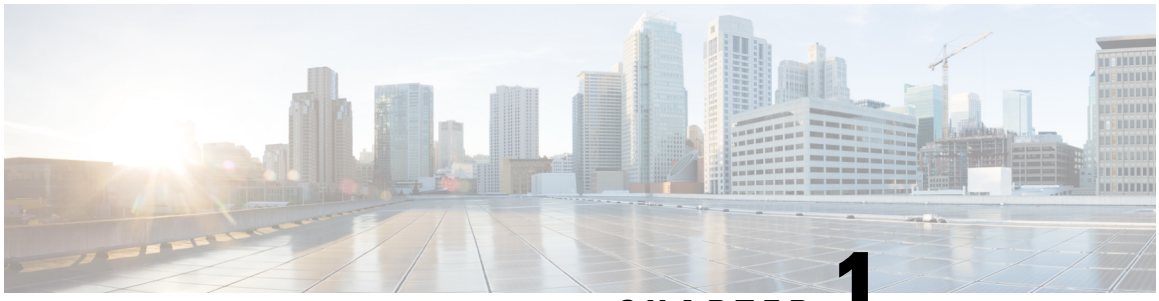
Cisco Nexus 7000 Series NX-OS System Management Configuration Guide

First Published: 2016-12-23

Last Modified: 2020-05-12

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CHAPTER 1

New and Changed Information

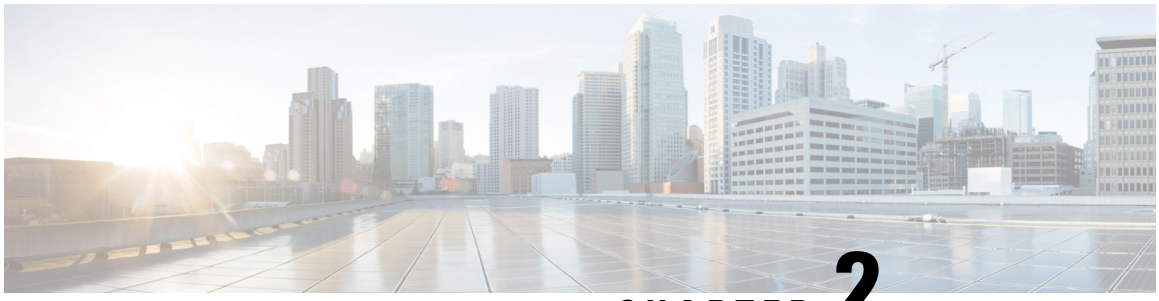
This chapter provides release-specific information for each new and changed feature in the Cisco Nexus 7000 Series NX-OS System Management Configuration Guide.

New and Changed Information

The table below summarizes the new and changed features for this document and shows the releases in which each feature is supported. Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Feature	Description	Changed in Release	Where Documented
iCAM Monitoring	Added the support to enable iCAM monitoring, view the history of traffic analytics, and predict the traffic analytics for the TCAM resources and entries.	8.2(1)	Configuring iCAM, on page 415
PTP	Added PTP support for M3-Series I/O modules.	8.2(1)	Configuring PTP, on page 61
iCAM	Added support for the iCAM feature.	8.0(1)	Configuring iCAM, on page 415

Feature	Description	Changed in Release	Where Documented
Graceful Insertion and Removal (GIR) Enhancements	Added support for Simple Network Management Protocol (SNMP) traps and snapshot delay. A CLI indicator has been added to show that the switch is in maintenance mode. The following keywords were added to the **system mode maintenance** command: **non-interactive** and **snapshot-delay**	8.0(1)	Configuring GIR (Cisco NX-OS Release 7.3(0)D1(1) and later releases), on page 383
Binary Tech Support	Added support for log-collecting framework that collects logs internally from all Cisco NX-OS processes that are running on the device. The **show tech-support all binary** *uri* command is introduced.	8.0(1)	Configuring System Message Logging, on page 81



CHAPTER 2

Overview

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

This chapter contains the following sections:

Licensing Requirements

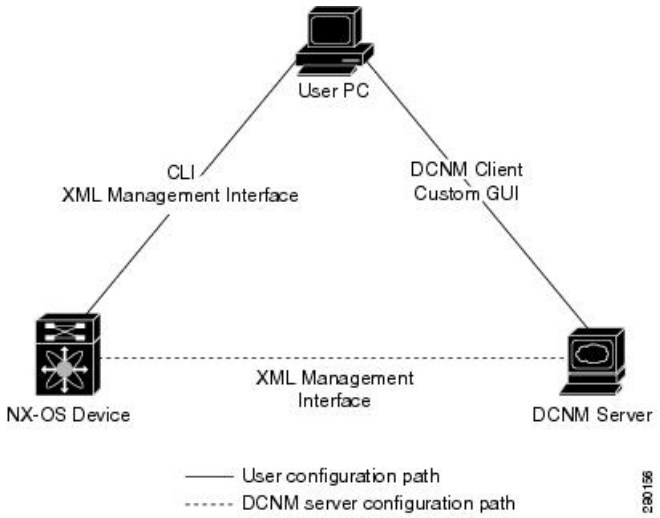
For a complete explanation of Cisco NX-OS licensing recommendations and how to obtain and apply licenses, see the *Cisco NX-OS Licensing Guide*.

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 1: Configuration Methods Book Links

Configuration Method	Document
CLI from a Secure Shell (SSH) session, a Telnet session, or the console port	*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide*
XML management interface	*Cisco NX-OS XML Management Interface User Guide*
Cisco DCNM client	*Cisco DCNM Fundamentals Guide*
User-defined GUI	*Web Services API Guide, Cisco DCNM for LAN Release 5.x*

This section includes the following topics:

- Configuring with CLI or XML Management Interface
- Configuring with Cisco DCNM or a Custom GUI

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 7000 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 or a Custom GUI

You can configure Cisco NX-OS devices using the Cisco DCNM client or from your own GUI as follows:

- **Cisco DCNM Client**—You can configure 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 management interface. For more information about the Cisco DCNM client, see the *Fundamentals Configuration Guide, Cisco DCNM for LAN, Release 5.x* .
- **Custom GUI**—You can create your own GUI to configure devices using the Cisco DCNM web services application program interface (API) on the Cisco DCNM server. You use the SOAP protocol to exchange XML-based configuration messages with the Cisco DCNM server. The Cisco DCNM server configures the device over the XML management interface. For more information about creating custom GUIs, see the *Web Services API Guide, Cisco DCNM for LAN, Release 5.x*

Cisco Fabric Services

Cisco Fabric Services (CFS) is a Cisco proprietary feature that distributes data, including configuration changes, to all Cisco NX-OS devices in a network.

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.

Precision Time Protocol

The Precision Time Protocol (PTP) is a time synchronization protocol for nodes distributed across a network. Its hardware timestamp feature provides greater accuracy than other time synchronization protocols such as Network Time Protocol (NTP). For more information about PTP.

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.

System Messages

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 a terminal session, a log file, and syslog servers on remote systems.

System message logging is based on RFC 3164. For more information about the system message format and the messages that the device generates, see the *Cisco NX-OS System Messages Reference*.

Smart Call Home

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

Rollback

The rollback feature allows you to take a snapshot, or checkpoint, of the device configuration and then reapply that configuration at any point without having to reload. Rollback allows any authorized administrator to apply this checkpoint configuration without requiring expert knowledge of the features configured in the checkpoint.

Session Manager allows you to create a configuration session and apply all commands within that session atomically.

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.

RMON

Remote monitoring (RMON) is an 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.

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.

Embedded Event Manager

The Embedded Event Manager (EEM) allows you to detect and handle critical events in the system. EEM provides event detection and recovery, including monitoring of events either as they occur or as thresholds are crossed.

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. ERSPAN uses a generic routing encapsulation (GRE) tunnel to carry traffic between switches.

ERSPAN consists of an ERSPAN source session, routable ERSPAN GRE-encapsulated traffic, and an ERSPAN destination session. You separately configure ERSPAN source sessions and destination sessions on different switches.

To configure an ERSPAN source session on one switch, you associate a set of source ports or VLANs with a destination IP address, ERSPAN ID number, and virtual routing and forwarding (VRF) name. To configure an ERSPAN destination session on another switch, you associate the destinations with the source IP address, the ERSPAN ID number, and a VRF name. The ERSPAN source session copies traffic from the source ports or source VLANs and forwards the traffic using routable GRE-encapsulated packets to the ERSPAN destination session. The ERSPAN destination session switches the traffic to the destinations.

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.

NetFlow

NetFlow identifies packet flows for both ingress and egress IP packets and provide statistics based on these packet flows. NetFlow does not require any change to either the packets themselves or to any networking device.

FabricPath

FabricPath brings the benefits of Layer 3 routing to Layer 2 switched networks to build a highly resilient and scalable Layer 2 fabric. The system manager is responsible for starting the FabricPath resources process and monitoring heartbeats.

EEE

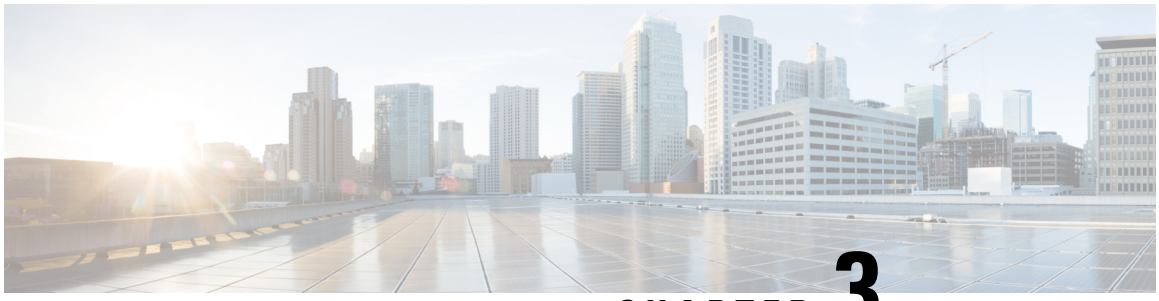
Energy Efficient Ethernet (EEE) is an IEEE 802.3az standard that is designed to reduce power consumption in Ethernet networks during idle periods. EEE can be enabled on devices that support low power idle (LPI) mode. Such devices can save power by entering LPI mode during periods of low utilization. In LPI mode, systems on both ends of the link can save power by shutting down certain services. EEE provides the protocol needed to transition into and out of LPI mode in a way that is transparent to upper layer protocols and applications.

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 CFS

This chapter describes how to use Cisco Fabric Services (CFS), a Cisco proprietary feature that distributes data, including configuration changes, to all Cisco NX-OS devices in a network.

This chapter includes the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

About CFS

You can use Cisco Fabric Services (CFS) to distribute and synchronize a configuration on one Cisco device with all other Cisco devices in your network. CFS provides you with consistent and, in most cases, identical configurations and behavior in your network.

Applications that Use CFS to Distribute Configuration Changes

CFS distributes configuration changes for the applications listed in the following table.

Table 2: CFS-Supported Applications

Application	Default State
Device alias	Enabled
DPVM	Enabled
FC domain	Disabled
FC port security	Disabled
FC timer	Disabled
IVR	Disabled
NTP	Disabled
RADIUS	Disabled
RSCN	Disabled
Smart Call Home	Disabled
TACACS+	Disabled
User roles	Disabled

CFS Distribution

CFS distributes configuration changes to multiple devices across a complete network. CFS supports the following types of distribution:

- CFS over Ethernet (CFSoE)—Distributes application data over an Ethernet network.
- CFS over IP (CFSoIP)—Distributes application data over an IPv4 network.
- CFS over Fibre Channel (CFSoFC)—Distributes application data over a Fibre Channel, such as a virtual storage area network (VSAN). If the device is provisioned with Fibre Channel ports, CFSoFC is enabled by default.

  Beginning with Cisco NX-OS Release 5.2, you can configure Fibre Channel over Ethernet (FCoE), which allows Fibre Channel traffic to be encapsulated over a physical Ethernet link. To run FCoE on a Cisco Nexus 7000 Series switch, you must configure a dedicated storage virtual device context (VDC). If FCoE is enabled on the device, CFSoFC services can be used. The applications that require CFS distribution to be enabled in the storage VDC are noted in the configuration instructions throughout this chapter. For more information on FCoE and storage VDCs, see the *Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500* and the Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide.

Note All of the information in this chapter applies to both CFSoIP and CFSoFC, unless otherwise noted.

CFS Distribution Modes

CFS supports three distribution modes to accommodate different feature requirements. Only one mode is allowed at a given time.

- Uncoordinated distributions—Distribute information that is not expected to conflict with that from a peer. Parallel uncoordinated distributions are allowed for an application.
- Coordinated distributions—Distribute information that can be manipulated and distributed from multiple devices (for example, the port security configuration). Coordinated distributions allow only one application distribution at a given time. CFS uses locks to enforce this. A coordinated distribution is not allowed to start if locks are acquired for the application anywhere in the network. A coordinated distribution consists of three stages:
  - A network lock is acquired.
  - The configuration is distributed and committed.
  - The network lock is released.

  CFS can execute these stages in response to an application request without intervention from the application or under complete control of the application.
- Unrestricted uncoordinated distributions—Allow multiple parallel distributions in the network in the presence of an existing coordinated distribution. Unrestricted uncoordinated distributions are allowed to run in parallel with all other types of distributions.

CFS Connectivity in a Mixed Fabric

CFS is an infrastructure component that also runs on the Cisco Nexus 7000 Series switches, Cisco Nexus 5000 Series switches, and Cisco MDS 9000 switches. A mixed fabric of different platforms (such as the Cisco Nexus 9000 Series, Cisco Nexus 7000 Series, Cisco Nexus 5000 Series, and Cisco MDS 9000 switches) can interact with each other.

Using CFSoIP, the respective CFS clients can also talk to their instances running on the other platforms. Within a defined domain and distribution scope, CFS can distribute the client's data and configuration to its peers running on other platforms.

All three platforms support both CFSoIP and CFSoFC. However, the Cisco Nexus 7000 Series and Cisco Nexus 5000 Series switches require an FC or FCoE plugin and corresponding configuration in order for CFSoFC to operate. Both options are available by default on the Cisco MDS 9000 switches.

Note Some applications are not compatible with their instances running on different platforms. Therefore, Cisco recommends that you carefully read the client guidelines for CFS distribution before committing the configuration.

For more information on CFS for the Cisco Nexus 7000 Series, Cisco Nexus 5000 Series, and Cisco MDS 9000 switches, see the *Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*, *Cisco Nexus 5000 Series NX-OS System Management Configuration Guide*, and *Cisco MDS 9000 Family NX-OS System Management Configuration Guide*, respectively.

CFS Merge Support

An application keeps the configuration synchronized in the fabric through CFS. When two such fabrics become reachable to one another, CFS triggers a merge. These two fabrics could have two different sets of configuration information that need to be reconciled in the event of a merge. CFS provides notification each time an application peer comes online. If a fabric with M application peers merges with another fabric with N application peers and if an application triggers a merge action on every notification, a link-up event results in MxN merges in the fabric.

CFS supports a protocol that reduces the number of merges required to one by handling the complexity of the merge at the CFS layer. This protocol runs per application per scope. The protocol involves selecting one device in a fabric as the merge manager for that fabric. The other devices do not have a role in the merge process.

During a merger of two networks, their designated managers exchange configuration databases. The application on one of them merges the databases, decides if the merge is successful, and notifies all other devices.

In the merge is successful, the merged database is distributed to all devices in the combined fabric, and the entire new fabric remains in a consistent state.

Locking the Network

When you configure an application that uses the CFS infrastructure, that application starts a CFS session and locks the network. When a network is locked, the device software allows configuration changes to this application only from the device holding the lock. If you make configuration changes to the application from another device, the device issues a message to inform the user about the locked status. The configuration changes are held in a pending database by that application.

If you start a CFS session that requires a network lock but forget to end the session, an administrator can clear the session. If you lock a network at any time, your username is remembered across restarts and switchovers. If another user (on the same machine) tries to perform configuration tasks, that user's attempts are rejected.

CFS Regions

A CFS region is a user-defined subset of devices for a given feature or application. You usually define regions to localize or restrict distribution based on devices that are close to one another. When a network covers many geographies with many different administrators who are responsible for subsets of devices, you can manage the scope of an application by setting up a CFS region.

CFS regions are identified by numbers ranging from 0 through 200. Region 0 is reserved as the default region and contains every device in the network. You can configure regions from 1 through 200.

Note If an application is moved (that is, assigned to a new region), its scope is restricted to that region, and it ignores all other regions for distribution or merging purposes. The assignment of the region to an application has precedence in distribution over its initial scope.

You can configure a CFS region to distribute configurations for multiple applications. However, on a given device, you can configure only one CFS region at a time to distribute the configuration for a given application. Once you assign an application to a CFS region, its configuration cannot be distributed within another CFS region.

High Availability

Stateless restarts are supported for CFS. 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*.

Prerequisites for CFS

CFS has the following prerequisites:

- CFS is enabled by default. All devices in the fabric must have CFS enabled, or they do not receive distributions.
- If CFS is disabled for an application, that application does not distribute any configuration, and it does not accept a distribution from other devices in the fabric.

Guidelines and Limitations for CFS

CFS has the following configuration guidelines and limitations:

- If the virtual port channel (vPC) feature is enabled for your device, do not disable CFSoE.

Note CFSoE must be enabled for the vPC feature to work.

- All CFSoIP-enabled devices with similar multicast addresses form one CFSoIP fabric.
- Make sure that CFS is enabled for the applications that you want to configure.
- Anytime you lock a fabric, your username is remembered across restarts and switchovers.
- Anytime you lock a fabric, configuration changes attempted by anyone else are rejected.
- While a fabric is locked, the application holds a working copy of configuration changes in a pending database or temporary storage area, not in the running configuration.
- Configuration changes that have not been committed yet (still saved as a working copy) are not in the running configuration and do not display in the output of **show** commands.
- If you start a CFS session that requires a fabric lock but forget to end the session, an administrator can clear the session.
- An empty commit is allowed if configuration changes are not previously made. In this case, the **commit** command results in a session that acquires locks and distributes the current database.
- You can use the **commit** command only on the specific device where the fabric lock was acquired.
- CFSoIP and CFSoE are not supported for use together.
- CFS regions can be applied only to CFSoIP applications.

- You cannot distribute the user role configuration between a Cisco MDS 9500 Series switch and the storage VDC configured for a Cisco Nexus 7000 Series switch. To prevent this distribution, make sure to assign the user role configuration in Cisco MDS and the Cisco Nexus 7000 storage VDC to different CFS regions.
- CFS uses the same MAC address 01:80:c2:00:00:0e as the standard IEEE protocol Link Layer Discovery Protocol (LLDP), and sniffer software such as Ethanalyzer or Wireshark decodes CFS traffic as LLDP traffic.

Default Settings for CFS

Table 3: Default CFS Parameters

Parameters	Default
CFS distribution on the device	Enabled
CFSoIP	Disabled
IPv4 multicast address	239.255.70.83
CFSoFC	Enabled, if FCoE is present
CFSoE	Disabled

Configuring CFS Distribution

Enabling CFS Distribution for Applications

Enabling CFS to Distribute Smart Call Home Configurations

You can enable CFS to distribute Call Home configurations to all Cisco NX-OS devices in the network. The entire Call Home configuration is distributed except the device priority and the sysContact names.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **callhome**	Enters Call Home configuration mode.
Step 3	switch(config-callhome)# **distribute**	Enables CFS to distribute Smart Call Home configuration updates.

	Command or Action	Purpose
Step 4	(Optional) switch(config-callhome)# **show** *application-name* **status**	For the specified application, displays the CFS distribution status.
Step 5	(Optional) switch(config-callhome)# **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# distribute
switch(config-callhome)# show callhome status
Distribution : Enabled
switch(config-callhome)# copy running-config startup-config
```

Enabling CFS to Distribute Device Alias Configurations

You can enable CFS to distribute device alias configurations in order to consistently administer and maintain the device alias database across all Cisco NX-OS devices in the fabric.

Before you begin

Make sure that you are in the storage VDC. To change to the storage VDC, use the **switchto vdc fcoe** command.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **device-alias distribute**	Enables CFS to distribute device alias configuration updates.
Step 3	(Optional) switch(config)# **show cfs application**	Displays the CFS distribution status.
Step 4	(Optional) switch(config)# **copy running-config startup config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to enable CFS to distribute device alias configurations:

```
switch(config)# device-alias distribute
switch(config)# show cfs application
----------------------------------------------
Application Enabled Scope
----------------------------------------------
device-alias Yes Physical-fc
```

```
switch(config)# copy running-config startup-config
[########################################] 100%
```

Enabling CFS to Distribute DPVM Configurations

You can enable CFS to distribute dynamic port VSAN membership (DPVM) configurations in order to consistently administer and maintain the DPVM database across all Cisco NX-OS devices in the fabric.

Before you begin

Make sure that you are in the storage VDC. To change to the storage VDC, use the **switchto vdc fcoe** command.

Make sure that you enable the DPVM feature. To do so, use the **feature dpvm** command.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **dpvm distribute**	Enables CFS to distribute DPVM configuration updates.
Step 3	(Optional) switch(config)# **show** *application-name* **status**	For the specified application, displays the CFS distribution status.
Step 4	(Optional) switch(config)# **copy running-config startup config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to enable CFS to distribute DPVM configurations:

```
switch(config)# dpvm distribute
switch(config)# show dpvm status
Distribution is enabled.
switch(config)# copy running-config startup-config
[########################################] 100%
```

Enabling CFS to Distribute FC Domain Configurations

You can enable CFS to distribute Fibre Channel (FC) domain configurations in order to synchronize the configuration across the fabric from the console of a single Cisco NX-OS device and to ensure consistency in the allowed domain ID lists on all devices in the VSAN.

Before you begin

Make sure that you are in the storage VDC. To change to the storage VDC, use the **switchto vdc fcoe** command.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **fcdomain distribute**	Enables CFS to distribute FC domain configuration updates.
Step 3	(Optional) switch(config)# **show** *application-name* **status**	For the specified application, displays the CFS distribution status.
Step 4	(Optional) switch(config)# **copy running-config startup config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to enable CFS to distribute FC domain configurations:

```
switch(config)# fcdomain distribute
switch(config)# show fcdomain status
fcdomain distribution is enabled
switch(config)# copy running-config startup-config
[########################################] 100%
```

Enabling CFS to Distribute FC Port Security Configurations

You can enable CFS to distribute Fibre Channel (FC) port security configurations in order to provide a single point of configuration for the entire fabric in the VSAN and to enforce the port security policies throughout the fabric.

Before you begin

Make sure that you are in the storage VDC. To change to the storage VDC, use the **switchto vdc fcoe** command.

Make sure that you enable the FC port security feature. To do so, use the **feature fc-port-security** command.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **fc-port-security distribute**	Enables CFS to distribute FC port security configuration updates.
Step 3	(Optional) switch(config)# **show cfs application**	Displays the CFS distribution status.
Step 4	(Optional) switch(config)# **copy running-config startup config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to enable CFS to distribute FC port security configurations:

```
switch(config)# fc-port-security distribute
switch(config)# show cfs application
----------------------------------------------
Application Enabled Scope
----------------------------------------------
fc-port-securi Yes Logical
switch(config)# copy running-config startup-config
[########################################] 100%
```

Enabling CFS to Distribute FC Timer Configurations

You can enable CFS to distribute Fibre Channel (FC) timer configurations for all Cisco NX-OS devices in the fabric.

Before you begin

Make sure that you are in the storage VDC. To change to the storage VDC, use the **switchto vdc fcoe** command.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **fctimer distribute**	Enables CFS to distribute FC timer configuration updates.
Step 3	(Optional) switch(config)# **show** *application-name* **status**	For the specified application, displays the CFS distribution status.
Step 4	(Optional) switch(config)# **copy running-config startup config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to enable CFS to distribute FC timer configurations:

```
switch(config)# fctimer distribute
switch(config)# show fctimer status
Distribution : Enabled
switch(config)# copy running-config startup-config
[########################################] 100%
```

Enabling CFS to Distribute IVR Configurations

You can enable CFS to distribute inter-VSAN routing (IVR) configurations in order to enable efficient IVR configuration management and to provide a single point of configuration for the entire fabric in the VSAN.

Before you begin

Make sure that you are in the storage VDC. To change to the storage VDC, use the **switchto vdc fcoe** command.

Make sure that you enable the IVR feature. To do so, use the **feature ivr** command.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **ivr distribute**	Enables CFS to distribute IVR configuration updates. **Note** You must enable IVR distribution on all IVR-enabled switches in the fabric.
Step 3	(Optional) switch(config)# **show cfs application**	Displays the CFS distribution status.
Step 4	(Optional) switch(config)# **copy running-config startup config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to enable CFS to distribute IVR configurations:

```
switch(config)# ivr distribute
switch(config)# show cfs application
----------------------------------------------
Application Enabled Scope
----------------------------------------------
ivr Yes Physical-fc
switch(config)# copy running-config startup-config
[########################################] 100%
```

Enabling CFS to Distribute NTP Configurations

You can enable CFS to distribute NTP configurations to all Cisco NX-OS devices in the network.

Before you begin

Make sure that you enable the NTP feature (using the **feature ntp** command).

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.

	Command or Action	Purpose
Step 2	switch(config)# **ntp distribute**	Enables CFS to distribute NTP configuration updates.
Step 3	(Optional) switch(config)# **show** *application-name* **status**	For the specified application, displays the CFS distribution status.
Step 4	(Optional) switch(config)# **copy running-config startup config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

```
switch# configure terminal
switch(config)# ntp distribute
switch(config)# show ntp status
Distribution : Enabled
switch(config)# copy running-config startup-config
```

Enabling CFS to Distribute RADIUS Configurations

You can enable CFS to distribute RADIUS configurations to all Cisco NX-OS devices in the network.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **radius distribute**	Enables CFS to distribute RADIUS configuration updates.
Step 3	(Optional) switch(config)# **show** *application-name* **status**	For the specified application, displays the CFS distribution status.
Step 4	(Optional) switch(config)# **copy running-config startup config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

```
switch# configure terminal
switch(config)# radius distribute
switch(config)# show radius status
Distribution : Enabled
switch(config)# copy running-config startup-config
```

Enabling CFS to Distribute RSCN Configurations

You can enable CFS to distribute registered state change notification (RSCN) configurations to all Cisco NX-OS devices in the fabric.

Before you begin

Make sure that you are in the storage VDC. To change to the storage VDC, use the **switchto vdc fcoe** command.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **rscn distribute**	Enables CFS to distribute RSCN configuration updates.
Step 3	(Optional) switch(config)# **show cfs application**	Displays the CFS distribution status.
Step 4	(Optional) switch(config)# **copy running-config startup config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to enable CFS to distribute RSCN configurations:

```
switch(config)# rscn distribute
switch(config)# show cfs application
----------------------------------------------
Application Enabled Scope
----------------------------------------------
rscn Yes Logical
switch(config)# copy running-config startup-config
[########################################] 100%
```

Enabling CFS to Distribute TACACS+ Configurations

You can enable CFS to distribute TACACS+ configurations to all Cisco NX-OS devices in the network.

Before you begin

Make sure that you enable the TACACS+ feature (using the **feature tacacs+** command).

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **tacacs+ distribute**	Enables CFS to distribute TACACS+ configuration updates.
Step 3	(Optional) switch(config)# **show** *application-name* **status**	For the specified application, displays the CFS distribution status.

	Command or Action	Purpose
Step 4	(Optional) switch(config)# **copy running-config startup config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

```
switch# configure terminal
switch(config)# tacacs+ distribute
switch(config)# show tacacs+ status
Distribution : Enabled
switch(config)# copy running-config startup-config
```

Enabling CFS to Distribute User Role Configurations

You can enable CFS to distribute user role configurations to all Cisco NX-OS devices in the network.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **role distribute**	Enables CFS to distribute user role configurations.
Step 3	(Optional) switch(config)# **show** *application-name* **status**	For the specified application, displays the CFS distribution status.
Step 4	(Optional) switch(config)# **copy running-config startup config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

```
switch# configure terminal
switch(config)# role distribute
switch(config)# show role status
Distribution : Enabled
switch(config)# copy running-config startup-config
```

Specifying a CFS Distribution Mode

You can specify and enable an Ethernet or IPv4 CFS distribution mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.

	Command or Action	Purpose
Step 2	switch(config)# **cfs** {**eth** | **ipv4**} **distribute**	Globally enables CFS distribution over Ethernet or IPv4 for all applications on the device.
Step 3	(Optional) switch(config)# **show cfs status**	Shows the current state of CFS, including the distribution mode.
Step 4	(Optional) switch(config)# **copy running-config startup config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

```
switch# configure terminal
switch(config)# cfs ipv4 distribute
switch(config)# show cfs status
Distribution : Enabled
Distribution over IP : Disabled
Distribution over Ethernet : Enabled
switch(config)# copy running-config startup-config
```

Configuring an IP Multicast Address for CFSoIP

For CFS protocol-specific distributions, such as the keepalive mechanism for detecting network topology changes, use the IP multicast address to send and receive information. You can configure the IP multicast address used to distribute CFSoIPv4.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **no cfs ipv4 distribute**	Globally disables CFSoIP distribution for all applications on the device. **Note** You must disable CFSoIP before you can change the multicast address.
Step 3	switch(config)# **cfs ipv4 mcast-address** *ip-address*	Configures the multicast address for CFS distribution over IPv4. The ranges of valid IPv4 addresses are 239.255.0.0 through 239.255.255.255 and 239.192/16 through 239.251/16.
Step 4	switch(config)# **cfs ipv4 distribute**	Globally enables CFSoIP distribution for all applications on the device.
Step 5	(Optional) switch(config)# **show cfs status**	Shows the current state of CFS, including whether it is enabled, its IP mode, and its multicast addresses.

	Command or Action	Purpose
Step 6	(Optional) switch(config)# **copy running-config startup config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

```
switch# configure terminal
switch(config)# no cfs ipv4 distribute
This will prevent CFS from distributing over IPv4 network.
Are you sure? (y/n) [n] y
switch(config)# cfs ipv4 mcast-address 239.255.1.1
Distribution over this IP type will be affected
Change multicast address for CFS-IP?
Are you sure? (y/n) [n] y
switch(config)# cfs ipv4 distribute
switch(config)# show cfs status
Distribution : Enabled
Distribution over IP : Enabled - mode IPv4
IPv4 multicast address : 239.255.1.1
switch(config)# copy running-config startup-config
```

Configuring CFS Regions

Creating a CFS Region

You can create a CFS region and add an application, such as Smart Call Home, to it.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)#**cfs region** *region-number*	Creates the region and enters the configuration mode for the specified region.
Step 3	switch(config-cfs-region)#*application-name*	For the specified region, adds the named application.
Step 4	(Optional) switch(config-cfs-region)#**show cfs regions brief**	Shows all configured regions and applications but does not show peers.
Step 5	(Optional) switch(config-cfs-region)# **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

```
switch# configure terminal
switch(config)# cfs region 4
```

```
switch(config-cfs-region)# callhome
switch(config-cfs-region)# show cfs regions brief
--------------------------------------
Region Application Enabled
--------------------------------------
4      callhome    yes
switch(config-cfs-region)# copy running-config startup-config
```

Moving an Application to a Different CFS Region

You can move an application to a different region. For example, you can move NTP from region 1 to region 2.

Note When you move an application, its scope is restricted to the new region. It ignores all other regions for distribution or merging purposes.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **cfs region** *region-number*	Enters the configuration mode for the specified region.
Step 3	Required: switch(config-cfs-region)# *application-name*	Specifies the applications to be moved.
Step 4	(Optional) switch(config-cfs-region)# **show cfs regions name** *application-name*	Displays peers and region information for a given application.
Step 5	(Optional) switch(config-cfs-region)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

```
switch# configure terminal
switch(config)# cfs region 2
switch(config-cfs-region)# callhome
switch(config-cfs-region)# show cfs regions name callhome
Region-ID : 2
Application: callhome
Scope : Physical-fc-ip
--------------------------------------------------------------------------
Switch WWN IP Address
--------------------------------------------------------------------------
20:00:00:22:55:79:a4:c1 172.28.230.85 [Local]
switch
Total number of entries = 1
switch(config-cfs-region)# copy running-config startup-config
```

Removing an Application from a CFS Region

You can remove an application from a region. Removing an application from a region is the same as moving the application back to the default region. The default region is usually region 0. This action brings the entire fabric into the scope of distribution for the application.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **cfs region** *region-number*	Enters the configuration mode for the specified region.
Step 3	Required: switch(config-cfs-region)# **no** *application-name*	Removes the specified application from the region.
Step 4	(Optional) Repeat Step 3 for each application that you want to remove from this region.	
Step 5	(Optional) switch(config-cfs-region)# **show cfs regions brief**	Shows all configured regions and applications but does not show peers.
Step 6	(Optional) switch(config-cfs-region)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

```
switch# configure terminal
switch(config)# cfs region 2
switch(config-cfs-region)# no ntp
switch(config-cfs-region)# show cfs regions brief
-------------------------------------
Region Application Enabled
-------------------------------------
4      tacacs+     yes
6      radius      yes
switch(config-cfs-region)# copy running-config startup-config
```

Deleting a CFS Region

You can delete a region and move all included applications back to the default region.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **no cfs region** *region-number*	Deletes the specified region after warning that this action causes all applications in the region to move to the default region.

	Command or Action	Purpose
		Note After you delete the region, you are returned to the global configuration mode.
Step 3	(Optional) switch(config)# **show cfs regions brief**	Shows all configured regions and applications but does not show peers.
Step 4	(Optional) switch(config)# **show cfs application name** *application-name*	Shows local application information by name.
Step 5	(Optional) switch(config)# **copy running-config startup config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

```
switch# configure terminal
switch(config)# no cfs region 4
WARNING: All applications in the region will be moved to default region.
Are you sure? (y/n) [n] y
switch(config)# show cfs regions brief
---------------------------------------
Region Application Enabled
---------------------------------------
6      callhome      no
switch(config)# show cfs application name callhome
Enabled : Yes
Timeout : 20s
Merge Capable : Yes
Scope : Physical-fc-ip
Region : Default
switch(config)# copy running-config startup-config
```

Creating and Distributing a CFS Configuration

You can create a configuration change for an application and then distribute it to its application peers.

Caution If you do not commit the changes, they are not distributed and saved in the running configuration of application peer devices.

Caution If you do not save the changes to the startup configuration in every application peer device where distributed, changes are retained only in their running configurations.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	Required: switch(config)# *application-name*	Specifies that CFS starts a session for the specified application name and locks the fabric.
Step 3	Required: switch(config-callhome)# *application-command*	Specifies that configuration changes are saved as a working copy and are not saved in the running configuration until you enter the **commit** command.
Step 4	(Optional) Repeat Step 3 for each configuration command that you want to add.	
Step 5	(Optional) switch(config-callhome)# **show** *application-name* **status**	For the specified application, displays the CFS distribution status.
Step 6	Required: switch(config-callhome)# **commit**	CFS distributes the configuration changes to the running configuration of every application peer device. If one or more external devices report a successful status, the software overwrites the running configuration with the changes from the CFS working copy and releases the fabric lock. If none of the external devices report a successful status, no changes are made, and the fabric lock remains in place.
Step 7	(Optional) switch(config-callhome)# **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

```
switch# configure terminal
switch(config)# snmp-server contact personname@companyname.com
switch(config)# callhome
switch(config-callhome)# email-contact admin@Mycompany.com
switch(config-callhome)# phone-contact +1-800-123-4567
switch(config-callhome)# street-address 123 Anystreet st. Anytown,AnyWhere
switch(config-callhome)# show callhome status
Distribution : Enabled
switch(config-callhome)# commit
switch(config-callhome)# copy running-config startup-config
```

Clearing a Locked Session

You can clear a lock held by an application from any device in the fabric.

Caution When you clear a lock in the fabric, any pending configurations in any device in the fabric are discarded.

Before you begin

You must have administrator permissions to release a lock.

Procedure

	Command or Action	Purpose
Step 1	(Optional) switch# **show** *application-name* **status**	Shows the current application state.
Step 2	Required: switch# **clear** *application-name* **session**	Clears the application configuration session and releases the lock on the fabric. All pending changes are discarded.
Step 3	(Optional) switch# **show** *application-name* **status**	Shows the current application state.

Example

```
switch# show ntp status
Distribution : Enabled
Last operational state: Fabric Locked
switch# clear ntp session
switch# show ntp status
Distribution : Enabled
Last operational state: No session
```

Discarding a CFS Configuration

You can discard configuration changes and release the lock.

Caution If you discard configuration changes, the application flushes the pending database and releases locks in the fabric.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	Required: switch(config)# *application-name* **abort**	Aborts the application configuration, discards the configuration changes, closes the CFS session, and releases the fabric lock.

	Command or Action	Purpose
		Note The **abort** command is supported only on the device where the fabric lock is acquired.
Step 3	(Optional) switch(config)# **show** *application-name* **session status**	For the specified application, displays the CFS session status.

Example

```
switch# configure terminal
switch(config)# ntp abort
This will prevent CFS from distributing the configuration to other switches.
Are you sure? (y/n) [n] y
switch(config)# show ntp session status
Last Action Time Stamp : Wed Aug 14 16:07:25 2013
Last Action : Abort
Last Action Result : Success
Last Action Failure Reason : none
```

Disabling CFS Distribution Globally

You can disable CFS distribution for a device, isolating the applications using CFS from fabric-wide distributions while maintaining physical connectivity. When CFS is globally disabled on a device, CFS operations are restricted to the device, and all CFS commands continue to function as if the device was physically isolated.

Before you begin

If the virtual port channel (vPC) feature is enabled, only IP distribution is disabled. You must first disable vPC before you can disable CFS distribution.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **no cfs distribute**	Globally disables CFS distribution for all applications on the device.
Step 3	(Optional) switch(config)# **show cfs status**	Displays the global CFS distribution status for the device.
Step 4	(Optional) switch(config)# **copy running-config startup config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

```
switch# configure terminal
switch(config)# no cfs distribute
This will prevent CFS from distributing the configuration to other switches.
Are you sure? (y/n) [n] y
switch(config)# show cfs status
Distribution : Disabled
Distribution over IP : Disabled
IPv4 multicast address : 239.255.70.83
Distribution over Ethernet : Disabled
switch(config)# copy running-config startup-config
```

Verifying the CFS Configuration

Command	Purpose
show *application-name* **session status**	Displays the configuration session status, including the last action, the result, and the reason if there was a failure.
show *application-name* **status**	For the specified application, displays the CFS distribution status.
show cfs application	Displays the applications that are currently CFS enabled.
show cfs application name *application-name*	Displays the details for a particular application, including the enabled or disabled state, timeout as registered with CFS, merge capability if registered with CFS for merge support, distribution scope, and distribution region.
show cfs internal	Displays information internal to CFS including memory statistics, event history, and so on.
show cfs lock	Displays all active locks.
show cfs merge status name *name* [**detail**]	Displays the merge status for a given application.
show cfs peers	Displays all the peers in the physical fabric.
show cfs regions	Displays all the applications with peers and region information.
show cfs status	Displays the status of CFS distribution on the device as well as IP distribution information.
show logging level cfs	Displays the CFS logging configuration.
show tech-support cfs	Displays information about the CFS configuration required by technical support when resolving a CFS issue.

Additional References for CFS

Related Documents

Related Topic	Document Title
CFS CLI commands	*Cisco Nexus 7000 Series NX-OS System Management Command Reference* *Cisco Nexus 7000 Series NX-OS SAN Switching Command Reference*
CFS configuration for device alias CFS configuration for DPVM CFS configuration for FC domain CFS configuration for FC port security CFS configuration for FC timer CFS configuration for IVR CFS configuration for RSCN	*Cisco Nexus 7000 Series NX-OS SAN Switching Configuration Guide*
FCoE	*Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500*
RADIUS	*Cisco Nexus 7000 Series NX-OS Security Configuration Guide*
TACACS+	*Cisco Nexus 7000 Series NX-OS Security Configuration Guide*
User roles	*Cisco Nexus 7000 Series NX-OS Security Configuration Guide*

MIBs

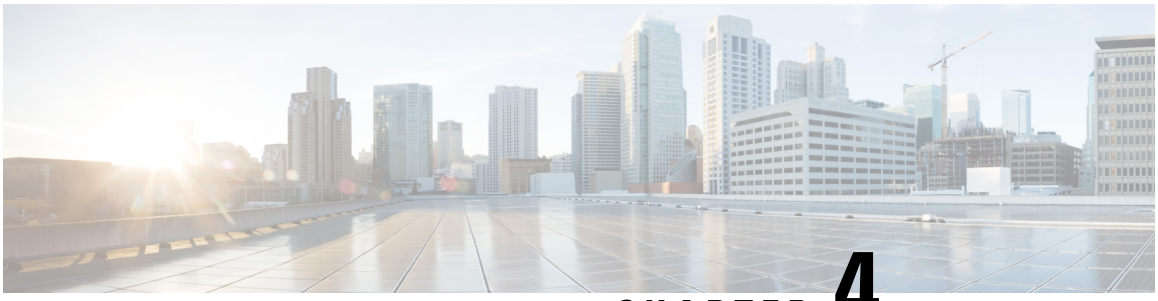
MIBs	MIBs Link
CISCO-CFS-MIB	To locate and download MIBs, go to the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Feature History for CFS

Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Table 4: Feature History for CFS

Feature Name	Release	Feature Information
CFS protocol	5.2(1)	Added CFS over Fibre Channel (CFSoFC) distribution support for device alias, DPVM, FC domain, FC port security, FC timer, IVR, and RSCN.
CFS protocol	4.1(2)	This feature was introduced.



CHAPTER 4

Configuring NTP

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

This chapter includes the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

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.

Note 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 Broadcast Associations

In a broadcast-based NTP association, an NTP server sends NTP broadcast packets throughout a network. Broadcast clients listen for the NTP broadcast packets sent by the server and do not engage in any polling.

NTP broadcast servers allow you to synchronize a large number of clients without creating a lot of NTP traffic because unsolicited messages are sent to a designated IPv4 local broadcast address, and ordinarily no request is expected from the clients.

NTP Multicast Associations

When the device operates as an NTP multicast server, it sends NTP multicast messages to a designated IPv4 or IPv6 multicast group IP address.

When the device operates as an NTP multicast client, it listens for NTP multicast packets that are sent by an NTP multicast server to a designated IPv4 or IPv6 multicast group IP address.

NTP multicast servers allow you to synchronize a large number of clients without creating a lot of NTP traffic because unsolicited messages are sent to a designated multicast group address, and ordinarily no request is expected from the clients.

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.

Distributing NTP Using CFS

Cisco Fabric Services (CFS) distributes the local NTP configuration to all Cisco devices in the network.

After enabling CFS on your device, a network-wide lock is applied to NTP whenever an NTP configuration is started. After making the NTP configuration changes, you can discard or commit them.

In either case, the CFS lock is then released from the NTP application.

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 7000 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 7000 Series NX-OS High Availability and Redundancy Guide*.

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

Virtualization Support

If you are running a Cisco NX-OS Release prior to 5.2, up to one instance of NTP is supported on the entire platform. You must configure NTP in the default virtual device context (VDC), and you are automatically placed in the default VDC unless you specify otherwise.

If you are running Cisco NX-OS Release 5.2 or later, multiple instances of NTP are supported, one instance per VDC. By default, Cisco NX-OS places you in the default VDC unless you specifically configure another VDC. Only one VDC (the default VDC by default) synchronizes the system clock at any given time. The NTP daemon in all other VDCs acts only as an NTP server for the other devices. To change which VDC synchronizes the system clock, use the clock protocol ntp vdc *vdc-id* command.

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 7000 Series NX-OS Unicast Routing Configuration Guide* for more information about VRFs.

For more information about VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*.

Prerequisites for NTP

NTP has the following prerequisites:

- To configure NTP, you must have connectivity to at least one server that is running NTP.
- To configure VDCs, you must install the appropriate license. See the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide* for configuration information and the *Cisco NX-OS Licensing Guide* for licensing information.

Guidelines and Limitations for NTP

NTP has the following configuration guidelines and limitations:

- The Cisco NX-OS software supports NTP version 4 (NTPv4).
- NTP server functionality is supported.
- You should have 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 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, you should configure all the devices as clients to that server.
- We recommend that you do not configure (just) two NTP servers. Instead, you should configure one, three, or four or more NTP servers.

  All NTP servers return the time together with an estimate of the current error. When using multiple time servers, NTP also wants these servers to agree on some time, meaning there must be one error interval where the correct time must be. When there are just two NTP servers, there might be an issue if both sources do not fall into the small common range because the NTP client will be unable to determine which source is more correct.
- 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.
- You must manually distribute NTP authentication keys on the NTP server and Cisco NX-OS devices across the network.
- If CFS is disabled for NTP, then NTP does not distribute any configuration and does not accept a distribution from other devices in the network.
- After CFS distribution is enabled for NTP, the entry of an NTP configuration command locks the network for NTP configuration until a **commit** command is entered. During the lock, no changes can be made to the NTP configuration by any other device in the network except the device that initiated the lock.
- If you use CFS to distribute NTP, all devices in the network should have the same VRFs configured as you use for NTP.

- If you configure NTP in a VRF, ensure that the NTP server and peers can reach each other through the configured VRFs
- You must manually distribute NTP authentication keys on the NTP server and Cisco NX-OS devices across the network.
- Use NTP broadcast or multicast associations when time accuracy and reliability requirements are modest, your network is localized, and the network has more than 20 clients. We recommend that you use NTP broadcast or multicast associations in networks that have limited bandwidth, system memory, or CPU resources.

Note Time accuracy is marginally reduced in NTP broadcast associations because information flows only one way.

- The NTP source-interface and source configuration has a limitation of getting applied only when configured on the client. If the configuration is done on the server (the switch with the NTP master), source address of the outgoing packet will still be that of the received destination address.

Default Settings for NTP

The following table lists the default settings for NTP parameters.

Parameters	Default
NTP	Enabled in all VDCs and for all interfaces. By default, NTP is enabled as server and client.
NTP passive (enabling NTP to form associations)	Enabled
NTP authentication	Disabled
NTP access	Enabled
NTP access group match all	Disabled
NTP broadcast server	Disabled
NTP multicast server	Disabled
NTP multicast client	Disabled
NTP logging	Disabled

Configuring NTP

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

Enabling or Disabling NTP in a VDC

You can enable or disable NTP in a particular VDC. NTP is enabled in all VDCs by default.

Procedure

	Command or Action	Purpose

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) **show ntp status**
	Example:
	`switch(config)# show ntp status`
	`Distribution: Enabled`
	`Last operational state: Fabric Locked`
		Displays the status of the NTP application.

Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Enabling or Disabling NTP on an Interface

You can enable or disable NTP in a particular interface. NTP is enabled in all VDCs by default.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# config t`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface***type slot/port*
	Example:
	`switch(config)# interface ethernet 6/1`
	`switch(config-if)#`
		Enters interface configuration mode.

	Command or Action	Purpose
Step 3	(Optional) [**no**]**ntp disable**{**ip** | **ipv6**} **Example:** `switch(config-if)# ntp disable ip`	Disables NTP IPv4 or IPv6 on the specified interface. Use the no form of this command to reenable NTP on the interface.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves the change persistently through reboots and restarts by copying 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

	Command or Action	Purpose

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

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ntp server** {*ip-address* | *ipv6-address* | *dns-name*} [**key** *key-id*] [**maxpoll** *max-poll*] [**minpoll** *min-poll*] [**prefer**] [**use-vrf** *vrf-name*] **Example:** `switch(config)# ntp server 192.0.2.10`	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. 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 16 seconds, and the default values are 6 and 4, respectively. Use the **prefer** keyword to make this server the preferred NTP server for the device. Use the **use-vrf** keyword to configure the NTP server to communicate over the specified VRF. The *vrf-name* argument can be **default**, **management**, or any case-sensitive, alphanumeric string up to 32 characters. **Note** If you configure a key to be used while communicating with the NTP server, make sure that the key exists as a trusted key on the device.
Step 3	[**no**] **ntp peer** {*ip-address* | *ipv6-address* | *dns-name*} [**key** *key-id*] [**maxpoll** *max-poll*] [**minpoll** *min-poll*] [**prefer**] [**use-vrf** *vrf-name*] **Example:** `switch(config)# ntp peer 2001:0db8::4101`	Forms an association with a peer. You can specify multiple peer associations. Use the **key** keyword to configure a key to be used while communicating with the NTP peer. The range for the *key-id* argument is from 1 to 65535. Use the **maxpoll** and **minpoll** keywords to configure the maximum and minimum intervals in which to poll a peer. The range for the *max-poll* and *min-poll* arguments is from 4 to 17 seconds, and the default values are 6 and 4, respectively. Use the **prefer** keyword to make this peer the preferred NTP peer for the device.

	Command or Action	Purpose
		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`	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`	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

Authentication for NTP servers and NTP peers is configured on a per-association basis using the key keyword on each **ntp server** and **ntp peer** command. Make sure that you configured all NTP server and peer associations with the authentication keys that you plan to specify. Any **ntp server** or **ntp peer** commands that do not specify the key keyword will continue to operate without authentication.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ntp authentication-key** *number* **md5** *md5-string* **Example:** `switch(config)# ntp authentication-key 42 md5 aNiceKey`	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 **ntp trusted-key** *number* command.

	Command or Action	Purpose
		The range for authentication keys is from 1 to 65535. For the MD5 string, you can enter up to eight alphanumeric characters. Beginning with Cisco NX-OS Release 7.3(0)D1(1), you can enter up to 32 alphanumeric characters for the MD5 string.
Step 3	(Optional) **show ntp authentication-keys** **Example:** `switch(config)# show ntp authentication-keys`	Displays the configured NTP authentication keys.

Step 4	[**no**] **ntp trusted-key** *number*
	Example:
	`switch# config t`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`switch(config)# ntp authentication-key 42 md5 aNiceKey`
	`switch(config)# ntp server 10.1.1.1 key 42`
	`switch(config)# ntp trusted-key 42`
	`switch(config)# ntp authenticate`
	`switch(config)# copy running-config startup-config`
	`[########################################] 100%`
	`switch(config)#`
		Specifies one or more keys (defined in Step 2) that a 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 5	(Optional) **show ntp trusted-keys** **Example:** `switch(config)# show ntp trusted-keys`	Displays the configured NTP trusted keys.
Step 6	[**no**] **ntp authenticate** **Example:** `switch(config)# ntp authenticate`	Enables or disables the NTP authentication feature. NTP authentication is disabled by default.
Step 7	(Optional) **show ntp authentication-status** **Example:** `switch(config)# show ntp authentication-status`	Displays the status of NTP authentication.
Step 8	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

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.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ntp access-group** {**peer** | **serve** | **serve-only** | **query-only**} *access-list-name* **Example:** `switch(config)# ntp access-group peer accesslist1`	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 time requests and NTP control queries 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.
Step 3	(Optional) **show ntp access-groups** **Example:** `switch(config)# show ntp access-groups`	Displays the NTP access group 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 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

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ntp source** *ip-address* **Example:** `switch(config)# ntp source 192.0.2.1`	Configures the source IP address for all NTP packets. The *ip-address* can be in IPv4 or IPv6 format.
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 NTP Source Interface

You can configure NTP to use a specific interface.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ntp source-interface** *interface* **Example:** `switch(config)# ntp source-interface ethernet 2/1`	Configures the source interface for all NTP packets. Use the **?** keyword to display a list of supported interfaces.
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 an NTP Broadcast Server

You can configure an NTP IPv4 broadcast server on an interface. The device then sends broadcast packets through that interface periodically. The client is not required to send a response.

Before you begin

Use the **switchto vdc** command to switch to the desired nondefault VDC.

Procedure

	Command or Action	Purpose

Step 1	**configure t**
	Example:
	`switch# config t`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface** *type slot/port*
	Example:
	`switch(config)# interface ethernet 6/1`
	`switch(config-if)#`
		Enters interface configuration mode.

Step 3	Required: [**no**] **ntp broadcast** [**destination** *ip-address*] [**key** *key-id*] [**version** *number*] **Example:** `switch(config-if)# ntp broadcast destination 192.0.2.10`	Enables an NTP IPv4 broadcast server on the specified interface. • destination *ip-address*—Configures the broadcast destination IP address. • key *key-id*—Configures the broadcast authentication key number. The range is from 1 to 65535. • version *number*—Configures the NTP version. The range is from 2 to 4.

Step 4	Required: **exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits interface configuration mode.

Step 5	(Optional) [**no**] **ntp broadcastdelay** *delay* **Example:** `switch(config)# ntp broadcastdelay 100`	(Optional) Configures the estimated broadcast round-trip delay in microseconds. The range is from 1 to 999999.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to configure an Ethernet interface to send NTP broadcast packets:

```
switch# configure terminal
switch(config)# interface ethernet6/1
switch(config-if)# ntp broadcast 192.0.2.10
```

Configuring an NTP Multicast Server

You can configure an NTP IPv4 or IPv6 multicast server on an interface. The device then sends multicast packets through that interface periodically.

Before you begin

Use the **switchto vdc** command to switch to the desired nondefault VDC.

Procedure

	Command or Action	Purpose

Step 1	**configure t**
	Example:
	`switch# config t`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface** *type slot/port*
	Example:
	`switch(config)# interface ethernet 6/1`
	`switch(config-if)#`
		Enters interface configuration mode.

Step 3	Required: [**no**] **ntp multicast** [*ipv4-address* | *ipv6-address*] [**key** *key-id*] [**ttl** *value*] [**version** *number*] **Example:** `switch(config-if)# ntp multicast FF02:1::FF0E:8C6C`	Enables an NTP IPv6 broadcast server on the specified interface. • destination *ip-address*—Configures the broadcast destination IP address. • key *key-id*—Configures the broadcast authentication key number. The range is from 1 to 65535. • ttl *value*—The time-to-live value of the multicast packets. The range is from 1 to 255. • version *number*—Configures the NTP version. **Note** For an IPv4 multicast server, the range is from 2 to 4.

	Command or Action	Purpose
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to configure an Ethernet interface to send NTP multicast packets:

```
switch# configure terminal
switch(config)# interface ethernet2/2
switch(config-if)# ntp multicast FF02::1:FF0E:8C6C
```

Configuring an NTP Multicast Client

You can configure an NTP multicast client on an interface. The device then listens to NTP multicast messages and discards any messages that come from an interface for which multicast is not configured.

Before you begin

Use the **switchto vdc** command to switch to the desired nondefault VDC

Procedure

	Command or Action	Purpose

Step 1	**configure t**
	Example:
	`switch# config t`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface** *type slot/port*
	Example:
	`switch(config)# interface ethernet 6/1`
	`switch(config-if)#`
		Enters interface configuration mode.

Step 3	Required: [**no**] **ntp multicast client** [*ipv4-address* | *ipv6-address*] **Example:** `switch(config-if)# ntp multicast FF02:1::FF0E:8C6C`	Enables an NTP IPv6 broadcast server on the specified interface.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Configuring NTP on a Secondary (Non-Default) VDC

You can configure a non-default VDC to get a timing update from the default VDC and its clients in order to synchronize with it.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **feature ntp**	Enables NTP in the non-default VDC.
Step 3	switch(config)# **ntp master**	Configures the device as an authoritative NTP server.
Step 4	(Optional) switch(config)# **ntp source-interface** *interface*	Configures the source interface for all NTP packets. The following list contains the valid values for *interface*. • ethernet • loopback • mgmt • port-channel • vlan
Step 5	(Optional) [**no**] **ntp source** *ip-address*	Configures the source IP address for all NTP packets. The *ip-address* can be in IPv4 or IPv6 format.
Step 6	(Optional) switch(config)# **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This examples show how to configure NTP on a secondary (non-default) VDC.

```
switch# configure terminal
switch(config)# feature ntp
switch(config)# ntp master
switch(config)# ntp source-interface ethernet
switch(config)# ntp source 192.0.2.2
switch(config)# copy running-config startup-config
```

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

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ntp logging** **Example:** `switch(config)# ntp logging`	Enables or disables system logs to be generated with significant NTP events. NTP logging is disabled by default.
Step 3	(Optional) **show ntp logging-status** **Example:** `switch(config)# show ntp logging-status`	Displays the NTP logging configuration status.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Enabling CFS Distribution for NTP

You can enable CFS distribution for NTP in order to distribute the NTP configuration to other CFS-enabled devices.

Before you begin

Make sure that you have enabled CFS distribution for the device.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# [**no**] **ntp distribute**	Enables or disables the device to receive NTP configuration updates that are distributed through CFS.
Step 3	(Optional) switch(config)# **show ntp status**	Displays the NTP CFS distribution status.
Step 4	(Optional) switch(config)# **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to enable the device to receive NTP configuration updates through CFS:

```
switch# configure terminal
switch(config)# ntp distribute
switch(config)# copy running-config startup-config
```

Committing NTP Configuration Changes

When you commit the NTP configuration changes, the effective database is overwritten by the configuration changes in the pending database and all the devices in the network receive the same configuration.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **ntp commit**	Distributes the NTP configuration changes to all Cisco NX-OS devices in the network and releases the CFS lock. This command overwrites the effective database with the changes made to the pending database.

Discarding NTP Configuration Changes

After making the configuration changes, you can choose to discard the changes instead of committing them. If you discard the changes, Cisco NX-OS removes the pending database changes and releases the CFS lock.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **ntp abort**	Discards the NTP configuration changes in the pending database and releases the CFS lock. Use this command on the device where you started the NTP configuration.

Releasing the CFS Session Lock

If you have performed an NTP configuration and have forgotten to release the lock by either committing or discarding the changes, you or another administrator can release the lock from any device in the network. This action also discards pending database changes.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **clear ntp session**	Discards the NTP configuration changes in the pending database and releases the CFS lock.

Verifying the NTP Configuration

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

Command	Purpose
show ntp access-groups	Displays the NTP access group configuration.
show ntp authentication-keys	Displays the configured NTP authentication keys.
show ntp authentication-status	Displays the status of NTP authentication.
show ntp internal	Displays internal NTP information.
show ntp logging-status	Displays the NTP logging status.
show ntp peer-status	Displays the status for all NTP servers and peers.
show ntp peers	Displays all the NTP peers.
show ntp rts-update	Displays the RTS update status.
show ntp source	Displays the configured NTP source IP address.
show ntp source-interface	Displays the configured NTP source interface.
show ntp statistics {**io** | **local** | **memory** | **peer** {**ipaddr** {*ipv4-addr* | *ipv6-addr*} | **name** *peer-name*}}	Displays the NTP statistics.
show ntp trusted-keys	Displays the configured NTP trusted keys.
show running-config ntp	Displays NTP information.

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 an NTP server and peer, enable NTP authentication, enable NTP logging, and then save the configuration in startup so that it is saved across reboots and restarts:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ntp server 192.0.2.105 key 42
switch(config)# ntp peer 2001:0db8::4101
switch(config)# show ntp peers
--------------------------------------------------
Peer IP Address Serv/Peer
```

```
-----------------------------------------------
2001:db8::4101 Peer (configured)
192.0.2.105 Server (configured)
switch(config)# ntp authentication-key 42 md5 aNiceKey
switch(config)# show ntp authentication-keys
----------------------------
Auth key MD5 String
----------------------------
42 aNicekey
switch(config)# ntp trusted-key 42
switch(config)# show ntp trusted-keys
Trusted Keys:
42
switch(config)# ntp authenticate
switch(config)# show ntp authentication-status
Authentication enabled.
switch(config)# ntp logging
switch(config)# show ntp logging
NTP logging enabled.
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

Related Topic	Document Title
Clock manager	*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide*
NTP CLI commands	*Cisco Nexus 7000 Series NX-OS System Management Command Reference*
VDCs and VRFs	*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*

MIBs

MIBs	MIBs Link
MIBs related to NTP	To locate and download supported MIBs, go to the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Feature History for NTP

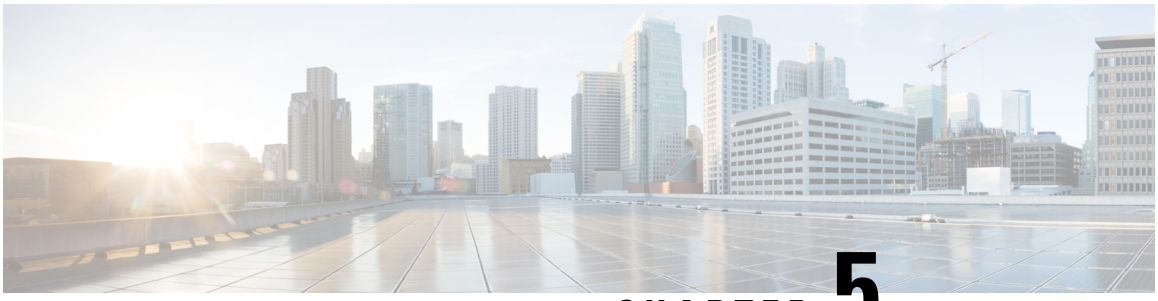
Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Table 5: Feature History for NTP

Feature Name	Releases	Feature Information
NTP	7.3(0)D1(1)	Increased the length of NTP authentication keys from 15 to 32 alphanumeric characters.
NTP	6.2(2)	Introduced the **ntp access-group match-all** command to cause the access group options to be scanned in order, from least restrictive to most restrictive.
NTP	6.2(2)	Introduced the **no ntp passive** command to prevent NTP from forming associations.

NTP	6.2(2)	Added the ability to configure NTP broadcast and multicast servers and multicast clients on an interface.
NTP	6.2(2)	Added the ability to enable or disable NTP on an interface.
NTP	6.1(1)	NTP access group options are now scanned in order from least restrictive to most restrictive.
NTP	6.1(1)	Increased the length of NTP authentication keys from 8 to 15 alphanumeric characters.
NTP	5.2(3)	Increased the length of NTP authentication keys from 8 to 15 alphanumeric characters.
NTP	5.2(1)	Added NTP support for all VDCs, enabling them to act as time servers.
NTP	5.2(1)	Changed the command to enable or disable NTP from [**no**] **ntp enable** to [**no**] feature ntp.
NTP	5.2(1)	Added the ability to configure the device as an authoritative NTP server, enabling it to distribute time even when it is not synchronized to an existing time server.
NTP access groups	5.2(1)	Added the **serve, serve-only**, and **query-only** access group options to control access to additional NTP services.
NTP access groups	5.0(2)	Added the ability to control access to NTP services by using access groups.
NTP authentication	5.0(2)	Added the ability to enable or disable NTP authentication.
NTP logging	5.0(2)	Added the ability to enable or disable NTP logging.
NTP server configuration	5.0(2)	Added the optional key keyword to the **ntp server** command to configure a key to be used while communicating with the NTP server.
CFS support	4.2(1)	Added the ability to distribute NTP configuration using CFS.

NTP source IP address or interface	4.1(3)	Added the ability set the source IP address or source interface that NTP includes in all NTP packets sent to peers.
NTP	4.0(3)	Added the ability to disable NTP.



CHAPTER 5

Configuring PTP

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

This chapter includes the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

About PTP

PTP is a time synchronization protocol for nodes distributed across a network. Its hardware timestamp feature provides greater accuracy than other time synchronization protocols such as the Network Time Protocol (NTP).

Beginning with Cisco NX-OS Release 7.3(0)D1(1), PTP also implements IEEE 802.1AS to support Audio Video Bridging (AVB) on Nexus 7700 platform for F3 line cards. For details on AVB configuration, see *"Cisco Nexus 7000 Audio Video Bridging Configuration Guide"*.

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 Device Types

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 Beginning with Cisco NX-OS Release 7.3(0)D1(1) release, the generalized-PTP clock mode is introduced to support AVB feature.

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.

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

After the master-slave hierarchy has been established, the clocks are synchronized as follows:

- The master sends a synchronization message to the slave and notes the time it was sent.
- The slave receives the synchronization message and notes the time that it was received. For every synchronization message, there is a follow-up message. Hence, the number of sync messages should be equal to the number of follow-up messages.
- The slave sends a delay-request message to the master and notes the time it was sent.
- The master receives the delay-request message and notes the time it was received.
- The master sends a delay-response message to the slave. The number of delay request messages should be equal to the number of delay response messages.
- The slave uses these timestamps to adjust its clock to the time of its master.

Pong

The network-monitoring tool Pong leverages the PTP's time synchronization infrastructure to diagnose the health of the network. Pong measures port-to-port delays and is similar to the network-monitoring utility Ping but provides for a greater depth of network diagnostics. Make sure to increase the interface MTU when you attempt pong to a destination that is several hops away.

Clock Manager

Clocks are resources that need to be shared across different processes and across different VDCs. Multiple time synchronization protocols (such as NTP and PTP) might be running in the system, and multiple instances of the same protocol might be running in different VDCs. The clock manager allows you to specify the protocol and a VDC running that protocol to control the various clocks in the system. For information on configuring the clock manager, see the *Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide*.

High Availability for PTP

Stateful restarts are 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 7000 Series NX-OS High Availability and Redundancy Guide*.

Virtualization Support

Cisco NX-OS supports multiple instances of PTP, one instance per virtual device context (VDC). By default, Cisco NX-OS places you in the default VDC unless you specifically configure another VDC. For more information about VDCs, see the C*isco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*.

Guidelines and Limitations for PTP

- PTP operates only in boundary clock mode. and in gPTP mode to support AVB. The end-to-end transparent clock and peer-to-peer transparent clock modes are not supported.
- Only one PTP process can control all of the port clocks through the clock manager.
- PTP supports transport over User Datagram Protocol (UDP).
- Transport over Ethernet is supported on AVB application.
- PTP supports only multicast communication. Negotiated unicast communication is supported on AVB application.
- PTP is limited to a single domain per network.
- All management messages are forwarded on ports on which PTP is enabled. Handling management messages is not supported.
- PTP-capable ports do not identify PTP packets and do not time-stamp or redirect those packets unless you enable PTP on those ports.
- PTP can be enabled on F1, F2, F2e, F3, F4, M2, and M3 Series module ports.
- PTP is not supported on the breakout ports, logical interfaces, sub interfaces, and FEX interfaces.
- For F1 Series modules, PTP is not supported on the port if priority flow control is enabled. Similarly, priority flow control is not supported if PTP is enabled on the same port.
- For F1 Series modules, Pong is not supported on the VDC if priority flow control is enabled on any of the ports in the same VDC. Similarly, priority flow control is not supported if Pong is enabled in the same VDC.
- Beginning with Cisco NX-OS Release 6.1, PTP is supported in Layer 3 mode for F2, F2e, and M2 Series modules.
- Beginning with Cisco NX-OS Release 6.2.6, PTP is supported in F3 Series modules.
- PTP Encapsulation is supported starting from in Cisco Nexus 7.3.0. The default value is Layer 3.
- PTP over FabricPath is not supported.

- Starting from Cisco NX-OS Release 8.2(1), PTP can be enabled on M3-Series I/O modules.
- Starting from Cisco NX-OS Release 8.4(1) Pong is supported on M3 Series modules.
- Starting from Cisco NX-OS Release 8.4(1), PTP can be enabled on F4-Series I/O modules.

Default Settings for PTP

The following table lists the default settings for PTP parameters.

Table 6: Default PTP Parameters

Parameters	Default
PTP	Disabled
PTP version	2
PTP domain	0
PTP priority 1 value when advertising the clock	255
PTP priority 2 value when advertising the clock	255
PTP announce interval	1 log second
PTP announce timeout	3 announce intervals
PTP minimum delay request interval	0 log seconds
PTP VLAN	1

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.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config) # [**no**] **feature ptp**	Enables or disables PTP on the device. **Note** Enabling PTP on the switch does not enable PTP on each interface.

	Command or Action	Purpose
Step 3	switch(config) # [**no**] **ptp source** *ip-address*	Configures the source IP address for all PTP packets. The *ip-address* can be in IPv4 or IPv6 format.
Step 4	(Optional) switch(config) # [**no**] **ptp domain** *number*	Configures the domain number to use for this clock. PTP domains allow you to use multiple independent PTP clocking subdomains on a single network. The range for the *number* is from 0 to 128.
Step 5	(Optional) switch(config) # [**no**] **ptp priority1** *value*	Configures the priority1 value to use when advertising this clock. This value overrides the default criteria (clock quality, clock class, and etc.) for best master clock selection. Lower values take precedence. The range for the *value* is from 0 to 255.
Step 6	(Optional) switch(config) # [**no**] **ptp priority2** *value*	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 *value* is from 0 to 255.
Step 7	(Optional) switch(config) # [**no**] **ptp encapsulation {layer-2 | layer-3}**	Configures the encapsulation that is to be used for PTP. In Layer 3 encapsulation, PTP packets are encapsulated with IP + UDP frame. In Layer 2 encapsulation, PTP packets are encapsulated within the Ethernet frame. The default PTP encapsulation is Layer-3; PTP mode is Boundary. Layer 2 encapsulation is supported only with AVB.
Step 8	(Optional) switch(config) # [**no**] **ptp mode {boundary-clock | generalized-PTP | transparent-clock peer-to-peer}**	Configures the PTP device mode. The default mode is *boundary-clock*. The generalized-PTP mode is used for AVB. The transparent-clock *peer-to-peer mode* is added for experimental purpose, not supported officially.
Step 9	(Optional) switch(config) # [**no**] **ptp switchlatency-estimated** *value*	Configures the maximum estimate switch latency value in nano-secs (ns). This value is used in AVB. The range is 0 - 2147483647. The default value is 5000.
Step 10	switch(config) # **end**	Exits global configuration mode and returns to Privileged EXEC mode.

	Command or Action	Purpose
Step 11	switch # **clock protocol ptp vdc** *var-number*	(Configured in the admin VDC.) Configures the local clock manager for PTP protocol. The range for the vdc number is 1 to 8.
Step 12	(Optional) switch # [**no**] **show ptp clock foreign-masters record [interface ethernet** *slot/ port*	Displays information about foreign masters.
Step 13	(Optional) switch # [**no**] **show ptp delay summary**	Displays link delay and residency delay information for all interfaces. It is used in AVB.
Step 14	(Optional) switch # [**no**] **show ptp parent**	Displays parent clock information.
Step 15	(Optional) switch # [**no**] **show ptp time-property**	Displays local clock time property information.
Step 16	(Optional) switch # [**no**] **show ptp corrections**	Displays the latest few corrections on this node.
Step 17	(Optional) switch # **show ptp brief**	Displays the PTP status.
Step 18	(Optional) switch # **show ptp clock**	Displays the properties of the local clock.
Step 19	(Optional) switch(config) # **show ptp clock**	Displays the properties of the local clock.

Example

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# show ptp brief
PTP port status
-----------------------
Port State
------- --------------
switch(config)# show ptp clock
PTP Device Type: Boundary clock
Clock Identity : 0:22:55:ff:ff:79:a4:c1
Clock Domain: 0
Number of PTP ports: 0
Priority1 : 1
Priority2 : 1
Clock Quality:
Class : 248
Accuracy : 254
Offset (log variance) : 65535
Offset From Master : 0
Mean Path Delay : 0
Steps removed : 0
Local clock time:Sun Jul 3 14:13:24 2011
switch(config)#
```

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

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config) # **interface ethernet** *slot/port*	Specifies the interface on which you are enabling PTP and enters the interface configuration mode.
Step 3	switch(config-if) # [**no**] **ptp**	Enables or disables PTP on an interface.
Step 4	(Optional) switch(config-if) # [**no**] **ptp announce** {**interval** *log seconds* | **timeout** *count*}	Configures the interval between PTP announce messages on an interface or the number of PTP intervals before a timeout occurs on an interface. The range for the PTP announcement interval is from 0 to 4 seconds, and the range for the interval timeout is from 2 to 10.
Step 5	(Optional) switch(config-if) # [**no**] **ptp delay request minimum interval** *log seconds*	Configures the minimum interval allowed between PTP delay-request messages when the port is in the master state. The range is from log(-6) to log(1) seconds. Where, log(-2) = 2 frames per second.
Step 6	(Optional) switch(config-if) # [**no**] **ptp sync interval** *log seconds*	Configures the interval between PTP synchronization messages on an interface.
Step 7	(Optional) switch(config-if) # [**no**] **ptp vlan** *vlan-id*	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 8	(Optional) switch(config-if) # **show ptp brief**	Displays the PTP status.
Step 9	(Optional) switch(config-if) # **show ptp port interface** *interface slot/port*	Displays the status of the PTP port.
Step 10	(Optional) switch(config-if)# **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to configure PTP on an interface and configure the intervals for the announce, delay-request, and synchronization messages:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
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 4
switch(config-if)# ptp sync interval -1
switch(config-if)# show ptp brief
PTP port status
-----------------------
Port State
------- --------------
Eth2/1 Master
switch(config-if)# show ptp port interface ethernet 2/1
PTP Port Dataset: Eth2/1
Port identity: clock identity: 0:22:55:ff:ff:79:a4:c1
Port identity: port number: 1028
PTP version: 2
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
switch(config-if)#
```

Verifying the PTP Configuration

Use one of the following commands to verify the configuration:

Table 7: PTP Show Commands

Command	Purpose
show ptp brief	Displays the PTP status.
show ptp clock	Displays the properties of the local clock, including clock identity.
show ptp clock foreign-masters-record	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.
show ptp corrections	Displays the last few PTP corrections.
show ptp parent	Displays the properties of the PTP parent.
show ptp port interface ethernet *slot/port*	Displays the status of the PTP port on the switch.

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# config t
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
Clock Identity : 0:22:55:ff:fe:79:a4:c1
Clock Domain: 0
Number of PTP ports: 0
Priority1 : 1
Priority2 : 1
Clock Quality:
  Class : 248
  Accuracy : 254
  Offset (log variance) : 65535
Offset From Master : 0
Mean Path Delay : 0
Steps removed : 0
Local clock time:Sun Jul 3 14:13:24 2011
```

This example shows how to configure PTP on an interface and configure the intervals for the announce, delay-request, and synchronization messages:

```
switch# config t
switch(config)# interface ethernet 2/1
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 4
switch(config-if)# ptp sync interval -1
switch(config-if)# show ptp brief
PTP port status
-----------------------
Port     State
------- --------------
Eth2/1    Master
switch(config-if)# show ptp port interface ethernet 2/1
PTP Port Dataset: Eth2/1
Port identity: clock identity: 0:22:55:ff:fe:79:a4:c1
Port identity: port number: 1028
PTP version: 2
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
```

Related Documents

Related Topic	Document Title
PTP CLI commands	*Cisco Nexus 7000 Series NX-OS System Management Command Reference*
Pong	*Cisco Nexus 7000 Series NX-OS Troubleshooting Guide*
Clock manager	*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide*
VDCs	*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*

Related Documents

Related Topic	Document Title
PTP CLI commands	*Cisco Nexus 7000 Series NX-OS System Management Command Reference*
VDCs	*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*
Pong	*Cisco Nexus 7000 Series NX-OS Troubleshooting Guide*
Clock manager	*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide*

MIBs

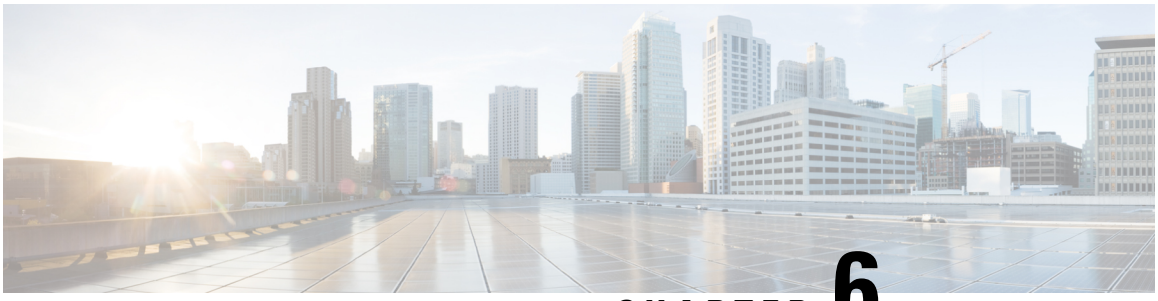
MIBs	MIBs link
CISCO-PTP-MIB	To locate and download supported MIBs, go to the following URL: ftp://ftp.cisco.com/pub/mibs/supportlists/nexus7000/Nexus7000MIBSupportList.html

Feature History for PTP

Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Table 8: Feature History for PTP

Feature Name	Releases	Feature Information
Pong	8.4(1)	Added Pong support for M3 Series modules.
PTP	8.4(1)	Added PTP support for F4-Series I/O modules.
PTP	8.2(1)	Added PTP support for M3-Series I/O modules.
PTP	7.3(0)D1(1)	Added support for AVB, 802.1AS, generalized-ptp mode, peer-delay-response mechanism, layer-2 encapsulation only for F3 line cards on Nexus 7700 chassis. For details, refer to *"Cisco Nexus AVB configuration Guide"*.
PTP	6.2(6)	Added support in F3 Series Modules.
PTP	6.1(1)	Added PTP support in Layer 3 mode for F2, F2e, and M2 Series modules.
PTP	6.1(1)	Added support for M2 Series modules.
PTP	6.1(1)	Changed the PTP MAC format from FF:FF to FF:FE.
PTP	6.1(1)	Deprecated the **vrf** option from the **ptp source** command.
PTP	6.0(1)	Added PTP support on port-channel member ports.
PTP	6.0(1)	Added support for F2 Series modules.
PTP	5.2(1)	This feature was introduced.



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:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

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/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 7000 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 7000 Series NX-OS High Availability and Redundancy Guide*.

Virtualization Support

Cisco NX-OS supports multiple instances of CDP, one instance per virtual device context (VDC). By default, Cisco NX-OS places you in the default VDC unless you specifically configure another VDC. For more information on VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*.

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.
- CDP is not supported for the Cisco Nexus 2000 Series Fabric Extender.

Default Settings for CDP

This table lists the default settings for CDP parameters.

Parameters	Default
CDP	Enabled globally and on all interfaces
CDP version	Version 2
CDP device ID	Serial number
CDP timer	60 seconds
CDP hold timer	180 seconds

Configuring CDP

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

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **cdp enable** **Example:** `switch(config)# cdp enable`	Enables or disables the CDP feature on the entire device. It is enabled by default.
Step 3	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

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

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface** *interface slot*/*port*
	Example:
	`switch(config)# interface ethernet 1/2`
	`switch(config-if)#`
		Enters interface configuration mode.

Step 3	[**no**] **cdp enable** **Example:** `switch(config-if)# cdp enable`	Enables or disables CDP on this interface. It is enabled by default. **Note** Make sure that CDP is enabled globally on the device.
Step 4	(Optional) **show cdp interface** *interface slot*/*port* **Example:** `switch(config-if)# show cdp interface ethernet 1/2`	Displays CDP information for an interface.

	Command or Action	Purpose
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring Optional CDP Parameters

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

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	(Optional) **cdp advertise** {**v1** | **v2**} **Example:** `switch(config)# cdp advertise v1`	Sets the CDP version supported by the device. The default is v2.
Step 3	(Optional) **cdp format device-id** {**mac-address** | **serial-number** | **system-name**} **Example:** `switch(config)# cdp format device-id mac-address`	Sets the CDP device ID. The options are as follows: • **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* **Example:** `switch(config)# cdp holdtime 150`	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.
Step 5	(Optional) **cdp timer** *seconds* **Example:** `switch(config)# cdp timer 50`	Sets the refresh time when CDP sends advertisements to neighbors. The range is from 5 to 254 seconds. The default is 60 seconds.
Step 6	(Optional) **copy running-config startup-config** **Example:**	Copies the running configuration to the startup configuration.

	Command or Action	Purpose
	`switch(config)# copy running-config startup-config`	

Verifying the CDP Configuration

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

Command	Purpose
show cdp all	Displays all interfaces that have CDP enabled.
show cdp entry {**all** | **name** *entry-name*}	Displays the CDP database entries.
show cdp global	Displays the CDP global parameters.
show cdp interface *interface slot/port*	Displays the CDP interface status.
show cdp neighbors {**device-id** | **interface** *interface slot/port*} [**detail**]	Displays the CDP neighbor status.
show cdp interface *interface slot/port*	Displays the CDP traffic statistics on an interface.

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:

```
config t
cdp enable
cdp timer 50
cdp holdtime 100
```

This example shows how to display the CDP global parameters:

```
switch# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute
Device-ID           Local Intrfce    Hldtme Capability    Platform        Port ID
Mgmt-switch
                    mgmt0             148    R S I         WS-C4948-10GE Gig1/37
switch88(FOX1518GRE6)
                    Eth1/25           164    R S I s       N5K-C5596UP   Eth1/25
switch89(FOX1518GQJ2)
                    Eth1/26           163    R S I s       N5K-C5596UP   Eth1/25
```

Additional References

Related Documents

Related Topic	Document Title
CDP CLI commands	*Cisco Nexus 7000 Series NX-OS System Management Command Reference*
VDCs and VRFs	*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*

MIBs

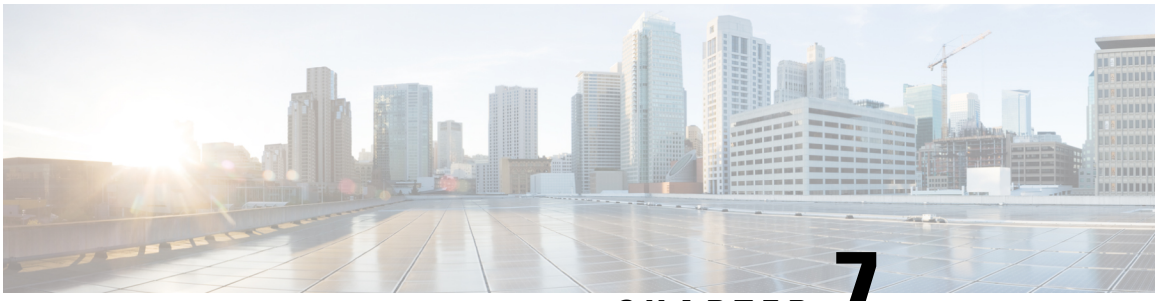
MIBs	MIBs Link
MIBs related to CDP	To locate and download supported MIBs, go to the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Feature History for CDP

Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Table 9: Feature History for CDP

Feature Name	Releases	Feature Information
CDP support for VTP domain name	4.2(1)	CDP advertises the VLAN Trunking Protocol (VTP) type-length-value field (TLV) in CDP version-2 packets.



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:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

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.

System message logging is based on RFC 3164. 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 10: System Message Severity Levels

Level	Description
0 – emergency	System unusable
1 – alert	Immediate action needed
2 – critical	Critical condition
3 – error	Error condition
4 – warning	Warning condition
5 – notification	Normal but significant condition
6 – informational	Informational message only
7 – debugging	Appears during debugging only

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.

Binary Tech Support

Binary tech support is a log-collecting framework that collects logs internally from all Cisco NX-OS processes that are running on the device. Enter the **show tech-support all binary** *uri* command to collect logs from across the entire device, including virtual device contexts (VDCs), and linecards. The logs are saved under one tarball that can be easily transferred for later analysis. If a line card fails during the log collection, binary tech support continues to collect logs from all remaining line cards and VDCs.

Virtualization Support

A virtual device context (VDC) is a logical representation of a set of system resources. System message logging applies only to the VDC where commands are entered.

For information about configuring VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide.*

Guidelines and Limitations for System Message Logging

System messages are logged to the console and the log file by default.

For the secure syslog server(s) to be reachable over in-band (non-management) interface, the CoPP profile may need tweaks especially when multiple logging servers are configured, and when lot of syslogs get generated in a short time (such as boot up, configuration application, and so on).

Platform related syslogs would be showing up only in the log file of the admin VDC or VDC 1 (default VDC) if the admin VDC is not in use. However, these events may impact the functionality of other VDCs (such as fabric CRC errors generated from specific modules, and so on). Hence it is required to configure syslog server in this VDC as well as have the IP reachability to syslog server in the admin VDC or VDC 1 (default VDC) in order to capture and monitor platform related syslog events.

Default Settings for System Message Logging

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

Table 11: Default System Message Logging Parameters

Parameters	Default
Console logging	Enabled at severity level 2
Monitor logging	Enabled at severity level 5
Log file logging	Enabled to log messages at severity level 5
Module logging	Enabled at severity level 5
Facility logging	Enabled
Time-stamp units	Seconds
Syslog server logging	Disabled
Syslog server configuration distribution	Disabled

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

	Command or Action	Purpose
Step 1	**terminal monitor** **Example:** `switch# terminal monitor`	Enables the device to log messages to the console.

Step 2	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 3	[**no**] **logging console** [*severity-level*] **Example:** `switch(config)# logging console 3`	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: • 0 – emergency • 1 – alert • 2 – critical • 3 – error • 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.

	Command or Action	Purpose
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:** `switch(config)# logging message interface type ethernet description`	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. The **no** option disables the printing of the interface description in the system message log for physical Ethernet interfaces.
Step 8	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

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

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **logging logfile** *logfile-name severity-level* [**size** *bytes*] **Example:** `switch(config)# logging logfile my_log 6`	Configures the name of the log file used to store system messages and the minimum severity level to log. When you configure a new logfile without specifying the size, the existing/previously specified logfile size is assigned and the default file size is not considered. 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 You can optionally specify a maximum file size. The default severity level is 5, and the default file size is 4194304 bytes. The file size range is from 4096 to 4194304 bytes.

Step 3	**logging event** {**link-status** | **trunk-status**} {**enable** | **default**}
	Example:
	`switch# logging event link-status default`
	`switch(config)#`
		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.

	Command or Action	Purpose
Step 4	(Optional) **show logging info** **Example:** `switch(config)# show logging info`	Displays the logging configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring Module and Facility Messages Logging

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

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **logging module** [*severity-level*] **Example:** `switch(config)# logging module 3`	Enables module log messages that have the specified severity level or higher. Severity levels range from 0 to 7: • 0 – emergency • 1 – alert • 2 – critical • 3 – error • 4 – warning • 5 – notification • 6 – informational • 7 – debugging If the severity level is not specified, the default of 5 is used. The **no** option disables module log messages.
Step 3	(Optional) **show logging module** **Example:** `switch(config)# show logging module`	Displays the module logging configuration.

	Command or Action	Purpose
Step 4	[**no**] **logging level** *facility severity-level* **Example:** `switch(config)# logging level aaa 2`	Enables logging messages from the specified facility that have the specified severity level or higher. Severity levels range from 0 to 7: • 0 – emergency • 1 – alert • 2 – critical • 3 – error • 4 – warning • 5 – notification • 6 – informational • 7 – debugging 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`	Displays 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	[**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 7	(Optional) **show logging timestamp** **Example:** `switch(config)# show logging timestamp`	Displays the logging time-stamp units configured.
Step 8	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring Syslog Servers

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

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 the *Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **logging server** *host* [*severity-level* [**use-vrf** *vrf-name*]]
	Example:
	`switch(config)# logging server 192.0.2.253`
	Example:
	`switch(config)# logging server 2001:db8::3 5 use-vrf red`
		Configures a syslog server at the specified hostname or IPv4 or IPv6 address. You can limit logging of messages to a particular VRF by using the **use-vrf** keyword. Severity levels range from 0 to 7:
		• 0 – emergency
		• 1 – alert
		• 2 – critical
		• 3 – error
		• 4 – warning
		• 5 – notification
		• 6 – informational
		• 7 – debugging
		The default outgoing facility is local7.
		The **no** option removes the logging server for the specified host.
		The first example forwards all messages on facility local 7. The second example forwards messages with severity level 5 or lower for VRF red.

Step 3	**logging source-interface** *interface* **Example:**	Sets the source interface whose IP address is displayed in the log messages. This static configuration ensures that same IP address

	Command or Action	Purpose
	`switch(config)# logging source-interface loopback 5`	appears in all log messages that are sent from an individual Cisco NX-OS device.
Step 4	(Optional) **show logging server** **Example:** `switch(config)# show logging server`	Displays the syslog server configuration. **Note** The output of this command will display the syslog server configuration details along with a message stating This server is temporarily unreachable." Please ignore this message.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring Destination Port for Forwarding Syslogs

You can specify the destination port to be used while forwarding the system messages to the remote server where they will be logged.

Note You will need to change the remote server syslog configuration file to listen to the specified user-defined port. By default, system messages are sent as a UDP payload over port number 514 to the remote server for logging.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **logging server** *host* [*severity-level* [**use-vrf** *vrf-name*]]
	Example:
	`switch(config)# logging server 192.0.2.253 port 600`
	Example:
	`switch(config)# logging server 192.0.2.253 5 port 600`
		Specifies the destination port on which the syslogs are forwarded to remote server. The port numbers range from 1 to 65535.
		The default destination port number is 514.
		Note To remove the custom destination port or to reset it to its default value, use the **logging server** command without specifying any port number. Optionally, you can specify the port number as 514.

	Command or Action	Purpose
		The first example forwards all messages on user-defined port number 600. The second example forwards messages with severity level 5 or lower on user-defined port number 600.
Step 3	(Optional) **show logging server** **Example:** `switch(config)# show logging server`	Displays the syslog server 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 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 12: Syslog fields in syslog.conf

Field	Description
Facility	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. **Note** Check your configuration before using a local facility.
Level	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.
Action	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.

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.

Procedure

	Command or Action	Purpose
Step 1	Required: **show logging last** *number-lines* **Example:** `switch# show logging last 40`	Displays the last number of lines in the logging file. You can specify from 1 to 9999 for the last number of lines.
Step 2	**show logging logfile** [**start-time** *yyyy mmm dd hh:mm:ss*] [**end-time** *yyyy mmm dd hh:mm:ss*] **Example:** `switch# show logging logfile start-time 2013 oct 1 15:10:0`	Displays the messages in the log file that have a timestamp within the span entered. If you do not enter an end time, the current time is used. You enter three characters for the month time field and digits for the year and day time fields.
Step 3	**show logging nvram** [**last** *number-lines*] **Example:** `switch# show logging nvram last 10`	Displays the messages in the NVRAM. To limit the number of lines displayed, you can enter the last number of lines to display. You can specify from 1 to 100 for the last number of lines.
Step 4	**clear logging logfile** **Example:**	Clears the contents of the log file.

	Command or Action	Purpose
	`switch# clear logging logfile`	
Step 5	**clear logging nvram** **Example:** `switch# clear logging nvram`	Clears the logged messages in NVRAM.

Verifying the System Message Logging Configuration

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

Command	Purpose
show logging console	Displays the console logging configuration.
show logging info	Displays the logging configuration.
show logging last *number-lines*	Displays the last number of lines of the log file.
show logging level [*facility*]	Displays the facility logging severity level configuration.
show logging logfile [**start-time** *yyyy mmm dd hh:mm:ss*] [**end-time** *yyyy mmm dd hh:mm:ss*]	Displays the messages in the log file.
show logging module	Displays the module logging configuration.
show logging monitor	Displays the monitor logging configuration.
show logging nvram [**last** *number-lines*]	Displays the messages in the NVRAM log.
show logging server	Displays the syslog server configuration.
show logging timestamp	Displays the logging time-stamp units configuration.

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

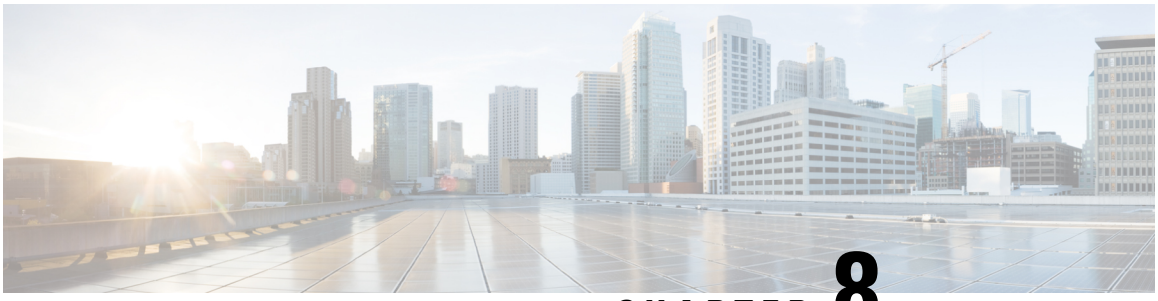
Related Topic	Document Title
System messages CLI commands	*Cisco Nexus 7000 Series NX-OS System Management Command Reference*
System messages	*Cisco NX-OS System Messages Reference*

Feature History for System Message Logging

Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Table 13: Feature History for System Message Logging

Feature Name	Releases	Feature Information
System message logging	7.2(0)D1(1)	This feature was introduced.
System message logging	5.2(1)	Added the ability to add the description for physical Ethernet interfaces and subinterfaces in the system message log.
Syslog servers	5.1(1)	Increased the number of supported syslog servers from three to eight.
IPv6 support	4.2(1)	Added support for IPv6 syslog hosts..
System message logging	4.0(1)	This feature was introduced.



CHAPTER 8

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:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

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.

Alert Group	Description	Executed Commands
Cisco-TAC	All critical alerts from the other alert groups destined for Smart Call Home.	Execute commands based on the alert group that originates the alert.
Configuration	Periodic events related to configuration.	**show module** **show version**
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** **show diagnostic result module** *number* **detail** **show module** **show tech-support gold** **show tech-support ha** **show tech-support platform**
Environmental	Events related to power, fan, and environment-sensing elements such as temperature alarms.	**show environment** **show logging last 200** **show module** **show version**

Alert Group	Description	Executed Commands
Inventory	Inventory status that is provided whenever a unit is cold booted or when FRUs are inserted or removed. This alert is considered a noncritical event, and the information is used for status and entitlement.	**show inventory** **show license usage** **show module** **show sprom all** **show system uptime** **show version**
License	Events related to licensing and license violations.	**show logging last 200**
Linecard hardware	Events related to standard or intelligent switching modules.	**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 ethpm** **show tech-support gold** **show tech-support ha** **show tech-support platform** **show version**
Supervisor hardware	Events related to supervisor modules.	**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** **show version**
Syslog port group	Events generated by the syslog PORT facility.	**show license usage** **show logging last 200**

Alert Group	Description	Executed Commands
System	Events generated by failure of a software system that is critical to unit operation.	**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**
Test	User-generated test message.	**show module** **show version**

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 14: Severity and Syslog Level Mapping

Smart Call Home Level	Keyword	Syslog Level	Description
9	Catastrophic	N/A	Network-wide catastrophic failure.
8	Disaster	N/A	Significant network impact.

Smart Call Home Level	Keyword	Syslog Level	Description
7	Fatal	Emergency (0)	System is unusable.
6	Critical	Alert (1)	Critical conditions that indicate that immediate attention is needed.
5	Major	Critical (2)	Major conditions.
4	Minor	Error (3)	Minor conditions.
3	Warning	Warning (4)	Warning conditions.
2	Notification	Notice (5)	Basic notification and informational messages. Possibly independently insignificant.
1	Normal	Information (6)	Normal event signifying return to normal state.
0	Debugging	Debug (7)	Debugging messages.

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 rovides 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

For more information about Smart Call Home, see the following Smart Call Home page:
https://supportforums.cisco.com/community/netpro/solutions/smart_services/smartcallhome

Distributing Smart Call Home Using CFS

You can use Cisco Fabric Services (CFS) to distribute a Smart Call Home configuration to all CFS-enabled devices in the network. The entire Smart Call Home configuration is distributed except the device priority and the sysContact names.

For more information about CFS, see the “Configuring CFS” section.

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 per virtual device context (VDC). Smart Call Home uses the contact information from the first registered VDC as the administrator contact for all VDCs on the physical device. For example, if you want the Smart Call Home to use the contact information from the default VDC, you should register using that VDC. You can update this information at the Smart Call Home web site at the following URL:

http://www.cisco.com/go/smartcall/

Smart Call Home registers the contacts for all other VDCs as users that can see all the Smart Call Home data for the physical device but cannot act as administrators. All registered users and the registered administrator receive all Smart Call Home notifications from all VDCs on the physical device.

By default, you are placed in the default VDC. In the default VDC, you can test Smart Call Home using the **callhome send** and **callhome test** commands. In a nondefault VDC, only the **callhome test** command is available. For more information on VDCs, see the Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide.

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.

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.
- If you configure VDCs, install the appropriate license. See the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide* for configuration information and the *Cisco NX-OS Licensing Guide* for licensing information.

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.
- If you distribute the Smart Call Home configuration using CFS, then the entire Smart Call Home configuration is distributed except device priority and the sysContact names.
- Currently CoPP does not protect packets for Smart Call Home using HTTP/HTTPS or SMTP method when connectivity is required inband. Return traffic for these services is subject to class-default CoPP class and leads to little to no connectivity.
- A system configured for Smart Call Home (SCH) feature where connectivity may fail during reporting if an explicit class for either the HTTPS method or the SMTP method is not defined in control-plane policing and there is continual violations in the CoPP class-default class. This issue is only seen when the configured destination from SCH is known inband.
- A syslog should be printed if inband is used for SCH where non-standard destination ports are used warning the user to add these ports. Consideration should also be made with a syslog warning when using either a HTTP or HTTPS proxy server on a non-administrative port to allow reachability to Cisco's web servers.
- In a mixed fabric environment with CFS enabled, Cisco devices running Cisco NX-OS Release 5.x can distribute 5.x configurations (multiple SMTP server support, HTTP VRF support, and HTTP proxy support) to other 5.x devices in the fabric over CFS. However, if an existing device upgrades to 5.x, these new configurations are not distributed to that device because a CFS merge is not triggered upon an upgrade. Therefore, we recommend applying the new configurations only when all the devices in the

fabric support them or performing an empty commit from an existing 5.x device (not the newly upgraded device) that has the new configurations.

Default Settings for Smart Call Home

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

Table 15: Default Smart Call Home Parameters

Parameters	Default
Destination message size for a message sent in full text format	2,500,000
Destination message size for a message sent in XML format	2,500,000
Destination message size for a message sent in short text format	4000
SMTP server port number if no port is specified	25
SMTP server priority if no priority is specified	50
Alert group association with profile	All for full-text-destination and short-text-destination profiles. The cisco-tac alert group for the CiscoTAC-1 destination profile.
Format type	XML
Smart Call Home message level	0 (zero)
HTTP proxy server use	Disabled and no proxy server configured

Configuring Smart Call Home

Note 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 104
2. Creating a Destination Profile, on page 106
3. Associating an Alert Group with a Destination Profile, on page 109
4. (Optional) Adding Show Commands to an Alert Group, on page 109
5. Enabling or Disabling Smart Call Home, on page 116
6. (Optional) Testing the Smart Call Home Configuration, on page 116

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.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

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

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

Step 4	**email-contact** *email-address* **Example:** `switch(config-callhome)# email-contact admin@Mycompany.com`	Configures the email address for the person primarily responsible for the device. The *email-address* can be up to 255 alphanumeric characters in email address format. **Note** You can use any valid email address. The address cannot contain spaces.
Step 5	**phone-contact** *international-phone-number* **Example:** `switch(config-callhome)# phone-contact +1-800-123-4567`	Configures the phone number in international phone number format for the person primarily responsible for the device. The *international-phone-number* can be up to 17 alphanumeric characters and must be in international phone number format. **Note** The phone number cannot contain spaces. Use the plus (+) prefix before the number.
Step 6	**streetaddress** *address* **Example:** `switch(config-callhome)# streetaddress 123 Anystreet st. Anytown,AnyWhere`	Configures the street address as an alphanumeric string with white spaces for the person primarily responsible for the device. The *address* can be up to 255 alphanumeric characters. Spaces are accepted.

	Command or Action	Purpose
Step 7	(Optional) **contract-id** *contract-number* **Example:** `switch(config-callhome)# contract-id Contract5678`	Configures the contract number for this device from the service agreement. The *contract-number* can be up to 255 alphanumeric characters in free format.
Step 8	(Optional) **customer-id** *customer-number* **Example:** `switch(config-callhome)# customer-id Customer123456`	Configures the customer number for this device from the service agreement. The *customer-number* can be up to 255 alphanumeric characters in free format.
Step 9	(Optional) **site-id** *site-number* **Example:** `switch(config-callhome)# site-id Site1`	Configures the site number for this device. The *site-number* can be up to 255 alphanumeric characters in free format.
Step 10	(Optional) **switch-priority** *number* **Example:** `switch(config-callhome)# switch-priority 3`	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. **Note** Switch priority is used by the operations personnel or TAC support personnel to decide which Call Home message should be responded to first. You can prioritize Call Home alerts of the same severity from each switch.
Step 11	**commit** **Example:** `switch(config-callhome)# commit`	Commits the Smart Call Home configuration commands.
Step 12	(Optional) **show callhome** **Example:** `switch(config-callhome)# show callhome`	Displays a summary of the Smart Call Home configuration.
Step 13	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

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

	Command or Action	Purpose

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	**destination-profile** *name*
	Example:
	`switch(config-callhome)#`
	`destination-profile Noc101`
		Creates a new destination profile. The name can be any alphanumeric string up to 31 characters.

Step 4	**destination-profile** *name* **format** {**XML** | **full-txt** | **short-txt**}
	Example:
	`switch(config-callhome)#`
	`destination-profile Noc101 format`
	`full-txt`
		Sets the message format for the profile. The name can be any alphanumeric string up to 31 characters.

Step 5	**commit** **Example:** `switch(config-callhome)# commit`	Commits the Smart Call Home configuration commands.

Step 6	(Optional) **show callhome destination-profile** [**profile** *name*]
	Example:
	`switch(config-callhome)# show callhome`
	`destination-profile profile Noc101`
		Displays information about one or more destination profiles.

Step 7	(Optional) **copy running-config startup-config**
	Example:
	`switch(config)# copy running-config`
	`startup-config`
		Copies the running configuration to the startup configuration.

What to do next

Associate one or more alert groups with a destination profile.

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

	Command or Action	Purpose

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	**destination-profile** {*name* | **CiscoTAC-1** | **full-txt-destination** | **short-txt-destination**} **email-addr** *address*
	Example:
	`switch(config-callhome)#`
	`destination-profile full-txt-destination`
	`email-addr person@place.com`
		Configures an email address for a user-defined or predefined destination profile. You can configure up to 50 email addresses in a destination profile.

Step 4	**destination-profile** {*name* | **CiscoTAC-1** | **full-txt-destination** | **short-txt-destination**} **http** *address*
	Example:
	`switch(config-callhome)#`
	`destination-profile CiscoTAC-1 http`
	`http://site.com/service/callhome`
		Configures an HTTP or HTTPS URL for a user-defined or predefined destination profile. The URL can be up to 255 characters.

Step 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

	Command or Action	Purpose
	Example: `switch(config-callhome)# destination-profile CiscoTAC-1 transport-method http`	choose determines the configured destination addresses of that type.
Step 6	**destination-profile** {*name* | **CiscoTAC-1** | **full-txt-destination** | **short-txt-destination**} **message-level** *number* **Example:** `switch(config-callhome)# destination-profile full-txt-destination message-level 5`	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.
Step 7	**destination-profile** {*name* | **CiscoTAC-1** | **full-txt-destination** | **short-txt-destination**} **message-size** *number* **Example:** `switch(config-callhome)# destination-profile full-txt-destination message-size 100000`	Configures the maximum message size for this destination profile. The range is from 0 to 5000000. The default is 2500000.
Step 8	**commit** **Example:** `switch(config-callhome)# commit`	Commits the Smart Call Home configuration commands.
Step 9	(Optional) **show callhome destination-profile** [**profile** *name*] **Example:** `switch(config-callhome)# show callhome destination-profile profile full-text-destination`	Displays information about one or more destination profiles.
Step 10	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

What to do next

Associate one or more alert groups with a destination profile.

Associating an Alert Group with a Destination Profile

Procedure

	Command or Action	Purpose

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	**destination-profile** {*name* | **CiscoTAC-1** | **full-txt-destination** | **short-txt-destination**} **alert-group** {**All** | **Cisco-TAC** | **Configuration** | **Diagnostic** | **EEM** | **Environmental** | **Inventory** | **License** | **Supervisor-Hardware** | **Syslog-group-port** | **System** | **Test**} **Example:** `switch(config-callhome)# destination-profile Noc101 alert-group All`	Associates an alert group with this destination profile. Use the **All** keyword to associate all alert groups with the destination profile.
Step 4	**commit** **Example:** `switch(config-callhome)# commit`	Commits the Smart Call Home configuration commands.
Step 5	(Optional) **show callhome destination-profile** [**profile** *name*] **Example:** `switch(config-callhome)# show callhome destination-profile profile Noc101`	Displays information about one or more destination profiles.
Step 6	(Optional) **copy running-config startup-config** **Example:** `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

	Command or Action	Purpose

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	**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 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.
Step 5	(Optional) **show callhome user-def-cmds** **Example:** `switch(config-callhome)# show callhome user-def-cmds`	Displays information about all user-defined **show** commands added to alert groups.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

What to do next

Configure Smart Call Home to connect to the SMTP email server.

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

	Command or Action	Purpose

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	**transport email mail-server** *ip-address* [**port** *number*] [**priority** *number*] [**use-vrf** *vrf-name*] **Example:** `switch(config-callhome)# transport email mail-server 192.0.2.1 use-vrf Red`	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. Also optionally configures the VRF to use when communicating with this SMTP server. The VRF specified is not used to send messages using HTTP.
Step 4	(Optional) **transport email from** *email-address* **Example:** `switch(config-callhome)# transport email from person@company.com`	Configures the email from field for Smart Call Home messages.
Step 5	(Optional) **transport email reply-to** *email-address* **Example:** `switch(config-callhome)# transport email reply-to person@company.com`	Configures the email reply-to field for Smart Call Home messages.

	Command or Action	Purpose
Step 6	**commit** **Example:** `switch(config-callhome)# commit`	Commits the Smart Call Home configuration commands.
Step 7	(Optional) **show callhome transport** **Example:** `switch(config-callhome)# show callhome transport`	Displays the transport-related configuration for Smart Call Home.
Step 8	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	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

	Command or Action	Purpose

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	**transport http use-vrf** *vrf-name* **Example:** `switch(config-callhome)# transport http use-vrf Blue`	Configures the VRF used to send email and other Smart Call Home messages over HTTP.
Step 4	**commit** **Example:** `switch(config-callhome)# commit`	Commits the Smart Call Home configuration commands.

	Command or Action	Purpose
Step 5	(Optional) **show callhome** **Example:** `switch(config-callhome)# show callhome`	Displays information about Smart Call Home.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

What to do next

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

Configuring an HTTP Proxy Server

Procedure

	Command or Action	Purpose

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	**transport http proxy server** *ip-address* [**port** *number*] **Example:** `switch(config-callhome)# transport http proxy server 192.0.2.1`	Configures the HTTP proxy server 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 8080.
Step 4	**transport http proxy enable** **Example:** `switch(config-callhome)# transport http proxy enable`	Enables Smart Call Home to send all HTTP messages through the HTTP proxy server. **Note** You can execute this command only after the proxy server address has been configured. **Note** The VRF used for transporting messages through the proxy server is the same as that configured using the **transport http use-vrf** command.

	Command or Action	Purpose
Step 5	**commit** **Example:** `switch(config-callhome)# commit`	Commits the Smart Call Home configuration commands.
Step 6	(Optional) **show callhome transport** **Example:** `switch(config-callhome)# show callhome transport`	Displays the transport-related configuration for Smart Call Home.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

What to do next

Optionally configure your device to periodically send inventory notifications.

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

	Command or Action	Purpose

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	**periodic-inventory notification** [**interval** *days*] [**timeofday** *time*] **Example:** `switch(config-callhome)# periodic-inventory notification interval 20`	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).
Step 4	**commit** **Example:**	Commits the Smart Call Home configuration commands.

	Command or Action	Purpose
	`switch(config-callhome)# commit`	
Step 5	(Optional) **show callhome** **Example:** `switch(config-callhome)# show callhome`	Displays information about Smart Call Home.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

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

	Command or Action	Purpose

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 duplicate-message throttle** **Example:** `switch(config-callhome)# no duplicate-message throttle`	Disables duplicate message throttling for Smart Call Home. Duplicate message throttling is enabled by default.
Step 4	**commit** **Example:** `switch(config-callhome)# commit`	Commits the Smart Call Home configuration commands.
Step 5	(Optional) **copy running-config startup-config** **Example:**	Copies the running configuration to the startup configuration.

	Command or Action	Purpose
	`switch(config)# copy running-config startup-config`	

What to do next

Enable Smart Call Home.

Enabling or Disabling Smart Call Home

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

Procedure

	Command or Action	Purpose

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.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

What to do next

Optionally generate a test message.

Testing the Smart Call Home Configuration

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

Procedure

	Command or Action	Purpose

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	**callhome send** [**configuration** | **diagnostic**] **Example:** `switch(config-callhome)# callhome send diagnostic`	Sends the specified Smart Call Home test message to all configured destinations.
Step 4	**callhome test** **Example:** `switch(config-callhome)# callhome test`	Sends a test message to all configured destinations.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Verifying the Smart Call Home Configuration

To display Smart Call Home configuration information, perform one of the following tasks:

Command	Purpose
show callhome	Displays the Smart Call Home configuration.
show callhome destination-profile *name*	Displays one or more Smart Call Home destination profiles.
show callhome merge	Displays the status of the last CFS merger for Smart Call Home.
show callhome pending	Displays the Smart Call Home configuration changes in the pending CFS database.
show callhome pending-diff	Displays the differences between the pending and running Smart Call Home configuration.

Command	Purpose
show callhome session-status	Displays the status of the last CFS commit or abort operation.
show callhomestatus	Displays the CFS distribution state (enabled or disabled) for Smart Call Home.
show callhome transport	Displays the transport-related configuration for Smart Call Home.
show callhome user-def-cmds	Displays CLI commands added to any alert groups.
show running-config callhome [**all**]	Displays the running configuration for Smart Call Home.
show startup-config callhome	Displays the startup configuration for Smart Call Home.
show tech-support callhome	Displays the technical support output for Smart Call Home.

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:

```
configure terminal
snmp-server contact person@company.com
callhome
distribute
email-contact admin@Mycompany.com
phone-contact +1-800-123-4567
streetaddress 123 Anystreet st. Anytown,AnyWhere
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-cmd 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:

```
configure terminal
callhome
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
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)

172.21.34.193 (priority 50, which is the default)

64.72.101.213 (priority 60)

Note 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.

Alert Group	Event Name	Description	Smart Call Home Severity Level
Configuration	PERIODIC_CONFIGURATION	Periodic configuration update message.	2
Diagnostic	DIAGNOSTIC_MAJOR_ALERT	GOLD generated a major alert.	7
	DIAGNOSTIC_MINOR_ALERT	GOLD generated a minor alert.	4
	DIAGNOSTIC_NORMAL_ALERT	Smart Call Home generated a normal diagnostic alert.	2

Alert Group	Event Name	Description	Smart Call Home Severity Level
Environmental and CISCO_TAC	FAN_FAILURE	Cooling fan has failed.	5
	POWER_SUPPLY_ALERT	Power supply warning has occurred.	6
	POWER_SUPPLY_FAILURE	Power supply has failed.	6
	POWER_SUPPLY_SHUTDOWN	Power supply has shut down.	6
	TEMPERATURE_ALARM	Thermal sensor going bad.	6
	TEMPERATURE_MAJOR_ALARM	Thermal sensor indicates temperature has reached operating major threshold.	6
	TEMPERATURE_MINOR_ALARM	Thermal sensor indicates temperature has reached operating minor threshold.	4
Inventory and CISCO_TAC	COLD_BOOT	Switch is powered up and reset to a cold boot sequence.	2
	HARDWARE_INSERTION	New piece of hardware has been inserted into the chassis.	2
	HARDWARE_REMOVAL	Hardware has been removed from the chassis.	2
	PERIODIC_INVENTORY	Periodic inventory message has been generated.	2
License	LICENSE_VIOLATION	Feature in use is not licensed and is turned off after grace period expiration.	6
Line module Hardware and CISCO_TAC	LINEmodule_FAILURE	Module operation has failed.	7
Supervisor Hardware and CISCO_TAC	SUP_FAILURE	Supervisor module operation has failed.	7
Syslog-group-port	PORT_FAILURE	syslog message that corresponds to the port facility has been generated.	6
	SYSLOG_ALERT	syslog alert message has been generated.	5

Alert Group	Event Name	Description	Smart Call Home Severity Level
System and CISCO_TAC	SW_CRASH	Software process has failed with a stateless restart, indicating an interruption of a service. Messages are sent for process crashes on supervisor modules.	5
	SW_SYSTEM_INCONSISTENT	Inconsistency has been detected in software or file system.	5
Test and CISCO_TAC	TEST	User generated test has occurred.	2

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.

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

Common Event Message Fields

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

Data Item (Plain Text and XML)	Description (Plain Text and XML)	XML Tag (XML Only)
Timestamp	Date and time stamp of event in ISO time notation: YYYY-MM-DD HH:MM:SS GMT+HH:MM.	/aml/header/time
Message name	Name of message.	/aml/header/name
Message type	Name of message type, such as reactive or proactive.	/aml/header/type
Message group	Name of alert group, such as syslog.	/aml/header/group
Severity level	Severity level of message.	/aml/header/level

Data Item (Plain Text and XML)	Description (Plain Text and XML)	XML Tag (XML Only)
Source ID	Product type for routing, such as the Catalyst 6500 series switch.	/aml/header/source
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 WS-C6509@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 WS-C6509@C@12345678.	/aml/header/serverId

Data Item (Plain Text and XML)	Description (Plain Text and XML)	XML Tag (XML Only)
Message description	Short text that describes the error.	/aml/body/msgDesc
Device name	Node that experienced the event (hostname of the device).	/aml/body/sysName
Contact name	Name of person to contact for issues associated with the node that experienced the event.	/aml/body/sysContact
Contact email	Email address of person identified as the contact for this unit.	/aml/body/sysContactEmail
Contact phone number	Phone number of the person identified as the contact for this unit.	/aml/body/sysContactPhone Number
Street address	Optional field that contains the street address for RMA part shipments associated with this unit.	/aml/body/sysStreetAddress
Model name	Model name of the device (the specific model as part of a product family name).	/aml/body/chassis/name
Serial number	Chassis serial number of the unit.	/aml/body/chassis/serialNo
Chassis part number	Top assembly number of the chassis.	/aml/body/chassis/partNo

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.

Data Item (Plain Text and XML)	Description (Plain Text and XML)	XML Tag (XML Only)
Command output name	Exact name of the issued CLI command.	/aml/attachments/attachment/name
Attachment type	Specific command output.	/aml/attachments/attachment/type
MIME type	Either plain text or encoding type.	/aml/attachments/attachment/mime
Command output text	Output of command automatically executed.	/aml/attachments/attachment/atdata

Fields for Reactive and Proactive Event Messages

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

Data Item (Plain Text and XML)	Description (Plain Text and XML)	XML Tag (XML Only)
Chassis hardware version	Hardware version of chassis.	/aml/body/chassis/hwVersion

Data Item (Plain Text and XML)	Description (Plain Text and XML)	XML Tag (XML Only)
Supervisor module software version	Top-level software version.	/aml/body/chassis/swVersion
Affected FRU name	Name of the affected FRU that is generating the event message.	/aml/body/fru/name
Affected FRU serial number	Serial number of the affected FRU.	/aml/body/fru/serialNo
Affected FRU part number	Part number of the affected FRU.	/aml/body/fru/partNo
FRU slot	Slot number of the FRU that is generating the event message.	/aml/body/fru/slot
FRU hardware version	Hardware version of the affected FRU.	/aml/body/fru/hwVersion
FRU software version	Software version(s) that is running on the affected FRU.	/aml/body/fru/swVersion

Fields for Inventory Event Messages

The following table describes the inventory event message format for full text or XML messages.

Data Item (Plain Text and XML)	Description (Plain Text and XML)	XML Tag (XML Only)
Chassis hardware version	Hardware version of the chassis.	/aml/body/chassis/hwVersion
Supervisor module software version	Top-level software version.	/aml/body/chassis/swVersion
FRU name	Name of the affected FRU that is generating the event message.	/aml/body/fru/name
FRU s/n	Serial number of the FRU.	/aml/body/fru/serialNo
FRU part number	Part number of the FRU.	/aml/body/fru/partNo
FRU slot	Slot number of the FRU.	/aml/body/fru/slot
FRU hardware version	Hardware version of the FRU.	/aml/body/fru/hwVersion
FRU software version	Software version(s) that is running on the FRU.	/aml/body/fru/swVersion

Fields for User-Generated Test Messages

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

Data Item (Plain Text and XML)	Description (Plain Text and XML)	XML Tag (XML Only)
Process ID	Unique process ID.	/aml/body/process/id
Process state	State of process (for example, running or halted).	/aml/body/process/processState

Data Item (Plain Text and XML)	Description (Plain Text and XML)	XML Tag (XML Only)
Process exception	Exception or reason code.	/aml/body/process/exception

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:Nexus7000
Switch Priority:0
Device Id:N7K-C7010@C@TXX12345678
Server Id:N7K-C7010@C@TXX12345678
Time of Event:2008-01-17 16:31:33 GMT+0000 Message Name:
Message Type: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 2008 Jan 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:N7K-C7010
Affected Chassis Serial Number:TXX12345678 Affected Chassis Hardware Version:0.405 Affected
 Chassis Software
Version:4.1(1) Affected Chassis Part No:73-10900-04 end chassis information:
start attachment
name:show logging logfile | tail -n 200
type:text
data:
2008 Jan 17 10:57:51 dc3-test %SYSLOG-1-SYSTEM_MSG : Logging logfile (messages) cleared by
 user
2008 Jan 17 10:57:53 dc3-test %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from
/dev/ttyS0 /dev/ttyS0_console
2008 Jan 17 10:58:35 dc3-test %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from
/dev/ttyS0 /dev/ttyS0_console
2008 Jan 17 10:59:00 dc3-test %DAEMON-3-SYSTEM_MSG: error: setsockopt IP_TOS 16: Invalid
argument: - sshd[14484]
2008 Jan 17 10:59:05 dc3-test %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from
/dev/ttyS0 /dev/ttyS0_console
2008 Jan 17 12:11:18 dc3-test %SYSMGR-STANDBY-5-SUBPROC_TERMINATED: "System Manager (gsync
 controller)" (PID 12000)
has finished with error code SYSMGR_EXITCODE_GSYNCFAILED_NONFATAL (12).
2008 Jan 17 16:28:03 dc3-test %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from
/dev/ttyS0 /dev/ttyS0_console
2008 Jan 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 .
2008 Jan 17 16:28:44 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID 3504) hasn't
caught signal 9 (no core).
2008 Jan 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.
2008 Jan 17 16:29:08 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID 23210) hasn't
 caught signal 9 (no core).
2008 Jan 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.
2008 Jan 17 16:29:17 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID 23294) hasn't
 caught signal 9 (no core).
2008 Jan 17 16:29:25 dc3-test %SYSMGR-2-HASWITCHOVER_PRE_START: This supervisor is becoming
 active (pre-start phase).
2008 Jan 17 16:29:25 dc3-test %SYSMGR-2-HASWITCHOVER_START: This supervisor is becoming
active.
2008 Jan 17 16:29:26 dc3-test %USER-3-SYSTEM_MSG: crdcfg_get_srvinfo: mts_send failed -
device_test
2008 Jan 17 16:29:27 dc3-test %NETSTACK-3-IP_UNK_MSG_MAJOR: netstack [4336] Unrecognized
message from MRIB. Major
type 1807
2008 Jan 17 16:29:27 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is DOWN in vdc 1
2008 Jan 17 16:29:27 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is DOWN in vdc 2
2008 Jan 17 16:29:27 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is DOWN in vdc 3
2008 Jan 17 16:29:27 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is DOWN in vdc 4
2008 Jan 17 16:29:28 dc3-test %SYSMGR-2-SWITCHOVER_OVER: Switchover completed.
2008 Jan 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:socket family : 2 - ntpd[19045]
2008 Jan 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:socket family : 10 - ntpd[19045]
2008 Jan 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:ipv6 only defined - ntpd[19045]
2008 Jan 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:bindv6 only defined - ntpd[19045]
2008 Jan 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:socket family : 2 - ntpd[19045]
2008 Jan 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:socket family : 0 - ntpd[19045]
2008 Jan 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:socket family : 0 - ntpd[19045]
2008 Jan 17 16:29:28 dc3-test %NETSTACK-3-CLIENT_GET: netstack [4336] HA client filter
recovery failed (0)
2008 Jan 17 16:29:28 dc3-test %NETSTACK-3-CLIENT_GET: netstack [4336] HA client filter
recovery failed (0)
2008 Jan 17 16:29:29 dc3-test %DAEMON-3-SYSTEM_MSG: ssh disabled, removing -
dcos-xinetd[19072]
2008 Jan 17 16:29:29 dc3-test %DAEMON-3-SYSTEM_MSG: Telnet disabled, removing -
dcos-xinetd[19072]
2008 Jan 17 16:29:31 dc3-test %DAEMON-3-SYSTEM_MSG: Telnet disabled, removing -
dcos-xinetd[19073]
2008 Jan 17 16:29:32 dc3-test %DAEMON-3-SYSTEM_MSG: ssh disabled, removing -
dcos-xinetd[19079]
2008 Jan 17 16:29:32 dc3-test %DAEMON-3-SYSTEM_MSG: Telnet disabled, removing -
dcos-xinetd[19079]
2008 Jan 17 16:29:34 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is UP in vdc 1
2008 Jan 17 16:29:34 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is UP in vdc 2
2008 Jan 17 16:29:34 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is UP in vdc 3
2008 Jan 17 16:29:34 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is UP in vdc 4
2008 Jan 17 16:29:34 dc3-test %DAEMON-3-SYSTEM_MSG: ssh disabled, removing -
dcos-xinetd[19105]
2008 Jan 17 16:29:34 dc3-test %DAEMON-3-SYSTEM_MSG: Telnet disabled, removing -
dcos-xinetd[19105]
2008 Jan 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
2008 Jan 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
2008 Jan 17 16:29:38 dc3-test %CALLHOME-2-EVENT: SUP_FAILURE
2008 Jan 17 16:29:46 dc3-test vsh[19166]: CLIC-3-FAILED_EXEC: Can not exec command <more>
return code <14>
2008 Jan 17 16:30:24 dc3-test vsh[23810]: CLIC-3-FAILED_EXEC: Can not exec command <more>
return code <14>
2008 Jan 17 16:30:24 dc3-test vsh[23803]: CLIC-3-FAILED_EXEC: Can not exec command <more>
return code <14>
2008 Jan 17 16:30:24 dc3-test vsh[23818]: CLIC-3-FAILED_EXEC: Can not exec command <more>
return code <14>
2008 Jan 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 .
```

```
2008 Jan 17 16:30:47 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID 4820) hasn't
caught signal 9
(no core).
2008 Jan 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 .
2008 Jan 17 16:31:02 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID 24239) hasn't
 caught signal 9
(no core).
2008 Jan 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 .
2008 Jan 17 16:31:14 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID 24401) hasn't
 caught signal 9
(no core).
2008 Jan 17 16:31:23 dc3-test %CALLHOME-2-EVENT: SW_CRASH alert for service: eltm
2008 Jan 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 .
2008 Jan 17 16:31:23 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID 24407) hasn't
 caught signal 9
(no core).
2008 Jan 17 16:31:24 dc3-test vsh[24532]: CLIC-3-FAILED_EXEC: Can not exec command <more>
return code <14>
2008 Jan 17 16:31:24 dc3-test vsh[24548]: CLIC-3-FAILED_EXEC: Can not exec command <more>
return code <14>
2008 Jan 17 16:31:24 dc3-test vsh[24535]: CLIC-3-FAILED_EXEC: Can not exec command <more>
return code <14>
2008 Jan 17 16:31:33 dc3-test %NETSTACK-3-INTERNAL_ERROR: netstack [4336] (null)
2008 Jan 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) end attachment start
attachment
name:show vdc membership
type:text
data:
vdc_id: 1 vdc_name: dc3-test interfaces:
Ethernet3/1 Ethernet3/2 Ethernet3/3
Ethernet3/4 Ethernet3/5 Ethernet3/6
Ethernet3/7 Ethernet3/8 Ethernet3/9
Ethernet3/10 Ethernet3/11 Ethernet3/12
Ethernet3/13 Ethernet3/14 Ethernet3/15
Ethernet3/16 Ethernet3/17 Ethernet3/18
Ethernet3/19 Ethernet3/20 Ethernet3/21
Ethernet3/22 Ethernet3/23 Ethernet3/24
Ethernet3/25 Ethernet3/26 Ethernet3/27
Ethernet3/28 Ethernet3/29 Ethernet3/30
Ethernet3/31 Ethernet3/32 Ethernet3/33
Ethernet3/34 Ethernet3/35 Ethernet3/36
Ethernet3/37 Ethernet3/38 Ethernet3/39
Ethernet3/40 Ethernet3/41 Ethernet3/42
Ethernet3/43 Ethernet3/44 Ethernet3/45
Ethernet3/46 Ethernet3/47 Ethernet3/48
vdc_id: 2 vdc_name: dc3-aaa interfaces:
vdc_id: 3 vdc_name: dc3-rbac interfaces:
vdc_id: 4 vdc_name: dc3-call interfaces:
end attachment
start attachment
name:show vdc current-vdc
type:text
data:
Current vdc is 1 - dc3-test
end attachment
start attachment
```

```
name:show license usage
type:text
data:
Feature Ins Lic Status Expiry Date Comments
Count
--------------------------------------------------------------------------------
LAN_ADVANCED_SERVICES_PKG Yes - In use Never -
LAN_ENTERPRISE_SERVICES_PKG Yes - Unused Never -
--------------------------------------------------------------------------------
end attachment
```

Sample Syslog Alert Notification in XML Format

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

```
<?xml version="1.0" encoding="UTF-8" ?>
<soap-env:Envelope xmlns:soap-env="http://www.w3.org/2003/05/soap-envelope">
<soap-env:Header>
<aml-session:Session xmlns:aml-session="http://www.cisco.com/2004/01/aml-session"
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:From>http://www.cisco.com/appliance/uri</aml-session:From>
<aml-session:MessageId>1004:TXX12345678:478F82E6</aml-session:MessageId>
</aml-session:Session>
</soap-env:Header>
<soap-env:Body>
<aml-block:Block xmlns:aml-block="http://www.cisco.com/2004/01/aml-block">
<aml-block:Header>
<aml-block:Type>http://www.cisco.com/2005/05/callhome/syslog</aml-block:Type>
<aml-block:CreationDate>2008-01-17 16:31:33 GMT+0000</aml-block:CreationDate>
<aml-block:Builder>
<aml-block:Name>DC3</aml-block:Name>
<aml-block:Version>4.1</aml-block:Version>
</aml-block:Builder>
<aml-block:BlockGroup>
<aml-block:GroupId>1005:TXX12345678:478F82E6</aml-block:GroupId>
<aml-block:Number>0</aml-block:Number>
<aml-block:IsLast>true</aml-block:IsLast>
<aml-block:IsPrimary>true</aml-block:IsPrimary>
<aml-block:WaitForPrimary>false</aml-block:WaitForPrimary>
</aml-block:BlockGroup>
<aml-block:Severity>5</aml-block:Severity>
</aml-block:Header>
<aml-block:Content>
<ch:CallHome xmlns:ch="http://www.cisco.com/2005/05/callhome" version="1.0">
<ch:EventTime>2008-01-17 16:31:33 GMT+0000</ch:EventTime> <ch:MessageDescription>SYSLOG_ALERT
 2008 Jan 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:Series>Nexus7000</ch:Series> </ch:Event> <ch:CustomerData>
<ch:UserData>
<ch:Email>contact@example.com</ch:Email>
</ch:UserData>
<ch:ContractData>
<ch:DeviceId>N7K-C7010@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>N7K-C7010</rme:Model>
<rme:HardwareVersion>0.405</rme:HardwareVersion>
<rme:SerialNumber>TXX12345678</rme:SerialNumber>
</rme:Chassis>
</ch:Device>
</ch:CallHome>
</aml-block:Content>
<aml-block:Attachments>
<aml-block:Attachment type="inline">
<aml-block:Name>show logging logfile | tail -n 200</aml-block:Name> <aml-block:Data
encoding="plain">
<![CDATA[2008 Jan 17 10:57:51 dc3-test %SYSLOG-1-SYSTEM_MSG : Logging logfile (messages)
cleared by user
2008 Jan 17 10:57:53 dc3-test %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from
/dev/ttyS0 /dev/ttyS0_console
2008 Jan 17 10:58:35 dc3-test %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from
/dev/ttyS0 /dev/ttyS0_console
2008 Jan 17 10:59:00 dc3-test %DAEMON-3-SYSTEM_MSG: error: setsockopt IP_TOS 16: Invalid
argument: - sshd[14484]
2008 Jan 17 10:59:05 dc3-test %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from
/dev/ttyS0 /dev/ttyS0_console
2008 Jan 17 12:11:18 dc3-test %SYSMGR-STANDBY-5-SUBPROC_TERMINATED: \"System Manager (gsync
 controller)\"
(PID 12000) has finished with error code SYSMGR_EXITCODE_GSYNCFAILED_NONFATAL (12).
2008 Jan 17 16:28:03 dc3-test %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from
/dev/ttyS0 /dev/ttyS0_console
2008 Jan 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 .
2008 Jan 17 16:28:44 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service \"eltm\" (PID 3504)
hasn&apos;t caught signal 9
(no core).
2008 Jan 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 .
2008 Jan 17 16:29:08 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service \"eltm\" (PID 23210)
hasn&apos;t caught signal 9
(no core).
2008 Jan 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 .
2008 Jan 17 16:29:17 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service \"eltm\" (PID 23294)
hasn&apos;t caught signal 9
(no core).
2008 Jan 17 16:29:25 dc3-test %SYSMGR-2-HASWITCHOVER_PRE_START: This supervisor is becoming
 active (pre-start phase).
2008 Jan 17 16:29:25 dc3-test %SYSMGR-2-HASWITCHOVER_START: This supervisor is becoming
active.
2008 Jan 17 16:29:26 dc3-test %USER-3-SYSTEM_MSG: crdcfg_get_srvinfo: mts_send failed -
device_test
2008 Jan 17 16:29:27 dc3-test %NETSTACK-3-IP_UNK_MSG_MAJOR: netstack [4336] Unrecognized
message from MRIB.
Major type 1807
2008 Jan 17 16:29:27 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is DOWN in vdc 1
2008 Jan 17 16:29:27 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is DOWN in vdc 2
2008 Jan 17 16:29:27 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is DOWN in vdc 3
2008 Jan 17 16:29:27 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is DOWN in vdc 4
```

```
2008 Jan 17 16:29:28 dc3-test %SYSMGR-2-SWITCHOVER_OVER: Switchover completed.
2008 Jan 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:socket family : 2 - ntpd[19045]
2008 Jan 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:socket family : 10 - ntpd[19045]
2008 Jan 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:ipv6 only defined - ntpd[19045]
2008 Jan 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:bindv6 only defined - ntpd[19045]
2008 Jan 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:socket family : 2 - ntpd[19045]
2008 Jan 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:socket family : 0 - ntpd[19045]
2008 Jan 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:socket family : 0 - ntpd[19045]
2008 Jan 17 16:29:28 dc3-test %NETSTACK-3-CLIENT_GET: netstack [4336] HA client filter
recovery failed (0)
2008 Jan 17 16:29:28 dc3-test %NETSTACK-3-CLIENT_GET: netstack [4336] HA client filter
recovery failed (0)
2008 Jan 17 16:29:29 dc3-test %DAEMON-3-SYSTEM_MSG: ssh disabled, removing -
dcos-xinetd[19072]
2008 Jan 17 16:29:29 dc3-test %DAEMON-3-SYSTEM_MSG: Telnet disabled, removing -
dcos-xinetd[19072]
2008 Jan 17 16:29:31 dc3-test %DAEMON-3-SYSTEM_MSG: Telnet disabled, removing -
dcos-xinetd[19073]
2008 Jan 17 16:29:32 dc3-test %DAEMON-3-SYSTEM_MSG: ssh disabled, removing -
dcos-xinetd[19079]
2008 Jan 17 16:29:32 dc3-test %DAEMON-3-SYSTEM_MSG: Telnet disabled, removing -
dcos-xinetd[19079]
2008 Jan 17 16:29:34 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is UP in vdc 1
2008 Jan 17 16:29:34 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is UP in vdc 2
2008 Jan 17 16:29:34 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is UP in vdc 3
2008 Jan 17 16:29:34 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is UP in vdc 4
2008 Jan 17 16:29:34 dc3-test %DAEMON-3-SYSTEM_MSG: ssh disabled, removing -
dcos-xinetd[19105]
2008 Jan 17 16:29:34 dc3-test %DAEMON-3-SYSTEM_MSG: Telnet disabled, removing -
dcos-xinetd[19105]
2008 Jan 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
2008 Jan 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
2008 Jan 17 16:29:38 dc3-test %CALLHOME-2-EVENT: SUP_FAILURE
2008 Jan 17 16:29:46 dc3-test vsh[19166]: CLIC-3-FAILED_EXEC: Can not exec command
&lt;more&gt; return code &lt;14&gt;
2008 Jan 17 16:30:24 dc3-test vsh[23810]: CLIC-3-FAILED_EXEC: Can not exec command
&lt;more&gt; return code &lt;14&gt;
2008 Jan 17 16:30:24 dc3-test vsh[23803]: CLIC-3-FAILED_EXEC: Can not exec command
&lt;more&gt; return code &lt;14&gt;
2008 Jan 17 16:30:24 dc3-test vsh[23818]: CLIC-3-FAILED_EXEC: Can not exec command
&lt;more&gt; return code &lt;14&gt;
2008 Jan 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 .
2008 Jan 17 16:30:47 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service \"eltm\" (PID 4820)
hasn&apos;t caught signal 9
(no core).
2008 Jan 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 .
2008 Jan 17 16:31:02 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service \"eltm\" (PID 24239)
hasn&apos;t caught signal 9
(no core).
2008 Jan 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 .
2008 Jan 17 16:31:14 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service \"eltm\" (PID 24401)
hasn&apos;t caught signal 9
(no core).
2008 Jan 17 16:31:23 dc3-test %CALLHOME-2-EVENT: SW_CRASH alert for service: eltm
```

```
2008 Jan 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 .
2008 Jan 17 16:31:23 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service \"eltm\" (PID 24407)
hasn&apos;t caught signal 9
(no core).
2008 Jan 17 16:31:24 dc3-test vsh[24532]: CLIC-3-FAILED_EXEC: Can not exec command
&lt;more&gt; return code &lt;14&gt;
2008 Jan 17 16:31:24 dc3-test vsh[24548]: CLIC-3-FAILED_EXEC: Can not exec command
&lt;more&gt; return code &lt;14&gt;
2008 Jan 17 16:31:24 dc3-test vsh[24535]: CLIC-3-FAILED_EXEC: Can not exec command
&lt;more&gt; return code &lt;14&gt;
2008 Jan 17 16:31:33 dc3-test %NETSTACK-3-INTERNAL_ERROR: netstack [4336] (null)
2008 Jan 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 vdc
membership</aml-block:Name>
<aml-block:Data encoding="plain"> <![CDATA[
vdc_id: 1 vdc_name: dc3-test interfaces:
Ethernet3/1 Ethernet3/2 Ethernet3/3
Ethernet3/4 Ethernet3/5 Ethernet3/6
Ethernet3/7 Ethernet3/8 Ethernet3/9
Ethernet3/10 Ethernet3/11 Ethernet3/12
Ethernet3/13 Ethernet3/14 Ethernet3/15
Ethernet3/16 Ethernet3/17 Ethernet3/18
Ethernet3/19 Ethernet3/20 Ethernet3/21
Ethernet3/22 Ethernet3/23 Ethernet3/24
Ethernet3/25 Ethernet3/26 Ethernet3/27
Ethernet3/28 Ethernet3/29 Ethernet3/30
Ethernet3/31 Ethernet3/32 Ethernet3/33
Ethernet3/34 Ethernet3/35 Ethernet3/36
Ethernet3/37 Ethernet3/38 Ethernet3/39
Ethernet3/40 Ethernet3/41 Ethernet3/42
Ethernet3/43 Ethernet3/44 Ethernet3/45
Ethernet3/46 Ethernet3/47 Ethernet3/48
vdc_id: 2 vdc_name: dc3-aaa interfaces:
vdc_id: 3 vdc_name: dc3-rbac interfaces:
vdc_id: 4 vdc_name: dc3-call interfaces:


]]>
</aml-block:Data>
</aml-block:Attachment>
<aml-block:Attachment type="inline">
<aml-block:Name>show vdc current-vdc</aml-block:Name> <aml-block:Data encoding="plain">
<![CDATA[Current vdc
is 1 - dc3-test ]]> </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_ADVANCED_SERVICES_PKG Yes - In use Never -
LAN_ENTERPRISE_SERVICES_PKG Yes - Unused Never -
--------------------------------------------------------------------------------
]]>
</aml-block:Data>
</aml-block:Attachment>
</aml-block:Attachments>
</aml-block:Block>
</soap-env:Body>
</soap-env:Envelope>
```

Additional References

Related Documents

Related Topic	Document Title
Smart Call CLI commands	*Cisco Nexus 7000 Series NX-OS System Management Command Reference*
VDCs and VRFs	*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*

MIBs

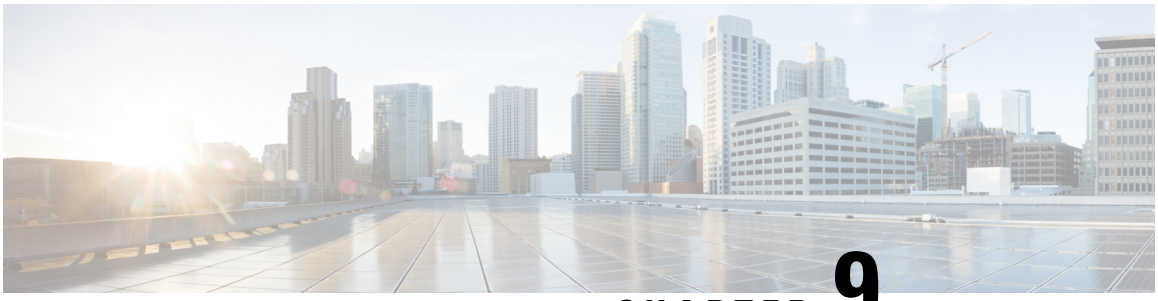
MIBs	MIBs Link
MIBs related to Smart Call Home	To locate and download supported MIBs, go to the following URL: ftp://ftp.cisco.com/pub/mibs/supportlists/nexus7000/Nexus7000MIBSupportList.html

Feature History for Smart Call Home

Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Table 16: Feature History for Smart Call Home

Feature Name	Releases	Feature Information
HTTP proxy server	5.2(1)	Added the ability to send HTTP messages through an HTTP proxy server.
SMTP server configuration	5.0(2)	Added the ability to configure multiple SMTP servers.
VRF support for HTTP transport of Smart Call Home messages	5.0(2)	VRFs can be used to send e-mail and other Smart Call Home messages over HTTP.
Crash notifications	4.0(1)	Messages are sent for process crashes on line cards.
Destination profile configuration	4.1(3)	The commands **destination-profile http** and destination-profile **transport-method** cannot be distributed.



CHAPTER 9

Configuring Rollback

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

This chapter contains the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

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 in the virtual device context (VDC) that you are logged into. You can create different checkpoint copies in each VDC. You cannot apply the checkpoint of one VDC into another VDC. By default, Cisco NX-OS places you in the default VDC. See the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*.

VDC configuration does not support checkpoints for any operations, including (but not limited to) VDC creation, VDC deletion, VDC suspension, VDC reloading, VDC renaming, VDC interface allocation, shared interface allocation, FCoE VLAN allocation, resource allocation, and resource templates. You should create your checkpoint from within a specific VDC.

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 apply a checkpoint configuration in a nondefault VDC if there is a change in the global configuration portion of the running configuration compared to the checkpoint configuration.
- Your checkpoint filenames must be 80 characters or less.
- You cannot start a checkpoint filename with the word *system*.
- Beginning in Cisco NX-OS Release 4.2(1), you can start a checkpoint filename with the word *auto*.
- Beginning in Cisco NX-OS Release 4.2(1), 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.
- A rollback fails for NetFlow if during a rollback, you try to modify a record that is programmed in the hardware.
- 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 are local to a virtual device context (VDC).

- Checkpoints created using the **checkpoint** and **checkpoint** *checkpoint_name* commands are present upon a switchover.
- Checkpoints created in the default VDC are present upon reload unless a **write-erase** command is issued before a reload.
- Checkpoints created in nondefault VDCs are present upon reload only if a **copy running-config startup-config** command is issued in the applicable VDC *and* the default VDC.
- A rollback to files on bootflash is supported only on files 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 storage VDC.
- Rollback is not supported in the Admin virtual device context (VDC) feature.
- Configure the **terminal dont-ask** command before executing the **rollback** command to a checkpoint. In a rollback patch, the rollback process does not pause for user interaction and takes the default values for interactive commands. Configuring the **terminal dont-ask** command before executing the **rollback** command helps in resolving this issue.
- 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.
- When you perform rollback, if the patch contains the **reload** command for the corresponding module along with the configuration commands for that module, rollback fails. This is because the rollback action does not wait for the module to come online; it starts executing the configuration commands on the module even as the reload process is in progress. To resolve this issue, manually execute the configuration commands for the module *after* the module is online.

  Examples:

  - A rollback fails when you execute the **bfd hw-offload-module** command or the **no** form of this command. In this instance, failure is because rollback cannot execute these commands when the switch interfaces that are a part of the BFD sessions are powered up. To resolve this issue, shut down all the interfaces that are a part of the BFD sessions using the **shutdown** command before executing the **bfd hw-offload-module** command or the **no** form of this command.
  - The following BFD command configurations are not supported during a rollback configuration:
    - **bfd** {**ipv4 | ipv6**} **echo**
    - **bfd** {**ipv4 | ipv6**} **per-link**
    - **bfd hw-offload-module** *module-number*
    - **port-channel bfd track-member-link**
    - **port-channel bfd destination** *destination-ip-address*
  - When an FEX is being configured while a rollback vPC is applied to an interface, the FEX goes offline momentarily. When this occurs, rollback does not wait for the FEX to come online, and executes the configuration commands for the interface, resulting in failure because the corresponding

FEX is not yet provisioned. To resolve this issue, manually execute the FEX-related configuration commands *after* the FEX is online.

- Checkpoint descriptions are not persistent across switch reloads. When a description for a checkpoint is created by using the **checkpoint** *description* command, the description is not visible in the output of the **show checkpoint summary** command after the switch is reloaded. If the checkpoint description can be qualified as a checkpoint name, we recommend using the same alphanumeric string for both the checkpoint name and description. The checkpoint name is visible in the output of the **show checkpoint summary** command even after the switch is reloaded

Default Settings for Rollbacks

This table lists the default settings for rollback parameters.

Parameters	Default
Rollback type	Atomic

Configuring Rollbacks

Note 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

	Command or Action	Purpose
Step 1	[**no**] **checkpoint** {[*cp-name*] [**description** *descr*] | **file** *file-name* } **Example:** `switch# checkpoint stable`	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.

	Command or Action	Purpose
Step 2	(Optional) **show checkpoint** *cp-name* [**all**] **Example:** `switch# show checkpoint stable`	Displays the contents of the checkpoint name.

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.

Note If you make a configuration change during an atomic rollback, the rollback will fail.

Procedure

	Command or Action	Purpose
Step 1	**show diff rollback-patch** {**checkpoint** *src-cp-name* | **running-config** | **startup-config** | **file** *source-file*} {**checkpoint** *dest-cp-name* | **running-config** | **startup-config** | **file** *dest-file*} **Example:** `switch# show diff rollback-patch checkpoint stable running-config`	Displays the differences between the source and destination checkpoint selections.
Step 2	**rollback running-config** {**checkpoint** *cp-name* | **file** *cp-file*} [**atomic** | **best-effort** | **stop-at-first-failure**] **Example:** `switch# rollback running-config checkpoint stable`	Creates a rollback to the specified checkpoint name or file. You can implement 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 is atomic. This example shows how to implement a rollback to a user checkpoint name.

Verifying the Rollback Configuration

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

Command	Purpose
show checkpoint *name* [**all**]	Displays the contents of the checkpoint name.
show checkpoint all [**user** | **system**]	Displays the contents of all checkpoints. You can limit the displayed checkpoints to user or system generated checkpoints.
show checkpoint summary [**user** | **system**]	Displays a list of all checkpoints. You can limit the displayed checkpoints to user or system generated checkpoints.
show diff rollback-patch {**checkpoint** *src-cp-name* | **running-config** | **startup-config** | **file** *source-file*} {**checkpoint** *dest-cp-name* | **running-config** | **startup-config** | **file** *dest-file*}	Displays the differences between the source and destination checkpoint selections.
show rollback log [**exec** | **verify**]	Displays the contents of the rollback log.

Use the **clear checkpoint database** command to delete all checkpoint files.

Note When a **checkpoint** is created, you can view the default configuration **priority-flow-control mode auto** using the **show run all** command. You cannot view the configuration **priority-flow-control mode auto** using the **show run** command for the interface.

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

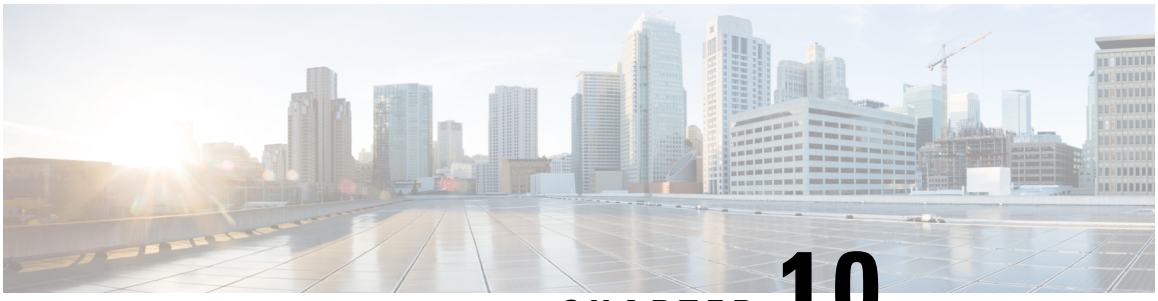
Related Topic	Document Title
Rollback CLI commands	*Cisco Nexus 7000 Series NX-OS System Management Command Reference*
VDCs	*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*
Configuration files	*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide*

Feature History for Rollback

Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Table 17: Feature History for Rollback

Feature Name	Releases	Feature Information
High Availability	4.2(1)	Checkpoint and rollback operations support high availability.
Guidelines and Limitations	4.2(1)	Checkpoint file naming conventions changed.
Automatically generated system checkpoints	4.2(1)	The software automatically generates a system checkpoint when disabling a feature or license expiration could cause loss of configuration information.
Guidelines and Limitations	4.1(3)	A rollback fails for NetFlow if during rollback, you try to modify a record that is programmed in the hardware. A rollback is not supported for checkpoints across software versions.



CHAPTER 10

Configuring Session Manager

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

This chapter contains the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

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.

Virtualization Support

By default, Cisco NX-OS places you in the default VDC. See the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*.

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:

- Session Manager supports only access control list (ACL) and quality of service (QoS) features.
- You can create up to 32 configuration sessions.
- You cannot issue an in-service software upgrade (ISSU) if an active session is in progress. You must commit the session, save it, or abort it before issuing an ISSU.
- You can configure a maximum of 20,000 commands across all sessions.
- You cannot simultaneously execute configuration commands in more then one configuration session or configuration terminal mode. Parallel configurations (for example, one configuration session and one configuration terminal) might cause validation or verification failures in the configuration session.
- If an interface reloads while you are configuring that interface in a configuration session, Session Manager may accept the commands even though the interface is not present in the device at that time.

Configuring Session Manager

Note 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

	Command or Action	Purpose

Step 1	**configure session** *name*
	Example:
	`switch# configure session myACLs`
	`switch(config-s)#`
		Creates a configuration session and enters session configuration mode. The name can be any alphanumeric string.
		Displays the contents of the session.

Step 2	(Optional) **show configuration session** [*name*] **Example:** `switch(config-s)# show configuration session myACLs`	Displays the contents of the session.
Step 3	(Optional) **save** *location* **Example:** `switch(config-s)# save bootflash:sessions/myACLs`	Saves the session to a file. The location can be in bootflash:, slot0:, or volatile:.

Configuring ACLs in a Session

You can configure ACLs within a configuration session.

Procedure

	Command or Action	Purpose

Step 1	**configure session** *name*
	Example:
	`switch# configure session myacls`
	`switch(config-s)#`
		Creates a configuration session and enters session configuration mode. The name can be any alphanumeric string.

Step 2	**ip access-list** *name*
	Example:
	`switch(config-s)# ip access-list acl1`
	`switch(config-s-acl)#`
		Creates an ACL and enters a configuration mode for that ACL.

	Command or Action	Purpose
Step 3	(Optional) **permit** *protocol source destination* **Example:** `switch(config-s-acl)# permit tcp any any`	Adds a permit statement to the ACL.

Step 4	**interface** *interface-type number*
	Example:
	`switch(config-s-acl)# interface e 2/1`
	`switch(config-s-if)#`
		Enters interface configuration mode.

Step 5	**ip access-group** *name* {**in** | **out**} **Example:** `switch(config-s-if)# ip access-group acl1 in`	Specifies the direction of traffic the access group is applied to.
Step 6	(Optional) **show configuration session** [*name*] **Example:** `switch(config-s)# show configuration session myacls`	Displays the contents of the session.

Verifying a Session

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

Command	Purpose
verify [**verbose**] **Example:** `switch(config-s)# verify`	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.

Committing a Session

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

Command	Purpose
commit [**verbose**] **Example:** `switch(config-s)# commit`	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.

Saving a Session

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

Command	Purpose
save *location* **Example:** `switch(config-s)# save bootflash:sessions/myACLs`	(Optional) Saves the session to a file. The location can be in bootflash:, slot0:, or volatile:.

Discarding a Session

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

Command	Purpose
abort **Example:** `switch(config-s)# abort switch#`	Discards the configuration session without applying the changes.

Verifying the Session Manager Configuration

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

Command	Purpose
show configuration session [*name*]	Displays the contents of the configuration session.
show configuration session status [*name*]	Displays the status of the configuration session.
show configuration session summary	Displays a summary of all the configuration sessions.

Configuration Example for Session Manager

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

```
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# config 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
```

```
switch#
```

Additional References

Related Documents

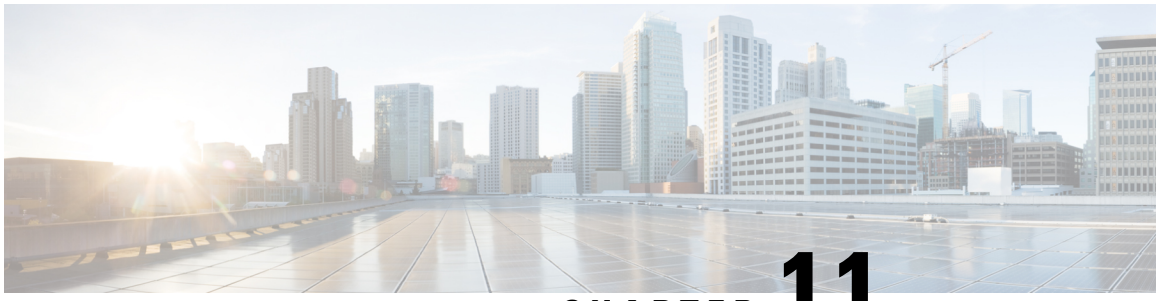
Related Topic	Document Title
Session Manager CLI commands	*Cisco Nexus 7000 Series NX-OS System Management Command Reference*
VDCs	*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*
Configuration files	*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide*

Feature History for Session Manager

Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Table 18: Feature History for Session Manager

Feature Name	Releases	Feature Information
Session Manager	4.0(1)	This feature was introduced.



CHAPTER 11

Configuring the Scheduler

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

This chapter includes the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

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.
    - Delta—A job begins at the specified start time and then at specified intervals (days:hours:minutes).
  - One-time mode—A job is completed only once at a specified time.

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.

Virtualization Support

Jobs are created in the virtual device context (VDC) that you are logged into. By default, Cisco NX-OS places you in the default VDC. For more information, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*.

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:
  - If the license has expired for a feature at the time the job for that feature is scheduled.
  - If a feature is disabled at the time when a job for that feature is scheduled.
  - If you have removed a module from a slot and a job for that slot is scheduled.
- 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.

Default Settings for the Scheduler

This table lists the scheduler default settings.

Parameters	Default
Scheduler state	Disabled
Log file size	16 KB

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

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# [**no**] **feature scheduler**	Enables or disables the scheduler.
Step 3	(Optional) switch(config)# **show scheduler config**	Displays the scheduler configuration.

	Command or Action	Purpose
Step 4	(Optional) switch(config)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Defining the Scheduler Log File Size

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

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **scheduler logfile size** *value*	Defines the scheduler log file size in kilobytes. The range is from 16 to 1024. The default is 16. **Note** If the size of the job output is greater than the size of the log file, then the output is truncated.
Step 3	(Optional) switch(config)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

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.

Note 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

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **scheduler aaa-authentication password** [**0** | **7**] *password*	Configures a cleartext password for the user who is currently logged in.
Step 3	switch(config)# **scheduler aaa-authentication username** *name* **password** [**0** | **7**] *password*	Configures a cleartext password for a remote user.

	Command or Action	Purpose
Step 4	(Optional) switch(config)# **show running-config | include "scheduler aaa-authentication"**	Displays the scheduler password information.
Step 5	(Optional) switch(config)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Defining a Job

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

Caution Once a job is defined, you cannot modify or remove a command. To change the job, you must delete it and create a new one.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **scheduler job name** *string*	Creates a job and enters job configuration mode. This example creates a scheduler job named backup-cfg.
Step 3	switch(config-job)# *command1* ;[*command2* ;*command3* ;...]	Defines the sequence of commands for the specified job. You must separate commands with a space and a semicolon (for example, " ;"). This example creates a scheduler job that saves the running configuration to a file in bootflash and then copies the file from bootflash to a TFTP server. The filename is created using the current time stamp and switch name.
Step 4	(Optional) switch(config-job)# **show scheduler job** [**name** *name*]	Displays the job information.
Step 5	(Optional) switch(config)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Deleting a Job

You can delete a job from the scheduler.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **no scheduler job name** *string*	Deletes the specified job and all commands defined within it.
Step 3	(Optional) switch(config-job)# **show scheduler job** [**name** *name*]	Displays the job information.
Step 4	(Optional) switch(config)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

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

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **scheduler schedule name** *string*	Creates a new schedule and places you in schedule configuration mode for that schedule.
Step 3	switch(config-schedule)# **job name** *string*	Associates a job with this schedule. You can add multiple jobs to a schedule.
Step 4	switch(config-schedule)# **time daily** *time*	Indicates the job starts every day at a designated time specified as HH:MM.
Step 5	switch(config-schedule)# **time weekly** [[*dow*:]*HH*:]*MM*	Indicates that the job starts on a specified day of the week.

	Command or Action	Purpose
		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	switch(config-schedule)# **time monthly** [[*dm*:]*HH*:]*MM*	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	switch(config-schedule)# **time start** {**now repeat** *repeat-interval* | *delta-time* [**repeat** *repeat-interval*]}	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) switch(config)# **show scheduler config**	Displays the scheduler configuration.
Step 9	(Optional) switch(config)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Clearing the Scheduler Log File

You can clear the scheduler log file.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **clear scheduler logfile**	Clears the scheduler log file.

Verifying the Scheduler Configuration

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

Command	Purpose
show scheduler config	Displays the scheduler configuration.
show scheduler job [**name** *string*]	Displays the jobs configured.
show scheduler logfile	Displays the contents of the scheduler log file.
show scheduler schedule [**name** *string*]	Displays the schedules configured.

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 bootflash and then copies the file from bootflash to a TFTP server (the filename is created using the current time stamp and switch name):

```
switch# configure terminal
switch(config)# scheduler job name backup-cfg
switch(config-job)# cli var name timestamp $(TIMESTAMP) ;copy running-config
bootflash:/$(SWITCHNAME)-cfg.$(timestamp) ;copy bootflash:/$(SWITCHNAME)-cfg.$(timestamp)
tftp://1.2.3.4/ vrf management
switch(config-job)# end
switch(config)#
```

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 schedule name daily
switch(config-if)# job name backup-cfg
switch(config-if)# time daily 1:00
switch(config-if)# 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 --------------------------------
`cli var name timestamp 2013-01-01-01.00.00`
`copy running-config bootflash:/$(HOSTNAME)-cfg.$(timestamp)`
`copy bootflash:/switch-cfg.2013-01-01-01.00.00 tftp://1.2.3.4/ vrf management `
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 --------------------------------
`cli var name timestamp 2013-01-02-01.00.00`
`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 `
Connection to Server Established.
[ ] 0.50KBTrying to connect to tftp server......
[###### ] 24.50KB
TFTP put operation was successful
==============================================================================
switch#
```

Related Documents

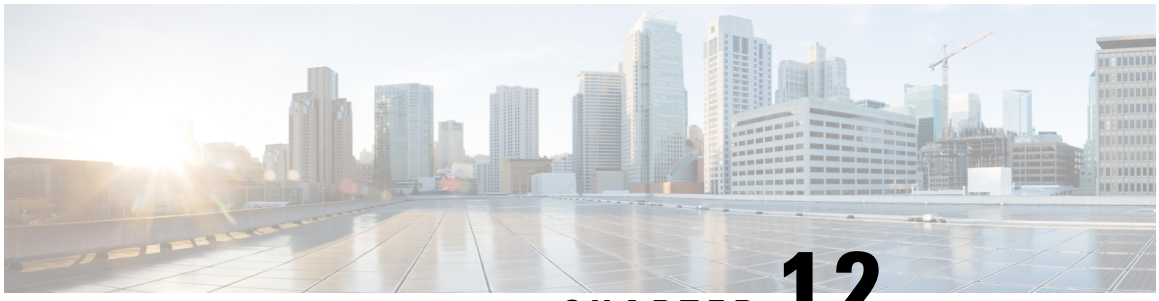
Related Topic	Document Title
Scheduler CLI commands	*Cisco Nexus 7000 Series NX-OS System Management Command Reference*
VDCs	*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*

Feature History for the Scheduler

Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Table 19: Feature History for the Scheduler

Feature Name	Releases	Feature Information
Scheduler	4.0(1)	This feature was introduced.



CHAPTER 12

Configuring SNMP

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

This chapter contains the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

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.

Trap Type	Description
generic	: coldStart
generic	: warmStart
entity	: entity_mib_change
entity	: entity_module_status_change
entity	: entity_power_status_change
entity	: entity_module_inserted
entity	: entity_module_removed
entity	: entity_unrecognised_module
entity	: entity_fan_status_change
entity	: entity_power_out_change
link	: linkDown
link	: linkUp

Trap Type	Description
link	: extended-linkDown
link	: extended-linkUp
link	: cieLinkDown
link	: cieLinkUp
link	: delayed-link-state-change
rf	: redundancy_framework
license	: notify-license-expiry
license	: notify-no-license-for-feature
license	: notify-licensefile-missing
license	: notify-license-expiry-warning
upgrade	: UpgradeOpNotifyOnCompletion
upgrade	: UpgradeJobStatusNotify
rmon	: risingAlarm
rmon	: fallingAlarm
rmon	: hcRisingAlarm
rmon	: hcFallingAlarm
entity	: entity_sensor

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.
- 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.

Note noAuthnoPriv is not supported in SNMPv3.

Table 20: SNMP Security Models and Levels

Model	Level	Authentication	Encryption	What Happens
v1	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v3	noAuthNoPriv	Username	No	Uses a username match for authentication.
v3	authNoPriv	HMAC-MD5 or HMAC-SHA	No	Provides authentication based on the Hash-Based Message Authentication Code (HMAC) Message Digest 5 (MD5) algorithm or the HMAC Secure Hash Algorithm (SHA).
v3	authPriv	HMAC-MD5 or HMAC-SHA	DES	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.

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.

Note 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.

Note 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.

AAA Exclusive Behavior in SNMPv3 Servers

The AAA exclusive behavior feature enables you to authenticate users based on location.

A unique SNMPv3 user is not authenticated if the user is not a local user or a remote AAA user. If the user exists in both the local and remote database, the user will be authenticated or rejected based on whether AAA exclusive behavior is enabled or not.

Table 21: AAA Exclusive Behavior Scenarios

User Location	AAA Server	AAA Exclusive Behavior	User Authentication
Local user database	Disabled	Enabled	User is authenticated.
Local user database	Enabled	Enabled	User is not authenticated.
Local user database	Enabled	Disabled	User is authenticated.
Local user database	Disabled	Disabled	User is authenticated.
Remote and local user databases (same username)	Enabled	Enabled	Remote user is authenticated, but the local user is not authenticated.[1]
Remote and local user databases (same username)	Disabled	Enabled	Local user is authenticated, but the remote user is not authenticated.
Remote and local user databases (same username)	Disabled	Disabled	Local user is authenticated, but the remote user is not authenticated.
Remote and local user databases (same username)	Enabled	Disabled	Local user is authenticated, but the remote user is not authenticated.

[1] This works only when there is FM/DM concept from NMS server where it syncs user credentials automatically to the N7k switch which results in expected SNMP walk output. Otherwise, the user credentials will not sync to switch and should be done manually using hidden CLI on switch.

Note When AAA servers are unreachable, a fallback option can be configured on the server so that a user is validated against the local user database. The SNMPv3 server returns an error if the user is not available in the local database or in the remote user database. The SNMPv3 server returns an "Unknown user" message without checking the availability of AAA servers when a user is not available in the remote user database.

Group-Based SNMP Access

Note 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 per virtual device context (VDC). By default, Cisco NX-OS places you in the default VDC. For more information, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*.

SNMP supports multiple MIB module instances and maps them to logical network entities. For more information, see the “Multiple Instance Support” section.

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. For more information, see the “Configuring SNMP Notification Receivers with VRFs” section.

Guidelines and Limitations for SNMP

SNMP has the following configuration guidelines and limitations:

- To clear snmp counters from an interface use the **clear counters interface all snmp** command, or this command can be applied per interface basis. This is done because there are different data structures for SNMP and CLI counters. This behavior is common across all Cisco Nexus platforms.
- 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/nexus7000/Nexus7000MIBSupportList.html

Default Settings for SNMP

The following table lists the default settings for SNMP parameters.

Parameters	Default
License notifications	Enabled

Configuring SNMP

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

Note You can configure up to 10 SNMP hosts on a device.

Configuring SNMP Users

You can configure a user for SNMP.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**snmp-server user** *name* [**auth** {**md5** | **sha**} *passphrase* [**auto**] [**priv** [**aes-128**] *passphrase*] [**engineID** *id*] [**localizedkey**]] **Example:** `switch(config)# snmp-server user Admin auth sha abcd1234 priv abcdefgh`	Configures an SNMP user with authentication and privacy parameters. The passphrase can be any case-sensitive, alphanumeric string up to 64 characters. If you use the **localizedkey** keyword, the passphrase can be any case-sensitive, alphanumeric string up to 130 characters. The engineID format is a 12-digit, colon-separated decimal number.
Step 3	(Optional) **show snmp user** **Example:** `switch(config) # show snmp user`	Displays information about one or more SNMP users.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

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

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**snmp-server user** *name* **enforcePriv** **Example:** `switch(config)# snmp-server user Admin enforcePriv`	Enforces SNMP message encryption for this user.
Step 3	**snmp-server globalEnforcePriv** **Example:** `switch(config)# snmp-server globalEnforcePriv`	Enforces SNMP message encryption for all users.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

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.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

	Command or Action	Purpose
Step 2	**snmp-server user** *name group* **Example:** `switch(config)# snmp-server user Admin superuser`	Associates this SNMP user with the configured user role.
Step 3	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Creating SNMP Communities

You can create SNMP communities for SNMPv1 or SNMPv2c.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal switch(config)#`	Enters global configuration mode.
Step 2	**snmp-server community** *name* {**group** *group* | **ro** | **rw**} **Example:** `switch(config)# snmp-server community public ro`	Creates an SNMP community string.
Step 3	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Filtering SNMP Requests

You can assign an access control list (ACL) to an SNMPv3 user or SNMPv3 community to filter incoming 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

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**snmp-server user** *name* [**use-ipv4acl** *ipv4acl-name*] [**use-ipv6acl** *ipv6acl-name*] **Example:** `switch(config)# snmp-server community public use-ipv4acl myacl`	Assigns an IPv4 or IPv6 ACL to an SNMPv3 user to filter SNMP requests. **Note** The AAA server must support the creation of SNMPv3 users.
Step 3	**snmp-server community** *name* [**use-ipv4acl** *ipv4acl-name*] [**use-ipv6acl** *ipv6acl-name*] **Example:** `switch(config)# snmp-server community public use-ipv4acl myacl`	Assigns an IPv4 or IPv6 ACL to an SNMPv3 community to filter SNMP requests.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Authenticating SNMPv3 Users Based on Location

You can authenticate local or remote SNMPv3 users based on their location.

Use the following command in global configuration mode to enable AAA exclusive behavior in SNMPv3 servers:

Command	Purpose
snmp-server aaa exclusive-behavior enable	Enables the AAA exclusive behavior in SNMPv3 servers to authenticate users based on location. Depending on the location of the user and whether the AAA server is enabled, the exclusive behavior is as follows: • If the user is a local user and the AAA server is enabled, queries for the user will fail with an "Unknown user" message. • If the user is a remote AAA user and the AAA server is disabled, queries for the user will fail with an "Unknown user" message. • If the user is both a local user and a remote AAA user and the AAA server is enabled, the queries with remote credentials will succeed, and queries with local credentials will fail with an "Incorrect password" message. If the AAA server is disabled, queries with local remote credentials will succeed, and queries with remote credentials will fail with an "Incorrect password" message.

Configuring SNMP Notification Receivers

You can configure Cisco NX-OS to generate SNMP notifications to multiple host receivers.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**snmp-server host** *ip-address* **traps version 1** *community* [**udp_port** *number*] **Example:** `switch(config)# snmp-server host 192.0.2.1 traps version 1 public`	Configures a host receiver for SNMPv1 traps. The *ip-address* can be an IPv4 or IPv6 address. The *community* can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535.
Step 3	**snmp-server host** *ip-address* {**traps** | **informs**} **version 2c** *community* [**udp_port** *number*] **Example:** `switch(config)# snmp-server host 192.0.2.1 informs version 2c public`	Configures a host receiver for SNMPv2c traps or informs. The *ip-address* can be an IPv4 or IPv6 address. The *community* can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535.

	Command or Action	Purpose
Step 4	**snmp-server host** *ip-address* {**traps** | **informs**} **version 3** {**auth** | **noauth** | **priv**} *username* [**udp_port** *number*] **Example:** `switch(config)# snmp-server host 192.0.2.1 informs version 3 auth NMS`	Configures a host receiver for SNMPv3 traps or informs. The *ip-address* can be an IPv4 or IPv6 address. The *username* can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535. **Note** The SNMP manager must know the user credentials (authKey/PrivKey) based on the SNMP engine ID of the Cisco NX-OS device to authenticate and decrypt the SNMPv3 messages.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

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

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal switch(config)#`	Enters global configuration mode.
Step 2	**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`	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.

	Command or Action	Purpose
		This configuration overrides the global source interface configuration.
Step 3	**snmp-server source-interface** {**traps** | **informs**} *if-type if-number* **Example:** `switch(config)# snmp-server source-interface traps ethernet 2/1`	Configures a source interface for sending out SNMPv2c traps or informs. Use **?** to determine the supported interface types.
Step 4	**show snmp source-interface** **Example:** `switch(config)# show snmp source-interface`	Displays information about configured source interfaces.

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

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal switch(config)#`	Enters global configuration mode.
Step 2	**snmp-server user** *name* [**auth** {**md5** | **sha**} *passphrase* [**auto**] [**priv** [**aes-128**] *passphrase*] [**engineID** *id*] **Example:** `switch(config)# snmp-server user NMS auth sha abcd1234 priv abcdefgh engineID 00:00:00:63:00:01:00:10:20:15:10:03`	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.
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 SNMP Notification Receivers with VRFs

SNMP adds entries into the cExtSnmpTargetVrfTable 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

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **snmp-server host** *ip-address* **use-vrf** *vrf-name* [**udp_port** *number*] **Example:** `switch(config)# snmp-server host 192.0.2.1 use-vrf Blue`	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. **Note** This command does not remove the host configuration.
Step 3	[**no**] **snmp-server host** *ip-address* **filter-vrf** *vrf-name* [**udp_port** *number*] **Example:** `switch(config)# snmp-server host 192.0.2.1 filter-vrf Red`	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

	Command or Action	Purpose
		ExtSnmpTargetVrfTable of the CISCO-SNMP-TARGET-EXT-MB. **Note** This command does not remove the host 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 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

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**snmp-server source-interface traps** *if-type if-number* **Example:** `switch(config)# snmp-server source-interface traps ethernet 1/2`	Globally configures a source interface for sending out SNMP traps. Use ? to determine the supported interface types. 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. **Note** To configure a source interface at the host level, use the **snmp-server host** *ip-address* **source-interface** *if-type if-number* command.
Step 3	(Optional) **show snmp source-interface** **Example:** `switch(config)# show snmp source-interface`	Displays information about configured source interfaces.
Step 4	**snmp-server host** *ip-address* **use-vrf** *vrf-name* [**udp_port** *number*] **Example:**	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

	Command or Action	Purpose
	`switch(config)# snmp-server host 171.71.48.164 use-vrf default`	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. **Note** 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.
Step 5	(Optional) **show snmp host** **Example:** `switch(config)# show snmp host`	Displays information about configured SNMP hosts.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Enabling SNMP Notifications

You can enable or disable notifications. If you do not specify a notification name, Cisco NX-OS enables all notifications.

Note 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 22: Enabling SNMP Notifications

MIB	Related Commands
All notifications	**snmp-server enable traps**
CISCO-AAA-SERVER-MIB	**snmp-server enable traps aaa** **snmp-server enable traps aaa server-state-change**
CISCO-BGP4-MIB	**snmp-server enable traps bgp**
CISCO-BGP-MIBv2	**snmp-server enable traps bgp cbgp2**

MIB	Related Commands
CISCO-STP-BRIDGE-MIB	**snmp-server enable traps bridge** **snmp-server enable traps bridge newroot** **snmp-server enable traps bridge topologychange**
CISCO-CALLHOME-MIB	**snmp-server enable traps callhome** **snmp-server enable traps callhome event-notify** **snmp-server enable traps callhome smtp-send-fail**
CISCO-CFS-MIB	**snmp-server enable traps cfs** **snmp-server enable traps cfs merge-failure** **snmp-server enable traps cfs state-change-notif**
CISCO-CONFIG-MAN-MIB	**snmp-server enable traps config** **snmp-server enable traps config ccmCLIRunningConfigChanged**
CISCO-EIGRP-MIB	**snmp-server enable traps eigrp** [*tag*]
ENTITY-MIB, CISCO-ENTITY-SENSOR-MIB	**snmp-server enable traps entity** **snmp-server enable traps entity entity_fan_status_change** **snmp-server enable traps entity entity_mib_change** **snmp-server enable traps entity entity_module_inserted** **snmp-server enable traps entity entity_module_removed** **snmp-server enable traps entity entity_module_status_change** **snmp-server enable traps entity entity_power_out_change** **snmp-server enable traps entity entity_power_status_change** **snmp-server enable traps entity entity_unrecognised_module**

MIB	Related Commands
CISCO-FEATURE-CONTROL-MIB	**snmp-server enable traps feature-control** **snmp-server enable traps feature-control FeatureOpStatusChange**
CISCO-HSRP-MIB	**snmp-server enable traps hsrp** **snmp-server enable traps hsrp state-change**
CISCO-LICENSE-MGR-MIB	**snmp-server enable traps license** **snmp-server enable traps license notify-license-expiry** **snmp-server enable traps license notify-license-expiry-warning** **snmp-server enable traps license notify-licensefile-missing** **snmp-server enable traps license notify-no-license-for-feature**
CISCO-INTERFACE-XCVR MONITOR-MIB	**snmp-server enable traps link cisco-xcvr-mon-status-chg**
IF-MIB	**snmp-server enable traps link** **snmp-server enable traps link IETF-extended-linkDown** **snmp-server enable traps link IETF-extended-linkUp** **snmp-server enable traps link cisco-extended-linkDown** **snmp-server enable traps link cisco-extended-linkUp** **snmp-server enable traps link linkDown** **snmp-server enable traps link Up**
OSPF-MIB, OSPF-TRAP-MIB	**snmp-server enable traps ospf** [*tag*] **snmp-server enable traps ospf lsa** **snmp-server enable traps ospf rate-limit** *rate*

MIB	Related Commands
CISCO-PORT-SECURITY-MIB	**snmp-server enable traps port-security** **snmp-server enable traps port-security** **access-secure-mac-violation** **snmp-server enable traps port-security** **trunk-secure-mac-violation**
CISCO-RF-MIB	**snmp-server enable traps rf** **snmp-server enable traps rf redundancy_framework**
CISCO-RMON-MIB	**snmp-server enable traps rmon** **snmp-server enable traps rmon fallingAlarm** **snmp-server enable traps rmon hcFallingAlarm** **snmp-server enable traps rmon hcRisingAlarm** **snmp-server enable traps rmon risingAlarm**
SNMPv2-MIB	**snmp-server enable traps snmp** **snmp-server enable traps snmp authentication**
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**

MIB	Related Commands
UPGRADE-MIB	**snmp-server enable traps upgrade** **snmp-server enable traps upgrade UpgradeJobStatusNotify** **snmp-server enable traps upgrade UpgradeOpNotifyOnCompletion**
ZONE-MIB	**zone** **zone default-zone-behavior-changes** **zone merge-failure** **zone merge-success** **zone request-reject1** **zone unsupp-mem**

Use the following commands in global configuration mode to enable the specified notification:

Command	Purpose
snmp-server enable traps	Enables all SNMP notifications.
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.
snmp-server enable traps bgp [**cbgp2**]	Enables CISCO-BGP4-MIB SNMP notifications. Optionally, enables the following specific notifications: • **bgp cbgp2**—Enables CISCO-BGP4-MIBv2 SNMP notifications.
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.

Command	Purpose
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.
snmp-server enable traps cfs [**merge-failure**] [**state-change-notif**]	Enables Cisco Fabric Services (CFS) notifications. Optionally, enables the following specific notifications: • **merge-failure**—Enables CFS merge-failure notifications. • **state-change-notif**—Enables CFS state-change notifications.
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.
snmp-server enable traps eigrp [*tag*]	Enables CISCO-EIGRP-MIB SNMP notifications.

Command	Purpose
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.
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.

Command	Purpose
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.
snmp-server enable traps link [**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 Internet Engineering Task Force (IETF) extended link state down notifications. • **IETF-extended-linkUp**—Enables Internet Engineering Task Force (IETF) extended link state up notifications. • **cisco-extended-linkDown**—Enables Cisco extended link state down notifications. • **cisco-extended-linkUp**—Enables Cisco 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.

Command	Purpose
snmp-server enable traps port-security [**access-secure-mac-violation**] [**trunk-secure-mac-violation**]	Enables port-security SNMP notifications. Optionally, enables the following specific notifications: • **access-secure-mac-violation**—Enables secure machine access control (MAC) violation notifications. • **trunk-secure-mac-violation**—Enables virtual LAN (VLAN) secure MAC violation 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.
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.
snmp-server enable traps snmp [**authentication**]	Enables general SNMP notifications. Optionally, enables the following specific notifications: • **authentication**—Enables SNMP authentication notifications.

Command	Purpose
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 STPX MIB inconsistency update notifications. • **loop-inconsistency**—Enables SNMP STPX MIB loop-inconsistency update notifications. • **root-inconsistency**—Enables SNMP STPX MIB root-inconsistency update notifications.
snmp-server enable traps sysmgr [**cseFailSwCoreNotifyExtended**]	Enables software change notifications. Optionally, enables the following specific notifications: • **cseFailSwCoreNotifyExtended**—Enables software core notifications.
snmp-server enable traps upgrade [**UpgradeJobStatusNotify**] [**UpgradeOpNotifyOnCompletion**]	Enables upgrade notifications. Optionally, enables the following specific notifications: • **UpgradeJobStatusNotify**—Enables upgrade job status notifications. • **UpgradeOpNotifyOnCompletion**—Enables upgrade global status notifications.
snmp-server enable traps vtp [**notifs**] [**vlancreate**] [**vlandelete**]	Enables VTP notifications. Optionally, enables the following specific notifications: • **notifs**—Enables VTP notifications. • **vlancreate**—Enables VLAN creation notifications. • **vlandelete**—Enables VLAN deletion notifications.

Command	Purpose
snmp-server enable traps zone [**default-zone-behavior-change**] [**merge-failure**] [**merge-success**] [**request-reject1**] [**unsupp-mem**]	Enables default zone change notifications. Optionally, enables the following specific notifications: • **default-zone-behavior-change**—Enables default zone behavior change notifications. • **merge-failure**—Enables merge failure notifications. • **merge-success**—Enables merge success notifications. • **request-reject1**—Enables request reject notifications. • **unsupp-mem**—Enables unsupported member notifications.

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

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface** *type slot/port* **Example:** `switch(config)# interface ethernet 2/2`	Disables SNMP link-state traps for the interface. This command is enabled by default.
Step 3	**no snmp trap link-status** **Example:** `switch(config-if)# no snmp trap link-status`	Disables SNMP link-state traps for the interface. This command is enabled by default.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Displaying SNMP ifIndex for an Interface

The SNMP ifIndex is used across multiple SNMP MIBs to link related interface information.

Procedure

	Command or Action	Purpose

Step 1	**show interface snmp-ifindex**
	Example:
	`switch# show interface snmp-ifindex | grep -i Eth12/1`
	`Eth12/1 441974784 (0x1a580000)`
		Displays the persistent SNMP ifIndex value from the IF-MIB for all interfaces. Optionally, use the | keyword and the **grep** keyword to search for a particular interface in the output.

Enabling a One-Time Authentication for SNMP over TCP

You can enable a one-time authentication for SNMP over a TCP session.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**snmp-server tcp-session** [**auth**] **Example:** `switch(config)# snmp-server tcp-session`	Enables a one-time authentication for SNMP over a TCP session. The default is disabled.
Step 3	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

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.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`switch# configure terminal` `switch(config)#`	
Step 2	**snmp-server contact** *name* **Example:** `switch(config)# snmp-server contact Admin`	Configures sysContact, which is the SNMP contact name.
Step 3	**snmp-server location** *name* **Example:** `switch(config)# snmp-server location Lab-7`	Configures sysLocation, which is the SNMP location.
Step 4	(Optional) **show snmp** **Example:** `switch(config)# show snmp`	Displays information about one or more destination profiles.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

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 7000 Series NX-OS Unicast Routing Configuration Guide* or the *Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide*.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **snmp-server context** *context-name* [**instance** *instance-name*] [**vrf** *vrf-name*] [**topology** *topology-name*] **Example:** `switch(config)# snmp-server context public1 vrf red`	Maps an SNMP context to a protocol instance, VRF, or topology. Before Release 6.2(2), the names can be any alphanumeric string up to 32 characters. In Release 6.2(2) and later releases, the string can include non alphanumeric characters. However, the best practice is to use alphanumeric characters only.

	Command or Action	Purpose
		The **no** option deletes the mapping between an SNMP context and a protocol instance, VRF, or topology. **Note** 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.
Step 3	(Optional) **snmp-server mib community-map** *community-name* **context** *context-name* **Example:** `switch(config)# snmp-server mib community-map public context public1`	Maps an SNMPv2c community to an SNMP context. The names can be any alphanumeric string up to 32 characters.
Step 4	(Optional) **show snmp context** **Example:** `switch(config)# show snmp context`	Displays information about one or more SNMP contexts.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Disabling SNMP

You can disable SNMP on the device.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal switch(config)#`	Enters global configuration mode.
Step 2	**no snmp-server protocol enable** **Example:** `switch(config)# no snmp-server protocol enable`	Disables SNMP. SNMP is enabled by default.

Managing the SNMP Server Counter Cache Update Timer

You can modify how long, in seconds Cisco NX-OS holds the cache port state.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**snmp-server counter cache-timeout** *seconds* **Example:** `switch(config)# snmp-server counter cache-timeout 1800`	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 value for the SNMP cache expiry timeout is 140 seconds. The range is 1-3600. For end of row (EoR) switching - The range is from 10 to 3600.
Step 3	(Optional) **show running-config snmp all** **Example:** `switch(config)# show running-config snmp all`	Displays the configured SNMP-server counter cache update timeout value.
Step 4	**no snmp-server counter cache enable** **Example:** `switch(config)# no snmp-server counter cache enable`	Disables the counter cache update. When the counter cache update is disabled, the value set in the timeout parameter determines length of time the port states are held the counter cache.

Modifying the AAA Synchronization Time

You can modify how long Cisco NX-OS holds the synchronized user configuration.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**snmp-server aaa-user cache-timeout** *seconds* **Example:** `switch(config)# snmp-server aaa-user cache-timeout 1200`	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.
Step 3	(Optional) **copy running-config startup-config** **Example:**	Copies the running configuration to the startup configuration.

	Command or Action	Purpose
	`switch(config)# copy running-config startup-config`	

Verifying SNMP Configuration

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

Command	Purpose
show interface snmp-ifindex	Displays the SNMP ifIndex value for all interfaces (from IF-MIB).
show running-config snmp [**all**]	Displays the SNMP running configuration.
show snmp	Displays the SNMP status.
show snmp community	Displays the SNMP community strings.
show snmp context	Displays the SNMP context mapping.
show snmp engineID	Displays the SNMP engineID.
show snmp group	Displays SNMP roles.
show snmp host	Displays information about configured SNMP hosts.
show snmp session	Displays SNMP sessions.
show snmp source-interface	Displays information about configured source interfaces.
show snmp trap	Displays the SNMP notifications enabled or disabled.
show snmp user	Displays SNMPv3 users.

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:

```
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:

```
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
switch(config)# show snmp host
-------------------------------------------------------------------
Host Port Version Level Type SecName
-------------------------------------------------------------------
171.71.48.164 162 v2c noauth trap public
Source interface: Ethernet 1/2
-------------------------------------------------------------------
switch(config)# snmp-server host 171.71.48.164 use-vrf default
switch(config)# show snmp host
-------------------------------------------------------------------
Host Port Version Level Type SecName
-------------------------------------------------------------------
171.71.48.164 162 v2c noauth trap public
Use VRF: default
Source interface: Ethernet 1/2
-------------------------------------------------------------------
```

This example shows how to configure SNMP to send traps using a globally configured inband port:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# snmp-server source-interface traps ethernet 1/2
switch(config)# show snmp source-interface
-------------------------------------------------------------------
Notification source-interface
-------------------------------------------------------------------
trap Ethernet1/2
inform -
-------------------------------------------------------------------
switch(config)# snmp-server host 171.71.48.164 use_vrf default
switch(config)# show snmp host
-------------------------------------------------------------------
Host Port Version Level Type SecName
-------------------------------------------------------------------
171.71.48.164 162 v2c noauth trap public
Use VRF: default
Source interface: 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
```

This example shows how to configure both IPv4 and IPv6 ACLs with the SNMPv3 “newstring” community:

```
switch# configure terminal
switch(config)# snmp-server community newstring use-ipv4acl myacl use-ipv6acl myacl1
switch(config)# show running-config snmp
version 6.2(2)
snmp-server aaa exclusive-behavior enable
snmp-server user admin network-admin auth md5 0x2f2429f3c9b21f1adbae8acc7783e355
priv 0x2f2429f3c9b21f1adbae8acc7783e355 localizedkey
rmon event 1 log trap public description FATAL(1) owner PMON@FATAL
rmon event 2 log trap public description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 log trap public description ERROR(3) owner PMON@ERROR
rmon event 4 log trap public description WARNING(4) owner PMON@WARNING
rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO
snmp-server community newstring group network-operator
snmp-server community newstring use-ipv4acl myacl use-ipv6acl myacl1
switch# show snmp community
Community   Group / Access   context acl_filter
newstring   network-operator         ipv4:myacl ipv6:myacl1
switch#
```

Additional References

Related Documents

Related Topic	Document Title
Rollback CLI commands	*Cisco Nexus 7000 Series NX-OS System Management Command Reference*
VDCs	*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*
IP ACLs and AAA	*Cisco Nexus 7000 Series NX-OS Security Configuration Guide*
MIBs	*Cisco Nexus 7000 Series and 9000 Series NX-OS MIB Quick Reference*

RFCs

RFC	Title
RFC 3414	*User-based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3)*
RFC 3415	*View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*

MIBs

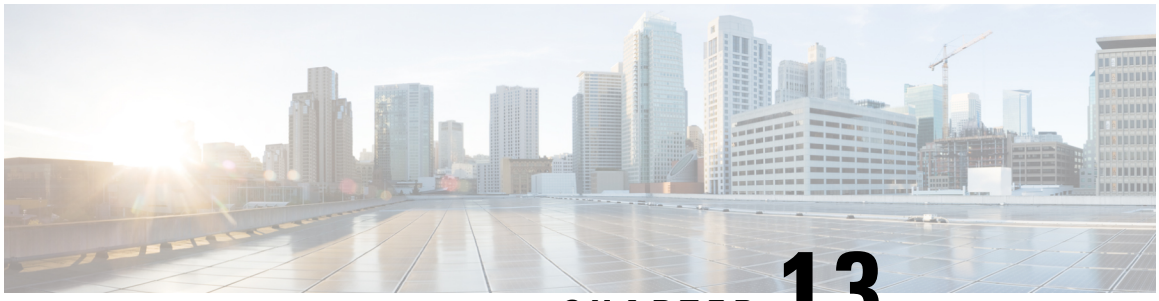
MIBs	MIBs Link
MIBs related to SNMP	To locate and download supported MIBs, go to the following URL: ftp://ftp.cisco.com/pub/mibs/supportlists/nexus7000/Nexus7000MIBSupportList.html

Feature History for SNMP

Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Table 23: Feature History for SNMP

Feature Name	Releases	Feature Information
SNMPv3 user and communities	6.2(2)	Added the ability to apply both IPv4 and IPv6 ACLs to the same SNMPv3 user or SNMPv3 community.
SNMPv3	6.2(2)	Added support for AAA exclusive behavior in SNMPv3 servers to authenticate users based on location.
SNMP notifications	5.0(2)	Updated the **snmp-server enable traps** commands.
IPv6 support	4.2(1)	Supports configuring IPv6 SNMP hosts.
Filter SNMP requests by community using an ACL	4.2(1)	Assigns an ACL to an SNMP community to filter SNMP requests.
Use interfaces for SNMP notification receivers	4.2(1)	Added support to designate an interface to act as the source interface for SNMP notifications.
SNMP AAA synchronization	4.0(3)	Added the ability to modify the synchronized user configuration timeout.
SNMP protocol	4.0(3)	Added the ability to disable the SNMP protocol.



CHAPTER 13

Configuring RMON

This chapter describes how to configure the remote monitoring (RMON) feature on Cisco NX-OS devices.

This chapter contains the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

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 hcalarms 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.

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.

Parameters	Default
RMON	Enabled
Alarms	None configured

Configuring RMON

Note 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

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**rmon alarm** *index mib-object sample-interval* {**absolute** | **delta**} **rising-threshold** *value* [*event-index*] **falling-threshold** *value* [*event-index*] [**owner** *name*] **Example:** `switch(config)# 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`	Creates an RMON alarm. The value range is from –2147483647 to 2147483647. The owner name can be any alphanumeric string.
Step 3	**rmon hcalarm** *index mib-object sample-interval* {**absolute** | **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*] **Example:** `switch(config)# rmon alarm 20 1.3.6.1.2.1.2.2.1.14.16777216 2900 delta rising-threshold-high 15 rising-threshold-low 151 falling-threshold-high 0 falling-threshold-low 0 owner test`	Creates an RMON high-capacity alarm. The value range is from –2147483647 to 2147483647. The owner name can be any alphanumeric string. The storage type range is from 1 to 5.
Step 4	(Optional) **show rmon** {**alarms** | **hcalarms**} **Example:** `switch(config)# show rmon alarms`	Displays information about RMON alarms or high-capacity alarms.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

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

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**rmon event** *index* [**description** *string*] [**log**] [**trap** *string*] [**owner** *name*] **Example:** `switch(config)# rmon event 1 trap trap1`	Configures an RMON event. The description string, trap string, and owner name can be any alphanumeric string.
Step 3	(Optional) **show rmon events** **Example:** `switch(config)# show rmon events`	Displays information about RMON events.
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 RMON Configuration

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

Command	Purpose
show rmon alarms	Displays information about RMON alarms.
show rmon events	Displays information about RMON events.
show rmon hcalarms	Displays information about RMON high-capacity alarms.
show rmon logs	Displays information about RMON logs.

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

Related Documents

Related Topic	Document Title
RMON CLI commands	*Cisco Nexus 7000 Series NX-OS System Management Command Reference*
VDCs and VRFs	*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*

MIBs

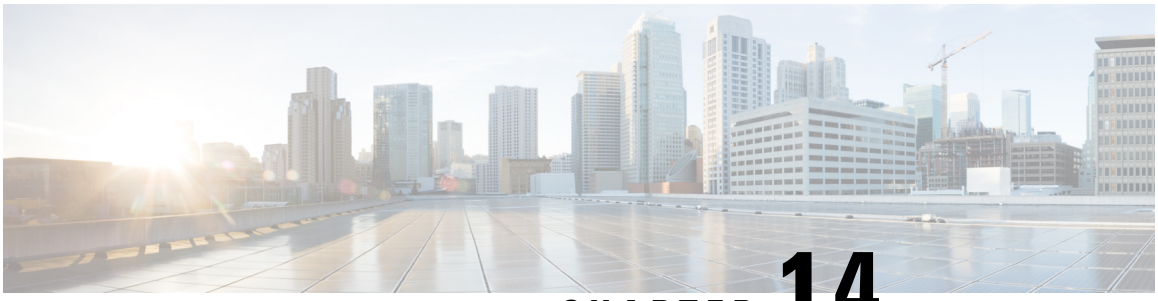
MIBs	MIBs Link
MIBs related to RMON	To locate and download supported MIBs, go to the following URL: ftp://ftp.cisco.com/pub/mibs/supportlists/nexus7000/Nexus7000MIBSupportList.html

Feature History for RMON

Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Table 24: Feature History for RMON

Feature Name	Releases	Feature Information
RMON	4.0(1)	This feature was introduced.



CHAPTER 14

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:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

Information About Online Diagnostics

Online diagnostics help you verify that hardware and internal data paths are operating as designed so that you can rapidly isolate faults.

Online Diagnostics Overview

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.

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 to run the complete set of bootup diagnostics.

Note Bootup tests are not available on demand.

The following tables describe the bootup diagnostic tests for a module and a supervisor:

Table 25: Bootup Diagnostic Tests for Modules

Test Name	Description	Supported Modules	Unsupported Modules
EOBCPortLoopback	Disruptive test, not an on-demand test. Ethernet out of band	All F1, M1, M3, F2, F2e and F2 modules	—
OBFL	Verifies the integrity of the onboard failure logging (OBFL) flash.	All F1, M1, M3, F2, F2e and F2 modules	—
FIPS	Disruptive test; run only when FIPS is enabled on the system. An internal test that runs during module bootup to validate the security device on the module.	N7K-M148GS-11 N7K-M148GS-11L N7K-M108X2-12L N7K-M132XP-12 N7K-M132XP-12L All M2 Modules	N7K-M148GT-11 N7K-M148GT-11L All F1 Modules All F2 Modules N7K-F248XT-25E All F3 Modules All M3 Modules

Test Name	Description	Supported Modules	Unsupported Modules
BootupPortLoopback	Disruptive test, not an on-demand test. A PortLoopback test that runs only during module bootup.	N7K-M148GS-11 N7K-M148GS-11L N7K-M108X2-12L N7K-M132XP-12 N7K-M132XP-12L All M2 Modules All F1 Modules All F2 Modules All F2e Modules N77-M348XP-23L N77-M324FQ-25L	N7K-M148GT-11 N7K-M148GT-11L All F3 Modules

Table 26: Bootup Diagnostic Tests for Supervisors

Test Name	Description	Supported Modules	Unsupported Modules
USB	Nondisruptive test. Checks the USB controller initialization on a module.	Sup1, Sup2, and Sup2E	—
CryptoDevice	Nondisruptive test. Checks the Cisco Trusted Security (CTS) device initialization on a module.	Sup1	Sup2 and Sup2E
ManagementPortLoopback	Disruptive test, not an on-demand test. Tests loop back on the management port of a module.	Sup1, Sup2, and Sup2E	—
EOBCPortLoopback	Disruptive test, not an on-demand test. Ethernet out of band.	Sup1, Sup2, and Sup2E	—
OBFL	Verifies the integrity of the onboard failure logging (OBFL) flash.	Sup1, Sup2, and Sup2E	—

Runtime or Health Monitoring Diagnostics

Runtime diagnostics are also called health monitoring (HM) diagnostics. These diagnostic tests 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.

Runtime 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 runtime tests. You can change the runtime interval for a runtime test.

Note Recommended best practice: Do not change the runtime interval from the default value.

The following tables describe the runtime diagnostic tests for a module and a supervisor.

Table 27: Runtime Diagnostic Tests for Modules

Test Name	Description	Default Interval	Supported Modules	Unsupported Modules
ASICRegisterCheck	Checks read/write access to scratch registers for the ASICs on a module.	1 min	All modules	—
PrimaryBootROM	Verifies the integrity of the primary boot device on a module.	30 min	All modules	—
SecondaryBootROM	Verifies the integrity of the secondary boot device on a module.	30 min	All modules	—
PortLoopback	Checks diagnostics at a per-port basis on all Admin Down ports.	15 min	N7K-M148GS-11 RF N7K-M148GS-11L N7K-M108X2-12L N7K-M132XP-12 RF N7K-M132XP-12L N77-F348XP-23 All M2, F1, F2, F3, and F2e modules N77-M348XP-23L N77-M324FQ-25L	N7K-M148GT-11 N7K-M148GT-11L

Test Name	Description	Default Interval	Supported Modules	Unsupported Modules
RewriteEngineLoopback	This is a nondisruptive per-port loopback test, and hence can run on ports that are up as well. It is designed to monitor the fabric to LC connectivity and can detect supervisor and fabric failures.	1 min	All M1, M2, F2, and F2e modules N77-M348XP-23L N77-M324FQ-25L	All F1 and F3 modules
SnakeLoopback	Performs a nondisruptive loopback on all ports, even those ports that are not in the shut state. The ports are formed into a snake during module boot up, and the supervisor checks the snake connectivity periodically.	20 min	All F1, F2, and F2e modules	All M1, M2, M3, and F3 modules
InternalPortLoopback	Nondisruptive per-port loopback test, and hence can run on ports that are up as well.	5 min	All M2, F2, and F2e modules N77-M348XP-23L N77-M324FQ-25L	All M1, F1, and F3 modules

Table 28: Runtime Diagnostic Tests for Supervisors

Test Name	Description	Default Interval	Supported Supervisors	Unsupported Supervisors
ASICRegisterCheck	Checks read/write access to scratch registers for the ASICs on a module.	20 sec	Sup1, Sup2, and Sup2E	—
NVRam	Verifies the sanity of the NVRAM blocks on a supervisor.	5 min	Sup1, Sup2, and Sup2E	—

Test Name	Description	Default Interval	Supported Supervisors	Unsupported Supervisors
RealTimeClock	Verifies that the real-time clock on the supervisor is ticking.	5 min	Sup1, Sup2, and Sup2E	—
PrimaryBootROM	Verifies the integrity of the primary boot device on a module.	30 min	Sup1, Sup2, and Sup2E	—
SecondaryBootROM	Verifies the integrity of the secondary boot device on a module.	30 min	Sup1, Sup2, and Sup2E	—
CompactFlash	Verifies access to the internal compact flash devices.	30 min	Sup1, Sup2, and Sup2E	—
ExternalCompactFlash	Verifies access to the external compact flash devices.	30 min	Sup1, Sup2, and Sup2E	—
PwrMgmtBus	Verifies the standby power management control bus.	30 sec	Sup1, Sup2, and Sup2E	—
SpineControlBus	Verifies the availability of the standby spine module control bus.	30 sec	Sup1 and Sup2	Sup2E
SystemMgmtBus	Verifies the availability of the standby system management bus.	30 sec	Sup1, Sup2, and Sup2E	—
StatusBus	Verifies the status transmitted by the status bus for the supervisor, modules, and fabric cards.	30 sec	Sup1, Sup2, and Sup2E	—

Test Name	Description	Default Interval	Supported Supervisors	Unsupported Supervisors
StandbyFabricLoopback	Verifies the connectivity of the standby supervisor to the crossbars on the spine card.	30 sec	Sup1, Sup2, and Sup2E	—
PCIeBus	Verifies PCIe connectivity from the supervisor to the crossbar ASICs on the fabric cards.	30 sec	Sup2 and Sup2E	—

Recovery Actions for Specified Health-Monitoring Diagnostics

Before Cisco NX-OS Release 6.2(8), runtime tests did not take corrective recovery actions when they detected a hardware failure. The default action through EEM included generating alerts (callhome, syslog) and logging (OBFL, exception logs). These actions are informative, but they did not remove faulty devices from the network, which can lead to network disruption, traffic black holing, and so forth. Before Cisco NX-OS Release 6.2(8), you must manually shut the devices to recover the network.

In Cisco NX-OS Release 6.2(8) and later releases, you can configure the system to take disruptive action if the system detects failure on one of the following runtime, or health-monitoring, tests:

- PortLoopback test
- RewriteEngineLoopback test
- SnakeLoopback test
- StandbyFabricLoopback test

The recovery actions feature is disabled by default. With this feature you can configure the system to take disruptive action as a result of repeated failures on the health-monitoring, or runtime, tests. This feature enables or disables the corrective, conservative action on all four tests, simultaneously; the corrective action taken differs for each test. After crossing the maximum consecutive failure count for that test, the system takes corrective action.

With the recovery actions feature enabled, he corrective action for each test is as follows:

- PortLoopback test—The system moves the port registering faults to an error-disabled state.
- RewriteEngineLookpback test—The system takes different corrective action depending on whether the fault is with the supervisor, the fabric, or the port, as follows:
  - On a chassis with a standby supervisor, when the system detects a fault with the supervisor, the system switches over to the standby supervisor. If there is no standby supervisor in the chassis, the system does not take any action.
  - After failures on the fabric, the system will reload the fabric 3 times. If failure persists, the system powers down the fabric.
  - After the failures on a port, the system moves the faulty port to the error-disabled state.

- SnakeLoopback test—After the test detects 10 consecutive failures with any port on the module, the system will move the faulty port to an error-disabled state.
- StandbyFabricLoopback test—The system attempts to reload the standby supervisor if it receives error on this test and continues to reload if the system keeps seeing the failure even after the reload. It cannot power off the standby supervisor.

Finally, the system maintains a history of the recovery actions that includes details of each action, the testing type, and the severity. You can display these counters.

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

Cisco NX-OS supports online diagnostics in the default virtual device context (VDC) or, beginning with Cisco NX-OS Release 6.1, in the admin VDC. By default, Cisco NX-OS places you in the default VDC.

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.

Guidelines and Limitations for Online Diagnostics

Online diagnostics has the following configuration guidelines and limitations:

- You cannot run disruptive online diagnostic tests on demand.
- The F1 Series modules support the following tests: ASICRegisterCheck, PrimaryBootROM, SecondaryBootROM, EOBCPortLoopback, PortLoopback, and BootupPortLoopback.
- Support for the RewriteEngineLoopback and SnakeLoopback tests on F1 Series modules is deprecated in Cisco NX-OS Release 5.2.

- Beginning with Cisco NX-OS Release 6.1, F2 Series modules support the RewriteEngineLoopback and SnakeLoopback tests.
- Beginning with Cisco NX-OS Release 7.3(0)DX(1), M3 Series modules support generic online diagnostics.

The following generic online diagnostics supported on M3 series:

Table 29: Generic Online Diagnostics Supported on M3 Series

ASICRegisterCheck	Health Monitoring/On Demand
PrimaryBootROM	Health Monitoring/On Demand
SecondaryBootROM	Health Monitoring/On Demand
EOBCPortLoopback	Bootup test only
OBFL	Bootup test only
PortLoopback	Health Monitoring/On Demand when port admin down only
RewriteEngineLoopback	Health Monitoring/On Demand
IntPortLoopback	Health Monitoring/On Demand
BootupPortLoopback	Bootup test only

Default Settings for Online Diagnostics

The following table lists the default settings for online diagnostic parameters.

Parameters	Default
Bootup diagnostics level	complete
Nondisruptive tests	active

Configuring Online Diagnostics

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

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.

Before you begin

Make sure that you are in the correct VDC. To change the VDC, use the **switchto vdc** command.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **diagnostic bootup level** {**complete** | **bypass**}	Configures the bootup diagnostic level to trigger diagnostics as follows when the device boots: • **complete**—Perform all bootup diagnostics. The default is complete. • **bypass**—Do not perform any bootup diagnostics.
Step 3	(Optional) switch(config)# **show diagnostic bootup level**	Displays the bootup diagnostic level (bypass or complete) that is currently in place on the device.
Step 4	(Optional) switch(config)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

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.

Note Recommended best practice: Do not change the runtime interval from the default value.

Before you begin

Make sure that you are in the correct VDC. To change the VDC, use the **switchto vdc** command.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.

	Command or Action	Purpose
Step 2	(Optional) switch(config)# **diagnostic monitor interval module** *slot* **test** [*test-id* | *name* | **all**] **hour** *hour* **min** *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: • *slot*—The range is from 1 to 10. • *test-id*—The range is from 1 to 14. • *name*—Can be any case-sensitive, alphanumeric string up to 32 characters. • *hour*—The range is from 0 to 23 hours. • *minute*—The range is from 0 to 59 minutes. • *second*—The range is from 0 to 59 seconds.
Step 3	switch(config)# [**no**] **diagnostic monitor module** *slot* **test** [*test-id* | *name* | **all**]	Activates the specified test. The argument ranges are as follows: • *slot*—The range is from 1 to 10. • *test-id*—The range is from 1 to 14. • *name*—Can be any case-sensitive, alphanumeric string up to 32 characters. The [**no**] form of this command inactivates the specified test. Inactive tests keep their current configuration but do not run at the scheduled interval.
Step 4	(Optional) switch(config)# **show diagnostic content module** {*slot* | **all**}	Displays information about the diagnostics and their attributes.

Setting a Diagnostic Test as Inactive

You can set a diagnostic test as inactive. Inactive tests keep their current configuration but do not run at the scheduled interval.

Use the following command in global configuration mode to set a diagnostic test as inactive:

Command	Purpose
no diagnostic monitor module slot test [**test-id**|**name** | **all**]	Inactivates the specified test. The following ranges are valid for the each keyword: • **slot** —The range is from 1 to 10. • **test-id** —The range is from 1 to 14. • **name** —Can be any case-sensitive alphanumeric string up to 32 characters

Configuring Corrective Action

You can configure the device to take corrective action when it detects failures on any of the following runtime diagnostic tests:

- PortLoopback
- RewriteEngineLoopback
- SnakeLoopback
- StandbyFabricLoopback

Note This feature enables or disables the corrective, conservative action on all four tests, simultaneously; the corrective action taken differs for each test.

Before you begin

Make sure that you are in the correct VDC. To change the VDC, use the **switchto vdc** command.

Procedure

	Command or Action	Purpose
Step 1	Required: switch# **configure terminal**	Enters global configuration mode.
Step 2	Required: switch(config)# [**no**] **diagnostic eem action conservative**	Enables or disables corrective actions when the system detects failures on port loopback, rewrite engine loopback, snake loopback, internal port loopback and standby fabric loopback tests. **Note** Use the **no** form of the command to disable these corrective actions.
Step 3	switch# **event gold** [**failure-type** {**sup** | **fabric** | **lc** | **port**}] **module** {*module* | **all**} **test** {*test-name* | *test-id*} [**severity** {**major** | **minor** | **moderate**}] **testing-type** {**bootup** | **monitoring** | **ondemand** | **scheduled**} **consecutive-failure** *count*	Triggers an event if the named online diagnostic test experiences the configured failure severity for the configured number of consecutive failures. The *module* specifies the number of the module that needs to be monitored. The *test-name* is the name of a configured online diagnostic test. The *test-id* specifies the test ID of the event criteria. The range is from 1 to 30. The *count* range is from 1 to 1000. **Note** This CLI command can be used to modify the consecutive failure count for GOLD system default policies.

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.

Before you begin

Make sure that you are in the correct VDC. To change the VDC, use the **switchto vdc** command.

Procedure

	Command or Action	Purpose
Step 1	(Optional) switch# **diagnostic ondemand iteration** *number*	Configures the number of times that the on-demand test runs. The range is from 1 to 999. The default is 1.
Step 2	(Optional) switch# **diagnostic ondemand action-on-failure** {**continue failure-count** *num-fails* | **stop**}	Configures the action to take if the on-demand test fails. The *num-fails* range is from 1 to 999. The default is 1.
Step 3	Required: switch# **diagnostic start module** *slot* **test** [*test-id* | *name* | **all** | **non-disruptive**] [**port** *port-number* | **all**]	Starts one or more diagnostic tests on a module. The module slot range is from 1 to 10. The *test-id* range is from 1 to 14. The test name can be any case-sensitive, alphanumeric string up to 32 characters. The port range is from 1 to 48.
Step 4	Required: switch# **diagnostic stop module** *slot* **test** [*test-id* | *name* | **all**]	Stops one or more diagnostic tests on a module. The module slot range is from 1 to 10. The *test-id* range is from 1 to 14. The test name can be any case-sensitive, alphanumeric string up to 32 characters.
Step 5	(Optional) switch# **show diagnostic status module** *slot*	Verifies that the diagnostic has been scheduled.

Clearing Diagnostic Results

You can clear diagnostic test results.

Use the following command in any mode to clear the diagnostic test results:

Command	Purpose
diagnostic clear result module [*slot* | **all**] **test** {*test-id* | **all**}	Clears the test result for the specified test. The valid ranges are as follows: • *slot*—The range is from 1 to 10. • *test-id*—The range is from 1 to 14.

Simulating Diagnostic Results

You can simulate diagnostic test results.

Use the following command in any mode to simulate a diagnostic test result or clear the simulated test results:

Command	Purpose
diagnostic test simulation module *slot* **test** *test-id* {**fail** | **random-fail** | **success**} [**port** *number* | **all**]	Simulates the test result for the specified test. The valid ranges are as follows: • *slot*—The range is from 1 to 10. • *test-id*—The range is from 1 to 14. • **port** *number*—The range is from 1 to 48.
diagnostic test simulation module *slot* **test** *test-id* **clear**	Clears the simulated results for the specified test. The valid ranges are as follows: • *slot*—The range is from 1 to 10. • *test-id*—The range is from 1 to 14.

Verifying the Online Diagnostics Configuration

To display online diagnostics configuration information, perform one of the following tasks:

Command	Purpose
show diagnostic bootup level	Displays information about bootup diagnostics.
show diagnostic content module {*slot* | **all**}	Displays information about diagnostic test content for a module.
show diagnostic description module *slot* **test** [*test-name* | **all**]	Displays the diagnostic description.
show diagnostic eem [**action** [**description**] | **policy module** {*module number* | **all**}]	Displays the Embedded Event Manager (EEM) action level and the EEM policies configured for the level.
show diagnostic events [**error** | **info**]	Displays diagnostic events by error and information event type.
show diagnostic ondemand setting	Displays information about on-demand diagnostics.
show diagnostic result module *slot* [**test** [*test-name* | **all**]] [**detail**]	Displays information about the results of a diagnostic.

Command	Purpose
show diagnostic simulation module *slot*	Displays information about a simulated diagnostic.
show diagnostic status module *slot*	Displays the test status for all tests on a module.
show event manager events action-log event-type [**gold** | **gold_sup_failure** | **gold_fabric_failure** | **gold_module_failure** | **gold_port_failure**]	Displays the recovery action history for the specified failure, including the number of switchovers, reloads, and poweroffs, as well as timestamp, failure reason, module-id, port list, test name, testing type, and severity. This data is maintained across ungraceful reloads.
show hardware capacity [**eobc** | **forwarding** | **interface** | **module** | **power**]	Displays information about the hardware capabilities and current hardware utilization by the system.
show module	Displays module information including the online diagnostic test status.

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
```

Additional References

For additional information related to implementing online diagnostics, see the following sections:

Related Documents

Topics	Document Title
Online diagnostics CLI commands	*Cisco Nexus 7000 Series NX-OS System Management Command Reference*

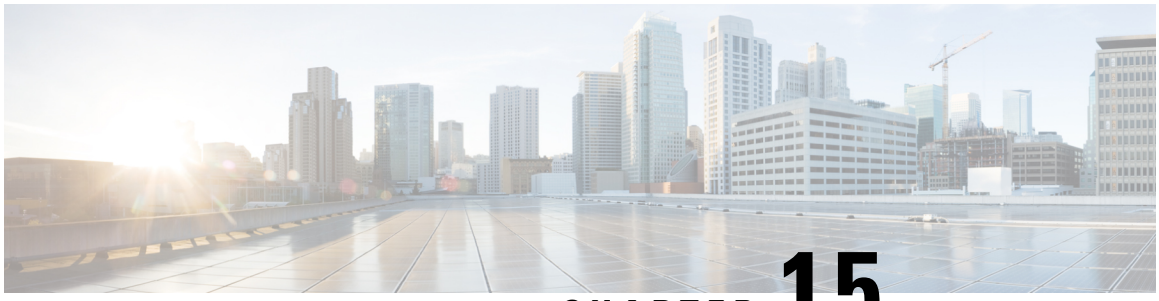
Topics	Document Title
VDCs and VRFs	*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*

Feature History Table for Online Diagnostics

The following table lists the release history for this feature.

Feature Name	Releases	Feature Information
Online diagnostics (GOLD)	7.3(0)DX(1)	Added support for M3 Series modules for the following diagnostic tests: ASICRegisterCheck, PrimaryBootROM, SecondaryBootROM, EOBCPortLoopback, OBFL, PortLoopback, RewriteEngineLoopback, IntPortLoopback, and IntPortLoopback.
Online diagnostics (GOLD)	7.2(0)D1(1)	This feature was introduced.
Online diagnostics (GOLD)	6.2(10)	• Added support for the N77-F348XP-23 module for the PortLoopback test. • Added support for all M2, F2, and F2e modules for the InternalPortLoopback test.
Recovery actions on specified health-monitoring diagnostics.	6.2(8)	Enables you to configure recovery actions for the following runtime diagnostic tests: PortLoopback, RewriteEngineLoopback, SnakeLoopback test , and StandbyFabricLoopback.
Online diagnostics (GOLD)	6.2(6)	Added support to all F3 modules except for N77-F348XP-23.
Online diagnostics (GOLD)	6.1(1)	• Added support for Supervisor 2 and M2 Series modules. • Added support for F2 Series modules for the RewriteEngineLoopback and SnakeLoopback tests. • Added support for configuring online diagnostics in the admin VDC.
Online diagnostics (GOLD)	5.2(1)	• Enabled the SpineControlBus test on the standby supervisor. • Deprecated the SnakeLoopback test on F1 Series modules.
Online diagnostics (GOLD)	5.1(2)	Added support for the SnakeLoopback test on F1 Series modules.
Online diagnostics (GOLD)	5.1(1)	Added support for the FIPS and BootupPortLoopback tests.
Online diagnostics (GOLD)	4.2(1)	Added support for the PortLoopback, StatusBus, and StandbyFabricLoopback tests.

Feature Name	Releases	Feature Information
Online diagnostics (GOLD)	4.0(1)	This feature was introduced.



CHAPTER 15

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 includes the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

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.

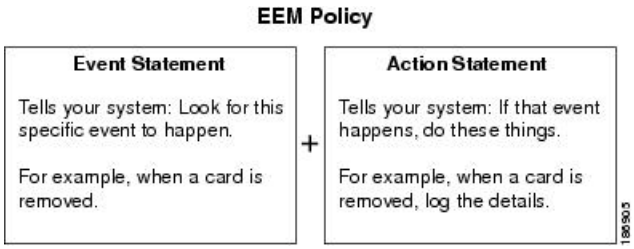
- Action statements—An action that EEM can take, such as sending an e-mail, or disabling an interface, to recover from an event.
- Policies—An event paired with one or more actions to troubleshoot or recover from the event.

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.

Figure 2: EEM Policy Statements



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 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.

The table below lists the system policies that can be completely overridden and policies that are only augmented.

System Policy	Can be completely overridden? Note Policies with default actions that cannot be completely overridden will be augmented.
__BootupPortLoopback	No
__FIPS	No
__IntPortLoopback	No
__PortLoopback	No
__RewriteEngineLoopback	No
__SnakeLoopback	No
__SwPortLoopback	No
__asic_register_check	Yes
__compact_flash	Yes
__eobc_port_loopback	Yes
__ethpm_debug_1	No
__ethpm_debug_2	No
__ethpm_debug_3	No
__ethpm_debug_4	No
__ethpm_link_flap	No
__external_compact_flash	Yes
__gold_obfl	Yes
__lcm_module_failure	Yes

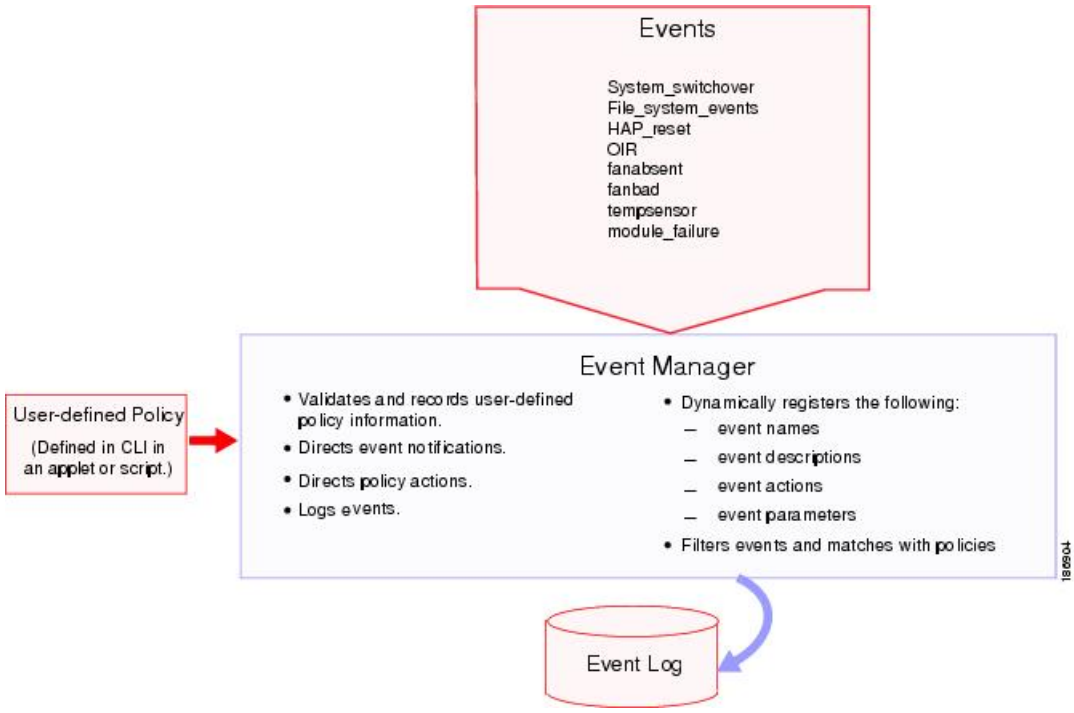
Event Statements

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.

Figure 3: EEM Overview



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 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 e-mail 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 foreshut 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

You configure EEM in the virtual device context (VDC) that you are logged into. By default, Cisco NX-OS places you in the default VDC. You must be in this VDC to configure policies for module-based events.

Not all actions or events are visible in all VDCs. You must have network-admin or vdc-admin privileges to configure policies.

See the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide* for more information on VDCs.

Prerequisites for EEM

EEM has the following prerequisites:

- The username: admin (with network-admin or vdc-admin user privileges) is required to configure EEM on a nondefault VDC.

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.
- If you want 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.
- An override policy that consists of an event statement and no 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, and only the * symbol can be used for argument replacement.
- 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.

- 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.
- EEM event correlation does not override the system default policies.
- Default action execution is not supported for policies that are configured with tagged events.
- While usign an EEM applet, the **copy r bootflash:last_config** command prompts for overriding the configuration file if the same file name is present. You need to add the **terminal dont-ask** if you are prompted to proceed with overwrtting a file in an EEM applet. Refer to the example given below.

```
event manager applet test
            event cli match "rollback *"
            action 1.0 cli command "terminal dont-ask"
            action 2.0 cli command "copy running-config bootflash:last_config"
            action 3.0 cli command "no terminal dont-ask"
```

- You can invoke EEM from Python. For more information about Python, see the *Cisco Nexus 7000 Series NX-OS Programmability Guide*.

Default Settings for EEM

This table lists the default settings for EEM parameters.

Parameters	Default
System policies	Active

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.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**event manager environment** *variable-name variable-value* **Example:**	Creates an environment variable for EEM. The *variable-name* can be any case-sensitive, alphanumeric string up to 29 characters. The *variable-value* can be any quoted alphanumeric string up to 39 characters.

	Command or Action	Purpose
	`switch(config)# event manager environment emailto “admin@anyplace.com”`	
Step 3	(Optional) **show event manager environment** {*variable-name* | **all**} **Example:** `switch(config)# show event manager environment all`	Displays information about the configured environment variables.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Defining a User Policy Using the CLI

You can define a user policy using the CLI to the device.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**event manager applet** *applet-name*
	Example:
	`switch(config)# event manager applet monitorShutdown`
	`switch(config-applet)#`
		Registers the applet with EEM and enters applet configuration mode. The *applet-name* can be any case-sensitive, alphanumeric string up to 29 characters.

Step 3	(Optional) **description** *policy-description* **Example:** `switch(config-applet)# description “Monitors interface shutdown.”`	Configures a descriptive string for the policy. The string can be any alphanumeric string up to 80 characters. Enclose the string in quotation marks.
Step 4	**event** *event-statement* **Example:** `switch(config-applet)# event cli match “conf t ; interface * ; shutdown”`	Configures the event statement for the policy. Repeat this step for multiple event statements. See Configuring Event Statements, on page 225.
Step 5	(Optional) **tag** *tag* {**and** | **andnot** | **or**} *tag* [**and** | **andnot** | **or** {*tag*}] {**happens** *occurs in seconds*} **Example:**	Correlates multiple events in the policy. The range for the *occurs* argument is from 1 to 4294967295. The range for the *seconds* argument is from 0 to 4294967295 seconds.

	Command or Action	Purpose
	`switch(config-applet)# tag one or two happens 1 in 10000`	
Step 6	**action** *label action-statement* **Example:** `switch(config-applet)# action 1.0 cli show interface e 3/1`	Configures an action statement for the policy. Repeat this step for multiple action statements. See Configuring Action Statements, on page 230.
Step 7	(Optional) **show event manager policy-state** *name* [**module** *module-id*] **Example:** `switch(config-applet)# show event manager policy-state monitorShutdown`	Displays information about the status of the configured policy.
Step 8	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring Event Statements

Use one of the following commands in Applet Configuration mode to configure an event statement:

Command	Purpose
event application [**tag** *tag*] **sub-system** *sub-system-id* **type** *event-type* **Example:** `switch(config-applet)# event application sub-system 798 type 1`	Triggers an event when an event specification matches the subsystem ID and application event type. The range for the *sub-system-id* and for the *event-type* is from 1 to 4294967295. The **tag** *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 cli [**tag** *tag*] **match** *expression* [**count** *repeats* | **time** *seconds*] **Example:** `switch(config-applet)# event cli match “conf t ; interface * ; shutdown”`	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.

Command	Purpose
event counter [**tag** *tag*] **name** *counter* **entry-val** *entry* **entry-op** {**eq** | **ge** | **gt** | **le** | **lt** | **ne**} [**exit-val** *exit* **exit-op** {**eq** | **ge** | **gt** | **le** | **lt** | **ne**}] **Example:** `switch(config-applet)# event counter name mycounter entry-val 20 gt`	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`	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`	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`	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	Purpose

event gold [**failure-type** {**sup** | **fabric** | **lc** | **port**}] **module** {*module* | **all**} **test** {*test-name* | *test-id*} [**severity** {**major** | **minor** | **moderate**}] **testing-type** {**bootup** | **monitoring** | **ondemand** | **scheduled**} **consecutive-failure** *count*
Example:
`switch(config-applet)# event gold failure-type module 2`
`test 7 ASICRegisterCheck testing-type ondemand consecutive-failure 2`
	Triggers an event if the named online diagnostic test experiences the configured failure severity for the configured number of consecutive failures.
	The *module* specifies the number of the module that needs to be monitored.
	The *test-name* is the name of a configured online diagnostic test. The *test-id* specifies the test ID of the event criteria. The range is from 1 to 30.
	The *count* range is from 1 to 1000.

event interface [**tag** *tag*] {**name** *interface slot*/*port* **parameter**} **Example:** `switch(config-applet)# event interface ethernet 2/2 parameter`	Triggers an event if the counter is exceeded for the specified interface. The **tag** *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 memory {**critical** | **minor** | **severe**} **Example:** `switch(config-applet)# event memory critical`	Triggers an event if a memory threshold is crossed. See also Configuring Memory Thresholds, on page 241.
event module [**tag** *tag*] **status** {**online** | **offline** | **any**} **module** {**all** | *module-num*} **Example:** `switch(config-applet)# event module status offline module all`	Triggers an event if the specified module enters the selected status. The **tag** *tag* keyword-argument pair identifies this specific event when multiple events are included in the policy.
event module-failure [**tag** *tag*] **type** *failure-type* **module** {*slot* | **all**} **count** *repeats* [**time** *seconds*] **Example:** `switch(config-applet)# event module-failure type lc-failed module 3 count 1`	Triggers an event if a module experiences the failure type configured. The **tag** *tag* keyword-argument pair identifies this specific event when multiple events are included in the policy. The *repeats* range is from 0 to 4294967295. The *seconds* range is from 0 to 4294967295, where 0 indicates no time limit.

Command	Purpose
event none **Example:** `switch(config-applet)# event none`	Manually runs the policy event without any events specified. **Note** To use this command, you must first enable the **feature evmed** command to enable generic event detectors.
event oir [**tag** *tag*] {**fan** | **module** | **powersupply**} {**anyoir** | **insert** | **remove**} [*number*] **Example:** `switch(config-applet)# event oir fan remove 4`	Triggers an event if the configured device element (fan, module, or power supply) is inserted or removed from the device. The **tag** *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.
event policy-default count *repeats* [**time** *seconds*] **Example:** `switch(config-applet)# event policy-default count 3`	Uses the event configured in the system policy. Use this option for overriding policies. The *repeats* range is from 1 to 65000. The *seconds* range is from 0 to 4294967295, where 0 indicates no time limit.
event poweroverbudget **Example:** `switch(config-applet)# event poweroverbudget`	Triggers an event if the power budget exceeds the capacity of the configured power supplies.

Command	Purpose
event snmp [**tag** *tag*] **oid** *oid* **get-type** {**exact** | **next**} **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`	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 **tag** *tag* keyword-argument pair identifies this specific event when multiple events are included in the policy. The *entry* and *exit* 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.
event storm-control **Example:** `switch(config-applet)# event storm-control`	Triggers an event if traffic on a port exceeds the configured storm control threshold.
event syslog [**occurs** *count*] {**pattern** *string* | **period** *time* | **priority** *level* | **tag** *tag*} **Example:** `switch(config-applet)# event syslog period 500`	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.
event sysmgr memory [**module** *module-num*] **major** *major-percent* **minor** *minor-percent* **clear** *clear-percent* **Example:** `switch(config-applet)# event sysmgr memory minor 80`	Triggers an event if the specified system manager memory threshold is exceeded. The range for the percentage is from 1 to 99.
event sysmgr switchover count *count* **time** *interval* **Example:** `switch(config-applet)# event sysmgr switchover count 10 time 1000`	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.
event temperature [**module** *slot*] [*sensor-number*] **threshold** {**any** | **major** | **minor**} **Example:** `switch(config-applet)# event temperature module 2 threshold any`	Triggers an event if the temperature sensor exceeds the configured threshold. The sensor range is from 1 to 18.

Command	Purpose
event timer {**absolute time** *time* **name** *name* | **countdown time** *time* **name** *name* | **cron cronentry** *string* | **tag** *tag* | **watchdog time** *time* **name** *name*} **Example:** `switch(config-applet)# event timer absolute time 100 name abtimer`	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 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** *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 [**tag** *tag*] *object-number* **state** {**any** | **down** | **up**} **Example:** `switch(config-applet)# event track 1 state down`	Triggers an event if the tracked object is in the configured state. The **tag** *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.

Configuring Action Statements

Use any of the following commands in Applet configuration (config-applet) mode to configure action statements:

Command	Purpose
action *label* **cli** *command1* [*command2...*] [**local**] **Example:** `switch(config-applet)# action 1.0 cli “show interface e 3/1“`	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. *number1* can be any number up to 16 digits. The range for *number2* is from 0 to 9.
action *label* **counter name** *counter* **value** *val* **op** {**dec** | **inc** | **nop** | **set**} **Example:** `switch(config-applet)# action 2.0 counter name mycounter value 20 op inc`	Modifies the counter by the configured value and operation. The action label is in the format number1.number2. *number1* can be any number up to 16 digits. The range for *number2* is from 0 to 9. The counter name can be any case-sensitive, alphanumeric string up to 28 characters. The *val* can be an integer from 0 to 2147483647 or a substituted parameter.
action *label* **event-default** **Example:** `switch(config-applet)# action 1.0 event-default`	Executes the default action for the associated event. The action label is in the format number1.number2. *number1* can be any number up to 16 digits. The range for *number2* is from 0 to 9.
action *label* **forceshut** [**module** *slot* | **xbar** *xbar-number*] **reset-reason** *seconds* **Example:** `switch(config-applet)# action 1.0 forceshut module 2 reset-reason “flapping links”`	Forces a module, crossbar, or the entire system to shut down. The action label is in the format number1.number2. *number1* can be any number up to 16 digits. The range for *number2* is from 0 to 9. The reset reason is a quoted alphanumeric string up to 80 characters.
action *label* **overbudgetshut** [**module** *slot*[-*slot*]] **Example:** `switch(config-applet)# action 1.0 overbudgetshut module 3-5`	Forces one or more modules or the entire system to shut down because of a power overbudget issue. The action label is in the format number1.number2. *number1* can be any number up to 16 digits. The range for *number2* is from 0 to 9.

Command	Purpose
action *label* **policy-default** **Example:** `switch(config-applet)# action 1.0 policy-default`	Executes the default action for the policy that you are overriding. The action label is in the format number1.number2. *number1* can be any number up to 16 digits. The range for *number2* is from 0 to 9.
action *label* **publish-event** **Example:** `switch(config-applet)# action 1.0 publish-event`	Forces the publication of an application-specific event. The action label is in the format number1.number2. *number1* can be any number up to 16 digits. The range for *number2* is from 0 to 9.
action *label* **reload** [**module** *slot*[*-slot*]] **Example:** `switch(config-applet)# action 1.0 reload module 3-5`	Forces one or more modules or the entire system to reload. The action label is in the format number1.number2. *number1* can be any number up to 16 digits. The range for *number2* is from 0 to 9.
action *label* **snmp-trap** {[**intdata1** *data* [**intdata2** *data*]] [**strdata** *string*]} **Example:** `switch(config-applet)# action 1.0 snmp-trap strdata “temperature problem”`	Sends an SNMP trap with the configured data. The action label is in the format number1.number2 *number1* can be any number up to 16 digits. The range for *number2* is from 0 to 9. The *data* arguments can by any number up to 80 digits. The *string* can be any alphanumeric string up to 80 characters.
action *label* **syslog** [**priority** *prio-val*] **msg** *error-message* **Example:** `switch(config-applet)# action 1.0 syslog priority notifications msg “cpu high”`	Sends a customized syslog message at the configured priority. The action label is in the format number1.number2. *number1* can be any number up to 16 digits. The range for *number2* is from 0 to 9. The *error-message* can be any quoted alphanumeric string up to 80 characters.
action *label* **end** **Example:** `switch(config-applet)# action 1.0 end`	Identifies the end of a conditional action block like if/else and while. The action label is in the format number1.number2. *number1* can be any number up to 16 digits. The range for *number2* is from 0 to 9.

Command	Purpose
action *label* **exit** [*result*] **Example:** `switch(config-applet)# action 1.0 exit 25`	Exits from the applet configuration mode that is currently running. 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.
action *label* **else** **Example:** `switch(config-applet)# action 1.0 else`	Identifies the beginning of an *else* conditional action block in an *if*/*else* action block. The action label is in the format number1.number2. *number1* can be any number up to 16 digits. The range for *number2* is from 0 to 9.
action *label* **elseif** *string-1* {**eq** | **gt** | **ge** | **lt** | **le** | **ne**} *string-2* `switch(config-applet)# action 1.0 elseif $x ge 10`	Identifies the beginning of an *elseif* conditional action block in an *else/if* action block. The action label is in the format number1.number2. *number1* can be any number up to 16 digits. The range for *number2* is from 0 to 9.
action *label* **if** *string-1* {**eq** | **gt** | **ge** | **lt** | **le** | **ne**} *string-2* `switch(config-applet)# action 1.0 if $x lt 10`	Identifies the beginning of an *if* conditional action block. The action label is in the format number1.number2. *number1* can be any number up to 16 digits. The range for *number2* is from 0 to 9.
action *label* **if** *string-1* {**eq** | **gt** | **ge** | **lt** | **le** | **ne**} *string-2* **goto** *label* `switch(config-applet)# action 2.0 if $x lt 10 goto 1.0`	Instructs the applet to jump to a given label if the specified condition is true. The action label is in the format number1.number2. *number1* can be any number up to 16 digits. The range for *number2* is from 0 to 9.
action *label* **puts** *string* **Example:** `switch(config-applet)# action 2.0 puts "Hello world"`	Enables the action of printing data directly to the terminal. The action label is in the format number1.number2. *number1* can be any number up to 16 digits. The range for *number2* is from 0 to 9.

Command	Purpose
action *label* **add** {*long-integer* | *variable-name*} {*long-integer* | *variable-name*} **Example:** `switch(config-applet)# action 2.0 add $var1 10`	Specifies the action of adding two variables. The action label is in the format number1.number2. *number1* can be any number up to 16 digits. The range for *number2* is from 0 to 9.
action *label* **decrement** *variable-name long-integer* **Example:** `switch(config-applet)# action 1.0 decrement $varname 12`	Specifies the action of decrementing the value of a variable. The action label is in the format number1.number2. *number1* can be any number up to 16 digits. The range for *number2* is from 0 to 9.
action *label* **increment** *variable-name long-integer* **Example:** `switch(config-applet)# action 2.0 increment $varname 12`	Specifies the action of incrementing the value of a variable. The action label is in the format number1.number2. *number1* can be any number up to 16 digits. The range for *number2* is from 0 to 9.
action *label* **multiply** {*long-integer1* | *variable-name1*} {*long-integer2* | *variable-name2*} `switch(config-applet)# action 2.0 multiply 12 35`	Specifies the action of multiplying a variable value with a long integer value. The action label is in the format number1.number2. *number1* can be any number up to 16 digits. The range for *number2* is from 0 to 9.
action *label* **subtract** {*long-integer1* | *variable-name1*} {*long-integer2* | *variable-name2*} **Example:** `switch(config-applet)# action 2.0 subtract $var1 $var2`	Specifies the action of subtracting the value of a variable from another one. The action label is in the format number1.number2. *number1* can be any number up to 16 digits. The range for *number2* is from 0 to 9.
action *label* **comment** *string* **Example:** `switch(config-applet)# action 2.0 comment keyvalue`	Adds comments to applets. The action label is in the format number1.number2. *number1* can be any number up to 16 digits. The range for *number2* is from 0 to 9.
action *label* **break** **Example:** `switch(config-applet)# action 2.0 break`	Specifies the action of exiting from a loop of actions. The action label is in the format number1.number2. *number1* can be any number up to 16 digits. The range for *number2* is from 0 to 9.

Command	Purpose
action *label* **continue** **Example:** `switch(config-applet)# action 2.0 continue`	Specifies the action of continuing with a loop of actions. The action label is in the format number1.number2. *number1* can be any number up to 16 digits. The range for *number2* is from 0 to 9.
action *label* **foreach** *string-iterator string-input* [*string-delimiter*] **Example:** `switch(config-applet)# action 3.1 foreach _iterator "orange blue green"`	Specifies the iteration of an input string using the delimiter as the tokenizing pattern. The action label is in the format number1.number2. *number1* can be any number up to 16 digits. The range for *number2* is from 0 to 9.
action *label* **while** *string-op-1 operator string-op-2* **Example:** `switch(config-applet)# action 3.2 while $i lt 10`	Identifies the beginning of a loop action block. The action label is in the format number1.number2. *number1* can be any number up to 16 digits. The range for *number2* is from 0 to 9. Valid values for *operator* are: ge, gt, eq, ne, lt, le.

Use any of the following action commands in Applet Configuration (config-applet) mode to enable string operations.

Command	Purpose
action *label* **append** *var-name* [*var-value*] `switch(config-applet)# action 4.2 append $var 12`	Specifies the action of appending the string value to the current value of a variable. The action label is in the format number1.number2. *number1* can be any number up to 16 digits. The range for *number2* is from 0 to 9. If the variable does not exist, it will be created and set to the given value.
action *label* **regexp** *string-pattern string-input* [*string-match* [*string-submatch1*] [*string-submatch2*] [*string-submatch3*]] `switch(config-applet)# action 4.3 regexp "(.*) (.*) (.*)" "one two three" _match _sub1`	Matches the regular expression in *string-pattern* on the *string-input*. *string-match* and *string-submatch* store the results of the match. The action label is in the format number1.number2. *number1* can be any number up to 16 digits. The range for *number2* is from 0 to 9.

Command	Purpose
action *label* **string compare** [**nocase**] [**length** *integer*] *string1 string2* `switch(config-applet)# action 4.5 string compare nocase length 3`	Compares two unequal strings. The result is stored in the inbuilt variable *$_string_result*. The action label is in the format number1.number2. *number* can be any number up to 16 digits. The range for *number2* is from 0 to 9.
action *label* **string equal** [**nocase**] [**length** *integer*] *string1 string2* `switch(config-applet)# action 4.5 string equal "contains" "data"`	Compares two strings and returns 1 if the two strings are equal. The result is stored in the inbuilt variable *$_string_result*. The action label is in the format number1.number2. *number1* can be any number up to 16 digits. The range for *number2* is from 0 to 9.
action *label* **string first** *string1 string2* [*index-value*] `switch(config-applet)# action 4.6 string first "contains" $str`	Returns the index of the first occurrence of *string1* within *string2*. *index-value* is optional and indicates the position to start the first test. The action label is in the format number1.number2. *number1* can be any number up to 16 digits. The range for *number2* is from 0 to 9.
action *label* **string index** *string* [*value* | *end*] `switch(config-applet)# action 4.7 string index "this is a test" 6`	Returns the characters specified at the given index-value. *end* denotes the last character of the string. The characters are stored in the inbuilt variable *$_string_result*. The action label is in the format number1.number2. *number1* can be any number up to 16 digits. The range for *number2* is from 0 to 9.
action *label* **string last** *string1 string2* [*index-value*] `switch(config-applet)# action 4.9 string last "contains" $str`	Returns the index of the last occurrence of *string1* within *string2*. The action label is in the format number1.number2. *number1* can be any number up to 16 digits. The range for *number2* is from 0 to 9.
action *label* **string length** *string* `switch(config-applet)# action 5.0 string length "contains"`	Returns the number of characters in a string. The result is stored in the inbuilt variable *$_string_result*. The action label is in the format number1.number2. *number1* can be any number up to 16 digits. The range for *number2* is from 0 to 9.
action *label* **string match** [**nocase**] *string-pattern string* `switch(config-applet)# action 5.2 string match "*Bl*" $str`	Matches *string* with a specified pattern, *string-pattern*. If they match, the result 1 is stored in the inbuilt variable *$_string_result*. The action label is in the format number1.number2. *number1* can be any number up to 16 digits. The range for *number2* is from 0 to 9.

Command	Purpose
action *label* **string range** *string start-index end-index* `switch(config-applet)# action 5.2 string range "$data" 4 9`	Stores a range of characters in a string, starting from the *start-index* and ending at *end-index*. The resultant characters are stored in the inbuilt variable *$_string_result*. The action label is in the format number1.number2. *number1* can be any number up to 16 digits. The range for *number2* is from 0 to 9.
action *label* **string replace** *string start-index end-index* [*new-string*] `switch(config-applet)# action 5.4 string replace $str 1 4 "test"`	Forms a new string by replacing specific characters of a string. If *new-string* is not specified, it replaces the characters with whitespace. The newly formed string is stored in the inbuilt variable *$_string_result*. 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.
action *label* **string tolower** *string* [*start-index*] [*end-index*] `switch(config-applet)# action 5.5 string tolower "$string" 11 16`	Stores a specific range of characters of a string in lowercase. The characters are stored in the inbuilt variable *$_string_result*. The action label is in the format number1.number2. *number1* can be any number up to 16 digits. The range for *number2* is from 0 to 9.
action *label* **string toupper** *string* [*start-index*] [*end-index*] `switch(config-applet)# action 5.6 string toupper "$string" 0 7`	Stores a specific range of characters of a string in uppercase. The characters are stored in the inbuilt variable *$_string_result* 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.
action *label* **string trim** *string1* [*string2*] `switch(config-applet)# action 5.7 string trim "$string"`	Trims the characters in *string2* from both ends of *string1*. By default, *string2* corresponds to whitespace. The action label is in the format number1.number2. *number1* can be any number up to 16 digits. The range for *number2* is from 0 to 9.
action *label* **string trimleft** *string1* [*string2*] `switch(config-applet)# action 5.7 string trimleft "$string" "Hello"`	Trims the characters in *string2* from the left end of *string1*. By default, *string2* corresponds to whitespace. The action label is in the format number1.number2. *number1* can be any number up to 16 digits. The range for *number2* is from 0 to 9.
action *label* **string trimright** *string1* [*string2*] `switch(config-applet)# action 5.7 string trimright "this is a testtest" "test"`	Trims the characters in *string2* from the right end of *string1*. By default, *string2* corresponds to whitespace. The action label is in the format number1.number2. *number1* can be any number up to 16 digits. The range for *number2* is from 0 to 9.

Command	Purpose
action *label* **set** *variable-name variable-value* `switch(config-applet)# action 6.0 set $string "Container"`	Sets the value of a variable. The action label is in the format number1.number2. *number1* can be any number up to 16 digits. The range for *number2* is from 0 to 9.

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. You can use the **terminal event-manager bypass** command to allow all EEM policies with CLI matches to execute the CLI command.

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.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

	Command or Action	Purpose
Step 2	**event manager policy** *policy-script* **Example:** `switch(config)# event manager policy moduleScript`	Registers and activates an EEM script policy. The *policy-script* can be any case-sensitive alphanumeric string up to 29 characters.
Step 3	**show event manager policy internal** *name* **Example:** `switch(config)# show event manager policy internal moduleScript`	(Optional) Displays information about the configured policy.
Step 4	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Scheduling an EEM Policy

You can schedule an EEM policy that is registered and set the policy scheduling options.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters the global configuration mode.

Step 2	**event manager scheduler applet thread class** *class-options* **number** *thread-number* **Example:** `switch(config)# event manager scheduler applet thread class default number 2`	Schedules an EEM policy and sets the policy scheduling options like class and thread number for execution.
Step 3	**event manager scheduler script thread class** *class-options* **range** *class-range* **number** *thread-number* **Example:** `switch(config)# event manager scheduler script thread class A B range D-E number 1`	Schedules an EEM policy and sets the script scheduling options.
Step 4	**event manager scheduler clear** {**all** | **policy** *job-id* | **queue-type applet** [**class** *class-options*]} [**processor {rp_primary | rp_standby}**] **Example:**	Clears the EEM policies that are currently executing or pending execution.

	Command or Action	Purpose
	`switch# event manager scheduler clear policy 2`	
Step 5	**event manager scheduler hold** {**all** | **policy** *job-id* | **queue-type applet** [**class** *class-options*]} **Example:** `switch# event manager scheduler hold policy 2`	Holds a scheduled EEM policy event or event queue in the EEM scheduler.
Step 6	**event manager scheduler modify** {**all** | **policy** *job-id* | **queue-type applet**} {**class** *class-options* [**queue-priority** {**high** | **last** | **low** | **normal**}] | **queue-priority** {**high** | **last** | **low** | **normal**} [**class** *class-options*]} **Example:** `switch# event manager scheduler modify all class A`	Modifies the scheduling parameters of the EEM policy.
Step 7	**event manager scheduler release** {**all** | **policy** *policy-id* | **queue-type applet** [**class** *class-options*]} **Example:** `switch# event manager scheduler release all`	Releases the EEM policies held through the event manger scheduler hold command.

Overriding a Policy

You can override a system policy.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	(Optional) **show event manager policy-state** *system-policy*
	Example:
	`switch(config-applet)# show event manager policy-state __ethpm_link_flap`
	`Policy __ethpm_link_flap`
	`Cfg count : 5`
	`Cfg time interval : 10.000000 (seconds)`
	`Hash default, Count 0`
		Displays information about the system policy that you want to override, including thresholds. Use the **show event manager system-policy** command to find the system policy names. For information about system policies, see Embedded Event Manager System Events and Configuration Examples, on page 489.

	Command or Action	Purpose
Step 3	**event manager applet** *applet-name* **override** *system-policy* **Example:** `switch(config)# event manager applet ethport override __ethpm_link_flap switch(config-applet)#`	Overrides a system policy and enters applet configuration mode. The *applet-name* can be any case-sensitive alphanumeric string up to 29 characters. The *system-policy* must be one of the existing system policies.
Step 4	(Optional) **description** *policy-description* **Example:** `description “Overrides link flap policy.”`	Configures a descriptive string for the policy. The string can be any alphanumeric string up to 80 characters. Enclose the string in quotation marks.
Step 5	Required: **event** *event-statement* **Example:** `switch(config-applet)# event policy-default count 2 time 1000`	Configures the event statement for the policy.
Step 6	Required: **action** *number action-statement* **Example:** `switch(config-applet)# action 1.0 syslog priority warnings msg “Link is flapping.”`	Configures an action statement for the policy. Repeat this step for multiple action statements.
Step 7	(Optional) **show event manager policy-state** *name* **Example:** `switch(config-applet)# show event manager policy-state ethport`	Displays information about the configured policy.
Step 8	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring Memory Thresholds

You can set the memory thresholds 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

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**system memory-thresholds minor** *minor* **severe** *severe* **critical** *critical* **Example:** `switch(config)# system memory-thresholds minor 60 severe 70 critical 80`	Configures the system memory thresholds that generate EEM memory events. The default values are as follows: • Minor-85 • Severe-90 • Critical-95 When these memory thresholds are exceeded, the system generates the following syslogs: • 2013 May 7 17:06:30 switch %$ %PLATFORM-2-MEMORY_ALERT: Memory Status Alert : MINOR • 2013 May 7 17:06:30 switch %$ %PLATFORM-2-MEMORY_ALERT: Memory Status Alert : SEVERE • 2013 May 7 17:06:30 switch %$ %PLATFORM-2-MEMORY_ALERT: Memory Status Alert : CRITICAL • 2013 May 7 17:06:35 switch %$ %PLATFORM-2-MEMORY_ALERT: Memory Status Alert : MINOR ALERT RECOVERED • 2013 May 7 17:06:35 switch %$ %PLATFORM-2-MEMORY_ALERT: Memory Status Alert : SEVERE ALERT RECOVERED • 2013 May 7 17:06:35 switch %$ %PLATFORM-2-MEMORY_ALERT: Memory Status Alert : CRITICAL ALERT RECOVERED
Step 3	(Optional) **system memory-thresholds threshold critical no-process-kill** **Example:** `switch(config)# system memory-thresholds threshold critical no-process-kill`	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.
Step 4	(Optional) **show running-config | include "system memory"** **Example:**	Displays information about the system memory configuration.

	Command or Action	Purpose
	`switch(config-applet)# show running-config | include “system memory”`	
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

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

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**event manager applet** *applet-name*
	Example:
	`switch(config)# event manager applet abc`
	`switch(config-applet)#`
		Registers an applet with EEM and enters applet configuration mode.

Step 3	**event syslog** [**tag** *tag*] {**occurs** *number* | **period** *seconds* | **pattern** *msg-text* | **priority** *priority*} **Example:** `switch(config-applet)# event syslog occurs 10`	Monitors syslog messages and invokes the policy based on the search string in the policy. • 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.

	Command or Action	Purpose
		• The **pattern** *msg-text* 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. • The **priority** *priority* 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.
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, use one of the following commands:

Command	Purpose
show event manager environment [*variable-name* | **all**]	Displays information about the event manager environment variables.
show event manager event-types [*event* | **all** | **module** *slot*]	Displays information about the event manager event types.
show event manager history events [**detail**] [**maximum** *num-events*] [**severity** {**catastrophic** | **minor** | **moderate** | **severe**}]	Displays the history of events for all policies.
show event manager policy internal [*policy-name*] [**inactive**]	Displays information about the configured policies.
show event manager policy-state *policy-name*	Displays information about the policy state, including thresholds.
show event manager script system [*policy-name* | **all**]	Displays information about the script policies.
show event manager system-policy [**all**]	Displays information about the predefined system policies.
show running-config eem	Displays information about the running configuration for EEM.

Command	Purpose
show startup-config eem	Displays information about the startup configuration for EEM.
show event manager policy active [**class** *class-options* | [**detailed**] [**queue-type** [**applet**]]	Displays the EEM policies that are executing.
show event manager policy pending [**class** *class-options* | [**detailed**] [**queue-type applet** [**detailed**]]	Displays the policies that are pending for execution.
show event manager scheduler thread detailed	Displays the scheduled activities of the EEM policies.

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.

```
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:

```
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:

```
event manager applet TEST
event cli match "conf t"
action 1.0 snmp-trap strdata "Configuration change"
action 2.0 event-default
```

Note 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.

```
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
```

Note For additional EEM configuration examples, see Embedded Event Manager System Events and Configuration Examples, on page 489.

This example shows how to monitor an interface shutdown with an EEM applet.

```
Devicek# sh run eem

!Command: show running-config eem
!Time: Thu Aug 24 00:21:17 2017

version 8.2(0)SK(1)
event manager applet E1
  event cli match "conf t ; interface * ; shutdown"
  action 1 syslog priority critical msg ""tracked interface shutdown" "
```

Related Documents

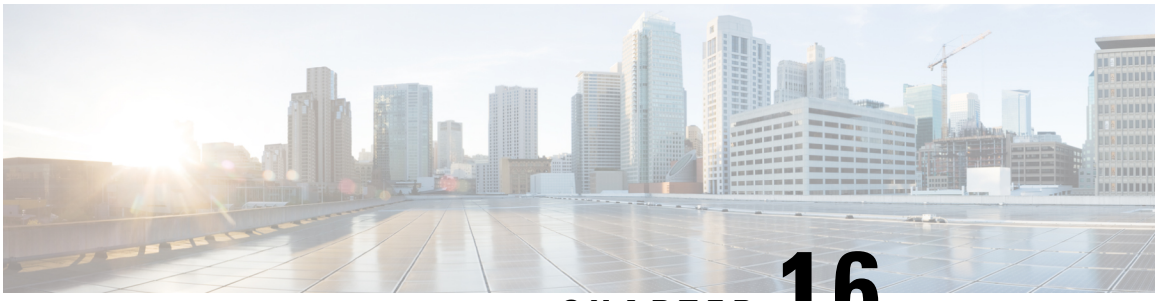
Related Topic	Document Title
EEM commands	*Cisco Nexus 7000 Series NX-OS System Management Command Reference*
VDCs	*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*

Feature History for EEM

Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Table 30: Feature History for EEM

Feature Name	Releases	Feature Information
EEM event correlation	5.2(1)	Added support for multiple event triggers in a single EEM policy.
Syslog as EEM publisher	5.1(1)	Added support to monitor syslog messages from the switch.
Memory thresholds configuration	4.1(3)	Added a configuration section for memory thresholds.



CHAPTER 16

Configuring Secure Erase

Information about Secure Erase

Beginning with Cisco NX-OS Release 8.2(8), the Secure Erase feature is introduced to erase all customer information for Nexus 7000 series switches. Secure Erase is an operation to remove all the identifiable customer information on Cisco NX-OS devices in conditions of product removal due to Return Merchandise Authorization (RMA), or upgrade or replacement, or system end-of-life.

Cisco Nexus 7000 switches consume storage to conserve system software images, switch configuration, software logs, and operational history. These areas can have customer-specific information such as details regarding network architecture, and design as well as a potential target for data thefts.

The Secure Erase process is used in the following two scenarios:

- Return Material Authorization (RMA) for a device - If you must return a device to Cisco for RMA, remove all the customer-specific data before obtaining an RMA certificate for the device.
- Recovering the compromised device - If the key material or credentials that are stored on a device is compromised, reset the device to factory configuration, and then reconfigure the device.

The device reloads to perform a factory reset which results in the switch entering the power-down mode. After a factory reset, the device clears all its environment variables including the MAC_ADDRESS and the SERIAL_NUMBER which are required to locate and load the software.

Prerequisites for Performing Secure Erase

- Ensure that all the software images, configurations, and personal data are backed up before performing the secure erase operation.
- Ensure that the device is not in stacking mode as factory reset is supported only in the standalone mode.
- Ensure that there is an uninterrupted power supply when the process is in progress.

- Ensure that you take a backup before you begin the secure erase process.
- Ensure that neither In-Service Software Upgrade (ISSU) nor In-Service Software Downgrade (ISSD) is in progress before starting the secure erase process.

Guidelines and Limitations for Secure Erase

- Software patches, if installed on the device, will not be restored after the Secure Erase operation.
- If the factory-reset command is issued through a session, the session is not restored after the completion of the factory reset process.
- The standby supervisor will be powered down after erasing it.
- If you configure secure erase of fex, the factory reset is initiated and fex configuration will be removed.
- After a successful factory reset, the switch will be powered down.
- You can erase information in order of modules, stand by supervisor, and active supervisor.
- The active supervisor and FEX modules will not be powered down. Only standby supervisor and line card modules will be powered down.

Configuring Secure Erase

To delete all necessary data before shipping to RMA, configure secure erase using the below command:

Procedure

	Command or Action	Purpose
Step 1	**factory-reset** [**fex** | **module** *mod*] **Example:** `Switch (config)# factory-reset [module <3>]`	Use the command with all options enabled. No system configuration is required to use the factory reset command. To initiate secure erase on fex, use **factory-reset fex**. To initiate secure erase on module, use **factory-reset mod**. After the factory reset process is successfully completed, the switch reboots and is powered down.

The erase procedure will be in the order of line card, standby supervisor, the active supervisor. It informs the target module of the erase request through the platform removes the module from the service and then reboots the card, which in turn triggers secure erase on the subsequent boot. Multiple modules can be done in parallel with each card responsible for notifying the active sup of success/failure upon completion.

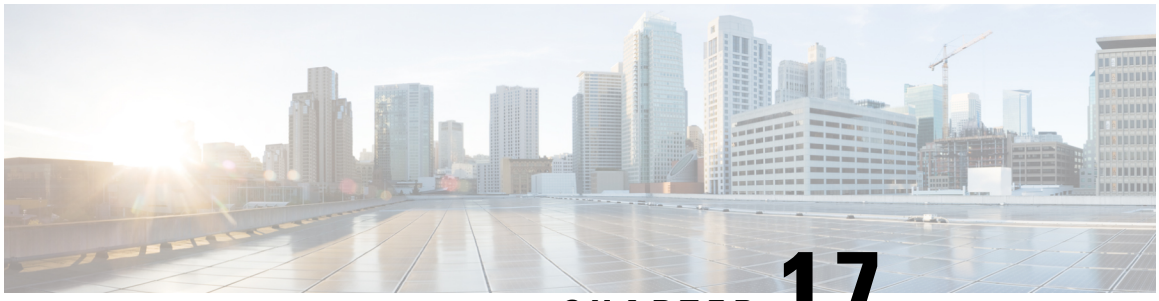
In the absence of an NX-OS image supporting these commands, a stand-alone image supporting erase will be provided. The user can then boot that secure erase image to trigger the data wipe.

Example

The following is an example output for configuring secure erase factory reset command for fex as follows:

```
switch# factory-reset fex {all | fex-id}
switch# factory-reset [fex <101>]

!!!! WARNING !!!!
The factory reset operation will erase ALL persistent storage on the specified module.
This includes configuration, all log data, and the full contents of flash and SSDs.
Special steps are taken in an effort to render data non-recoverable. Please, proceed with
caution and understanding that this operation cannot be undone and will leave the system
in a fresh-from-factory state.
!!!! WARNING !!!!

Continue? (y/n) y

A module reload is required for the reset operation to proceed.
Please, wait...
reloading fex 101 ...
Waiting for fex: 101 to complete factory-reset !!
.....................................................................................................
All detected storage devices on fex 101 have been wiped and reinitialized!
```

Configuring Secure Erase



CHAPTER 17

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:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

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
- Environmental history
- OBFL-specific history information
- ASIC interrupt and error statistics history
- ASIC register dumps

When you use the **show logging onboard internal xbar** command on a switch containing fabric modules, the output logs contain the hardware parameter values at that instance of time when the command is executed. Starting from Cisco NX-OS Release 8.4(1), the **show logging onboard internal xbar** command output will also have logs from the specific time when data loss, if any, occurs. This enhancement will further help in debugging the error.

Virtualization Support

You must be in the default virtual device context (VDC) to configure and display OBFL information. See the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide* for more information on VDCs.

Prerequisites for OBFL

If you configure VDCs, install the appropriate license and enter the desired VDC. See the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide* for configuration information and the *Cisco NX-OS Licensing Guide* for licensing information.

You must have network-admin user privileges and be logged into the default VDC.

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 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 used in Cisco IOS.

Default Settings for OBFL

The following table lists the default settings for OBFL parameters.

Parameters	Default
OBFL	All features enabled

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

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**hw-module logging onboard**
	Example:
	`switch(config)# hw-module logging onboard`
	`Module: 7 Enabling ... was successful.`
	`Module: 10 Enabling ... was successful.`
	`Module: 12 Enabling ... was successful.`
		Enables all OBFL features.

Step 3	**hw-module logging onboard counter-stats**
	Example:
	`switch(config)# hw-module logging onboard counter-stats`
	`Module: 7 Enabling counter-stats ... was successful.`
	`Module: 10 Enabling counter-stats ... was successful.`
	`Module: 12 Enabling counter-stats ... was successful.`
		Enables the OBFL counter statistics.

	Command or Action	Purpose

Step 4	**hw-module logging onboard cpuhog**
	Example:
	`switch(config)# hw-module logging onboard cpuhog`
	`Module: 7 Enabling cpu-hog ... was successful.`
	`Module: 10 Enabling cpu-hog ... was successful.`
	`Module: 12 Enabling cpu-hog ... was successful.`
		Enables the OBFL CPU hog events.

Step 5	**hw-module logging onboard environmental-history**
	Example:
	`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.`
		Enables the OBFL environmental history.

Step 6	**hw-module logging onboard error-stats**
	Example:
	`switch(config)# hw-module logging onboard error-stats`
	`Module: 7 Enabling error-stats ... was successful.`
	`Module: 10 Enabling error-stats ... was successful.`
	`Module: 12 Enabling error-stats ... was successful.`
		Enables the OBFL error statistics.

Step 7	**hw-module logging onboard interrupt-stats**
	Example:
	`switch(config)# hw-module logging onboard interrupt-stats`
	`Module: 7 Enabling interrupt-stats ... was successful.`
	`Module: 10 Enabling interrupt-stats ... was successful.`
	`Module: 12 Enabling interrupt-stats ... was successful.`
		Enables the OBFL interrupt statistics.

Step 8	**hw-module logging onboard module** *slot*
	Example:
	`switch(config)# hw-module logging onboard module 7`
	`Module: 7 Enabling ... was successful.`
		Enables the OBFL information for a module.

	Command or Action	Purpose

Step 9	**hw-module logging onboard obfl-logs**
	Example:
	`switch(config)# hw-module logging onboard obfl-logs`
	`Module: 7 Enabling obfl-log ... was successful.`
	`Module: 10 Enabling obfl-log ... was successful.`
	`Module: 12 Enabling obfl-log ... was successful.`
		Enables the boot uptime, device version, and OBFL history.

Step 10	(Optional) **show logging onboard** **Example:** `switch(config)# show logging onboard`	Displays information about OBFL.
Step 11	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Verifying the OBFL Configuration

To display OBFL information stored in flash on a module, perform one of the following tasks:

Command	Purpose
show logging onboard boot-uptime	Displays the boot and uptime information.
show logging onboard counter-stats	Displays statistics on all ASIC counters.
show logging onboard credit-loss	Displays OBFL credit loss logs.
show logging onboard device-version	Displays device version information.
show logging onboard endtime	Displays OBFL logs to a specified end time.
show logging onboard environmental-history	Displays environmental history.
show logging onboard error-stats	Displays error statistics.
show logging onboard exception-log	Displays exception log information.
show logging onboard interrupt-stats	Displays interrupt statistics.
show logging onboard internal xbar	Displays OBFL information for fabric modules.
show logging onboard module *slot*	Displays OBFL information for a specific module.
show logging onboard obfl-history	Displays history information.
show logging onboard obfl-logs	Displays log information.
show logging onboard stack-trace	Displays kernel stack trace information.

Command	Purpose
show logging onboard starttime	Displays OBFL logs from a specified start time.
show logging onboard status	Displays OBFL status information.

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-uptime/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-uptime/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

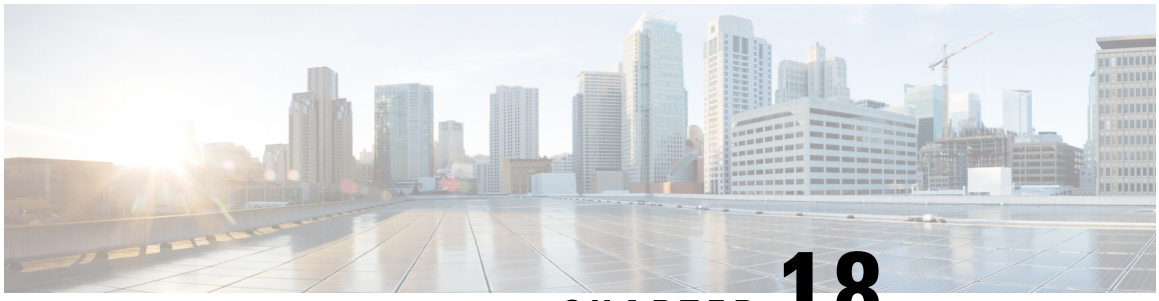
Related Topic	Document Title
OBFL CLI commands	*Cisco Nexus 7000 Series NX-OS System Management Command Reference*
Configuration files	*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide*
VDCs	*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*

Feature History for OBFL

Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Table 31: Feature History for OBFL

Feature Name	Releases	Feature Information
OBFL	4.0(1)	This feature was introduced.



CHAPTER 18

Configuring SPAN

This chapter describes how to configure an Ethernet switched port analyzer (SPAN) to analyze traffic between ports on Cisco NX-OS devices.

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

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, egress, or both directions of traffic. SPAN sources include the following:

- Ethernet ports

- Port channels
- The inband interface to the control plane CPU
- VLANs (ingress only)—When a VLAN is specified as a SPAN source, all supported interfaces in the VLAN are SPAN sources.
- Remote SPAN (RSPAN) VLANs
- Fabric port channels connected to the Cisco Nexus 2000 Series Fabric Extender (FEX)
- Satellite ports and host interface port channels on the Cisco Nexus 2000 Series Fabric Extender— These interfaces are supported in Layer 2 access mode, Layer 2 trunk mode, and Layer 3 mode.

Note Layer 3 subinterfaces are not supported.

Note A single SPAN session can include mixed sources in any combination of the above.

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.
- An RSPAN VLAN cannot be used as a SPAN source.
- 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.

Characteristics of Destination Ports

SPAN destination ports have the following characteristics:

- Destinations for a SPAN session include Ethernet ports or port-channel interfaces in either access or trunk mode.
- 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.
- All SPAN destinations configured for a given session receive all spanned traffic.

- An RSPAN VLAN cannot be used as a SPAN destination.
- You can configure SPAN destinations to inject packets to disrupt a certain TCP packet stream in support of the Intrusion Detection System (IDS).
- You can configure SPAN destinations to enable a forwarding engine to learn the MAC address of the IDS.
- F Series module FabricPath core ports, Fabric Extender host interface (HIF) ports, HIF port channels, and fabric port-channel ports are not supported as SPAN destination ports.
- Shared interfaces cannot be used as SPAN destinations.
- VLAN ACL redirects to SPAN destination ports are not supported
- All SPAN destinations configured for a given session receive all spanned traffic.

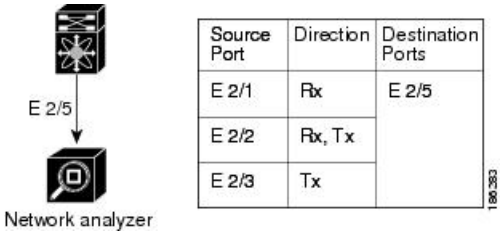
SPAN Sessions

You can create SPAN sessions to designate sources and destinations to monitor.

See the *Cisco Nexus 7000 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 4: SPAN Configuration



Extended SPAN Sessions

Cisco NX-OS Release 6.2(2) and later releases support extended SPAN sessions in addition to the two traditional SPAN sessions supported in prior releases. Extended SPAN sessions can be traditional or unidirectional. The session direction is specified during session creation. A pool of 12 independent session resources are available. Unidirectional sessions use one resource, and traditional sessions use two resources. These 12 resources are shared between local and SPAN source sessions across all VDCs.

If you are configuring an extended SPAN session on a Cisco Nexus 7710 switch or a Cisco Nexus 7718 switch, the following applies:

- The **mode extended** command must be used with the third configuration session.
- You can configure 16 sessions as unidirectional or bidirectional, as required.
- You do not need to maintain two traditional sessions.
- You do not need to use the resource manager to reserve the two traditional sessions.

4K VLANs per SPAN Session

Cisco NX-OS Release 7.3(0)D1(1) and later releases support 4K VLANs per SPAN session. You can use the **source interface all** command to enable the monitor session on the switch to monitor all VLANs and ports in the VDC such as physical ports, Port Channels, FEX ports and FEX Port Channels. The 4K VLANs per SPAN Session feature also enables monitoring of a higher number of specific VLAN sources than the VLAN source limits currently supported in the monitor session by using the **filter vlan** command with the **source interface all** command to filter the irrelevant VLANs.

The 4K VLANs per SPAN Session feature has the following characteristics:

- This is not supported on M3 series modules.
- You will not be able to capture any traffic on the M3 Series modules in spite of configuring the**source interface all** command.
- You can use the **source interface all** command for multiple sessions in the same VDC.
- Supports all session parameters such as MTU truncation, Sampling and Rate Limiting.
- Simple and Complex Rule-based SPAN is supported with the **source interface all** command. This enables traffic flow-based monitoring using a set of filter rules across the VDC.
- Traffic generated by Supervisors is not spanned.
- Supported only in Ethernet VDCs of Cisco Nexus 7000 Series switches.
- Supported only in extended SPAN sessions.

Rule-Based SPAN

Rule-based SPAN filters the ingress or egress SPAN traffic based on a set of rules. For Cisco NX-OS releases prior to 6.2(2), you can filter on VLANs, the destination index, and the source index. Beginning with Cisco NX-OS Release 6.2(2), you can filter the SPAN traffic based on a combination of fields in the Layer 2, Layer 3, or Layer 4 header packet.

Every SPAN session (traditional and extended) has an associated filter. Every SPAN session has one filter resource. A simple filter has only one rule, and you can add multiple fields or conditions to this rule. The packets are replicated only if all the conditions are met.

Table 32: Supported Filter Fields

Ethernet	IPv4	IPv6	ARP/RARP	FCoE

Frame Type	Frame Type	Frame Type	Frame Type	Frame Type
VLAN	VLAN	VLAN	VLAN	VLAN
TR	TR	TR	TR	TR
BPDU	BPDU	BPDU	BPDU	BPDU
Port Channel Lane	Port Channel Lane	Port Channel Lane	Port Channel Lane	Port Channel Lane
Flow Hash	Flow Hash	Flow Hash	Flow Hash	Flow Hash
L2 MAC DA	L2 MAC DA	L2 MAC DA	L2 MAC DA	L2 MAC DA
L2 MAC SA	L2 MAC SA	L2 MAC SA	L2 MAC SA	L2 MAC SA
EtherType	EtherType	EtherType	EtherType	EtherType
CoS/VL	CoS/VL	CoS/VL	CoS/VL	CoS/VL
	ToS	ToS	ARP	FCD_ID
	L4 Protocol	L4 Protocol	Request	FCS_ID
	IPv4 SA	IPv6 SA	Sender IP	SOF
	IPv4 DA	IPv6 DA	Target IP	R_CTL
				TYPE
				Cmd_Code

Exception SPAN

Exception SPAN enables you to span exception packets. Packets that have failed an intrusion detection system (IDS), Layer 3 IP verification, and FabricPath are treated as exception packets.

Note Beginning with Cisco NX-OS Release 6.2(10), you can remove the FabricPath and VLAN tag headers from SPAN packets. Use the **system default switchport monitor exclude header** and the **switchport monitor exclude header** commands. See the *Cisco Nexus 7000 Series NX-OS Security Command Reference* for more information on these commands.

An exception SPAN session is supported in either one of the two traditional bidirectional SPAN sessions or in one of the extended SPAN sessions. Rate limiters, MTU truncation, and sampling are supported in the exception SPAN session. Only the exception packets sent to the drop destination interface are supported as a SPAN source. Exception packets that are pushed to the supervisor, ACLQoS, or Layer 2 are not spanned. Each VDC supports one exception SPAN session.

Extended SPAN is supported in the egress direction only. In the case of an extended SPAN Rx session, the exception source configuration will be rejected.

Virtual SPAN Sessions

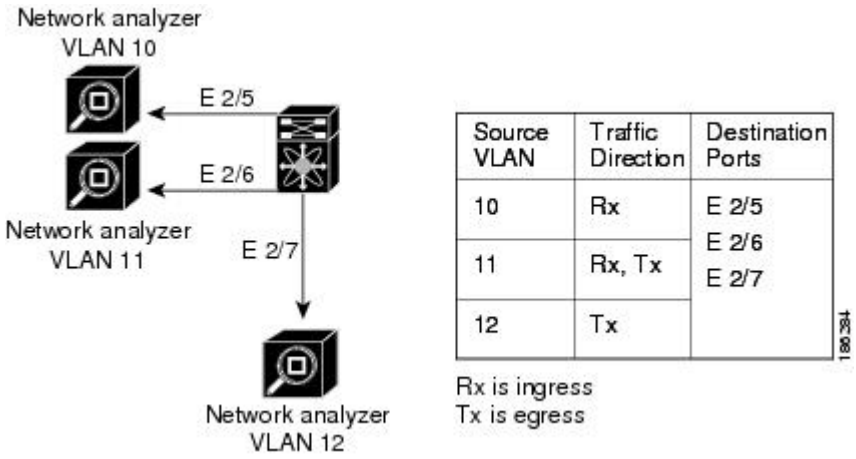
You can create a virtual SPAN session to monitor multiple VLAN sources and choose only VLANs of

interest to transmit on multiple destination ports. For example, you can configure SPAN on a trunk port and monitor traffic from different VLANs on different destination ports.

The figure below shows a virtual SPAN configuration. The virtual SPAN session copies traffic from the three VLANs to the three specified destination ports. You can choose which VLANs to allow on each destination port to limit the traffic that the device transmits on it. In the figure below, the device transmits packets from one VLAN at each destination port.

Note Virtual SPAN sessions cause all source packets to be copied to all destinations, whether the packets are required at the destination or not. VLAN traffic filtering occurs at the egress destination port level.

Figure 5: Virtual SPAN Configuration



For information about configuring a virtual SPAN session see the *Configuring a Virtual SPAN Session* section.

Network Analysis Module

You can also use the Cisco Network Analysis Module (NAM) to monitor SPAN data sources for application performance, traffic analysis, and packet header analysis.

To use NAM for monitoring the Cisco Nexus 7000 SPAN data sources, see the *Cisco Nexus 7000 Series Network analysis Module (NAM-NX1) Quick Start 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 7000 Series NX-OS High Availability and Redundancy Guide*.

Virtualization Support

A virtual device context (VDC) is a logical representation of a set of system resources. SPAN applies only to the VDC where the commands are entered.

For information about configuring VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*.

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 7000 Series NX-OS Interfaces Configuration Guide*.

Guidelines and Limitations for SPAN

General SPAN Guidelines and Limitations

- For SPAN session limits, see the *Cisco Nexus 7000 Series NX-OS Verified Scalability Guide*.
- SPAN is not supported for management ports.
- All SPAN replication is performed in the hardware. The supervisor CPU is not involved.
- Link Aggregation Control Protocol (LACP) Port Channel is not supported as a SPAN destination.

Note Monitor session allows LACP PO to be added as SPAN destination even though the same is not supported. This does not impact any functionality.

- A destination port can only be configured in one SPAN session at a time.
- You cannot configure a port as both a source and destination port.
- If a module is not in the VDC in which the inband interface is sourced, packets destined to the supervisor cannot be captured.
- For Cisco NX-OS releases prior to 6.1, you can monitor the inband interface only from the default VDC. Inband traffic from all VDCs is monitored. Beginning with Cisco NX-OS Release 6.1, the monitoring of the inband interface is no longer restricted to the default VDC:
  - Only users with the network admin privilege can add the inband interface as a SPAN source.
  - The inband interface can be added as a source from any VDC except the admin VDC, but at any time, only one VDC can have the inband interface as a source.
- Inband SPAN is treated as a shared resource. If a particular VDC does not have the resource allocated to it, inband port sourcing is rejected. Similarly, if a VDC that has the inband supervisor resource allocated to it removes the inband port from the source list of all monitor sessions, the inband resource is released from that VDC.
- For the supervisor inband interface, SPAN is supported only in the VDC in which the inband interface is sourced. If a module is part of a VDC in which the inband interface is not sourced, at least one interface

of the module must be in the VDC in which the inband interface is sourced in order to capture supervisor inband packets from this module.

- A single SPAN session can include mixed sources in any combination of the following:
  - Ethernet ports, but not subinterfaces
  - VLANs, that can be assigned to port channel subinterfaces
  - The inband interface to the control plane CPU
- When a SPAN session contains both source interfaces and source VLAN clauses, there is a possibility that other VLANs also will be spanned.
- Destination ports do not participate in any spanning tree instance. SPAN output includes bridge protocol data unit (BPDU) Spanning-Tree Protocol hello packets.
- When a SPAN session contains source ports or VLAN sources 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
- You can enable SPAN for a source port before it becomes operationally active. Thus for Layer 2 ports, traffic flooded to the VLANs that contain these ports are captured even when the link is not connected for the ports.
- For VLAN SPAN sessions with both ingress and egress configured, two packets (one from ingress and one from egress) are forwarded from the destination port if the packets get switched on the same VLAN.
- Beginning with Cisco NX-OS Release 6.2(2), the spanning of inband interfaces is as follows:
  - For Supervisor 1 systems, the two bidirectional traditional sessions can support an inband SPAN source.
  - For Supervisor 2 and Supervisor 2e systems, all the SPAN sessions can support an inband SPAN source.
  - Only one VDC can support inband SPAN at a time.
- You can configure an RSPAN VLAN for use only as a SPAN session source.
- You can configure a SPAN session on the local device only.
- If you span a fabricpath core interface when inter-VLAN routing is enabled across Layer 2 multi-path (L2MP), it is not possible to capture the traffic egressing out of the core interface.
- SPAN is supported on Fabric Extender interfaces in Layer 2 access mode, Layer 2 trunk mode, and Layer 3 mode. Layer 3 subinterfaces are not supported.
- Cisco NX-OS does not span Link Layer Discovery Protocol (LLDP) or Link Aggregation Control Protocol (LACP) packets when the source interface is a Fabric Extender HIF (downlink) port or HIF port channel.
- 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.

- The rate limit percentage of a SPAN session is based on 10G, 40G, and 100G for the respective modules (that is, 1 percent corresponds to 0.1G, 0.4G, or 1G respectively), and the value is applied per every forwarding engine instance.
- Beginning with Cisco NX-OS Release 6.1, SPAN is supported for Supervisor 2.
- SPAN does not capture pause frames in a Fibre Channel over Ethernet (FCoE) network because pause frames sent from the virtual expansion (VE) port are generated and terminated by the outermost MAC layer. For more information on FCoE, see the *Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500*.
- On both Supervisor 1 and Supervisor 2, you cannot monitor the FCoE inband traffic.
- You can monitor both ingress and egress FCoE traffic can be monitored in a local SPAN session through Ethernet interfaces, including shared interfaces, or VLANs. For shared interfaces, you can monitor the FCoE traffic only in the storage VDC.
- The MAC in MAC (MiM) header in SPAN copies is preserved for the following SPAN destinations:
  - F2e modules with Release 6.2 or later releases.
  - F3 series modules with any Cisco NX-OS Release.
  - For F3 series modules with Release 6.2.(6a), 6.2.(6b), or 6.2(8), the Fabricpath (FP) header is preserved unconditionally. In Release 6.2.10, the FP header is preserved by default, but this behavior can changed by using the **switchport monitor exclude header** command to remove the FP or VLAN tag header for a specified SPAN destination in a VDC or the **system default switchport monitor exclude header** command to remove the FP or VLAN tag header for all destinations ports in the VDC. In Release 6.2.12, you can remove the FabricPath and VLAN tag headers using the **switchport monitor exclude header** command at the SPAN destination.
- The MiM header in SPAN copies is not preserved for the following SPAN destinations:
  - F1 and F2 series modules with any Cisco NX-OS Release.
  - F2e modules with Release 6.1(x).
  - For F3 series modules with Release 6.2.6, the FabricPath (FP) header is not preserved.

Guidelines and Limitations for F1 Series Module

- Prior to Cisco NX-OS Release 7.2(0)D1(1), multiple SPAN destinations are not supported when an F Series module is present in a VDC. If multiple SPAN destinations are configured in a SPAN session, the session is disabled until the F Series module is powered down or moved to another VDC or the multiple SPAN destinations are reduced to a single destination.

  Starting from Cisco NX-OS Release 7.2(0)D1(1), multiple destination SPAN sessions are supported. Only the primary destination is used to transmit SPAN packets originated from Fx modules. Traffic from M series module goes to every destination port.
- A FabricPath core port is not supported as a SPAN destination when an F Series module is present in a VDC. However, a FabricPath core port can be configured as a SPAN source interface.

- F1 Series modules are Layer 2 domain modules. Packets from Layer 3 sources can be spanned and directed to an F1 Series module SPAN destination. An F1 Series module interface cannot be configured as Layer 3, but it can receive Layer 3 traffic in a SPAN destination mode.
- When using SPAN sessions on F1 Series or F2 Series modules, ensure that the total amount of source traffic in a given session is less than or equal to the capacity of the SPAN destination interface or port channel for that session. If the SPAN source traffic exceeds the capacity of the SPAN destination, packet drops might occur on the SPAN source interfaces. This guideline does not apply to F2e, F3 or M3 Series modules.
- MTU truncation and the SPAN rate limit are supported on F Series and M2 Series modules and Supervisor 2.

Note You cannot enable MTU truncation and the SPAN rate limit for the same SPAN session on F1 Series modules. If you configure both for one session, only the rate limit is allowed on F1 Series modules, and MTU truncation is disabled until you disable the rate limit configuration. This limitation does not apply to F2 and M2 Series modules or Supervisor 2.

- For F1 Series modules, MTU truncation on egress spanned FabricPath (core) packets has 16 fewer bytes than the configured value because the SPAN destination removes the core header. In addition, when trunk ports are used as the SPAN destination, the spanned ingress packets have 4 more bytes than the configured MTU truncation size.
- For certain rate limit and packet size values on F Series modules, M2 Series modules, and Supervisor 2, the SPAN packet rate is less than the configured value because of the internal accounting of packet sizes and internal headers.
- SPAN sampling is supported only on F Series modules.
- Traditional SPAN sessions support traffic from the F Series and M Series modules. Extended SPAN sessions support traffic only from the F Series and M2 Series modules.
- F1 Series modules have limited support for rule-based SPAN. They do not support IPv6 source IP and IPv6 destination IP filters. They support only IPv4 and IPv6 ToS filters with values from 0 to 3. Port channel member lane, FCoE source ID, and FCoE destination ID are not supported.

Guidelines and Limitations for F2/F2e Series Modules

- For certain rate limit and packet size values on F Series modules, M2 Series modules, and Supervisor 2, the SPAN packet rate is less than the configured value because of the internal accounting of packet sizes and internal headers.
- SPAN sampling is supported only on F Series modules.
- Traditional SPAN sessions support traffic from the F Series and M Series modules. Extended SPAN sessions support traffic only from the F Series and M2 Series modules.
- When the supervisor inband interface is monitored in the transmit direction on F2 Series modules, a 12-byte SHIM header is inserted after SMAC in SPAN packets.

- Prior to Cisco NX-OS Release 7.2(0)D1(1), multiple SPAN destinations are not supported when an F Series module is present in a VDC. If multiple SPAN destinations are configured in a SPAN session, the session is disabled until the F Series module is powered down or moved to another VDC or the multiple SPAN destinations are reduced to a single destination.

  Starting from Cisco NX-OS Release 7.2(0)D1(1), multiple destination SPAN sessions are supported. Only the primary destination is used to transmit SPAN packets originated from Fx modules. Traffic from M series module goes to every destination port.

- A FabricPath core port is not supported as a SPAN destination when an F Series module is present in a VDC. However, a FabricPath core port can be configured as a SPAN source interface.
- SPAN source functionality on satellite ports and host interface port channels is not supported when the FEX is connected to F2 or F2e Series modules.
- When using SPAN sessions on F1 Series or F2 Series modules, ensure that the total amount of source traffic in a given session is less than or equal to the capacity of the SPAN destination interface or port channel for that session. If the SPAN source traffic exceeds the capacity of the SPAN destination, packet drops might occur on the SPAN source interfaces. This guideline does not apply to F2e, F3 or M3 Series modules.
- VLANs containing FEX interfaces can be a SPAN source, but the ingress traffic through the F2 Series module-based FEX ports cannot be captured.
- F2 Series modules support FEX, but they do not support FEX SPAN. Therefore, the FEX interfaces connected through the F2 Series modules cannot be made SPAN sources.
- You can span Fabric port channels on F2 Series modules.
- Layer 3 multicast egress packets cannot be spanned on F2 Series modules.
- MTU truncation and the SPAN rate limit are supported on F Series and M2 Series modules and Supervisor 2. These features are not supported on M1 Series modules.
- For F2 Series modules, ingress FEX packets spanned through the Fabric port channel have 6 fewer bytes than the configured MTU size because the VNTag header is removed on the SPAN destination.
- For F2 Series modules, egress SPAN packets of all traffic that ingresses on Layer 2 ports (including edge-to-edge traffic) have 16 fewer bytes than the configured MTU size because a MAC-in-MAC header is added internally and removed at the SPAN destination.
- For F2, F2e, and F3 Series modules using SPAN destination port channels, SPAN traffic is distributed among the member ports. However, the distribution pattern can be different from that of regular (non-SPAN destination) port channels. For example, you can have even load distribution for regular port channels but uneven load distribution (or no load balancing) for SPAN destination port channels.
- For certain rate limit and packet size values on F Series modules, M2 Series modules, and Supervisor 2, the SPAN packet rate is less than the configured value because of the internal accounting of packet sizes and internal headers.
- SPAN sampling is supported only on F Series modules. It is not supported on M Series modules.
- Beginning with Cisco NX-OS Release 6.1, FCoE SPAN on F2 Series modules is supported for storage VDCs.
- Hardware session 15 is used by NetFlow on F2 and F2e Series modules. Any extended session using this hardware ID will not span incoming traffic on the F2 and the F2e ports.

- F2 and F2e Series modules have limited support for rule-based SPAN. They do not support wildcards in the IPv6 source IP filter and IPv6 destination IP filter. They do not support egress SPAN filtering for destination MAC addresses and source MAC addresses.

Guidelines and Limitations for F3 Series Module

- For certain rate limit and packet size values on F Series modules, M2 Series modules, and Supervisor 2, the SPAN packet rate is less than the configured value because of the internal accounting of packet sizes and internal headers.
- SPAN sampling is supported only on F Series modules.
- Traditional SPAN sessions support traffic from the F Series and M Series modules. Extended SPAN sessions support traffic only from the F Series and M2 Series modules.
- Layer 3 multicast egress packets cannot be spanned on F3 Series modules.
- Prior to Cisco NX-OS Release 7.2(0)D1(1), multiple SPAN destinations are not supported when an F Series module is present in a VDC. If multiple SPAN destinations are configured in a SPAN session, the session is disabled until the F Series module is powered down or moved to another VDC or the multiple SPAN destinations are reduced to a single destination.

  Starting from Cisco NX-OS Release 7.2(0)D1(1), multiple destination SPAN sessions are supported. Only the primary destination is used to transmit SPAN packets originated from Fx modules. Traffic from M series module goes to every destination port.
- MTU truncation and the SPAN rate limit are supported on F Series and M2 Series modules and Supervisor 2.
- A FabricPath core port is not supported as a SPAN destination when an F Series module is present in a VDC. However, a FabricPath core port can be configured as a SPAN source interface.
- F3 Series modules do not support wildcards in the IPv6 source IP filters and the IPv6 destination IP filters.

Guidelines and Limitations for M1/M1XL Series Modules

- SPAN sampling is not supported on M Series modules.
- Traditional SPAN sessions support traffic from the F Series and M Series modules. Extended SPAN sessions support traffic only from the F Series and M2 Series modules.
- Beginning with Cisco NX-OS Release 5.2, you can configure the Cisco Nexus 2000 Series Fabric Extender (FEX) interfaces and the fabric port channels that are connected to the Cisco Nexus 2000 Series Fabric Extender as SPAN sources. However, you cannot configure them as SPAN destinations.

Note SPAN on Fabric Extender interfaces and fabric port channels is supported on the M1 Series and M2 Series modules. SPAN runs on the Cisco Nexus 7000 Series device, not on the Fabric Extender.

- If a port channel is the SPAN destination interface for SPAN traffic that is sourced from a Cisco Nexus 7000 M1 Series module, only a single member interface will receive copied source packets. The same limitation does not apply to SPAN traffic sourced from all other Cisco Nexus series modules, including the Cisco Nexus 7000 M1-XL Series modules.
- MTU truncation and the SPAN rate limit are not supported on M1 Series modules.
- Multicast best effort mode applies only to M1 Series modules.
- Extended SPAN sessions cannot source incoming traffic on M1 Series modules in either the ingress or egress direction.
- Traditional SPAN sessions support traffic from the F Series and M Series modules. Extended SPAN sessions support traffic only from the F Series and M2 Series modules.
- M1 Series modules and Supervisor 1 do not support rule-based SPAN. They support only VLAN filtering.
- M1 and M2 Series modules support exception SPAN only in the nonadministration VDC, and at least one interface of the module must be present for the VDC.

Guidelines and Limitations for M2/M2XL Series Modules

- Beginning with Cisco NX-OS Release 5.2, you can configure the Cisco Nexus 2000 Series Fabric Extender (FEX) interfaces and the fabric port channels that are connected to the Cisco Nexus 2000 Series Fabric Extender as SPAN sources. However, you cannot configure them as SPAN destinations.

Note SPAN on Fabric Extender interfaces and fabric port channels is supported on the M1 Series and M2 Series modules. SPAN runs on the Cisco Nexus 7000 Series device, not on the Fabric Extender.

- For certain rate limit and packet size values on F Series modules, M2 Series modules, and Supervisor 2, the SPAN packet rate is less than the configured value because of the internal accounting of packet sizes and internal headers.
- Packets may get dropped when the ingress SPAN configured on M2 module and on any other next gen line card module such as F3, M3 having SPAN destination ports; and if the configured monitor sessions on M2 modules and its hardware session IDs (check the **show monitor resource session all** command output for hw_ssn_id) are more than 11. To overcome this issue, shut down all the SPAN sessions/unconfigure and re-configure the sessions.
- SPAN sampling is not supported on M Series modules.
- Traditional SPAN sessions support traffic from the F Series and M Series modules. Extended SPAN sessions support traffic only from the F Series and M2 Series modules.
- M1 and M2 Series modules support exception SPAN only in the nonadministration VDC, and at least one interface of the module must be present for the VDC.
- For MTU truncation on M2 Series modules, the truncated length of SPAN packets is rounded down to the nearest multiplier of 16 bytes. For example, with an MTU configuration value of 65 to 79, packets are truncated to 64 bytes.

- Only eight sessions can support rate limiting on M2 Series modules. Any additional hardware sessions will not apply the configured rate limiter on M2 Series modules.
- M1 and M2 Series modules support exception SPAN only in the nonadministration VDC, and at least one interface of the module must be present for the VDC.

Guidelines and Limitations for M3 Series Modules

- Beginning with Cisco NX-OS Release 7.3(1)DX(1), SPAN is supported on M3 Series modules.
- SPAN sampling is supported on M Series modules and Supervisor 2.
- Extended SPAN sessions support traffic from M3 Series modules.
- If a monitor session has a source with both VLAN and a physical port, traffic may span on ports which may not be a part of the monitor session. This is applicable when M3-series I/O modules are used.

Default Settings for SPAN

The following table lists the default settings for SPAN parameters.

Parameters	Default
SPAN sessions	Created in the shut state
MTU truncation	Disabled
Multicast best effort mode	Disabled
SPAN rate limit for traditional SPAN sessions	Disabled
SPAN rate limit for extended SPAN sessions	Enabled
SPAN sampling	Disabled

Configuring SPAN

Note 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.

For sources, you can specify Ethernet ports, port channels, the supervisor inband interface, and VLANs (ingress only).

A single SPAN session can include mixed sources in any combination of Ethernet ports, VLANs, or the inband interface to the control plane CPU. You cannot specify Ethernet port subinterfaces as sources for a SPAN session.

Note

- To use a Layer 3 port-channel subinterface as a SPAN source in the monitor session, you must specify the VLAN ID that you entered when configuring IEEE 802.1Q VLAN encapsulation for the subinterface as the filter VLAN. When you use the main interface and the SPAN VLAN filter to filter the 802.1Q VLANs on the subinterfaces, SPAN shows the traffic for all subinterfaces on the SPAN destination port.
- When VLANs containing trunk members are configured as SPAN sources, and another set of VLANs are configured as SPAN VLAN filters, then the unwanted traffic from those filter VLANs can be potentially captured.

When you specify the supervisor inband interface for a SPAN source, the device monitors all packets that arrive on the supervisor hardware (ingress).

For destination ports, you can specify Ethernet ports or port channels in either access or trunk mode. You must enable monitor mode on all destination ports.

For bidirectional traditional sessions, you can configure the sessions without specifying the direction of the traffic.

For extended SPAN sessions, you can configure the sessions in one of the following ways:

- Configure a bidirectional session by not specifying any direction when you create the session and changing the mode to extended by entering the **mode extended** command.
- Configure a unidirectional session by specifying the traffic direction when you create the session.

Before you begin

Make sure you are in the correct VDC. To switch VDCs, use the switchto vdc command.

You must have already configured the destination ports in access or trunk mode. For more information, see the *Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide*.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface ethernet** *interface slot*/*port*]
	Example:
	`switch(config)# interface ethernet 2/5`
	`switch(config-if)#`
		Enters interface configuration mode on the selected slot and port.

	Command or Action	Purpose

Step 3	**switchport**
	Example:
	`switch(config-if)# switchport`
	`switch(config-if)#`
		Configures switchport parameters for the selected slot and port or range of ports.

Step 4	**switchport mode** [**access** | **trunk** | **private-vlan**]
	Example:
	`switch(config-if)# switchport mode trunk`
	`switch(config-if)#`
		Configures switchport parameters for the selected slot and port or range of ports.
		• access
		• trunk
		• private-vlan

Step 5	**switchport monitor** [**ingress** [**learning**]] **Example:** `switch(config-if)# switchport monitor`	Configures the switchport interface as a SPAN destination: • **ingress**— Allows the SPAN destination port to inject packets that disrupt a certain TCP packet stream, for example, in networks with IDS. • **ingress learning**— Allows the SPAN destination port to inject packets, and allows the learning of MAC addresses, for example, the IDS MAC address.
Step 6	(Optional) Repeat Steps 2 and 3 to configure monitoring on additional SPAN destinations	—
Step 7	**no monitor session** *session-number* **Example:** `switch(config)# no monitor session 3`	Clears the configuration of the specified SPAN session. The new session configuration is added to the existing session configuration.

Step 8	**monitor session** *session-number* [**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)#`
		Clears the configuration of the specified SPAN session. The new session configuration is added to the existing session configuration.
		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 keywords are as follows:
		• rx—Specifies an ingress extended SPAN session.

	Command or Action	Purpose
		• tx—Specifies an egress extended SPAN session. • shut—Specifies a shut state for the selected session.
Step 9	**mode extended** **Example:** `switch(config-monitor)# mode extended`	(Optional) Configures the SPAN session as an extended bidirectional session. **Note** You cannot use this command for a unidirectional SPAN session.
Step 10	**description***description* **Example:** `switch(config-monitor)# description my_span_session_3`	Configures a description for the session. By default, no description is defined. The description can be up to 32 alphanumeric characters.

Step 11	**source** {**interface** {**all** | *type*} | **vlan** {*number* | *range*}} [**rx** | **tx** | **both**]
	Example:
	`switch(config-monitor)# source interface ethernet 2/1-3, ethernet 3/1 rx`
	Example:
	`switch(config-monitor)# source interface port-channel 2`
	Example:
	`switch(config-monitor)# source interface sup-eth 0 both`
	Example:
	`switch(config-monitor)# source vlan 3, 6-8 rx`
	Example:
	`switch(config-monitor)# source interface ethernet 101/1/1-3`
	Example:
	`switch(config-monitor)# source interface all rx`
		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, a Cisco Nexus 2000 Series Fabric Extender interface, or a fabric port channel connected to a Cisco Nexus 2000 Series Fabric Extender.
		You can configure one or more sources, as either a series of comma-separated entries or a range of numbers. You can specify up to 128 interfaces. The VLAN range is from 1 to 3967. The VLAN range of 4048 to 4093 is also supported for Cisco NX-OS releases prior to 6.1.
		You can specify the traffic direction to copy as ingress (rx), egress (tx), or both. By default, the direction is both. For a unidirectional session, the direction of the source must match the direction specified in the session. Beginning with Cisco NX-OS Release 7.3(0)D1(1), you can use the **all** keyword to enable the monitor session to monitor all VLANs and ports in the VDC such as physical ports, Port Channels, FEX ports and FEX Port Channels. The **all** keyword is supported only in Extended SPAN sessions.

Step 12	(Optional) Repeat Step 11 to configure all SPAN sources.	—
Step 13	(Optional) **filter vlan** {*number* | *range*} [**include-untagged**]	(Optional) Configures which VLANs to select from the configured sources. You can

	Command or Action	Purpose
	Example: `switch(config-monitor)# filter vlan 3-5, 7`	configure one or more VLANs, as either a series of comma-separated entries, or a range of numbers. The VLAN range is from 1 to 3967. The VLAN range of 4048 to 4093 is also supported for Cisco NX-OS releases prior to 6.1. The include-untagged keyword applies a VLAN access map to one or more VLANs and includes untagged frames on a port with Layer 3 subinterfaces. You can enable monitoring of a higher number of specific VLAN sources than the VLAN source limits currently supported in extended SPAN monitor session by using the **filter vlan** command with the **source interface all** command to filter the irrelevant VLANs.
Step 14	(Optional) Repeat Step 13 to configure all source VLANs to filter.	—
Step 15	Required: **destination interface** *type* {*number* | *range*} **Example:** `switch(config-monitor)# destination interface ethernet 2/5, ethernet 3/7`	Configures destinations for copied source packets. You can configure one or more destinations as either a series of comma-separated entries or a range of numbers. You can specify up to 128 interfaces. **Note** SPAN destination ports must be either access or trunk ports. **Note** The Cisco Nexus 2000 Series Fabric Extender interfaces and the fabric port channels connected to the Cisco Nexus 2000 Series Fabric Extender cannot be configured as SPAN destinations.
Step 16	(Optional) Repeat Step 15 to configure all SPAN destination ports.	—
Step 17	Required: **no shut** **Example:** `switch(config-monitor)# no shut`	Enables the SPAN session. By default, the session is created in the shut state.
Step 18	(Optional) **show monitor session** {**all** | *session-number* | **range** *session-range*} [**brief**] **Example:** `switch(config-monitor)# show monitor session 3`	Displays the SPAN configuration.

	Command or Action	Purpose
Step 19	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring Multi-Destination SPAN on F2 Series Modules

If you are configuring a multiple destination port for a SPAN session on a Cisco Nexus 7000 switch, do the following:

- Remove the module type restriction when configuring multiple SPAN destination port to allow a SPAN session.
- Designate a primary destination port for VDCs with any Fx module or supervisor to activate a SPAN session.

Note The primary destination configuration does not impact transmission of SPAN packets originating from the M-series module; the primary destination has be active for the SPAN session to be activated.

For sources, you can specify ports, VLANs, or RSPAN VLANs.

Before you begin

Multiple destination SPAN sessions were not supported in VDCs with F–series modules (F1/F2/F2E/F3), and hence even if the sessions were configured, they were not enabled in the VDCs. Starting from Cisco NX-OS Release 7.2, multiple destination SPAN sessions are supported. The primary destination is used to transmit SPAN packets originated from Fx modules.

BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switch to vdc** command).

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**no monitor session** *session-number* **Example:** `switch(config)# no monitor session 3`	Clears the configuration of the specified SPAN session. The new session configuration is added to the existing session configuration.

	Command or Action	Purpose

Step 3	**monitor session** *session-number*
	Example:
	`switch(config)# monitor session 4 rx`
	`switch(config-monitor)#`
	Example:
	`switch(config)# monitor session 3 tx`
	`switch(config-monitor)#`
		Enters the monitor configuration mode. The new session configuration is added to the existing session configuration, which specifies the SPAN session for which the source rate limit is to be configured. By default, the session is created in the shut state, and the session is a local SPAN session.

Step 4	**source** {**interface** *type* | **vlan** {*number* | *range*}} [**rx** | **tx** | **both**] **Example:** `switch(config-monitor)# source interface ethernet 2/1-3, ethernet 3/1 rx`	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, or a range of VLANs. You can configure one or more sources, as either a series of comma-separated entries or a range of numbers. You can specify up to 128 interfaces. You can specify the traffic direction to copy as ingress (rx), egress (tx), or both. By default, the direction is both. **Note** Source VLANs are supported only in the ingress (rx) direction.
Step 5	(Optional) Repeat Step 4 to configure all virtual SPAN VLAN sources.	—
Step 6	Required: **destination interface** *type* {*number* | *range*} [primary] **Example:** `switch(config-monitor)# destination interface ethernet 2/5, ethernet 3/7 primary`	Configures destinations for copied source packets. You can configure one or more destinations as either a series of comma-separated entries or a range of numbers. However, only one such primary port can be configured in a session. You can specify up to 128 interfaces. **Note** SPAN destination ports must be either access or trunk ports.
Step 7	Required: **no rate-limit** **Example:** `switch(config-monitor)# no rate limit`	Sets the rate limit for the SPAN traffic.
Step 8	Required: **no destination interface** *type* {*number* | *range*} [primary] **Example:** `switch(config-monitor)# destination interface ethernet 2/5, ethernet 3/7 primary`	Checks the configuration to ensure that the primary attribute is not configured on the destination port. Displays an error message if more than one port is configured. **Note** ERROR: Cannot configure more than one "Primary" destination port in a session.

	Command or Action	Purpose
Step 9	(Optional) Repeat Step 12 to configure all source VLANs to filter.	—
Step 10	Required: **no shut** **Example:** `switch(config-monitor)# no shut`	Enables the SPAN session. By default, the session is created in the shut state.
Step 11	(Optional) **show monitor session** {**all** | *session-number* | **range** *session-range*} [**brief**] **Example:** `switch(config-monitor)# show monitor session 3`	Displays the SPAN configuration.
Step 12	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring Multiple SPAN Sessions on a SPAN Destination Port

BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switch to vdc** command).

Before you begin

With the introduction of multiple SPAN sessions, it is important to share the destination interface across multiple SPAN sessions, which not only reduce the N7K hardware cost of the SPAN sessions and the traffic monitoring equipment, it can also simplify the overall network connections.

- Rate limiter 'auto' mode is not allowed with span session(s) having shared span destination port(s).
- The 'manual' mode is recommended when the rate limit is required for individual SPAN session.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**monitor session** *session-number*[*session-type*]
	Example:
	`switch(config)# monitor session 3 span`
	`switch(config-monitor)#`
		Enters the monitor configuration mode and specifies a SPAN session.

	Command or Action	Purpose
Step 3	Required: **destination interface** {**ethernet x/y** | **port-channel z**} **Example:** `switch(config-monitor)# destination interface ethernet1/2`	(Optional) Specifies the option to add a destination port. **Note** Rate limit auto should be disabled for sharing SPAN destination ports across multiple sessions. However, if the rate limit auto is enabled for a destination port and the destination port is already used in any other SPAN session, there will be a request to disable the auto mode first.
Step 4	Required: **no rate-limit** {**auto** | **rate-value**} **Example:** `switch(config-monitor-local)# no rate-limit auto`	(Optional) Enables the rate limit. **Note** Auto rate limit should be disabled for sharing SPAN destination ports across multiple sessions. If a shared destination port is configured in the span session, the CLI gets rejected until you remove the shared destination port.

Configuring a Virtual SPAN Session

You can configure a virtual SPAN session to copy packets from source ports, VLANs, and RSPAN VLANs to destination ports on the local device. By default, SPAN sessions are created in the shut state.

For sources, you can specify ports, VLANs, or RSPAN VLANs.

Before you begin

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

You have already configured the destination ports in trunk mode. For more information, see the Cisco

Nexus 7000 Series NX-OS Interfaces Configuration Guide.

You have already configured the destination ports to monitor a SPAN session with the **switchport monitor** command.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal switch(config)#`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**no monitor session** *session-number* **Example:** `switch(config)# no monitor session 3`	Clears the configuration of the specified SPAN session. The new session configuration is added to the existing session configuration.

Step 3	**monitor session** *session-number*
	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)#`
		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.

Step 4	**source** {**interface** *type* | **vlan** {*number* | *range*}} [**rx** | **tx** | **both**]
	Example:
	`switch(config-monitor)# source interface ethernet 2/1-3, ethernet 3/1 rx`
	Example:
	`switch(config-monitor)# source interface port-channel 2`
	Example:
	`switch(config-monitor)# source interface sup-eth 0 both`
	Example:
	`switch(config-monitor)# source vlan 3, 6-8 rx`
	Example:
	`switch(config-monitor)# source interface ethernet 101/1/1-3`
		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, or a range of VLANs.
		You can configure one or more sources, as either a series of comma-separated entries or a range of numbers. You can specify up to 128 interfaces.
		You can specify the traffic direction to copy as ingress (rx), egress (tx), or both. By default, the direction is both.
		Note Source VLANs are supported only in the ingress (rx) direction.
		For a unidirectional session, the direction of the source must match the direction specified in the session.

Step 5	(Optional) Repeat Step 4 to configure all virtual SPAN VLAN sources.	—
Step 6	Required: **destination interface** *type* {*number* | *range*} **Example:** `switch(config-monitor)# destination interface ethernet 2/5, ethernet 3/7`	Configures destinations for copied source packets. You can configure one or more destinations as either a series of comma-separated entries or a range of numbers. You can specify up to 128 interfaces. **Note** SPAN destination ports must be either access or trunk ports.
Step 7	(Optional) Repeat Step 12 to configure all source VLANs to filter.	—

	Command or Action	Purpose
Step 8	Required: **no shut** **Example:** `switch(config-monitor)# no shut`	Enables the SPAN session. By default, the session is created in the shut state.
Step 9	(Optional) **show monitor session** {**all** | *session-number* | **range** *session-range*} [**brief**] **Example:** `switch(config-monitor)# show monitor session 3`	Displays the SPAN configuration.
Step 10	Required: **interface ethernet** *slot/port [port]* **Example:** `switch(config)# interface ethernet 2/5 switch(config-if)#`	Enters interface configuration mode on the selected slot and port or range of ports.
Step 11	(Optional) **switchport trunk allowed vlan** {**all** | *session-number* | **range** *session-range*} [**brief**] **Example:** `switch(config-monitor)# show monitor session 3`	Configures the range of VLANs that are allowed on the interface. You can add to or remove from the existing VLANs, you can select all VLANs except those VLANs that you specify, or you can select all or none of the VLANs. By default, all VLANs are allowed on the interface. You can configure one or more VLANs as either a series of comma-separated entries or a range of numbers. The VLAN range is from 1 to 3967. The VLAN range of 4048 to 4093 is also supported for Cisco NX-OS releases prior to 6.1.
Step 12	(Optional) Repeat Steps 10 and 11 to configure the allowed VLANs on each destination port.	
Step 13	(Optional) **show interface ethernet** **Example:** `switch(config)# interface ethernet 2/5 switch(config-if)#`	(Optional) Displays the interface trunking configuration for the selected slot and port or range of ports.
Step 14	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring an RSPAN VLAN

You can specify a remote SPAN (RSPAN) VLAN as a SPAN session source.

Before you begin

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**vlan** *vlan*
	Example:
	`switch(config)# vlan 901`
	`switch(config-vlan)#`
		Enters VLAN configuration mode for the VLAN specified.

Step 3	**remote-span** **Example:** `switch(config-vlan)# remote-span`	Configures the VLAN as an RSPAN VLAN.

Step 4	**exit**
	Example:
	`switch(config-vlan)# exit`
	`switch(config)#`
		Exits VLAN configuration mode.

Step 5	(Optional) **show vlan** **Example:** `switch(config)# show vlan`	(Optional) Displays the VLAN configuration. Remote SPAN VLANs are listed together.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

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

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **monitor session** {*session-range* | **all**} **shut** **Example:** `switch(config)# monitor session 3 shut`	Shuts down the specified SPAN sessions. By default, sessions are created in the shut state. The **no** form of the command resumes (enables) the specified SPAN sessions. By default, sessions are created in the shut state. **Note** If a monitor session is enabled but its operational status is down, to enable the session, you must first specify the **monitor session shut** command followed by the **no monitor session shut** command.

Step 3	**monitor session** *session-number*
	Example:
	`switch(config)# monitor session 3`
	`switch(config-monitor)#`
		Enters the monitor configuration mode. The new session configuration is added to the existing session configuration.

Step 4	[**no**] **shut** **Example:** `switch(config-monitor)# shut`	Shuts down the SPAN session. By default, the session is created in the shut state. The **no** form of the command enables the SPAN session. By default, the session is created in the shut state.
Step 5	(Optional) **show monitor** **Example:** `switch(config-monitor)# show monitor`	Displays the status of SPAN sessions.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring MTU Truncation for Each SPAN Session

To reduce the SPAN traffic bandwidth, you can configure the maximum bytes allowed for each replicated packet in a SPAN session. This value is called the maximum transmission unit (MTU) truncation size. Any SPAN packet larger than the configured size is truncated to the configured size.

Note MTU truncation and the SPAN rate limit cannot be enabled for the same SPAN session on F1 Series modules. If you configure both for one session, only the rate limit is allowed on F1 Series modules, and MTU truncation is disabled until you disable the rate limit configuration. This limitation does not apply to F2 and M2 Series modules or Supervisor 2.

Note MTU truncation and SPAN sampling can be enabled at the same time and have no precedence over each other because they are applied to different aspects of the source packet (size versus packet count).

Before you begin

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**monitor session** *session-number*
	Example:
	`switch(config)# monitor session 3`
	`switch(config-monitor)#`
		Enters the monitor configuration mode and specifies the SPAN session for which the MTU truncation size is to be configured.

Step 3	Required: **[no] mtu***mtu* **Example:** `switch(config-monitor)# mtu 64`	Configures the MTU truncation size for packets in the specified SPAN session. The range is from 64 to 1500 bytes.

Step 4	**show monitor session** *session-number*
	Example:
	`switch(config)# monitor session 3`
	`switch(config-monitor)#`
		(Optional) Displays the status of SPAN sessions, including the configuration status of MTU truncation, the maximum bytes allowed for each packet per session, and the modules on which MTU truncation is and is not supported.

Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring a Source Rate Limit for Each SPAN Session

When a SPAN session is configured with multiple interfaces or VLANs as the sources in a high-traffic environment, the destination port can be overloaded, causing the normal data traffic to be disrupted at the source port. You can alleviate this problem as well as traffic overload on the source forwarding instance by configuring a source rate limit for each SPAN session.

Note MTU truncation and the SPAN rate limit cannot be enabled for the same SPAN session on F1 Series modules. If you configure both for one session, only the rate limit is allowed on F1 Series modules, and MTU truncation is disabled until you disable the rate limit configuration. This limitation does not apply to F2 and M2 Series modules or Supervisor 2.

Note SPAN sampling takes precedence over SPAN source rate limiting. Rate limiting takes effect after sampling is completed on SPAN source packets.

Before you begin

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**monitor session** *session-number*
	Example:
	`switch(config)# monitor session 3`
	`switch(config-monitor)#`
		Enters the monitor configuration mode and specifies the SPAN session for which the source rate limit is to be configured.

Step 3	Required: **[no] rate-limit {auto** | *rate-limit*} **Example:** `switch(config-monitor)# rate-limit auto`	Configures the source rate limit for SPAN packets in the specified SPAN session in automatic or manual: • Auto mode—Automatically calculates the rate limit on a per-gigabyte basis as follows: destination bandwidth / aggregate source bandwidth. For example, if the rate limit per gigabyte is 0.5, for every 1G of source traffic, only 0.5G of packets are spanned. For ingress traffic, the per-gigabyte limit is applied to each forwarding engine of the F Series module based on how many ports

	Command or Action	Purpose
		are used as the SPAN source so that the source can be spanned at the maximum available bandwidth. For egress traffic, the per-gigabyte limit is applied to each forwarding engine of the F Series module without considering how many ports are used as the SPAN source. • Manual mode—Specifies the percentage of the maximum rate of SPAN packets that can be sent out from each forwarding engine on a module. The range is from 1 to 100. For example, if the rate limit is 10 percent, the maximum rate of SPAN packets that can be sent out from each of the forwarding engines on an F Series module is 1G (or 10 percent of the 10G line rate).

Step 4	**show monitor session** *session-number*
	Example:
	`switch(config)# monitor session 3`
	`switch(config-monitor)#`
		(Optional) Displays the status of SPAN sessions, including the configuration status of the rate limit, the percentage of the maximum SPAN rate allowed per session, and the modules on which the rate limit is and is not supported.

Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring Sampling for Each SPAN Session

Beginning with Cisco NX-OS Release 6.1, you can configure a sampling range for spanned traffic in order to reduce the SPAN traffic bandwidth and to monitor peer-to-peer traffic. Packet range-based sampling is used to provide an accurate count of the SPAN source packets.

Note Sampling and MTU truncation can be enabled at the same time and have no precedence over each other because they are applied to different aspects of the source packet (packet count versus size). However, sampling takes precedence over SPAN source rate limiting. Rate limiting takes effect after sampling is completed on SPAN source packets.

Before you begin

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**monitor session** *session-number*
	Example:
	`switch(config)# monitor session 3`
	`switch(config-monitor)#`	

Step 3	**monitor session** *session-number* [*rt* | *tx*] [*shut*] **Example:** `switch(config-monitor)# sampling 100`	Configures the sampling range for SPAN source packets. The sampling value is the range in which one packet out of x packets will be spanned, where x is from 2 to 1023. In this example, 1 out of every 100 packets will be spanned.
Step 4	(Optional) **show monitor session** {**all** | *session-number* | **range** *session-range*} [**brief**] **Example:** `switch(config-monitor)# show monitor session 3`	Displays the status of SPAN sessions, including the configuration status of SPAN sampling, the sampling value, and the modules on which sampling is and is not supported.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Complex Rule-based SPAN

Before you begin

Complex filter rules can be created with multiple filters and product table resources. A few keywords, **Match**, **Permit**, **Deny** and **Filter-list** have been introduced in this release. The "Match" keyword helps to match on the fields and values set by the user. "Permit" keyword followed by the filter names allow a SPAN copy to be generated if all filters are hit. "Deny" keyword followed by the filter names allow a SPAN copy to be generated if all the filters are missed. "Filter-list" is a keyword that specifies all the rules defined by the permit and deny keywords.

Note Each filter list can contain multiple 'permit-deny' rules.

Creating Filters

BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**monitor filter***filter-name*
	Example:
	`switch(config)# monitor filter test-filter`
	`switch(config-monitor-filter)#`
		Enters the monitor filter configuration mode.
		Note The length of the string should not exceed 32 characters.

Step 3	**match** [**eth-type** *eth-type* | **src-mac** *mac-address mac-mask* | **dest-mac** *mac-address mac-mask* | **frame-type** *[arp | eth | fcoe |ipv4 |ipv6*]
	Example:
	`switch(config-monitor-filter)# match eth-type 0x0800`
	`switch(config-monitor-filter)# match src-mac 40:55:39:0c:98:c1 ff:ff:ff:ff:ff:00 dest-mac 40:55:39:0c:98:c1 ff:ff:ff:ff:ff:00`
		Match specific fields in the packet under monitor filter configuration mode.
		Note Specifying match criteria in the same line or in multiple lines will have the same result.

Creating Filter-Lists

BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**monitor filter-list***filter-list-name*
	Example:
	`switch(config)# monitor filter-list sample-filter-list`
	`switch(config-monitor-filter-list)#`
		Enters the monitor filter configuration mode.
		Note The length of the string should not exceed 32 characters.

	Command or Action	Purpose

Step 3	**permit filter** *filter-names* **deny filter***filter-names*
	Example:
	`switch(config-monitor-filter-list)# permit filter test-filter deny filter test-filter1`
	`switch(config-monitor-filter-list)#`
	`switch(config-monitor-filter-list)# permit filter test-filter2`
	`switch(config-monitor-filter-list)#`
	`switch(config-monitor-filter-list)# deny filter test-filter3`
	`switch(config-monitor-filter-list)#`
		Use this command to permit and/or deny filters within the filter-list.
		Note
		• When the command **permit filter** *filter-names* **deny filter***filter-names* is specified in the same line, the rule matches all permit and deny criteria, where packets matching filter x and filter y in permit filter X and deny filter Y are SPAN-ed—this is an AND condition.
		• When the command **permit filter** *filter-names* **deny filter***filter-names* is specified in separate lines, the rule matches either permit or deny criteria, where packets match filter x OR filter y in permit filter X and deny filter Y are SPAN-ed—it is an OR condition.

Associating a Filter List to a Monitor Session

BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Note If you want to attach a complex filter to a SPAN session, ensure that there are no filters already attached to the SPAN session.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

	Command or Action	Purpose

Step 2	**monitor session** *session-number* [*rt* | *tx*]
	Example:
	`switch(config)# monitor session 3 rx`
	`switch(config-monitor)# filter filter-list sample-filter-list`
		Enters the monitor configuration mode and specifies the SPAN session. The optional keywords are as follows:
		• rx—Specifies an ingress extended SPAN session.
		• tx—Specifies an egress extended SPAN session.
		Note • If you are attaching a filter-list to a SPAN session on a Cisco Nexus 7000 series switch, then the **mode extended** command should be specified within the SPAN session.
		• The direction of the filter is derived from the SPAN session direction.

Step 3	**exit** **Example:** `switch(config-monitor)# exit`	Returns to the global configuration mode.

Configuring a Session with Rules Enabled

To create a local/erspan-source unidirectional/bidirectional session, configure the following:

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**monitor session** *session-number* [*rt* | *tx*] [*shut*]
	Example:
	`switch(config)# monitor session 3 rx`
	`switch(config-monitor)#`
		Enters the monitor configuration mode to configure a local SPAN/ERSPAN session. The optional keywords are as follows:
		• rx—Specifies an ingress extended SPAN session.
		• tx—Specifies an egress extended SPAN session.
		• shut—Specifies a shut state for the selected session.

	Command or Action	Purpose
Step 3	**mode extended** **Example:** `switch(config-monitor)# mode extended`	(Optional) Changes mode to extended mode for bidirectional sessions.
Step 4	**filter frame-type source-ip src-ip** **Example:** `switch(config-monitor)# filter frame-type ipv4 src-ip 10.1.1.3/32 cos 3`	Associates the rule-based filters to the session.

Step 5	Required: **source interface ethernet x/y**
	Example:
	`switch(conf-monitor)# source interface Ethernet 4/7`
	`switch(conf-monitor)# destination interface Ethernet 4/7`
		Associates the source port and the destination port.

Step 6	Required: **no shut** **Example:** `switch(config-monitor)# no shut`	Brings up the session. **Note** Filter command can be split into separate lines and configured under the session mode. All the filters specified under a session will be under the AND rule.

Configuring the Multicast Best Effort Mode for a SPAN Session

You can configure the multicast best effort mode for any SPAN session. By default, SPAN replication occurs on both the ingress and egress modules. When you enable the multicast best effort mode, SPAN replication occurs only on the ingress module for multicast traffic or on the egress module for packets that egress out of Layer 3 interfaces (that is, on the egress module, packets that egress out of Layer 2 interfaces are not replicated for SPAN).

Note For Layer 3 multicast traffic, SPAN replication occurs on the egress module. If traffic is multicasted to multiple egress modules, you could capture multiple SPAN copies for each packet (that is, one copy from each egress module).

Before you begin

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`switch# configure terminal` `switch(config)#`	

Step 2	**monitor session** *session-number*
	Example:
	`switch(config)# monitor session 3`
	`switch(config-monitor)#`
		Enters the monitor configuration mode and specifies the SPAN session for which the source rate limit is to be configured.

Step 3	Required: **[no] multicast best-effort** **Example:** `switch(config-monitor)# multicast best-effort`	Configures the multicast best effort mode for the specified SPAN session.

Step 4	**show monitor session** *session-number*
	Example:
	`switch(config)# monitor session 3`
	`switch(config-monitor)#`
		(Optional) Displays the status of SPAN sessions, including the configuration status of the rate limit, the percentage of the maximum SPAN rate allowed per session, and the modules on which the rate limit is and is not supported.

Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring Rule-Based SPAN

You can configure filters for ingress or egress SPAN traffic based on a set of rules. A simple filter has only one rule, and multiple fields or conditions can be added to this rule. The packets are spanned only if all conditions are met.

Before you begin

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**monitor session** *session-number* [**shut**]
	Example:
	`switch(config)# monitor session 3`
	`switch(config-monitor)#`
		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 keywords are as follows:

	Command or Action	Purpose
		• **rx**—Specifies an ingress extended SPAN session. • **tx**—Specifies an egress extended SPAN session. • **shut**—Specifies a shut state for the selected session.
Step 3	**mode extended** **Example:** `switch(config-monitor)# mode extended`	(Optional) Configures the SPAN session as an extended bidirectional session.

Step 4	[**no**] **filter**[*vlan-range*] [**bpdu** [**true** | **false**]] [**cos** *cos-value*] [**dest-mac***dest-mac*] [**eth-type** *eth-value*] [**flow-hash** *flow-value*] [**frame-type** [**eth** | **arp** | **fcoe** | **ipv4** | **ipv6**]] [**pc-lane** *port-number*] [**src_mac** *mac-address*] [**trace-route** [**true** | **false**]]
	Example:
	`switch(config-monitor)# filter vlan 10,20`
	`switch(config-monitor)# filter frame-type arp trace-route true`
	`switch(config-monitor)# filter bpdu false`
		Configures the filter for the SPAN session. To remove the filter from the session, enter the **no** form of the command. The optional keywords are as follows:
		• **vlan**—Specifies a filter based on a VLAN range.
		• **bpdu**—Specifies a filter based on the bridge protocol data unit (BPDU) class of packets.
		• **cos**—Specifies a filter based on the class of service (CoS) in the dotlq header.
		• **dest-mac**—Specifies a filter based on a destination MAC address.
		• **eth-type**—Specifies a filter based on the Ethernet type.
		• **flow-hash**—Specifies a filter based on the result bundle hash (RBH) value.
		• **frame-type**—Specifies a filter based on a frame type.
		• **pc-lane**—Specifies a filter based on a member of the port channel.
		• **src-mac**—Specifies a filter based on a source MAC address.
		• **trace-route**—Specifies a filter based on the route bit in the header.

Step 5	(Optional) [**no**]**filter frame-type eth** **Example:**	(Optional) Configures the Ethernet frame type filter for the SPAN session. To remove the filter from the session, enter the **no** form of the command.

	Command or Action	Purpose
	`switch(config-monitor)# filter frame-type eth`	
Step 6	(Optional) [**no**]**filter frame-type arp** [[**arp-rarp** [**arp** | **rarp**]] [**req-resp** [**req** | **rsp**]] [**sender-ip** *ip-address*] [**target-ip** *ip-address*]] **Example:** `switch(config-monitor)# filter frame-type arp arp-rarp arp`	(Optional) Configures the ARP frame type filter for the SPAN session. To remove the filter from the session, enter the **no** form of the command. The optional keywords are as follows: • **arp-rarp**—Specifies an ARP or RARP frame type filter. • **req-resp**—Specifies a filter based on a request or response. • **sender-ip**—Specifies a filter based on a sender IP address. • **target-ip**—Specifies a filter based on a target IP address.
Step 7	(Optional) [**no**]**filter frame-type fcoe fcoe** [[**fc-sid** *FC-source-ID*] [**fc-did** *FC-dest-ID*] [**fcoe-type** *fcoe-value*] [**r-ctl** *r-ctl-value*] [**sof** *sof-value*] [**cmd-code** *cmd-value*]] **Example:** `switch(config-monitor)# filter frame-type fcoe`	(Optional) Configures the FCoE frame type filter for the SPAN session. To remove the filter from the session, enter the **no** form of the command. The optional keywords are as follows: • **fc-sid**—Specifies a filter based on an FC source ID. • **fc-did**—Specifies a filter based on an FC destination ID. • **fcoe-type**—Specifies a filter based on an FCoE type. • **r-ctl**—Specifies a filter based on the routing control flags (R CTL) value. • **sof**—Specifies a filter based on the start of frame (SOF) packets. • **cmd-code**—Specifies a filter based on a command code.
Step 8	(Optional) [**no**]**filter frame-type ipv4** [[**src-ip** *src-ip*] [**dest-ip** *dest-ip*] [**tos** tos-value] [**l4-protocol** *l4-value*]] **Example:** `switch(config-monitor)# filter frame-type ipv4 l4-protocol 3`	(Optional) Configures the IPv4 frame type filter for the SPAN session. To remove the filter from the session, enter the no form of the command. The optional keywords are as follows: • **src-ip**—Specifies a filter based on an IPv4 source IP address.

	Command or Action	Purpose
		• **dest-ip**—Specifies a filter based on an IPv4 destination IP address. • **tos**—Specifies a filter based on the type of service (TOS) in the IP header. • **l4-protocol**—Specifies a filter based on a Layer 4 protocol number set in the protocol field of the IP header.
Step 9	(Optional) [**no**]**filter frame-type ipv6** [[**src-ip** *src-ip*] [**dest-ip** *dest-ip*] [**tos** tos-value] [**l4-protocol** *l4-value*]] **Example:** `switch(config-monitor)# filter frame-type ipv6 src-ip 10.0.0.1`	(Optional) Configures the IPv6 frame type filter for the SPAN session. To remove the filter from the session, enter the no form of the command. The optional keywords are as follows: • **src-ip**—Specifies a filter based on an IPv6 source IP address. • **dest-ip**—Specifies a filter based on an IPv4 destination IP address. • **tos**—Specifies a filter based on the type of service (TOS) in the IP header. • **l4-protocol**—Specifies a filter based on a Layer 4 protocol number set in the protocol field of the IP header.
Step 10	(Optional) Repeat Steps 4 to 9 for all filters for the session.	
Step 11	**source** {**interface** *type* | **vlan** {*number* | *range*}} [**rx** | **tx** | **both**] **Example:** `switch# configure terminal switch(config)#`	(Optional) 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, a Cisco Nexus 2000 Series Fabric Extender interface, or a fabric port channel connected to a Cisco Nexus 2000 Series Fabric Extender can configure one or more sources, as either a series of comma-separated entries or a range of numbers. You can specify up to 128 interfaces. The VLAN range is from 1 to 3967. The VLAN range of 4048 to 4093 is also supported for Cisco NX-OS releases prior to 6.1. You can specify the traffic direction to copy as ingress (rx), egress (tx), or both. By default, the direction is both.

	Command or Action	Purpose
		For a unidirectional session, the direction of the source must match the direction specified in the session.
Step 12	**destination interface** *type* {*number* | *range*} **Example:** `switch(config-monitor)# destination interface ethernet 2/5, ethernet 3/7`	Configures destinations for copied source packets. You can configure one or more destinations as either a series of comma-separated entries or a range of numbers. You can specify up to 128 interfaces. **Note** SPAN destination ports must be either access or trunk ports. **Note** The Cisco Nexus 2000 Series Fabric Extender interfaces and the fabric port channels connected to the FEX cannot be configured as SPAN destinations.
Step 13	**no shut** **Example:** `switch(config-monitor)# no shut`	Enables the SPAN session. By default, the session is created in the shut state.
Step 14	(Optional) **show monitor session** {**all** | *session-number* | **range** *session-range*} [**brief**] **Example:** `switch(config-monitor)# show monitor session 3`	Displays the SPAN configuration.
Step 15	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring Exception SPAN

You can configure the device to span exception packets.

Before you begin

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**monitor session** *session-number* [**rx**|**tx**| **both**]
	Example:
	`switch(config)# monitor session 3`
	`switch(config-monitor)#`
		Enters the monitor configuration mode and specifies the SPAN session. The optional keywords are as follows:.
		• **rx**—Specifies an ingress extended SPAN session.
		• **tx**—Specifies an egress extended SPAN session.
		• **shut**—Specifies a shut state for the selected session.

Step 3	(Optional) **mode extended** **Example:** `switch(config-monitor)# mode extended`	(Optional) Configures the SPAN session as an extended bidirectional session form of the command.
Step 4	(Optional) [**source exception**{**layer3**|**fabricpath**|**other** | **all**} **Example:** `switch(config-monitor)# filter frame-type eth`	Configures the source as an exception SPAN session. These exception types are supported: • **layer3**—Specifies the Layer 3 exception type. • **fabricpath**—Specifies the FabricPath exception type. • **other**—Specifies other exceptions that are dropped through redirect registers programmed with a drop destination interface. • **all**—Includes all Layer 3, FabricPath, and other exceptions.
Step 5	**destination interface** *type [number |range}* **Example:** `switch(config-monitor)# destination interface ethernet 2/5, ethernet 3/7`	Configures destinations for copied source packets. You can configure one or more destinations as either a series of comma-separated entries or a range of numbers. You can specify up to 128 interfaces. **Note** SPAN destination ports must be either access or trunk ports.

	Command or Action	Purpose
		Note The Cisco Nexus 2000 Series Fabric Extender interfaces and the fabric port channels connected to the FEX cannot be configured as SPAN destinations.
Step 6	**no shut** **Example:** `switch(config)# no shut`	Enables the SPAN session. By default, the session is created in the shut state.
Step 7	**show monitor session** *session-number* **Example:** `switch(config)# show monitor session 3`	(Optional) Displays the status of SPAN sessions, including the configuration status of the rate limit, the percentage of the maximum SPAN rate allowed per session, and the modules on which the rate limit is and is not supported.
Step 8	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Removing FabricPath and VNTAG Headers

If you are working with a device connected to a SPAN destination port that does not understand FabricPath or VNTAG headers, you may want those headers stripped from the packet.

You can do this at either the global or port level. If you want to strip the headers to all SPAN destination ports in the VDC, you can apply the global command. If you want to apply the command only to a certain port, you can use the port-level command. If the ports are not SPAN destination ports, the command is rejected.

When you enter both the global and port-level configurations for this feature, the port-level overrides the global configuration.

Note The port-level command overrides the global command. So you can configure the device to strip the headers globally and then issue the no form of the port-level command to exclude the specified ports from stripping the headers.

Removing Headers Globally

Before you begin

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **system default switchport monitor exclude header**	Removes the FabricPath and VNTAG headers for all SPAN destination ports in the VDC. Use the **no** form of the command to preserve the headers on packets for SPAN destination ports.
Step 3	(Optional) switch(config)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Removing Headers per Port

Before you begin

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface** *type* {*module* | *port*}	Enters the interface mode and specifies the port or ports from which you want to remove the FabricPath and VNTAG headers.
Step 3	(Optional) switch(config)# [**no**]**switchport monitor exclude header**	Removes the FabricPath and VNTAG headers for the specified SPAN destination ports in the VDC. Use the **no** form of the command to preserve the headers on packets for SPAN destination ports.
Step 4	(Optional) switch(config)# **exit**	Returns to global configuration mode.
Step 5	(Optional) switch# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Verifying the SPAN Configuration

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

Command	Purpose
show monitor session {**all** | *session-number* | **range** *session-range*} [**brief**]	Displays the SPAN session configuration.

Command	Purpose
show resource monitor-session	Displays the resources that are available for the traditional sessions.
show resource monitor-session-extended	Displays the resources that are available for the extended session.
show running-config	Displays configuration of the commands for removing the FabricPath and VNTAG headers for SPAN.

Configuration Examples for SPAN

Configuration Example for a SPAN Session

To configure a 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 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
```

Configuration Example to Monitor All VLANs and Ports in an Extended SPAN Monitor Session

Example

This example shows how to monitor all VLANs and ports in an Extended SPAN monitor session:

```
switch# configure terminal
switch(config)# monitor session 3
switch(config-monitor)# mode extended
switch(config-monitor)# source interface all
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
```

This example shows how to monitor a higher number of specific VLAN sources than the VLAN source limits currently supported in the extended SPAN monitor session:

```
switch# configure terminal
switch(config)# monitor session 2
switch(config-monitor)# mode extended
switch(config-monitor)# source interface all
switch(config-monitor)# filter vlan 1-1000
switch(config-monitor)# destination interface ethernet 4/1
switch(config-monitor)# no shut
switch(config-monitor)# exit
switch(config)# show monitor session 2
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 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 Virtual SPAN Session

Procedure

Step 1 Configure destination ports in access or trunk mode, and enable SPAN monitoring.

Example:

```
switch# configure terminal
 switch(config)# interface ethernet 3/1
  switch(config-if)# switchport
  switch(config-if)# switchport mode trunk
  switch(config-if)# switchport trunk allowed vlan add 100-200
  switch(config-if)# switchport monitor
  switch(config-if)# no shut
  switch(config-if)# exit
switch(config)# interface ethernet 3/2
  switch(config-if)# switchport
  switch(config-if)# switchport mode trunk
  switch(config-if)# switchport trunk allowed vlan add 201-300
  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 4
switch(config)# monitor session 4tx
  switch(config-monitor)# source vlan 100-300
  switch(config-monitor)# destination interface ethernet 3/1-2
  switch(config-monitor)# no shut
  switch(config-monitor)# exit
switch(config)# show monitor session 4
switch(config)# copy running-config startup-config
```

Configuration Example for a SPAN Session with a Private VLAN Source

To configure a SPAN session that includes a private VLAN source, follow these steps:

Procedure

Step 1 Configure source VLANs.

Example:

```
switch# configure terminal
  switch(config)# vlan 100
    switch(config-vlan)# private-vlan primary
    switch(config-vlan)# exit
    switch(config)# interface ethernet 3/1
  switch(config-if)# switchport
    switch(config-if)# switchport access vlan 100
    switch(config-if)# no shut
    switch(config-if)# exit
  switch(config)# interface ethernet 3/2
    switch(config-if)# switchport
    switch(config-if)# switchport mode trunk
    switch(config-if)# switchport trunk native vlan 100
    switch(config-if)# no shut
    switch(config-if)# exit
  switch(config)#
```

Step 2 Configure destination ports in access or trunk mode, and enable SPAN monitoring.

Example:

```
switch# configure terminal
  switch(config)# interface ethernet 3/3
    switch(config-if)# switchport
    switch(config-if)# switchport mode trunk
    switch(config-if)# switchport trunk allowed vlan add 100-200
  switch(config-if)# switchport monitor
    switch(config-if)# switchport access vlan 100
    switch(config-if)# no shut
    switch(config-if)# exit
  switch(config)#
```

Step 3 Configure a SPAN session.

Example:

```
switch# no monitor session 3
switch(config)# monitor session 3
  switch(config-if)# source vlan 100
  switch(config-if)# destination interface ethernet 3/3
  switch(config-if)# no shut
  switch(config-if)# exit
switch(config-if)# show monitor session 3
switch(config-if)# copy running-config startup-config
```

Configuration Example for SPAN with MTU Truncation and SPAN Sampling

Example

This example shows how to configure MTU truncation and SPAN sampling for a SPAN session:

```
switch# configure terminal
switch(config)# monitor session 3
switch(config-monitor)# mtu 100
switch(config-monitor)# sampling 10
switch(config-monitor)# show monitor session 3
```

Configuration Example for Rule-Based SPAN

Example

This example shows how to configure a rule-based SPAN session:

```
switch# configure terminal
switch(config)# monitor session 3
switch(config-monitor)# mode extended
switch(config-monitor)# filter frame-type ipv4 src-ip 10.1.1.1/24
switch(config-monitor)# source interface ethernet 2/1-3, ethernet 3/1 rx
switch(config-monitor)# destination interface ethernet 2/5, ethernet 3/7
switch(config-monitor)# no shut
switch(config)# show monitor session 3
```

Configuration Example for Exception SPAN

Example

This example shows how to configure a SPAN session to span exception packets:

```
switch# configure terminal
switch(config)# monitor session 3
switch(config-monitor)# source exception all
switch(config-monitor)# destination interface ethernet 2/5, ethernet 3/7
switch(config-monitor)# no shut
switch(config)# show monitor session 3
```

Related Documents

Table 33: Related Documents

Related Topic	Document Title
Cisco Network Analysis Module (NAM)	*Cisco Network Analysis Module (NAM) for Nexus 7000 Quick Start Guide*

VDCs	*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*
Fabric Extender	*Cisco Nexus 2000 Series Fabric Extender Software Configuration Guide*
SPAN commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco Nexus 7000 Series NX-OS System Management Command Reference*

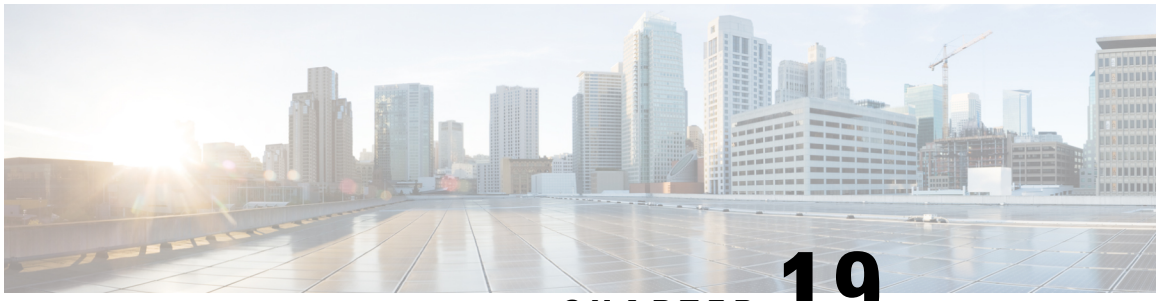
Feature History for SPAN

Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Table 34: Feature History for SPAN

Feature Name	Releases	Feature Information
SPAN	7.3(0)DX(1)	Added support for M3 Series modules.
SPAN	7.3(0)D1(1)	Added support for 4K VLANs per SPAN Session.
SPAN	6.2(10)	Added support to remove FabricPath and VLAN tag headers from SPAN packets.
SPAN	6.2(2)	Added NAM support for SPAN data sources.
SPAN	6.2(2)	Added support for FEX ports as a SPAN source in the Tx direction only on F2e Series modules
SPAN	6.2(2)	Added support for extended SPAN.
SPAN	6.2(2)	Added support for rule-based SPAN.
SPAN	6.2(2)	Added support for exception SPAN.
SPAN	6.1(1)	Added support for SPAN sampling.
SPAN	6.1(1)	Allowed the inband interface to be added as a source from any VDC except the admin VDC.
SPAN	6.1(1)	Added support for Supervisor 2.
SPAN	6.1(1)	Added support for M2 Series modules.

SPAN	6.1(1)	Added FCoE SPAN support on F2 Series modules for storage VDCs.
SPAN	6.0(1)	Added support for F2 Series modules.
SPAN	5.2(1)	Added SPAN source support for Cisco Nexus 2000 Series Fabric Extender interfaces.
SPAN	5.2(1)	Added the ability to configure MTU truncation, the source rate limit, and the multicast best effort mode for each SPAN session.
SPAN	5.1(1)	Added support for F1 Series modules and increased the number of supported SPAN sessions from 18 to 48.
SPAN	4.1(3)	Added a table of SPAN session limits.



CHAPTER 19

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.

This chapter contains the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

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 Types

Cisco NX-OS Release 6.1 and later releases support ERSPAN Type II and Type III. All previous Cisco NX-OS releases support only ERSPAN Type II.

ERSPAN Type III supports all of the ERSPAN Type II features and functionality and adds these enhancements:

- Provides timestamp information in the ERSPAN Type III header that can be used to calculate packet latency among edge, aggregate, and core switches.
- Identifies possible traffic sources using the ERSPAN Type III header fields.
- Provides the ability to configure timestamp granularity across all VDCs to determine how the clock manager synchronizes the ERSPAN timers.

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 and port channels.
- The inband interface to the control plane CPU—You can monitor the inband interface only from the default virtual device context (VDC). Inband traffic from all VDCs is monitored.
- VLANs (ingress only)—When a VLAN is specified as an ERSPAN source, all supported interfaces in the VLAN are ERSPAN sources.
- Fabric port channels connected to the Cisco Nexus 2000 Series Fabric Extender (FEX).
- Satellite ports and host interface port channels on the Cisco Nexus 2000 Series Fabric Extender— These interfaces are supported in Layer 2 access mode, Layer 2 trunk mode, and Layer 3 mode.

Note Layer 3 subinterfaces are not supported.

Note A single ERSPAN session can include mixed sources in any combination of the above.

See the *Cisco Nexus 7000 Series NX-OS Verified Scalability Guide* for information on the number of supported ERSPAN sessions.

ERSPAN source ports have the following characteristics:

- A port configured as a source port cannot also be configured as a destination port.
- ERSPAN does not monitor any packets that are generated by Supervisor 1, regardless of their source. This limitation does not apply to Supervisor 2.

ERSPAN Destinations

Destination ports receive the copied traffic from ERSPAN sources.

ERSPAN destination ports have the following characteristics:

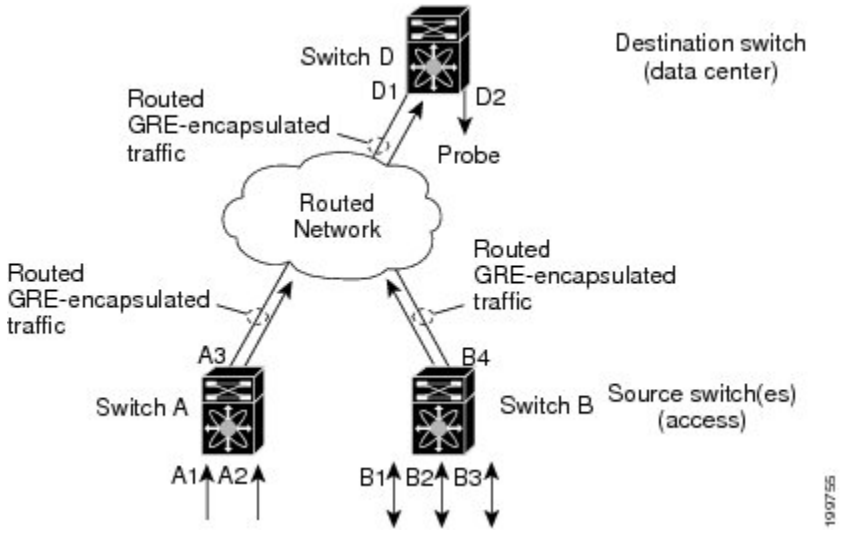
- Destinations for an ERSPAN session include Ethernet ports or port-channel interfaces in either access or trunk mode.
- A port configured as a destination port cannot also be configured as a source port.
- A destination port can be configured in only one ERSPAN session at a time.
- Destination ports do not participate in any spanning tree instance or any Layer 3 protocols.
- Ingress and ingress learning options are not supported on monitor destination ports.
- F Series module core ports, Fabric Extender host interface (HIF) ports, HIF port channels, and fabric port-channel ports are not supported as ERSPAN destination ports.

ERSPAN Sessions

You can create ERSPAN sessions that designate sources and destinations to monitor.

The figure below shows an ERSPAN configuration.

Figure 6: ERSPAN Configuration



Extended ERSPAN Session

Cisco NX-OS Release 6.2(2) and later releases support extended ERSPAN sessions in addition to the two traditional ERSPAN sessions in prior releases. Extended ERSPAN sessions can be bidirectional or unidirectional. The session direction is specified during session creation. A pool of 12 independent session resources are available. Unidirectional sessions use one resource, and bidirectional use two resources. These 12 resources are shared between local and ERSPAN source sessions across all VDCs.

If you are configuring an extended SPAN session on a Cisco Nexus 70xx or a Cisco Nexus 77xx switch, the following applies:

- You can configure 16 sessions as unidirectional or bidirectional, as required.
- You do not need to maintain two traditional sessions.

- You do not need to use the resource manager to reserve the two traditional sessions.
- ERSPAN ACL-based filtering is not supported.

Note On a Cisco Nexus 77xx switch, all sessions are extended by default and are not classified as Traditional sessions or Extended sessions. The **mode extended** command is not supported on Cisco Nexus 77xx switches.

4K VLANs per ERSPAN Session

Cisco NX-OS Release 7.3(0)D1(1) and later releases support 4K VLANs per ERSPAN session. You can use the **source interface all** command to enable the monitor session on the switch to monitor all VLANs and ports in the VDC such as physical ports, Port Channels, FEX ports and FEX Port Channels. The 4K VLANs per ERSPAN Session feature also enables monitoring of a higher number of specific VLAN sources than the VLAN source limits currently supported in the monitor session by using the **filter vlan** command with the **source interface all** command to filter the irrelevant VLANs.

The 4K VLANs per ERSPAN Session feature has the following characteristics:

- You can use the **source interface all** command for multiple sessions in the same VDC.
- Supports all session parameters such as MTU truncation, Sampling and Rate Limiting.
- Simple and Complex Rule-based SPAN is supported with the **source interface all** command. This enables traffic flow-based monitoring using a set of filter rules across the VDC.
- Traffic generated by Supervisors is not spanned.
- Supported only in Ethernet VDCs of Cisco Nexus 7000 Series switches.
- Supported only in extended SPAN sessions.

Rule-Based ERSPAN

Rule-based ERSPAN filters the ingress or egress ERSPAN traffic based on a set of rules. For Cisco NX-OS releases prior to 6.2(2), you can filter on VLANs, the destination index, and the source index. Beginning with Cisco NX-OS Release 6.2(2), you can filter the ERSPAN traffic based on a combination of fields in the Layer 2, Layer 3, or Layer 4 header packet.

Every ERSPAN session (traditional and extended) has an associated filter. Every ERSPAN session has one filter resource. A simple filter has only one rule, and you can add multiple fields or conditions to this rule. The packets are spanned only if all conditions are met.

Ethernet	IPv4	IPv6	ARP/RARP	FCoE
Frame Type	Frame Type	Frame Type	Frame Type	Frame Type
VLAN	VLAN	VLAN	VLAN	VLAN
TR	TR	TR	TR	TR
BPDU	BPDU	BPDU	BPDU	BPDU
Port Channel	Port Channel	Port Channel	Port Channel	Port Channel
Lane	Lane	Lane	Lane	Lane
Flow Hash	Flow Hash	Flow Hash	Flow Hash	Flow Hash
L2 MAC DA	L2 MAC DA	L2 MAC DA	L2 MAC DA	L2 MAC DA
L2 MAC SA	L2 MAC SA	L2 MAC SA	L2 MAC SA	L2 MAC SA
EtherType	EtherType	EtherType	EtherType	EtherType
CoS/VL	CoS/VL	CoS/VL	CoS/VL	CoS/VL
	ToS	ToS	ARP	FCD_ID
	L4 Protocol	L4 Protocol	Request	FCS_ID
	IPv4 SA	IPv6 SA	Sender IP	SOF
	IPv4 DA	IPv6 DA	Target IP	R_CTL
				TYPE
				Cmd_Code
				Sec_Hdr Exists

Exception ERSPAN

Exception ERSPAN enables you to span exception packets. Packets that have failed an intrusion detection system (IDS), Layer 3 IP verification, and FabricPath are treated as exception packets.

The exception ERSPAN session is supported in either one of the two traditional ERSPAN sessions or in one of the extended ERSPAN sessions. Rate limiters, MTU truncation, and sampling are supported in the exception ERSPAN session. Only the exception packets sent to the drop destination interface are supported as an ERSPAN source. Exception packets that are pushed to the supervisor, the ACLQoS, or Layer 2 are not spanned. Each VDC supports one exception ERSPAN session.

Exception ERSPAN is supported in the egress direction only. In the case of an extended ERSPAN Rx session, the exception source configuration will be rejected.

Network Analysis Module

You can also use the Cisco Network Analysis Module (NAM) to monitor ERSPAN data sources for application performance, traffic analysis, and packet header analysis.

To use NAM for monitoring the Cisco Nexus 7000 ERSPAN data sources, see the *Cisco Nexus 7000 Series Network Analysis Module (NAM-NX1) Quick Start Guide*.

High Availability

The ERSPAN 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 7000 Series NX-OS High Availability and Redundancy Guide*.

Virtualization Support

A virtual device context (VDC) is a logical representation of a set of system resources. ERSPAN applies only to the VDC where the commands are entered.

Note You can monitor the inband interface only from the default VDC. Inband traffic from all VDCs is monitored.

For information about configuring VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*.

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 7000 Series NX-OS Interfaces Configuration Guide*.

Guidelines and Limitations for ERSPAN

ERSPAN has the following configuration guidelines and limitations:

- For ERSPAN session limits, see the *Cisco Nexus 7000 Series NX-OS Verified Scalability Guide*.
- All ERSPAN replication is performed in the hardware. The supervisor CPU is not involved.
- Control plane traffic generated by Supervisor 2 can be ERSPAN encapsulated but cannot be filtered by an ERSPAN ACL.
- Control plane packets generated by Supervisor 1 cannot be ERSPAN encapsulated or filtered by an ERSPAN ACL.
- When you configure ERSPAN source on a Cisco Nexus 7000 Series switch that acts as a MPLS PE and the destination of the ERSPAN session is remote across the MPLS network, the ERSPAN packet will be transmitted as a regular IP packet and does not include the MPLS label. It causes the packet being dropped at the remote PE.
- ERSPAN and ERSPAN ACLs are not supported on F1 Series modules. For the VDCs that have F1 Series modules only, you can configure ERSPAN source and destination sessions and ERSPAN ACL source sessions but never come up.

- ERSPAN source sessions are supported on F2 Series and F2e (enhanced) Series modules. Beginning with Cisco NX-OS Release 6.2(2), ERPSPAN destination sessions are also supported on these modules. However, ERSPAN ACL sessions are not supported on F2 Series and F2e Series modules.
- ERSPAN source, destination, and ACL sessions are supported on M Series modules.
- The decapsulation of generic routing encapsulation (GRE) or ERSPAN packets received on an F1 Series module is not supported.
- ERSPAN and ERSPAN ACL sessions are terminated identically at the destination router.
- ERSPAN is not supported for management ports.
- ERSPAN does not support packet fragmentation. The "do not fragment" bit is set in the IP header of ERSPAN packets.
- A destination port can be configured in only one ERSPAN session at a time.
- You cannot configure a port as both a source and destination port.
- A single ERSPAN session can include mixed sources in any combination of the following:
  - Ethernet ports or port channels but not subinterfaces
  - VLANs (ingress only)
  - The inband interface or port channels to the control plane CPU

Note ERSPAN does not monitor any packets that are generated by the supervisor, regardless of their source.

- Destination ports do not participate in any spanning tree instance or Layer 3 protocols.
- When an ERSPAN session contains source ports or VLAN sources that are monitored in the transmit or transmit and receive direction, packets that these ports receive might be replicated to the ERSPAN 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
- You can enable ERSPAN for a source port before it becomes operationally active. For Layer 2 ports, traffic flooded to the VLANs that contain these ports are captured even when the link is not connected for the ports.
- For VLAN ERSPAN sessions with both ingress and egress configured, two packets (one from ingress and one from egress) are forwarded from the destination port if the packets get switched on the same VLAN.
- You can monitor the inband interface only from the default VDC. Inband traffic from all VDCs is monitored.

- A FabricPath core port is not supported as an ERSPAN destination when an F2 Series or F2e Series module is present in a VDC. However, a FabricPath core port can be configured as an ERSPAN source interface.
- When using ERSPAN sessions on F2 Series or F2e Series modules, ensure that the total amount of source traffic in a given session is less than or equal to the capacity of the ERSPAN destination interface or port channel for that session. If the ERSPAN source traffic exceeds the capacity of the ERSPAN destination, packet drops might occur on the ERSPAN source interfaces.
- Beginning with Cisco NX-OS Release 5.2, you can configure the Cisco Nexus 2000 Series Fabric Extender (FEX) interfaces and the fabric port channels connected to the Cisco Nexus 2000 Series Fabric Extender as ERSPAN sources. However, you cannot configure them as ERSPAN destinations.

Note ERSPAN on Fabric Extender interfaces and fabric port channels is supported on the M1 Series and M2 Series modules. ERSPAN runs on the Cisco Nexus 7000 Series device, not on the Fabric Extender. F2 Series and F2e Series modules support FEX, but they do not support FEX ERSPAN. Therefore, the FEX interfaces that are connected through the F2 Series and F2e Series modules cannot be made ERSPAN sources.

- You can span Fabric port channels on F2 Series and F2e Series modules.
- VLANs that contain FEX interfaces can be an ERSPAN source, but the ingress traffic through the F2 Series or F2e Series module-based FEX ports cannot be captured.
- Layer 3 multicast egress packets cannot be spanned on F2 Series or F2e Series modules.
- ERSPAN is supported on Fabric Extender interfaces in Layer 2 access mode, Layer 2 trunk mode, and Layer 3 mode. Layer 3 subinterfaces are not supported.
- For ERSPAN sessions, the recommended MTU size is 144 bytes or greater because MTU truncation occurs after the packets are encapsulated.
- The rate limit percentage of an ERSPAN session is based on 10G, 40G, and 100G for the respective modules (that is, 1 percent corresponds to 0.1G, 0.4G, or 1G respectively), and the value is applied per every forwarding engine instance.
- MTU truncation and the ERSPAN source rate limit are supported only on F2 Series, F2e Series, and M2 Series modules and Supervisor 2. They are not supported on M1 Series modules.
- For F2 Series and F2e Series modules, spanned FabricPath (core) packets have a 16-byte core header at the ERSPAN destination, and ingress FEX packets spanned through the fabric port channel have a 6-byte Vntag header at the ERSPAN destination. In addition, when trunk ports are used as the ERSPAN destination, the spanned packets have a 4-byte VLAN tag.
- For F2 Series and F2e Series modules, egress ERSPAN packets of all traffic that ingresses on Layer 2 ports (including edge-to-edge traffic) have a 16-byte MAC-in-MAC header at the ERSPAN destination.
- While setting IP TTL in the ERSPAN header,
  - In M-series LC, after ERSPAN encapsulation / de-capsulation, the packets are sent to EARL for recirculating and hence, the TTL is decremented by EARL.

  - In F2/F2e, there are no overheads of recirculating and hence, there is digression from the actual behavior of TTL decrements.
  - F1 series does not support ERSPAN.

- For MTU truncation on M2 Series modules, the truncated length of ERSPAN packets is rounded down to the nearest multiplier of 16 bytes. For example, with an MTU configuration value of 65 to 79, packets are truncated to 64 bytes.
- For certain rate limit and packet size values on F2 Series modules, F2e Series modules, M2 Series modules, and Supervisor 2, the ERSPAN packet rate is less than the configured value because of the internal accounting of packet sizes and internal headers.
- ERSPAN sampling is supported only on F2 Series and F2e Series modules. It is not supported on M Series modules.
- Multicast best effort mode applies only to M1 Series modules.
- Beginning with Cisco NX-OS Release 6.1, ERSPAN source sessions are supported on Supervisor 2, but ERSPAN ACL sessions are not.
- ERSPAN Type III source is supported only on F2 Series, F2e Series, and M2 Series modules.
- ERSPAN Type III termination is supported only on M2 Series modules. That is, Type III ERSPAN packets are decapsulated only when they reach their destination through M2 Series modules.
- Beginning with Cisco NX-OS Release 6.2(2), ERSPAN packets ingressing the destination switch on F2 Series or F2e Series modules can be terminated. IPv4 termination is supported but not IPv6 termination. F2 Series module termination on VDC virtual routing and forwarding (VRF) instances is not supported.
- Supervisor 2 supports ERSPAN Type II and ERSPAN Type III for inband ports, but timestamps are not synchronized with the Precision Time Protocol (PTP) master timers.
- 1588 granularity mode is not supported in Cisco NX-OS Release 6.1 and is rejected if selected.
- M2 Series modules support 100 microseconds (ms), 100 nanoseconds (ns), and ns granularity. F2 Series and F2e Series modules support only 100 ms and 100 ns granularity.
- When ERSPAN traffic is terminated on M2 Series modules, drops can occur at higher rates because all ERSPAN traffic for one session converges into one forwarding instance.
- If the global granularity configuration is not supported for a particular module, that module reverts to 100-ms granularity. For example, if granularity is set to ns, all M2 Series modules will enable ns granularities, and all F2 Series and F2e Series modules will internally enable and send packets with the 100-ms timestamp. Use the **show monitor session** command to display the supported and unsupported granularities for each module.
- F2 Series and F2e Series modules do not use the access control list (ACL) complex for ERSPAN Type III ACLs, so an ACL filter cannot be applied to F2 Series and F2e Series module traffic. However, for M2 Series modules, it is possible to encapsulate the packets using the Type III header after applying an ACL.
- F2 Series and F2e Series modules support a 32-bit timestamp in the ERSPAN Type III header while M2 Series modules support a 64-bit timestamp.
- If you enable ERSPAN on a vPC and ERSPAN packets need to be routed to the destination through the vPC, packets that come through the vPC peer-link cannot be captured.

- Extended ERSPAN sessions cannot source incoming traffic on M1 Series modules in either the ingress or egress direction.
- Traditional SPAN sessions support traffic from F Series and M Series modules. Extended SPAN sessions support traffic only from F Series and M2 Series modules.
- Hardware session 15 is used by NetFlow on F2 and F2e Series modules. Any extended session using this hardware ID will not span incoming traffic on the F2 and the F2e ports.
- Only eight sessions can support rate limiting on M2 Series modules. Any additional hardware sessions will not apply the configured rate limiter on M2 Series modules.
- M1 Series modules and Supervisor 1 do not support rule-based ERSPAN. They support only VLAN filtering.
- M1 and M2 Series modules support exception ERSPAN only in the nonadministration VDC, and at least one interface of the module must be present for the VDC.
- F1 Series modules have limited support for rule-based ERSPAN. They do not support the IPv6 source IP filter and the IPv6 destination IP filter. They support only IPv4 and IPv6 ToS filters with values from 0 to 3. Port-channel member lane, FCoE source ID, and FCoE destination ID are not supported.
- F2 and F2e Series modules have limited support for rule-based ERSPAN. They do not support wildcards in the IPv6 source IP filter and IPv6 destination IP filter, and they do not support egress ERSPAN filtering for destination MAC addresses and source MAC addresses.
- ERSPAN ACLs are not supported for use with OTV.
- ERSPAN source sessions are supported on F3 Series modules. Beginning with Cisco NX-OS Release 7.2, ERPSPAN destination sessions are also supported on these modules. However, ERSPAN ACL sessions are not supported on F3 Series modules.
- The ERSPAN termination takes place at the ingress point of entry of the destination switch (and not the final destination), so the ingress module at the destination switch must support ERSPAN termination. Beginning with Cisco NX-OS release 7.2(0)D1(1), ERSPAN Termination is supported on F3 linecards.
- Beginning with Cisco NX-OS Release 7.3(0)DX(1), ERSPAN source and destination sessions are supported on M3 Series modules.

Default Settings

The following table lists the default settings for ERSPAN parameters.

Table 35: Default ERSPAN Parameters

Parameters	Default
ERSPAN sampling	Disabled
ERSPAN sessions	Created in the shut state
ERSPAN source rate limit for traditional ERSPAN sessions	Disabled

Parameters	Default
ERSPAN source rate limit for extended ERSPAN sessions	Enabled
Global granularity of ERSPAN Type III sessions	100 microseconds
MTU truncation	Disabled
Multicast best effort mode	Disabled

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.

For sources, you can specify Ethernet ports, port channels, the supervisor inband interface, and VLANs (ingress only). A single ERSPAN session can include mixed sources in any combination of Ethernet ports, VLANs, or the inband interface to the control plane CPU.

For traditional sessions, you can configure the sessions without specifying the direction of the traffic.

Note ERSPAN does not monitor any packets that are generated by the supervisor, regardless of their source.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **monitor erspan origin ip-address** *ip-address* **global**	Configures the ERSPAN global origin IP address.
Step 3	switch(config)# **no monitor session** {*session-number* | **all**}	Clears the configuration of the specified ERSPAN session. The new session configuration is added to the existing session configuration.
Step 4	switch(config)# **monitor session** {*session-number* | **all**} **type erspan-source** [**shut**]	Configures an ERSPAN Type II source session. By default the session is bidirectional.

	Command or Action	Purpose
		The optional keyword shut specifies a shut state for the selected session.
Step 5	switch(config-erspan-src)# **description** *description*	Configures a description for the session. By default, no description is defined. The description can be up to 32 alphanumeric characters.
Step 6	switch(config-erspan-src)# **source** {[**interface** [**all**] [*type slot/port*[*-port*][*, type slot/port*[*-port*]]] [**port-channel** *channel-number*]] [**vlan** {*number* | *range*}]} [**rx** | **tx** | **both**]	Configures the sources and traffic direction in which to copy packets. You can enter a range of Ethernet ports, a port channel, an inband interface, or a range of VLANs. 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. The default direction is both. **Note** Source VLANs are supported only in the ingress (rx) direction. For a unidirectional session, the direction of the source must match the direction specified in the session. Beginning with Cisco NX-OS Release 7.3(0)D1(1), you can use the **all** keyword to enable the monitor session to monitor all VLANs and ports in the VDC such as physical ports, Port Channels, FEX ports and FEX Port Channels. The **all** keyword is supported only in extended ERSPAN sessions.
Step 7	(Optional) Repeat Step 6 to configure all ERSPAN sources.	—
Step 8	(Optional) switch(config-erspan-src)# **filter vlan** {*number* | *range*}	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. For information on the VLAN range, see the *Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*. You can enable monitoring of a higher number of specific VLAN sources than the VLAN source limits currently supported in extended ERSPAN monitor session by using the **filter vlan** command with the **source interface all** command to filter the irrelevant VLANs.

	Command or Action	Purpose
Step 9	(Optional) Repeat Step 8 to configure all source VLANs to filter.	—
Step 10	(Optional) switch(config-erspan-src)# **filter access-group** *acl-filter*	Associates an ACL with the ERSPAN session. **Note** You can create an ACL using the standard ACL configuration process. For more information, see the *Cisco Nexus 7000 Series NX-OS Security Configuration Guide*.
Step 11	switch(config-erspan-src)# **destination ip** *ip-address*	Configures the destination IP address in the ERSPAN session. Only one destination IP address is supported per ERSPAN source session.
Step 12	switch(config-erspan-src)# **erspan-id** *erspan-id*	Configures the ERSPAN ID for the ERSPAN source session. The ERSPAN range is from 1 to 1023.
Step 13	switch(config-erspan-src)# **vrf** *vrf-name*	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.
Step 14	(Optional) switch(config-erspan-src)# **ip ttl** *ttl-number*	Configures the IP time-to-live (TTL) value for the ERSPAN traffic. The range is from 1 to 255.
Step 15	(Optional) switch(config-erspan-src)# **ip dscp** *dscp-number*	Configures the differentiated services code point (DSCP) value of the packets in the ERSPAN traffic. The range is from 0 to 63.
Step 16	switch(config-erspan-src)# **no shut**	Enables the ERSPAN source session. By default, the session is created in the shut state.
Step 17	switch(config-erspan-src)# **exit**	Exits the monitor configuration mode.
Step 18	(Optional) switch(config)# **show monitor session** {**all** | *session-number* | **range** *session-range*} [**brief**]	Displays the ERSPAN session configuration.
Step 19	(Optional) switch(config)# **show running-config monitor**	Displays the running ERSPAN configuration.
Step 20	(Optional) switch(config)# **show startup-config monitor**	Displays the ERSPAN startup configuration.
Step 21	(Optional) switch(config)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Configuring an ERSPAN Destination Session

You can configure an ERSPAN destination session to copy packets from a source IP address to destination ports on the local device. By default, ERSPAN destination sessions are created in the shut state.

Before you begin

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Ensure that you have already configured the destination ports in monitor mode. For more information, see the *Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide*.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface ethernet** *slot/port*[*-port*]	Enters interface configuration mode on the selected slot and port or range of ports.
Step 3	switch(config-if)# **switchport**	Configures switchport parameters for the selected slot and port or range of ports.
Step 4	switch(config-if)# **switchport mode** [**access** | **trunk**]	Configures the following switchport modes for the selected slot and port or range of ports: • access • trunk
Step 5	switch(config-if)# **switchport monitor**	Configures the switchport interface as an ERSPAN destination.
Step 6	(Optional) Repeat Steps 2 to 5 to configure monitoring on additional ERSPAN destinations.	—
Step 7	switch(config-if)# **no monitor session** {*session-number* | **all**}	Clears the configuration of the specified ERSPAN session. The new session configuration is added to the existing session configuration.
Step 8	switch(config-if)# **monitor session** {*session-number* | **all**} **type erspan-destination**	Configures an ERSPAN destination session.
Step 9	switch(config-erspan-dst)# **description** *description*	Configures a description for the session. By default, no description is defined. The description can be up to 32 alphanumeric characters.
Step 10	switch(config-erspan-dst)# **source ip** *ip-address*	Configures the source IP address in the ERSPAN session. Only one source IP address is supported per ERSPAN destination session.

	Command or Action	Purpose
		Note The source IP address must be the IP address on the local device that is configured as the destination IP address on the ERSPAN source. This is the interface on the local device where the Cisco Nexus 7000 device expects to receive packets for decapsulation.
Step 11	switch(config-erspan-dst)# **destination** {[**interface** [*type slot/port*[*-port*][, *type slot/port*[*-port*]]] | [**port-channel** *channel-number*]]}	Configures a destination for copied source packets. You can configure one or more interfaces as a series of comma-separated entries. **Note** You can configure destination ports as trunk ports. For more information, see the *Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide*.
Step 12	(Optional) Repeat Step 11 to configure all ERSPAN destination ports.	—
Step 13	switch(config-erspan-dst)# **erspan-id** *erspan-id*	Configures the ERSPAN ID for the ERSPAN session. The range is from 1 to 1023.
Step 14	switch(config-erspan-dst)# **vrf** *vrf-name*	Configures the VRF that the ERSPAN destination session uses for traffic forwarding.
Step 15	switch(config-erspan-dst)# **no shut**	Enables the ERSPAN destination session. By default, the session is created in the shut state.
Step 16	switch(config-erspan-dst)# **exit**	Exits monitor configuration mode.
Step 17	switch(config)# **exit**	Exits global configuration mode.
Step 18	(Optional) switch# **show monitor session** {**all** | *session-number* | **range** *session-range*} [**brief**]	Displays the ERSPAN session configuration.
Step 19	(Optional) switch# **show running-config monitor**	Displays the running ERSPAN configuration.
Step 20	(Optional) switch# **show startup-config monitor**	Displays the ERSPAN startup configuration.
Step 21	(Optional) switch# **copy running-config startup-config** [**vdc-all**]	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

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **monitor session** {*session-range* | **all**} **shut**	Shuts down the specified ERSPAN sessions. By default, sessions are created in the shut state.
Step 3	switch(config)# **no monitor session** {*session-range* | **all**} **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 session shut** command followed by the **no monitor session shut** command.
Step 4	switch(config)# **monitor session** *session-number* **type erspan-source**	Enters the monitor configuration mode for the ERSPAN source type. The new session configuration is added to the existing session configuration.
Step 5	switch(config-erspan-src)# **monitor session** *session-number* **type erspan-destination**	Enters the monitor configuration mode for the ERSPAN destination type.
Step 6	switch(config-erspan-src)# **shut**	Shuts down the ERSPAN session. By default, the session is created in the shut state.
Step 7	switch(config-erspan-src)# **no shut**	Enables the ERSPAN session. By default, the session is created in the shut state.
Step 8	switch(config-erspan-src)# **exit**	Exits the monitor configuration mode.
Step 9	(Optional) switch(config)# **show monitor session all**	Displays the status of ERSPAN sessions.
Step 10	(Optional) switch(config)# **show running-config monitor**	Displays the ERSPAN running configuration.
Step 11	(Optional) switch(config)# **show startup-config monitor**	Displays the ERSPAN startup configuration.

	Command or Action	Purpose
Step 12	(Optional) switch(config)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Configuring MTU Truncation for Each ERSPAN Session

Beginning with Cisco NX-OS Release 6.1, in order to reduce the ERSPAN traffic bandwidth, you can configure the maximum bytes allowed for each replicated packet in an ERSPAN session. This value is called the maximum transmission unit (MTU) truncation size. Any ERSPAN packet larger than the configured size is truncated to the configured size.

Note MTU truncation and ERSPAN sampling can be enabled at the same time and have no precedence over each other because they are applied to different aspects of the source packet (size versus packet count).

Note Do not enable MTU truncation if the destination ERSPAN router is a Cisco Catalyst 6000 Series switch because the Cisco Catalyst 6000 Series switch drops these truncated packets.

Before you begin

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **monitor session** *session-number* **type erspan-source**	Enters the monitor configuration mode for the ERSPAN source type and specifies the ERSPAN session for which the MTU truncation size is to be configured.
Step 3	(Optional) switch(config-erspan-src)# **header-type** *version*	Changes the ERSPAN source session from Type II to Type III.
Step 4	switch(config-erspan-src)# [**no**] **mtu** *mtu*	Configures the MTU truncation size for packets in the specified ERSPAN session. The range is from 176 to 1500 bytes.
Step 5	switch(config-erspan-src)# **exit**	Exits monitor configuration mode.
Step 6	switch(config)# **exit**	Exits global configuration mode.
Step 7	(Optional) switch# **show monitor session** *session-number*	Displays the status of ERSPAN sessions, including the configuration status of MTU truncation, the maximum bytes allowed for each

	Command or Action	Purpose
		packet per session, and the modules on which MTU truncation is and is not supported.
Step 8	(Optional) switch# **copy running-config startup-config** [**vdc-all**]	Copies the running configuration to the startup configuration.

Configuring a Source Rate Limit for Each ERSPAN Session

When an ERSPAN session is configured with multiple interfaces as the sources in a high-traffic environment, the destination port can be overloaded, causing the normal data traffic to be disrupted at the source port. Beginning with Cisco NX-OS Release 6.1, you can alleviate this problem as well as traffic overload on the source forwarding instance by configuring a source rate limit for each ERSPAN session.

Note ERSPAN sampling takes precedence over ERSPAN source rate limiting. Rate limiting takes effect after sampling is completed on ERSPAN source packets.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **monitor session** *session-number* **type erspan-source**	Enters the monitor configuration mode for the ERSPAN source type and specifies the ERSPAN session for which the source rate limit is to be configured.
Step 3	(Optional) switch(config-erspan-src)# **header-type** *version*	Changes the ERSPAN source session from Type II to Type III.
Step 4	switch(config-erspan-src)# [**no**] **rate-limit** {**auto** | *rate-limit*}	Configures the source rate limit for ERSPAN packets in the specified ERSPAN session in automatic or manual mode: • Auto mode—Automatically calculates the rate limit on a per-gigabyte basis as follows: destination bandwidth / aggregate source bandwidth. For example, if the rate limit per gigabyte is 0.5, for every 1G of source traffic, only 0.5G of packets are spanned. For ingress traffic, the per-gigabyte limit is applied to each forwarding engine of the F2 Series or F2e Series module based on how many ports are used as the ERSPAN source so that the source can be spanned at the maximum available bandwidth. For

	Command or Action	Purpose
		egress traffic, the per-gigabyte limit is applied to each forwarding engine of the F2 Series or F2e Series module without considering how many ports are used as the ERSPAN source. • Manual mode—Specifies the percentage of the maximum rate of ERSPAN packets that can be sent out from each forwarding engine on a module. The range is from 1 to 100. For example, if the rate limit is 10 percent, the maximum rate of ERSPAN packets that can be sent out from each of the forwarding engines on an F2 Series or F2e Series module is 1G (or 10 percent of the 10G line rate).
Step 5	switch(config-erspan-src)# **exit**	Exits monitor configuration mode.
Step 6	switch(config)# **exit**	Exits global configuration mode.
Step 7	(Optional) switch# **show monitor session** *session-number*	Displays the status of ERSPAN sessions, including the configuration status of the rate limit, the percentage of the maximum ERSPAN rate allowed per session, and the modules on which the rate limit is and is not supported.
Step 8	(Optional) switch# **copy running-config startup-config** [**vdc-all**]	Copies the running configuration to the startup configuration.

Configuring Sampling for Each ERSPAN Session

Beginning with Cisco NX-OS Release 6.1, you can configure a sampling range for spanned traffic in order to reduce the ERSPAN traffic bandwidth and to monitor peer-to-peer traffic. Packet range-based sampling is used to provide an accurate count of the ERSPAN source packets.

Note Sampling and MTU truncation can be enabled at the same time and have no precedence over each other because they are applied to different aspects of the source packet (packet count versus size). However, sampling takes precedence over ERSPAN source rate limiting. Rate limiting takes effect after sampling is completed on ERSPAN source packets.

Before you begin

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **monitor session** *session-number* **type erspan-source**	Enters the monitor configuration mode for the ERSPAN source type and specifies the ERSPAN session for which ERSPAN sampling is to be configured.
Step 3	(Optional) switch(config-erspan-src)# **header-type** *version*	Changes the ERSPAN source session from Type II to Type III.
Step 4	switch(config-erspan-src)# [**no**] **sampling** *range*	Configures the sampling range for ERSPAN source packets. The sampling value is the range in which one packet out of x packets will be spanned, where x is from 2 to 1023. In this example, 1 out of every 100 packets will be spanned.
Step 5	switch(config-erspan-src)# **exit**	Exits monitor configuration mode.
Step 6	switch(config)# **exit**	Exits global configuration mode.
Step 7	(Optional) switch# **show monitor session** *session-number*	Displays the status of ERSPAN sessions, including the configuration status of ERSPAN sampling, the sampling value, and the modules on which sampling is and is not supported.
Step 8	(Optional) switch# **copy running-config startup-config** [**vdc-all**]	Copies the running configuration to the startup configuration.

Configuring the Multicast Best Effort Mode for an ERSPAN Session

You can configure the multicast best effort mode for any ERSPAN session. By default, ERSPAN replication occurs on both the ingress and egress modules. When you enable the multicast best effort mode, ERSPAN replication occurs only on the ingress module for multicast traffic or on the egress module for packets that egress out of Layer 3 interfaces (that is, on the egress module, packets that egress out of Layer 2 interfaces are not replicated for ERSPAN).

Note For Layer 3 multicast traffic, ERSPAN replication occurs on the egress module. If traffic is multicasted to multiple egress modules, you could capture multiple ERSPAN copies for each packet (that is, one copy from each egress module).

Before you begin

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **monitor session** *session-number* **type erspan-source**	Enters the monitor configuration mode for the ERSPAN source type and specifies the ERSPAN session for which the multicast best effort mode is to be configured.
Step 3	(Optional) switch(config-erspan-src)# **header-type** *version*	Changes the ERSPAN source session from Type II to Type III.
Step 4	switch(config-erspan-src)# [**no**] **multicast best-effort**	Configures the multicast best effort mode for the specified ERSPAN session.

Configuring Rule-Based ERSPAN

You can configure filters for ingress or egress ERSPAN traffic based on a set of rules. A simple filter has only one rule, and multiple fields or conditions can be added to this rule. The packets are spanned only if all conditions are met.

Before you begin

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **monitor erspan origin ip-address** *ip-address* **global**	Configures the ERSPAN global origin IP address. The global origin IP address can be configured in either the default VDC or the admin VDC. The value that is configured in this VDC is valid across all VDCs. Any change made in the default or admin VDC is applied across all nondefault VDCs.
Step 3	(Optional) switch(config)# **monitor erspan granularity** {**100_ms** | **100_ns** | **1588** | **ns**}	Specifies the granularity of all ERSPAN Type III sessions across all VDCs. The granularity options are 100 microseconds (ms), 100 nanoseconds (ns), IEEE 1588 (in seconds or nanoseconds), and nanoseconds.

	Command or Action	Purpose
		Note The clock manager adjusts the ERSPAN timers based on the granularity setting. If you configure IEEE 1588, the clock manager synchronizes the ERSPAN timers across switches. Otherwise, the clock manager synchronizes the ERSPAN timer with the master timer in the switch. **Note** 1588 granularity mode is not supported in Cisco NX-OS Release 6.1 and is rejected if selected. **Note** M2 Series modules support 100 ms, 100 ns, and ns granularity. F2 series and F2e Series modules support only 100 ms and 100 ns granularity. **Note** This command can be applied only in the default VDC.
Step 4	switch(config)# **no monitor session** {*session-number* | **all**}	Clears the configuration of the specified ERSPAN session. The new session configuration is added to the existing session configuration.
Step 5	switch(config)# **monitor session** {*session-number* | **all**} **type erspan-source** [**rx** | **tx**] [**shut**]	Configures an ERSPAN Type II source session. By default the session is bidirectional. The optional keywords are as follows: • **rx**—Specifies an ingress extended ERSPAN source session. • **tx**—Specifies an egress extended ERSPAN source session. • **shut**—Specifies a shut state for the selected session.
Step 6	(Optional) switch(config-erspan-src)# **mode extended**	Configures the ERSPAN source session as an extended bidirectional session. **Note** You cannot use this command on a unidirectional ERSPAN source session.
Step 7	(Optional) switch(config-erspan-src)# **header-type** *version*	Changes the ERSPAN source session from Type II to Type III.

	Command or Action	Purpose
		Note You can use the no form of this command to change an ERSPAN source session from Type III to Type II.
Step 8	(Optional) switch(config-erspan-src)# **description** *description*	Configures a description for the session. By default, no description is defined. The description can be up to 32 alphanumeric characters.
Step 9	switch(config-erspan-src)# [**no**] **filter** [**access-group** *acl-filter*] [**vlan** *vlan-range*] [**bpdu** [**true** | **false**]] [**cos** *cos-value*] [**dest-mac** *dest-mac*] [**eth-type** *eth-value*] [**flow-hash** *flow-value*] [**frame-type** [**eth** | **arp** | **fcoe** | **ipv4** | **ipv6**]] [**pc-lane** *port-number*] [**src_mac** *mac-address*] [**trace-route** [**true** | **false**]]	Configures the filter for the ERSPAN session. To remove the filter from the session, enter the **no** form of the command. The optional keywords are as follows: • **access-group**—Specifies a filter based on an access control group. • **vlan**—Specifies a filter based on a VLAN range. • **bpdu**—Specifies a filter based on the bridge protocol data unit (BPDU) class of packets. • **cos**—Specifies a filter based on the class of service (CoS) in the dotlq header. • **dest-mac**—Specifies a filter based on a destination MAC address. • **eth-type**—Specifies a filter based on the Ethernet type. • **flow-hash**—Specifies a filter based on the result bundle hash (RBH) value. • **frame-type**—Specifies a filter based on a frame type. • **pc-lane**—Specifies a filter based on a member of the port channel. • **src-mac**—Specifies a filter based on a source MAC address. • **trace-route**—Specifies a filter based on the route bit in the header.
Step 10	(Optional) switch(config-erspan-src)# [**no**] **filter frame-type eth**	Configures the Ethernet frame type filter for the ERSPAN session. To remove the filter from the session, enter the **no** form of the command.

	Command or Action	Purpose
Step 11	(Optional) switch(config-erspan-src)# [**no**] **filter frame-type arp** [[**arp-rarp** [**arp** | **rarp**]] [**req-resp** [**req** | **rsp**]] [**sender-ip** *ip-address*] [**target-ip** *ip-address*]]	Configures the ARP frame type filter for the ERSPAN session. To remove the filter from the session, enter the no form of the command. • **arp-rarp**—Specifies an ARP or RARP frame type filter. • **req-resp**—Specifies a filter based on a request or response. • **sender-ip**—Specifies a filter based on a sender IP address. • **target-ip**—Specifies a filter based on a target IP address.
Step 12	(Optional) switch(config-erspan-src)# [**no**] **filter frame-type fcoe** [[**fc-sid** *FC-source-ID*] [**fc-did** *FC-dest-ID*] [**fcoe-type** *fcoe-value*] [**r-ctl** *r-ctl-value*] [**sof** *sof-value*] [**cmd-code** *cmd-value*]]	Configures the FCoE frame type filter for the ERSPAN session. To remove the filter from the session, enter the **no** form of the command. The optional keywords are as follows: • **fc-sid**—Specifies a filter based on an FC source ID. • **fc-did**—Specifies a filter based on an FC destination ID. • **fcoe-type**—Specifies a filter based on an FCoE type. • **r-ctl**—Specifies a filter based on the routing control flags (R CTL) value. • **sof**—Specifies a filter based on the start of frame (SOF) packets. • **cmd-code**—Specifies a filter based on a command code.
Step 13	(Optional) switch(config-erspan-src)# [**no**] **filter frame-type ipv4** [[**src-ip** *src-ip*] [**dest-ip** *dest-ip*] [**tos** *tos-value*] [**l4-protocol** *l4-value*]]	Configures the IPv4 frame type filter for the ERSPAN session. To remove the filter from the session, enter the **no** form of the command. The optional keywords are as follows: • **src-ip**—Specifies a filter based on an IPv4 source IP address. • **dest-ip**—Specifies a filter based on an IPv4 destination IP address. • **tos**—Specifies a filter based on the type of service (ToS) in the IP header.

	Command or Action	Purpose
		• **l4-protocol**—Specifies a filter based on a Layer 4 protocol number set in the protocol field of the IP header.
Step 14	(Optional) switch(config-erspan-src)# [**no**] **filter frame-type ipv6** [[**src-ip** *src-ip*] [**dest-ip** *dest-ip*] [**tos** *tos-value*] [**l4-protocol** *l4-value*]]	Configures the IPv6 frame type filter for the ERSPAN session. To remove the filter from the session, enter the **no** form of the command. The optional keywords are as follows: • **src-ip**—Specifies a filter based on an IPv6 source IP address. • **dest-ip**—Specifies a filter based on an IPv6 destination IP address. • **tos**—Specifies a filter based on the type of service (ToS) in the IP header. • **l4-protocol**—Specifies a filter based on a Layer 4 protocol number set in the protocol field of the IP header.
Step 15	(Optional) Repeat Steps 9 to 14 for all filters for the session.	—
Step 16	switch(config-erspan-src)# **source** {[**interface** [*type slot/port* [*-port*] [,*type slot/port*[*-port*]]] [**port-channel** *channel-number*]] | [**vlan** {*number* | *range*}]} [**rx** | **tx** | **both**]	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, a Cisco Nexus 2000 Series Fabric Extender interface, or a fabric port channel connected to a Cisco Nexus 2000 Series Fabric Extender. You can configure one or more sources, as either a series of comma-separated entries or a range of numbers. You can specify up to 128 interfaces. The VLAN range is from 1 to 3967. The VLAN range of 4048 to 4093 is also supported for Cisco NX-OS releases prior to 6.1. You can specify the traffic direction to copy as ingress (rx), egress (tx) , or both. By default, the direction is both. For a unidirectional session, the direction of the source must match the direction specified in the session.
Step 17	(Optional) Repeat Step 16 to configure all ERSPAN sources.	—

	Command or Action	Purpose
Step 18	switch(config-erspan-src)# **destination ip** *ip-address*	Configures the destination IP address in the ERSPAN session. Only one destination IP address is supported per ERSPAN source session. **Note** The Cisco Nexus 2000 Series Fabric Extender interfaces and the fabric port channels connected to the FEX cannot be configured as ERSPAN destinations.
Step 19	switch(config-erspan-src)# **erspan-id** *erspan-id*	Configures the ERSPAN ID for the ERSPAN session. The ERSPAN range is from 1 to 1023.
Step 20	switch(config-erspan-src)# **vrf** *vrf-name*	Configures the 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.
Step 21	(Optional) switch(config-erspan-src)# **ip ttl** *ttl-number*	Configures the IP time-to-live (TTL) value for the ERSPAN traffic. The range is from 1 to 255.
Step 22	(Optional) switch(config-erspan-src)#**ip dscp** *dscp-number*	Configures the differentiated services code point (DSCP) value of the packets in the ERSPAN traffic. The range is from 0 to 63.
Step 23	switch(config-erspan-src)# **no shut**	Enables the ERSPAN session. By default, the session is created in the shut state.
Step 24	switch(config-erspan-src)# **exit**	Exits monitor configuration mode.
Step 25	switch(config)# **exit**	Exits global configuration mode.
Step 26	(Optional) switch# **show monitor session** {**all** | *session-number* | **range** *session-range*} [**brief**]	Displays the status of ERSPAN sessions, including the configuration status of the multicast best effort mode and the modules on which the best effort mode is and is not supported.
Step 27	(Optional) switch# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Configuring Exception ERSPAN

You can configure the device to span exception packets.

Before you begin

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **monitor session** *session-number* **type erspan-source** [**rx** | **tx**] [**shut**]	Enters the monitor configuration mode and specifies the ERSPAN session. The exception ERSPAN is supported in the egress direction only. In the case of an extended ERSPAN Rx session, the exception source configuration will be rejected. The optional keywords are as follows: • **rx**—Specifies an ingress extended ERSPAN source session. • **tx**—Specifies an egress extended ERSPAN source session. • **shut**—Specifies a shut state for the selected session.
Step 3	(Optional) switch(config-erspan-src)# **mode extended**	Configures the ERSPAN session as an extended bidirectional session.
Step 4	switch(config-erspan-src)# **source exception** {**layer3** | **fabricpath** | **other** | **all**}	Configures the source as an exception ERSPAN session. These exception types are supported: • **layer3**—Specifies the Layer 3 exception type for F2 Series and M Series modules. • **fabricpath**—Specifies the FabricPath exception type for F Series modules. • **other**—Specifies exceptions for M Series modules that are dropped through redirect registers programmed with a drop destination interface. • **all**—Includes all Layer 3, FabricPath, and other exceptions.
Step 5	switch(config-erspan-src)# **destination ip** *ip-address*	Configures the destination IP address in the ERSPAN session. Only one destination IP address is supported per ERSPAN source session. **Note** The Cisco Nexus 2000 Series Fabric Extender interfaces and the fabric port channels connected to the FEX cannot be configured as ERSPAN destinations.

	Command or Action	Purpose
Step 6	switch(config-erspan-src)# **no shut**	Enables the ERSPAN session. By default, the session is created in the shut state.
Step 7	switch(config-erspan-src)# **exit**	Exits module configuration mode.
Step 8	switch(config)# **exit**	Exits global configuration mode.
Step 9	(Optional) switch# **show monitor session** *session-number*	Displays the status of ERSPAN sessions, including the configuration status of the multicast best effort mode and the modules on which the best effort mode is and is not supported.
Step 10	(Optional) switch# **copy running-config startup-config** [**vdc-all**]	Copies the running configuration to the startup configuration.

Verifying the ERSPAN Configuration

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

Command	Purpose
show monitor session {**all** | *session-number* | **range** *session-range*} [**brief**]	Displays the ERSPAN session configuration.
show running-config monitor	Displays the running ERSPAN configuration.
show startup-config monitor	Displays the ERSPAN startup configuration.
show resource monitor-session-extended	Displays the resources that are available for the extended session.
show resource monitor-session-mx-exception-src	Displays the resources that are available for the exception session.

For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS System Management Command Reference*.

Configuration Examples for ERSPAN

Configuration Example for an ERSPAN Type III Source Session

This example shows how to configure an ERSPAN Type III source session:

```
switch# configure terminal
switch(config)# interface ethernet 14/30
switch(config-if)# no shut
```

```
switch(config-if)# exit
switch(config)# monitor erspan origin ip-address 3.3.3.3 global
switch(config)# monitor erspan granularity 100_ns
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# mode extended
switch(config-erspan-src)# header-type 3
switch(config-erspan-src)# source interface ethernet 14/30
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 to Monitor All VLANs and Ports in an Extended ERSPAN Monitor Session

This example shows how to monitor all VLANs and ports in an extended ERSPAN monitor session:

```
switch# configure terminal
switch(config)# monitor session 1 type erspan-source
switch(config-monitor)# mode extended
switch(config-monitor)# source interface all
switch(config-monitor)# destination interface ethernet 14/29
switch(config-monitor)# vrf default
switch(config-monitor)# erspan-id 200
switch(config-monitor)# no shut
switch(config-monitor)# exit
switch(config)# show monitor session 1
switch(config)# copy running-config startup-config
```

This example shows how to monitor a higher number of specific VLAN sources than the VLAN source limits currently supported in an extended ERSPAN monitor session:

```
switch# configure terminal
switch(config)# monitor session 2 type erspan-source
switch(config-monitor)# mode extended
switch(config-monitor)# source interface all tx
switch(config-monitor)# destination ip 192.0.2.1
switch(config-monitor)# vrf default
switch(config-monitor)# erspan-id 200
switch(config-monitor)# filter vlan 1-1000
switch(config-monitor)# no shut
switch(config-monitor)# exit
switch(config)# show monitor session 2
switch(config)# copy running-config startup-config
```

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 Destination Session

This example shows how to configure an ERSPAN destination session:

```
switch# configure terminal
switch(config)# interface e14/29
switch(config-if)# no shut
switch(config-if)# switchport
switch(config-if)# switchport monitor
switch(config-if)# exit
switch(config)# monitor session 2 type erspan-destination
switch(config-erspan-dst)# source ip 9.1.1.2
switch(config-erspan-dst)# destination interface e14/29
switch(config-erspan-dst)# erspan-id 1
switch(config-erspan-dst)# vrf default
switch(config-erspan-dst)# no shut
switch(config-erspan-dst)# exit
switch(config)# show monitor session 2
```

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)# header-type 3
switch(config-erspan-src)# filter access_group erspan_filter
```

Configuration Example for ERSPAN with MTU Truncation and ERSPAN Sampling

This example shows how to configure MTU truncation and ERSPAN sampling for an ERSPAN session:

```
switch# configure terminal
```

```
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# mtu 100
switch(config-erspan-src)# sampling 10
switch(config-erspan-src)# show monitor session 1
```

Configuration Example for ERSPAN Using the Multicast Best Effort Mode

This example shows how to configure the multicast best effort mode for an ERSPAN session:

```
switch# configure terminal
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# multicast best-effort
switch(config-erspan-src)# show monitor session 1
```

Configuration Example for Rule-Based ERSPAN

This example shows how to configure a rule-based ERSPAN session:

```
switch# configure terminal
switch(config)# monitor erspan origin ip-address 10.0.0.1 global
switch(config)# monitor erspan granularity 100_ns
switch(config)# no monitor session 3
switch(config)# monitor session 3 type erspan-source
switch(config-erspan-src)# mode extended
switch(config-erspan-src)# header-type 3
switch(config-erspan-src)# description erspan_src_session_3
switch(config-erspan-src)# filter frame-type ipv4 src-ip 10.1.1.1/24
switch(config-erspan-src)# filter vlan 10,20
switch(config-erspan-src)# source interface ethernet 2/1-3, ethernet 3/1 rx
switch(config-erspan-src)# destination ip 10.1.1.1
switch(config-erspan-src)# erspan-id 5
switch(config-erspan-src)# vrf default
switch(config-erspan-src)# ip ttl 25
switch(config-erspan-src)# ip dscp 42
switch(config-erspan-src)# no shut
switch# show monitor session 3
```

Configuration Example for Exception ERSPAN

This example shows how to configure an exception ERSPAN session:

```
switch# configure terminal
switch(config)# monitor session 3 type erspan-source
switch(config-erspan-src)# mode extended
switch(config-erspan-src)# source exception all
switch(config-erspan-src)# destination ip 10.1.1.1
switch(config-erspan-src)# no shut
switch# show monitor session 3
```

Related Documents

Related Topic	Document Title

ERSPAN commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco Nexus 7000 Series NX-OS System Management Command Reference*
VDCs	*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*
Cisco Network Analysis Module (NAM)	*Cisco Network Analysis Module (NAM) for Nexus 7000 Quick Start Guide*
Fabric Extender	*Cisco Nexus 2000 Series Fabric Extender Software Configuration Guide*

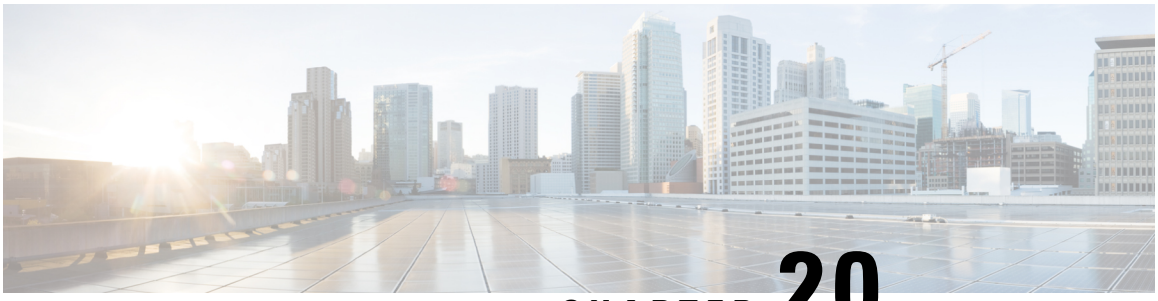
Feature History for ERSPAN

Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Table 36: Feature History for ERSPAN

Feature Name	Releases	Feature Information
ERSPAN	7.3(0)DX(1)	Added support for ERSPAN source and destination sessions on M3 Series modules.
ERSPAN	7.3(0)D1(1)	Added support for 4K VLANs per ERSPAN Session.
ERSPAN	6.2(2)	Added support for ERSPAN destination sessions on F2 and F2e Series modules.
ERSPAN	6.2(2)	Added NAM support for ERSPAN data sources.
ERSPAN	6.2(2)	Added support for extended ERSPAN.
ERSPAN	6.2(2)	Added support for rule-based ERSPAN.
ERSPAN	6.2(2)	Added support for exception ERSPAN.
ERSPAN	6.2(2)	Added support for ERSPAN termination on F2 or F2e Series modules.
ERSPAN	6.1(2)	Added support for F2e Series modules.
ERSPAN	6.1(1)	Added support for ERSPAN Type III.

ERSPAN	6.1(1)	Added support for Supervisor 2.
ERSPAN	6.1(1)	Added support for F2 and M2 Series modules.
ERSPAN	6.1(1)	Added support for ERSPAN sampling.
ERSPAN	6.1(1)	Added the ability to configure MTU truncation and the source rate limit for each ERSPAN session.
ERSPAN	6.0(1)	ERSPAN and ERSPAN ACLs are not supported on F2 Series modules.
ERSPAN	5.2(1)	Added ERSPAN source support for Cisco Nexus 2000 Series Fabric Extender interfaces.
ERSPAN	5.2(1)	Added the ability to configure the multicast best effort mode for an ERSPAN session.
ERSPAN and ERSPAN ACLs	5.1(1)	This feature was introduced.
ERSPAN	7.2	ERSPAN source sessions are supported on F3 Series modules. However, ERSPAN ACL sessions are not supported on F3 Series modules.



CHAPTER 20

Configuring LLDP

This chapter describes how to configure the Link Layer Discovery Protocol (LLDP) in order to discover other devices on the local network.

This chapter includes the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

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 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
- Port VLAN
- System capabilities
- System description
- System name

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 into a specific DCBXP TLV. This TLV is designed to provide an acknowledgement to the received LLDP packet. In this way, DCBXP adds a lightweight acknowledgement mechanism on top of LLDP so that any application that needs a request-response semantic from a link-level protocol can make use of DCBXP.

Other applications 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 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 TLV—Carries information about which VLANs will be used by specific protocols.

Note For information on the quality of service (QoS) features, see the *Cisco Nexus 7000 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 7000 Series NX-OS High Availability and Redundancy Guide*.

Virtualization Support

One instance of LLDP is supported.

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.
- LLDP can discover Linux servers, provided they are not using a converged network adapter (CNA). LLDP cannot discover other types of servers.
- 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.
- DCBXP is not supported for the Cisco Nexus 2000 Series Fabric Extender.
- Beginning with Cisco NX-OS Release 5.2, LLDP is supported for the Cisco Nexus 2000 Series Fabric Extender. LLDP packets can now be sent and received through the Fabric Extender ports for neighbor discovery.
  - All LLDP configuration on Fabric Extender ports occurs on the supervisor. LLDP configuration and **show** commands are not visible on the Fabric Extender console.
  - LLDP is not supported for a Fabric Extender-virtual port channel (vPC) connection.

Default Settings for LLDP

This table lists the LLDP default settings.

Parameters	Default
Global LLDP	Disabled

Parameters	Default
LLDP on interfaces	Enabled, after LLDP is enabled globally
LLDP hold time (before discarding)	120 seconds
LLDP reinitialization delay	2 seconds
LLDP timer (packet update frequency)	30 seconds
LLDP TLVs	Enabled
LLDP receive	Enabled, after LLDP is enabled globally
LLDP transmit	Enabled, after LLDP is enabled globally
DCBXP	Enabled, provided LLDP is enabled

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

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# [**no**] **feature lldp**	Enables or disables LLDP on the device. LLDP is disabled by default.
Step 3	(Optional) switch(config)# **show running-config lldp**	Displays the global LLDP configuration. If LLDP is enabled, it shows "feature lldp." If LLDP is disabled, it shows an "Invalid command" error.
Step 4	(Optional) switch(config)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

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

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface** *interface slot/port*	Specifies the interface on which you are enabling LLDP and enters the interface configuration mode.
Step 3	switch(config-if)# [**no**] **lldp transmit**	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.
Step 4	switch(config-if)# [**no**] **lldp receive**	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.
Step 5	(Optional) switch(config-if)# **show lldp interface** *interface slot/port*	Displays the LLDP configuration on the interface.
Step 6	(Optional) switch(config)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

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

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	(Optional) switch(config)# [**no**] **lldp holdtime** *seconds*	Specifies the amount of time in seconds that a receiving device should hold the information sent by your device before discarding it. The range is 10 to 255 seconds; the default is 120 seconds.
Step 3	(Optional) switch(config)# [**no**] **lldp reinit** *seconds*	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.

	Command or Action	Purpose
Step 4	(Optional) switch(config)# [**no**] **lldp timer** *seconds*	Specifies the transmission frequency of LLDP updates in seconds. The range is 5 to 254 seconds; the default is 30 seconds.
Step 5	(Optional) switch(config)# **show lldp timers**	Displays the LLDP hold time, delay time, and update frequency configuration.
Step 6	(Optional) switch(config)# [**no**] **lldp tlv-select** *tlv*	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.
Step 7	(Optional) switch(config)# **show lldp tlv-select**	Displays the LLDP TLV configuration.
Step 8	(Optional) switch(config)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Verifying the LLDP Configuration

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

Command	Purpose
show running-config lldp	Displays the global LLDP configuration.
show lldp interface *interface slot*/*port*	Displays the LLDP interface configuration.
show lldp timers	Displays the LLDP hold time, delay time, and update frequency configuration.
show lldp tlv-select	Displays the LLDP TLV configuration.
show lldp dcbx interface *interface slot*/*port*	Displays the local DCBX control status.
show lldp neighbors {**detail** | **interface** *interface slot*/*port*}	Displays the LLDP neighbor device status.
show lldp traffic	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.
show lldp traffic interface *interface slot*/*port*	Displays the number of LLDP packets sent and received on the interface.

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
```

Related Documents

Related Topic	Related Topic
LLDP commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco Nexus 7000 Series NX-OS System Management Command Reference*
VDCs	*Cisco Nexus 2000 Series Fabric Extender Software Configuration Guide*
Fabric Extender	*Cisco Network Analysis Module (NAM) for Nexus 7000 Quick Start Guide*

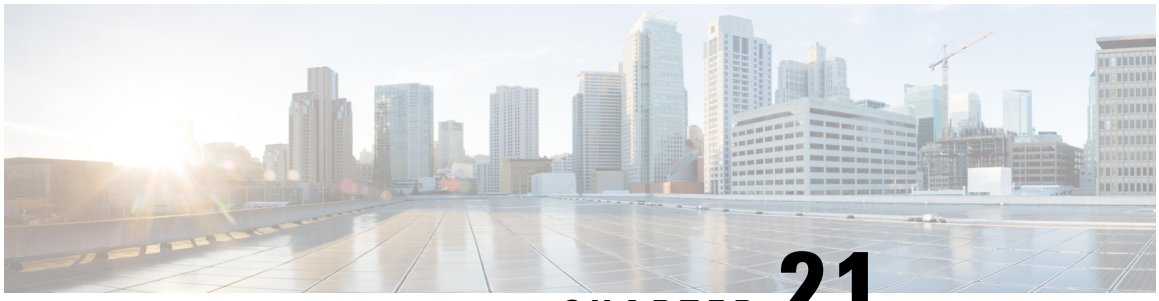
Feature History for LLDP

Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Table 37: Feature History for LLDP

Feature Name	Releases	Feature Information
LLDP	5.2(1)	Added LLDP support for the Cisco Nexus 2000 Series Fabric Extender.
DCBXP	5.1(1)	This feature was introduced.

LLDP	5.0(2)	This feature was introduced.



CHAPTER 21

Configuring NetFlow

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

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “New and Changed Information” chapter or the Feature History table.

NetFlow

NetFlow identifies packet flows for both ingress and egress IP packets and provide statistics based on these packet flows. NetFlow does not require any change to either the packets themselves or to any networking device.

Netflow Overview

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. Cisco NX-OS exports a flow as part of a NetFlow export User Datagram Protocol (UDP) datagram under the following circumstances:

- The flow has been inactive or active for too long.
- The flow cache is getting full.
- One of the counters (packets or bytes) has exceeded its maximum value.
- 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 in either full or sampled mode. Cisco NX-OS analyzes all packets on the interface or subinterface for full NetFlow mode. For sampled mode, you configure the rate at which Cisco NX-OS analyzes packets.

Flow Records

A flow record defines the keys that NetFlow uses to identify packets in the flow as well as 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-bit 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 interface output
- 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 collector is listening for NetFlow packets)

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 will be inactive.

Cisco NX-OS exports data to the collector whenever a timeout occurs or when the flow is terminated (TCP FIN or RST received, for example). You can configure the following timers to force a flow export:

- Active timeout—Removes the cache entries from the cache. Prevents long-lasting flows from becoming invisible to the collector for a long period of time. The value of the active timeout should always be greater than that of the inactive timeout. Active timeout is supported on the M1, M2, F3 and M3 Series modules.
- Inactive timeout—Removes the cache entries from the cache. Inactive timeout is supported on the M1, M2, F3 and M3 Series modules.
- Fast timeout—Flushes low-hitting flows for the M1 and M2 Series modules.
- Aggressive timeout—Aggressively times out the flows when the cache starts getting full for the M1 and M2 Series modules.
- Session timeout—Ages the flows if the TCP close connection handshake is observed (FIN/FIN_ACK packets). Session timeout is supported on M1 and M2 Series modules.
- Flush cache timeout—Flushes the cache for F2, F2e, and F3 Series modules.

Note The first five timeouts are applicable only to the NetFlow cache on M Series modules. The flow timeout is supported only for F2, F2e, and F3 Series modules.

The active and inactive timeouts exist by default and cannot be unconfigured. Only their time values can be configured.

Export Formats

Cisco NX-OS supports the Version 5 and Version 9 export formats. We recommend that you use the Version 9 export format for the following reasons:

- More efficient network utilization
- Support for IPv6 and Layer 2 fields

If you configure the Version 5 export format, you have these limitations:

- Fixed field specifications
- No support for IPv6 and Layer 2 fields
- The Netflow.InputInterface and Netflow.OutputInterface represent a 16-bit I/O descriptor (IOD) of the interface.

Note The IOD information of the interface can be retrieved using the show system internal im info global command.

Note Cisco NX-OS supports UDP as the transport protocol for exports to up to two collectors.

Note M1 Series modules support the configuration change from the Version 5 to Version 9 export format, but F2, F2e, and F3 Series modules do not.

Flow Monitors

A flow monitor references the flow record and flow exporter. You apply a flow monitor to an interface.

Samplers

Cisco NX-OS supports sampled NetFlow. This feature samples incoming and outgoing packets on an interface. The packets sampled then qualify to create flows.

Sampled NetFlow reduces the amount of export data sent to the collector by limiting the number of packets that create flows and the number of flows. It is essential when flows are created on a line card or external device, instead of on the forwarding engine. F2, F2e, F3, and M3 Series modules support only sampled NetFlow.

Implementing NetFlow on F2 and F2e Series modules creates flows in the software. Too many packets trying to create or update flows can increase the load on the CPU, thereby increasing the need for a protective rate limiter. The rate limiter limits the number of packets that reach the CPU to approximately 1000 packets per second. F3 and M3 Series modules use a special hardware called FSA, which is used as a NetFlow processor, to create flows.

The sampling mode supported on F2, F2e, F3, M3, M1, and M2 modules is M out of N, where M packets are selected randomly out of every N packets for sampling, and only those packets can create flows.

Note With the F2 and F2e Series modules, you will need to be aware of the scaling factor to be configured, which is the additional sampling of 1:100 multiplied by the configured sampling. If you overlook this factor, you will not see the actual in the reported rate.

Rate limiter limits the number of packets that reach the CPU to approximately 1000 packets per second on the F2 and F2e Series modules. On the F3 Series module, rate limiting of 500 PPS per ASIC (SoC) is implemented. Hence, for Cisco NX-OS 7000, if the F3 Series module has 6 SoCs, then it will rate limit 500*6=3000 PPS to the CPU, per F3 Series module; and for Cisco NX-OS 7700, if the F3 Series module has 12 SoCs, then it will rate limit 500*12=6000 PPS to the CPU, per F3 Series module.

The F3 and M3 Series module supports more sampling rate, 1:131071 compared to 1:8191 on other F2 and F2e series modules.

Note The F3 series module supports an increased sampling rate on version 9. Performance on the F3 series module for the 7.2(0)D1(1) release has improved by 20 to 50 times the packet processing capability when compared to a 6.2.x release. It is enhanced to 50000 pps. Due to the increased speed, you can use a lower sampling rate on the F3 series module for this release. For example, a sampling of 1:4000 can be replaced with a sampling of 1:80.

On M3 series modules, the default rate limit value is 8000 PPS per ASIC (SoC). In such a scenario, the Cisco Nexus 7700 M3-Series 48-Port 1/10G Ethernet Module (with 2 SoCs) will rate limit 8000*2=16000 PPS only to the CPU per M3 Series module. Use the **hardware rate-limiter layer-2 netflow** *rate* **module** *m3module* command on a specific M3 Series module to configure the rate limit value to 24000 PPS. This configuration will enable the M3 series module to rate limit 24000*2=48000 PPS to the CPU per M3 Series module.

Similarly, the Cisco Nexus 7700 M3-Series 24-Port 40G Ethernet Module (with 4 SoCs) will rate limit 8000*4=32000 PPS only to the CPU per M3 Series module. Use the **hardware rate-limiter layer-2 netflow** *rate* **module** *m3module* command on a specific M3 Series module to configure the rate limit value to 12000 PPS. This configuration will enable the M3 Series module to rate limit 12000*4=48000 PPS to the CPU per M3 Series module.

The following limitations apply to sampled NetFlow and F2 Series and F2e Series modules:

- An additional sampling of 1:100 is applied over the configured value for F2 Series and F2e Series modules. For example, if the configured sampling is 1 in 200, the actual applied sampling is 1 in 20000. When you configure the sampler value to 1:4956, the system does not start the rate-limiter. This value is calculated based on the maximum traffic that would cross a module.
- The accuracy of the sampled NetFlow compared with the traditional NetFlow is dependent on the sampling rate configured. If the sampling rate is 1:1, the sampled NetFlow is exactly accurate as the traditional NetFlow. And if the sampling rate is 1:100, the sampled NetFlow is less accurate than the traditional, but it still yields statistical patterns that allow you to monitor the device.

Netflow on CoPP Interface Support

Netflow on CoPP Interface Support features enables application of Netflow on packets that are destined to the supervisor module, which is the control plane.

Netflow on CoPP Interface Support feature enables the monitoring of packets that are egressing to the control plane. This monitoring feature was added in NX-OS release 7.3(0)D1(1).

For more information on Control Plane Policing, See the *Cisco Nexus 7000 Series NX-OS Security Configuration Guide*.

Network Analysis Module

You can also use the Cisco Network Analysis Module (NAM) to monitor NetFlow data sources. NAM enables traffic analysis views and reports such as hosts, applications, conversations, VLAN, and QoS. See the NAM configuration example in the Configuration Examples for NetFlow.

To use NAM for monitoring the Cisco Nexus 7000 NetFlow data sources, see the *Cisco Nexus 7000 Series Network Analysis Module (NAM-NX1) Quick Start Guide*.

High Availability

Cisco NX-OS supports stateful restarts for NetFlow. After a reboot or supervisor switchover, Cisco NX-OS applies the running configuration.

Because the flow cache is not preserved across restarts of the process and packets that come to the software during restarts cannot be processed, all of the flows during switchovers are lost and cannot be recovered.

Virtualization Support

A virtual device context (VDC) is a logical representation of a set of system resources. Within each VDC, you can configure NetFlow. By default, Cisco NX-OS places you in the default VDC and any flows that you define in this mode are only available for interfaces in the default VDC.

For information about configuring VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*.

Prerequisites for NetFlow

NetFlow has the following prerequisites:

- You must understand the resources required on your device because NetFlow consumes additional memory and CPU resources.
- If you configure VDCs, install the appropriate license and enter the desired VDC. See the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide for configuration information and the Cisco NX-OS Licensing Guide* for licensing information.

Guidelines and Limitations for NetFlow

NetFlow has the following configuration guidelines and limitations:

- You must configure a source interface for the NDE export. If you do not configure a source interface, the flow exporter will remain in a disabled state.
- You must configure a valid record name for every flow monitor.
- All of the NetFlow timeouts, except the flow timeout, are applicable only to M1 and M2 Series modules. The flow timeout is supported only for F2, F2e, and F3 Series modules. Only active and inactive timeouts are applicable for M3 Series modules.
- A rollback will fail if you try to modify a record that is programmed in the hardware during a rollback.
- Only Layer 2 NetFlow is applied on Layer 2 interfaces, and only Layer 3 NetFlow is applied on Layer 3 interfaces.
- 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.
- If you change a Layer 2 interface to a Layer 3 interface, the software removes the Layer 2 NetFlow configuration from the interface.

- Use NetFlow v9 export to see the full 32-bit SNMP ifIndex values at the NetFlow connector.
- The maximum number of supported NetFlow entries is 512,000.
- On tunnel interface, NetFlow is not supported, even though its configurable.
- The Cisco Nexus 2000 Series Fabric Extender (FEX) supports a Layer 3 NetFlow configuration on FEX ports.
- The Cisco Nexus 2000 Series FEX supports bridged NetFlow (for flows within a VLAN).
- M1 Series modules support the configuration change from the Version 5 to Version 9 export format, but F2, F2e, and F3 Series modules do not.
- F2, F2e, F3, and M3 Series modules do not support the following changes:
  - Changing the fields in a record that is applied on the active monitor.
  - Changing the sampling mode value on a sampler that is applied on the active monitor.
- Beginning with Cisco NX-OS Release 5.2, NetFlow is supported on switch virtual interfaces (SVIs) for F1 Series ports, if at least one M1 Series module is present. SVI NetFlow is for traffic that is routed between VLANs.
- For M Series modules, if you apply a Layer 3 NetFlow input flow monitor to an SVI and apply a Layer 2 NetFlow input flow monitor to a Layer 2 interface such as a trunk that allows the same underlying VLAN, all input flows into both interfaces are reported by the Layer 2 NetFlow flow monitor only.
- F2, F2e, F3, and M3 Series modules support only sampled NetFlow.
- Beginning with Cisco NX-OS Release 6.1(2), sampled NetFlow is supported on F2 and F2e Series modules.
- Beginning with Cisco NX-OS Release 6.2(6), sampled NetFlow is supported on F3 Series modules.
- Egress NetFlow is not supported on F2, F2e modules, and on any mixed VDC the modules are present in.
- Beginning from Cisco NX-OS Release 7.2(0)D1(1), Egress NetFlow is supported on F3 modules.
- Beginning from Cisco NX-OS Release 7.2(1)D1(1), Sub-interfaces are supported on F2, F2e, and F3 series modules.
- Beginning from Cisco NX-OS Release 7.3(0)DX(1), ingress and egress NetFlow is supported on M3 Series modules.
- By default, you cannot use ingress NetFlow sampling and DHCP relay together on the same interface. However, beginning with Cisco NX-OS Release 6.2(2), you can override the default and configure these two features on the same interface using the **hardware access-list resource feature bank-mapping command**, after you have entered the necessary commands to enable each of these features individually. For more information on this command, see the **Configuring IP ACLs** chapter of the *Cisco Nexus 7000 Series NX-OS Security Configuration Guide*.
- Beginning with Cisco NX-OS Release 6.2(2), full NetFlow is supported on the Cisco NetFlow Generation Appliance (NGA) through SPAN. Sampled NetFlow is supported on the NGA through sampled SPAN.

NetFlow has the following limitations for mixed VDCs with both M1, M2 Series and F2, F2e, F3, and M3 Series modules:

- A VDC is classified as a mixed VDC only when it contains at least one F2e Series port or at least one F3 Series port.
- Layer 2 NetFlow—Sampled and full NetFlow is supported on the M1 and M2 Series module ports, and only sampled NetFlow is supported on the F2e, F3 and M3 Series module ports.
- Layer 3 NetFlow—Sampled and full NetFlow is supported on the M1 and M2 Series module ports. The F2 and F2e Series module ports come up in proxy mode and, therefore, cannot be configured as Layer 3 ports. Thus, Layer 3 NetFlow and subinterface NetFlow do not work with these ports. Sampled NetFlow is supported on F3 and M3 Series module ports.
- VLANs, SVIs, and port channels—Only sampled NetFlow is supported on VLANs, SVIs, and port channels for both the M1 and M2 Series and F2e, F3, and M3 Series modules.
- Subinterfaces (physical/port channels)—NetFlow configuration is supported on the F2, F2e, F3, and M3 Series module interfaces.
- Dynamic configuration change is not available in the mixed VDC for the policies applied on the M1 and M2 Series and F2e, F3, and M3 Series modules.
- Flow timeout applies only to the F2e and F3 Series modules. Other NetFlow timers apply to the M1 and M2 Series modules. Only active and inactive timeouts are applicable for M3 Series modules.
- Egress NetFlow is completely blocked in VDCs that contain both M Series and F2e and F3 Series modules.

Guidelines and Limitations Specific to NetFlow on CoPP Interface Support feature:

- The feature can be configured only on the default VDC.
- Only unicast packets are supported.
- The feature supports capture of Layer 3 NetFlow fields only. Capture of Layer 2 fields are not supported.
- The feature requires mandatory configuration of a sampler.
- After the feature is enabled, it is applied on all the line cards in the system as follows:
  - M1/M2 line cards create sampled flows in the hardware table. The global routing table, with 512,000 entries, is shared with the regular NetFlow.
  - F2/F2e line cards create sampled flows in the software table. The limits on the size of packets per second (PPS) per table is shared with the regular NetFlow. An additional 1:100 sampler is also applicable as usual.
  - F3 line cards create flows in the software. The limits on the size of PPS per table is shared with the regular NetFlow.
  - The feature can be applied only in the egress direction, because the packets egress to the supervisor module.

Default Settings for NetFlow

The following table lists the default settings for NetFlow parameters.

Table 38: Default NetFlow Parameters

Parameters	Default
Egress and ingress cache size	512,000
Flow active timeout	1800 seconds
Flow timeout (for F2, F2e, and F3 Series modules only)	15 seconds
Flow timeout aggressive threshold	Disabled
Flow timeout fast threshold	Disabled
Flow timeout inactive	15 seconds
Flow timeout session aging	Disabled

Configuring NetFlow

To configure NetFlow, follow these steps:

Procedure

Step 1 Enable the NetFlow feature.

Step 2 Define a flow record by specifying keys and fields to the flow.

Step 3 Define an optional flow exporter by specifying the export format, protocol, destination, and other parameters.

Step 4 Define a flow monitor based on the flow record and flow exporter.

Step 5 Apply the flow monitor to a source interface, subinterface, VLAN interface.

Enabling the NetFlow Feature

You must globally enable NetFlow before you can configure any flows.

Use the following command in global configuration mode to enable NetFlow:

Command	Purpose

feature netflow
`Example:`
`switch(config)# feature netflow`
	Enables the NetFlow feature.

Command	Purpose

no feature netflow Example: `switch(config)# no feature netflow`	Disables the NetFlow feature. The default is disabled.

Creating a Flow Record

You can create a flow record and add keys to match on and nonkey fields to collect in the flow.

Before you begin

Make sure that you are in the correct VDC. To change the VDC, use the **switchto vdc** command.

Procedure

	Command or Action	Purpose

Step 1	**configure t**
	Example:
	`switch# config t`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**flow record** *name*
	Example:
	`switch(config)# flow record Test`
	`switch(config-flow-record)#`
		Creates a flow record and enters flow record configuration mode. You can enter up to 63 alphanumeric characters for the flow record name.

Step 3	(Optional) **description***string* **Example:** `switch(config-flow-record)# description Ipv4Flow`	(Optional) Describes this flow record as a maximum 63-character string.
Step 4	(Optional) **match***type* **Example:** `switch(config-flow-record)# match transport destination-port`	Specifies a match key. **Note** The **match transport destination-port** and the **match ip protocol** commands are required to export Layer 4 port data.
Step 5	**collect** *type* **Example:** `switch(config-flow-record)# collect counter packets`	(Optional) Specifies the collection field.
Step 6	**show flow record** [**name**] [*record-name*] |**netflow-original** | **netflow protocol-port** | **netflow {ipv4** | **ipv6}** {**original-input** | **original-output**}}	(Optional) Displays information about NetFlow flow records. You can enter up to 63 alphanumeric characters for the flow record name.

	Command or Action	Purpose
	Example: `switch(config-flow-exporter)# show flow record netflow protocol-port`	
Step 7	**copy running-config startup-config** **Example:** `switch(config-flow-exporter)# copy running-config startup-config`	(Optional) Saves this configuration change.

Specifying the Match Parameters

You must configure at least one of the following match parameters for flow records:

Command	Purpose
match ip {**protocol** | **tos**} **Example:** `switch(config-flow-record)# match ip protocol`	Specifies the IP protocol or ToS fields as keys **Note** The **match transport destination-port** and the **match ip protocol** commands are required to export Layer 4 port data. The data is collected and displayed in the output of the **show hardware flow ip** command but is not collected and exported until you configure both commands.
match ipv4 {**destination address** | **source address**} **Example:** `switch(config-flow-record)# match ipv4 destination address`	Specifies the IPv4 source or destination address as a key.
match ipv6 {**destination address** | **source address** | **flow-label** | **opitons** } **Example:** `switch(config-flow-record)# match ipv6 flow label`	Specifies the IPv6 key.

Command	Purpose
match transport {**destination-port** | **source-port**} **Example:** `switch(config-flow-record)# match transport destination-port`	Specifies the transport source or destination port as a key. **Note** The **match transport destination-port** and the **match ip protocol** commands are required to export Layer 4 port data. The data is collected and displayed in the output of the **show hardware flow ip** command but is not collected and exported until you configure both commands.
match datalink {**mac source-address** | **mac destination-address** | **ethertype** | **vlan**} **Example:** `switch(config-flow-record)# match datalink ethertype`	Specifies the Layer 2 attribute as a key.

Specifying the Collect Parameters

You must configure at least one of the following collect parameters for flow records:

Command	Purpose

collect counter {**bytes** | **packets**} [**long**]
Example:
`switch(config-flow-record)#`
`switch(config-flow-record)# collect counter packets`
	Collects either packet-based or byte counters from the flow. You can optionally specify that 64-bit counters are used.

collect flow sampler id **Example:** `switch(config-flow-record)# collect flow sampler`	Collects the sampler identifier used for the flow.
collect timestamp sys-uptime {**first** | **last**} **Example:** `switch(config-flow-record)# collect timestamp sys-uptime last`	Collects the system up time for the first or last packet in the flow.
collect transport tcp flags **Example:** `switch(config-flow-record)# collect transport tcp flags`	Collects the TCP transport layer flags for the packets in the flow.

Command	Purpose
collect ip version **Example:** `switch(config-flow-record)# collect ip version`	Collects the IP version for the flow.

Creating a Flow Exporter

The flow exporter configuration defines the export parameters for a flow and specifies reachability information for remote NetFlow collector.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**flow exporter***name* **Example:** `switch(config)# flow exporter flow-exporter-one`	Creates a flow exporter and enters flow exporter configuration mode. You can enter up to 63 alphanumeric characters for the flow exporter name.
Step 3	**destination** { **ipv4-address** | **ipv6-address**} [**use-vrf** *name*] **Example:** `switch(config-flow-exporter)# destination 192.0.2.1`	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.
Step 4	**source interface-type** *name/port* **Example:** `switch(config-flow-exporter)# source ethernet 2/1`	Specifies the interface to use to reach the NetFlow collector at the configured destination.
Step 5	(Optional) **description** *string* **Example:** `switch(config-flow-exporter)# description exportversion9`	(Optional) Describes this flow exporter. You can enter up to 63 alphanumeric characters for the description.
Step 6	(Optional) **dscp** *value* **Example:** `switch(config-flow-exporter)# dscp 0`	(Optional) Specifies the differentiated services codepoint value. The range is from 0 to 63.

	Command or Action	Purpose
Step 7	(Optional) **transport udp** *port* **Example:** `switch(config-flow-exporter)# transport udp 200`	(Optional) Specifies the UDP port to use to reach the NetFlow collector. The range is from 0 to 65535. **Note** If you do not specify the UDP port, 9995 is selected as the default.
Step 8	**version** {**5** | **9**} **Example:** `switch(config-flow-exporter)# version 9`	Specifies the NetFlow export version. Choose version 9 to enter the flow exporter version 9 configuration submode.
Step 9	(Optional) **option** {**exporter-stats** | **interface-table** | **sampler-table**} **timeout** *seconds* **Example:** `switch(config-flow-exporter-version-9)# option exporter-stats timeout 1200`	Sets the flow exporter statistics resend timer. The range is from 1 to 86400 seconds.
Step 10	(Optional) **template data timeout** *seconds* **Example:** `switch(config-flow-exporter-version-9)# template data timeout 1200`	Sets the template data resend timer. The range is from 1 to 86400 seconds.
Step 11	**exit** **Example:** `switch(config-flow-exporter-version-9)# exit`	Returns to flow exporter configuration mode.
Step 12	**exit** **Example:** `switch(config-flow-exporter)# exit`	Returns to global configuration mode.
Step 13	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Creating a Flow Monitor

You can create a flow monitor and associate it with a flow record and a flow exporter. All 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.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**flow monitor***name* **Example:** `switch(config)# flow monitor flow-monitor-one`	Creates a flow monitor and enters flow monitor configuration mode. You can enter up to 63 alphanumeric characters for the flow monitor name.
Step 3	(Optional) **description** *string* **Example:** `switch(config-flow-monitor)# description IPv4Monitor`	Describes this flow monitor. You can enter up to 63 alphanumeric characters for the description.
Step 4	(Optional) **exporter** *name* **Example:** `switch(config-flow-monitor)# export v9`	Associates a flow exporter with this flow monitor. You can enter up to 63 alphanumeric characters for the exporter name.
Step 5	**record** {*name* **netflow-original** | **netflow protocol-port** | **netflow** {**ipv4** | **ipv6**} {**original-input** | **original-output**}} **Example:** `switch(config-flow-monitor)# record IPv4Flow`	Associates a flow record with the specified flow monitor. You can enter up to 63 alphanumeric characters for the record name.
Step 6	**exit** **Example:** `switch(config-flow-monitor)# exit`	Returns to global configuration mode.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Creating a Sampler

You can create a flow sampler to definer the NetFlow sampling rate for a flow.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`switch# configure terminal` `switch(config)#`	
Step 2	**sampler** *name* **Example:** `switch(config)# sampler testsampler`	Creates a sampler and enters flow sampler configuration mode. You can enter up to 63 alphanumeric characters for the flow sampler name.
Step 3	(Optional) **description** *string* **Example:** `switch(config-flow-sampler)# description samples`	(Optional) Describes this sampler. You can enter up to 63 alphanumeric characters for the description.
Step 4	**mode** *sample-number* **out-of** *packet-number* **Example:** `switch(config-flow-sampler)# mode 1 out-of 128`	Defines the number of samples to take per the number of packets received. The sample-number range is from 1 to 64, and the packet-number range is from 1 to 65536 packets.
Step 5	**exit** **Example:** `switch(config-flow-sampler)# exit`	Returns to global configuration mode.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Applying a Flow Monitor to an Interface

Note You can not apply a flow monitor to an egress interface, only ingress Netflow is supported.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface** *interface-type slot/port* **Example:** `switch(config)# interface ethernet 2/1`	Enters interface configuration mode. The interface type can be Ethernet (including subinterfaces), port channel, or VLAN interface.

	Command or Action	Purpose
Step 3	**ip flow monitor** *name* **input sampler** *name* **Example:** `switch(config-if)# ip flow monitor testmonitor input sampler testsampler`	Associates an IPv4 flow monitor and a sampler to the interface for input packets. You can enter up to 63 alphanumeric characters for the flow monitor name and the sampler name.
Step 4	**ipv6 flow monitor** *name* **input sampler** *name* **Example:** `switch(config-if)# ipv6 flow monitor testmonitorv6 input sampler testsamplerv6`	Associates an IPv6 flow monitor and a sampler to the interface for input packets. You can enter up to 63 alphanumeric characters for the flow monitor name and the sampler name.
Step 5	**layer2-switched flow monitor** *name* **input sampler** *name* **Example:** `switch(config-if)# layer2-switched flow monitor testmonitorl2 input sampler testsamplerl2`	Associates a Layer 2-switched flow monitor and a sampler to the interface for input packets. You can enter up to 63 alphanumeric characters for the flow monitor name and the sampler name.
Step 6	**exit** **Example:** `switch(config-if)# exit`	Returns to global configuration mode.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Configuring Netflow on CoPP Interface Support

You can create a flow record and add keys to match on and nonkey fields to collect in the flow.

Before you begin

Perform the following configuration on the default VDC.

Procedure

Step 1 Enter global configuration mode:

switch# **configure terminal**

Step 2 Enter control-plane configuration mode. Enable users to associate attributes that are associated with the control plane of the device:

switch(config)# **control-plane**

Step 3 Associate an IPv4 flow monitor and a sampler to the control-plane for output packets. You can enter up to 63 alphanumeric characters for the flow monitor name and the sampler name:

switch(config-cp)# **ip flow monitor** *name* **output sampler** *name*

What to do next

You must perform the following tasks to complete configuring Netflow on COPP Interface Support feature:

Creating a Flow Record, on page 360

Creating a Flow Monitor

Creating a Sampler, on page 365

Configuring Bridged NetFlow on a VLAN

You can apply a flow monitor and a sampler to a VLAN.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**vlan configuration** *vlan-id* **Example:** `switch(config)# vlan configuration 30`	Enters VLAN configuration mode. The vlan-id range is from 1 to 3967 or from 4048 to 4093. **Note** VLAN configuration mode enables you to configure VLANs independently of their creation, which is required for VTP client support.
Step 3	{**ip ipv6**} **flow monitor** *name* **input sampler** *name* **Example:** `switch(config-vlan-config)# ip flow monitor testmonitor input sampler testsampler`	Associates a flow monitor and a sampler to the VLAN for input packets. You can enter up to 63 alphanumeric characters for the flow monitor name and the sampler name.
Step 4	**exit** **Example:** `switch(config-vlan-config)# exit`	Returns to global configuration mode.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Configuring Layer 2 NetFlow

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.

Before you begin

Make sure that you are in the correct VDC. To change the VDC, use the **switchto vdc** command.

Procedure

	Command or Action	Purpose

Step 1	**configure t**
	Example:
	`switch# configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
		Enters global configuration mode.

Step 2	Required: **flow record** *name* **Example:** `switch(config)# flow record L2_record`	Enters flow record configuration mode. For more information about configuring flow records, see the "Creating a Flow Record" section.
Step 3	Required: **match datalink** {**mac source-address** | **mac destination-address** | **ethertype** | **vlan**} **Example:** `switch(config-flow-record)# match datalink ethertype`	Specifies the Layer 2 attribute as a key.
Step 4	Required: **interface** {**ethernet** *slotport*} | {**port-channel** *number*} **Example:**	Enters interface configuration mode. The interface type can be a physical Ethernet port or a port channel.

	Command or Action	Purpose
	`switch(config-flow-record)# interface Ethernet 6/3`	
Step 5	Required: **switchport** **Example:** `switch(config-if)# switchport`	Changes the interface to a Layer 2 physical interface. For information about configuring switch ports, see the *Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*.
Step 6	Required: **mac packet-classify** **Example:** `switch(config-if)# mac packet-classify`	Forces MAC classification of packets. For more information about using the mac packet-classify command, see the *Cisco Nexus 7000 Series NX-OS Security Configuration Guide.* **Note** You must use this command to capture flows.
Step 7	Required: **layer2-switched flow monitor** *flow-name* **input** [**sampler** *sampler-name*] **Example:** `switch(config-vlan)# layer2-switched flow monitor L2_monitor input sampler L2_sampler`	Associates a flow monitor and an optional sampler to the switch port input packets. • You can enter up to 63 alphanumeric characters for the flow monitor name and the sampler name.
Step 8	Required: **show flow record netflow layer2-switched input** **Example:** `switch(config-if# show flow record netflow layer2-switched input`	(Optional) Displays information about the Layer 2 NetFlow default record.
Step 9	Required: **copy running-config startup-config** **Example:** `switch(config-vlan)# copy running-config startup-config`	(Optional) Saves this configuration change.

Configuring NetFlow Timeouts

You can optionally configure global NetFlow timeouts that apply to all flows in the system.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal switch(config)#`	Enters global configuration mode.

	Command or Action	Purpose
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.
Step 3	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Verifying the NetFlow Configuration

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

Command	Purpose
show flow exporter [*name*]	Displays information about NetFlow flow exporters and statistics. You can enter up to 63 alphanumeric characters for the flow exporter name.
show flow interface [*interface-type slot/port*]	Displays information about NetFlow interfaces.
show flow record [*name*]	Displays information about NetFlow flow records. You can enter up to 63 alphanumeric characters for the flow record name.
show flow record netflow layer2-switched input	Displays information about the Layer 2 NetFlow configuration.
show flow timeout	Displays information about NetFlow timeouts.
show sampler [*name*]	Displays information about NetFlow samplers. You can enter up to 63 alphanumeric characters for the sampler name.
show hardware ip flow	Displays information about NetFlow hardware IP flows.
show running-config netflow	Displays the NetFlow configuration that is currently on your device.

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 Examples for NetFlow

This example shows how to configure a NetFlow exporter configuration for IPv4 :

```
feature netflow
flow exporter ee
 version 9
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
```

This example shows a NetFlow exporter configuration for IPv4 from the Cisco Nexus 7000 Series switch to NAM:

```
flow exporter pw
  destination 172.20.101.87 use-vrf management
  transport udp 3000
  source mgmt0
  version 9

flow record pw
  match ipv4 source address
  match ipv4 destination address
  match ip protocol
  match ip tos
  match transport source-port
  match transport destination-port
  collect counter bytes long
  collect counter packets long
  collect timestamp sys-uptime first
  collect timestamp sys-uptime last
  collect ip version

flow monitor pw
  record pw
  exporter pw

interface Ethernet2/9
  ip flow monitor pw input
  ip flow monitor pw output
```

Verification Examples for NetFlow CoPP Interface Support

Sample Output for the show hardware flow ip Command

```
 switch(config-if)# show hardware flow ip

D - Direction; L4 Info - Protocol:Source Port:Destination Port
```

```
IF - Interface: (Eth)ernet, (S)vi, (V)lan, (P)ortchannel, (T)unnel
TCP Flags: Ack, Flush, Push, Reset, Syn, Urgent

D  IF          SrcAddr         DstAddr         L4 Info         PktCnt     TCP Fl
--+-----------+---------------+---------------+---------------+----------+------
CP sup-eth1    010.014.014.002 010.014.014.001 001:00000:00000 0000000021 ......
```

Sample Output for the show running-configuration netflow Command

```
 switch# show running-configuration netflow

version 7.3(0)D1(1)

feature netflow

flow timeout active 60
flow exporter exp1
  destination 10.76.80.132 use-vrf management
  transport udp 9995
  source mgmt0
  version 9
    template data timeout 5
    option sampler-table timeout 8
sampler s3
  mode 2 out-of 3
flow monitor M2
  record netflow ipv4 original-input
  exporter exp1
control-plane
  ip flow monitor M2 output sampler s3
```

Related Documents

Related Topic	Related Topic
NetFlow CLI commands	*Cisco Nexus 7000 Series NX-OS System Management Command Reference*
VDCs and VRFs	*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*
Cisco Network Analysis Module (NAM)	*Cisco Network Analysis Module (NAM) for Nexus 7000 Quick Start Guide*
Cisco NetFlow Generation Appliance (NGA)	*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*

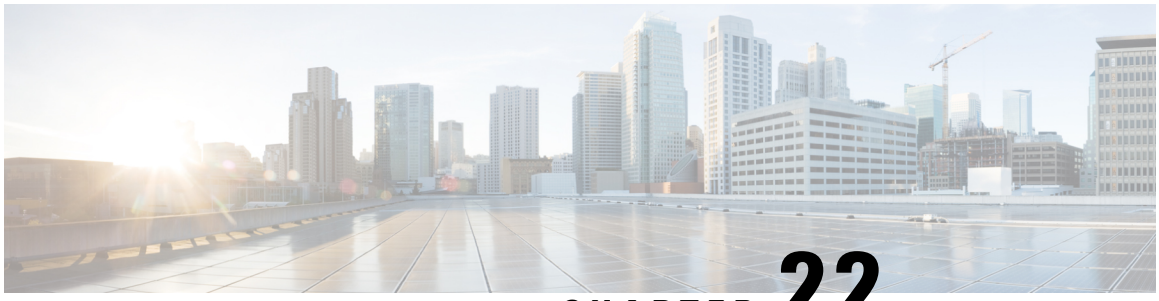
Feature History for NetFlow

Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Table 39: Feature History for NetFlow

Feature Name	Releases	Feature Information
NetFlow	8.0(1)	The first switched and the last switched sizes are changed to 8 bytes (from 4 bytes).
NetFlow	7.3(2)D1(2)	The first switched and the last switched sizes are changed to 8 bytes (from 4 bytes).
NetFlow	7.3(0)DX(1)	Added support for NetFlow on M3 Series modules.
NetFlow	7.3(0)D1(1)	Added Netflow on CoPP Interface support.
NetFlow	7.2(0)D1(1)	Enhanced the F3 Series module packet processing rate to 50000 pps.
NetFlow	6.2(6)	Added support for F3 Series modules.
NetFlow	6.2(2)	Added support for ingress NetFlow sampling and DHCPrelay to be configured on the same interface.
NetFlow	6.2(2)	Added NAM support for NetFlow data sources.
NetFlow	6.2(2)	Added support for full NetFlow and sampled NetFlow on the Cisco NetFlow Generation Appliance (NGA).
NetFlow	6.1(2)	Added support for sampled NetFlow on F2 Series and F2eSeries modules.
NetFlow	6.1(2)	Added the flow timeout seconds command for F2 Series and F2e Series modules.
NetFlow	6.0(1)	NetFlow is not supported on F2 Series modules.
NetFlow	6.0(1)	Added support for the collect routing forwarding-status command to trigger the collection of flows denied by ACL entries.
NetFlow	5.2(1)	NetFlow is supported on switch virtual interfaces (SVIs) for F1 Series ports.

Bridged NetFlow	5.1(1)	VLAN configuration mode, which enables you to configure VLANs independently of their creation, is supported when configuring bridged NetFlow on a VLAN.
NetFlow verification	5.0(2)	You can specify the NetFlow instance for which you want to display NetFlow IPv4 flows and NetFlow table utilization.
Layer 2 NetFlow	4.2(1)	You can define Layer 2 keys in flexible NetFlow records that you can use to capture flows in Layer 2 interfaces.
Rollback during NetFlow	4.1(3)	Rollback fails for NetFlow if, during rollback, you try to modify a record that is programmed in the hardware.



CHAPTER 22

Configuring EEE

This chapter describes how to configure Energy Efficient Ethernet (EEE) on Cisco NX-OS devices.

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “New and Changed Information” chapter or the Feature History table.

Information About EEE

EEE

Energy Efficient Ethernet (EEE) is an IEEE 802.3az standard that is designed to reduce power consumption in Ethernet networks during idle periods. EEE can be enabled on devices that support low power idle (LPI) mode. Such devices can save power by entering LPI mode during periods of low utilization. In LPI mode, systems on both ends of the link can save power by shutting down certain services. EEE provides the protocol needed to transition into and out of LPI mode in a way that is transparent to upper layer protocols and applications.

EEE LPI Sleep Threshold

The EEE LPI sleep threshold specifies how long an interface should wait to go to sleep after detecting an idle state. You can configure the threshold to be aggressive or nonaggressive.

EEE Latency

The EEE latency specifies the EEE delay that is added to your traffic. The default value is a constant latency of 6 microseconds.

Virtualization Support

By default, Cisco NX-OS places you in the default virtual device context (VDC) unless you specifically configure another VDC. For more information about VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*.

Prerequisites for EEE

EEE has the following prerequisites:

- To configure VDCs, you must install the appropriate license. See the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide* for configuration information and the *Cisco NX-OS Licensing Guide* for licensing information.

Guidelines and Limitations

Guidelines and Limitations:

- Only F2e (enhanced) copper port modules support EEE. F2e fiber port modules do not support EEE
- EEE is supported only for 10-Gigabit link speeds. It is not supported for 1-Gigabit link speeds.
- Changing the EEE configuration resets the interface because the device has to restart Layer 1 autonegotiation.
- You might want to enable the Link Layer Discovery Protocol (LLDP) for devices that require longer wakeup times before they are able to accept data on their receive paths. Doing so enables the device to negotiate for extended system wakeup times from the transmitting link partner.

Default Settings

Lists the default settings for EEE parameters.

Table 40: Default EEE Parameters

Parameters	Default

EEE	Disabled
EEE LPI sleep threshold	Nonaggressive
EEE latency	6 microseconds

Configuring EEE

This section includes the following topics:

- Enabling or Disabling EEE
- Configuring the EEE LPI Sleep Threshold

Enabling or Disabling EEE

You can enable or disable EEE on an interface that is connected to an EEE-capable link partner.

Before you begin

Make sure that you are in the correct VDC. To change the VDC, use the **switchto vdc** command.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Places you in global configuration mode.
Step 2	switch(config)# **interface ethernet** *slot/port*	Enters global configuration mode.
Step 3	switch(config-if)# [**no**] **power efficient-ethernet auto**	Enables or disables EEE on the specified interface. When EEE is enabled, the device advertises and auto negotiates EEE to its link partner.
Step 4	(Optional) switch(config-if)# **show interface ethernet** *slot/port*	Displays the EEE status on the interface.
Step 5	(Optional) switch(config)# **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Configuring the EEE LPI Sleep Threshold

You can configure the EEE LPI sleep threshold on an interface to specify how aggressively you want it to go to sleep

Before you begin

Make sure that you are in the correct VDC. To change the VDC, use the **switchto vdc** command.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Places you in global configuration mode.
Step 2	switch(config)# **interface ethernet** *slot/port*	Enters global configuration mode.
Step 3	switch(config-if)# [**no**] **power efficient-ethernet sleep threshold aggressive**	Configures the EEE LPI sleep threshold on the interface to be aggressive or nonaggressive. The no form of this command enables the nonaggressive threshold. • Aggressive—Causes the device to enter LPI mode after 20 microseconds of detecting an idle state. • Nonaggressive—Causes the device to enter LPI mode after 600 microseconds of detecting an idle state.
Step 4	(Optional) switch(config)# **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Verifying the EEE Configuration

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

Table 41: EEE on an Ethernet interface

Command	Purpose
show environment power detail	Displays the current power usage.
show interface ethernet *slot/port*	Displays the EEE status on the interface. The options are as follows: • N/A—The interface is not capable of EEE. • Disabled—EEE is disabled on this interface. • Disagreed—EEE autonegotiation with the link partner has failed • Operational—EEE is enabled and operational on this interface.
show interface ethernet *slot/port* **capabilities**	Displays whether the interface is EEE capable.

show interface ethernet *slot/port* **counters detailed**	Displays the following EEE statistics on the interface: • Tx LPI usecs—The amount of time (in microseconds) that the transmitting link partner waits before it starts transmitting data after leaving LPI mode. • Rx LPI usecs—The amount of time (in microseconds) that the receiving link partner requests that the transmitting link partner wait before transmitting data after leaving LPI mode. • Tx LPI requests—The number of times that the transmitting link partner makes a request to enter LPI mode. • Rx LPI indications—The number of times the receiving link partner detects that the transmitting link partner has entered LPI mode.

Configuration Examples for EEE

Example

This example shows how to enable EEE on an Ethernet interface:

```
switch# config t
switch(config)# interface ethernet 7/1
switch(config-if)# power efficient-ethernet auto
switch(config-if)# power efficient-ethernet sleep threshold aggressive
switch(config-if)# show interface ethernet 7/1
Ethernet7/1 is up
   EEE(efficient-ethernet): Operational
```

Related Documents

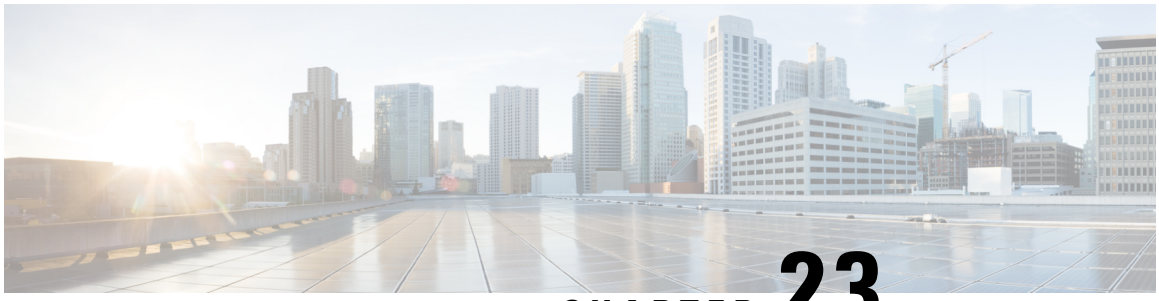
Related Topic	Document Title
EEE CLI commands	*Cisco Nexus 7000 Series NX-OS System Management Command Reference*
VDCs	*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*

Feature History for EEE

Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Table 42: Feature History for EEE

Feature Name	Releases	Feature Information
EEE	6.1(2)	This feature was introduced.



CHAPTER 23

Configuring GIR (Cisco NX-OS Release 7.3(0)D1(1) and later releases)

This chapter includes the following sections:

Information About GIR

You can use Graceful Insertion and Removal (GIR) to put a switch in maintenance mode in order to perform debugging or an upgrade. When switch maintenance is complete, you can return the switch to normal mode.

When you place the switch in maintenance mode, all protocols are isolated from the network. When normal mode is restored, all the protocols are brought back up.

In Cisco NX-OS 7.2(0)D1(1) release, the default mode for GIR is "**shutdown**". When you place the switch in maintenance mode, all protocols are gracefully brought down and all physical ports are shut down. When normal mode is restored, all the protocols and ports are brought back up. The following protocols are supported:

- Border Gateway Protocol (BGP)
- BGPv6
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- EIGRPv6
- Intermediate System-to-Intermediate System (ISIS)

- ISISv6
- Open Shortest Path First (OSPF)
- OSPFv3
- RIP

Also supported are:

- Virtual port channel (vPC) switches

Note GIR is not supported on vPC+ switches.

- Interfaces
- FabricPath

Starting with Cisco NX-OS Release 7.3(0)D1(1), the default mode for GIR is "**isolate**". Use the **system mode maintenance** command to put all the enabled protocols in maintenance mode. The switch will use the **isolate** command to isolate the protocols from the network. The switch will then be isolated from the network but is not shut down. Routing protocols will be running on the switch to maintain neighborship with peer switches when it is isolated from the network. The **isolate** command is applied on the protocol instance and is applicable for the following protocols:

- Border Gateway Protocol (BGP)
- BGPv6
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- EIGRPv6
- Intermediate System-to-Intermediate System (ISIS)
- ISISv6
- Open Shortest Path First (OSPF)
- OSPFv3
- FabricPath (Only applicable for Spine switches)

Note

- You can use the **system mode maintenance shutdown** command to use the "**shutdown**" mode for GIR as in the Cisco NX-OS Release 7.2(0)D1(1).
- When you cold boot a switch that has custom profile configured and is running a Cisco NX-OS Release 7.3(1)D1(1) image to any other Cisco NX-OS Release that does not support maintenance mode, the same configuration file cannot be used after write-erase reload.
- In normal mode, the processing of protocols will happen in an order that is the reverse of the order in which the protocols are processed in maintenance mode. Similarly, in maintenance mode, the processing of protocols will happen in an order that is the reverse of the order in which the protocols are processed in normal mode.
- A syslog message is generated when the switch moves to maintenance mode from normal mode and vice-versa.

Maintenance Profile

Maintenance profile contains a set of commands that will be applied sequentially during graceful removal or graceful insertion.

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.

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.

System-generated Profile

You can allow the system to generate a maintenance-mode or normal-mode profile with specific configuration commands. The system generates a maintenance-mode profile when you use the **system mode maintenance** command or a normal-mode profile when you use the **no system mode maintenance** command.

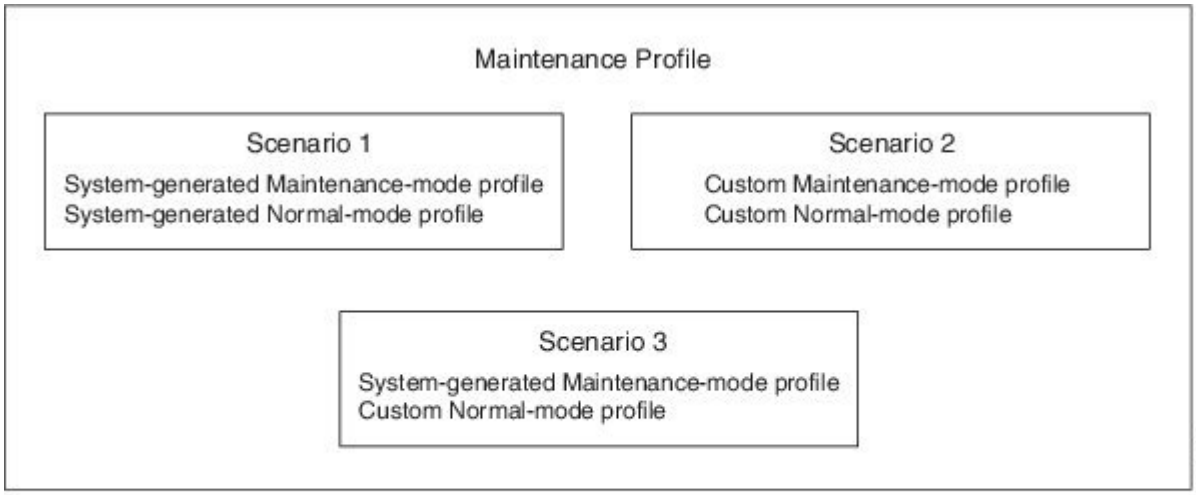
Custom Profile

You can create a custom maintenance-mode or normal-mode profile with configuration commands that can be applied during graceful removal or graceful insertion to isolate, shut down, or restore the protocols individually (or perform additional configurations). You can use a custom profile when the system-generated profile does not provide the required configuration or if you need to enhance the existing system-generated or custom profile to include additional functionality specific to your deployment. Use the **configure maintenance profile maintenance-mode** command to configure a custom maintenance-mode profile with the required commands or the **configure maintenance profile normal-mode** command to configure a custom normal-mode profile with the required commands.

The system-generated profile will overwrite the custom profile and vice-versa. The system can have either a system-generated maintenance-mode profile or a custom maintenance-mode profile at a time. Similarly, the

system can have either a system-generated normal-mode profile or a custom normal-mode profile at a time. The scenarios are as given in the figure below:

Figure 7: Maintenance Profile Scenarios



Note We recommend using Scenario 1 or 2.

Unplanned Maintenance

You can put the switch in unplanned maintenance mode when the switch reloads due to a critical failure. For switches with a single supervisor, configure a reset reason CLI using the **system mode maintenance on-reload reset-reason** command to enable the switch to go into maintenance mode after a switch reloads due to a critical failure. For switches with dual supervisors, SUP switchover occurs when there is a critical failure of the switch and the switch will not go into maintenance mode. The maintenance-mode profile existing in the startup configuration is applied when the switch goes in to unplanned maintenance mode. If no maintenance mode profile exists in the startup configuration, a system-generated maintenance-mode profile is created and applied when the switch goes in to unplanned maintenance mode.

Maintenance Mode Timer

Use the **system mode maintenance timeout** command before entering maintenance mode to keep the switch in maintenance mode for a specified number of minutes. You can also use this command while the switch is in maintenance mode to change the number of minutes for which the switch will be in maintenance mode. The timer will then restart from that instant with the new timer value. Once the configured time elapses, the switch returns to normal mode automatically without using the **no system mode maintenance mode** command. Use the **no system mode maintenance timeout** command to disable the timer.

Snapshot

Use the **snapshot** command to capture the running states of selected features and to store the running states on the persistent storage media.

You can use snapshots to compare the state of a switch before it went into maintenance mode and after it came back to normal mode. 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 summary and details of each feature.

There are two types of snapshots:

- System-generated snapshot—This is generated by the system when you use the **[no] system mode maintenance** command. The system creates the before_maintenance snapshot just before the system goes into maintenance mode. The system creates the after_maintenance snapshot just before the system goes into normal mode. The system overwrites any old snapshots when you use the **[no] system mode maintenance** command. Use the **snapshot delete** {**all** | *snapshot-name*} command to delete the system-generated snapshots.

  In certain scenarios, the system-generated after_maintenance snapshot may be taken when hardware programming is ongoing. In such cases, we recommend taking a user-generated snapshot after the system has completed hardware programming and is in a stable state. You can then compare the new after_maintenance snapshot with the before_maintenance snapshot.

  Starting with Cisco NX-OS release 8.0(1), the **[no] system mode maintenance** command has been enhanced to execute a normal mode profile and activate a timer ensuring that sufficient time is provided for the switch to complete any hardware programming that may be going on before the after_maintenance snapshot is taken. Once the timer expires, the after_maintenance snapshot is taken in the background and a new warning syslog message, MODE_SNAPSHOT_DONE, is sent after the snapshot is complete. The default delay timer value is 120 seconds. The output of the **[no] system mode maintenance** command displays the delay timer value, in seconds, after which 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
  ```

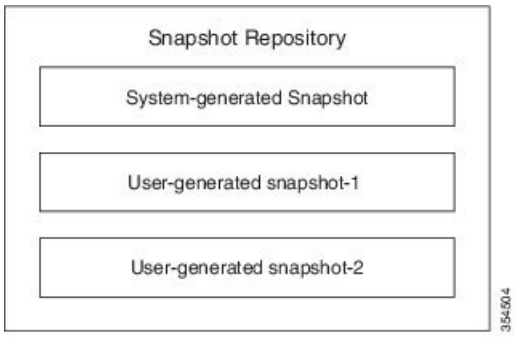
  Use the **system mode maintenance snapshot-delay** [*delay-in-seconds*] command to change the delay timer value. The delay timer range is from 0 to 65535.

  Use the **show maintenance snapshot-delay** command to display the snapshot delay timer value.

- User-generated snapshot—Use the **snapshot create** *name description* command to create a user-generated snapshot. Use the**snapshot delete** {**all** | *snapshot-name*} command to delete user-generated snapshots.

The system-generated and user-generated snapshots are stored in the snapshot repository.

Figure 8: Snapshot Repository



The following table lists the snapshot sections with the corresponding show commands:

Name of the Section	Corresponding 'show' command
bgp-sessions	show bgp sessions vrf all
eigrp	show ip eigrp topology summary
eigrpv6	show ipv6 eigrp topology summary
interface	show interface
ospf	show ip ospf vrf all
ospfv3	show ipv6 ospfv3 vrf all
isis	show isis database detail vrf all
rip	show ip rip vrf all
route-summary	show ip route summary vrf all
routev6-summary	show ipv6 route summary vrf all
vpc	show vpc

Suppress FIB Pending

The Suppress Forwarding Information Base (FIB) Pending feature uses the Border Gateway Protocol-Routing Information Base (BGP-RIB) and the Enhanced Interior Gateway Routing Protocol-Routing Information Base (EIGRP-RIB) feedback mechanism to avoid premature route advertisements and subsequent packet loss in a network. This mechanism is enabled by default and ensures that routes are installed locally before they are advertised to a neighbor.

BGP and EIGRP wait for feedback from RIB indicating that the routes that EIGRP or BGP installed in the RIB are installed in the FIB before EIGRP or BGP sends out updates to the neighbors. EIGRP or BGP will

send out updates of only those routes that have versions up to the version that FIB has installed. This selective update ensures that EIGRP or BGP does not send out premature updates resulting in attracting traffic even before the data plane is programmed after a switch reload, line card reload, or when the switch moves to normal mode from maintenance mode.

GIR SNMP Traps

Starting with Cisco NX-OS Release 8.0(1), support for Simple Network Management Protocol (SNMP) traps has been added to the Graceful Insertion and Removal (GIR) mechanism. You can enable the switch to send an SNMP trap notification when the switch moves from normal mode to maintenance mode and vice-versa. Use the **snmp-server enable traps mmode cseMaintModeChangeNotify** command to enable the switch to send an SNMP trap notification when the switch moves to maintenance mode. Use the **snmp-server enable traps mmode cseNormalModeChangeNotify** command to enable the switch to send an SNMP trap notification when the switch moves to normal mode. By default, both SNMP traps are disabled.

Guidelines and Limitations for GIR

- Custom maintenance profile has to be used for custom topologies and protocols that are not supported by automatic or system-generated profiles.
- Before starting with maintenance, ensure that the switch is not attracting any data traffic after the switch has been put in maintenance mode. You can use counters and statistics to ensure that there is no data traffic on the switch.
- Use the **system mode maintenance always-use-custom-profile** command when using custom profiles to ensure that the custom profile is not overwritten by the system-generated profile.
- Snapshot information is not copied automatically to the standby supervisor in a dual supervisor system.
- GIR may not provide zero application traffic loss for certain topologies and configurations.
- Starting with Cisco NX-OS Release 7.3(0)D1(1), we recommend not using the **configure profile [maintenance-mode | normal-mode] type admin** command and we strongly recommend using the **configure maintenance profile [maintenance-mode | normal-mode]** command.
- You cannot perform an in-service software upgrade (ISSU) or an in-service software downgrade (ISSD) in maintenance mode.

Configuring Custom Maintenance Mode and Custom Normal Mode Profile

You can create the maintenance-mode profile or normal-mode profile with configuration commands that can be applied during graceful removal or graceful insertion. We recommend using the **system mode maintenance always-use-custom-profile** command after configuring custom maintenance mode and custom normal mode profiles to ensure that custom profiles are always used during maintenance mode operations.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure maintenance profile** [**maintenance-mode** | **normal-mode**]	Enters a configuration session for the maintenance-mode profile or the normal-mode profile. **Note** Depending on which protocols you have configured, enter the appropriate commands to bring down the protocols.
Step 2	Required: switch# **end**	Closes the maintenance mode profile.

Example

This example shows how to create a custom maintenance mode profile:

```
switch# configure maintenance profile maintenance-mode
Please configure 'system mode maintenance always-use-custom-profile' if you want to use
custom profile always for maintenance mode.
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-mm-profile)# router bgp 100
switch(config-mm-profile-router)# isolate
switch(config-mm-profile-router)# exit
switch(config-mm-profile)# sleep instance 1 10
switch(config-mm-profile)# interface ethernet 1/1
switch(config-mm-profile-if-verify)# shutdown
switch(config-mm-profile-if-verify)# end
Exit maintenance profile mode.
```

This example shows how to create a custom normal mode profile:

```
switch# configure maintenance profile normal-mode
Please configure 'system mode maintenance always-use-custom-profile' if you want to use
custom profile always for maintenance mode.
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-mm-profile)# interface ethernet 1/1
switch(config-mm-profile-if-verify)# no shutdown
switch(config-mm-profile-if-verify)# exit
switch(config-mm-profile)# sleep instance 1 20
switch(config-mm-profile)# router bgp 100
switch(config-mm-profile-router)# no isolate
switch(config-mm-profile-router)# end
Exit maintenance profile mode.
```

```
switch# show maintenance profile
[Normal Mode]
interface Ethernet1/1
no shutdown
sleep instance 1 20
router bgp 100
no isolate
[Maintenance Mode]
router bgp 100
isolate
```

```
sleep instance 1 20
interface Ethernet1/1
shutdown
```

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.

Procedure

	Command or Action	Purpose
Step 1	switch# **snapshot create** *name description*	Creates a snapshot. The *name* variable can be 64 characters in length. The *description* variable can be 256 characters in length. Use the **snapshot delete** {**all** | *snapshot-name*} command to delete all snapshots or a specific snapshot.
Step 2	(Optional) switch# **show snapshots**	Displays snapshots present on the switch.
Step 3	(Optional) switch# **show snapshots compare** *snapshot-name-1 snapshot-name-2* [**summary**]	Displays a comparison of two snapshots. The **summary** keyword displays just enough information to see the overall changes between the two snapshots.

Example

This example shows how to create a snapshot:

```
switch# snapshot create before_maint taken before maint
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
Executing 'show vpc'... Done
Executing 'show ip ospf vrf all'... Done
Feature 'ospfv3' not enabled, skipping...
Executing 'show isis database detail vrf all'... Done
Executing 'show ip rip vrf all'... Done
Executing user-specified 'show ip route detail vrf all'... Done
Snapshot 'before_maint' created
```

This example shows how to display the snapshots present on the switch:

```
switch# show snapshots
Snapshot Name           Time                         Description
--------------------------------------------------------------------------------
before_maint            Wed Oct 14 10:56:50 2015       taken before maint
```

This example displays a comparison between two snapshots:

```
switch# show snapshots compare before_maintenance after_maintenance summary
================================================================================
Feature changed                        before_maintenance after_maintenance
================================================================================
basic summary
   # of interfaces                          50              50
   # of vlans                               0               0
   # of ipv4 routes  vrf default            13              13
   # of ipv4 paths   vrf default            13              13
   # of ipv4 routes  vrf management         14              14
   # of ipv4 paths   vrf management         14              14
   # of ipv6 routes  vrf default            3               3
   # of ipv6 paths   vrf default            3               3

interfaces
   # of eth interfaces                      48              48
   # of eth interfaces up                   1               1
   # of eth interfaces down                 47              47
   # of eth interfaces other                0               0

   # of vlan interfaces                     0               0
   # of vlan interfaces up                  0               0
   # of vlan interfaces down                0               0
   # of vlan interfaces other               0               0
```

This example shows how to delete a snapshot:

```
switch# snapshot delete before_maint
switch# show snapshots
Snapshot Name           Time                            Description
--------------------------------------------------------------------------------
```

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

	Command or Action	Purpose
Step 1	switch# **snapshot section add** *section "show-command" row-id element-key1* [*element-key2*]	Adds a user-specified section to snapshots. The *section* variable 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*

	Command or Action	Purpose
		argument needs to be specified to be able to distinguish among row entries. **Note** To delete a user-specified section from snapshots, use the **snapshot section delete** *section* section command.
Step 2	(Optional) switch# **show snapshots sections**	Displays the user-specified snapshot sections.

Example

The following example shows how to add the **show ip route detail vrf all** command to the snapshot:

```
switch# snapshot section add v4route "show ip route detail vrf all" ROW_prefix ipprefix
switch# show snapshots sections
user-specified snapshot sections
--------------------------------
[v4route]
show command: show ip route detail vrf all
row id: ROW_prefix
key1: ipprefix
key2: -
```

The following example shows how to add the **show ipv6 route detail vrf all** command to the snapshot:

```
switch# snapshot section add routev6 "show ipv6 route detail vrf all" ROW_prefix ipprefix
added section "routev6"

switch# show snapshots sections
user-specified snapshot sections
--------------------------------
[routev6]
show command: show ipv6 route detail vrf all
row id: ROW_prefix
key1: ipprefix
key2: -
```

The following example shows how to delete a user-specified snapshot section:

```
switch# snapshot section delete v4route
deleted section ”v4route"

switch# show snapshots sections
user-specified snapshot sections
--------------------------------
none
```

The following example displays the XML output of the **show ip route detail vrf all** command:

```
switch(config)# show ip route detail vrf all | xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="http://w
ww.cisco.com/nxos:7.3.0.D1.1.:urib">
 <nf:data>
  <show>
   <ip>
```

```
<__readonly__>
  <TABLE_vrf>
   <ROW_vrf>
    <vrf-name-out>default</vrf-name-out>
    <TABLE_addrf>
     <ROW_addrf>
      <addrf>ipv4</addrf>
      <TABLE_prefix>
       <ROW_prefix>
        <ipprefix>0.0.0.0/32</ipprefix>
        <ucast-nhops>1</ucast-nhops>
        <mcast-nhops>0</mcast-nhops>
        <attached>false</attached>
       … <snip>
       </ROW_prefix>
```

Dumping Snapshot Sections

Procedure

	Command or Action	Purpose
Step 1	switch# **show snapshots dump** *snapshot-name*	Displays the content of the various sections in a generated snapshot.

Example

The following example shows how to dump content of the various sections in a generated snapshot:

```
switch# show snapshots dump new
File:  interface.xml        Snapshot:  new
================================================================================
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="http://w
ww.cisco.com/nxos:7.3.0.D1.1.:if_manager">
 <nf:data>
  <show>
   <interface>
    <__readonly__>
     <TABLE_interface>
      <ROW_interface>
       <interface>mgmt0</interface>
       <state>up</state>
       <admin_state>up</admin_state>
       <eth_hw_desc>GigabitEthernet</eth_hw_desc>
       <eth_hw_addr>5cfc.666d.3b34</eth_hw_addr>
       <eth_bia_addr>5cfc.666d.3b34</eth_bia_addr>
       <eth_ip_addr>5.24.100.101</eth_ip_addr>
       <eth_ip_mask>16</eth_ip_mask>
       <eth_ip_prefix>5.24.0.0</eth_ip_prefix>
       <eth_mtu>1500</eth_mtu>
    … <snip> …
```

Entering Maintenance Mode

If you are going to create your own profile rather than using the system mode maintenance command to do it for you, see the Configuring Custom Maintenance Mode and Custom Normal Mode Profile section.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	Required: switch(config)# **system mode maintenance** [**always-use-custom-profile** |**dont-generate-profile** |**non-interactive** |**on-reload reset-reason** *reason* |**shutdown** | **snapshot-delay** *delay-in-seconds*|**timeout** *value*]	Puts all enabled protocols in maintenance mode (using the **isolate** command). Use the **dont-generate-profile** and **shutdown** options to put the switch in maintenance mode. • **dont-generate-profile**—Prevents the dynamic searching of enabled protocols and executes commands configured in a maintenance mode profile. Use this option if you want the system to execute commands in a custom maintenance mode profile. • **shutdown**—Shuts down all protocols and interfaces except the management interface (using the **shutdown** command). This option is disruptive while the default (using the **isolate** command) is not. The **on-reload reset-reason**, **timeout** and **always-use-custom-profile** options are used to configure maintenance mode parameters and will not put the switch in maintenance mode. • **timeout** *value*—Keeps the switch in maintenance mode for a specified number of minutes. The range is from 5 to 65535. We recommend setting the timeout value to at least 60 minutes. Once the configured time elapses, the switch returns to normal mode automatically. The **no system mode maintenance timeout** command disables the timer • **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

	Command or Action	Purpose
		event of a system crash. The maintenance mode reset reasons are as follows: • HW_ERROR—Hardware error • SVC_FAILURE—Critical service failure • KERN_FAILURE—Kernel panic • WDOG_TIMEOUT—Watchdog timeout • FATAL_ERROR—Fatal error • MANUAL_RELOAD---Manual reload • MAINTENANCE—Reloads the switch in maintenance mode if the switch was already in maintenance mode before reload. • MATCH_ANY—Any of the above reasons • ANY_OTHER—Any reload reason not specified above. The system prompts you to continue. Enter y to continue or n to terminate the process. **Note** We recommend configuring the reset reason and saving it to the startup configuration. This enables the switch to go into the maintenance mode after a switch reloads due to any reason. • **always-use-custom-profile**—Use this option to apply the existing custom maintenance mode profile and prevent creation of autogenerated maintenance mode profile. This option forces the dont-generate-profile option to be used even if it has not been specified using the **system mode maintenance** command. You cannot use the "shutdown" option when this option is being used. Starting from Cisco NX-OS Release 8.0(1), the following keywords were introduced:

	Command or Action	Purpose
		• **non-interactive**—Use this option to put the switch in maintenance mode without presenting any switch prompts. • **snapshot-delay** *delay-in-seconds*—Use this option to change the snapshot delay timer value. The default snapshot delay timer value is 120 seconds. The range is from 0 to 65535.
Step 3	(Optional) switch# **show system mode**	Displays the current system mode. This command also displays the current state of the maintenance mode timer when the switch is in maintenance mode.

Example

Note Starting with Cisco NX-OS Release 8.0(1), a visible CLI indicator has been added to show that the system is in maintenance mode. For example, switch(config)# will appear as switch(maint-mode)(config)#.

This example shows how to put all the protocols in maintenance mode using the **system mode maintenance** command on a switch running the Cisco NX-OS Release 8.0(1):

```
switch# configure terminal
switch(config)# system mode maintenance
Following configuration will be applied:

router bgp 100
  isolate
router ospf 100
  isolate
router isis 100
  isolate

Do you want to continue (y/n)? [no] y

Generating before_maintenance snapshot before going into maintenance mode

Starting to apply commands...

Applying : router bgp 100
Applying :   isolate
Applying : router ospf 100
Applying :   isolate
Applying : router isis 100
Applying :   isolate

Maintenance mode operation successful.
switch(maint-mode)(config)# 2016 Dec  5 06:19:13 switch %$ VDC-1 %$ %MMODE-2-MODE_CHANGED:
 System changed to "maintenance" mode.

switch(maint-mode)(config)#
```

This example shows how to put all the protocols in maintenance mode using the **system mode maintenance** command on a switch running the Cisco NX-OS Release 7.3(0)D1(1):

```
switch# configure terminal
switch(config)# system mode maintenance
Following configuration will be applied:

router bgp 100
  isolate
router ospf 100
  isolate
router isis 100
  isolate

Do you want to continue (y/n)? [no] y

Generating a snapshot before going into maintenance mode

Starting to apply commands...

Applying : router bgp 100
Applying :   isolate
Applying : router ospf 100
Applying :   isolate
Applying : router isis 100
Applying :   isolate

Maintenance mode operation successful.
```

This example shows how to shut down all protocols and interfaces on the switch:

```
switch# configure terminal
switch(config)# system mode maintenance shutdown
Following configuration will be applied:

router bgp 64581
  shutdown
router eigrp p2
  shutdown
  address-family ipv6 unicast
    shutdown
router eigrp 0
  shutdown
  address-family ipv6 unicast
    shutdown
router ospf 200
  shutdown
router isis 70
  shutdown
vpc domain 2
  shutdown
system interface shutdown

NOTE: 'system interface shutdown' will shutdown all interfaces excluding mgmt 0
Do you want to continue (yes/no)? [no] yes

Generating a snapshot before going into maintenance mode

Starting to apply commands...

Applying : router bgp 64581
Applying :   shutdown
Applying : router eigrp p2
Applying :   shutdown
```

```
Applying :   address-family ipv6 unicast
Applying :     shutdown
Applying : router eigrp 0
Applying :   shutdown
Applying :   address-family ipv6 unicast
Applying :     shutdown
Applying : router ospf 200
Applying :   shutdown
Applying : router isis 70
Applying :   shutdown
Applying : vpc domain 2
Applying :   shutdown2016 Jan 15 11:10:36.080386 CP-BL26-N7K-1A %$ VDC-1 %$
%VPC-2-VPC_SHUTDOWN: vPC shutdown status is ON

Applying : system interface shutdown

Maintenance mode operation successful.
switch(config)# 2016 Jan 15 11:10:42.057678 switch %$ VDC-1 %$ %MMODE-2-MODE_CHANGED: System
 changed to "maintenance" mode.
2016 Jan 15 11:10:42.058167 switch %$ VDC-1 %$ %MMODE-2-MODE_CHANGE_WARN: System will be
moved to "normal" mode in 5 minutes
```

This example shows how to keep the switch in maintenance mode for a specific number of minutes:

```
switch# configure terminal
switch (config)# system mode maintenance timeout 25

switch# show system mode
System Mode: Maintenance
Maintenance Mode Timer: 24 minutes 55 seconds remaining
```

This example shows how to automatically boot the switch into maintenance mode if a fatal error occurs:

```
switch# configure terminal
switch(config)# system mode maintenance on-reload reset-reason fatal_error
```

This example shows how to place the switch in maintenance mode by using a previously created maintenance mode profile :

```
switch# configure terminal
switch(config)# system mode maintenance dont-generate-profile

Following configuration will be applied:

router bgp 100
  isolate
sleep instance 1 10
interface Ethernet1/1
  shutdown

Do you want to continue (y/n)? [no] y

Generating a snapshot before going into maintenance mode

Starting to apply commands...

Applying : router bgp 100
Applying :   isolate
Applying : sleep instance 1 10
Applying : interface Ethernet1/1
Applying :   shutdown
```

```
Maintenance mode operation successful.
```

This example shows how to apply the existing custom maintenance mode profile and prevent creation of auto-generated maintenance mode profile:

```
switch# configure terminal
switch(config)# system mode maintenance always-use-custom-profile
```

This example shows how to put the switch in maintenance mode without presenting any switch prompts:

```
switch# configure terminal
switch(config)# system mode maintenance non-interactive
System mode switch to maintenance mode started. Will continue in background.
switch(config)# 2016 Dec  5 08:46:42 switch %$ VDC-1 %$ %MMODE-2-MODE_CHANGED: System changed
 to "maintenance" mode.

switch(maint-mode)(config)#
```

This example shows how to change the snapshot delay timer value:

```
switch# configure terminal
switch(config)# system mode maintenance snapshot-delay 150
```

Returning to Normal Mode

Note Starting with Cisco NX-OS Release 8.0(1), a visible CLI indicator has been added to show that the system is in maintenance mode. For example, switch(config)# will appear as switch(maint-mode)(config)#.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	Required: switch# **no system mode maintenance** [**dont-generate-profile** | **non-interactive**]	Executes a previously created normal mode profile file or a dynamically created normal mode profile file. The **dont-generate-profile** keyword suppresses the creation of the normal mode maintenance profile and also prevents reusing the existing normal mode maintenance profile. The **non-interactive** keyword enables the switch to exit the maintenance mode without presenting any switch prompts. The system prompts you to continue. Enter **y** to continue or **n** to terminate the process. Starting from Cisco NX-OS Release 8.0(1), the **non-interactive** keyword was introduced. The **non-interactive** keyword puts the switch in

	Command or Action	Purpose
		normal mode from maintenance mode without presenting any switch prompts. **Note** For large configurations, the interfaces will be up after a certain interval of time.

Example

This example shows how to return to normal mode from maintenance mode on a switch running the Cisco NX-OS Release 8.0(1):

```
 switch(maint-mode)(config)# no system mode maintenance
Following configuration will be applied:

interface Ethernet1/1
  no shutdown
sleep instance 1 20
router bgp 100
  no isolate

Do you want to continue (y/n)? [no] yes

Starting to apply commands...

Applying : interface Ethernet1/1
Applying :   no shutdown
Applying : sleep instance 1 20
Applying : router bgp 100
Applying :   no isolate

Maintenance mode operation successful.

The after_maintenance snapshot will be generated in 120 seconds
After that time, please use 'show snapshots compare before_maintenance after_maintenance'
to check the health of the system
switch(config)# 2016 Dec  5 06:20:23 switch %$ VDC-1 %$ %MMODE-2-MODE_CHANGED: System changed
 to "normal" mode.


switch# show system mode
System Mode: Normal
```

This example shows how to return to normal mode from maintenance mode on a switch running the Cisco NX-OS Release 7.3(0)D1(1):

```
switch# configure terminal
switch(config)# no system mode maintenance
Following configuration will be applied:

interface Ethernet1/1
  no shutdown
sleep instance 1 20
router bgp 100
  no isolate

Do you want to continue (y/n)? [no] yes
```

```
Starting to apply commands...

Applying : interface Ethernet1/1
Applying :   no shutdown
Applying : sleep instance 1 20
Applying : router bgp 100
Applying :   no isolate

Maintenance mode operation successful.

Generating Current Snapshot

Please use 'show snapshots compare before_maintenance after_maintenance' to check the health
 of the system
switch(config)#


switch(config)# show system mode
System Mode: Normal
```

This example shows how to return to normal mode from maintenance mode by using the **dont-generate-profile** keyword:

```
switch(config)# no system mode maintenance dont-generate-profile
Following configuration will be applied:

interface Ethernet1/1
  no shutdown
sleep instance 1 20
router bgp 100
  no isolate

Do you want to continue (y/n)? [no] yes

Starting to apply commands...

Applying : interface Ethernet1/1
Applying :   no shutdown
Applying : sleep instance 1 20
Applying : router bgp 100
Applying :   no isolate

Maintenance mode operation successful.

The after_maintenance snapshot will be generated in 120 seconds
After that time, please use 'show snapshots compare before_maintenance after_maintenance'
to check the health of the system
switch(config)# 2016 Dec  5 08:51:46 switch %$ VDC-1 %$ %MMODE-2-MODE_CHANGED: System changed
 to "normal" mode.


switch(config)# show system mode
System Mode: Normal
```

This example shows how to return to normal mode from maintenance mode by using the **non-interactive** keyword:

```
switch(config)# no system mode maintenance non-interactive
System mode switch to normal mode started. Will continue in background.
switch(maint-mode)(config)# 2016 Dec  5 08:48:01 switch %$ VDC-1 %$ %MMODE-2-MODE_CHANGED:
 System changed to "normal" mode.
```

```
switch(config)# show system mode
System Mode: Normal
```

Deleting a Maintenance Profile

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	Required: switch# **no configure maintenance profile** {**normal-mode** | **maintenance-mode**}	Deletes the normal mode or maintenance mode profiles.

Example

This example shows how to delete a maintenance profile:

```
switch# configure terminal
switch(config)# no configure maintenance profile maintenance-mode
```

Configuration Examples for GIR

This example shows how to create custom maintenance mode profile:

```
switch# configure maintenance profile maintenance-mode
Please configure 'system mode maintenance always-use-custom-profile' if you want to use
custom
profile always for maintenance mode.
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-mm-profile)# router bgp 100
switch(config-mm-profile-router)# isolate
switch(config-mm-profile-router)# exit
switch(config-mm-profile)# sleep instance 1 10
switch(config-mm-profile)# interface ethernet 1/1
switch(config-mm-profile-if-verify)# shutdown
switch(config-mm-profile-if-verify)# end
Exit maintenance profile mode.
```

This example shows how to create custom normal mode profile:

```
switch# configure maintenance profile normal-mode
Please configure 'system mode maintenance always-use-custom-profile' if you want to use
custom
profile always for maintenance mode.
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-mm-profile)# interface ethernet 1/1
switch(config-mm-profile-if-verify)# no shutdown
switch(config-mm-profile-if-verify)# exit
switch(config-mm-profile)# sleep instance 1 20
switch(config-mm-profile)# router bgp 100
switch(config-mm-profile-router)# no isolate
switch(config-mm-profile-router)# end
```

```
Exit maintenance profile mode.
```

This example shows how to create a custom maintenance mode and normal mode profile for IPv6 protocols:

```
switch# configure terminal
switch(config)# configure maintenance profile maintenance-mode
Please configure 'system mode maintenance always-use-custom-profile' if you want to use
custom
profile always for maintenance mode.
switch(config-mm-profile)# router ospfv3 ospf_ipv6
switch(config-mm-profile-router)# shutdown
switch(config-mm-profile-router)# exit
switch(config-mm-profile)# router eigrp 660
switch(config-mm-profile-router)# address-family ipv6 unicast
switch(config-mm-profile-router-af)# shutdown
switch(config-mm-profile-router-af)# exit
switch(config-mm-profile)# router isis isp
switch(config-mm-profile-router)# set-overload-bit always
switch(config-mm-profile-router)# address-family ipv6 unicast
switch(config-mm-profile-router-af)# shutdown
switch(config-mm-profile-router-af)# exit


switch# configure terminal
switch(config)# configure maintenance profile normal-mode
Please configure 'system mode maintenance always-use-custom-profile' if you want to use
custom
profile always for maintenance mode.
switch(config-mm-profile)# router isis isp
switch(config-mm-profile-router)# no set-overload-bit always
switch(config-mm-profile-router)# address-family ipv6 unicast
switch(config-mm-profile-router-af)# no shutdown
switch(config-mm-profile-router-af)# exit
switch(config-mm-profile)# router eigrp 660
switch(config-mm-profile-router)# address-family ipv6 unicast
switch(config-mm-profile-router-af)# no shutdown
switch(config-mm-profile-router-af)# exit
switch(config-mm-profile)# router ospfv3 ospf_ipv6
switch(config-mm-profile-router)# no shutdown
switch(config-mm-profile-router)# exit


switch# show maintenance profile
[Normal mode]
router isis isp
  no set-overload-bit always
  address-family ipv6 unicast
   no shutdown
router eigrp 660
  address-family ipv6 unicast
   no shutdown
router ospfv3 ospf_ipv6
   no shutdown
[Maintenance Mode]
router ospfv3 ospf_ipv6
  shutdown
router eigrp 660
  address-family ipv6 unicast
   shutdown
router isis isp
  set-overload-bit always
  address-family ipv6 unicast
   shutdown
```

This example shows how to create a custom maintenance mode profile and custom normal mode profile for VPC:

```
switch# configure terminal
switch(config)# configure maintenance profile maintenance-mode
switch(config-mm-profile)# router bgp 100
switch(config-mm-profile-router)# isolate
switch(config-mm-profile-router)# exit
switch(config-mm-profile)# interface port channel 5
switch(config-mm-profile-if-verify)# vpc orphan port suspend
switch(config-mm-profile-if-verify)# exit
switch(config-mm-profile)# interface port channel 6
switch(config-mm-profile-if-verify)# vpc orphan port
suspend switch(config-mm-profile-if-verify)# exit
switch(config-mm-profile)# sleep instance 1 5
switch(config-mm-profile)# vpc domain 1
switch(config-mm-profile-vpc-domain)# shutdown


switch# configure terminal
switch(config)# configure maintenance profile normal-mode
switch(config-mm-profile)# vpc domain 1
switch(config-mm-profile-vpc-domain)# no shutdown
switch(config-mm-profile-vpc-domain)# exit
switch(config-mm-profile)# sleep instance 1 60
switch(config-mm-profile)# interface port channel 5
switch(config-mm-profile-if-verify)# no vpc orphan port suspend
switch(config-mm-profile-if-verify)# exit
switch(config-mm-profile)# interface port channel 6
switch(config-mm-profile-if-verify)# no vpc orphan port suspend
switch(config-mm-profile-if-verify)# exit
switch(config-mm-profile)# router bgp 100
switch(config-mm-profile-router)# no isolate


switch# show maintenance profile
[Normal Mode]
vpc domain 1
  no shutdown
sleep instance 1 60
interface port-channel 5
  no vpc orphan-port suspend
interface port-channel 6
  no vpc orphan-port suspend router
bgp 100
  no isolate

[Maintenance Mode]
router bgp 100
  isolate
interface port-channel 5 vpc
  orphan-port suspend
interface port-channel 6 vpc
  orphan-port suspend
sleep instance 1 5
  vpc domain 1 shutdown
```

This example shows how to use the **isolate** command to put all protocols into maintenance mode:

```
switch(config)# system mode maintenance

Following configuration will be applied:

router bgp 100
```

```
  isolate
router ospf 100
  isolate
router isis 100
  isolate

Do you want to continue (y/n)? [no] y

Generating a snapshot before going into maintenance mode

Starting to apply commands...

Applying : router bgp 100
Applying :   isolate
Applying : router ospf 100
Applying :   isolate
Applying : router isis 100
Applying :   isolate

Maintenance mode operation successful.
```

This example shows how to use the **isolate** command to put all protocols into maintenance mode on a switch running the Cisco NX-OS Release 8.0(1):

```
switch# configure terminal
switch(config)# system mode maintenance
Following configuration will be applied:

router bgp 100
  isolate
router ospf 100
  isolate
router isis 100
  isolate

Do you want to continue (y/n)? [no] y

Generating before_maintenance snapshot before going into maintenance mode

Starting to apply commands...

Applying : router bgp 100
Applying :   isolate
Applying : router ospf 100
Applying :   isolate
Applying : router isis 100
Applying :   isolate

Maintenance mode operation successful.
switch(maint-mode)(config)# 2016 Dec  5 06:19:13 switch %$ VDC-1 %$ %MMODE-2-MODE_CHANGED:
 System changed to "maintenance" mode.

switch(maint-mode)(config)#
```

This example shows how to shut down all protocols and interfaces on the switch:

```
switch# configure terminal
switch(config)# system mode maintenance shutdown

Following configuration will be applied:

router bgp 64581
  shutdown
router eigrp p2
```

```
  shutdown
  address-family ipv6 unicast
    shutdown
router eigrp 0
  shutdown
  address-family ipv6 unicast
    shutdown
router ospf 200
  shutdown
router isis 70
  shutdown
vpc domain 2
  shutdown
system interface shutdown

NOTE: 'system interface shutdown' will shutdown all interfaces excluding mgmt 0
Do you want to continue (yes/no)? [no] yes

Generating a snapshot before going into maintenance mode

Starting to apply commands...

Applying : router bgp 64581
Applying :   shutdown
Applying : router eigrp p2
Applying :   shutdown
Applying :   address-family ipv6 unicast
Applying :     shutdown
Applying : router eigrp 0
Applying :   shutdown
Applying :   address-family ipv6 unicast
Applying :     shutdown
Applying : router ospf 200
Applying :   shutdown
Applying : router isis 70
Applying :   shutdown
Applying : vpc domain 2
Applying :   shutdown2016 Jan 15 11:10:36.080386 CP-BL26-N7K-1A %$ VDC-1 %$
%VPC-2-VPC_SHUTDOWN: vPC shutdown status is ON

Applying : system interface shutdown

Maintenance mode operation successful.
switch(config)# 2016 Jan 15 11:10:42.057678 CP-BL26-N7K-1A %$ VDC-1 %$ %MMODE-2-MODE_CHANGED:
 System changed to "maintenance" mode.
2016 Jan 15 11:10:42.058167 CP-BL26-N7K-1A %$ VDC-1 %$ %MMODE-2-MODE_CHANGE_WARN: System
will be moved to "normal" mode in 5 minutes
```

This example shows how to return to normal mode from maintenance mode:

```
switch# configure terminal
switch(config)# no system mode maintenance dont-generate-profile

Following configuration will be applied:
interface Ethernet1/1
  no shutdown
  sleep instance 1 20
router bgp 100
  no isolate
Do you want to continue (y/n)? [no] yes
Starting to apply commands...
Applying : interface Ethernet1/1
Applying :   no shutdown
Applying : sleep instance 1 20
```

```
Applying : router bgp 100
Applying :   no isolate
Maintenance mode operation successful.
Generating Current Snapshot
Please use 'show snapshots compare before_maintenance after_maintenance' to check the
health of the system
```

This example shows how to return to normal mode from maintenance mode on a switch running the Cisco NX-OS Release 8.0(1):

```
 switch(maint-mode)(config)# no system mode maintenance
Following configuration will be applied:

interface Ethernet1/1
  no shutdown
sleep instance 1 20
router bgp 100
  no isolate

Do you want to continue (y/n)? [no] yes

Starting to apply commands...

Applying : interface Ethernet1/1
Applying :   no shutdown
Applying : sleep instance 1 20
Applying : router bgp 100
Applying :   no isolate

Maintenance mode operation successful.

The after_maintenance snapshot will be generated in 120 seconds
After that time, please use 'show snapshots compare before_maintenance after_maintenance'
to check the health of the system
switch(config)# 2016 Dec  5 06:20:23 switch %$ VDC-1 %$ %MMODE-2-MODE_CHANGED: System changed
 to "normal" mode.


switch# show system mode
System Mode: Normal
```

This example shows how to create custom maintenance mode and normal mode profiles for FabricPath:

```
switch# configure maintenance profile maintenance-mode
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-mm-profile)# fabricpath domain default
switch(config-mm-profile-fabricpath-isis)# set-overload-bit always
switch(config-mm-profile-fabricpath-isis)# end
Exit maintenance profile mode.
switch#

switch# configure maintenance profile normal-mode
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-mm-profile)# fabricpath domain default
switch(config-mm-profile-fabricpath-isis)# no set-overload-bit always
switch(config-mm-profile-fabricpath-isis)# end
Exit maintenance profile mode.
switch#


switch# show maintenance profile
[Normal Mode]
fabricpath domain default
```

```
  no set-overload-bit always
[Maintenance Mode]
fabricpath domain default
  set-overload-bit always
```

This example shows how to create custom maintenance mode and normal mode profiles for a virtual Port Channel (vPC):

```
switch# configure maintenance profile maintenance-mode
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-mm-profile)# vpc domain 1
switch(config-mm-profile-vpc-domain)# shutdown
switch(config-mm-profile-vpc-domain)# exit
switch(config-mm-profile)# system interface shutdown
switch(config-mm-profile)# end
Exit maintenance profile mode.
switch#


switch# configure maintenance profile normal-mode
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-mm-profile)# vpc domain 1
switch(config-mm-profile-vpc-domain)# no shutdown
switch(config-mm-profile-vpc-domain)# exit
switch(config-mm-profile)# no system interface shutdown
switch(config-mm-profile)# end
Exit maintenance profile mode.
switch#



switch# show maintenance profile
[Normal Mode]
vpc domain 1
  no shutdown
no system interface shutdown
[Maintenance Mode]
vpc domain 1
  shutdown
system interface shutdown
```

This example shows the configuration to be used when there are port-channel or regular L2 ethernet interfaces (except vPC peer link) which carry vPC VLAN traffic and when the corresponding Switch Virtual Interface (SVI) state should not be controlled by these interfaces:

```
Port-channel configuration
switch(config)# interface port-channel3
switch(config-if)# description "L2-Cross Link eth3/3 eth4/3 eth5/3 eth6/3"
switch(config-if)# switchport
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan 1101-1500
switch(config-if)# spanning-tree port type network
switch(config-if)# lacp min-links 2
switch(config-if)# switchport autostate exclude vlan 1101-1500


L2 Ethernet configuration
switch(config)# interface ethernet 3/3
switch(config-if)# switchport
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan 1101-1500
switch(config-if)# switchport autostate exclude vlan 1101-1500
```

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 **route-map my-rmap-deny** in maintenance mode configuration to exclude SVIs having tag 200 configuration.

```
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 **route-map my-rmap-permit** in normal mode configuration to include SVIs having tag 200 configuration.

```
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
```

Verifying GIR

Use the following commands to verify the configuration:

Command	Purpose
show interface brief	Displays abbreviated interface information.
show maintenance on-reload reset-reason	Displays the reset reasons for which the switch comes up in maintenance mode.
show maintenance profile [maintenance-mode | normal-mode]	Displays the details of the maintenance mode or normal mode profile.
show maintenance snapshot-delay	Displays the after_maintenance snapshot-delay timer value.
show maintenance timeout	Displays the maintenance mode timeout period, after which the switch automatically returns to normal mode.
show tech-support mmode	Displays maintenance mode information for Cisco technical support.
show {running--config | startup--config} mmode [all]	Displays the maintenance-mode section of the running or startup configuration. The **all** option includes the default values.
show snapshots	Displays snapshots present on the switch.
show snapshots compare *snapshot-name-1 snapshot-name-2* [**summary | ipv4routes | ipv6routes**]	Displays a comparison of two snapshots. The **summary** option displays just enough information to see the overall changes between the two snapshots. The **ipv4routes** and the **ipv6routes** options display the changes in IPv4 and IPv6 routes between the two snapshots.
show snapshots dump *snapshot-name*	Displays content of the various sections in a generated snapshot.
show snapshots sections	Displays the user-specified snapshot sections.
show system mode	Displays the current system mode. This command also displays the current state of the maintenance mode timer when the switch is in maintenance mode.

Verifying GIR at Protocol Level

BGP (Maintenance mode)

Use the **show bgp process** command to display BGP status in maintenance mode:

```
switch# show bgp process

BGP Process Information
BGP Process ID                 : 11725
BGP Protocol Started, reason:  : configuration
BGP Protocol Tag               : 100
BGP Protocol State         : Running (Isolate)
```

```
BGP MMODE                  : Initialized
BGP Memory State               : OK
BGP asformat                   : asplain

BGP attributes information
Number of attribute entries    : 1
HWM of attribute entries       : 1
Bytes used by entries          : 100
Entries pending delete         : 0
HWM of entries pending delete  : 0
BGP paths per attribute HWM    : 3
BGP AS path entries            : 0
Bytes used by AS path entries  : 0
```

Use the **show bgp internal all statistics** command to display the number of BGP IPv4 and IPv6 prefixes that have been programmed and also the number of BGP IPv4 and IPv6 prefixes that have not been programmed:

```
BGP internal statistics information for VRF default, address family IPv4 Unicast
  Total prefixes in BGP Table: 3
  Total prefixes pending programming in HW: 0
BGP internal statistics information for VRF default, address family IPv6 Unicast
  Total prefixes in BGP Table: 0
  Total prefixes pending programming in HW: 0
```

EIGRP (Maintenance mode)

Use the **show ip eigrp** command to display EIGRP status in maintenance mode:

```
switch# show ip eigrp
IP-EIGRP AS 100 ID 30.1.1.1 VRF default
  Process-tag: 100
  Instance Number: 1
  Status: running (isolate)
  Authentication mode: none
  Authentication key-chain: none
  Metric weights: K1=1 K2=0 K3=1 K4=0 K5=0
  IP proto: 88 Multicast group: 224.0.0.10
  Int distance: 90 Ext distance: 170
  Max paths: 8
  Number of EIGRP interfaces: 1 (0 loopbacks)
  Number of EIGRP passive interfaces: 0
  Number of EIGRP peers: 1
  Redistributing:
    direct route-map passall
    static route-map passall
  Graceful-Restart: Enabled
  Stub-Routing: Disabled
  NSF converge time limit/expiries: 120/0
  NSF route-hold time limit/expiries: 240/6
  NSF signal time limit/expiries: 20/0
  Redistributed max-prefix: Disabled
  MMODE: Initialized
  Suppress-FIB-Pending Configured
```

ISIS (Maintenance mode)

Use the **show isis protocol** command to display ISIS status in maintenance mode:

```
switch# show isis protocol
ISIS process : 100
 Instance number :  1
 UUID: 1090519320
 Process ID 6969
```

```
VRF: default
  System ID : 0300.0000.0004  IS-Type : L2
  SAP : 412  Queue Handle : 16
  Maximum LSP MTU: 1492
  Stateful HA enabled
  Graceful Restart enabled. State: Inactive
  Last graceful restart status : none
  Start-Mode Complete
  BFD IPv4 is globally disabled for ISIS process: 100
  BFD IPv6 is globally disabled for ISIS process: 100
  Topology-mode is base
  Metric-style : advertise(wide), accept(narrow, wide)
  Area address(es) :
    10
  Process is up and running (isolate)
  VRF ID: 1
  Stale routes during non-graceful controlled restart
  Interfaces supported by IS-IS :
    Ethernet1/2
```

OSPF (Maintenance mode)

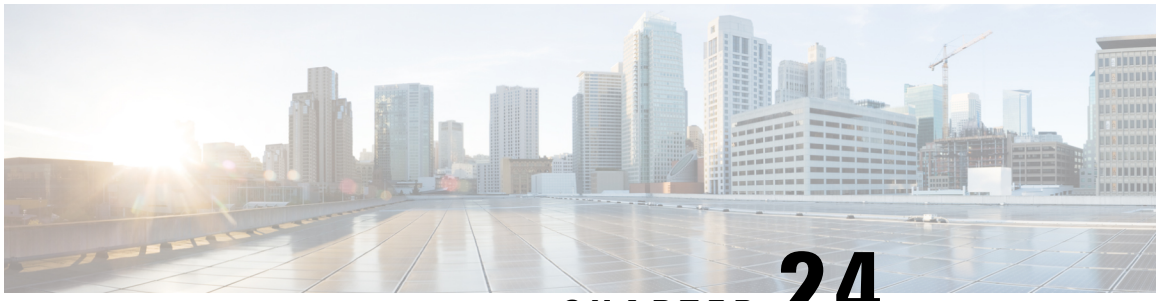
Use the **show ip ospf internal** command to display OSPF status in maintenance mode:

```
switch# show ip ospf internal

ospf 100
ospf process tag 100
ospf process instance number 1
ospf process uuid 1090519321
ospf process linux pid 6968
ospf process state running (isolate)
System uptime 6d06h
SUP uptime 2 6d06h

Server up : L3VM|IFMGR|RPM|AM|CLIS|URIB|U6RIB|IP|IPv6|SNMP|MMODE
Server required  : L3VM|IFMGR|RPM|AM|CLIS|URIB|IP|SNMP
Server registered: L3VM|IFMGR|RPM|AM|CLIS|URIB|IP|SNMP|MMODE
Server optional  : MMODE

Early hello : OFF
Force write PSS: FALSE
OSPF mts pkt sap 324
OSPF mts base sap 320
```

Feature History for GIR

The table below summarizes the new and changed features for this document and shows the releases in which each feature is supported. Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Feature Name	Release	Information
Graceful Insertion and Removal (GIR) Enhancements	8.0(1)	Support for Simple Network Management Protocol (SNMP) traps and snapshot delay. A CLI indicator to show that the switch is in maintenance mode. The following keywords were added to the **system mode maintenance** command: **non-interactive** and **snapshot-delay**.
Graceful Insertion and Removal (GIR)	7.3(0)D1(1)	The default mode for GIR is “isolate”. Support for Unplanned Maintenance, Maintenance Mode timer, Supress FIB Pending, Adding Show commands to snapshots and dumping snapshot sections.
Graceful Insertion and Removal (GIR)	7.2(0)D1(1)	This feature was introduced. The default mode for GIR is “shutdown”. Refer Configuring GIR (Cisco NX-OS Release 7.2(0)D1(1)).



CHAPTER 24

Configuring iCAM

This chapter includes the following sections:

Feature History for iCAM

This table lists the release history for this feature.

Table 43: Feature History for iCAM

Feature Name	Releases	Feature Information
Scale Monitoring	8.4(1)	Scale monitoring has been expanded to cover the following technology groups: BFD, FEX, FabricPath, Interfaces, Layer 2 Switching, Multicast Routing, NetFlow, OTV, PTP, PVLAN, QoS, Security, SPAN, System Management, Unicast Routing, VXLAN EVPN.
Remote Integrated Services Engine (RISE)	8.4(1)	Support for the RISE feature has been deprecated.

Feature Name	Releases	Feature Information
iCAM Scale Monitoring	8.3(1)	This feature was introduced.
iCAM TCAM Monitoring	8.2(1)	• Added the functionality to enable iCAM monitoring, viewing the history of traffic analytics, and predicting the traffic analytics.
iCAM	8.0(1)	This feature was introduced. The following commands were introduced: • **feature icam** • **show icam {entries | resource} module** *module-number* **inst** *instance-number*

Information About iCAM

From Cisco NX-OS Release 8.0(1), the Intelligent CAM (iCAM) analytics and machine-learning feature is supported on Cisco Nexus 7000 Series Switches and Cisco Nexus 7700 Switches. The iCAM feature enables you to view the traffic analytics per feature, Ternary Content-Addressable Memory (TCAM) resources and ability to monitor network scale parameters..Before the iCAM feature, it was difficult to get information about the traffic flow through various subnets and applications and an overall view of how many TCAM or Static Random Access Memory (SRAM) resource entries were used or free with various features.

For example, the resource entries utilized in the ACL Classification TCAM per feature, like Router-ACL (RACL), Vlan-ACL (VACL), Port-ACL (PACL), Policy Based Routing (PBR), QoS (Quality of Service), NAT, Intelligent Traffic Director (ITD), Web Cache Communication Protocol (WCCP), or Remote Integrated Services Engine (RISE), could not be determined. Some features might use bulk of the TCAM resources, and some of those TCAM entries might not be in use.

To overcome these limitations, the iCAM feature provides analytics related to network traffic, TCAM usage per feature, detailed analysis per TCAM bank. This helps in effectively utilizing the available TCAM space.

An iCAM process runs on the Supervisor module. It interacts with various components on the line card and collects the hardware resource utilization statistics, performs data processing, and presents a summarized output. It also provides insights about the top hitters and bottom hitters for each feature, like ACL and PBR entries. Using iCAM, you can get packet counts per TCAM entry, sort and search through these entries, and get the top or bottom specified percentage of entries. The traffic analytics helps in better utilization of TCAM space, and better understanding of network traffic.

The iCAM is a VDC global process; it can be enabled only on the default VDC.

The iCAM does not require additional hardware or software. It provides useful traffic telemetry and analytics.

iCAM enables you to perform the following:

- View traffic and usage analytics per supported function, Ternary Content-Addressable Memory (TCAM) resources, and TCAM entries.
- Allows you to plan better by understanding the Ternary Content-Addressable Memory (TCAM) usage per feature, enabling you to use TCAM space effectively.
- Verify, detect, plan, and predict your environment against Cisco-verified scale numbers for the different supported functions (Layer 2 switching, unicast routing, multicast routing, and VXLAN).
- Maintain historical usage, functional scale analytics of different supported functions, including entries and resource usage of FIB and ACL TCAM.
- Predict scale (usage level) monitoring for different supported functions in addition to predicted scale for ACL and FIB TCAM entries.
- View health monitoring data (such as CPU, memory, power supply) and information on Intelligent Traffic Director (ITD) services.

Overview of iCAM Monitoring

From Cisco NX-OS Release 8.2(1), you can use iCAM in an IPv4 network to view the traffic analytics based on the type of TCAM entries and the type of TCAM resources. You can set a global monitoring interval to determine how often iCAM should collect data for statistics. You can also set a global interval history, which determines the number of intervals for which iCAM should store statistics.

Based on a default or user-configured scale level threshold on a per-function basis, iCAM generates alerts through system logging messages generation to notify network administrators.

You can obtain traffic and scale (usage level) monitoring for the following resources and functions:

- ACL TCAM entries
- IPv4 multicast TCAM entries
- ACL TCAM resource utilization
- Forward information base (FIB) TCAM resource utilization
- BFD
- FEX
- FabricPath
- Interfaces
- Layer 2 Switching
- Multicast Routing
- NetFlow
- OTV
- PTP
- PVLAN
- QoS

- Security
- SPAN
- System Management
- Unicast Routing
- VXLAN

Overview of Scale Monitoring

iCAM scale monitoring provides you the ability to verify, detect, plan, and predict your environment against Cisco verified scale numbers. You can configure all scale monitoring features with default limits and thresholds or customize the threshold values to your specific needs.

Scale monitoring capabilities include:

- Track system scale limits in comparison to Cisco verified limits.
- Two-hour polling interval by default, configurable to one-hour.
- Track average and peak utilizations, along with timestamps for peak utilizations.
- User-configurable scale limits and alert thresholds.
- JSON/XML compatible for off box Orchestrator interaction.
- Per-ASIC instance and Per-VDC Awareness.
- Event-history support.
- Scale predictability - Planning via a centralized data base for historical data.

From Cisco NX-OS Release 8.4(1), Scale Monitoring supports the following features:

- BFD
- FEX
- FabricPath
- vPC FEX
- Interfaces—BFD, Port-channel, vPC, GRE, Sub-interfaces
- Layer 2 Switching—Layer 2 infrastructure, Spanning Tree Protocol
- Multicast Routing
- OTV
- PVLAN
- QoS
- Security—ACLs, DHCP, UDP Relay
- System Management—SPAN, ERSPAN, PTP, NetFlow

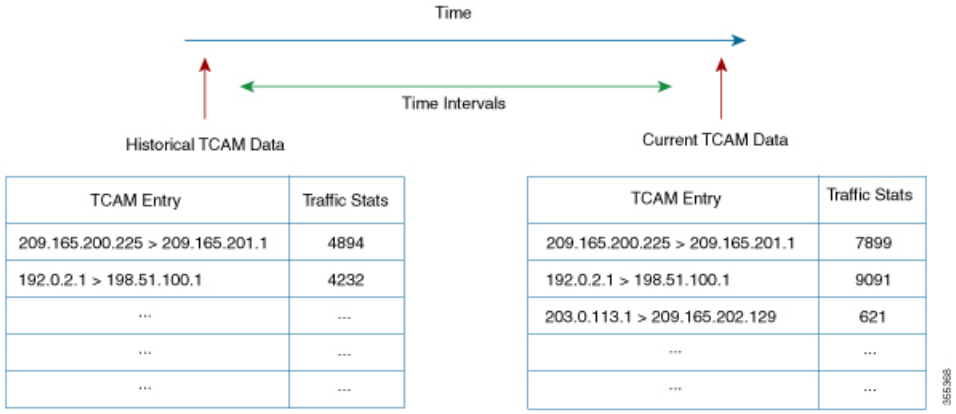
- Unicast Routing—OSPF
- VXLAN

Historical Analytics Using iCAM

From Cisco NX-OS Release 8.2(1), you can use iCAM to obtain the historical traffic analytics of entries and resources. When iCAM monitoring is enabled for resources and entries, the traffic data is periodically polled and stored in the iCAM database. The history option for iCAM entries displays the cumulative traffic stats and average packets per second. The history option for TCAM resources displays the snapshots of TCAM statistics of the past.

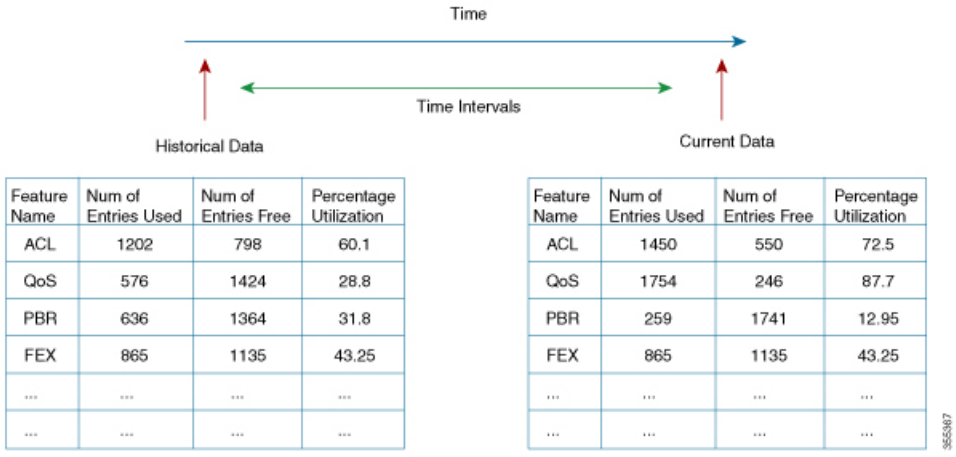
The following figure shows the historical traffic data:

Figure 9: Historical Traffic Data



The following figure shows the historical resource utilization:

Figure 10: Historical Resource Utilization

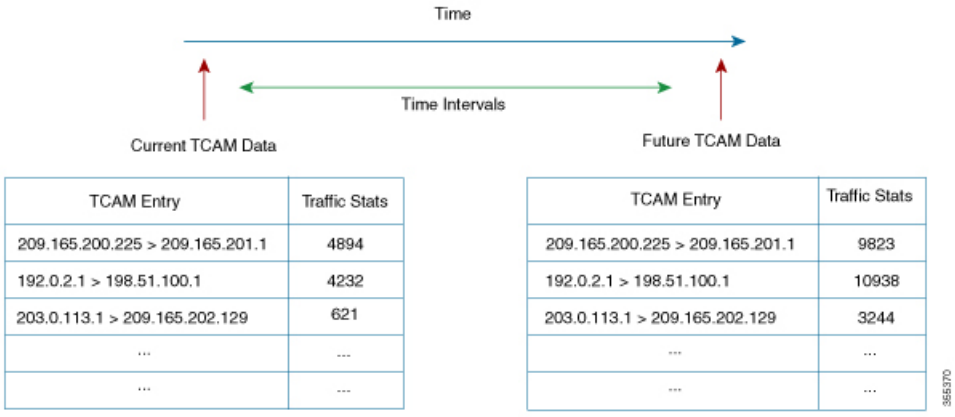


Predicting Traffic Analytics Using iCAM

From Cisco NX-OS Release 8.2(1), you can use iCAM to predict the traffic on entries and resources for a future date. The predictions are based on the data history collected by iCAM. When iCAM monitoring is enabled for resources and entries, the traffic data is periodically polled and stored in the iCAM database. The iCAM feature uses machine-learning algorithms to analyze the historical data and predicts the TCAM usage for a future date and time.

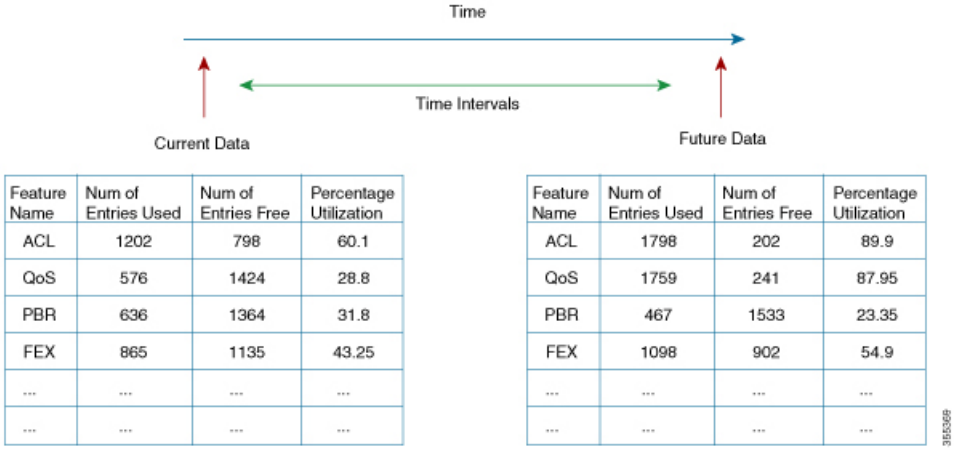
The following figure shows the predicted traffic data:

Figure 11: Predicted Traffic Data



The following figure shows the predicted resource utilization:

Figure 12: Predicted Resource Utilization



Benefits of iCAM

- Allows users to obtain application traffic analytics, like the HTTP traffic and the traffic consumed by an IP or subnet.
- Does not require additional hardware or software.

- Users can get the iCAM analytics and machine-learning feature by upgrading the Cisco NX-OS software.
- Allows users to plan better by understanding the Ternary Content-Addressable Memory (TCAM) usage per feature.

Default Settings for iCAM

This table lists the default settings for iCAM.

Table 44: Default iCAM Settings

Parameter	Default
iCAM	Disabled
iCAM monitor interval	1
iCAM interval duration	7200 sec
Number of intervals in iCAM monitor history	168 (2 weeks)
Filter	All the features are displayed
Sort order	Descending
Percentage of entries displayed	1

Enabling iCAM

Procedure

Step 1 Enter global configuration mode:

switch# **configure terminal**

Step 2 Enable the iCAM feature on the device:

switch(config)# **feature icam**

The **no** form of this command disables the iCAM feature.

Step 3 Exit the global configuration mode:

switch(config)# **exit**

Example: Configuring iCAM

This running configuration example shows how to configure the iCAM feature.

```
configure terminal
 feature icam
 exit
```

Enabling iCAM Monitoring on Resources and Traffic

Before you begin

Ensure that you have enabled the iCAM feature on the device.

Procedure

Step 1 Enter global configuration mode:

switch# **configure terminal**

Step 2 Enable monitoring on the required entries and resources:

- Enable monitoring on the TCAM entries:

  switch(config)# **icam monitor entries acl module** *module* **inst** *instance*

- Enable monitoring on the multicast entries:

  switch(config)# **icam monitor entries multicast module** *module*

- Enable monitoring on the ACL TCAM resources:

  switch(config)# **icam monitor resource acl-tcam module** *module* **inst** *instance*

- Enable monitoring on the FIB TCAM resources:

  switch(config)# **icam monitor resource fib-tcam module** *module* **inst** *instance*

Use the **no** form of these commands to disable monitoring on the corresponding resources or entries.

Step 3 Exit the global configuration mode:

switch(config)# **exit**

Example: Enabling iCAM Monitoring on Resources and Entries

This running configuration example shows how to enable iCAM monitoring on the TCAM entries. Replace the <*placeholders*> with relevant values for your setup.

```
configure terminal
 icam monitor entries acl module <3> inst <4>
```

```
exit
```

This running configuration example shows how to enable iCAM monitoring for the multicast entries. Replace the <*placeholders*> with relevant values for your setup.

```
configure terminal
 icam monitor entries multicast module <3>
 exit
```

This running configuration example shows how to enable iCAM monitoring on the ACL TCAM resources. Replace the <*placeholders*> with relevant values for your setup.

```
configure terminal
 icam monitor resource acl-tcam module <3> inst <5>
 exit
```

This running configuration example shows how to enable iCAM monitoring on the FIB TCAM resources. Replace the <*placeholders*> with relevant values for your setup.

```
configure terminal
 icam monitor resource fib-tcam module <3> inst <5>
 exit
```

Configuring iCAM Monitoring

Before you begin

Ensure that you have enabled the iCAM feature on a device.

Procedure

Step 1 Enter global configuration mode:

switch# **configure terminal**

Step 2 Set the iCAM monitor interval and the global interval history:

switch(config)# **icam monitor interval** *interval-hours* **num_intervals** *num-intervals*

Use the **no** form of this command to reset to the default values. The default value of the global monitoring interval is 2 hours and the default value of the interval history is 168. The default values might change when more data is collected on the accuracy of machine-learning.

Step 3 Exit the global configuration mode:

switch(config)# **exit**

Example: Configuring iCAM Monitor Interval

This running configuration example shows how to set the iCAM monitor interval and the global interval history. Replace the <*placeholders*> with relevant values for your setup.

```
configure terminal
 icam monitor interval <2> num_intervals <90>
 exit
```

Configuring Scale Monitoring

Procedure

Step 1 Enter global configuration mode:

switch# **configure terminal**

Step 2 Enable the iCAM feature. The **no** form of this command disables the iCAM feature.

switch(config)# **feature icam**

You must enable iCAM monitoring if you want to configure and record history and predict TCAM entries or resources.

Step 3 Enable all features with default limits and thresholds.

switch(config)# **[no]icammonitorscale**

Step 4 Enables you to customize the limit for a specific BFD feature to override its default limit. Feature limit range is 1 to 4294967295 for this step and for the following 4-18 steps with **icam monitor scale feature** form.

Note: The **icam monitor scale**<*technology*> <*feature*>**limit val** command does not enable scale monitoring for this feature but only configures scale limit for the feature.

switch(config)# **[no]icam monitor scale bfd** {**mh-sess | sess | sess-15x3 | sess-300x3 | sess-50x3 | sess-subintf** }**limit** *new feature limit*

Step 5 Enables you to customize the limit for a specific fabricpath feature to override its default limit. Feature limit range is 1 to 4294967295.

switch(config)# **[no]icam monitor scale fabricpath** {**mcast-group | switch-id | vlan** }**limit** *new feature limit*

Step 6 Enables you to customize the limit for a specific FEX feature to override its default limit. Feature limit range is 1 to 4294967295.

switch(config)# **[no]icam monitor scale fex** { **actv-actv | fex-count | interfaces** }**limit** *new feature limit*

Step 7 Enables you to customize the limit for a specific interface feature to override its default limit. Feature limit range is 1 to 4294967295.

switch(config)# **[no]icam monitor scale interface** {**gre tunnel | port-channel port-channel-count | subinterf subinterf-count | vpc { fcoe | fex | vpc-count | vpcplus}** }**limit** *new feature limit*

Step 8 Enables you to customize the limit for a specific Layer 2 switching feature to override its default limit. Feature limit range is 1 to 4294967295..

switch(config)# **[no]icam monitor scale 12-switching** {**infra | stp {mst-instance | mst-vport | rpvst-lport | rpvst-vport} | vlan vlan-count** }**limit** *new feature limit*

Step 9 Enables you to customize the limit for a specific multicast routing feature to override its default limit. Feature limit range is 1 to 4294967295.

switch(config)# **[no]icam monitor scale multicast-routing** {**igmp group | pim neighbor | routing-forwarding route-v4** }**limit** *new feature limit*

Step 10 Enables you to customize the limit for a specific netflow feature to override its default limit. Feature limit range is 1 to 4294967295.

switch(config)# **[no]icam monitor scale netflow ppslimit** *new feature limit*

Step 11 Enables you to customize the limit for a specific OTV feature to override its default limit. Feature limit range is 1 to 4294967295.

switch(config)# **[no]icam monitor scale otv** {**datagroup | localmroute | overlay | vlan** }**limit** *new feature limit*

Step 12 Enables you to customize the limit for a specific PTP feature to override its default limit. Feature limit range is 1 to 4294967295.

switch(config)# **[no]icam monitor scale ptp num-clients limit** *new feature limit*

Step 13 Enables you to customize the limit for a specific PVLAN feature to override its default limit. Feature limit range is 1 to 4294967295.

switch(config)# **[no]icam monitor scale pvlan** {**host-ports | isol-trunk-ports | primary-vlans | prom-ports | prom-trunk-ports | secondary-vlans** }**limit** *new feature limit*

Step 14 Enables you to customize the limit for a specific QoS feature to override its default limit. Feature limit range is 1 to 4294967295.

switch(config)# **[no]icam monitor scale qos** {**classmaps | policers** }**limit** *new feature limit*

Step 15 Enables you to customize the limit for a specific security feature to override its default limit. Feature limit range is 1 to 4294967295.

switch(config)# **[no]icam monitor scale security** {**acl {ace | acl-count | infs-applied | l4op-label | non-l4op-label } | cts {ip-sgt-mappings-using-sxp | sxp-connection} | dhcp {relay-agent | snoop-binding | snoop-vlan} | udp-relay {obj | port}** }**limit** *new feature limit*

Step 16 Enables you to customize the limit for a specific SPAN feature to override its default limit. Feature limit range is 1 to 4294967295.

switch(config)# **[no]icam monitor scale span** {**erspan-dst-sess | extended-sess** }**limit** *new feature limit*

Step 17 Enables you to customize the limit for a specific unicast routing feature to override its default limit. Feature limit range is 1 to 4294967295.

switch(config)# **[no]icam monitor scale unicast-routing ospf** {**area | lsa | nbr | passive-intf | vrf** }**limit** *new feature limit*

Step 18 Enables you to customize the limit for a specific VXLAN feature to override its default limit. Feature limit range is 1 to 4294967295..

switch(config)# **[no]icam monitor scale vxlan** {**bd | encap-prof | mac | vni | vsi-intf** }**limit** *new feature limit*

Step 19 (Optional) Specify the iCAM monitor interval limits.

switch(config)# **[no]icammonitorinterval***interval-hours***num_intervals***number-of-intervals*

- interval-hours— iCAM monitor interval in hours. The range is 1 to 24 hours.
- number-of-intervals— iCAM monitor history. The range is 168 to 1344.

Step 20 (Optional) Specify the iCAM change percent threshold limits.

switch(config)# **[no]icammonitorscalethreshold info***info-threshold-percent***warning***warning-threshold-percent***critical***critical-threshold-percent*

- info—Configures the info threshold. The range is 1 to 100 percent, default value is 80 percent.
- warning—Configures the warning threshold. The range is 1 to 100 percent, default value is 90 percent.
- critical—Configures the critical threshold. The range is 1 to 100 percent, default value is 100 percent.

Step 21 (Optional) Exits the global configuration mode.

switch(config)# **exit**

Step 22 (Optional) Display data from the default scale monitoring thresholds.

switch# **showicamscale**

- Verified Scale—CCO QA verified scale numbers that are based on software version and hardware.
- Customer Configured Scale—Displays the difference between configured and verified.
- Threshold Exceeded —Displays the highest threshold level exceeded.

Step 23 (Optional) Display the utilization data including average and peak utilization data, peak timestamp, 7-day totals, and total counts.

switch# **showicamscaleutilization**

Step 24 (Optional) Display the hit count and the last timestamp of the exceeding configured scale for each configured threshold. Use the hit count for each threshold to determine if the event is an anomaly or frequently occuring. The Last Info Exceeded Timestamp displays the last timestamp of the exceeding configured scale.

switch# **showicamscalethresholds**

Step 25 (Optional) Display the scale history and sort the history records by the current scale value or by the polled time stamp.

switch# **showicamscale history***number of intervals***sort**{**current-scale {ascending | descending}** | **polled-timestamp {newest | oldest}**}

Step 26 Display the BFD data. You can customize the display of BFD data. Use ? to display a list of supported BFD keywords.

switch# **show icam scale bfd**

Step 27 Display the fabricpath data. You can customize the display of fabricpath data. Use ? to display a list of supported fabricpath keywords.

switch# **show icam scale fabricpath**

Step 28 Display the fabric extender data. You can customize the display of FEX data. Use ? to display a list of supported FEX keywords.

switch# **show icam scale fex**

Step 29 Display the interface data. You can customize the display of interface data. Use ? to display a list of supported interface keywords.

switch# **show icam scale interface**

Step 30 Display the Layer 2 switching data. You can customize the display of Layer 2 switching data. Use ? to display a list of supported Layer 2 switching keywords.

switch# **show icam scale l2-switching**

Step 31 Display the multicast routing data. You can customize the display of multicast routing data. Use ? to display a list of supported multicast routing keywords.

switch# **show icam scale multicast-routing**

Step 32 Display the netflow data. You can customize the display of netflow data. Use ? to display a list of supported netflow keywords.

switch# **show icam scale netflow**

Step 33 Display the OTV data. You can customize the display of OTV data. Use ? to display a list of supported OTV keywords.

switch# **show icam scale otv**

Step 34 Display the PTP data. You can customize the display of PTP data. Use ? to display a list of supported PTP keywords.

switch# **show icam scale ptp**

Step 35 Display the PVLAN data. Use ? to display a list of supported PVLAN keywords.

switch# **show icam scale pvlan**

Step 36 Display the QoS data. Use ? to display a list of supported QoS keywords.

switch# **show icam scale qos**

Step 37 Display the security data. Use ? to display a list of supported security keywords.

switch# **show icam scale security**

Step 38 Display the SPAN data. Use ? to display a list of supported SPAN keywords.

switch# **show icam scale span**

Step 39 Display the unicast routing data. Use ? to display a list of supported unicast routing keywords.

switch# **show icam scale unicast-routing**

Step 40 Display the VXLAN data. Use ? to display a list of supported VXLAN keywords.

switch# **show icam scale vxlan**

Step 41 Displays the traffic prediction of scale monitoring.

switch# **show icam prediction scale** *year month day time*

- year—Specifies the year in the YYYY format. The values range from 1970 to 2030.
- month—Specifies the month as Jan, Feb, or so on. The values are case sensitive.
- day—Specifies the day of the month in the DD format. The values range from 1 to 31.
- time—Specifies the time in the HH:MM:SS format.

Example: Verifying Scale Monitoring

The following examples display sample data from PVLAN scale monitoring with the associated keywords.

```
switch# show icam scale pvlan
Retrieving data.  This may take some time ...
================================================
Info Threshold =  80 percent (default)          |
Warning Threshold =  90 percent (default)       |
Critical Threshold = 100 percent (default)      |
All timestamps are in UTC                       |
================================================

-----------------------------------------------------------------------------------------------
Scale Limits for PVLAN
-----------------------------------------------------------------------------------------------

                  Feature  Verified     Config       Cur     Cur   Threshold
 Polled
                              Scale      Scale     Scale    Util    Exceeded
Timestamp
-----------------------------------------------------------------------------------------------

      PVLAN Primary VLANs         -          -         -      -           -
      -
                  (VDC:1)        25          1        151500.00    Critical   2019-06-05
21:33:43
                  (VDC:2)        25          1         1 100.00    Critical   2019-06-05
21:33:43
    PVLAN Secondary VLANs         -          -         -      -           -
      -
                  (VDC:1)        75         75         2   2.66        None   2019-06-05
21:33:43
                  (VDC:2)        75         75         0   0.00        None   2019-06-05
21:33:43
         PVLAN Host Ports         -          -         -      -           -
      -
                  (VDC:1)        20         20         0   0.00        None   2019-06-05
21:33:43
                  (VDC:2)        20         20         0   0.00        None   2019-06-05
21:33:43
   PVLAN Promiscous Ports         -          -         -      -           -
      -
                  (VDC:1)        16         16         0   0.00        None   2019-06-05
21:33:43
```

```
                (VDC:2)        16         16         0   0.00        None   2019-06-05
21:33:43
  PVLAN Promisc Trk Ports         -          -         -      -           -
      -
                (VDC:1)       150        150         0   0.00        None   2019-06-05
21:33:43
                (VDC:2)       150        150         0   0.00        None   2019-06-05
21:33:43
 PVLAN Isolated Trk Ports         -          -         -      -           -
      -
                (VDC:1)        30         30         0   0.00        None   2019-06-05
21:33:43
                (VDC:2)        30         30         0   0.00        None   2019-06-05
21:33:43
```

```
switch# show icam scale pvlan thresholds
================================================
Info Threshold =  80 percent (default)          |
Warning Threshold =  90 percent (default)       |
Critical Threshold = 100 percent (default)      |
All timestamps are in UTC                       |
================================================
```

```
-----------------------------------------------------------------------------------------------------------------------------------------------
Scale Limits for PVLAN
-----------------------------------------------------------------------------------------------------------------------------------------------

                 Feature  Verified     Config    Current     Info             Last Info
 Warning          Last Warning  Critical         Last Critical
                           Scale      Scale      Scale     Exceeded    Exceeded Timestamp
  Exceeded    Exceeded Timestamp  Exceeded    Exceeded Timestamp
-----------------------------------------------------------------------------------------------------------------------------------------------

      PVLAN Primary VLANs         -          -         -         -                     -
       -                     -         -                     -
                 (VDC:1)        25          1        15         3   2019-06-05 20:48:19
       3   2019-06-05 20:48:19         3   2019-06-05 20:48:19
                 (VDC:2)        25          1         1         3   2019-06-05 20:48:19
       3   2019-06-05 20:48:19         3   2019-06-05 20:48:19
    PVLAN Secondary VLANs         -          -         -         -                     -
       -                     -         -                     -
                 (VDC:1)        75         75         2         0                     -
       0                     -         0                     -
                 (VDC:2)        75         75         0         0                     -
       0                     -         0                     -
         PVLAN Host Ports         -          -         -         -                     -
       -                     -         -                     -
                 (VDC:1)        20         20         0         0                     -
       0                     -         0                     -
                 (VDC:2)        20         20         0         0                     -
       0                     -         0                     -
   PVLAN Promiscous Ports         -          -         -         -                     -
       -                     -         -                     -
                 (VDC:1)        16         16         0         0                     -
       0                     -         0                     -
                 (VDC:2)        16         16         0         0                     -
       0                     -         0                     -
  PVLAN Promisc Trk Ports         -          -         -         -                     -
       -                     -         -                     -
                 (VDC:1)       150        150         0         0                     -
       0                     -         0                     -
                 (VDC:2)       150        150         0         0                     -
       0                     -         0                     -
 PVLAN Isolated Trk Ports         -          -         -         -                     -
       -                     -         -                     -
```

```
                (VDC:1)        30         30         0         0                    -
       0                    -         0                    -
                (VDC:2)        30         30         0         0                    -
       0                    -         0                    -

switch# show icam scale pvlan history 3 sort current-scale ascending
================================================
Info Threshold =  80 percent (default)          |
Warning Threshold =  90 percent (default)       |
Critical Threshold = 100 percent (default)      |
All timestamps are in UTC                       |
================================================

-------------------------------------------------------------------------------------------------
Scale Limits for PVLAN
-------------------------------------------------------------------------------------------------

                  Feature  Verified     Config       Cur     Cur   Threshold
 Polled
                              Scale      Scale     Scale    Util    Exceeded
Timestamp
-------------------------------------------------------------------------------------------------

      PVLAN Primary VLANs         -          -         -      -           -
      -
                (VDC:1)        25          1        151500.00    Critical   2019-06-05
18:48:17
                                                    151500.00    Critical   2019-06-05
19:48:18
                                                    151500.00    Critical   2019-06-05
20:48:19
                (VDC:2)        25          1         1 100.00    Critical   2019-06-05
18:48:17
                                                     1 100.00    Critical   2019-06-05
19:48:18
                                                     1 100.00    Critical   2019-06-05
20:48:19
    PVLAN Secondary VLANs         -          -         -      -           -
      -
                (VDC:1)        75         75         2   2.66        None   2019-06-05
18:48:17
                                                    2   2.66        None   2019-06-05
19:48:18
                                                    2   2.66        None   2019-06-05
20:48:19
                (VDC:2)        75         75         0   0.00        None   2019-06-05
18:48:17
                                                    0   0.00        None   2019-06-05
19:48:18
                                                    0   0.00        None   2019-06-05
20:48:19
         PVLAN Host Ports         -          -         -      -           -
      -
                (VDC:1)        20         20         0   0.00        None   2019-06-05
18:48:17
                                                    0   0.00        None   2019-06-05
19:48:18
                                                    0   0.00        None   2019-06-05
20:48:19
                (VDC:2)        20         20         0   0.00        None   2019-06-05
18:48:17
                                                    0   0.00        None   2019-06-05
19:48:18
                                                    0   0.00        None   2019-06-05
20:48:19
```

```
   PVLAN Promiscous Ports          -           -         -      -           -
      -
                  (VDC:1)         16          16         0   0.00        None   2019-06-05
18:48:17
                                                         0   0.00        None   2019-06-05
19:48:18
                                                         0   0.00        None   2019-06-05
20:48:19
                  (VDC:2)         16          16         0   0.00        None   2019-06-05
18:48:17
                                                         0   0.00        None   2019-06-05
19:48:18
                                                         0   0.00        None   2019-06-05
20:48:19
  PVLAN Promisc Trk Ports         -           -         -      -           -
      -
                  (VDC:1)        150         150         0   0.00        None   2019-06-05
18:48:17
                                                         0   0.00        None   2019-06-05
19:48:18
                                                         0   0.00        None   2019-06-05
20:48:19
                  (VDC:2)        150         150         0   0.00        None   2019-06-05
18:48:17
                                                         0   0.00        None   2019-06-05
19:48:18
                                                         0   0.00        None   2019-06-05
20:48:19
 PVLAN Isolated Trk Ports         -           -         -      -           -
      -
                  (VDC:1)         30          30         0   0.00        None   2019-06-05
18:48:17
                                                         0   0.00        None   2019-06-05
19:48:18
                                                         0   0.00        None   2019-06-05
20:48:19
                  (VDC:2)         30          30         0   0.00        None   2019-06-05
18:48:17
                                                         0   0.00        None   2019-06-05
19:48:18
                                                         0   0.00        None   2019-06-05
20:48:19
```

```
switch# show icam scale pvlan utilization
================================================
Info Threshold =  80 percent (default)          |
Warning Threshold =  90 percent (default)       |
Critical Threshold = 100 percent (default)      |
All timestamps are in UTC                       |
================================================

-----------------------------------------------------------------------------------------------------------------------
Scale Limits for PVLAN
-----------------------------------------------------------------------------------------------------------------------

                  Feature  Verified     Config       Cur    Cur    Avg  7-Day
7-Day Peak   Peak                  Peak
                            Scale      Scale     Scale   Util   Util   Util
Timestamp   Util             Timestamp
-----------------------------------------------------------------------------------------------------------------------

      PVLAN Primary VLANs         -           -         -      -      -      -
        -      -                      -
                  (VDC:1)         25          1        151500.001500.001500.00   2019-06-05
 07:25:461500.00   2019-06-05 07:25:46
```

```
                (VDC:2)        25          1         1 100.00 100.00 100.00   2019-06-05
07:25:46 100.00   2019-06-05 07:25:46
   PVLAN Secondary VLANs         -          -         -      -      -      -
       -      -                      -
                (VDC:1)        75         75         2   2.66   2.66   2.66   2019-06-05
07:25:46   2.66   2019-06-05 07:25:46
                (VDC:2)        75         75         0   0.00   0.00   0.00   2019-06-05
07:25:46   0.00   2019-06-05 07:25:46
        PVLAN Host Ports         -          -         -      -      -      -
       -      -                      -
                (VDC:1)        20         20         0   0.00   0.00   0.00   2019-06-05
07:25:46   0.00   2019-06-05 07:25:46
                (VDC:2)        20         20         0   0.00   0.00   0.00   2019-06-05
07:25:46   0.00   2019-06-05 07:25:46
  PVLAN Promiscous Ports         -          -         -      -      -      -
       -      -                      -
                (VDC:1)        16         16         0   0.00   0.00   0.00   2019-06-05
07:25:46   0.00   2019-06-05 07:25:46
                (VDC:2)        16         16         0   0.00   0.00   0.00   2019-06-05
07:25:46   0.00   2019-06-05 07:25:46
 PVLAN Promisc Trk Ports         -          -         -      -      -      -
       -      -                      -
                (VDC:1)       150        150         0   0.00   0.00   0.00   2019-06-05
07:25:46   0.00   2019-06-05 07:25:46
                (VDC:2)       150        150         0   0.00   0.00   0.00   2019-06-05
07:25:46   0.00   2019-06-05 07:25:46
PVLAN Isolated Trk Ports         -          -         -      -      -      -
       -      -                      -
                (VDC:1)        30         30         0   0.00   0.00   0.00   2019-06-05
07:25:46   0.00   2019-06-05 07:25:46
                (VDC:2)        30         30         0   0.00   0.00   0.00   2019-06-05
07:25:46   0.00   2019-06-05 07:25:46
```

Displaying Current, Historical, and Predictive Traffic Analytics of TCAM Entries

The TCAM entries and traffic analytics are listed per module and per TCAM instance. To display the current, historical, or predictive traffic analytics of TCAM entries, use the following commands:

Command	Description
show icam entries acl module module **inst** *instance* [**history** *num-intervals*] [**sort** {[**filter** *feature-name* [**exact**]] [**sort-order** *sort-order-list*] [**top** *top-percentage*]}]	Lists TCAM entries based on the options selected. • **history**—Displays the traffic history of entries for the specified number of intervals. • **sort**—Specifies how to filter or sort the list of TCAM entries. You must use at least one option if you filter TCAM entries using the **sort** keyword. • **filter** *feature-name*—Filters the TCAM entries based on the feature name. **Note** By default, all the features are displayed. Enclose the feature name in quotation marks if it contains more than one word, like QoS COPP. • **exact**—Filters the TCAM entries based on the exact feature name. **Note** This keyword can be used only when filtering the TCAM entries by feature names. • **sort-order**—Sorts the entries in either ascending or descending order. **Note** The valid values are 1 and 2. 1 displays the list in ascending order and 2 displays the list in descending order. The entries are sorted in descending order by default. • **top** *top-percentage*—Displays the top TCAM entries, sorted by packet count, based on the specified percentage. **Note** The valid values are from 1 to 100. The default value is 1%.
show icam entries multicast module *module* [**history** *num-intervals*] [**sort** {[**sort-order** *sort-order-list*] [**top** *top-percentage*]}]	Lists the multicast entries per module.

Command	Description
show icam prediction entries acl module *module* **inst** *inst year month day time* [**top** *top-percentage*]	Displays the traffic prediction of the TCAM entries. • *year*—Specifies the year in the YYYY format. The values range from 1970 to 2030. • *month*—Specifies the month as Jan, Feb, or so on. **Note** The values are case sensitive. • *day*—Specifies the day of the month in the DD format. The values range from 1 to 31. • *time*—Specifies the time in the HH:MM:SS format. • **top** *top-percentage*—Displays the top TCAM entries, sorted by packet count, based on the specified percentage. **Note** Valid values are from 1 to 10. The default value is 1%.
show icam prediction entries multicast module *module year month day time* [**top** *top-percentage*]	Displays the traffic prediction of the multicast entries.

Note

- The history and prediction can be displayed only for resources and entries that have monitoring enabled.
- The entries and resources are sorted based on the packet count.

You can use the output of the above commands to generate a chord diagram. A chord diagram provides a simple view of complex traffic flows. You can identify an anomalous traffic flow using a chord diagram.

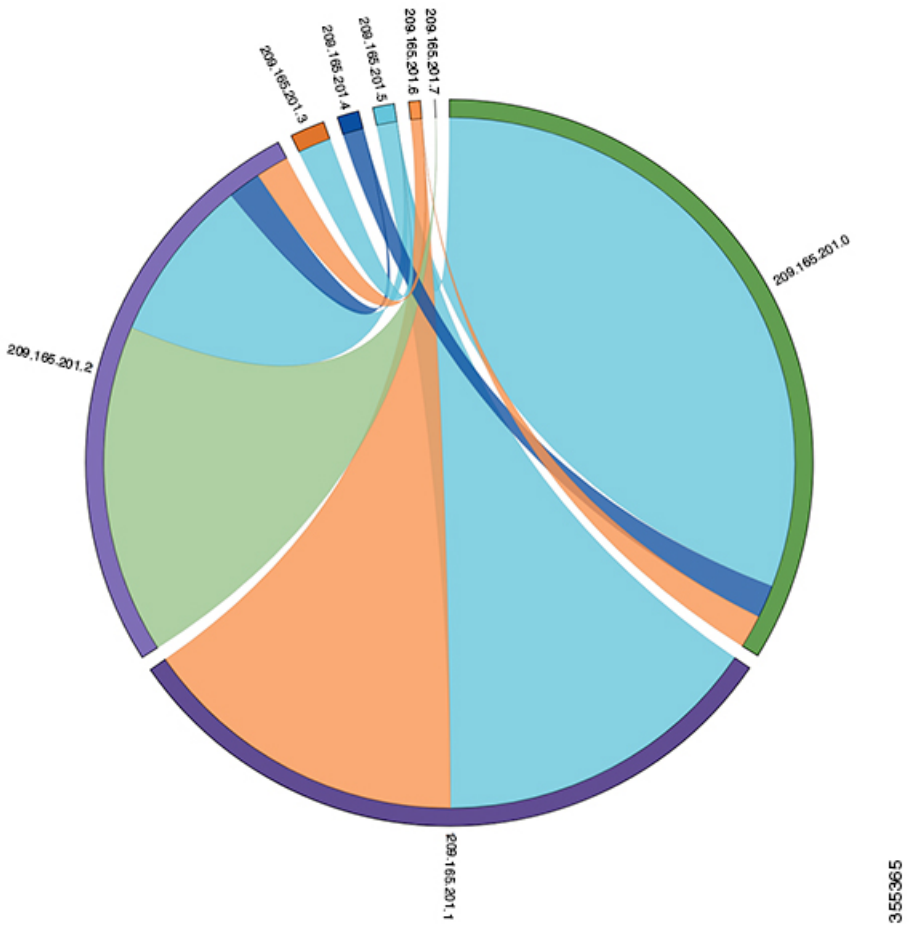
This example shows how to view the top 2% traffic flow of the TCAM entries for a current date.

```
switch# show icam entries acl module 5 inst 0 sort top 2
Retrieving data from linecard.  This may take some time ...

TCAM Entries (Mod 5,Inst 0)
------------------------------------------------------------------------------------------------------------------

 Feature  Pkt_Type                                    Source IP/Mask Dest IP/Mask     Action
      ifindex         Stats
------------------------------------------------------------------------------------------------------------------

    RACL    IPv4                          ip 209.165.201.3/27 209.165.202.131/27     Permit
   0x1a200000    1531248034
    RACL    IPv4                          ip 209.165.201.2/27 209.165.202.132/27     Permit
   0x1a200000     765624017
    RACL    IPv4                          ip 209.165.201.1/27 209.165.202.134/27     Permit
   0x1a200000     765624017
    RACL    IPv4                          ip 209.165.201.2/27 209.165.202.131/27     Permit
```

```
   0x1a200000     765624017
    RACL    IPv4                          ip 209.165.201.1/27 209.165.202.131/27     Permit
   0x1a200000     382812009
    RACL    IPv4                                    ip 0.0.0.0/0 0.0.0.0/0       Deny
   0x1a201000     241001297
    RACL    IPv4                          ip 209.165.201.3/27 209.165.202.133/27     Permit
   0x1a200000      76562402
    RACL    IPv4                          ip 209.165.201.1/27 209.165.202.132/27     Permit
   0x1a200000      76562402
    RACL    IPv4                          ip 209.165.201.1/27 209.165.202.133/27     Permit
   0x1a200000      76562402
    RACL    IPv4                          ip 209.165.201.3/27 209.165.202.132/27     Permit
   0x1a200000      76562402
    RACL    IPv4                          ip 209.165.201.8/27 209.165.202.131/27     Permit
   0x1a200000      76562402
    RACL    IPv4                          ip 209.165.202.132/27 209.165.201.2/27     Permit
   0x1a201000      48731168
    RACL    IPv4                          ip 209.165.202.133/27 209.165.201.3/27     Permit
   0x1a201000      48186974
    RACL    IPv4                          ip 209.165.202.131/27 209.165.201.2/27     Permit
   0x1a201000      47334529
QoS COPP    IPv4                                pim 0.0.0.0/0 209.165.202.135/27        QoS
          0x0         17973
QoS COPP    IPv4                               igmp 0.0.0.0/0 209.165.202.136/27        QoS
          0x0          4319
QoS COPP     ARP  arp-rarp/all ip 0.0.0.0/0 0.0.0.0/0 0000.0000.0000 0000.0000.00       QoS
          0x0            15
QoS COPP    IPv4                                     udp 0.0.0.0/0 0.0.0.0/0        QoS
          0x0             4
    VACL    IPv4                                    icmp 0.0.0.0/0 0.0.0.0/0     Permit
          0x0             0
    VACL    IPv4                                     udp 0.0.0.0/0 0.0.0.0/0     Permit
          0x0             0
    VACL    IPv4                                     tcp 0.0.0.0/0 0.0.0.0/0     Permit
          0x0             0
    VACL    IPv4                                     tcp 0.0.0.0/0 0.0.0.0/0     Permit
          0x0             0
    VACL    IPv4                                     udp 0.0.0.0/0 0.0.0.0/0     Permit
          0x0             0
    VACL    IPv4                               tcp 209.165.202.137/27 0.0.0.0/0     Permit
          0x0             0
    VACL    IPv4                               tcp 209.165.202.137/27 0.0.0.0/0     Permit
          0x0             0
    VACL    IPv4                               tcp 209.165.202.137/27 0.0.0.0/0     Permit
          0x0             0
    VACL    IPv4                               tcp 209.165.202.137/27 0.0.0.0/0     Permit
          0x0             0
    VACL    IPv4                               tcp 209.165.202.138/27 0.0.0.0/0     Permit
          0x0             0
    VACL    IPv4                               udp 209.165.202.139/27 0.0.0.0/0     Permit
          0x0             0
```

You can use the output in this example to generate a chord diagram. The following figure shows the traffic flow, which is generated using the output in this example:

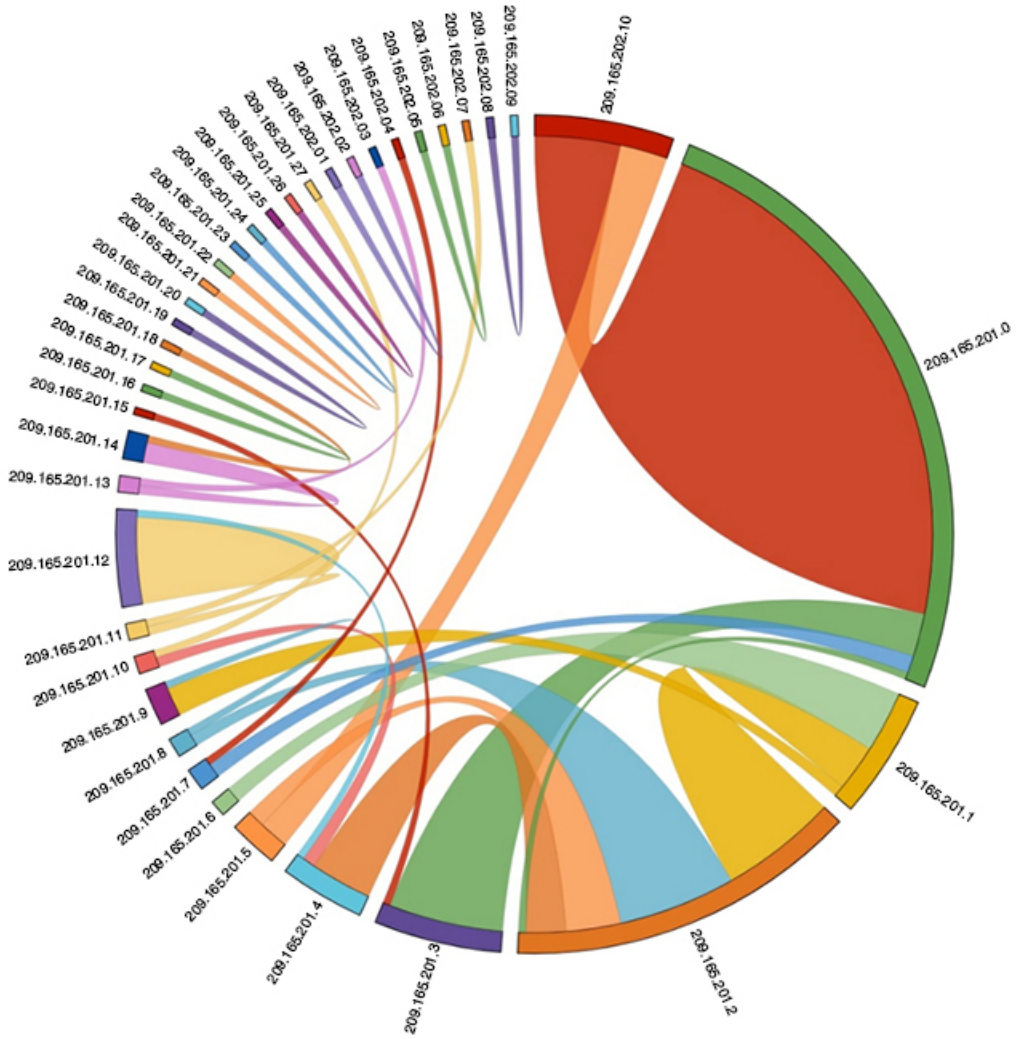
Figure 13: Chord Diagram



Every arc in the chord diagram represents the traffic flow from a source address to a destination address. The thick end of the chord represents the source address and the thin end represents the destination address. The thickness of the arc represents the percentage of the traffic. The **Stats** column in the output of the **show icam entries** command gives the information about the number of packets or traffic hitting a TCAM entry. The traffic from a single source to multiple destinations and from multiple sources to single destination can be visualized using the chord diagram.

The following figure shows the anomaly visualization of the traffic flow:

Figure 14: Anomaly Visualization



In the figure, the arcs with traffic from 209.165.201.0 to 209.165.202.10 can be easily identified as an anomalous traffic pattern.

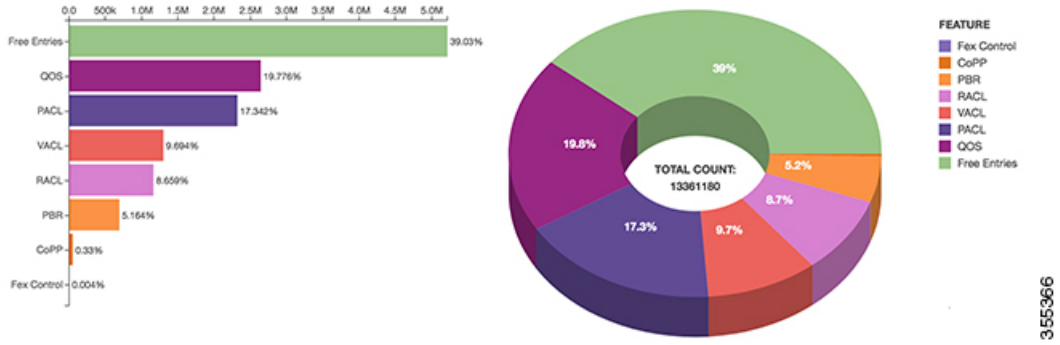
Displaying Current, Historical, and Predictive TCAM Resource Usage per Feature

To display the current, historical, or predictive TCAM usage, use the following commands:

Command	Description
show icam resource {**acl-tcam** | **fib-tcam**} **module** *module* **inst** *instance* [**history** *num-intervals*]	Displays analytics per module and per instance for resources. • **history**—Displays the traffic history of resources for the specified number of intervals. • *num-intervals*—Number of intervals in the history.
show icam prediction resource acl-tcam module *module* **inst** *inst year month day time*	Displays the traffic prediction of the ACL-TCAM features such as ACL, QoS, PBR, WCCP, and so on. • *year*—Specifies the year in the YYYY format. The values range from 1970 to 2030. • *month*—Specifies the month as Jan, Feb, or so on. **Note** The values are case sensitive. • *day*—Specifies the day of the month in the DD format. The values range from 1 to 31. • *time*—Specifies the time in the HH:MM:SS format.
show icam prediction resource fib-tcam module *module* **inst** *inst year month day time*	Displays the traffic prediction of the FIB TCAM resources.

You can generate a donut chart or a bar graph using the output of the above commands. The following figure shows the TCAM resource usage per feature:

Figure 15: Donut Chart Representing TCAM Resource Usage per Feature



Explanation of the Display Outputs

When you enable iCAM monitoring for an entry or a resource, the corresponding traffic statistics or resources usage snapshot is stored in the database once in every interval.

This example shows the historical view of the TCAM entries monitored by iCAM. The **Stats** column shows the total amount of packets hitting the entry in the last five intervals. The **Rate** column shows the average traffic rate in packets per second in the last five intervals.

```
switch# show icam entries acl module 5 inst 0 history 5
================================================================================================================================
TCAM Entries (Mod 5,Inst 0): Cumulative stats for last 5 intervals
--------------------------------------------------------------------------------------------------------------------------------
Feature  Pkt_Type                                          Source IP/Mask Dest IP/Mask    Action
      ifindex     Stats  Rate(pps)
--------------------------------------------------------------------------------------------------------------------------------

    FEX    IPv4                                               ip 0.0.0.0/0 0.0.0.0/0   Redirect
   0x15090000         0          0
    FEX    IPv6  ip 0x00000000000000000000000000000000/0 0x00000000000000000000  Redirect
   0x15090000         0          0
    FEX     MAC     0000.0000.0000 0000.0000.0000 0000.0000.0000 0000.0000.0000   Redirect
   0x15090000         0          0
    FEX     ARP  arp-rarp/all ip 0.0.0.0/0 0.0.0.0/0 0000.0000.0000 0000.0000.00  Redirect
   0x15090000         0          0
   RACL    IPv4                                     ip 209.165.201.1/27 0.0.0.0/0     Permit
   0x1a200000     23423        945
   RACL    IPv4                                     ip 209.165.201.2/27 0.0.0.0/0     Permit
   0x1a200000  23946237     718353
   RACL    IPv4                                     ip 209.165.201.3/27 0.0.0.0/0     Permit
   0x1a200000     83675        585
   RACL    IPv4                                     ip 209.165.201.4/27 0.0.0.0/0     Permit
   0x1a200000         0          0
   RACL    IPv4                                     ip 209.165.201.5/27 0.0.0.0/0     Permit
   0x1a200000   9693487      45986
   RACL    IPv4                                     ip 209.165.201.6/27 0.0.0.0/0     Permit
   0x1a200000   9693487      45986
   RACL    IPv4                                            ip 0.0.0.0/0 0.0.0.0/0       Deny
   0x1a200000   9693487      45986
QoS COPP   IPv4                                          tcp 0.0.0.0/0 0.0.0.0/0        QoS
         0x0         0          0
QoS COPP   IPv4                      udp 0.0.0.0/0 ip 209.165.201.7/27 0.0.0.0/0        QoS
         0x0         0          0
```

This example shows the historical view of the TCAM resource utilization as snapshots. Each snapshot displays the state of TCAM utilization in the corresponding time interval.

```
switch# show icam resource fib_tcam module 5 inst 0 history 5
================================================================================
FIB TCAM Resource Utilization (Mod 5, Inst 0)
--------------------------------------------------------------------------------
          Type        logical       physical   Percent_Util          Timestamp (UTC)
--------------------------------------------------------------------------------
  IPV4 unicast             16             16           0.00      2017-09-12 06:06:53
                           16             16           0.00      2017-09-12 07:06:53
                           16             16           0.00      2017-09-12 08:06:53
                           16             16           0.00      2017-09-12 09:06:53
                           16             16           0.00      2017-09-12 10:06:53
       DIAG_80              0              0           0.00      2017-09-12 06:06:53
                            0              0           0.00      2017-09-12 07:06:53
                            0              0           0.00      2017-09-12 08:06:53
```

```
                              0              0          0.00      2017-09-12 09:06:53
                              0              0          0.00      2017-09-12 10:06:53
IPV4 multicast                6              6          0.00      2017-09-12 06:06:53
                             45             45          0.10      2017-09-12 07:06:53
                             45             45          0.10      2017-09-12 08:06:53
                             62             62          0.17      2017-09-12 09:06:53
                             62             62          0.17      2017-09-12 10:06:53
          MPLS                0              0          0.00      2017-09-12 06:06:53
                              0              0          0.00      2017-09-12 07:06:53
                              0              0          0.00      2017-09-12 08:06:53
                              0              0          0.00      2017-09-12 09:06:53
                              0              0          0.00      2017-09-12 10:06:53
```

Example: iCAM CLI Outputs

The following example shows how to view the running configuration for iCAM:

```
switch# show running-config icam
!Command: show running-config icam
!Time: Tue Sep  5 21:49:50 2017

version 8.2(1)
feature icam
icam monitor interval 1 num_intervals 168
icam monitor resource acl-tcam module 3 inst 4
icam monitor resource acl-tcam module 3 inst 5
icam monitor entries acl module 3 inst 5
icam monitor resource fib-tcam module 3 inst 5
icam monitor entries multicast module 3
```

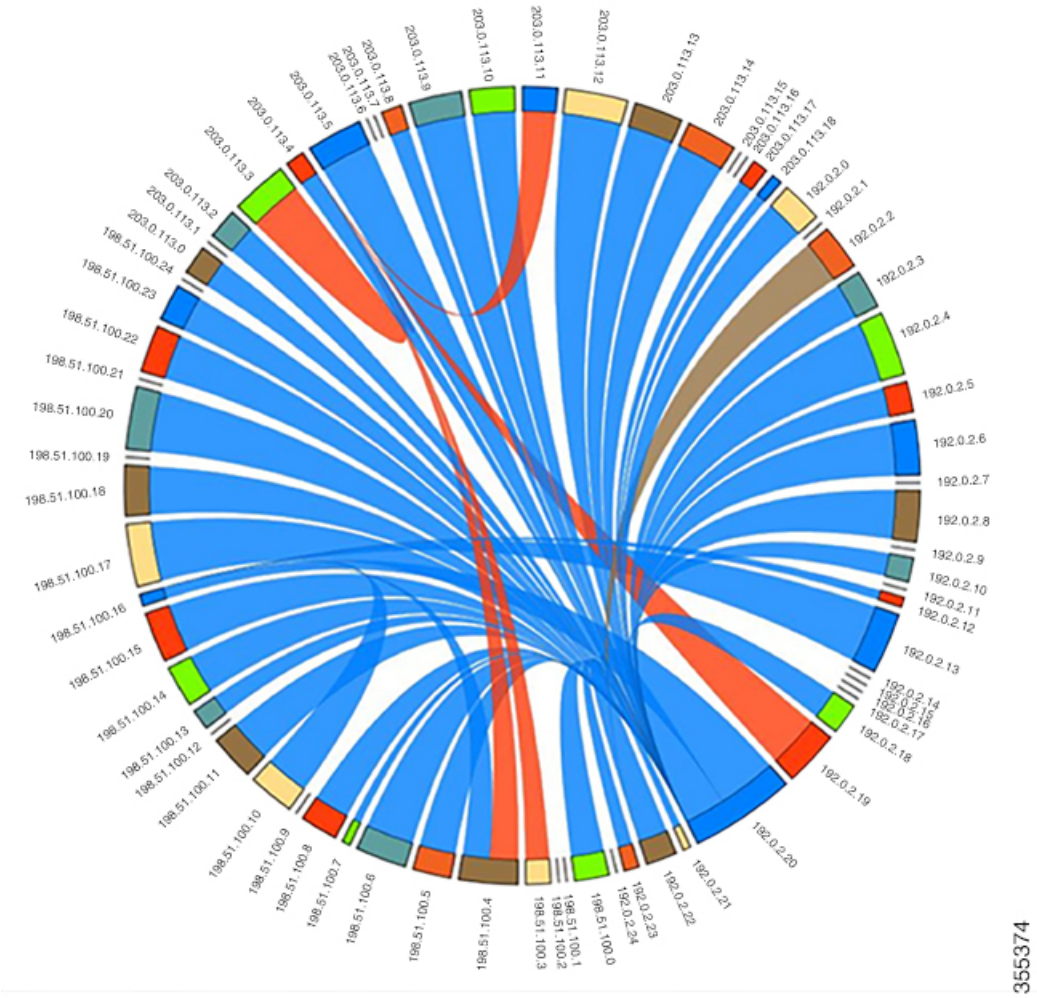
This example shows how to view current TCAM entries and their traffic statistics.

```
switch# show icam entries acl module 3 inst 5
Retrieving data from linecard.  This may take some time ...

================================================================================================================
TCAM Entries (Mod 3,Inst 5)
----------------------------------------------------------------------------------------------------------------

 Feature  Pkt_Type                                      Source IP/Mask Dest IP/Mask     Action
      ifindex   Stats
----------------------------------------------------------------------------------------------------------------

    FEX    IPv4                                              ip 0.0.0.0/0 0.0.0.0/0   Redirect
   0x15090000       0
    FEX    IPv6  ip 0x00000000000000000000000000000000/0 0x00000000000000000000   Redirect
   0x15090000       0
    FEX     MAC      0000.0000.0000 0000.0000.0000 0000.0000.0000 0000.0000.0000   Redirect
   0x15090000       0
    FEX     ARP  arp-rarp/all ip 0.0.0.0/0 0.0.0.0/0 0000.0000.0000 0000.0000.00   Redirect
   0x15090000       0
    RACL    IPv4                                 tcp 209.165.200.225/27 0.0.0.0/0     Permit
   0x1a10a000       0
    RACL    IPv4                                   tcp 209.165.201.1/27 0.0.0.0/0     Permit
   0x1a10a000       0
    RACL    IPv4                                 tcp 209.165.202.129/27 0.0.0.0/0     Permit
   0x1a10a000       0
    RACL    IPv4                                 tcp 209.165.202.139/27 0.0.0.0/0     Permit
```

```
   0x1a10a000       0
    RACL    IPv4                                tcp 209.165.202.140/27 0.0.0.0/0     Permit
   0x1a10a000       0
QoS COPP    IPv4                                    udp 0.0.0.0/0 209.165.201.3/27
QoS          0x0       0
QoS COPP    IPv4                                    udp 0.0.0.0/0 209.165.201.3/27
QoS          0x0       0
QoS COPP    IPv4                                        209.165.201.1/27 0.0.0.0/0
QoS          0x0       0
QoS COPP    IPv4                                    udp 0.0.0.0/0 209.165.201.1/27
QoS          0x0       0
QoS COPP    IPv4                                    udp 0.0.0.0/0 209.165.201.1/27
QoS          0x0       0
QoS COPP    IPv4                                    udp 0.0.0.0/0 209.165.201.7/27
QoS          0x0       0
QoS COPP    IPv4                                    udp 0.0.0.0/0 209.165.201.7/27
QoS          0x0       0
QoS COPP    IPv4                                   udp 0.0.0.0/0 209.165.201.11/27
QoS          0x0       0
QoS COPP    IPv4                                   udp 0.0.0.0/0 209.165.201.11/27
QoS          0x0       0
QoS COPP    IPv4                                    ip 0.0.0.0/0 209.165.201.14/27
QoS          0x0       0
```

The following chord diagram is a simple representation of a complex traffic flow, where the traffic flow between the various sources and destinations is uniform.

Figure 16: Chord Diagram Representing Uniform Traffic Flow



This example shows how to view the top 10% of TCAM entries for a current date and filtered by a feature name.

```
switch# show icam entries acl module 3 inst 5 sort filter "qos copp" top 10
Retrieving data from linecard. This may take some time ...
```

```
TCAM Entries (Mod 3,Inst 5)
------------------------------------------------------------------------------------------------------------------

 Feature  Pkt_Type                                        Source IP/Mask Dest IP/Mask    Action
    ifindex       Stats
------------------------------------------------------------------------------------------------------------------
QoS COPP    IPv4                                                ip 0.0.0.0/0 0.0.0.0/0       QoS
        0x0    38408890
QoS COPP     MAC  0000.0000.0000 0000.0000.0000 0180.c200.000e ffff.ffff.ffff 350      QoS
        0x0          254
QoS COPP     MAC     0000.0000.0000 0000.0000.0000 0100.0ccc.cccc ffff.ffff.ffff       QoS
        0x0           23
QoS COPP    IPv4                                       udp 0.0.0.0/0 209.165.201.1/27       QoS
        0x0            0
```

```
QoS COPP    IPv4                                    udp 0.0.0.0/0 209.165.201.1/27       QoS
        0x0           0
```

This example shows how to view current TCAM entries filtered by a feature name using the **exact** keyword.

```
switch# show icam entries acl module 7 inst 0 sort filter QoS exact top 100
Retrieving data from linecard. This may take some time ...
================================================================================================
TCAM Entries (Mod 7,Inst 0)
------------------------------------------------------------------------------------------------

   Feature  Pkt_Type                     Source IP/Mask Dest IP/Mask     Action      ifindex
      Stats
------------------------------------------------------------------------------------------------

      QoS    IPv4            ip 209.165.201.1/27 209.165.202.129/27       QoS   0x1a316000
          0
      QoS    IPv4            ip 209.165.201.1/27 209.165.202.129/27       QoS   0x1a316000
          0
      QoS    IPv4            ip 209.165.201.2/27 209.165.202.129/27       QoS   0x1a316000
          0
      QoS    IPv4            ip 209.165.201.2/27 209.165.202.129/27       QoS   0x1a316000
          0
      QoS    IPv4            ip 209.165.201.3/27 209.165.202.129/27       QoS   0x1a316000
          0
      QoS    IPv4            ip 209.165.201.3/27 209.165.202.129/27       QoS   0x1a316000
          0
      QoS    IPv4                    ip 0.0.0.0/0 0.0.0.0/0               QoS   0x1a316000
          0
      QoS    IPv4                    ip 0.0.0.0/0 0.0.0.0/0               QoS   0x1a316000
          0
```

This example shows how to view the history of TCAM entries monitored by iCAM.

```
switch# show icam entries acl module 3 inst 5 history 2
================================================================================================
TCAM Entries (Mod 3,Inst 5): Cumulative stats for last 2 intervals
------------------------------------------------------------------------------------------------
Feature  Pkt_Type                                    Source IP/Mask Dest IP/Mask    Action
      ifindex   Stats   Rate(pps)
------------------------------------------------------------------------------------------------

    FEX    IPv4                                          ip 0.0.0.0/0 0.0.0.0/0   Redirect
   0x15090000       0           0
    FEX    IPv6  ip 0x00000000000000000000000000000000/0 0x00000000000000000000  Redirect
   0x15090000       0           0
    FEX     MAC     0000.0000.0000 0000.0000.0000 0000.0000.0000 0000.0000.0000   Redirect
   0x15090000       0           0
    FEX     ARP  arp-rarp/all ip 0.0.0.0/0 0.0.0.0/0 0000.0000.0000 0000.0000.00  Redirect
   0x15090000       0           0
   RACL    IPv4                                  tcp 209.165.201.1/27 0.0.0.0/0     Permit
   0x1a10a000       0           0
   RACL    IPv4                                  tcp 209.165.201.2/27 0.0.0.0/0     Permit
   0x1a10a000       0           0
   RACL    IPv4                                  tcp 209.165.201.3/27 0.0.0.0/0     Permit
   0x1a10a000       0           0
   RACL    IPv4                                  tcp 209.165.201.4/27 0.0.0.0/0     Permit
   0x1a10a000       0           0
   RACL    IPv4                                  tcp 209.165.201.5/27 0.0.0.0/0     Permit
   0x1a10a000       0           0
QoS COPP   IPv4                                  udp 0.0.0.0/0 209.165.201.1/27        QoS
          0x0       0           0
```

```
QoS COPP   IPv4                                    udp 0.0.0.0/0 209.165.201.1/27        QoS
          0x0       0           0
QoS COPP   IPv4                                    udp 0.0.0.0/0 209.165.201.1/27        QoS
          0x0       0           0
QoS COPP   IPv4                                    udp 0.0.0.0/0 209.165.201.1/27        QoS
          0x0       0           0
QoS COPP   IPv4                                    udp 0.0.0.0/0 209.165.201.7/27        QoS
          0x0       0           0
QoS COPP   IPv4                                    udp 0.0.0.0/0 209.165.201.7/27        QoS
          0x0       0           0
QoS COPP   IPv4                                   udp 0.0.0.0/0 209.165.201.11/27        QoS
          0x0       0           0
QoS COPP   IPv4                                   udp 0.0.0.0/0 209.165.201.11/27        QoS
          0x0       0           0
```

This example shows how to view the history of top 1% of TCAM entries filtered by a feature name.

```
switch# show icam entries acl module 3 inst 5 history 2 sort filter "qos copp" top 1
```

```
================================================================================================================================
TCAM Entries (Mod 3,Inst 5): Cumulative stats for last 2 intervals
--------------------------------------------------------------------------------------------------------------------------------

 Feature  Pkt_Type                                        Source IP/Mask Dest IP/Mask    Action
    ifindex   Stats  Rate(pps)
--------------------------------------------------------------------------------------------------------------------------------
QoS COPP     MAC  0000.0000.0000 0000.0000.0000 0180.c200.000e ffff.ffff.ffff 350       QoS
        0x0      48          0
QoS COPP     MAC     0000.0000.0000 0000.0000.0000 0100.0ccc.cccc ffff.ffff.ffff        QoS
        0x0       4          0
QoS COPP    IPv4                                          tcp 0.0.0.0/0 0.0.0.0/0        QoS
        0x0       0          0
QoS COPP    IPv4                                          tcp 0.0.0.0/0 0.0.0.0/0        QoS
        0x0       0          0
```

This example displays the prediction for the traffic statistics of TCAM entries on a module and an instance for which iCAM monitoring is enabled.

```
switch# show icam prediction entries acl module 3 inst 5 2018 Jan 27 11:35:30
Generating predictions, this may take some time ...
```

```
================================================================================================================================
TCAM Entries Prediction (Mod 3,Inst 5)
--------------------------------------------------------------------------------------------------------------------------------

   Feature  Pkt_Type                                      Source IP/Mask Dest IP/Mask
Action     ifindex        Stats    Prediction
--------------------------------------------------------------------------------------------------------------------------------

  QoS COPP    IPv4                                           ip 0.0.0.0/0 0.0.0.0/0
QoS         0x0     38408890      38408890
  QoS COPP     MAC  0000.0000.0000 0000.0000.0000 0180.c200.000e ffff.ffff.ffff 350
QoS         0x0          485           501
  QoS COPP     MAC     0000.0000.0000 0000.0000.0000 0100.0ccc.cccc ffff.ffff.ffff
QoS         0x0           42            43
       FEX    IPv4                                        ip 0.0.0.0/0 0.0.0.0/0   Redirect
  0x15090000            0             0
```

This example displays the predictive analytics of the top 2% TCAM entries.

```
switch# show icam prediction entries acl module 3 inst 5 2018 Jan 27 11:35:30 top 2
Generating predictions, this may take some time ...
```

```
==============================================================================================================
TCAM Entries Prediction (Mod 3,Inst 5)
--------------------------------------------------------------------------------------------------------------

   Feature  Pkt_Type                                        Source IP/Mask Dest IP/Mask
Action     ifindex        Stats    Prediction
--------------------------------------------------------------------------------------------------------------

  QoS COPP    IPv4                                             ip 0.0.0.0/0 0.0.0.0/0
QoS         0x0      38408890     38408890
  QoS COPP     MAC  0000.0000.0000 0000.0000.0000 0180.c200.000e ffff.ffff.ffff 350
QoS         0x0           485          501
  QoS COPP     MAC     0000.0000.0000 0000.0000.0000 0100.0ccc.cccc ffff.ffff.ffff
QoS         0x0            42           43
      FEX    IPv6  ip 0x00000000000000000000000000000000/0 0x00000000000000000000  Redirect
  0x15090000             0            0
       FEX    IPv4                                           ip 0.0.0.0/0 0.0.0.0/0   Redirect
  0x15090000             0            0
      FEX    ARP  arp-rarp/all ip 0.0.0.0/0 0.0.0.0/0 0000.0000.0000 0000.0000.00  Redirect
  0x15090000             0            0
      FEX    MAC    0000.0000.0000 0000.0000.0000 0000.0000.0000 0000.0000.0000   Redirect
  0x15090000             0            0
```

This example shows how to view iCAM monitoring of the multicast entries for a current date.

```
switch# show icam entries multicast module 3
Retrieving data from linecard.  This may take some time ...

==============================================================================================================
Multicast Entries (Mod 3)
--------------------------------------------------------------------------------------------------------------

    VDC_ID       TABLE_ID          Source/Mask        Group/Mask                   RPF
       Stats
--------------------------------------------------------------------------------------------------------------

        1             1           0.0.0.0/0        209.165.201.9/27
          1
        1             1    209.165.201.18/27        209.165.201.10/27   Ethernet3/12
      912494
        1             1    209.165.201.19/27        209.165.201.10/27   Ethernet3/12
      912494
        1             1    209.165.201.20/27        209.165.201.10/27   Ethernet3/12
      912494
        1             1    209.165.201.21/27        209.165.201.10/27   Ethernet3/12
      912493
        1             1    209.165.201.22/27        209.165.201.10/27   Ethernet3/12
      912493
        1             1    209.165.201.23/27        209.165.201.10/27   Ethernet3/12
      912493
        1             1    209.165.201.24/27        209.165.201.10/27   Ethernet3/12
      912493
        1             1    209.165.201.25/27        209.165.201.10/27   Ethernet3/12
      912493
        1             1    209.165.201.26/27        209.165.201.10/27   Ethernet3/12
      912480
        1             1    209.165.201.27/27        209.165.201.10/27   Ethernet3/12
      912479
        1             1    209.165.201.28/27        209.165.201.10/27   Ethernet3/12
      912479
        1             1    209.165.201.29/27        209.165.201.10/27   Ethernet3/12
      912479
```

```
   1              1    209.165.201.30/27        209.165.201.10/27   Ethernet3/12
912479
   1              1   209.165.202.129/27        209.165.201.10/27   Ethernet3/12
912479
   1              1   209.165.202.130/27        209.165.201.10/27   Ethernet3/12
912479
   1              1   209.165.202.131/27        209.165.201.10/27   Ethernet3/12
912471
   1              1   209.165.202.132/27        209.165.201.10/27   Ethernet3/12
912470
   1              1   209.165.202.133/27        209.165.201.10/27   Ethernet3/12
912470
   1              1   209.165.202.134/27        209.165.201.10/27   Ethernet3/12
912442
   1              1   209.165.202.135/27        209.165.201.10/27   Ethernet3/12
912442
   1              1   209.165.202.136/27        209.165.201.10/27   Ethernet3/12
912442
   1              1   209.165.202.137/27        209.165.201.10/27   Ethernet3/12
912441
   1              1   209.165.202.138/27        209.165.201.10/27   Ethernet3/12
912441
   1              1   209.165.202.139/27        209.165.201.10/27   Ethernet3/12
912441
   1              1   209.165.202.140/27        209.165.201.10/27   Ethernet3/12
912441
   1              1   209.165.202.141/27        209.165.201.10/27   Ethernet3/12
912431
   1              1   209.165.202.142/27        209.165.201.10/27   Ethernet3/12
912431
   1              1   209.165.202.143/27        209.165.201.10/27   Ethernet3/12
912431
   1              1   209.165.202.144/27        209.165.201.10/27   Ethernet3/12
912431
   1              1   209.165.202.145/27        209.165.201.10/27   Ethernet3/12
912411
   1              1   209.165.202.146/27        209.165.201.10/27   Ethernet3/12
912412
   1              1   209.165.202.147/27        209.165.201.10/27   Ethernet3/12
912411
   1              1   209.165.202.148/27        209.165.201.10/27   Ethernet3/12
912411
   1              1   209.165.202.149/27        209.165.201.10/27   Ethernet3/12
912411
   1              1   209.165.202.150/27        209.165.201.10/27   Ethernet3/12
912345
   1              1   209.165.202.151/27        209.165.201.10/27   Ethernet3/12
912345
   1              1   209.165.202.152/27        209.165.201.10/27   Ethernet3/12
912345
   1              1   209.165.202.153/27        209.165.201.10/27   Ethernet3/12
912345
   1              1   209.165.202.154/27        209.165.201.10/27   Ethernet3/12
912345
   1              1   209.165.202.155/27        209.165.201.10/27   Ethernet3/12
912345
   1              1   209.165.202.156/27        209.165.201.10/27   Ethernet3/12
912344
   1              1   209.165.202.157/27        209.165.201.10/27   Ethernet3/12
912333
   1              1   209.165.202.158/27        209.165.201.10/27   Ethernet3/12
912333
```

This example shows how to view the top 1% multicast entries monitored by iCAM for a current date.

```
switch# show icam entries multicast module 3 sort top 1
Retrieving data from linecard. This may take some time ...
================================================================================================================
Multicast Entries (Mod 3)
----------------------------------------------------------------------------------------------------------------

    VDC_ID       TABLE_ID          Source/Mask        Group/Mask                   RPF
           Stats
----------------------------------------------------------------------------------------------------------------

         1              1   209.165.200.225/27        209.165.201.10/27   Ethernet3/12
          933495
         1              1   209.165.200.226/27        209.165.201.10/27   Ethernet3/12
          933491
         1              1   209.165.200.227/27        209.165.201.10/27   Ethernet3/12
          933488
         1              1   209.165.200.228/27        209.165.201.10/27   Ethernet3/12
          933483
         1              1   209.165.200.229/27        209.165.201.10/27   Ethernet3/12
          933483
         1              1   209.165.200.230/27        209.165.201.10/27   Ethernet3/12
          933480
         1              1   209.165.200.231/27        209.165.201.10/27   Ethernet3/12
          933476
         1              1   209.165.200.232/27        209.165.201.10/27   Ethernet3/12
          933474
         1              1   209.165.200.233/27        209.165.201.10/27   Ethernet3/12
          933469
         1              1   209.165.200.234/27        209.165.201.10/27   Ethernet3/12
          933469
         1              1   209.165.200.235/27        209.165.201.10/27   Ethernet3/12
          933466
         1              1   209.165.200.236/27        209.165.201.10/27   Ethernet3/12
          933462
         1              1   209.165.200.237/27        209.165.201.10/27   Ethernet3/12
          933456
         1              1   209.165.200.238/27        209.165.201.10/27   Ethernet3/12
          933455
         1              1     209.165.201.1/27        209.165.201.10/27   Ethernet3/12
          933455
         1              1     209.165.201.2/27        209.165.201.10/27   Ethernet3/12
          933452
         1              1     209.165.201.3/27        209.165.201.10/27   Ethernet3/12
          933449
         1              1     209.165.201.4/27        209.165.201.10/27   Ethernet3/12
          933442
         1              1     209.165.201.5/27        209.165.201.10/27   Ethernet3/12
          933441
         1              1     209.165.201.6/27        209.165.201.10/27   Ethernet3/12
          933441
         1              1     209.165.201.7/27        209.165.201.10/27   Ethernet3/12
          933441
         1              1     209.165.201.8/27        209.165.201.10/27   Ethernet3/12
          933435
         1              1     209.165.201.9/27        209.165.201.10/27   Ethernet3/12
          933434
         1              1    209.165.201.11/27        209.165.201.10/27   Ethernet3/12
          933418
         1              1    209.165.201.12/27        209.165.201.10/27   Ethernet3/12
          933202
         1              1    209.165.201.13/27        209.165.201.10/27   Ethernet3/12
          933202
```

```
1               1    209.165.201.14/27        209.165.201.10/27   Ethernet3/12
 933202
1               1    209.165.201.15/27        209.165.201.10/27   Ethernet3/12
 933202
1               1    209.165.201.16/27        209.165.201.10/27   Ethernet3/12
 933202
1               1    209.165.201.17/27        209.165.201.10/27   Ethernet3/12
 933202
1               1    209.165.201.18/27        209.165.201.10/27   Ethernet3/12
 933202
1               1    209.165.201.19/27        209.165.201.10/27   Ethernet3/12
 933202
1               1    209.165.201.20/27        209.165.201.10/27   Ethernet3/12
 933188
1               1    209.165.201.21/27        209.165.201.10/27   Ethernet3/12
 933187
1               1    209.165.201.22/27        209.165.201.10/27   Ethernet3/12
 933187
1               1    209.165.201.23/27        209.165.201.10/27   Ethernet3/12
 933187
1               1    209.165.201.24/27        209.165.201.10/27   Ethernet3/12
 933187
1               1    209.165.201.25/27        209.165.201.10/27   Ethernet3/12
 933187
1               1    209.165.201.26/27        209.165.201.10/27   Ethernet3/12
 933187
1               1    209.165.201.27/27        209.165.201.10/27   Ethernet3/12
 933179
1               1    209.165.201.28/27        209.165.201.10/27   Ethernet3/12
 933178
1               1    209.165.201.29/27        209.165.201.10/27   Ethernet3/12
 933178
1               1    209.165.201.30/27        209.165.201.10/27   Ethernet3/12
 933150
1               1   209.165.202.129/27        209.165.201.10/27   Ethernet3/12
 933150
1               1   209.165.202.130/27        209.165.201.10/27   Ethernet3/12
 933150
1               1   209.165.202.131/27        209.165.201.10/27   Ethernet3/12
 933149
1               1   209.165.202.132/27        209.165.201.10/27   Ethernet3/12
 933149
1               1   209.165.202.133/27        209.165.201.10/27   Ethernet3/12
 933149
1               1   209.165.202.134/27        209.165.201.10/27   Ethernet3/12
 933149
1               1   209.165.202.135/27        209.165.201.10/27   Ethernet3/12
 933139
```

This example shows how to view the history of multicast entries monitored by iCAM.

```
switch# show icam entries multicast module 3 history 2
================================================================================================================================
Multicast Entries (Mod 3): Cumulative stats for last 2 intervals
--------------------------------------------------------------------------------------------------------------------------------

    VDC_ID       TABLE_ID          Source/Mask       Group/Mask                  RPF
          Stats      Rate(pps)
--------------------------------------------------------------------------------------------------------------------------------

        1              1           0.0.0.0/0        209.165.201.9/27
             0              0
        1              1    209.165.201.18/27       209.165.201.10/27   Ethernet3/12
        165792            690
```

```
1               1    209.165.201.19/27       209.165.201.10/27   Ethernet3/12
165792             690
1               1    209.165.201.20/27       209.165.201.10/27   Ethernet3/12
165793             690
1               1    209.165.201.21/27       209.165.201.10/27   Ethernet3/12
165793             690
1               1    209.165.201.22/27       209.165.201.10/27   Ethernet3/12
165792             690
1               1    209.165.201.23/27       209.165.201.10/27   Ethernet3/12
165792             690
1               1    209.165.201.24/27       209.165.201.10/27   Ethernet3/12
165792             690
1               1    209.165.201.25/27       209.165.201.10/27   Ethernet3/12
165792             690
1               1    209.165.201.26/27       209.165.201.10/27   Ethernet3/12
165792             690
1               1    209.165.201.27/27       209.165.201.10/27   Ethernet3/12
165792             690
1               1    209.165.201.28/27       209.165.201.10/27   Ethernet3/12
165792             690
1               1    209.165.201.29/27       209.165.201.10/27   Ethernet3/12
165792             690
1               1    209.165.201.30/27       209.165.201.10/27   Ethernet3/12
165792             690
1               1   209.165.202.129/27       209.165.201.10/27   Ethernet3/12
165792             690
1               1   209.165.202.130/27       209.165.201.10/27   Ethernet3/12
165792             690
1               1   209.165.202.131/27       209.165.201.10/27   Ethernet3/12
165792             690
1               1   209.165.202.132/27       209.165.201.10/27   Ethernet3/12
165792             690
1               1   209.165.202.133/27       209.165.201.10/27   Ethernet3/12
165792             690
1               1   209.165.202.134/27       209.165.201.10/27   Ethernet3/12
165792             690
1               1   209.165.202.135/27       209.165.201.10/27   Ethernet3/12
165792             690
1               1   209.165.202.136/27       209.165.201.10/27   Ethernet3/12
165792             690
1               1   209.165.202.137/27       209.165.201.10/27   Ethernet3/12
165792             690
1               1   209.165.202.138/27       209.165.201.10/27   Ethernet3/12
165792             690
1               1   209.165.202.139/27       209.165.201.10/27   Ethernet3/12
165792             690
1               1   209.165.202.140/27       209.165.201.10/27   Ethernet3/12
165792             690
1               1   209.165.202.141/27       209.165.201.10/27   Ethernet3/12
165792             690
1               1   209.165.202.142/27       209.165.201.10/27   Ethernet3/12
165792             690
1               1   209.165.202.143/27       209.165.201.10/27   Ethernet3/12
165792             690
1               1   209.165.202.144/27       209.165.201.10/27   Ethernet3/12
165792             690
1               1   209.165.202.145/27       209.165.201.10/27   Ethernet3/12
165792             690
1               1   209.165.202.146/27       209.165.201.10/27   Ethernet3/12
165792             690
1               1   209.165.202.147/27       209.165.201.10/27   Ethernet3/12
165792             690
1               1   209.165.202.148/27       209.165.201.10/27   Ethernet3/12
165792             690
```

```
        1             1   209.165.202.149/27       209.165.201.10/27   Ethernet3/12
        165792           690
        1             1   209.165.202.150/27       209.165.201.10/27   Ethernet3/12
        165792           690
        1             1   209.165.202.151/27       209.165.201.10/27   Ethernet3/12
        165792           690
        1             1   209.165.202.152/27       209.165.201.10/27   Ethernet3/12
        165792           690
        1             1   209.165.202.153/27       209.165.201.10/27   Ethernet3/12
        165792           690
        1             1   209.165.202.154/27       209.165.201.10/27   Ethernet3/12
        165792           690
        1             1   209.165.202.155/27       209.165.201.10/27   Ethernet3/12
        165792           690
        1             1   209.165.202.156/27       209.165.201.10/27   Ethernet3/12
        165792           690
        1             1   209.165.202.157/27       209.165.201.10/27   Ethernet3/12
        165792           690
        1             1   209.165.202.158/27       209.165.201.10/27   Ethernet3/12
        165792           690
.
.
.
```

This example shows how to view the history of top 1% multicast entries monitored by iCAM.

```
switch# show icam entries multicast module 3 history 2 sort top 1
```

```
Multicast Entries (Mod 3): Cumulative stats for last 2 intervals
-------------------------------------------------------------------------------------------------------------

    VDC_ID       TABLE_ID          Source/Mask        Group/Mask                  RPF
           Stats      Rate(pps)
-------------------------------------------------------------------------------------------------------------

        1             1   209.165.200.225/27       209.165.201.10/27   Ethernet3/12
         165725           690
        1             1   209.165.200.226/27       209.165.201.10/27   Ethernet3/12
         165725           690
        1             1   209.165.200.227/27       209.165.201.10/27   Ethernet3/12
         165725           690
        1             1   209.165.200.228/27       209.165.201.10/27   Ethernet3/12
         165725           690
        1             1   209.165.200.229/27       209.165.201.10/27   Ethernet3/12
         165725           690
        1             1   209.165.200.230/27       209.165.201.10/27   Ethernet3/12
         165725           690
        1             1   209.165.200.231/27       209.165.201.10/27   Ethernet3/12
         165725           690
        1             1   209.165.200.232/27       209.165.201.10/27   Ethernet3/12
         165725           690
        1             1   209.165.200.233/27       209.165.201.10/27   Ethernet3/12
         165725           690
        1             1   209.165.200.234/27       209.165.201.10/27   Ethernet3/12
         165725           690
        1             1   209.165.200.235/27       209.165.201.10/27   Ethernet3/12
         165724           690
        1             1   209.165.200.236/27       209.165.201.10/27   Ethernet3/12
         165724           690
        1             1   209.165.200.237/27       209.165.201.10/27   Ethernet3/12
         165724           690
        1             1   209.165.200.238/27       209.165.201.10/27   Ethernet3/12
         165724           690
        1             1     209.165.201.1/27       209.165.201.10/27   Ethernet3/12
```

```
 165724            690
1              1     209.165.201.2/27        209.165.201.10/27   Ethernet3/12
 165724            690
1              1     209.165.201.3/27        209.165.201.10/27   Ethernet3/12
 165724            690
1              1     209.165.201.4/27        209.165.201.10/27   Ethernet3/12
 165724            690
1              1     209.165.201.5/27        209.165.201.10/27   Ethernet3/12
 165724            690
1              1     209.165.201.6/27        209.165.201.10/27   Ethernet3/12
 165724            690
1              1     209.165.201.7/27        209.165.201.10/27   Ethernet3/12
 165724            690
1              1     209.165.201.8/27        209.165.201.10/27   Ethernet3/12
 165724            690
1              1     209.165.201.9/27        209.165.201.10/27   Ethernet3/12
 165724            690
1              1    209.165.201.11/27        209.165.201.10/27   Ethernet3/12
 165724            690
1              1    209.165.201.12/27        209.165.201.10/27   Ethernet3/12
 165724            690
1              1    209.165.201.13/27        209.165.201.10/27   Ethernet3/12
 165724            690
1              1    209.165.201.14/27        209.165.201.10/27   Ethernet3/12
 165724            690
1              1    209.165.201.15/27        209.165.201.10/27   Ethernet3/12
 165724            690
1              1    209.165.201.16/27        209.165.201.10/27   Ethernet3/12
 165724            690
1              1    209.165.201.17/27        209.165.201.10/27   Ethernet3/12
 165724            690
1              1    209.165.201.18/27        209.165.201.10/27   Ethernet3/12
 165724            690
1              1    209.165.201.19/27        209.165.201.10/27   Ethernet3/12
 165724            690
1              1    209.165.201.20/27        209.165.201.10/27   Ethernet3/12
 165724            690
1              1    209.165.201.21/27        209.165.201.10/27   Ethernet3/12
 165724            690
1              1    209.165.201.22/27        209.165.201.10/27   Ethernet3/12
 165724            690
1              1    209.165.201.23/27        209.165.201.10/27   Ethernet3/12
 165724            690
1              1    209.165.201.24/27        209.165.201.10/27   Ethernet3/12
 165724            690
1              1    209.165.201.25/27        209.165.201.10/27   Ethernet3/12
 165724            690
1              1    209.165.201.26/27        209.165.201.10/27   Ethernet3/12
 165724            690
1              1    209.165.201.27/27        209.165.201.10/27   Ethernet3/12
 165724            690
1              1    209.165.201.28/27        209.165.201.10/27   Ethernet3/12
 165724            690
1              1    209.165.201.29/27        209.165.201.10/27   Ethernet3/12
 165724            690
1              1    209.165.201.30/27        209.165.201.10/27   Ethernet3/12
 165724            690
1              1   209.165.202.129/27        209.165.201.10/27   Ethernet3/12
 165724            690
1              1   209.165.202.130/27        209.165.201.10/27   Ethernet3/12
 165724            690
1              1   209.165.202.131/27        209.165.201.10/27   Ethernet3/12
 165724            690
1              1   209.165.202.132/27        209.165.201.10/27   Ethernet3/12
```

```
 165724            690
1              1   209.165.202.133/27        209.165.201.10/27   Ethernet3/12
 165724            690
1              1   209.165.202.134/27        209.165.201.10/27   Ethernet3/12
 165724            690
1              1   209.165.202.135/27        209.165.201.10/27   Ethernet3/12
 165724            690
```

This example displays the predictive analytics of the multicast entries.

```
switch# show icam prediction entries multicast module 3 2020 Jul 19 08:10:29
Generating predictions, this may take some time ...

================================================================================================================================
Multicast Entries Prediction (Mod 3)
--------------------------------------------------------------------------------------------------------------------------------

    VDC_ID       TABLE_ID           Source/Mask                Group/Mask             RPF
              Stats         Prediction
--------------------------------------------------------------------------------------------------------------------------------

         1              1    209.165.202.129/27        209.165.200.225/27   Ethernet3/12
           1679387            1679387
         1              1     209.165.201.23/27        209.165.200.225/27   Ethernet3/12
           1679419            1679419
         1              1     209.165.201.24/27        209.165.200.225/27   Ethernet3/12
           1679411            1679411
         1              1     209.165.201.25/27        209.165.200.225/27   Ethernet3/12
           1679411            1679411
         1              1     209.165.201.26/27        209.165.200.225/27   Ethernet3/12
           1679411            1679411
         1              1     209.165.201.27/27        209.165.200.225/27   Ethernet3/12
           1679411            1679411
         1              1     209.165.201.28/27        209.165.200.225/27   Ethernet3/12
           1679404            1679404
         1              1     209.165.201.29/27        209.165.200.225/27   Ethernet3/12
           1679403            1679403
         1              1     209.165.201.30/27        209.165.200.225/27   Ethernet3/12
           1679403            1679403
         1              1      209.165.201.8/27        209.165.200.225/27   Ethernet3/12
           1679113            1679113
         1              1      209.165.201.7/27        209.165.200.225/27   Ethernet3/12
           1679113            1679113
         1              1      209.165.201.4/27        209.165.200.225/27   Ethernet3/12
           1679141            1679141
         1              1      209.165.201.3/27        209.165.200.225/27   Ethernet3/12
           1679142            1679142
         1              1      209.165.201.6/27        209.165.200.225/27   Ethernet3/12
           1679113            1679113
         1              1      209.165.201.5/27        209.165.200.225/27   Ethernet3/12
           1679141            1679141
         1              1    209.165.200.238/27        209.165.200.225/27   Ethernet3/12
           1679150            1679150
         1              1    209.165.200.237/27        209.165.200.225/27   Ethernet3/12
           1679150            1679150
         1              1      209.165.201.2/27        209.165.200.225/27   Ethernet3/12
           1679150            1679150
         1              1      209.165.201.1/27        209.165.200.225/27   Ethernet3/12
           1679150            1679150
         1              1    209.165.200.226/27        209.165.200.225/27   Ethernet3/12
           1679166            1679166
         1              1     209.165.201.22/27        209.165.200.225/27   Ethernet3/12
           1679422            1679422
         1              1     209.165.201.21/27        209.165.200.225/27   Ethernet3/12
           1679424            1679424
```

```
        1             1     209.165.201.20/27        209.165.200.225/27   Ethernet3/12
          1679424           1679424
        1             1     209.165.201.19/27        209.165.200.225/27   Ethernet3/12
          1679425           1679425
        1             1     209.165.201.18/27        209.165.200.225/27   Ethernet3/12
          1679431           1679431
        1             1     209.165.201.17/27        209.165.200.225/27   Ethernet3/12
          1679435           1679435
        1             1     209.165.201.16/27        209.165.200.225/27   Ethernet3/12
          1679438           1679438
        1             1     209.165.201.15/27        209.165.200.225/27   Ethernet3/12
          1679438           1679438
        1             1     209.165.201.14/27        209.165.200.225/27   Ethernet3/12
          1679443           1679443
        1             1     209.165.201.13/27        209.165.200.225/27   Ethernet3/12
          1679445           1679445
        1             1    209.165.200.235/27        209.165.200.225/27   Ethernet3/12
          1679150           1679150
        1             1    209.165.200.236/27        209.165.200.225/27   Ethernet3/12
          1679150           1679150
        1             1    209.165.200.233/27        209.165.200.225/27   Ethernet3/12
          1679165           1679165
        1             1    209.165.200.234/27        209.165.200.225/27   Ethernet3/12
          1679151           1679151
        1             1    209.165.200.231/27        209.165.200.225/27   Ethernet3/12
          1679165           1679165
        1             1    209.165.200.232/27        209.165.200.225/27   Ethernet3/12
          1679165           1679165
        1             1    209.165.200.229/27        209.165.200.225/27   Ethernet3/12
          1679165           1679165
        1             1    209.165.200.230/27        209.165.200.225/27   Ethernet3/12
          1679165           1679165
        1             1    209.165.200.227/27        209.165.200.225/27   Ethernet3/12
          1679166           1679166
        1             1    209.165.200.228/27        209.165.200.225/27   Ethernet3/12
          1679166           1679166
        1             1     209.165.201.12/27        209.165.200.225/27   Ethernet3/12
          1679103           1679103
        1             1      209.165.201.9/27        209.165.200.225/27   Ethernet3/12
          1679112           1679112
        1             1     209.165.201.10/27        209.165.200.225/27   Ethernet3/12
          1679113           1679113
        1             1     209.165.201.11/27        209.165.200.225/27   Ethernet3/12
          1679113           1679113
.
.
.
```

This example displays the predictive analytics of the top 1% multicast entries.

```
switch# show icam prediction entries multicast module 3 2020 Jul 19 08:10:29 top 1
Generating predictions, this may take some time ...

================================================================================================================================
Multicast Entries Prediction (Mod 3)
--------------------------------------------------------------------------------------------------------------------------------

    VDC_ID       TABLE_ID           Source/Mask               Group/Mask            RPF
      Stats   Prediction
--------------------------------------------------------------------------------------------------------------------------------

        1             1    209.165.202.129/27        209.165.200.225/27   Ethernet3/12
    1679387      1679387
```

```
     1             1     209.165.201.23/27        209.165.200.225/27   Ethernet3/12
1679419       1679419
     1             1     209.165.201.24/27        209.165.200.225/27   Ethernet3/12
1679411       1679411
     1             1     209.165.201.25/27        209.165.200.225/27   Ethernet3/12
1679411       1679411
     1             1     209.165.201.26/27        209.165.200.225/27   Ethernet3/12
1679411       1679411
     1             1     209.165.201.27/27        209.165.200.225/27   Ethernet3/12
1679411       1679411
     1             1     209.165.201.28/27        209.165.200.225/27   Ethernet3/12
1679404       1679404
     1             1     209.165.201.29/27        209.165.200.225/27   Ethernet3/12
1679403       1679403
     1             1     209.165.201.30/27        209.165.200.225/27   Ethernet3/12
1679403       1679403
     1             1      209.165.201.8/27        209.165.200.225/27   Ethernet3/12
1679113       1679113
     1             1      209.165.201.7/27        209.165.200.225/27   Ethernet3/12
1679113       1679113
     1             1      209.165.201.4/27        209.165.200.225/27   Ethernet3/12
1679141       1679141
     1             1      209.165.201.3/27        209.165.200.225/27   Ethernet3/12
1679142       1679142
     1             1      209.165.201.6/27        209.165.200.225/27   Ethernet3/12
1679113       1679113
     1             1      209.165.201.5/27        209.165.200.225/27   Ethernet3/12
1679141       1679141
     1             1    209.165.200.238/27        209.165.200.225/27   Ethernet3/12
1679150       1679150
     1             1    209.165.200.237/27        209.165.200.225/27   Ethernet3/12
1679150       1679150
     1             1      209.165.201.2/27        209.165.200.225/27   Ethernet3/12
1679150       1679150
     1             1      209.165.201.1/27        209.165.200.225/27   Ethernet3/12
1679150       1679150
     1             1    209.165.200.226/27        209.165.200.225/27   Ethernet3/12
1679166       1679166
     1             1     209.165.201.22/27        209.165.200.225/27   Ethernet3/12
1679422       1679422
     1             1     209.165.201.21/27        209.165.200.225/27   Ethernet3/12
1679424       1679424
     1             1     209.165.201.20/27        209.165.200.225/27   Ethernet3/12
1679424       1679424
     1             1     209.165.201.19/27        209.165.200.225/27   Ethernet3/12
1679425       1679425
     1             1     209.165.201.18/27        209.165.200.225/27   Ethernet3/12
1679431       1679431
     1             1     209.165.201.17/27        209.165.200.225/27   Ethernet3/12
1679435       1679435
     1             1     209.165.201.16/27        209.165.200.225/27   Ethernet3/12
1679438       1679438
     1             1     209.165.201.15/27        209.165.200.225/27   Ethernet3/12
1679438       1679438
     1             1     209.165.201.14/27        209.165.200.225/27   Ethernet3/12
1679443       1679443
     1             1     209.165.201.13/27        209.165.200.225/27   Ethernet3/12
1679445       1679445
     1             1    209.165.200.235/27        209.165.200.225/27   Ethernet3/12
1679150       1679150
     1             1    209.165.200.236/27        209.165.200.225/27   Ethernet3/12
1679150       1679150
     1             1    209.165.200.233/27        209.165.200.225/27   Ethernet3/12
1679165       1679165
```

```
        1              1    209.165.200.234/27        209.165.200.225/27   Ethernet3/12
    1679151      1679151
        1              1    209.165.200.231/27        209.165.200.225/27   Ethernet3/12
    1679165      1679165
        1              1    209.165.200.232/27        209.165.200.225/27   Ethernet3/12
    1679165      1679165
        1              1    209.165.200.229/27        209.165.200.225/27   Ethernet3/12
    1679165      1679165
        1              1    209.165.200.230/27        209.165.200.225/27   Ethernet3/12
    1679165      1679165
        1              1    209.165.200.227/27        209.165.200.225/27   Ethernet3/12
    1679166      1679166
        1              1    209.165.200.228/27        209.165.200.225/27   Ethernet3/12
    1679166      1679166
        1              1     209.165.201.12/27        209.165.200.225/27   Ethernet3/12
    1679103      1679103
        1              1      209.165.201.9/27        209.165.200.225/27   Ethernet3/12
    1679112      1679112
        1              1     209.165.201.10/27        209.165.200.225/27   Ethernet3/12
    1679113      1679113
        1              1     209.165.201.11/27        209.165.200.225/27   Ethernet3/12
    1679113      1679113
.
.
.
```

This example shows how to view iCAM monitoring of the ACL TCAM resources for a current date.

```
switch# show icam resource acl-tcam module 3 inst 4
--------------------------------------------------------------------------------------------
Feature Hardware Resource Utilization (Mod 3,Inst 4)
--------------------------------------------------------------------------------------------

Ingress Resources
--------------------------------------------------------------------------------------------
    Feature TCAM# BANK# Feature_Entries   Free_Entries   Percent_Util     Timestamp (UTC)
--------------------------------------------------------------------------------------------
       PACL     0     0               4           4072           0.09 2017-09-05 22:05:28
       CoPP     1     1             420           3656          10.25 2017-09-05 22:05:28
FEX Control     1     0               5           4071           0.12 2017-09-05 22:05:28

Egress Resources
--------------------------------------------------------------------------------------------
    Feature TCAM# BANK# Feature_Entries   Free_Entries   Percent_Util     Timestamp (UTC)
--------------------------------------------------------------------------------------------

============================================================================================
ACL TCAM Resource Utilization (Mod 3,Inst 4)
--------------------------------------------------------------------------------------------
                  Used    Free   Percent_Util          Timestamp (UTC)
--------------------------------------------------------------------------------------------
Tcam 0 Bank 0       24    4072           0.58      2017-09-05 22:05:28
Tcam 0 Bank 1       20    4076           0.48      2017-09-05 22:05:28
Tcam 1 Bank 0       25    4071           0.61      2017-09-05 22:05:28
Tcam 1 Bank 1      440    3656          10.74      2017-09-05 22:05:28
```

This example shows how to view the history of iCAM monitoring of the ACL TCAM resources.

```
switch# show icam resource acl-tcam module 3 inst 4 history 2
--------------------------------------------------------------------------------------------
Feature Hardware Resource Utilization (Mod 3,Inst 4)
--------------------------------------------------------------------------------------------
```

```
Ingress Resources
---------------------------------------------------------------------------------------
    Feature TCAM# BANK# Feature_Entries   Free_Entries   Percent_Util     Timestamp (UTC)
---------------------------------------------------------------------------------------
       PACL     0     0               4           4072           0.09 2017-09-05 22:09:12
                                      4           4072           0.09 2017-09-05 23:09:12
       CoPP     1     1             420           3656          10.25 2017-09-05 22:09:12
                                    420           3656          10.25 2017-09-05 23:09:12
FEX Control     1     0               5           4071           0.12 2017-09-05 22:09:12
                                      5           4071           0.12 2017-09-05 23:09:12

Egress Resources
---------------------------------------------------------------------------------------
        Feature TCAM# BANK# Feature_Entries   Free_Entries   Percent_Util Timestamp (UTC)
---------------------------------------------------------------------------------------

=======================================================================================
ACL TCAM Resource Utilization (Mod 3,Inst 4)
---------------------------------------------------------------------------------------
                  Used    Free   Percent_Util          Timestamp (UTC)
---------------------------------------------------------------------------------------
Tcam 0 Bank 0       24    4072           0.58      2017-09-05 22:09:12
                    24    4072           0.58      2017-09-05 23:09:12
Tcam 0 Bank 1       20    4076           0.48      2017-09-05 22:09:12
                    20    4076           0.48      2017-09-05 23:09:12
Tcam 1 Bank 0       25    4071           0.61      2017-09-05 22:09:12
                    25    4071           0.61      2017-09-05 23:09:12
Tcam 1 Bank 1      440    3656          10.74      2017-09-05 22:09:12
                   440    3656          10.74      2017-09-05 23:09:12
```

This example shows how to view iCAM monitoring of the FIB TCAM resources for a current date.

```
switch# show icam resource fib-tcam module 3 inst 5
=======================================================================================
FIB TCAM Resource Utilization (Mod 3, Inst 5)
---------------------------------------------------------------------------------
          Type        logical       physical   Percent_Util          Timestamp (UTC)
---------------------------------------------------------------------------------
  IPV4 unicast             16             16           0.02      2017-09-05 22:09:19
       DIAG_80              1              1           0.00      2017-09-05 22:09:19
IPV4 multicast           5005           5005           7.82      2017-09-05 22:09:19
          MPLS              0              0           0.00      2017-09-05 22:09:19
      EOM Peer              0              0           0.00      2017-09-05 22:09:19
      MPLS VPN              0              0           0.00      2017-09-05 22:09:19
        FCMPLS              0              0           0.00      2017-09-05 22:09:19
          FCOE              0              0           0.00      2017-09-05 22:09:19
IPV6 LinkLocal              1              2           0.00      2017-09-05 22:09:19
  IPV6 unicast              4              8           0.01      2017-09-05 22:09:19
IPV6 multicast              5             20           0.03      2017-09-05 22:09:19
```

This example shows how to view the history of the FIB TCAM resources monitored by iCAM.

```
switch# show icam resource fib-tcam module 3 inst 5 history 2
=======================================================================================
FIB TCAM Resource Utilization (Mod 3, Inst 5)
---------------------------------------------------------------------------------
          Type        logical       physical   Percent_Util          Timestamp (UTC)
---------------------------------------------------------------------------------
  IPV4 unicast             16             16           0.02      2017-09-05 22:17:14
                           16             16           0.02      2017-09-05 23:17:14
       DIAG_80              1              1           0.00      2017-09-05 22:17:14
                            1              1           0.00      2017-09-05 23:17:14
```

```
IPV4 multicast          5005           5005           7.82      2017-09-05 22:17:14
                        5005           5005           7.82      2017-09-05 23:17:14
          MPLS             0              0           0.00      2017-09-05 22:17:14
                           0              0           0.00      2017-09-05 23:17:14
      EOM Peer             0              0           0.00      2017-09-05 22:17:14
                           0              0           0.00      2017-09-05 23:17:14
      MPLS VPN             0              0           0.00      2017-09-05 22:17:14
                           0              0           0.00      2017-09-05 23:17:14
        FCMPLS             0              0           0.00      2017-09-05 22:17:14
                           0              0           0.00      2017-09-05 23:17:14
          FCOE             0              0           0.00      2017-09-05 22:17:14
                           0              0           0.00      2017-09-05 23:17:14
IPV6 LinkLocal             1              2           0.00      2017-09-05 22:17:14
                           1              2           0.00      2017-09-05 23:17:14
  IPV6 unicast             4              8           0.01      2017-09-05 22:17:14
                           4              8           0.01      2017-09-05 23:17:14
IPV6 multicast             5             20           0.03      2017-09-05 22:17:14
                           5             20           0.03      2017-09-05 23:17:14
```

This example shows how to view the history of the FIB TCAM resources monitored by iCAM.

```
switch# show icam resource fib-tcam module 3 inst 5 history 4
================================================================================
FIB TCAM Resource Utilization (Mod 3, Inst 5)
--------------------------------------------------------------------------------
          Type        logical       physical   Percent_Util          Timestamp (UTC)
--------------------------------------------------------------------------------
  IPV4 unicast            16             16           0.02      2017-09-05 22:13:13
                          16             16           0.02      2017-09-05 23:13:13
                          16             16           0.02      2017-09-06 00:13:14
                          16             16           0.02      2017-09-06 01:13:14
       DIAG_80             1              1           0.00      2017-09-05 22:13:13
                           1              1           0.00      2017-09-05 23:13:13
                           1              1           0.00      2017-09-06 00:13:14
                           1              1           0.00      2017-09-06 01:13:14
 IV4 multicast          5005           5005           7.82      2017-09-05 22:13:13
                        5005           5005           7.82      2017-09-05 23:13:13
                        5005           5005           7.82      2017-09-06 00:13:14
                        5005           5005           7.82      2017-09-06 01:13:14
          MPLS             0              0           0.00      2017-09-05 22:13:13
                           0              0           0.00      2017-09-05 23:13:13
                           0              0           0.00      2017-09-06 00:13:14
                           0              0           0.00      2017-09-06 01:13:14
      EOM Peer             0              0           0.00      2017-09-05 22:13:13
                           0              0           0.00      2017-09-05 23:13:13
                           0              0           0.00      2017-09-06 00:13:14
                           0              0           0.00      2017-09-06 01:13:14
      MPLS VPN             0              0           0.00      2017-09-05 22:13:13
                           0              0           0.00      2017-09-05 23:13:13
                           0              0           0.00      2017-09-06 00:13:14
                           0              0           0.00      2017-09-06 01:13:14
        FCMPLS             0              0           0.00      2017-09-05 22:13:13
                           0              0           0.00      2017-09-05 23:13:13
                           0              0           0.00      2017-09-06 00:13:14
                           0              0           0.00      2017-09-06 01:13:14
          FCOE             0              0           0.00      2017-09-05 22:13:13
                           0              0           0.00      2017-09-05 23:13:13
                           0              0           0.00      2017-09-06 00:13:14
                           0              0           0.00      2017-09-06 01:13:14
IPV6 LinkLocal             1              2           0.00      2017-09-05 22:13:13
                           1              2           0.00      2017-09-05 23:13:13
                           1              2           0.00      2017-09-06 00:13:14
                           1              2           0.00      2017-09-06 01:13:14
```

```
  IPV6 unicast              4              8           0.01      2017-09-05 22:13:13
                            4              8           0.01      2017-09-05 23:13:13
                            4              8           0.01      2017-09-06 00:13:14
                            4              8           0.01      2017-09-06 01:13:14
IPV6 multicast              5             20           0.03      2017-09-05 22:13:13
                            5             20           0.03      2017-09-05 23:13:13
                            5             20           0.03      2017-09-06 00:13:14
                            5             20           0.03      2017-09-06 01:13:14
```

This example displays the predictive analytics of the ACL TCAM resources.

```
switch# show icam prediction resource acl-tcam module 3 inst 4 2018 Jan 27 11:35:30
Generating predictions, this may take some time ...

-----------------------------------------------------------------------------------------------
Feature Hardware Resource Prediction (Mod 3,Inst 4)
-----------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------

       Feature   Direction   TCAM#   BANK#   Feature_Entries    Free_Entries    Percent_Util
-----------------------------------------------------------------------------------------------

           PACL     ingress       0       0                 4            4072
0.00
    FEX Control     ingress       1       0                 5            4071
0.00
           CoPP     ingress       1       1               420            3656
10.00

===============================================================================================
ACL TCAM Resource Prediction (Mod 3,Inst 4)
-----------------------------------------------------------------------------------------------

                  Used    Free   Percent_Util
-----------------------------------------------------------------------------------------------
Tcam 1 Bank 1      440    3656          10.74
Tcam 1 Bank 0       25    4071           0.61
Tcam 0 Bank 1       20    4076           0.48
Tcam 0 Bank 0       24    4072           0.58
```

This example displays the predictive analytics of the FIB TCAM resources.

```
switch# show icam prediction resource fib-tcam module 3 inst 5 2025 Dec 20 10:20:37
Generating predictions, this may take some time ...

============================================================
 FIB TCAM Resource Prediction (Mod 3, Inst 5)
------------------------------------------------------------
           Type        logical       physical   Percent_Util
------------------------------------------------------------
         FCMPLS              0              0           0.00
   IPV4 unicast             16             16           0.00
        DIAG_80              1              1           0.00
       EOM Peer              0              0           0.00
           MPLS              0              0           0.00
 IPV6 multicast              5             20           0.00
 IPV6 LinkLocal              1              2           0.00
           FCOE              0              0           0.00
       MPLS VPN              0              0           0.00
 IPV4 multicast           5005           5005           7.00
   IPV6 unicast              4              8           0.00
```

Example: Obtaining JSON Outputs for iCAM Configurations

This example shows how to view top 1% TCAM entries for a current date in JSON format.

```
switch# show icam entries acl module 5 inst 0 sort top 1 | json
{"module": 5,
"instance": 0,
"TABLE_ACL_entries": {
 "ROW_ACL_entries": [
  {
   "Feature": "QoS COPP",
   "Pkt_Type": "IPv4",
   "SourceIP_Mask_DestIP_Mask": "ip 0.0.0.0/0 0.0.0.0/0",
   "Action": "QoS",
   "ifindex": "0x0"
   "Stats": 2637573806
  },
  {
   "Feature": "RACL",
   "Pkt_Type": "IPv4",
   "SourceIP_Mask_DestIP_Mask": "ip 209.165.201.1/27 209.165.201.2/27",
   "Action": "Permit",
   "ifindex": "0x1a200000"
   "Stats": 1247078657
  },
  {
   "Feature": "QoS COPP",
   "Pkt_Type": "IPv4",
   "SourceIP_Mask_DestIP_Mask": "ip 0.0.0.0/0 0.0.0.0/0",
   "Action": "QoS",
   "ifindex": "0x0"
   "Stats": 745341269
  },
  {
   "Feature": "RACL",
   "Pkt_Type": "IPv4",
   "SourceIP_Mask_DestIP_Mask": "ip 209.165.201.3/27 209.165.201.4/27",
   "Action": "Permit",
   "ifindex": "0x1a200000"
   "Stats": 745341269
  }
 ]
}
}
```

This example shows how to view top 10% multicast entries for a current date in JSON format.

```
switch# show icam entries multicast module 5 sort top 10 | json
{
 "module": 5,
 "TABLE_MULTICAST_entries": {
  "ROW_ACL_entries": {
   "Vdc": 1,
   "Table_Id": 1,
   "Source_Mask": "209.165.201.18/27",
   "Group_Mask": "209.165.201.10/27",
   "Rpf": "Ethernet5/2"
   "Stats": 5318470244
  }
 }
}
```

This example shows how to view iCAM monitoring of the ACL TCAM resources for a current date in JSON format.

```
switch# show icam resource acl_tcam module 5 inst 0 | json
{
  "module": 5,
  "instance": 0,
  "TABLE_feature_resource": {
   "ROW_feature_resource": [
    {
     "Feature": "CoPP",
     "TCAM": 1,
     "BANK": 1,
      "TABLE_ingress_stats": {
       "ROW_ingress_stats": {
        "Feature_Entries": 442,
        "Free_Entries": 32306,
        "Percent_Util": 1.34,
        "Timestamp": "2017-08-09 14:36:19"
        }
       }
      },
     {
     "Feature": "FEX Control",
     "TCAM": 1,
     "BANK": 0,
      "TABLE_ingress_stats": {
       "ROW_ingress_stats": {
        "Feature_Entries": 5,
        "Free_Entries": 32733,
        "Percent_Util": 0.01,
        "Timestamp": "2017-08-09 14:36:19"
        }
       }
      },
    {
     "Feature": "RACL",
     "TCAM": 1,
     "BANK": 0,
      "TABLE_ingress_stats": {
       "ROW_ingress_stats": {
        "Feature_Entries": 10,
        "Free_Entries": 32733,
        "Percent_Util": 0.03,
        "Timestamp": "2017-08-09 14:36:19"
        }
       }
      }
     ]
    },
   "mod": 5,
   "inst": 0,
   "TABLE_tcam_bank_utilization": {
    "ROW_tcam_bank_utilization": {
     {
      "Tcam_no": "Tcam 0",
      "Bank_no": "Bank 0",
      "TABLE_tcam_bank_stats": {
       "ROW_tcam_bank_stats": {
        "Used": 20,
        "Free": 32748,
        "Percent_Util": 0.06,
        "Timestamp": "2017-08-09 14:36:19"
        }
```

```
      }
     },
     {
      "Tcam_no": "Tcam 0",
      "Bank_no": "Bank 1",
      "TABLE_tcam_bank_stats": {
       "ROW_tcam_bank_stats": {
        "Used": 20,
        "Free": 32748,
        "Percent_Util": 0.06,
        "Timestamp": "2017-08-09 14:36:19"
       }
      }
     },
     {
      "Tcam_no": "Tcam 1",
      "Bank_no": "Bank 0",
      "TABLE_tcam_bank_stats": {
       "ROW_tcam_bank_stats": {
        "Used": 35,
        "Free": 32733,
        "Percent_Util": 0.1,
        "Timestamp": "2017-08-09 14:36:19"
       }
      }
     },
     {
      "Tcam_no": "Tcam 1",
      "Bank_no": "Bank 1",
      "TABLE_tcam_bank_stats": {
       "ROW_tcam_bank_stats": {
        "Used": 462,
        "Free": 32306,
        "Percent_Util": 1.4,
        "Timestamp": "2017-08-09 14:36:19"
       }
      }
     }
    ]
   }
}
```


This example shows how to view iCAM monitoring of the FIB TCAM resources for a current date in JSON format.

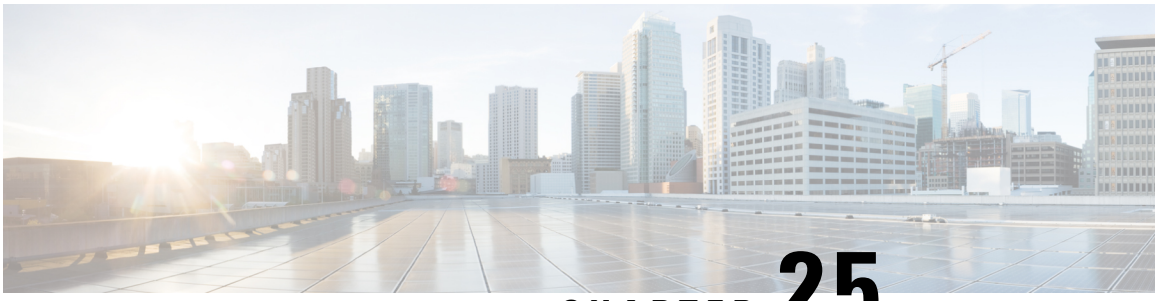

```
switch# show icam resource fib_tcam module 5 inst 0 | json
 {
  "module": 5,
  "instance": 0,
  "TABLE_fib_resource": {
   "ROW_fib_resource": [
    {
     "Class": "IPv4 unicast",
     "TABLE_fib_stats": {
     "ROW_fib_stats": {
      "Log_Entries": 16,
      "Phy_Entries": 16,
      "Percent_Util": 0.0,
      "Timestamp": "2017-08-09 14:37:59"
     }
    }
   },
  {
     "Class": "DIAG_80",
```

```
      "TABLE_fib_stats": {
      "ROW_fib_stats": {
       "Log_Entries": 0,
       "Phy_Entries": 0,
       "Percent_Util": 0.0,
       "Timestamp": "2017-08-09 14:37:59"
      }
     }
    },
    {
      "Class": "IPv4 unicast",
      "TABLE_fib_stats": {
      "ROW_fib_stats": {
       "Log_Entries": 6,
       "Phy_Entries": 6,
       "Percent_Util": 0.0,
       "Timestamp": "2017-08-09 14:37:59"
      }
     }
    }
   ]
  }
}
```


Additional References for iCAM

Related Documents

Related Topic	Document Title
Command Reference	*Cisco Nexus 7000 Series NX-OS System Management Command Reference*



CHAPTER 25

Performing Software Maintenance Upgrades

This chapter describes how to perform software maintenance upgrades on Cisco NX-OS devices.

This chapter contains the following sections:

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.
- In a dual-supervisor system, both the active and standby supervisor modules have to be synchronized with each other.

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.
- You cannot activate multiple SMUs in one command.

- Per-VDC SMUs are not supported.
- Activation is performed only after the package compatibility checks have been passed. If a conflict is found, an error message displays.
- 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.
- SMUs are dependent on your physical device. So, an SMU for the Cisco Nexus 7000 Series will not work for the Cisco Nexus 7700 Series and vice versa.
- 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.
- SMUs are dependent on the version of Cisco NX-OS software release installed. You need to install SMUs compatible with your release. Moving to another Cisco NX-OS software release using reload or ISSU will inactivate the SMUs installed for the previously installed Cisco NX-OS software release. For example, if you have SMUs for Cisco NX-OS Release 7.2.0 in your Supervisor 2 setup, moving to an image of another release, say Cisco NX-OS Release 7.2.2 will cause the SMU to become inactive.
- SMU will be deactivated if you are loading an image of the Cisco NX-OS software release prior to NX-OS Release 7.2.0 that does not support SMUs. However, moving back to Cisco NX-OS Release 7.2.0 will activate the SMU.

Information About Performing a Software Maintenance Upgrades

Overview of SMUs

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.

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.

Actual deployment of SMUs might vary based on your device. Usually, software can be patched simply by restarting the process. However, based on the device, if the process to be patched cannot be restarted, the SMU is implemented either through a reload or ISSU.

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 reload of the whole switch and a parallel reload of supervisors and line cards.
- Line card SMU—Based on the line card type. The supervisor pushes the SMU to all impacted line cards. Activation of the line card SMU requires a reload of the switch.

- Prerequisite SMU—Requires activation before a dependent SMU is loaded. A SMU can have one or more SMU as prerequisites.
- Supersede SMU— Contains cumulative fix for previously loaded SMUs and supersedes the former.

For information on upgrading your device to a new feature or maintenance release, see the *Cisco Nexus 7000 Series NX-OS Software Upgrade and Downgrade Guide*.

An SMU consists of the SMU binary file. The naming convention for an SMU is as below:

<platform>-<pkg-type>.<release_version>.<CDET>.<file-type>

For example:

n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin

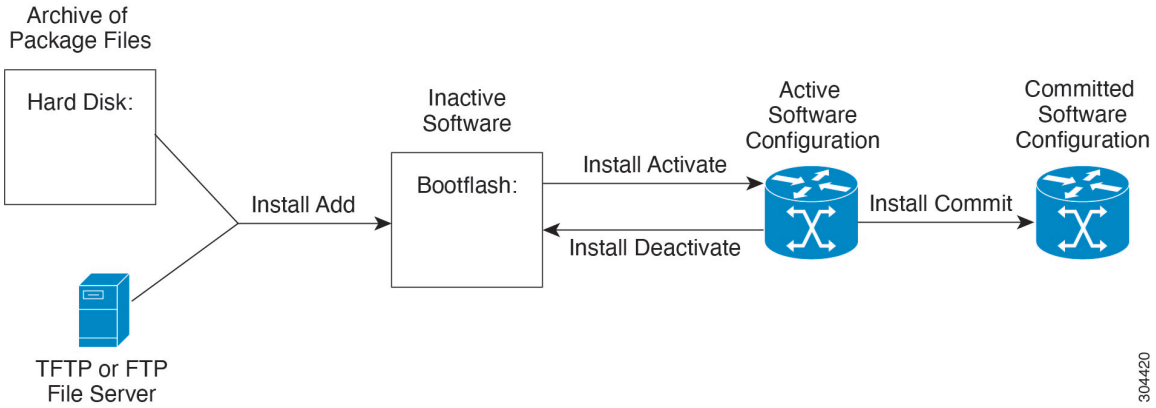
Package Management

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. (Optional) Deactivate and remove the package, when desired.

The following figure illustrates the key steps in the package management process.

Figure 17: 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 on the line cards can be patched and only those processes that can be restarted are restarted. Restarting processes in the line cards are equivalent to a soft reset.

- For line card SMUs, the system behaves as if it were going through an upgrade.
- The line cards might reload.
- The complete system might reload.
- No processes in the line cards might be affected.

Note You must address any issues that result from the revised configuration and reapply the configuration, if necessary.

Tip When you activate packages, use the **test** option to test the effects of a command without impacting the running system. After the activation process completes, enter the **show install log** command to display the process results.

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 stable and prepared for the software changes.

Procedure

	Command or Action	Purpose
Step 1	**show install active** **Example:** `switch# show install active`	Displays the active software on the device. Use this command to determine what software should be added on the device.
Step 2	**show module** **Example:** `switch# show module`	Confirms that all modules are in the stable state.

	Command or Action	Purpose
Step 3	**show clock** **Example:** `switch# show clock`	Verifies that the system clock is correct. Software operations use certificates based on device clock times.
Step 4	**show install pkg-info** *SMU_name* **Example:** `Device# show install pkg-info n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin`	Displays details regarding the contents of the SMU, that is, SMU restart type, platform, processes affected, and so on.

Example

This example shows how to display the active packages for the entire system. Use this information to determine if a software change is required.

Before SMU installation:

```
switch# show install active

Boot Images:

Kickstart Image: bootflash:/ n7700-s2-kickstart.7.2.0.D1.1.bin
System Image: bootflash:/ n7700-s2-dk9.7.2.0.D1.1.bin

Active Packages:
Active Packages on Module #1:
```

After SMU installation:

```
Switch# show install active

Boot Images:

Kickstart Image: bootflash:/n7700-s2-kickstart.7.2.0.D1.1.bin
System Image: bootflash:/n7700-s2-dk9.7.2.0.D1.1.bin

Active Packages:

  n7700-s2-dk9.7.2.0.D1.1.CSCuo7721.bin

Active Packages on Module #1:
  n7700-s2-dk9.7.2.0.D1.1.CSCuo7721.bin
```

This example shows how to display the current system clock setting:

```
switch# show clock

02:14:51.474 PST Wed Jan 04 2014
```

This example shows how to display details of the installed package. Use this information to determine if a software change is required.

```
switch# show install pkg-info n7700-s2-dk9.7.2.0.D1.1. CSCuo07721.bin

Contents of Package file 'n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin'
            Expiry date: Sun Oct 22 11:39:35 2017
            Uncompressed size: 224905
            Vendor: Cisco Systems
```

```
Restart type: restart
Desc: Bug Fix for CDET: CSCuo07721
Build: Built on Tue Aug  4 01:12:10 2015
Source: By Unknown
Platform: Nexus7700
Supersedes: None
Superseded By: None
Pre-requisite: None
Restart information: Ethpm
Pre-install activate scripts: None
Post-install activate scripts: None
Pre-install deactivate scripts: None
Post-install deactivate scripts: None
```

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

Step 3 In the Select a Product list, choose **Switches** > **Data Center Switches** > **Cisco Nexus 7000 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.

Tip Verify there is enough space on the bootflash.

If the SMU package files are located on a remote TFTP, FTP, SCP, 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.
- Secure Copy—SCP allows files to be transferred from a network server that supports Secure Shell (SSH) and uses the secure copy protocol(SCP).
- 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 7000 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 45: Commands for Copying SMU Package Files to the Device

Command	Purpose
copy tftp://*hostname-or-ipaddress*/*directory-path*/*filename* **bootflash:** `switch# copy tftp://10.1.1.1/images/ n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin 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.

Command	Purpose
copy ftp://*username***:***password***@***hostname-or-ipaddress***/***directory-path***/***filename*** bootflash:** `switch# copy ftp://john:secret@10.1.1.1/images/ n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin 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.

Command	Purpose
copy sftp://*hostname-or-ipaddress*/*directory-path*/*filename* **bootflash:** `switch# copy sftp://10.1.1.1/images n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin bootflash:`	Copies the package file from the SFTP server to the bootflash:. • *username*—The username of the user who has access privileges to the directory in which the package file is stored. • *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.
copy scp://*username*@*scpserver.cisco.com*//*directory-path*/*filename* **bootflash:** `switch# copy scp://john@10.1.1.1//download/n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin bootflash:n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin`	Copies the package file from the SCP 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.

After the SMU package file has been transferred to a network file server or the local storage device, you are ready to add and activate the file.

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 The SMU package being activated must be compatible with the currently active software to operate. When 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 for a process does not deactivate SMUs applied for other processes. However, previously active SMUs for the same process will be 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.

Procedure

	Command or Action	Purpose
Step 1	Connect to the console port and log in.	Establishes a CLI management session to the console port.
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: n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin`	Unpacks the package software files from the local storage device or network server and adds them to the bootflash: on active and standby supervisors. Installs the SMU code from the local storage device or network server and adds them to the bootflash: on the active and standby supervisor. After the **install add** process, the SMU patch still requires activation as described in steps 4-7. The *filename* argument can take any of these formats: • **bootflash:***filename* • **tftp:**//*hostname-or-ipaddress/directory-path/filename* • **ftp:**//*username*:*password*@*hostname-or-ipaddress/directory-path/filename* • **sftp:**//*hostname-or-ipaddress/directory-path/filename* • **usb1:***filename* Multiple versions of an SMU package can be added to the storage device without impacting the currently running software, but only one version of a package can be activated.

	Command or Action	Purpose
		Note Though the **install add** function copies the SMU code to any standby supervisor present in the system, it does not copy the SMU .bin file to a standby supervisor bootflash, as the SMU .bin file is not required on both active and standby bootflash. It can manually be copied to the standby bootflash, if required.
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* [**test**]
	Example:
	`switch# install activate n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin`
	`Install operation 158 completed successfully at Tue Jun 9 19:09:33 2015`
		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.)
		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.
		Tip When you activate packages, use the **test** keyword to test the effects of a command without impacting the running system. 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.

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.

Note 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 #unique_608.

Procedure

	Command or Action	Purpose
Step 1	**install commit** *filename* **Example:** `switch# install commit n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin`	Commits the current set of packages so that these packages are used if the device is restarted.
Step 2	(Optional) **show install committed** **Example:** `switch# show install committed`	Displays which packages are committed.

Example

This example shows how to commit active SMU packages on the device and then verify the committed packages:

```
switch#  install commit n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin
Install operation 2 completed successfully at Thu Jan 9 01:20:46 2014

switch# show install committed
Boot Images:
      Kickstart Image: bootflash:/n7700-s2-kickstart.7.2.0.D1.1.bin
      System Image: bootflash:/ n7700-s2-dk9.7.2.0.D1.1.bin

Committed Packages:
      n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin
```

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 deactivate the current package and install active and install commit commands to activate the previous package.

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

	Command or Action	Purpose
Step 1	Connect to the console port and log in.	Establishes a CLI management session to the console port.
Step 2	**install deactivate** *filename* **Example:** `switch# install deactivate n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin`	Deactivates a package that was added to the device and turns off the package features for the line card. **Note** Press **?** after a partial package name to display all possible matches available for deactivation. If there is only one match, press the **Tab** key to fill in the rest of the package name.
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 n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin`
	`Proceed with removing n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin? (y/n)? [n] y`
	Example:
	`switch# install remove inactive`
	`Proceed with removing? (y/n)? [n] y`
		Removes the inactive package.
		• 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 remove** command with the *filename* argument.
		• To remove all inactive packages from all nodes in the system, use the **install remove** command with the **inactive** keyword.

Example

This example shows how to deactivate a package, commit the changes, and remove the inactive package from the device:

```
switch# install deactivate n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin
Install operation 3 completed successfully at Thu Jan 9 01:20:36 2014

switch# show install inactive
Inactive Packages: n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin

switch# install commit
Install operation 4 completed successfully at Thu Jan 9 01:20:46 2014

switch# install remove n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin
Proceed with removing n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin? (y/n)? [n] y
Install operation 5 completed successfully at Thu Jan 9 01:20:57 2014
```

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
Thu Jan 9 01:26:09 2014
Install operation 1 by user 'admin' at Thu Jan 9 01:19:19 2014
Install add bootflash: n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin
Install operation 1 completed successfully at Thu Jan 9 01:19:24 2014
---------------------------------------
Install operation 2 by user 'admin' at Thu Jan 9 01:19:29 2014
Install activate n7700-s2-dk9.7.2.0.D1.1.bin
Install operation 2 completed successfully at Thu Jan 9 01:19:45 2014
---------------------------------------
Install operation 3 by user 'admin' at Thu Jan 9 01:20:05 2014
Install commit n7700-s2- dk9.7.2.0.D1.1.bin
Install operation 3 completed successfully at Thu Jan 9 01:20:08 2014
---------------------------------------
Install operation 4 by user 'admin' at Thu Jan 9 01:20:21 2014
Install deactivate n7700-s2-dk9.7.2.0.D1.1.bin
Install operation 4 completed successfully at Thu Jan 9 01:20:36 2014
---------------------------------------
Install operation 5 by user 'admin' at Thu Jan 9 01:20:43 2014
Install commit n7700-s2-dk9.7.2.0.D1.1.bin
Install operation 5 completed successfully at Thu Jan 9 01:20:46 2014
---------------------------------------
Install operation 6 by user 'admin' at Thu Jan 9 01:20:55 2014
Install remove n7700-s2-dk9.7.2.0.D1.1.bin
Install operation 6 completed successfully at Thu Jan 9 01:20:57 2014
---------------------------------------
```

```
Install operation 7 by user 'admin' at Thu Jan 9 01:21:07 2014
Install remove
Install operation 7 completed successfully at Thu Jan 9 01:21:10 201
```

This example shows how to display additional information, including any impact to nodes and processes:

```
switch# show install log detail
Thu Jan 9 01:24:03 2014
Install operation 1 by user 'admin' at Thu Jan 9 01:19:19 2014
Installer started downloading the package: / n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin
via bootflash
Install add bootflash: n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin
Copying file at Thu Jan 9 01:19:20 2014
Download success, 238545 bytes received
Verifying package
Checking MD5 at Thu Jan 9 01:19:21 2014
MD5 checksum OK
Checking HW platform at Thu Jan 9 01:19:22 2014
Checking SW platform at Thu Jan 9 01:19:23 2014
Package verified successfully
Sending patch file to plugin manager at Thu Jan 9 01:19:23 2014
The following package is now available to be activated: n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin

Install operation 1 completed successfully at Thu Jan 9 01:19:24 2014
----------------------------------------
Install operation 2 by user 'admin' at Thu Jan 9 01:19:29 2014
Install activate n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin
Install activate action started
The software will be activated with process restart
2 processes affected
sysinfo (modified)
vman (modified)
Install operation 2 completed successfully at Thu Jan 9 01:19:45 2014
----------------------------------------
Install operation 3 by user 'admin' at Thu Jan 9 01:20:05 2014
Install commit n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin
MD5 checksum OK for patch: n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin
Install operation 3 completed successfully at Thu Jan 9 01:20:08 2014
----------------------------------------
Install operation 4 by user 'admin' at Thu Jan 9 01:20:21 2014
Install deactivate n7700-s2-dk9.7.2.0.D1.1.bin
Install deactivate action started
The software will be deactivated with process restart
2 processes affected
sysinfo (modified)
vman (modified)
Install operation 4 completed successfully at Thu Jan 9 01:20:36 2014
----------------------------------------
Install operation 5 by user 'admin' at Thu Jan 9 01:20:43 2014
Install commit n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin
MD5 checksum OK for patch: n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin
Install operation 5 completed successfully at Thu Jan 9 01:20:46 2014
----------------------------------------
Install operation 6 by user 'admin' at Thu Jan 9 01:20:55 2014
Install remove n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin
Install operation 6 completed successfully at Thu Jan 9 01:20:57 2014
----------------------------------------
Install operation 7 by user 'admin' at Thu Jan 9 01:21:07 2014
Install remove
Install operation 7 completed successfully at Thu Jan 9 01:21:10 2014
```

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 Sun Mar 9 00:42:10 2014
Install activate n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin
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 Sun Mar 9 00:42:12 2014
```

This example shows the details of the specific SMUs:

```
switch# show install package
Boot Images:
     Kickstart Image: bootflash:/ n7700-s2-kickstart.7.2.0.D1.1.bin
     System Image: bootflash:/ n7700-s2-dk9.7.2.0.D1.1.bin
----------------------------------------------------------------
n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin             Active Committed

Modules

       Module #3: Active Committed

       Module #4: Active Committed

n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin             Inactive

Modules

       Module #3: Inactive

       Module #4: Inactive
```

Where to Go Next

For information about configuring control policies, see the "Configuring ISG Control Policies" module.

Additional References

Related Documents

Related Topic	Document Title
Software upgrades	*Cisco Nexus 7000 Series NX-OS Software Upgrade and Downgrade Guide*
System management commands	*System Management Command Reference*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Related Documents

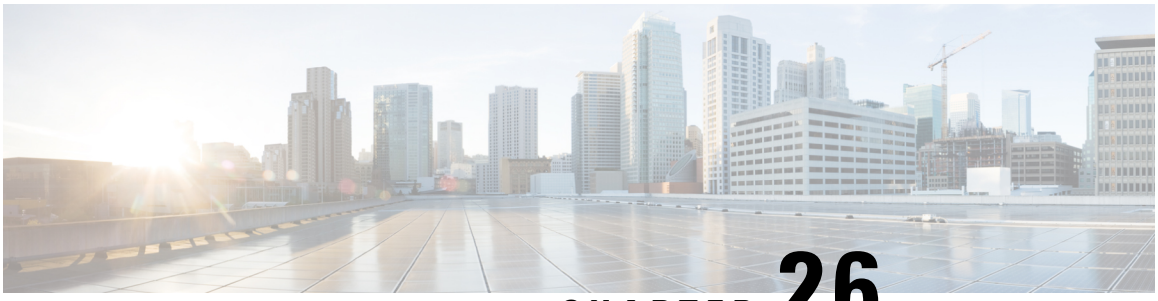
Related Topic	Document Title
Software upgrades	*Cisco Nexus 7000 Series NX-OS Software Upgrade and Downgrade Guide*

Feature Information for Performing Software Maintenance Upgrades

The following table provides release information about the SMU package files supported for this software. This table lists only the software release that introduced support for a given SMU package. Unless noted otherwise, subsequent releases of that software also support that SMU package.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

SMU Package File	Releases	Description
n7000-s2-dk9.7.2.1.CSCuo07721.bin	7.2(0)	Restart type: restart Platform: Nexus7700 Supersedes: None Superseded By: None Restart information: *CSCuo07721* Pre-install activate scripts: None Post-install activate scripts: None Pre-install deactivate scripts: None Post-install deactivate scripts: None



CHAPTER 26

Converting CLI Commands to Network Configuration Format

This chapter explains how to install and use the XMLIN tool to convert CLI commands to the Network Configuration (NETCONF) protocol.

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “New and Changed Information” chapter or the Feature History table.

Information About XMLIN

The XMLIN tool converts CLI commands to the Network Configuration (NETCONF) protocol format. NETCONF is a network management protocol that provides mechanisms to install, manipulate, and delete the configuration of network devices. It uses XML-based encoding for configuration data and protocol messages. The NX-OS implementation of the NETCONF protocol supports the following protocol operations: <get>, <edit-config>, <close-session>, <kill-session>, and <exec-command>.

The XMLIN tool converts show, EXEC, and configuration commands to corresponding NETCONF <get>, <exec-command>, and <edit-config> requests. You can enter multiple configuration commands into a single NETCONF <edit-config> instance.

The XMLIN tool also converts the output of show commands to XML format.

Installing and Using the XMLIN Tool

You can install the XMLIN tool and then use it to convert configuration commands to NETCONF format.

Before you begin

Although the XMLIN tool is usually capable of generating NETCONF instances of commands even if the corresponding feature sets or the required hardware capabilities are not available on the device, you might have to install some feature sets before entering the **xmlin** command.

Procedure

	Command or Action	Purpose
Step 1	switch# **xmlin**	
Step 2	switch(xmlin)# **configure terminal**	Enters global configuration mode.
Step 3	Configuration commands	Converts configuration commands to NETCONF format.
Step 4	(Optional) switch(config)(xmlin)# **end**	Generates the corresponding <edit-config> request. **Note** You must enter the **end** command to finish the current XML configuration before you generate an XML instance for a **show** command.
Step 5	(Optional) switch(config-if-verify)(xmlin)# **show** *commands*	Converts **show** commands to NETCONF format.
Step 6	(Optional) switch(config-if-verify)(xmlin)# **exit**	Returns to EXEC mode.

Converting Show Command Output to XML

You can convert the output of show commands to XML.

Before you begin

Make sure that all features for the commands you want to convert are installed and enabled on the device. Otherwise, the commands will fail.

You can use the **terminal verify-only** command to verify that a feature is enabled without entering it on the device.

Make sure that all required hardware for the commands you want to convert are present on the device. Otherwise, the commands will fail.

Make sure that the XMLIN tool is installed.

Procedure

	Command or Action	Purpose
Step 1	switch# *show-command* | **xmlin**	Enters global configuration mode. **Note** You cannot use this command with configuration commands.

Configuration Examples for XMLIN

The following example shows how the XMLIN tool is installed on the device and used to convert a set of configuration commands to an <edit-config> instance.

```
switch# xmlin
****************************************
Loading the xmlin tool. Please be patient.
****************************************
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright ©) 2002-2013, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

switch(xmlin)# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)(xmlin)# interface ethernet 2/1
% Success
switch(config-if-verify)(xmlin)# cdp enable
% Success
switch(config-if-verify)(xmlin)# end
<?xml version="1.0"?>
<nf:rpc xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns="http://www.cisco.com/nxos:6.2.2.:configure_"
xmlns:m="http://www.cisco.com/nxos:6.2.2.:_exec"
xmlns:m1="http://www.cisco.com/nxos:6.2.2.:configure__if-eth-base" message-id="1">
  <nf:edit-config>
     <nf:target>
      <nf:running/>
  </nf:target>
  <nf:config>
    <m:configure>
      <m:terminal>
        <interface>
           <__XML__PARAM__interface>
              <__XML__value>Ethernet2/1</__XML__value>
              <m1:cdp>
                <m1:enable/>
              </m1:cdp>
            </__XML__PARAM__interface>
          </interface>
         </m:terminal>
        </m:configure>
```

```
        </nf:config>
       </nf:edit-config>
     </nf:rpc>
    ]]>]]>
```

The following example shows how you must enter the **end** command to finish the current XML configuration before you generate an XML instance for a **show** command.

```
switch(xmlin)# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)(xmlin)# interface ethernet 2/1
switch(config-if-verify)(xmlin)# show interface ethernet 2/1
******************************************************
Please type "end" to finish and output the current XML document before building a new one.
******************************************************
% Command not successful

switch(config-if-verify)(xmlin)# end
<?xml version="1.0"?>
<nf:rpc xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns="http://www.cisco.com/nxos:6.2.2.:configure_"
xmlns:m="http://www.cisco.com/nxos:6.2.2.:_exec" message-id="1">
    <nf:edit-config>
      <nf:target>
         <nf:running/>
      </nf:target>
      <nf:config>
         <m:configure>
           <m:terminal>
              <interface>
                 <__XML__PARAM__interface>
                    <__XML__value>Ethernet2/1</__XML__value>
                 </__XML__PARAM__interface>
              </interface>
           </m:terminal>
           </m:configure>
         </nf:config>
      </nf:edit-config>
    </nf:rpc>
   ]]>]]>

switch(xmlin)# show interface ethernet 2/1
<?xml version="1.0"?>
<nf:rpc xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns="http://www.cisco.com/nxos:6.2.2.:if_manager" message-id="1">
  <nf:get>
    <nf:filter type="subtree">
      <show>
      <interface>
        <__XML__PARAM__ifeth>
           <__XML__value>Ethernet2/1</__XML__value>
        </__XML__PARAM__ifeth>
      </interface>
     </show>
   </nf:filter>
  </nf:get>
</nf:rpc>
]]>]]>
switch(xmlin)# exit
switch#
```

The following example shows how you can convert the output of the **show interface brief** command to XML.

```
switch# show interface brief | xmlin
<?xml version="1.0"?>
<nf:rpc xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns="http://www.cisco.com/nxos:6.2.2.:if_manager"

message-id="1">
  <nf:get>
    <nf:filter type="subtree">
       <show>
          <interface>
              <brief/>
          </interface>
       </show>
     </nf:filter>
   </nf:get>
</nf:rpc>
]]>]]>
```

Related Documents

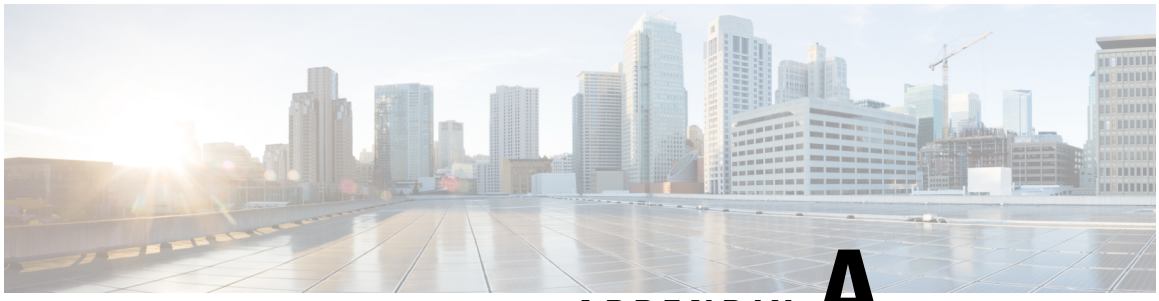
Related Topic	Document Title
XMLIN commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco Nexus 7000 Series NX-OS System Management Command Reference*

Feature History for XMLIN

Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Table 46: Feature History for XMLIN

Feature Name	Releases	Feature Information
XMLIN	6.2(2)	This feature was introduced.



APPENDIX A

IETF RFCs supported by Cisco NX-OS System Management

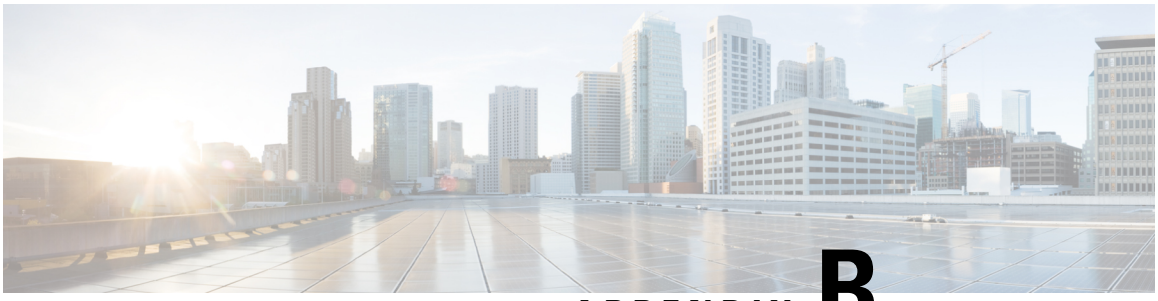
This appendix lists the IETF RFCs for system management supported in Cisco NX-OS.

IETF RFCs Supported by Cisco NX-OS System Management

This appendix lists the IETF RFCs for system management supported in Cisco NX-OS.

RFCs	Title
RFC 2819	*Remote Network Monitoring Management Information Base*
RFC 3164	*The BSD syslog Protocol*
RFC 3411 and RFC 3418	*An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*
RFC 3954	*Cisco Systems NetFlow Services Export Version 9*

IETF RFCs supported by Cisco NX-OS System Management



APPENDIX B

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

The following table lists the Embedded Event Manager (EEM) system policies.

Event	Description
__PortLoopback	Do CallHome, log error in Syslog/OBFL/Exception Log, and disable further HM testing on affected ports after 10 consecutive failures of GOLD "PortLoopback" test
__RewriteEngineLoopback	Do CallHome, log error in Syslog/OBFL/Exception Log, and disable further HM testing on affected ports after 10 consecutive failures of GOLD "RewriteEngine" test
__asic_register_check	Do CallHome, log error, and disable further HM testing for that ASIC device/instance after 20 consecutive failures of GOLD "ASICRegisterCheck" test
__compact_flash	Do CallHome, log error, and disable further HM testing after 20 consecutive failures of GOLD "CompactFlash" test
__crypto_device	Do CallHome and log error when GOLD "CryptoDevice" test fails

Embedded Event Manager System Events and Configuration Examples

Event	Description
__eobc_port_loopback	Do CallHome and log error when GOLD "EOBCPortLoopback" test fails
__ethpm_debug_1	Action: none
__ethpm_debug_2	Action: none
__ethpm_debug_3	Action: none
__ethpm_debug_4	Action: none
__ethpm_link_flap	More than 30 link flaps in a 420-second interval. Action: Error. Disable the port
__external_compact_flash	Do CallHome, log error, and disable further HM testing after 20 consecutive failures of GOLD "ExternalCompactFlash" test
__lcm_module_failure	Power cycle two times and then power down
__management_port_loopback	Do CallHome and log error when GOLD "ManagementPortLoopback" test fails
__nvram	Do CallHome, log error, and disable further HM testing after 20 consecutive failures of GOLD "NVRAM" test
__pfm_fanabsent_all_systemfan	Shuts down if both fan trays (f1 and f2) are absent for 2 minutes
__pfm_fanbad_all_systemfan	Syslog when fan goes bad
__pfm_fanbad_any_singlefan	Syslog when fan goes bad
__pfm_power_over_budget	Syslog warning for insufficient power overbudget
__pfm_tempev_major	TempSensor Major Threshold. Action: Shutdown
__pfm_tempev_minor	TempSensor Minor Threshold. Action: Syslog
__primary_bootrom	Do CallHome, log error, and disable further HM testing after 20 consecutive failures of GOLD "PrimaryBootROM" test
__pwr_mgmt_bus	Do CallHome, log error, and disable further HM testing for the module or spine-card after 20 consecutive failures of GOLD "PwrMgmtBus" test
__real_time_clock	Do CallHome, log error, and disable further HM testing after 20 consecutive failures of GOLD "RealTimeClock" test

Event	Description
__secondary_bootrom	Do CallHome, log error, and disable further HM testing after 20 consecutive failures of GOLD "SecondaryBootROM" test
__spine_control_bus	Do CallHome, log error, and disable further HM testing for that module or spine-card after 20 consecutive failures of GOLD "SpineControlBus" test
__standby_fabric_loopback	Do CallHome, log error, and disable further HM testing after 10 consecutive failures
__status_bus	Do CallHome, log error, and disable further HM testing after 5 consecutive failures of GOLD "StatusBus" test
__system_mgmt_bus	Do Call Home, log error, and disable further HM testing for that fan or power supply after 20 consecutive failures of GOLD "SystemMgmtBus" test
__usb	Do Call Home and log error when GOLD "USB" test fails

EEM Events

The following table describes the EEM events you can use on the device.

EEM Event	Description
application	Publishes an application-specific event.
cli	CLI command is entered that matches a pattern with a wildcard.
counter	EEM counter reaches a specified value or range.
fanabsent	System fan tray is absent.
fanbad	System fan generates a fault.
fib	Monitors routes or TCAM usage in the unicast FIB.
gold	GOLD test failure condition is hit.
interface	Interface counter exceeds a threshold.
memory	Available system memory exceeds a threshold.
module	Specified module enters the selected status.
module-failure	Module failure is generated.

EEM Event	Description
none	Runs the policy event without any events specified.
oir	Online insertion or removal occurs.
policy-default	Default parameters and thresholds are used for the events in the system policy you override.
poweroverbudget	Platform software detects a power budget condition.
snmp	SNMP object ID (OID) state changes.
storm-control	Platform software detects an Ethernet packet storm condition.
syslog	Monitors syslog messages and invokes the policy based on the search string in the policy.
sysmgr	System manager generates an event.
temperature	Temperature level in the system exceeds a threshold.
timer	Specified time is reached.
track	Tracked object changes state.

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:

```
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:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)#
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:

```
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:

```
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):

```
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:

```
switch# configure terminal
switch(config)# no event manager applet myappletname override __pfm_tempev_major
```

```
switch(config)# end
```

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):

```
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:

```
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:

```
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:

```
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:

```
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
switch(config-applet)# end
```

```
switch# configure terminal
switch(config)# event manager applet myappletname override __pfm_tempev_major
switch(config-applet)# event temperature module 3 threshold major
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_tempev_major
switch(config)# end
```

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:

```
switch# configure terminal
switch(config)# event manager applet myapplet1 override __pfm_tempev_major
switch(config-applet)# end
switch# 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:

```
switch# configure terminal
switch(config)# event manager applet myapplet1 override __pfm_tempev_major
switch(config-applet)# end
switch# 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# 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# 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:

```
switch# configure terminal
switch(config)# event manager applet myapplet1 override __pfm_tempev_major
switch(config-applet)# end
switch# configure terminal
switch(config)# event manager applet myapplet2 override __pfm_tempev_major
switch(config-applet)# event temperature module 9 threshold major
switch(config-applet)# action 2 policy-default
switch(config-applet)# 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# configure terminal
switch(config)# event manager applet myapplet1 override __pfm_tempev_major
switch(config-applet)# end
switch# configure terminal
switch(config)# event manager applet myapplet2 override __pfm_tempev_major
switch(config-applet)# event temperature module 2 sensor 3 threshold major
switch(config-applet)# action 2 policy-default
switch(config-applet)# end
switch# configure terminal
switch(config)# event manager applet myapplet3 override __pfm_tempev_major
switch(config-applet)# event temperature module 2 sensor 4 threshold major
switch(config-applet)# action 3 policy-default
switch(config-applet)# end
switch# configure terminal
switch(config)# event manager applet myapplet4 override __pfm_tempev_major
switch(config-applet)# event temperature module 2 sensor 7 threshold major
switch(config-applet)# action 4 policy-default
switch(config-applet)# end
switch# configure terminal
switch(config)# event manager applet myapplet5 override __pfm_tempev_major
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# configure terminal
switch(config)# event manager applet myappletname override __pfm_fanabsent_any_singlefan
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-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# configure terminal
switch(config)# 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):

```
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:

[**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:

```
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:

[**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:

```
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 my5a1 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 forceshut 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:

```
switch(config)# 2013 May 20 00:08:27 p1b-57 %$ VDC-1 %$ %EEM_ACTION-2-CRIT: “Module is
removed”
```

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
```

Note In this example, port channel 3000 is the vPC peer link, and Ethernet 2/24 is the vPC keepalive link.

You need to copy the following files to the bootflash:

- A directory called: /eem/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:

```
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:

Embedded Event Manager System Events and Configuration Examples

```
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
```