs.

The default rollback type is atomic.

When you are ready to roll back to a checkpoint configuration, you can view the changes that will be applied to your current running configuration before committing to the rollback operation. If an error occurs during
the rollback operation, you can choose to cancel the operation, or ignore the error and proceed with the rollback. If you cancel the operation, Cisco NX-OS provides a list of changes already applied before the error occurred. You need to clean up these changes manually.

Automatically Generated System Checkpoints

The Cisco NX-OS software automatically generates system checkpoints to help you avoid a loss of configuration information. System checkpoints are generated by the following events:

- Disabling an enabled feature with the `no feature` command
- Removing an instance of a Layer 3 protocol, such as with the `no router bgp` command or the `no ip pim sparse-mode` command
- License expiration of a feature

If one of these events causes system configuration changes, the feature software creates a system checkpoint that you can use to roll back to the previous system configuration. The system generated checkpoint filenames begin with “system-” and include the feature name. For example, the first time that you disable the EIGRP feature, the system creates the checkpoint named `system-fm-__inst_1__eigrp`.

High Availability

Whenever a checkpoint is created using the `checkpoint` or `checkpoint checkpoint_name` commands, the checkpoint is synchronized to the standby unit.

A rollback remembers the states of the checkpoint operation, so if the checkpoint operation is interrupted and the system is left in an inconsistent state, a rollback can complete the checkpoint operation (synchronize the checkpoint with the standby unit) before proceeding with the rollback operation.

Your checkpoint files are still available after a process restart or supervisor switchover. Even if there is an interruption during the process restart or supervisor switchover, the checkpoint will complete successfully before proceeding with the operation. In a supervisor switchover, the checkpoint is completed on the new active unit.

If a process restart or supervisor switchover occurs during a rollback operation, after the restart or switchover completes, the rollback will resume from its previous state and complete successfully.

Virtualization Support

Cisco NX-OS creates a checkpoint of the running configuration. You can create different checkpoint copies.
Licensing Requirements for Rollbacks

<table>
<thead>
<tr>
<th>Product</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco NX-OS</td>
<td>The rollback feature requires no license. Any feature not included in a license package is bundled with the nx-os image and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the Cisco NX-OS Licensing Guide.</td>
</tr>
</tbody>
</table>

Prerequisites for Rollbacks

To configure rollback, you must have network-admin user privileges.

Guidelines and Limitations for Rollbacks

Rollbacks have the following configuration guidelines and limitations:

- You can create up to ten checkpoint copies.
- Your checkpoint filenames must be 80 characters or less.
- You cannot start a checkpoint filename with the word system.
- You can start a checkpoint filename with the word auto.
- You can name a checkpoint file summary or any abbreviation of the word summary.
- Only one user can perform a checkpoint, rollback, or copy the running configuration to the startup configuration at the same time.
- After the system executes the write erase or reload command, checkpoints are deleted. You can use the clear checkpoint database command to clear out all checkpoint files.
- Although a rollback is not supported for checkpoints across software versions, users can perform a rollback at their own discretion and can use the best-effort mode to recover from errors.
- When checkpoints are created on bootflash, differences with the running-system configuration cannot be performed before performing the rollback, and the system reports “No Changes.”
- Checkpoints created using the checkpoint and checkpoint checkpoint_name commands are present upon a switchover.
- Checkpoints are present upon reload unless a write-erase command is issued before a reload.
- A rollback to files on bootflash is supported only on files that are created using the checkpoint checkpoint_name command and not on any other type of ASCII file.
- Checkpoint names must be unique. You cannot overwrite previously saved checkpoints with the same name.
• Rollback is not supported in the context of auto configurations. Checkpoints do not store auto configurations. Therefore, after a rollback is performed, the corresponding auto configurations will not be present.

• Multiple port VLAN mappings configured on an interface during a rollback operation cause the rollback feature to fail.

**Default Settings for Rollbacks**

This table lists the default settings for rollback parameters.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rollback type</td>
<td>Atomic</td>
</tr>
</tbody>
</table>

**Configuring Rollbacks**

Be aware that the Cisco NX-OS commands may differ from the Cisco IOS commands.

**Creating a Checkpoint**

You can create up to ten checkpoints of your configuration.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Creates a checkpoint of the running configuration to either a user checkpoint name or a file. The checkpoint name can be any alphanumeric string up to 80 characters but cannot contain spaces. If you do not provide a name, Cisco NX-OS sets the checkpoint name to user-checkpoint-number where number is from 1 to 10. The description can contain up to 80 alphanumeric characters, including spaces. You can use the no form of the checkpoint command to remove a checkpoint name. Use the delete command to remove a checkpoint file.</td>
</tr>
<tr>
<td>[no] checkpoint {{cp-name} [description descr]</td>
<td>[file file-name] }</td>
</tr>
<tr>
<td>Example:</td>
<td>switch# checkpoint stable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Displays the contents of the checkpoint name.</td>
</tr>
<tr>
<td>(Optional) show checkpoint cp-name [all]</td>
<td></td>
</tr>
</tbody>
</table>
Implementing a Rollback

You can implement a rollback to a checkpoint name or file. Before you implement a rollback, you can view the differences between source and destination checkpoints that reference current or saved configurations.

If you make a configuration change during an atomic rollback, the rollback will fail.

Note

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> show diff rollback-patch {checkpoint src-cp-name</td>
<td>running-config</td>
</tr>
<tr>
<td>Example: switch# show diff rollback-patch checkpoint stable running-config</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> rollback running-config {checkpoint cp-name</td>
<td>file cp-file} {atomic</td>
</tr>
<tr>
<td>Example: switch# rollback running-config checkpoint stable</td>
<td></td>
</tr>
</tbody>
</table>

Verifying the Rollback Configuration

To display the rollback configuration information, perform one of the following tasks:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show checkpoint name [all]</td>
<td>Displays the contents of the checkpoint name.</td>
</tr>
</tbody>
</table>
### Command

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`show checkpoint all [user</td>
<td>system]`</td>
</tr>
<tr>
<td>`show checkpoint summary [user</td>
<td>system]`</td>
</tr>
<tr>
<td>`show diff rollback-patch [checkpoint src-cp-name</td>
<td>running-config</td>
</tr>
<tr>
<td>`show rollback log [exec</td>
<td>verify]`</td>
</tr>
</tbody>
</table>

Use the `clear checkpoint database` command to delete all checkpoint files.

### Configuration Example for Rollback

This example shows how to create a checkpoint file and then implements a best-effort rollback to a user checkpoint name:

```
checkpoint stable
rollback running-config checkpoint stable best-effort
```

### Additional References

#### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration files</td>
<td><em>Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide</em></td>
</tr>
</tbody>
</table>
IETF RFCs supported by Cisco NX-OS System Management

This appendix lists the IETF RFCs for system management supported in Cisco NX-OS.

- IETF RFCs Supported by Cisco NX-OS System Management, on page 377

IETF RFCs Supported by Cisco NX-OS System Management

This appendix lists the IETF RFCs for system management supported in Cisco NX-OS.

<table>
<thead>
<tr>
<th>RFCs</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 2579</td>
<td>Textual Conventions for SMIv2</td>
</tr>
<tr>
<td>RFC 2819</td>
<td>Remote Network Monitoring Management Information Base</td>
</tr>
<tr>
<td>RFC 2863</td>
<td>The Interfaces Group MIB</td>
</tr>
<tr>
<td>RFC 3176</td>
<td>InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks</td>
</tr>
<tr>
<td>RFC 3413</td>
<td>Simple Network Management Protocol (SNMP) Applications</td>
</tr>
<tr>
<td>RFC 3417</td>
<td>Transport Mappings for the Simple Network Management Protocol (SNMP)</td>
</tr>
</tbody>
</table>
Embedded Event Manager System Events and Configuration Examples

This appendix describes the Embedded Event Manager (EEM) system policies, events, and policy configuration examples.

This appendix includes the following sections:

- EEM System Policies, on page 379
- EEM Events, on page 381
- Configuration Examples for EEM Policies, on page 382

### EEM System Policies

The following table lists the Embedded Event Manager (EEM) system policies.

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>__PortLoopback</td>
<td>Do CallHome, log error in Syslog/OBFL/Exception Log, and disable further HM testing on affected ports after 10 consecutive failures of GOLD &quot;PortLoopback&quot; test</td>
</tr>
<tr>
<td>__RewriteEngineLoopback</td>
<td>Do CallHome, log error in Syslog/OBFL/Exception Log, and disable further HM testing on affected ports after 10 consecutive failures of GOLD &quot;RewriteEngine&quot; test</td>
</tr>
<tr>
<td>__asic_register_check</td>
<td>Do CallHome, log error, and disable further HM testing for that ASIC device/instance after 20 consecutive failures of GOLD &quot;ASICRegisterCheck&quot; test</td>
</tr>
<tr>
<td>__compact_flash</td>
<td>Do CallHome, log error, and disable further HM testing after 20 consecutive failures of GOLD &quot;CompactFlash&quot; test</td>
</tr>
<tr>
<td>__crypto_device</td>
<td>Do CallHome and log error when GOLD &quot;CryptoDevice&quot; test fails</td>
</tr>
<tr>
<td>Event</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>__eobc_port_loopback</td>
<td>Do CallHome and log error when GOLD &quot;EOBCPortLoopback&quot; test fails</td>
</tr>
<tr>
<td>__ethpm_debug_1</td>
<td>Action: none</td>
</tr>
<tr>
<td>__ethpm_debug_2</td>
<td>Action: none</td>
</tr>
<tr>
<td>__ethpm_debug_3</td>
<td>Action: none</td>
</tr>
<tr>
<td>__ethpm_debug_4</td>
<td>Action: none</td>
</tr>
<tr>
<td>__ethpm_link_flap</td>
<td>More than 30 link flaps in a 420-second interval. Action: Error. Disable the port</td>
</tr>
<tr>
<td>__external_compact_flash</td>
<td>Do CallHome, log error, and disable further HM testing after 20 consecutive failures of GOLD &quot;ExternalCompactFlash&quot; test</td>
</tr>
<tr>
<td>__lcm_module_failure</td>
<td>Power cycle two times and then power down</td>
</tr>
<tr>
<td>__management_port_loopback</td>
<td>Do CallHome and log error when GOLD &quot;ManagementPortLoopback&quot; test fails</td>
</tr>
<tr>
<td>__nvram</td>
<td>Do CallHome, log error, and disable further HM testing after 20 consecutive failures of GOLD &quot;NVRAM&quot; test</td>
</tr>
<tr>
<td>__pfm_fanabsent_all_systemfan</td>
<td>Shuts down if both fan trays (f1 and f2) are absent for 2 minutes</td>
</tr>
<tr>
<td>__pfm_fanbad_all_systemfan</td>
<td>Syslog when fan goes bad</td>
</tr>
<tr>
<td>__pfm_fanbad_any_singlefan</td>
<td>Syslog when fan goes bad</td>
</tr>
<tr>
<td>__pfm_power_over_budget</td>
<td>Syslog warning for insufficient power overbudget</td>
</tr>
<tr>
<td>__pfm_tempev_major</td>
<td>TempSensor Major Threshold. Action: Shutdown</td>
</tr>
<tr>
<td>__pfm_tempev_minor</td>
<td>TempSensor Minor Threshold. Action: Syslog</td>
</tr>
<tr>
<td>__primary_bootrom</td>
<td>Do CallHome, log error, and disable further HM testing after 20 consecutive failures of GOLD &quot;PrimaryBootROM&quot; test</td>
</tr>
<tr>
<td>__pwr_mgmt_bus</td>
<td>Do CallHome, log error, and disable further HM testing for the module or spine-card after 20 consecutive failures of GOLD &quot;PwrMgmtBus&quot; test</td>
</tr>
<tr>
<td>__real_time_clock</td>
<td>Do CallHome, log error, and disable further HM testing after 20 consecutive failures of GOLD &quot;RealTimeClock&quot; test</td>
</tr>
</tbody>
</table>
EEM Events

The following table describes the EEM events you can use on the device.

<table>
<thead>
<tr>
<th>EEM Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>application</td>
<td>Publishes an application-specific event.</td>
</tr>
<tr>
<td>cli</td>
<td>CLI command is entered that matches a pattern with a wildcard.</td>
</tr>
<tr>
<td>counter</td>
<td>EEM counter reaches a specified value or range.</td>
</tr>
<tr>
<td>fanabsent</td>
<td>System fan tray is absent.</td>
</tr>
<tr>
<td>fanbad</td>
<td>System fan generates a fault.</td>
</tr>
<tr>
<td>fib</td>
<td>Monitors routes or TCAM usage in the unicast FIB.</td>
</tr>
<tr>
<td>gold</td>
<td>GOLD test failure condition is hit.</td>
</tr>
<tr>
<td>interface</td>
<td>Interface counter exceeds a threshold.</td>
</tr>
<tr>
<td>memory</td>
<td>Available system memory exceeds a threshold.</td>
</tr>
<tr>
<td>module</td>
<td>Specified module enters the selected status.</td>
</tr>
<tr>
<td>module-failure</td>
<td>Module failure is generated.</td>
</tr>
</tbody>
</table>

---

**Event**

<table>
<thead>
<tr>
<th>EEM Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>secondary_bootrom</td>
<td>Do CallHome, log error, and disable further HM testing after 20 consecutive failures of GOLD &quot;SecondaryBootROM&quot; test</td>
</tr>
<tr>
<td>spine_control_bus</td>
<td>Do CallHome, log error, and disable further HM testing for that module or spine-card after 20 consecutive failures of GOLD &quot;SpineControlBus&quot; test</td>
</tr>
<tr>
<td>standby_fabric_loopback</td>
<td>Do CallHome, log error, and disable further HM testing after 10 consecutive failures</td>
</tr>
<tr>
<td>status_bus</td>
<td>Do CallHome, log error, and disable further HM testing after 5 consecutive failures of GOLD &quot;StatusBus&quot; test</td>
</tr>
<tr>
<td>system_mgmt_bus</td>
<td>Do Call Home, log error, and disable further HM testing for that fan or power supply after 20 consecutive failures of GOLD &quot;SystemMgmtBus&quot; test</td>
</tr>
<tr>
<td>usb</td>
<td>Do Call Home and log error when GOLD &quot;USB&quot; test fails</td>
</tr>
</tbody>
</table>
### EEM Event System Events

<table>
<thead>
<tr>
<th>EEM Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>Runs the policy event without any events specified.</td>
</tr>
<tr>
<td>oir</td>
<td>Online insertion or removal occurs.</td>
</tr>
<tr>
<td>policy-default</td>
<td>Default parameters and thresholds are used for the events in the system policy you override.</td>
</tr>
<tr>
<td>poweroverbudget</td>
<td>Platform software detects a power budget condition.</td>
</tr>
<tr>
<td>snmp</td>
<td>SNMP object ID (OID) state changes.</td>
</tr>
<tr>
<td>storm-control</td>
<td>Platform software detects an Ethernet packet storm condition.</td>
</tr>
<tr>
<td>syslog</td>
<td>Monitors syslog messages and invokes the policy based on the search string in the policy.</td>
</tr>
<tr>
<td>sysmgr</td>
<td>System manager generates an event.</td>
</tr>
<tr>
<td>temperature</td>
<td>Temperature level in the system exceeds a threshold.</td>
</tr>
<tr>
<td>timer</td>
<td>Specified time is reached.</td>
</tr>
<tr>
<td>track</td>
<td>Tracked object changes state.</td>
</tr>
</tbody>
</table>

---

## Configuration Examples for EEM Policies

### Configuration Examples for CLI Events

#### Monitoring Interface Shutdown

This example shows how to monitor an interface shutdown:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# event manager applet monitorShutdown
switch(config-applet)#
switch(config-applet)# description "Monitors interface shutdown."
switch(config-applet)# event cli match "conf t; interface *; shutdown"
switch(config-applet)# action 1.0 cli show interface e 3/1
switch(config)# copy running-config startup-config
```

---

**Note**

Outputs of `show` commands entered as part of EEM policy are archived in the logflash as text files with the "eem_archive_" prefix. To view the archived output, use the `show file logflash:eem_archive_n` command.
Monitoring Module Powerdown

This example shows how to monitor a module powerdown:

```plaintext
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# event manager applet monitorPoweroff
switch(config-applet)#
switch(config-applet)# description "Monitors module power down."
switch(config-applet)# event cli match "conf t; poweroff *"
switch(config-applet)# action 1.0 cli show module
switch(config)# copy running-config startup-config
```

Adding a Trigger to Initiate a Rollback

This example shows how to add a trigger to initiate a rollback:

```plaintext
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# event manager applet rollbackTrigger
switch(config-applet)#
switch(config-applet)# description "Rollback trigger."
switch(config-applet)# event cli match "rollback *"
switch(config-applet)# action 1.0 cli copy running-config bootflash:last_config
switch(config)# copy running-config startup-config
```

Configuration Examples to Override (Disable) Major Thresholds

Preventing a Shutdown When Reaching a Major Threshold

This example shows how to prevent a shutdown caused by reaching a major threshold:

```plaintext
switch# configure terminal
switch(config)# event manager applet myappletname override __pfm_tempev_major
switch(config)# end
```

This example shows how to revert to the default configuration:

```plaintext
switch# configure terminal
switch(config)# no event manager applet myappletname override __pfm_tempev_major
switch(config)# end
```

Disabling One Bad Sensor

This example shows how to disable only sensor 3 on module 2 when sensor 3 is malfunctioning (all other sensors are unaffected):

```plaintext
switch# configure terminal
switch(config)# event manager applet myappletname override __pfm_tempev_major
switch(config-applet)# event temperature module 2 sensor 3 threshold major
switch(config-applet)# end
```

This example shows how to revert to the default configuration:

```plaintext
switch# configure terminal
switch(config)# no event manager applet myappletname override __pfm_tempev_major
```
Disabling Multiple Bad Sensors

This example shows how to disable sensors 5, 6, and 7 on module 2 when these sensors are malfunctioning (all other sensors are unaffected):

```plaintext
switch# configure terminal
switch(config)# event manager applet myappletname override __pfm_tempev_major
switch(config-applet)# event temperature module 2 sensor 5 threshold major
switch(config-applet)# end
switch# configure terminal
switch(config)# event manager applet myappletname override __pfm_tempev_major
switch(config-applet)# event temperature module 2 sensor 6 threshold major
switch(config-applet)# end
switch# configure terminal
switch(config)# event manager applet myappletname override __pfm_tempev_major
switch(config-applet)# event temperature module 2 sensor 7 threshold major
switch(config-applet)# end
```

This example shows how to revert to the default configuration:

```plaintext
switch# configure terminal
switch(config)# no event manager applet myappletname override __pfm_tempev_major
switch(config)# end
```

Overriding (Disabling) an Entire Module

This example shows how to disable module 2 when it is malfunctioning:

```plaintext
switch# configure terminal
switch(config)# event manager applet myappletname override __pfm_tempev_major
switch(config-applet)# event temperature module 2 threshold major
switch(config-applet)# end
```

This example shows how to revert to the default configuration:

```plaintext
switch# configure terminal
switch(config)# no event manager applet myappletname override __pfm_tempev_major
switch(config)# end
```

Overriding (Disabling) Multiple Modules and Sensors

This example shows how to disable sensors 3, 4, and 7 on module 2 and all sensors on module 3 when they are malfunctioning:

```plaintext
switch# configure terminal
switch(config)# event manager applet myappletname override __pfm_tempev_major
switch(config-applet)# event temperature module 2 sensor 3 threshold major
switch(config-applet)# end
switch# configure terminal
switch(config)# event manager applet myappletname override __pfm_tempev_major
switch(config-applet)# event temperature module 2 sensor 4 threshold major
switch(config-applet)# end
switch# configure terminal
switch(config)# event manager applet myappletname override __pfm_tempev_major
switch(config-applet)# event temperature module 2 sensor 7 threshold major
```
Enabling One Sensor While Disabling All Remaining Sensors of All Modules

This example shows how to disable all sensors on all modules except sensor 4 on module 9:

```plaintext
switch(config-applet)# configure terminal
switch(config)# event manager applet myapplet1 override __pfm_tempev_major
switch(config-applet)# end

switch(config-applet)# configure terminal
switch(config)# event manager applet myapplet2 override __pfm_tempev_major
switch(config-applet)# event temperature module 9 sensor 4 threshold major
switch(config-applet)# action 2 policy-default
switch(config-applet)# end
```

Enabling Multiple Sensors While Disabling All Remaining Sensors of All Modules

This example shows how to disable all sensors on all modules except sensors 4, 6, and 7 on module 9:

```plaintext
switch(config-applet)# configure terminal
switch(config)# event manager applet myapplet1 override __pfm_tempev_major
switch(config-applet)# end

switch(config-applet)# configure terminal
switch(config)# event manager applet myapplet2 override __pfm_tempev_major
switch(config-applet)# event temperature module 9 sensor 4 threshold major
switch(config-applet)# action 2 policy-default
switch(config-applet)# end

switch(config-applet)# configure terminal
switch(config)# event manager applet myapplet3 override __pfm_tempev_major
switch(config-applet)# event temperature module 9 sensor 6 threshold major
switch(config-applet)# action 3 policy-default
switch(config-applet)# end

switch(config-applet)# configure terminal
switch(config)# event manager applet myapplet4 override __pfm_tempev_major
switch(config-applet)# event temperature module 9 sensor 7 threshold major
switch(config-applet)# action 4 policy-default
switch(config-applet)# end
```

Enabling All Sensors of One Module While Disabling All Sensors of the Remaining Modules

This example shows how to disable all sensors on all modules except all sensors on module 9:

```plaintext
switch(config-applet)# configure terminal
switch(config)# event manager applet myapplet1 override __pfm_tempev_major
switch(config-applet)# end

switch(config-applet)# configure terminal
switch(config)# event manager applet myapplet2 override __pfm_tempev_major
switch(config-applet)# event temperature module 9 threshold major
```

This examples show how to revert to the default configuration:

```plaintext
switch# configure terminal
switch(config)# no event manager applet myappletname override __pfm_tempev_major
switch(config)# end
```
Enabling a Combination of Sensors on Modules While Disabling All Sensors of the Remaining Modules

This example shows how to disable all sensors on all modules except sensors 3, 4, and 7 on module 2 and all sensors on module 3:

```
switch(config-applet)# event manager applet myapplet1 override __pfm_tempev_major
switch(config-applet)# end
```

```
switch(config-applet)# event temperature module 2 sensor 3 threshold major
switch(config-applet)# action 2 policy-default
switch(config-applet)# end
```

```
switch(config-applet)# event temperature module 2 sensor 4 threshold major
switch(config-applet)# action 3 policy-default
switch(config-applet)# end
```

```
switch(config-applet)# event temperature module 2 sensor 7 threshold major
switch(config-applet)# action 4 policy-default
switch(config-applet)# end
```

```
switch(config-applet)# event temperature module 3 threshold major
switch(config-applet)# action 5 policy-default
switch(config-applet)# end
```

Configuration Examples to Override (Disable) Shutdown for Fan Tray Removal

Overriding (Disabling) a Shutdown for Removal of One or More Fan Trays

This example shows how to disable a shutdown so that you can remove one or more (or all) fan trays:

```
switch(config-applet)# event manager applet myappletname override __pfm_fanabsent_any_singlefan
switch(config-applet)# end
```

This example shows how to revert to the default configuration:

```
switch(config-applet)# no event manager applet myappletname override __pfm_fanabsent_any_singlefan
switch(config-applet)# end
```

Overriding (Disabling) a Shutdown for Removal of a Specified Fan Tray

This example shows how to disable a shutdown so that you can remove a specified fan tray (fan tray 3):

```
switch(config-applet)# event manager applet myappletname override __pfm_fanabsent_any_singlefan
switch(config-applet)# event fanabsent fan 3 time 60
switch(config-applet)# end
```
This example shows how to revert to the default configuration:

```
switch# configure terminal
switch(config)# no event manager applet myappletname override __pfm_fanabsent_any_singlefan
switch(config)# end
```

**Overriding (Disabling) a Shutdown for Removal of Multiple Specified Fan Trays**

This example shows how to disable a shutdown so that you can remove multiple specified fan trays (fan trays 2, 3, and 4):

```
switch# configure terminal
switch(config)# event manager applet myapplet1 override __pfm_fanabsent_any_singlefan
switch(config-applet)# event fanabsent fan 2 time 60
switch(config-applet)# end
switch# configure terminal
switch(config)# event manager applet myapplet2 override __pfm_fanabsent_any_singlefan
switch(config-applet)# event fanabsent fan 3 time 60
switch(config-applet)# end
switch# configure terminal
switch(config)# event manager applet myapplet3 override __pfm_fanabsent_any_singlefan
switch(config-applet)# event fanabsent fan 4 time 60
switch(config-applet)# end
```

This example shows how to revert to the default configuration:

```
switch# configure terminal
switch(config)# no event manager applet myappletname override __pfm_fanabsent_any_singlefan
switch(config)# end
```

**Overriding (Disabling) a Shutdown for Removal of All Fan Trays Except One**

This example shows how to disable a shutdown so that you can remove all fan trays except one (fan tray 2):

```
switch# configure terminal
switch(config)# event manager applet myapplet1 override __pfm_fanabsent_any_singlefan
switch(config-applet)# end
switch# configure terminal
switch(config)# event manager applet myapplet2 override __pfm_fanabsent_any_singlefan
switch(config-applet)# event fanabsent fan 2 time 60
switch(config-applet)# action 2 policy-default
switch(config-applet)# end
```

**Overriding (Disabling) a Shutdown for Removal of Fan Trays Except for a Specified Set of Fan Trays**

This example shows how to disable a shutdown so that you can remove fans except for a specified set of fan trays (fan trays 2, 3, and 4):

```
switch# configure terminal
switch(config)# event manager applet myapplet1 override __pfm_fanabsent_any_singlefan
switch(config-applet)# end
switch(config)# event manager applet myapplet2 override __pfm_fanabsent_any_singlefan
switch(config-applet)# event fanabsent fan 2,3,4 time 60
switch(config-applet)# action 2 policy-default
switch(config-applet)# end
```
Overriding (Disabling) a Shutdown for Removal of All Fan Trays Except One from a Set of Fan Trays

This example shows how to disable a shutdown so that you can remove all fan trays except one from a set of fan trays (fan trays 2, 3, or 4):

```plaintext
switch# configure terminal
switch(config)# event manager applet myapplet1 override __pfm_fanabsent_any_singlefan
switch(config-applet)# end

switch# configure terminal
switch(config)# event manager applet myapplet2 override __pfm_fanabsent_any_singlefan
switch(config-applet)# event fanabsent fan 2 time 60
switch(config-applet)# action 2 policy-default
switch(config-applet)# end

switch# configure terminal
switch(config)# event manager applet myapplet3 override __pfm_fanabsent_any_singlefan
switch(config-applet)# event fanabsent fan 3 time 60
switch(config-applet)# action 3 policy-default
switch(config-applet)# end

switch# configure terminal
switch(config)# event manager applet myapplet4 override __pfm_fanabsent_any_singlefan
switch(config-applet)# event fanabsent fan 4 time 60
switch(config-applet)# action 4 policy-default
switch(config-applet)# end
```

Configuration Examples to Create a Supplemental Policy

Creating a Supplemental Policy for the Fan Tray Absent Event

This example shows how to create a supplemental policy using the `event fanabsent` command:

```plaintext
[no] event fanabsent [fan fan-tray-number] time time-interval
```

In addition to the default policy, this example shows how to execute the policy myappletname and action 3 if fan tray 1 is absent for 60 seconds:

```plaintext
switch# configure terminal
switch(config)# event manager applet myappletname
switch(config-applet)# event fanabsent fan 1 time 60
switch(config-applet)# action 3 cli "show env fan"
switch(config-applet)# end
```

Creating a Supplemental Policy for the Temperature Threshold Event

This example shows how to create a supplemental policy using the `event temperature` command:

```plaintext
[no] event temperature [mod module-number] [sensor sensor-number] threshold {major | minor | any}
```

In addition to the default policy, this example shows how to execute the policy myappletname and action 1 if the temperature crosses the minor threshold on sensor 3 of module 2:

```plaintext
switch# configure terminal
switch(config)# event manager applet myappletname
switch(config-applet)# event temperature module 2 sensor 3 threshold minor
switch(config-applet)# action 1 cli "show environ temperature"
switch(config-applet)# end
```
Configuration Examples for the Power Over-Budget Policy

The power over-budget policy gets triggered when the available power capacity drops below zero and the device is no longer able to keep the previously powered-up modules in the powered-up state. The default action is to print a syslog to notify the user of the occurrence of power over budget.

You can enable an additional action to power down modules until the available power recovers from the red (negative) zone.

### Shutting Down Modules

If you do not specify any modules, the power over-budget shutdown starts from slot 1 and shuts down modules until the power recovers from the red (negative) zone. Empty slots and slots that contain a supervisor, standby supervisor, spine, or crossbar are skipped.

This example shows how to shut down modules starting from module 1 when the available power drops below zero:

```
switch# configure terminal
switch(config)# event manager applet <myappletname4a> override __pfm_power_over_budget
switch(config-applet)# event poweroverbudget
switch(config-applet)# action 4 overbudgetshut
switch(config-applet)# end
```

### Shutting Down a Specified List of Modules

You can specify a list of modules that the power over-budget action uses to shut down modules until the power recovers from the red (negative) zone. Empty slots and slots that contain a supervisor, standby supervisor, spine, or crossbar are skipped.

This example shows how to shut down modules from a specified list of modules (1, 2, 7, 8) when the available power drops below zero:

```
switch# configure terminal
switch(config)# event manager applet <myappletname4b> override __pfm_power_over_budget
switch(config-applet)# event poweroverbudget
switch(config-applet)# action 5 overbudgetshut module 1,2,7,8
switch(config-applet)# end
```

### Configuration Examples to Select Modules to Shut Down

#### Using the Policy Default to Select Nonoverridden Modules to Shut Down

This example shows how to use the policy default to select the nonoverridden modules to shut down when a major threshold is exceeded:

```
switch# configure terminal
switch(config)# event manager applet my5al override __pfm_tempev_major
switch(config-applet)# end
switch# configure terminal
switch(config)# event manager applet my5a2 override __pfm_tempev_major
switch(config-applet)# event temperature module 1-3 sensor 4 threshold major
switch(config-applet)# action 5 policy-default
switch(config-applet)# end
```
Using Parameter Substitution to Select Nonoverridden Modules to Shut Down

This example shows how to use parameter substitution to select the nonoverridden modules to shut down when a major threshold is exceeded:

```
switch# configure terminal
switch(config)# event manager applet my5b1 override __pfm_tempev_major
switch(config-applet)# end
switch# configure terminal
switch(config)# event manager applet my5b2 override __pfm_tempev_major
switch(config-applet)# event temperature module 1-3 sensor 8 threshold major
switch(config-applet)# action 6 force shut module my_module_list reset "temperature-sensor policy trigger"
switch(config-applet)# end
```

To create event manager parameters, use the `event manager environment` command. To display the values of event manager parameters, use the `show event manager environment all` command.

Configuration Examples for the Online Insertion Removal Event

The online insertion removal (OIR) event does not have a default policy.

This example shows how to configure the OIR event using the `event oir` command:

```
event oir device-type event-type [device-number]
```

The `device-type` can be `fan`, `module`, or `powersupply`.

The `event-type` can be `insert`, `remove`, or `anyoir` (insert or remove).

The optional `device-number` specifies a single device. If omitted, all devices are selected.

This example shows how to configure the insert event:

```
switch# configure terminal
switch(config)# event manager applet myoir
switch(config-applet)# event oir module insert
switch(config-applet)# action 1 syslog priority critical msg "OIR insert event: A Module is inserted"
```

This example shows how to configure the remove event:

```
switch# configure terminal
switch(config)# event manager applet myoir
switch(config-applet)# event oir module remove
switch(config-applet)# action 1 syslog priority critical msg "OIR remove event: A Module is removed"
```

Configuration Example to Generate a User Syslog

This example shows how to generate a user syslog using the `action syslog` command:

```
switch# configure terminal
switch(config)# event manager applet myoir
switch(config-applet)# event oir module remove
switch(config-applet)# action 1 syslog priority critical msg "Module is removed"
```

When this event is triggered, the system generates a syslog as follows:
Configuration Example to Monitor Syslog Messages

This example shows how to monitor syslog messages from the switch:

```
switch(config)# event manager applet a1
switch(config-applet)# event syslog occurs 6 period 4294967 pattern "authentication failed"
```

When this event is triggered, the action defined in the policy is executed.

Configuration Examples for SNMP Notification

Polling an SNMP OID to Generate an EEM Event

The SNMP object ID (OID) CISCO-SYSTEM-EXT-MIB::cseSysCPUUtilization is used for querying the CPU utilization of the switch:

```
cseSysCPUUtilization OBJECT-TYPE
SYNTAX Gauge32 (0..100 )
UNITS "%"
MAX-ACCESS read-only
STATUS current
DESCRIPTION "The average utilization of CPU on the active supervisor."
::= { ciscoSysInfoGroup 1 }
```

This example shows the use of an SNMP OID that is polled at an interval of 10 seconds and has a threshold value of 95 percent:

```
switch# configure terminal
switch(config)# event manager applet test_policy
switch(config-applet)# event snmp oid 1.3.6.1.4.1.9.9.305.1.1.1.0 get-type exact entry-op gt entry-val 95 exit-op lt exit-val 90 poll-interval 10
```

Sending an SNMP Notification in Response to an Event in the Event Policy

You can use this type of configuration to cause a critical event trigger to generate an SNMP notification.

This example shows how to send an SNMP notification for an event from the Event Manager applet configuration mode:

```
switch(config-applet)# action 1.1 snmp-trap intdata1 100 intdata2 300 strdata "CPU Hogging at switch1"
switch(config-applet)# action 1.1 snmp-trap intdata1 100 intdata2 300 strdata "Port Failure eth9/1"
```

This configuration triggers an SNMP notification (trap) from the switch to SNMP hosts. The SNMP payload carries the values of user-defined fields intdata1, intdata2, and strdata.

Configuration Example for Port Tracking

This example shows how to configure the state of one port to match the state of another port (port tracking).
To configure the port tracking of Ethernet interface 3/23 by Ethernet interface 1/2, follow these steps:

**Procedure**

**Step 1** Create an object to track the status of Ethernet interface 3/23.

**Example:**

```
switch# configure terminal
switch(config)# track 1 interface ethernet 3/23
switch(config-track)# end
```

**Step 2** Configure an EEM event to shut Ethernet interface 1/2 when the tracking object shuts down.

**Example:**

```
switch(config)# event manager applet track_3_23_down
switch(config-applet)# event track 1 state down
switch(config-applet)# action 1 syslog msg EEM applet track_3_23_down shutting down port eth1/2 due to eth3/23 being down
switch(config-applet)# action 2 cli conf term
switch(config-applet)# action 3 cli interface ethernet 1/2
switch(config-applet)# action 4 cli shut
switch(config-applet)# end
```

**Step 3** Configure an EEM event to bring up Ethernet interface 1/2 when Ethernet interface 3/23 comes up.

**Example:**

```
switch# configure terminal
switch(config)# event manager applet track_3_23_up
switch(config-applet)# event track 1 state up
switch(config-applet)# action 1 syslog msg EEM applet track_3_23_down bringing up port eth1/2 due to eth3/23 being up
switch(config-applet)# action 2 cli conf term
switch(config-applet)# action 3 cli interface ethernet 1/2
switch(config-applet)# action 4 cli no shut
switch(config-applet)# end
```

**Configuration Example to Register an EEM Policy with the EEM**

This example shows how to register an EEM policy with the EEM:

Basic switch configuration:

```
event manager applet vpc_check_peer_at_startup
event track 101 state up
action 1.0 cli copy bootflash:eem/user_script_policies/load_schedules running-config

feature scheduler

!!## 2 x dummy loopbacks are required ##!!
interface loopback 101
interface loopback 102

track 1 list boolean or
```
object 13
object 12
object 102
track 2 list boolean and
object 13
object 12
track 12 interface Ethernet 2/24 line-protocol
track 13 interface port-channel 3000 line-protocol
track 101 interface loopback 101 line-protocol
track 102 interface loopback 102 line-protocol

In this example, port channel 3000 is the vPC peer link, and Ethernet 2/24 is the vPC keepalive link.

Note
You need to copy the following files to the bootflash:

- A directory called: /em/user_script_policies needs to be created on the supervisor bootflash.
- These five files need to be created and loaded into the above directory:
  - load_schedules
  - remove_vpc_if_peer_failed
  - clean_up
  - unload_schedules
  - restore_vpc

Configuration for the load_schedules file:

```plaintext
feature scheduler

configure terminal
scheduler job name vpc_check
configure terminal
event manager policy remove_vpc_if_peer_failed
end

configure terminal
scheduler job name clean_up
configure terminal
event manager policy clean_up
end

configure terminal
scheduler job name trigger
configure terminal
interface loopback 102
shutdown
no shutdown
end

configure terminal
scheduler schedule name load_vpc_check
time start +00:00:04
job name vpc_check

scheduler schedule name trigger_vpc_check
time start +00:00:05
job name trigger

scheduler schedule name load_clean_up
```
time start +00:00:08
job name clean_up

scheduler schedule name trigger_clean_up
time start +00:00:10
job name trigger

Configuration for the remove_vpc_if_peer_failed file:

event manager applet remove_vpc_if_peer_failed
event track 1 state down
action 1.0 cli show run vpc > bootflash://sup-active/eem/user_script_policies/vpc_saved.cfg
action 2.0 cli show run vpc > bootflash://sup-standby/eem/user_script_policies/vpc_saved.cfg
action 3.0 cli configure terminal
action 4.0 cli no feature vpc
action 5.0 syslog msg severity alert "##### WARNING!!!! PEER SWITCH FAILED TO COME ONLINE. VPC CONFIG REMOVED #####"
action 6.0 cli event manager policy restore_vpc
action 7.0 cli copy bootflash:eem/user_script_policies/unload_schedules running-config
action 8.0 cli no event manager applet remove_vpc_if_peer_failed
action 9.0 cli end

Configuration for the clean_up file:

event manager applet clean_up
event track 102 state up
action 1.0 cli configure terminal
action 2.0 cli no event manager applet remove_vpc_if_peer_failed
action 3.0 cli copy bootflash:eem/user_script_policies/unload_schedules running
action 4.0 cli no event manager applet clean_up
action 5.0 end

Configuration for the unload_schedules file:

no scheduler schedule name load_vpc_check
no scheduler schedule name trigger_vpc_check
no scheduler schedule name load_clean_up
no scheduler schedule name trigger_clean_up
no scheduler job name vpc_check
no scheduler job name trigger
no scheduler job name clean_up

Configuration for the restore_vpc file:

event manager applet restore_vpc
event track 2 state up
action 1.0 cli copy bootflash:eem/user_script_policies/vpc_saved.cfg running-config
action 2.0 syslog msg severity alert "##### VPC PEER DETECTED. VPC CONFIG RESTORED #####"
action 3.0 cli configure terminal
action 4.0 cli copy bootflash:eem/user_script_policies/unload_schedules running-config
action 5.0 cli no event manager applet restore_vpc
action 6.0 cli end
Configuration Limits for Cisco NX-OS System Management

The configuration limits are documented in the *Cisco Nexus 9000 Series NX-OS Verified Scalability Guide*.  
• Configuration Limits for Cisco NX-OS System Management, on page 395

**Configuration Limits for Cisco NX-OS System Management**

The features supported by Cisco NX-OS have maximum configuration limits. Some of the features have configurations that support limits less than the maximum limits.

The configuration limits are documented in the *Cisco Nexus 9000 Series NX-OS Verified Scalability Guide*. 
enable 111
erspan-id 256
event 202, 211
event application 202
event cli 203
event counter 203
event fanabsent 203
event fanbad 203
event fib adjacency extra 203
event fib resource team usage 203
event fib route {extra | inconsistent | missing} 203
event gold module 204
event interface 204
event manager applet 201, 210, 213
event manager environment 201
event manager policy 210
event memory {critical | minor | severe} 204
event module 204
event module-failure 204
event none 204
event oir 205
event policy-default count 205
event poweroverbudget 205
event snmp 205
event storm-control 205
event syslog 206
event syslog {occurs | period | pattern | priority} 213
event syslog tag {occurs | period | pattern | priority} 213
event syslog memory 206
event syslog switchcounter count 206
event timer 207
event track 207
exporter 289

F
feature lldp 272
feature netflow 284
feature ntp 57
feature ptp 40
feature scheduler 135
feature sflo w 298
filter access-group 237
flow exporter 287
flow monitor 289
flow record 284, 291

G
guestshell 358
guestshell sync 358

H
hardware acl tap-agg 311
hardware multicast global-tx-span 242
hw-module logging onboard 219
hw-module logging onboard counter-stats 219
hw-module logging onboard cpuhog 219
hw-module logging onboard environmental-history 219
hw-module logging onboard error-stats 220
hw-module logging onboard interrupt-stats 220
hw-module logging onboard module 220
hw-module logging onboard obfl-logs 220

I
import 17
import interface 17
import running-config 17
install activate 350
install add bootflash 349
install add ftp 349
install add tftp 349
install add usb 1 349
install add usb 2 349
install commit 351, 352
install deactivate 352
install remove 352
ip access-group 130
ip access-list 129, 240, 262, 312
ip dscp 256
ip flow monitor 290
ip port access-group 314, 317
ip ttl 256
ipv6 flow monitor 290
isolate 324

J
job name 140

L
layer2-switched flow monitor 292
lldp dbx version 274
lldp holdtime 275
lldp receive 273
lldp reinit 275
lldp timer 275
lldp tlv-select 275
lldp transmit 273
logging console 76
logging event {link-status | trunk-status} {enable | default} 79
logging level 80, 82
logging logfile 79
logging message interface type ethernet description 78
logging module 80
logging monitor 77
logging origin-id 78
logging server 83, 84
logging source-interface loopback 83
logging timestamp {microseconds | milliseconds | seconds} 82

M
mac access-list 312
mac packet-classify 291
mac port access-group 314, 317
marker-packet 256
match 285
match datalink 285, 291
match ip 286
match ipv4 286
match ipv6 286
match transport 286
mode tap-aggregation 314
monitor erspan origin ip-address 254
monitor session 236, 242, 254, 257
monitor session all shut 242, 257
monitor session all type erspan-source 254
monitor session in erspan source 263
mpls strip 316
mpls strip dest-mac 318
mpls strip label 318
mpls strip label-age 319
mtu 241

N
NetFlow 290, 292
bridged on VLAN 290
timeouts 292
no duplicate-message throttle 111
no isolate 324
no monitor session 236, 254, 258
no monitor session all shut 258
no scheduler job name 139
no shut 238, 256, 258
no shutdown 324
no snmp trap link-status 169
no snmp-server protocol enable 172
no switch-profile 19
no system interface shutdown 324
no system mode maintenance 336
no system mode maintenance dont-generate-profile 336
no system mode maintenance on-reload reset-reason 334
ntp access-group {peer | serve | serve-only | query-only} 62
ntp authenticate 60
ntp authentication-key 60
ntp logging 64
ntp master 57

O
option exporter-stats 288
option interface-table 288

P
periodic-inventory notification 110
periodic-inventory notification interval 110
periodic-inventory notification timeofday 110
permit 130, 313
permit ip 240, 262
permit udf 240, 262
phone-contact 100
ptp 41
ptp announce {interval | timeout} 41
ptp announce interval 42
ptp delay-request minimum interval 42
ptp device-type boundary-clock 40
ptp device-type generalized-ptp 40
ptp domain 40
ptp priority1 40
ptp priority2 40
ptp source 40
ptp sync interval 42, 43
ptp vlan 43
python instance 325, 328

R
record 289
reload 239, 242, 262
rmon alarm 182
rmon event 183
rmon hcalarm 182
rollback running-config {checkpoint | file} 375
run bash 354

S
save 129, 131
scheduler aaa-authentication password 137
scheduler aaa-authentication username 137
scheduler job name 138
scheduler logfile size 136
scheduler schedule name 139
sflow agent-ip 303
sflow collector-ip 301
sflow collector-port 302
INDEX

sflow counter-poll-interval 300
sflow data-source interface ethernet 304
sflow data-source interface port-channel 304
sflow max-datatype-size 300
sflow max-sampled-size 299
sflow sampling-rate 298
show callhome 101, 108, 110, 113
show callhome destination-profile 102, 104, 105, 113
show callhome destination-profile profile 102, 104, 105
show callhome transport 107, 109, 113
show callhome user-def-cmds 106, 113
show checkpoint 375
show checkpoint all 375, 376
show checkpoint all system 376
show checkpoint all user 376
show checkpoint summary 376
show checkpoint summary system 376
show checkpoint summary user 376
show clock 344
show configuration session 129, 130, 131
show configuration session status 131
show configuration session summary 131
show diagnostic bootup level 190, 193
show diagnostic content module 192, 193
show diagnostic description module 193
show diagnostic events 194
show diagnostic ondemand setting 194
show diagnostic result module 194
show diagnostic simulation module 194
show diagnostic status module 192, 194
show diff rollback-patch {checkpoint | running-config | startup-config}

show event manager environment 201, 214
show event manager environment all 201, 214
show event manager event-types 214
show event manager event-types all 214
show event manager event-types module 214
show event manager history events 214
show event manager policy-state 202, 211, 214
show event manager script-system 214
show event manager script-system all 214
show event manager system-policy 196, 200, 214
show event manager system-policy all 214
show feature 298
show flow cache 293
show flow exporter 293
show flow interface 293
show flow record 285, 293
show flow record netflow layer2-switched input 292, 293
show hardware capacity 194
show install active 344, 350
show install committed 351
show install inactive 350, 352
show install log 350, 355
show install log detail 356
show install packages 354
show interface brief 337
show interface snmp-ifindex 170, 175
show ip access-lists 264, 313, 315
show ldp all 276
show ldp dcbx interface 276
show ldp interface 273, 276
show ldp neighbors detail 276
show ldp neighbors interface 276
show ldp timers 275, 276
show ldp tlv-select 275, 276
show ldp traffic 276
show ldp traffic interface 276
show logging console 77, 88
show logging info 78, 88
show logging last 88
show logging level 81, 88
show logging logfile 88
show logging logfile end-time 88
show logging logfile start-time 88
show logging module 80, 88
show logging monitor 77, 88
show logging nvram 88
show logging nvram last 88
show logging onboard 221
show logging onboard boot-uptime 221
show logging onboard counter-stats 221
show logging onboard credit-loss 221
show logging onboard device-version 221
show logging onboard endtime 221
show logging onboard environmental-history 221
show logging onboard error-stats 221
show logging onboard exception-log 221
show logging onboard interrupt-stats 221
show logging onboard module 221
show logging onboard obfl-history 221
show logging onboard obfl-logs 221
show logging onboard stack-trace 221
show logging onboard start-time 222
show logging onboard status 222
show logging origin-id 78, 89
show logging server 83, 84, 89
show logging timestamp 82, 89
show mac access-lists 313, 315
show maintenance on-reload reset-reasons 338
show maintenance profile 338
show maintenance profile maintenance-mode 327, 338
show maintenance profile normal-mode 329, 338
show maintenance timeout 338
show module 194, 344
show monitor 243

show monitor session  238, 241, 243, 256, 260, 264
show monitor session all  238, 243, 258, 260, 264
show monitor session range  238, 243, 260, 264
show mpls strip labels  320
show mpls strip labels all  320
show mpls strip labels dynamic  320
show mpls strip labels static  320
show ntp access-groups  63, 64
show ntp authentication-keys  60, 64
show ntp authentication-status  61, 65
show ntp logging-status  64, 65
show ntp peer-status  65
show ntp peers  59, 65
show ntp rts-update  65
show ntp source  65
show ntp source-interface  65
show ntp statistics {io | local | memory | peer {ipaddr | name}}  65
show ntp trusted-keys  60, 65
show process  304
show ptp brief  43, 49
show ptp clock  50
show ptp clock foreign-masters-record  50
show ptp corrections  50
show ptp counters  50
show ptp parent  50
show ptp port interface  43
show ptp port interface ethernet  50
show ptp time-property  50
show qos dcbxp interface  276
show rmon {alarms | hcalarms}  182
show rmon alarms  183
show rmon events  183
show rmon hcalarms  184
show rmon logs  184
show rollback log  376
show rollback log exec  376
show rollback log verify  376
show running-config {include "scheduler aaa-authentication"  137
show running-config {include "system memory"  212
show running-config callhome  113
show running-config eem  196, 214
show running-config ldp  272, 276
show running-config mmode  338
show running-config monitor  257, 258, 264
show running-config netflow  293
show running-config ntp  57, 65
show running-config ptp  50
show running-config sflow  304
show running-config sflow all  304
show running-config snmp  175
show running-config switch-profile  20
show scheduler config  136, 140, 141
show scheduler job  138, 139, 141
show scheduler job name  138, 139
show scheduler logfile  141
show scheduler schedule  141
show sflow  298, 299, 300, 302, 303, 304
show snapshots  330, 338
show snapshots compare  330, 332, 338
show snapshots dump  338
show snapshots sections  332, 338
show snmp  171, 175
show snmp community  175
show snmp context  172, 175
show snmp engineID  175
show snmp group  175
show snmp host  161, 175
show snmp session  175
show snmp source-interface  158, 160, 175
show snmp trap  175
show snmp user  152, 175
show startup-config callhome  113
show startup-config eem  214
show startup-config mmode  338
show startup-config monitor  257, 258, 265
show startup-config switch-profile  20
show switch-profile  14, 16, 18, 20
show system mode  334, 336, 338
show tech-support callhome  113
show ttag brief  50
shut  243, 258
shutdown  324
site-id  100
sleep instance  325
snapshot create  330
snapshot delete  330
snapshot section add  331
snapshot section delete  332
snmp-server aaa-user cache-timeout  173
snmp-server community  154, 155
snmp-server contact  99, 171
snmp-server context  172
snmp-server counter cache timeout  173
snmp-server enable traps  164
snmp-server enable traps aaa  164
snmp-server enable traps bgp  164
snmp-server enable traps bridge  164
snmp-server enable traps callhome  165
snmp-server enable traps config  165
snmp-server enable traps eigrp  165
snmp-server enable traps entity  165
snmp-server enable traps feature-control  166
snmp-server enable traps hsrp  166
snmp-server enable traps license  166
snmp-server enable traps link  167
snmp-server enable traps ospf  167
snmp-server enable traps rf  167
snmp-server enable traps rmon  168
snmp-server enable traps snmp  168
snmp-server enable traps syslog  168
snmp-server enable traps syslog  168
INDEX

snmp-server enable traps upgrade 169
snmp-server enable traps vtp 169
snmp-server globalEnforcePriv 153
snmp-server host 156, 157, 159, 160
snmp-server location 171
snmp-server mib community-map 172
snmp-server name 152
snmp-server source-interface {traps | informs} 157
snmp-server source-interface traps 160
snmp-server tcp-session 170
snmp-server user 153, 154, 158
source 287
source interface 241, 263
SPAN sessions 281
    configuring 281
statistics per-entry 313
storm-control action trap 169
streetaddress 100
switch-priority 100
switch-profile 13, 15, 17
switchport 14, 236, 291, 314, 317
switchport monitor 236
sync-peer destination 18
sync-peers destination 14, 19
system interface shutdown 324
system memory-thresholds minor 212
system memory-thresholds threshold critical no-process-kill 212
system mode maintenance dont-generate-profile 333
system mode maintenance on-reload reset-reason 334
system mode maintenance shutdown 334
system mode maintenance timeout 334

T

tag 202
template data timeout 288
terminal event-manager bypass 209
terminal monitor 76
time daily 140
time monthly 140
time start 140
time start now 140
time start repeat 140
time weekly 140
transport email from 107
transport email mail-server 106
transport email reply-to 107
transport http proxy enable 109
transport http proxy server 109
transport http use-vrf 108
transport udp 288

U

udf 238, 261

V

verify 16, 130
version 9 288
vlan configuration 290
vrf 256