Cisco Nexus 5000 Series NX-OS System Management Configuration Guide

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

Text Part Number: OL-20922-02

CONTENTS

Preface

This preface describes the audience, organization, and conventions of the Cisco Nexus 5000 Series NX-OS System Management Configuration Guide. It also provides information on how to obtain related documentation.

Audience

This preface describes the audience, organization, and conventions of the . It also provides information on how to obtain related documentation.

Document Organization

This document is organized into the following chapters:

Chapter	Description
New and Changed Information	Describes the new and changed information for the Cisco Nexus 5000 Series NX-OS system management software.
System Management Overview	Provides an overview of the system management features that are used to monitor and manage the Nexus 5000 series.
Using Cisco Fabric Services	Explains the use of the Cisco Fabric Services (CFS) infrastructure to enable efficient database distribution.
Configuring User Accounts and RBAC	Describes how to create and manage users accounts and assign roles that limit access to operations.

Chapter	Description
Configuring Session Manager	Describes how to configure Session Manager to implement your configuration changes in batch mode.
Configuring Online Diagnostics	Describes how to configure the generic online diagnostics (GOLD) feature to provide verification of hardware components during switch bootup or reset, and to monitor the health of the Nexus 5000 series.
Configuring System Message Logging	Describes how system message logging is configured and displayed.
Configuring Smart Call Home	Provides details on the Call Home service and includes information on Call Home, event triggers, contact information, destination profiles, and e-mail options.
Configuring SNMP	Provides details on how you can use SNMP to modify a role that was created.
Configuring RMON	Provides details on using RMONs to configure alarms and events.

Document Conventions

Command descriptions use the following conventions:

Convention	Description
bold	Bold text indicates the commands and keywords that you enter literally as shown.
Italic	Italic text indicates arguments for which the user supplies the values.
[x]	Square brackets enclose an optional element(keyword or argument).
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical bar indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical bar indicate a required choice.
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
`variable`	Indicates a variable for which you supply values, in context where italics cannot be used.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Screen examples use the following conventions:

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

This document uses the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Documentation for Nexus 5000 Series NX-OS Software

Cisco NX-OS documentation is available at the following URL:

http://www.cisco.com/en/US/products/ps9670/tsd_products_support_series_home.htmll

The documentation set for the Cisco Nexus 5000 Series NX-OS software includes the following documents:

Release Notes

- *Cisco Nexus 5000 Series and Cisco Nexus 2000 Series Release Notes*
- *Cisco Nexus 5000 Series Switch Release Notes*

Cisco Nexus 5000 Series NX-OS Configuration Guides

- *Cisco Nexus 5000 Series NX-OS Fibre Channel over Ethernet Configuration Guide*
- *Cisco Nexus 5000 Series NX-OS Layer 2 Switching Configuration Guide*
- *Cisco Nexus 5000 Series NX-OS Quality of Service Configuration Guide*
- *Cisco Nexus 5000 Series NX-OS SAN Switching Configuration Guide*
- *Cisco Nexus 5000 Series NX-OS Security Configuration Guide*

- *Cisco Nexus 5000 Series NX-OS System Management Configuration Guide*
- *Cisco Nexus 5000 Series Switch CLI Software Configuration Guide*
- *Cisco Nexus 5000 Series Fabric Manager Configuration Guide, Release 3.4(1a)*

Installation and Upgrade Guides

- *Cisco Nexus 5000 Series Hardware Installation Guide*
- *Regulatory Compliance and Safety Information for the Cisco Nexus 5000 Series*

Cisco NX-OS Command References

- *Cisco Nexus 5000 Series Command Reference*

Cisco NX-OS Technical References

- *Cisco Nexus 5000 MIBs Reference*

Cisco NX-OS Error and System Messages

- *Cisco NX-OS System Messages Reference*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

CHAPTER 1

New and Changed Information

This chapter provides release-specific information for each new and changed feature in the Cisco Nexus 5000 Series NX-OS System Management Configuration Guide.

New and Changed Information

This chapter provides release-specific information for each new and changed feature in the *Cisco Nexus 5000 Series NX-OS System Management Configuration Guide, Release 4.1(3)N2(1)*.

The latest version of this document is available at the following Cisco website:

http://www.cisco.com/en/US/products/ps9670/products_installation_and_configuration_guides_list.html

To check for additional information about Cisco NX-OS Release 4.2(1)N1(1), see the *Cisco Nexus 5000 Series NX-OS Release Notes* available at the following Cisco website:

http://www.cisco.com/en/US/products/ps9670/prod_release_notes_list.html

This table summarizes the new and changed features documented in the *Cisco Nexus 5000 Series NX-OS System Management Configuration Guide, Release 4.2(1)N1(1)*, and tells you where they are documented.

Table 1: New and Changed System Management Features for Cisco NX-OS Release 4.2(1)N1(1)

Feature	Description	Changed in Release	Where Documented
ACLs for SNMP Communities	Allows you to assign ACLs to a community to filter incoming SNMP requests.	4.2(1)N1(1)	Configuring SNMP

This table summarizes the new and changed features documented in the *Cisco Nexus 5000 Series NX-OS System Management Configuration Guide, Release 4.1(3)N2(1)*, and tells you where they are documented.

Table 2: New and Changed System Management Features for Cisco NX-OS Release 4.1(3)N2(1)

Feature	Description	Changed in Release	Where Documented
Logging with VRF option	Allows you to set up a logging server with a specific VRF.	4.1(3)N2(1)	Configuring syslog Servers

Documentation Organization

As of Cisco NX-OS Release 4.1(3)N2(1), the Cisco Nexus 5000 Series configuration information is available in new feature-specific configuration guides for the following information:

- System Management
- Layer 2 Switching
- SAN Switching
- Fibre Channel over Ethernet
- Security
- Quality of Service

The information in these new guides previously existed in the *Cisco Nexus 5000 Series CLI Configuration Guide* which remains available on Cisco.com and should be used for all software releases prior to Cisco Nexus 5000 NX-OS Software Rel 4.1(3). Each new configuration guide addresses the features that are introduced in or are available in a particular release. Select and view the configuration guide that pertains to the software installed in your switch.

The information in the new *Cisco Nexus 5000 Series NX-OS Security Configuration Guide* previously existed in Part 4: System Management of the *Cisco Nexus 5000 Series CLI Configuration Guide*.

For a complete list of Cisco Nexus 5000 Series document titles, see the list of Related Documentation in the "Preface."

CHAPTER 2

Overview

Cisco Nexus 5000 Series switches support Cisco NX-OS system management features including Cisco Fabric Services, online diagnostics, Call Home, SNMP, and RMON.

System Management Overview

The system management features documented in this guide are described below:

Cisco Fabric Services

The Cisco MDS NX-OS software uses the Cisco Fabric Services (CFS) infrastructure to enable efficient database distribution and to promote device flexibility. CFS simplifies SAN provisioning by automatically distributing configuration information to all switches in a fabric.

User Accounts and RBAC

User accounts and role-based access control (RBAC) allow you to define the rules for an assigned role. Roles restrict the authorization that the user has to access management operations. Each user role can contain multiple rules and each user can have multiple roles.

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.

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.

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 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.

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

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.

CHAPTER 3

Using Cisco Fabric Services

This chapter contains the following sections:

Using Cisco Fabric Services

Cisco Nexus 5000 Series switches provide Cisco Fabric Services (CFS) capability, which simplifies provisioning by automatically distributing configuration information to all switches in the network. Switch features can use the CFS infrastructure to distribute feature data or configuration data required by the feature.

Information About CFS

Some features in the Cisco Nexus 5000 Series switch require configuration synchronization with other switches in the network to function correctly. Synchronization through manual configuration at each switch in the network can be a tedious and error-prone process.

Cisco Fabric Services (CFS) provides a common infrastructure for automatic configuration synchronization in the network. It provides the transport function and a set of common services to the features. CFS has the ability to discover CFS capable switches in the network and discovering feature capabilities in all CFS capable switches.

Cisco Nexus 5000 Series switches support CFS message distribution over Fibre Channel, IPv4 or IPv6 networks. If the switch is provisioned with Fibre Channel ports, CFS over Fibre Channel is enabled by default. CFS over IP must be explicitly enabled.

CFS provides the following features:

- Peer-to-peer protocol with no client-server relationship at the CFS layer.
- CFS message distribution over Fibre Channel, IPv4 or IPv6 networks.
- Three modes of distribution.
  - Coordinated distributions: Only one distribution is allowed in the network at any given time.
  - Uncoordinated distributions: Multiple parallel distributions are allowed in the network except when a coordinated distribution is in progress.

- Unrestricted uncoordinated distributions: Multiple parallel distributions are allowed 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.

The following features are supported for CFS distribution over IP:

- One scope of distribution over an IP network:
  - Physical scope: The distribution spans the entire IP network.

The following features are supported for CFS distribution over Fibre Channel SANs:

- Three scopes of distribution over SAN fabrics.
  - Logical scope: The distribution occurs within the scope of a VSAN.
  - Physical scope: The distribution spans the entire physical topology.
  - Over a selected set of VSANs: Some features require configuration distribution over some specific VSANs. These features can specify to CFS the set of VSANs over which to restrict the distribution.
- Supports a merge protocol that facilitates the merge of feature configuration during a fabric merge event (when two independent SAN fabrics merge).

CFS Distribution

The CFS distribution functionality is independent of the lower layer transport. Cisco Nexus 5000 Series switches support CFS distribution over IP and CFS distribution over Fibre Channel. Features that use CFS are unaware of the lower layer transport.

CFS Distribution Modes

CFS supports three distribution modes to accommodate different feature requirements:

- Uncoordinated Distribution
- Coordinated Distribution
- Unrestricted Uncoordinated Distributions

Only one mode is allowed at any given time.

Uncoordinated Distribution

Uncoordinated distributions are used to distribute information that is not expected to conflict with that from a peer. Parallel uncoordinated distributions are allowed for a feature.

Coordinated Distribution

Coordinated distributions allow only one feature distribution at a given time. CFS uses locks to enforce this. A coordinated distribution is not allowed to start if locks are taken for the feature 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.

Coordinated distribution has two variants:

- CFS driven —The stages are executed by CFS in response to an feature request without intervention from the feature.
- Feature driven—The stages are under the complete control of the feature.

Coordinated distributions are used to distribute information that can be manipulated and distributed from multiple switches, for example, the port security configuration.

Unrestricted Uncoordinated Distributions

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.

Disabling or Enabling CFS Distribution on a Switch

If the switch is provisioned with Fibre Channel ports, CFS over Fibre Channel is enabled by default. CFS over IP must be explicitly enabled.

You can globally disable CFS on a switch to isolate the features using CFS from network-wide distributions while maintaining physical connectivity. When CFS is globally disabled on a switch, CFS operations are restricted to the switch.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **no cfs distribute**
3. (Optional) switch(config)# **cfs distribute**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters configuration mode.
Step 2	switch(config)# **no cfs distribute**	Globally disables CFS distribution (CFS over Fibre Channel or IP) for all applications on the switch.
Step 3	switch(config)# **cfs distribute**	(Optional) Enables CFS distribution on the switch. This is the default.

Verifying CFS Distribution Status

The **show cfs status** command displays the status of CFS distribution on the switch.

```
switch# show cfs status
Distribution : Enabled
Distribution over IP : Enabled - mode IPv4
IPv4 multicast address : 239.255.70.83
IPv6 multicast address : ff15::efff:4653
Distribution over Ethernet : Enabled
```

CFS Distribution over IP

CFS distribution over IP supports the following features:

- Physical distribution over an entirely IP network.
- Physical distribution over a hybrid Fibre Channel and IP network with the distribution reaching all switches that are reachable over either Fibre Channel or IP.

Note The switch attempts to distribute information over Fibre Channel first and then over the IP network if the first attempt over Fibre Channel fails. CFS does not send duplicate messages if distribution over both IP and Fibre Channel is enabled.

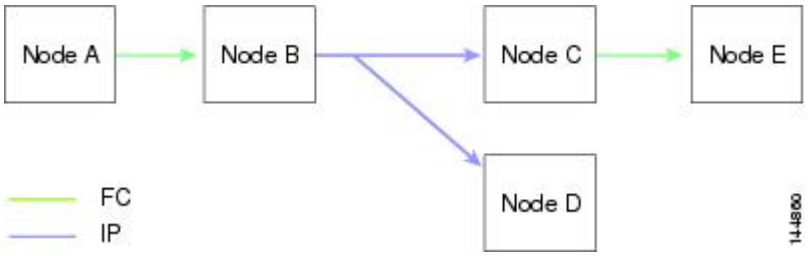
- Distribution over IP version 4 (IPv4) or IP version 6 (IPv6).

  Note CFS cannot distribute over both IPv4 and IPv6 from the same switch.

- Keepalive mechanism to detect network topology changes using a configurable multicast address.
- Compatibility with Cisco MDS 9000 Family switches running release 2.x or later.

The following figure (*Network Example 1*) shows a network with both Fibre Channel and IP connections. Node A forwards an event to node B over Fibre Channel. Node B forwards the event node C and node D using unicast IP. Node C forwards the event to node E using Fibre Channel.

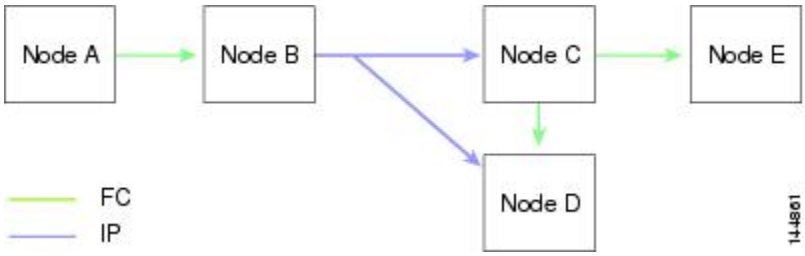
Figure 1: Network Example 1 with Fibre Channel and IP Connections



The following figure (*Network Example 2*) is the same as the previous figure except that node C and node D are connected using Fibre Channel. All processes is the same in this example because node B has node C and

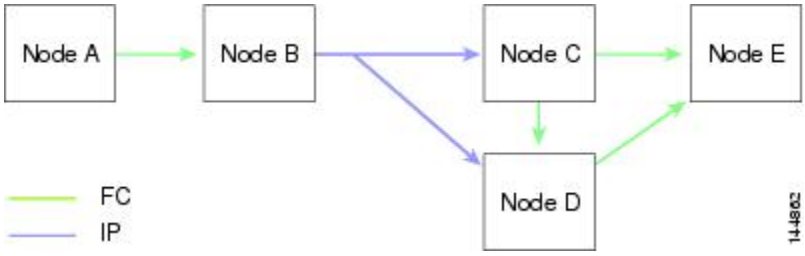
node D the distribution list for IP. Node C does not forward to node D because node D is already in the distribution list from node B.

Figure 2: Network Example 2 with Fibre Channel and IP Connections



The following figure (*Network Example 3*) is the same as the previous figure except that node D and node E are connected using IP. Both node C and node D forward the event to E because the node E is not in the distribution list from node B.

Figure 3: Network Example 3 with Fibre Channel and IP Connections



CFS Distribution over Fibre Channel

For FCS distribution over Fibre Channel, the CFS protocol layer resides on top of the FC2 layer. CFS uses the FC2 transport services to send information to other switches. CFS uses a proprietary SW_ILS (0x77434653) protocol for all CFS packets. CFS packets are sent to or from the switch domain controller addresses.

CFS Distribution Scopes

Different applications on the Cisco Nexus 5000 Series switches need to distribute the configuration at various levels. The following levels are available when using CFS distribution over Fibre Channel:

- VSAN level (logical scope)

  Applications that operate within the scope of a VSAN have the configuration distribution restricted to the VSAN. An example application is port security where the configuration database is applicable only within a VSAN.

  Note Logical scope is not supported for FCS distribution over IP.

- Physical topology level (physical scope)

Some applications (such as NTP) need to distribute the configuration to the entire physical topology.

- Between two selected switches

  Some applications operate only between selected switches in the network.

CFS Merge Support

CFS Merge is supported for CFS distribution over Fibre Channel.

An application keeps the configuration synchronized in a SAN fabric through CFS. Two such fabrics might merge as a result of an ISL coming up between them. 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 M×N 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 switch in a fabric as the merge manager for that fabric. The other switches do not have a role in the merge process.

During a merge, the merge manager in the two fabrics exchange their configuration databases with each other. The application on one of them merges the information, decides if the merge is successful, and informs all switches in the combined fabric of the status of the merge.

In case of a successful merge, the merged database is distributed to all switches in the combined fabric and the entire new fabric remains in a consistent state. You can recover from a merge failure by starting a distribution from any of the switches in the new fabric. This distribution restores all peers in the fabric to the same configuration database.

CFS Support for Applications

CFS Application Requirements

All switches in the network must be CFS capable. Switches that are not CFS capable do not receive distributions and result in part of the network not receiving the intended distribution. CFS has the following requirements:

- Implicit CFS usage—The first time you issue a CFS task for a CFS-enabled application, the configuration modification process begins and the application locks the network.
- Pending database—The pending database is a temporary buffer to hold uncommitted information. The uncommitted changes are not applied immediately to ensure that the database is synchronized with the database in the other switches in the network. When you commit the changes, the pending database overwrites the configuration database (also known as the active database or the effective database).
- CFS distribution enabled or disabled on a per-application basis—The default (enable or disable) for CFS distribution state differs between applications. If CFS distribution is disabled for an application, then that application does not distribute any configuration nor does it accept a distribution from other switches in the network.
- Explicit CFS commit—Most applications require an explicit commit operation to copy the changes in the temporary buffer to the application database, to distribute the new database to the network, and to

release the network lock. The changes in the temporary buffer are not applied if you do not perform the commit operation.

Enabling CFS for an Application

All CFS-based applications provide an option to enable or disable the distribution capabilities.

Applications have the distribution enabled by default.

The application configuration is not distributed by CFS unless distribution is explicitly enabled for that application.

Verifying Application Registration Status

The **show cfs application** command displays the applications that are currently registered with CFS. The first column displays the application name. The second column indicates whether the application is enabled or disabled for distribution (enabled or disabled). The last column indicates the scope of distribution for the application (logical, physical, or both).

Note The **show cfs application** command only displays applications registered with CFS. Conditional services that use CFS do not appear in the output unless these services are running.

```
switch# show cfs application

----------------------------------------------
 Application    Enabled   Scope
----------------------------------------------
 ntp            No        Physical-all
 fscm           Yes       Physical-fc
 rscn           No        Logical
 fctimer        No        Physical-fc
 syslogd        No        Physical-all
 callhome       No        Physical-all
 fcdomain       Yes       Logical
 device-alias   Yes       Physical-fc
Total number of entries = 8
```

The **show cfs application name** command displays the details for a particular application. It displays the enabled/disabled state, timeout as registered with CFS, merge capability (if it has registered with CFS for merge support), and lastly the distribution scope.

```
switch# show cfs application name fscm

Enabled         : Yes
 Timeout        : 100s
 Merge Capable  : No
 Scope          : Physical-fc
```

Locking the Network

When you configure (first time configuration) a feature (or application) that uses the CFS infrastructure, that feature starts a CFS session and locks the network. When a network is locked, the switch software allows configuration changes to this feature only from the switch holding the lock. If you make configuration changes to the feature from another switch, the switch 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 user name is remembered across restarts and switchovers. If another user (on the same machine) tries to perform configuration tasks, that user's attempts are rejected.

Verifying CFS Lock Status

The **show cfs lock** command displays all the locks that are currently acquired by any application. For each application the command displays the application name and scope of the lock taken. If the application lock is taken in the physical scope, then this command displays the switch WWN, IP address, user name, and user type of the lock holder. If the application is taken in the logical scope, then this command displays the VSAN in which the lock is taken, the domain, IP address, user name, and user type of the lock holder.

```
switch# show cfs lock

Application: ntp
Scope      : Physical
-------------------------------------------------------------------
 Switch WWN               IP Address       User Name    User Type
-------------------------------------------------------------------
 20:00:00:05:30:00:6b:9e  10.76.100.167    admin        CLI/SNMP v3
 Total number of entries = 1

Application: port-security
Scope      : Logical
-----------------------------------------------------------
 VSAN   Domain   IP Address       User Name    User Type
-----------------------------------------------------------
 1      238      10.76.100.167    admin        CLI/SNMP v3
 2      211      10.76.100.167    admin        CLI/SNMP v3
 Total number of entries = 2
```

The **show cfs lock name** command displays the lock details for the specified application:

```
switch# show cfs lock name ntp
Scope      : Physical
-------------------------------------------------------------------
 Switch WWN               IP Address       User Name    User Type
-------------------------------------------------------------------
 20:00:00:05:30:00:6b:9e  10.76.100.167    admin        CLI/SNMP v3

 Total number of entries = 1
```

Committing Changes

A commit operation saves the pending database for all application peers and releases the lock for all switches.

In general, the commit function does not start a session, only a lock function starts a session. However, an empty commit is allowed if configuration changes are not previously made. In this case, a commit operation results in a session that acquires locks and distributes the current database.

When you commit configuration changes to a feature using the CFS infrastructure, you receive a notification about one of the following responses:

- One or more external switches report a successful status—The application applies the changes locally and releases the network lock.
- None of the external switches report a successful state—The application considers this state a failure and does not apply the changes to any switch in the network. The network lock is not released.

You can commit changes for a specified feature by entering the **commit** command for that feature.

Discarding Changes

If you discard configuration changes, the application flushes the pending database and releases locks in the network. Both the abort and commit functions are only supported from the switch from which the network lock is acquired.

You can discard changes for a specified feature by using the **abort** command for that feature.

Saving the Configuration

Configuration changes that have not been applied yet (still in the pending database) are not shown in the running configuration. The configuration changes in the pending database overwrite the configuration in the effective database when you commit the changes.

Caution If you do not commit the changes, they are not saved to the running configuration.

Clearing a Locked Session

You can clear locks held by an application from any switch in the network to recover from situations where locks are acquired and not released. This function requires Admin permissions.

Caution Exercise caution when using this function to clear locks in the network. Any pending configurations in any switch in the network is flushed and lost.

CFS Regions

About CFS Regions

A CFS region is a user-defined subset of switches for a given feature or application in its physical distribution scope. When a network spans a vast geography, you may need to localize or restrict the distribution of certain profiles among a set of switches based on their physical proximity. CFS regions allow you to create multiple islands of distribution within the network for a given CFS feature or application. CFS regions are designed to restrict the distribution of a feature's configuration to a specific set or grouping of switches in a network.

Note You can only configure a CFS region based on physical switches. You cannot configure a CFS region in a VSAN.

Example Scenario

The Call Home application triggers alerts to network administrators when a situation arises or something abnormal occurs. When the network covers many geographies, and there are multiple network administrators who are each responsible for a subset of switches in the network, the Call Home application sends alerts to all network administrators regardless of their location. For the Call Home application to send message alerts

selectively to network administrators, the physical scope of the application has to be fine tuned or narrowed down. This is achieved by implementing CFS regions.

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

If the feature is moved, that is, assigned to a new region, its scope is restricted to that region; it ignores all other regions for distribution or merging purposes. The assignment of the region to a feature has precedence in distribution over its initial physical scope.

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

Managing CFS Regions

Creating CFS Regions

You can create a CFS region.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **cfs region** *region-id*

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters configuration mode.
Step 2	switch(config)# **cfs region** *region-id*	Creates a region.

Assigning Applications to CFS Regions

You can assign an application on a switch to a region.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **cfs region** *region-id*
3. switch(config-cfs-region)# *application*

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters configuration mode.
Step 2	switch(config)# **cfs region** *region-id*	Creates a region.
Step 3	switch(config-cfs-region)# *application*	Adds application(s) to the region. **Note** You can add any number of applications on the switch to a region. If you try adding an application to the same region more than once, you see the error message, "Application already present in the same region."

The following example shows how to assign applications to a region:

```
switch# configure terminal
switch(config)# cfs region 1
switch(config-cfs-region)# ntp
switch(config-cfs-region)# callhome
```

Moving an Application to a Different CFS Region

You can move an application from one region to another region.

SUMMARY STEPS

1. switch# **configure**
2. switch(config)# **cfs region** *region-id*
3. switch(config-cfs-region)# *application*

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure**	Enters configuration mode.
Step 2	switch(config)# **cfs region** *region-id*	Enters CFS region configuration submode.
Step 3	switch(config-cfs-region)# *application*	Indicates application(s) to be moved from one region into another. **Note** If you try moving an application to the same region more than once, you see the error message, "Application already present in the same region."

The following example shows how to move an application into Region 2 that was originally assigned to Region 1:

```
switch# configure terminal
switch(config)# cfs region 2
switch(config-cfs-region)# ntp
```

Removing an Application from a Region

Removing an application from a region is the same as moving the application back to the default region (Region 0). This brings the entire network into the scope of distribution for the application.

SUMMARY STEPS

1. switch# **configure**
2. switch(config)# **cfs region** *region-id*
3. switch(config-cfs-region)# **no** *application*

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure**	Enters configuration mode.
Step 2	switch(config)# **cfs region** *region-id*	Enters CFS region configuration submode.
Step 3	switch(config-cfs-region)# **no** *application*	Removes application(s) that belong to the region.

Deleting CFS Regions

Deleting a region nullifies the region definition. All the applications bound by the region are released back to the default region.

SUMMARY STEPS

1. switch# **configure**
2. switch(config)# **no cfs region** *region-id*

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure**	Enters configuration mode.
Step 2	switch(config)# **no cfs region** *region-id*	Deletes the region. **Note** You see the warning, "All the applications in the region will be moved to the default region."

Configuring CFS over IP

Enabling CFS over IPv4

You can enable or disable CFS over IPv4.

Note CFS cannot distribute over both IPv4 and IPv6 from the same switch.

SUMMARY STEPS

1. switch# **configure**
2. switch(config)# **cfs ipv4 distribute**
3. (Optional) switch(config)# **no cfs ipv4 distribute**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure**	Enters configuration mode.
Step 2	switch(config)# **cfs ipv4 distribute**	Globally enables CFS over IPv6 for all applications on the switch.
Step 3	switch(config)# **no cfs ipv4 distribute**	(Optional) Disables (default) CFS over IPv6 on the switch.

Enabling CFS over IPv6

You can enable or disable CFS over IPv6.

Note CFS cannot distribute over both IPv4 and IPv6 from the same switch.

SUMMARY STEPS

1. switch# **configure**
2. switch(config)# **cfs ipv6 distribute**
3. (Optional) switch(config)# **no cfs ipv6 distribute**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure**	Enters configuration mode.
Step 2	switch(config)# **cfs ipv6 distribute**	Globally enables CFS over IPv6 for all applications on the switch.
Step 3	switch(config)# **no cfs ipv6 distribute**	(Optional) Disables (default) CFS over IPv6 on the switch.

Verifying the CFS Over IP Configuration

To verify the CFS over IP configuration, use the **show cfs status** command.

```
switch# show cfs status
Distribution : Enabled
Distribution over IP : Enabled - mode IPv4
IPv4 multicast address : 239.255.70.83
IPv6 multicast address : ff15::efff:4653
```

Configuring IP Multicast Address for CFS over IP

All CFS over IP enabled switches with similar multicast addresses form one CFS over IP network. CFS protocol-specific distributions, such as the keepalive mechanism for detecting network topology changes, use the IP multicast address to send and receive information.

Note CFS distributions for application data use directed unicast.

Configuring IPv4 Multicast Address for CFS

You can configure a CFS over IP multicast address value for IPv4. The default IPv4 multicast address is 239.255.70.83.

SUMMARY STEPS

1. switch# **configure**
2. switch(config)# **cfs ipv4 mcast-address** *ipv4-address*
3. (Optional) switch(config)# **no cfs ipv4 mcast-address** *ipv4-address*

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure**	Enters configuration mode.
Step 2	switch(config)# **cfs ipv4 mcast-address** *ipv4-address*	Configures the IPv4 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 3	switch(config)# **no cfs ipv4 mcast-address** *ipv4-address*	(Optional) Reverts to the default IPv4 multicast address for CFS distribution over IPv4. The default IPv4 multicast address for CFS is 239.255.70.83.

Configuring IPv6 Multicast Address for CFS

You can configure a CFS over IP multicast address value for IPv6. The default IPv6 multicast address is ff13:7743:4653.

SUMMARY STEPS

1. switch# **configure**
2. switch(config)# **cfs ipv6 mcast-address** *ipv4-address*
3. (Optional) switch(config)# **no cfs ipv6 mcast-address** *ipv4-address*

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure**	Enters configuration mode.
Step 2	switch(config)# **cfs ipv6 mcast-address** *ipv4-address*	Configures the IPv6 multicast address for CFS distribution over IPv6. The range of valid IPv6 addresses is ff15::/16 (ff15::0000:0000 through ff15::ffff:ffff) and ff18::/16 (ff18::0000:0000 through ff18::ffff:ffff).
Step 3	switch(config)# **no cfs ipv6 mcast-address** *ipv4-address*	(Optional) Reverts to the default IPv6 multicast address for CFS distribution over IPv6. The default IPv6 multicast address for CFS over IP is ff15::efff:4653.

Verifying IP Multicast Address Configuration for CFS over IP

To verify the IP multicast address configuration for CFS over IP, use the **show cfs status** command:

```
switch# show cfs status
Fabric distribution Enabled
IP distribution Enabled mode ipv4
IPv4 multicast address : 10.1.10.100
IPv6 multicast address : ff13::e244:4754
```

Displaying CFS Distribution Information

The **show cfs merge status name** command displays the merge status for a given application. The following example displays the output for an application distributing in logical scope. It shows the merge status in all valid VSANs on the switch. The command output shows the merge status as one of the following: Success, Waiting, or Failure or In Progress. In case of a successful merge, all the switches in the network are shown under the local network. In case of a merge failure or a merge in progress, the local network and the remote network involved in the merge are indicated separately. The application server in each network that is mainly responsible for the merge is indicated by the term Merge Master.

```
switch# show cfs merge status name port-security

Logical [VSAN 1] Merge Status: Failed
Local Fabric
----------------------------------------------------------------
 Domain Switch WWN               IP Address
----------------------------------------------------------------
 238    20:00:00:05:30:00:6b:9e  10.76.100.167   [Merge Master]
```

```
Remote Fabric
----------------------------------------------------------------
 Domain Switch WWN               IP Address
----------------------------------------------------------------
 236    20:00:00:0e:d7:00:3c:9e  10.76.100.169    [Merge Master]

Logical [VSAN 2] Merge Status: Success
Local Fabric
----------------------------------------------------------------
 Domain Switch WWN               IP Address
----------------------------------------------------------------
 211    20:00:00:05:30:00:6b:9e  10.76.100.167    [Merge Master]
 1      20:00:00:0e:d7:00:3c:9e  10.76.100.169

Logical [VSAN 3] Merge Status: Success
Local Fabric
----------------------------------------------------------------
 Domain Switch WWN               IP Address
----------------------------------------------------------------
 221    20:00:00:05:30:00:6b:9e  10.76.100.167    [Merge Master]
 103    20:00:00:0e:d7:00:3c:9e  10.76.100.169
```

The following example of the **show cfs merge status name** command output displays an application using the physical scope with a merge failure. The command uses the specified application name to display the merge status based on the application scope.

```
switch# show cfs merge status name ntp

Physical  Merge Status: Failed
Local Fabric
---------------------------------------------------------
 Switch WWN               IP Address
---------------------------------------------------------
 20:00:00:05:30:00:6b:9e  10.76.100.167    [Merge Master]

Remote Fabric
---------------------------------------------------------
 Switch WWN               IP Address
---------------------------------------------------------
 20:00:00:0e:d7:00:3c:9e  10.76.100.169    [Merge Master]
```

The **show cfs peers** command output displays all the switches in the physical network in terms of the switch WWN and the IP address. The local switch is indicated as Local.

```
switch# show cfs peers

Physical Fabric
--------------------------------------------------
 Switch WWN               IP Address
--------------------------------------------------
 20:00:00:05:30:00:6b:9e  10.76.100.167   [Local]
 20:00:00:0e:d7:00:3c:9e  10.76.100.169

 Total number of entries = 2
```

The **show cfs peers name** command displays all the peers for which a particular application is registered with CFS. The command output shows all the peers for the physical scope or for each of the valid VSANs on the switch, depending on the application scope. For physical scope, the switch WWNs for all the peers are indicated. The local switch is indicated as Local.

```
switch# show cfs peers name ntp

Scope      : Physical

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

Switch WWN               IP Address

--------------------------------------------------
```

```
20:00:00:44:22:00:4a:9e  172.22.92.27    [Local]

20:00:00:05:30:01:1b:c2  172.22.92.215
```

The following example **show cfs peers name** command output displays all the application peers (all switches in which that application is registered). The local switch is indicated as Local.

```
switch# show cfs peers name port-security
Scope      : Logical [VSAN 1]

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

Domain   Switch WWN               IP Address

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

124      20:00:00:44:22:00:4a:9e  172.22.92.27    [Local]

98       20:00:00:05:30:01:1b:c2  172.22.92.215

Total number of entries = 2


Scope      : Logical [VSAN 3]

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

Domain   Switch WWN               IP Address

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

224      20:00:00:44:22:00:4a:9e  172.22.92.27    [Local]

151      20:00:00:05:30:01:1b:c2  172.22.92.215

Total number of entries = 2
```

Default CFS Settings

The following table lists the default settings for CFS configurations.

Table 3: Default CFS Parameters

Parameters	Default
CFS distribution on the switch	Enabled.
Database changes	Implicitly enabled with the first configuration change.
Application distribution	Differs based on application.
Commit	Explicit configuration is required.
CFS over IP	Disabled.
IPv4 multicast address	239.255.70.83.

Parameters	Default
IPv6 multicast address	ff15::efff:4653.

The CISCO-CFS-MIB contains SNMP configuration information for any CFS-related functions. Refer to the *Cisco Nexus 5000 Series MIB Quick Reference* for more information on this MIB.

CHAPTER 4

Configuring User Accounts and RBAC

This chapter contains the following sections:

Configuring User Accounts and RBAC

This section describes how to configure user accounts and role-based access control (RBAC) on the Cisco Nexus 5000 Series switch.

Information About User Accounts and RBAC

You can create and manage users accounts and assign roles that limit access to operations on the Cisco Nexus 5000 Series switch. RBAC allows you to define the rules for an assign role that restrict the authorization that the user has to access management operations.

About User Accounts

Tip The following words are reserved and cannot be used to configure users: bin, daemon, adm, lp, sync, shutdown, halt, mail, news, uucp, operator, games, gopher, ftp, nobody, nscd, mailnull, rpc, rpcuser, xfs, gdm, mtsuser, ftpuser, man, and sys.

Note User passwords are not displayed in the configuration files.

Caution The Cisco Nexus 5000 Series switch does not support all numeric usernames, whether created with TACACS+ or RADIUS, or created locally. Local users with all numeric names cannot be created. If an all numeric user name exists on an AAA server and is entered during login, the user is not logged in.

Characteristics of Strong Passwords

A strong password has the following characteristics:

- At least eight characters long
- Does not contain many consecutive characters (such as "abcd")
- Does not contain many repeating characters (such as "aaabbb")
- Does not contain dictionary words
- Does not contain proper names
- Contains both uppercase and lowercase characters
- Contains numbers

The following are examples of strong passwords:

- If2CoM18
- 2009AsdfLkj30
- Cb1955S21

Note Clear text passwords can contain alphanumeric characters only. Special characters, such as the dollar sign ($) or the percent sign (%), are not allowed.

Tip If a password is trivial (such as a short, easy-to-decipher password), the Cisco Nexus 5000 Series switch will reject your password configuration. Be sure to configure a strong password as shown in the sample configuration. Passwords are case sensitive.

About User Roles

User roles contain rules that define the operations allowed for the user who is assigned the role. Each user role can contain multiple rules and each user can have multiple roles. For example, if role1 allows access only to configuration operations, and role2 allows access only to debug operations, then users who belong to both role1 and role2 can access configuration and debug operations. You can also limit access to specific VSANs, VLANs and interfaces.

The Cisco Nexus 5000 Series switch provides the following default user roles:

- network-admin (superuser)—Complete read and write access to the entire Cisco Nexus 5000 Series switch.
- network-operator—Complete read access to the Cisco Nexus 5000 Series switch.

Note If you belong to multiple roles, you can execute a combination of all the commands permitted by these roles. Access to a command takes priority over being denied access to a command. For example, suppose a user has RoleA, which denied access to the configuration commands. However, the users also has RoleB, which has access to the configuration commands. In this case, the users has access to the configuration commands.

About Rules

The rule is the basic element of a role. A rule defines what operations the role allows the user to perform. You can apply rules for the following parameters:

- Command—A command or group of commands defined in a regular expression.
- Feature—Commands that apply to a function provided by the Cisco Nexus 5000 Series switch.
  - Enter the **show role feature** command to display the feature names available for this parameter.
- Feature group—Default or user-defined group of features.
  - Enter the **show role feature-group** command to display the default feature groups available for this parameter.

These parameters create a hierarchical relationship. The most basic control parameter is the command. The next control parameter is the feature, which represents all commands associated with the feature. The last control parameter is the feature group. The feature group combines related features and allows you to easily manage of the rules.

You can configure up to 256 rules for each role. The user-specified rule number determines the order in which the rules are applied. Rules are applied in descending order. For example, if a role has three rules, rule 3 is applied before rule 2, which is applied before rule 1.

About User Role Policies

You can define user role policies to limit the switch resources that the user can access. You can define user role policies to limit access to interfaces, VLANs and VSANs.

User role policies are constrained by the rules defined for the role. For example, if you define an interface policy to permit access to specific interfaces, the user will not have access to the interfaces unless you configure a command rule for the role to permit the interface command.

If a command rule permits access to specific resources (interfaces, VLANs or VSANs), the user is permitted to access these resources, even if they are not listed in the user role policies associated with that user.

Related Topics

- Changing User Role Interface Policies, page 29

Guidelines and Limitations for User Accounts

User account and RBAC have the following configuration guidelines and limitations:

- You can add up to 256 rules to a user role.
- You can assign a maximum of 64 user roles to a user account.

Note A user account must have at least one user role.

Configuring User Accounts

You can create a maximum of 256 user accounts on a Cisco Nexus 5000 Series switch. User accounts have the following attributes:

- Username
- Password
- Expiry date
- User roles

User accounts can have a maximum of 64 user roles.

Note Changes to user account attributes do not take effect until the user logs in and creates a new session.

To configure a user account, perform this task:

SUMMARY STEPS

1. (Optional) switch(config)# **show role**
2. switch# **configure terminal**
3. switch(config)# **username** *user-id* [**password** *password*] [**expire** *date*] [**role** *role-name*]
4. (Optional) switch# **show user-account**
5. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch(config)# **show role**	(Optional) Displays the user roles available. You can configure other user roles, if necessary.
Step 2	switch# **configure terminal**	Enters configuration mode.
Step 3	switch(config)# **username** *user-id* [**password** *password*] [**expire** *date*] [**role** *role-name*]	Configures a user account. The *user-id* argument is a case-sensitive, alphanumeric character string with a maximum length of 28 characters. The default password is undefined.

	Command or Action	Purpose
		Note If you do not specify a password, the user might not be able to log in to the Cisco Nexus 5000 Series switch. The expire *date* option format is YYYY-MM-DD. The default is no expiry date.
Step 4	switch# **show user-account**	(Optional) Displays the role configuration.
Step 5	switch# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

The following example shows how to configure a user account:

```
switch# configure terminal
switch(config)# username NewUser password 4Ty18Rnt

switch(config)# exit
switch# show user-account
```

Configuring RBAC

Creating User Roles and Rules

Each user role can have up to 256 rules. You can assign a user role to more that one user account.

The rule number you specify determines the order in which the rules are applied. Rules are applied in descending order. For example, if a role has three rules, rule 3 is applied before rule 2, which is applied before rule 1.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **role name** *role-name*
3. switch(config-role)# **rule** *number* {**deny** | **permit**} **command** *command-string*
4. switch(config-role)# **rule** *number* {**deny** | **permit**} {**read** | **read-write**}
5. switch(config-role)# **rule** *number* {**deny** | **permit**} {**read** | **read-write**} **feature** *feature-name*
6. switch(config-role)# **rule** *number* {**deny** | **permit**} {**read** | **read-write**} **feature-group** *group-name*
7. (Optional) switch(config-role)# **description** *text*
8. (Optional) switch# **show role**
9. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	switch(config)# **role name** *role-name*	Specifies a user role and enters role configuration mode. The*role-name* argument is a case-sensitive, alphanumeric character string with a maximum length of 16 characters.
Step 3	switch(config-role)# **rule** *number* {**deny** | **permit**} **command** *command-string*	Configures a command rule. The *command-string* argument can contain spaces and regular expressions. For example, "interface ethernet *" includes all Ethernet interfaces. Repeat this command for as many rules as needed.
Step 4	switch(config-role)# **rule** *number* {**deny** | **permit**} {**read** | **read-write**}	Configures a read only or read and write rule for all operations.
Step 5	switch(config-role)# **rule** *number* {**deny** | **permit**} {**read** | **read-write**} **feature** *feature-name*	Configures a read-only or read-and-write rule for a feature. Use the **show role feature** command to display a list of features. Repeat this command for as many rules as needed.
Step 6	switch(config-role)# **rule** *number* {**deny** | **permit**} {**read** | **read-write**} **feature-group** *group-name*	Configures a read-only or read-and-write rule for a feature group. Use the **show role feature-group** command to display a list of feature groups. Repeat this command for as many rules as needed.
Step 7	switch(config-role)# **description** *text*	(Optional) Configures the role description. You can include spaces in the description.
Step 8	switch# **show role**	(Optional) Displays the user role configuration.
Step 9	switch# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

The following example shows how to create user roles and specify rules:

```
switch# configure terminal
switch(config)# role name UserA
switch(config-role)# rule deny command clear users
switch(config-role)# rule deny read-write
switch(config-role)# description This role does not allow users to use clear commands
switch(config-role)# end
switch(config)# show role
```

Creating Feature Groups

You can create feature groups.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **role feature-group** *group-name*
3. (Optional) switch# **show role feature-group**
4. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters configuration mode.
Step 2	switch(config)# **role feature-group** *group-name*	Specifies a user role feature group and enters role feature group configuration mode. The *group-name* argument is a case-sensitive, alphanumeric character string with a maximum length of 32 characters.
Step 3	switch# **show role feature-group**	(Optional) Displays the role feature group configuration.
Step 4	switch# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

Changing User Role Interface Policies

You can change a user role interface policy to limit the interfaces that the user can access.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **role name** *role-name*
3. switch(config-role)# **interface policy deny**
4. switch(config-role-interface)# **permit interface** *interface-list*
5. switch(config-role-interface)# **exit**
6. (Optional) switch(config-role)# **show role**
7. (Optional) switch(config-role)# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters configuration mode.
Step 2	switch(config)# **role name** *role-name*	Specifies a user role and enters role configuration mode.

	Command or Action	Purpose
Step 3	switch(config-role)# **interface policy deny**	Enters role interface policy configuration mode.
Step 4	switch(config-role-interface)# **permit interface** *interface-list*	Specifies a list of interfaces that the role can access. Repeat this command for as many interfaces as needed. For this command, you can specify Ethernet interfaces, Fibre Channel interfaces, and virtual Fibre Channel interfaces.
Step 5	switch(config-role-interface)# **exit**	Exits role interface policy configuration mode.
Step 6	switch(config-role)# **show role**	(Optional) Displays the role configuration.
Step 7	switch(config-role)# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

The following example shows how to change a user role interface policy to limit the interfaces that the user can access:

```
switch# configure terminal
switch(config)# role name UserB
switch(config-role)# interface policy deny
switch(config-role-interface)# permit interface ethernet 2/1
switch(config-role-interface)# permit interface fc 3/1
switch(config-role-interface)# permit interface vfc 30/1
```

You can specify a list of interfaces that the role can access. You can specify it for as many interfaces as needed.

Changing User Role VLAN Policies

You can change a user role VLAN policy to limit the VLANs that the user can access.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **role name** *role-name*
3. switch(config-role)# **vlan policy deny**
4. switch(config-role-vlan)# **permit vlan** *vlan-list*
5. (Optional) switch# **show role**
6. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters configuration mode.
Step 2	switch(config)# **role name** *role-name*	Specifies a user role and enters role configuration mode.

	Command or Action	Purpose
Step 3	switch(config-role)# **vlan policy deny**	Enters role VLAN policy configuration mode.
Step 4	switch(config-role-vlan)# **permit vlan** *vlan-list*	Specifies a range of VLANs that the role can access. Repeat this command for as many VLANs as needed.
Step 5	switch# **show role**	(Optional) Displays the role configuration.
Step 6	switch# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

Changing User Role VSAN Policies

You can change a user role VSAN policy to limit the VSANs that the user can access.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config-role)# **role name** *role-name*
3. switch(config-role)# **vsan policy deny**
4. switch(config-role-vsan)# **permit vsan** *vsan-list*
5. (Optional) switch# **show role**
6. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters configuration mode.
Step 2	switch(config-role)# **role name** *role-name*	Specifies a user role and enters role configuration mode.
Step 3	switch(config-role)# **vsan policy deny**	Enters role VSAN policy configuration mode.
Step 4	switch(config-role-vsan)# **permit vsan** *vsan-list*	Specifies a range of VSANs that the role can access. Repeat this command for as many VSANs as needed.
Step 5	switch# **show role**	(Optional) Displays the role configuration.
Step 6	switch# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

Verifying User Accounts and RBAC Configuration

To display user account and RBAC configuration information, perform one of the following tasks:

Command	Purpose
switch# **show role**	Displays the user role configuration
switch# **show role feature**	Displays the feature list.
switch# **show role feature-group**	Displays the feature group configuration.
switch# **show startup-config security**	Displays the user account configuration in the startup configuration.
switch# **show running-config security** [**all**]	Displays the user account configuration in the running configuration. The all keyword displays the default values for the user accounts.
switch# **show user-account**	Displays user account information.

Default User Account and RBAC Settings

The following table lists the default settings for user accounts and RBAC parameters.

Table 4: Default User Accounts and RBAC Parameters

Parameters	Default
User account password	Undefined.
User account expiry date.	None.
Interface policy	All interfaces are accessible.
VLAN policy	All VLANs are accessible.
VFC policy	All VFCs are accessible.
VETH policy	All VETHs are accessible.

CHAPTER 5

Configuring Session Manager

This chapter contains the following sections:

Configuring Session Manager

This section describes how to configure the Session Manager features in Cisco NX-OS.

Information 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 implements the changes atomically 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.

Configuration Guidelines and Limitations

Session Manager has the following configuration guidelines and limitations:

- Session Manager supports only the ACL feature.

- You can create up to 32 configuration sessions.
- You can configure a maximum of 20,000 commands across all sessions.

Configuring Session Manager

Creating a Session

You can create up to 32 configuration sessions. To create a configuration session, perform this task:

SUMMARY STEPS

1. switch# **configure session** *name*
2. (Optional) switch(config-s)# **show configuration session** [*name*]
3. (Optional) switch(config-s)# **save** *location*

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure session** *name*	Creates a configuration session and enters session configuration mode. The name can be any alphanumeric string.
Step 2	switch(config-s)# **show configuration session** [*name*]	(Optional) Displays the contents of the session.
Step 3	switch(config-s)# **save** *location*	(Optional) Saves the session to a file. The location can be in bootflash or volatile.

Configuring ACLs in a Session

You can configure ACLs within a configuration session. To configure ACLs within a configuration session, perform this task:

SUMMARY STEPS

1. switch# **configure session** *name*
2. switch(config-s)# **ip access-list** *name*
3. (Optional) switch(config-s-acl)# **permit** *protocol source destination*
4. switch(config-s-acl)# **interface** *interface-type number*
5. switch(config-s-if)# **ip port access-group** *name* **in**
6. (Optional) switch# **show configuration session** [*name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure session** *name*	Creates a configuration session and enters session configuration mode. The name can be any alphanumeric string.
Step 2	switch(config-s)# **ip access-list** *name*	Creates an ACL.
Step 3	switch(config-s-acl)# **permit** *protocol source destination*	(Optional) Adds a permit statement to the ACL.
Step 4	switch(config-s-acl)# **interface** *interface-type number*	Enters interface configuration mode.
Step 5	switch(config-s-if)# **ip port access-group** *name* **in**	Adds a port access group to the interface.
Step 6	switch# **show configuration session** [*name*]	(Optional) Displays the contents of the session.

Verifying a Session

To verify a session, use the following command in session mode:

Command	Purpose
switch(config-s)# **verify** [**verbose**]	Verifies the commands in the configuration session.

Committing a Session

To commit a session, use the following command in session mode:

Command	Purpose
switch(config-s)# **commit** [**verbose**]	Commits the commands in the configuration session.

Saving a Session

To save a session, use the following command in session mode:

Command	Purpose
switch(config-s)# **save** *location*	(Optional) Saves the session to a file. The location can be in bootflash or volatile.

Discarding a Session

To discard a session, use the following command in session mode:

Command	Purpose
switch(config-s)# **abort**	Discards the configuration session without applying the commands.

Session Manager Example Configuration

This example shows how to create a configuration session for ACLs:

```
switch# configure session name test2
switch(config-s)# ip access-list acl2
switch(config-s-acl)# permit tcp any any
switch(config-s-acl)# exit
switch(config-s)# interface Ethernet 1/4
switch(config-s-ip)# ip port access-group acl2 in
switch(config-s-ip)# exit
switch(config-s)# verify
switch(config-s)# exit
switch# show configuration session test2
```

Verifying Session Manager Configuration

To verify Session Manager configuration information, use the following commands:

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

CHAPTER 6

Configuring Online Diagnostics

This chapter describes how to configure the generic online diagnostics (GOLD) feature. It contains the following sections:

Information About Online Diagnostics

Online diagnostics provide verification of hardware components during switch bootup or reset, and they monitor the health of the hardware during normal switch operation.

Online Diagnostics Overview

Cisco Nexus 5000 Series switches support bootup diagnostics and runtime diagnostics. Bootup diagnostics include disruptive tests and nondisruptive tests that run during system bootup and system reset.

Runtime diagnostics (also known as health monitoring diagnostics) include nondisruptive tests that run in the background during normal operation of the switch.

Bootup Diagnostics

Bootup diagnostics detect faulty hardware before bringing the switch online. Bootup diagnostics also check the data path and control path connectivity between the supervisor and the ASICs. The following table describes the diagnostics that are run only during switch bootup or reset.

Table 5: Bootup Diagnostics

Diagnostic	Description
PCIe	Tests PCI express (PCIe) access.

Diagnostic	Description
NVRAM	Verifies the integrity of the NVRAM.
In band port	Tests connectivity of the inband port to the supervisor.
Management port	Tests the management port.
Memory	Verifies the integrity of the DRAM.

Bootup diagnostics also include a set of tests that are common with health monitoring diagnostics.

Bootup diagnostics log any failures to the onboard failure logging (OBFL) system. Failures also trigger an LED display to indicate diagnostic test states (on, off, pass, or fail).

You can configure Cisco Nexus 5000 Series switches to either bypass the bootup diagnostics, or run the complete set of bootup diagnostics.

Health Monitoring Diagnostics

Health monitoring diagnostics provide information about the health of the switch. They detect runtime hardware errors, memory errors, software faults, and resource exhaustion.

Health monitoring diagnostics are nondisruptive and run in the background to ensure the health of a switch that is processing live network traffic.

The following table describes the health monitoring diagnostics for the switch.

Table 6: Health Monitoring Diagnostics Tests

Diagnostic	Description
LED	Monitors port and system status LEDs.
Power Supply	Monitors the power supply health state.
Temperature Sensor	Monitors temperature sensor readings.
Test Fan	Monitors fan speed and fan control.

The following table describes the health monitoring diagnostics that also run during system boot or system reset.

Table 7: Health Monitoring and Bootup Diagnostics Tests

Diagnostic	Description
SPROM	Verifies the integrity of backplane and supervisor SPROMs.
Fabric engine	Tests the switch fabric ASICs.

Diagnostic	Description
Fabric port	Tests the ports on the switch fabric ASIC.
Forwarding engine	Tests the forwarding engine ASICs.
Forwarding engine port	Tests the ports on the forwarding engine ASICs.
Front port	Tests the components (such as PHY and MAC) on the front ports.

Expansion Module Diagnostics

During switch bootup or reset, the bootup diagnostics include tests for the in-service expansion modules in the switch.

When you insert an expansion module into a running switch, a set of diagnostics tests are run. The following table describes the bootup diagnostics for an expansion module. These tests are common with the bootup diagnostics. If the bootup diagnostics fail, the expansion module is not placed into service.

Table 8: Expansion Module Bootup and Health Monitoring Diagnostics

Diagnostic	Description
SPROM	Verifies the integrity of backplane and supervisor SPROMs.
Fabric engine	Tests the switch fabric ASICs.
Fabric port	Tests the ports on the switch fabric ASIC.
Forwarding engine	Tests the forwarding engine ASICs.
Forwarding engine port	Tests the ports on the forwarding engine ASICs.
Front port	Tests the components (such as PHY and MAC) on the front ports.

Health monitoring diagnostics are run on in-service expansion modules. The following table describes the additional tests that are specific to health monitoring diagnostics for expansion modules.

Table 9: Expansion Module Health Monitoring Diagnostics

Diagnostic	Description
LED	Monitors port and system status LEDs.
Temperature Sensor	Monitors temperature sensor readings.

Configuring Online Diagnostics

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 boot up time.

Note We recommend that you set the bootup online diagnostics level to complete. We do not recommend bypassing the bootup online diagnostics.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **diagnostic bootup level** [**complete** | **bypass**]
3. (Optional) switch# **show diagnostic bootup level**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters configuration mode.
Step 2	switch(config)# **diagnostic bootup level** [**complete** | **bypass**]	Configures the bootup diagnostic level to trigger diagnostics when the device boots, as follows: • complete—Performs all bootup diagnostics. This is the default value. • bypass—Does not perform any bootup diagnostics.
Step 3	switch# **show diagnostic bootup level**	(Optional) Displays the bootup diagnostic level (bypass or complete) that is currently in place on the switch.

The following example shows how to configure the bootup diagnostics level to trigger the complete diagnostics:

```
switch# configure terminal
switch(config)# diagnostic bootup level complete
```

Verifying Online Diagnostics Configuration

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

Command	Purpose
show diagnostic bootup level	Displays the bootup diagnostics level.
show diagnostic result module *slot*	Displays the results of the diagnostics tests.

Default GOLD Settings

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

Table 10: Default Online Diagnostics Parameters

Parameters	Default
Bootup diagnostics level	complete

CHAPTER 7

Configuring System Message Logging

This chapter describes how to configure system message logging on the Cisco Nexus 5000 Series switch and contains the following sections:

Information 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.

By default, the Cisco Nexus 5000 Series switch outputs messages to terminal sessions.

By default, the switch 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 11: 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

Level	Description
5 – notification	Normal but significant condition
6 – informational	Informational message only
7 – debugging	Appears during debugging only

The switch 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.

Related Topics

- Configuring Module and Facility Messages Logging, page 48
- Configuring System Message Logging to a File, page 47
- Configuring System Message Logging to Terminal Sessions, page 44

syslog Servers

syslog servers run on remote systems that are configured to log system messages based on the syslog protocol. You can configure the Cisco Nexus 5000 Series to sends its logs to up to three syslog servers.

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

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

Configuring System Message Logging

Configuring System Message Logging to Terminal Sessions

You can configure the switch to log messages by their severity level to console, Telnet, and SSH sessions.

By default, logging is enabled for terminal sessions.

SUMMARY STEPS

1. switch# **terminal monitor**
2. switch# **configure terminal**
3. switch(config)# **logging console** [*severity-level*]
4. (Optional) switch(config)# **no logging console** [*severity-level*]
5. switch(config)# **logging monitor** [*severity-level*]
6. (Optional) switch(config)# **no logging monitor** [*severity-level*]
7. (Optional) switch# **show logging console**
8. (Optional) switch# **show logging monitor**
9. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **terminal monitor**	Copies syslog messages from the console to the current terminal session.
Step 2	switch# **configure terminal**	Enters configuration mode.
Step 3	switch(config)# **logging console** [*severity-level*]	Enables the switch to log messages to the console session based on a specified severity level or higher (a lower number value 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.
Step 4	switch(config)# **no logging console** [*severity-level*]	(Optional) Disables logging messages to the console.
Step 5	switch(config)# **logging monitor** [*severity-level*]	Enables the switch to log messages to the monitor based on a specified severity level or higher (a lower number value indicates a higher severity level). Severity levels range from 0 to 7: • 0 – emergency • 1 – alert • 2 – critical

	Command or Action	Purpose
		• 3 – error • 4 – warning • 5 – notification • 6 – informational • 7 – debugging If the severity level is not specified, the default of 2 is used. The configuration applies to Telnet and SSH sessions.
Step 6	switch(config)# **no logging monitor** [*severity-level*]	(Optional) Disables logging messages to telnet and SSH sessions.
Step 7	switch# **show logging console**	(Optional) Displays the console logging configuration.
Step 8	switch# **show logging monitor**	(Optional) Displays the monitor logging configuration.
Step 9	switch# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

The following example shows how to configure a logging level of 3 for the console:

```
switch# configure terminal
switch(config)# logging console 3
```

The following example shows how to display the console logging configuration:

```
switch# show logging console
Logging console:                enabled (Severity: error)
```

The following example shows how to disable logging for the console:

```
switch# configure terminal
switch(config)# no logging console
```

The following example shows how to configure a logging level of 4 for the terminal session:

```
switch# terminal monitor
switch# configure terminal
switch(config)# logging monitor 4
```

The following example shows how to display the terminal session logging configuration:

```
switch# show logging monitor
Logging monitor:                enabled (Severity: warning)
```

The following example shows how to disable logging for the terminal session:

```
switch# configure terminal
switch(config)# no logging monitor
```

Configuring System Message Logging to a File

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

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **logging logfile** *logfile-name severity-level* [**size** *bytes*]
3. (Optional) switch(config)# **no logging logfile** [*logfile-name severity-level* [**size** *bytes*]]
4. (Optional) switch# **show logging info**
5. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters configuration mode.
Step 2	switch(config)# **logging logfile** *logfile-name severity-level* [**size** *bytes*]	Configures the name of the log file used to store system messages and the minimum severity level to log. You can optionally specify a maximum file size. The default severity level is 5 and the file size is 4194304. Severity levels range from 0 to 7: • 0 – emergency • 1 – alert • 2 – critical • 3 – error • 4 – warning • 5 – notification • 6 – informational • 7 – debugging The file size is from 4096 to 10485760 bytes.
Step 3	switch(config)# **no logging logfile** [*logfile-name severity-level* [**size** *bytes*]]	(Optional) Disables logging to the log file.
Step 4	switch# **show logging info**	(Optional) Displays the logging configuration.
Step 5	switch# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

The following example shows how to configure a switch to log system messages to a file:

```
switch# configure terminal
switch(config)# logging logfile my_log 6 size 4194304
```

The following example shows how to display the logging configuration (some of the output has been removed for brevity):

```
switch# show logging info
Logging console:                enabled (Severity: debugging)
Logging monitor:                enabled (Severity: debugging)
Logging linecard:               enabled (Severity: notifications)
Logging fex:            enabled (Severity: notifications)
Logging timestamp:              Seconds
Logging server:                 disabled
Logging logfile:                enabled
        Name - my_log: Severity - informational Size - 4194304
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
aaa                     3                       3
aclmgr                  3                       3
afm                     3                       3
altos                   3                       3
auth                    0                       0
authpriv                3                       3
bootvar                 5                       5
callhome                2                       2
capability              2                       2
cdp                     2                       2
cert_enroll             2                       2
...
```

Related Topics

- Displaying and Clearing Log Files, page 55

Configuring Module and Facility Messages Logging

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

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **logging module** [*severity-level*]
3. switch(config)# **logging level** *facility severity-level*
4. (Optional) switch(config)# **no logging module** [*severity-level*]
5. (Optional) switch(config)# **no logging level** [*facility severity-level*]
6. (Optional) switch# **show logging module**
7. (Optional) switch# **show logging level** [*facility*]
8. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	switch(config)# **logging module** [*severity-level*]	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.
Step 3	switch(config)# **logging level** *facility severity-level*	Enables logging messages from the specified facility that have the specified severity level or higher. Severity levels 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.
Step 4	switch(config)# **no logging module** [*severity-level*]	(Optional) Disables module log messages.
Step 5	switch(config)# **no logging level** [*facility severity-level*]	(Optional) Resets the logging severity level for the specified facility to its default level. If you do not specify a facility and severity level, the switch resets all facilities to their default levels.
Step 6	switch# **show logging module**	(Optional) Displays the module logging configuration.

	Command or Action	Purpose
Step 7	switch# **show logging level** [*facility*]	(Optional) Displays the logging level configuration and the system default level by facility. If you do not specify a facility, the switch displays levels for all facilities.
Step 8	switch# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

The following example shows how to configure the severity level of module and specific facility messages:

```
switch# configure terminal
switch(config)# logging module 3
switch(config)# logging level aaa 2
```

Configuring Logging Timestamps

You can configure the time-stamp units of messages logged by the Cisco Nexus 5000 Series switch.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **logging timestamp** {**microseconds** | **milliseconds** | **seconds**}
3. (Optional) switch(config)# **no logging timestamp** {**microseconds** | **milliseconds** | **seconds**}
4. (Optional) switch# **show logging timestamp**
5. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters configuration mode.
Step 2	switch(config)# **logging timestamp** {**microseconds** | **milliseconds** | **seconds**}	Sets the logging time-stamp units. By default, the units are seconds.
Step 3	switch(config)# **no logging timestamp** {**microseconds** | **milliseconds** | **seconds**}	(Optional) Resets the logging time-stamp units to the default of seconds.
Step 4	switch# **show logging timestamp**	(Optional) Displays the logging time-stamp units configured.
Step 5	switch# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

The following example shows how to configure the time-stamp units of messages:

```
switch# configure terminal
switch(config)# logging timestamp milliseconds
switch(config)# exit
switch# show logging timestamp
Logging timestamp:              Milliseconds
```

Configuring syslog Servers

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

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **logging server** *host* [*severity-level* [**use-vrf** *vrf-name* [**facility** *facility*]]]
3. (Optional) switch(config)# **no logging server** *host*
4. (Optional) switch# **show logging server**
5. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters configuration mode.
Step 2	switch(config)# **logging server** *host* [*severity-level* [**use-vrf** *vrf-name* [**facility** *facility*]]]	Configures a host to receive syslog messages. • The *host* argument identifies the host name or the IPv4 or IPv6 address of the syslog server host. • The *severity-level* argument limits the logging of messages to the syslog server to a specified level. Severity levels range from 0 to 7. Refer to Table 11: System Message Severity Levels , page 43 • The **use vrf** *vrf-name* keyword argument identifies the *default* or *management* values for the VRF name. If a specific VRF is not identified, management is the default. However, if management is configured, it will not be listed in the output of the **show-running** command because it is the default. If a specific VRF is configured, the **show-running** command output will list the VRF for each server. **Note** The current CFS distribution does not support VRF. If CFS distribution is enabled, then the logging server configured with the default VRF will be distributed as the management VRF. • The facility argument names the syslog facility type. The facilities are listed in the Cisco Nexus 5000 Series Command Reference. The default outgoing facility is local7.

	Command or Action	Purpose
Step 3	switch(config)# **no logging server** *host*	(Optional) Removes the logging server for the specified host.
Step 4	switch# **show logging server**	(Optional) Displays the syslog server configuration.
Step 5	switch# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

The following examples show how to configure a syslog server:

```
switch# configure terminal
switch(config)# logging server 172.28.254.254 5
use-vrf default facility local3
```

```
switch# configure terminal
switch(config)# logging server 172.28.254.254 5
use-vrf mgmt0 facility local3
```

Table 12: Related Commands

Command	Descriptions
show logging server	Displays the configured syslog servers.

Configuring syslog 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 13: 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.

Field	Description
Action	Destination for messages, which can be a filename, a host name preceded by the at sign (@), or a comma-separated list of users or an asterisk (*) for all logged-in users.

SUMMARY STEPS

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:
2. Create the log file by entering these commands at the shell prompt:
3. Make sure the system message logging daemon reads the new changes by checking myfile.log after entering this command:

DETAILED STEPS

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:

```
debug.local7            /var/log/myfile.log
```

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

```
$ 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:

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

Configuring syslog Server Configuration Distribution

You can distribute the syslog server configuration to other switches in the network by using the Cisco Fabric Services (CFS) infrastructure.

After you enable syslog server configuration distribution, you can modify the syslog server configuration and view the pending changes before committing the configuration for distribution. As long as distribution is enabled, the switch maintains pending changes to the syslog server configuration.

Note If the switch is restarted, the syslog server configuration changes that are kept in volatile memory may be lost.

Before You Begin

You must have configured one or more syslog servers.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **logging distribute**
3. switch(config)# **logging commit**
4. switch(config)# **logging abort**
5. (Optional) switch(config)# **no logging distribute**
6. (Optional) switch# **show logging pending**
7. (Optional) switch# **show logging pending-diff**
8. (Optional) switch# **show logging internal info**
9. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters configuration mode.
Step 2	switch(config)# **logging distribute**	Enables distribution of syslog server configuration to network switches using the CFS infrastructure. By default, distribution is disabled.
Step 3	switch(config)# **logging commit**	Commits the pending changes to the syslog server configuration for distribution to the switches in the fabric.
Step 4	switch(config)# **logging abort**	Cancels the pending changes to the syslog server configuration.
Step 5	switch(config)# **no logging distribute**	(Optional) Disables distribution of syslog server configuration to network switches using the CFS infrastructure. You cannot disable distribution when configuration changes are pending. See the **logging commit** and **logging abort** commands. By default, distribution is disabled.
Step 6	switch# **show logging pending**	(Optional) Displays the pending changes to the syslog server configuration.
Step 7	switch# **show logging pending-diff**	(Optional) Displays the differences from the current syslog server configuration to the pending changes of the syslog server configuration.
Step 8	switch# **show logging internal info**	(Optional) Displays information about the current state of syslog server distribution and the last action taken.
Step 9	switch# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

Related Topics

- Information About CFS, page 5

Displaying and Clearing Log Files

You can display or clear messages in the log file and the NVRAM.

SUMMARY STEPS

1. switch# **show logging last** *number-lines*
2. switch# **show logging logfile** [**start-time** *yyyy mmm dd hh:mm:ss*] [**end-time** *yyyy mmm dd hh:mm:ss*]
3. switch# **show logging nvram** [**last** *number-lines*]
4. switch# **clear logging logfile**
5. switch# **clear logging nvram**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **show logging last** *number-lines*	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	switch# **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 that have a time stamp 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	switch# **show logging nvram** [**last** *number-lines*]	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	switch# **clear logging logfile**	Clears the contents of the log file.
Step 5	switch# **clear logging nvram**	Clears the logged messages in NVRAM.

The following example shows how to display messages in a log file:

```
switch# show logging last 40
switch# show logging logfile start-time 2007 nov 1 15:10:0
switch# show logging nvram last 10
```

The following example shows how to clear messages in a log file:

```
switch# clear logging logfile
switch# clear logging nvram
```

Verifying System Message Logging Configuration

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

Command	Purpose
switch# **show logging console**	Displays the console logging configuration.

Command	Purpose
switch# **show logging info**	Displays the logging configuration.
switch# **show logging internal info**	Displays the syslog distribution information.
switch# **show logging last** *number-lines*	Displays the last number of lines of the log file.
switch# **show logging level** [*facility*]	Displays the facility logging severity level configuration.
switch# **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.
switch# **show logging module**	Displays the module logging configuration.
switch# **show logging monitor**	Displays the monitor logging configuration.
switch# **show logging nvram** [**last** *number-lines*]	Displays the messages in the NVRAM log.
switch# **show logging pending**	Displays the syslog server pending distribution configuration.
switch# **show logging pending-diff**	Displays the syslog server pending distribution configuration differences.
switch# **show logging server**	Displays the syslog server configuration.
switch# **show logging session**	Displays the logging session status.
switch# **show logging status**	Displays the logging status.
switch# **show logging timestamp**	Displays the logging time-stamp units configuration.

Default System Message Logging Settings

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

Table 14: Default System Message Logging Parameters

Parameters	Default
Console logging	Enabled at severity level 2
Monitor logging	Enabled at severity level 2
Log file logging	Enabled to log:messages at severity level 5
Module logging	Enabled at severity level 5

Parameters	Default
Facility logging	Enabled;
Time-stamp units	Seconds
syslog server logging	Disabled
syslog server configuration distribution	Disabled

CHAPTER 8

Configuring Smart Call Home

This chapter contains the following sections:

Configuring Smart Call Home

Information About Call Home

Call Home provides e-mail-based notification of critical system events. Cisco Nexus 5000 Series switches provide 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.

Call Home Overview

You can use Call Home to notify an external entity when an important event occurs on your device. Call Home delivers alerts to multiple recipients that you configure in *destination profiles*.

Call Home includes a fixed set of predefined alerts on your switch. These alerts are grouped into alert groups and CLI commands to are assigned to execute when an alert in an alert group occurs. The switch includes the command output in the transmitted Call Home message.

The Call Home feature offers the following advantages:

- 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—Matching readable format that uses the Extensible Markup Language (XML) and the Adaptive Messaging Language (AML) XML schema definition (XSD). The XML format enables communication with the Cisco Systems Technical Assistance Center (Cisco-TAC).

- Multiple concurrent message destinations. You can configure up to 50 e-mail 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 Call Home message if the alert occurs.
- One or more e-mail destinations—The list of receipents for the Call Home messages generated by alert groups assigned to this destination profile.
- Message format—The format for the Call Home message (short text, full text, or XML).
- Message severity level—The Call Home severity level that the alert must meet before the switch generates a Call Home message to all e-mail addresses in the destination profile. The Cisco Nexus 5000 Series switch does not generate an alert if the 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 Nexus 5000 Series switches support the following predefined destination profiles:

- CiscoTAC-1—Supports the Cisco-TAC alert group in XML message format.
- full-text-destination—Supports the full text message format.
- short-text-destination—Supports the short text message format.

Call Home Alert Groups

An alert group is a predefined subset of Call Home alerts that are supported in all Cisco Nexus 5000 Series switches. Alert groups allow you to select the set of Call Home alerts that you want to send to a predefined or custom destination profile. The switch sends Call Home alerts to e-mail destinations in a destination profile only if that Call Home alert belongs to one of the alert groups associated with that destination profile and if the alert has a Call Home message severity at or above the message severity set in the destination profile.

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

Table 15: Alert Groups and Executed Commands

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.
Diagnostic	Events generated by diagnostics.	**show diagnostic result module all detail** **show moduleshow version**

Alert Group	Description	Executed Commands
		show tech-support platform callhome
Supervisor hardware	Events related to supervisor modules.	**show diagnostic result module all detail** **show moduleshow version** **show tech-support platform callhome**
Linecard hardware	Events related to standard or intelligent switching modules.	**show diagnostic result module all detail** **show moduleshow version** **show tech-support platform callhome**
Configuration	Periodic events related to configuration.	**show version** **show module** **show running-config all** **show startup-config**
System	Events generated by failure of a software system that is critical to unit operation.	**show system redundancy status** **show tech-support**
Environmental	Events related to power, fan, and environment-sensing elements such as temperature alarms.	**show environment** **show logging last 1000** **show module show version** **show tech-support platform callhome**
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 module** **show version** **show license usage** **show inventory** **show sprom all** **show system uptime**

Call Home maps the syslog severity level to the corresponding 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 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.

Related Topics

- Call Home Message Levels , page 62

Call Home Message Levels

Call Home allows you to filter messages based on their level of urgency. You can associate each destination profile (predefined and user defined) with a Call Home message level threshold. The switch does not generate any Call Home messages with a value lower than this threshold for the destination profile. The Call Home message level ranges from 0 (lowest level of urgency) to 9 (highest level of urgency), and the default is 0 (Cisco Nexus 5000 Series sends all messages).

Call Home messages that are sent for syslog alert groups have the syslog severity level mapped to the Call Home message level.

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

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

Table 16: Severity and syslog Level Mapping

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

Call Home Level	Keyword	syslog Level	Description
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 Systems, you can register your devices for the Smart Call Home service. Smart Call Home provides fast resolution of system problems by analyzing Call Home messages sent from your devices and providing background information and recommendations. For issues that can be identified as known, particularly GOLD diagnostics failures, Automatic Service Requests will be generated with the Cisco-TAC.

Smart Call Home offers the following features:

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

You need the following items to register:

- The SMARTnet contract number for your switch.
- Your e-mail address
- Your Cisco.com ID

For more information about Smart Call Home, see the Smart Call Home page at this URL: http://www.cisco.com/go/smartcall/

Prerequisites for Call Home

Call Home has the following prerequisites:

- You must configure an e-mail server.
- You must configure the contact name (SNMP server contact), phone, and street address information before you enable Call Home. This step is required to determine the origin of messages received.
- Your switch must have IP connectivity to an e-mail server.
- If you use Smart Call Home, you need an active service contract for the device that you are configuring.

Configuration Guidelines and Limitations

Call Home has the following configuration guidelines and limitations:

- If there is no IP connectivity or if the interface in the VRF to the profile destination is down, the switch cannot send the Call Home message.
- Operates with any SMTP server.

Configuring Call Home

Procedures for Configuring Call Home

SUMMARY STEPS

1. Assign contact information.
2. Configure destination profiles.
3. Associate one or more alert groups to each profile.
4. (Optional) Add additional **show** commands to the alert groups.
5. Configure transport options.
6. Enable Call Home.
7. (Optional) Test Call Home messages.

DETAILED STEPS

Step 1 Assign contact information.

Step 2 Configure destination profiles.

Step 3 Associate one or more alert groups to each profile.

Step 4 (Optional) Add additional **show** commands to the alert groups.

Step 5 Configure transport options.

Step 6 Enable Call Home.

Step 7 (Optional) Test Call Home messages.

Configuring Contact Information

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

SUMMARY STEPS

1. switch# **configuration terminal**
2. switch(config)# **snmp-server contact** *sys-contact*
3. switch(config)# **callhome**
4. switch(config-callhome)# **email-contact** *email-address*
5. switch(config-callhome)# **phone-contact** *international-phone-number*
6. switch(config-callhome)# **streetaddress** *address*
7. (Optional) switch(config-callhome)# **contract-id** *contract-number*
8. (Optional) switch(config-callhome)# **customer-id** *customer-number*
9. (Optional) switch(config-callhome)# **site-id** *site-number*
10. (Optional) switch(config-callhome)# **switch-priority** *number*
11. (Optional) switch# **show callhome**
12. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configuration terminal**	Enters configuration mode.
Step 2	switch(config)# **snmp-server contact** *sys-contact*	Configures the SNMP sysContact.
Step 3	switch(config)# **callhome**	Enters callhome configuration mode.
Step 4	switch(config-callhome)# **email-contact** *email-address*	Configures the e-mail address for the primary person responsible for the switch. Up to 255 alphanumeric characters are accepted in e-mail address format. **Note** You can use any valid e-mail address. The address cannot contain spaces.
Step 5	switch(config-callhome)# **phone-contact** *international-phone-number*	Configures the phone number in international phone number format for the primary person responsible for the device. Up to 17 alphanumeric characters are accepted in international format. **Note** The phone number cannot contain spaces. Be sure to use the + prefix before the number.
Step 6	switch(config-callhome)# **streetaddress** *address*	Configures the street address as an alphanumeric string with white paces for the primary person responsible for the switch. Up to 255 alphanumeric characters are accepted, including spaces.
Step 7	switch(config-callhome)# **contract-id** *contract-number*	(Optional) Configures the contract number for this switch from the service agreement. The contract number can be up to 255 alphanumeric characters in free format.

	Command or Action	Purpose
Step 8	switch(config-callhome)# **customer-id** *customer-number*	(Optional) Configures the customer number for this switch from the service agreement. The customer number can be up to 255 alphanumeric characters in free format.
Step 9	switch(config-callhome)# **site-id** *site-number*	(Optional) Configures the site number for this switch. The site number can be up to 255 alphanumeric characters in free format.
Step 10	switch(config-callhome)# **switch-priority** *number*	(Optional) Configures the switch priority for this switch. The range is from 0 to 7, with 0 being the highest priority and 7 the lowest. The default is 7.
Step 11	switch# **show callhome**	(Optional) Displays a summary of the Call Home configuration.
Step 12	switch# **copy running-config startup-config**	(Optional) Saves this configuration change.

This example shows how to configure the contact information for Call Home:

```
switch# configuration terminal
switch(config)# snmp-server contact personname@companyname.com
switch(config)# callhome
switch(config-callhome)# email-contact personname@companyname.com
switch(config-callhome)# phone-contact +1-800-123-4567
switch(config-callhome)# street-address 123 Anystreet St., Anycity, Anywhere
```

Creating a Destination Profile

You must create a user-defined destination profile and configure the message format for that new destination profile.

SUMMARY STEPS

1. switch# **configuration terminal**
2. switch(config)# **callhome**
3. switch(config-callhome)# **destination-profile** {**ciscoTAC-1** {**alert-group** *group* | **email-addr** *address* | **http** *URL* | **transport-method** {**email** | **http**}} | *profile-name* {**alert-group** *group* | **email-addr** *address* | **format** {**XML** | **full-txt** | **short-txt**} | **http** *URL* | **message-level** *level* | **message-size** *size* | **transport-method** {**email** | **http**}} | **full-txt-destination** {**alert-group** *group* | **email-addr** *address* | **http** *URL* | **message-level** *level* | **message-size** *size* | **transport-method** {**email** | **http**}} | **short-txt-destination** {**alert-group** *group* | **email-addr** *address* | **http** *URL* | **message-level** *level* | **message-size** *size* | **transport-method** {**email** | **http**}}}
4. (Optional) switch# **show callhome destination-profile** [**profile** *name*]
5. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configuration terminal**	Enters configuration mode.
Step 2	switch(config)# **callhome**	Enters callhome configuration mode.
Step 3	switch(config-callhome)# **destination-profile** {**ciscoTAC-1** {**alert-group** *group* | **email-addr** *address* | **http** *URL* | **transport-method** {**email** | **http**}} | *profile-name* {**alert-group** *group* | **email-addr** *address* | **format** {**XML** | **full-txt** | **short-txt**} | **http** *URL* | **message-level** *level* | **message-size** *size* | **transport-method** {**email** | **http**}} | **full-txt-destination** {**alert-group** *group* | **email-addr** *address* | **http** *URL* | **message-level** *level* | **message-size** *size* | **transport-method** {**email** | **http**}} | **short-txt-destination** {**alert-group** *group* | **email-addr** *address* | **http** *URL* | **message-level** *level* | **message-size** *size* | **transport-method** {**email** | **http**}}}	Creates a new destination profile and sets the message format for the profile. The profile-name can be any alphanumeric string up to 31 characters. For further details about this command, see the *Cisco Nexus 5000 Series Command Reference*.
Step 4	switch# **show callhome destination-profile** [**profile** *name*]	(Optional) Displays information about one or more destination profiles.
Step 5	switch# **copy running-config startup-config**	(Optional) Saves this configuration change.

This example shows how to create a destination profile for Call Home:

```
switch# configuration terminal
switch(config)# callhome
switch(config-callhome)# destination-profile Noc101 format full-text
```

Modifying a Destination Profile

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

- Destination address—The actual address, pertinent to the transport mechanism, to which the alert should be sent.
- Message formatting—The message format used for sending the alert (full text, short text, or XML).
- Message level—The Call Home message severity level for this destination profile.
- Message size—The allowed length of a Call Home message sent to the e-mail addresses in this destination profile.

Note You cannot modify or delete the CiscoTAC-1 destination profile.

SUMMARY STEPS

1. switch# **configuration terminal**
2. switch(config)# **callhome**
3. switch(config-callhome)# **destination-profile** {*name* | **full-txt-destination** | **short-txt-destination**} **email-addr** *address*
4. **destination-profile** {*name* | **full-txt-destination** | **short-txt-destination**} **message-level** *number*
5. switch(config-callhome)# **destination-profile** {*name* | **full-txt-destination** | **short-txt-destination**} **message-size** *number*
6. (Optional) switch# **show callhome destination-profile** [**profile** *name*]
7. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configuration terminal**	Enters configuration mode.
Step 2	switch(config)# **callhome**	Enters callhome configuration mode.
Step 3	switch(config-callhome)# **destination-profile** {*name* | **full-txt-destination** | **short-txt-destination**} **email-addr** *address*	Configures an e-mail address for a user-defined or predefined destination profile. You can configure up to 50 e-mail addresses in a destination profile.
Step 4	**destination-profile** {*name* | **full-txt-destination** | **short-txt-destination**} **message-level** *number*	Configures the Call Home message severity level for this destination profile. The switch sends only alerts that have a matching or higher Call Home severity level to destinations in this profile. The range is from 0 to 9, where 9 is the highest severity level.
Step 5	switch(config-callhome)# **destination-profile** {*name* | **full-txt-destination** | **short-txt-destination**} **message-size** *number*	Configures the maximum message size for this destination profile. The range is from 0 to 5000000 for full-txt-destination and the default is 2500000; from 0 to 100000 for short-txt-destination and the default is 4000; 5000000 for CiscoTAC-1, which is not changeable.
Step 6	switch# **show callhome destination-profile** [**profile** *name*]	(Optional) Displays information about one or more destination profiles.
Step 7	switch# **copy running-config startup-config**	(Optional) Saves this configuration change.

This example shows how to modify a destination profile for Call Home:

```
switch# configuration terminal
switch(config)# callhome
switch(config-callhome)# destination-profile full-text-destination email-addr
person@example.com
switch(config-callhome)# destination-profile full-text-destination message-level 5
switch(config-callhome)# destination-profile full-text-destination message-size 10000
```

Related Topics

- Associating an Alert Group with a Destination Profile, page 69

Associating an Alert Group with a Destination Profile

To associate one or more alert groups with a destination profile, perform this task:

SUMMARY STEPS

1. switch# **configuration terminal**
2. switch(config)# **callhome**
3. switch(config-callhome)# **destination-profile** *name* **alert-group** {**All** | **Cisco-TAC** | **Configuration** | **Diagnostic** | **Environmental** | **Inventory** | **License** | **Linecard-Hardware** | **Supervisor-Hardware** | **Syslog-group-port** | **System** | **Test**}
4. (Optional) switch# **show callhome destination-profile** [**profile** *name*]
5. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configuration terminal**	Enters configuration mode.
Step 2	switch(config)# **callhome**	Enters callhome configuration mode.
Step 3	switch(config-callhome)# **destination-profile** *name* **alert-group** {**All** | **Cisco-TAC** | **Configuration** | **Diagnostic** | **Environmental** | **Inventory** | **License** | **Linecard-Hardware** | **Supervisor-Hardware** | **Syslog-group-port** | **System** | **Test**}	Associates an alert group with this destination profile. Use the **All** keyword to associate all alert groups with the destination profile.
Step 4	switch# **show callhome destination-profile** [**profile** *name*]	(Optional) Displays information about one or more destination profiles.
Step 5	switch# **copy running-config startup-config**	(Optional) Saves this configuration change.

This example shows how to associate all alert groups with the destination profile Noc101:

```
switch# configuration terminal
switch(config)# callhome
switch(config-callhome)# destination-profile Noc101 alert-group All
```

Adding show Commands to an Alert Group

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

SUMMARY STEPS

1. switch# **configuration terminal**
2. switch(config)# **callhome**
3. switch(config-callhome)# **alert-group** {**Configuration** | **Diagnostic** | **Environmental** | **Inventory** | **License** | **Linecard-Hardware** | **Supervisor-Hardware** | **Syslog-group-port** | **System** | **Test**} **user-def-cmd** *show-cmd*
4. (Optional) switch# **show callhome user-def-cmds**
5. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configuration terminal**	Enters configuration mode.
Step 2	switch(config)# **callhome**	Enters callhome configuration mode.
Step 3	switch(config-callhome)# **alert-group** {**Configuration** | **Diagnostic** | **Environmental** | **Inventory** | **License** | **Linecard-Hardware** | **Supervisor-Hardware** | **Syslog-group-port** | **System** | **Test**} **user-def-cmd** *show-cmd*	Adds the **show** command output to any Call Home messages sent for this alert group. Only valid **show** commands are accepted. **Note** You cannot add user-defined CLI **show** commands to the CiscoTAC-1 destination profile.
Step 4	switch# **show callhome user-def-cmds**	(Optional) Displays information about all user-defined **show** commands added to alert groups.
Step 5	switch# **copy running-config startup-config**	(Optional) Saves this configuration change.

This example shows how to add the **show ip routing** command o the Cisco-TAC alert group:

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

Configuring E-Mail

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

SUMMARY STEPS

1. switch# **configuration terminal**
2. switch(config)# **callhome**
3. switch(config-callhome)# **transport email smtp-server** *ip-address* [**port** *number*] [**use-vrf** *vrf-name*]
4. (Optional) switch(config-callhome)# **transport email from** *email-address*
5. (Optional) switch(config-callhome)# **transport email reply-to** *email-address*
6. (Optional) switch# **show callhome transport-email**
7. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configuration terminal**	Enters configuration mode.
Step 2	switch(config)# **callhome**	Enters callhome configuration mode.
Step 3	switch(config-callhome)# **transport email smtp-server** *ip-address* [**port** *number*] [**use-vrf** *vrf-name*]	Configures the SMTP server as either the domain name server (DNS) name, IPv4 address, or IPv6 address). Optionally you can configure the port number. The port ranges is from 1 to 65535. The default port number is 25. Also optionally you can configure the VRF to use when communicating with this SMTP server.
Step 4	switch(config-callhome)# **transport email from** *email-address*	(Optional) Configures the e-mail from field for Call Home messages.
Step 5	switch(config-callhome)# **transport email reply-to** *email-address*	(Optional) Configures the e-mail reply-to field for Call Home messages.
Step 6	switch# **show callhome transport-email**	(Optional) Displays information about the e-mail configuration for Call Home.
Step 7	switch# **copy running-config startup-config**	(Optional) Saves this configuration change.

This example shows how to configure the e-mail options for Call Home messages:

```
switch# configuration terminal
switch(config)# callhome
switch(config-callhome)# transport email smtp-server 192.0.2.10 use-vrf Red
switch(config-callhome)# transport email from person@example.com
switch(config-callhome)# transport email reply-to person@example.com
```

Configuring Periodic Inventory Notification

You can configure the switch 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 switch generates two Call Home notifications; periodic configuration messages and periodic inventory messages.

SUMMARY STEPS

1. switch# **configuration terminal**
2. switch(config)# **callhome**
3. switch(config-callhome)# **periodic-inventory notification** [**interval** *days*] [**timeofday** *time*]
4. (Optional) switch# **show callhome**
5. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configuration terminal**	Enters configuration mode.
Step 2	switch(config)# **callhome**	Enters callhome configuration mode.
Step 3	switch(config-callhome)# **periodic-inventory notification** [**interval** *days*] [**timeofday** *time*]	Configures the periodic inventory messages. The interval range is from 1 to 30 days. The default is 7 days. The timeofday value is in HH:MM format.
Step 4	switch# **show callhome**	(Optional) Displays information about Call Home.
Step 5	switch# **copy running-config startup-config**	(Optional) Saves this configuration change.

This example shows how to configure the periodic inventory messages to generate every 20 days:

```
switch# configuration terminal
switch(config)# callhome
switch(config-callhome)# periodic-inventory notification interval 20
```

Disabling Duplicate Message Throttle

You can limit the number of duplicate messages received for the same event. By default, the switch 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, then the switch discards further messages for that alert type.

Command	Purpose
switch(config-callhome)# **no duplicate-message throttle**	Disables duplicate message throttling for Call Home. Enabled by default.

Enabling or Disabling Call Home

Once you have configured the contact information, you can enable the Call Home function in callhome configuration mode.

Command	Purpose
switch(config-callhome)# **enable**	Enables Call Home. Disabled by default.

You can disable Call Home in the callhome configuration mode.

Command	Purpose
switch(config-callhome)# **no enable**	Disables Call Home. Disabled by default

You can enable Call Home distribution using CFS in the callhome configuration mode.

Command	Purpose
switch(config-callhome)# **distribute**	Enables Call Home distribution using CFS. Disabled by default.

You can commit Call Home configuration changes and distribute using CFS in the callhome configuration mode.

Command	Purpose
switch(config-callhome)# **commit**	Commits Call Home configuration changes and distributes the changes to call CFS-enabled devices.

You can discard Call Home configuration changes and release the CFS lock in callhome configuration mode.

Command	Purpose
switch(config-callhome)# **abort**	Discards Call Home configuration changes and releases the CFS lock. Use this command if you are the CFS lock owner or if you are logged into the device that holds the CFS lock

Testing Call Home Communications

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

Command	Purpose
switch(config-callhome)# **callhome send diagnostic**	Sends the specified Call Home test message to all configured destinations.
switch(config-callhome)# **callhome test**	Sends a test message to all configured destinations. **callhome test** and **callhome test inventory** commands are supported.

Verifying Call Home Configuration

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

Command	Purpose
switch# **show callhome**	Displays the status for Call Home.
switch# **show callhome destination-profile** *name*	Displays one or more Call Home destination profiles.
switch# **show callhome merge**	Displays the status of the last CFS merge for Call Home.
switch# **show callhome pending**	Displays the Call Home configuration changes in the pending CFS database.
switch# **show callhome pending-diff**	Displays the differences between the pending and running Call Home configuration.
switch# **show callhome session**	Displays the status of the last Call Home CFS command.
switch# **show callhome status**	Displays the Call Home status.
switch# **show callhome transport-email**	Displays the e-mail configuration for Call Home.
switch# **show callhome user-def-cmds**	Displays CLI commands added to any alert groups.
switch# **show running-config** [**callhome** | **callhome-all**]	Displays the running configuration for Call Home.
switch# **show startup-config callhome**	Displays the startup configuration for Call Home.
switch# **show tech-support callhome**	Displays the technical support output for Call Home.

Default Call Home Settings

The following table lists the default settings for Call Home parameters.

Table 17: Default Call Home Parameters

Parameters	Default
Destination message size for a message sent in full text format.	4000000
Destination message size for a message sent in XML format.	4000000

Parameters	Default
Destination message size for a message sent in short text format.	4000
SMTP server port number if no port is specified.	25
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
Call Home message level.	0 (zero)

Additional References

Call Home Message Formats

Call Home supports the following message formats:

- Short Text Message Format
- Common Fields for All Full Text and XML Messages
- Inserted Fields for a Reactive or Proactive Event Message
- Inserted Fields for an Inventory Event Message
- Inserted Fields for a User-Generated Test Message

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

Table 18: Short Text Message Format

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

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

Table 19: Common Fields for All Full Text and XML Messages

Data Item(Plain Text and XML)	Description(Plain Text and XML)	XML Tag (XML Only)
Time stamp	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. Specific event names are listed in the preceding table.	/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
Source ID	Product type for routing. Specifically Catalyst 6500.	/aml/header/source
Device ID	Unique device identifier (UDI) for 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 backplane IDPROM.	/aml/ header/deviceID

Data Item(Plain Text and XML)	Description(Plain Text and XML)	XML Tag (XML Only)
	• @ 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	
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 is the unique device identifier (UDI) of the device.	/aml/header/serverID

Data Item(Plain Text and XML)	Description(Plain Text and XML)	XML Tag (XML Only)
	The format is *type@Sid@serial*: • *type* is the product model number from 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	
Message description	Short text that describes the error.	/aml/body/msgDesc
Device name	Node that experienced the event (host name 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 e-mail	E-mail address of person identified as the contact for this unit.	/aml/body/sysContactEmail
Contact phone number	Phone number of the person identified	/aml/body/sysContactPhoneNumber

Data Item(Plain Text and XML)	Description(Plain Text and XML)	XML Tag (XML Only)
	as the contact for this unit.	
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
Fields specific to a particular alert group message are inserted here.		
The following fields may be repeated if multiple CLI commands are executed for this alert group.		
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/data

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

Table 20: Inserted Fields for a Reactive or Proactive Event Message

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
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

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

Table 21: Inserted Fields for an Inventory Event Message

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

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

Table 22: Inserted Fields for a User-Generated Test Message

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
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:

```
source:MDS9000
Switch Priority:7
Device Id:WS-C6509@C@FG@07120011
Customer Id:Example.com
Contract Id:123
Site Id:San Jose
Server Id:WS-C6509@C@FG@07120011
Time of Event:2004-10-08T11:10:44
Message Name:SYSLOG_ALERT
Message Type:Syslog
Severity Level:2
System Name:10.76.100.177
Contact Name:User Name
Contact Email:person@example.com
Contact Phone:+1-408-555-1212
Street Address:#1234 Any Street, Any City, Any State, 12345
Event Description:2006 Oct  8 11:10:44 10.76.100.177 %PORT-5-IF_TRUNK_UP: %$VLAN 1%$ Interface
 e2/5, vlan 1 is up

syslog_facility:PORT
start chassis information:
Affected Chassis:WS-C6509
Affected Chassis Serial Number:FG@07120011
Affected Chassis Hardware Version:0.104
Affected Chassis Software Version:3.1(1)
Affected Chassis Part No:73-8607-01
end chassis information:
```

Sample syslog Alert Notification in XML Format

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

```
From: example
Sent: Wednesday, April 25, 2007 7:20 AM
To: User (user)
Subject: System Notification From Router - syslog - 2007-04-25 14:19:55
GMT+00:00
```

```xml
<?xml version="1.0" encoding="UTF-8"?>
<soap-env:Envelope xmlns:soap-env="http://www.w3.org/2003/05/soap-envelope">
<soap-env:Header>
<aml-session:Session xmlns:aml-session="http://www.example.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.example.com/services/DDCEService</aml-session:To>
<aml-session:Path>
<aml-session:Via>http://www.example.com/appliance/uri</aml-session:Via>
</aml-session:Path>
<aml-session:From>http://www.example.com/appliance/uri</aml-session:From>
<aml-session:MessageId>M2:69000101:C9D9E20B</aml-session:MessageId>
</aml-session:Session>
</soap-env:Header>
<soap-env:Body>
<aml-block:Block xmlns:aml-block="http://www.example.com/2004/01/aml-block">
<aml-block:Header>
<aml-block:Type>http://www.example.com/2005/05/callhome/syslog</aml-block:Type>
<aml-block:CreationDate>2007-04-25 14:19:55 GMT+00:00</aml-block:CreationDate>
<aml-block:Builder>
<aml-block:Name>Cat6500</aml-block:Name>
<aml-block:Version>2.0</aml-block:Version>
</aml-block:Builder>
<aml-block:BlockGroup>
<aml-block:GroupId>G3:69000101:C9F9E20C</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>2</aml-block:Severity>
</aml-block:Header>
<aml-block:Content>
<ch:Call Home xmlns:ch="http://www.example.com/2005/05/callhome" version="1.0">
<ch:EventTime>2007-04-25 14:19:55 GMT+00:00</ch:EventTime>
<ch:MessageDescription>03:29:29: %CLEAR-5-COUNTERS: Clear counter on all interfaces by
console</ch:MessageDescription>
<ch:Event>
<ch:Type>syslog</ch:Type>
<ch:SubType></ch:SubType>
<ch:Brand>Cisco Systems</ch:Brand>
<ch:Series>Catalyst 6500 Series Switches</ch:Series>
</ch:Event>
<ch:CustomerData>
<ch:UserData>
<ch:Email>person@example.com</ch:Email>
</ch:UserData>
<ch:ContractData>
<ch:CustomerId>12345</ch:CustomerId>
<ch:SiteId>building 1</ch:SiteId>
<ch:ContractId>abcdefg12345</ch:ContractId>
<ch:DeviceId>WS-C6509@C@69000101</ch:DeviceId>
</ch:ContractData>
<ch:SystemInfo>
<ch:Name>Router</ch:Name>
<ch:Contact></ch:Contact>
<ch:ContactEmail>user@example.com</ch:ContactEmail>
<ch:ContactPhoneNumber>+1-408-555-1212</ch:ContactPhoneNumber>
<ch:StreetAddress>#1234 Any Street, Any City, Any State, 12345</ch:StreetAddress>
</ch:SystemInfo>
</ch:CustomerData>
<ch:Device>
<rme:Chassis xmlns:rme="http://www.example.com/rme/4.0">
<rme:Model>WS-C6509</rme:Model>
<rme:HardwareVersion>1.0</rme:HardwareVersion>
<rme:SerialNumber>69000101</rme:SerialNumber>
<rme:AdditionalInformation>
<rme:AD name="PartNumber" value="73-3438-03 01" />
<rme:AD name="SoftwareVersion" value="4.0(20080421:012711)" />
</rme:AdditionalInformation>
</rme:Chassis>
</ch:Device>
</ch:Call Home>
```

```
</aml-block:Content>
<aml-block:Attachments>
<aml-block:Attachment type="inline">
<aml-block:Name>show logging</aml-block:Name>
<aml-block:Data encoding="plain">
<![CDATA[
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited, 0 flushes, 0 overruns,
 xml disabled, filtering disabled)
    Console logging: level debugging, 53 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging: level debugging, 53 messages logged, xml disabled,
                    filtering disabled
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    Trap logging: level informational, 72 message lines logged

Log Buffer (8192 bytes):

00:00:54: curr is 0x20000

00:00:54: RP: Currently running ROMMON from F2 region
00:01:05: %SYS-5-CONFIG_I: Configured from memory by console
00:01:09: %SYS-5-RESTART: System restarted --
Cisco IOS Software, s72033_rp Software (s72033_rp-ADVENTERPRISEK9_DBG-VM), Experimental
Version 12.2(20070421:012711)

Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 26-Apr-07 15:54 by xxx

Firmware compiled 11-Apr-07 03:34 by integ Build [100]


00:01:01: %PFREDUN-6-ACTIVE: Initializing as ACTIVE processor for this switch
00:01:01: %SYS-3-LOGGER_FLUSHED: System was paused for 00:00:00 to ensure console debugging
 output.
00:03:00: SP: SP: Currently running ROMMON from F1 region
00:03:07: %C6K_PLATFORM-SP-4-CONFREG_BREAK_ENABLED: The default factory setting for config
 register is 0x2102.It is advisable to retain 1 in 0x2102 as it prevents returning to ROMMON
 when break is issued.

00:03:18: %SYS-SP-5-RESTART: System restarted --
Cisco IOS Software, s72033_sp Software (s72033_sp-ADVENTERPRISEK9_DBG-VM), Experimental
Version 12.2(20070421:012711)
```

```
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 26-Apr-07 18:00 by xxx
00:03:18: %SYS-SP-6-BOOTTIME: Time taken to reboot after reload =  339 seconds
00:03:18: %OIR-SP-6-INSPS: Power supply inserted in slot 1
00:03:18: %C6KPWR-SP-4-PSOK: power supply 1 turned on.
00:03:18: %OIR-SP-6-INSPS: Power supply inserted in slot 2
00:01:09: %SSH-5-ENABLED: SSH 1.99 has been enabled
00:03:18: %C6KPWR-SP-4-PSOK: power supply 2 turned on.
00:03:18: %C6KPWR-SP-4-PSREDUNDANTMISMATCH: power supplies rated outputs do not match.
00:03:18: %C6KPWR-SP-4-PSREDUNDANTBOTHSUPPLY: in power-redundancy mode, system is operating
 on both power supplies.
00:01:10: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
00:01:10: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
00:03:20: %C6KENV-SP-4-FANHIOUTPUT: Version 2 high-output fan-tray is in effect
00:03:22: %C6KPWR-SP-4-PSNOREDUNDANCY: Power supplies are not in full redundancy, power
usage exceeds lower capacity supply
00:03:26: %FABRIC-SP-5-FABRIC_MODULE_ACTIVE: The Switch Fabric Module in slot 6 became
active.
00:03:28: %DIAG-SP-6-RUN_MINIMUM: Module 6: Running Minimal Diagnostics...
00:03:50: %DIAG-SP-6-DIAG_OK: Module 6: Passed Online Diagnostics
00:03:50: %OIR-SP-6-INSCARD: Card inserted in slot 6, interfaces are now online
00:03:51: %DIAG-SP-6-RUN_MINIMUM: Module 3: Running Minimal Diagnostics...
00:03:51: %DIAG-SP-6-RUN_MINIMUM: Module 7: Running Minimal Diagnostics...
00:03:51: %DIAG-SP-6-RUN_MINIMUM: Module 9: Running Minimal Diagnostics...
00:01:51: %MFIB_CONST_RP-6-REPLICATION_MODE_CHANGE: Replication Mode Change Detected. Current
 system replication mode is Ingress
00:04:01: %DIAG-SP-6-DIAG_OK: Module 3: Passed Online Diagnostics
00:04:01: %OIR-SP-6-DOWNGRADE: Fabric capable module 3 not at an appropriate hardware
revision level, and can only run in flowthrough mode
00:04:02: %OIR-SP-6-INSCARD: Card inserted in slot 3, interfaces are now online
00:04:11: %DIAG-SP-6-DIAG_OK: Module 7: Passed Online Diagnostics
00:04:14: %OIR-SP-6-INSCARD: Card inserted in slot 7, interfaces are now online
00:04:35: %DIAG-SP-6-DIAG_OK: Module 9: Passed Online Diagnostics
00:04:37: %OIR-SP-6-INSCARD: Card inserted in slot 9, interfaces are now online
00:00:09: DaughterBoard (Distributed Forwarding Card 3)

Firmware compiled 11-Apr-07 03:34 by integ Build [100]


00:00:22: %SYS-DFC4-5-RESTART: System restarted --
Cisco DCOS Software, c6lc2 Software (c6lc2-SPDBG-VM), Experimental Version
4.0(20080421:012711)

Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 26-Apr-08 17:20 by xxx
00:00:23: DFC4: Currently running ROMMON from F2 region
00:00:25: %SYS-DFC2-5-RESTART: System restarted --
Cisco IOS Software, c6slc Software (c6slc-SPDBG-VM), Experimental Version
12.2(20070421:012711)

Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 26-Apr-08 16:40 by username1
00:00:26: DFC2: Currently running ROMMON from F2 region
00:04:56: %DIAG-SP-6-RUN_MINIMUM: Module 4: Running Minimal Diagnostics...
00:00:09: DaughterBoard (Distributed Forwarding Card 3)

Firmware compiled 11-Apr-08 03:34 by integ Build [100]

slot_id is 8

00:00:31: %FLASHFS_HES-DFC8-3-BADCARD: /bootflash:: The flash card seems to be corrupted
00:00:31: %SYS-DFC8-5-RESTART: System restarted --
Cisco DCOS Software, c6lc2 Software (c6lc2-SPDBG-VM), Experimental Version
4.0(20080421:012711)
```

```
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 26-Apr-08 17:20 by username1
00:00:31: DFC8: Currently running ROMMON from S (Gold) region
00:04:59: %DIAG-SP-6-RUN_MINIMUM: Module 2: Running Minimal Diagnostics...
00:05:12: %DIAG-SP-6-RUN_MINIMUM: Module 8: Running Minimal Diagnostics...
00:05:13: %DIAG-SP-6-RUN_MINIMUM: Module 1: Running Minimal Diagnostics...
00:00:24: %SYS-DFC1-5-RESTART: System restarted --
Cisco DCOS Software, c6slc Software (c6slc-SPDBG-VM), Experimental Version
4.0(20080421:012711)

Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 26-Apr-08 16:40 by username1
00:00:25: DFC1: Currently running ROMMON from F2 region
00:05:30: %DIAG-SP-6-DIAG_OK: Module 4: Passed Online Diagnostics
00:05:31: %SPAN-SP-6-SPAN_EGRESS_REPLICATION_MODE_CHANGE: Span Egress HW Replication Mode
Change Detected. Current replication mode for unused asic session 0 is Centralized
00:05:31: %SPAN-SP-6-SPAN_EGRESS_REPLICATION_MODE_CHANGE: Span Egress HW Replication Mode
Change Detected. Current replication mode for unused asic session 1 is Centralized
00:05:31: %OIR-SP-6-INSCARD: Card inserted in slot 4, interfaces are now online
00:06:02: %DIAG-SP-6-DIAG_OK: Module 1: Passed Online Diagnostics
00:06:03: %OIR-SP-6-INSCARD: Card inserted in slot 1, interfaces are now online
00:06:31: %DIAG-SP-6-DIAG_OK: Module 2: Passed Online Diagnostics
00:06:33: %OIR-SP-6-INSCARD: Card inserted in slot 2, interfaces are now online
00:04:30: %XDR-6-XDRIPCNOTIFY: Message not sent to slot 4/0 (4) because of IPC error timeout.
 Disabling linecard. (Expected during linecard OIR)
00:06:59: %DIAG-SP-6-DIAG_OK: Module 8: Passed Online Diagnostics
00:06:59: %OIR-SP-6-DOWNGRADE_EARL: Module 8 DFC installed is not identical to system PFC
and will perform at current system operating mode.
00:07:06: %OIR-SP-6-INSCARD: Card inserted in slot 8, interfaces are now online

Router#]]></aml-block:Data>
</aml-block:Attachment>
</aml-block:Attachments>
</aml-block:Block>
</soap-env:Body>
</soap-env:Envelope>
```

CHAPTER 9

Configuring SNMP

This chapter describes the configuration of the Simple Network Management Protocol (SNMP) on Cisco Nexus 5000 Series switches and contains the following sections:

Information 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 5000 Series switch 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

Note Cisco NX-OS does not support SNMP sets for Ethernet MIBs.

The Cisco Nexus 5000 Series switch supports SNMPv1, SNMPv2c and SNMPv3. Both SNMPv1 and SNMPv2c use a community-based form of security. SNMP is defined in RFC 3410 (http://tools.ietf.org/html/rfc3410), RFC 3411 (http://tools.ietf.org/html/rfc3411), RFC 3412 (http://tools.ietf.org/html/rfc3412), RFC 3413 (http://tools.ietf.org/html/rfc3413), RFC 3414 (http://tools.ietf.org/html/rfc3414), RFC 3415 (http://tools.ietf.org/html/rfc3415), RFC 3416 (http://tools.ietf.org/html/rfc3416), RFC 3417 (http://tools.ietf.org/html/rfc3417), RFC 3418 (http://tools.ietf.org/html/rfc3418), and RFC 3584 (http://tools.ietf.org/html/rfc3584).

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. Traps are less reliable than informs because the SNMP manager does not send any acknowledgment when it receives a trap. The switch 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 Cisco Nexus 5000 Series switch never receives a response, it can send the inform request again.

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

Related Topics

- Configuring SNMP Notification Receivers, page 93

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.

User-Based Security Model

The following table identifies what the combinations of security models and levels mean.

Table 23: 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.

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 non-maliciously.

- 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 along with the aes-128 token indicates 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 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 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 user configuration in the following ways:

- The auth passphrase specified in the **snmp-server user** command becomes the password for the CLI user.
- The password specified in the **username** command becomes as the auth and priv passphrases for the SNMP user.
- Deleting a user using either SNMP or the CLI results in the user being deleted for both SNMP and the CLI.
- User-role mapping changes are synchronized in SNMP and the CLI.

Note When you configure passphrase/password in localized key/encrypted format, Cisco NX-OS does not synchronize the password.

Group-Based SNMP Access

Note Because group is a standard SNMP term used industry-wide, roles are referred to 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 three accesses: read access, write access, and notification access. Each access can be enabled or disabled within each group.

You can begin communicating with the agent once your user name is created, your roles are set up by your administrator, and you are added to the roles.

Configuration Guidelines and Limitations

SNMP has the following configuration guidelines and limitations:

- Cisco NX-OS supports read-only access to Ethernet MIBs.

Configuring SNMP

Configuring SNMP Users

To configure a user for SNMP, perform this task:

SUMMARY STEPS

1. switch# **configuration terminal**
2. switch(config)# **snmp-server user** *name* [**auth** {**md5** | **sha**} *passphrase* [**auto**] [**priv** [**aes-128**] *passphrase*] [**engineID** *id*] [**localizedkey**]]
3. (Optional) switch# **show snmp user**
4. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	switch(config)# **snmp-server user** *name* [**auth** {**md5** | **sha**} *passphrase* [**auto**] [**priv** [**aes-128**] *passphrase*] [**engineID** *id*] [**localizedkey**]]	Configures an SNMP user with authentication and privacy parameters.
Step 3	switch# **show snmp user**	(Optional) Displays information about one or more SNMP users.
Step 4	switch# **copy running-config startup-config**	(Optional) Saves this configuration change.

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 securityLevel parameter of either noAuthNoPriv or authNoPriv.

You can enforce SNMP message encryption for a specific user.

Command	Purpose
switch(config)# **snmp-server user** *name* **enforcePriv**	Enforces SNMP message encryption for this user.

You can enforce SNMP message encryption for all users.

Command	Purpose
switch(config)# **snmp-server globalEnforcePriv**	Enforces SNMP message encryption for all users.

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.

Command	Purpose
switch(config)# **snmp-server user** *name group*	Associates this SNMP user with the configured user role.

Creating SNMP Communities

You can create SNMP communities for SNMPv1 or SNMPv2c.

To create an SNMP community string in a global configuration mode, perform this task:

Command	Purpose
switch(config)# **snmp-server community** *name group* {**ro** | **rw**}	Creates an SNMP community string.

Filtering SNMP Requests

You can assign an access list (ACL) to a 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)

See the *Cisco Nexus 5000 Series NX-OS Security Configuration Guide* for more information on creating ACLs. The ACL applies to both IPv4 and IPv6 over UDP and TCP. After creating the ACL, assign the ACL to the SNMP community.

Use the following command in global configuration mode to assign an ACL to a community to filter SNMP requests:

Command	Purpose
switch(config)# **snmp-server community** *community name* **use-acl** *acl-name* **Example:** `switch(config)# snmp-server community public use-acl my_acl_for_public`	Assigns an ACL to an SNMP community to filter SNMP requests.

Before You Begin

Create an ACL to assign to the SNMP community.

Assign the ACL to the SNMP community.

Configuring SNMP Notification Receivers

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

You can configure a host receiver for SNMPv1 traps in a global configuration mode.

Command	Purpose
switch(config)# **snmp-server host** *ip-address* **traps version 1** *community* [**udp_port** *number*]	Configures a host receiver for SNMPv1 traps. The community can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535.

You can configure a host receiver for SNMPv2c traps or informs in a global configuration mode.

Command	Purpose
switch(config)# **snmp-server host** *ip-address* {**traps** | **informs**} **version 2c** *community* [**udp_port** *number*]	Configures a host receiver for SNMPv2c traps or informs. The community can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535.

You can configure a host receiver for SNMPv3 traps or informs in a global configuration mode.

Command	Purpose
switch(config)# **snmp-server host** *ip-address* {**traps** | **informs**} **version 3** {**auth** | **noauth** | **priv**} *username* [**udp_port** *number*]	Configures a host receiver for SNMPv2c traps or informs. 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 engineID of the Cisco Nexus 5000 Series switch to authenticate and decrypt the SNMPv3 messages.

The following example shows how to configure a host receiver for an SNMPv1 trap:

```
switch(config)# snmp-server host 192.0.2.1 traps version 1 public
```

The following example shows how to configure a host receiver for an SNMPv2 inform:

```
switch(config)# snmp-server host 192.0.2.1 informs version 2c public
```

The following example shows how to configure a host receiver for an SNMPv3 inform:

```
switch(config)# snmp-server host 192.0.2.1 informs version 3 auth NMS
```

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.

The Cisco Nexus 5000 Series switch 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 the Cisco Nexus 5000 Series switch to authenticate and decrypt the informs.

Command	Purpose
switch(config)# **snmp-server user** *name* [**auth** {**md5** | **sha**} *passphrase* [**auto**] [**priv** [**aes-128**] *passphrase*] [**engineID** *id*]	Configures the notification target user with the specified engine ID for notification host receiver. The engineID format is a 12-digit colon-separated hexadecimal number.

The following example shows how to configure a notification target user:

```
switch(config)# snmp-server user NMS auth sha abcd1234 priv abcdefgh engineID
00:00:00:63:00:01:00:a1:ac:15:10:03
```

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** CLI command enables both traps and informs, depending on the configured notification host receivers.

The following table lists the CLI commands that enable the notifications for Cisco NX-OS MIBs.

Table 24: Enabling SNMP Notifications

MIB	Related Commands
All notifications	**snmp-server enable traps**
CISCO-AAA-SERVER-MIB	**snmp-server enable traps aaa**
ENITY-MIB, CISCO-ENTITY-FRU-CONTROL-MIB, CISCO-ENTITY-SENSOR-MIB	**snmp-server enable traps entity** **snmp-server enable traps entity fru**
CISCO-LICENSE-MGR-MIB	**snmp-server enable traps license**
IF-MIB	**snmp-server enable traps link**
CISCO-PSM-MIB	**snmp-server enable traps port-security**
SNMPv2-MIB	**snmp-server enable traps snmp** **snmp-server enable traps snmp authentication**

MIB	Related Commands
CISCO-FCC-MIB	**snmp-server enable traps fcc**
CISCO-DM-MIB	**snmp-server enable traps fcdomain**
CISCO-NS-MIB	**snmp-server enable traps fcns**
CISCO-FCS-MIB	**snmp-server enable traps fcs discovery-complete** **snmp-server enable traps fcs request-reject**
CISCO-FDMI-MIB	**snmp-server enable traps fdmi**
CISCO-FSPF-MIB	**snmp-server enable traps fspf**
CISCO-PSM-MIB	**snmp-server enable traps port-security**
CISCO-RSCN-MIB	**snmp-server enable traps rscn** **snmp-server enable traps rscn els** **snmp-server enable traps rscn ils**
CISCO-ZS-MIB	**snmp-server enable traps zone** **snmp-server enable traps zone default-zone-behavior-change** **snmp-server enable traps zone merge-failure** **snmp-server enable traps zone merge-success** **snmp-server enable traps zone request-reject** **snmp-server enable traps zone unsupp-mem**

Note The license notifications are enabled by default. All other notifications are disabled by default.

To enable the specified notification in the global configuration mode, perform one of the following tasks:

Command	Purpose
switch(config)# **snmp-server enable traps**	Enables all SNMP notifications.
switch(config)# **snmp-server enable traps aaa** [**server-state-change**]	Enables the AAA SNMP notifications.
switch(config)# **snmp-server enable traps entity** [**fru**]	Enables the ENTITY-MIB SNMP notifications.
switch(config)# **snmp-server enable traps license**	Enables the license SNMP notification.

Command	Purpose
switch(config)# **snmp-server enable traps port-security**	Enables the port security SNMP notifications.
switch(config)# **snmp-server enable traps snmp** [**authentication**]	Enables the SNMP agent notifications.

Configuring Link Notifications

You can configure which linkUp/linkDown notifications to enable on a device. You can enable the following types of linkUp/linkDown notifications:

- Cisco—Cisco NX-OS sends only the Cisco-defined notifications (cieLinkUp, cieLinkDow in CISCO-IF-EXTENSION-MIB.my), if ifLinkUpDownTrapEnable (defined in IF-MIB) is enabled for that interface.
- IETF—Cisco NX-OS sends only the IETF-defined notifications (linkUp, linkDown in IF-MIB) with only the defined varbinds, if ifLinkUpDownTrapEnable (defined in IF-MIB) is enabled for that interface.
- IEFT extended—Cisco NX-OS sends only the IETF-defined notifications (linkUp, linkDown defined in IF-MIB), if ifLinkUpDownTrapEnable (defined in IF-MIB) is enabled for that interface. Cisco NX-OS adds additional varbinds specific to Cisco Systems in addition to the varbinds defined in the IF-MIB. This is the default setting.
- IEFT Cisco—Cisco NX-OS sends the notifications (linkUp, linkDown) defined in IF-MIB and notifications (cieLinkUp, cieLinkDown) defined in CISCO-IF-EXTENSION-MIB.my , if ifLinkUpDownTrapEnable (defined in IF-MIB) is enabled for that interface. Cisco NX-OS sends only the varbinds defined in the linkUp and linkDown notifications.
- IEFT extended Cisco—Cisco NX-OS sends the notifications (linkUp, linkDown) defined in IF-MIB and notifications (cieLinkUp, cieLinkDown) defined in CISCO-IF-EXTENSION-MIB.my, if ifLinkUpDownTrapEnable (defined in IF-MIB) is enabled for that interface. Cisco NX-OS adds additional varbinds specific to Cisco Systems in addition to the varbinds defined in the IF-MIB for the linkUp and linkDown notifications.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **snmp-server enable traps link** [**cisco**] [**ietf** | **ietf-extended**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters configuration mode.
Step 2	switch(config)# **snmp-server enable traps link** [**cisco**] [**ietf** | **ietf-extended**]	Enables the link SNMP 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).

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** *type slot/port*
3. switch(config -if)# **no snmp trap link-status**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters configuration mode.
Step 2	switch(config)# **interface** *type slot/port*	Specifies the interface to be changed.
Step 3	switch(config -if)# **no snmp trap link-status**	Disables SNMP link-state traps for the interface. Enabled by default.

Enabling One-Time Authentication for SNMP over TCP

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

Command	Purpose
switch(config)# **snmp-server tcp-session** [**auth**]	Enables a one-time authentication for SNMP over a TCP session. Default is disabled.

Assigning SNMP Switch Contact and Location Information

You can assign the switch contact information, which is limited to 32 characters (without spaces), and the switch location.

SUMMARY STEPS

1. switch# **configuration terminal**
2. switch(config)# **snmp-server contact** *name*
3. switch(config)# **snmp-server location** *name*
4. (Optional) switch# **show snmp**
5. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configuration terminal**	Enters configuration mode.
Step 2	switch(config)# **snmp-server contact** *name*	Configures sysContact, the SNMP contact name.
Step 3	switch(config)# **snmp-server location** *name*	Configures sysLocation, the SNMP location.
Step 4	switch# **show snmp**	(Optional) Displays information about one or more destination profiles.
Step 5	switch# **copy running-config startup-config**	(Optional) Saves this configuration change.

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.

SUMMARY STEPS

1. switch# **configuration terminal**
2. switch(config)# **snmp-server context** *context-name* [**instance** *instance-name*] [**vrf** *vrf-name*] [**topology** *topology-name*]
3. switch(config)# **snmp-server mib community-map** *community-name* **context** *context-name*
4. (Optional) switch(config)# **no snmp-server context** *context-name* [**instance** *instance-name*] [**vrf** *vrf-name*] [**topology** *topology-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configuration terminal**	Enters configuration mode.
Step 2	switch(config)# **snmp-server context** *context-name* [**instance** *instance-name*] [**vrf** *vrf-name*] [**topology** *topology-name*]	Maps an SNMP context to a protocol instance, VRF, or topology. The names can be any alphanumeric string up to 32 characters.
Step 3	switch(config)# **snmp-server mib community-map** *community-name* **context** *context-name*	Maps an SNMPv2c community to an SNMP context. The names can be any alphanumeric string up to 32 characters.
Step 4	switch(config)# **no snmp-server context** *context-name* [**instance** *instance-name*] [**vrf** *vrf-name*] [**topology** *topology-name*]	(Optional) Deletes the mapping between an SNMP context and a protocol instance, VRF, or topology. The names can be any alphanumeric string up to 32 characters.

	Command or Action	Purpose
		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.

Verifying SNMP Configuration

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

Command	Purpose
switch# **show snmp**	Displays the SNMP status.
switch# **show snmp community**	Displays the SNMP community strings.
switch# **show snmp engineID**	Displays the SNMP engineID.
switch# **show snmp group**	Displays SNMP roles.
switch# **show snmp sessions**	Displays SNMP sessions.
switch# **show snmp trap**	Displays the SNMP notifications enabled or disabled.
switch# **show snmp user**	Displays SNMPv3 users.

Default SNMP Settings

The following table lists the default settings for SNMP parameters.

Table 25: Default SNMP Parameters

Parameters	Default
license notifications	enabled
linkUp/Down notification type	ietf-extended

CHAPTER 10

Configuring RMON

This chapter contains the following sections:

Configuring RMON

Information About RMON

RMON is an Internet Engineering Task Force (IETF) standard monitoring specification that allows various network agents and console systems to exchange network monitoring data. The Cisco NX-OS supports RMON alarms, events and logs to monitor Cisco Nexus 5000 Series switches

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 disabled by default and no events or alarms are configured in Cisco Nexus 5000 Series. You can configure your RMON alarms and events 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, 1.3.6.1.2.1.2.2.1.17 represents ifOutOctets.17).

When you create an alarm, you specify the following parameters:

- MIB object to monitor
- Sampling interval—The interval that the Cisco Nexus 5000 Series switch uses to collect a sample value of the MIB object.
- The 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 Cisco Nexus 5000 Series switch triggers a rising alarm or resets a falling alarm.
- Falling threshold—The value at which the Cisco Nexus 5000 Series switch triggers a falling alarm or resets a rising alarm.
- Events—The action that the Cisco Nexus 5000 Series switch 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.

Configuration Guidelines and Limitations

RMON has the following configuration guidelines and limitations:

- You must configure an SNMP user an notification receiver to use the SNMP notification event type.
- You can only configure an RMON alarm on a MIB object that resolves to an integer.

Configuring RMON

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.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **rmon alarm** *index mib-object sample-interval* {**absolute** | **delta**} **rising-threshold** *value* [*event-index*] **falling-threshold** *value* [*event-index*] [**owner** *name*]
3. switch(config)# **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*]
4. (Optional) switch# **show rmon** {**alarms** | **hcalarms**}
5. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters configuration mode.
Step 2	switch(config)# **rmon alarm** *index mib-object sample-interval* {**absolute** | **delta**} **rising-threshold** *value* [*event-index*] **falling-threshold** *value* [*event-index*] [**owner** *name*]	Creates an RMON alarm. The value range is from -2147483647 to 2147483647. The owner name can be any alphanumeric string.
Step 3	switch(config)# **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*]	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	switch# **show rmon** {**alarms** | **hcalarms**}	(Optional) Displays information about RMON alarms or high-capacity alarms.
Step 5	switch# **copy running-config startup-config**	(Optional) Saves this configuration change.

The following example shows how to configure RMON alarms:

```
switch# configure terminal
switch(config)# rmon alarm 1 1.3.6.1.2.1.2.2.1.17.83886080 5 delta rising-threshold 5 1
falling-threshold 0 owner test
switch(config)# exit
switch# show rmon alarms
Alarm 1 is active, owned by test
 Monitors 1.3.6.1.2.1.2.2.1.17.83886080 every 5 second(s)
 Taking delta samples, last value was 0
 Rising threshold is 5, assigned to event 1
 Falling threshold is 0, assigned to event 0
 On startup enable rising or falling alarm
```

Configuring RMON Events

You can configure RMON events to associate with RMON alarms. You can reuse the same event with multiple RMON alarms.

Ensure you have configured an SNMP user and enabled SNMP notifications.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **rmon event** *index* [**description** *string*] [**log**] [**trap**] [**owner** *name*]
3. (Optional) switch(config)# **show rmon** {**alarms** | **hcalarms**}
4. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters configuration mode.
Step 2	switch(config)# **rmon event** *index* [**description** *string*] [**log**] [**trap**] [**owner** *name*]	Configures an RMON event. The description string and owner name can be any alphanumeric string.
Step 3	switch(config)# **show rmon** {**alarms** | **hcalarms**}	(Optional) Displays information about RMON alarms or high-capacity alarms.
Step 4	switch# **copy running-config startup-config**	(Optional) Saves this configuration change.

Verifying RMON Configuration

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

Command	Purpose
switch# **show rmon alarms**	Displays information about RMON alarms.
switch# **show rmon events**	Displays information about RMON events.
switch# **show rmon hcalarms**	Displays information about RMON hcalarms.
switch# **show rmon logs**	Displays information about RMON logs.

Default RMON Settings

The following table lists the default settings for RMON parameters.

Table 26: Default RMON Parameters

Parameters	Default
Alarms	None configured.
Events	None configured.

INDEX

R

S

T

U