



Cisco Nexus 5000 Series NX-OS System Management Configuration Guide, Release 5.0(2)N1(1)

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

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

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

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

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

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

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at <http://cisco.com/go/trademarks>. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

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

© 2010 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface xi

Audience xi

Document Organization xi

Document Conventions xii

Related Documentation for Nexus 5000 Series NX-OS Software xiii

Obtaining Documentation and Submitting a Service Request xiv

New and Changed Information 1

New and Changed Information 1

Overview 3

System Management Overview 3

Configuring Switch Profiles 5

Configuring Switch Profiles 5

Information About Switch Profiles 5

Switch Profile Configuration Modes 6

Configuration Validation 7

Software Upgrades and Downgrades With Switch Profiles 7

Prerequisites for Switch Profiles 8

Configuration Guidelines and Limitations 8

Configuring Switch Profiles 8

Adding a Switch to a Switch Profile 10

Adding or Modifying Switch Profile Commands 12

Importing a Switch Profile 14

Importing Configurations in a vPC Topology 16

Verifying Commands in a Switch Profile 16

Isolating a Peer Switch 17

Deleting a Switch Profile 18

Deleting a Switch From a Switch Profile 18

Verifying the Switch Profile Configuration 19

Configuration Examples for Switch Profiles	20
Creating a Switch Profile on a Local and Peer Switch	20
Verifying the Synchronization Status	22
Showing the Running Configuration	22
Displaying the Switch Profile Synchronization Between the Local and the Peer Switch	23
Displaying the Verify and Commit on the Local and the Peer Switch	23
Displaying the Successful and Unsuccessful Synchronization Between the Local and the Peer Switch	25
Displaying the Switch Profile Buffer	25
Importing Configurations	26
Migrating to Cisco NX-OS Release 5.0(2)N1(1) Using the import Command	28
Replacing a Cisco Nexus 5000 Series Switch	29
Replacing a Cisco Nexus 2000 Series Fabric Extender	30
Installing a New Cisco Nexus 2000 Series Fabric Extender	31
Synchronizing Configurations	31
Configuring Module Pre-Provisioning	33
Information About Module Pre-Provisioning	33
Guidelines and Limitations	34
Enabling Module Pre-Provisioning	34
Removing Module Pre-Provisioning	35
Verifying the Pre-Provisioned Configuration	36
Configuration Examples for Pre-Provisioning	37
Using Cisco Fabric Services	39
Using Cisco Fabric Services	39
Information About CFS	39
CFS Distribution	40
CFS Distribution Modes	40
Uncoordinated Distribution	40
Coordinated Distribution	40
Unrestricted Uncoordinated Distributions	41
Disabling or Enabling CFS Distribution on a Switch	41
Verifying CFS Distribution Status	42
CFS Distribution over IP	42
CFS Distribution over Fibre Channel	43
CFS Distribution Scopes	43

CFS Merge Support	44
CFS Support for Applications	44
CFS Application Requirements	44
Enabling CFS for an Application	45
Verifying Application Registration Status	45
Locking the Network	45
Verifying CFS Lock Status	46
Committing Changes	46
Discarding Changes	47
Saving the Configuration	47
Clearing a Locked Session	47
CFS Regions	47
About CFS Regions	47
Example Scenario	47
Managing CFS Regions	48
Creating CFS Regions	48
Assigning Applications to CFS Regions	48
Moving an Application to a Different CFS Region	49
Removing an Application from a Region	50
Deleting CFS Regions	50
Configuring CFS over IP	50
Enabling CFS over IPv4	50
Enabling CFS over IPv6	51
Verifying the CFS Over IP Configuration	52
Configuring IP Multicast Address for CFS over IP	52
Configuring IPv4 Multicast Address for CFS	52
Configuring IPv6 Multicast Address for CFS	52
Verifying IP Multicast Address Configuration for CFS over IP	53
Displaying CFS Distribution Information	53
Default CFS Settings	55
Configuring User Accounts and RBAC	57
Configuring User Accounts and RBAC	57
Information About User Accounts and RBAC	57
About User Accounts	57
Characteristics of Strong Passwords	58

About User Roles	58
About Rules	59
About User Role Policies	59
Guidelines and Limitations for User Accounts	59
Configuring User Accounts	60
Configuring RBAC	61
Creating User Roles and Rules	61
Creating Feature Groups	62
Changing User Role Interface Policies	63
Changing User Role VLAN Policies	64
Changing User Role VSAN Policies	65
Verifying User Accounts and RBAC Configuration	66
Default User Account and RBAC Settings	66
Configuring Session Manager	67
Configuring Session Manager	67
Information About Session Manager	67
Configuration Guidelines and Limitations	67
Configuring Session Manager	68
Creating a Session	68
Configuring ACLs in a Session	68
Verifying a Session	69
Committing a Session	69
Saving a Session	69
Discarding a Session	69
Session Manager Example Configuration	70
Verifying Session Manager Configuration	70
Configuring Online Diagnostics	71
Information About Online Diagnostics	71
Online Diagnostics Overview	71
Bootup Diagnostics	71
Health Monitoring Diagnostics	72
Expansion Module Diagnostics	73
Configuring Online Diagnostics	74
Verifying Online Diagnostics Configuration	74
Default GOLD Settings	75

Configuring System Message Logging	77
Information About System Message Logging	77
syslog Servers	78
Configuring System Message Logging	78
Configuring System Message Logging to Terminal Sessions	78
Configuring System Message Logging to a File	81
Configuring Module and Facility Messages Logging	82
Configuring Logging Timestamps	84
Configuring syslog Servers	85
Configuring syslog on a UNIX or Linux System	86
Configuring syslog Server Configuration Distribution	87
Displaying and Clearing Log Files	89
Verifying System Message Logging Configuration	89
Default System Message Logging Settings	90
Configuring Smart Call Home	93
Configuring Smart Call Home	93
Information About Call Home	93
Call Home Overview	93
Destination Profiles	94
Call Home Alert Groups	94
Call Home Message Levels	96
Obtaining Smart Call Home	97
Prerequisites for Call Home	97
Configuration Guidelines and Limitations	98
Configuring Call Home	98
Procedures for Configuring Call Home	98
Configuring Contact Information	98
Creating a Destination Profile	100
Modifying a Destination Profile	101
Associating an Alert Group with a Destination Profile	103
Adding show Commands to an Alert Group	103
Configuring E-Mail	104
Configuring Periodic Inventory Notification	105
Disabling Duplicate Message Throttle	106
Enabling or Disabling Call Home	106

Testing Call Home Communications	107
Verifying Call Home Configuration	108
Default Call Home Settings	108
Additional References	109
Call Home Message Formats	109
Sample syslog Alert Notification in Full-Text Format	115
Sample syslog Alert Notification in XML Format	115
Configuring Rollback	121
Information About Rollback	121
Guidelines and Limitations	121
Creating a Checkpoint	122
Implementing a Rollback	123
Verifying the Rollback Configuration	124
Configuring SNMP	125
Information About SNMP	125
SNMP Functional Overview	125
SNMP Notifications	126
SNMPv3	126
Security Models and Levels for SNMPv1, v2, v3	126
User-Based Security Model	127
CLI and SNMP User Synchronization	128
Group-Based SNMP Access	129
Configuration Guidelines and Limitations	129
Configuring SNMP	129
Configuring SNMP Users	129
Enforcing SNMP Message Encryption	130
Assigning SNMPv3 Users to Multiple Roles	130
Creating SNMP Communities	130
Filtering SNMP Requests	131
Configuring SNMP Notification Receivers	131
Configuring the Notification Target User	132
Enabling SNMP Notifications	133
Configuring Link Notifications	135
Disabling Link Notifications on an Interface	136
Enabling One-Time Authentication for SNMP over TCP	136

Assigning SNMP Switch Contact and Location Information	136
Configuring the Context to Network Entity Mapping	137
Verifying SNMP Configuration	138
Default SNMP Settings	138
Configuring RMON	139
Configuring RMON	139
Information About RMON	139
RMON Alarms	139
RMON Events	140
Configuration Guidelines and Limitations	140
Configuring RMON	140
Configuring RMON Alarms	140
Configuring RMON Events	142
Verifying RMON Configuration	142
Default RMON Settings	142
Configuring SPAN	145
Configuring SPAN	145
SPAN Sources	145
Characteristics of Source Ports	145
SPAN Destinations	146
Characteristics of Destination Ports	146
Configuring SPAN	147
Creating and Deleting a SPAN Session	147
Configuring the Destination Port	147
Configuring an Ethernet Destination Port	147
Configuring Fibre Channel Destination Port	148
Configuring Source Ports	149
Configuring Source Port Channels, VLANs, or VSANs	150
Configuring the Description of a SPAN Session	151
Activating a SPAN Session	151
Suspending a SPAN Session	152
Displaying SPAN Information	152



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, page xi](#)
- [Document Organization, page xi](#)
- [Document Conventions, page xii](#)
- [Related Documentation for Nexus 5000 Series NX-OS Software, page xiii](#)
- [Obtaining Documentation and Submitting a Service Request, page xiv](#)

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.
<i>Italic</i>	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.
<code>variable</code>	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
<code>screen font</code>	Terminal sessions and information the switch displays are in screen font.
boldface screen font	Information you must enter is in boldface screen font.
<i>italic screen font</i>	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.html

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, page 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*.

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 a specific Cisco NX-OS Release, 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 5.0(2)N1(1)*, and tells you where they are documented.

Table 1: New and Changed System Management Features for Cisco NX-OS Release 5.0(2)N1(1)

Feature	Description	Changed in Release	Where Documented
Switch Profiles	Added configuration information for the switch profiles feature.	5.0(2)N1(1)	Configuring Switch Profiles
Configuration Rollback	Added information on configuring the rollback feature.	5.0(2)N1(1)	Configuring Rollback
Pre-Provisioning	Added configuration information for configuring offline interfaces and modules using the pre-provision feature.	5.0(2)N1(1)	Configuring Pre-Provisioning

Feature	Description	Changed in Release	Where Documented
SPAN updates for the Cisco Nexus 5548 Switch	Updated information about source ports.	5.0(2)N1(1)	Configuring SPAN

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 2: 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

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 NX-OS 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 NX-OS 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, page 3](#)

System Management Overview

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

Switch Profiles

Configuration synchronization allows administrators to make configuration changes on one switch and have the system automatically synchronize the configuration to a peer switch. This eliminates misconfigurations and reduces the administrative overhead of having to configure both vPC members simultaneously.

The configuration synchronization mode (config-sync) allows users to create switch profiles to synchronize local and peer switch.

Module Pre-Provisioning

Module pre-provisioning feature allows users to pre-configure interfaces before inserting or attaching a module to a Cisco Nexus 5000 Series switch. If a module goes offline, users can also use pre-provisioning to make changes to the interface configurations for the offline module. In some vPC topologies, pre-provisioning is required for the configuration synchronization feature. Pre-provisioning allows users to synchronize the configuration for an interface that is online with one peer but offline with another peer.

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.

Configuration Rollback

The configuration rollback feature allows users to take a snapshot, or user checkpoint, of the Cisco NX-OS configuration and then reapply that configuration to a switch at any point without having to reload the switch. A rollback allows any authorized administrator to apply this checkpoint configuration without requiring expert knowledge of the features configured in the checkpoint.

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.

SPAN

The Switched Port Analyzer (SPAN) feature (sometimes called port mirroring or port monitoring) selects network traffic for analysis by a network analyzer. The network analyzer can be a Cisco SwitchProbe, a Fibre Channel Analyzer, or other Remote Monitoring (RMON) probes.



CHAPTER 3

Configuring Switch Profiles

The chapter includes the following topics:

- [Configuring Switch Profiles, page 5](#)
- [Prerequisites for Switch Profiles, page 8](#)
- [Configuration Guidelines and Limitations, page 8](#)
- [Configuring Switch Profiles, page 8](#)
- [Adding a Switch to a Switch Profile, page 10](#)
- [Adding or Modifying Switch Profile Commands, page 12](#)
- [Importing a Switch Profile, page 14](#)
- [Importing Configurations in a vPC Topology, page 16](#)
- [Verifying Commands in a Switch Profile, page 16](#)
- [Isolating a Peer Switch, page 17](#)
- [Deleting a Switch Profile, page 18](#)
- [Deleting a Switch From a Switch Profile, page 18](#)
- [Verifying the Switch Profile Configuration, page 19](#)
- [Configuration Examples for Switch Profiles, page 20](#)

Configuring Switch Profiles

This section describes how to configure switch profiles in Cisco NX-OS Release 5.0(2)N1(1) on the Cisco Nexus 5000 Series switch.

Information About Switch Profiles

Several applications require consistent configuration across Cisco Nexus 5000 Series switches in the network. For example, with a Virtual Port Channel (vPC), you must have identical configurations. Mismatched configurations can cause errors or misconfigurations that can result in service disruptions. The configuration

synchronization (config-sync) feature in Cisco NX-OS Release 5.0(2)N1(1), allows you to configure one switch profile and have the configuration be automatically synchronized to the peer switch.

A switch profile provides the following benefits:

- Allows configurations to be synchronized between switches.
- Merges configurations when connectivity is established between two switches.
- Provides control of exactly which configuration gets synchronized.
- Ensures configuration consistency across peers through merge and mutual-exclusion checks.
- Provides verify and commit semantics.
- Supports configuring and synchronizing port profile configurations.
- Provides an import command to migrate existing vPC configurations to a switch profile.

Switch Profile Configuration Modes

The Cisco NX-OS Release 5.0(2)N1(1) switch profile feature includes the following configuration modes:

- Configuration Synchronization Mode
- Switch Profile Mode
- Switch Profile Import Mode

Configuration Synchronization Mode

Beginning with Cisco NX-OS Release 5.0(2)N1(1), the configuration synchronization mode (config-sync) allows you to create switch profiles. After entering the **config sync** command, you can create and name the switch profile that displays the switch profile mode. You must enter the **config sync** command on the local and the peer switch that you want to synchronize.

Switch Profile Mode

The switch profile mode allows you to add supported configuration commands to a switch profile that is later synchronized with a peer switch. Commands that you enter in the switch profile mode are buffered until you enter the **commit** command.

Switch Profile Import Mode

When you upgrade from an earlier release to Cisco NX-OS Release 5.0(2)N1(1), you have the option to enter the **import** command to copy supported running-configuration commands to a switch profile. After entering the **import** command, the switch profile mode (config-sync-sp) changes to the switch profile import mode (config-sync-sp-import). The switch profile import mode allows you to import existing switch configurations from the running configuration and specify which commands you want to include in the switch profile.

Because different topologies require different commands that are included in a switch profile, the **import** command mode allows you to modify the imported set of commands to suit a specific topology. For example, a dual homed Fabric Extender (FEX) topology requires that most of the configuration is synchronized. In other vPC topologies, the configuration that needs to be synchronized might be a much smaller set of commands.

You need to enter the **commit** command to complete the import process and move the configuration into the switch profile. Because configuration changes are not supported during the import process, if you added new

commands before entering the **commit** command, the switch profile remains unsaved and the switch remains in the switch profile import mode. You can remove the added commands or abort the import. Unsaved configurations are lost if the process is aborted. You can add new commands can be added to the switch profile after the import is complete.

Configuration Validation

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

- Mutual Exclusion Checks
- Merge Checks

Mutual Exclusion Checks

To reduce the possibility of overriding configuration settings that are included in a switch profile, mutual exclusion (mutex) checks the switch profile commands against the commands that exist on the local switch and the commands on the peer switch. A command that is included in a switch profile cannot be configured outside of the switch profile or on a peer switch. This requirement reduces the possibility that an existing command is unintentionally overwritten.

As a part of the commit process, the mutex-check occurs on both switches if the peer switch is reachable, otherwise the mutex-check is performed locally. Configuration changes made from the configuration terminal occur only on the local switch.

If a mutex-check identifies errors, they are reported as a mutex failure and they must be manually corrected.

The following exceptions apply to the mutual exclusion policy:

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

Merge Checks

Merge checks are done on the peer switch that is receiving a configuration. The merge checks ensure that the received configuration does not conflict with the switch profile configuration that already exists on the receiving switch. The merge check occurs during the merge or commit process. Errors are reported as merge failures and must be manually corrected.

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

Software Upgrades and Downgrades With Switch Profiles

When you downgrade from Cisco NX-OS Release 5.0(2)N1(1) to an earlier release, you are prompted to remove an existing switch profile that is not supported on earlier releases.

When you upgrade from an earlier release to Cisco NX-OS Release 5.0(2)N1(1), you have the option to move some of the running-configuration commands to a switch profile. The import command allows you to import

relevant switch profile commands. An upgrade can occur if there are buffered configurations (uncommitted); however, the uncommitted configurations are lost.

When you perform an In Service Software Upgrade (ISSU) on one of the switches included in a switch profile, a configuration synchronization cannot occur because the peer is unreachable.

Prerequisites for Switch Profiles

Switch profiles have the following prerequisites:

- You must enable CFSoIP distribution over mgmt0 on both switches by entering the **cfs ipv4 distribute** command.
- You must configure a switch profile with the same name on both peer-switches by entering the **config sync** and **switch-profile** commands.
- Configure each switch as peer switch by entering the **sync-peers destination** command

Configuration Guidelines and Limitations

Switch profiles have the following configuration guidelines and limitations:

- You can only enable configuration synchronization using the mgmt0 interface.
- You must configure synchronized peers with the same switch profile name.
- Commands that are qualified for a switch profile configuration are allowed to be configured in the configuration switch profile (config-sync-sp) mode.
- Supported switch profile commands relate to vPC commands. FCoE commands are not supported.
- One switch profile session can be in progress at a time. Attempts to start another session will fail.
- Supported command changes made from the configuration terminal mode are blocked when a switch profile session is in progress. You should not make unsupported command changes from the configuration terminal mode when a switch profile session is in progress..
- When you enter the **commit** command and a peer switch is reachable, the configuration is applied to both peer switches or neither switch. If there is a commit failure, the commands remain in the switch profile buffer. You can then make necessary corrections and try the commit again.
- Cisco recommends that you enable pre-provisioning for all Gigabit-Ethernet Modules (GEMs) and Cisco Nexus Fabric Extender modules whose interface configurations are synchronized using the configuration synchronization feature. Follow these guidelines in Cisco Nexus Fabric Extender A/A topologies where the Fabric Extenders might not be online on one switch and its configuration is changed and synchronized on the other switch. In this scenario, if you do not enable pre-provisioning, a commit fails and the configuration is rolled back on both switches.

Configuring Switch Profiles

You can create and configure a switch profile. Enter the switch-profile *name* command in the configuration synchronization mode (config-sync).

Before You Begin

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

SUMMARY STEPS

1. configuration terminal
2. cfs ipv4 distribute
3. config sync
4. switch-profile *name*
5. sync-peers destination *IP-address*
6. show switch-profile *name* status
7. exit
8. copy running-config startup-config

DETAILED STEPS

	Command or Action	Purpose
Step 1	configuration terminal Example: switch# configuration terminal switch(config)#	Enters the configuration terminal mode.
Step 2	cfs ipv4 distribute Example: switch(config)# cfs ipv4 distribute switch(config)#	Enables CFS distribution between the peer switches.
Step 3	config sync Example: switch# config sync switch(config-sync)#	Enters the configuration synchronization mode.
Step 4	switch-profile <i>name</i> Example: switch(config-sync)# switch-profile abc switch(config-sync-sp)#	Configures the switch profile, names the switch profile, and enters the switch profile synchronization configuration mode.
Step 5	sync-peers destination <i>IP-address</i> Example: switch(config-sync-sp)# sync-peers destination 10.1.1.1 switch(config-sync-sp)#	Configures the peer switch.

	Command or Action	Purpose
Step 6	show switch-profile <i>name</i> status Example: <pre>switch(config-sync-sp)# show switch-profile abc status switch(config-sync-sp)#</pre>	(Optional) Views the switch profile on the local switch and the peer switch information.
Step 7	exit Example: <pre>switch(config-sync-sp)# exit switch#</pre>	Exits the switch profile configuration mode and returns to EXEC mode.
Step 8	copy running-config startup-config Example: <pre>switch# copy running-config startup-config switch#</pre>	(Optional) Copies the running configuration to the startup configuration.

The following example shows how to configure a switch profile and shows the switch profile status.

```
switch# configuration terminal
switch(config)# cfs ipv4 distribute
switch(config-sync)# switch-profile abc
switch(config-sync-sp)# sync-peers destination 10.1.1.1
switch(config-sync-sp)# show switch-profile abc status
Start-time: 15801 usecs after Mon Aug 23 06:21:08 2010
End-time: 6480 usecs after Mon Aug 23 06:21:13 2010

Profile-Revision: 1
Session-type: Initial-Exchange
Peer-triggered: Yes
Profile-status: Sync Success

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

Peer information:
-----
IP-address: 10.1.1.1
Sync-status: In Sync.
Status: Commit Success
Error(s):
switch(config-sync-sp)# exit
switch#
```

Adding a Switch to a Switch Profile

Enter the **sync-peers destination** *destination IP* command in the switch profile configuration mode to add the switch to a switch profile.

Follow these guidelines when adding switches:

- Switches are identified by their IP address.
- Destination IPs are the IP addresses of the switches that you want to synchronize.

- The committed switch profile is synchronized with the newly added peers (when they are online) providing that the peer switch is also configured with configuration synchronization.

Before You Begin

After creating a switch profile on the local switch, you must add the second switch that will be included in the synchronization.

SUMMARY STEPS

1. **config sync**
2. **switch-profile** *name*
3. **sync-peers destination** *destination IP*
4. **exit**
5. (Optional) **show switch-profile peer**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	config sync Example: <pre>switch# config sync switch(config-sync)#</pre>	Enters configuration synchronization mode.
Step 2	switch-profile <i>name</i> Example: <pre>switch(config-sync)# switch-profile abc switch(config-sync-sp)#</pre>	Configures the switch profile, names the switch profile, and enters the switch profile synchronization configuration mode.
Step 3	sync-peers destination <i>destination IP</i> Example: <pre>switch(config-sync-sp)# sync-peers destination 10.1.1.1 switch(config-sync-sp)#</pre>	Adds a switch to the switch profile.
Step 4	exit Example: <pre>switch(config-sync-sp)# exit switch#</pre>	Exits switch profile configuration mode.
Step 5	show switch-profile peer Example: <pre>switch# show switch-profile peer</pre>	(Optional) Displays the switch profile peer configuration.

	Command or Action	Purpose
Step 6	copy running-config startup-config Example: switch# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Adding or Modifying Switch Profile Commands

To modify a command in a switch profile, add the modified command to the switch profile and enter the commit command to apply the command and synchronize the switch profile to the peer switch if it is reachable.

Follow these guidelines when adding or modifying switch profile commands:

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

Before You Begin

After configuring a switch profile on the local and the peer switch, you must add and commit the supported commands to the switch profile. The commands are added to the switch profile buffer until you enter the **commit** command. The **commit** command does the following:

- Triggers the mutex check and the merge check to verify the synchronization.
- Creates a checkpoint with a rollback infrastructure.
- Applies the configuration on the local switch and the peer switch.
- Executes a rollback on all switches if there is a failure with an application on any of the switches in the switch profile.
- Deletes the checkpoint.

SUMMARY STEPS

1. **config sync**
2. **switch-profile name**
3. **command arugument**
4. (Optional) **show switch-profile name buffer**
5. **verify**
6. **commit**
7. (Optional) **show switch-profile name status**
8. **exit**
9. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	config sync Example: switch# config sync switch(config-sync)#	Enters configuration synchronization mode.
Step 2	switch-profile name Example: switch(config-sync)# switch-profile abc switch(config-sync-sp)#	Configures the switch profile, names the switch profile, and enters switch profile synchronization configuration mode.
Step 3	command arugument Example: switch(config-sync-sp)# interface Port-channel100 switch(config-sync-sp-if)# speed 1000 switch(config-sync-sp-if)# interface Ethernet1/1 switch(config-sync-sp-if)# speed 1000 switch(config-sync-sp-if)# channel-group 100	Adds a command to the switch profile.
Step 4	show switch-profile name buffer Example: switch(config-sync-sp)# show switch-profile abc buffer switch(config-sync-sp)#	(Optional) Displays the configuration commands in the switch profile buffer.
Step 5	verify Example: switch(config-sync-sp)# verify	Verifies the commands in the switch profile buffer.
Step 6	commit Example: switch(config-sync-sp)# commit	Saves the commands in the switch profile and synchronizes the configuration with the peer switch.
Step 7	show switch-profile name status Example: switch(config-sync-sp)# show switch-profile abc status switch(config-sync-sp)#	(Optional) Displays the status of the switch profile on the local switch and the status on the peer switch.
Step 8	exit Example: switch(config-sync-sp)# exit switch#	Exits the switch profile configuration mode.

	Command or Action	Purpose
Step 9	copy running-config startup-config Example: switch# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

The following example shows how to create a switch profile, configure a peer switch, and add commands to the switch profile.

```
switch# configuration terminal
switch(config)# cfs ipv4 distribute
switch(config-sync)# switch-profile abc
switch(config-sync-sp)# sync-peers destination 10.1.1.1
switch(config-sync-sp)# interface port-channel100
switch(config-sync-sp-if)# speed 1000
switch(config-sync-sp-if)# interface Ethernet1/1
switch(config-sync-sp-if)# speed 1000
switch(config-sync-sp-if)# channel-group 100
switch(config-sync-sp)# verify
switch(config-sync-sp)# commit
switch(config-sync-sp)# exit
switch#
```

The following example shows an existing configuration with a defined switch profile. The second example shows how the switch profile command changed by adding the modified command to the switch profile.

```
switch# show running-config
switch-profile abc
  interface Ethernet1/1
    switchport mode trunk
    switchport trunk allowed vlan 1-10

Switch# config sync
Switch(config-sync)# switch-profile abc
Switch(config-sync-sp)# interface Ethernet1/1
Switch(config-sync-sp-if)# switchport trunk allowed vlan 5-10
Switch(config-sync-sp-if)# commit

Switch# show running-config
switch-profile abc
  interface Ethernet1/1
    switchport mode trunk
    switchport trunk allowed vlan 5-10
```

Importing a Switch Profile

You can import a switch profile based on the set of commands that you want to import. The following three ways can be used to import commands that were added using the configuration terminal mode:

Follow these guidelines when adding switches:

- Add selected commands to the switch profile.
- Add supported commands that were specified for an interface.
- Add supported system-level commands.

When you import commands to a switch profile, the switch profile buffer must be empty.

If new commands are added during the import, the switch profile remains unsaved and the switch remains in the switch profile import mode. You can enter the **abort** command to stop the import. For additional information importing a switch profile, see the “Switch Profile Import Mode” section.

SUMMARY STEPS

1. **config sync**
2. **switch-profile** *name*
3. **import** {*interfaceport/slot* | *running-config*}
4. **commit**
5. (Optional) **abort**
6. **exit**
7. (Optional) **show switch-profile**
8. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	config sync Example: <pre>switch# config sync switch(config-sync)#</pre>	Enters the configuration synchronization mode.
Step 2	switch-profile <i>name</i> Example: <pre>switch(config-sync)# switch-profile abc switch(config-sync-sp)#</pre>	Configures the switch profile, names the switch profile, and enters the switch profile synchronization configuration mode.
Step 3	import { <i>interfaceport/slot</i> <i>running-config</i> } Example: <pre>switch(config-sync-sp)# import ethernet 1/2 switch(config-sync-sp-import)#</pre>	Identifies the commands that you want to import and enters switch profile import mode. <ul style="list-style-type: none"> • <CR>—Adds selected commands. • interface—Adds the supported commands for a specified interface. • running-config—Adds supported system-level commands.
Step 4	commit Example: <pre>switch(config-sync-sp-import)# commit</pre>	Imports the commands and saves the commands to the switch profile.
Step 5	abort Example: <pre>switch(config-sync-sp-import)# abort</pre>	(Optional) Aborts the import process.
Step 6	exit Example: <pre>switch(config-sync-sp)# exit switch#</pre>	Exits the switch profile import mode.

	Command or Action	Purpose
Step 7	show switch-profile Example: switch# show switch-profile	(Optional) Displays the switch profile configuration.
Step 8	copy running-config startup-config Example: switch# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Importing Configurations in a vPC Topology

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



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

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



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

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

Verifying Commands in a Switch Profile

You can verify the commands that are included in a switch profile, enter the verify command in switch profile mode.

SUMMARY STEPS

1. **config sync**
2. **switch-profile *name***
3. **verify**
4. **exit**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	config sync Example: <pre>switch# config sync switch(config-sync)#</pre>	Enters configuration synchronization mode.
Step 2	switch-profile <i>name</i> Example: <pre>switch(config-sync)# switch-profile abc switch(config-sync-sp)#</pre>	Configures the switch profile, names the switch profile, and enters switch profile synchronization configuration mode.
Step 3	verify Example: <pre>switch(config-sync-sp)# verify</pre>	Verifies the commands in the switch profile buffer.
Step 4	exit Example: <pre>switch(config-sync-sp)# exit switch#</pre>	Exits the switch profile configuration mode.
Step 5	copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	(Optional) Copies the running configuration to the startup configuration.

Isolating a Peer Switch

You can isolate a peer switch in order to make changes to a switch profile. This process can be used when you want to block a configuration synchronization or when you want to debug configurations.

Isolating a peer switch requires that you remove the switch from the switch profile and then add the peer switch back to the switch profile.

**Note**

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

To temporarily isolate a peer switch, follow these steps:

- 1 Remove a peer switch from a switch profile.
- 2 Make changes to the switch profile and commit the changes.
- 3 Enter debug commands.
- 4 Undo the changes that were made to the switch profile in Step 2 and commit.
- 5 Add the peer switch back to the switch profile.

Deleting a Switch Profile

You can delete a switch profile by selecting the all-config or the local-config option:

- **all-config**—Deletes the switch profile on both peer switches (when both are reachable). If you choose this option and one of the peers is unreachable, only the local switch profile is deleted. the all-config option completely deletes the switch profile on both peer switches.
- **local-config**—Deletes the switch profile on the local switch only.

SUMMARY STEPS

1. **config sync**
2. **no switch-profile name** {*all-config* | *local-config*}
3. **exit**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	config sync Example: switch# config sync switch(config-sync)#	Enters the configuration synchronization mode.
Step 2	no switch-profile name { <i>all-config</i> <i>local-config</i> } Example: switch(config-sync)# no switch-profile abc local-config switch(config-sync-sp)#	Deletes the switch profile as follows: <ul style="list-style-type: none"> • all-config—Deletes the switch profile on the local and peer switch. If the peer switch is not reachable, only the local switch profile is deleted. • local-config—Deletes the switch profile and local configuration.
Step 3	exit Example: switch(config-sync-sp)# exit switch#	Exits configuration synchronization mode.
Step 4	copy running-config startup-config Example: switch# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Deleting a Switch From a Switch Profile

You can delete a switch from a switch profile.

SUMMARY STEPS

1. **config sync**
2. **switch-profile** *name*
3. **no sync-peers destination** *destination IP*
4. **exit**
5. (Optional) **show switch-profile**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	config sync Example: <pre>switch# config sync switch(config-sync)#</pre>	Enters configuration synchronization mode.
Step 2	switch-profile <i>name</i> Example: <pre>switch(config-sync)# switch-profile abc switch(config-sync-sp)#</pre>	Configures the switch profile, names the switch profile, and enters the switch profile synchronization configuration mode.
Step 3	no sync-peers destination <i>destination IP</i> Example: <pre>switch(config-sync-sp)# no sync-peers destination 10.1.1.1 switch(config-sync-sp)#</pre>	Removes the specified switch from the switch profile.
Step 4	exit Example: <pre>switch(config-sync-sp)# exit switch#</pre>	Exits the switch profile configuration mode.
Step 5	show switch-profile Example: <pre>switch# show switch-profile</pre>	(Optional) Displays the switch profile configuration.
Step 6	copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	(Optional) Copies the running configuration to the startup configuration.

Verifying the Switch Profile Configuration

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

Command	Purpose
show switch-profile <i>name</i>	Displays the commands in a switch profile.
show switch-profile <i>name</i> buffer	Displays the uncommitted commands in a switch profile, the commands that were moved, and the commands that were deleted.
show switch-profile <i>name</i> peer <i>IP-address</i>	Displays the synchronization status for a peer switch.
show switch-profile <i>name</i> session-history	Displays the status of the last 20 switch profile sessions.
show switch-profile <i>name</i> status	Displays the configuration synchronization status of a peer switch.
show running-config expand-port-profile	Displays details about the port profile.
show running-config exclude-provision	Displays the configurations for offline pre-provisioned interfaces that are hidden.
show running-config switch-profile	Displays the running configuration for the switch profile on the local switch.
show startup-config switch-profile	Displays the startup configuration for the switch profile on the local switch.

For detailed information about the fields in the output from these commands, see the *Cisco Nexus 5000 Series Command Reference*.

Configuration Examples for Switch Profiles

This section includes the following examples:

Creating a Switch Profile on a Local and Peer Switch

The following example shows how to create a successful switch profile configuration on a local and peer switch including configuring QoS policies; a vPC peer-link, and a vPC in a switch profile. The example includes the following tasks in the order that they must be completed:

- 1 Enable CFSolP distribution.
- 2 Create a switch profile and configure the peer switch.
- 3 Verify the switch profile status on both peer switches.
- 4 Add the configuration commands that will be applied to the local and the peer switch.
- 5 View the buffered commands.
- 6 Verify the commands.
- 7 Commit the commands to the switch profile.

Enable CFSolP distribution on the local and the peer switch.

```
switch# configuration terminal
switch(config)# cfs ipv4 distribute
```

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

```
switch(config-sync)# switch-profile abc
switch(config-sync-sp)# sync-peers destination 10.1.1.1
```

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

```
switch(config-sync-sp)# show switch-profile abc status
```

```
Start-time: 15801 usecs after Mon Aug 23 06:21:08 2010
End-time: 6480 usecs after Mon Aug 23 06:21:13 2010
```

```
Profile-Revision: 1
Session-type: Initial-Exchange
Peer-triggered: Yes
Profile-status: Sync Success
```

Local information:

```
-----
Status: Commit Success
Error(s):
```

Peer information:

```
-----
IP-address: 10.1.1.1
Sync-status: In Sync.
Status: Commit Success
Error(s):
```

Add the configuration commands to the switch profile on the local switch. The commands will be applied to the peer switch when the commands are committed.

```
switch(config-sync-sp)# class-map type qos c1
switch(config-sync-sp-cmap-qos)# match cos 2
switch(config-sync-sp-cmap-qos)# class-map type qos c2
switch(config-sync-sp-cmap-qos)# match cos 5
switch(config-sync-sp-cmap-qos)# policy-map type qos p1
switch(config-sync-sp-pmap-qos)# class c1
switch(config-sync-sp-pmap-c-qos)# set qos-group 2
switch(config-sync-sp-pmap-c-qos)# class c2
switch(config-sync-sp-pmap-c-qos)# set qos-group 3
switch(config-sync-sp-pmap-c-qos)# system qos
switch(config-sync-sp-sys-qos)# service-policy type qos input p1
switch(config-sync-sp-sys-qos)# vlan 1-50
switch(config-sync-sp-vlan)# interface port-channel 100
switch(config-sync-sp-if)# vpc peer-link
switch(config-sync-sp-if)# switchport mode trunk
switch(config-sync-sp-if)# interface port-channel 10
switch(config-sync-sp-if)# vpc 1
switch(config-sync-sp-if)# switchport mode trunk
switch(config-sync-sp-if)# switchport trunk allowed vlan 1, 10-50
```

View the buffered commands.

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

```
-----
Seq-no  Command
-----
1       class-map type qos match-all c1
1.1     match cos 2
2       class-map type qos match-all c2
2.1     match cos 5
3       policy-map type qos p1
3.1     class c1
3.1.1   set qos-group 2
3.2     class c2
3.2.1   set qos-group 3
4       system qos
4.1     service-policy type qos input p1
5       vlan 2-50
6       interface port-channel100
6.1     vpc peer-link
6.2     switchport mode trunk
7       interface port-channel10
7.1     vpc 1
```

```

7.2      switchport mode trunk
7.3      switchport trunk allowed vlan 1, 10-50

```

Verify the commands in the switch profile.

```

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

```

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

```

switch(config-sync-sp)# commit
Commit Successful
switch(config-sync)#

```

Verifying the Synchronization Status

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

```

switch(config-sync)# show switch-profile switch-profile status

Start-time: 804935 usecs after Mon Aug 23 06:41:10 2010
End-time: 956631 usecs after Mon Aug 23 06:41:20 2010

Profile-Revision: 2
Session-type: Commit
Peer-triggered: No
Profile-status: Sync Success

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

Peer information:
-----
IP-address: 10.1.1.1
Sync-status: In Sync.
Status: Commit Success
Error(s):

switch(config-sync)#

```

Showing the Running Configuration

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

```

switch(config-sync)# show running-config switch-profile
switch-profile sp
  sync-peers destination 10.1.1.1
  class-map type qos match-all c1
    match cos 2
  class-map type qos match-all c2
    match cos 5
  policy-map type qos p1
    class c1
      set qos-group 2
    class c2
      set qos-group 3
  system qos
    service-policy type qos input p1
  vlan 2-50

interface port-channel10
  switchport mode trunk
  vpc 1
  switchport trunk allowed vlan 1,10-50

interface port-channel100
  switchport mode trunk

```

```
vpc peer-link
switch(config-sync)#
```

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

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

```
switch1# show switch-profile sp status

Start-time: 491815 usecs after Thu Aug 12 11:54:51 2010
End-time: 449475 usecs after Thu Aug 12 11:54:58 2010

Profile-Revision: 1
Session-type: Initial-Exchange
Peer-triggered: No
Profile-status: Sync Success

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

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

switch1#

switch2# show switch-profile sp status

Start-time: 503194 usecs after Thu Aug 12 11:54:51 2010
End-time: 532989 usecs after Thu Aug 12 11:54:58 2010

Profile-Revision: 1
Session-type: Initial-Exchange
Peer-triggered: Yes
Profile-status: Sync Success

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

Peer information:
-----
IP-address: 10.193.194.51
Sync-status: In Sync.
Status: Commit Success
Error(s):

switch2#
```

Displaying the Verify and Commit on the Local and the Peer Switch

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

```
switch1# configure sync
Enter configuration commands, one per line.  End with CNTL/Z.
sw01(config-sync)# switch-profile sp
Switch-Profile started, Profile ID is 1
sw01(config-sync-sp)# interface Ethernet1/1
sw01(config-sync-sp-if)# description foo
```

```

sw01(config-sync-sp-if)# verify
Verification Successful
sw01(config-sync-sp)# commit
Commit Successful
sw01(config-sync)# show running-config switch-profile
switch-profile sp
  sync-peers destination 10.193.194.52
  interface Ethernet1/1
    description foo
sw01(config-sync)# show switch-profile sp status

Start-time: 171513 usecs after Wed Aug 11 17:51:28 2010
End-time: 676451 usecs after Wed Aug 11 17:51:43 2010

Profile-Revision: 3
Session-type: Commit
Peer-triggered: No
Profile-status: Sync Success

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

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

switch1(config-sync)#

switch2# show running-config switch-profile
switch-profile sp
  sync-peers destination 10.193.194.51
  interface Ethernet1/1
    description foo
switch2# show switch-profile sp status

Start-time: 265716 usecs after Wed Aug 11 16:51:28 2010
End-time: 734702 usecs after Wed Aug 11 16:51:43 2010

Profile-Revision: 3
Session-type: Commit
Peer-triggered: Yes
Profile-status: Sync Success

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

Peer information:
-----
IP-address: 10.193.194.51
Sync-status: In Sync.
Status: Commit Success
Error(s):

switch2#

```

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

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

```
switch1# show switch-profile abc peer
```

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

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

Displaying the Switch Profile Buffer

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

```
switch1# configure sync
Enter configuration commands, one per line.  End with CNTL/Z.
switch1(config-sync)# switch-profile sp
Switch-Profile started, Profile ID is 1
switch1(config-sync-sp)# vlan 101
switch1(config-sync-sp-vlan)# ip igmp snooping querier 10.101.1.1
switch1(config-sync-sp-vlan)# exit
switch1(config-sync-sp)# mac address-table static 0000.0000.0001 vlan 101 drop
switch1(config-sync-sp)# interface Ethernet1/2
switch1(config-sync-sp-if)# switchport mode trunk
switch1(config-sync-sp-if)# switchport trunk allowed vlan 101
switch1(config-sync-sp-if)# exit
switch1(config-sync-sp)# show switch-profile sp buffer
-----
Seq-no  Command
-----
1       vlan 101
1.1     ip igmp snooping querier 10.101.1.1
2       mac address-table static 0000.0000.0001 vlan 101 drop
3       interface Ethernet1/2
3.1     switchport mode trunk
3.2     switchport trunk allowed vlan 101

switch1(config-sync-sp)# buffer-move 3 1
switch1(config-sync-sp)# show switch-profile sp buffer
-----
Seq-no  Command
-----
1       interface Ethernet1/2
1.1     switchport mode trunk
1.2     switchport trunk allowed vlan 101
2       vlan 101
2.1     ip igmp snooping querier 10.101.1.1
3       mac address-table static 0000.0000.0001 vlan 101 drop

switch1(config-sync-sp)# buffer-delete 1
switch1(config-sync-sp)# show switch-profile sp buffer
-----
```

```

Seq-no  Command
-----
2       vlan 101
2.1     ip igmp snooping querier 10.101.1.1
3       mac address-table static 0000.0000.0001 vlan 101 drop

switch1(config-sync-sp)# buffer-delete all
switch1(config-sync-sp)# show switch-profile sp buffer
switch1(config-sync-sp)#

```

Importing Configurations

The following example shows how to import an interface configuration:

```

switch# show running-config interface Ethernet1/3

!Command: show running-config interface Ethernet1/3
!Time: Wed Aug 11 18:12:44 2010

version 5.0(2)N1(1)

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

switch# configure sync
Enter configuration commands, one per line.  End with CNTL/Z.
sw01(config-sync)# switch-profile sp
Switch-Profile started, Profile ID is 1

switch(config-sync-sp)# import interface Ethernet1/3
switch(config-sync-sp-import)# show switch-profile sp buffer
-----
Seq-no  Command
-----
1       interface Ethernet1/3
1.1     switchport mode trunk
1.2     switchport trunk allowed vlan 1-100

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

```

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

```

switch(config-sync)# switch-profile sp
Switch-Profile started, Profile ID is 1
switch(config-sync-sp)# import running-config
switch(config-sync-sp-import)# show switch-profile sp buffer
-----
Seq-no  Command
-----
1       logging event link-status default
2       vlan 1
3       port-profile type ethernet pp1
3.1     bandwidth 5000
3.2     bandwidth inherit
3.3     speed 10000
3.4     state enabled
4       interface port-channel3
4.1     switchport mode trunk
4.2     vpc peer-link
4.3     spanning-tree port type network
5       interface port-channel30
5.1     switchport mode trunk
5.2     vpc 30
5.3     switchport trunk allowed vlan 2-10
6       interface port-channel31
6.1     switchport mode trunk
6.2     vpc 31

```



```

6.3      switchport trunk allowed vlan 11-20
7        interface port-channel101
7.1      switchport mode fex-fabric
7.2      fex associate 101
8        interface port-channel102
8.1      switchport mode fex-fabric
8.2      vpc 102
8.3      fex associate 102
9        interface port-channel103
9.1      switchport mode fex-fabric
9.2      vpc 103
9.3      fex associate 103
10       interface Ethernet1/1
11       interface Ethernet1/2
12       interface Ethernet1/3
13       interface Ethernet1/4
13.1     switchport mode trunk
13.2     channel-group 3
14       interface Ethernet1/5
14.1     switchport mode trunk
14.2     channel-group 3
15       interface Ethernet1/6
15.1     switchport mode trunk
15.2     channel-group 3
16       interface Ethernet1/7
16.1     switchport mode trunk
16.2     channel-group 3
17       interface Ethernet1/8
18       interface Ethernet1/9
18.1     switchport mode trunk
18.2     switchport trunk allowed vlan 11-20
18.3     channel-group 31 mode active
19       interface Ethernet1/10
19.1     switchport mode trunk
19.2     switchport trunk allowed vlan 11-20
19.3     channel-group 31 mode active
20       interface Ethernet1/11
21       interface Ethernet1/12
...
45       interface Ethernet2/4
45.1     fex associate 101
45.2     switchport mode fex-fabric
45.3     channel-group 101
46       interface Ethernet2/5
46.1     fex associate 101
46.2     switchport mode fex-fabric
46.3     channel-group 101
47       interface Ethernet2/6
47.1     fex associate 101
47.2     switchport mode fex-fabric
47.3     channel-group 101
48       interface Ethernet2/7
48.1     fex associate 101
48.2     switchport mode fex-fabric
48.3     channel-group 101
49       interface Ethernet2/8
49.1     fex associate 101
...
89       interface Ethernet100/1/32
90       interface Ethernet100/1/33
91       interface Ethernet100/1/34
92       interface Ethernet100/1/35
93       interface Ethernet100/1/36
...
105      interface Ethernet100/1/48
switch(config-sync-sp-import)#

```

The following example shows how to import selected supported commands. First, show the port profile running configuration to identify the configuration that you are going to import.

```

switch# show running-config port-profile

!Command: show running-config port-profile

```

```

!Time: Thu Aug 12 12:09:11 2010

version 5.0(2)N1(1)
port-profile type ethernet ppl
    bandwidth 5000
    bandwidth inherit
    speed 10000
    state enabled

switch#

switch# configure sync
Enter configuration commands, one per line.  End with CNTL/Z.
sw01(config-sync)# switch-profile sp
Switch-Profile started, Profile ID is 1
switch(config-sync-sp)# import
switch(config-sync-sp-import)# port-profile type ethernet ppl
switch(config-sync-sp-import-if)#    bandwidth 5000
switch(config-sync-sp-import-if)#    bandwidth inherit
switch(config-sync-sp-import-if)#    speed 10000
switch(config-sync-sp-import-if)#    state enabled
switch(config-sync-sp-import-if)# show switch-profile sp buffer
-----
Seq-no  Command
-----
1       port-profile type ethernet ppl
1.1     bandwidth 5000
1.2     bandwidth inherit
1.3     speed 10000
1.4     state enabled

switch(config-sync-sp-import-if)# verify
Verification Successful
switch(config-sync-sp-import)# commit
Commit Successful
sw01(config-sync)# show running-config switch-profile
switch-profile sp
  sync-peers destination 10.193.194.52
  port-profile type ethernet ppl
    bandwidth 5000
    bandwidth inherit
    speed 10000
    state enabled
switch(config-sync)#

```

Migrating to Cisco NX-OS Release 5.0(2)N1(1) Using the import Command

The following tasks show how to migrate to Cisco NX-OS Release 5.0(2)N1(1) in an Active/Active and Straight-Through topology.

Migrating to Cisco NX-OS Release 5.0(2)N1(1) in a Fabric Extender A-A Topology

This examples shows the tasks used to migrate to Cisco NX-OS Release 5.0(2)N1(1) in a Fabric Extender A-A topology. For details on the tasks, see the appropriate sections in this chapter.

- 1 Ensure configurations are the same on both switches.
- 2 Configure the switch-profile with same name on both switches.
- 3 Enter the **import running-config** command on both switches.
- 4 Enter the **show switch-profile <name> buffer** command to ensure all configurations are correctly imported on both switches.
- 5 Remove unwanted configuration settings by editing the buffer. See "Displaying the Switch Profile Buffer".
- 6 Enter the **commit** command on both switches.

- 7 Enter the **sync-peers destination** *IP-address* command to configure the peer switch on both switches.
- 8 Enter the **show switch-profile** *<name>* **status** command to ensure both switches are synchronized.

Migrating to Cisco NX-OS Release 5.0(2)N1(1) in a Fabric Extender Fabric Extender Straight-Through Topology

This examples shows the tasks used to migrate to Cisco NX-OS Release 5.0(2)N1(1) in a Fabric Extender Straight-Through topology. For details on the tasks, see the appropriate sections in this chapter.

- 1 Ensure the vPC port-channel configurations are the same on both switches.
- 2 Configure the switch-profile with the same name on both switches.
- 3 Enter the **import interface port-channel** *x-y*, **port-channel** *z* command for all vPC port-channels on both switches.
- 4 Enter the **show switch-profile** *<name>* **buffer** command to ensure all configurations are correctly imported on both switches.
- 5 Remove unwanted configuration settings by editing the buffer. See "Displaying the Switch Profile Buffer".
- 6 Enter the **commit** command on both switches
- 7 Enter the **sync-peers destination** *IP-address* command to configure the peer switch on both switches.
- 8 Enter the **show switch-profile** *<name>* **status** command to ensure both switches are synchronized.

Replacing a Cisco Nexus 5000 Series Switch

When a Cisco Nexus 5000 Series switch has been replaced, perform the following configuration steps on the replacement switch to synchronize it with the existing Cisco Nexus 5000 Series switch. The procedure can be done in a hybrid Fabric Extender A/A topology and Fabric Extender Straight-Through topology.

- 1 Do not connect any peer-link, vPC, A/A or Straight-Through topology fabric ports to the replacement switch.
- 2 Boot the replacement switch. The switch comes up with no configuration.
- 3 Enable pre-provisioning on all Fabric Extender A/A and ST modules.
- 4 Configure the replacement switch:

If the running-configuration was saved offline, follow steps 5-9 to apply the configuration.

If the running-configuration was not saved offline, you can obtain it from the peer switch if the configuration synchronization feature is enabled. (See Steps 1 and 2 from "Creating a Switch Profile on a Local and Peer Switch" then begin with step 10 below).

If neither condition is met, manually add the configuration and then begin with step 10 below.
- 5 Edit the configuration file to remove the **sync-peer** command if using the configuration synchronization feature.
- 6 Configure the mgmt port IP address and download the configuration file.
- 7 Copy the saved configuration file to the running configuration.
- 8 Verify the configuration is correct by entering the **show running-config** command and the **show provision failed-config slot** command.

- 9 If switch-profile configuration changes were made on the peer switch while the replacement switch was out-of-service, apply those configurations in the switch-profile and then enter the commit command.
- 10 Shutdown all Fabric Extender ST topology ports that are included in a vPC topology.
- 11 Connect the Fabric Extender ST topology fabric ports.
- 12 Wait for Fabric Extender ST topology switches to come online.
- 13 Ensure the vPC role priority of the existing switch is better than the replacement switch.
- 14 Connect the peer-link ports to the peer switch.
- 15 Connect the Fabric Extender A/A topology fabric ports.
- 16 Connect the switch vPC ports.
- 17 Enter the **no shutdown** command on all Fabric Extender ST vPC ports.
- 18 Verify that all vPC switches and the Fabric Extenders on the replacement switch come online and that there is no disruption in traffic.
- 19 If you are using the configuration synchronization feature, add the sync-peer configuration to the switch-profile if this wasn't enabled in Step 4.
- 20 If you are using the configuration synchronization feature, enter the **show switch-profile name status** command to ensure both switches are synchronized.

Replacing a Cisco Nexus 2000 Series Fabric Extender

When a Cisco Nexus 2000 Series Fabric Extender needs to be replaced, use the following procedure for the least disruption.

Replacing a Fabric Extender in an Active/Active Topology

Because the hosts behind a Fabric Extender in an A/A Topology are by definition singly connected, there will be traffic disruption for those hosts.

If the replacement Fabric Extender is a different model, pre-provisioning for the new type will not be allowed until the old Fabric Extender is disconnected. Perform the following tasks to retain the configuration on both Nexus 5000 Series switches.

- 1 Save configuration for Fabric Extender interfaces to a file.
- 2 Replace the Fabric Extender.
- 3 Connect all Fabric Extender fabric and host ports.
- 4 Copy the file to the running configuration after the Fabric Extender comes online.
- 5 If the configuration needs to be applied before the Fabric Extender comes online, that slot needs to be pre-provisioned.

Replacing a Fabric Extender in a Straight-Through Topology

If the replacement Fabric Extender is the same model as the original Fabric Extender, then there is no disruption; the configuration on the Fabric Extender interfaces remain unchanged.

If the replacement Fabric Extender is a different model, then pre-provisioning for the new Fabric Extender will not be allowed until the old Fabric Extender is disconnected. Follow these steps to retain the configuration.

- 1 Save the Fabric Extender interface configurations to a file.
- 2 Disconnect the Fabric Extender fabric ports and wait until the Fabric Extender is offline.
- 3 Pre-provision the slot with the new Fabric Extender model.
- 4 Modify the configuration file if necessary for the new Fabric Extender if the configurations are incompatible

**Note**

For vPC ports, this might affect consistency.

- 5 Copy the file to the running configuration.
- 6 Connect the Fabric Extender fabric and host ports and then wait for the Fabric Extender to come online.
- 7 Verify that all ports and vPC switches are up with the correct configuration.

Installing a New Cisco Nexus 2000 Series Fabric Extender

With pre-provisioning, the new Fabric Extender can be fully configured before the Fabric Extender is connected to a Cisco Nexus 5000 Series switch.

- 1 Pre-provision the slot with the Fabric Extender model.
- 2 Configure the interfaces as though the Fabric Extender is connected.
- 3 Connect the Fabric Extender and wait for it to come online.
- 4 Verify that all configurations are applied correctly

**Note**

All configurations are applied serially in a best-effort fashion when the Fabric Extender comes online.

Synchronizing Configurations

Synchronizing Configurations After a Cisco Nexus 5000 Series Switch Reboots

If a Nexus 5000 switch reboots while a new configuration is committed on a peer switch using a switch-profile, follow these steps to synchronize the peer switches after the reload.

- 1 Reapply configurations that were changed on the peer switch during the reboot.
- 2 Enter the **commit** command.
- 3 Verify that the configuration is applied correctly and both peers are back synchronized.

Synchronizing Configurations When a vPC Peer-link Fails

When a peer-link fails and both switches are operational, the secondary switch would shut down its vPC ports. In a Fabric Extender A/A topology, the A/A Fabric Extender is disconnected on the secondary. If the configuration is changed in a switch-profile on the primary switch, the configuration will not be accepted on

the secondary switch unless the A/A Fabric Extender is pre-provisioned. Therefore, it is recommended that all A/A Fabric Extenders be pre-provisioned when using the configuration synchronization feature.

Synchronizing Configurations When the mgmt0 Interface Connectivity is Lost

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

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

Synchronizing Configurations When an ISSU is Performed on One Switch and a Configuration Change is Made on the Peer Switch

In a vPC topology, configuration changes on the peer switch are not allowed when an ISSU is performed on the other switch. In topologies Without vPCs, configuration changes are allowed and the switch undergoing an ISSU will synchronize the new configurations when the upgrade is complete.



CHAPTER 4

Configuring Module Pre-Provisioning

This chapter describes how to configure pre-provisioning for offline interfaces or modules in the Cisco Nexus 5000 Series switch.

This chapter includes the following sections:

- [Information About Module Pre-Provisioning, page 33](#)
- [Guidelines and Limitations, page 34](#)
- [Enabling Module Pre-Provisioning, page 34](#)
- [Removing Module Pre-Provisioning, page 35](#)
- [Verifying the Pre-Provisioned Configuration, page 36](#)
- [Configuration Examples for Pre-Provisioning, page 37](#)

Information About Module Pre-Provisioning

The pre-provisioning feature allows you to preconfigure interfaces before inserting or attaching a module to a Cisco Nexus 5000 Series switch. If a module goes offline, you can also use pre-provisioning to make changes to the interface configurations for the offline module. When a pre-provisioned module comes online, the pre-provisioning configurations are applied. If any configurations were not applied, a syslog is generated. The syslog lists the configurations that were not accepted.

In some Virtual Port Channel (vPC) topologies, pre-provisioning is required for the configuration synchronization feature. Pre-provisioning allows you to synchronize the configuration for an interface that is online with one peer but offline with another peer.

Supported Hardware

The pre-provisioning feature supports the following hardware:

- N2K-C2148T Fabric Extender 48x1G 4x10G Module
- N2K-C2232P Fabric Extender 32x10G Module
- N2K-C2248T Fabric Extender 48x1G 4x10G Module
- N51-M16EP Cisco 16x10-Gigabit Ethernet Expansion Module

- N51-M8E8FP Cisco 8 Port 1/2/4/8G FC and 8 Port 10-Gigabit Ethernet Expansion Module
- N5K-M1008 Cisco 8 Port Fiber Channel Expansion Module 8 x SFP
- N5K-M1060 Cisco 6 Port Fiber Channel Expansion Module 6 x SFP
- N5K-M1404 Expansion Module 4 x 10GBase-T LAN, 4 x Fiber Channel
- N5K-M1600 Cisco 6-port 10 Gigabit Ethernet SFP Module 6 x SFP

Upgrades and Downgrades

When upgrading from Cisco NX-OS Release 4.2(1)N2(1) and earlier releases to Cisco NX-OS Release 5.0(2)N1(1), there are no configuration implications. When upgrading from a release that supports pre-provisioning to another release that supports the feature including InService Software Upgrades (ISSU), pre-provisioned configurations are retained across the upgrade.

When downgrading from an image that supports pre-provisioning to an image that does not support pre-provisioning, you are prompted to remove pre-provisioning configurations.

Guidelines and Limitations

Pre-provisioning has the following configuration guidelines and limitations:

- When a module comes online, commands that are not applied are listed in the syslog.
- If a slot is pre-provisioned for module A and if you insert module B into the slot, module B does not come online.
- There is no MIB support for pre-provisioned interfaces.
- Cisco DCNM is not supported.

Enabling Module Pre-Provisioning

You can enable pre-provisioning on a module that is offline. Enter the **provision model *model*** command in module pre-provision mode.



Note

After enabling pre-provisioning, you can configure the interfaces as though they are online.

SUMMARY STEPS

1. **configuration terminal**
2. **slot *slot***
3. **provision model *model***
4. **exit**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configuration terminal Example: switch# config t switch(config)#	Enters global configuration mode.
Step 2	slot <i>slot</i> Example: switch(config)# slot 101 switch(config-slot)#	Selects the slot to pre-provision and enters slot configuration mode.
Step 3	provision model <i>model</i> Example: switch(config-slot)# provision model N2K-C2248T switch(config-slot)#	Selects the module that you want to pre-provision.
Step 4	exit Example: switch(config-slot)# exit switch#	Exits slot configuration mode.
Step 5	copy running-config startup-config Example: switch# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

This example shows how to select slot 101 and the N2K-C2232P module to pre-provision.

```
switch# configure terminal
switch(config)# slot 101
switch(config-slot)# provision model N2K-C2232P
switch(config-slot)# exit
```

Removing Module Pre-Provisioning

You can remove a module that has been pre-provisioned.

SUMMARY STEPS

1. **configuration terminal**
2. **slot *slot***
3. **no provision model *model***
4. **exit**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configuration terminal Example: switch# config t switch(config)#	Enters global configuration mode.
Step 2	slot slot Example: switch(config)# slot 101 switch(config-slot)#	Selects the slot to pre-provision and enters slot configuration mode.
Step 3	no provision model model Example: switch(config-slot)# no provision model N2K-C2248T switch(config-slot)#	Removes pre-provisioning from the module.
Step 4	exit Example: switch(config-slot)# exit switch#	Exits slot configuration mode.
Step 5	copy running-config startup-config Example: switch# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

This example shows how to remove a preprovisioned module from a chassis slot:

```
switch(config)# slot 2
switch(config-slot)# no provision model N5K-M1404
switch(config-slot)#
```

Verifying the Pre-Provisioned Configuration

To display the pre-provisioned configuration, perform one of the following tasks:

Command	Purpose
show provision	Displays provisioned modules.
show module	Displays module information.
show switch-profile	Displays switch profile information.
show running-config exclude-provision	Displays the running configuration without the pre-provisioned interfaces or modules that are offline.
show provision failed-config	Displays the pre-provisioned commands that were not applied to the configuration when the interface or module came online.

Command	Purpose
	This command also displays a history of failed commands.
show provision failed-config interface	Displays the commands that were not applied when the interface or module came online.
show running-config	Displays the running configuration including the pre-provisioned configuration.
show startup-config	Displays the startup configuration including the pre-provisioned configuration.

Configuration Examples for Pre-Provisioning

The following example shows how to enable pre-provisioning on slot 110 on the Cisco Nexus 2232P Fabric Extender and how to pre-provision interface configuration commands on the Ethernet 110/1/1 interface.

```
switch# configure terminal
switch(config)# slot 110
switch(config-slot)# provision model N2K-C2232P
switch(config-slot)# exit

switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface Ethernet110/1/1
switch(config-if)# description module is preprovisioned
switch(config-if)# show running-config interface Ethernet110/1/1
Time: Wed Aug 25 21:29:44 2010

version 5.0(2)N1(1)

interface Ethernet110/1/1
  description module is preprovisioned
```

The following example shows the list of pre-provisioned commands that were not applied when the module came online.

```
switch(config-if-range)# show provision failed-config 101
The following config was not applied for slot 33
=====

interface Ethernet101/1/1
  service-policy input test

interface Ethernet101/1/2
  service-policy input test

interface Ethernet101/1/3
  service-policy input test
```

This example shows how to remove all pre-provisioned modules from a slot:

```
switch(config)# slot 2
switch(config-slot)# no provision model
switch(config-slot)#
```




CHAPTER 5

Using Cisco Fabric Services

This chapter contains the following sections:

- [Using Cisco Fabric Services, page 39](#)

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).



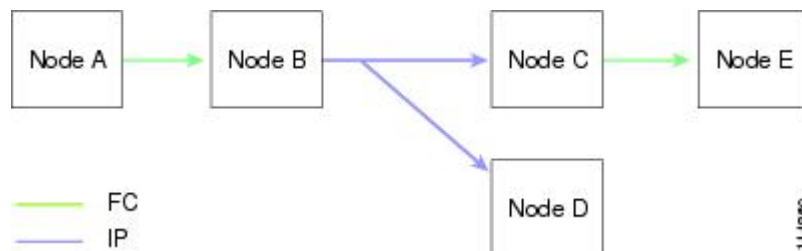
Note

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.

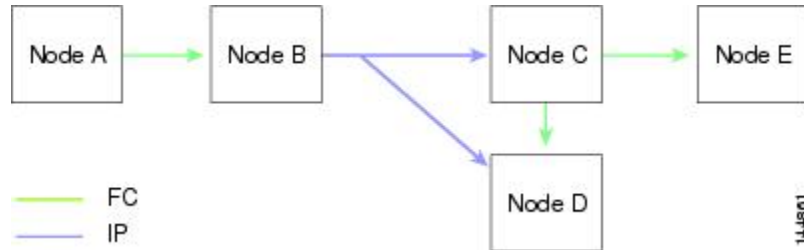
Figure 1: Network Example 1 with Fibre Channel and IP Connections



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

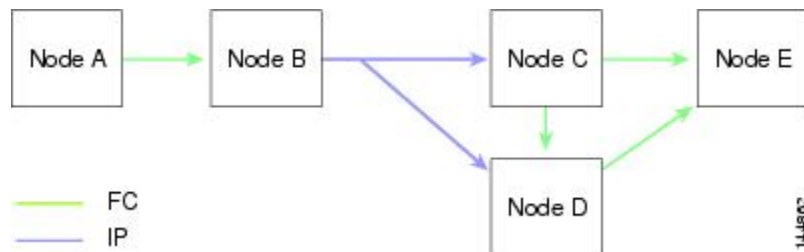
node D the distribution list for IP. Node C does not forward to node D because node D is already in the distribution list from node B.

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
fdomain	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 <i>region-id</i>	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 <i>region-id</i>	Creates a region.
Step 3	switch(config-cfs-region)# <i>application</i>	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 <i>region-id</i>	Enters CFS region configuration submode.
Step 3	switch(config-cfs-region)# <i>application</i>	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 <i>region-id</i>	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 <i>region-id</i>	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 <i>ipv4-address</i>	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 <i>ipv4-address</i>	(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 <i>ipv4-address</i>	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 <i>ipv4-address</i>	(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 6

Configuring User Accounts and RBAC

This chapter contains the following sections:

- [Configuring User Accounts and RBAC, page 57](#)

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, nsd, 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 63](#)

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	<code>switch(config)# show role</code>	(Optional) Displays the user roles available. You can configure other user roles, if necessary.
Step 2	<code>switch# configure terminal</code>	Enters configuration mode.
Step 3	<code>switch(config)# username user-id [password password] [expire date] [role role-name]</code>	Configures a user account. The <i>user-id</i> 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 <i>date</i> 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 than 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 <i>role-name</i>	Specifies a user role and enters role configuration mode. The <i>role-name</i> 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 <i>command-string</i>	Configures a command rule. The <i>command-string</i> 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 <i>feature-name</i>	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 <i>group-name</i>	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 <i>text</i>	(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 <i>group-name</i>	Specifies a user role feature group and enters role feature group configuration mode. The <i>group-name</i> 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 <i>role-name</i>	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 <i>vlan-list</i>	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 <i>role-name</i>	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 <i>vsan-list</i>	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 7

Configuring Session Manager

This chapter contains the following sections:

- [Configuring Session Manager, page 67](#)

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 <i>name</i>	Creates a configuration session and enters session configuration mode. The name can be any alphanumeric string.
Step 2	switch(config-s)# show configuration session [<i>name</i>]	(Optional) Displays the contents of the session.
Step 3	switch(config-s)# save <i>location</i>	(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 <i>name</i>	Creates a configuration session and enters session configuration mode. The name can be any alphanumeric string.
Step 2	switch(config-s)# ip access-list <i>name</i>	Creates an ACL.
Step 3	switch(config-s-acl)# permit <i>protocol source destination</i>	(Optional) Adds a permit statement to the ACL.
Step 4	switch(config-s-acl)# interface <i>interface-type number</i>	Enters interface configuration mode.
Step 5	switch(config-s-if)# ip port access-group <i>name in</i>	Adds a port access group to the interface.
Step 6	switch# show configuration session [<i>name</i>]	(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 <i>location</i>	(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 [<i>name</i>]	Displays the contents of the configuration session.
switch# show configuration session status [<i>name</i>]	Displays the status of the configuration session.
switch# show configuration session summary	Displays a summary of all the configuration sessions.



CHAPTER 8

Configuring Online Diagnostics

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

- [Information About Online Diagnostics, page 71](#)
- [Configuring Online Diagnostics, page 74](#)
- [Verifying Online Diagnostics Configuration, page 74](#)
- [Default GOLD Settings, page 75](#)

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: <ul style="list-style-type: none"> • 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 <i>slot</i>	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 9

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, page 77](#)
- [Configuring System Message Logging, page 78](#)
- [Verifying System Message Logging Configuration, page 89](#)
- [Default System Message Logging Settings, page 90](#)

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 82](#)
- [Configuring System Message Logging to a File, page 81](#)
- [Configuring System Message Logging to Terminal Sessions, page 78](#)

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 send 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 [<i>severity-level</i>]	<p>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:</p> <ul style="list-style-type: none"> • 0 – emergency • 1 – alert • 2 – critical • 3 – error • 4 – warning • 5 – notification • 6 – informational • 7 – debugging <p>If the severity level is not specified, the default of 2 is used.</p>
Step 4	switch(config)# no logging console [<i>severity-level</i>]	(Optional) Disables logging messages to the console.
Step 5	switch(config)# logging monitor [<i>severity-level</i>]	<p>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:</p> <ul style="list-style-type: none"> • 0 – emergency • 1 – alert • 2 – critical

	Command or Action	Purpose
		<ul style="list-style-type: none"> • 3 – error • 4 – warning • 5 – notification • 6 – informational • 7 – debugging <p>If the severity level is not specified, the default of 2 is used.</p> <p>The configuration applies to Telnet and SSH sessions.</p>
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]	<p>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.</p> <p>Severity levels range from 0 to 7:</p> <ul style="list-style-type: none"> • 0 – emergency • 1 – alert • 2 – critical • 3 – error • 4 – warning • 5 – notification • 6 – informational • 7 – debugging <p>The file size is from 4096 to 10485760 bytes.</p>
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 89](#)

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 <i>[severity-level]</i>	<p>Enables module log messages that have the specified severity level or higher. Severity levels range from 0 to 7:</p> <ul style="list-style-type: none"> • 0 – emergency • 1 – alert • 2 – critical • 3 – error • 4 – warning • 5 – notification • 6 – informational • 7 – debugging <p>If the severity level is not specified, the default of 5 is used.</p>
Step 3	switch(config)# logging level facility <i>severity-level</i>	<p>Enables logging messages from the specified facility that have the specified severity level or higher. Severity levels from 0 to 7:</p> <ul style="list-style-type: none"> • 0 – emergency • 1 – alert • 2 – critical • 3 – error • 4 – warning • 5 – notification • 6 – informational • 7 – debugging <p>To apply the same severity level to all facilities, use the all facility. For defaults, see the show logging level command.</p>
Step 4	switch(config)# no logging module <i>[severity-level]</i>	<p>(Optional) Disables module log messages.</p>
Step 5	switch(config)# no logging level <i>[facility severity-level]</i>	<p>(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.</p>
Step 6	switch# show logging module	<p>(Optional) Displays the module logging configuration.</p>

	Command or Action	Purpose
Step 7	switch# show logging level [<i>facility</i>]	(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 [<i>severity-level</i> [use-vrf <i>vrf-name</i> [<i>facility facility</i>]]]	<p>Configures a host to receive syslog messages.</p> <ul style="list-style-type: none"> • The <i>host</i> argument identifies the host name or the IPv4 or IPv6 address of the syslog server host. • The <i>severity-level</i> 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 77 • The use vrf vrf-name keyword argument identifies the <i>default</i> or <i>management</i> 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. <p>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.</p> <ul style="list-style-type: none"> • The <i>facility</i> 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 <i>host</i>	(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                                                                                                                                                                                                                                                                                             |
|---------------|---------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | switch# <b>configure terminal</b>                 | Enters configuration mode.                                                                                                                                                                                                                                                                          |
| <b>Step 2</b> | switch(config)# <b>logging distribute</b>         | Enables distribution of syslog server configuration to network switches using the CFS infrastructure. By default, distribution is disabled.                                                                                                                                                         |
| <b>Step 3</b> | switch(config)# <b>logging commit</b>             | Commits the pending changes to the syslog server configuration for distribution to the switches in the fabric.                                                                                                                                                                                      |
| <b>Step 4</b> | switch(config)# <b>logging abort</b>              | Cancels the pending changes to the syslog server configuration.                                                                                                                                                                                                                                     |
| <b>Step 5</b> | switch(config)# <b>no logging distribute</b>      | (Optional)<br>Disables distribution of syslog server configuration to network switches using the CFS infrastructure. You cannot disable distribution when configuration changes are pending. See the <b>logging commit</b> and <b>logging abort</b> commands. By default, distribution is disabled. |
| <b>Step 6</b> | switch# <b>show logging pending</b>               | (Optional)<br>Displays the pending changes to the syslog server configuration.                                                                                                                                                                                                                      |
| <b>Step 7</b> | switch# <b>show logging pending-diff</b>          | (Optional)<br>Displays the differences from the current syslog server configuration to the pending changes of the syslog server configuration.                                                                                                                                                      |
| <b>Step 8</b> | switch# <b>show logging internal info</b>         | (Optional)<br>Displays information about the current state of syslog server distribution and the last action taken.                                                                                                                                                                                 |
| <b>Step 9</b> | switch# <b>copy running-config startup-config</b> | (Optional)<br>Copies the running configuration to the startup configuration.                                                                                                                                                                                                                        |

## Related Topics

- [Information About CFS, page 39](#)

## 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                                                                                                                                                                                                                                            |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | switch# <b>show logging last</b> <i>number-lines</i>                                                                                  | Displays the last number of lines in the logging file. You can specify from 1 to 9999 for the last number of lines.                                                                                                                                |
| <b>Step 2</b> | switch# <b>show logging logfile</b> [ <b>start-time</b> <i>yyyy mmm dd hh:mm:ss</i> ] [ <b>end-time</b> <i>yyyy mmm dd hh:mm:ss</i> ] | 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. |
| <b>Step 3</b> | switch# <b>show logging nvram</b> [ <b>last</b> <i>number-lines</i> ]                                                                 | 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.                                                         |
| <b>Step 4</b> | switch# <b>clear logging logfile</b>                                                                                                  | Clears the contents of the log file.                                                                                                                                                                                                               |
| <b>Step 5</b> | switch# <b>clear logging nvram</b>                                                                                                    | 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# <b>show logging console</b> | Displays the console logging configuration. |

| Command                                                                                                                               | Purpose                                                                    |
|---------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| switch# <b>show logging info</b>                                                                                                      | Displays the logging configuration.                                        |
| switch# <b>show logging internal info</b>                                                                                             | Displays the syslog distribution information.                              |
| switch# <b>show logging last</b> <i>number-lines</i>                                                                                  | Displays the last number of lines of the log file.                         |
| switch# <b>show logging level</b> [ <i>facility</i> ]                                                                                 | Displays the facility logging severity level configuration.                |
| switch# <b>show logging logfile</b> [ <b>start-time</b> <i>yyyy mmm dd hh:mm:ss</i> ] [ <b>end-time</b> <i>yyyy mmm dd hh:mm:ss</i> ] | Displays the messages in the log file.                                     |
| switch# <b>show logging module</b>                                                                                                    | Displays the module logging configuration.                                 |
| switch# <b>show logging monitor</b>                                                                                                   | Displays the monitor logging configuration.                                |
| switch# <b>show logging nvram</b> [ <b>last</b> <i>number-lines</i> ]                                                                 | Displays the messages in the NVRAM log.                                    |
| switch# <b>show logging pending</b>                                                                                                   | Displays the syslog server pending distribution configuration.             |
| switch# <b>show logging pending-diff</b>                                                                                              | Displays the syslog server pending distribution configuration differences. |
| switch# <b>show logging server</b>                                                                                                    | Displays the syslog server configuration.                                  |
| switch# <b>show logging session</b>                                                                                                   | Displays the logging session status.                                       |
| switch# <b>show logging status</b>                                                                                                    | Displays the logging status.                                               |
| switch# <b>show logging timestamp</b>                                                                                                 | 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 10

## Configuring Smart Call Home

---

This chapter contains the following sections:

- [Configuring Smart Call Home, page 93](#)

## 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 be 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 recipients 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.                                              | <b>show diagnostic result module all detail</b><br><b>show moduleshow version</b> |

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

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 96

## 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

- 
- |               |                                                                     |
|---------------|---------------------------------------------------------------------|
| <b>Step 1</b> | Assign contact information.                                         |
| <b>Step 2</b> | Configure destination profiles.                                     |
| <b>Step 3</b> | Associate one or more alert groups to each profile.                 |
| <b>Step 4</b> | (Optional) Add additional <b>show</b> commands to the alert groups. |
| <b>Step 5</b> | Configure transport options.                                        |
| <b>Step 6</b> | Enable Call Home.                                                   |
| <b>Step 7</b> | (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                                                                                                                                                                                                                                                                                              |
|---------------|---------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | switch# <b>configuration terminal</b>                                           | Enters configuration mode.                                                                                                                                                                                                                                                                           |
| <b>Step 2</b> | switch(config)# <b>snmp-server contact</b> <i>sys-contact</i>                   | Configures the SNMP sysContact.                                                                                                                                                                                                                                                                      |
| <b>Step 3</b> | switch(config)# <b>callhome</b>                                                 | Enters callhome configuration mode.                                                                                                                                                                                                                                                                  |
| <b>Step 4</b> | switch(config-callhome)# <b>email-contact</b> <i>email-address</i>              | 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.<br><br><b>Note</b> You can use any valid e-mail address. The address cannot contain spaces.                                                |
| <b>Step 5</b> | switch(config-callhome)# <b>phone-contact</b> <i>international-phone-number</i> | 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.<br><br><b>Note</b> The phone number cannot contain spaces. Be sure to use the + prefix before the number. |
| <b>Step 6</b> | switch(config-callhome)# <b>streetaddress</b> <i>address</i>                    | Configures the street address as an alphanumeric string with white spaces for the primary person responsible for the switch. Up to 255 alphanumeric characters are accepted, including spaces.                                                                                                       |
| <b>Step 7</b> | switch(config-callhome)# <b>contract-id</b> <i>contract-number</i>              | (Optional)<br>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                                                                                                                                                               |
|----------------|-----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 8</b>  | switch(config-callhome)# <b>customer-id</b><br><i>customer-number</i> | (Optional)<br>Configures the customer number for this switch from the service agreement. The customer number can be up to 255 alphanumeric characters in free format. |
| <b>Step 9</b>  | switch(config-callhome)# <b>site-id</b><br><i>site-number</i>         | (Optional)<br>Configures the site number for this switch. The site number can be up to 255 alphanumeric characters in free format.                                    |
| <b>Step 10</b> | switch(config-callhome)# <b>switch-priority</b><br><i>number</i>      | (Optional)<br>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.         |
| <b>Step 11</b> | switch# <b>show callhome</b>                                          | (Optional)<br>Displays a summary of the Call Home configuration.                                                                                                      |
| <b>Step 12</b> | switch# <b>copy running-config startup-config</b>                     | (Optional)<br>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                                                                                                                                                                                                                                                       |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | switch# <b>configuration terminal</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Enters configuration mode.                                                                                                                                                                                                                                    |
| <b>Step 2</b> | switch(config)# <b>callhome</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Enters callhome configuration mode.                                                                                                                                                                                                                           |
| <b>Step 3</b> | switch(config-callhome)# <b>destination-profile</b> {ciscoTAC-1<br>{alert-group group   email-addr address   http URL  <br>transport-method {email   http}}   profile-name {alert-group<br>group   email-addr address   format {XML   full-txt   short-txt}<br>  http URL   message-level level   message-size size  <br>transport-method {email   http}}   full-txt-destination<br>{alert-group group   email-addr address   http URL   message-level<br>level   message-size size   transport-method {email   http}}  <br>short-txt-destination {alert-group group   email-addr address  <br>http URL   message-level level   message-size size  <br>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.<br><br>For further details about this command, see the <i>Cisco Nexus 5000 Series Command Reference</i> . |
| <b>Step 4</b> | switch# <b>show callhome destination-profile</b> [profile name]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | (Optional)<br>Displays information about one or more destination profiles.                                                                                                                                                                                    |
| <b>Step 5</b> | switch# <b>copy running-config startup-config</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | (Optional)<br>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                                                                                                                                                                                                                                                                    |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | switch# <b>configuration terminal</b>                                                                                                                              | Enters configuration mode.                                                                                                                                                                                                                                                 |
| <b>Step 2</b> | switch(config)# <b>callhome</b>                                                                                                                                    | Enters callhome configuration mode.                                                                                                                                                                                                                                        |
| <b>Step 3</b> | switch(config-callhome)# <b>destination-profile</b> { <i>name</i>   <b>full-txt-destination</b>   <b>short-txt-destination</b> } <b>email-addr</b> <i>address</i>  | 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.                                                                                                                   |
| <b>Step 4</b> | <b>destination-profile</b> { <i>name</i>   <b>full-txt-destination</b>   <b>short-txt-destination</b> } <b>message-level</b> <i>number</i>                         | 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.       |
| <b>Step 5</b> | switch(config-callhome)# <b>destination-profile</b> { <i>name</i>   <b>full-txt-destination</b>   <b>short-txt-destination</b> } <b>message-size</b> <i>number</i> | 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. |
| <b>Step 6</b> | switch# <b>show callhome destination-profile</b> [ <i>profile name</i> ]                                                                                           | (Optional)<br>Displays information about one or more destination profiles.                                                                                                                                                                                                 |
| <b>Step 7</b> | switch# <b>copy running-config startup-config</b>                                                                                                                  | (Optional)<br>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 103](#)

**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                                                                                                                                         |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | switch# <b>configuration terminal</b>                                                                                                                                                                                                                                                                                                       | Enters configuration mode.                                                                                                                      |
| <b>Step 2</b> | switch(config)# <b>callhome</b>                                                                                                                                                                                                                                                                                                             | Enters callhome configuration mode.                                                                                                             |
| <b>Step 3</b> | switch(config-callhome)# <b>destination-profile</b> <i>name</i> <b>alert-group</b> { <b>All</b>   <b>Cisco-TAC</b>   <b>Configuration</b>   <b>Diagnostic</b>   <b>Environmental</b>   <b>Inventory</b>   <b>License</b>   <b>Linecard-Hardware</b>   <b>Supervisor-Hardware</b>   <b>Syslog-group-port</b>   <b>System</b>   <b>Test</b> } | Associates an alert group with this destination profile. Use the <b>All</b> keyword to associate all alert groups with the destination profile. |
| <b>Step 4</b> | switch# <b>show callhome destination-profile</b> [ <i>profile name</i> ]                                                                                                                                                                                                                                                                    | (Optional)<br>Displays information about one or more destination profiles.                                                                      |
| <b>Step 5</b> | switch# <b>copy running-config startup-config</b>                                                                                                                                                                                                                                                                                           | (Optional)<br>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                                                                                                                                                                                                                                               |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | switch# <b>configuration terminal</b>                                                                                                                                                                              | Enters configuration mode.                                                                                                                                                                                                                            |
| <b>Step 2</b> | switch(config)# <b>callhome</b>                                                                                                                                                                                    | Enters callhome configuration mode.                                                                                                                                                                                                                   |
| <b>Step 3</b> | switch(config-callhome)# <b>alert-group {Configuration   Diagnostic   Environmental   Inventory   License   Linecard-Hardware   Supervisor-Hardware   Syslog-group-port   System   Test} user-def-cmd show-cmd</b> | Adds the <b>show</b> command output to any Call Home messages sent for this alert group. Only valid <b>show</b> commands are accepted.<br><br><b>Note</b> You cannot add user-defined CLI <b>show</b> commands to the CiscoTAC-1 destination profile. |
| <b>Step 4</b> | switch# <b>show callhome user-def-cmds</b>                                                                                                                                                                         | (Optional)<br>Displays information about all user-defined <b>show</b> commands added to alert groups.                                                                                                                                                 |
| <b>Step 5</b> | switch# <b>copy running-config startup-config</b>                                                                                                                                                                  | (Optional)<br>Saves this configuration change.                                                                                                                                                                                                        |

This example shows how to add the **show ip routing** command to 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                                                                                                                                                                                                                                                                                                                    |
|---------------|----------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | switch# <b>configuration terminal</b>                                                                                            | Enters configuration mode.                                                                                                                                                                                                                                                                                                 |
| <b>Step 2</b> | switch(config)# <b>callhome</b>                                                                                                  | Enters callhome configuration mode.                                                                                                                                                                                                                                                                                        |
| <b>Step 3</b> | switch(config-callhome)# <b>transport email smtp-server</b> <i>ip-address</i> [ <i>port number</i> ] [ <i>use-vrf vrf-name</i> ] | 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.<br><br>Also optionally you can configure the VRF to use when communicating with this SMTP server. |
| <b>Step 4</b> | switch(config-callhome)# <b>transport email from</b> <i>email-address</i>                                                        | (Optional)<br>Configures the e-mail from field for Call Home messages.                                                                                                                                                                                                                                                     |
| <b>Step 5</b> | switch(config-callhome)# <b>transport email reply-to</b> <i>email-address</i>                                                    | (Optional)<br>Configures the e-mail reply-to field for Call Home messages.                                                                                                                                                                                                                                                 |
| <b>Step 6</b> | switch# <b>show callhome transport-email</b>                                                                                     | (Optional)<br>Displays information about the e-mail configuration for Call Home.                                                                                                                                                                                                                                           |
| <b>Step 7</b> | switch# <b>copy running-config startup-config</b>                                                                                | (Optional)<br>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                                                                                                                                             |
|---------------|------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | switch# <b>configuration terminal</b>                                                                            | Enters configuration mode.                                                                                                                          |
| <b>Step 2</b> | switch(config)# <b>callhome</b>                                                                                  | Enters callhome configuration mode.                                                                                                                 |
| <b>Step 3</b> | switch(config-callhome)# <b>periodic-inventory notification</b> [interval <i>days</i> ] [timeofday <i>time</i> ] | 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. |
| <b>Step 4</b> | switch# <b>show callhome</b>                                                                                     | (Optional)<br>Displays information about Call Home.                                                                                                 |
| <b>Step 5</b> | switch# <b>copy running-config startup-config</b>                                                                | (Optional)<br>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)# <b>no duplicate-message throttle</b> | 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)# <b>enable</b> | Enables Call Home. Disabled by default. |

You can disable Call Home in the callhome configuration mode.

| Command                                   | Purpose                                 |
|-------------------------------------------|-----------------------------------------|
| switch(config-callhome)# <b>no enable</b> | Disables Call Home. Disabled by default |

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

| Command                                    | Purpose                                                        |
|--------------------------------------------|----------------------------------------------------------------|
| switch(config-callhome)# <b>distribute</b> | 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)# <b>commit</b> | 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)# <b>abort</b> | 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)# <b>callhome send diagnostic</b> | Sends the specified Call Home test message to all configured destinations.                                                              |
| switch(config-callhome)# <b>callhome test</b>            | Sends a test message to all configured destinations.<br><b>callhome test</b> and <b>callhome test inventory</b> commands are supported. |

## Verifying Call Home Configuration

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

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

| <b>Data Item(Plain Text and XML)</b> | <b>Description(Plain Text and XML)</b>                                                                                                                                                                                                                                                                           | <b>XML Tag (XML Only)</b> |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|
| Time stamp                           | Date and time stamp of event in ISO time notation:<br><br><i>YYYY-MM-DD<br/>HH:MM:SS<br/>GMT+HH:MM</i>                                                                                                                                                                                                           | /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 <i>type@Sid@serial</i> :<br><br><ul style="list-style-type: none"> <li>• <i>type</i> is the product model number from backplane IDPROM.</li> </ul> | /aml/<br>header/deviceID  |

| Data Item(Plain Text and XML) | Description(Plain Text and XML)                                                                                                                                                                                                                                                         | XML Tag (XML Only)          |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|
|                               | <ul style="list-style-type: none"> <li>• <i>@</i> is a separator character.</li> <li>• <i>Sid</i> is C, identifying the serial ID as a chassis serial number.</li> <li>• <i>serial</i> is the number identified by the Sid field.</li> </ul> <p>An example is<br/>WSC609@C@12345678</p> |                             |
| Customer ID                   | Optional user-configurable field used for contract information or other ID by any support service.                                                                                                                                                                                      | /aml/<br>header/customerID  |
| Contract ID                   | Optional user-configurable field used for contract information or other ID by any support service.                                                                                                                                                                                      | /aml/ header<br>/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)           |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
|                               | <p>The format is <i>type@Sid@serial</i>:</p> <ul style="list-style-type: none"> <li>• <i>type</i> is the product model number from backplane IDPROM.</li> <li>• <i>@</i> is a separator character.</li> <li>• <i>Sid</i> is C, identifying the serial ID as a chassis serial number.</li> <li>• <i>serial</i> is the number identified by the Sid field.</li> </ul> <p>An example is WSC609@C@12345678</p> |                              |
| 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/sysContactPhoneNum |

| 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/alerts/alertData      |
| Attachment type                                                                                  | Specific command output.                                                                          | /aml/alerts/alertData      |
| MIME type                                                                                        | Either plain text or encoding type.                                                               | /aml/alerts/alertData      |
| Command output text                                                                              | Output of command automatically executed.                                                         | /aml/alerts/alertData      |

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 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:Block>
 </soap-env:Body>
</soap-env:Envelope>

```

```

</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 11

## Configuring Rollback

---

This chapter describes how to configure the rollback feature on the Cisco Nexus 5000 Series switch.

This chapter includes the following sections:

- [Information About Rollback, page 121](#)
- [Guidelines and Limitations, page 121](#)
- [Creating a Checkpoint, page 122](#)
- [Implementing a Rollback, page 123](#)
- [Verifying the Rollback Configuration, page 124](#)

## Information About Rollback

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

You can create a checkpoint copy of the current running configuration at any time. Cisco NX-OS saves this checkpoint as an ASCII file which you can use to roll back the running configuration to the checkpoint configuration at a future time. You can create multiple checkpoints to save different versions of your running configuration.

When you roll back the running configuration, you can trigger an atomic rollback. An atomic rollback implements a rollback only if no errors occur.

## Guidelines and Limitations

Rollback has the following configuration guidelines and limitations:

- You can create up to ten checkpoint copies.
- You cannot apply the checkpoint file of one switch into another switch.
- Your checkpoint file names must be 75 characters or less.

- You cannot start a checkpoint filename with the word **system**.
- Beginning in Cisco NX-OS Release 5.0(2)N1(1), you can start a checkpoint filename with the word **auto**.
- Beginning in Cisco NX-OS Release 5.0(2)N1(1), you can name a checkpoint file **summary** or any abbreviation of the word **summary**.
- Only one user can perform a checkpoint, rollback, or copy the running configuration to the startup configuration at the same time.
- After you enter the **write erase** and **reload** command, checkpoints are deleted. You can use the **clear checkpoint database** command to clear out all checkpoint files.
- When checkpoints are created on bootflash, differences with the running-system configuration cannot be performed before performing the rollback, and the system reports “No Changes.”
- Checkpoints are local to a switch.
- Checkpoints that are created using the **checkpoint** and **checkpoint checkpoint\_name** commands are present upon a switchover for all switches.
- A rollback to files on bootflash is supported only on files that are created using the **checkpoint checkpoint\_name** command and not on any other type of ASCII file.
- Checkpoint names must be unique. You cannot overwrite previously saved checkpoints with the same name.
- The Cisco NX-OS commands may differ from the Cisco IOS commands.

## Creating a Checkpoint

You can create up to ten checkpoints of your configuration per switch.

### SUMMARY STEPS

1. switch# **checkpoint** { [ *cp-name* ] [ **description** *descr* ] | **file** *file-name* }
2. (Optional) switch# **no checkpoint** *cp-name*
3. (Optional) switch# **show checkpoint** *cp-name* [ **all** ]

### DETAILED STEPS

|               | Command or Action                                                                                                                                                                     | Purpose                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | switch# <b>checkpoint</b> { [ <i>cp-name</i> ] [ <b>description</b> <i>descr</i> ]   <b>file</b> <i>file-name</i> }<br><br><b>Example:</b><br>switch# <b>checkpoint</b> <i>stable</i> | Creates a checkpoint of the running configuration to either a user checkpoint name or a file. The checkpoint name can be any alphanumeric string up to 80 characters but cannot contain spaces. If you do not provide a name, Cisco NX-OS sets the checkpoint name to user-checkpoint-<number> where number is from 1 to 10.<br><br>The description can contain up to 80 alphanumeric characters, including spaces. |



|               | Command or Action                                                                                                     | Purpose                                                                                                                                                                      |
|---------------|-----------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 2</b> | switch# <b>no checkpoint</b> <i>cp-name</i><br><br><b>Example:</b><br>switch# no checkpoint stable                    | (Optional)<br>You can use the <b>no</b> form of the <b>checkpoint</b> command to remove a checkpoint name.<br><br>Use the <b>delete</b> command to remove a checkpoint file. |
| <b>Step 3</b> | switch# <b>show checkpoint</b> <i>cp-name</i> [ <b>all</b> ]<br><br><b>Example:</b><br>switch# show checkpoint stable | (Optional) Displays the contents of the checkpoint name.                                                                                                                     |

## Implementing a Rollback

You can implement a rollback to a checkpoint name or file. Before you implement a rollback, you can view the differences between source and destination checkpoints that reference current or saved configurations.



### Note

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

### SUMMARY STEPS

1. **show diff rollback-patch** {**checkpoint** *src-cp-name* | **running-config** | **startup-config** | **file** *source-file*} {**checkpoint** *dest-cp-name* | **running-config** | **startup-config** | **file** *dest-file*}
2. **rollback running-config** {**checkpoint** *cp-name* | **file** *cp-file*} **atomic**

### DETAILED STEPS

|               | Command or Action                                                                                                                                                                                                                                                                                                                                                              | Purpose                                                                                 |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>show diff rollback-patch</b> { <b>checkpoint</b> <i>src-cp-name</i>   <b>running-config</b>   <b>startup-config</b>   <b>file</b> <i>source-file</i> } { <b>checkpoint</b> <i>dest-cp-name</i>   <b>running-config</b>   <b>startup-config</b>   <b>file</b> <i>dest-file</i> }<br><br><b>Example:</b><br>switch# show diff rollback-patch checkpoint stable running-config | Displays the differences between the source and destination checkpoint selections.      |
| <b>Step 2</b> | <b>rollback running-config</b> { <b>checkpoint</b> <i>cp-name</i>   <b>file</b> <i>cp-file</i> } <b>atomic</b><br><br><b>Example:</b><br>switch# rollback running-config checkpoint stable                                                                                                                                                                                     | Creates an atomic rollback to the specified checkpoint name or file if no errors occur. |

This example shows how to create a checkpoint file and then implements an atomic rollback to a user checkpoint name:

```
switch# checkpoint stable
switch# rollback running-config checkpoint stable atomic
```

## Verifying the Rollback Configuration

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

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



### Note

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



# CHAPTER 12

## 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, page 125](#)
- [Configuration Guidelines and Limitations, page 129](#)
- [Configuring SNMP, page 129](#)
- [Verifying SNMP Configuration, page 138](#)
- [Default SNMP Settings, page 138](#)

## 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 131](#)

## 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# <b>configuration terminal</b> | Enters configuration mode. |

|               | Command or Action                                                                                                                                                        | Purpose                                                             |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|
| <b>Step 2</b> | switch(config)# <b>snmp-server user</b> <i>name</i> [auth {md5   sha} <i>passphrase</i> [auto] [priv [aes-128] <i>passphrase</i> ] [engineID <i>id</i> ] [localizedkey]] | Configures an SNMP user with authentication and privacy parameters. |
| <b>Step 3</b> | switch# <b>show snmp user</b>                                                                                                                                            | (Optional)<br>Displays information about one or more SNMP users.    |
| <b>Step 4</b> | switch# <b>copy running-config startup-config</b>                                                                                                                        | (Optional)<br>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)# <b>snmp-server user</b> <i>name</i> <b>enforcePriv</b> | Enforces SNMP message encryption for this user. |

You can enforce SNMP message encryption for all users.

| Command                                              | Purpose                                         |
|------------------------------------------------------|-------------------------------------------------|
| switch(config)# <b>snmp-server globalEnforcePriv</b> | 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)# <b>snmp-server user</b> <i>name</i> <i>group</i> | 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)# <b>snmp-server community</b> <i>name</i><br><i>group</i> { <b>ro</b>   <b>rw</b> } | 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)# <b>snmp-server community</b> <i>community</i><br><i>name</i> <b>use-acl</b> <i>acl-name</i><br><br><b>Example:</b><br>switch(config)# snmp-server community public<br>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)# <b>snmp-server host</b> <i>ip-address</i> <b>traps version 1</b> <i>community</i> [ <i>udp_port number</i> ] | 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)# <b>snmp-server host</b> <i>ip-address</i> { <b>traps</b>   <b>informs</b> } <b>version 2c</b> <i>community</i> [ <i>udp_port number</i> ] | 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)# <b>snmp-server host</b> <i>ip-address</i> { <b>traps</b>   <b>informs</b> } <b>version 3</b> { <b>auth</b>   <b>noauth</b>   <b>priv</b> } <i>username</i> [ <i>udp_port number</i> ] | 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)# <b>snmp-server user</b> <i>name</i> [auth { <b>md5</b>   <b>sha</b> } <i>passphrase</i> [auto] [priv [ <b>aes-128</b> ] <i>passphrase</i> ] [ <b>engineID</b> <i>id</i> ] | 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                                                       | <b>snmp-server enable traps</b>                                                             |
| CISCO-AAA-SERVER-MIB                                                    | <b>snmp-server enable traps aaa</b>                                                         |
| ENTITY-MIB,<br>CISCO-ENTITY-FRU-CONTROL-MIB,<br>CISCO-ENTITY-SENSOR-MIB | <b>snmp-server enable traps entity</b><br><b>snmp-server enable traps entity fru</b>        |
| CISCO-LICENSE-MGR-MIB                                                   | <b>snmp-server enable traps license</b>                                                     |
| IF-MIB                                                                  | <b>snmp-server enable traps link</b>                                                        |
| CISCO-PSM-MIB                                                           | <b>snmp-server enable traps port-security</b>                                               |
| SNMPv2-MIB                                                              | <b>snmp-server enable traps snmp</b><br><b>snmp-server enable traps snmp authentication</b> |

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

**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)# <b>snmp-server enable traps</b>                                     | Enables all SNMP notifications.            |
| switch(config)# <b>snmp-server enable traps aaa</b><br><b>[server-state-change]</b> | Enables the AAA SNMP notifications.        |
| switch(config)# <b>snmp-server enable traps entity</b><br><b>[fru]</b>              | Enables the ENTITY-MIB SNMP notifications. |
| switch(config)# <b>snmp-server enable traps license</b>                             | Enables the license SNMP notification.     |

| Command                                                               | Purpose                                       |
|-----------------------------------------------------------------------|-----------------------------------------------|
| switch(config)# <b>snmp-server enable traps port-security</b>         | Enables the port security SNMP notifications. |
| switch(config)# <b>snmp-server enable traps snmp [authentication]</b> | 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, cieLinkDown 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.
- IETF 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.
- IETF 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.
- IETF 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                              |
|---------------|-------------------------------------------------------------------------------------|--------------------------------------|
| <b>Step 1</b> | switch# <b>configure terminal</b>                                                   | Enters configuration mode.           |
| <b>Step 2</b> | switch(config)# <b>snmp-server enable traps link [cisco] [ietf   ietf-extended]</b> | 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                                                               |
|---------------|--------------------------------------------------------|-----------------------------------------------------------------------|
| <b>Step 1</b> | switch# <b>configure terminal</b>                      | Enters configuration mode.                                            |
| <b>Step 2</b> | switch(config)# <b>interface</b> <i>type slot/port</i> | Specifies the interface to be changed.                                |
| <b>Step 3</b> | switch(config-if)# <b>no snmp trap link-status</b>     | 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)# <b>snmp-server tcp-session [auth]</b> | 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                                                                    |
|---------------|---------------------------------------------------------|----------------------------------------------------------------------------|
| <b>Step 1</b> | switch# <b>configuration terminal</b>                   | Enters configuration mode.                                                 |
| <b>Step 2</b> | switch(config)# <b>snmp-server contact</b> <i>name</i>  | Configures sysContact, the SNMP contact name.                              |
| <b>Step 3</b> | switch(config)# <b>snmp-server location</b> <i>name</i> | Configures sysLocation, the SNMP location.                                 |
| <b>Step 4</b> | switch# <b>show snmp</b>                                | (Optional)<br>Displays information about one or more destination profiles. |
| <b>Step 5</b> | switch# <b>copy running-config startup-config</b>       | (Optional)<br>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                                                                                                                                                            |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | switch# <b>configuration terminal</b>                                                                                                                                              | Enters configuration mode.                                                                                                                                         |
| <b>Step 2</b> | switch(config)# <b>snmp-server context</b> <i>context-name</i> [ <b>instance</b> <i>instance-name</i> ] [ <b>vrf</b> <i>vrf-name</i> ] [ <b>topology</b> <i>topology-name</i> ]    | Maps an SNMP context to a protocol instance, VRF, or topology. The names can be any alphanumeric string up to 32 characters.                                       |
| <b>Step 3</b> | switch(config)# <b>snmp-server mib community-map</b> <i>community-name</i> <b>context</b> <i>context-name</i>                                                                      | Maps an SNMPv2c community to an SNMP context. The names can be any alphanumeric string up to 32 characters.                                                        |
| <b>Step 4</b> | switch(config)# <b>no snmp-server context</b> <i>context-name</i> [ <b>instance</b> <i>instance-name</i> ] [ <b>vrf</b> <i>vrf-name</i> ] [ <b>topology</b> <i>topology-name</i> ] | (Optional)<br>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                                                                                                                                                                                                                              |
|--|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  |                   | <b>Note</b> Do not enter an instance, VRF, or topology to delete a context mapping. If you use the <b>instance</b> , <b>vrf</b> , or <b>topology</b> 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# <b>show snmp</b>           | Displays the SNMP status.                            |
| switch# <b>show snmp community</b> | Displays the SNMP community strings.                 |
| switch# <b>show snmp engineID</b>  | Displays the SNMP engineID.                          |
| switch# <b>show snmp group</b>     | Displays SNMP roles.                                 |
| switch# <b>show snmp sessions</b>  | Displays SNMP sessions.                              |
| switch# <b>show snmp trap</b>      | Displays the SNMP notifications enabled or disabled. |
| switch# <b>show snmp user</b>      | 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 13

## Configuring RMON

---

This chapter contains the following sections:

- [Configuring RMON, page 139](#)

## 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 event 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 as a 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                                                                                                                                                                              |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | switch# <b>configure terminal</b>                                                                                                                                                                                                                                          | Enters configuration mode.                                                                                                                                                           |
| <b>Step 2</b> | switch(config)# <b>rmon alarm</b> <i>index mib-object sample-interval {absolute   delta} rising-threshold value [event-index] falling-threshold value [event-index] [owner name]</i>                                                                                       | Creates an RMON alarm. The value range is from -2147483647 to 2147483647. The owner name can be any alphanumeric string.                                                             |
| <b>Step 3</b> | switch(config)# <b>rmon hcalarm</b> <i>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]</i> | Creates an RMON high-capacity alarm. The value range is from -2147483647 to 2147483647. The owner name can be any alphanumeric string.<br><br>The storage type range is from 1 to 5. |
| <b>Step 4</b> | switch# <b>show rmon {alarms   hcalarms}</b>                                                                                                                                                                                                                               | (Optional)<br>Displays information about RMON alarms or high-capacity alarms.                                                                                                        |
| <b>Step 5</b> | switch# <b>copy running-config startup-config</b>                                                                                                                                                                                                                          | (Optional)<br>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                                                                                         |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | switch# <b>configure terminal</b>                                                                                                               | Enters configuration mode.                                                                      |
| <b>Step 2</b> | switch(config)# <b>rmon event</b> <i>index</i> [ <b>description</b> <i>string</i> ] [ <b>log</b> ] [ <b>trap</b> ] [ <b>owner</b> <i>name</i> ] | Configures an RMON event. The description string and owner name can be any alphanumeric string. |
| <b>Step 3</b> | switch(config)# <b>show rmon</b> { <b>alarms</b>   <b>hcalarms</b> }                                                                            | (Optional)<br>Displays information about RMON alarms or high-capacity alarms.                   |
| <b>Step 4</b> | switch# <b>copy running-config startup-config</b>                                                                                               | (Optional)<br>Saves this configuration change.                                                  |

## Verifying RMON Configuration

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

| Command                           | Purpose                                   |
|-----------------------------------|-------------------------------------------|
| switch# <b>show rmon alarms</b>   | Displays information about RMON alarms.   |
| switch# <b>show rmon events</b>   | Displays information about RMON events.   |
| switch# <b>show rmon hcalarms</b> | Displays information about RMON hcalarms. |
| switch# <b>show rmon logs</b>     | 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. |





## CHAPTER 14

# Configuring SPAN

---

This chapter includes the following sections:

- [Configuring SPAN, page 145](#)

## Configuring SPAN

The Switched Port Analyzer (SPAN) feature (sometimes called port mirroring or port monitoring) selects network traffic for analysis by a network analyzer. The network analyzer can be a Cisco SwitchProbe, a Fibre Channel Analyzer, or other Remote Monitoring (RMON) probes.

## SPAN Sources

SPAN sources refer to the interfaces from which traffic can be monitored. The Cisco Nexus 5000 Series switch supports Ethernet, Fibre Channel, virtual Fibre Channel, port channels, SAN port channels, VLANs, and VSANs as SPAN sources. With VLANs or VSANs, all supported interfaces in the specified VLAN or VSAN are included as SPAN sources. You can choose the SPAN traffic in the ingress direction, the egress direction, or both directions for Ethernet, Fibre Channel, and virtual Fibre Channel source interfaces:

- Ingress source (Rx)—Traffic entering the switch through this source port is copied to the SPAN destination port.
- Egress source (Tx)—Traffic exiting the switch through this source port is copied to the SPAN destination port.



### Note

---

On the Cisco Nexus 5548 Switch, Fibre Channel ports and VSAN ports cannot be configured as ingress source ports in a SPAN session.

---

## Characteristics of Source Ports

A source port, also called a monitored port, is a switched interface that you monitor for network traffic analysis. The switch supports any number of ingress source ports (up to the maximum number of available ports on the switch) and any number of source VLANs or VSANs.

A source port has these characteristics:

- Can be of any port type: Ethernet, Fibre Channel, virtual Fibre Channel, port channel, SAN port channel, VLAN, and VSAN.
- Cannot be monitored in multiple SPAN sessions.
- Cannot be a destination port.
- Each source port can be configured with a direction (ingress, egress, or both) to monitor. For VLAN and VSAN sources, the monitored direction can only be ingress and applies to all physical ports in the group. The RX/TX option is not available for VLAN or VSAN SPAN sessions.
- Beginning with Cisco NX-OS Release 5.0(2)N1(1), Port Channel and SAN Port Channel interfaces can be configured as ingress or egress source ports.
- Source ports can be in the same or different VLANs or VSANs.
- For VLAN or VSAN SPAN sources, all active ports in the source VLAN or VSAN are included as source ports.
- For Cisco NX-OS Release 4.2(1)N2(1) and earlier, the Cisco Nexus 5010 Switch and the Cisco Nexus 5020 Switch supports a maximum of two egress SPAN source ports.
- Beginning with NX-OS Release 5.0(2)N1(1), there is no limit to the number of egress SPAN source ports.
- On the Cisco Nexus 5548 Switch, Fibre Channel ports and VSAN ports cannot be configured as ingress source ports in a SPAN session.

## SPAN Destinations

SPAN destinations refer to the interfaces that monitors source ports. The Cisco Nexus 5000 Series switch supports Ethernet and Fibre Channel interfaces as SPAN destinations.

| Source SPAN           | Dest SPAN       |
|-----------------------|-----------------|
| Ethernet              | Ethernet        |
| Fibre Channel         | Fibre Channel   |
| Fibre Channel         | Ethernet (FCoE) |
| Virtual Fibre Channel | Fibre Channel   |
| Virtual Fibre Channel | Ethernet (FCoE) |

## Characteristics of Destination Ports

Each local SPAN session must have a destination port (also called a monitoring port) that receives a copy of traffic from the source ports, VLANs, or VSANs. A destination port has these characteristics:

- Can be any physical port, Ethernet, Ethernet (FCoE), or Fibre Channel, and virtual Fibre Channel ports cannot be destination ports.



- Cannot be a source port.
- Cannot be a port channel or SAN port channel group.
- Does not participate in spanning tree while the SPAN session is active.
- Is excluded from the source list and is not monitored if it belongs to a source VLAN of any SPAN session.
- Receives copies of sent and received traffic for all monitored source ports. If a destination port is oversubscribed, it can become congested. This congestion can affect traffic forwarding on one or more of the source ports.

## Configuring SPAN

### Creating and Deleting a SPAN Session

You create a SPAN session by assigning a session number using the monitor command. If the session already exists, any additional configuration is added to that session.

#### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **monitor session** *session-number*

#### DETAILED STEPS

|               | Command or Action                                            | Purpose                                                                                                          |
|---------------|--------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | switch# <b>configure terminal</b>                            | Enters configuration mode.                                                                                       |
| <b>Step 2</b> | switch(config)# <b>monitor session</b> <i>session-number</i> | Enters the monitor configuration mode. New session configuration is added to the existing session configuration. |

### Configuring the Destination Port

#### Configuring an Ethernet Destination Port



#### Note

The SPAN destination port can only be a physical port on the switch.

You can configure an Ethernet interface as a SPAN destination port.

## SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface ethernet** *slot/port*
3. switch(config-if)# **switchport monitor**
4. switch(config-if)# **exit**
5. switch(config)# **monitor session** *session-number*
6. switch(config-monitor)# **destination interface ethernet** *slot/port*

## DETAILED STEPS

|               | Command or Action                                                              | Purpose                                                                                                                  |
|---------------|--------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | switch# <b>configure terminal</b>                                              | Enters configuration mode.                                                                                               |
| <b>Step 2</b> | switch(config)# <b>interface ethernet</b> <i>slot/port</i>                     | Enters interface configuration mode for the specified Ethernet interface selected by the slot and port values.           |
| <b>Step 3</b> | switch(config-if)# <b>switchport monitor</b>                                   | Sets the interface to monitor mode. Priority flow control is disabled when the port is configured as a SPAN destination. |
| <b>Step 4</b> | switch(config-if)# <b>exit</b>                                                 | Reverts to global configuration mode.                                                                                    |
| <b>Step 5</b> | switch(config)# <b>monitor session</b> <i>session-number</i>                   | Enters the monitor configuration mode.                                                                                   |
| <b>Step 6</b> | switch(config-monitor)# <b>destination interface ethernet</b> <i>slot/port</i> | Configures the Ethernet destination port.                                                                                |

The following example shows configuring an Ethernet SPAN destination port:

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# switchport monitor
switch(config-if)# exit
switch(config)# monitor session 2
switch(config-monitor)# destination interface ethernet 1/3
```

## Configuring Fibre Channel Destination Port

**Note**

The SPAN destination port can only be a physical port on the switch.

You can configure a Fibre Channel port as a SPAN destination port.

## SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface fc slot/port**
3. switch(config-if)# **switchport mode SD**
4. switch(config-if)# **switchport speed 1000**
5. switch(config-if)# **exit**
6. switch(config)# **monitor session session-number**
7. switch(config-monitor)# **destination interface fc slot/port**

## DETAILED STEPS

|               | Command or Action                                                 | Purpose                                                                                                             |
|---------------|-------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | switch# <b>configure terminal</b>                                 | Enters configuration mode.                                                                                          |
| <b>Step 2</b> | switch(config)# <b>interface fc slot/port</b>                     | Enters interface configuration mode for the specified Fibre Channel interface selected by the slot and port values. |
| <b>Step 3</b> | switch(config-if)# <b>switchport mode SD</b>                      | Sets the interface to SPAN destination (SD) mode.                                                                   |
| <b>Step 4</b> | switch(config-if)# <b>switchport speed 1000</b>                   | Sets the interface speed to 1000. The auto speed option is not allowed.                                             |
| <b>Step 5</b> | switch(config-if)# <b>exit</b>                                    | Reverts to global configuration mode.                                                                               |
| <b>Step 6</b> | switch(config)# <b>monitor session session-number</b>             | Enters the monitor configuration mode.                                                                              |
| <b>Step 7</b> | switch(config-monitor)# <b>destination interface fc slot/port</b> | Configures the Fibre Channel destination port.                                                                      |

The following example shows configuring an Ethernet SPAN destination port:

```
switch# configure terminal
switch(config)# interface fc 2/4
switch(config-if)# switchport mode SD
switch(config-if)# switchport speed 1000
switch(config-if)# exit
switch(config)# monitor session 2
switch(config-monitor)# destination interface fc 2/4
```

## Configuring Source Ports

You can configure the source ports for a SPAN session. The source ports can be Ethernet, Fibre Channel, or virtual Fibre Channel ports.

## SUMMARY STEPS

1. switch(config-monitor)# **source interface type slot/port [rx | tx | both]**

## DETAILED STEPS

|               | Command or Action                                                                      | Purpose                                                                                                                                                                                                                                                                                    |
|---------------|----------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | switch(config-monitor)# <b>source interface</b> <i>type slot/port [rx   tx   both]</i> | Configures sources and the traffic direction in which to duplicate packets. You can enter a range of Ethernet, Fibre Channel, or virtual Fibre Channel ports. You can specify the traffic direction to duplicate as ingress (rx), egress (tx), or both. By default, the direction is both. |

The following example shows configuring an Ethernet SPAN source port:

```
switch# configure terminal
switch(config)# monitor session 2
switch(config-monitor)# source interface ethernet 1/16
```

The following example shows configuring a Fibre Channel SPAN source port:

```
switch(config-monitor)# source interface fc 2/1
```

The following example shows configuring a virtual Fibre Channel SPAN source port:

```
switch(config-monitor)# source interface vfc 129
```

## Configuring Source Port Channels, VLANs, or VSANs

You can configure the source channels for a SPAN session. These ports can be port channels, SAN port channels, VLANs, and VSANs. The monitored direction can only be ingress and applies to all physical ports in the group.

**Note**

The Cisco Nexus 5000 Series switch supports two active SPAN sessions. The Cisco Nexus 5548 Switch supports four active SPAN sessions. When you configure more than two SPAN sessions, the first two sessions are active. During startup, the order of active sessions is reversed; the last two sessions are active. For example, if you configured ten sessions 1 to 10 where 1 and 2 are active, after a reboot, sessions 9 and 10 will be active. To enable deterministic behavior, explicitly suspend the sessions 3 to 10 with the **monitor session session-number shut** command. See *Suspending a SPAN Session*.

## SUMMARY STEPS

1. switch(config-monitor)# **source** {**interface** {**port-channel** | **san-port-channel**} *channel-number rx | vlan vlan-range | vsan vsan-range* }

## DETAILED STEPS

|               | Command or Action                                                                                                                                                         | Purpose                                                                                                                          |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | switch(config-monitor)# <b>source</b> { <b>interface</b> { <b>port-channel</b>   <b>san-port-channel</b> } <i>channel-number rx   vlan vlan-range   vsan vsan-range</i> } | Configures port channel, SAN port channel, VLAN, or VSAN sources. For VLAN or VSAN sources, the monitored direction is implicit. |

The following example shows configuring a port channel SPAN source:

```
switch# configure terminal
switch(config)# monitor session 2
switch(config-monitor)# source interface port-channel 1 rx
```

The following example shows configuring a SAN port channel SPAN source:

```
switch(config-monitor)# source interface san-port-channel 3 rx
```

The following example shows configuring a VLAN SPAN source:

```
switch(config-monitor)# source vlan 1
```

The following example shows configuring a VSAN SPAN source:

```
switch(config-monitor)# source vsan 1
```

## Configuring the Description of a SPAN Session

You can provide a descriptive name of the SPAN session for ease of reference.

### SUMMARY STEPS

1. switch(config-monitor)# **description** *description*

### DETAILED STEPS

|               | Command or Action                                             | Purpose                                         |
|---------------|---------------------------------------------------------------|-------------------------------------------------|
| <b>Step 1</b> | switch(config-monitor)# <b>description</b> <i>description</i> | Applies a descriptive name to the SPAN session. |

The following example shows configuring a description of a SPAN session:

```
switch# configure terminal
switch(config)# monitor session 2
switch(config-monitor)# description monitoring ports fc2/2-fc2/4
```

## Activating a SPAN Session

The default is to keep the session state shut. You can open a session that duplicates packets from sources to destinations.

### SUMMARY STEPS

1. switch(config)# **no monitor session** {all | *session-number*} **shut**

### DETAILED STEPS

|               | Command or Action                                                                    | Purpose                                           |
|---------------|--------------------------------------------------------------------------------------|---------------------------------------------------|
| <b>Step 1</b> | switch(config)# <b>no monitor session</b> {all   <i>session-number</i> } <b>shut</b> | Opens the specified SPAN session or all sessions. |

The following example shows activating a SPAN session:

```
switch(config)# no monitor session 3 shut
```

## Suspending a SPAN Session

The default is to keep the session state shut. You can suspend a SPAN session.

### SUMMARY STEPS

1. switch(config)# **monitor session** {all | session-number} **shut**

### DETAILED STEPS

|        | Command or Action                                                         | Purpose                                              |
|--------|---------------------------------------------------------------------------|------------------------------------------------------|
| Step 1 | switch(config)# <b>monitor session</b> {all   session-number} <b>shut</b> | Suspends the specified SPAN session or all sessions. |

The following example shows suspending a SPAN session:

```
switch(config)# monitor session 3 shut
```



#### Note

The Cisco Nexus 5000 Series switch supports two active SPAN sessions. The Cisco Nexus 5548 Switch supports four active SPAN sessions. When you configure more than two SPAN sessions, the first two sessions are active. During startup, the order of active sessions is reversed; the last two sessions are active. For example, if you configured ten sessions 1 to 10 where 1 and 2 are active, after a reboot, sessions 9 and 10 will be active. To enable deterministic behavior, explicitly suspend the sessions 3 to 10 with the **monitor session session-number shut** command.

## Displaying SPAN Information

To display SPAN information, perform this task:

### SUMMARY STEPS

1. switch# **show monitor** [session {all | session-number | range session-range} [brief]]

### DETAILED STEPS

|        | Command or Action                                                                          | Purpose                          |
|--------|--------------------------------------------------------------------------------------------|----------------------------------|
| Step 1 | switch# <b>show monitor</b> [session {all   session-number   range session-range} [brief]] | Displays the SPAN configuration. |

This example shows how to display SPAN session information:

```
switch# show monitor
SESSION STATE REASON DESCRIPTION
----- -
2 up The session is up
3 down Session suspended
4 down No hardware resource
```

This example shows how to display SPAN session details:

```
switch# show monitor session 2
 session 2

type : local
state : up
source intf :
 rx : fc3/1
 tx : fc3/1
 both : fc3/1
source VLANs :
 rx :
source VSANs :
 rx : 1
destination ports : Eth3/1
```







## INDEX

### C

- call home
  - smart call home feature [97](#)
- Call Home
  - description [93](#)
  - message format options [93](#)
- Call Home messages
  - configuring levels [96](#)
  - format options [93](#)
- call home notifications
  - full-txt format for syslog [115](#)
  - XML format for syslog [115](#)
- changed information
  - description [1](#)

### D

- default settings
  - rollback [70](#)
- device IDs
  - call home format [109](#)
- diagnostics
  - configuring [73](#)
  - default settings [74](#)
  - expansion modules [73](#)
  - health monitoring [72](#)
  - runtime [71](#)

### E

- e-mail notifications
  - Call Home [93](#)
- executing a session [69](#)

### G

- GOLD diagnostics
  - configuring [73](#)
  - expansion modules [73](#)
  - health monitoring [72](#)
  - runtime [71](#)

### H

- health monitoring diagnostics
  - information [72](#)

### I

- IDs
  - serial IDs [109](#)

### L

- linkDown notifications [135, 136](#)
- linkUp notifications [135, 136](#)

### N

- new information
  - description [1](#)

### P

- passwords
  - strong characteristics [57](#)

## R

- roles
  - authentication [57](#)
- rollback
  - checkpoint copy [67](#)
  - creating a checkpoint copy [67](#)
  - default settings [70](#)
  - deleting a checkpoint file [67](#)
  - description [67](#)
  - example configuration [67](#)
  - guidelines [67](#)
  - high availability [67](#)
  - implementing a rollback [67](#)
  - limitations [67](#)
  - reverting to checkpoint file [67](#)
  - verifying configuration [70](#)
- runtime diagnostics
  - information [71](#)

## S

- serial IDs
  - description [109](#)
- server IDs
  - description [109](#)
- session manager [67, 69, 70](#)
  - committing a session [69](#)
  - configuring an ACL session (example) [70](#)
  - description [67](#)
  - discarding a session [69](#)
  - guidelines [67](#)
  - limitations [67](#)
  - saving a session [69](#)
  - verifying configuration [70](#)
  - verifying the session [69](#)
- smart call home
  - description [97](#)

- smart call home (*continued*)
  - registration requirements [97](#)
  - Transport Gateway (TG) aggregation point [97](#)
- SMARTnet
  - smart call home registration [97](#)
- SNMP
  - access groups [129](#)
  - group-based access [129](#)
  - server contact name [97](#)
  - user synchronization with CLI [128](#)
  - Version 3 security features [126](#)
- SNMP (Simple Network Management Protocol)
  - versions [126](#)
- SNMPv3
  - assigning multiple roles [130](#)
  - security features [126](#)
- source IDs
  - call home event format [109](#)
- SPAN
  - egress sources [145](#)
  - ingress sources [145](#)
  - sources for monitoring [145](#)
- SPAN sources
  - egress [145](#)
  - ingress [145](#)
- Switched Port Analyzer [145](#)

## T

- trap notifications [126](#)

## U

- user accounts
  - password characteristics [57](#)
- users
  - description [57](#)