CONTENTS

New and Changed Information xv

Preface xix

Audience xix

Document Organization xix

Document Conventions xx

Related Documentation xxi

Obtaining Documentation and Submitting a Service Request xxii

Overview 1-1

Cisco NX-OS Device Configuration Methods 1-1

Configuring with CLI or XML Management Interface 1-3

Configuring with DCNM or a Custom GUI 1-3

Cisco Fabric Services 1-3

Network Time Protocol 1-3

Cisco Discovery Protocol 1-3

System Messages 1-4

Call Home 1-4

Rollback 1-4

Session Manager 1-4

Scheduler 1-5

SNMP 1-5

RMON 1-5

Online Diagnostics 1-5

Embedded Event Manager 1-5

SPAN 1-6

On-Board Failure Logging 1-6

NetFlow 1-6

Troubleshooting Features 1-6
## Configuring CFS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information About CFS</td>
<td>2-1</td>
</tr>
<tr>
<td>Merging Application Databases</td>
<td>2-2</td>
</tr>
<tr>
<td>Applications that Use CFS to Distribute Configuration Changes</td>
<td>2-2</td>
</tr>
<tr>
<td>CFS Distribution</td>
<td>2-2</td>
</tr>
<tr>
<td>CFS Regions</td>
<td>2-3</td>
</tr>
<tr>
<td>High Availability</td>
<td>2-3</td>
</tr>
<tr>
<td>Virtualization Support</td>
<td>2-3</td>
</tr>
<tr>
<td>Licensing Requirements for CFS</td>
<td>2-4</td>
</tr>
<tr>
<td>Prerequisites for CFS</td>
<td>2-4</td>
</tr>
<tr>
<td>Guidelines and Limitations</td>
<td>2-4</td>
</tr>
<tr>
<td>Configuring CFS Distribution</td>
<td>2-5</td>
</tr>
<tr>
<td>Enabling CFS Distribution for Applications</td>
<td>2-5</td>
</tr>
<tr>
<td>Specifying a CFS Distribution Mode</td>
<td>2-10</td>
</tr>
<tr>
<td>Configuring an IP Multicast Address for CFS Over IP</td>
<td>2-11</td>
</tr>
<tr>
<td>Configuring CFS Regions</td>
<td>2-13</td>
</tr>
<tr>
<td>Creating and Distributing a CFS Configuration</td>
<td>2-19</td>
</tr>
<tr>
<td>Clearing a Locked Session</td>
<td>2-20</td>
</tr>
<tr>
<td>Discarding a Configuration</td>
<td>2-21</td>
</tr>
<tr>
<td>Disabling CFS Distribution Globally</td>
<td>2-22</td>
</tr>
<tr>
<td>Verifying the CFS Configuration</td>
<td>2-24</td>
</tr>
<tr>
<td>Default Settings</td>
<td>2-24</td>
</tr>
<tr>
<td>Additional References</td>
<td>2-25</td>
</tr>
<tr>
<td>Related Documents</td>
<td>2-25</td>
</tr>
<tr>
<td>MIBs</td>
<td>2-25</td>
</tr>
<tr>
<td>Feature History for CFS</td>
<td>2-25</td>
</tr>
</tbody>
</table>

## Configuring NTP

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information About NTP</td>
<td>3-1</td>
</tr>
<tr>
<td>NTP Overview</td>
<td>3-1</td>
</tr>
<tr>
<td>Distributing NTP Using CFS</td>
<td>3-2</td>
</tr>
<tr>
<td>High Availability</td>
<td>3-2</td>
</tr>
<tr>
<td>Virtualization Support</td>
<td>3-2</td>
</tr>
<tr>
<td>Licensing Requirements for NTP</td>
<td>3-3</td>
</tr>
<tr>
<td>Prerequisites for NTP</td>
<td>3-3</td>
</tr>
<tr>
<td>Guidelines and Limitations</td>
<td>3-3</td>
</tr>
<tr>
<td>Configuring NTP</td>
<td>3-3</td>
</tr>
<tr>
<td>Enabling or Disabling the NTP Protocol</td>
<td>3-4</td>
</tr>
</tbody>
</table>
Contents

syslog Servers  5-2
Virtualization Support  5-2
Licensing Requirements for System Message Logging  5-3
Guidelines and Limitations  5-3
Configuring System Message Logging  5-3
  Configuring System Message Logging to Terminal Sessions  5-3
  Logging System Messages to a File  5-5
  Configuring Module and Facility Messages Logged  5-6
  Configuring syslog Servers  5-7
  Displaying and Clearing Log Files  5-9
Verifying System Message Logging Configuration  5-10
System Message Logging Example Configuration  5-11
Default Settings  5-11
Additional References  5-12
  Related Documents  5-12
  Standards  5-12
Feature History for System Message Logging  5-12

CHAPTER 6

Configuring Smart Call Home  6-1
Information About Call Home  6-1
  Call Home Overview  6-2
  Destination Profiles  6-2
  Call Home Alert Groups  6-3
  Call Home Message Urgency Levels  6-5
  Obtaining Smart Call Home  6-6
  Distributing Call Home Using CFS  6-7
  Database Merge Guidelines  6-7
  High Availability  6-7
  Virtualization Support  6-7
Licensing Requirements for Call Home  6-8
Prerequisites for Call Home  6-8
Guidelines and Limitations  6-8
Configuring Call Home  6-8
  Configuring Contact Information  6-9
  Creating a Destination Profile  6-11
  Modifying a Destination Profile  6-13
  Associating an Alert Group and a Destination Profile  6-15
  Adding show Commands to an Alert Group  6-16
### Configuring E-Mail  6-18
### Configuring Periodic Inventory Notifications  6-19
### Disabling Duplicate Message Throttle  6-20
### Enabling or Disabling Call Home  6-21
### Testing Call Home Communications  6-21

### Verifying Call Home Configuration  6-22
### Call Home Example Configuration  6-22
### Default Settings  6-23
### Additional References  6-23
  - Event Triggers  6-23
  - Message Formats  6-25
  - Sample syslog Alert Notification in Full-Text Format  6-28
  - Sample syslog Alert Notification in XML Format  6-31
### Related Documents  6-35
### Standards  6-35
### MIBs  6-35

### Feature History for Smart Call Home  6-35

### CHAPTER  7
### Configuring Rollback  7-1
### Information About Rollback  7-1
  - Rollback Overview  7-1
  - Automatically Generated System Checkpoints  7-2
  - High Availability  7-2
  - Virtualization Support  7-3
### Licensing Requirements  7-3
### Prerequisites for Rollback  7-3
### Guidelines and Limitations  7-3
### Configuring Rollback  7-4
  - Creating a Checkpoint  7-4
  - Implementing a Rollback  7-5
### Verifying the Rollback Configuration  7-6
### Rollback Example Configuration  7-7
### Default Settings  7-7
### Additional References  7-7
  - Related Documents  7-8
  - Standards  7-8
### Feature History for Rollback  7-8
 CHAPTER 8
Configuring Session Manager 8-1
Information About Session Manager 8-1
Session Manager Overview 8-1
High Availability 8-2
Virtualization Support 8-2
Licensing Requirements for Session Manager 8-2
Prerequisites for Session Manager 8-2
Guidelines and Limitations 8-2
Configuring Session Manager 8-3
Creating a Session 8-3
Configuring ACLs in a Session 8-4
Verifying a Session 8-5
Committing a Session 8-5
Saving a Session 8-5
Discarding a Session 8-6
Verifying the Session Manager Configuration 8-6
Session Manager Example Configuration 8-6
Additional References 8-7
  Related Documents 8-7
  Standards 8-7

 CHAPTER 9
Configuring the Scheduler 9-1
Information About the Scheduler 9-1
Scheduler Overview 9-2
Remote User Authentication 9-2
Logs 9-2
High Availability 9-2
Virtualization Support 9-2
Licensing Requirements for the Scheduler 9-3
Prerequisites for the Scheduler 9-3
Guidelines and Limitations 9-3
Configuring the Scheduler 9-3
  Enabling the Scheduler 9-4
  Defining the Scheduler Log File Size 9-5
  Configuring Remote User Authentication 9-5
  Defining a Job 9-6
  Deleting a Job 9-7
  Defining a Timetable 9-8
Send document comments to nexus7k-docfeedback@cisco.com.

Clearing the Scheduler Log File 9-10
Disabling the Scheduler 9-11
Verifying the Scheduler Configuration 9-12
Scheduler Example Configurations 9-12
  Creating a Scheduler Job 9-13
  Scheduling a Scheduler Job 9-13
  Displaying the Job Schedule 9-13
  Displaying the Results of Running Scheduler Jobs 9-13
Default Settings 9-14
Additional References 9-14
  Related Documents 9-14
  Standards 9-15

CHAPTER 10 Configuring SNMP 10-1
Information About SNMP 10-1
  SNMP Functional Overview 10-2
  SNMP Notifications 10-2
  SNMPv3 10-2
  SNMP and Embedded Event Manager 10-5
  Multiple Instance Support 10-5
  High Availability 10-6
  Virtualization Support 10-6
Licensing Requirements for SNMP 10-6
Prerequisites for SNMP 10-6
Guidelines and Limitations 10-7
Configuring SNMP 10-7
  Configuring SNMP Users 10-7
  Enforcing SNMP Message Encryption 10-8
  Assigning SNMPv3 Users to Multiple Roles 10-9
  Creating SNMP Communities 10-9
  Filtering SNMP Requests 10-10
  Configuring SNMP Notification Receivers 10-10
  Configuring a Source Interface for SNMP Notifications 10-11
  Configuring the Notification Target User 10-12
  Configuring SNMP Notification Receivers with VRFs 10-12
  Configuring SNMP to Send Traps Using an Inband Port 10-13
  Enabling SNMP Notifications 10-15
  Disabling LinkUp/LinkDown Notifications on an Interface 10-17
  Displaying SNMP ifIndex for an Interface 10-18
Send document comments to nexus7k-docfeedback@cisco.com.

CHAPTER 15
Configuring Onboard Failure Logging
  Feature History for SPAN 14-18

Information About OBFL 15-1
  OBFL Overview 15-1
  Virtualization Support 15-2
Licensing Requirements for OBFL 15-2
Prerequisites for OBFL 15-2
Guidelines and Limitations 15-2
Configuring OBFL 15-3
Verifying the OBFL Configuration 15-6
OBFL Example Configuration 15-7
Default Settings 15-7
Additional References 15-7
  Related Documents 15-8
  Standards 15-8

CHAPTER 16
Configuring NetFlow 16-1

Information About NetFlow 16-1
  NetFlow Overview 16-1
  High Availability 16-3
  Virtualization Support 16-4
Licensing Requirements for NetFlow 16-4
Prerequisites for NetFlow 16-4
Guidelines and Limitations 16-4
Configuring NetFlow 16-5
  Enabling the NetFlow Feature 16-5
  Creating a Flow Record 16-6
  Creating a Flow Exporter 16-9
  Creating a Flow Monitor 16-11
  Creating a Sampler 16-12
  Applying a Flow to an Interface 16-13
  Configuring Bridged NetFlow on a VLAN 16-14
  Configuring Layer 2 NetFlow 16-15
  Configuring NetFlow Timeouts 16-17
Verifying NetFlow Configuration 16-18
Monitoring NetFlow 16-18
New and Changed Information

This chapter provides release-specific information for each new and changed feature in the Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.x. The latest version of this document is available at the following Cisco website:


To check for additional information about Cisco NX-OS Release 4.2, see the Cisco NX-OS Release Notes available at the following Cisco website:


Table 1 summarizes the new and changed features for the Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.x, and tells you where they are documented.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Changed in Release</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory thresholds</td>
<td>Changed the minor, severe, and critical default memory thresholds from 70, 80, and 90 to 85, 90, and 95.</td>
<td>4.2(4)</td>
<td>Chapter 13, “Configuring Memory Thresholds”</td>
</tr>
<tr>
<td>CDP support for VTP domain name</td>
<td>CDP advertises the VLAN Trunking Protocol (VTP) type-length-value field (TLV) in CDP version-2 packets.</td>
<td>4.2(1)</td>
<td>Chapter 4, “VTP Feature Support”</td>
</tr>
<tr>
<td>CFS Distribution for NTP</td>
<td>You can use Cisco Fabric Services (CFS) to distribute an NTP configuration to all CFS-enabled switches in the network.</td>
<td>4.2(1)</td>
<td>Chapter 3, “Distributing NTP Using CFS”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Chapter 2, “Enabling CFS to Distribute NTP Configurations”</td>
</tr>
<tr>
<td>Automatically generated system checkpoints</td>
<td>The software automatically generates a system checkpoint when disabling a feature or Layer 3 protocol, or license expiration could cause loss of configuration information.</td>
<td>4.2(1)</td>
<td>Chapter 7, “Automatically Generated System Checkpoints”</td>
</tr>
<tr>
<td>Checkpoints and rollback</td>
<td>The checkpoint and rollback features now provide full support for high availability.</td>
<td>4.2(1)</td>
<td>Chapter 7, “High Availability.”</td>
</tr>
<tr>
<td>Filter SNMP requests by community using an ACL</td>
<td>You can assign an ACL to an SNMP community to filter SNMP requests</td>
<td>4.2(1)</td>
<td>Chapter 10, “Filtering SNMP Requests”</td>
</tr>
</tbody>
</table>
**Table 1  New and Changed Features for Release 4.2 (continued)**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Changed in Release</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 support</td>
<td>Supports configuring IPv6 SNMP hosts.</td>
<td>4.2(1)</td>
<td>Chapter 10, “Configuring SNMP”</td>
</tr>
<tr>
<td>SNMP notifications added</td>
<td>The <code>snmp-server enable traps</code> command is added. The <code>snmp-server enable traps</code> &lt;br&gt; <code>trap-arg-scope-global</code> command is added.</td>
<td>4.2(1)</td>
<td>Chapter 10, “Enabling SNMP Notifications”</td>
</tr>
<tr>
<td>Use interfaces for SNMP</td>
<td>You can use the <code>snmp-server host</code> &lt;br&gt; <code>source-interface</code> command to assign a host on an interface. You can use the <code>snmp-server source-interface</code> command to designate an interface to receive SNMP notifications.</td>
<td>4.2(1)</td>
<td>Chapter 10, “Configuring SNMP Notification Receivers”</td>
</tr>
<tr>
<td>Diagnostics PortLoopback and St</td>
<td>StandbyFabricLoopback now included PortLoopback (test ID 5) and StandbyFabricLoopback (test ID 16).</td>
<td>4.2(1)</td>
<td>Chapter 12, “Runtime or Health Monitoring Diagnostics”</td>
</tr>
<tr>
<td>EEM events</td>
<td>You can use the <code>event module status</code> command to trigger an event when module status varies between online and offline. You can use the <code>event sysmgr memory</code> command to trigger an event. You can use the <code>event sysmgr switchover</code> command to trigger an event.</td>
<td>4.2(1)</td>
<td>Chapter 13, “Configuring Event Statements”</td>
</tr>
<tr>
<td>Layer 2 NetFlow</td>
<td>You can define Layer 2 keys in flexible NetFlow records that you can use to capture flows in Layer 2 interfaces.</td>
<td>4.2(1)</td>
<td>Chapter 16, “Guidelines and Limitations”&lt;br&gt; Chapter 16, “Configuring Layer 2 NetFlow”</td>
</tr>
<tr>
<td>CFS</td>
<td>Corrected examples in TACACS+ configuration.</td>
<td>4.1(4)</td>
<td>Chapter 2, “Enabling CFS to Distribute TACACS+ Configurations”</td>
</tr>
<tr>
<td>Rollback</td>
<td>Added the following note: &lt;br&gt;Note: If you make a configuration change during atomic rollback, the rollback will fail.</td>
<td>4.1(4)</td>
<td>Chapter 7, “Implementing a Rollback”</td>
</tr>
<tr>
<td>Call Home</td>
<td>Added new commands to support HTTP and HTTPS: &lt;br&gt; <code>destination_profile http</code> and <code>destination_profile transport-method</code>. &lt;br&gt;Note: These command are not distributable with CFS. As a workaround, enter these commands after the <code>commit</code> command.</td>
<td>4.1(3)</td>
<td>Chapter 6, “Modifying a Destination Profile”</td>
</tr>
<tr>
<td>Call Home</td>
<td>Updated the Prerequisites and Guidelines and Limitations sections.</td>
<td>4.1(3)</td>
<td>Chapter 6, “Prerequisites for Call Home”&lt;br&gt; Chapter 6, “Guidelines and Limitations”</td>
</tr>
</tbody>
</table>

Note: The changes listed above apply to the Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.x.
### New and Changed Features for Release 4.2 (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Changed in Release</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rollback</td>
<td>Rollback fails for NetFlow if during rollback, you try to modify a record that is programmed in the hardware. Rollback is not supported for checkpoints across software versions.</td>
<td>4.1(3)</td>
<td>Chapter 7, “Guidelines and Limitations”</td>
</tr>
</tbody>
</table>
| Rollback | The default rollback type is atomic. | 4.1(3) | Chapter 7, “Rollback Overview”  
Chapter 7, “Implementing a Rollback” |
| EEM | Added a configuration section for memory thresholds.  
Added a table of system policies. | 4.1(3) | Chapter 13, “Configuring Memory Thresholds”  
“Embedded Event Manager System Events and Configuration Examples” |
| SPAN | Added a table of SPAN session limits. | 4.1(3) | Chapter 14, “Guidelines and Limitations” |
| NetFlow | Rollback fails for NetFlow if during rollback, you try to modify a record that is programmed in the hardware. | 4.1(3) | Chapter 16, “Guidelines and Limitations” |
| CFS | Cisco Fabric Services (CFS) distributes data, including configuration changes, to all Cisco NX-OS devices in a network. | 4.1(2) | Chapter 2, “Configuring CFS Distribution” |
| SPAN | Cisco Ethernet switched port analyzer (SPAN) destinations are enhanced to support intrusion detection by allowing the following:  
• Injecting packets to disrupt a TCP packet stream.  
• Enabling a forwarding engine to learn the MAC address of the IDS. | 4.1(2) | Chapter 14, “Configuring SPAN” |
Send document comments to nexus7k-docfeedback@cisco.com.
Preface

This preface describes the audience, organization and conventions of the Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.x. It also provides information on how to obtain related documentation.

This chapter includes the following sections:
- Audience, page xix
- Document Organization, page xix
- Document Conventions, page xx
- Related Documentation, page xxi
- Obtaining Documentation and Submitting a Service Request, page xxii

Audience

This publication is for experienced network administrators who configure and maintain Cisco NX-OS devices.

Document Organization

This document is organized into the following chapters:

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1, “Overview”</td>
<td>Provides an overview of the features in this document.</td>
</tr>
<tr>
<td>Chapter 2, “Configuring CFS”</td>
<td>Describes how to use Cisco Fabric Services (CFS) to distribute data, including configuration changes, to all Cisco NX-OS devices in a network.</td>
</tr>
<tr>
<td>Chapter 3, “Configuring NTP”</td>
<td>Describes how to configure the Network Time Protocol (NTP).</td>
</tr>
<tr>
<td>Chapter 4, “Configuring CDP”</td>
<td>Describes how to configure the Cisco Discovery Protocol (CDP).</td>
</tr>
<tr>
<td>Chapter 5, “Configuring System Message Logging”</td>
<td>Describes how to configure logging for system messages.</td>
</tr>
</tbody>
</table>
Send document comments to nexus7k-docfeedback@cisco.com.

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 6, “Configuring Smart Call Home”</td>
<td>Describes how to configure the smart Call Home feature for e-mail-based notification of critical system policies.</td>
</tr>
<tr>
<td>Chapter 7, “Configuring Rollback”</td>
<td>Describes how to create configuration snapshots with the rollback feature and how to apply commands in batch mode with the Session Manager.</td>
</tr>
<tr>
<td>Chapter 8, “Configuring Session Manager”</td>
<td>Describes how to apply commands in batch mode with the Session Manager.</td>
</tr>
<tr>
<td>Chapter 9, “Configuring the Scheduler”</td>
<td>Describes how to schedule batch configuration jobs.</td>
</tr>
<tr>
<td>Chapter 10, “Configuring SNMP”</td>
<td>Describes how to configure SNMP and enable SNMP notifications.</td>
</tr>
<tr>
<td>Chapter 11, “Configuring RMON”</td>
<td>Describes how to monitor the device by configuring RMON alarms and events.</td>
</tr>
<tr>
<td>Chapter 12, “Configuring Online Diagnostics”</td>
<td>Describes how to configure online diagnostics to monitor the software and hardware.</td>
</tr>
<tr>
<td>Chapter 13, “Configuring the Embedded Event Manager”</td>
<td>Describes how to configure the Embedded Event Manager.</td>
</tr>
<tr>
<td>Chapter 15, “Configuring Onboard Failure Logging”</td>
<td>Describes how to configure on-board failure logging to log failure data to persistent storage.</td>
</tr>
<tr>
<td>Chapter 14, “Configuring SPAN”</td>
<td>Describes how to configure SPAN to monitor traffic into and out of a port.</td>
</tr>
<tr>
<td>Chapter 16, “Configuring NetFlow”</td>
<td>Describes how to configure NetFlow to gather statistics on input and output traffic.</td>
</tr>
<tr>
<td>Appendix A, “IETF RFCs supported by Cisco NX-OS System Management”</td>
<td>Lists supported IETF RFCs.</td>
</tr>
<tr>
<td>Appendix B, “Embedded Event Manager System Events and Configuration Examples”</td>
<td>Lists the EEM system policies.</td>
</tr>
</tbody>
</table>

**Document Conventions**

Command descriptions use these conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface font</strong></td>
<td>Commands and keywords are in boldface.</td>
</tr>
<tr>
<td><em>italic font</em></td>
<td>Arguments for which you supply values are in italics.</td>
</tr>
<tr>
<td>[   ]</td>
<td>Elements in square brackets are optional.</td>
</tr>
<tr>
<td>[ x</td>
<td>y</td>
</tr>
<tr>
<td>string</td>
<td>A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.</td>
</tr>
</tbody>
</table>
Screen examples use these conventions:

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

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

Cisco NX-OS includes the following documents:

**Release Notes**

Cisco Nexus 7000 Series NX-OS Release Notes, Release 4.2

**NX-OS Configuration Guides**

Cisco Nexus 7000 Series NX-OS Getting Started with Virtual Device Contexts
Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 4.x
Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 4.x
Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 4.x
Cisco Nexus 7000 Series NX-OS Quality of Service Configuration Guide, Release 4.x
Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 4.x
Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide, Release 4.x
Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.x
Cisco Nexus 7000 Series NX-OS Software Upgrade and Downgrade Guide, Release 4.x
Cisco NX-OS Licensing Guide
Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide
Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.x
Send document comments to nexus7k-docfeedback@cisco.com.

Cisco NX-OS System Messages Reference
Cisco Nexus 7000 Series NX-OS MIB Quick Reference

Cisco Nexus 7000 Series NX-OS Command Reference Master Index
Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference
Cisco Nexus 7000 Series NX-OS Interfaces Command Reference
Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference
Cisco Nexus 7000 Series NX-OS Quality of Service Command Reference
Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference
Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference
Cisco Nexus 7000 Series NX-OS Security Command Reference
Cisco Nexus 7000 Series NX-OS Virtual Device Context Command Reference
Cisco Nexus 7000 Series NX-OS System Management Command Reference

Other Software Document
Cisco Nexus 7000 Series NX-OS Troubleshooting Guide

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:

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.
Overview

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

This chapter includes the following sections:

- Cisco NX-OS Device Configuration Methods, page 1-1
- Cisco Fabric Services, page 1-3
- Network Time Protocol, page 1-3
- Cisco Discovery Protocol, page 1-3
- System Messages, page 1-4
- Call Home, page 1-4
- Rollback, page 1-4
- Session Manager, page 1-4
- Scheduler, page 1-5
- SNMP, page 1-5
- RMON, page 1-5
- Online Diagnostics, page 1-5
- Embedded Event Manager, page 1-5
- On-Board Failure Logging, page 1-6
- SPAN, page 1-6
- NetFlow, page 1-6
- Troubleshooting Features, page 1-6

Cisco NX-OS Device Configuration Methods

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

Figure 1-1 shows the device configuration methods available to a network user.
Table 1-1 lists the configuration method and the document where you can find more information.

<table>
<thead>
<tr>
<th>Configuration Method</th>
<th>Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLI from SSH¹, Telnet session or console port</td>
<td>Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 4.x</td>
</tr>
<tr>
<td>DCNM client</td>
<td>Cisco DCNM Fundamentals Configuration Guide, Release 4.2</td>
</tr>
<tr>
<td>User-defined GUI</td>
<td>Cisco DCNM Web Services API Guide, Release 4.2</td>
</tr>
</tbody>
</table>

¹. Secure shell (SSH).

This section includes the following topics:
- Configuring with CLI or XML Management Interface, page 1-3
- Configuring with DCNM or a Custom GUI, page 1-3
Configuring with CLI or XML Management Interface

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

- CLI from an SSH session, a Telnet Session, or the Console Port—You can configure devices using the CLI from an SSH session, a Telnet session, or the console port. SSH provides a secure connection to the device. For more information, see the Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 4.x.
- XML Management Interface over SSH—You can configure devices using the XML management interface, which is a programmatic method based on the NETCONF protocol that complements the CLI functionality. For more information, see the Cisco NX-OS XML Management Interface User Guide.

Configuring with DCNM or a Custom GUI

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

- DCNM Client—You can configure devices using the DCNM client, which runs on your local PC and uses web services on the DCNM server. The DCNM server configures the device over the XML management interface. For more information about the DCNM client, see the Cisco DCNM Fundamentals Configuration Guide.
- Custom GUI—You can create your own GUI to configure devices using the DCNM web services application program interface (API) on the DCNM server. You use the SOAP protocol to exchange XML-based configuration messages with the DCNM server. The DCNM server configures the device over the XML management interface. For more information about creating custom GUIs, see the Cisco DCNM Web Services API Guide, Release 4.2.

Cisco Fabric Services

Cisco Fabric Services (CFS) is a Cisco proprietary feature that distributes data, including configuration changes, to all Cisco NX-OS devices in a network. For more information about CFS, see Chapter 2, “Configuring CFS.”

Network Time Protocol

The Network Time Protocol (NTP) synchronizes the time of day among a set of distributed time servers and clients so that you can correlate time-specific information, such as system logs, received from the devices in your network. For more information about NTP, see Chapter 3, “Configuring NTP.”

Cisco Discovery Protocol

You can use the Cisco Discovery Protocol (CDP) to discover and view information about all Cisco equipment that is directly attached to your device. CDP runs on all Cisco-manufactured equipment including routers, bridges, access and communication servers, and switches. CDP is media and protocol independent, and gathers the protocol addresses of neighboring devices, discovering the platform of
those devices. CDP runs over the data link layer only. Two systems that support different Layer 3 protocols can learn about each other. For more information about CDP, see Chapter 4, “Configuring CDP.”

**System Messages**

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

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

For information about configuring system messages, see Chapter 5, “Configuring System Message Logging.”

**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.

For information about configuring Call Home, see Chapter 6, “Configuring Smart Call Home.”

**Rollback**

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

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

For more information, see the Chapter 7, “Configuring Rollback.”

**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.

For more information, see the Chapter 8, “Configuring Session Manager.”
Scheduler

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

For more information, see Chapter 9, “Configuring the Scheduler.”

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.

For more information, see Chapter 10, “Configuring SNMP.”

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.

For more information, see Chapter 11, “Configuring RMON.”

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.

For information about configuring online diagnostics, see Chapter 12, “Configuring Online Diagnostics.”

Embedded Event Manager

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

For information about configuring EEM, see Chapter 13, “Configuring the Embedded Event Manager.”
SPAN

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

For information about configuring SPAN, see Chapter 14, “Configuring SPAN.”

On-Board Failure Logging

You can configure a device to log failure data to persistent storage, which you can retrieve and display for analysis at a later time. This on-board failure logging (OBFL) feature stores failure and environmental information in nonvolatile memory on the module. This information is useful for analysis of failed modules. For information about configuring OBFL, see Chapter 15, “Configuring Onboard Failure Logging.”

NetFlow

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

For information about configuring NetFlow, see Chapter 16, “Configuring NetFlow.”

Troubleshooting Features

Cisco NX-OS provides troubleshooting tools such as ping, traceroute, Ethanalyzer, and the Blue Beacon feature. See the Cisco Nexus 7000 Series NX-OS Troubleshooting Guide for details on these features.

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

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

For information on collecting and using the generated information relating to service failures, see the Cisco Nexus 7000 Series NX-OS Troubleshooting Guide.
Configuring CFS

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

This chapter includes the following sections:

- Information About CFS, page 2-1
- Licensing Requirements for CFS, page 2-4
- Prerequisites for CFS, page 2-4
- Guidelines and Limitations, page 2-4
- Configuring CFS Distribution, page 2-5
- Verifying the CFS Configuration, page 2-23
- Default Settings, page 2-23
- Additional References, page 2-23
- Feature History for CFS, page 2-24

Information About CFS

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

This section includes the following topics:

- Merging Application Databases, page 2-2
- Applications that Use CFS to Distribute Configuration Changes, page 2-2
- CFS Distribution, page 2-2
- CFS Regions, page 2-3
- High Availability, page 2-3
- Virtualization Support, page 2-3
Merging Application Databases

When a new device is detected in your network, CFS manages the merging, or synchronizing, of its configuration with that of the other devices. CFS also coordinates and minimizes the number of merges by designating one device to manage merges per application per region. The other devices do not play any role in the merge process.

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

If the merger is successful, the merged database is distributed to all devices in the combined fabric and the entire new fabric emerges in a consistent state. You can recover from a merge failure by starting a distribution from any device in the new fabric. This distribution restores all peers in the fabric to the same configuration database.

Applications that Use CFS to Distribute Configuration Changes

CFS distributes configuration changes for the applications shown in Table 2-2.

**Table 2-1 CFS-Supported Applications**

<table>
<thead>
<tr>
<th>Application</th>
<th>Default state</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS</td>
<td>Disabled</td>
</tr>
<tr>
<td>TACACS+</td>
<td>Disabled</td>
</tr>
<tr>
<td>User and administrator roles</td>
<td>Disabled</td>
</tr>
<tr>
<td>Call Home</td>
<td>Disabled</td>
</tr>
<tr>
<td>NTP</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

CFS Distribution

CFS distributes configuration changes to multiple devices in a defined region or across a complete network.

The following steps provide an overview of how CFS distributes application configurations.

1. You enable CFS to distribute configurations for an application, such as Call Home.
2. You enter a command to change the configuration for a CFS application, such as Call Home.
3. CFS checks if an active fabric lock indicates that a configuration change is already in progress for this application.

**Note**

Only one CFS session for an application can be active at a time. CFS uses locks to enforce this restriction. Distribution is not allowed to start if locks are in place for the application anywhere else in the fabric.
4. One of the following occurs:
   – If an active fabric lock exists for this application, CFS rejects the command. No changes are
     permitted until the existing fabric lock is released.
   – If there is not an active fabric lock for this application, then CFS starts a session and locks the
     fabric for this application.

5. You enter the remaining configuration commands for the application.

6. You commit the configuration by using the `commit` command.

7. CFS distributes the configuration and releases the lock.

**CFS Regions**

A CFS region is a user-defined subset of devices for a given feature or application. You will usually
define regions to localize or restrict distribution based on devices that are close to one another.

When a network covers many geographies with many different administrators who are responsible for
subsets of devices, you can manage the physical scope of an application by setting up a CFS region.

CFS regions are identified by numbers 0 through 200. Region 0 is the default region. You can configure
region number 1 through 200.

**Note**

If a feature is moved, that is, assigned to a new region, its scope is restricted to that region and it ignores
all other regions for distribution or merging purposes.

You can set up a CFS region to distribute configurations for multiple features. However, on a given
device, 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.

**Note**

The default region is used to distribute changes to all devices in a fabric. Region 0 is reserved as the
default region and contains every device in the fabric. If you remove an application from a region and
do not assign it to a different region, it is added to the default region (region 0).

**High Availability**

Stateless restarts are supported for CFS. After a reboot or a supervisor switchover, the running
configuration is applied. For more information on high availability, see the Cisco Nexus 7000 Series
NX-OS High Availability and Redundancy Guide.

**Virtualization Support**

CFS is configured per VDC.

When you access Cisco NX-OS, it places you in the default VDC unless you specify a different VDC.
For more information on VDCs, see the Cisco Nexus 7000 Series NX-OS Virtual Device Context
Licensing Requirements for CFS

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

Prerequisites for CFS

CFS has the following prerequisites:

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

Guidelines and Limitations

CFS has the following configuration guidelines and limitations:

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

Caution: CFS over Ethernet must be enabled for the vPC feature to work.

- CFS distributions for application data use directed unicast.
- All CFS over IP enabled devices with similar multicast addresses form one CFS over IP fabric.
- Make sure that CFS is enabled for the applications you want to configure. For detailed information, see the “Enabling CFS Distribution for Applications” procedure on page 2-5.
- Any time you lock a fabric, your username is remembered across restarts and switchovers.
- Any time you lock a fabric, configuration changes attempted by anyone else are rejected.
- While a fabric is locked, the application holds a working copy of configuration changes in a pending database or temporary storage area—not in the running configuration.
- Configuration changes that have not been committed yet (still saved as a working copy) are not in the running configuration and do not display in the output of `show` commands.
- The working copy overwrites the running configuration when you commit the changes.
- If you start a CFS session that requires a fabric lock but forget to end the session, an administrator can clear the session. For more information, see the “Clearing a Locked Session” procedure on page 2-19.
- CFSoIP and CFSoE are not supported for use together.
- CFS regions can be applied only to CFSoIP and CFSoFC clients.
An empty commit is allowed if configuration changes are not previously made. In this case, the commit command results in a session that acquires locks and distributes the current database.

You can only use the commit command on the specific device where the fabric lock was acquired.

### Configuring CFS Distribution

This section describes how to configure CFS and includes the following topics:

- Enabling CFS Distribution for Applications, page 2-5
- Specifying a CFS Distribution Mode, page 2-10
- Configuring an IP Multicast Address for CFS Over IP, page 2-11
- Configuring CFS Regions, page 2-12
- Creating and Distributing a CFS Configuration, page 2-18
- Discarding a Configuration, page 2-20
- Disabling CFS Distribution Globally, page 2-21

### Enabling CFS Distribution for Applications

This section includes the following topics:

- Enabling CFS to Distribute Call Home Configurations, page 2-5
- Enabling CFS to Distribute RADIUS Configurations, page 2-6
- Enabling CFS to Distribute TACACS+ Configurations, page 2-7
- Enabling CFS to Distribute Role Configurations, page 2-8
- Enabling CFS to Distribute NTP Configurations, page 2-9

*Note* See the *Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 4.x* for more information on CFS for RADIUS, TACACS+, and roles. See Chapter 6, “Configuring Smart Call Home” for more information on Call Home, and see Chapter 3, “Configuring NTP” for more information on NTP.

### Enabling CFS to Distribute Call Home Configurations

You can enable CFS to distribute Call Home configurations.

**BEFORE YOU BEGIN**

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

**SUMMARY STEPS**

1. `config t`
2. `callhome`
3. `distribute`
4. **show application_name status**  
5. **copy running-config startup-config**

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>config t</td>
<td>Places you in global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
|      | switch# config t  
|      | switch(config)# |
| 2    | switch(config)# callhome | Places you in callhome configuration mode. |
|      | Example:  
|      | switch(config)# callhome  
|      | switch(config-callhome)# |
| 3    | switch(config)# distribute | Enables CFS to distribute Call Home configuration updates. |
|      | Example:  
|      | switch(config-callhome)# distribute  
|      | switch(config-callhome)# |
| 4    | **show application_name status** | (Optional) For the specified application, displays the CFS distribution status. |
|      | Example:  
|      | switch(config-callhome)# show callhome status |
| 5    | **copy running-config startup-config** | (Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration. |
|      | Example:  
|      | switch(config)# copy running-config startup-config |

This example shows how to enable CFS to distribute Call Home configurations:

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

**Enabling CFS to Distribute RADIUS Configurations**

You can enable CFS to distribute RADIUS configurations.

**BEFORE YOU BEGIN**

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

**SUMMARY STEPS**

1. **config t**  
2. **radius distribute**
Chapter 2      Configuring CFS

Send document comments to nexus7k-docfeedback@cisco.com.

3. show radius status
4. copy running-config startup-config

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 config t</td>
<td>Places you in global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# config t</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td>Step 2 switch(config)# radius distribute</td>
<td>For the specified application, enables the device to receive configuration updates that are distributed through CFS.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# radius distribute</td>
<td></td>
</tr>
<tr>
<td>Step 3 show radius status</td>
<td>(Optional) For the specified application, displays the CFS distribution status.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# show radius status</td>
<td></td>
</tr>
<tr>
<td>Step 4 copy running-config startup-config</td>
<td>(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

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

```
switch(config)# radius distribute
switch(config)# show radius status
Distribution : Enabled
```

```
[########################################] 100%
```

Enabling CFS to Distribute TACACS+ Configurations

You can enable CFS to distribute TACACS+ configurations.

BEFORE YOU BEGIN

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

SUMMARY STEPS

1. config t
2. tacacs+ distribute
3. show tacacs+ status
4. copy running-config startup-config
Send document comments to nexus7k-docfeedback@cisco.com.

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> config t</td>
<td>Places you in global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# config t</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> switch(config)# tacacs+ distribute</td>
<td>Enables CFS to distribute configuration updates for TACACS+.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# tacacs+ distribute</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> show tacacs+ status</td>
<td>(Optional) Displays the CFS distribution status for TACACS+.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# show tacacs+ status</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> copy running-config startup-config</td>
<td>(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

This example shows how to enable CFS to distribute TACACS+ configurations:
```
switch(config)# tacacs+ distribute
switch(config)# show tacacs+ status
Distribution : Enabled
Last operational state: No session
switch(config)# copy running-config startup-config
[################################################] 100%
```

**Enabling CFS to Distribute Role Configurations**

You can enable CFS to distribute role configurations.

**BEFORE YOU BEGIN**

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

**SUMMARY STEPS**

1. config t
2. role distribute
3. show role status
4. copy running-config startup-config
Chapter 2  Configuring CFS

Configuring CFS Distribution

Send document comments to nexus7k-docfeedback@cisco.com.

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>config t</td>
</tr>
<tr>
<td>Example:</td>
<td>switch# config t</td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>switch(config)# role distribute</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# role distribute</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>show role status</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# show role status</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>copy running-config startup-config</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# copy running-config startup-config</td>
</tr>
</tbody>
</table>

This example shows how to enable CFS to distribute Call Home configurations:

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

**Enabling CFS to Distribute NTP Configurations**

You can enable CFS to distribute NTP configurations.

**BEFORE YOU BEGIN**

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

**SUMMARY STEPS**

1. config t
2. ntp distribute
3. show application_name status
4. copy running-config startup-config
DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>config t</code></td>
<td>Places you in global configuration mode.</td>
</tr>
</tbody>
</table>
|      | **Example:**  
|      | `switch# config t`  
|      | `switch(config)#` | |
| 2    | `ntp distribute` | Enables CFS to distribute NTP configuration updates. |
|      | **Example:**  
|      | `switch(config)# ntp distribute` | |
| 3    | `show application_name status` | (Optional) For the specified application, displays the CFS distribution status. |
|      | **Example:**  
|      | `switch(config)# show ntp status` | |
| 4    | `copy running-config startup-config` | (Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration. |
|      | **Example:**  
|      | `switch(config)# copy running-config startup-config` | |

This example shows how to enable CFS to distribute Call Home configurations:

```
switch(config)# ntp distribute  
switch(config)# show ntp status  
Distribution: Enabled  
[########################################] 100%
```

### Specifying a CFS Distribution Mode

You can specify and enable a CFS distribution mode (Ethernet or IPv4).

**BEFORE YOU BEGIN**

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

**SUMMARY STEPS**

1. `config t`
2. `cfs [eth | ipv4] distribute`
3. `show cfs status`
4. `copy running-config startup-config`
## Configuring an IP Multicast Address for CFS Over IP

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

You can configure the IP multicast address used to distribute CFS over IP for either of the following:

- IPv4—The default IPv4 multicast address is 239.255.70.83.

### BEFORE YOU BEGIN

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

You must disable CFS IP distribution before changing the multicast address.

### SUMMARY STEPS

1. `config t`
2. `no cfs [ipv4] distribute`
3. `cfs [ipv4] mcast-address ip_address`
Chapter 2  Configuring CFS

Send document comments to nexus7k-docfeedback@cisco.com.

4.  show cfs status
5.  copy running-config startup-config

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>config t</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch# config t Enter configuration commands, one per line. End with CNTL/Z. switch(config)#</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Places you in global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>no cfs [ipv4] distribute</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config)# no cfs ipv4 distribute This will prevent CFS from distributing over IPv4 network. Are you sure? [y/n] [n] y switch(config)#</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Globally disables CFS over IP distribution for all applications on the device.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>CFS over IP must be disabled before you can change the multicast address.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>cfs [ipv4] mcast-address ip_address</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config)# cfs ipv4 mcast-address 239.255.1.1 Distribution over this IP type will be affected Change multicast address for CFS-IP? Are you sure? [y/n] [n] y</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Configures the multicast address for CFS distribution over IPv4. The ranges of valid IPv4 addresses are 239.255.0.0 through 239.255.255.255 and 239.192/16 through 239.251/16. The default IPv4 address is 239.255.70.83.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>show cfs status</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config)# show cfs status Distribution : Enabled Distribution over IP : Enabled - mode IPv4 IPv4 multicast address : 239.255.1.1 switch(config)#</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Shows the current state of CFS including whether it is enabled, its IP mode, and its multicast addresses. In this example, CFS is shown as being distributed over IPv4 on 239.255.1.1.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>copy running-config startup-config</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config)# copy running-config startup-config</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

Configuring CFS Regions

This section describes how to create and configure a CFS region and includes the following topics:
- Creating a CFS Region, page 2-13
- Moving an Application to a Different Region, page 2-14
- Removing an Application from a Region, page 2-15
- Deleting a CFS Region, page 2-16
Creating a CFS Region

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

BEFORE YOU BEGIN

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

SUMMARY STEPS

1. `config t`
2. `cfs region region_number`
3. `application_name`
4. `show cfs region brief`
5. `copy running-config startup-config`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>config t</code></td>
<td>Places you in global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>switch# config t</code></td>
<td>Enter configuration commands, one per line. End with CNTL/Z.</td>
</tr>
<tr>
<td><code>switch(config)#</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>cfs region region_number</code></td>
<td>Creates the region and places you into Configuration mode for the specified region.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>In this example, region 4 is created.</td>
</tr>
<tr>
<td><code>switch(config)# cfs region 4</code></td>
<td></td>
</tr>
<tr>
<td><code>switch(config-cfs-region)#</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>application_name</code></td>
<td>For the specified region, adds the named applications.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>switch(config-cfs-region)# callhome</code></td>
<td></td>
</tr>
<tr>
<td><code>switch(config-cfs-region)#</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>show cfs region brief</code></td>
<td>(Optional) Shows all configured regions and applications (does not show peers).</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>In this example, the Call Home application is shown in region 4.</td>
</tr>
<tr>
<td><code>switch(config-cfs-region)# show cfs region brief</code></td>
<td></td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Region</td>
<td>Application</td>
</tr>
<tr>
<td>4</td>
<td>callhome</td>
</tr>
<tr>
<td><code>switch(config-cfs-region)#</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> <code>copy running-config startup-config</code></td>
<td>(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>switch(config)# copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>
Moving an Application to a Different Region

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

**Note**

When an application is moved, its scope is restricted to the new region; it ignores all other regions for distribution or merging purposes.

**BEFORE YOU BEGIN**

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

**SUMMARY STEPS**

1. `config t`
2. `cfs region region_number`
3. `application_name`
4. `show cfs region`
5. `copy running-config startup-config`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>config t</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch# config t Enter configuration commands, one per line. End with CTRL/Z. switch(config)#</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>cfs region region_number</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config)# cfs region 2 switch(config-cfs-region)#</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>application_name</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config-cfs-region)# callhome switch(config-cfs-region)# radius</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>show cfs region name application_name</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config-cfs-region)# show cfs region name callhome</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>copy running-config startup-config</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config)# copy running-config startup-config</td>
</tr>
</tbody>
</table>
This example shows how to move the Call Home application to CFS region 2:

```
switch# config t
switch(config)# cfs region 2
switch(config-cfs-region)# callhome
switch(config-cfs-region)# show cfs region name callhome

Region-ID : 2
Application: callhome
Scope : Physical-fc-ip
-----------------------------------------------
Switch WWN                IP Address
-----------------------------------------------
  20:00:00:22:55:79:a4:c1 172.28.230.85           [Local]
```

Total number of entries = 1

```
switch(config-cfs-region)#
```

Removing an Application from a Region

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

BEFORE YOU BEGIN

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

SUMMARY STEPS

1. `config t`
2. `cfs region region_number`
3. `no application_name`
4. Repeat Step 3 for each application you want to remove from this region.
5. `show cfs region brief`
6. `copy running-config startup-config`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> config t</td>
<td>Places you in global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch# config t</td>
<td></td>
</tr>
<tr>
<td>Enter configuration commands, one per line. End with CNTL/Z.</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> cfs region region_number</td>
<td>Places you in Configuration mode for the specified region.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config)# cfs region 2</td>
<td></td>
</tr>
<tr>
<td>switch(config-cfs-region)#</td>
<td></td>
</tr>
</tbody>
</table>
Configuring CFS Distribution

Chapter 2  Configuring CFS

Send document comments to nexus7k-docfeedback@cisco.com.

### Configuring CFS Distribution

**Chapter 2: Configuring CFS**

#### Configuring CFS Distribution

**Before You Begin**

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

**Summary Steps**

1. `config t`
2. `no cfs region region_number`
3. `show cfs region brief`
4. `show cfs application name application-name`
5. `copy running-config startup-config`

**Deleting a CFS Region**

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

**Before You Begin**

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

**Summary Steps**

1. `config t`
2. `no cfs region region_number`
3. `show cfs region brief`
4. `show cfs application name application-name`
5. `copy running-config startup-config`

---

**Command | Purpose**
--- | ---
`Step 3` no application_name | Removes the specified application from the region.

**Example:**

```
switch(config-cfs-region)# no ntp
```

**Step 4** (Optional) Repeat Step 3 for each application you want to remove from this region.

**Step 5** `show cfs region brief`

**Example:**

```
switch(config-cfs-region)# show cfs region brief
```

```
<table>
<thead>
<tr>
<th>Region</th>
<th>Application</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>tacacs+</td>
<td>yes</td>
</tr>
<tr>
<td>6</td>
<td>radius</td>
<td>yes</td>
</tr>
</tbody>
</table>
```

**Step 6** `copy running-config startup-config` (Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

**Example:**

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

---

**Step 3**

---

**Step 4**

---

**Step 5**

---

**Step 6**

---
## Chapter 2  Configuring CFS

Send document comments to nexus7k-docfeedback@cisco.com.

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Places you in global configuration mode.</td>
</tr>
<tr>
<td>config t</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch# config t</td>
<td>Enter configuration commands, one per line. End with CNTL/Z.</td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Deletes the specified region after warning that this action causes all applications in the region to move to the default region. After deleting the region, you are returned to global configuration mode.</td>
</tr>
<tr>
<td>no cfs region region_number</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config)# no cfs region 4</td>
<td>WARNING: All applications in the region will be moved to default region. Are you sure? (y/n) [n]</td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Shows all configured regions and applications (does not show peers). In this example, region 4 is absent.</td>
</tr>
<tr>
<td>show cfs region brief</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config)# show cfs region brief</td>
<td></td>
</tr>
<tr>
<td>-----------------------------</td>
<td></td>
</tr>
<tr>
<td>Region</td>
<td>Application</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>6</td>
<td>radius</td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Shows local application information by name. In this case, the Call Home application is shown as now belonging to the default region.</td>
</tr>
<tr>
<td>show cfs application name application-name</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch# show cfs application name callhome</td>
<td></td>
</tr>
<tr>
<td>Enabled</td>
<td>: Yes</td>
</tr>
<tr>
<td>Timeout</td>
<td>: 20s</td>
</tr>
<tr>
<td>Merge Capable</td>
<td>: Yes</td>
</tr>
<tr>
<td>Scope</td>
<td>: Physical-fc-ip</td>
</tr>
<tr>
<td>Region</td>
<td>: Default</td>
</tr>
<tr>
<td>switch#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config)# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>
Creating and Distributing a CFS Configuration

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

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

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

BEFORE YOU BEGIN

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

SUMMARY STEPS

1. `config t`
2. `application_name`
3. `application_command`
4. Repeat Step 3 for each configuration command you want to make.
5. `show application_name status`
6. `commit`
7. `copy running-config startup-config`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>config t</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>switch# config t</code>&lt;br&gt;<code>switch(config)#</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>application_name</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>switch(config)# callhome</code>&lt;br&gt;<code>switch(config-callhome)#</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>application_command</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>switch(config-callhome)# email-contact admin@Mycompany.com</code></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>(Optional) Repeat Step 3 for each configuration command you want to make.</td>
</tr>
</tbody>
</table>
This example shows how to configure and distribute the contact information for Call Home:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# snmp-server contact personname@companyname.com
switch(config)# callhome
switch(config-callhome)# email-contact admin@Mycompany.com
switch(config-callhome)# phone-contact +1-800-123-4567
switch(config-callhome)# street-address 123 Anystreet st. Anytown,AnyWhere
switch(config-callhome)# commit
```

Clearing a Locked Session

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

You must have admin permissions to release a lock.

⚠️ Caution

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

BEFORE YOU BEGIN

Make sure that you are in the correct VDC. To change the VDC, use the `switchto vdc` command.
Chapter 2 Configuring CFS

Configuring CFS Distribution

Send document comments to nexus7k-docfeedback@cisco.com.

SUMMARY STEPS

1. `config t`
2. `show application_name status`
3. `clear application_name session`
4. `show application_name status`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> config t</td>
<td>Places you in global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# config t</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> show application_name status</td>
<td>Shows the current application state.</td>
</tr>
<tr>
<td>switch(config)# show ntp status</td>
<td></td>
</tr>
<tr>
<td>Distribution : Enabled</td>
<td>In this example, NTP is shown as locked.</td>
</tr>
<tr>
<td>Last operational state: Fabric Locked</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> clear application_name session</td>
<td>Clears the application configuration session and releases the lock on the fabric.</td>
</tr>
<tr>
<td>Example:</td>
<td>All pending changes are discarded.</td>
</tr>
<tr>
<td>switch# clear ntp session</td>
<td></td>
</tr>
<tr>
<td>switch#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> show application_name status</td>
<td>Shows the current application state.</td>
</tr>
<tr>
<td>Example:</td>
<td>This example shows that the lock is removed from the NTP application.</td>
</tr>
<tr>
<td>switch# show ntp status</td>
<td></td>
</tr>
<tr>
<td>Distribution : Enabled</td>
<td></td>
</tr>
<tr>
<td>Last operational state: No session</td>
<td></td>
</tr>
<tr>
<td>switch#</td>
<td></td>
</tr>
</tbody>
</table>

Discarding a Configuration

You can discard configuration changes and release the lock.

⚠️ Caution

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

BEFORE YOU BEGIN

Make sure that you are in the correct VDC. To change the VDC, use the `switchto vdc` command.
Disabling CFS Distribution Globally

You can disable CFS distribution for a device, isolating the applications using CFS from fabric-wide distributions while maintaining physical connectivity.

When CFS is globally disabled on a device, CFS operations are restricted to the device and all CFS commands continue to function as if the device were physically isolated.

BEFORE YOU BEGIN

Make sure that you are in the correct VDC. To change the VDC, use the switchto vdc command.
## Configuring CFS Distribution

Send document comments to nexus7k-docfeedback@cisco.com.

### SUMMARY STEPS

1. config t
2. no cfs distribute
3. show cfs status
4. copy running-config startup-config

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> config t</td>
<td>Places you in global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch# config t</td>
<td></td>
</tr>
<tr>
<td>Enter configuration commands, one per line.</td>
<td></td>
</tr>
<tr>
<td>End with CNTL/Z.</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> switch(config)# no cfs distribute</td>
<td>Globally disables CFS distribution for all applications on the device.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config)# no cfs distribute</td>
<td></td>
</tr>
<tr>
<td>This will prevent CFS from distributing the configuration to other switches.</td>
<td></td>
</tr>
<tr>
<td>Are you sure? (y/n) [n] y</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td>If the virtual port channel (vPC) feature is enabled, then only IP distribution is disabled. You must first disable vPC before you can disable CFS distribution.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> show cfs status</td>
<td>(Optional) Displays the global CFS distribution status (enabled/disabled) for the device.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config)# show cfs status</td>
<td></td>
</tr>
<tr>
<td>Distribution : Enabled</td>
<td></td>
</tr>
<tr>
<td>Distribution over IP : Disabled</td>
<td></td>
</tr>
<tr>
<td>IPv4 multicast address : 239.255.70.83</td>
<td></td>
</tr>
<tr>
<td>Distribution over Ethernet : Disabled</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> copy running-config startup-config</td>
<td>(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config)# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>
Verifying the CFS Configuration

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

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

Default Settings

Table 2-2 lists the default settings for CFS parameters.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFS distribution on the device</td>
<td>Enabled</td>
</tr>
<tr>
<td>CFS over IP</td>
<td>Disabled</td>
</tr>
<tr>
<td>IPv4 multicast address</td>
<td>239.255.70.83</td>
</tr>
</tbody>
</table>

Additional References

For additional information, see the following sections:

- Related Documents, page 2-24
- MIBs, page 2-24
Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFS CLI commands</td>
<td><em>Cisco Nexus 7000 Series NX-OS System Management Command Reference</em></td>
</tr>
<tr>
<td>CFS configuration for Call Home</td>
<td><em>Configuring Smart Call Home, page 6-1</em></td>
</tr>
<tr>
<td>VDCs and VRFs</td>
<td><em>Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.x</em></td>
</tr>
<tr>
<td>CFS configuration for TACACS+</td>
<td><em>Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 4.x</em></td>
</tr>
<tr>
<td>CFS configuration for RADIUS</td>
<td><em>Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 4.x</em></td>
</tr>
<tr>
<td>CFS configuration for roles</td>
<td><em>Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 4.x</em></td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>• CISCO-CFS-MIB</td>
<td><em>Cisco NX-OS MIB Support</em></td>
</tr>
</tbody>
</table>

Feature History for CFS

This section provides the CFS release history.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFS protocol</td>
<td>4.1(2)</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
CHAPTER 3

Configuring NTP

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

- Information About NTP, page 3-1
- Licensing Requirements for NTP, page 3-3
- Prerequisites for NTP, page 3-3
- Guidelines and Limitations, page 3-3
- Configuring NTP, page 3-3
- Verifying NTP Configuration, page 3-9
- NTP Example Configuration, page 3-10
- Default Settings, page 3-10
- Additional References, page 3-10
- Feature History for NTP, page 3-11

Information About NTP

This section includes the following topics:

- NTP Overview, page 3-1
- Distributing NTP Using CFS, page 3-2
- High Availability, page 3-2
- Virtualization Support, page 3-2

NTP Overview

The Network Time Protocol (NTP) synchronizes the time of day among a set of distributed time servers and clients so that you can correlate events when you receive system logs and other time-specific events from multiple network devices. With the User Datagram Protocol (UDP) as its transport protocol, NTP uses standard Universal Time Coordinated (UTC).
An NTP server usually receives its time from a source such as a radio clock or an atomic clock attached to a time server and then distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two machines to within a millisecond of each other.

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

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

Before synchronizing, NTP compares the time reported by several network devices and does not synchronize with one that is significantly different, even if it is a stratum 1.

Because Cisco NX-OS cannot connect to a radio or atomic clock and act as a stratum 1 server, we recommend that you use the public NTP servers available on the Internet.

If the network is isolated from the Internet, Cisco NX-OS allows you to configure the time as though it were synchronized through NTP, even though it was not.

**Note**
You can create NTP peer relationships to designate the time-serving hosts that you want your networking device to consider synchronizing with and to keep accurate time if a server failure occurs.

### Distributing NTP Using CFS

Cisco Fabric Services (CFS) distributes the local NTP configuration to all Cisco devices in the network. After enabling CFS on your device, a network-wide lock is applied to NTP whenever an NTP configuration is started. After making the NTP configuration changes, you can discard or commit them. In either case, the CFS lock is then released from the NTP application.

For more information about CFS, see the “Configuring CFS” section on page 2-1.

### High Availability

Stateless restarts are supported for NTP. After a reboot or a supervisor switchover, the running configuration is applied. For more information on high availability, see the Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide.

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

### Virtualization Support

Up to one instance of NTP is supported on the entire platform. You must configure NTP in the default VDC. You are automatically placed in the default VDC unless you specify otherwise. For more information about VDCs, see the Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.x.

NTP recognizes virtual routing and forwarding (VRF) instances. NTP uses the default VRF if you do not configure a specific VRF for the NTP server and NTP peer. See the Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 4.x for more information about VRFs.
Licensing Requirements for NTP

<table>
<thead>
<tr>
<th>Product</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>NX-OS</td>
<td>NTP requires no license and is bundled with the Cisco NX-OS system images at no extra charge to you. For a complete explanation of the NX-OS licensing scheme, see the Cisco NX-OS Licensing Guide.</td>
</tr>
</tbody>
</table>

Prerequisites for NTP

NTP has the following prerequisites:

- To configure NTP, you must have connectivity to at least one server that is running NTP.
- NTP must be configured in the default VDC. It cannot be configured in any other VDC except the default VDC.
- To configure VDCs, you must install the Advanced Services license. See the Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.x.

Guidelines and Limitations

NTP has the following configuration guidelines and limitations:

- NTP server functionality is not supported in Cisco NX-OS Release 4.2.
- You should have a peer association with another device only when you are sure that your clock is reliable (which means that you are a client of a reliable NTP server).
- A peer configured alone takes on the role of a server and should be used as a backup. If you have two servers, you can configure several devices to point to one server and the remaining devices to point to the other server. You can then configure a peer association between these two servers to create a more reliable NTP configuration.
- If you only have one server, you should configure all the devices as clients to that server.
- You can configure up to 64 NTP entities (servers and peers).
- If CFS is disabled for NTP, then NTP does not distribute any configuration and does not accept a distribution from other devices in the network.
- After CFS distribution is enabled for NTP, then the entry of an NTP configuration command locks the network for NTP configuration until a commit command is entered. During the lock, no changes can be made to the NTP configuration by any other device in the network except the device that initiated the lock.
- If you use CFS to distribute NTP, all devices in the network should have the same VRFs configured as you use for NTP.
- If you configure NTP in a VRF, ensure the NTP server and peers can reach each other through the configured VRFs.

Configuring NTP

This section includes the following topics:
Configuring NTP

Chapter 3 Configuring NTP

Send document comments to nexus7k-docfeedback@cisco.com.

- Enabling or Disabling the NTP Protocol, page 3-4
- Configuring an NTP Server and Peer, page 3-5
- Configuring the NTP Source IP Address, page 3-7
- Configuring the NTP Source Interface, page 3-7
- Configuring NTP on a Secondary (Non-Default) VDC, page 3-7
- Enabling CFS Distribution for NTP, page 3-8
- Committing NTP Configuration Changes, page 3-9
- Discarding NTP Configuration Changes, page 3-9
- Releasing CFS Session Lock, page 3-10

Note

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

Enabling or Disabling the NTP Protocol

You can enable or disable NTP. NTP is enabled by default. You can disable NTP and then reenable it.

BEFORE YOU BEGIN

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

SUMMARY STEPS

1. config t
2. [no] ntp enable
3. show ntp status
4. copy running-config startup-config

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 config t</td>
<td>Places you in global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# config t</td>
<td></td>
</tr>
<tr>
<td>Enter configuration commands, one per line. End with CNTL/Z.</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td>Step 2 [no] ntp enable</td>
<td>Enables or disables the NTP protocol on the entire device. NTP is enabled by default.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# ntp enable</td>
<td></td>
</tr>
</tbody>
</table>
Configuring NTP

This example shows how to disable NTP:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# no ntp enable
```

Configuring an NTP Server and Peer

You can configure an NTP server and peer. You need to know the IP address or DNS names of your NTP server and its peers.

**BEFORE YOU BEGIN**

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

- If you plan to use CFS to distribute your NTP configuration to other devices, then you should have already completed the following:
  - Enable CFS distribution using the “Configuring CFS Distribution” section on page 2-5.
  - Enable CFS for NTP using the “Enabling CFS Distribution for NTP” section on page 3-7.

**SUMMARY STEPS**

1. `config t`
2. `ntp server {ip-address | ipv6-address | dns-name} [prefer] [use-vrf vrf-name]`
3. `ntp peer {ip-address | ipv6-address | dns-name} [prefer] [use-vrf vrf-name]`
4. `show ntp peers`
5. `copy running-config startup-config`

**Step 3**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ntp status</code></td>
<td>(Optional) Displays the status of the NTP application.</td>
</tr>
</tbody>
</table>

Example:

```
switch(config)# show ntp status
Distribution : Enabled
Last operational state: Fabric Locked
```

**Step 4**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

Example:

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

(Optional) Displays the status of the NTP application.

(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>config t</strong></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch# config t</code></td>
</tr>
<tr>
<td></td>
<td>Enter configuration commands, one per line. End with CNTL/Z.</td>
</tr>
<tr>
<td></td>
<td><code>switch(config)#</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>`ntp server [ip-address</td>
</tr>
<tr>
<td>Example:</td>
<td><code>switch(config)# ntp server 192.0.2.10</code></td>
</tr>
<tr>
<td></td>
<td>Forms an association with a server. Optionally configures the NTP server</td>
</tr>
<tr>
<td></td>
<td>to communicate over the specified VRF. The <code>vrf-name</code> can be any</td>
</tr>
<tr>
<td></td>
<td>case-sensitive alphanumeric string up to 64 characters. Optionally</td>
</tr>
<tr>
<td></td>
<td>use the <code>prefer</code> keyword to make this the preferred NTP server for</td>
</tr>
<tr>
<td></td>
<td>the device.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>`ntp peer [ip-address</td>
</tr>
<tr>
<td></td>
<td><code>switch(config)# ntp peer 2001:0db8::4101</code></td>
</tr>
<tr>
<td></td>
<td>Forms an association with a peer. You can specify multiple peer</td>
</tr>
<tr>
<td></td>
<td>associations. Optionally configures the NTP peer to communicate over</td>
</tr>
<tr>
<td></td>
<td>the specified VRF. Optionally use the <code>prefer</code> keyword to make this</td>
</tr>
<tr>
<td></td>
<td>the preferred NTP peer for the device. The <code>vrf-name</code> can be any</td>
</tr>
<tr>
<td></td>
<td>case-sensitive alphanumeric string up to 64 characters.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>show ntp peers</code></td>
</tr>
<tr>
<td>Example:</td>
<td><code>switch(config)# show ntp peers</code></td>
</tr>
<tr>
<td></td>
<td>(Optional) Displays the configured server and peers.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>copy running-config startup-config</code></td>
</tr>
<tr>
<td>Example:</td>
<td><code>switch(config)# copy running-config startup-config</code></td>
</tr>
<tr>
<td></td>
<td>(Optional) Saves the change persistently through reboots and restarts</td>
</tr>
<tr>
<td></td>
<td>by copying the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

This example shows how to configure an NTP server and peer:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ntp server 192.0.2.105 use-vrf Red
switch(config)# ntp peer 2001:0db8::4101 use-vrf Red
switch(config)# show ntp peers
```

```
Peer IP Address Serv/Peer
2001:0db8::4101 Peer (configured)
192.0.2.105 Server (configured)
```

```
switch(config)# copy running-config startup-config
[########################################] 100%
switch(config)#
```
Configuring the NTP Source IP Address

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

To configure the NTP source IP address, use the following command in global configuration mode:

```
ntp source ip-address
```

**Example:**
```
switch(config)# ntp source 192.0.2.1
```

Configures the source IP address for all NTP packets. The `ip-address` can be in IPv4 or IPv6 format.

**Configuring the NTP Source Interface**

You can configure NTP to use a specific interface.

To configure the NTP source interface, use the following command in global configuration mode:

```
ntp source-interface interf
```

**Example:**
```
switch(config)# ntp source-interface ethernet 2/1
```

Configures the source interface for all NTP packets. Use the `?` keyword to display a list of supported interfaces.

**Configuring NTP on a Secondary (Non-Default) VDC**

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

**BEFORE YOU BEGIN**

Use the `switchto vdc` command to switch to the desired non-default VDC.

**SUMMARY STEPS**

1. `config t`
2. `feature ntp`
3. `ntp master`
4. (Optional) `ntp source-interface interface`
5. (Optional) `ntp source ip-address`
6. (Optional) `copy running-config startup-config`
DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>config t</code></td>
</tr>
</tbody>
</table>
|         | **Example:** | switch# config t  
Enter configuration commands, one per line.  
End with CNTL/Z.  
switch(config)# |
| Step 2  | `feature ntp` | Enables NTP in the non-default VDC. |
|         | **Example:** | switch(config)# feature ntp |
| Step 3  | `ntp master` | Configures the device as an authoritative NTP server. |
|         | **Example:** | switch(config)# ntp master |
| Step 4  | `ntp source-interface interface` | (Optional) Configures the source interface for all NTP packets. Use the ? keyword to display a list of supported interfaces. |
|         | **Example:** | switch(config)# ntp source-interface ethernet 2/1 |
| Step 5  | `ntp source ip-address` | (Optional) Configures the source IP address for all NTP packets. The `ip-address` can be in IPv4 or IPv6 format. |
|         | **Example:** | switch(config)# ntp source 192.0.2.1 |
| Step 6  | `copy running-config startup-config` | (Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration. |
|         | **Example:** | switch(config)# copy running-config startup-config |

Enabling CFS Distribution for NTP

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

BEFORE YOU BEGIN

- You have already enabled CFS distribution for the device using the “Configuring CFS Distribution” section on page 2-5.

SUMMARY STEPS

1. `configure terminal`
2. `ntp distribute`
3. `show ntp status`
4. `copy running-config startup-config`
Chapter 3  Configuring NTP

Send document comments to nexus7k-docfeedback@cisco.com.

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Places you into CLI Global Configuration mode.</td>
</tr>
<tr>
<td>Example: switch# configure terminal switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> switch(config)# ntp distribute</td>
<td>Enables the device to receive NTP configuration updates that are distributed through CFS.</td>
</tr>
<tr>
<td>Example: switch(config)# ntp distribute</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> show ntp status</td>
<td>(Optional) Displays the NTP CFS distribution status.</td>
</tr>
<tr>
<td>Example: switch(config)# show ntp status</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> copy running-config startup-config</td>
<td>(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.</td>
</tr>
<tr>
<td>Example: switch(config)# copy run start [########################################] 100% switch(config)#</td>
<td></td>
</tr>
</tbody>
</table>

**Committing NTP Configuration Changes**

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

To commit the NTP configuration changes, use the following command in global configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ntp commit</td>
<td>Distributes the NTP configuration changes to all switches in the network and releases the CFS lock. Overwrites the effective database with the changes made to the pending database.</td>
</tr>
<tr>
<td>Example: switch(config)# ntp commit switch(config)#</td>
<td></td>
</tr>
</tbody>
</table>

**Discarding NTP Configuration Changes**

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

To discard NTP configuration changes, use the following command in global configuration mode:
Verifying NTP Configuration

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ntp peer-status</code></td>
<td>Displays the status for all NTP servers and peers.</td>
</tr>
<tr>
<td><code>show ntp peers</code></td>
<td>Displays all the NTP peers.</td>
</tr>
<tr>
<td><code>show ntp pending peers</code></td>
<td>Displays the temporary CFS database for NTP.</td>
</tr>
<tr>
<td><code>show ntp pending-diff</code></td>
<td>Displays the difference between the pending CFS database and the current NTP configuration.</td>
</tr>
<tr>
<td><code>show ntp session status</code></td>
<td>Displays the NTP CFS distribution session information</td>
</tr>
<tr>
<td><code>show ntp statistics</code></td>
<td>Displays the NTP statistics.</td>
</tr>
<tr>
<td><code>show ntp status</code></td>
<td>Displays the NTP CFS distribution status</td>
</tr>
</tbody>
</table>

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

Releasing CFS Session Lock

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

To release the session lock from any device and discard any pending database changes, use the following command in global configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>clear ntp session</code></td>
<td>Discards the NTP configuration changes in the pending database and releases the CFS lock.</td>
</tr>
</tbody>
</table>

Verifying NTP Configuration

Send document comments to nexus7k-docfeedback@cisco.com.
NTP Example Configuration

This example shows how to configure an NTP server and peer and then save the configuration in startup so that it is saved across reboots and restarts:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ntp server 192.0.2.105
switch(config)# ntp peer 2001:0db8::4101
switch(config)# show ntp peers
--------------------------------------------------
          Peer IP Address         Serv/Peer
--------------------------------------------------
          2001:db8::4101             Peer (configured)
          192.0.2.105                Server (configured)
switch(config)# copy running-config startup-config
[########################################] 100%
switch(config)#
```

Default Settings

Table 3-1 lists the default settings for NTP parameters.

**Table 3-1 Default NTP Parameters**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Additional References

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

- Related Documents, page 3-11
- MIBs, page 3-12

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP CLI commands</td>
<td>Cisco Nexus 7000 Series NX-OS System Management Command Reference</td>
</tr>
<tr>
<td>VDCs and VRFs</td>
<td>Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.x</td>
</tr>
</tbody>
</table>
### Feature History for NTP

Table 3-2 lists the release history for this feature.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFS support</td>
<td>4.2(1)</td>
<td>Added ability to distribute NTP configuration using CFS. See the “Enabling CFS Distribution for NTP” section on page 3-8.</td>
</tr>
<tr>
<td>NTP source IP address or interface</td>
<td>4.1(3)</td>
<td>Added ability set the source IP address or source interface that NTP includes in all NTP packets sent to peers.</td>
</tr>
<tr>
<td>NTP protocol</td>
<td>4.0(3)</td>
<td>Added ability to disable the NTP protocol. See the “Enabling or Disabling the NTP Protocol” section on page 3-4.</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISCO-NTP-MIB</td>
<td>To locate and download MIBs, go to the following URL:</td>
</tr>
</tbody>
</table>
Configuring CDP

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

- Information About CDP, page 4-1
- Licensing Requirements for CDP, page 4-3
- Prerequisites for CDP, page 4-3
- Guidelines and Limitations, page 4-3
- Configuring CDP, page 4-3
- Verifying the CDP Configuration, page 4-7
- CDP Example Configuration, page 4-7
- Default Settings, page 4-8
- Additional References, page 4-8
- Feature History for CDP, page 4-9

Information About CDP

This section includes the following topics:

- CDP Overview, page 4-1
- VTP Feature Support, page 4-2
- High Availability, page 4-3

CDP Overview

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

CDP gathers protocol addresses of neighboring devices and discovers the platform of those devices. CDP runs over the data link layer only. Two systems that support different Layer 3 protocols can learn about each other.
Each device that you configure for CDP sends periodic advertisements to a multicast address. Each device advertises at least one address at which it can receive SNMP messages. The advertisements also contain hold-time information, which indicates the length of time that a receiving device should hold CDP information before removing it. You can configure the advertisement or refresh timer and the hold timer.

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

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

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

All CDP packets include a VLAN ID. If you configure CDP on a Layer 2 access port, the CDP packets sent from that access port include the access port VLAN ID. If you configure CDP on a Layer 2 trunk port, the CDP packets sent from that trunk port include the lowest configured VLAN ID allowed on that trunk port. The trunk port can receive CDP packets that include any VLAN ID in the allowed VLAN list for that trunk port. For more information on VLANs, see the Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 4.x.

### VTP Feature Support

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

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

You can view the VTP information with the `show cdp neighbors details` command.
High Availability

Cisco NX-OS supports stateless restarts for CDP. After a reboot or a supervisor switchover, Cisco NX-OS applies the running configuration. For more information on high availability, see the Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide.

Virtualization Support

<table>
<thead>
<tr>
<th>Product</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>NX-OS</td>
<td>Cisco NX-OS supports multiple instances of CDP, one instance per virtual device context (VDC). By default, Cisco NX-OS places you in the default VDC unless you specifically configure another VDC. For more information on VDCs, see the Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.x.</td>
</tr>
</tbody>
</table>

Licensing Requirements for CDP

CDP requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the NX-OS licensing scheme, see the Cisco NX-OS Licensing Guide.

Prerequisites for CDP

CDP has the following prerequisites:

If you configure VDCs, install the Advanced Services license and enter the desired VDC (see the Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.x).

Guidelines and Limitations

CDP has the following configuration guidelines and limitations:

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

Configuring CDP

This section includes the following topics:

- Enabling or Disabling CDP Globally, page 4-4
- Enabling or Disabling CDP on an Interface, page 4-5
- Configuring Optional CDP Parameters, page 4-6
Configuring CDP

Enabling or Disabling CDP Globally

CDP is enabled by default. You can disable CDP and then reenable it.

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

BEFORE YOU BEGIN

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

SUMMARY STEPS

1. config t
2. cdp enable
3. copy running-config startup-config

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>config t</td>
<td>Places you in global configuration mode.</td>
</tr>
</tbody>
</table>

Example:

switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)#

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>cdp enable</td>
<td>Enables the CDP feature on the entire device. This is enabled by default.</td>
</tr>
</tbody>
</table>

Example:

switch(config)# cdp enable

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Saves this configuration change.</td>
</tr>
</tbody>
</table>

Example:

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

Use the no cdp enable command to disable the CDP feature on the device.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>no cdp enable</td>
<td>Disables the CDP feature on the device.</td>
</tr>
</tbody>
</table>

Example:

switch(config)# no cdp enable
Send document comments to nexus7k-docfeedback@cisco.com.

This example shows how to enable the CDP feature:

```bash
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# cdp enable
```

### Enabling or Disabling CDP on an Interface

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

### BEFORE YOU BEGIN

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

### SUMMARY STEPS

1. `config t`
2. `interface interface-type slot/port`
3. `cdp enable`
4. `show cdp interface interface-type slot/port`
5. `copy running-config startup-config`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1 config t</strong></td>
<td>Places you in global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# config t</td>
<td></td>
</tr>
<tr>
<td>Enter configuration commands, one per line. End with CNTL/Z.</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2 interface interface-type slot/port</strong></td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# interface ethernet 1/2</td>
<td></td>
</tr>
<tr>
<td>switch(config-if)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3 cdp enable</strong></td>
<td>Enables CDP on this interface. This is enabled by default.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config-if)#</td>
<td></td>
</tr>
<tr>
<td>cdp enable</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> Ensure that CDP is enabled on the device (see the “Enabling or Disabling CDP Globally” section on page 4-4).</td>
<td></td>
</tr>
</tbody>
</table>
Configuring CDP

This example shows how to disable CDP on Ethernet 1/2:

```
switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# interface ethernet 1/2
switch(config-if)# no cdp enable
switch(config-if)# copy running-config startup-config
```

This example shows how to enable CDP on port channel 2:

```
switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# interface port-channel 2
switch(config-if)# cdp enable
switch(config-if)# copy running-config startup-config
```

Configuring Optional CDP Parameters

You can use the following optional commands in global configuration mode to modify CDP:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`cdp advertise {v1</td>
<td>v2}`</td>
</tr>
</tbody>
</table>
| `cdp format device-id {mac-address | other | serial-number}` | Sets the CDP device ID. The options are as follows:  
  - `mac-address`—MAC address of the chassis.  
  - `other`—Chassis serial number  
  - `serial-number`—Chassis serial number/Organizationally Unique Identifier (OUI)  
  The default is other. |
Verifying the CDP Configuration

Use the following commands to display the CDP configuration:

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

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

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

CDP Example Configuration

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

```
cfg t
cdp enable
cdp timer 50
cdp holdtime 100
```
Table 4-1 lists the CDP default settings.

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

Additional References

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

- Related Documents, page 4-8
- MIBs, page 4-8

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDP CLI commands</td>
<td>Cisco Nexus 7000 Series NX-OS System Management Command Reference</td>
</tr>
<tr>
<td>VDCs and VRFs</td>
<td>Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.x</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISCO-CDP-MIB</td>
<td>To locate and download MIBs, go to the following URL:</td>
</tr>
</tbody>
</table>
Feature History for CDP

Table 4-2 lists the release history for this feature.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDP support for VTP domain name</td>
<td>4.2(1)</td>
<td>CDP advertises the VLAN Trunking Protocol (VTP) type-length-value field (TLV) in CDP version-2 packets. See VTP Feature Support, page 4-2.</td>
</tr>
</tbody>
</table>
Configuring System Message Logging

This chapter describes how to configure system message logging on Cisco NX-OS devices. This chapter includes the following sections:

- Information About System Message Logging, page 5-1
- Licensing Requirements for System Message Logging, page 5-3
- Guidelines and Limitations, page 5-3
- Configuring System Message Logging, page 5-3
- Verifying System Message Logging Configuration, page 5-10
- System Message Logging Example Configuration, page 5-11
- Default Settings, page 5-11
- Additional References, page 5-12
- Feature History for System Message Logging, page 5-12

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.

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

By default, the device outputs messages to terminal sessions. For information about configuring logging to terminal sessions, see the “Configuring System Message Logging to Terminal Sessions” section on page 5-3.

By default, the device logs system messages to a log file. For information about configuring logging to a file, see the “Logging System Messages to a File” section on page 5-5.

Table 5-1 describes the severity levels used in system messages. When you configure the severity level, the system outputs messages at that level and lower.
Information About System Message Logging

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

You can configure which system messages should be logged based on the facility that generated the message and its severity level. For information about facilities, see the Cisco Nexus 7000 Series NX-OS System Management Command Reference. For information about configuring the severity level by module and facility, see the “Configuring Module and Facility Messages Logged” section on page 5-6.

This section includes the following topics:

- syslog Servers, page 5-2
- Virtualization Support, page 5-2

### syslog Servers

The syslog servers run on remote systems that log system messages based on the syslog protocol. You can configure up to three IPv4 or IPv6 syslog servers. For information about configuring syslog servers, see the “Configuring syslog Servers” section on page 5-7.

**Note**

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

### Virtualization Support

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

For information about configuring VDCs, see the Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.x.

---

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

The device logs the most recent 100 messages of severity 0, 1, or 2 to the NVRAM log. You cannot configure logging to the NVRAM.
Licensing Requirements for System Message Logging

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

Guidelines and Limitations

System messages are logged to the console and the logfile by default.

Configuring System Message Logging

This section includes the following topics:

- Configuring System Message Logging to Terminal Sessions, page 5-3
- Logging System Messages to a File, page 5-5
- Configuring Module and Facility Messages Logged, page 5-6
- Configuring syslog Servers, page 5-7
- Displaying and Clearing Log Files, page 5-9

**Note**

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

Configuring System Message Logging to Terminal Sessions

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

**BEFORE YOU BEGIN**

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

**SUMMARY STEPS**

1. `terminal monitor`
2. `config t`
3. `logging console [severity-level]`
   - `no logging console`
4. `show logging console`
### Configuring System Message Logging

5. **logging monitor** \([\text{severity-level}]\)
   
   no logging monitor

6. **show logging monitor**

7. **copy running-config startup-config**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>terminal monitor</td>
</tr>
<tr>
<td>Example:</td>
<td>switch# terminal monitor</td>
</tr>
<tr>
<td></td>
<td>Enables the device to log messages to the console.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>config t</td>
</tr>
<tr>
<td>Example:</td>
<td>switch# config t</td>
</tr>
<tr>
<td></td>
<td>Enter configuration commands, one per line. End with (\text{CNTL}/Z).</td>
</tr>
<tr>
<td></td>
<td>switch(config)#</td>
</tr>
<tr>
<td></td>
<td>Places you in global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>logging console ([\text{severity-level}])</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# logging console 3</td>
</tr>
<tr>
<td></td>
<td>Configures the device to log messages to the console session based on a specified severity level or higher. Severity levels, which can range from 0 to 7, are listed in Table 5-1. If the severity level is not specified, the default of 2 is used.</td>
</tr>
<tr>
<td></td>
<td>no logging console ([\text{severity-level}])</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# no logging console</td>
</tr>
<tr>
<td></td>
<td>Disables the device’s ability to log messages to the console.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>show logging console</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# show logging console</td>
</tr>
<tr>
<td></td>
<td>(Optional) Displays the console logging configuration.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>logging monitor ([\text{severity-level}])</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# logging monitor 3</td>
</tr>
<tr>
<td></td>
<td>Enables the device to log messages to the monitor based on a specified severity level or higher. The configuration applies to Telnet and SSH sessions. Severity levels, which can range from 0 to 7, are listed in Table 5-1. If the severity level is not specified, the default of 2 is used.</td>
</tr>
<tr>
<td></td>
<td>no logging monitor ([\text{severity-level}])</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# no logging monitor</td>
</tr>
<tr>
<td></td>
<td>Disables logging messages to Telnet and SSH sessions.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>show logging monitor</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# show logging monitor</td>
</tr>
<tr>
<td></td>
<td>(Optional) Displays the monitor logging configuration.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>copy running-config startup-config</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# copy running-config startup-config</td>
</tr>
<tr>
<td></td>
<td>(Optional) Copies the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>
Send document comments to nexus7k-docfeedback@cisco.com.

Logging System Messages to a File

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

For information about displaying and clearing log files, see the “Displaying and Clearing Log Files” section on page 5-9.

BEFORE YOU BEGIN

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

SUMMARY STEPS

1. `config t`
2. `logging logfile logfile-name severity-level [size bytes]`
   - no logging logfile [logfile-name severity-level [size bytes]]
3. `show logging info`
4. `copy running-config startup-config`

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>config t</td>
</tr>
<tr>
<td>Example:</td>
<td>switch# config t</td>
</tr>
<tr>
<td></td>
<td>switch(config)#</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>logging logfile logfile-name severity-level [size bytes]</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# logging logfile my_log 6</td>
</tr>
<tr>
<td></td>
<td>no logging logfile [logfile-name severity-level [size bytes]]</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# no logging logfile</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>show logging info</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# show logging info</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>copy running-config startup-config</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# copy running-config startup-config</td>
</tr>
</tbody>
</table>
Configuring Module and Facility Messages Logged

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

BEFORE YOU BEGIN

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

SUMMARY STEPS

1. `config t`
2. `logging module [severity-level]`
   
   Example:
   
   `switch(config)# logging module 3`

3. `no logging module`
   
   Example:
   
   `switch(config)# no logging module`

4. `logging level facility severity-level`

5. `show logging level [facility]`

6. `logging timestamp {microseconds | milliseconds | seconds}`

7. `show logging timestamp`

8. `copy running-config startup-config`

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>config t</code></td>
<td>Places you in global configuration mode.</td>
</tr>
</tbody>
</table>
| **Example:**
switch# config t
Enter configuration commands, one per line. End with CNTRL/Z.
switch(config)# | |
| **Step 2** `logging module [severity-level]` | Enables module log messages that have the specified severity level or higher. Severity levels, which range from 0 to 7, are listed in Table 5-1. If the severity level is not specified, the default of 5 is used. |
| **Example:**
switch(config)# logging module 3 | |
| **Step 3** `no logging module [severity-level]` | Disables module log messages. |
| **Example:**
switch(config)# no logging module | |
| `show logging module` | (Optional) Displays the module logging configuration. |
| `copy running-config startup-config` | |
Send document comments to nexus7k-docfeedback@cisco.com.

### Configuring System Message Logging

#### Configuring syslog Servers

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

**Note**

We recommend that you configure the syslog server to use the management virtual routing and forwarding (VRF) instance. For more information on VRFs, see the *Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 4.x*.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 4**

  **logging level** *facility severity-level*

  *Example:*

  `switch(config)# logging level aaa 2`

  Enables logging messages from the specified facility that have the specified severity level or higher. The facilities are listed in the *Cisco Nexus 7000 Series NX-OS System Management Command Reference*. Severity levels, which range from 0 to 7, are listed in Table 5-1. To apply the same severity level to all facilities, use the **all** facility. For defaults, see the **show logging level** command.

  **no logging level** `[facility severity-level]`

  *Example:*

  `switch(config)# no logging level aaa 3`

  Resets the logging severity level for the specified facility to its default level. If you do not specify a facility and severity level, the device resets all facilities to their default levels.

| **Step 5**

  **show logging level** `[facility]`

  *Example:*

  `switch(config)# show logging level aaa`

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

| **Step 6**

  **logging timestamp** `{microseconds | milliseconds | seconds}`

  *Example:*

  `switch(config)# logging timestamp milliseconds`

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

  **no logging timestamp** `{microseconds | milliseconds | seconds}`

  *Example:*

  `switch(config)# no logging timestamp milliseconds`

  Resets the logging time-stamp units to the default of seconds.

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

| **Step 7**

  **show logging timestamp**

  *Example:*

  `switch(config)# show logging timestamp`

  (Optional) Displays the logging time-stamp units configured.

| **Step 8**

  **copy running-config startup-config**

  *Example:*

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

  (Optional) Copies the running configuration to the startup configuration.
## Configuring System Message Logging

**BEFORE YOU BEGIN**

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

### SUMMARY STEPS

1. `config t`
2. `logging server host [severity-level [use-vrf vrf-name]]`
   - `no logging server host`
3. `show logging server`
4. `copy running-config startup-config`

### Command and Purpose

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong>&lt;br&gt;<code>config t</code>&lt;br&gt;&lt;br&gt;<code>Example:</code>&lt;br&gt;<code>switch# config t</code>&lt;br&gt;Enter configuration commands, one per line. End with CNTL/Z.&lt;br&gt;<code>switch(config)#</code></td>
<td>Places you in global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong>&lt;br&gt;<code>logging server host [severity-level [use-vrf vrf-name]]</code>&lt;br&gt;&lt;br&gt;<code>Example 1:</code>&lt;br&gt;<code>switch(config)# logging server 192.0.2.253</code>&lt;br&gt;<code>Example 2:</code>&lt;br&gt;<code>switch(config)# logging server 2001::db*::3 5 use-vrf red</code></td>
<td>Configures a syslog server at the specified hostname or IPv4 or IPv6 address. You can limit logging of messages to a particular VRF by using the <code>use-vrf</code> keyword. In Cisco NX-OS Release 4.2 or higher, the default VRF is default. Severity levels, which range from 0 to 7, are listed in Table 5-1. The default outgoing facility is local7. Example 1 forwards all messages on facility local 7. Example 2 forwards messages with severity level 5 or lower for VRF red.</td>
</tr>
<tr>
<td><code>no logging server host</code>&lt;br&gt;&lt;br&gt;<code>Example:</code>&lt;br&gt;<code>switch(config)# no logging server host</code></td>
<td>Removes the logging server for the specified host.</td>
</tr>
<tr>
<td><strong>Step 3</strong>&lt;br&gt;<code>show logging server</code>&lt;br&gt;&lt;br&gt;<code>Example:</code>&lt;br&gt;<code>switch(config)# show logging server</code></td>
<td>(Optional) Displays the syslog server configuration.</td>
</tr>
<tr>
<td><strong>Step 4</strong>&lt;br&gt;<code>copy running-config startup-config</code>&lt;br&gt;&lt;br&gt;<code>Example:</code>&lt;br&gt;<code>switch(config)# copy running-config startup-config</code></td>
<td>(Optional) Copies the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

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
```
To configure a syslog server on a UNIX or Linux system, follow these 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~
```

### Displaying and Clearing Log Files

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

**BEFORE YOU BEGIN**

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

**SUMMARY STEPS**

1. `show logging last number-lines`
2. `show logging logfile [start-time yyyymmmdd hh:mm:ss] [end-time yyyymmmdd hh:mm:ss]`
3. `show logging nvram [last number-lines]`
4. `clear logging logfile`
5. `clear logging nvram`
## Verifying System Message Logging Configuration

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

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

### Verifying System Message Logging Configuration

**Step 1**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show logging last number-lines</code></td>
<td>Displays the last number of lines in the logging file. You can specify from 1 to 9999 for the last number of lines.</td>
</tr>
<tr>
<td>Example: <code>switch# show logging last 40</code></td>
<td></td>
</tr>
</tbody>
</table>

**Step 2**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show logging logfile [start-time yyyy mmm dd hh:mm:ss] [end-time yyyy mmm dd hh:mm:ss]</code></td>
<td>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.</td>
</tr>
<tr>
<td>Example: <code>switch# show logging logfile start-time 2007 nov 1 15:10:0</code></td>
<td></td>
</tr>
</tbody>
</table>

**Step 3**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show logging nvram [last number-lines]</code></td>
<td>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.</td>
</tr>
<tr>
<td>Example: <code>switch# show logging nvram last 10</code></td>
<td></td>
</tr>
</tbody>
</table>

**Step 4**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>clear logging logfile</code></td>
<td>Clears the contents of the log file.</td>
</tr>
<tr>
<td>Example: <code>switch# clear logging logfile</code></td>
<td></td>
</tr>
</tbody>
</table>

**Step 5**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>clear logging nvram</code></td>
<td>Clears the logged messages in NVRAM.</td>
</tr>
<tr>
<td>Example: <code>switch# clear logging nvram</code></td>
<td></td>
</tr>
</tbody>
</table>
System Message Logging Example Configuration

This example shows how to configure system message logging:

```plaintext
config t
  logging console 3
  logging monitor 3
  logging logfile my_log 6
  logging module 3
  logging level aaa 2
  logging timestamp milliseconds
  logging distribute
  logging server 172.28.254.253
  logging server 172.28.254.254 5 local3
  logging commit
  copy running-config startup-config
```

Default Settings

Table 5-3 lists the default settings for system message logging parameters.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console logging</td>
<td>Enabled at severity level 2</td>
</tr>
<tr>
<td>Monitor logging</td>
<td>Enabled at severity level 5</td>
</tr>
<tr>
<td>Log file logging</td>
<td>Enabled to log messages at severity level 5</td>
</tr>
<tr>
<td>Module logging</td>
<td>Enabled at severity level 5</td>
</tr>
<tr>
<td>Facility logging</td>
<td>Enabled; for severity levels, see the Cisco Nexus 7000 Series NX-OS System Management Command Reference.</td>
</tr>
<tr>
<td>Time-stamp units</td>
<td>Seconds</td>
</tr>
<tr>
<td>syslog server logging</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
Additional References

For additional information related to implementing system message logging, see the following sections:

- Related Documents, page 5-12
- Standards, page 5-12

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>System messages CLI commands</td>
<td>Cisco NX-OS System Management Command Reference</td>
</tr>
<tr>
<td>System messages</td>
<td>Cisco NX-OS System Messages Reference</td>
</tr>
</tbody>
</table>

Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
</tr>
</tbody>
</table>

Feature History for System Message Logging

Table 5-4 lists the release history for this feature.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 support</td>
<td>4.2(1)</td>
<td>Added support for IPv6 syslog hosts.</td>
</tr>
<tr>
<td>System Message Logging</td>
<td>4.0(1)</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
CHAPTER 6

Configuring Smart Call Home

This chapter describes how to configure the Smart Call Home feature of the Cisco NX-OS devices. This chapter includes the following sections:
- Information About Call Home, page 6-1
- Licensing Requirements for Call Home, page 6-8
- Prerequisites for Call Home, page 6-8
- Guidelines and Limitations, page 6-8
- Configuring Call Home, page 6-8
- Verifying Call Home Configuration, page 6-22
- Call Home Example Configuration, page 6-23
- Default Settings, page 6-23
- Additional References, page 6-24
- Feature History for Smart Call Home, page 6-36

Information About Call Home

This section includes the following topics:
- Call Home Overview, page 6-2
- Destination Profiles, page 6-2
- Call Home Alert Groups, page 6-3
- Call Home Message Urgency Levels, page 6-5
- Obtaining Smart Call Home, page 6-6
- Distributing Call Home Using CFS, page 6-7
- Database Merge Guidelines, page 6-7
- High Availability, page 6-7
- Virtualization Support, page 6-7
Information About Call Home

Send document comments to nexus7k-docfeedback@cisco.com.

Call Home Overview

Call Home provides an e-mail-based notification for critical system policies. A range of message formats are available for 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 provides the following:

- 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.
- 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 Cisco NX-OS generates a Call Home message to all e-mail addresses in the destination profile. For more information about Call Home severity levels, see the “Call Home Message Urgency Levels” section on page 6-5. Cisco NX-OS 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 NX-OS supports the following predefined destination profiles:

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

See the “Message Formats” section on page 6-25 for more information about the message formats.
Call Home Alert Groups

An alert group is a predefined subset of Call Home alerts that are supported in all Cisco NX-OS devices. Alert groups allow you to select the set of Call Home alerts that you want to send to a predefined or custom destination profile. Cisco NX-OS 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 (see the “Call Home Message Urgency Levels” section on page 6-5).

Table 6-1 lists supported alert groups and the default CLI command output included in Call Home messages generated for the alert group.

<table>
<thead>
<tr>
<th>Alert Group</th>
<th>Description</th>
<th>Executed Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco-TAC</td>
<td>All critical alerts from the other alert groups destined for Smart Call Home.</td>
<td>Execute commands based on the alert group that originates the alert.</td>
</tr>
<tr>
<td>Configuration</td>
<td>Periodic events related to configuration.</td>
<td><code>show module</code> <code>show running-configuration vdc-all all</code> <code>show startup-configuration vdc-all</code> <code>show vdc current</code> <code>show vdc membership</code> <code>show version</code></td>
</tr>
<tr>
<td>Diagnostic</td>
<td>Events generated by diagnostics.</td>
<td><code>show diagnostic result module all detail</code> <code>show diagnostic result module number detail</code> <code>show hardware</code> <code>show logging last 200</code> <code>show module</code> <code>show sprom all</code> <code>show tech-support gold</code> <code>show tech-support platform</code> <code>show tech-support sysmgr</code> <code>show vdc current</code> <code>show vdc membership</code> <code>show version</code></td>
</tr>
<tr>
<td>EEM</td>
<td>Events generated by EEM.</td>
<td><code>show diagnostic result module all detail</code> <code>show diagnostic result module number detail</code> <code>show module</code> <code>show tech-support gold</code> <code>show tech-support platform</code> <code>show tech-support sysmgr</code> <code>show vdc current</code> <code>show vdc membership</code></td>
</tr>
<tr>
<td>Environmental</td>
<td>Events related to power, fan, and environment-sensing elements such as temperature alarms.</td>
<td><code>show environment</code> <code>show logging last 200</code> <code>show module</code> <code>show vdc current</code> <code>show vdc membership</code> <code>show version</code></td>
</tr>
</tbody>
</table>
### Table 6-1  Alert Groups and Executed Commands (continued)

<table>
<thead>
<tr>
<th>Alert Group</th>
<th>Description</th>
<th>Executed Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory</td>
<td>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.</td>
<td>show inventory&lt;br&gt;show license usage&lt;br&gt;show module&lt;br&gt;show system uptime&lt;br&gt;show sprom all&lt;br&gt;show vdc current&lt;br&gt;show vdc membership&lt;br&gt;show version</td>
</tr>
<tr>
<td>License</td>
<td>Events related to licensing and license violations.</td>
<td>show license usage vdc all&lt;br&gt;show logging last 200&lt;br&gt;show vdc current&lt;br&gt;show vdc membership</td>
</tr>
<tr>
<td>Linemodule hardware</td>
<td>Events related to standard or intelligent switching modules.</td>
<td>show diagnostic result module all detail&lt;br&gt;show diagnostic result module number detail&lt;br&gt;show hardware&lt;br&gt;show logging last 200&lt;br&gt;show module&lt;br&gt;show sprom all&lt;br&gt;show tech-support ethpm&lt;br&gt;show tech-support gold&lt;br&gt;show tech-support platform&lt;br&gt;show tech-support sysmgr&lt;br&gt;show vdc current&lt;br&gt;show vdc membership&lt;br&gt;show version</td>
</tr>
<tr>
<td>Supervisor hardware</td>
<td>Events related to supervisor modules.</td>
<td>show diagnostic result module all detail&lt;br&gt;show hardware&lt;br&gt;show logging last 200&lt;br&gt;show module&lt;br&gt;show sprom all&lt;br&gt;show tech-support ethpm&lt;br&gt;show tech-support gold&lt;br&gt;show tech-support platform&lt;br&gt;show tech-support sysmgr&lt;br&gt;show vdc current&lt;br&gt;show vdc membership&lt;br&gt;show version</td>
</tr>
<tr>
<td>Syslog port group</td>
<td>Events generated by the syslog PORT facility.</td>
<td>show license usage&lt;br&gt;show logging last 200&lt;br&gt;show vdc current&lt;br&gt;show vdc membership</td>
</tr>
</tbody>
</table>
Information About Call Home

Table 6-1  Alert Groups and Executed Commands (continued)

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

Call Home maps the syslog severity level to the corresponding Call Home severity level for syslog port group messages (see the “Call Home Message Urgency Levels” section on page 6-5).

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.

Call Home Message Urgency Levels

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

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

Note

Call Home does not change the syslog message level in the message text. The syslog messages in the Call Home log appear as they are described in the Cisco NX-OS System Messages Reference.

Table 6-2 lists each Call Home message level keyword and the corresponding syslog level for the syslog port alert group.

Table 6-2  Severity and syslog Level Mapping

<table>
<thead>
<tr>
<th>Call Home Level</th>
<th>Keyword</th>
<th>syslog Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>Catastrophic</td>
<td>N/A</td>
<td>Network-wide catastrophic failure.</td>
</tr>
<tr>
<td>8</td>
<td>Disaster</td>
<td>N/A</td>
<td>Significant network impact.</td>
</tr>
<tr>
<td>7</td>
<td>Fatal</td>
<td>Emergency (0)</td>
<td>System is unusable.</td>
</tr>
<tr>
<td>6</td>
<td>Critical</td>
<td>Alert (1)</td>
<td>Critical conditions that indicate that immediate attention is needed.</td>
</tr>
</tbody>
</table>
Information About Call Home

Obtaining Smart Call Home

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

Smart Call Home offers the following features:

- Continuous device health monitoring and real-time diagnostic alerts.
- Analysis of Call Home messages and, if needed, Automatic Service Request generation, routed to the correct TAC team, including detailed diagnostic information to speed problem resolution.
- Secure message transport directly from your device or through a downloadable Transport Gateway (TG) aggregation point. You can use a TG aggregation point to support multiple devices or in cases where security dictates that your devices may not be connected directly to the Internet.
- Web-based access to 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 information to register:

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

For more information about Smart Call Home, see the following Smart Call Home page:

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

<table>
<thead>
<tr>
<th>Call Home Level</th>
<th>Keyword</th>
<th>syslog Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Major</td>
<td>Critical (2)</td>
<td>Major conditions.</td>
</tr>
<tr>
<td>4</td>
<td>Minor</td>
<td>Error (3)</td>
<td>Minor conditions.</td>
</tr>
<tr>
<td>3</td>
<td>Warning</td>
<td>Warning (4)</td>
<td>Warning conditions.</td>
</tr>
<tr>
<td>2</td>
<td>Notification</td>
<td>Notice (5)</td>
<td>Basic notification and informational messages. Possibly independently insignificant.</td>
</tr>
<tr>
<td>1</td>
<td>Normal</td>
<td>Information (6)</td>
<td>Normal event signifying return to normal state.</td>
</tr>
<tr>
<td>0</td>
<td>Debugging</td>
<td>Debug (7)</td>
<td>Debugging messages.</td>
</tr>
</tbody>
</table>

Table 6-2 Severity and syslog Level Mapping (continued)
Distributing Call Home Using CFS

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

For more information about CFS, see the “Configuring CFS” section on page 2-1.

Database Merge Guidelines

When merging two Call Home databases, the following guidelines apply:

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

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

High Availability

Stateless restarts are supported for Call Home. After a reboot or supervisor switchover, the running configuration is applied.

Virtualization Support

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

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

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

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

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

<table>
<thead>
<tr>
<th>Product</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>NX-OS</td>
<td>Call Home requires no license, is bundled with the system images, and is provided at no extra charge to you. For a complete explanation of the NX-OS licensing scheme, see the Cisco NX-OS Licensing Guide.</td>
</tr>
</tbody>
</table>

Prerequisites for Call Home

Call Home has the following prerequisites:

- To send messages to an e-mail address, you must first configure an e-mail server. To send messages using HTTP, you must have access to an HTTPS server and have a valid certificate installed on the Nexus device.
- Your device must have IP connectivity to an e-mail server or HTTPS server.
- You must first configure the contact name (SNMP server contact), phone, and street address information. This step is required to determine the origin of messages received.
- If you use Smart Call Home, you need an active service contract for the device that you are configuring.
- If you configure VDCs, install the Advanced Services license (see the Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.x). This license is required for VDCs only, not for Call Home.

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, Call Home messages cannot be sent.
- Call Home operates with any SMTP server.
- Call Home messages sent through HTTP use the same VRF that you configure in the Call Home SMTP server.
- If you distribute the Call Home configuration using CFS, then the entire Call Home configuration is distributed except switch priority and the sysContact names.

Configuring Call Home

If you distribute the Call Home configuration using CFS, see the “Configuring Smart Call Home” section on page 6-1.
This section includes the following topics:

- Configuring Contact Information, page 6-9
- Creating a Destination Profile, page 6-11
- Modifying a Destination Profile, page 6-13
- Associating an Alert Group and a Destination Profile, page 6-15
- Adding show Commands to an Alert Group, page 6-17
- Configuring E-Mail, page 6-18
- Configuring Periodic Inventory Notifications, page 6-20
- Disabling Duplicate Message Throttle, page 6-21
- Enabling or Disabling Call Home, page 6-21
- Testing Call Home Communications, page 6-22

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

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

1. Configuring Contact Information, page 6-9
2. Creating a Destination Profile, page 6-11
3. Associating an Alert Group and a Destination Profile, page 6-15
4. (Optional) Adding show Commands to an Alert Group, page 6-17
5. (Optional) Creating and Distributing a CFS Configuration, page 2-19
6. Enabling or Disabling Call Home, page 6-21
7. (Optional) Testing Call Home Communications, page 6-22

Configuring Contact Information

You can configure the contact information for Call Home.

BEFORE YOU BEGIN

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

SUMMARY STEPS

1. `config t`
2. `snmp-server contact sys-contact`
3. `callhome`
4. `email-contact email-address`
5. `phone-contact international-phone-number`
6. `streetaddress address`
7. `contract-id contract-number`
8. `customer-id customer-number`
Chapter 6  Configuring Smart Call Home

Send document comments to nexus7k-docfeedback@cisco.com.

9. site-id site-number
10. switch-priority number
11. commit
12. show callhome
13. copy running-config startup-config

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 config t</td>
<td>Places you in global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# config t</td>
<td>Enter configuration commands, one per line. End with CNTL/Z.</td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
</tbody>
</table>

Step 2 snmp-server contact sys-contact
Example:
switch(config)# snmp-server contact personname@companyname.com

Step 3 callhome
Example:
switch(config)# callhome
switch(config-callhome)#

Step 4 email-contact email-address
Example:
switch(config-callhome)# email-contact admin@Mycompany.com

Step 5 phone-contact international-phone-number
Example:
switch(config-callhome)# phone-contact +1-800-123-4567

Step 6 streetaddress address
Example:
switch(config-callhome)# streetaddress 123 Anystreet st. Anytown, AnyWhere

Step 7 contract-id contract-number
Example:
switch(config-callhome)# contract-id Contract5678

(Optional) Configures the contract number for this device from the service agreement. The contract number can be up to 255 alphanumeric characters in free format.
### Configuring Call Home

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

```
switch(config)# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# snmp-server contact personname@companyname.com
switch(config)# callhome
switch(config-callhome)# email-contact admin@Mycompany.com
switch(config-callhome)# phone-contact +1-800-123-4567
switch(config-callhome)# streetaddress 123 Anystreet st. Anytown,AnyWhere
switch(config-callhome)# commit
```

### Creating a Destination Profile

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

**BEFORE YOU BEGIN**

Make sure that you are in the correct VDC (or use the `switchto vdc` command).

**SUMMARY STEPS**

1. `config t`
2. `callhome`
3. `destination-profile name`

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 8</strong></td>
<td><code>customer-id customer-number</code></td>
</tr>
<tr>
<td>Example:</td>
<td><code>switch(config-callhome)# customer-id Customer123456</code></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><code>site-id site-number</code></td>
</tr>
<tr>
<td>Example:</td>
<td><code>switch(config-callhome)# site-id Site1</code></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td><code>switch-priority number</code></td>
</tr>
<tr>
<td>Example:</td>
<td><code>switch(config-callhome)# switch-priority 3</code></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td><code>commit</code></td>
</tr>
<tr>
<td>Example:</td>
<td><code>switch(config-callhome)# commit</code></td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td><code>show callhome</code></td>
</tr>
<tr>
<td>Example:</td>
<td><code>switch(config-callhome)# show callhome</code></td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td><code>copy running-config startup-config</code></td>
</tr>
<tr>
<td>Example:</td>
<td><code>switch(config)# copy running-config startup-config</code></td>
</tr>
</tbody>
</table>
### Configuring Call Home

**Send document comments to nexus7k-docfeedback@cisco.com.**

4. `destination-profile name format {XML | full-txt | short-txt}`
5. `commit`
6. `show callhome destination-profile [profile name]`
7. `copy running-config startup-config`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>config t</td>
</tr>
<tr>
<td><strong>Example:</strong> switch# config t</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enter configuration commands, one per line. End with CNTL/Z. switch(config)#</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>callhome</td>
</tr>
<tr>
<td><strong>Example:</strong> switch(config)# callhome</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config-callhome)#</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>destination-profile name</td>
</tr>
<tr>
<td><strong>Example:</strong> switch(config-callhome)# destination-profile Noc101</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>destination-profile name format {XML</td>
</tr>
<tr>
<td><strong>Example:</strong> switch(config-callhome)# destination-profile Noc101 format full-txt</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>commit</td>
</tr>
<tr>
<td><strong>Example:</strong> switch(config-callhome)# commit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>show callhome destination-profile [profile name]</td>
</tr>
<tr>
<td><strong>Example:</strong> switch(config-callhome)# show callhome destination-profile profile Noc101</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>copy running-config startup-config</td>
</tr>
<tr>
<td><strong>Example:</strong> switch(config)# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

(Optional) Displays information about one or more destination profiles. (Optional) Saves this configuration change.
This example shows how to create a destination profile for Call Home:

```bash
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# callhome
switch(config-callhome)# destination-profile Noc101
switch(config-callhome)# destination-profile Noc101 format full-text
switch(config-callhome)# commit
```

### Modifying a Destination Profile

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

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

See the “Associating an Alert Group and a Destination Profile” section on page 6-15 for information on configuring an alert group for a destination profile.

### BEFORE YOU BEGIN

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

### SUMMARY STEPS

1. config t
2. callhome
3. destination profile {name | CiscoTAC-1 | full-txt-destination | short-txt-destination} email-addr address
4. destination profile {name | CiscoTAC-1 | full-txt-destination | short-txt-destination} http address
5. destination profile {name | CiscoTAC-1 | full-txt-destination | short-txt-destination} transport-method {email | http}
6. destination profile {name | CiscoTAC-1 | full-txt-destination | short-txt-destination} message-level number
7. destination profile {name | CiscoTAC-1 | full-txt-destination | short-txt-destination} message-size number
8. commit
9. show call-home destination-profile [profile name]
10. copy running-config startup-config
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>config t</strong>&lt;br&gt;Example:&lt;br&gt;switch# config t&lt;br&gt;Enter configuration commands, one per line. End with CNTL/Z.&lt;br&gt;switch(config)#</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>callhome</strong>&lt;br&gt;Example:&lt;br&gt;switch(config)# callhome&lt;br&gt;switch(config-callhome)#</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>**destination-profile {name</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>**destination-profile {name</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>**destination-profile {name</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>**destination-profile {name</td>
</tr>
</tbody>
</table>
Configuring Call Home

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

```plaintext
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# callhome
switch(config-callhome)# destination-profile full-txt-destination message-size 10000
```

Configures the maximum message size for this destination profile. The range is from 0 to 5000000. The default is 2500000.

```plaintext
Step 7 destination-profile {name | CiscoTAC-1 | full-txt-destination | short-txt-destination} message-size number
Example:
switch(config-callhome)# destination-profile full-txt-destination message-size 100000
```

Commits the callhome configuration commands.

```plaintext
Step 8 commit
Example:
switch(config-callhome)# commit
```

(Optional) Displays information about one or more destination profiles.

```plaintext
Step 9 show callhome destination-profile {profile name}
Example:
switch(config-callhome)# show callhome destination-profile full-txt-destination
```

(Optional) Saves this configuration change.

```plaintext
Step 10 copy running-config startup-config
Example:
switch(config)# copy running-config startup-config
```

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

```plaintext
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# callhome
switch(config-callhome)# destination-profile full-txt-destination email-addr person@place.com
switch(config-callhome)# destination-profile full-txt-destination message-level 5
switch(config-callhome)# destination-profile full-txt-destination message-size 10000
switch(config-callhome)# commit
```

Associating an Alert Group and a Destination Profile

You can associate one or more alert groups with a destination profile.

BEFORE YOU BEGIN

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

SUMMARY STEPS

1. `config t`
2. `callhome`
3. `destination profile {name | CiscoTAC-1 | full-txt-destination | short-txt-destination}
   alert-group {All | Cisco-TAC | Configuration | Diagnostic | EEM | Environmental | Inventory | License | Linecard-Hardware | Supervisor-Hardware | Syslog-group-port | System | Test}`
4. `commit`
5. `show callhome destination-profile [profile name]`
6. `copy running-config startup-config`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>config t</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# config t</td>
<td>Enter configuration commands, one per line. End with CNTL/Z.</td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>callhome</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# callhome</td>
<td>switch(config-callhome)#</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>destination-profile {name</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config-callhome)# destination-profile Noc101 alert-group All</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>commit</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config-callhome)# commit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>show callhome destination-profile [profile name]</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config-callhome)# show callhome destination-profile profile Noc101</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>copy running-config startup-config</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

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

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# callhome
switch(config-callhome)# destination-profile Noc101 alert-group All
switch(config-callhome)# commit
```
Adding show Commands to an Alert Group

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

**Note**

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

**BEFORE YOU BEGIN**

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

**SUMMARY STEPS**

1. `config t`
2. `callhome`
3. `alert-group {Configuration | Diagnostic | EEM | Environmental | Inventory | License | Linecard-Hardware | Supervisor-Hardware | Syslog-group-port | System | Test} user-def-cmd show-cmd`
4. `commit`
5. `show call-home user-def-cmds`
6. `copy running-config startup-config`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>config t</code></td>
</tr>
<tr>
<td>Example:</td>
<td>switch# config t Enter configuration commands, one per line. End with CNTL/Z. switch(config)#</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>callhome</code></td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# callhome switch(config-callhome)#</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>`alert-group {Configuration</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config-callhome)# alert-group Configuration user-def-cmd show ip route</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>commit</code></td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config-callhome)# commit</td>
</tr>
</tbody>
</table>
Configuring Call Home

This example shows how to add the `show ip route` command to the Cisco-TAC alert group:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# callhome
switch(config-callhome)# alert-group Configuration user-def-cmd show ip route
switch(config-callhome)# commit
```

### 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.

**BEFORE YOU BEGIN**

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

**SUMMARY STEPS**

1. `config t`
2. `callhome`
3. `transport email smtp-server ip-address [port number] [use-vrf vrf-name]`
4. `transport email from email-address`
5. `transport email reply-to email-address`
6. `commit`
7. `show callhome transport-email`
8. `copy running-config startup-config`

This example shows how to add the `show ip route` command to the Cisco-TAC alert group:

```
switch(config-callhome)# show callhome user-def-cmds
```

**Example:**

```
switch(config-callhome)# show callhome user-def-cmds
```

(Optional) Displays information about all user-defined `show` commands added to alert groups.

**Step 6**

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

(Optional) Saves this configuration change.

**Step 6**

```
switch(config-callhome)# show callhome transport-email
```

(Optional) Displays information about all user-defined `transport-email` commands added to alert groups.

**Step 6**

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

(Optional) Saves this configuration change.
Send document comments to nexus7k-docfeedback@cisco.com.

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>config t&lt;br&gt;<strong>Example:</strong>&lt;br&gt;switch# config t&lt;br&gt;Enter configuration commands, one per line. End with CNTL/Z.&lt;br&gt;switch(config)#</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>callhome&lt;br&gt;<strong>Example:</strong>&lt;br&gt;switch(config)# callhome&lt;br&gt;switch(config-callhome)#</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>transport email smtp-server ip-address</td>
</tr>
<tr>
<td>transport email smtp-server ip-address [port number] [use-vrf vrf-name]</td>
<td><strong>Example:</strong>&lt;br&gt;switch(config-callhome)# transport email smtp-server 192.0.2.1 use-vrf Red</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>transport email from email-address</td>
</tr>
<tr>
<td>transport email from email-address</td>
<td><strong>Example:</strong>&lt;br&gt;switch(config-callhome)# transport email from <a href="mailto:person@company.com">person@company.com</a></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>transport email reply-to email-address</td>
</tr>
<tr>
<td>transport email reply-to email-address</td>
<td><strong>Example:</strong>&lt;br&gt;switch(config-callhome)# transport email reply-to <a href="mailto:person@company.com">person@company.com</a></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>commit&lt;br&gt;<strong>Example:</strong>&lt;br&gt;switch(config-callhome)# commit</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>show callhome transport-email&lt;br&gt;<strong>Example:</strong>&lt;br&gt;switch(config-callhome)# show callhome transport-email</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>copy running-config startup-config&lt;br&gt;<strong>Example:</strong>&lt;br&gt;switch(config)# copy running-config startup-config</td>
</tr>
</tbody>
</table>

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

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# callhome
switch(config-callhome)# transport email smtp-server 192.0.2.10 use-vrf Red
switch(config-callhome)# transport email from person@company.com
switch(config-callhome)# transport email reply-to person@company.com
switch(config-callhome)# commit
```
Configuring Periodic Inventory Notifications

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. Cisco NX-OS generates two Call Home notifications, periodic configuration messages and periodic inventory messages.

BEFORE YOU BEGIN

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

SUMMARY STEPS

1. `config t`
2. `callhome`
3. `periodic-inventory notification [interval days | timeofday time]`
4. `commit`
5. `show callhome`
6. `copy running-config startup-config`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>config t</code></td>
<td>Places you in global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>switch# config t</code></td>
<td>Enter configuration commands, one per line. End with CNTL/Z.</td>
</tr>
<tr>
<td><code>switch(config)#</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>callhome</code></td>
<td>Enters callhome configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>switch(config)# callhome</code></td>
<td></td>
</tr>
<tr>
<td><code>switch(config-callhome)#</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> `periodic-inventory notification [interval days</td>
<td>timeofday time]`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>switch(config-callhome)# periodic-inventory notification interval 20</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>commit</code></td>
<td>Commits the callhome configuration commands.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>switch(config-callhome)# commit</code></td>
<td></td>
</tr>
</tbody>
</table>
Configuring Call Home

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

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# callhome
switch(config-callhome)# periodic-inventory notification interval 20
switch(config-callhome)# commit
```

Disabling Duplicate Message Throttle

You can limit the number of duplicate messages received for the same event. By default, Cisco NX-OS 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 Cisco NX-OS disables further messages for that alert type.

Use the following commands in Call Home configuration mode to disable duplicate message throttling:

```
Step 1
Command: no duplicate-message throttle
Example: switch(config-callhome)# no duplicate-message throttle
Purpose: Disables duplicate message throttling for Smart Call Home. Enabled by default.

Step 2
Command: commit
Example: switch(config-callhome)# commit
Purpose: Commits the callhome configuration commands.
```

Enabling or Disabling Call Home

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

---

**Send document comments to nexus7k-docfeedback@cisco.com.**
Use the following commands in Call Home configuration mode to enable Call Home:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables Smart Call Home. Disabled by default.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config-callhome)# enable</td>
<td>Note To disable Smart Call Home, use the <strong>no enable</strong> command in Smart Call Home configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>commit</td>
<td>Commits the callhome configuration commands.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config-callhome)# commit</td>
<td></td>
</tr>
</tbody>
</table>

**Testing Call Home Communications**

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

Use the following commands in any mode to generate a test Call Home message:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>callhome send [configuration</td>
<td>diagnostic]</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config-callhome)# callhome send diagnostic</td>
<td>Note This command is available only in the default VDC.</td>
</tr>
<tr>
<td>callhome test</td>
<td>Sends a test message to all configured destinations.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config-callhome)# callhome test</td>
<td></td>
</tr>
</tbody>
</table>

**Verifying Call Home Configuration**

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show callhome</td>
<td>Displays the Call Home configuration.</td>
</tr>
<tr>
<td>show callhome destination-profile name</td>
<td>Displays one or more Call Home destination profiles.</td>
</tr>
<tr>
<td>show callhome merge</td>
<td>Displays the status of the last CFS merger for Call Home.</td>
</tr>
<tr>
<td>show callhome pending</td>
<td>Displays the Call Home configuration changes in the pending CFS database.</td>
</tr>
<tr>
<td>show callhome pending-diff</td>
<td>Displays the differences between the pending and running Call Home configuration.</td>
</tr>
<tr>
<td>show callhome session status</td>
<td>Displays the status of the last CFS commit or abort operation.</td>
</tr>
</tbody>
</table>
Call Home Example Configuration

This example shows how to create a destination profile called Noc101, associate the Cisco-TAC alert group to that profile, and configure contact and e-mail information:

```
config t
  snmp-server contact person@company.com
  callhome
distribute
  email-contact admin@Mycompany.com
  phone-contact +1-800-123-4567
  streetaddress 123 Anystreet st. Anytown,AnyWhere
  destination-profile Noc101 format full-txt
  destination-profile full-text-destination email-addr person@company.com
  destination-profile full-text-destination message-level 5
  destination-profile Noc101 alert-group Configuration
  alert-group Configuration user-def-cmd show ip route
  transport email smtp-server 192.0.2.10 use-vrf Red
  enable
  commit
```

Default Settings

Table 6-3 lists the default settings for Call Home parameters.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination message size for a message sent in full text format.</td>
<td>2,500,000</td>
</tr>
<tr>
<td>Destination message size for a message sent in XML format.</td>
<td>2,500,000</td>
</tr>
<tr>
<td>Destination message size for a message sent in short text format.</td>
<td>4000</td>
</tr>
<tr>
<td>SMTP server port number if no port is specified.</td>
<td>25</td>
</tr>
</tbody>
</table>
Table 6-3  Default Call Home Parameters (continued)

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert group association with profile.</td>
<td>All for full-text-destination and short-text-destination profiles. The cisco-tac alert group for the CiscoTAC-1 destination profile.</td>
</tr>
<tr>
<td>Format type.</td>
<td>XML</td>
</tr>
<tr>
<td>Call Home message level.</td>
<td>0 (zero)</td>
</tr>
</tbody>
</table>

Additional References

For additional information related to implementing Call Home, see the following sections:

- Event Triggers, page 6-24
- Message Formats, page 6-25
- Sample syslog Alert Notification in Full-Text Format, page 6-29
- Sample syslog Alert Notification in XML Format, page 6-32
- Related Documents, page 6-35
- Standards, page 6-36
- MIBs, page 6-36

Event Triggers

Table 6-4 lists the event triggers and their Call Home message severity levels.

Table 6-4  Event Triggers

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

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

Message Formats

Call Home supports the following message formats:

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

Table 6-5 describes the short text formatting option for all message types.

Table 6-5  Short Text Message Format

<table>
<thead>
<tr>
<th>Data Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device identification</td>
<td>Configured device name</td>
</tr>
<tr>
<td>Date/time stamp</td>
<td>Time stamp of the triggering event</td>
</tr>
</tbody>
</table>
Table 6-5  Short Text Message Format (continued)

<table>
<thead>
<tr>
<th>Data Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error isolation message</td>
<td>Plain English description of triggering event</td>
</tr>
<tr>
<td>Alarm urgency level</td>
<td>Error level such as that applied to system message</td>
</tr>
</tbody>
</table>

Table 6-6 describes the first set of common event message fields for full text or XML messages.

Table 6-6  Common Fields for Full Text and XML Messages

<table>
<thead>
<tr>
<th>Data Item (Plain Text and XML)</th>
<th>Description (Plain Text and XML)</th>
<th>XML Tag (XML Only)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time stamp</td>
<td>Date and time stamp of event in ISO time notation: YYYY-MM-DD HH:MM:SS GMT+HH:MM.</td>
<td>/aml/header/time</td>
</tr>
<tr>
<td>Message name</td>
<td>Name of message. Specific event names are listed in Table 6-4.</td>
<td>/aml/header/name</td>
</tr>
<tr>
<td>Message type</td>
<td>Name of message type, such as reactive or proactive.</td>
<td>/aml/header/type</td>
</tr>
<tr>
<td>Message group</td>
<td>Name of alert group, such as syslog.</td>
<td>/aml/header/group</td>
</tr>
<tr>
<td>Severity level</td>
<td>Severity level of message (see the “Call Home Message Urgency Levels” section on page 6-5).</td>
<td>/aml/header/level</td>
</tr>
<tr>
<td>Source ID</td>
<td>Product type for routing, such as the Catalyst 6500 series switch.</td>
<td>/aml/header/source</td>
</tr>
<tr>
<td>Device ID</td>
<td>Unique device identifier (UDI) for the end device that generated the message. This field should be empty if the message is nonspecific to a device. The format is type@Sid@serial.</td>
<td>/aml/header/deviceId</td>
</tr>
<tr>
<td>Customer ID</td>
<td>Optional user-configurable field used for contract information or other ID by any support service.</td>
<td>/aml/header/customerID</td>
</tr>
<tr>
<td>Contract ID</td>
<td>Optional user-configurable field used for contract information or other ID by any support service.</td>
<td>/aml/header/contractId</td>
</tr>
<tr>
<td>Site ID</td>
<td>Optional user-configurable field used for Cisco-supplied site ID or other data meaningful to alternate support service.</td>
<td>/aml/header/siteId</td>
</tr>
<tr>
<td>Server ID</td>
<td>If the message is generated from the device, this is the unique device identifier (UDI) of the device. The format is type@Sid@serial.</td>
<td>/aml/header/serverId</td>
</tr>
<tr>
<td></td>
<td>• type is the product model number from the backplane IDPROM.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• @ is a separator character.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Sid is C, identifying the serial ID as a chassis serial number.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• serial is the number identified by the Sid field.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>An example is WS-C6509@C@12345678.</td>
<td></td>
</tr>
</tbody>
</table>
Table 6-6  Common Fields for Full Text and XML Messages (continued)

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

Table 6-7 describes the fields specific to alert group messages for full text and XML. These fields may be repeated if multiple CLI commands are executed for an alert group.

Table 6-7  Fields Specific to Alert Group Messages for Full Text and XML Messages

<table>
<thead>
<tr>
<th>Data Item (Plain Text and XML)</th>
<th>Description (Plain Text and XML)</th>
<th>XML Tag (XML Only)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command output name</td>
<td>Exact name of the issued CLI command.</td>
<td>/aml/attachments/attachment/name</td>
</tr>
<tr>
<td>Attachment type</td>
<td>Specific command output.</td>
<td>/aml/attachments/attachment/type</td>
</tr>
<tr>
<td>MIME type</td>
<td>Either plain text or encoding type.</td>
<td>/aml/attachments/attachment/mime</td>
</tr>
<tr>
<td>Command output text</td>
<td>Output of command automatically executed (see the “Call Home Alert Groups” section on page 6-3).</td>
<td>/aml/attachments/attachment/atdata</td>
</tr>
</tbody>
</table>

Table 6-8 describes the reactive and proactive event message format for full text or XML messages.

Table 6-8  Inserted Fields for a Reactive and Proactive Event Message

<table>
<thead>
<tr>
<th>Data Item (Plain Text and XML)</th>
<th>Description (Plain Text and XML)</th>
<th>XML Tag (XML Only)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis hardware version</td>
<td>Hardware version of chassis.</td>
<td>/aml/body/chassis/hwVersion</td>
</tr>
<tr>
<td>Supervisor module software version</td>
<td>Top-level software version.</td>
<td>/aml/body/chassis/swVersion</td>
</tr>
<tr>
<td>Affected FRU name</td>
<td>Name of the affected FRU that is generating the event message.</td>
<td>/aml/body/frm/name</td>
</tr>
</tbody>
</table>
Send document comments to nexus7k-docfeedback@cisco.com.

### Table 6-8 Inserted Fields for a Reactive and Proactive Event Message (continued)

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

Table 6-9 describes the inventory event message format for full text or XML messages.

### Table 6-9 Inserted Fields for an Inventory Event Message

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

Table 6-10 describes the user-generated test message format for full text or XML.

### Table 6-10 Inserted Fields for a User-Generated Test Message

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

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

Severity Level:5
Series:Nexus7000
Switch Priority:0
Device Id:N7K-C7010@C@TXX12345678
Server Id:N7K-C7010@C@TXX12345678
Time of Event:2008-01-17 16:31:33 GMT+0000 Message Name:
Message Type:syslog
System Name:dc3-test
Contact Name:Jay Tester
Contact Email:contact@example.com
Contact Phone:+91-80-1234-5678
Street Address:#1 Any Street
Event Description:SYSLOG_ALERT 2008 Jan 17 16:31:33 dc3-test %ETHPORT-2-IF_SEQ_ERROR:
Error (0x20) while communicating with component MTS_SAP_ELM
opcode:MTS_OPC_ETHPM_PORT_PHY_CLEANUP (for:RID_PORT: Ethernet3/1)

syslog_facility:ETHPORT
start chassis information:
Affected Chassis:N7K-C7010
Affected Chassis Serial Number:TXX12345678 Affected Chassis Hardware Version:0.405
Affected Chassis Software Version:4.1(1) Affected Chassis Part No:73-10900-04 end chassis information:
start attachment
name:show logging logfile | tail -n 200
type:text
data:
2008 Jan 17 10:57:51 dc3-test %SYSLOG-1-SYSTEM_MSG : Logging logfile (messages) cleared by user
2008 Jan 17 10:57:53 dc3-test %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from /dev/ttyS0 /dev/ttyS0_console
2008 Jan 17 10:58:35 dc3-test %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from /dev/ttyS0 /dev/ttyS0_console
2008 Jan 17 10:59:00 dc3-test %DAEMON-3-SYSTEM_MSG: error: setsockopt IP_TOS 16:
Invalid argument: - sshd[14484]
2008 Jan 17 10:59:05 dc3-test %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from /dev/ttyS0 /dev/ttyS0_console
2008 Jan 17 12:11:18 dc3-test %SYSGR-5-STANDEY-5-SUBPROC_TERMINATED: 'System Manager (gsync controller)' (PID 12000) has finished with error code SYSMGR_EXITCODE_GSYNCFAILED_NONFATAL (12).
2008 Jan 17 16:28:03 dc3-test %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from /dev/ttyS0 /dev/ttyS0_console
2008 Jan 17 16:28:44 dc3-test %SYSGR-3-BASIC_TRACE: core_copy: PID 2579 with message Core not generated by system for eltm(0). WCOREDUMP(9) returned zero.
2008 Jan 17 16:28:44 dc3-test %SYSGR-2-SERVICE_CRASHED: Service "eltm" (PID 3504) hasn't caught signal 9 (no core).
2008 Jan 17 16:29:08 dc3-test %SYSGR-3-BASIC_TRACE: core_copy: PID 2579 with message Core not generated by system for eltm(0). WCOREDUMP(9) returned zero.
2008 Jan 17 16:29:08 dc3-test %SYSGR-2-SERVICE_CRASHED: Service "eltm" (PID 3504) hasn't caught signal 9 (no core).
2008 Jan 17 16:29:17 dc3-test %SYSGR-3-BASIC_TRACE: core_copy: PID 2579 with message Core not generated by system for eltm(0). WCOREDUMP(9) returned zero.
2008 Jan 17 16:29:17 dc3-test %SYSGR-2-SERVICE_CRASHED: Service "eltm" (PID 23210) hasn't caught signal 9 (no core).
2008 Jan 17 16:29:17 dc3-test %SYSGR-2-SERVICE_CRASHED: Service "eltm" (PID 23294) hasn't caught signal 9 (no core).
2008 Jan 17 16:29:25 dc3-test %SYSGR-2-HASWITCHOVER_PRE_START: This supervisor is becoming active (pre-start phase).
2008 Jan 17 16:29:25 dc3-test %SYSGR-2-HASWITCHOVER_START: This supervisor is becoming active.
2008 Jan 17 16:29:26 dc3-test %USER-3-SYSTEM_MSG: crdcfg_get_srvinfo: mts_send failed - device_test
Send document comments to nexus7k-docfeedback@cisco.com.

2008 Jan 17 16:29:27 dc3-test %NETSTACK-3-IP_UNK_MSG_MAJOR: netstack [4336] Unrecognized message from MRIB. Major type 1807
2008 Jan 17 16:29:27 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is DOWN in vdc 1
2008 Jan 17 16:29:27 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is DOWN in vdc 2
2008 Jan 17 16:29:27 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is DOWN in vdc 3
2008 Jan 17 16:29:27 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is DOWN in vdc 4
2008 Jan 17 16:29:28 dc3-test %DAMON-3-SYSTEM_MSG: ntp:socket family : 2 - ntpd[19045]
2008 Jan 17 16:29:28 dc3-test %DAMON-3-SYSTEM_MSG: ntp:ipv6 only defined - ntpd[19045]
2008 Jan 17 16:29:28 dc3-test %DAMON-3-SYSTEM_MSG: ntp:bindv6 only defined - ntpd[19045]
2008 Jan 17 16:29:28 dc3-test %DAMON-3-SYSTEM_MSG: ntp:socket family : 10 - ntpd[19045]
2008 Jan 17 16:29:28 dc3-test %DAMON-3-SYSTEM_MSG: ntp:socket family : 0 - ntpd[19045]
2008 Jan 17 16:29:28 dc3-test %DAMON-3-SYSTEM_MSG: ntp:socket family : 0 - ntpd[19045]
2008 Jan 17 16:29:29 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is UP in vdc 1
2008 Jan 17 16:29:29 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is UP in vdc 2
2008 Jan 17 16:29:29 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is UP in vdc 3
2008 Jan 17 16:29:29 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is UP in vdc 4
2008 Jan 17 16:29:31 dc3-test %DAMON-3-SYSTEM_MSG: Telnet disabled, removing - dcos-xinetd[19072]
2008 Jan 17 16:29:31 dc3-test %DAMON-3-SYSTEM_MSG: ssh disabled, removing - dcos-xinetd[19072]
2008 Jan 17 16:29:31 dc3-test %DAMON-3-SYSTEM_MSG: ssh disabled, removing - dcos-xinetd[19073]
2008 Jan 17 16:29:32 dc3-test %DAMON-3-SYSTEM_MSG: Telnet disabled, removing - dcos-xinetd[19079]
2008 Jan 17 16:29:32 dc3-test %DAMON-3-SYSTEM_MSG: ssh disabled, removing - dcos-xinetd[19079]
2008 Jan 17 16:29:34 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is UP in vdc 1
2008 Jan 17 16:29:34 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is UP in vdc 2
2008 Jan 17 16:29:34 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is UP in vdc 3
2008 Jan 17 16:29:34 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is UP in vdc 4
2008 Jan 17 16:29:34 dc3-test %CALLHOME-2-EVENT: SUP_FAILURE
2008 Jan 17 16:29:46 dc3-test vsh[19166]: CLIC-3-FAILED_EXEC: Can not exec command <more> return code <14>
2008 Jan 17 16:30:24 dc3-test vsh[23810]: CLIC-3-FAILED_EXEC: Can not exec command <more> return code <14>
2008 Jan 17 16:30:24 dc3-test vsh[23803]: CLIC-3-FAILED_EXEC: Can not exec command <more> return code <14>
2008 Jan 17 16:31:02 dc3-test vsh[23818]: CLIC-3-FAILED_EXEC: Can not exec command <more> return code <14>
2008 Jan 17 16:31:02 dc3-test %SYSMGR-3-BASIC_TRACE: core_copy: PID 2630 with message Core not generated by system for eltm(0). WCOREDUMP(9) returned zero .
2008 Jan 17 16:30:47 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service 'eltm' (PID 4820) hasn't caught signal 9 (no core)
2008 Jan 17 16:31:02 dc3-test %SYSMGR-3-BASIC_TRACE: core_copy: PID 2630 with message Core not generated by system for eltm(0). WCOREDUMP(9) returned zero .
2008 Jan 17 16:31:02 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service 'eltm' (PID 24239) hasn't caught signal 9 (no core).
2008 Jan 17 16:31:14 dc3-test %SYSMGR-3-BASIC_TRACE: core_copy: PID 2630 with message
Core not generated by system for eltm(0). WCOREDUMP(9) returned zero.
2008 Jan 17 16:31:14 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID 24401)
hasn’t caught signal 9 (no core).
2008 Jan 17 16:31:23 dc3-test %CALLHOME-2-EVENT: SW_CRASH alert for service: eltm
2008 Jan 17 16:31:23 dc3-test %SYSMGR-3-BASIC_TRACE: core_copy: PID 2630 with message
Core not generated by system for eltm(0). WCOREDUMP(9) returned zero.
2008 Jan 17 16:31:23 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID 24407)
hasn’t caught signal 9 (no core).
2008 Jan 17 16:31:24 dc3-test vsh[24532]: CLIC-3-FAILED_EXEC: Can not exec command
<more> return code <14>
2008 Jan 17 16:31:24 dc3-test vsh[24548]: CLIC-3-FAILED_EXEC: Can not exec command
<more> return code <14>
2008 Jan 17 16:31:24 dc3-test vsh[24535]: CLIC-3-FAILED_EXEC: Can not exec command
<more> return code <14>
2008 Jan 17 16:31:33 dc3-test %NETSTACK-3-INTERNAL_ERROR: netstack [4336] (null)
2008 Jan 17 16:31:33 dc3-test %ETHPORT-2-IF_SEQ_ERROR: Error (0x20) while
communicating with component MTS_SAP_ELTM opcode:MTS_OPC_ETHPM_PORT_PHY_CLEANUP
(for:RID_PORT: Ethernet3/1) end attachment start attachment
name:show vdc membership
type:text
data:

vdc_id: 1 vdc_name: dc3-test interfaces:
Ethernet3/1 Ethernet3/2 Ethernet3/3
Ethernet3/4 Ethernet3/5 Ethernet3/6
Ethernet3/7 Ethernet3/8 Ethernet3/9
Ethernet3/10 Ethernet3/11 Ethernet3/12
Ethernet3/13 Ethernet3/14 Ethernet3/15
Ethernet3/16 Ethernet3/17 Ethernet3/18
Ethernet3/19 Ethernet3/20 Ethernet3/21
Ethernet3/22 Ethernet3/23 Ethernet3/24
Ethernet3/25 Ethernet3/26 Ethernet3/27
Ethernet3/28 Ethernet3/29 Ethernet3/30
Ethernet3/31 Ethernet3/32 Ethernet3/33
Ethernet3/34 Ethernet3/35 Ethernet3/36
Ethernet3/37 Ethernet3/38 Ethernet3/39
Ethernet3/40 Ethernet3/41 Ethernet3/42
Ethernet3/43 Ethernet3/44 Ethernet3/45
Ethernet3/46 Ethernet3/47 Ethernet3/48

vdc_id: 2 vdc_name: dc3-aaa interfaces:

vdc_id: 3 vdc_name: dc3-rbac interfaces:

vdc_id: 4 vdc_name: dc3-call interfaces:

end attachment start attachment
name:show vdc current-vdc
type:text
data:
Current vdc is 1 - dc3-test end attachment start attachment
name:show license usage
type:text
data:
Feature Ins Lic Status Expiry Date Comments
Count
--------------------------------------------------------------------------------
LANADVANCEDSERVICES_PKG Yes - In use Never -
Sample syslog Alert Notification in XML Format

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

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<soap-env:Envelope xmlns:soap-env="http://www.w3.org/2003/05/soap-envelope">
  <soap-env:Header>
      soap-env:mustUnderstand="true"
      soap-env:role="http://www.w3.org/2003/05/soap-envelope/role/next">
      <aml-session:To>http://tools.cisco.com/neddce/services/DDCEService</aml-session:To>
      <aml-session:Path>
        <aml-session:Via>http://www.cisco.com/appliance/uri</aml-session:Via>
      </aml-session:Path>
      <aml-session:MessageId>1004:TXX12345678:478F82E6</aml-session:MessageId>
    </aml-session:Session>
  </soap-env:Header>
  <soap-env:Body>
      <aml-block:Header>
        <aml-block:Type>http://www.cisco.com/2005/05/callhome/syslog</aml-block:Type>
        <aml-block:CreationDate>2008-01-17 16:31:33 GMT+0000</aml-block:CreationDate>
        <aml-block:Builder>
          <aml-block:Name>DC3</aml-block:Name>
        </aml-block:Builder>
        <aml-block:Version>4.1</aml-block:Version>
      </aml-block:Header>
      <aml-block:Content>
        <ch:CallHome xmlns:ch="http://www.cisco.com/2005/05/callhome" version="1.0">
          <ch:MessageDescription>SYSLOG_ALERT 2008 Jan 17 16:31:33 dc3-test %ETHPORT-2-IF_SEQ_ERROR: Error (0x20) while communicating with component MTS_SAP_ELTM opcode:MTS_OPCODE_ETHPM_PORT_PHY_CLEANUP (for:RID_PORT: Ethernet3/1)</ch:MessageDescription>
          <ch:Event>
            <ch:Type>syslog</ch:Type>
            <ch:SubType></ch:SubType>
            <ch:Brand>Cisco</ch:Brand>
            <ch:Series>Nexus7000</ch:Series>
            <ch:CustomerData>
              <ch:UserData>
                <ch:Email>contact@example.com</ch:Email>
              </ch:UserData>
              <ch:ContractData>
                <ch:DeviceId>N7K-C7010@C@TXX12345678</ch:DeviceId>
              </ch:ContractData>
              <ch:SystemInfo>
                <ch:Name>Jay Tester</ch:Name>
                <ch:ContactPhoneNumber>+91-80-1234-5678</ch:ContactPhoneNumber>
                <ch:StreetAddress>#1, Any Street</ch:StreetAddress>
              </ch:SystemInfo>
              <ch:Device>
                <rme:Chassis xmlns:rme="http://www.cisco.com/rme/4.1">
                  <rme:Model>N7K-C7010</rme:Model>
                  <rme:HardwareVersion>0.405</rme:HardwareVersion>
                  <rme:SerialNumber>TXX12345678</rme:SerialNumber>
                </rme:Chassis>
              </ch:Device>
            </ch:ContractData>
            <ch:Device>
              <rme:Chassis xmlns:rme="http://www.cisco.com/rme/4.1">
                <rme:Model>N7K-C7010</rme:Model>
                <rme:HardwareVersion>0.405</rme:HardwareVersion>
                <rme:SerialNumber>TXX12345678</rme:SerialNumber>
              </rme:Chassis>
            </ch:Device>
            <ch:Device>
              <rme:Chassis xmlns:rme="http://www.cisco.com/rme/4.1">
                <rme:Model>N7K-C7010</rme:Model>
                <rme:HardwareVersion>0.405</rme:HardwareVersion>
                <rme:SerialNumber>TXX12345678</rme:SerialNumber>
              </rme:Chassis>
            </ch:Device>
            <ch:Device>
              <rme:Chassis xmlns:rme="http://www.cisco.com/rme/4.1">
                <rme:Model>N7K-C7010</rme:Model>
                <rme:HardwareVersion>0.405</rme:HardwareVersion>
                <rme:SerialNumber>TXX12345678</rme:SerialNumber>
              </rme:Chassis>
            </ch:Device>
            <ch:Device>
              <rme:Chassis xmlns:rme="http://www.cisco.com/rme/4.1">
                <rme:Model>N7K-C7010</rme:Model>
                <rme:HardwareVersion>0.405</rme:HardwareVersion>
                <rme:SerialNumber>TXX12345678</rme:SerialNumber>
              </rme:Chassis>
            </ch:Device>
            <ch:Device>
              <rme:Chassis xmlns:rme="http://www.cisco.com/rme/4.1">
                <rme:Model>N7K-C7010</rme:Model>
                <rme:HardwareVersion>0.405</rme:HardwareVersion>
                <rme:SerialNumber>TXX12345678</rme:SerialNumber>
              </rme:Chassis>
            </ch:Device>
            <ch:Device>
              <rme:Chassis xmlns:rme="http://www.cisco.com/rme/4.1">
                <rme:Model>N7K-C7010</rme:Model>
                <rme:HardwareVersion>0.405</rme:HardwareVersion>
                <rme:SerialNumber>TXX12345678</rme:SerialNumber>
              </rme:Chassis>
            </ch:Device>
          </ch:CustomerData>
        </ch:CallHome>
      </aml-block:Content>
    </aml-block:Block>
  </soap-env:Body>
</soap-env:Envelope>
```
### Chapter 6  Configuring Smart Call Home

Additional References

Send document comments to nexus7k-docfeedback@cisco.com.

```
</rme:Chassis>
</ch:Device>
</ch:CallHome>
</aml-block:Content>
</aml-block:Attachments>
<aml-block:Attachment type="inline">
<aml-block:Name>show logging logfile | tail -n 200</aml-block:Name> <aml-block:Data encoding="plain">
<![CDATA[
2008 Jan 17 10:57:51 dc3-test %SYSLOG-1-SYSTEM_MSG : Logging logfile (messages) cleared by user
2008 Jan 17 10:57:53 dc3-test %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from /dev/ttyS0 /dev/ttyS0_console
2008 Jan 17 10:58:35 dc3-test %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from /dev/ttyS0 /dev/ttyS0_console
2008 Jan 17 10:59:00 dc3-test %DAEMON-3-SYSTEM_MSG: error: setsockopt IP_TOS 16: Invalid argument: - sshd[14484]
2008 Jan 17 10:59:05 dc3-test %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from /dev/ttyS0 /dev/ttyS0_console
2008 Jan 17 12:11:18 dc3-test %SYSGR-STDOUT-5-SUBPROC_TERMINATED: \"System Manager (gsync controller)\" (PID 12000) has finished with error code SYSGR_EXITCODE_GSYNCFAILED_NONFATAL (12).
2008 Jan 17 16:28:03 dc3-test %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from /dev/ttyS0 /dev/ttyS0_console
2008 Jan 17 16:28:44 dc3-test %SYSGR-3-BASIC_TRACE: core_copy: PID 2579 with message Core not generated by system for eltm(0). WCOREDUMP(9) returned zero.
2008 Jan 17 16:28:44 dc3-test %SYSGR-2-SERVICE_CRASHED: Service \"eltm\" (PID 3504) hasnakapos;t caught signal 9 (no core).
2008 Jan 17 16:29:08 dc3-test %SYSGR-3-BASIC_TRACE: core_copy: PID 2579 with message Core not generated by system for eltm(0). WCOREDUMP(9) returned zero.
2008 Jan 17 16:29:08 dc3-test %SYSGR-2-SERVICE_CRASHED: Service \"eltm\" (PID 23210) hasnakapos;t caught signal 9 (no core).
2008 Jan 17 16:29:17 dc3-test %SYSGR-3-BASIC_TRACE: core_copy: PID 2579 with message Core not generated by system for eltm(0). WCOREDUMP(9) returned zero.
2008 Jan 17 16:29:17 dc3-test %SYSGR-2-SERVICE_CRASHED: Service \"eltm\" (PID 23294) hasnakapos;t caught signal 9 (no core).
2008 Jan 17 16:29:28 dc3-test %SYSGR-2-SWITCHOVER_PRE_START: This supervisor is becoming active (pre-start phase).
2008 Jan 17 16:29:28 dc3-test %SYSGR-2-SWITCHOVER_PRE_START: This supervisor is becoming active.
2008 Jan 17 16:29:26 dc3-test %USER-3-SYSTEM_MSG: crdcfg_get_srvinfo: mts_send failed - device_test
2008 Jan 17 16:29:27 dc3-test %NETSTACK-3-IP_UNK_MSG_MAJOR: netstack [4336] Unrecognized message from MRIB. Major type 1807
2008 Jan 17 16:29:27 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is DOWN in vdc 1
2008 Jan 17 16:29:27 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is DOWN in vdc 2
2008 Jan 17 16:29:27 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is DOWN in vdc 3
2008 Jan 17 16:29:27 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is DOWN in vdc 4
2008 Jan 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:socket family : 2 - ntpd[19045]
2008 Jan 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:socket family : 10 - ntpd[19045]
2008 Jan 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:ipv6 only defined - ntpd[19045]
2008 Jan 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:bindv6 only defined - ntpd[19045]
2008 Jan 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:socket family : 2 - ntpd[19045]
2008 Jan 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:socket family : 0 - ntpd[19045]
2008 Jan 17 16:29:28 dc3-test %NETSTACK-3-CLIENT_GET: netstack [4336] HA client filter recovery failed (0)
2008 Jan 17 16:29:28 dc3-test %NETSTACK-3-CLIENT_GET: netstack [4336] HA client filter recovery failed (0)
2008 Jan 17 16:29:29 dc3-test %DAEMON-3-SYSTEM_MSG: ssh disabled, removing - dcos-xinetd[19072]
2008 Jan 17 16:29:29 dc3-test %DAEMON-3-SYSTEM_MSG: Telnet disabled, removing - dcos-xinetd[19072]

Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.x 6-33
```
2008 Jan 17 16:29:31 dc3-test %DAEMON-3-SYSTEM_MSG: Telnet disabled, removing - dcos-xinetd[19073]
2008 Jan 17 16:29:32 dc3-test %DAEMON-3-SYSTEM_MSG: ssh disabled, removing - dcos-xinetd[19079]
2008 Jan 17 16:29:32 dc3-test %DAEMON-3-SYSTEM_MSG: Telnet disabled, removing - dcos-xinetd[19079]
2008 Jan 17 16:29:34 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is UP in vdc 1
2008 Jan 17 16:29:34 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is UP in vdc 2
2008 Jan 17 16:29:34 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is UP in vdc 3
2008 Jan 17 16:29:34 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is UP in vdc 4
2008 Jan 17 16:29:34 dc3-test %DAEMON-3-SYSTEM_MSG: ssh disabled, removing - dcos-xinetd[19105]
2008 Jan 17 16:29:34 dc3-test %DAEMON-3-SYSTEM_MSG: Telnet disabled, removing - dcos-xinetd[19105]
2008 Jan 17 16:29:35 dc3-test %PLATFORM-2-PS_AC_IN_MISSING: Power supply 2 present but all AC inputs are not connected, ac-redundancy might be affected
2008 Jan 17 16:29:35 dc3-test %PLATFORM-2-PS_AC_IN_MISSING: Power supply 3 present but all AC inputs are not connected, ac-redundancy might be affected
2008 Jan 17 16:29:38 dc3-test %CALLHOME-2-EVENT: SUP_FAILURE
2008 Jan 17 16:29:46 dc3-test vsh[19166]: CLIC-3-FAILED_EXEC: Can not exec command &lt;more&gt;&lt; return code &lt;14&gt;
2008 Jan 17 16:30:24 dc3-test vsh[23810]: CLIC-3-FAILED_EXEC: Can not exec command &lt;more&gt;&lt; return code &lt;14&gt;
2008 Jan 17 16:30:24 dc3-test vsh[23803]: CLIC-3-FAILED_EXEC: Can not exec command &lt;more&gt;&lt; return code &lt;14&gt;
2008 Jan 17 16:30:24 dc3-test vsh[23818]: CLIC-3-FAILED_EXEC: Can not exec command &lt;more&gt;&lt; return code &lt;14&gt;
2008 Jan 17 16:30:47 dc3-test %SYSMGR-3-BASIC_TRACE: core_copy: PID 2630 with message Core not generated by system for eltm(0). WCOREDUMP(9) returned zero.
2008 Jan 17 16:30:47 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID 4820) hasn't caught signal 9 (no core).
2008 Jan 17 16:31:02 dc3-test %SYSMGR-3-BASIC_TRACE: core_copy: PID 2630 with message Core not generated by system for eltm(0). WCOREDUMP(9) returned zero.
2008 Jan 17 16:31:02 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID 24239) hasn't caught signal 9 (no core).
2008 Jan 17 16:31:14 dc3-test %SYSMGR-3-BASIC_TRACE: core_copy: PID 2630 with message Core not generated by system for eltm(0). WCOREDUMP(9) returned zero.
2008 Jan 17 16:31:14 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID 24401) hasn't caught signal 9 (no core).
2008 Jan 17 16:31:23 dc3-test %CALLHOME-2-EVENT: SW_CRASH alert for service: eltm
2008 Jan 17 16:31:23 dc3-test %SYSMGR-3-BASIC_TRACE: core_copy: PID 2630 with message Core not generated by system for eltm(0). WCOREDUMP(9) returned zero.
2008 Jan 17 16:31:23 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID 24407) hasn't caught signal 9 (no core).
2008 Jan 17 16:31:24 dc3-test vsh[24532]: CLIC-3-FAILED_EXEC: Can not exec command &lt;more&gt;&lt; return code &lt;14&gt;
2008 Jan 17 16:31:24 dc3-test vsh[24548]: CLIC-3-FAILED_EXEC: Can not exec command &lt;more&gt;&lt; return code &lt;14&gt;
2008 Jan 17 16:31:24 dc3-test vsh[24535]: CLIC-3-FAILED_EXEC: Can not exec command &lt;more&gt;&lt; return code &lt;14&gt;
2008 Jan 17 16:31:33 dc3-test %NETSTACK-3-INTERNAL_ERROR: netstack [4336] (null)
2008 Jan 17 16:31:33 dc3-test %ETHPORT-2-IP_SEQ_ERROR: Error (0x20) while communicating with component MTS_SAP_ELTM opcode:MTS_OPC_ETHPM_PORT_PHY_CLEANUP (for RID_PORT: Ethernet3/1 )
 show vdc membership

Send document comments to nexus7k-docfeedback@cisco.com.
Chapter 6  Configuring Smart Call Home

Additional References

<table>
<thead>
<tr>
<th>vdc_id</th>
<th>vdc_name</th>
<th>interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>dc3-aaa</td>
<td>Ethernet3/22, Ethernet3/23, Ethernet3/24</td>
</tr>
<tr>
<td>3</td>
<td>dc3-rbac</td>
<td>Ethernet3/25, Ethernet3/26, Ethernet3/27</td>
</tr>
<tr>
<td>4</td>
<td>dc3-call</td>
<td>Ethernet3/28, Ethernet3/29, Ethernet3/30</td>
</tr>
</tbody>
</table>

vdc_id: 2 vdc_name: dc3-aaa interfaces:

vdc_id: 3 vdc_name: dc3-rbac interfaces:

vdc_id: 4 vdc_name: dc3-call interfaces:

```xml
<soap-env:Body>
  <aml-block:Attachment type="inline">
    <aml-block:Name>show vdc current-vdc</aml-block:Name> <aml-block:Data encoding="plain">
      <![CDATA[Current vdc is 1 - dc3-test ]]> </aml-block:Data> 
  </aml-block:Attachment> 
  <aml-block:Attachment type="inline">
    <aml-block:Name>show license usage</aml-block:Name> 
    <aml-block:Data encoding="plain">
      <![CDATA[Feature                      Ins  Lic   Status Expiry Date Comments
             Count                        ]]> 
      LAN_ADVANCED_SERVICES_PKG     Yes   -   In use Never   -                      
      LAN_ENTERPRISE_SERVICES_PKG   Yes   -   Unused Never  -                      ]]> 
    </aml-block:Data> 
  </aml-block:Attachment>
</soap-env:Body>
```

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Home CLI commands</td>
<td>Cisco Nexus 7000 Series NX-OS System Management Command Reference</td>
</tr>
<tr>
<td>VDCs and VRFs</td>
<td>Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.x</td>
</tr>
</tbody>
</table>
Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>—</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISCO-CALLHOME-MIB</td>
<td>To locate and download MIBs, go to the following URL: <a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a></td>
</tr>
</tbody>
</table>

Feature History for Smart Call Home

Table 6-11 lists the release history for this feature.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Profile Configuration</td>
<td>4.1(3)</td>
<td>The commands <code>destination profile http</code> and <code>destination profile transport-method</code> cannot be distributed. See the “Modifying a Destination Profile” section on page 6-13.</td>
</tr>
</tbody>
</table>
CHAPTER 7

Configuring Rollback

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

This chapter includes the following sections:

- Information About Rollback, page 7-1
- Licensing Requirements, page 7-3
- Prerequisites for Rollback, page 7-3
- Guidelines and Limitations, page 7-3
- Configuring Rollback, page 7-4
- Verifying the Rollback Configuration, page 7-6
- Rollback Example Configuration, page 7-7
- Default Settings, page 7-7
- Additional References, page 7-7
- Feature History for Rollback, page 7-8

Information About Rollback

This section includes the following topics:

- Rollback Overview, page 7-1
- Automatically Generated System Checkpoints, page 7-2
- High Availability, page 7-2
- Virtualization Support, page 7-3

Rollback Overview

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 device at any point without having to reload the device. A rollback allows any authorized administrator to apply this checkpoint configuration without requiring expert knowledge of the features configured in the checkpoint.

Cisco NX-OS automatically creates system checkpoints as described in the “Automatically Generated System Checkpoints” section on page 7-2. You can use either a user or system checkpoint to perform a rollback.
Information About Rollback

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

When you roll back the running configuration, you can trigger the following rollback types:

- **atomic**—Implement a rollback only if no errors occur.
- **best-effort**—Implement a rollback and skip any errors.
- **stop-at-first-failure**—Implement a rollback that stops if an error occurs.

The default rollback type is atomic.

When you are ready to roll back to a checkpoint configuration, you can view the changes that will be applied to your current running configuration before committing to the rollback operation. If an error occurs during the rollback operation, you can choose to cancel the operation, or ignore the error and proceed with the rollback. If you cancel the operation, Cisco NX-OS provides a list of changes already applied before the error occurred. You need to clean up these changes manually.

Automatically Generated System Checkpoints

The Cisco NX-OS software automatically generates system checkpoints to help you avoid a loss of configuration information. System checkpoints are generated by the following events:

- Disabling an enabled feature with the `no feature` command
- Removing an instance of a Layer 3 protocol, such as with the `no router bgp` command or the `no ip pim sparse-mode` command
- License expiration of a feature

If one of these events causes system configuration changes, the feature software creates a system checkpoint that you can use to roll back to the previous system configuration.

The system generated checkpoint file names begin with “system-” and include the feature name. For example, the first time that you disable the EIGRP feature, the system creates the checkpoint named `system-fm__inst_1__eigrp`.

High Availability

Whenever a checkpoint is created using the `checkpoint` or `checkpoint checkpoint_name` commands, the checkpoint is synchronized to the standby unit.

Rollback remembers the states of the checkpoint operation, so if the checkpoint operation is interrupted and the system is left in an inconsistent state, rollback can complete the checkpoint operation (synchronize the checkpoint with the standby unit) before proceeding with the rollback operation.

Your checkpoint files are still available after a process restart or supervisor switchover. Even if there is an interruption during the process restart or supervisor switchover, the checkpoint will complete successfully before proceeding with the operation. In a supervisor switchover, the checkpoint is completed on the new active unit.

If a process restart or supervisor switchover occurs during a rollback operation, after the restart or switchover completes, the rollback will resume from its previous state and complete successfully.
Virtualization Support

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

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

Licensing Requirements

Prerequisites for Rollback

If you configure VDCs, install the Advanced Services license and go to the specific VDC. For more information, see the Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.x.

To configure the rollback feature, you must have network-admin or vdc-admin user privileges.

Guidelines and Limitations

Rollback has the following configuration guidelines and limitations:

- You can create up to ten checkpoint copies per VDC.
- You cannot apply the checkpoint file of one VDC into another VDC.
- You cannot apply a checkpoint configuration in a nondefault VDC if there is a change in the global configuration portion of the running configuration compared to the checkpoint configuration.
- Your checkpoint file names must be 75 characters or less.
- You cannot start a checkpoint filename with the word system.
- Beginning in Cisco NX-OS Release 4.2(1), you can start a checkpoint filename with the word auto.
- Beginning in Cisco NS-OS Release 4.2(1), you can name a checkpoint file summary or any abbreviation of the word summary.
- Only one user can perform a checkpoint, rollback, or copy the running configuration to the startup configuration at the same time in a VDC.
- After the system executes the write erase or reload command, checkpoints are deleted. You can use the clear checkpoint database command to clear out all checkpoint files.
Configuring Rollback

This section includes the following topics:

- Creating a Checkpoint, page 7-4
- Implementing a Rollback, page 7-5

Note

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

Creating a Checkpoint

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

BEFORE YOU BEGIN

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

SUMMARY STEPS

1. `checkpoint { [cp-name] [description descr] | file file-name }
   no checkpoint cp-name
2. `show checkpoint cp-name [all]`
Configuring Rollback

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>`checkpoint ([cp-name] [description descr]</td>
<td>file file-name)`</td>
</tr>
<tr>
<td>Example: <code>switch# checkpoint stable</code></td>
<td></td>
</tr>
<tr>
<td><code>no checkpoint cp-name</code></td>
<td>You can use the <code>no</code> form of the <code>checkpoint</code> command to remove a checkpoint name. Use the <code>delete</code> command to remove a checkpoint file.</td>
</tr>
<tr>
<td>Example: <code>switch# no checkpoint stable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>(Optional) Displays the contents of the checkpoint name.</td>
</tr>
<tr>
<td><code>show checkpoint cp-name [all]</code></td>
<td></td>
</tr>
<tr>
<td>Example: <code>switch# show checkpoint stable</code></td>
<td></td>
</tr>
</tbody>
</table>

Implementing a Rollback

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

For information about automatically generated system checkpoints, see the “Automatically Generated System Checkpoints” section on page 7-2.

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

BEFORE YOU BEGIN

You are logged in to the device in EXEC mode for the correct VDC. To go to the correct VDC, use the `switchto vdc` command.

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 | best-effort | stop-at-first-failure]`
## Verifying the Rollback Configuration

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show checkpoint name [all]</td>
<td>Displays the contents of the checkpoint name.</td>
</tr>
<tr>
<td>show checkpoint all [user</td>
<td>system]</td>
</tr>
<tr>
<td>show checkpoint summary [user</td>
<td>system]</td>
</tr>
<tr>
<td>show diff rollback-patch {checkpoint src-cp-name</td>
<td>running-config</td>
</tr>
<tr>
<td>show rollback log [exec</td>
<td>verify]</td>
</tr>
</tbody>
</table>
Use the `clear checkpoint database` command to delete all checkpoint files.

## Rollback Example Configuration

This example shows how to create a checkpoint file and then implements a best-effort rollback to a user checkpoint name:

```
checkpoint stable
rollback running-config checkpoint stable best-effort
```

## Default Settings

Table 7-1 lists the default settings for rollback parameters.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>rollback type</td>
<td>atomic</td>
</tr>
</tbody>
</table>

## Additional References

For additional information related to implementing a rollback, see the following sections:
- Related Documents, page 7-8
- Standards, page 7-8
Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rollback CLI commands</td>
<td>Cisco Nexus 7000 Series NX-OS System Management Command Reference</td>
</tr>
<tr>
<td>configuration files</td>
<td>Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 4.x</td>
</tr>
<tr>
<td>VDCs</td>
<td>Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.x</td>
</tr>
</tbody>
</table>

Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>—</td>
</tr>
</tbody>
</table>

Feature History for Rollback

Table 7-2 lists the release history for this feature.

Table 7-2 Feature History for Rollback

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Availability</td>
<td>4.2(1)</td>
<td>Checkpoint and rollback operations support high availability.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See the “High Availability” section on page 7-2.</td>
</tr>
<tr>
<td>Guidelines and Limitations</td>
<td>4.2(1)</td>
<td>Checkpoint file naming conventions changed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rollback to files on bootflash is supported only on files created using the checkpoint checkpoint_name command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See the “Guidelines and Limitations” section on page 7-3.</td>
</tr>
<tr>
<td>Automatically generated system checkpoints</td>
<td>4.2(1)</td>
<td>The software automatically generates a system checkpoint when disabling a feature or license expiration could cause loss of configuration information.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See the “Automatically Generated System Checkpoints” section on page 7-2.</td>
</tr>
<tr>
<td>Guidelines and Limitations</td>
<td>4.1(3)</td>
<td>A rollback fails for NetFlow if during rollback, you try to modify a record that is programmed in the hardware.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A rollback is not supported for checkpoints across software versions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See the “Guidelines and Limitations” section on page 7-3.</td>
</tr>
</tbody>
</table>
Configuring Session Manager

This chapter describes how to configure Session Manager on Cisco NX-OS devices. This chapter includes the following sections:

- Information About Session Manager, page 8-1
- Licensing Requirements for Session Manager, page 8-2
- Prerequisites for Session Manager, page 8-2
- Guidelines and Limitations, page 8-2
- Configuring Session Manager, page 8-3
- Verifying the Session Manager Configuration, page 8-6
- Session Manager Example Configuration, page 8-6
- Additional References, page 8-7

Information About Session Manager

This section includes the following topics:

- Session Manager Overview, page 8-1
- High Availability, page 8-2
- Virtualization Support, page 8-2

Session Manager Overview

Session Manager allows you to implement configuration changes in batch mode, using the following phases:

- Configuration session—Creates a list of commands that you want to implement in Session Manager mode.
- Validation—Provides a basic semantic check on your configuration. Cisco NX-OS returns an error if the semantic check fails on any part of the configuration.
- Verification—Verifies the configuration as a whole, based on the existing hardware and software configuration and resources. Cisco NX-OS returns an error if the configuration does not pass this verification phase.
**Commit**—Cisco NX-OS verifies the complete configuration and applies the changes to the device. If a failure occurs, Cisco NX-OS reverts to the original configuration.

**Abort**—Discards the configuration changes before implementation.

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

**High Availability**

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

**Virtualization Support**

By default, Cisco NX-OS places you in the default VDC. See the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.x*.

**Licensing Requirements for Session Manager**

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

**Prerequisites for Session Manager**

If you configure VDCs, install the Advanced Services license and go to the specific VDC. For more information, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.x*.

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

**Guidelines and Limitations**

Session Manager has the following configuration guidelines and limitations:

- Session Manager supports only the ACL and QoS features.
- You can create up to 32 configuration sessions per VDC.
- You cannot issue an in-service software upgrade (ISSU) if an active session is in progress. You must commit the session, save it, or abort it before issuing an ISSU.
- You can configure a maximum of 20,000 commands across all sessions in a VDC.
You cannot simultaneously execute configuration commands in more than one configuration session or configuration terminal mode. Parallel configurations (for example, one configuration session and one configuration terminal) may cause validation or verification failures in the configuration session.

If an interface reloads while you are configuring that interface in a configuration session, Session Manager may accept the commands even though the interface is not present in the device at that time.

### Configuring Session Manager

This section includes the following topics:
- Creating a Session, page 8-3
- Configuring ACLs in a Session, page 8-4
- Verifying a Session, page 8-5
- Committing a Session, page 8-5
- Saving a Session, page 8-5
- Discarding a Session, page 8-6

**Note**

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

### Creating a Session

You can create up to 32 configuration sessions.

**BEFORE YOU BEGIN**

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

**SUMMARY STEPS**

1. `configure session name`
2. `show configuration session [name]`
3. `save location`
DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure session name</td>
<td>Creates a configuration session and enters session configuration mode. The name can be any alphanumeric string.</td>
</tr>
<tr>
<td>show configuration session [name]</td>
<td>(Optional) Displays the contents of the session.</td>
</tr>
<tr>
<td>save location</td>
<td>(Optional) Saves the session to a file. The location can be in bootflash:, slot0:, or volatile:</td>
</tr>
</tbody>
</table>

Configuring ACLs in a Session

You can configure ACLs within a configuration session.

BEFORE YOU BEGIN

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

SUMMARY STEPS

1. configure session name
2. ip access-list name
3. permit protocol source destination
4. interface interface-type number
5. ip access-group name {in | out}
6. show configuration session [name]

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure session name</td>
<td>Creates a configuration session and enters session configuration mode. The name can be any alphanumeric string.</td>
</tr>
<tr>
<td>ip access-list name</td>
<td>Creates an ALC and enters a configuration mode for that ACL.</td>
</tr>
</tbody>
</table>
# Configuring Session Manager

## Step 3: Configuring a Session

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong> permit protocol source destination</td>
<td>(Optional) Adds a permit statement to the ACL</td>
</tr>
</tbody>
</table>

**Example:**
```
switch(config-s-acl)# permit tcp any any
```

## Step 4: Committing a Session

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong> interface interface-type number</td>
<td>Enters interface configuration mode</td>
</tr>
</tbody>
</table>

**Example:**
```
switch(config-s-acl)# interface e 2/1
switch(config-s-if)#
```

## Step 5: Saving a Session

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong> ip access-group name in</td>
<td>Specifies the direction of traffic the access group is applied to.</td>
</tr>
</tbody>
</table>

**Example:**
```
switch(config-s-if)# ip access-group acl1 in
```

## Verifying a Session

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

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

**Example:**
```
switch(config-s)# verify
```

## Committing a Session

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

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

**Example:**
```
switch(config-s)# commit
```

## Saving a Session

Use the following command in session mode to save a session:
Verifying the Session Manager Configuration

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

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

Session Manager Example Configuration

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

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

For additional information related to implementing Session Manager, see the following sections:

- Related Documents, page 8-7
- Standards, page 8-7

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Manager CLI commands</td>
<td><em>Cisco Nexus 7000 Series NX-OS System Management Command Reference</em></td>
</tr>
<tr>
<td>configuration files</td>
<td><em>Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 4.x</em></td>
</tr>
<tr>
<td>VDCs</td>
<td><em>Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.x</em></td>
</tr>
</tbody>
</table>

Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
</tr>
</tbody>
</table>
CHAPTER 9

Configuring the Scheduler

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

This chapter includes the following sections:

- Information About the Scheduler, page 9-1
- Licensing Requirements for the Scheduler, page 9-3
- Prerequisites for the Scheduler, page 9-3
- Guidelines and Limitations, page 9-3
- Configuring the Scheduler, page 9-3
- Verifying the Scheduler Configuration, page 9-12
- Scheduler Example Configurations, page 9-12
- Default Settings, page 9-14
- Additional References, page 9-14

Information About the Scheduler

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

- Quality of Service policy changes
- Data backup
- Saving a configuration

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

This section includes the following topics:

- Scheduler Overview, page 9-2
- Remote User Authentication, page 9-2
- Logs, page 9-2
- High Availability, page 9-2
- Virtualization Support, page 9-2
Information About the Scheduler

Send document comments to nexus7k-docfeedback@cisco.com.

Chapter 9 Configuring the Scheduler

Scheduler Overview

The scheduler defines a job and its timetable as follows:

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

Remote User Authentication

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

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

Logs

The scheduler maintains a log file containing the job output. If the size of the job output is greater than the size of the log file, then the output is truncated. For more information, see the “Defining the Scheduler Log File Size” procedure on page 9-5.

High Availability

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

Virtualization Support

Jobs are created in the virtual device context (VDC) that you are logged into. By default, Cisco NX-OS places you in the default VDC. For more information, see the Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.x.
Chapter 9      Configuring the Scheduler

Licensing Requirements for the Scheduler

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

Prerequisites for the Scheduler

The scheduler has the following prerequisites:

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

Guidelines and Limitations

The scheduler has the following configuration guidelines and limitations:

- The scheduler can fail if it encounters one of the following while performing a job:
  - If the license has expired for a feature at the time the job for that feature is scheduled.
  - If a feature is disabled at the time when a job for that feature is scheduled.
  - If you have removed a module from a slot and a job for that slot is scheduled.
- Verify that you have configured the time. The scheduler does not apply a default timetable. If you create a schedule and assign jobs and do not configure the time, the job is not started.
- While defining a job, verify that no interactive or disruptive commands (for example, `copy bootflash: file ftp: URI`, `write erase`, and other similar commands) are specified because the job is started and conducted noninteractively.

Configuring the Scheduler

This section includes the following topics:

- Enabling the Scheduler, page 9-4
- Defining the Scheduler Log File Size, page 9-5
- Configuring Remote User Authentication, page 9-5
- Defining a Job, page 9-6
- Deleting a Job, page 9-7
- Defining a Timetable, page 9-8
- Clearing the Scheduler Log File, page 9-10
- Disabling the Scheduler, page 9-11
Enabling the Scheduler

You can enable the scheduler feature so that you can configure and schedule jobs.

BEFORE YOU BEGIN

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

SUMMARY STEPS

1. config t
2. feature scheduler
3. show scheduler config
4. copy running-config startup-config

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> config t</td>
<td>Places you in global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> switch# config t</td>
<td>Enter configuration commands, one per line. End with CNTL/Z. switch(config)#</td>
</tr>
<tr>
<td><strong>Step 2</strong> feature scheduler</td>
<td>Enables the scheduler in the current VDC.</td>
</tr>
<tr>
<td><strong>Example:</strong> switch(config)# feature scheduler</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> show scheduler config</td>
<td>(Optional) Displays the scheduler configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong> switch(config)# show scheduler config config terminal feature scheduler scheduler logfile size 16 end switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> copy running-config startup-config</td>
<td>(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong> switch(config)# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>
Defining the Scheduler Log File Size

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

**BEFORE YOU BEGIN**

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

**SUMMARY STEPS**

1. `config t`
2. `scheduler logfile size value`
3. `copy running-config startup-config`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>config t</code></td>
<td>Places you in global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> switch# config t Enter configuration commands, one per line. End with CNTL/Z. switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>scheduler logfile size value</code></td>
<td>Defines the scheduler log file size in kilobytes. The range is from 16 to 1024. The default is 16. Note: If the size of the job output is greater than the size of the log file, then the output is truncated.</td>
</tr>
<tr>
<td><strong>Example:</strong> switch(config)# scheduler logfile size 1024</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>copy running-config startup-config</code></td>
<td>(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong> switch(config)# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

**Configuring Remote User Authentication**

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

**Note** Remote users must authenticate with their clear text password before creating and configuring jobs.

**Note** Remote user passwords are always shown in encrypted form in the output of the `show running-config` command. The encrypted option (7) in the command supports the ASCII device configuration.

**BEFORE YOU BEGIN**

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

SUMMARY STEPS

1. `config t`
2. `scheduler aaa-authentication password [0 | 7] password`
3. `scheduler aaa-authentication username name password [0 | 7] password`
4. `show running-config | include "scheduler aaa-authentication"`
5. `copy running-config startup-config`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>config t</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch# config t Enter configuration commands, one per line. End with CNTL/Z. switch(config)#</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>`scheduler aaa-authentication password [0</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config)# scheduler aaa-authentication password X12y34Z56a</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>`scheduler aaa-authentication username name password [0</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config)# scheduler aaa-authentication username newuser password Z98y76X54b</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>`show running-config</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config)# show running-config</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>copy running-config startup-config</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config)# copy running-config startup-config</td>
</tr>
</tbody>
</table>

Defining a Job

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

⚠️ Caution

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

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

SUMMARY STEPS

1. `config t`
2. `scheduler job name string`
3. `command1 ; [command2 ; command3 ; ... ]`
4. `show scheduler job [name]`
5. `copy running-config startup-config`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Placing you in global configuration mode.</strong></td>
</tr>
<tr>
<td><strong>config t</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch# config t</td>
<td></td>
</tr>
<tr>
<td>Enter configuration commands, one per line.</td>
<td></td>
</tr>
<tr>
<td>End with CNTL/Z.</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Creates a job and enters job configuration mode.</strong></td>
</tr>
<tr>
<td><strong>scheduler job name string</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config)# scheduler job name backup-cfg</td>
<td></td>
</tr>
<tr>
<td>switch(config-job)</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Defines the sequence of commands for the specified job.</strong></td>
</tr>
<tr>
<td><strong>command1 ; [command2 ; command3 ; ... ]</strong></td>
<td><strong>You must separate commands with a space and a semicolon (for example, “ ;”).</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>This example creates a scheduler job that saves the running configuration to a file in bootflash and then copies the file from bootflash to a TFTP server. The file name is created using the current time stamp and switch name.</strong></td>
</tr>
<tr>
<td>switch(config-job)# cli var name timestamp</td>
<td></td>
</tr>
<tr>
<td>$(TIMESTAMP) ; copy running-config bootflash:/$(SWITCHNAME)-cfg.$(timestamp) ; copy bootflash:/$(SWITCHNAME)-cfg.$(timestamp) tftp://1.2.3.4/vrf management</td>
<td></td>
</tr>
<tr>
<td>switch(config-job)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>(Optional) Displays the job information.</strong></td>
</tr>
<tr>
<td><strong>show scheduler job [name]</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config-job)# show scheduler job</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.</strong></td>
</tr>
<tr>
<td><strong>copy running-config startup-config</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config-job)# copy running-config</td>
<td></td>
</tr>
<tr>
<td>startup-config</td>
<td></td>
</tr>
</tbody>
</table>

Deleting a Job

You can delete a job from the scheduler.
Configuring the Scheduler

BEFORE YOU BEGIN

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

SUMMARY STEPS

1. `config t`
2. `no scheduler job name string`
3. `show scheduler job [name]`
4. `copy running-config startup-config`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>config t</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>switch# config t</code> Enter configuration commands, one per line. End with CNTL/Z. <code>switch(config)#</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>no scheduler job name string</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>switch(config)# no scheduler job name configsave switch(config-job)</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>show scheduler job [name]</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>switch(config-job)# show scheduler job name configsave</code></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>copy running-config startup-config</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>switch(config)# copy running-config startup-config</code></td>
</tr>
</tbody>
</table>

Defining a Timetable

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

If you do not specify the time for the `time` commands, the scheduler assumes the current time. For example, if the current time is March 24, 2008, 22:00 hours, then jobs are started as follows:

- For the `time start 23:00 repeat 4:00:00` command, the scheduler assumes a start time of March 24, 2008, 23:00 hours.
- For the `time daily 55` command, the scheduler assumes a start time every day at 22:55 hours.
- For the `time weekly 23:00` command, the scheduler assumes a start time every Friday at 23:00 hours.
For the time monthly 23:00 command, the scheduler assumes a start time on the 24th of every month at 23:00 hours.

Note
The scheduler will not begin the next occurrence of a job before the last one completes. For example, you have scheduled a job to be completed at one-minute intervals beginning at 22:00; but the job requires two minutes to complete. The scheduler starts the first job at 22:00, completes it at 22:02, and then observes a one-minute interval before starting the next job at 22:03.

BEFORE YOU BEGIN
Make sure that you are in the correct VDC. To change the VDC, use the switch to vdc command.

SUMMARY STEPS

1. config t
2. scheduler schedule name string
3. job name string
4. time daily time
time weekly [[dow:] HH:]MM
time monthly [[dm:] HH:] MM
time start {now repeat repeat-interval | delta-time [repeat repeat-interval]}
5. show scheduler schedule [name]
6. copy running-config startup-config

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 config t</td>
<td>Places you in global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch# config t</td>
</tr>
<tr>
<td></td>
<td>Enter configuration commands, one per line. End with CNTL/Z.</td>
</tr>
<tr>
<td></td>
<td>switch(config)#</td>
</tr>
<tr>
<td>Step 2 scheduler schedule name string</td>
<td>Creates a new schedule and places you in schedule configuration mode for that schedule.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# scheduler schedule name weekendbackupqos</td>
</tr>
<tr>
<td></td>
<td>switch(config-schedule)#</td>
</tr>
<tr>
<td>Step 3 job name string</td>
<td>Associates a job with this schedule. You can add multiple jobs to a schedule.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config-schedule)# job name offpeakZoning</td>
</tr>
</tbody>
</table>
## Configuring the Scheduler

### Clearing the Scheduler Log File

You can clear the scheduler log file.

**BEFORE YOU BEGIN**

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

---

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>time daily time</code></td>
<td>Indicates the job starts every day at a designated time specified as HH:MM.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> switch(config-schedule)# time daily 23:00</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>time weekly [{dow:}HH:]MM</code></td>
<td>Indicates that the job starts on a specified day of the week.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> switch(config-schedule)# time weekly Sun:23:00</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>time monthly [{dm:}HH:]MM</code></td>
<td>Indicates the job starts on a specified day each month (dm). If you specify either 29, 30, or 31, the job is started on the last day of each month.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> switch(config-schedule)# time monthly 28:23:00</td>
<td></td>
</tr>
<tr>
<td></td>
<td>`time start {now repeat repeat-interval</td>
<td>delta-time [repeat repeat-interval]}`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> switch(config-schedule)# time start now repeat 48:00</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>show scheduler config</code></td>
<td>(Optional) Displays the scheduler configuration.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> switch(config)# show scheduler config</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> switch(config)# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>
SUMMARY STEPS

1. `config t`
2. `clear scheduler logfile`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>config t</code></td>
<td>Places you in global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> switch# config t Enter configuration commands, one per line. End with CNTL/Z. switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>clear scheduler logfile</code></td>
<td>Clears the scheduler log file.</td>
</tr>
<tr>
<td><strong>Example:</strong> switch(config)# clear scheduler logfile</td>
<td></td>
</tr>
</tbody>
</table>

Disabling the Scheduler

You can disable the scheduler feature.

BEFORE YOU BEGIN

The scheduler feature must be enabled before you can configure and schedule jobs. Make sure that you are in the correct VDC. To change the VDC, use the `switchto vdc` command.

SUMMARY STEPS

1. `config t`
2. `no feature scheduler`
3. `show scheduler config`
4. `copy running-config startup-config`
Verifying the Scheduler Configuration

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>config t</td>
<td>Places you in global configuration mode.</td>
</tr>
<tr>
<td>no feature scheduler</td>
<td>Disables the scheduler in the current VDC.</td>
</tr>
<tr>
<td>show scheduler config</td>
<td>(Optional) Displays the scheduler configuration. In this example, the</td>
</tr>
<tr>
<td></td>
<td>scheduler feature is disabled so the command is not recognized.</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Saves the change persistently through reboots and restarts</td>
</tr>
<tr>
<td></td>
<td>by copying the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

### Command or Action

- `show scheduler config`: Displays the scheduler configuration.
- `show scheduler job [name string]`: Displays the jobs configured.
- `show scheduler logfile`: Displays the contents of the scheduler log file.
- `show scheduler schedule [name string]`: Displays the schedules configured.

### Scheduler Example Configurations

This section includes the following topics:

- Creating a Scheduler Job, page 9-13
- Scheduling a Scheduler Job, page 9-13
- Displaying the Job Schedule, page 9-13
- Displaying the Results of Running Scheduler Jobs, page 9-13
Creating a Scheduler Job

This example shows how to create a scheduler job that saves the running configuration to a file in bootflash and then copies the file from bootflash to a TFTP server (the filename is created using the current time stamp and switch name):

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

Scheduling a Scheduler Job

This example shows how to schedule a scheduler job called backup-cfg to run daily at 1 a.m.:

```
switch# config t
switch(config)# scheduler schedule name daily
switch(config-if)# job name backup-cfg
switch(config-if)# time daily 1:00
switch(config-if)# end
switch(config)#
```

Displaying the Job Schedule

This example shows how to display the job schedule:

```
switch# show scheduler schedule
Schedule Name : daily
User Name : admin
Schedule Type : Run every day at 1 Hrs 00 Mins
Last Execution Time : Fri Jan 2 1:00:00 2009
Last Completion Time: Fri Jan 2 1:00:01 2009
Execution count : 2

Job Name            Last Execution Status
back-cfg                          Success (0)
```

Displaying the Results of Running Scheduler Jobs

This example shows how to display the results of scheduler jobs that have been executed by the scheduler:

```
switch# show scheduler logfile
Job Name       : back-cfg                          Job Status: Failed (1)
Schedule Name  : daily                            User Name : admin
Completion time: Fri Jan 1 1:00:01 2009
--------------------------------- Job Output ---------------------------------
`cli var name timestamp 2009-01-01-01.00.00`
```
Default Settings

Table 9-1 lists the scheduler default settings.

Table 9-1 Default Command Scheduler Parameters

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

Additional References

For additional information related to the scheduler, see the following sections:

- Related Documents, page 9-14
- Standards, page 9-15

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduler CLI commands</td>
<td>Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.x</td>
</tr>
<tr>
<td>VDCs</td>
<td>Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.x</td>
</tr>
</tbody>
</table>
Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support</td>
<td></td>
</tr>
<tr>
<td>for existing standards has not been modified by this feature.</td>
<td></td>
</tr>
</tbody>
</table>
CHAPTER 10

Configuring SNMP

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

This chapter includes the following sections:

- Information About SNMP, page 10-1
- Licensing Requirements for SNMP, page 10-7
- Prerequisites for SNMP, page 10-7
- Guidelines and Limitations, page 10-8
- Configuring SNMP, page 10-8
- Verifying SNMP Configuration, page 10-24
- SNMP Example Configurations, page 10-24
- Default Settings, page 10-25
- Additional References, page 10-25
- Feature History for SNMP, page 10-26

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.

This section includes the following topics:

- SNMP Functional Overview, page 10-2
- SNMP Notifications, page 10-2
- SNMPv3, page 10-3
- SNMP and Embedded Event Manager, page 10-6
- Multiple Instance Support, page 10-6
- High Availability, page 10-7
- Virtualization Support, page 10-7
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. Cisco NX-OS supports the agent and MIB. To enable the SNMP agent, you must define the relationship between the manager and the agent.

- A managed information base (MIB)—The collection of managed objects on the SNMP agent.

SNMP is defined in RFCs 3411 to 3418.

Cisco NX-OS supports SNMPv1, SNMPv2c, and SNMPv3. Both SNMPv1 and SNMPv2c use a community-based form of security.

Cisco NX-OS supports SNMP over IPv6.

SNMP Notifications

A key feature of SNMP is the ability to generate notifications from an SNMP agent. These notifications do not require that requests be sent from the SNMP manager. Notifications can indicate improper user authentication, restarts, the closing of a connection, loss of a connection to a neighbor router, or other significant events.

Cisco NX-OS generates SNMP notifications as either traps or informs. A trap is an asynchronous, unacknowledged message sent from the agent to the SNMP managers listed in the host receiver table (see the “Configuring SNMP Notification Receivers with VRFs” section on page 10-14). Informs are asynchronous messages sent from the SNMP agent to the SNMP manager which the manager must acknowledge receipt of.

Traps are less reliable than informs because the SNMP manager does not send any acknowledgment when it receives a trap. Cisco NX-OS 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 Cisco NX-OS never receives a response, it can send the inform request again.

You can configure Cisco NX-OS to send notifications to multiple host receivers. See the “Configuring SNMP Notification Receivers” section on page 10-11 for more information about host receivers.

Table 10-1 lists the SNMP traps that are enabled by default.

<table>
<thead>
<tr>
<th>Trap Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>generic</td>
<td>: coldStart</td>
</tr>
<tr>
<td>generic</td>
<td>: warmStart</td>
</tr>
<tr>
<td>entity</td>
<td>: entity_mib_change</td>
</tr>
<tr>
<td>entity</td>
<td>: entity_module_status_change</td>
</tr>
<tr>
<td>entity</td>
<td>: entity_power_status_change</td>
</tr>
<tr>
<td>entity</td>
<td>: entity_moduleInserted</td>
</tr>
<tr>
<td>entity</td>
<td>: entity_moduleRemoved</td>
</tr>
<tr>
<td>entity</td>
<td>: entity_unrecognised_module</td>
</tr>
</tbody>
</table>

Table 10-1 SNMP Traps Enabled By Default
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 as follows:

- **Message integrity**—Ensures that a packet has not been tampered with while it was in-transit.
- **Authentication**—Determines that 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.

This section includes the following topics:

- **Security Models and Levels for SNMPv1, v2, v3**, page 10-4
- **User-Based Security Model**, page 10-4
- **CLI and SNMP User Synchronization**, page 10-5
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. Table 10-2 identifies what the combinations of security models and levels mean.

### Table 10-2 SNMP Security Models and Levels

<table>
<thead>
<tr>
<th>Model</th>
<th>Level</th>
<th>Authentication</th>
<th>Encryption</th>
<th>What Happens</th>
</tr>
</thead>
<tbody>
<tr>
<td>v1</td>
<td>noAuthNoPriv</td>
<td>Community string</td>
<td>No</td>
<td>Uses a community string match for authentication.</td>
</tr>
<tr>
<td>v2c</td>
<td>noAuthNoPriv</td>
<td>Community string</td>
<td>No</td>
<td>Uses a community string match for authentication.</td>
</tr>
<tr>
<td>v3</td>
<td>noAuthNoPriv</td>
<td>Username</td>
<td>No</td>
<td>Uses a username match for authentication.</td>
</tr>
<tr>
<td>v3</td>
<td>authNoPriv</td>
<td>HMAC-MD5 or HMAC-SHA</td>
<td>No</td>
<td>Provides authentication based on the Hash-Based Message Authentication Code (HMAC) Message Digest 5 (MD5) algorithm or the HMAC Secure Hash Algorithm (SHA).</td>
</tr>
<tr>
<td>v3</td>
<td>authPriv</td>
<td>HMAC-MD5 or HMAC-SHA</td>
<td>DES</td>
<td>Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard.</td>
</tr>
</tbody>
</table>

User-Based Security Model

The SNMPv3 User-Based Security Model (USM) refers to SNMP message-level security and offers the following services:

- Message integrity—Ensures that messages have not been altered or destroyed in an unauthorized manner and that data sequences have not been altered to an extent greater than can occur nonmaliciously.
- Message origin authentication—Ensures that the claimed identity of the user on whose behalf received data was originated is confirmed.
Message confidentiality—Ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes.

SNMPv3 authorizes management operations only by configured users and encrypts SNMP messages. Cisco NX-OS uses two authentication protocols for SNMPv3:

- HMAC-MD5-96 authentication protocol
- HMAC-SHA-96 authentication protocol

Cisco NX-OS uses Advanced Encryption Standard (AES) as one of the privacy protocols for SNMPv3 message encryption and conforms with RFC 3826.

The `priv` option offers a choice of DES or 128-bit AES encryption for SNMP security encryption. The `priv` option and the `aes-128` token indicate that this privacy password is for generating a 128-bit AES key. The AES `priv` password can have a minimum of eight characters. If the passphrases are specified in clear text, you can specify a maximum of 64 case-sensitive alphanumeric characters. If you use the localized key, you can specify a maximum of 130 characters.

**Note** For an SNMPv3 operation that uses the external AAA server, you must use AES for the privacy protocol in the user configuration on the external AAA server.

CLI and SNMP User Synchronization

SNMPv3 user management can be centralized at the Access Authentication and Accounting (AAA) server level. This centralized user management allows the SNMP agent in Cisco NX-OS to leverage the user authentication service of the AAA server. Once user authentication is verified, the SNMP PDUs are processed further. Additionally, the AAA server is also used to store user group names. SNMP uses the group names to apply the access/role policy that is locally available in the switch.

Any configuration changes made to the user group, role, or password results in database synchronization for both SNMP and AAA.

Cisco NX-OS synchronizes user configuration in the following ways:

- The authentication passphrase specified in the `snmp-server user` command becomes the password for the CLI user.
- The password specified in the `username` command becomes the authentication and privacy passphrases for the SNMP user.
- If you create or delete a user using either SNMP or the CLI, the user is created or deleted for both SNMP and the CLI.
- User-role mapping changes are synchronized in SNMP and the CLI.
- Role changes (deletions or modifications) from the CLI are synchronized to SNMP.

**Note** When you configure a passphrase/password in localized key/encrypted format, Cisco NX-OS does not synchronize the user information (password, roles, and so on).

Cisco NX-OS holds the synchronized user configuration for 60 minutes by default. See the “Modifying the AAA Synchronization Time” section on page 10-23 for information on how to modify this default value.
Information About SNMP

Group-Based SNMP Access

Because group is a standard SNMP term used industry-wide, we refer to role(s) as group(s) in this SNMP section.

SNMP access rights are organized by groups. Each group in SNMP is similar to a role through the CLI. Each group is defined with read access or read-write access.

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

SNMP and Embedded Event Manager

The Embedded Event Manager (EEM) feature monitors events, including SNMP MIB objects, and triggers an action based on these events. One of the actions could be to send an SNMP notification. EEM sends the cEventMgrPolicyEvent of CISCO-EMBEDDED-EVENT-MGR-MIB as the SNMP notification.

See Chapter 13, “Configuring the Embedded Event Manager” for more information about EEM.

Multiple Instance Support

A device can support multiple instances of a logical network entity, such as protocol instances or VRFs. Most existing MIBs cannot distinguish between these multiple logical network entities. For example, the original OSPF-MIB assumes a single protocol instance on a device, but you can now configure multiple OSPF instances on a device.

SNMPv3 uses contexts to distinguish between these multiple instances. An SNMP context is a collection of management information you can access through the SNMP agent. A device can support multiple contexts for different logical network entities. An SNMP context allows the SNMP manager to access one of the multiple instances of a MIB module supported on the device for the different logical network entities.

Cisco NX-OS supports the CISCO-CONTEXT-MAPPING-MIB to map between SNMP contexts and logical network entities. You can associate an SNMP context to a VRF, protocol instance, or topology.

SNMPv3 supports contexts with the contextName field of the SNMPv3 PDU. You can map this contextName field to a particular protocol instance or VRF.

For SNMPv2c, you can map the SNMP community to a context using the snmpCommunityContextName MIB object in the SNMP-COMMUNITY-MIB (RFC 3584). You can then map this snmpCommunityContextName to a particular protocol instance or VRF using the CISCO-CONTEXT-MAPPING-MIB or the CLI.

To map an SNMP context to a logical network entity, follow these steps:

---

**Step 1** Create the SNMPv3 context.

**Step 2** Determine the logical network entity instance.

**Step 3** Map the SNMPv3 context to a logical network entity.
Step 4 Optionally, map the SNMPv3 context to an SNMPv2c community.

For more information, see the “Configuring the Context to Network Entity Mapping” section on page 10-21.

High Availability

Cisco NX-OS supports stateless restarts for SNMP. After a reboot or supervisor switchover, Cisco NX-OS applies the running configuration.

Virtualization Support

Cisco NX-OS supports one instance of the SNMP per virtual device context (VDC). By default, Cisco NX-OS places you in the default VDC. For more information, see the Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.x

SNMP supports multiple MIB module instances and maps them to logical network entities. For more information, see the “Multiple Instance Support” section on page 10-6.

SNMP is also VRF aware. You can configure SNMP to use a particular VRF to reach the SNMP notification host receiver. You can also configure SNMP to filter notifications to an SNMP host receiver based on the VRF where the notification occurred. For more information, see the “Configuring SNMP Notification Receivers with VRFs” section on page 10-14).

Licensing Requirements for SNMP

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

Prerequisites for SNMP

SNMP has the following prerequisites:

- If you configure VDCs, install the Advanced Services license and enter the desired VDC. For more information, see the Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.x.
Guidelines and Limitations

SNMP has the following configuration guidelines and limitations:

- Cisco NX-OS supports read-only access to some SNMP MIBs. See the Cisco NX-OS MIB support list at the following URL for more information:

Configuring SNMP

This section includes the following topics:

- Configuring SNMP Users, page 10-8
- Enforcing SNMP Message Encryption, page 10-9
- Assigning SNMPv3 Users to Multiple Roles, page 10-10
- Creating SNMP Communities, page 10-10
- Filtering SNMP Requests, page 10-11
- Configuring SNMP Notification Receivers, page 10-11
- Configuring a Source Interface for SNMP Notifications, page 10-12
- Configuring the Notification Target User, page 10-13
- Configuring SNMP Notification Receivers with VRFs, page 10-14
- Configuring SNMP to Send Traps Using an Inband Port, page 10-15
- Enabling SNMP Notifications, page 10-17
- Displaying SNMP ifIndex for an Interface, page 10-19
- Disabling LinkUp/LinkDown Notifications on an Interface, page 10-19
- Enabling a One-time Authentication for SNMP over TCP, page 10-19
- Assigning the SNMP Device Contact and Location Information, page 10-20
- Configuring the Context to Network Entity Mapping, page 10-21
- Disabling SNMP, page 10-23
- Modifying the AAA Synchronization Time, page 10-23

Note

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

Configuring SNMP Users

You can configure a user for SNMP.

BEFORE YOU BEGIN

Make sure that you are in the correct VDC. To change the VDC, use the switchto vdc command.
Chapter 10 Configuring SNMP

Send document comments to nexus7k-docfeedback@cisco.com.

SUMMARY STEPS

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

DETAILED STEPS

This example shows how to configure the SNMP contact and location information:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)#
```

```
switch(config)# snmp-server user Admin auth sha abcd1234 priv abcdefgh
```

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 authorizationError for any SNMPv3 PDU request using securityLevel parameter of either noAuthNoPriv or authNoPriv.
Use the following command in global configuration mode to enforce SNMP message encryption for a user:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>snmp-server user name enforcePriv</code></td>
<td>Enforces SNMP message encryption for this user.</td>
</tr>
</tbody>
</table>

**Example:**

```
switch(config)# snmp-server user Admin enforcePriv
```

Use the following command in global configuration mode to enforce SNMP message encryption for all users:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>snmp-server globalEnforcePriv</code></td>
<td>Enforces SNMP message encryption for all users.</td>
</tr>
</tbody>
</table>

**Example:**

```
switch(config)# snmp-server globalEnforcePriv
```

## 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.

Use the following command in global configuration mode to assign a role to an SNMP user:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>snmp-server user name group</code></td>
<td>Associates this SNMP user with the configured user role.</td>
</tr>
</tbody>
</table>

**Example:**

```
switch(config)# snmp-server user Admin superuser
```

## Creating SNMP Communities

You can create SNMP communities for SNMPv1 or SNMPv2c.

Use the following command in global configuration mode to create an SNMP community string:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`snmp-server community name group (ro</td>
<td>rw)`</td>
</tr>
</tbody>
</table>

**Example:**

```
switch(config)# snmp-server community public ro
```
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 7000 Series NX-OS Security Configuration Guide, Release 4.x for more information on creating ACLs. The ACL applies to both IPv4 and IPv6 over UDP and TCP.

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

```
config)

```

Configure SNMP Notification Receivers

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

Use the following command in global configuration mode to configure a host receiver for SNMPv1 traps:

```

```
Use the following command in global configuration mode to configure a host receiver for SNMPv2c traps or informs:

```
Command
snmp-server host ip-address {traps | informs} version 2c community [udp_port number]

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

Use the following command in global configuration mode to configure a host receiver for SNMPv3 traps or informs:

```
Command
snmp-server host ip-address {traps | informs} version 3 {auth | noauth | priv} username [udp_port number]

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

The SNMP manager must know the user credentials (authKey/PrivKey) based on the SNMP engine ID of the Cisco NX-OS device to authenticate and decrypt the SNMPv3 messages.

### Configuring a Source Interface for SNMP Notifications

You can configure SNMP to use the IP address of an interface as the source IP address for notifications. When a notification is generated, its source IP address is based on the IP address of this configured interface. You can configure this as follows:

- All notifications sent to all SNMP notification receivers.
- All notifications sent to a specific SNMP notification receiver. This configuration overrides the global source interface configuration.

The source interface IP address for outgoing trap packets does not guarantee that the device will use the same interface to send the trap. The source interface IP address defines the source address inside of the SNMP trap, and the connection is opened with the address of the egress interface as source.
Send document comments to nexus7k-docfeedback@cisco.com.

Use the following command in global configuration mode to configure a host receiver on a source interface:

```
Command | Purpose
--- | ---
```

```
<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>snmp-server host ip-address source-interface if-type if-number [udp_port number]</code></td>
<td>Configures a host receiver for SNMPv2c traps or informs. The <code>ip-address</code> can be an IPv4 or IPv6 address. Use <code>?</code> to determine the supported interface types. The UDP port number range is from 0 to 65535. This configuration overrides the global source interface configuration.</td>
</tr>
</tbody>
</table>

Example:
```
switch(config)# snmp-server host 192.0.2.1 source-interface ethernet 2/1
```

Use the following command in global configuration mode to configure a source interface for sending out all SNMP notifications:

```
Command | Purpose
--- | ---
```

```
<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`snmp-server source-interface {traps</td>
<td>informs} if-type if-number`</td>
</tr>
</tbody>
</table>

Example:
```
switch(config)# snmp-server source-interface traps ethernet 2/1
```

Use the `show snmp source-interface` command to display information about configured source interfaces.

### Configuring the Notification Target User

You must configure a notification target user on the device to send SNMPv3 inform notifications to a notification host receiver.

Cisco NX-OS uses the credentials of the notification target user to encrypt the SNMPv3 inform notification messages to the configured notification host receiver.

**Note**

For authenticating and decrypting the received inform PDU, the notification host receiver should have the same user credentials as configured in Cisco NX-OS to authenticate and decrypt the informs.

Use the following command in global configuration mode to configure the notification target user:

```
Command | Purpose
--- | ---
```

```
<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`snmp-server user name [auth {md5</td>
<td>sha} passphrase {auto} [priv {aes-128} passphrase] [engineID id]`</td>
</tr>
</tbody>
</table>

Example:
```
switch(config)# snmp-server user NMS auth sha abcd1234 priv abcdefgh engineID 00:00:00:63:00:01:00:10:20:15:10:03
```
Configuring SNMP Notification Receivers with VRFs

SNMP adds entries into the cExtSnmpTargetVrfTable of the CISCO-SNMP-TARGET-EXT-MIB when you configure the VRF reachability and filtering options for an SNMP notification receiver.

**Note**

You must configure the host before configuring the VRF reachability or filtering options.

You can configure Cisco NX-OS to use a configured VRF to reach the host receiver.

Use the following command in global configuration mode to configure a VRF to use for sending notifications to the host receiver:

```
Command
snmp-server host ip-address use-vrf vrf_name [udp_port number]

Example:
switch(config)# snmp-server host 192.0.2.1 use-vrf Blue
```

```
no snmp-server host ip-address use-vrf vrf_name [udp_port number]

Example:
switch(config)# no snmp-server host 192.0.2.1 use-vrf Blue
```

You can configure Cisco NX-OS filter notifications based on the VRF in which the notification occurred.

Use the following command in global configuration mode to filter notifications based on a configured VRF:

```
Command
snmp-server host ip-address filter-vrf vrf_name [udp_port number]

Example:
switch(config)# snmp-server host 192.0.2.1 filter-vrf Red
```

Configures SNMP to use the selected VRF to communicate with the host receiver. The `ip-address` can be an IPv4 or IPv6 address. The VRF name can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535. This command adds an entry into the ExtSnmpTargetVrfTable of the CISCO-SNMP-TARGET-EXT-MIB.

Removes the VRF reachability information for the configured host, and removes the entry from the ExtSnmpTargetVrfTable of the CISCO-SNMP-TARGET-EXT-MIB. The `ip-address` can be an IPv4 or IPv6 address. Does not remove the host configuration.

Filters notifications to the notification host receiver based on the configured VRF. The `ip-address` can be an IPv4 or IPv6 address. The VRF name can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535. This command adds an entry into the ExtSnmpTargetVrfTable of the CISCO-SNMP-TARGET-EXT-MIB.
Configuring SNMP to Send Traps Using an Inband Port

You can configure SNMP to send traps using an inband port. To do so, you must configure the source interface (at the global or host level) and the VRF used to send the traps.

**SUMMARY STEPS**

1. `config t`
2. `snmp-server source-interface traps if-type if-number`
3. `show snmp source-interface`
4. `snmp-server host ip-address use-vrf vrf_name [udp_port number]`
5. `show snmp host`
6. `copy running-config startup-config`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no snmp-server host ip-address filter-vrf vrf_name</code></td>
<td>Removes the VRF filter information for the configured host, and removes the entry from the ExtSnmpTargetVrfTable of the CISCO-SNMP-TARGET-EXT-MB. The <code>ip-address</code> can be an IPv4 or IPv6 address. This command does not remove the host configuration.</td>
</tr>
</tbody>
</table>

**Example:**

```
switch(config)# no snmp-server host 192.0.2.1 filter-vrf Red
```

Removes the VRF filter information for the configured host, and removes the entry from the ExtSnmpTargetVrfTable of the CISCO-SNMP-TARGET-EXT-MB. The `ip-address` can be an IPv4 or IPv6 address. This command does not remove the host configuration.

---

**Command**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>config t</code></td>
<td>Places you in global configuration mode.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>switch# config t</code></td>
<td><strong>Enter configuration commands, one per line. End with CNTL/Z.</strong></td>
</tr>
<tr>
<td><code>switch(config)#</code></td>
<td></td>
</tr>
</tbody>
</table>

**Step 2**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>snmp-server source-interface traps if-type if-number</code></td>
<td>Globally configures a source interface for sending out SNMP traps. Use <code>?</code> to determine the supported interface types. You can configure the source interface at the global level or at a host level. When the source interface is configured globally, any new host configuration uses the global configuration to send the traps.</td>
</tr>
</tbody>
</table>

**Note**

To configure a source interface at the host level, use this command: `snmp-server host ip-address source-interface if-type if-number`. |
## Configuring SNMP

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

```plaintext
switch# config t  
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# snmp-server source-interface traps ethernet 1/2
switch(config)# show snmp source-interface
```

### Command Purpose

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>show snmp source-interface</td>
<td>(Optional) Displays information about configured source interfaces.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>switch(config)# show snmp source-interface</td>
</tr>
<tr>
<td>4</td>
<td>snmp-server host ip-address use-vrf vrf_name [udp_port number]</td>
<td>Configures SNMP to use the selected VRF to communicate with the host receiver. The <code>ip-address</code> can be an IPv4 or IPv6 address. The VRF name can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535. This command adds an entry into the ExtSnmpTargetVrfTable of the CISCO-SNMP-TARGET-EXT-MB.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>switch(config)# snmp-server host 171.71.48.164 use_vrf default</td>
</tr>
<tr>
<td>5</td>
<td>show snmp host</td>
<td>(Optional) Displays information about configured SNMP hosts.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>switch(config)# show snmp host</td>
</tr>
<tr>
<td>6</td>
<td>copy running-config startup-config</td>
<td>(Optional) Saves this configuration change.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>switch(config)# copy running-config startup-config</td>
</tr>
</tbody>
</table>

### Notes

- **Step 4**
  - By default, SNMP sends the traps using the management VRF. If you do not want to use the management VRF, you must use this command to specify the desired VRF.

---

### Command Purpose

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>show snmp source-interface</td>
<td>(Optional) Displays information about configured source interfaces.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>switch(config)# show snmp source-interface</td>
</tr>
<tr>
<td>4</td>
<td>snmp-server host ip-address use-vrf vrf_name [udp_port number]</td>
<td>Configures SNMP to use the selected VRF to communicate with the host receiver. The <code>ip-address</code> can be an IPv4 or IPv6 address. The VRF name can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535. This command adds an entry into the ExtSnmpTargetVrfTable of the CISCO-SNMP-TARGET-EXT-MB.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>switch(config)# snmp-server host 171.71.48.164 use_vrf default</td>
</tr>
<tr>
<td>5</td>
<td>show snmp host</td>
<td>(Optional) Displays information about configured SNMP hosts.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>switch(config)# show snmp host</td>
</tr>
<tr>
<td>6</td>
<td>copy running-config startup-config</td>
<td>(Optional) Saves this configuration change.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>switch(config)# copy running-config startup-config</td>
</tr>
</tbody>
</table>

---

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

```plaintext
switch# config t  
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# snmp-server source-interface traps ethernet 1/2
switch(config)# show snmp source-interface
```

---

Note

- By default, SNMP sends the traps using the management VRF. If you do not want to use the management VRF, you must use this command to specify the desired VRF.
Enabling SNMP Notifications

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

Table 10-3 lists the commands that enable the notifications for Cisco NX-OS MIBs.

The `snmp-server enable traps` command enables both traps and informs, depending on the configured notification host receivers.

<table>
<thead>
<tr>
<th>MIB</th>
<th>Related Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>All notifications</td>
<td><code>snmp-server enable traps</code></td>
</tr>
<tr>
<td>CISCO-AAA-SERVER-MIB</td>
<td><code>snmp-server enable traps aaa</code></td>
</tr>
<tr>
<td>CISCO-STP-BRIDGE-MIB</td>
<td><code>snmp-server enable traps bridge</code></td>
</tr>
<tr>
<td>CISCO-CALLHOME-MIB</td>
<td><code>snmp-server enable traps callhome</code></td>
</tr>
<tr>
<td></td>
<td><code>snmp-server enable traps callhome event-notify</code></td>
</tr>
<tr>
<td></td>
<td><code>snmp-server enable traps callhome smtp-send-fail</code></td>
</tr>
<tr>
<td>CISCO-EIGRP-MIB</td>
<td><code>snmp-server enable traps eigrp</code></td>
</tr>
<tr>
<td>ENTITY-MIB,</td>
<td><code>snmp-server enable traps entity</code></td>
</tr>
<tr>
<td>CISCO-ENTITY-FRU-CONTROL-MIB,</td>
<td><code>snmp-server enable traps entity fru</code></td>
</tr>
<tr>
<td>CISCO-ENTITY-SENSOR-MIB</td>
<td></td>
</tr>
<tr>
<td>CISCO-HSRP-MIB</td>
<td><code>snmp-server enable traps hsrp</code></td>
</tr>
<tr>
<td></td>
<td><code>snmp-server enable traps hsrp state-change</code></td>
</tr>
<tr>
<td>CISCO-LICENSE-MGR-MIB</td>
<td><code>snmp-server enable traps license</code></td>
</tr>
<tr>
<td>IF-MIB</td>
<td><code>snmp-server enable traps link</code></td>
</tr>
<tr>
<td>CISCO-RF-MIB</td>
<td><code>snmp-server enable traps rf</code></td>
</tr>
<tr>
<td>SNMPv2-MIB</td>
<td><code>snmp-server enable traps snmp</code></td>
</tr>
<tr>
<td></td>
<td><code>snmp-server enable traps snmp authentication</code></td>
</tr>
<tr>
<td>CISCO-STPX-MIB</td>
<td><code>snmp-server enable traps stpx</code></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>snmp-server enable traps</code></td>
<td>Enables all SNMP notifications.</td>
</tr>
<tr>
<td><code>snmp-server enable traps aaa</code></td>
<td>Enables the AAA SNMP notifications.</td>
</tr>
<tr>
<td><code>snmp-server enable traps aaa server-state-change</code></td>
<td></td>
</tr>
</tbody>
</table>

Example:
```
switch(config)# snmp-server enable traps
switch(config)# snmp-server enable traps aaa
```
# Configuring SNMP

## Command

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`snmp-server enable traps bridge [newroot</td>
<td>topologychange]`</td>
</tr>
<tr>
<td>Example: <code>switch(config)# snmp-server enable traps bridge newroot</code></td>
<td></td>
</tr>
</tbody>
</table>
| `snmp-server enable traps callhome [event-notify] [smtp-send-fail]` | Enables the CISCO-CALLHOME-MIB SNMP notifications. Optionally, enables the following specific notifications:  
  - `event-notify`—Enables Call Home external event notifications.  
  - `smtp-send-fail`—Enables SMTP message send fail notifications. |
| Example: `switch(config)# snmp-server enable traps callhome` | |
| `snmp-server enable traps eigrp` | Enables the CISCO-EIGRP-MIB SNMP notifications. |
| Example: `switch(config)# snmp-server enable traps eigrp` | |
| `snmp-server enable traps entity [fru]` | Enables the ENTITY-MIB SNMP notifications. |
| Example: `switch(config)# snmp-server enable traps entity` | |
| `snmp-server enable traps hsrp [state-change]` | Enables the HSRP-MIB SNMP notifications. |
| Example: `switch(config)# snmp-server enable traps hsrp` | |
| `snmp-server enable traps license` | Enables the license SNMP notification. |
| Example: `switch(config)# snmp-server enable traps license` | |
| `snmp-server enable traps link` | Enables the link SNMP notifications. |
| Example: `switch(config)# snmp-server enable traps link` | |
| `snmp-server enable traps rf` | Enables the redundancy framework (RF) SNMP notifications. |
| Example: `switch(config)# snmp-server enable traps rf` | |
| `snmp-server enable traps [trap-arg [trap_sub_category] | snmp [authentication]]` | Enables the SNMP agent notifications. |
| Example: `switch(config)# snmp-server enable traps snmp` | |
Disabling LinkUp/LinkDown Notifications on an Interface

You can disable linkUp and linkDown notifications on an individual interface. You can use these limits notifications on a flapping interface (an interface that transitions between up and down repeatedly).

Use the following command in interface configuration mode to disable linkUp/linkDown notifications for the interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>no snmp trap link-status</td>
<td>Disables SNMP link-state traps for the interface. This command is enabled by default.</td>
</tr>
</tbody>
</table>

Displaying SNMP ifIndex for an Interface

The SNMP ifIndex is used across multiple SNMP MIBs to link related interface information. The ifIndex is also used by NetFlow to collect information on an interface.

Use the following command in any mode to display the SNMP ifIndex values for interfaces:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interface snmp-ifindex</td>
<td>Displays the persistent SNMP ifIndex value from IF-MIB for all interfaces. Optionally, use the</td>
</tr>
</tbody>
</table>

Enabling a One-time Authentication for SNMP over TCP

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

Use the following command in global configuration mode to enable a one-time authentication for SNMP over TCP:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>snmp-server enable traps</td>
<td>Enables the SNMP agent notifications at global scope.</td>
</tr>
</tbody>
</table>
| snmp-server enable traps stpx \[
|  | Enables the STPX SNMP notifications. |
|  | {inconsistency | loop-inconsistency | root-inconsistency} |
|  | switch(config)# snmp-server enable traps stpx root-inconsistency |
Assigning the SNMP Device Contact and Location Information

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

BEFORE YOU BEGIN

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

SUMMARY STEPS

1. `config t`
2. `snmp-server contact name`
3. `snmp-server location name`
4. `show snmp`
5. `copy running-config startup-config`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>config t</code></td>
<td>Places you in global configuration mode.</td>
</tr>
<tr>
<td><code>snmp-server tcp-session</code></td>
<td>Enables a one-time authentication for SNMP over a TCP session. The default is disabled.</td>
</tr>
</tbody>
</table>

Example:

```
switch(config)# snmp-server tcp-session
```

Assigning the SNMP Device Contact and Location Information

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

BEFORE YOU BEGIN

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

SUMMARY STEPS

1. `config t`
2. `snmp-server contact name`
3. `snmp-server location name`
4. `show snmp`
5. `copy running-config startup-config`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>config t</code></td>
<td>Places you in global configuration mode.</td>
</tr>
<tr>
<td><code>snmp-server tcp-session</code></td>
<td>Enables a one-time authentication for SNMP over a TCP session. The default is disabled.</td>
</tr>
</tbody>
</table>

Example:

```
switch(config)# snmp-server tcp-session
```
Configuring SNMP

This example shows how to configure the SNMP contact and location information:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# snmp contact Admin
switch(config)# snmp location Lab-7
```

### Configuring the Context to Network Entity Mapping

You can configure an SNMP context to map to a logical network entity, such as a protocol instance or VRF.

**BEFORE YOU BEGIN**

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

Determine the logical network entity instance. For more information on VRFs and protocol instances, see the *Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 4.x*, or the *Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide, Release 4.x*.

**SUMMARY STEPS**

1. `config t`
2. `snmp-server context context-name [instance instance-name] [vrf vrf-name] [topology topology-name]`
3. `snmp-server mib community-map community-name context context-name`
4. `show snmp context`
5. `copy running-config startup-config`

This example shows how to configure the SNMP contact and location information:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# snmp contact Admin
switch(config)# snmp location Lab-7
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 4**

show snmp

Example:

`switch(config)# show snmp`

| **Step 5**

`copy running-config startup-config`

Example:

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

(Optional) Displays information about one or more destination profiles.

(Optional) Saves this configuration change.
### Chapter 10  Configuring SNMP

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>config t</code></td>
<td>Places you in global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch# config t</td>
<td>Enter configuration commands, one per line. End with CNTL/Z.</td>
</tr>
<tr>
<td></td>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><code>snmp-server context context-name</code></td>
<td>Maps an SNMP context to a protocol instance, VRF, or topology. The names can be any alphanumeric string up to 32 characters.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# snmp-server context public1 vrf red</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><code>snmp-server mib community-map community-name context context-name</code></td>
<td>(Optional) Maps an SNMPv2c community to an SNMP context. The names can be any alphanumeric string up to 32 characters.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# snmp-server mib community-map public context public1</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><code>show snmp context</code></td>
<td>(Optional) Displays information about one or more SNMP contexts.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# show snmp context</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Saves this configuration change.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

This example shows how to map VRF red to the SNMPv2c public community string:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# vrf context red
switch(config-vrf)# exit
switch(config)# snmp-server context public1 vrf red
switch(config)# snmp-server mib community-map public context public1
```

This example shows how to map OSPF instance Enterprise to the same SNMPv2c public community string:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# feature ospf
switch(config)# router ospf Enterprise
switch(config-router)# exit
switch(config)# snmp-server context public1 instance Enterprise
switch(config)# snmp-server mib community-map public context public1
```

Use the following command in global configuration mode to delete the mapping between an SNMP context and a logical network entity:

```
```
Disabling SNMP

You can disable SNMP on a device.

Use the following command in global configuration mode to disable SNMP:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>no snmp-server protocol enable</td>
<td>Enables SNMP. This command is enabled by default.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Example:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>switch(config)# no snmp-server protocol enable</td>
<td></td>
</tr>
</tbody>
</table>

Modifying the AAA Synchronization Time

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

Use the following command in global configuration mode to modify the AAA synchronization time:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>snmp-server aaa-user cache-timeout seconds</td>
<td>Configures how long the AAA synchronized user configuration stays in the local cache. The range is from 1 to 86400 seconds. The default is 3600.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Example:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>switch(config)# snmp-server aaa-user cache-timeout 1200.</td>
<td></td>
</tr>
</tbody>
</table>
Verifying SNMP Configuration

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

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

SNMP Example Configurations

This example shows how to configure Cisco NX-OS to send the Cisco linkUp or Down notifications to one notification host receiver using the Blue VRF and defines two SNMP users, Admin and NMS:

cfg t
snmp-server contact Admin@company.com
snmp-server user Admin auth sha abcd1234 priv abcdefgh
snmp-server user NMS auth sha abcd1234 priv abcdefgh engineID 00:00:00:63:00:01:00:22:32:15:10:03
snmp-server host 192.0.2.1 informs version 3 auth NMS
snmp-server host 192.0.2.1 use-vrf Blue
snmp-server enable traps link cisco

This example shows how to configure SNMP to send traps using an inband port configured at the host level:

switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# snmp-server host 171.71.48.164 version 2c public
switch(config)# snmp-server host 171.71.48.164 source-interface ethernet 1/2
switch(config)# show snmp host

<table>
<thead>
<tr>
<th>Host</th>
<th>Port</th>
<th>Version</th>
<th>Level</th>
<th>Type</th>
<th>SecName</th>
</tr>
</thead>
<tbody>
<tr>
<td>171.71.48.164</td>
<td>162</td>
<td>v2c</td>
<td>noauth</td>
<td>trap</td>
<td>public</td>
</tr>
</tbody>
</table>
Default Settings

Table 10-4 lists the default settings for SNMP parameters.

### Table 10-4  Default SNMP Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>license notifications</td>
<td>Enabled.</td>
</tr>
</tbody>
</table>

Additional References

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

- Related Documents, page 10-25
- Standards, page 10-26
- MIBs, page 10-26

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP CLI commands</td>
<td>Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.x</td>
</tr>
<tr>
<td>VDCs and VRFs</td>
<td>Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.x</td>
</tr>
</tbody>
</table>
Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>—</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>• SNMP-COMMUNITY-MIB</td>
<td>To locate and download MIBs, go to the following URL:</td>
</tr>
<tr>
<td>• SNMP-FRAMEWORK-MIB</td>
<td></td>
</tr>
<tr>
<td>• SNMP-NOTIFICATION-MIB</td>
<td></td>
</tr>
<tr>
<td>• SNMP-TARGET-MIB</td>
<td></td>
</tr>
<tr>
<td>• SNMPv2-MIB</td>
<td></td>
</tr>
</tbody>
</table>

Feature History for SNMP

Table 10-5 lists the release history for this feature.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 support</td>
<td>4.2(1)</td>
<td>Supports configuring IPv6 SNMP hosts.</td>
</tr>
<tr>
<td>Filter SNMP requests by community using an ACL</td>
<td>4.2(1)</td>
<td>Assigns an ACL to an SNMP community to filter SNMP requests. See the “Filtering SNMP Requests” section on page 10-11</td>
</tr>
<tr>
<td>Use interfaces for SNMP notification receivers</td>
<td>4.2(1)</td>
<td>Adds support to designate an interface to act as the source interface for SNMP notifications. See the “Configuring SNMP Notification Receivers” section on page 10-11</td>
</tr>
<tr>
<td>SNMP AAA synchronization</td>
<td>4.0(3)</td>
<td>Adds ability to modify the synchronized user configuration timeout. See the “Modifying the AAA Synchronization Time” section on page 10-23.</td>
</tr>
<tr>
<td>SNMP protocol</td>
<td>4.0(3)</td>
<td>Added ability to disable the SNMP protocol. See the “Disabling SNMP” section on page 10-23.</td>
</tr>
</tbody>
</table>
Configuring RMON

This chapter describes how to configure the RMON feature on Cisco NX-OS devices. This chapter includes the following sections:

- Information About RMON, page 11-1
- Licensing Requirements for RMON, page 11-3
- Prerequisites for RMON, page 11-3
- Guidelines and Limitations, page 11-3
- Configuring RMON, page 11-3
- Verifying RMON Configuration, page 11-6
- RMON Example Configuration, page 11-6
- Related Topics, page 11-7
- Default Settings, page 11-7
- Additional References, page 11-7

Information About RMON

RMON is a Simple Network Management Protocol (SNMP) Internet Engineering Task Force (IETF) standard monitoring specification that allows various network agents and console systems to exchange network monitoring data. Cisco NX-OS supports RMON alarms, events, and logs to monitor Cisco NX-OS devices.

An RMON alarm monitors a specific management information base (MIB) object for a specified interval, triggers an alarm at a specified threshold value (threshold), and resets the alarm at another threshold value. You can use alarms with RMON events to generate a log entry or an SNMP notification when the RMON alarm triggers.

RMON is disabled by default and no events or alarms are configured in Cisco NX-OS. You can configure your RMON alarms and events by using the CLI or an SNMP-compatible network management station.

This section includes the following topics:

- RMON Alarms, page 11-2
- RMON Events, page 11-2
- High Availability, page 11-2
- Virtualization Support, page 11-3
Chapter 11  Configuring RMON

Information About RMON

You can set an alarm on any MIB object that resolves into an SNMP INTEGER type. The specified object must be an existing SNMP MIB object in standard dot notation (for example, 1.3.6.1.2.1.2.2.1.14 represents ifInOctets.14).

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

- MIB object to monitor.
- Sampling interval—The interval that Cisco NX-OS uses to collect a sample value of the MIB object.
- Sample type—Absolute samples take the current snapshot of the MIB object value. Delta samples take two consecutive samples and calculate the difference between them.
- Rising threshold—The value at which Cisco NX-OS triggers a rising alarm or resets a falling alarm.
- Falling threshold—The value at which Cisco NX-OS triggers a falling alarm or resets a rising alarm.
- Events—The action that Cisco NX-OS takes when an alarm (rising or falling) triggers.

**Note**
Use the hcalarms option to set an alarm on a 64-bit integer MIB object.

For example, you can set a delta type rising alarm on an error counter MIB object. If the error counter delta exceeds this value, you can trigger an event that sends an SNMP notification and logs the rising alarm event. This rising alarm will not occur again until the delta sample for the error counter drops below the falling threshold.

**Note**
The falling threshold must be less than the rising threshold.

RMON Events

You can associate a particular event to each RMON alarm. RMON supports the following event types:

- SNMP notification—Sends an SNMP risingAlarm or fallingAlarm notification when the associated alarm triggers.
- Log—Adds an entry in the RMON log table when the associated alarm triggers.
- Both—Sends an SNMP notification and adds an entry in the RMON log table when the associated alarm triggers.

You can specify a different even for a falling alarm and a rising alarm.

High Availability

Cisco NX-OS supports stateless restarts for RMON. After a reboot or supervisor switchover, Cisco NX-OS applies the running configuration.
Virtualization Support

Cisco NX-OS supports one instance of the RMON per virtual device context (VDC). By default, Cisco NX-OS places you in the default VDC. See the Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.x.

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

Licensing Requirements for RMON

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

Prerequisites for RMON

RMON has the following prerequisites:

If you configure VDCs, install the Advanced Services license and enter the desired VDC (see the Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.x).

Guidelines and Limitations

RMON has the following configuration guidelines and limitations:

- You must configure an SNMP user and a notification receiver to use the SNMP notification event type.
- You can only configure an RMON alarm on a MIB object that resolves to an integer.
- When you configure an RMON alarm, the object identifier must be complete with its index so that it refers to only one object. For example, 1.3.6.1.2.1.2.2.1.14 corresponds to cpmCPUTotal5minRev, and .1 corresponds to index cpmCPUTotalIndex, which creates object identifier 1.3.6.1.2.1.2.1.14.1.

Configuring RMON

This section includes the following topics:

- Configuring RMON Alarms, page 11-4
- Configuring RMON Events, page 11-5

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

You can configure RMON alarms on any integer-based SNMP MIB object.

You can optionally specify the following parameters:

- The event-number to trigger if the rising or falling threshold exceeds the specified limit.
- The owner of the alarm.

## BEFORE YOU BEGIN

Ensure that you have configured an SNMP user and enabled SNMP notifications (see the “Configuring SNMP” section on page 10-7).

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

## SUMMARY STEPS

1. `config t`
2. `rmon alarm index mib-object sample-interval {absolute | delta} rising-threshold value [event-index] falling-threshold value [event-index] [owner name]`  
   or
   ```
   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]
   ```
3. `show rmon [alarms | hcalarms]`
4. `copy running-config startup-config`

## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>config t</code></td>
<td>Places you in global configuration mode.</td>
</tr>
</tbody>
</table>

**Example:**
```bash
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)#
```
Configuring RMON

Configuring RMON Events

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

BEFORE YOU BEGIN

Ensure that you have configured an SNMP user and enabled SNMP notifications (see the “Configuring SNMP” section on page 10-7).

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

SUMMARY STEPS

1. `config t`
2. `rmon event index [description string] [log] [trap] [owner name]`

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>rmon alarm index mib-object\nsample-interval {absolute</td>
<td>delta}\nrising-threshold value [event-index]\nfalling-threshold value [event-index]\n[owner name]</td>
<td>Creates an RMON alarm. The value range is from –2147483647 to 2147483647. The owner name can be any alphanumeric string.</td>
</tr>
</tbody>
</table>

Example:
```
switch(config)# rmon alarm 20
1.3.6.1.2.1.2.1.14.1 2900 delta
rising-threshold 1500 1
falling-threshold 0 owner test
```

rmon hcalarm index mib-object\nsample-interval {absolute | delta}\nrising-threshold-high value\nrising-threshold-low value [event-index]\nfalling-threshold-high value\nfalling-threshold-low value [event-index] [owner name] [storagetype type] | Creates an RMON high capacity alarm. The value range is from –2147483647 to 2147483647. The owner name can be any alphanumeric string. The storage type range is from 1 to 5. | |

Example:
```
switch(config)# rmon alarm 20
1.3.6.1.2.1.2.1.14.1.6777216 2900 delta
rising-threshold-high 15
rising-threshold-low 151
falling-threshold-high 0
falling-threshold-low 0 owner test
```

Step 3 show rmon {alarms | hcalarms} | (Optional) Displays information about rmon alarms or high capacity alarms. | |

Example:
```
switch(config)# show rmon alarms
```

Step 4 copy running-config startup-config | (Optional) Saves this configuration change. | |

Example:
```
switch(config)# copy running-config startup-config
```
### Verifying RMON Configuration

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show rmon alarms</td>
<td>Displays information about RMON alarms.</td>
</tr>
<tr>
<td>show rmon events</td>
<td>Displays information about RMON events.</td>
</tr>
<tr>
<td>show rmon hcalarms</td>
<td>Displays information about RMON hcalarms.</td>
</tr>
<tr>
<td>show rmon logs</td>
<td>Displays information about RMON logs.</td>
</tr>
</tbody>
</table>

### RMON Example Configuration

This example shows how to create a delta rising alarm on ifInOctets.14 and associates a notification event with this alarm:

```bash
config t
rmon alarm 20 1.3.6.1.2.1.2.1.2.1.14.1 2900 delta rising-threshold 1500 1
falling-threshold 0 owner test
rmon event 1 trap
```
Related Topics

See the following related topics:

- Configuring SNMP, page 10-1.

Default Settings

Table 11-1 lists the default settings for RMON parameters.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarms</td>
<td>None configured.</td>
</tr>
<tr>
<td>Events</td>
<td>None configured.</td>
</tr>
</tbody>
</table>

Additional References

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

- Related Documents, page 11-7
- Standards, page 11-7
- MIBs, page 11-8

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RMON CLI commands</td>
<td>Cisco Nexus 7000 Series NX-OS System Management Command Reference</td>
</tr>
<tr>
<td>VDCs and VRFs</td>
<td>Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.x</td>
</tr>
</tbody>
</table>

Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td></td>
</tr>
</tbody>
</table>
## MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>RMON-MIB</td>
<td>To locate and download MIBs, go to the following URL: <a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a></td>
</tr>
</tbody>
</table>
CHAPTER 12

Configuring Online Diagnostics

This chapter describes how to configure the generic online diagnostics (GOLD) feature on Cisco NX-OS devices.

This chapter includes the following sections:

- Information About Online Diagnostics, page 12-1
- Licensing Requirements for Online Diagnostics, page 12-5
- Prerequisites for Online Diagnostics, page 12-5
- Guidelines and Limitations, page 12-5
- Configuring Online Diagnostics, page 12-5
- Verifying Online Diagnostics Configuration, page 12-10
- Online Diagnostic Example Configuration, page 12-11
- Default Settings, page 12-11
- Additional References, page 12-11
- Feature History for Online Diagnostics, page 12-12

For complete syntax and usage information for the commands in this chapter, see the Cisco Nexus 7000 Series NX-OS System Management Command Reference.

Information About Online Diagnostics

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

This section includes the following topics:

- Online Diagnostic Overview, page 12-2
- Bootup Diagnostics, page 12-2
- Runtime or Health Monitoring Diagnostics, page 12-3
- On-Demand Diagnostics, page 12-4
- High Availability, page 12-4
- Virtualization Support, page 12-4
Online Diagnostic Overview

With online diagnostics, you can test and verify the hardware functionality of the device while the device is connected to a live network.

The online diagnostics contain tests that check different hardware components and verify the data path and control signals. Disruptive online diagnostic tests (such as the disruptive loopback test) and nondisruptive online diagnostic tests (such as the ASIC register check) run during bootup, line module online insertion and removal (OIR), and system reset. The nondisruptive online diagnostic tests run as part of the background health monitoring, and you can run these tests on demand.

Online diagnostics are categorized as bootup, runtime or health-monitoring diagnostics, and on-demand diagnostics. Bootup diagnostics run during bootup, health-monitoring tests run in the background, and on-demand diagnostics run once or at user-designated intervals when the device is connected to a live network.

Bootup Diagnostics

Bootup diagnostics run during bootup and detect faulty hardware before Cisco NX-OS brings a module online. For example, if you insert a faulty module in the device, bootup diagnostics test the module and take it offline before the device uses the module to forward traffic.

Bootup diagnostics also check the connectivity between the supervisor and module hardware and the data and control paths for all the ASICs. Table 12-1 describes the bootup diagnostic tests for a supervisor.

<table>
<thead>
<tr>
<th>Test ID</th>
<th>Diagnostic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ManagementPortLoopback</td>
<td>Disruptive test, not an on-demand test</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tests loopback on the management port of a module.</td>
</tr>
<tr>
<td>2</td>
<td>EOBCPortLoopback</td>
<td>Disruptive test, not an on-demand test</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ethernet out of band</td>
</tr>
<tr>
<td>4</td>
<td>USB</td>
<td>Nondisruptive test</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Checks the USB controller initialization on a module.</td>
</tr>
<tr>
<td>5</td>
<td>CryptoDevice</td>
<td>Nondisruptive test</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Checks the Cisco Trusted Security (CTS) device initialization on a module.</td>
</tr>
</tbody>
</table>

Note: Modules run the EOBCPortLoopback diagnostic as a nondisruptive bootup test, using test ID 1.

Bootup diagnostics log failures to onboard failure logging (OBFL) and syslog and trigger a diagnostic LED indication (on, off, pass, or fail).

You can configure Cisco NX-OS to either bypass the bootup diagnostics or run the complete set of bootup diagnostics. See the “Setting the Bootup Diagnostic Level” section on page 12-5.
Runtime or Health Monitoring Diagnostics

Runtime diagnostics are also called health monitoring (HM) diagnostics. These diagnostics provide information about the health of a live device. They detect runtime hardware errors, memory errors, the degradation of hardware modules over time, software faults, and resource exhaustion.

Health monitoring diagnostics are nondisruptive and run in the background to ensure the health of a device that is processing live network traffic. You can enable or disable health monitoring tests or change their runtime interval. Table 12-2 describes the health monitoring diagnostics and test IDs for a supervisor.

<table>
<thead>
<tr>
<th>Test ID</th>
<th>Diagnostic</th>
<th>Default Interval</th>
<th>Default Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>ASICRegisterCheck</td>
<td>20 seconds</td>
<td>active</td>
<td>Checks read/write access to scratch registers for the ASICs on a module.</td>
</tr>
<tr>
<td>5</td>
<td>PortLoopback</td>
<td>15 minutes</td>
<td>active</td>
<td>Verifies connectivity through every port that is administratively down on every module in the system.</td>
</tr>
<tr>
<td>6</td>
<td>NVRAM</td>
<td>30 seconds</td>
<td>active</td>
<td>Verifies the sanity of the NVRAM blocks on a supervisor.</td>
</tr>
<tr>
<td>7</td>
<td>RealTimeClock</td>
<td>5 minutes</td>
<td>active</td>
<td>Verifies that the real-time clock on the supervisor is ticking.</td>
</tr>
<tr>
<td>8</td>
<td>PrimaryBootROM</td>
<td>30 minutes</td>
<td>active</td>
<td>Verifies the integrity of the primary boot device on the supervisor.</td>
</tr>
<tr>
<td>9</td>
<td>SecondaryBootROM</td>
<td>30 minutes</td>
<td>active</td>
<td>Verifies the integrity of the secondary boot device on the supervisor.</td>
</tr>
<tr>
<td>10</td>
<td>CompactFlash</td>
<td>30 minutes</td>
<td>active</td>
<td>Verifies access to the internal compact flash devices.</td>
</tr>
<tr>
<td>11</td>
<td>ExternalCompactFlash</td>
<td>30 minutes</td>
<td>active</td>
<td>Verifies access to the external compact flash devices.</td>
</tr>
<tr>
<td>12</td>
<td>PwrMgmtBus</td>
<td>30 seconds</td>
<td>active</td>
<td>Verifies the standby power management control bus.</td>
</tr>
<tr>
<td>13</td>
<td>SpineControlBus</td>
<td>30 seconds</td>
<td>active</td>
<td>Verifies the availability of the standby spine module control bus.</td>
</tr>
<tr>
<td>14</td>
<td>SystemMgmtBus</td>
<td>30 seconds</td>
<td>active</td>
<td>Verifies the availability of the standby system management bus.</td>
</tr>
<tr>
<td>15</td>
<td>StatusBus</td>
<td>30 seconds</td>
<td>active</td>
<td>Verifies the status transmitted the status bus for the supervisor, modules, and fabric cards.</td>
</tr>
<tr>
<td>16</td>
<td>StandbyFabricLoopback</td>
<td>60 seconds</td>
<td>active</td>
<td>Verifies the connectivity of the standby supervisor to the crossbars on the spine card.</td>
</tr>
</tbody>
</table>
Information About Online Diagnostics

Table 12-3 describes the health monitoring diagnostics for a module.

<table>
<thead>
<tr>
<th>Test ID</th>
<th>Diagnostic</th>
<th>Default Interval</th>
<th>Default Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>ASICRegisterCheck</td>
<td>1 minute</td>
<td>active</td>
<td>Checks read/write access to scratch registers for the ASICs on a module.</td>
</tr>
<tr>
<td>3</td>
<td>PrimaryBootROM</td>
<td>30 minutes</td>
<td>active</td>
<td>Verifies the integrity of the primary boot device on a module.</td>
</tr>
<tr>
<td>4</td>
<td>SecondaryBootROM</td>
<td>30 minutes</td>
<td>active</td>
<td>Verifies the integrity of the secondary boot device on a module.</td>
</tr>
<tr>
<td>5</td>
<td>PortLoopback</td>
<td>15 minutes</td>
<td>active</td>
<td>Tests the packet path from the supervisor module to the physical port in ADMIN DOWN state on modules.</td>
</tr>
<tr>
<td>6</td>
<td>RewriteEngineLoopback</td>
<td>60 seconds</td>
<td>active</td>
<td>Tests nondisruptive loopback for all ports up to the Rewrite Engine ASIC device.</td>
</tr>
</tbody>
</table>

1. PortLoopback test supported on 32-port 10-Gbps Ethernet module and 48-port 1-G optical ethernet module.

On-Demand Diagnostics

On-demand tests help localize faults and are usually needed in one of the following situations:

- To respond to an event that has occurred, such as isolating a fault.
- In anticipation of an event that may occur, such as a resource exceeding its utilization limit.

You can run all the health monitoring tests on demand.

You can schedule on-demand diagnostics to run immediately. See the “Starting or Stopping an On-Demand Diagnostic Test” section on page 12-8 for more information.

You can also modify the default interval for a health monitoring test. See the “Activating a Diagnostic Test” section on page 12-6 for more information.

High Availability

A key part of high availability is detecting hardware failures and taking corrective action while the device runs in a live network. Online diagnostics in high availability detect hardware failures and provide feedback to high availability software components to make switchover decisions.

Cisco NX-OS supports stateless restarts for online diagnostics. After a reboot or supervisor switchover, Cisco NX-OS applies the running configuration.

Virtualization Support

Cisco NX-OS supports online diagnostics in the default virtual device context (VDC). By default, Cisco NX-OS places you in the default VDC. See the Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.x for more information.
Licensing Requirements for Online Diagnostics

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

Prerequisites for Online Diagnostics

Online diagnostics have the following prerequisite:

- If you configure VDCs, install the Advanced Services license and go to the VDC that you want to configure. For more information, see the document, *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.x*.

Guidelines and Limitations

You cannot run disruptive online diagnostic tests on demand.

Configuring Online Diagnostics

This section includes the following topics:

- Setting the Bootup Diagnostic Level, page 12-5
- Activating a Diagnostic Test, page 12-6
- Setting a Diagnostic Test as Inactive, page 12-8
- Starting or Stopping an On-Demand Diagnostic Test, page 12-8
- Clearing Diagnostic Results, page 12-9
- Simulating Diagnostic Results, page 12-10

**Note**

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

Setting the Bootup Diagnostic Level

You can configure the bootup diagnostics to run the complete set of tests, or you can bypass all bootup diagnostic tests for a faster module bootup time.
Configuring Online Diagnostics

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

### BEFORE YOU BEGIN

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

### SUMMARY STEPS

1. **config t**
2. **diagnostic bootup level** `[complete | bypass]`
3. **show diagnostic bootup level**
4. **copy running-config startup-config**

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>config t</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch# config t</td>
</tr>
<tr>
<td>Enter configuration commands, one per line. End with CNTL/Z.</td>
<td>switch(config)#</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>diagnostic bootup level</strong> `[complete</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config)# diagnostic bootup level complete</td>
</tr>
<tr>
<td>• complete—Perform all bootup diagnostics. The default is complete.</td>
<td></td>
</tr>
<tr>
<td>• bypass—Do not perform any bootup diagnostics.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>show diagnostic bootup level</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config)# show diagnostic bootup level</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>copy running-config startup-config</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config)# copy running-config startup-config</td>
</tr>
</tbody>
</table>

### Activating a Diagnostic Test

You can set a diagnostic test as active and optionally modify the interval (in hours, minutes, and seconds) at which the test runs.

### BEFORE YOU BEGIN

Make sure that you are in the correct VDC. To change the VDC, use the `switchto vdc` command.
## Chapter 12 Configuring Online Diagnostics

**Send document comments to nexus7k-docfeedback@cisco.com.**

### SUMMARY STEPS

1. `config t`
2. `diagnostic monitor interval module slot test [test-id | name | all] hour hour min minutes second sec`
3. `diagnostic monitor module slot test [test-id | name | all]`
4. `show diagnostic content module {slot | all}`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong>&lt;br&gt;<code>config t</code>&lt;br&gt;Example: switch# config t&lt;br&gt;Enter configuration commands, one per line. End with CNTL/Z.&lt;br&gt;switch(config)#</td>
<td>Places you in global configuration mode.</td>
</tr>
</tbody>
</table>
| **Step 2**<br>`diagnostic monitor interval module slot test [test-id | name | all] hour hour min minutes second sec`<br>Example: switch(config)# diagnostic monitor interval module 6 test 3 hour 1 min 0 sec 0 | (Optional) Configures the interval at which the specified test is run. If no interval is set, the test runs at the interval set previously, or the default interval. The argument ranges are as follows:  
  - slot—The range is from 1 to 10.  
  - test-id—The range is from 1 to 14.  
  - name—Can be any case-sensitive alphanumeric string up to 32 characters.  
  - hour —The range is from 0 to 23 hours.  
  - minute—The range is from 0 to 59 minutes.  
  - second —The range is from 0 to 59 seconds. |
| **Step 3**<br>`diagnostic monitor module slot test [test-id | name | all]`<br>Example: switch(config)# diagnostic monitor interval module 6 test 3 | Activates the specified test. The argument ranges are as follows:  
  - slot—The range is from 1 to 10.  
  - test-id—The range is from 1 to 14.  
  - name—Can be any case-sensitive alphanumeric string up to 32 characters. |
| **Step 4**<br>`show diagnostic content module {slot | all}`<br>Example: switch(config)# show diagnostic content module 6 | (Optional) Displays information about the diagnostics and their attributes. |
Chapter 12      Configuring Online Diagnostics

Setting a Diagnostic Test as Inactive

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

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>no diagnostic monitor module slot test [test-id</td>
<td>name</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Starting or Stopping an On-Demand Diagnostic Test

You can start or stop an on-demand diagnostic test. You can optionally modify the number of iterations to repeat this test, and the action to take if the test fails.

We recommend that you only manually start a disruptive diagnostic test during a scheduled network maintenance time.

BEFORE YOU BEGIN

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

SUMMARY STEPS

1. diagnostic ondemand iteration number
2. diagnostic ondemand action-on-failure {continue failure-count num-fails | stop}
3. diagnostic start module slot test [test-id | name | all | non-disruptive] [port port-number | all]
4. diagnostic stop module slot test [test-id | name | all]
5. show diagnostic status module slot
Configuring Online Diagnostics

Send document comments to nexus7k-docfeedback@cisco.com.

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>diagnostic ondemand iteration number</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>switch# diagnostic ondemand iteration 5</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>**diagnostic ondemand action-on-failure {continue failure-count num-fails</td>
</tr>
<tr>
<td>Example:</td>
<td>switch# diagnostic ondemand action-on-failure stop</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>**diagnostic start module slot test [test-id</td>
</tr>
<tr>
<td>Example:</td>
<td>switch# diagnostic start module 6 test all</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>**diagnostic stop module slot test [test-id</td>
</tr>
<tr>
<td>Example:</td>
<td>switch# diagnostic stop module 6 test all</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>show diagnostic status module slot</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>switch# show diagnostic status module 6</td>
</tr>
</tbody>
</table>

Clearing Diagnostic Results

You can clear diagnostic test results.

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>**diagnostic clear result module [slot</td>
<td>all] test [test-id</td>
</tr>
<tr>
<td>Example:</td>
<td>switch# diagnostic clear result module 2 test all</td>
</tr>
<tr>
<td>The argument ranges are as follows:</td>
<td></td>
</tr>
<tr>
<td>• slot—The range is from 1 to 10.</td>
<td></td>
</tr>
<tr>
<td>• test-id—The range is from 1 to 14.</td>
<td></td>
</tr>
</tbody>
</table>
Simulating Diagnostic Results

You can simulate a diagnostic test result.

Use the following command in any mode to simulate a diagnostic test result:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>diagnostic test simulation module slot test test-id {fail</td>
<td>random-fail</td>
</tr>
</tbody>
</table>

Example:
```
switch# diagnostic test simulation module 2 test 2 fail
```

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>diagnostic test simulation module slot test test-id clear</td>
<td>Clears the simulated test result. The test-id range is from 1 to 14.</td>
</tr>
</tbody>
</table>

Example:
```
switch# diagnostic test simulation module 2 test 2 clear
```

Verifying Online Diagnostics Configuration

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show diagnostic bootup level</td>
<td>Displays information about bootup diagnostics.</td>
</tr>
<tr>
<td>show diagnostic content module [slot</td>
<td>all]</td>
</tr>
<tr>
<td>show diagnostic description module slot test [test-name</td>
<td>all]</td>
</tr>
<tr>
<td>show diagnostic events [error</td>
<td>info]</td>
</tr>
<tr>
<td>show diagnostic ondemand setting</td>
<td>Displays information about on-demand diagnostics.</td>
</tr>
<tr>
<td>show diagnostic results module slot [test [test-name</td>
<td>all]] [detail]</td>
</tr>
<tr>
<td>show diagnostic simulation module slot</td>
<td>Displays information about a simulated diagnostic.</td>
</tr>
<tr>
<td>show diagnostic status module slot</td>
<td>Displays the test status for all tests on a module.</td>
</tr>
</tbody>
</table>
Online Diagnostic Example Configuration

This example shows how to start all on-demand tests on module 6:

```
diagnostic start module 6 test all
```

This example shows how to activate test 2 and set the test interval on module 6:

```
conf t
    diagnostic monitor module 6 test 2
    diagnostic monitor interval module 6 test 2 hour 3 min 30 sec 0
```

Default Settings

Table 12-4 lists the default settings for online diagnostic parameters.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bootup diagnostics level</td>
<td>complete</td>
</tr>
<tr>
<td>Nondisruptive tests</td>
<td>active</td>
</tr>
</tbody>
</table>

Additional References

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

- Related Documents, page 12-11
- Standards, page 12-12

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online diagnostics CLI commands</td>
<td>Cisco Nexus 7000 Series NX-OS System Management Command Reference</td>
</tr>
<tr>
<td>VDCs and VRFs</td>
<td>Cisco Nexus 7000 Series NX-OS Virtual Device Context Command Reference</td>
</tr>
</tbody>
</table>
Feature History for Online Diagnostics

Table 12-5 lists the release history for this feature.

Table 12-5  Feature History for Online Diagnostics

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updated GOLD tests</td>
<td>4.2(1)</td>
<td>Added support for PortLoopback, StatusBus, and StandbyFabricLoopback tests.</td>
</tr>
<tr>
<td>Online diagnostics (GOLD)</td>
<td>4.0(q)</td>
<td>Feature was introduced.</td>
</tr>
</tbody>
</table>
CHAPTER 13

Configuring the Embedded Event Manager

This chapter describes how to configure the Embedded Event Manager (EEM) to detect and handle critical events on Cisco NX-OS devices.

This chapter includes the following sections:

- Information About EEM, page 13-1
- Licensing Requirements for EEM, page 13-5
- Prerequisites for EEM, page 13-6
- Guidelines and Limitations, page 13-6
- Configuring EEM, page 13-6
- Verifying EEM Configuration, page 13-17
- EEM Example Configuration, page 13-17
- Default Settings, page 13-18
- Additional References, page 13-18
- Feature History for EEM, page 13-19

Information About EEM

EEM monitors events that occur on your device and takes action to recover or troubleshoot these events, based on your configuration.

This section includes the following topics:

- EEM Overview, page 13-2
- Policies, page 13-2
- Event Statements, page 13-3
- Action Statements, page 13-4
- VSH Script Policies, page 13-4
- Environment Variables, page 13-5
- High Availability, page 13-5
- Virtualization Support, page 13-5
EEM Overview

EEM consists of three major components:

- **Event statements**—Events to monitor from another Cisco NX-OS component that may require some action, workaround, or notification.
- **Action statements**—An action that EEM can take, such as sending an e-mail, or disabling an interface, to recover from an event.
- **Policies**—An event paired with one or more actions to troubleshoot or recover from the event.

Policies

An EEM policy consists of an event statement and one or more action statements. The event statement defines the event to look for as well as the filtering characteristics for the event. The action statement defines the action EEM takes when the event occurs.

Figure 13-1 shows the two basic statements in an EEM policy.

**Figure 13-1  EEM Policy Statements**

```
EEM Policy

<table>
<thead>
<tr>
<th>Event Statement</th>
<th>Action Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tells your system: Look for this specific event to happen. For example, when a card is removed.</td>
<td>Tells your system: If that event happens, do these things. For example, when a card is removed, log the details.</td>
</tr>
</tbody>
</table>
```

You can configure EEM policies using the CLI or using a VSH script.

EEM gives you a device-wide view of policy management. You configure EEM policies on the supervisor, and EEM pushes the policy to the correct module based on the event type. EEM takes any actions for a triggered event either locally on the module or on the supervisor (the default option).

EEM maintains event logs on the supervisor.

Cisco NX-OS has a number of preconfigured system policies. These system policies define many common events and actions for the device. System policy names begin with two underscore characters (_ _).

You can create user policies to suit your network. If you create a user policy, any actions in your policy occur after EEM triggers any system policy actions related to the same event as your policy. To configure a user policy, see the “Defining a User Policy Using the CLI” section on page 13-7.

You can also override some system policies. The overrides that you configure take the place of the system policy. You can override the event or the actions.

Use the `show event manager system-policy` command to view the preconfigured system policies and determine which policies that you can override.

To configure an overriding policy, see the “Overriding a Policy” section on page 13-14.
You should use the `show running-config eem` command to check the configuration of each policy. An override policy that consists of an event statement and no action statement triggers no action and no notification of failures.

Your override policy should always include an event statement. An override policy without an event statement overrides all possible events in the system policy.

### Event Statements

An event is any device activity for which some action, such as a workaround or a notification, should be taken. In many cases, these events are related to faults in the device such as when an interface or a fan malfunctions.

EEM defines event filters so only critical events or multiple occurrences of an event within a specified time period trigger an associated action.

Figure 13-2 shows events that are handled by EEM.

---

**Event Manager**

- Validates and records user-defined policy information.
- Directs event notifications.
- Directs policy actions.
- Logs events.
- Dynamically registers the following:
  - event names
  - event descriptions
  - event actions
  - event parameters
- Filters events and matches with policies

---

**Events**

- link_flip
- storm_control
- metro_crc_fcs
- metro_fatal
- metro_r1p2_buf
- metro_fabric_u1f_ill_gen_code
- metro_fifo_full_fatal
- metro_fifo_full_non_fatal
- metro_illegal_pkt_len
- metroבסוף mismatch
- metro_intr_threshold
- URE_error
- LTL_party_error
- r2d2_internal_en-fatal_inter
- r2d2_internal_fatal_inter
- r2d2_cpu_fatal_interr
- r2d2_pkt_mgr_fatal_interrupts
- r2d2_pkt_mgr_non-fatal_inter
- r2d2_queue_fatal_inter
- r2d2_ingress_side_buffer_fatal
- r2d2_egress_side_buffer_non-
- r2d2_egress_side_buffer_fatal
- r2d2_10g_MAC_non-fatal_inter
- r2d2_MAC_MII_link_change
- r2d2_10g_MAC_non-fatal_int
- r2d2_RMC_fatal_interrupts
- r2d2_TMC_fatal_interrupts
- r2d2_DMC_non-fatal_interrupt
- r2d2_strm_counter_sslog_sta
- r2d2_strm_counter_sslog_00
- octopus_fatal_error
- octopus_severe_error
- octopus_chico_error
- gold
- counter

---

**User-defined Policy**

(Defined in CLI in an applet or script.)

---

**Event Log**
Event statements specify the event that triggers a policy to run. You can configure only one event statement per policy.

EEM schedules and runs policies on the basis of event statements. EEM examines the event and action commands and runs them as defined.

**Note**
If you want to allow the triggered event to process any default actions, you must configure the EEM policy to allow the event default action statement.

### Action Statements

Action statements describe the action triggered by a policy. Each policy can have multiple action statements. If no action is associated with a policy, EEM still observes events but takes no actions.

EEM supports the following actions in action statements:

- Execute any CLI commands.
- Update a counter.
- Log an exception.
- Force the shutdown of any module.
- Reload the device.
- Shut down specified modules because the power is over budget.
- Generate a syslog message.
- Generate a Call Home event.
- Generate an SNMP notification.
- Use the default action for the system policy.

**Note**
If you want to allow the triggered event to process any default actions, you must configure the EEM policy to allow the default action. For example, if you match a CLI command in a match statement, you must add the event-default action statement to the EEM policy or EEM will not allow the CLI command to execute.

**Note**
Verify that your action statements within your user policy or overriding policy do not negate each other or adversely affect the associated system policy.

### VSH Script Policies

You can also write policies in a VHS script, using a text editor. These policies have an event statement and action statement(s) just as other policies, and these policies can either augment or override system policies. After you write your script policy, copy it to the device and activate it. To configure a policy in a script, see the “Defining a Policy using a VSH Script” section on page 13-12.
Environment Variables

You can define environment variables for EEM that are available for all policies. Environment variables are useful for configuring common values that you can use in multiple policies. For example, you can create an environment variable for the IP address of an external e-mail server.

You can use an environment variable in action statements by using the parameter substitution format. Example 13-1 shows a sample action statement to force a module 1 shutdown, with a reset reason of “EEM action.”

**Example 13-1 Action Statement**

```
switch (config-eem-policy)# action 1.0 force-shut module 1 reset-reason "EEM action."
```

If you define an environment variable for the shutdown reason, called default-reason, you can replace that reset reason with the environment variable, as shown in Example 13-2.

**Example 13-2 Action Statement with Environment Variable**

```
switch (config-eem-policy)# action 1.0 force-shut module 1 reset-reason $default-reason
```

You can reuse this environment variable in any policy. For more information on environment variables, see the “Defining an Environment Variable” section on page 13-6.

High Availability

Cisco NX-OS supports stateless restarts for EEM. After a reboot or supervisor switchover, Cisco NX-OS applies the running configuration.

Virtualization Support

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

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

See the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.x*, for more information on VDCs.

Licensing Requirements for EEM

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

EEM has the following prerequisites:

- You must have network-admin or vdc-admin user privileges to configure EEM.

Guidelines and Limitations

EEM has the following configuration guidelines and limitations:

- The maximum number of configurable EEM policies is 500.
- Action statements within your user policy or overriding policy should not negate each other or adversely affect the associated system policy.
- If you want to allow a triggered event to process any default actions, you must configure the EEM policy to allow the default action. For example, if you match a CLI command in a match statement, you must add the event-default action statement to the EEM policy or EEM will not allow the CLI command to execute.
- An override policy that consists of an event statement and no action statement triggers no action and no notification of failures.
- An override policy without an event statement overrides all possible events in the system policy.

Configuring EEM

You can create policies that contain actions to take based on system policies. To display information about the system policies, use the `show event manager system-policy` command. For more information about system policies, see the “Embedded Event Manager System Events and Configuration Examples” appendix.

This section includes the following topics:

- Defining an Environment Variable, page 13-6
- Defining a User Policy Using the CLI, page 13-7
- Defining a Policy using a VSH Script, page 13-12
- Registering and Activating a VSH Script Policy, page 13-13
- Overriding a Policy, page 13-14
- Configuring Memory Thresholds, page 13-15

Defining an Environment Variable

You can define a variable to serve as a parameter in an EEM policy.

BEFORE YOU BEGIN

Make sure that you are in the correct VDC. To change the VDC, use the `switchto vdc` command.
Send document comments to nexus7k-docfeedback@cisco.com.

SUMMARY STEPS

1. config t
2. event manager environment variable-name variable-value
3. show event manager environment
4. copy running-config startup-config

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> config t</td>
<td>Places you in global configuration mode.</td>
</tr>
<tr>
<td>Example: switch# config t</td>
<td></td>
</tr>
<tr>
<td>Example: switch(config)#</td>
<td></td>
</tr>
<tr>
<td>Example: switch(config)#</td>
<td></td>
</tr>
<tr>
<td>Example: switch(config)#</td>
<td></td>
</tr>
<tr>
<td>Example: switch(config)#</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong> event manager environment variable-name variable-value</td>
<td>Creates an environment variable for EEM. The variable-name can be any case-sensitive alphanumeric string up to 29 characters. The variable-value can be any quoted alphanumeric string up to 39 characters.</td>
</tr>
<tr>
<td>Example: switch(config)# event manager environment emailto &quot;<a href="mailto:admin@anyplace.com">admin@anyplace.com</a>&quot;</td>
<td></td>
</tr>
<tr>
<td>Example: switch(config)# event manager environment emailto &quot;<a href="mailto:admin@anyplace.com">admin@anyplace.com</a>&quot;</td>
<td></td>
</tr>
<tr>
<td>Example: switch(config)# event manager environment emailto &quot;<a href="mailto:admin@anyplace.com">admin@anyplace.com</a>&quot;</td>
<td></td>
</tr>
<tr>
<td>Example: switch(config)# event manager environment emailto &quot;<a href="mailto:admin@anyplace.com">admin@anyplace.com</a>&quot;</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong> show event manager environment</td>
<td>(Optional) Displays information about the configured environment variables.</td>
</tr>
<tr>
<td>Example: switch(config-applet)# show event manager environment</td>
<td></td>
</tr>
<tr>
<td>Example: switch(config-applet)# show event manager environment</td>
<td></td>
</tr>
<tr>
<td>Example: switch(config-applet)# show event manager environment</td>
<td></td>
</tr>
<tr>
<td>Example: switch(config-applet)# show event manager environment</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong> copy running-config startup-config</td>
<td>(Optional) Saves this configuration change.</td>
</tr>
<tr>
<td>Example: switch(config)# copy running-config startup-config</td>
<td></td>
</tr>
<tr>
<td>Example: switch(config)# copy running-config startup-config</td>
<td></td>
</tr>
<tr>
<td>Example: switch(config)# copy running-config startup-config</td>
<td></td>
</tr>
<tr>
<td>Example: switch(config)# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

Defining a User Policy Using the CLI

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

This section includes the following topics:

- Configuring Event Statements, page 13-8
- Configuring Action Statements, page 13-11

BEFORE YOU BEGIN

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

SUMMARY STEPS

1. config t
2. event manager applet applet-name
3. description policy-description
Chapter 13  Configuring the Embedded Event Manager

Send document comments to nexus7k-docfeedback@cisco.com.

4. event event-statement
5. action number[number2] action-statement
   (Repeat Step 5 for multiple action statements.)
6. show event manager policy-state name [module module-id]
7. copy running-config startup-config

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>config t</td>
</tr>
<tr>
<td>Example:</td>
<td>Places you in global configuration mode.</td>
</tr>
<tr>
<td>switch# config t</td>
<td></td>
</tr>
<tr>
<td>Enter configuration commands, one per line. End with CNTRL/Z.</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
</tbody>
</table>

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

| Step 3  | description policy-description |
| Example: | (Optional) Configures a descriptive string for the policy. The string can be any alphanumeric string up to 80 characters. Enclose the string in quotation marks. |
| switch(config-applet)# description "Monitors interface shutdown." |

| Step 4  | event event-statement |
| Example: | Configures the event statement for the policy. See the “Configuring Event Statements” section on page 13-8. |
| switch(config-applet)# event cli match "shutdown" |

| Step 5  | action number[number2] action-statement |
| Example: | Configures an action statement for the policy. See the “Configuring Action Statements” section on page 13-11. |
| switch(config-applet)# action 1.0 cli show interface e 3/1 |
| Repeat Step 5 for multiple action statements. |

| Step 6  | show event manager policy-state name [module module-id] |
| Example: | (Optional) Displays information about the status of the configured policy. |
| switch(config-applet)# show event manager policy-state monitorShutdown |

| Step 7  | copy running-config startup-config |
| Example: | (Optional) Saves this configuration change. |
| switch(config)# copy running-config startup-config |

Configuring Event Statements

Use one the following commands in EEM configuration mode to configure an event statement:
## Configuring EEM

### Command

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>event cli match expression [count repeats</td>
<td>time seconds]</td>
</tr>
<tr>
<td>event counter name counter entry-val entry entry-op {eq</td>
<td>ge</td>
</tr>
<tr>
<td>event fanabsent [fan number] time seconds</td>
<td>Triggers an event if a fan is removed from the device for more than the configured time, in seconds. The number range is module dependent. The seconds range is from 10 to 64000.</td>
</tr>
<tr>
<td>event fanbad [fan number] time seconds</td>
<td>Triggers an event if a fan fails for more than the configured time, in seconds. The number range is module dependent. The seconds range is from 10 to 64000.</td>
</tr>
<tr>
<td>event gold module {slot</td>
<td>all} test test-name {severity (major</td>
</tr>
<tr>
<td>event memory {critical</td>
<td>minor</td>
</tr>
<tr>
<td>event module-failure type failure-type module {slot</td>
<td>all} count repeats [time seconds]</td>
</tr>
<tr>
<td>event module status {online</td>
<td>offline</td>
</tr>
</tbody>
</table>
## Command Purpose

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| event oir (fan | module | powersupply) (anyoir | insert | remove) [number] | Triggers an event if the configured device element (fan, module, or power supply) is inserted or removed from the device. You can optionally configure a specific fan, module, or power supply number. The *number* range is as follows:
- Fan number—Module dependent.
- Module number—Device dependent.
- Power supply number—The range is from 1 to 3. |
| **Example:** switch(config-applet)# event oir fan remove 4 | |
| event policy-default count repeats [time seconds] | Uses the event configured in the system policy. Use this option for overriding policies. The *repeats* range is from 1 to 65000. The *seconds* range is from 0 to 4294967295, where 0 indicates no time limit. |
| **Example:** switch(config-applet)# event policy-default count 3 | |
| event poweroverbudget | Triggers an event if the power budget exceeds the capacity of the configured power supplies. |
| **Example:** switch(config-applet)# event poweroverbudget | |
| event snmp oid oid get-type (exact | next) entry-op (eq | ge | gt | le | lt | ne) entry-val entry [exit-comb (and | or)] exit-op (eq | ge | gt | le | lt | ne) exit-val exit exit-time time polling-interval interval | Triggers an event if the SNMP OID crosses the entry threshold based on the entry operation. The event resets immediately or optionally, you can configure the event to reset after the counter passes the exit threshold. The OID is in dotted decimal notation. The *entry* and *exit* value ranges are from 0 to 18446744073709551615. The time, in seconds, is from 0 to 2147483647. The interval, in seconds, is from 1 to 2147483647. |
| **Example:** switch(config-applet)# event snmp oid 1.3.6.1.2.1.31.1.1.1.6 get-type next entry-op lt 300 entry-val 0 exit-op eq 400 exit-time 30 polling-interval 300 | |
| event storm-control | Triggers an event if traffic on a port exceeds the configured storm control threshold. |
| **Example:** switch(config-applet)# event storm-control | |
| event sysmgr memory (module | module-num) major major-percent minor minor-percent clear clear-percent | Triggers an event if the specified system manager memory threshold is exceeded. The range for the percentage is from 1 to 99. |
| **Example:** switch(config-applet)# event sysmgr memory minor 80 | |
| event sysmgr switchover count count time interval | Triggers an event if the specified switchover count is exceeded within the time interval specified. The switchover count is from 1 to 65000. The time interval is from 0 to 2147483647. |
| **Example:** switch(config-applet)# event sysmgr switchover count 10 time 1000 | |
### Configuring EEM

**Configuring Action Statements**

Use the following commands in EEM configuration mode to configure action statements:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **event temperature** [module slot] [sensor number] threshold {any | major | minor} | Triggers an event if the temperature sensor exceeds the configured threshold. The sensor range is from 1 to 18.  
Example:  
switch(config-applet)# event temperature module 2 threshold any |
| **event track** object-number state {any | down | up} | Triggers an event if the tracked object is in the configured state. The **object-number** range is from 1 to 500.  
Example:  
switch(config-applet)# event track 1 state down |
| **action** number[.number2] cli command1 [command2...] [local] | Runs the configured CLI commands. You can optionally run the commands on the module where the event occurred. The action label is in the format number1.number2.  
**number** can be any number up to 16 digits. The range for **number2** is from 0 to 9.  
Example:  
switch(config-applet)# action 1.0 cli "show interface e 3/1" |
| **action** number[.number2] counter name counter value val op {dec | inc | nop | set} | Modifies the counter by the configured value and operation. The action label is in the format number1.number2.  
**number** can be any number up to 16 digits. The range for **number2** is from 0 to 9.  
The counter name can be any case-sensitive, alphanumeric string up to 28 characters. The **val** can be an integer from 0 to 2147483647 or a substituted parameter.  
Example:  
switch(config-applet)# action 2.0 counter name mycounter value 20 op inc |
| **action** number[.number2] event-default | Executes the default action for the associated event. The action label is in the format number1.number2.  
**number** can be any number up to 16 digits. The range for **number2** is from 0 to 9.  
Example:  
switch(config-applet)# action 1.0 event-default |
| **action** number[.number2] forcesshut [module slot | xbar xbar-number] reset-reason seconds | Forces a module, crossbar, or the entire system to shut down. The action label is in the format number1.number2.  
**number** can be any number up to 16 digits. The range for **number2** is from 0 to 9.  
The reset reason is a quoted alphanumeric string up to 80 characters.  
Example:  
switch(config-applet)# action 1.0 forcesshut module 2 reset-reason "flapping links" |
Configuring EEM

Chapter 13      Configuring the Embedded Event Manager

Note

If you want to allow the triggered event to process any default actions, you must configure the EEM policy to allow the default action. For example, if you match a CLI command in a match statement, you must add the event-default action statement to the EEM policy or EEM will not allow the CLI command to execute. You can use the terminal event-manager bypass command to allow all EEM policies with CLI matches to execute the CLI command.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>action number[.number2] overbudgetshut [module slot [- slot]]</td>
<td>Forces one or more modules or the entire system to shut down because of a power overbudget issue. number can be any number up to 16 digits. The range for number2 is from 0 to 9.</td>
</tr>
<tr>
<td>Example: switch(config-applet)# action 1.0 overbudgetshut module 3-5</td>
<td></td>
</tr>
<tr>
<td>action number[.number2] policy-default</td>
<td>Executes the default action for the policy that you are overriding. The action label is in the format number1.number2. number can be any number up to 16 digits. The range for number2 is from 0 to 9.</td>
</tr>
<tr>
<td>Example: switch(config-applet)# action 1.0 policy-default</td>
<td></td>
</tr>
<tr>
<td>action number[.number2] reload [module slot [- slot]]</td>
<td>Forces one or more modules or the entire system to reload. number can be any number up to 16 digits. The range for number2 is from 0 to 9.</td>
</tr>
<tr>
<td>Example: switch(config-applet)# action 1.0 reload module 3-5</td>
<td></td>
</tr>
<tr>
<td>action number[.number2] snmp-trap { [intdata1 data [intdata2 data] [strdata string]}</td>
<td>Sends an SNMP trap with the configured data. number can be any number up to 16 digits. The range for number2 is from 0 to 9. The data arguments can by any number up to 80 digits. The string can be any alphanumeric string up to 80 characters.</td>
</tr>
<tr>
<td>Example: switch(config-applet)# action 1.0 snmp-trap strdata &quot;temperature problem&quot;</td>
<td></td>
</tr>
<tr>
<td>action number[.number2] syslog [priority prio-val] msg error-message</td>
<td>Sends a customized syslog message at the configured priority. number can be any number up to 16 digits. The range for number2 is from 0 to 9. The error-message can be any quoted alphanumeric string up to 80 characters.</td>
</tr>
<tr>
<td>Example: switch(config-applet)# action 1.0 syslog priority notifications msg &quot;cpu high&quot;</td>
<td></td>
</tr>
</tbody>
</table>

Defining a Policy using a VSH Script

You can define a policy using a VSH script.

BEFORE YOU BEGIN

Make sure that you are in the correct VDC. To change the VDC, use the switchto vdc command.
Ensure that you are logged in with administrator privileges.
Ensure that your script name is the same name as the script filename.
Configuring EEM

Chapter 13      Configuring the Embedded Event Manager

**Send document comments to nexus7k-docfeedback@cisco.com.**

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>config t</td>
<td>Places you in global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch# config t</td>
<td>Enter configuration commands, one per line. End with CNTL/Z.</td>
</tr>
<tr>
<td></td>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>event manager policy policy-script</td>
<td>Registers and activates an EEM script policy. The policy-script can be any case-sensitive alphanumeric string up to 29 characters.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# event manager policy moduleScript</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>show event manager policy name</td>
<td>(Optional) Displays information about the configured policy.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config-applet)# show event manager policy moduleScript</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>copy running-config startup-config</td>
<td>(Optional) Saves this configuration change.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

Registering and Activating a VSH Script Policy

You can register and activate a policy defined in a VSH script.

**BEFORE YOU BEGIN**

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

**SUMMARY STEPS**

1. `config t`
2. `event manager policy policy-script`
3. `show event manager policy name`
4. `copy running-config startup-config`

**DETAILED STEPS**

**Command**

**Purpose**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>config t</td>
<td>Places you in global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch# config t</td>
<td>Enter configuration commands, one per line. End with CNTL/Z.</td>
</tr>
<tr>
<td></td>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>event manager policy policy-script</td>
<td>Registers and activates an EEM script policy. The policy-script can be any case-sensitive alphanumeric string up to 29 characters.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# event manager policy moduleScript</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>show event manager policy name</td>
<td>(Optional) Displays information about the configured policy.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config-applet)# show event manager policy moduleScript</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>copy running-config startup-config</td>
<td>(Optional) Saves this configuration change.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>
You can override a system policy.

**BEFORE YOU BEGIN**

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

**SUMMARY STEPS**

1. `config t`
2. `show event manager policy-state system-policy`
3. `event manager applet applet-name override system-policy`
4. `description policy-description`
5. `event event-statement`
6. `action number action-statement`
   (Repeat Step 6 for multiple action statements.)
7. `show event manager policy-state name`
8. `copy running-config startup-config`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**

*Example:*
```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)#
```

Places you in global configuration mode.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 2**

*Example:*
```
switch(config-applet)# show event manager policy-state __ethpm_link_flap
Policy __ethpm_link_flap
  Cfg count : 5
  Cfg time interval : 10.000000 (seconds)
  Hash default, Count 0
```

(Optional) Displays information about the system policy that you want to override, including thresholds. Use the `show event manager system-policy` command to find the system policy names. For information about system policies, see the “Embedded Event Manager System Events and Configuration Examples” appendix.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 3**

*Example:*
```
switch(config)# event manager applet ethport override __ethpm_link_flap
switch(config-applet)#
```

Overrides a system policy and enters applet configuration mode. The `applet-name` can be any case-sensitive alphanumeric string up to 29 characters. The `system-policy` must be one of the existing system policies.
## Configuring Memory Thresholds

You can set the memory thresholds used to trigger events and set whether the operating system should kill processes if it cannot allocate memory.

### BEFORE YOU BEGIN

Make sure that you are in the correct VDC. To change the VDC, use the `switchto vdc` command. Ensure that you are logged in with administrator privileges.

### SUMMARY STEPS

1. `config t`
2. `system memory-thresholds minor minor severe severe critical critical`
3. `system memory-thresholds threshold critical no-process-kill`
4. `show running-config | include “system memory”`
5. `copy running-config startup-config`

---

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td><code>description policy-description</code></td>
<td>(Optional) Configures a descriptive string for the policy. The string can be any alphanumeric string up to 80 characters. Enclose the string in quotation marks.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>switch(config-applet)# description &quot;Overrides link flap policy.&quot;</code></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><code>event event-statement</code></td>
<td>Configures the event statement for the policy. See the “Configuring Event Statements” section on page 13-8.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>switch(config-applet)# event policy-default count 2 time 1000</code></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td><code>action number action-statement</code></td>
<td>Configures an action statement for the policy. See the “Configuring Action Statements” section on page 13-11. Repeat Step 6 for multiple action statements.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>switch(config-applet)# action 1.0 syslog priority warnings msg &quot;Link is flapping.&quot;</code></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td><code>show event manager policy-state name</code></td>
<td>(Optional) Displays information about the configured policy.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>switch(config-applet)# show event manager policy-state ethport</code></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Saves this configuration change.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>switch(config)# copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>
## Configuring EEM

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>config t</td>
<td>Places you in global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch# config t</td>
<td>Enter configuration commands, one per line. End with CNTL/Z.</td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>system memory-thresholds minor minor severe severe critical critical</td>
<td>Configures the system memory thresholds that generate EEM memory events. The default values are as follows:</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config)# system memory-thresholds minor 60 severe 70 critical 80</td>
<td></td>
</tr>
<tr>
<td></td>
<td>When these memory thresholds are exceeded, the system generates the following syslogs:</td>
</tr>
<tr>
<td></td>
<td>• 2009 May 7 17:06:30 switch %$ VDC-1 %$ %PLATFORM-2-MEMORY_ALERT: Memory Status Alert : MINOR</td>
</tr>
<tr>
<td></td>
<td>• 2009 May 7 17:06:30 switch %$ VDC-1 %$ %PLATFORM-2-MEMORY_ALERT: Memory Status Alert : SEVERE</td>
</tr>
<tr>
<td></td>
<td>• 2009 May 7 17:06:30 switch %$ VDC-1 %$ %PLATFORM-2-MEMORY_ALERT: Memory Status Alert : CRITICAL</td>
</tr>
<tr>
<td></td>
<td>• 2009 May 7 17:06:35 switch %$ VDC-1 %$ %PLATFORM-2-MEMORY_ALERT: Memory Status Alert : MINOR ALERT RECOVERED</td>
</tr>
<tr>
<td></td>
<td>• 2009 May 7 17:06:35 switch %$ VDC-1 %$ %PLATFORM-2-MEMORY_ALERT: Memory Status Alert : SEVERE ALERT RECOVERED</td>
</tr>
<tr>
<td></td>
<td>• 2009 May 7 17:06:35 switch %$ VDC-1 %$ %PLATFORM-2-MEMORY_ALERT: Memory Status Alert : CRITICAL ALERT RECOVERED</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>system memory-thresholds threshold critical no-process-kill</td>
<td>(Optional) Configures the system to not kill processes when the memory cannot be allocated. The default value is to allow the system to kill processes, starting with the one that consumes the most memory.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config)# system memory-thresholds threshold critical no-process-kill</td>
<td></td>
</tr>
</tbody>
</table>
Verifying EEM Configuration

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show event manager environment [variable-name</td>
<td>all]</td>
</tr>
<tr>
<td>show event manager event-types [event</td>
<td>all</td>
</tr>
<tr>
<td>show event manager history events [detail] [maximum num-events] [severity {catastrophic</td>
<td>minor</td>
</tr>
<tr>
<td>show event manager policy internal [policy-name] [inactive]</td>
<td>Displays information about the configured policies.</td>
</tr>
<tr>
<td>show event manager policy-state policy-name</td>
<td>Displays information about the policy state, including thresholds.</td>
</tr>
<tr>
<td>show event manager script system [policy-name</td>
<td>all]</td>
</tr>
<tr>
<td>show event manager system-policy [all]</td>
<td>Displays information about the predefined system policies.</td>
</tr>
<tr>
<td>show running-config eem</td>
<td>Displays information about the running configuration for EEM.</td>
</tr>
<tr>
<td>show startup-config eem</td>
<td>Displays information about the startup configuration for EEM.</td>
</tr>
</tbody>
</table>

EEM Example Configuration

This example shows how to override the _lcm_module_failure system policy by changing the threshold for just module 3 hitless upgrade failures. This example also sends a syslog message. The settings in the system policy, _lcm_module_failure, apply in all other cases.

```
event manager applet example2 override _lcm_module_failure
event module-failure type hitless-upgrade-failure module 3 count 2
action 1 syslog priority errors msg module 3 "upgrade is not a hitless upgrade!"
```
Default Settings

This example shows how to override the `__ethpm_link_flap` system policy and shuts down the interface.

```plaintext
event manager applet ethport override __ethpm_link_flap
  event policy-default count 2 time 1000
  action 1 cli conf t
  action 2 cli int et1/1
  action 3 cli no shut
```

This example creates an EEM policy that allows the CLI command to execute but triggers an SNMP notification when a user enters configuration mode on the device:

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

**Note**

You must add the `default-event` action statement to the EEM policy or EEM will not allow the CLI command to execute.

---

### Default Settings

**Table 13-1** lists the default settings for EEM parameters.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>system policies</td>
<td>Active</td>
</tr>
</tbody>
</table>

**Additional References**

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

- Related Documents, page 13-19
- Standards, page 13-19
Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>EEM commands</td>
<td>Cisco Nexus 7000 Series NX-OS System Management Command Reference</td>
</tr>
<tr>
<td>VDCs</td>
<td>Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.x</td>
</tr>
</tbody>
</table>

Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>—</td>
</tr>
</tbody>
</table>

Feature History for EEM

Table 13-2 lists the release history for this feature.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory thresholds</td>
<td>4.2(4)</td>
<td>Changed the minor, severe, and critical default memory thresholds from 70, 80, and 90 to 85, 90, and 95.</td>
</tr>
<tr>
<td>Memory Thresholds Configuration</td>
<td>4.1(3)</td>
<td>Added a configuration section for memory thresholds. See the “Configuring Memory Thresholds” section on page 13-15.</td>
</tr>
</tbody>
</table>
CHAPTER 14

Configuring SPAN

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

This chapter includes the following sections:

- Information About SPAN, page 14-1
- Licensing Requirements for SPAN, page 14-5
- Prerequisites for SPAN, page 14-5
- Guidelines and Limitations, page 14-5
- Configuring SPAN, page 14-6
- Verifying the SPAN Configuration, page 14-15
- SPAN Example Configurations, page 14-15
- Additional References, page 14-17
- Feature History for SPAN, page 14-18

Information About SPAN

SPAN analyzes all traffic between source ports by directing the SPAN session traffic to a destination port with an external analyzer attached to it.

You can define the sources and destinations to monitor in a SPAN sessions on the local device.

This section includes the following topics:

- SPAN Sources, page 14-2
- SPAN Destinations, page 14-2
- SPAN Sessions, page 14-3
- Virtual SPAN Sessions, page 14-3
- Multiple SPAN Sessions, page 14-4
- High Availability, page 14-4
- Virtualization Support, page 14-4
Information About SPAN

Send document comments to nexus7k-docfeedback@cisco.com.

SPAN Sources

The interfaces from which traffic can be monitored are called SPAN sources. Sources designate the traffic to monitor and whether to copy ingress, egress, or both directions of traffic. SPAN sources include the following:

- Ethernet ports
- VLANs—When a VLAN is specified as a SPAN source, all supported interfaces in the VLAN are SPAN sources.
- Remote SPAN (RSPAN) VLANs
- The inband interface to the control plane CPU—You can monitor the inband interface only from the default VDC. Inband traffic from all VDCs is monitored.

Note

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

Characteristics of Source Ports

SPAN source ports have the following characteristics:

- A port configured as a source port cannot also be configured as a destination port.
- An RSPAN VLAN can only be used as a SPAN source.
- If you use the supervisor inband interface as a SPAN source, the following packets are monitored:
  - All packets that arrive on the supervisor hardware (ingress)
  - All packets generated by the supervisor hardware (egress)

SPAN Destinations

SPAN destinations refer to the interfaces that monitor source ports. Destination ports receive the copied traffic from SPAN sources.

Characteristics of Destination Ports

SPAN destination ports have the following characteristics:

- Destinations for a SPAN session include Ethernet ports or port-channel interfaces in either access or trunk mode.
- A port configured as a destination port cannot also be configured as a source port.
- A destination port can be configured in only one SPAN session at a time.
- Destination ports do not participate in any spanning tree instance. SPAN output includes Bridge Protocol Data Unit (BPDU) Spanning-Tree Protocol hello packets.
- An RSPAN VLAN cannot be used as a SPAN destination.
- You can configure SPAN destinations to inject packets to disrupt a certain TCP packet stream in support of the Intrusion Detection System (IDS).
- You can configure SPAN destinations to enable a forwarding engine to learn the MAC address of the IDS.
**SPAN Sessions**

You can create up to 18 SPAN sessions designating sources and destinations to monitor.

**Note**

Only two SPAN sessions can be running simultaneously.

**Figure 14-1** shows a SPAN configuration. Packets on three Ethernet ports are copied to destination port Ethernet 2/5. Only traffic in the direction specified is copied.

**Figure 14-1** SPAN Configuration

<table>
<thead>
<tr>
<th>Source Port</th>
<th>Direction</th>
<th>Destination Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>E 2/1</td>
<td>Rx</td>
<td>E 2/5</td>
</tr>
<tr>
<td>E 2/2</td>
<td>Rx, Tx</td>
<td></td>
</tr>
<tr>
<td>E 2/3</td>
<td>Tx</td>
<td></td>
</tr>
</tbody>
</table>

**Virtual SPAN Sessions**

You can create a virtual SPAN session to monitor multiple VLAN sources and choose only VLANs of interest to transmit on multiple destination ports. For example, you can configure SPAN on a trunk port and monitor traffic from different VLANs on different destination ports.

**Figure 14-2** shows a virtual SPAN configuration. The virtual SPAN session copies traffic from the three VLANs to the three specified destination ports. You can choose which VLANs to allow on each destination port to limit the traffic that the device transmits on it. In **Figure 14-2**, the device transmits packets from one VLAN at each destination port.

**Note**

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

For information about configuring a virtual SPAN session, see the “Configuring a Virtual SPAN Session” section on page 14-10.

Multiple SPAN Sessions

Although you can define up to 18 SPAN sessions, only two SPAN sessions can be running simultaneously. You can shut down an unused SPAN session.

For information about shutting down SPAN sessions, see the “Shutting Down or Resuming a SPAN Session” section on page 14-13.

High Availability

The SPAN feature supports stateless and stateful restarts. After a reboot or supervisor switchover, Cisco NX-OS applies the running configuration.

Virtualization Support

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

Note

You can monitor the inband interface only from the default VDC. Inband traffic from all VDCs is monitored.

For information about configuring VDCs, see the Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.x.
Licensing Requirements for SPAN

The following table shows the licensing requirements for this feature:

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

Prerequisites for SPAN

SPAN has the following prerequisites:

- You must first configure the ports on each device to support the desired SPAN configuration. For more information, see the Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 4.x.

Guidelines and Limitations

SPAN has the following configuration guidelines and limitations:

- Table 1 lists the SPAN session limits.

<table>
<thead>
<tr>
<th>Description</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configured SPAN sessions</td>
<td>18</td>
</tr>
<tr>
<td>Simultaneously running SPAN sessions</td>
<td>2</td>
</tr>
<tr>
<td>Source interfaces per session</td>
<td>128</td>
</tr>
<tr>
<td>Source VLANs per session¹</td>
<td>32</td>
</tr>
<tr>
<td>Destination interfaces per session</td>
<td>32</td>
</tr>
</tbody>
</table>

¹ If you specify a VLAN range greater than 32, the first 32 VLANs are added as source VLANs to the SPAN session even if the VLANs have not been created. For example, if you specify a VLAN range of 1-40 for the SPAN session, only VLANs 1-32 are added to the SPAN session. To add only specific VLANs within a range, you must add the VLANs explicitly.

- SPAN is not supported for management ports.
- A destination port can only be configured in one SPAN session at a time.
- You cannot configure a port as both a source and destination port.
- A single SPAN session can include mixed sources in any combination of the following:
  - Ethernet ports, but not subinterfaces.
  - VLANs, which can be assigned to port channel subinterfaces
  - The inband interface to the control plane CPU
- Destination ports do not participate in any spanning tree instance. SPAN output includes Bridge Protocol Data Unit (BPDU) Spanning-Tree Protocol hello packets.
• When a SPAN session contains source ports that are monitored in the transmit or transmit and receive direction, packets that these ports receive may be replicated to the SPAN destination port even though the packets are not actually transmitted on the source ports. Some examples of this behavior on source ports include:
  – Traffic that results from flooding
  – Broadcast and multicast traffic
• For VLAN SPAN sessions with both ingress and egress configured, two packets (one from ingress and one from egress) are forwarded from the destination port if the packets get switched on the same VLAN.
• VLAN SPAN monitors only the traffic that leaves or enters Layer 2 ports in the VLAN.
• You can monitor the inband interface only from the default VDC. Inband traffic from all VDCs is monitored.
• You can configure an RSPAN VLAN for use only as a SPAN session source.
• You can configure a SPAN session on the local device only.
• SPAN sessions cannot capture packets with broadcast or multicast MAC addresses that reach the supervisor, such as ARP requests and Open Shortest Path First (OSPF) protocol hello packets, if the source of the session is the supervisor ethernet in-band interface. To capture these packets, you must use the physical interface as the source in the SPAN sessions.
• All SPAN replication is performed in the hardware. The supervisor CPU is not involved.

Configuring SPAN

This section includes the following topics:

- Configuring a SPAN Session, page 14-6
- Configuring a Virtual SPAN Session, page 14-10
- Configuring an RSPAN VLAN, page 14-12
- Shutting Down or Resuming a SPAN Session, page 14-13

Note
Cisco NX-OS commands for this feature may differ from those in Cisco IOS.

Configuring a SPAN Session

You can configure a SPAN session on the local device only. By default, SPAN sessions are created in the shut state.

For sources, you can specify Ethernet ports, port channels, the supervisor inband interface, VLANs, and RSPAN VLANs. You can specify private VLANs (primary, isolated, and community) in SPAN sources.

A single SPAN session can include mixed sources in any combination of Ethernet ports, VLANs, or the inband interface to the control plane CPU. You cannot specify Ethernet port subinterfaces as sources for a SPAN session.
To use a Layer 3 port-channel subinterface as a SPAN source in the monitor session, you must specify the vlan ID that you entered when configuring IEEE 802.1Q VLAN encapsulation for the subinterface as the filter VLAN. When you use the main interface and the SPAN VLAN filter to filter the 802.1Q VLANs on the subinterfaces, SPAN shows the traffic for all subinterfaces on the SPAN destination port.

When you specify the supervisor inband interface for a SPAN source, the device monitors all packets that arrive on the supervisor hardware (ingress) and all packets generated by the supervisor hardware (egress).

For destination ports, you can specify Ethernet ports or port-channels in either access or trunk mode. You must enable monitor mode on all destination ports.

BEFORE YOU BEGIN

Make sure that you are in the correct VDC. To switch VDCs, use the `switchto vdc` command.

- You must have already configured the destination ports in access or trunk mode. For more information, see the Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 4.x at the following.

SUMMARY STEPS

1. `config t`
2. `interface ethernet slot/port[-port]`
3. `switchport`
4. `switchport mode [access | trunk | private-vlan]`
5. `switchport monitor [ingress [learning]]`
6. Repeat Steps 2 and 3 to configure monitoring on additional SPAN destinations.
7. `no monitor session session-number`
8. `monitor session session-number`
9. `description description`
10. `source {interface type | vlan {number | range} [rx | tx | both]`
11. Repeat Step 8 to configure all SPAN sources.
12. `filter vlan {number | range}`
13. Repeat Step 10 to configure all source VLANs to filter.
14. `destination interface type {number | range}`
15. Repeat Step 12 to configure all SPAN destination ports.
16. `no shut`
17. `show monitor session {all | session-number | range session-range} [brief]`
18. `copy running-config startup-config`
# Configuring SPAN

## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>config t</code></td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
| **Example:** | switch# config t  
switch(config)# |
| **Step 2** | Enters interface configuration mode on the selected slot and port or range of ports. |
| `interface ethernet slot[/port]` | |
| **Example:** | switch(config)# interface ethernet 2/5  
switch(config-if)# |
| **Step 3** | Configures switchport parameters for the selected slot and port or range of ports. |
| `switchport` | |
| **Example:** | switch(config-if)# switchport  
switch(config-if)# |
| **Step 4** | Configures the switchport mode for the selected slot and port or range of ports. |
| `switchport mode [access | trunk | private-vlan]` | 
- access  
- trunk  
- private-vlan |
| **Example:** | switch(config-if)# switchport mode trunk  
switch(config-if)# |
| **Step 5** | Configures the switchport interface as a SPAN destination: |
| `switchport monitor [ingress [learning]]` | - **ingress** Allows the SPAN destination port to inject packets that disrupt a certain TCP packet stream, for example, in networks with IDS.  
- **ingress learning** Allows the SPAN destination port to inject packets, and learning adds the ability for the switch to learn the MAC address of the downstream network analysis device. |
| **Example:** | switch(config-if)# switchport monitor |
| **Step 6** | *(Optional) Repeat Steps 2 and 3 to configure monitoring on additional SPAN destinations.* |
| **Step 7** | Clears the configuration of the specified SPAN session. The new session configuration is added to the existing session configuration. |
| `no monitor session session-number` | |
| **Example:** | switch(config)# no monitor session 3 |
| **Step 8** | Enters the monitor configuration mode. The new session configuration is added to the existing session configuration. By default, the session is created in the shut state. |
| `monitor session session-number` | |
| **Example:** | switch(config)# monitor session 3  
switch(config-monitor)# |
| **Step 9** | Configures a description for the session. By default, no description is defined. The description can be up to 32 alphanumeric characters. |
| `description description` | |
| **Example:** | switch(config-monitor)# description my_span_session_3 |
Send document comments to nexus7k-docfeedback@cisco.com.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>`source {interface type</td>
<td>vlan (1-3967,4048-4093)} [rx</td>
</tr>
<tr>
<td>11</td>
<td>(Optional) Repeat Step 8 to configure all SPAN sources.</td>
<td>—</td>
</tr>
<tr>
<td>12</td>
<td>`filter vlan (number</td>
<td>range)`</td>
</tr>
<tr>
<td>13</td>
<td>(Optional) Repeat Step 10 to configure all source VLANs to filter.</td>
<td>—</td>
</tr>
<tr>
<td>14</td>
<td>`destination interface type {number</td>
<td>range}`</td>
</tr>
<tr>
<td>15</td>
<td>(Optional) Repeat Step 12 to configure all SPAN destination ports.</td>
<td>—</td>
</tr>
<tr>
<td>16</td>
<td><code>no shut</code></td>
<td>Enables the SPAN session. By default, the session is created in the shut state. <strong>Note</strong> Only two SPAN sessions can be running simultaneously.</td>
</tr>
<tr>
<td>17</td>
<td>`show monitor session {all</td>
<td>session-number</td>
</tr>
<tr>
<td>18</td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Copies the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>
Configuring a Virtual SPAN Session

You can configure a virtual SPAN session to copy packets from source ports, VLANs, and RSPAN VLANs to destination ports on the local device. By default, SPAN sessions are created in the shut state.

For sources, you can specify ports, VLANs, or RSPAN VLANs.

For destination ports, you can specify Ethernet ports. You can choose which VLANs to allow on each destination port to limit the traffic that the device transmits on it.

BEFORE YOU BEGIN

1. Ensure that you are in the correct VDC (or use the switchto vdc command).
2. You have already configured the destination ports in trunk mode. For more information, see the Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 4.x.
3. You have already configured the destination ports to monitor a SPAN session with the switchport monitor command.

SUMMARY STEPS

1. config t
2. no monitor session session-number
3. monitor session session-number
4. source {interface type | vlan} {number | range} [rx | tx | both]
5. Repeat Step 4 to configure all virtual SPAN VLAN sources.
6. destination interface type {number | range}
7. Repeat Step 6 to configure all virtual SPAN destination ports.
8. no shut
9. show monitor session {all | session-number | range session-range} [brief]
10. interface ethernet slot/port[-port]
11. switchport
12. switchport mode trunk
13. switchport trunk allowed vlan { {number | range} | add {number | range} | except {number | range} | remove {number | range} | all | none}
14. Repeat Steps 10 and 11 to configure the allowed VLANs on each destination port.
15. show interface ethernet slot/port[-port] trunk
16. copy running-config startup-config
## Chapter 14  Configuring SPAN

**Send document comments to nexus7k-docfeedback@cisco.com.**

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>config t</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch# config t</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>no monitor session session-number</td>
<td>Clears the configuration of the specified SPAN session. New session configuration is added to the existing session configuration.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# no monitor session 3</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>monitor session session-number</td>
<td>Enters the monitor configuration mode. A new session configuration is added to the existing session configuration.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# monitor session 3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config-monitor)#</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>source {interface type</td>
<td>vlan} {number</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config-monitor)# source vlan 3, 6-8 tx</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>(Optional) Repeat Step 4 to configure all virtual SPAN source VLANs.</td>
<td>—</td>
</tr>
<tr>
<td>6</td>
<td>destination interface type {number</td>
<td>range}</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config-monitor)# destination interface ethernet 2/5, ethernet 3/7</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>(Optional) Repeat Step 6 to configure all virtual SPAN destination ports.</td>
<td>—</td>
</tr>
<tr>
<td>8</td>
<td>no shut</td>
<td>Enables the SPAN session. By default, the session is created in the shut state.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config-monitor)# no shut</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>show monitor session {all</td>
<td>session-number</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config-monitor)# show monitor session 3</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring SPAN

**Configuring an RSPAN VLAN**

You can specify a remote SPAN (RSPAN) VLAN as a SPAN session source.

**BEFORE YOU BEGIN**

Ensure that you are in the correct VDC (or use the `switchto vdc` command).

**SUMMARY STEPS**

1. `config t`
2. `vlan vlan`

---

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 10</strong></td>
<td><strong>interface ethernet slot/port[-port]</strong>&lt;br&gt;&lt;br&gt;Example:&lt;br&gt;<code>switch(config)# interface ethernet 2/5&lt;br&gt;switch(config-if)#</code></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td><code>switchport</code>&lt;br&gt;&lt;br&gt;Example:&lt;br&gt;<code>switch(config-if)# switchport&lt;br&gt;switch(config-if)#</code></td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td><code>switchport mode trunk</code>&lt;br&gt;&lt;br&gt;Example:&lt;br&gt;<code>switch(config-if)# switchport mode trunk&lt;br&gt;switch(config-if)#</code></td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td>`switchport trunk allowed vlan {{number</td>
</tr>
<tr>
<td><strong>Step 14</strong></td>
<td>(Optional) Repeat Steps 10 and 11 to configure the allowed VLANS on each destination port.</td>
</tr>
<tr>
<td><strong>Step 15</strong></td>
<td><code>show interface ethernet slot/port[-port] trunk</code>&lt;br&gt;&lt;br&gt;Example:&lt;br&gt;<code>switch(config-if)# show interface ethernet 2/5 trunk</code></td>
</tr>
<tr>
<td><strong>Step 16</strong></td>
<td><code>copy running-config startup-config</code>&lt;br&gt;&lt;br&gt;Example:&lt;br&gt;<code>switch(config-if)# copy running-config startup-config</code></td>
</tr>
</tbody>
</table>
Send document comments to nexus7k-docfeedback@cisco.com.

3. remote-span
4. exit
5. show vlan
6. copy running-config startup-config

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>config t</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch# config t</td>
</tr>
<tr>
<td></td>
<td>switch(config)#</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>vlan vlan</code></td>
<td>Enters VLAN configuration mode for the VLAN specified.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config)# vlan 901</td>
</tr>
<tr>
<td></td>
<td>switch(config-vlan)#</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>remote-span</code></td>
<td>Configures the VLAN as an RSPAN VLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config-vlan)# remote-span</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td><code>exit</code></td>
<td>Exits VLAN configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config-vlan)# exit</td>
</tr>
<tr>
<td></td>
<td>switch(config)#</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td><code>show vlan</code></td>
<td>(Optional) Displays the VLAN configuration. Remote SPAN VLANs</td>
</tr>
<tr>
<td></td>
<td>are listed together.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config)# show vlan</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config)# copy running-config</td>
</tr>
<tr>
<td></td>
<td>switch(config)# startup-config</td>
</tr>
</tbody>
</table>

**Shutting Down or Resuming a SPAN Session**

You can shut down SPAN sessions to discontinue the copying of packets from sources to destinations. Because only two SPAN sessions can be running simultaneously, you can shut down one session in order to free hardware resources to enable another session. By default, SPAN sessions are created in the shut state.

You can resume (enable) SPAN sessions to resume the copying of packets from sources to destinations. In order to enable a SPAN session that is already enabled but operationally down, you must first shut it down and then enable it.

You can configure the shut and enabled SPAN session states with either a global or monitor configuration mode command.
BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the `switchto vdc` command).

SUMMARY STEPS

1. `config t`
2. `monitor session {session-range | all} shut`
3. `no monitor session {session-range | all} shut`
4. `monitor session session-number`
5. `shut`
6. `no shut`
7. `show monitor`
8. `copy running-config startup-config`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>config t</code></td>
</tr>
<tr>
<td>Example:</td>
<td><code>switch# config t</code> <code>switch(config)#</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>`monitor session {session-range</td>
</tr>
<tr>
<td>Example:</td>
<td><code>switch(config)# monitor session 3 shut</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>`no monitor session {session-range</td>
</tr>
<tr>
<td>Example:</td>
<td><code>switch(config)# no monitor session 3 shut</code></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If a monitor session is enabled but its operational status is down, then to enable the session, you must first specify the <code>monitor session shut</code> command followed by the <code>no monitor session shut</code> command.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>monitor session session-number</code></td>
</tr>
<tr>
<td>Example:</td>
<td><code>switch(config)# monitor session 3</code> <code>switch(config-monitor)#</code></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>shut</code></td>
</tr>
<tr>
<td>Example:</td>
<td><code>switch(config-monitor)# shut</code></td>
</tr>
</tbody>
</table>
Verifying the SPAN Configuration

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show monitor session {all</td>
<td>session-number</td>
</tr>
</tbody>
</table>

For detailed information about the fields in the output from these commands, see the *Cisco NX-OS System Management Command Reference*.

SPAN Example Configurations

This section includes the following topics:

- SPAN Session Example Configuration, page 14-15
- Virtual SPAN Session Example Configuration, page 14-16
- Private VLAN Source in SPAN Session Example Configuration, page 14-16

SPAN Session Example Configuration

To configure a SPAN session, follow these steps:

Step 1 Configure destination ports in access or trunk mode, and enable SPAN monitoring.
```
switch# config t
switch(config)# interface ethernet 2/5
switch(config-if)# switchport
switch(config-if)# switchport mode trunk
switch(config-if)# switchport monitor
switch(config-if)# no shut
switch(config-if)# exit
```
Step 2 Configure a SPAN session.

switch(config)# no monitor session 3
switch(config)# monitor session 3
switch(config-monitor)# source interface ethernet 2/1-3, ethernet 3/1 rx
switch(config-monitor)# source interface port-channel 2
switch(config-monitor)# source interface sup-eth 0 both
switch(config-monitor)# source vlan 3, 6-8 tx
switch(config-monitor)# filter vlan 3-5, 7
switch(config-monitor)# destination interface ethernet 2/5
switch(config-monitor)# no shut
switch(config-monitor)# exit
switch(config)# show monitor session 3
switch(config)# copy running-config startup-config

Virtual SPAN Session Example Configuration

To configure a virtual SPAN session, follow these steps:

Step 1 Configure destination ports in access or trunk mode, and enable SPAN monitoring.

switch# config t
switch(config)# interface ethernet 3/1
switch(config-if)# switchport
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan add 100-200
switch(config-if)# switchport monitor
switch(config-if)# no shut
switch(config-if)# exit
switch(config)# interface ethernet 3/2
switch(config-if)# switchport
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan add 201-300
switch(config-if)# switchport monitor
switch(config-if)# no shut
switch(config-if)# exit
switch(config)#

Step 2 Configure a SPAN session.

switch(config)# no monitor session 3
switch(config)# monitor session 3
switch(config-monitor)# source vlan 100-300
switch(config-monitor)# destination interface ethernet 3/1-2
switch(config-monitor)# no shut
switch(config-monitor)# exit
switch(config)# show monitor session 3
switch(config)# copy running-config startup-config

Private VLAN Source in SPAN Session Example Configuration

To configure a SPAN session that includes a private VLAN source, follow these steps:
Step 1  Configure source VLANs.

```
switch# config t
switch(config)# vlan 100
switch(config-vlan)# private-vlan primary
switch(config-vlan)# exit
switch(config)# interface ethernet 3/1
switch(config-if)# switchport
switch(config-if)# switchport access vlan 100
switch(config-if)# no shut
switch(config-if)# exit
switch(config)# interface ethernet 3/2
switch(config-if)# switchport
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk native vlan 100
switch(config-if)# no shut
switch(config-if)# exit
switch(config)#
```

Step 2  Configure destination ports in access or trunk mode, and enable SPAN monitoring.

```
switch# config t
switch(config)# interface ethernet 3/3
switch(config-if)# switchport
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan add 100-200
switch(config-if)# switchport monitor
switch(config-if)# no shut
switch(config-if)# exit
switch(config)#
```

Step 3  Configure a SPAN session.

```
switch(config)# no monitor session 3
switch(config)# monitor session 3
switch(config-monitor)# source vlan 100
switch(config-monitor)# destination interface ethernet 3/3
switch(config-monitor)# no shut
switch(config-monitor)# exit
switch(config)# show monitor session 3
switch(config)# copy running-config startup-config
```

Additional References

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

- Related Documents, page 14-18
- Standards, page 14-18
Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>VDCs</td>
<td>Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.x</td>
</tr>
<tr>
<td>SPAN commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples</td>
<td>Cisco Nexus 7000 Series NX-OS System Management Command Reference</td>
</tr>
</tbody>
</table>

Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>—</td>
</tr>
</tbody>
</table>

Feature History for SPAN

Table 14-2 lists the release history for this feature.

Table 14-2 Feature History for SPAN

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guidelines and Limitations</td>
<td>4.1(3)</td>
<td>Added a table of SPAN session limits. See the “Table 1SPAN Session Limits” section on page 14-5.</td>
</tr>
</tbody>
</table>
Configuring Onboard Failure Logging

This chapter describes how to configure the onboard failure logging (OBFL) features on Cisco NX-OS devices.

This chapter includes the following sections:
- Information About OBFL, page 15-1
- Licensing Requirements for OBFL, page 15-2
- Prerequisites for OBFL, page 15-2
- Guidelines and Limitations, page 15-2
- Configuring OBFL, page 15-3
- Verifying the OBFL Configuration, page 15-6
- OBFL Example Configuration, page 15-7
- Default Settings, page 15-7
- Additional References, page 15-7

Information About OBFL

This section includes the following topics:
- OBFL Overview, page 15-1
- Virtualization Support, page 15-2

OBFL Overview

Cisco NX-OS provides the ability to log failure data to persistent storage, which you can retrieve and display for analysis at a later time. This onboard failure logging (OBFL) feature stores failure and environmental information in nonvolatile memory on the module. The information will help analyze failed modules.

The data stored by OBFL include the following:
- Time of initial power-on
- Slot number of the module in the chassis
- Initial temperature of the module
Licensing Requirements for OBFL

The following table shows the licensing requirements for this feature:

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

Prerequisites for OBFL

If you configure VDCs, install the Advanced Services license and enter the desired VDC (see the Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.x). You must have network-admin user privileges and be logged into the default VDC.

Guidelines and Limitations

OBFL has the following guidelines and limitations:

- OBFL is enabled by default.
- OBFL flash supports a limited number of writes and erases. The more logging you enable, the faster you use up this number of writes and erases.
**Configuring OBFL**

You can configure the OBFL features on Cisco NX-OS devices.

**BEFORE YOU BEGIN**

Make sure you are in global configuration mode.

**SUMMARY STEPS**

1. `hw-module logging onboard`
2. `hw-module logging onboard environmental-history`
3. `hw-module logging onboard error-stats`
4. `hw-module logging onboard interrupt-stats`
5. `hw-module logging onboard module slot`
6. `hw-module logging onboard module obfl-log`
7. `show logging onboard`
8. `copy running-config startup-config`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>config t</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch# config t</td>
</tr>
<tr>
<td></td>
<td>switch(config)#</td>
</tr>
<tr>
<td><strong>Step 1</strong></td>
<td>hw-module logging onboard</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config)# hw-module logging onboard</td>
</tr>
<tr>
<td></td>
<td>Module: 7 Enabling ... was successful.</td>
</tr>
<tr>
<td></td>
<td>Module: 10 Enabling ... was successful.</td>
</tr>
<tr>
<td></td>
<td>Module: 12 Enabling ... was successful.</td>
</tr>
</tbody>
</table>
### Chapter 15      Configuring Onboard Failure Logging

#### Command Purpose

<table>
<thead>
<tr>
<th>Step 2</th>
<th>hw-module logging onboard environmental-history</th>
<th>Enables the OBFL environmental history.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>switch(config)# hw-module logging onboard environmental-history</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Module: 7  Enabling environmental-history ... was successful.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Module: 10  Enabling environmental-history ... was successful.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Module: 12  Enabling environmental-history ... was successful.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>hw-module logging onboard error-stats</th>
<th>Enables the OBFL error statistics.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>switch(config)# hw-module logging onboard error-stats</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Module: 7  Enabling error-stats ... was successful.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Module: 10  Enabling error-stats ... was successful.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Module: 12  Enabling error-stats ... was successful.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>hw-module logging onboard interrupt-stats</th>
<th>Enables the OBFL interrupt statistics.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>switch(config)# hw-module logging onboard interrupt-stats</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Module: 7  Enabling interrupt-stats ... was successful.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Module: 10  Enabling interrupt-stats ... was successful.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Module: 12  Enabling interrupt-stats ... was successful.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>hw-module logging onboard module slot</th>
<th>Enables the OBFL information for a module.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>switch(config)# hw-module logging onboard module 7</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Module: 7  Enabling ... was successful.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>hw-module logging onboard obfl-log</th>
<th>Enables the boot uptime, device version, and OBFL history.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>switch(config)# hw-module logging onboard obfl-log</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Module: 7  Enabling obfl-log ... was successful.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Module: 10  Enabling obfl-log ... was successful.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Module: 12  Enabling obfl-log ... was successful.</td>
<td></td>
</tr>
</tbody>
</table>
## Chapter 15 Configuring Onboard Failure Logging

### Configuring OBFL

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>show logging onboard</code></td>
<td>(Optional) Displays information about OBFL.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)# show logging onboard</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>-------------------------------</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>OBFL Status</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>-----------------------------</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Switch OBFL Log:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Enabled</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Module: 7 OBFL Log: Enabled</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>cpu-hog Enabled</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>environmental-history Enabled</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>error-stats Enabled</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>exception-log</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Fri Mar 21 19:07:33 2008 (957597 us)</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Module 2 SecondaryBootROM test has failed 20 times with error BIOS file checksum</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Library could not be opened</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>*** /lc/isan/lib/libcrdcfg.so: undefined symbol: get_slot_id ***</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>plog_show_data_type: Error opening library statcl, func_name statcl_disp_func</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Saves this configuration change.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)# copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>
Verifying the OBFL Configuration

Use the `show logging onboard status` command to display the configuration status of OBFL.

```
switch# show logging onboard status
----------------------------
OBFL Status
----------------------------
Switch OBFL Log:                                    Enabled
Module:  2 OBFL Log:                                Enabled
cpu-hog                                          Enabled
environmental-history                             Enabled
error-stats                                      Enabled
exception-log                                   Enabled
interrupt-stats                                  Enabled
mem-leak                                         Enabled
miscellaneous-error                             Enabled
obf1-log (boot-uptime/device-version/obf1-history) Enabled
register-log                                     Enabled
stack-trace                                      Enabled
system-health                                    Enabled
Module:  6 OBFL Log:                                Enabled
cpu-hog                                          Enabled
environmental-history                             Enabled
error-stats                                      Enabled
exception-log                                   Enabled
interrupt-stats                                  Enabled
mem-leak                                         Enabled
miscellaneous-error                             Enabled
obf1-log (boot-uptime/device-version/obf1-history) Enabled
register-log                                     Enabled
stack-trace                                      Enabled
system-health                                    Enabled
temp Error                                       Enabled
```

Use the following commands to display OBFL information stored in flash on a module:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show logging onboard boot-uptime</code></td>
<td>Displays the boot and uptime information.</td>
</tr>
<tr>
<td><code>show logging onboard counter-stats</code></td>
<td>Displays statistics on all ASIC counters.</td>
</tr>
<tr>
<td><code>show logging onboard device-version</code></td>
<td>Displays device version information.</td>
</tr>
<tr>
<td><code>show logging onboard endtime</code></td>
<td>Displays OBFL logs to a specified end time.</td>
</tr>
<tr>
<td><code>show logging onboard environmental-history</code></td>
<td>Displays environmental history.</td>
</tr>
<tr>
<td><code>show logging onboard error-stats</code></td>
<td>Displays error statistics.</td>
</tr>
<tr>
<td><code>show logging onboard exception-log</code></td>
<td>Displays exception log information.</td>
</tr>
<tr>
<td><code>show logging onboard interrupt-stats</code></td>
<td>Displays interrupt statistics.</td>
</tr>
<tr>
<td><code>show logging onboard kernel-trace</code></td>
<td>Displays kernel trace information.</td>
</tr>
<tr>
<td><code>show logging onboard module slot</code></td>
<td>Displays OBFL information for a specific module.</td>
</tr>
<tr>
<td><code>show logging onboard obf1-history</code></td>
<td>Displays history information.</td>
</tr>
<tr>
<td><code>show logging onboard obf1-logs</code></td>
<td>Displays log information.</td>
</tr>
</tbody>
</table>
OBFL Example Configuration

This example shows how to enable OBFL on module 2 for environmental information:

```
conf t
hw-module logging onboard module 2 environmental-history
```

Default Settings

Table 15-1 lists the default settings for OBFL parameters.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>OBFL</td>
<td>All features enabled</td>
</tr>
</tbody>
</table>

Additional References

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

- Related Documents, page 15-8
- Standards, page 15-8
Chapter 15 Configuring Onboard Failure Logging

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>OBFL CLI commands</td>
<td>Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.x</td>
</tr>
<tr>
<td>configuration files</td>
<td>Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 4.x</td>
</tr>
<tr>
<td>VDCs</td>
<td>Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.x</td>
</tr>
</tbody>
</table>

Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>—</td>
</tr>
</tbody>
</table>
Configuring NetFlow

This chapter describes how to configure the NetFlow feature on Cisco NX-OS devices. This chapter includes the following sections:

- Information About NetFlow, page 16-1
- Licensing Requirements for NetFlow, page 16-4
- Prerequisites for NetFlow, page 16-4
- Guidelines and Limitations, page 16-4
- Configuring NetFlow, page 16-5
- Verifying NetFlow Configuration, page 16-18
- Monitoring NetFlow, page 16-18
- NetFlow Example Configuration, page 16-19
- Default Settings, page 16-19
- Additional References, page 16-19
- Feature History for NetFlow, page 16-20

Information About NetFlow

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

This section includes the following topics:

- NetFlow Overview, page 16-1
- High Availability, page 16-3
- Virtualization Support, page 16-4

NetFlow Overview

NetFlow uses flows to provide statistics for accounting, network monitoring, and network planning. A flow is a unidirectional stream of packets that arrives on a source interface (or VLAN) and has the same values for the keys. A key is an identified value for a field within the packet. You create a flow using a flow record to define the unique keys for your flow.
Information About NetFlow

Cisco NX-OS supports the Flexible NetFlow feature that enables enhanced network anomalies and security detection. Flexible NetFlow allows you to define an optimal flow record for a particular application by selecting the keys from a large collection of predefined fields. For more information on the flow records, see the “Flow Records” section on page 16-2.

All key values must match for the packet to count in a given flow. A flow might gather other fields of interest, depending on the export record version that you configure. Flows are stored in the NetFlow cache.

You can export the data that NetFlow gathers for your flow by using an exporter and export this data to a remote NetFlow collector. Cisco NX-OS exports a flow as part of a NetFlow export User Datagram Protocol (UDP) datagram under the following circumstances:

- The flow has been inactive or active for too long.
- The flow cache is getting full.
- One of the counters (packets or bytes) has exceeded its maximum value.
- You have forced the flow to export.

For more information on exporters, see the “Exporters” section on page 16-2.

You define the size of the data that you want to collect for a flow using a monitor. The monitor combines the flow record and exporter with the NetFlow cache information. For more information on monitors, see the “Monitors” section on page 16-3.

Cisco NX-OS can gather NetFlow statistics in either full or sampled mode. Cisco NX-OS analyzes all packets on the interface or subinterface for full NetFlow mode. For sampled mode, you configure the sampling algorithm and rate that Cisco NX-OS analyzes packets. For more information on samplers, see the “Samplers” section on page 16-3.

Flow Records

A flow record defines the keys that NetFlow uses to identify packets in the flow as well as other fields of interest that NetFlow gathers for the flow. You can define a flow record with any combination of keys and fields of interest. Cisco NX-OS supports a rich set of keys. A flow record also defines the types of counters gathered per flow. You can configure 32-bit or 64-bit packet or byte counters. Cisco NX-OS enables the following match fields as the defaults when you create a flow record:

- match interface input
- match interface output
- match flow direction

For more information, see the “Creating a Flow Record” section on page 16-6.

Exporters

An exporter contains network layer and transport layer details for the NetFlow export packet. You can configure the following information in an exporter:

- Export destination IP address
- Source interface
- UDP port number (where the collector is listening for NetFlow packets)
- Export format
Information About NetFlow

**Note**
NetFlow export packets use the IP address that is assigned to the source interface. If the source interface does not have an IP address assigned to it, the exporter will be inactive.

Cisco NX-OS exports data to the collector whenever a timeout occurs or when the flow is terminated (TCP Fin or Rst received, for example). You can configure the following timers to force a flow export:

- Active timeout—Cisco NX-OS does not remove the cache entries from the cache.
- Inactive timeout—Cisco NX-OS removes the cache entries from the cache.

**Export Formats**

Cisco NX-OS supports the Version 5 and Version 9 export formats. We recommend that you use the Version 9 export format for the following reasons:

- Variable field specification format
- Support for IPv6, Layer 2, and MPLS fields
- More efficient network utilization

If you configure the Version 5 export format, you have these limitations:

- Fixed field specifications
- No support for IPv6, Layer 2, or MPLS fields
- The Netflow.InputInterface and Netflow.OutputInterface represent a 16-bit I/O descriptor (IOD) of the interface.

**Note**
The IOD information of the interface can be retrieved using the `show system internal info global` command.

For information about the Version 9 export format, see RFC 3954.

**Note**
Cisco NX-OS supports UDP as the transport protocol for exports to up to two collectors.

**Monitors**

A monitor references the flow record and flow exporter. You apply a monitor to an interface.

**Samplers**

If you are using sampled mode, you use the sampler to specify the rate at which packets are sampled. On high bandwidth interfaces, applying NetFlow processing to every single packet can result in high CPU utilization. Sampler configuration is for high-speed interfaces. You can configure samples for M out of N. For example, 100 out of every 10,000 packets are sampled.
High Availability

Cisco NX-OS supports stateful restarts for NetFlow. After a reboot or supervisor switchover, Cisco NX-OS applies the running configuration.

Virtualization Support

A virtual device context (VDC) is a logical representation of a set of system resources. Within each VDC, you can configure NetFlow. By default, Cisco NX-OS places you in the default VDC and any flows that you define in this mode are only available for interfaces in the default VDC.

For information about configuring VDCs, see the Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.x.

Licensing Requirements for NetFlow

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

Prerequisites for NetFlow

NetFlow has the following prerequisite:

- You must understand the resources required on your device because NetFlow consumes additional memory and CPU resources.

If you configure VDCs, install the Advanced Services license and enter the desired VDC. For more information, see the Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.x.

Guidelines and Limitations

NetFlow has the following configuration guidelines and limitations:

- You must configure a source interface. If you do not configure a source interface, the exporter will remain in a disabled state.
- You must configure a valid record name for every flow monitor.
- A rollback will fail if you try to modify a record that is programmed in the hardware during a rollback.
- Only Layer 2 NetFlow is applied on Layer 2 interfaces, and only Layer 3 NetFlow is applied on Layer 3 interfaces.
- If you add a member to a port channel that is already configured for Layer 2 NetFlow, its NetFlow configuration is removed and the Layer 2 configuration of the port channel is added to it.
If you change a Layer 2 interface to a Layer 3 interface, the software removes the Layer 2 NetFlow configuration from the interface.

Use v9 export to see the full 32-bit SNMP ifIndex values at the NetFlow connector.

**Configuring NetFlow**

To configure NetFlow, follow these steps:

1. **Step 1** Enable the NetFlow feature (see the “Enabling the NetFlow Feature” section on page 16-5).
2. **Step 2** Define a flow record by specifying keys and fields to the flow (see the “Creating a Flow Record” section on page 16-6).
3. **Step 3** Define an optional flow exporter by specifying the export format, protocol, destination, and other parameters (see the “Creating a Flow Exporter” section on page 16-9).
4. **Step 4** Define a flow monitor based on the flow record and flow exporter (see the “Creating a Flow Monitor” section on page 16-11).
5. **Step 5** Apply the flow monitor to a source interface, subinterface, VLAN interface (see the “Applying a Flow to an Interface” section on page 16-13), or a VLAN (see the “Configuring Bridged NetFlow on a VLAN” section on page 16-14).

This section includes the following topics:

- Enabling the NetFlow Feature, page 16-5
- Creating a Flow Record, page 16-6
- Creating a Flow Exporter, page 16-9
- Creating a Flow Monitor, page 16-11
- Creating a Sampler, page 16-12
- Applying a Flow to an Interface, page 16-13
- Configuring Bridged NetFlow on a VLAN, page 16-14
- Configuring Layer 2 NetFlow, page 16-15
- Configuring NetFlow Timeouts, page 16-17

**Note**

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

**Enabling the NetFlow Feature**

You must globally enable NetFlow before you can configure any flows.
Use the following command in global configuration mode to enable NetFlow:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>feature netflow</td>
<td>Enables the NetFlow feature.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td>feature netflow</td>
<td></td>
</tr>
</tbody>
</table>

Use the following command in global configuration mode to disable NetFlow and remove all flows:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>no feature netflow</td>
<td>Disables the NetFlow feature. The default is</td>
</tr>
<tr>
<td></td>
<td>disabled.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td>no feature netflow</td>
<td></td>
</tr>
</tbody>
</table>

### Creating a Flow Record

You can create a flow record and add keys to match on and fields to collect in the flow.

**BEFORE YOU BEGIN**

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

**SUMMARY STEPS**

1. `config t`
2. `flow record name`
3. `description string`
4. `match type`
5. `collect type`
6. `show flow record [name] [record-name] netflow-original netflow protocol-port netflow {ipv4 | ipv6} {original-input | original-output}`
7. `copy running-config startup-config`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Places you in global configuration mode.</td>
</tr>
<tr>
<td>config t</td>
<td></td>
</tr>
</tbody>
</table>

**Example:**

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)#
```
## Configuring NetFlow

### Specifying the Match Parameters

You must configure at least one of the following match parameters for flow records:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`match ip {protocol</td>
<td>tos}`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>switch(config-flow-record)# match ip protocol</code></td>
<td></td>
</tr>
<tr>
<td>`match ipv4 {destination address</td>
<td>source address}`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>switch(config-flow-record)# match ipv4 destination address</code></td>
<td></td>
</tr>
</tbody>
</table>

---

**Send document comments to nexus7k-docfeedback@cisco.com.**
## Specifying the Collect Parameters

You must configure at least one of the following collect parameters for flow records:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>match ipv6</strong> *(destination address</td>
<td>source address</td>
</tr>
<tr>
<td><strong>Example:</strong> switch(config-flow-record)# match ipv6 flow-label</td>
<td></td>
</tr>
<tr>
<td><strong>match transport</strong> *(destination-port</td>
<td>source-port)*</td>
</tr>
<tr>
<td><strong>Example:</strong> switch(config-flow-record)# match transport destination-port</td>
<td></td>
</tr>
<tr>
<td><strong>match datalink</strong> *(mac source-address</td>
<td>mac destination-address</td>
</tr>
<tr>
<td><strong>Example:</strong> switch(config-flow-record)# match datalink ethertype</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>collect counter</strong> *(bytes</td>
<td>packets)* <em>(long)</em></td>
</tr>
<tr>
<td><strong>Example:</strong> switch(config-flow-record)# collect counter packets</td>
<td></td>
</tr>
<tr>
<td><strong>collect flow</strong> *(direction</td>
<td>sampler id)*</td>
</tr>
<tr>
<td><strong>Example:</strong> switch(config-flow-record)# collect flow direction</td>
<td></td>
</tr>
<tr>
<td><strong>collect routing</strong> *(destination</td>
<td>source)* *(as</td>
</tr>
<tr>
<td><strong>Example:</strong> switch(config-flow-record)# collect routing destination as</td>
<td></td>
</tr>
<tr>
<td><strong>collect routing forwarding-status</strong></td>
<td>Collects the forwarding status of the packet.</td>
</tr>
<tr>
<td><strong>Example:</strong> switch(config-flow-record)# collect routing forwarding-status</td>
<td></td>
</tr>
<tr>
<td><strong>collect routing next-hop address ipv4</strong> <em>(bgp)</em></td>
<td>Collects the next-hop IPv4 address.</td>
</tr>
<tr>
<td><strong>Example:</strong> switch(config-flow-record)# collect routing next-hop address ipv4</td>
<td></td>
</tr>
</tbody>
</table>
Creating a Flow Exporter

You can create a flow export to define the export parameters for a flow.

BEFORE YOU BEGIN

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

SUMMARY STEPS

1. `config t`
2. `flow exporter name`
3. `destination {ipv4-address | ipv6-address} [use-vrf name]`
4. `source interface-type number`
5. `version {5 | 9}`
6. `show flow exporter [name]`
7. `copy running-config startup-config`

---

### Command Purpose

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>collect routing next-hop address ipv6</code>&lt;br&gt;<code>[bgp]</code></td>
<td>Collects the next-hop IPv6 address.</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;<code>switch(config-flow-record)# collect routing next-hop address ipv6</code></td>
<td></td>
</tr>
<tr>
<td>`collect timestamp sys-uptime {first</td>
<td>last}`</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;<code>switch(config-flow-record)# collect timestamp sys-uptime last</code></td>
<td></td>
</tr>
<tr>
<td><code>collect transport tcp flags</code></td>
<td>Collects the TCP transport layer flags for the packets in the flow.</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;<code>switch(config-flow-record)# collect transport tcp flags</code></td>
<td></td>
</tr>
<tr>
<td><code>collect routing next-hop address ipv6</code>&lt;br&gt;<code>[bgp]</code></td>
<td>Collects the next-hop IPv6 address.</td>
</tr>
<tr>
<td>`collect timestamp sys-uptime {first</td>
<td>last}`</td>
</tr>
<tr>
<td><code>collect transport tcp flags</code></td>
<td>Collects the TCP transport layer flags for the packets in the flow.</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;<code>switch(config-flow-record)# collect transport tcp flags</code></td>
<td></td>
</tr>
</tbody>
</table>
# Configuring NetFlow

## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>config t</td>
</tr>
<tr>
<td>Example: switch# config t Enter configuration commands, one per line. End with CNTL/Z. switch(config)#</td>
<td>Places you in global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>flow exporter name</td>
</tr>
<tr>
<td>Example: switch(config)# flow exporter ExportTest switch(config-flow-exporter)#</td>
<td>Creates a flow exporter and enters flow exporter configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>destination {ipv4-address</td>
</tr>
<tr>
<td>Example: switch(config-flow-exporter)# destination 192.0.2.1</td>
<td>Sets the destination IPv4 or IPv6 address for this exporter. You can optionally configure the VRF to use to reach the NetFlow collector.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>source interface-type number</td>
</tr>
<tr>
<td>Example: switch(config-flow-exporter)# source ethernet 2/1</td>
<td>Specifies the interface to use to reach the NetFlow collector at the configured destination.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>version {5</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>show flow exporter [name]</td>
</tr>
<tr>
<td>Example: switch(config-flow-exporter)# show flow exporter</td>
<td>(Optional) Displays information about NetFlow flow exporters.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>copy running-config startup-config</td>
</tr>
<tr>
<td>Example: switch(config-flow-exporter)# copy running-config startup-config</td>
<td>(Optional) Saves this configuration change.</td>
</tr>
</tbody>
</table>

You can optionally configure the following parameters for flow exporters:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>description string</td>
<td>Describes this flow exporter as a maximum 63-character string.</td>
</tr>
<tr>
<td>Example: switch(config-flow-exporter)# description ExportV9</td>
<td></td>
</tr>
</tbody>
</table>
You can optionally configure the following parameters in flow exporter version configuration submode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>dscp value</td>
<td>Specifies the differentiated services codepoint value. The range is from 0 to 63.</td>
</tr>
<tr>
<td>transport udp number</td>
<td>Specifies the UDP port to use to reach the NetFlow collector. The range is from 0 to 65535.</td>
</tr>
</tbody>
</table>

Example:

```
switch(config-flow-exporter)# dscp 0
```

```
switch(config-flow-exporter)# transport udp 200
```

You can optionally configure the following parameters in flow exporter version configuration submode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>option {exporter-stats</td>
<td>interface-table</td>
</tr>
<tr>
<td>template data timeout seconds</td>
<td>Sets the template data resend timer. The range is from 1 to 86400 seconds.</td>
</tr>
</tbody>
</table>

Example:

```
switch(config-flow-exporter-version-9)# option exporter-stats timeout 1200
```

```
switch(config-flow-exporter-version-9)# template data timeout 1200
```

Creating a Flow Monitor

You can create a flow monitor and associate it with a flow record and a flow exporter.

**BEFORE YOU BEGIN**

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

**SUMMARY STEPS**

1. config t
2. flow monitor name
3. description string
4. exporter name
5. record {name | netflow-original | netflow protocol-port | netflow {ipv4 | ipv6} {original-input | original-output}}
6. show flow monitor [name]
7. copy running-config startup-config
## Configuring NetFlow

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>config t</strong>&lt;br&gt;<strong>Example:</strong> switch# config t&lt;br&gt;Enter configuration commands, one per line. End with CNTL/Z.&lt;br&gt;switch(config)#</td>
</tr>
<tr>
<td>Step 2</td>
<td><strong>flow monitor name</strong>&lt;br&gt;<strong>Example:</strong> switch(config)# flow monitor MonitorTest&lt;br&gt;switch(config-flow-monitor)#</td>
</tr>
<tr>
<td>Step 3</td>
<td><strong>description string</strong>&lt;br&gt;<strong>(Optional) Describes the flow monitor with an alphanumeric string up to 63 characters.</strong>&lt;br&gt;<strong>Example:</strong> switch(config-flow-monitor)# description Ipv4Monitor</td>
</tr>
<tr>
<td>Step 4</td>
<td><strong>exporter name</strong>&lt;br&gt;<strong>Example:</strong> switch(config-flow-monitor)# exporter Exportv9</td>
</tr>
<tr>
<td>Step 5</td>
<td>**record {name</td>
</tr>
<tr>
<td>Step 6</td>
<td><strong>show flow monitor [name]</strong>&lt;br&gt;<strong>(Optional) Displays information about NetFlow flow monitors.</strong>&lt;br&gt;<strong>Example:</strong> switch(config-flow-monitor)# show flow monitor</td>
</tr>
<tr>
<td>Step 7</td>
<td><strong>copy running-config startup-config</strong>&lt;br&gt;<strong>(Optional) Saves this configuration change.</strong>&lt;br&gt;<strong>Example:</strong> switch(config-flow-monitor)# copy running-config startup-config</td>
</tr>
</tbody>
</table>

### Creating a Sampler

You can create a sampler to define the NetFlow sampling rate for a flow.

### BEFORE YOU BEGIN

Make sure that you are in the correct VDC. To change the VDC, use the switchto vdc command.
Send document comments to nexus7k-docfeedback@cisco.com.

SUMMARY STEPS

1. `config t`
2. `sampler name`
3. `description string`
4. `mode samples out-of packets`
5. `show sampler [name]`
6. `copy running-config startup-config`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>config t</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enter configuration commands, one per line. End with CNTL/Z.</td>
</tr>
<tr>
<td></td>
<td>switch(config)#</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>sampler name</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config-flow-sampler)#</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>description string</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>mode samples out-of packets</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>show sampler [name]</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>copy running-config startup-config</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>

Applying a Flow to an Interface

You can apply a flow monitor and an optional sampler to an interface.

BEFORE YOU BEGIN

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

SUMMARY STEPS

1. `config t`
2. `interface interface-type number`
3. `ip flow monitor name {input | output} [sampler name]`
4. `ipv6 flow monitor name {input | output} [sampler name]`
5. `show flow interface [interface-type number]`
6. `copy running-config startup-config`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>config t</code></td>
<td>Places you in global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch# config t</td>
</tr>
<tr>
<td>Enter configuration commands, one per line. End with CNTL/Z. switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>interface interface-type number</code></td>
<td>Enters interface configuration mode. The interface type can be Ethernet (including subinterfaces), port channel, VLAN, SVI, or tunnel.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# interface ethernet 2/1</td>
</tr>
<tr>
<td>switch(config-if)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> `ip flow monitor name {input</td>
<td>output} [sampler name]`</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config-if)# ip flow monitor MonitorTest input</td>
</tr>
<tr>
<td><strong>Step 4</strong> `ipv6 flow monitor name {input</td>
<td>output} [sampler name]`</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config-if)# ipv6 flow monitor MonitorTest input</td>
</tr>
<tr>
<td><strong>Step 5</strong> <code>show flow interface [interface-type number]</code></td>
<td>(Optional) Displays information about NetFlow on an interface.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config-if)# show flow interface</td>
</tr>
<tr>
<td><strong>Step 6</strong> <code>copy running-config startup-config</code></td>
<td>(Optional) Saves this configuration change.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config-if)# copy running-config startup-config</td>
</tr>
</tbody>
</table>

Configuring Bridged NetFlow on a VLAN

You can apply a flow monitor and an optional sampler to a VLAN.
### Chapter 16 Configuring NetFlow

#### BEFORE YOU BEGIN

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

#### SUMMARY STEPS

1. `config t`
2. `vlan vlan-id`
3. `ip flow monitor name {input | output} [sampler name]`
4. `copy running-config startup-config`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> config t</td>
<td>Places you in global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch# config t</td>
<td>Enter configuration commands, one per line. End with CNTL/Z.</td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> vlan vlan-id</td>
<td>Enters VLAN configuration mode. The <code>vlan-id</code> range is from 1 to 3967 or from 4048 to 4093.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config)# vlan 30</td>
<td></td>
</tr>
<tr>
<td>switch(config-vlan)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ip flow monitor name (input</td>
<td>output) [sampler name]</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config-vlan)# ip flow monitor MonitorTest input</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> copy running-config startup-config</td>
<td>(Optional) Saves this configuration change.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config-vlan)# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring Layer 2 NetFlow

You can define Layer 2 keys in flexible NetFlow records that you can use to capture flows in Layer 2 interfaces. The Layer 2 keys are as follows:

- Source and destination MAC addresses
- Source VLAN ID
- EtherType from the Ethernet frame

You can apply Layer 2 NetFlow to the following interfaces for the ingress direction:

- Switch ports in access mode
- Switch ports in trunk mode
- Layer 2 port channels
You cannot apply Layer 2 NetFlow to VLANs, egress interfaces, or Layer 3 interfaces such as VLAN interfaces.

Before you begin

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

Summary steps

1. `config t`
2. `flow record name`
3. `match datalink {mac source-address | mac destination-address | ethertype | vlan}`
4. `interface {ethernet slot/port} | {port-channel number}`
5. `switchport`
6. `mac packet-classify`
7. `layer2-switched flow monitor flow-name input [sampler sampler-name]`
8. `show flow record netflow layer2-switched input`
9. `copy running-config startup-config`

Detailed steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>config t</code></td>
<td>Places you in global configuration mode.</td>
</tr>
<tr>
<td>Example:&lt;br&gt;switch# config t&lt;br&gt;Enter configuration commands, one per line. End with CNTL/Z.&lt;br&gt;switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>flow record name</code></td>
<td>Enters flow record configuration mode. For more information about configuring flow records, see the “Creating a Flow Record” section on page 16-6.</td>
</tr>
<tr>
<td>Example:&lt;br&gt;switch(config)# flow record L2_record</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> `match datalink {mac source-address</td>
<td>mac destination-address</td>
</tr>
<tr>
<td>Example:&lt;br&gt;switch(config-flow-record)# match datalink ethertype</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> `interface {ethernet slot/port}</td>
<td>{port-channel number}`</td>
</tr>
<tr>
<td>Example 1:&lt;br&gt;switch(config)# interface ethernet 2/1&lt;br&gt;switch(config-if)#</td>
<td></td>
</tr>
<tr>
<td>Example 2:&lt;br&gt;switch(config)# interface port-channel 8&lt;br&gt;switch(config-if)#</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 16 Configuring NetFlow

Configuring NetFlow

You can optionally configure global NetFlow timeouts that apply to all flows.

Use the following commands in global configuration mode to configure NetFlow timeout parameters:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>flow timeout active seconds</strong></td>
<td>Sets the active timeout value in seconds. The range is from 60 to 4092. The default is 1800.</td>
</tr>
<tr>
<td>Example: switch(config)# flow timeout active 90</td>
<td></td>
</tr>
<tr>
<td><strong>flow timeout aggressive threshold percent</strong></td>
<td>Enables using a percentage that you want the NetFlow table to be before aggressive aging starts. The range is from 50 to 99. The default is disabled.</td>
</tr>
<tr>
<td>Example: switch(config)# flow timeout aggressive threshold 90</td>
<td></td>
</tr>
<tr>
<td><strong>flow timeout fast seconds threshold packets</strong></td>
<td>Enables using a fast timeout value and the number of packets in a flow before aging begins. The fast timeout range in seconds is from 32 to 512. The packet range is from 1 to 4000. The default is disabled.</td>
</tr>
<tr>
<td>Example: switch(config)# flow timeout fast 40 threshold 1200</td>
<td></td>
</tr>
</tbody>
</table>
Verifying NetFlow Configuration

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show flow exporter [name]</td>
<td>Displays information about NetFlow flow exporters and statistics.</td>
</tr>
<tr>
<td>show flow interface [interface-type number]</td>
<td>Displays information about NetFlow interfaces.</td>
</tr>
<tr>
<td>show flow monitor [name] [cache [detailed]]</td>
<td>Displays information about NetFlow flow monitors and statistics.</td>
</tr>
<tr>
<td>show flow record [name]</td>
<td>Displays information about NetFlow flow records.</td>
</tr>
<tr>
<td>show flow record netflow layer2-switched input</td>
<td>Displays information about the Layer 2 NetFlow configuration.</td>
</tr>
<tr>
<td>show flow timeout</td>
<td>Displays information about NetFlow timeouts.</td>
</tr>
<tr>
<td>show hardware flow aging [vdc vdc_id] [detail] [module module]</td>
<td>Displays information about NetFlow aging flows in the hardware.</td>
</tr>
<tr>
<td>show hardware flow entry address table-address type {ip</td>
<td>ipv6} [module module]</td>
</tr>
<tr>
<td>show hardware flow ip [interface type number - monitor monitor_name</td>
<td>profile profile-id</td>
</tr>
<tr>
<td>show hardware flow sampler [all</td>
<td>count</td>
</tr>
<tr>
<td>show hardware flow utilization [module module]</td>
<td>Displays information about NetFlow table utilization in the hardware.</td>
</tr>
<tr>
<td>show sampler [name]</td>
<td>Displays information about NetFlow samplers.</td>
</tr>
</tbody>
</table>

Monitoring NetFlow

Use the show flow exporter command to display NetFlow statistics.
NetFlow Example Configuration

This example shows how to create a flow and apply it to an interface:

```
feature netflow
flow exporter ee
version 9
flow record rr
    match ipv4 source address
    match ipv4 destination address
    collect counter bytes
    collect counter packets
flow monitor foo
    record rr
    exporter ee
interface Ethernet2/45
    ip flow monitor foo output
    ip address 10.20.1.1/24
    no shutdown
```

Default Settings

Table 16-1 lists the default settings for NetFlow parameters.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Egress and Ingress cache size</td>
<td>512K</td>
</tr>
<tr>
<td>Flow active timeout</td>
<td>1800 seconds</td>
</tr>
<tr>
<td>Flow timeout aggressive threshold</td>
<td>disabled</td>
</tr>
<tr>
<td>Flow timeout fast threshold</td>
<td>disabled</td>
</tr>
<tr>
<td>Flow timeout inactive</td>
<td>15 seconds</td>
</tr>
<tr>
<td>Flow timeout session aging</td>
<td>disabled</td>
</tr>
</tbody>
</table>

Additional References

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

- Related Documents, page 16-20
- Standards, page 16-20
Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetFlow CLI commands</td>
<td>Cisco Nexus 7000 Series NX-OS System Management Command Reference</td>
</tr>
<tr>
<td>VDCs and VRFs</td>
<td>Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.x</td>
</tr>
</tbody>
</table>

Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>—</td>
</tr>
</tbody>
</table>

Feature History for NetFlow

Table 16-2 lists the release history for this feature.

<table>
<thead>
<tr>
<th>Table 16-2 Feature History for Rollback</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feature Name</td>
</tr>
<tr>
<td>Layer 2 NetFlow</td>
</tr>
<tr>
<td>Rollback during NetFlow</td>
</tr>
</tbody>
</table>
IETF RFCs supported by Cisco NX-OS System Management

This appendix lists the IETF RFCs for system management supported in Cisco NX-OS.

<table>
<thead>
<tr>
<th>RFCs</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 2819</td>
<td>Remote Network Monitoring Management Information Base</td>
</tr>
<tr>
<td>RFC 3164</td>
<td>The BSD syslog Protocol</td>
</tr>
<tr>
<td>RFCs 3411 to 3418</td>
<td>An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks</td>
</tr>
<tr>
<td>RFC 3954</td>
<td>Cisco Systems NetFlow Services Export Version 9</td>
</tr>
</tbody>
</table>
Send document comments to nexus7k-docfeedback@cisco.com.
Embedded Event Manager System Events and Configuration Examples

This appendix describes the Embedded Event Manager (EEM) system policies, events, and policy configuration examples.

This appendix includes the following sections:
- EEM System Policies, page B-1
- EEM Events, page B-3
- EEM Policy Configuration Examples, page B-3

### EEM System Policies

Table B-1 lists the Embedded Event Manager (EEM) system policies.

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>__PortLoopback</td>
<td>Do CallHome, log error in Syslog/OBFL/Exception Log and disable further HM testing on affected ports after 20 consecutive failures of GOLD &quot;PortLoopback&quot; test</td>
</tr>
<tr>
<td>__RewriteEngineLoopback</td>
<td>Do CallHome, log error in Syslog/OBFL/Exception Log and disable further HM testing on affected ports after 20 consecutive failures of GOLD &quot;RewriteEngine&quot; test</td>
</tr>
<tr>
<td>__asic_register_check</td>
<td>Do CallHome, log error and disable further HM testing for that ASIC device/instance after 20 consecutive failures of GOLD &quot;ASICRegisterCheck&quot; test</td>
</tr>
<tr>
<td>__compact_flash</td>
<td>Do CallHome, log error and disable further HM testing after 20 consecutive failures of GOLD &quot;CompactFlash&quot; test</td>
</tr>
<tr>
<td>__crypto_device</td>
<td>Do CallHome and log error when GOLD &quot;CryptoDevice&quot; test fails</td>
</tr>
<tr>
<td>__eobc_port_loopback</td>
<td>Do CallHome and log error when GOLD &quot;EOBCPortLoopback&quot; test fails</td>
</tr>
<tr>
<td>__ethpm_debug_1</td>
<td>Action: none</td>
</tr>
</tbody>
</table>
### EEM System Policies (continued)

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>__ethpm_link_flap</td>
<td>Too many link flaps in a short interval. Action: Error Disable the port</td>
</tr>
<tr>
<td>__external_compact_flash</td>
<td>Do CallHome, log error and disable further HM testing after 20 consecutive failures of GOLD &quot;ExternalCompactFlash&quot; test</td>
</tr>
<tr>
<td>__lcm_module_failure</td>
<td>Power-cycle 2 times then power-down</td>
</tr>
<tr>
<td>__management_port_loopback</td>
<td>Do CallHome and log error when GOLD &quot;ManagementPortLoopback&quot; test fails</td>
</tr>
<tr>
<td>__nvram</td>
<td>Do CallHome, log error and disable further HM testing after 20 consecutive failures of GOLD &quot;NVRAM&quot; test</td>
</tr>
<tr>
<td>__pfm_fanabsent_all_systemfan</td>
<td>Shutdown if both fans (f1 &amp; f2) are together absent for two minutes</td>
</tr>
<tr>
<td>__pfm_fanabsent_any_singlefan</td>
<td>Shutdown half-chassis if fan absent for three minutes</td>
</tr>
<tr>
<td>__pfm_fanbad_all_systemfan</td>
<td>Shutdown if both fans (f1 &amp; f2) are together bad for two minutes</td>
</tr>
<tr>
<td>__pfm_fanbad_any_singlefan</td>
<td>Syslog when fan goes bad</td>
</tr>
<tr>
<td>__pfm_power_over_budget</td>
<td>Syslog warning for insufficient power over budget</td>
</tr>
<tr>
<td>__pfm_tempev_major</td>
<td>TempSensor Major Threshold. Action: Shutdown</td>
</tr>
<tr>
<td>__primary_bootrom</td>
<td>Do CallHome, log error and disable further HM testing after 20 consecutive failures of GOLD &quot;PrimaryBootROM&quot; test</td>
</tr>
<tr>
<td>__pwr_mgmt_bus</td>
<td>Do CallHome, log error and disable further HM testing for the module or spine-card after 20 consecutive failures of GOLD &quot;PwrMgmtBus&quot; test</td>
</tr>
<tr>
<td>__real_time_clock</td>
<td>Do CallHome, log error and disable further HM testing after 20 consecutive failures of GOLD &quot;RealTimeClock&quot; test</td>
</tr>
<tr>
<td>__secondary_bootrom</td>
<td>Do CallHome, log error and disable further HM testing after 20 consecutive failures of GOLD &quot;SecondaryBootROM&quot; test</td>
</tr>
<tr>
<td>__spine_control_bus</td>
<td>Do CallHome, log error and disable further HM testing for that module or spine-card after 20 consecutive failures of GOLD &quot;SpineControlBus&quot; test</td>
</tr>
<tr>
<td>__status_bus</td>
<td>Do CallHome, log error and disable further HM testing after 5 consecutive failures of GOLD &quot;StatusBus&quot; test</td>
</tr>
<tr>
<td>__standby_fabric_loopback</td>
<td>Do CallHome, log error in Syslog/OBFL/ExceptionLog and disable further HM testing for that module after 10 consecutive failures</td>
</tr>
<tr>
<td>__system_mgmt_bus</td>
<td>Do Call Home, log error and disable further HM testing for that FAN/PS after 20 consecutive failures</td>
</tr>
<tr>
<td>__usb</td>
<td>Do Call Home and log error</td>
</tr>
</tbody>
</table>
EEM Events

Table B-2 describes the EEM events you can use on the device.

<table>
<thead>
<tr>
<th>EEM Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cli</td>
<td>CLI command is entered that matches a pattern with a wildcard.</td>
</tr>
<tr>
<td>counter</td>
<td>EEM counter reaches a specified value or range.</td>
</tr>
<tr>
<td>fanabsent</td>
<td>System fan is absent.</td>
</tr>
<tr>
<td>fanbad</td>
<td>System fan generates a fault.</td>
</tr>
<tr>
<td>gold</td>
<td>GOLD test failure condition is hit.</td>
</tr>
<tr>
<td>memory</td>
<td>Available system memory exceeds a threshold.</td>
</tr>
<tr>
<td>module-failure</td>
<td>Module failure is generated.</td>
</tr>
<tr>
<td>oir</td>
<td>Online insertion or removal occurs.</td>
</tr>
<tr>
<td>policy-default</td>
<td>Default parameters and thresholds are used for the events in the system policy you override.</td>
</tr>
<tr>
<td>poweroverbudget</td>
<td>Platform software detects a power budget condition.</td>
</tr>
<tr>
<td>snmp</td>
<td>SNMP object ID (OID) state changes.</td>
</tr>
<tr>
<td>storm-control</td>
<td>Platform software detects an Ethernet packet storm condition.</td>
</tr>
<tr>
<td>sysmgr</td>
<td>System manager generates an event.</td>
</tr>
<tr>
<td>temperature</td>
<td>Temperature level in the system exceeds a threshold.</td>
</tr>
<tr>
<td>track</td>
<td>Tracked object changes state.</td>
</tr>
</tbody>
</table>

EEM Policy Configuration Examples

This section includes the following topics:

- Configuration Examples for CLI Events, page B-4
- Configuration Examples to Override (Disable) Major Thresholds, page B-5
- Configuration Examples to Override (Disable) Shutdown for Fan Removal, page B-8
- Configuration Examples to Create a Supplemental Policy, page B-10
- Configuration Examples for the Power Over-Budget Policy, page B-11
- Configuration Examples to Select Modules to Shut Down, page B-12
- Configuration Examples for the Online Insertion Removal Event, page B-13
- Configuration Example to Generate a User syslog, page B-13
- Configuration Examples for SNMP Notification, page B-13
- Configuration Example for Port Tracking, page B-14
Configuration Examples for CLI Events

This section includes the following examples of CLI event configuration:

- Monitoring Interface Shutdown, page B-4
- Monitoring Module Powerdown, page B-4
- Adding a Trigger to Initiate a Rollback, page B-4

Monitoring Interface Shutdown

This example shows how to monitor an interface shutdown:

```plaintext
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# event manager applet monitorShutdown
switch(config-applet)#
switch(config-applet)# description "Monitors interface shutdown."
switch(config-applet)# event cli match "conf t; interface *; shutdown"
switch(config-applet)# action 1.0 cli show interface e 3/1
switch(config)# copy running-config startup-config
```

**Note**

Outputs of `show` commands entered as part of EEM policy are archived in the logflash as text files with the "eem_archive_" prefix. To view the archived output, use the `show file logflash:eem_archive_` command.

Monitoring Module Powerdown

This example shows how to monitor a module powerdown:

```plaintext
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# event manager applet monitorPoweroff
switch(config-applet)#
switch(config-applet)# description "Monitors module power down."
switch(config-applet)# event cli match "conf t; poweroff *"
switch(config-applet)# action 1.0 cli show module
switch(config)# copy running-config startup-config
```

Adding a Trigger to Initiate a Rollback

This example shows how to add a trigger to initiate a rollback:

```plaintext
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)#
switch(config)# event manager applet rollbackTrigger
switch(config-applet)#
switch(config-applet)# description "Rollback trigger."
switch(config-applet)# event cli match "rollback *"
switch(config-applet)# action 1.0 cli copy running-config bootflash:last_config
switch(config)# copy running-config startup-config
```
Configuration Examples to Override (Disable) Major Thresholds

This section includes the following topics:

- Preventing a Shutdown When Reaching a Major Threshold, page B-5
- Disabling One Bad Sensor, page B-5
- Disabling Multiple Bad Sensors, page B-6
- Overriding (Disabling) an Entire Module, page B-6
- Overriding (Disabling) Multiple Modules and Sensors, page B-6
- Enabling One Sensor While Disabling All Remaining Sensors of All Modules, page B-7
- Enabling Multiple Sensors While Disabling All Remaining Sensors of All Modules, page B-7
- Enabling All Sensors of One Module While Disabling All Sensors of the Remaining Modules, page B-7
- Enabling a Combination of Sensors on Modules While Disabling All Sensors of the Remaining Modules, page B-8

Preventing a Shutdown When Reaching a Major Threshold

This example shows how to prevent a shutdown caused by reaching a major threshold:

```
switch# config t
switch(config)# event manager applet myappletname override __pfm_tempev_major
switch(config)# end
```

This example shows how to revert to the default configuration:

```
switch# config t
switch(config)# no event manager applet myappletname override __pfm_tempev_major
switch(config)# end
```

Disabling One Bad Sensor

This example shows how to disable only sensor 3 on module 2 when sensor 3 is malfunctioning (all other sensors are unaffected):

```
switch# config t
switch(config)# event manager applet myappletname override __pfm_tempev_major
switch(config-applet)# event temperature module 2 sensor 3 threshold major
switch(config-applet)# end
```

This example shows how to revert to the default configuration:

```
switch# config t
switch(config)# no event manager applet myappletname override __pfm_tempev_major
switch(config)# end
```
Disabling Multiple Bad Sensors

This example shows how to disable sensors 5, 6, and 7 on module 2 when these sensors are malfunctioning (all other sensors are unaffected):

```
switch# config t
switch(config)# event manager applet myappletname override __pfmTempev_major
switch(config-applet)# event temperature module 2 sensor 5 threshold major
switch(config-applet)# end
```

```
switch# config t
switch(config)# event manager applet myappletname override __pfmTempev_major
switch(config-applet)# event temperature module 2 sensor 6 threshold major
switch(config-applet)# end
```

```
switch# config t
switch(config)# event manager applet myappletname override __pfmTempev_major
switch(config-applet)# event temperature module 2 sensor 7 threshold major
switch(config-applet)# end
```

This example shows how to revert to the default configuration:

```
switch# config t
switch(config)# no event manager applet myappletname override __pfm_tempev_major
switch(config)# end
```

Overriding (Disabling) an Entire Module

This example shows how to disable module 2 when it is malfunctioning:

```
switch# config t
switch(config)# event manager applet myappletname override __pfm_tempev_major
switch(config-applet)# event temperature module 2 threshold major
switch(config-applet)# end
```

This example shows how to revert to the default configuration:

```
switch# config t
switch(config)# no event manager applet myappletname override __pfm_tempev_major
switch(config)# end
```

Overriding (Disabling) Multiple Modules and Sensors

This example shows how to disable sensors 3, 4, and 7 on module 2 and all sensors on module 3 when they are malfunctioning:

```
switch# config t
switch(config)# event manager applet myappletname override __pfm_tempev_major
switch(config-applet)# event temperature module 2 sensor 3 threshold major
switch(config-applet)# end
```

```
switch# config t
switch(config)# event manager applet myappletname override __pfm_tempev_major
switch(config-applet)# event temperature module 2 sensor 4 threshold major
switch(config-applet)# end
```

```
switch# config t
switch(config)# event manager applet myappletname override __pfm_tempev_major
switch(config-applet)# event temperature module 2 sensor 7 threshold major
switch(config-applet)# end
```

```
switch# config t
switch(config)# event manager applet myappletname override __pfm_tempev_major
switch(config-applet)# event temperature module 3 threshold major
switch(config-applet)# end
```
This example shows how to revert to the default configuration:

```
switch# config t
switch(config)# no event manager applet myappletname override __pfm_tempev_major
switch(config)# end
```

**Enabling One Sensor While Disabling All Remaining Sensors of All Modules**

This example shows how to disable all sensors on all modules except sensor 4 on module 9:

```
switch# config t
switch(config)# event manager applet myapplet1 override __pfm_tempev_major
switch(config-applet)# end
switch# config t
switch(config)# event manager applet myapplet2 override __pfm_tempev_major
switch(config-applet)# event temperature module 9 sensor 4 threshold major
switch(config-applet)# action 2 policy-default
switch(config-applet)# end
```

**Enabling Multiple Sensors While Disabling All Remaining Sensors of All Modules**

This example shows how to disable all sensors on all modules except sensors 4, 6, and 7 on module 9:

```
switch# config t
switch(config)# event manager applet myapplet1 override __pfm_tempev_major
switch(config-applet)# end
switch# config t
switch(config)# event manager applet myapplet2 override __pfm_tempev_major
switch(config-applet)# event temperature module 9 sensor 4 threshold major
switch(config-applet)# action 2 policy-default
switch(config-applet)# end
switch# config t
switch(config)# event manager applet myapplet3 override __pfm_tempev_major
switch(config-applet)# event temperature module 9 sensor 6 threshold major
switch(config-applet)# action 3 policy-default
switch(config-applet)# end
switch# config t
switch(config)# event manager applet myapplet4 override __pfm_tempev_major
switch(config-applet)# event temperature module 9 sensor 7 threshold major
switch(config-applet)# action 4 policy-default
switch(config-applet)# end
```

**Enabling All Sensors of One Module While Disabling All Sensors of the Remaining Modules**

This example shows how to disable all sensors on all modules except all sensors on module 9:

```
switch# config t
switch(config)# event manager applet myapplet1 override __pfm_tempev_major
switch(config-applet)# end
switch# config t
switch(config)# event manager applet myapplet2 override __pfm_tempev_major
switch(config-applet)# event temperature module 9 threshold major
switch(config-applet)# action 2 policy-default
switch(config-applet)# end
```

Send document comments to nexus7k-docfeedback@cisco.com.
Enabling a Combination of Sensors on Modules While Disabling All Sensors of the Remaining Modules

This example shows how to disable all sensors on all modules except sensors 3, 4, and 7 on module 2 and all sensors on modules 3 and 4:

```bash
switch# config t
switch(config)# event manager applet myapplet1 override __pfm_tempev_major
switch(config-applet)# end
switch# config t
switch(config)# event manager applet myapplet2 override __pfm_tempev_major
switch(config-applet)# event temperature module 2 sensor 3 threshold major
switch(config-applet)# action 2 policy-default
switch(config-applet)# end
switch# config t
switch(config)# event manager applet myapplet3 override __pfm_tempev_major
switch(config-applet)# event temperature module 2 sensor 4 threshold major
switch(config-applet)# action 3 policy-default
switch(config-applet)# end
switch# config t
switch(config)# event manager applet myapplet4 override __pfm_tempev_major
switch(config-applet)# event temperature module 2 sensor 7 threshold major
switch(config-applet)# action 4 policy-default
switch(config-applet)# end
switch# config t
switch(config)# event manager applet myapplet5 override __pfm_tempev_major
switch(config-applet)# event temperature module 3 threshold major
switch(config-applet)# action 5 policy-default
switch(config-applet)# end
```

Configuration Examples to Override (Disable) Shutdown for Fan Removal

This section includes the following topics:
- Overriding (Disabling) a Shutdown for Removal of One or More Fans, page B-8
- Overriding (Disabling) a Shutdown for Removal of a Specified Fan, page B-9
- Overriding (Disabling) a Shutdown for Removal of Multiple Specified Fans, page B-9
- Overriding (Disabling) a Shutdown for Removal of All Fans Except One, page B-9
- Overriding (Disabling) a Shutdown for Removal of Fans Except for a Specified Set of Fans, page B-10
- Overriding (Disabling) a Shutdown for Removal of All Fans Except One from a Set of Fans, page B-10

Overriding (Disabling) a Shutdown for Removal of One or More Fans

This example shows how to disable a shutdown so that you can remove one or more (or all) fans:

```bash
switch# config t
switch(config)# event manager applet myappletname override __pfm_fanabsent_any_singlefan
switch(config-applet)# end
```

This example shows how to revert to the default configuration:
Overriding (Disabling) a Shutdown for Removal of a Specified Fan

This example shows how to disable a shutdown so that you can remove a specified fan (fan 3):

```plaintext
switch# config t
switch(config)# no event manager applet myappletname override __pfm_fanabsent_any_singlefan
switch(config-applet)# end
```

Overriding (Disabling) a Shutdown for Removal of Multiple Specified Fans

This example shows how to disable a shutdown so that you can remove multiple specified fans (fans 2, 3, and 4):

```plaintext
switch# config t
switch(config)# event manager applet myapplet1 override __pfm_fanabsent_any_singlefan
switch(config-applet)# event fanabsent fan 2 time 60
switch(config-applet)# end
switch(config)# event manager applet myapplet2 override __pfm_fanabsent_any_singlefan
switch(config-applet)# event fanabsent fan 3 time 60
switch(config-applet)# end
switch(config)# event manager applet myapplet3 override __pfm_fanabsent_any_singlefan
switch(config-applet)# event fanabsent fan 4 time 60
switch(config-applet)# end
```

Overriding (Disabling) a Shutdown for Removal of All Fans Except One

This example shows how to disable a shutdown so that you can remove all fans except one (fan 2):

```plaintext
switch# config t
switch(config)# event manager applet myapplet1 override __pfm_fanabsent_any_singlefan
switch(config-applet)# end
switch(config)# event manager applet myapplet2 override __pfm_fanabsent_any_singlefan
switch(config-applet)# event fanabsent fan 2 time 60
switch(config-applet)# action 2 policy-default
switch(config-applet)# end
```
Appendix B  Embedded Event Manager System Events and Configuration Examples

EEM Policy Configuration Examples

Send document comments to nexus7k-docfeedback@cisco.com.

Overriding (Disabling) a Shutdown for Removal of Fans Except for a Specified Set of Fans

This example shows how to disable a shutdown so that you can remove fans except for a specified set of fans (fans 2, 3, and 4):

```
switch# config t
switch(config)# event manager applet myapplet1 override __pfm_fanabsent_any_singlefan
switch(config-applet)# end
switch(config)# event manager applet myapplet2 override __pfm_fanabsent_any_singlefan
switch(config-applet)# event fanabsent fan 2,3,4 time 60
switch(config-applet)# action 2 policy-default
switch(config-applet)# end
```

Overriding (Disabling) a Shutdown for Removal of All Fans Except One from a Set of Fans

This example shows how to disable a shutdown so that you can remove all fans except one from a set of fans (fans 2, 3, or 4):

```
switch# config t
switch(config)# event manager applet myapplet1 override __pfm_fanabsent_any_singlefan
switch(config-applet)# end
switch# config t
switch(config)# event manager applet myapplet2 override __pfm_fanabsent_any_singlefan
switch(config-applet)# event fanabsent fan 2 time 60
switch(config-applet)# action 2 policy-default
switch(config-applet)# end
switch# config t
switch(config)# event manager applet myapplet3 override __pfm_fanabsent_any_singlefan
switch(config-applet)# event fanabsent fan 3 time 60
switch(config-applet)# action 3 policy-default
switch(config-applet)# end
switch# config t
switch(config)# event manager applet myapplet4 override __pfm_fanabsent_any_singlefan
switch(config-applet)# event fanabsent fan 4 time 60
switch(config-applet)# action 4 policy-default
switch(config-applet)# end
```

Configuration Examples to Create a Supplemental Policy

This section includes the following topics:

- Creating a Supplemental Policy for the Fan Absent Event, page B-10
- Creating a Supplemental Policy for the Temperature Threshold Event, page B-11

Creating a Supplemental Policy for the Fan Absent Event

This example shows how to create a supplemental policy using the `event fanabsent` command:

```
[no] event fanabsent [fan fan-number] time time-interval
```

In addition to the default policy, this example shows how to execute the policy myappletname and action 3 if fan 1 is absent for 60 seconds:
Creating a Supplemental Policy for the Temperature Threshold Event

This example shows how to create a supplemental policy using the `event temperature` command:

```
[no] event temperature [mod module-number] [sensor sensor-number] threshold {major | minor | any}
```

In addition to the default policy, this example shows how to execute the policy `myappletname` and action 1 if the temperature crosses the minor threshold on sensor 3 of module 2:

```
switch# config t
switch(config)# event manager applet myappletname
switch(config-applet)# event temperature module 2 sensor 3 threshold minor
switch(config-applet)# action 1 cli "show environ temperature"
switch(config-applet)# end
```

Configuration Examples for the Power Over-Budget Policy

The power over-budget policy gets triggered when the available power capacity drops below zero and the device is no longer able to keep the previously powered-up modules in the powered-up state. The default action is to print a syslog to notify the user of the occurrence of power over budget.

You can enable an additional action to power down modules until the available power recovers from the red (negative) zone.

This section includes the following topics:
- Shuting Down Modules, page B-11
- Shuting Down a Specified List of Modules, page B-12

Shutting Down Modules

If you do not specify any modules, the power over-budget shutdown starts from slot 1 and shuts down modules until the power recovers from the red (negative) zone. Empty slots and slots that contain a supervisor, standby supervisor, spine, or crossbar are skipped.

This example shows how to shut down modules starting from module 1 when the available power drops below zero:

```
switch# config t
switch(config)# event manager applet <myappletname>4a> override __pfm_power_over_budget
switch(config-applet)# event poweroverbudget
switch(config-applet)# action & overbudgetshut
switch(config-applet)# end
```
Shutting Down a Specified List of Modules

You can specify a list of modules that the power over-budget action uses to shut down modules until the power recovers from the red (negative) zone. Empty slots and slots that contain a supervisor, standby supervisor, spine, or crossbar are skipped.

This example shows how to shut down modules from a specified list of modules (1, 2, 7, 8) when the available power drops below zero:

```bash
switch# config t
switch(config)# event manager applet <myappletname> override __pfm_power_over_budget
switch(config-applet)# event poweroverbudget
switch(config-applet)# action 5 overbudgetshut module 1,2,7,8
switch(config-applet)# end
```

Configuration Examples to Select Modules to Shut Down

This section includes the following topics:

- Using the Policy Default to Select Nonoverridden Modules to Shut Down, page B-12
- Using Parameter Substitution to Select Nonoverridden Modules to Shut Down, page B-12

Using the Policy Default to Select Nonoverridden Modules to Shut Down

This example shows how to use the policy default to select the nonoverridden modules to shut down when a major threshold is exceeded:

```bash
switch# config t
switch(config)# event manager applet my5a1 override __pfm_tempev_major
switch(config-applet)# end
switch# config t
switch(config)# event manager applet my5a2 override __pfm_tempev_major
switch(config-applet)# event temperature module 1-3 sensor 4 threshold major
switch(config-applet)# action 5 policy-default
switch(config-applet)# end
```

Using Parameter Substitution to Select Nonoverridden Modules to Shut Down

This example shows how to use parameter substitution to select the nonoverridden modules to shut down when a major threshold is exceeded:

```bash
switch# config t
switch(config)# event manager applet my5b1 override __pfm_tempev_major
switch(config-applet)# end
switch# config t
switch(config)# event manager applet my5b2 override __pfm_tempev_major
switch(config-applet)# event temperature module 1-3 sensor 8 threshold major
switch(config-applet)# action 6 forceshut module my_module_list reset "temperature-sensor policy trigger"
switch(config-applet)# end
```

To create event manager parameters, use the `event manager environment` command. To display the values of event manager parameters, use the `show event manager environment all` command.
Configuration Examples for the Online Insertion Removal Event

The online insertion removal (OIR) event does not have a default policy. This example shows how to configure the OIR event using the \texttt{event oir} command:

```
switch# config t
switch(config)# event manager applet myoir
switch(config-applet)# event oir module insert
switch(config-applet)# action 1 syslog priority critical msg "OIR insert event: A Module is inserted"
```

This example shows how to configure the insert event:

```
switch# config t
switch(config)# event manager applet myoir
switch(config-applet)# event oir module insert
switch(config-applet)# action 1 syslog priority critical msg "OIR insert event: A Module is inserted"
```

This example shows how to configure the remove event:

```
switch# config t
switch(config)# event manager applet myoir
switch(config-applet)# event oir module remove
switch(config-applet)# action 1 syslog priority critical msg "OIR remove event: A Module is removed"
```

Configuration Example to Generate a User syslog

This example shows how to generate a user syslog using the \texttt{action syslog} command.

```
switch# config t
switch(config)# event manager applet myoir
switch(config-applet)# event oir module remove
switch(config-applet)# action 1 syslog priority critical msg "Module is removed"
```

When this event is triggered, the system will generate a syslog as follows:

```
p1b-57(config)# 2008 Feb 20 00:08:27 p1b-57 %$ VDC-1 %$ %EEM_ACTION-2-CRIT: "Module is removed"
2008 Feb 20 00:08:27 p1b-57 %$ VDC-1 %$ %PLATFORM-2-MOD_REMOVE: Module 2 removed (Serial number JAB120101PW)
```

Configuration Examples for SNMP Notification

This section includes the following topics:

- Polling an SNMP OID to Generate an EEM Event, page B-14
- Sending an SNMP Notification in Response to an Event in the Event Policy, page B-14
EEM Policy Configuration Examples

Send document comments to nexus7k-docfeedback@cisco.com.

Polling an SNMP OID to Generate an EEM Event

The SNMP object ID (OID) CISCO-SYSTEM-EXT-MIB::cseSysCPUUtilization is used for querying the CPU utilization of the switch:

```plaintext
cseSysCPUUtilization OBJECT-TYPE
SYNTAX          Gauge32 (0..100 )
UNITS           "%"
MAX-ACCESS      read-only
STATUS          current
DESCRIPTION
   "The average utilization of CPU on the active supervisor."
::= { ciscoSysInfoGroup 1 }
```

This example shows the use of an SNMP OID that is polled at an interval of 10 seconds and has a threshold value of 95 percent:

```plaintext
switch# config t
switch(config)# event manager applet test_policy
switch(config-applet)# event snmp oid 1.3.6.1.4.1.9.9.305.1.1.1.0 get-type exact entry-op gt entry-val 95 exit-op lt exit-val 90 poll-interval 10
```

Sending an SNMP Notification in Response to an Event in the Event Policy

You can use this type of configuration to cause a critical event trigger to generate an SNMP notification. This example shows how to send an SNMP notification for an event from the Event Manager applet configuration mode:

```plaintext
switch(config-applet)# action 1.1 snmp-trap intdata1 100 intdata2 300 strdata "CPU Hogging at switch1"
switch(config-applet)# action 1.1 snmp-trap intdata1 100 intdata2 300 strdata "Port Failure eth9/1"
```

This configuration triggers an SNMP notification (trap) from the switch to SNMP hosts. The SNMP payload carries the values of user-defined fields intdata1, intdata2, and strdata.

Configuration Example for Port Tracking

This example shows how to configure the state of one port to match the state of another port (port tracking).

To configure port tracking of Ethernet interface 3/23 by Ethernet interface 1/2, follow these steps:

**Step 1** Create an object to track the status of Ethernet interface 3/23.

```plaintext
switch# config t
switch(config)# track 1 interface ethernet 3/23
switch(config-track)# end
```

**Step 2** Configure an EEM event to shut Ethernet interface 1/2 when the tracking object shuts down.

```plaintext
switch(config)# event manager applet track_3_23_down
switch(config-applet)# event track 1 state down
switch(config-applet)# action 1 syslog msg EEM applet track_3_23_down shutting down port eth1/2 due to eth3/23 being down
switch(config-applet)# action 2 cli conf term
switch(config-applet)# action 3 cli interface ethernet 1/2
switch(config-applet)# action 4 cli shut
```
Switch(config-applet)# end

Step 3 Configure an EEM event to bring up Ethernet interface 1/2 when Ethernet interface 3/23 comes up.

Switch# config t
Switch(config)# event manager applet track_3_23_up
Switch(config-applet)# event track 1 state up
Switch(config-applet)# action 1 syslog msg EEM applet track_3_23_down bringing up port eth1/2 due to eth3/23 being up
Switch(config-applet)# action 2 cli conf term
Switch(config-applet)# action 3 cli interface ethernet 1/2
Switch(config-applet)# action 4 cli no shut
Switch(config-applet)# end
Send document comments to nexus7k-docfeedback@cisco.com.
INDEX

B

bootup diagnostics 12-2

C

Call Home
- alert groups 6-3
- benefits 6-2
- CFS support 2-2
- configuring contact information 6-9
- configuring e-mail 6-18
- configuring inventory notification 6-18, 6-19
- default settings 6-23
- description 6-1 to 6-7
- destination profiles
  - associating an alert group 6-15
  - attributes 6-13
  - creating 6-11
  - description 6-2
  - modifying 6-13
  - predefined 6-2
- disabling 6-21
- disabling duplicate message throttle 6-20
- e-mail notifications 1-4
- enabling 6-21
- event triggers (table) 6-23
- example configuration 6-22
- guidelines 6-8
- high availability 6-7
- licensing requirements 6-8
- limitations 6-8

mapping message levels to syslog levels (table) 6-5
message formats
  - full text (table) 6-25, 6-26
  - full-text format, example 6-28
  - inventory events (table) 6-27
  - options 6-2
  - proactive events (table) 6-27
  - reactive events (table) 6-27
  - short text (table) 6-25
  - XML (table) 6-25, 6-26
  - XML format, example 6-31
- message levels 6-5
- MIBs 6-35
- modifying an alert group 6-16
- prerequisites 6-8
- sending a test message 6-21
- Smart Call Home feature 6-6
- verifying configuration 6-22
- virtualization support 6-7

CDP
- clearing cache 4-7
- clearing statistics 4-7
- configuring timers, example 4-7
- default settings 3-10, 4-8
- description 4-1
- disabling the feature 4-4
- enabling globally 4-4
- enabling on an interface 4-5
- guidelines 4-3
- licensing requirements 4-3
- limitations 4-3
- MIBs (table) 3-11, 4-8
- optional parameters 4-6
prerequisites 4-3
TLV fields 4-2
verifying configuration 4-7
version 4-8
virtualization 4-3
VLAN ID 4-2
VTP 4-2

CFS
  default settings 2-24
description 2-1 to 2-3
disabling on a switch 2-22
distribution modes 2-2
enabling on a switch 2-22
features supported 2-2
guidelines 2-4
high availability 2-3
licensing requirements 2-4
limitations 2-4
MIBs (table) 2-25
NTP 3-2
prerequisites 2-4
virtualization 2-3

CFS applications
  clearing session locks 2-20
  committing changes 2-19
discarding changes 2-21
enabling 2-5
enabling distribution for Call Home 2-5, 2-9
enabling distribution for RADIUS 2-6
enabling distribution for roles 2-8
enabling distribution for TACACS+ 2-7
fabric locking 2-19

CFS distribution mode 2-10

CFS over IP
  configuring IP multicast addresses 2-11
default settings 2-24

CFS regions
  creating 2-13
  deleting 2-17

D

default settings
  Call Home 6-23
  CDP 3-10, 4-8
  EEM 13-18
  NetFlow 16-19
  NTP 3-10, 4-8
  OBFL 15-7
  online diagnostics 12-11
  RMON 11-7
  rollback 7-7
  Scheduler 9-14
  SNMP 10-23
  system messages 5-11
diagnostics
  bootup 12-2
  on demand 12-4
  runtime 12-3
distribution mode 2-10
documentation
  additional publications i-xxi
  conventions i-xx
Index

E

EEM
- actions 13-4
- activating a script policy 13-13
- allow CLI commands to execute 13-12
- configuring action statements 13-11
- configuring event statements 13-8
- default settings 13-18
- defining an environment variable 13-6
- defining a policy 13-7
- defining script policies 13-12
- description 13-1 to 13-5
- environment variables 13-5
- event logs 13-2
- events 13-3
- example configuration 13-17
- guidelines 13-6
- high availability 13-5
- licensing requirements 13-5
- limitations 13-6
- override policy 13-2
- override policy (note) 13-3
- override policy actions (note) 13-4
- overriding a system policy 13-14
- parameter substitution 13-5
- policies 13-2
- prerequisites 13-6
- registering a script policy 13-13
- script policies 13-4
- SNMP support 10-5
- system policies 13-2
- verifying configuration 13-17
- virtualization support 13-5
- EEM overriding a system policy (example) 13-17
- embedded event manager. See EEM
- executing a session 8-5
- exporter map 16-2

F

features, new and changed (table) i-xv

G

GOLD. See online diagnostics

H

health monitoring diagnostics 12-3
- high availability
  - CDP 3-2, 4-3
  - CFS 2-3
  - EEM 13-5
  - NetFlow 16-3
  - NTP 3-2, 4-3
- online diagnostics 12-4
- RMON 11-2
- rollback 7-2
- SNMP 10-6
- SPAN 14-4

L

licensing requirements
- Call Home 6-8
- CDP 4-3
- CFS 2-4
- EEM 13-5
- NetFlow 16-4
- NTP 3-3
- OBFL 15-2
- online diagnostics 12-5
- RMON 11-3
- rollback 7-3
- Scheduler 9-3
- session manager 8-2
Send document comments to nexus7k-docfeedback@cisco.com.

SNMP 10-6
SPAN 14-5
system messages 5-3

M

MIBs
   Call Home 6-35
   CDP 3-11, 4-8
   CFS 2-25
description 10-2
location to download 10-24
   NTP 3-11, 4-8
   RMON 11-8
   SNMP 10-24
mode, CFS distribution 2-10
monitor map 16-3

N

NetFlow
   applying a monitor map to an interface 16-13
   applying a monitor map to a VLAN 16-14
   applying a sampler map to an interface 16-13
   configuring Bridged NetFlow 16-14
   configuring NetFlow 16-5
   configuring timeouts 16-17
   creating a monitor map 16-11
   creating an export map 16-9
   creating a record map 16-6
   creating a sampler map 16-12
default settings 16-19
description 16-1 to 16-4
disabling 16-6
enabling 16-5
example configuration 16-19
exporter map 16-2
export formats 16-3
flows 16-1
full mode 16-2
high availability 16-3
keys 16-1
licensing requirements 16-4
monitor map 16-3
record map 16-2
sampled mode 16-2
sampler map 16-3
specifying collect parameters 16-8
specifying match parameters 16-7
verifying configuration 16-18
virtualization support 16-4
Netflow
   configuring Layer 2 keys 16-15
Network Time Protocol. See NTP
NTP
   CFS 3-2
   CFS support 2-2
clearing a session 3-9
clearing statistics 3-9
   configuring a server and peer, example 3-10
   configuring peer 3-5
   configuring server 3-5
default settings 3-10, 4-8
description 3-1
feature history (table) 3-11
guidelines 3-3
high availability 3-2, 4-3
licensing requirements 3-3
limitations 3-3
MIBs (table) 3-11, 4-8
prerequisites 3-3
source interface 3-7
stratum 3-2
verifying configuration 2-24
virtualization 3-2, 4-3
ntp
   source IP address 3-7
Send document comments to nexus7k-docfeedback@cisco.com.

O

OBFL
  clearing statistics 15-7
  default settings 15-7
  description 15-1
  enabling 15-3
  example configuration 15-7
  guidelines 15-2
  licensing requirements 15-2
  limitations 15-2
  prerequisites 15-2
  verifying configuration 15-6
  virtualization support 15-2
on-board failure logging. See OBFL
on demand diagnostics 12-4
online diagnostics
  activating a diagnostics test 12-6
  bootup 12-2
  clearing the test results 12-9
  configuring the bootup diagnostic level 12-5
  default settings 12-11
  description 12-1 to 12-5
  example configuration 12-11
  feature history (table) 12-12
  guidelines 12-5
  health monitoring 12-3
  high availability 12-4
  licensing requirements 12-5
  limitations 12-5
  on demand 12-4
  prerequisites 12-5
  runtime 12-3
  setting a diagnostic test as inactive 12-8
  simulating a test result 12-10
  starting an on-demand test 12-8
  stopping an on-demand test 12-8
  verifying configuration 12-10
  virtualization support 12-4
VRFs 12-5

R

RADIUS
  CFS support 2-2
  record map 16-2
related documents i-xxi
RMON
  alarms 11-2
  configuring alarms 11-4
  configuring events 11-5
  default settings 11-5
  description 11-1
  events 11-2
  example configuration 11-6
  guidelines 11-3
  high availability 11-2
  licensing requirements 11-3
  limitations 11-3
  MIBs 11-8
  prerequisites 11-3
  verifying configuration 11-6
  virtualization support 11-3
VRFs 11-3
roles
  CFS support 2-2
rollback
  checkpoint copy 7-2
  creating a checkpoint copy 7-4
  default settings 7-7
  description 7-1
  example configuration 7-7
  guidelines 7-3
  high availability 7-2
  implementing a rollback 7-5
  licensing requirements 7-3
  limitations 7-3
  prerequisites 7-3
S

sampler map  16-3

Scheduler
  authentication  9-2
  clearing the logfile  9-10
  configuring  9-3
  configuring authentication  9-5
  configuring logfile  9-5
  default settings  9-14
  defining a timetable  9-8
  defining jobs  9-6
  deleting a job  9-7
  description  9-1
  disabling the feature  9-11
  enabling the feature  9-4
  guidelines  9-3
  high availability  9-2
  licensing requirements  9-3
  limitations  9-3
  prerequisites  9-3
  verifying configuration  9-12
  virtualization support  9-2

scheduler
  execution logs  9-2

session manager  8-5
  committing a session  8-5
  configuring ACLs  8-4
  configuring an ACL session (example)  8-6
  creating a session  8-3
  description  8-1
  discarding a session  8-6
  guidelines  8-2
  high availability  8-2

Simple Network Management Protocol. See SNMP

Smart Call Home
  description  6-6
  registration requirements  6-6
  SMARTnet registration  6-6

SNMP
  agent  10-2
  assigning contact  10-18
  assigning location  10-18
  assigning multiple user roles  10-9
  authentication  10-4
  configuring a user  10-7
  configuring context to network entity mapping  10-19
  context mapping  10-5
  contexts  10-5
  creating communities  10-9
  default settings  10-23
  description  10-1 to 10-6
  disabling protocol  10-21
  display ifIndex values  10-18
  EEM support  10-5
  enabling one-time authentication  10-18
  enforcing encryption  10-8
  engine ID format  10-8
  example configuration  10-22
  feature history (table)  10-24
  filtering SNMP requests  10-10
  group-based access  10-5
  guidelines  10-7
  high availability  10-6
  licensing requirements  10-6
  limitations  10-7
manager 10-2
MIBs 10-2
MIBs supported 10-24
multiple instance support 10-5
notifications
  configuring LinkUp/LinkDown notifications 10-17
  configuring notification receivers 10-10
  configuring notification receivers with VRFs 10-12
  configuring source interface for 10-11
  configuring the notification target user 10-12
  description 10-2
  enabling individual notifications 10-15
  informs 10-2
  trap 10-2
notification source interface 10-12
prerequisites 10-6
RFCs 10-2
RMON 11-1
user synchronization with CLI 10-4
versions
  security models and levels 10-3
  SNMPv3 10-2
  USM 10-3
virtualization support 10-6
VRFs 10-6
SNMP requests
  filtering 10-10
SPAN
  configuring an RSPAN VLAN 14-12
  configuring a PVLAN source in a session (example) 14-16
  configuring a session 14-6
  configuring a session (example) 14-15
  configuring a virtual SPAN session 14-10
  configuring a virtual SPAN session (example) 14-16
  description 14-1
  enabling a session 14-13
  guidelines 14-5
high availability 14-4
licensing requirements 14-5
limitations 14-5
multiple sessions 14-4
prerequisites 14-5
session destinations 14-7
session limits 14-5
sessions 14-3
session sources 14-6
shutting down a session 14-13
subinterface restriction 14-7
verifying configuration 14-15
virtualization support 14-4
virtual SPAN sessions 14-3
switched port analyzer. See SPAN
syslog
  See system messages
system checkpoints 7-2
system messages
  clearing a log file 5-9
  configuring (example) 5-11
  configuring a syslog server 5-7
  configuring a syslog server on a Linux system 5-9
  configuring a syslog server on a UNIX system 5-9
  configuring severity level to log 5-6
  configuring timestamp 5-11
default settings 5-11
description 5-1
  displaying a log file guidelines 5-3
  listing messages 5-12
logging to a file 5-5
logging to a terminal session 5-3
logging to the console port 5-3
RFC 5-1
severity levels (table) 5-2
syslog server 5-2
verifying configuration 5-10
virtualization support 5-2

T

TACACS+
  CFS support 2-2
trap. See SNMP
troubleshooting 1-6

U

uncoordinated CFS distribution 2-2
users
  CFS support 2-2

V

virtualization
  CFS 2-3
  NTP 3-2
VTP
  CDP 4-2