Cisco Nexus 7000 Series NX-OS CLI Management Best Practices Guide

First Published: February 2011
Last Modified: August 2011

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

Text Part Number: OL-24154-01

Cisco Nexus 7000 Series NX-OS CLI Management Best Practices Guide

CONTENTS

Preface

This preface describes the audience, organization, and conventions of the *Cisco Nexus 7000 Series CLI Management Best Practices Guide.* It also provides information on how to obtain related documentation.

This chapter includes the following sections:

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:

Chapter	Description
Chapter 1, Overview	Describes the purpose of this guide.
Chapter 2, Initial Configuration	Describes the Cisco NX-OS best practices that are typically configured when a Cisco Nexus 7000 Series switch is powered up for the first time.
Chapter 3, Connecting to the Management Network and Securing Access	Describes the Cisco NX-OS recommended best practices for connecting a Cisco Nexus 7000 Series switch to the management network(s) and securing access to the CLI.
Chapter 4, Protecting the CPU	Describes the recommended best practices for protecting the CPU against Denial of Service (DoS) attacks.

Chapter	Description
Chapter 5, Integrated Intrusion Detection Security	Describes two types of Intrusion Detection System packet checks that are enabled in Cisco NX-OS software.
Chapter 6, Cisco NX-OS Software Upgrade or Downgrade	Describes the Cisco NX-OS best practices for upgrading or downgrading Cisco NX-OS system software.
Chapter 7, EPLD Software Upgrade or Downgrade	Describes the recommended procedure for upgrading or downgrading an electronic programmable logic device (EPLD).
Chapter 8, Enabling and Disabling Features	Describes the process for enabling and disabling software features.
Chapter 9, IP Management	Describes the Cisco NX-OS best practices that are recommended when configuring IP management protocols.
Chapter 10, Management Tools for Usability	Describes Cisco NX-OS features that are recommended for managing a device.
Chapter 11, Verifying Hardware Diagnostics and Logging	Describes the Cisco NX-OS recommended features and procedures for managing and troubleshooting potential hardware faults.
Chapter 12,Managing Hardware Resource Utilization	Describes Cisco NX-OS procedures that are recommended for managing hardware resources such as the CPU, memory, and I/O module TCAM table utilization.
Chapter 13, Collecting Data for the Cisco TAC	Describes the recommended procedures for collecting troubleshooting information that should be attached to a TAC case.

Document Conventions

Command descriptions use these conventions:

Convention	Description
boldface font	Commands and keywords are in boldface.
italic font	Arguments for which you supply values are in italics.
{ }	Elements in curly brackets are required.
[ ]	Elements in square brackets are optional.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Screen examples use these conventions:

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

This document uses the following conventions:

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

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

Related Documentation

Cisco NX-OS includes the following documents:

Release Notes

Cisco Nexus 7000 Series NX-OS Release Notes, Release 4.1

NX-OS Configuration Guides

Cisco Nexus 7000 Series NX-OS Getting Started with Virtual Device Contexts, Release 4.1

Cisco Nexus 7000 Series OTV Quick Start Guide

Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 4.1

Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 4.1

Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 4.1

Cisco Nexus 7000 Series NX-OS Quality of Service Configuration Guide, Release 4.1

Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 4.1

Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide, Release 4.1

Cisco Nexus 7000 Series NX-OS MPLS Configuration Guide, Release 5.x

Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 4.1

Cisco Nexus 7000 Series NX-OS OTV Configuration Guide

Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.1

Cisco Nexus 7000 Series NX-OS FabricPath Configuration Guide

Cisco Nexus 7000 Series NX-OS Software Upgrade and Downgrade Guide, Release 4.1

Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.1

Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide, Release 4.1

Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.1

Cisco NX-OS FCoE Configuration Guide

Configuring the Cisco Nexus 2000 Series Fabric Extender

Cisco Nexus 7000 Series NX-OS XML Management Interface User Guide, Release 4.1

Cisco MDS 9000 Family and Nexus 7000 Series NX-OS System Messages Reference, Release 4.1

Cisco Nexus 7000 Series NX-OS MIB Quick Reference

NX-OS Command References

Cisco Nexus 7000 Series NX-OS Command Reference Master Index, Release 4.1

Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference, Release 4.1

Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 4.1

Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 4.1

Cisco Nexus 7000 Series NX-OS Quality of Service Command Reference, Release 4.1

Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 4.1

Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference, Release 4.1

Cisco Nexus 7000 Series NX-OS MPLS Command Reference

Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.1

Cisco Nexus 7000 Series NX-OS OTV Command Reference

Cisco Nexus 7000 Series NX-OS Virtual Device Context Command Reference, Release 4.1

Cisco Nexus 7000 Series NX-OS FabricPath Command Reference

Cisco Nexus 7000 Series NX-OS System Management Command Reference, Release 4.1

Cisco NX-OS FCoE Command Reference

Other Software Document

Cisco Nexus 7000 Series NX-OS Troubleshooting Guide, Release 4.x

Obtaining Documentation and Submitting a Service Request

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

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

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

CHAPTER 1

Overview

This document provides a quick reference of recommended best practices for managing a Cisco Nexus 7000 Series switch using the Cisco NX-OS command-line interface (CLI). This document includes configuration best practices and procedural recommendations for the most common protocols and features deployed in production networks. It is intended to supplement the Cisco Nexus 7000 Series Switches product documentation that is available on cisco.com and should not be used as a replacement for that documentation.

This document is organized in feature specific chapters to add structure and clarity when protocols and features are related to each other. It is important to understand that the recommended best practices do not need to be implemented simultaneously or in any particular order. Not all best practice recommendations are applicable to every network environment.

CHAPTER 2

Initial Configuration

This chapter provides Cisco NX-OS best practices that are that typically configured when a Cisco Nexus 7000 Series switch is powered up for the first time and the user is connected to the RS-232 console port on the active supervisor module.

This chapter includes the following sections:

Setup Utility (First Time Setup)

Introduced: Cisco NX-OS Release 4.0(1)

The Setup Utility is automatically executed when a Cisco Nexus 7000 chassis is powered up for the first time, or if the configuration is erased with the **write erase** command, and the chassis is reloaded (The Setup Utility can also be manually executed any time using the **setup** Exec command). The Setup Utility was created to assist the administrator with some initial configuration parameters, but is not required and can be bypassed if the administrator chooses to do so. The following table contains the parameters that can be configured using the Setup Utility. If the Setup Utility is bypassed, the value in the Default Value column will be automatically configured. The Initial Startup Parameters are always required.

Table 2-1 Required Initial Startup Parameters

Initial Startup Parameter (Required)	Default Value
Enforce Secure Password Standard	yes
Admin Password	no default

Table 2-2 Optional Startup Utility

Startup Utility (Optional)	Default Value
Create another login account	no
Configure read-only SNMP community string	no

Table 2-2 Optional Startup Utility (continued)

Startup Utility (Optional)	Default Value
Configure read-write SNMP community string	no
Enter switch name	no default
Enable License Grace Period	no
Out-of-band (mgmt0) management configuration	yes
Mgmt0 IPV4 address	no default
Mgmt0 IPv4 netmask	no default
Configure the default gateway	yes
IPv4 address of the default gateway	no default
Configure advanced IP options	no
Enable Telnet service	no
Enable SSH service	yes
Type of SSH Key (dsa/rsa)	RSA
Number of RSA Key bits	1024
Configure the NTP server	no
Configure the Default Interface Layer (L3/L2)	L3
Configure the default switchport interface state (shut/no shut)	shutdown
Configure best practices CoPP profile (strict/moderate/lenient/none)	strict
Configure CMP processor on current sup (Slot 5)	yes
CMP IPv4 address	no default
IPv4 address of the default gateway	no default
Configure CMP processor on current sup (Slot 6)	yes
CMP IPv4 address	no default
IPv4 address of the default gateway	no default

Global Configuration Parameters

This section provides Cisco NX-OS best practices that are recommended when configuring global parameters related to general system management.

Terminal CLI Access (SSHv2)

Introduced: Cisco NX-OS Release 4.0(1)

Cisco NX-OS software supports SSHv2 and Telnet for remote terminal CLI access. SSHv2 is enabled by default and is preferred since it increases security with encryption. If SSHv2 is disabled, it can be enabled with the **feature ssh** command (The **feature ssh** command is not displayed in the

running-configuration when it is enabled). SSHv2 uses a 1024 bit RSA key by default. The **ssh key** command can be used to create a new or stronger RSA/DSA key. If a key is already configured, the **force** option can be used to overwrite the existing key.

```
n7000(config)# feature ssh
n7000(config)# ssh key rsa 2048
```

Note In Cisco NX-OS Release 4.0(1) SSHv2 was enabled with the **service ssh** command. It was changed to **feature ssh** in Cisco NX-OS Release 4.1(2).

Hostname

Introduced: Cisco NX-OS Release 4.0(1)

A recognizable hostname should be configured to identify the Cisco Nexus 7000 Series device when administrators access the CLI. If Virtual Device Contexts (VDCs) are configured, a unique hostname should be configured per VDC.

```
n7000(config)# hostname N7K-1-Core-L3
```

Boot Variables

Introduced: Cisco NX-OS Release 4.0(1)

Boot variables specify what version of Cisco NX-OS software boots after a system has been reloaded. The boot variables should always be configured to ensure the expected version of Cisco NX-OS software is booted if an unplanned chassis reload occurs. A kickstart and system image are required to properly boot a Cisco Nexus 7000 Series switch. (The image version numbers have to match.) Cisco NX-OS images can be booted from bootflash: or slot0: (bootflash: is recommended since the memory cannot be removed from the supervisor module). In the following example, Cisco NX-OS Release 5.1(1) kickstart and system boot variables are configured for both supervisor modules in the chassis (default behavior) since the **sup-1** and **sup-2** options have been omitted.

```
n7000(config)# boot kickstart bootflash:n7000-s1-kickstart.5.1.1.bin
n7000(config)# boot system bootflash:n7000-s1-dk9.5.1.1.bin
```

MOTD Login Banner

Introduced: Cisco NX-OS Release 4.0(1)

A Message Of The Day (MOTD) login banner is recommended to notify users they are attempting to log into a device. This banner will be displayed prior to the user authentication process and serves as a warning to deter unauthorized users from attempting to log in. The end delimiter character cannot be used within the contents of the banner. The following example uses a capital Z. (Production devices should have a more detailed disclaimer.)

```
n7000(config)# banner motd Z
Enter TEXT message. End with the character 'Z'.
> Authorized Access Only!
> Z
n7000(config)#
```

Password Strength-Check

Introduced: Cisco NX-OS Release 4.1(2)

The Password Strength-Check feature is enabled by default to force users to configure secure passwords when configuring users in the local database for authentication. We recommend that you keep the Password Strength-Check feature enabled. If it is disabled, it can be enabled with the following global configuration command.

```
n7000(config)# password strength-check
```

Power Budget

Introduced: Cisco NX-OS Release 4.0(1)

The power budget can be monitored and managed using the **show environmental power** command. Cisco NX-OS Release 5.0(2a) introduced real-time power draw for the fan trays and all I/O modules released in Cisco NX-OS Release 5.x software. The configured power redundancy mode determines how the available power is allocated (See the next section for details on the power redundancy mode.)

```
n7000# show environment power
pow_reserved 4800
Power Supply:
Voltage: 50 Volts
Power                                  Actual        Total
Supply    Model                        Output     Capacity    Status
                                      (Watts )     (Watts )
-------  -------------------  -----------  -----------  --------------
1        N7K-AC-6.0KW               786 W       6000 W     Ok
2        N7K-AC-6.0KW               830 W       6000 W     Ok
3        ------------                 0 W          0 W     Absent

                                       Actual        Power
Module    Model                         Draw    Allocated    Status
                                      (Watts )     (Watts )
-------  -------------------  -----------  -----------  --------------
3        N7K-M108X2-12L             395 W        650 W    Powered-Up
4        N7K-M108X2-12L             382 W        650 W    Powered-Up
5        N7K-SUP1                   N/A          210 W    Powered-Up
6        N7K-SUP1                   N/A          210 W    Powered-Up
Xb1      N7K-C7010-FAB-1            N/A           60 W    Powered-Up
Xb2      N7K-C7010-FAB-1            N/A           60 W    Powered-Up
Xb3      N7K-C7010-FAB-1            N/A           60 W    Powered-Up
Xb4      N7K-C7010-FAB-1            N/A           60 W    Powered-Up
Xb5      N7K-C7010-FAB-1            N/A           60 W    Powered-Up
fan1     N7K-C7010-FAN-S            116 W        720 W    Powered-Up
fan2     N7K-C7010-FAN-S            116 W        720 W    Powered-Up
fan3     N7K-C7010-FAN-F             11 W        120 W    Powered-Up
fan4     N7K-C7010-FAN-F             11 W        120 W    Powered-Up

N/A - Per module power not available

Power Usage Summary:
--------------------
Power Supply redundancy mode (configured)              Redundant
Power Supply redundancy mode (operational)             Redundant

Total Power Capacity (based on configured mode)             6000 W
Total Power of all Inputs (cumulative)                     12000 W
Total Power Output (actual draw)                            1616 W
```

Power Redundancy Mode

Introduced: Cisco NX-OS Release 4.0(1)

The recommended power redundancy mode will vary per Cisco Nexus 7000 Series chassis depending on the number of power supplies and the number of inputs and associated input voltage (110v/220v). Each redundancy mode provides different power allocations to allow the administrator to select the mode that is best suited for their installation. The default mode is **ps-redundant,** which is recommended for most installations. Use caution when configuring **combined** mode, since power redundancy will not be available for the chassis.

Table 2-3 Power Redundancy Mode

Redundancy Mode	Description
combined	This mode does not provide power redundancy for the chassis – All input power is available to the chassis. (Power is not reserved for backup as with the other modes)
insrc-redundant	Input Source (GRID) Redundancy – The available power is based on the lesser of the two grids through the power supplies. The difference (50%) is reserved for backup.
ps-redundant	Power Supply Redundancy – Provides an extra power supply in the event one fails or is removed from the chassis.
redundant	Input Source (GRID) + Power Supply Redundancy – The available power is the lesser of the available power for the power supply mode and input source voltage. The difference (50%) is reserved for backup.

```
n7000(config)# power redundancy-mode redundant
```

Powering Off Unused I/O and Fabric Modules

Introduced: Cisco NX-OS Release 4.0(1)

We recommend that you power off all I/O (Ethernet) and fabric modules that are not in use to reduce unnecessary power draw. We also recommend that you power off all I/O and fabric modules slots that are not installed to give the administrator control when powering them up. This reduces risk by preventing newly installed modules from powering up outside of a change control window.

```
n7000(config)# poweroff module 1
n7000(config)# poweroff xbar 4

n7000(config)# poweroff module 3
NOTICE: module <3> status is either absent or not powered up (or denied)... Proceeding
anyway
```

Cisco NX-OS Licensing

This section contains a brief explanation of the Cisco NX-OS licensing model and installation procedure. Always install all required licenses to avoid unnecessary network outages that can occur if a licensed feature is enabled and the grace period expires.

Installation Process

Introduced: Cisco NX-OS Release 4.0(1)

The Cisco NX-OS licensing model allows features to be enabled on a pay as you grow basis. When you purchase a Cisco NX-OS license, you obtain a license file based on the chassis host ID that gets installed on a specific chassis. (Cisco NX-OS software allows Layer-2 connectivity with basic Layer-3 functionality by default.) If you do not have a license for a specific feature, a 120-day grace period can be enabled using the global **license grace-period** configuration command. (The grace period is not recommended for production networks.) After 120 days, all features that are enabled that require a license that is not installed on the chassis are automatically removed from the running-configuration.

See the latest Cisco Nexus 7000 Series Licensing Configuration Guide for a list of features that are included with each license type.

When two supervisor modules are installed in a chassis, the chassis is the only component that requires a new license to be reissued and reinstalled if it is replaced. All other components including a supervisor module can be replaced without having to reissue or reinstall the license. If only one supervisor module is installed in a chassis, a new license will have to be reinstalled from a backup copy if the supervisor module or the chassis is replaced.

Licenses are installed per chassis in the default VDC (1). Installing a license is a non-disruptive procedure.

Summary Installation Steps:

1. Obtain the chassis host ID, which is used to generate the license, by entering the **show license host-id** command**.**
2. Locate the Product Authorization Key (PAK) and go to the Product License Registration web page on cisco.com
3. Follow the instructions to generate the license file and download it.
4. Transfer the license file the Cisco Nexus 7000 Series supervisor module (i.e. bootflash: or slot0:)
5. Install the license using the following **install license** Exec command.

```
n7000# install license bootflash:license_file.lic
Installing license  ..done
```

Verifying the License Status

Introduced: Cisco NX-OS Release 4.0(1)

The Cisco NX-OS license status can be verified using the following command.

```
n7000# show license usage
Feature                      Ins  Lic   Status Expiry Date Comments
                                 Count
--------------------------------------------------------------------------------
SCALABLE_SERVICES_PKG         No    -   Unused             -
TRANSPORT_SERVICES_PKG        No    -   Unused             -
LAN_ADVANCED_SERVICES_PKG     No    -   Unused             -
LAN_ENTERPRISE_SERVICES_PKG   No    -   Unused             -
--------------------------------------------------------------------------------
```

Backing Up a License File

Introduced: Cisco NX-OS Release 4.0(1)

You should always keep your license files in a safe location in the event they have to be reinstalled. If you don't have a license file for a particular chassis, you can create a backup copy for the chassis if it already has the license installed. Once the backup file is created, it should be transferred to safe location.

```
n7000# copy licenses bootflash:license_file.tar
Backing up license done
```

CHAPTER 3

Connecting to the Management Network and Securing Access

This chapter provides Cisco NX-OS recommended best practices for connecting a Cisco Nexus 7000 Series switch to the management network(s) and securing access to the CLI.

This chapter includes the following sections:

Out-of-Band Management Connectivity

A Nexus 7000 is typically managed using a combination of different connectivity methods that give the network administrator CLI access and the ability to manage the chassis using IP management protocols such as SNMP, Syslog and NTP. The following table illustrates the different connectivity methods available to manage a Nexus 7000 chassis. We recommend that you manage a chassis using a combination of out-of-band methods to separate the management traffic from the production traffic. This approach improves security by preventing Denial of Service (DoS) attacks originated from malicious users, or inadvertently by traffic over-subscription.

It is important to understand the functionality that the supervisor module CMP port provides. The CMP port provides lights-out CLI console access to the supervisor module over an IP network using SSHv2 or Telnet. The CMP port allows an administrator to attach to the console, monitor the console, reload the supervisor module or the entire chassis. It does not provide in-band management capabilities for IP protocols like SNMP or NTP.

Table 3-1 Connectivity Options for Port Types and Module Types

Connectivity Options	Port Type	Module Type
Out-of-band (RS-232 Serial CLI)	Console port (recommended)	Supervisor
	Auxiliary port	Supervisor

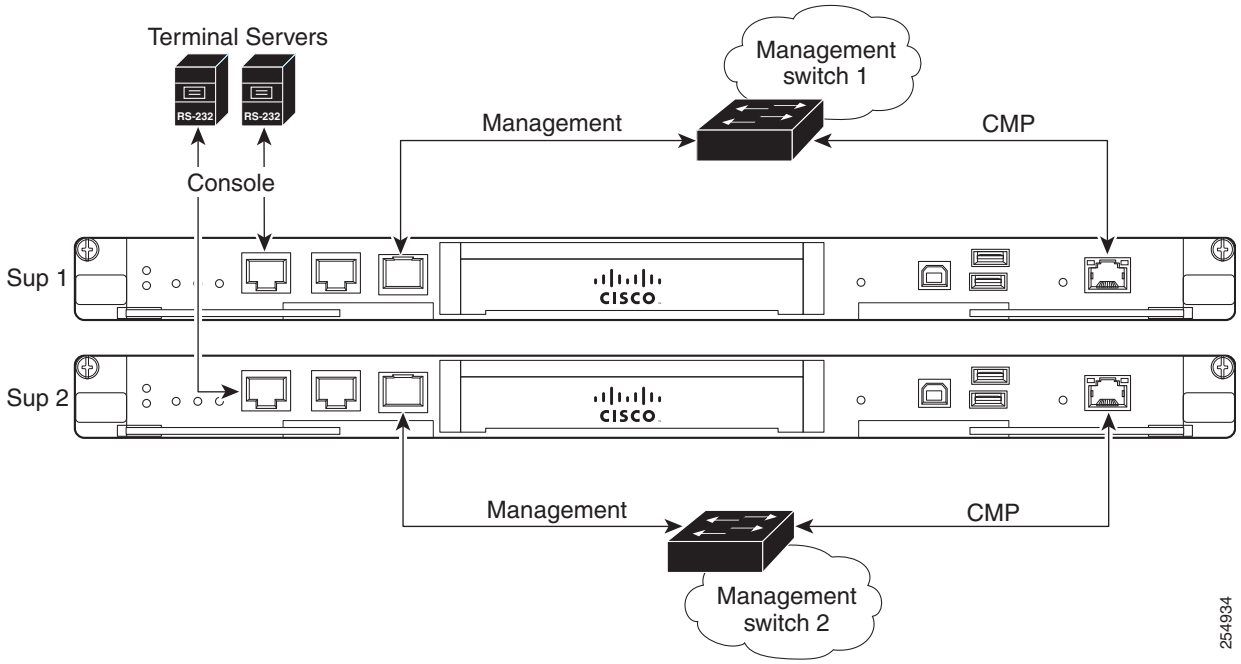
Table 3-1 Connectivity Options for Port Types and Module Types

Connectivity Options	Port Type	Module Type
Out-of-band (SSH/Telnet CLI)	Connectivity Management Port (CMP) recommended	Supervisor
Out-of-band (SSH/Telnet CLI and IP Mgmt)	Management port (mgmt0) recommended	Supervisor
In-band (SSH/Telnet CLI and IP Mgmt)	Ethernet/Loopback/SVI, etc.	I/O module

To reduce the likelihood for loosing connectivity to a Nexus 7000 with two supervisor modules, we recommend connecting the console port, CMP, and the management port per supervisor module.

The console ports should be connected to two different terminal servers and the supervisor CMP and mgmt0 ports should be connected to a redundant out-of-band Ethernet network to improve availability and security. The following diagram illustrates the connectivity required per chassis with redundant supervisor modules.

Figure 3-1 Connectivity per Chassis with Redundant Supervisor Modules



Note In this out-of-band management design, the CoPP policy should be modified to deny in-band management protocols if there are any IP addresses configured on I/O module ports such as Ethernet, loopbacks, port channels, SVIs, etc.

Note This is just a basic example. Redundant network management designs are beyond the scope of this document.

Console Port Configuration

This section contains Cisco NX-OS recommended best practices for the console port.

Exec-Timeout

Introduced: Cisco NX-OS Release 4.0(1)

The console port should be configured with a timeout to automatically log off administrators who are idle for a specified time period. The console **exec-timeout** is disabled by default. A ten or fifteen minute timeout is usually acceptable for most security policies.

```
n7000(config)# line console
n7000(config-console)# exec-timeout 10
```

Port Speed

Introduced: Cisco NX-OS Release 4.0(1)

The console port speed (baud rate) should be increased to the largest value supported by the connected terminal server. The console speed defaults to 9,600 bps and can be configured up to 115,200 bps. A larger value will improve the user experience by increasing the speed that data is displayed on the console port.

```
n7000(config)# line console
n7000(config-console)# speed 115200
```

VTY Port Configuration

This section contains Cisco NX-OS recommended best practices for the VTY (Terminal) port configuration used for SSHv2 and Telnet sessions.

Exec-Timeout

Introduced: Cisco NX-OS Release 4.0(1)

The VTY port should be configured with a timeout to automatically log off users that are idle for a specified time period. The VTY **exec-timeout** is disabled by default. A ten or fifteen minute timeout is usually acceptable for most security policies.

```
n7000(config)# line vty
n7000(config-line)# exec-timeout 10
```

Session Limit

Introduced: Cisco NX-OS Release 4.0(1)

The VTY session limit determines how many SSHv2 sessions, Telnet sessions, or both that can be active simultaneously. The session-limit defaults to 32 active sessions. This should be reduced to a more practical limit such as 5 or 10 sessions to improve security.

```
n7000(config)# line vty
n7000(config-line)# session-limit 5
```

Access-List

Introduced: Cisco NX-OS 5.1(1)

An access class should be applied to the VTY port to increase security by restricting SSH and Telnet access to specific source and destination IP addresses. An access class configured on the VTY port is applicable when using an in-band or out-of-band management strategy. An access-class is configured per traffic direction, **in** applies to inbound sessions and **out** applies to outbound sessions.

Statistics can be enabled with the access list **statistics per-entry**. The following example illustrates a basic policy that permits SSH traffic from a specific subnet to all IP addresses configured in the current VDC. All traffic is permitted if an access-class is applied to the VTY port and the associated access-list is deleted from the configuration.

```
n7000(config)# ip access-list vty-acl-in
n7000(config-acl)# permit tcp x.x.x.x/24 any eq 22

n7000(config)# line vty
n7000(config-line)# ip access-class vty-acl-in in
```

Supervisor Management Port Configuration

This section contains the Cisco NX-OS recommended best practices for the supervisor module mgmt0 port.

Access List

Introduced: Cisco NX-OS Release 4.0(1)

The supervisor module mgmt0 port should be configured with an inbound access list to increase security by restricting access to specific source host/subnet addresses destined to specific management protocols configured on the Nexus 7000. The access-list entries will vary depending on the management protocols that are enabled. Access-list statistics can be tracked per ACL entry if the ACL command **statistics per-entry** is configured. The supervisor module CPU performs access-list processing when an access-list is applied to the mgmt0 port.

```
n7000(config)# ip access-list mgmt0-access
n7000(config-acl)# statistics per-entry
n7000(config-acl)# permit tcp x.x.x.x/x b.b.b.b/32 eq 22
n7000(config-acl)# permit udp x.x.x.x/x b.b.b.b/32 eq snmp
n7000(config-acl)# permit tcp x.x.x.x/x b.b.b.b/32 eq tacacs
n7000(config-acl)# permit udp x.x.x.x/x b.b.b.b/32 eq ntp

n7000(config)# interface mgmt0
n7000(config-if)# ip access-group mgmt0-access in
n7000(config-if)# ip address b.b.b.b/xx
```

Access-List Logging

Introduced: Cisco NX-OS Release 5.0(2a)

Access lists can be configured on the mgmt0 port to collect additional data per entry using the **log** keyword. The access-list logging cache can be displayed to audit the data collected from the logged access-list entry.

```
n7000(config)# ip access-list mgmt0-access
n7000(config-acl)# permit tcp x.x.x.x/x b.b.b.b/32 eq 22 log

n7000# show log ip access-list cache
Source IP        Destination IP     S-Port  D-Port    Interface   Protocol          Hits
-------------------------------------------------------------------------------------
x.x.x.x          x.x.x.x             60741   22        mgmt0      (6)TCP            136


Number of cache entries: 1
-------------------------------------------------------------------------------------
```

Supervisor CMP Port Configuration

This section contains the Cisco NX-OS recommended best practices for configuring the supervisor module Connectivity Management Port (CMP).

Access List

Introduced: Cisco NX-OS Release 4.0(1)

The supervisor module CMP port should be configured with an access list to increase security by restricting access to specific source host/subnets addresses destined to specific management protocols enabled on the CMP port. SSHv2 is typically the only protocol required on the CMP port. Use the **attach cmp** command to configure the CMP port with an access-list.

```
n7000-cmp5(config)# ip access-list cmp-access
n7000-cmp5(config-acl)# permit tcp x.x.x.x 0.0.0.0 range 1024 65535 b.b.b.b 0.0.0.0 range 22 22

n7000-cmp5(config)# interface cmp-mgmt
n7000-cmp5(config-if)# ip address b.b.b.b/xx
n7000-cmp5(config-if)# ip access-group cmp-access in
```

Note The access-list syntax on the CMP port differs from the Cisco NX-OS access-list syntax.

CHAPTER 4

Protecting the CPU

This chapter provides the recommended best practices for protecting the CPU against Denial of Service (DoS) attacks.

This chapter includes the following sections:

CoPP Policy

This section contains a brief overview of the Control Plane Policing (CoPP) Policy. The CoPP policy is an important security feature that prevents Denial of Service (DoS) attacks that can impact the supervisor module CPU. The Cisco NX-OS software defaults to a “strict” policy that was developed to protect the CPU from the most common threats. We recommend that you enable a CoPP policy any time IP addresses are configured on an I/O module port such as an Ethernet port, SVI, port-channel, etc. A detailed explanation and recommendation for the CoPP Policy is outside the of scope for this document.

Denying In-Band Management Protocols

Introduced: Cisco NX-OS Release 4.0(1)

While this document does not cover the CoPP policy in detail, we recommend that you modify the CoPP policy to drop in-band management traffic destined to the Cisco Nexus 7000 Series switches to increase security. If all IP management traffic is traversing the out-of-band management network, there should not be any need to receive any IP management traffic in-band. The CoPP policy does not get applied to traffic received on the mgmt0 interface.

Recommended steps:

1. Identify the enabled management protocols that should have their traffic dropped in-band, such as SSHv2, SNMP, SCP, TFTP, FTP, etc.
2. Create a new access control list(s) and a new class map(s), or reference the existing class map with the **class-map type control-plane match-any copp-system-class-management** command that references existing access control lists.
3. Insert the new class map or modify the existing class map identified in step 2 in the existing CoPP service policy (copp-system-policy), and then configure it to drop all traffic that conforms to the policy.

This example uses the existing **copp-system-class-management** class-map and associated ACLs. The police rate was modified to aggressively drop traffic that conforms to the policy.

```
n7000(config)# policy-map type control-plane copp-system-policy
n7000(config-pmap)# class copp-system-class-management
n7000(config-pmap-c)# police 1 conform drop
```

Note As of Cisco NX-OS Release 5.1(1), the default **copp-system-class-management** class map contains the following protocols: FTP, NTP, NTP6, RADIUS, SFTP, SNMP, SSH, SSH6, TACACS, Telnet, TFTP, TFTP6, RADIUS, TACACS6, and Telnet6.

Syslog Message Thresholds

Introduced: Cisco NX-OS Release 5.1(1)

A Syslog message threshold can be configured per CoPP class map under the control plane policy map. We recommend that you configure a Syslog message threshold for class maps as a method to inform the proper personnel that the CoPP policy is dropping traffic. The following example configures a threshold at 39,600 kb/s with a severity level of 5, so packet drops within the critical class (routing protocols) are logged.

```
n7000(config)# policy-map type control-plane copp-system-policy
n7000(config-pmap)# class copp-system-class-critical
n7000(config-pmap-c)# logging drop threshold 39600000 level 5
```

Syslog Message Example:

```
n7000# show log logfile

%COPP-5-COPP_DROPS5: CoPP drops exceed threshold in class: copp-system-class-critical,
check show policy-map interface control-plane for more info.
```

CPU Rate Limit Logging

Introduced: Cisco NX-OS Release 5.1(1)

This section was included for reference and may not be required.

Rate limiting can be configured globally and per interface to create a system log message if packets sent to or from the supervisor module CPU exceed the configured packet per second (pps) threshold. The rate limiter can be configured to measure traffic based on direction using the **input** (received), **output** (transmitted) or **both** (configures received and transmitted simultaneously) options. The global default threshold is 10,000 pps configured for **both**. The threshold can be modified to a value between 0 and 100,000 pps. This feature can be applied globally and per interface. This feature does not drop packets; it only sends a notification log message.

Global Configuration:

```
n7000(config)# rate-limit cpu direction both pps 2000 action log
```

Per Interface Configuration:

```
n7000(config)# interface ethernet 1/26
n7000(config-if)# rate-limit cpu direction both pps 2000 action log
```

Verification:

```
Global Verification:

n7000# show system internal pktmgr internal control sw-rate-limit
inband pps global threshold 2000  outband pps global threshold 2000
```

Per Interface Verification:

```
n7000# show system internal pktmgr interface ethernet 1/26
Ethernet1/26, ordinal: 305
  SUP-traffic statistics: (sent/received)
    Packets: 5412033 / 6677105
    Bytes: 1614312187 / 2003104556
    Instant packet rate: 2872 pps / 2871 pps
    Packet rate limiter (Out/In): 2000 pps / 2000 pps
    Average packet rates(1min/5min/15min/EWMA):
    Packet statistics:
      Tx: Unicast 5365387, Multicast 46640
          Broadcast 6
      Rx: Unicast 6677093, Multicast 0
          Broadcast 12
```

Syslog:

```
n7000# show log logfile

%NETSTACK-5-NOTICE:  netstack [3647]  Ingress PPS (2861) exceeding threshold on i/f
Ethernet1/26
```

CHAPTER 5

Integrated Intrusion Detection Security

The Cisco NX-OS software provides IPv4 and IPv6 Intrusion Detection packet checks to increase security in the network by dropping packets that match specific criteria that are typically not required in most production networks. Most Intrusion Detection System (IDS) packet checks are enabled by default and should be left enabled unless there is a specific reason to disable them.

This chapter includes the following sections:

Verifying IDS Check Status and Counters

Introduced: Cisco NX-OS Release 4.0(1)

The **show hardware forwarding ip verify** command should be used to verify the IDS packet check status and associated counters. The **module** option displays counters for a specific module as opposed to all modules. The "Packets Failed" counter displays the number of packets dropped for each IDS packet check. This output can be useful when troubleshooting potential network related application issues. In some rare situations, an IDS packet check may need to be disabled if an application meets the IDS packet check criteria. Cisco NX-OS Release 5.0(3) introduced Syslog messages and Embedded Event Manager (EEM) trigger support when packets are dropped. The IDS packet check counters can be cleared using the **clear hardware forwarding ip verify protocol** command. The **module** option allows the administrator to clear the counters for a specific module.

```
n7000# show hardware forwarding ip verify

IPv4 and v6 IDS Checks          Status     Packets Failed
------------------------------+---------+------------------
address source broadcast        Enabled    0
address source multicast        Enabled    0
address destination zero        Enabled    0
address identical               Enabled    0
address reserved                Enabled    0
address class-e                 Disabled   --
checksum                        Enabled    0
protocol                        Enabled    0
fragment                        Disabled   --
length minimum                  Enabled    0
length consistent               Enabled    0
length maximum max-frag         Enabled    0
length maximum udp              Disabled   --
length maximum max-tcp          Enabled    0
```

```
tcp flags                      Disabled   --
tcp tiny-frag                  Enabled    0
version                        Enabled    0
-----------------------------+---------+------------------
IPv6 IDS Checks                Status     Packets Failed
-----------------------------+---------+------------------
length consistent              Enabled    0
length maximum max-frag        Enabled    0
length maximum udp             Disabled   --
length maximum max-tcp         Enabled    0
```

Disabling/Enabling IDS Packet Checks

Introduced: Cisco NX-OS Release 4.0(1)

This section was included for reference and may not be required.

There may be some situations when an IDS packet check needs to be disabled for an application to function properly. The following global command can be used to disable and enable a packet check. This example disables and enables the “length maximum max-tcp” IDS check. Other packet checks can be configured using the same procedure.

```
n7000(config)# no hardware ip verify length maximum max-tcp

n7000(config)# hardware ip verify length maximum max-tcp
```

CHAPTER 6

Cisco NX-OS Software Upgrade or Downgrade

This chapter provides the Cisco NX-OS best practices for upgrading and downgrading Cisco NX-OS system software. The Cisco NX-OS system software can be upgraded or downgraded using two different methods. The In-Service-Software-Upgrade (ISSU) is the recommended procedure, especially when performing a nondisruptive upgrade for a chassis that has two supervisor modules installed. However, the traditional method is documented as well since it is applicable to lab environments and production environments that may require a fast downgrade.

This chapter includes the following sections:

Recommended Upgrade Procedure (ISSU)

Introduced: Cisco NX-OS Release 4.0(1)

An In-Service-Software-Upgrade (ISSU) allows a Nexus 7000 with two supervisor modules to be upgraded or downgraded with a single command. It automatically changes the boot variables, performs a compatibility check, and prompts the administrator to continue once he or she has verified the expected outcome. Once the process starts, it upgrades the system software seamlessly without any downtime. The chassis continues to forward packets (hitless) throughout the process while the individual chassis components are upgraded. The upgrade or downgrade time will vary (30 – 50 minutes) depending on the chassis type and how many modules are installed. The CMP port on each supervisor module will require a manual reload to complete the process. This manual step prevents users from being disconnected if they are monitoring the procedure from the CMP ports.

For best results, follow these recommendations:

- Connect to both supervisor modules' console or CMP ports if you want to monitor the entire upgrade (which we recommend you do).
- Only perform ISSU upgrades in stable environments where there are no link flaps, STP state changes, etc.
- You cannot perform an ISSU if a Session Manager session is active. The active session must be committed, aborted, or saved.

```
n7000# install all kickstart bootflash:n7000-s1-kickstart.5.1.1.bin system
bootflash:n7000-s1-dk9.5.1.1.bin

n7000# reload cmp module 5
```

```
n7000# reload cmp module 6
```

Note This procedure can be used for a chassis with one supervisor module, but the process is disruptive because the chassis requires a reload.

Verifying Software Compatibility (ISSU and Chassis Reload)

Introduced: Cisco NX-OS Release 4.0(1)

Before downgrading software, verify if there are any incompatibilities to make sure features can be properly disabled before performing the downgrade. This will inform the administrator if there are any features that will be automatically removed from the configuration and allow the administrator to take action prior to the downgrade. This command should be run regardless if the ISSU or traditional downgrade method is performed.

```
n7000# show incompatibility-all system bootflash:n7000-s1-dk9.4.2.4.bin

Checking incompatible configuration(s) for vdc 'n7000':
------------------------------------------------------------

<CLI Output Omitted>

6) Service : otv , Capability : CAP_FEATURE_OTV
Description : Overlay Transport Virtualization
Capability requirement : STRICT
Disable command : no feature otv

7) Service : bfd , Capability : CAP_FEATURE_BFD_V2
Description : Feature bfd is enabled.
Capability requirement : STRICT
Disable command : Disable bfd using"no feature bfd"

<CLI Output Omitted>
```

Traditional Upgrade or Downgrade Procedure (Chassis Reload)

Introduced: Cisco NX-OS Release 4.0(1)

The traditional upgrade procedure is documented because it is recommended for these specific scenarios:

- In lab environments where continuous uptime is not a requirement
- In production environments in the unlikely event that an upgrade needs to be downgraded in a timely manner
- In situations where ISSU or ISSD is not supported for the respective images

Before you begin, save and back up all configurations before reloading the system to load the new software. Follow these steps to upgrade the Cisco NX-OS software:

1. Configure the boot variable for the Cisco NX-OS software kickstart image.

   ```
   n7000# boot kickstart bootflash:n7000-s1-kickstart.5.2.1.bin
   ```

2. Configure the boot variable for the Cisco NX-OS software system image.

   ```
   n7000# boot system bootflash:n7000-s1-dk9.5.2.1.bin
   ```

3. Save the running configuration to the startup configuration.

```
n7000# copy running-config startup-config vdc-all
```

4. Verify that the "Current Boot Variables" and the "Boot Variables on next reload" match the expected image.

```
n7000# show boot

Current Boot Variables:

sup-1
kickstart variable = bootflash:/n7000-s1-kickstart.5.2.1.bin
system variable = bootflash:/n7000-s1-dk9.5.2.1.bin

Boot Variables on next reload:

sup-1
kickstart variable = bootflash:/n7000-s1-kickstart.5.2.1.bin
system variable = bootflash:/n7000-s1-dk9.5.2.1.bin
```

5. Verify that the image location matches the above boot statements. In redundant supervisor chassis, the images auto-synchronize from active to standby once the boot statements are set.

```
n7000# show boot auto-copy list

n7000# dir bootflash://sup-active/

  161980383    Aug 15 17:52:03 2011  n7000-s1-dk9.5.2.1.bin

   29471232    Aug 15 18:01:38 2011  n7000-s1-kickstart.5.2.1.bin

n7000# dir bootflash://sup-standby/

  161980383    Aug 15 18:04:55 2011  n7000-s1-dk9.5.2.1.bin

   29471232    Aug 15 18:06:18 2011  n7000-s1-kickstart.5.2.1.bin
```

6. After you verify the image location and statements, reload the Cisco NX-OS device.

```
n7000# reload
```

CHAPTER 7

EPLD Software Upgrade or Downgrade

This chapter contains the recommended procedure for upgrading or downgrading an electronic programmable logic device (EPLD). EPLDs are hardware components such as ASICs on I/O modules that can be upgraded without having to replace the hardware. EPLD upgrades are typically not required, but in some cases, such as new chassis installs or chassis redeployments, we recommend that you upgrade to the latest EPLD version to ensure that all upgradable hardware components have the latest feature enhancements and caveat fixes.

This chapter includes the following sections:

EPLD Upgrade/Downgrade Verification

Introduced: Cisco NX-OS Release 4.2(6)

Before starting an EPLD upgrade, an upgrade verification check should be performed on the chassis to understand what EPLD upgrades are required and the impact that each upgrade will have. This will assist in planning when determining if any of the upgrades will impact production traffic that could create an unnecessary network outage.

```
n7000# show install all impact epld bootflash:n7000-s1-epld.5.1.1.img

Compatibility check:
Module  Type  Upgradable        Impact   Reason
------  ----  ----------    ----------   ------
     1    LC         Yes    disruptive   Module Upgradable
     2    LC         Yes    disruptive   Module Upgradable
     4    LC          No          none   Module is not Online
     5   SUP         Yes    disruptive   Module Upgradable
     7    LC         Yes    disruptive   Module Upgradable
     8    LC         Yes    disruptive   Module Upgradable
     9    LC         Yes    disruptive   Module Upgradable
    10    LC         Yes    disruptive   Module Upgradable
     1  Xbar         Yes    disruptive   Module Upgradable
     2  Xbar         Yes    disruptive   Module Upgradable
     3  Xbar         Yes    disruptive   Module Upgradable
     1   FAN         Yes    disruptive   Module Upgradable
     2   FAN         Yes    disruptive   Module Upgradable
     3   FAN         Yes    disruptive   Module Upgradable
     4   FAN         Yes    disruptive   Module Upgradable

Retrieving EPLD versions... Please wait.
```

```
Images will be upgraded according to following table:

Module  Type           EPLD      Running-Version   New-Version  Upg-Required
------  ----  -------------      ---------------   -----------  ------------
     1    LC  Power Manager              4.008       4.008           No
     1    LC  IO                         1.015       1.016           Yes
     1    LC  Forwarding Engine          1.006       1.006           No
     1    LC  FE Bridge(1)             186.005     186.006           Yes
     1    LC  FE Bridge(2)             186.005     186.006           Yes
     1    LC  Linksec Engine(1)          2.006       2.006           No
     1    LC  Linksec Engine(2)          2.006       2.006           No
     1    LC  Linksec Engine(3)          2.006       2.006           No
     1    LC  Linksec Engine(4)          2.006       2.006           No
     1    LC  Linksec Engine(5)          2.006       2.006           No
     1    LC  Linksec Engine(6)          2.006       2.006           No
     1    LC  Linksec Engine(7)          2.006       2.006           No
```

EPLD Upgrade Procedure

Introduced: Cisco NX-OS Release 4.0(1)

This section was included for reference and is typically not required, but we recommend that you read it. Cisco NX-OS software can be upgraded without upgrading to the latest EPLD image. Customers should review the EPLD release notes on cisco.com and determine if they need to upgrade their EPLDs based on new features or caveat fixes. Customers performing a new install may want to upgrade EPLDs to the latest version to reduce the likelihood for having to upgrade EPLDs in the future.

EPLDs are upgraded per component when using the **install** command. Only one component can be upgraded at a time. Upgrading a single component provides granular control to avoid any unnecessary network impact. The ELPD upgrades can take up to 30 minutes per I/O module. The same procedure can be used to downgrade a component, although downgrades are typically not required.

For best results, follow these recommendations:

- Only upgrade the EPLDs on an I/O module that is not passing production traffic. (Redirect traffic before starting the upgrade.)
- To save time, make sure the I/O module being upgraded is not powered off. If the module is powered off, the module will be powered on, and all upgradable components on the module will be updated regardless if they require it. This will take more time to upgrade the I/O module.
- Use the **install all epld** command to start a rolling EPLD upgrade for the entire chassis. This procedure should only be used for non-production chassis, or if the production chassis is not passing any “production” traffic.
- Do not disrupt the upgrade process for a component.

```
n7000# install module 1 epld bootflash:n7000-s1-epld.5.1.1.img

Retrieving EPLD versions... Please wait.

Images will be upgraded according to following table:
Module  Type           EPLD      Running-Version   New-Version  Upg-Required
------  ----  -------------      ---------------   -----------  ------------
     1    LC  Power Manager              4.008       4.008           No
     1    LC  IO                         1.015       1.016           Yes
     1    LC  Forwarding Engine          1.006       1.006           No
     1    LC  FE Bridge(1)             186.005     186.006           Yes
```

```
    1    LC  FE Bridge(2)              186.005      186.006         Yes
    1    LC  Linksec Engine(1)          2.006       2.006           No
    1    LC  Linksec Engine(2)          2.006       2.006           No
    1    LC  Linksec Engine(3)          2.006       2.006           No
    1    LC  Linksec Engine(4)          2.006       2.006           No
    1    LC  Linksec Engine(5)          2.006       2.006           No
    1    LC  Linksec Engine(6)          2.006       2.006           No
    1    LC  Linksec Engine(7)          2.006       2.006           No
    1    LC  Linksec Engine(8)          2.006       2.006           No

Module 1 will be powered down.
Do you want to continue? (yes/no) [n]:
```

CHAPTER 8

Enabling and Disabling Features

Introduced: Cisco NX-OS Release 4.0(1)

Cisco NX-OS software has the ability to enable and disable specific features, such as OSPF and PIM. By default, Cisco NX-OS software enables only those features that are required for initial networking connectivity. This approach optimizes the operating system and increases availability by not running additional processes that are not required.

If a feature is not enabled, the process for that feature is not running, and the configuration and verification (show) commands are not available from the CLI. Once a feature is enabled, the configuration and verification commands can be executed. Depending on the feature, the process will not start until the feature is configured (such as **router ospf 10**). We recommend that you keep the features disabled, or disable them if they are no longer required.

```
n7000# show process | grep ospf
-     NR          -             1     -  ospf

n7000# show process | grep pim
-     NR          -             0     -  pim


n7000(config)# feature ospf
n7000(config)# router ospf 10

n7000(config)# feature pim


n7000# show feature

Feature Name          Instance  State
--------------------  --------  --------
bfd                   1         disabled
bfd_app               1         disabled
bgp                   1         disabled

<CLI Output Omitted>

ospf                  1         enabled
ospf                  2         enabled (not-running)
ospf                  3         enabled (not-running)
ospf                  4         enabled (not-running)
ospfv3                1         disabled
ospfv3                2         disabled
ospfv3                3         disabled
ospfv3                4         disabled
otv                   1         disabled
pbr                   1         disabled
pim                   1         enabled (not-running)
```

```
pim6                  1         disabled

<CLI Output Omitted>

vrrp                  1         disabled
vtp                   1         disabled
wccp                  1         disabled


n7000# show process | grep ospf
9074      S  775d327b            1     -  ospf
```

CHAPTER 9

IP Management

This chapter provides Cisco NX-OS recommended best practices for configuring IP management protocols.

This chapter includes the following sections:

Network Time Protocol (NTP)

We recommend configuring NTP on all network devices so that the timestamps in the logs and other management data are synchronized on all devices. Using NTP is beneficial when correlating network events across the network. Cisco NX-OS supports NTP client mode and peer mode operations.

Redundant NTP Servers

Introduced: Cisco NX-OS Release 4.0(1)

Multiple NTP servers should be configured for redundancy. The primary NTP server should be configured with the **prefer** option, and the VRF instance should be configured to use the management VRF instance for out-of-band connectivity.

```
n7000(config)# ntp server a.a.a.a prefer use-vrf management
n7000(config)# ntp server a.a.a.a use-vrf management

n7000(config)# ntp peer b.b.b.b prefer use-vrf management
n7000(config)# ntp peer b.b.b.b use-vrf management
```

Time zone / Daylight Savings

Introduced: Cisco NX-OS Release 4.0(1)

The clock time zone and daylight savings parameters should be configured if the default values are not desired. If these values are not configured, the clock will default to UTC without daylight savings adjustments.

```
n7000(config)# clock timezone PST -8 0
n7000(config)# clock summer-time PST
```

NTP Source Interface / IP Address

Introduced: Cisco NX-OS Release 4.1(3)

Specifying a NTP source interface or IP address is recommended when using a VRF instance other than the management VRF instance. This allows security devices such as firewalls to identify the source of the NTP packet. It the source interface or IP address is not specified; the primary IP address on the originating (outbound) interface is used. If the NTP traffic is associated to the management VRF instance, the mgmt0 interface IP address is selected. You cannot configure an NTP interface and IP source address simultaneously.

```
n7000(config)# ntp source-interface ethernet 2/1

n7000(config)# ntp source x.x.x.x
```

NTP Logging

Introduced: Cisco NX-OS Release 5.0(2a)

NTP logging is disabled by default. NTP messages can be logged to assist when troubleshooting NTP synchronization issues.

```
n7000(config)# ntp logging
```

MD5 Authentication

Introduced: Cisco NX-OS Release 5.0(2a)

MD5 authentication should be enabled to prevent a device from synchronizing its clock from a rogue NTP server or peer. The same trusted authentication key needs to be configured on the NTP client(s), peer(s), and server(s). An NTP client will not synchronize its clock if it receives an NTP message from an NTP server or peer using a different authentication key.

```
n7000(config)# ntp server a.a.a.a use-vrf management key 1
n7000(config)# ntp peer b.b.b.b use-vrf management key 1

n7000(config)# ntp authentication-key 1 md5 <password>
n7000(config)# ntp trusted-key 1
n7000(config)# ntp authenticate
```

Access Control List

Introduced: Cisco NX-OS Release 5.0(2a)

Access control lists (ACLs) should be configured to increase security by restricting access to specific NTP peers or servers. Collecting ACL statistics with the **statistics per-entry** is optional, but useful when verifying packets are being received from specific NTP peers or servers.

```
n7000(config)# ntp server a.a.a.a use-vrf management
n7000(config)# ntp peer b.b.b.b use-vrf management
n7000(config)# ntp source x.x.x.x
n7000(config)# ntp access-group peer ntp-peers
```

```
n7000(config)# ip access-list ntp-peers
n7000(config-acl)# statistics per-entry
n7000(config-acl)# permit udp a.a.a.a/32 x.x.x.x/32 eq ntp
n7000(config-acl)# permit udp b.b.b.b/32 x.x.x.x/32 eq ntp
```

Simple Network Management Protocol (SNMP)

Cisco NX-OS supports SNMP v1, v2c, and v3. We recommend that you use SNMPv3 to increase security because it has authentication and encryption capabilities for username, passwords, and payload data.

Basic Configuration (Contact/Location)

Introduced: Cisco NX-OS Release 4.0(1)

Specify the contact and location information so the device is identifiable when being polled by the SNMP management servers.

```
n7000(config)# snmp-server contact Cisco Systems
n7000(config)# snmp-server location San Jose, CA
```

Users (Version 3)

Introduced: Cisco NX-OS Release 4.0(1)

SNMPv3 is the recommended SNMP version because of the additional security authentication and encryption mechanisms. By default, all user accounts in the local database are synchronized to a SNMP user that can be used by an SNMP server to authenticate SNMPv3 requests. Additional user accounts/SNMP user accounts can be created for SNMP polling and sending SNMP inform notifications. In the following example the default "admin" user is displayed and another SNMP user called "snmp-user" is created. The Engine-ID only needs to be configured for SNMP users configured to send v3 notifications (The Engine ID value is based on the SNMP notification server's engine ID).

```
n7000# show run snmp

snmp-server user admin network-admin auth md5 0x272298231264cbf31dbd423455345253 priv
aes-128 0x272298231264cbf31dbd423455345253 localizedkey

n7000(config)# snmp-server user snmp-user auth md5 <password> priv aes-128 <password>
engineID 80:00:00:09:03:00:0C:29:13:92:B9
```

Community Strings (Version 1 and 2c)

Introduced: Cisco NX-OS Release 4.0(1)

If an SNMPv3 capable management server is not available, SNMP version 1 and 2c can be enabled using the **snmp-server community** command. SNMP v2c provides additional capabilities beyond SNMPv1. SNMP can be configured for read-only or read-write access. Only enable read-only access (network-operator) to increase security.

```
n7000(config)# snmp-server community <password> group network-operator

n7000(config)# snmp-server community <password> group network-admin
```

Note The **snmp-server community <password> ro** command is automatically converted to the **snmp-server community <password> group network-operator** command. The **snmp-server community <password> rw** command is automatically converted to the **snmp-server <password> group network-admin** command.

Notification / Trap Receivers

Introduced: Cisco NX-OS Release 4.0(1)

SNMP notification receivers should be configured to inform the SNMP network management servers about network events. Receivers can be configured for SNMPv1, SNMPv2c, and SNMPv3 for a specific VRF instance. SNMP v3 is recommended because of the additional authentication and encryption capabilities. SNMPv3 requires an SNMP user that is configured with the SNMP recipients Engine-ID.

Version 3 (Recommended)

```
n7000(config)# snmp-server host x.x.x.x version 3 priv snmp-user
n7000(config)# snmp-server host x.x.x.x use-vrf management
```

Version 2c

```
n7000(config)# snmp-server host x.x.x.x traps version 2c <password>
n7000(config)# snmp-server host x.x.x.x informs version 2c <password>
n7000(config)# snmp-server host x.x.x.x use-vrf management
```

Version 1

```
n7000(config)# snmp-server host x.x.x.x traps version 1 <password>
n7000(config)# snmp-server host x.x.x.x use-vrf management
```

Notification / Trap Events

Introduced: Cisco NX-OS Release 4.0(1)

SNMP Notifications or Traps should be enabled to notify the SNMP management server(s) about important events. Enable all SNMP notifications/traps, or enable specific notifications/traps of interest depending on what features are enabled. Some notifications/traps are enabled by default. Use the **show snmp-server trap** command to verify what traps are enabled. SNMP Notifications or Traps will be sent depending on how the SNMP host recipients are configured.

Enable All Notifications/Traps

```
n7000(config)# snmp-server enable traps
```

Enable Individual Notifications/Traps

```
n7000(config)# snmp-server enable traps feature-control
n7000(config)# snmp-server enable traps callhome smtp-send-fail
n7000(config)# snmp-server enable traps snmp authentication
```

Interface Link-Status Traps

Introduced: Cisco NX-OS Release 4.0(1)

SNMP interface link-status traps are enabled by default. SNMP link-status traps can be disabled per interface. It may be beneficial to disable interface traps in certain environments. However, we always recommend that you keep interface traps enabled for critical infrastructure or server interfaces.

```
n7000(config)# interface ethernet 1/1
n7000(config-if)# no snmp trap link-status
```

Community String Access Control List

Introduced: Cisco NX-OS Release 4.2(1)

Access control lists (ACLs) should always be applied to community strings (SNMP v1 and v2c) to restrict access to specific source and destination IP addresses.

```
n7000(config)# ip access-list snmp-acl
n7000(config-acl)# permit udp host x.x.x.x host x.x.x.x eq snmp

n7000(config)# snmp-server community <password> group network-operator
n7000(config)# snmp-server community <password> use-acl snmp-acl
```

Source Interface

Introduced: Cisco NX-OS Release 4.2(1)

Specify the source interface for **informs** and **traps** if the management VRF instance is not being used. This allows security devices such as firewalls to identify the source of the SNMP packet. If the source interface or IP address is not specified the primary IP address on the originating (outbound) interface is selected. The **inform** feature only applies to SNMP v2c and v3. You can configure the source interface globally for all SNMP hosts or per SNMP host.

Global Configuration:

```
n7000(config)# snmp source-interface informs loopback0
n7000(config)# snmp source-interface traps loopback0
```

Per Server Configuration:

```
n7000(config)# snmp-server host a.a.a.a source-interface loopback0
```

Disabling SNMP

Introduced: Cisco NX-OS Release 4.2(1)

SNMP is enabled by default. However, SNMP v1 and v2c will not respond to SNMP requests unless a community string is configured. SNMPv3 will respond to SNMP requests if the SNMPv3 capable server polls the Cisco Nexus 7000 Series device. (The SNMP user “admin” is configured by default.) If SNMP is not a requirement it should be disabled with the following command to increase security.

```
n7000(config)# no snmp-server protocol enable
```

System Message Logging

Cisco NX-OS software saves system messages to a local log file (log:messages) in DRAM. (The most recent 100 severity 0, 1, or 2 messages are saved in NVRAM.) Cisco NX-OS software also logs system messages to the logflash (logflash://sup-local/log/messages) by default, which provides persistent logging data after a system reload.

Syslog Server

Introduced: Cisco NX-OS Release 4.0(1)

Up to eight Syslog servers can be configured to receive system messages. We recommend that you configure at least two Syslog servers for redundancy and use the management VRF instance for traffic isolation. The severity filter for log messages can be specified per server (the default severity filter is 5). In the following example, two servers are configured with a severity filter of 6. Setting the severity filter to 6 ensures that messages with a severity of 0 (emergency) through 6 (informational) are sent to each server. Selecting the severity filter will depend on how much information should be collected on the servers. We do not recommend configuring a severity filter less than 5.

```
n7000(config)# logging server a.a.a.a 6 use-vrf management
n7000(config)# logging server b.b.b.b 6 use-vrf management
```

Source Interface

Introduced: Cisco NX-OS Release 4.0(1)

If the default VRF instance is used to reach the Syslog server(s), a loopback interface can be specified as the source IP address. This allows security devices such as firewalls to identify the source of the Syslog packet. If a source interface is not specified, the primary IP address of the originating (outbound) interface is selected.

```
n7000(config)# logging source-interface loopback 0
```

Link Status Events

Introduced: Cisco NX-OS Release 4.0(1)

All interface link status (up/down) messages are logged by default. Link status events can be configured globally or per interface. The following global command disables link status logging messages for all interfaces. The interface command enables link status logging messages for a specific interface. This scenario may be beneficial to filter out excessive messages, except for mission critical infrastructure or server interfaces.

```
n7000(config)# no logging event link-status default

n7000(config)# interface ethernet x/x
n7000(config-if)# logging event port link-status
```

Timestamps

Introduced: Cisco NX-OS Release 4.0(1)

System message logging defaults to one-second time units. Timestamps can be configured for millisecond and microseconds for finer granularity. We recommend using timestamps in milliseconds or microseconds when troubleshooting time sensitive issues.

```
n7000(config)# logging timestamp milliseconds
```

Per Feature Severity Level

Introduced: Cisco NX-OS Release 4.0(1)

Cisco NX-OS software supports configured severity levels per feature. We recommend that you configure the severity level for the features that require a higher level of manageability in the network. The following example demonstrates the configuration and verification commands for NTP. The **logging level all <severity #>** command can be used to change the current severity level for all features.

```
n7000(config)# logging level ntp 7

n7000# show logging level ntp
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
ntp                     2                       7

0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)

n7000(config)# logging level all 5
```

Viewing Log File Contents

Introduced: Cisco NX-OS Release 4.0(1)

The following **show logging** commands are useful when viewing and managing system message log files.

```
n7000# show logging logfile  <-  Displays the contents of the default log file.

n7000# show logging last 10  <-  Displays the last # of lines of the default log file.

n7000# show logging NVRAM   <- Displays contents of the log file stored in NVRAM.

n7000# show file logflash://sup-local/log/messages <- Displays contents in logflash.
```

Clearing Log File Contents

Introduced: Cisco NX-OS Release 4.0(1)

The following **clear** commands are useful if it is desirable to clear the contents of the system message log files.

```
n7000# clear logging logfile  <- Clears the contents of the default log file.
```

```
n7000# clear logging nvram    <- Clears the contents of the default log file stored in
NVRAM.
```

Smart Call Home

Smart Call Home provides an automated method for sending standard text e-mail or XML notifications to recipients such as a network operation center (NOC), a specific engineer, or the Cisco TAC to auto-generate a TAC case. Enabling Call Home for both internal and Cisco TAC recipients is recommended to speed up problem resolution.

Internal and Cisco TAC Recipients (Destination-Profiles)

Introduced: Cisco NX-OS Release 4.0(1)

Although Smart Call Home was introduced in Cisco NX-OS Release 4.0(1), the following example is based on Cisco NX-OS Release 5.0(2a) CLI syntax. In this example: Call Home is configured to send a full-text e-mail to two different e-mail servers for redundancy using the management VRF instance for traffic isolation. For the destination profile "Internal-NOC" the mail server a.a.a.a is preferred due to the lower priority. If it does not respond, mail server b.b.b.b will be used.

```
n7000(config)# callhome

n7000(config-callhome)# contract-id Cisco-Contract-#
n7000(config-callhome)# customer-id xyz.com

n7000(config-callhome)# site-id n7000-Kirkland-DC
n7000(config-callhome)# streetaddress 12345 Street NE, Kirkland, WA
n7000(config-callhome)# email-contact Cisco-Customer@xyz.com
n7000(config-callhome)# phone-contact +1-800-123-4567

n7000(config-callhome)# destination-profile Internal-NOC
n7000(config-callhome)# destination-profile Internal-NOC format full-txt
n7000(config-callhome)# destination-profile Internal-NOC email-addr call-home-noc@xyz.com
n7000(config-callhome)# destination-profile Internal-NOC alert-group all

n7000(config-callhome)# destination-profile CiscoTAC-1 email-addr callhome@cisco.com

n7000(config-callhome)# transport email mail-server a.a.a.a priority 10 use-vrf management
n7000(config-callhome)# transport email mail-server b.b.b.b use-vrf management

n7000(config-callhome)# transport email from call-home@xyz.com
n7000(config-callhome)# transport email reply-to call-home@xy.com
```

Note The **transport email snmp-server** command is the original command supported in Cisco NX-OS Release 4.x and NX-OS Release 5. X software. The **transport email mail-server** command was introduced in NX-OS Release 5.0(2a) to add support for multiple servers and priorities.

Testing Call Home Recipients

Introduced: Cisco NX-OS Release 4.0(1)

Always test the Call Home recipients during the initial Call Home configuration to ensure Call Home works as expected.

```
n7000# callhome test
```

CHAPTER 10

Management Tools for Usability

This chapter describes Cisco NX-OS software features that are recommended for managing a device. The topics covered include changing the configuration, verifying the supervisor module status, or replacing hardware.

This chapter includes the following sections:

Implementing Configuration Changes

This section includes recommended procedural best practices when modifying the Cisco NX-OS configuration.

Configuration Rollback

Introduced: Cisco NX-OS Release 4.0(1)

The configuration rollback feature allows an administrator to create configuration checkpoints that allow for a configuration to be easily rolled back in the event the new configuration changes don't operate as expected. We recommend that you use the configuration rollback feature to create a configuration checkpoint prior to making changes in a production network during change-control procedures. This allows the original configuration to be re-applied with one command if there are any unforeseen issues. Beginning in Cisco NX-OS Release 4.2(1) auto-checkpoints are created if a feature is disabled (manually or by license expiration). VDC removal due to license expiration will not generate an auto-checkpoint. Beginning in Cisco NX-OS Release 4.2(1) checkpoints are saved to the standby supervisor as long as they are not created using the **checkpoint file** command. The following example demonstrates the procedure for basic checkpoint and rollback operation.

```
n7000# checkpoint ospf-change-control
.....Done
```

```
n7000(config)# interface ethernet x/x
n7000(config-if)# ip address x.x.x.x/xx
n7000(config-if)# ip router ospf 10 area 0
n7000(config-if)# no shutdown

n7000# show run interface ethernet x/x

interface Ethernetx/x
  ip address x.x.x.x/xx
  ip router ospf 10 area 0.0.0.0
  no shutdown

n7000# rollback running-config checkpoint ospf-change-control
Note: Applying config parallelly may fail Rollback verification
Collecting Running-Config
Generating Rollback Patch
Executing Rollback Patch
Generating Running-config for verification
Generating Patch for verification

n7000# show run interface ethernet x/x
```

Session Manager

Introduced: Cisco NX-OS Release 4.0(1)

Session Manger allows ACL and QoS configurations to be applied to the running-configuration in batch mode. This is useful for verifying hardware resources such as TCAM space is available before applying the configuration. The Session Manager should always be used when applying ACLs or configuring QoS. The following example illustrates the process for configuring, verifying and applying an ACL to an interface.

```
n7000# configure session apply-acl
Config Session started, Session ID is 1
Enter configuration commands, one per line.  End with CNTL/Z.
n7000(config-s)# ip access-list inbound-acl
n7000(config-s-acl)# deny ip 10.0.0.0/8 any
n7000(config-s-acl)# deny ip 172.16.0.0/12 any
n7000(config-s-acl)# deny ip 192.168.0.0/16 any
n7000(config-s-acl)# interface ethernet x/x
n7000(config-s-if)# ip access-group inbound-acl in
n7000(config-s-if)# verify
Verification Successful
n7000(config-s)# commit
Commit Successful
```

Supervisor Redundancy

To ensure high availability, we recommend that you have two supervisor modules installed per chassis. This section contains information for verifying the status of a redundant supervisor modules and performing a manual supervisor switchover if necessary.

Verifying Supervisor Status

Introduced: Cisco NX-OS Release 4.0(1)

When two supervisor modules are present, one supervisor module should be in an “Active with HA standby”state, and other supervisor module should be in an “HA Standby” state during normal operation of the switch.

```
n7000# show system redundancy status

Redundancy mode
---------------
      administrative:    HA
         operational:    HA

This supervisor (sup-1)
-----------------------
    Redundancy state:    Active
    Supervisor state:    Active
    Internal state:      Active with HA standby

Other supervisor (sup-2)
------------------------
    Redundancy state:    Standby
    Supervisor state:    HA standby
```

Manual Switchover

Introduced: Cisco NX-OS Release 4.0(1)

This section was included for reference and may not be required.

A supervisor switchover can be manually initiated in a chassis with two supervisor modules present. Once the switchover is performed, the previous active supervisor reloads and come back online as the standby supervisor. You cannot manually perform a switchover if the Standby supervisor is not in an “HA standby” state.

```
n7000# system switchover
```

Locator LED

Introduced: Cisco NX-OS Release 4.0(1)

Cisco NX-OS software supports a Locator LED feature that is useful when physically identifying hardware components (chassis, fans, fabrics, modules, power-supplies) and ports on Ethernet I/O modules. The Locator LED feature should be used when working with remote-hands support teams that are responsible for performing physical tasks such as replacing hardware or working with Ethernet ports (adds, moves, etc.). Use the **no locator-led** command to disable the locator LED for a chassis component or interface.

```
n7000# locator-led chassis
n7000# locator-led fan 1
n7000# locator-led module 1
n7000# locator-led powersupply 1
n7000# locator-led xbar 1

n7000(config)# interface ethernet 1/1
n7000(config-if)# beacon
```

```
n7000# show locator-led status
Component        Locator LED Status
-------------------------------------
Chassis          ON
Module  1        ON
Module  2        off
Module  5        off
Xbar  1          ON
Xbar  2          off
Xbar  3          off
PowerSupply  1   ON
PowerSupply  2   off
PowerSupply  3   off
Fan  1           ON
Fan  2           off
Fan  3           off
```

Note The Cisco NX-OS CLI syntax changed in Cisco NX-OS Release 4.1(2). The **locator-led** command replaced the deprecated **blink** command. Ethernet ports on an I/O module do not display their status in the output of the **show locator-led status** command. Use the **show interface** command or view the running-configuration to determine if a port Locator LED (Beacon) is enabled or disabled.

Ethanalyzer

Introduced: Cisco NX-OS Release 4.0(1)

The Ethernet Analyzer should be used when troubleshooting control plane protocols and high CPU utilization. Ethernet Analyzer allows the administrator to capture packets sent to and from the supervisor module CPU. Brief or detailed information per packet can be captured and viewed using the CLI or exported to a protocol analyzer such as Wireshark. When troubleshooting, a brief capture should be performed to identify the interesting packets, and a detailed capture should be performed to dissect the interesting packets in more detail. Captures can be redirected to files and stored locally using the **write** or **>** option. Ethanalyzer will capture 10 frames by default. The **limit-captured-frames <0-2147483647>** option can be used to increase the frame count. A value of **0** means there is no limit and a 10MB circular buffer is created.

Brief Capture:

```
n7000# ethanalyzer local interface inband
Capturing on inband
2010-06-02 20:44:40.327808 192.168.20.1 -> 224.0.0.5    OSPF Hello Packet
2010-06-02 20:44:41.480658 192.168.20.2 -> 207.68.169.104 DNS Standard query A
print.cisco.com
2010-06-02 20:44:41.730633 192.168.20.2 -> 207.68.169.104 DNS Standard query A
print.cisco.com
2010-06-02 20:44:41.730638 192.168.20.2 -> 65.54.238.85 DNS Standard query A
print.cisco.com
2010-06-02 20:44:42.480586 192.168.20.2 -> 65.54.238.85 DNS Standard query A
print.cisco.com

<Text Omitted>
```

Detailed Capture:

```
n7000# ethanalyzer local interface inband limit-captured-frames 100 detail
Capturing on inband
Capturing on inband
```

```
Frame 1 (60 bytes on wire, 60 bytes captured)
    Arrival Time: Oct  2, 2010 22:07:57.150394000
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 60 bytes
    Capture Length: 60 bytes
    [Frame is marked: False]
    [Protocols in frame: eth:llc:stp]
IEEE 802.3 Ethernet
    Destination: 01:80:c2:00:00:00 (01:80:c2:00:00:00)
        Address: 01:80:c2:00:00:00 (01:80:c2:00:00:00)

<Text Omitted>
```

Writing a Brief Capture to a File:

```
n7000# ethanalyzer local interface inband write bootflash:cpu.
```

Reading a Capture File:

```
n7000# ethanalyzer local read bootflash:cpu.txt
```

Redirecting a Detailed Capture to a File:

```
n7000# ethanalyzer local interface detail > cpu-1.txt
```

Reading a Capture File:

```
n7000# show file bootflash:cpu-1.txt
```

Note The **inband** option captures packets on the I/O modules, and the **mgmt** option captures packets on the supervisor module mgmt0 port.

Note The CLI syntax has changed slightly from Cisco NX-OS Release 4.x to Release 5.x. This CLI output is captured from NX-OS Release 5.1(1).

Switched Port Analyzer

Introduced: Cisco NX-OS Release 4.0(1)

Switched Port Analyzer (SPAN) can be used to mirror traffic from a source to a destination when troubleshooting or for providing data for network services such as Intrusion Prevention Systems (IPS). While this document does not cover SPAN in detail, We recommend that you disable local and ERSPAN sessions with the **shut** command if they are not required to be active after troubleshooting. This preserves hardware resources by preventing unnecessary traffic from being flooded across the fabric. The ERSPAN feature was introduced in Cisco NX-OS Release 5.1(1).

Local SPAN:

```
n7000(config)# monitor session 1
n7000(config-monitor)# shut
```

Encapsulated Remote (ERSPAN):

```
n7000(config)# monitor session 1 type erspan-source
n7000(config-erspan-src)# shut
```

```
n7000(config)# monitor session 1 type erspan-destination
n7000(config-erspan-dst)# shut
```

Performing a Debug

This section contains the Cisco NX-OS recommended best practices for performing a debug. Always use caution when executing a debug command since network performance can be impacted.

Redirecting Output to a File

Introduced: Cisco NX-OS Release 4.0(1)

By default, debug output is logged to the console and monitor sessions (SSH/Telnet), which can impact network performance. When performing a debug, the output should be redirected to a file as opposed to the console or a terminal session to reduce processing overhead on the supervisor module CPU. In the following example, the debug output is redirected to a file for analysis. The redirected debug output is saved in the log: directory. Once the debug output is redirected to a file, the output can be viewed and/or copied to a remote destination. The pipe option can be used to parse the log file. The **show debug** command displays the current debug status and the **no debug all** command will disable all debugging.

Note Do not leave an unintended debug running that is not required.

```
n7000# debug logfile cdp-debug
n7000# debug cdp all
n7000# no debug cdp all

n7000# dir log:cdp-debug
      14560    Nov 01 22:05:18 2010  cdp-debug

n7000# show debug logfile cdp-debug
2010 Nov  1 22:02:02.948577 cdp: Going to send CDP version 2 pkt on Ethernet7/3
2010 Nov  1 22:02:02.948662 cdp: Sent CDP packet untagged on interface 0x1a30200
0
2010 Nov  1 22:02:02.948696 cdp: Going to send CDP version 2 pkt on Ethernet10/1
8

<Text Omitted>

n7000# show debug logfile cdp-debug | include Ethernet10/1
```

CHAPTER 11

Verifying Hardware Diagnostics and Logging

This chapter contains the Cisco NX-OS recommended features and procedures for managing and troubleshooting potential hardware faults.

This chapter includes the following sections:

Online Diagnostics

Generic Online Diagnostics (GOLD) provides hardware testing verification that is useful for detecting hardware faults. If a fault is detected, corrective action is taken to mitigate the fault to reduce potential network outages. GOLD tests are executed when a chassis is powered up, for an online insertion and removal (OIR) event, as health checks occur in the background (continuous testing), and on demand from the CLI.

Enabling GOLD

Introduced: Cisco NX-OS Release 4.0(1)

Generic Online Diagnostics are enabled by default. (We do not recommend disabling online diagnostics.) In the event online diagnostics have been disabled, they can be enabled using the following command.

```
n7000(config)# diagnostic bootup level complete
```

Understanding Diagnostic Contents (Per Module)

Introduced: Cisco NX-OS Release 4.0(1)

The **show diagnostic content** command displays the available tests for a module and the associated attributes for each test. This is useful for determining what tests are available for a module and if the tests are disruptive prior to running an on-demand test.

```
n7000# show diagnostic content module 1

Module 1: 10/100/1000 Mbps Ethernet Module

Diagnostics test suite attributes:
```

```
B/C/* - Bypass bootup level test / Complete bootup level test / NA
P/*   - Per port test / NA
M/S/* - Only applicable to active / standby unit / NA
D/N/* - Disruptive test / Non-disruptive test / NA
H/*   - Always enabled monitoring test / NA
F/*   - Fixed monitoring interval test / NA
X/*   - Not a health monitoring test / NA
E/*   - Sup to line card test / NA
L/*   - Exclusively run this test / NA
T/*   - Not an ondemand test / NA
A/I/* - Monitoring is active / Monitoring is inactive / NA

                                                    Testing Interval
ID     Name                                 Attributes      (hh:mm:ss)
____   ___________________________________  ____________    _____________
 1)    EOBCPortLoopback-------------->      C**N**X**T*      -NA-
 2)    ASICRegisterCheck------------->      ***N******A      00:01:00
 3)    PrimaryBootROM---------------->      ***N******A      00:30:00
 4)    SecondaryBootROM-------------->      ***N******A      00:30:00
 5)    PortLoopback------------------>      CP*N***E**A      00:15:00
```

On-Demand Tests

Introduced: Cisco NX-OS Release 4.0(1)

On Demand tests should be executed anytime hardware is suspected to be faulty. An on-demand test is executed from Exec mode. GOLD tests can be disruptive and non-disruptive, so caution should be taken to prevent any network outages. If a GOLD test is disruptive the administrator will be prompted to continue.

```
n7000# diagnostic start module 1 test 6 port 1
```

Verifying GOLD Test Results (Per Module)

Introduced: Cisco NX-OS Release 4.0(1)

The following command checks the GOLD test results for module 1. The **detail** option provides timestamp information for each test, which is useful for determining when a test may have passed or failed.

```
n7000# show diagnostic result module 1

Current bootup diagnostic level: complete
Module 1: 10/100/1000 Mbps Ethernet Module

        Test results: (. = Pass, F = Fail, I = Incomplete,
        U = Untested, A = Abort, E = Error disabled)

         1) EOBCPortLoopback--------------> .
         2) ASICRegisterCheck-------------> .
         3) PrimaryBootROM----------------> .
         4) SecondaryBootROM--------------> .
         5) PortLoopback:

          Port   1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16
          -----------------------------------------------------
                 U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U

          Port  17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
          -----------------------------------------------------
```

```
                U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U

Port  33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
-------------------------------------------------
```

Onboard Failure-Logging

Onboard Failure Logging (OBFL) provides persistent event logging per module that contains detailed information that can be useful when troubleshooting. OBFL is enabled by default and should not be disabled. The data in some of the OBFL logs may be difficult to understand, but the logs are useful when the Cisco TAC is diagnosing a potential hardware issue.

Enabling/Disabling OBFL

Introduced: Cisco NX-OS Release 4.0(1)

This section was included for reference and may not be required.

An OBFL log can be disabled per system or per module. The following example illustrates how to enable an OBFL log per module in the event it was previously disabled. This action is typically not required since they are enabled by default.

```
n7000(config)# hw-module logging onboard module 1 environmental-history
    Module:  1   Enabling environmental-history ... was successful.
```

Viewing Log Contents

Introduced: Cisco NX-OS Release 4.0(1)

OBFL logs can be viewed per system (all logs), per log type (i.e. environmental-history) for all modules, and per module/log type. The “l” option can be used to redirect output to a file if the contents need to be sent to a remote destination. Since logs are persistent they can contain a large amount of data.

```
n7000# show logging onboard  module 1 environmental-history
----------------------------
    Module:  1
----------------------------
========== Sensor Temperature History Log ==========
-------------------------------------------------
Fri Apr  9 11:20:24 2010 sensor 13 temperature 53
Fri Apr  9 11:36:25 2010 sensor 14 temperature 54

<Text Omitted>
```

Clearing Log Contents

Introduced: Cisco NX-OS Release 4.0(1)

The following **clear log onboard** command can be used to clear the contents for all logs, a log type for all modules, or a specific log type for a specified module.

```
n7000# clear log onboard ?
  <CR>
  counter-stats          Clear OBFL counter statistics
  environmental-history  Clear OBFL environmental history
```

```
error-stats             Clear OBFL error statistics
exception-log           Clear OBFL exception log
fex                     Clear OBFL information for FEX
internal                Clear Logging Onboard Internal
interrupt-stats         Clear OBFL interrupt statistics
module                  Clear OBFL information for Module
obfl-logs               Clear OBFL (boot-uptime/device-version/obfl-history).
stack-trace             Clear OBFL stack trace
```

CHAPTER 12

Managing Hardware Resource Utilization

This chapter contains Cisco NX-OS procedures recommended when managing hardware resources utilization such as the CPU, memory and I/O module TCAM table utilization.

This chapter includes the following sections:

CPU Processes

This section contains information for verifying the CPU utilization for the supervisor module.

Utilization

Introduced: Cisco NX-OS Release 4.0(1)

The **show system resources** command displays the high level CPU utilization for the supervisor module. The **show process cpu** command with the sort option lists all of the processes sorted by the highest CPU utilization per process. The **show process cpu history** command displays the CPU history in three increments: 60 seconds, 60 minutes, 72 hours. Viewing the CPU history is valuable when correlating a network event with the past CPU utilization. The sort and history options for the **show process cpu** command were introduced in Cisco NX-OS Release 4.2(1).

It should be noted that Cisco NX-OS takes advantage of preemptive CPU multitasking, so processes can take advantage of an Idle CPU to complete tasks faster. Therefore, the history option may report CPU spikes that do not necessarily mean there is an issue. Additional investigation should take place if the average CPU remains close to 100%.

```
n7000# show system resources
Load average:   1 minute: 0.06   5 minutes: 0.04   15 minutes: 0.00
Processes   :   310 total, 1 running
```

```
CPU states  :   0.0% user,   0.5% kernel,   99.5% idle
Memory usage:   4135780K total,   1180900K used,   2954880K free
                     0K buffers,  759580K cache

n7000# show process cpu sort

PID    Runtime(ms)  Invoked   uSecs  1Sec    Process
-----  -----------  --------  -----  ------  -----------
 3102         1692    371648      4    2.0%  platform
    1          162     49364      3    0.0%  init

<Text Omitted>


n7000# show process cpu history

                  1    1                1                      1
    151 2    1  176 6112 2212    1   21  511 1  2    31 151 1 10
100
 90
 80
 70
 60
 50
 40
 30
 20               #                    #
 10  #           ## #  #                #               #     #
    0....5....1....1....2....2....3....3....4....4....5....5....
              0    5    0    5    0    5    0    5    0    5
```

Restarting a Process

Introduced: Cisco NX-OS Release 4.0(1)

This section is included for reference and may not be required.

Some Cisco NX-OS processes can be restarted with the **restart** command. A process should not require a manual restart, but in the event it does a process can be restarted without re-configuring the protocol, or reloading the chassis. Restarting a process may be disruptive, so this feature should be used with caution.

```
n7000# restart ospf 10
```

Memory

This section contains information for verifying the supervisor module DRAM and Flash memory utilization.

DRAM Utilization

Introduced: Cisco NX-OS Release 4.0(1)

The supervisor module memory utilization for a chassis can be monitored with the following commands. The **show system resources** command displays the overall memory utilization for the supervisor module and the **show process memory** command displays memory utilization per process per VDC.

```
n7000# show system resources
Load average:   1 minute: 0.06   5 minutes: 0.04   15 minutes: 0.00
Processes   :   310 total, 1 running
CPU states  :   0.0% user,   0.5% kernel,   99.5% idle
Memory usage:   4135780K total,   1180900K used,   2954880K free
                      0K buffers,  759580K cache

n7000# show process memory

PID    MemAlloc  MemLimit    MemUsed     StackBase/Ptr      Process
-----  --------  ----------  ----------  -----------------  ----------------

<Text Omitted>

11849   2994176  329981836   127692800   bffff5e0/bfffc820  nfm
12019  13029376  334518976   115449856   bfffe1c0/bfffde30  ospf
12266    155648  0           1712128     bfffe800/bfffe5cc  more
12267   1118208  0           48463872    bffff670/bfff9c08  vsh
12268         0  0           0           bfffe410/bfffdd28  ps

<Text Omitted>
```

Flash Utilization

Introduced: Cisco NX-OS Release 4.0(1)

The flash file system capacity can be verified for each supervisor module. The following example has one supervisor module in slot 5. The bootflash: refers to the 2 GB onboard flash, and the logflash, and slot0 refers to the external compact flash slots on the supervisor module. The **dir** command displays the contents for each type of flash memory (output not displayed).

```
n7000# show hardware capacity | begin flash
         5       bootflash     1767480     1055144     40
         5       logflash      7997912     7555672      5
         5       slot0         1996928     1652944     17

n7000# dir bootflash:
n7000# dir logflash:
n7000# dir slot0:
```

MAC Address TCAM Tables

This section contains information for verifying the MAC address TCAM table utilization and modifying the aging-time if necessary.

Utilization

Introduced: Cisco NX-OS Release 4.0(1)

The Cisco Nexus 7000 Series uses a distributed forwarding architecture in which each Ethernet M series module has a forwarding engine responsible for forwarding packets. A forwarding engine on an M series module is capable of storing 128,000 MAC Address entries. MAC address tables are synchronized between Ethernet M series modules that have ports configured in the same Virtual Device Context (VDC). The following command is useful for verifying the MAC address table capacity for all modules in a chassis.

```
n7000# show hardware capacity forwarding | begin L2

L2 Forwarding Resources
-----------------------
  L2 entries: Module   total    used   mcast   ucast   lines   lines_full
              1       131072       6       1       5    8192            0
              2       131072       6       1       5    8192            0

<Text Omitted>
```

Aging Time

Introduced: Cisco NX-OS Release 4.0(1)

This section was included for reference and may not be required.

The default MAC-Address table aging time is 1,800 seconds (30 minutes). The aging time can be modified to a more or less aggressive timeout value. The MAC Address aging time should be consistent for all of the devices within a switched domain.

```
n7000(config)# mac address-table aging-time ?
  <0-0>         0 disables aging
  <120-918000>  Aging time in seconds.
```

Unicast or Multicast TCAM Tables

This section contains information for verifying the unicast/multicast TCAM table utilization.

Utilization

Introduced: Cisco NX-OS Release 4.0(1)

The Cisco Nexus 7000 Series uses a distributed forwarding architecture in which each Ethernet M series module has a forwarding engine responsible for forwarding packets. A forwarding engine on an M series module is capable of storing 128,000 IPv4/IPv6 routing entries or 1,000,000 entries if it is an XL module with a Scalable-Feature license installed. IPv4/IPv6 unicast/multicast tables are synchronized between Ethernet M series modules that have ports configured in the same Virtual Device Context (VDC). The following example displays the default TCAM allocation for a non-XL module. Beginning in Cisco NX-OS Release 4.2(1), Cisco NX-OS supports dynamic TCAM allocation. This allows for better resource utilization in the event and address family (i.e. IPv6 unicast) requires additional entries.

```
n7000# show hardware capacity forwarding | begin TCAM

Key: Log/Phys = Logical entries / Physical entries
Note: IPv4 Multicast/IPv6 Unicast entries share one FIB TCAM entry pool

Module 1 usage:
Route Type            Used      %Used      Free      %Free      Total
                   (Log/Phys)            (Log/Phys)           (Log/Phys)
------------------------------------------------------------------------
IPv4 Unicast:        19/19         0    57325/57325     99    57344/57344
IPv4 Multicast:       4/8          0    16380/32760     99    16384/32768
IPv6 Unicast:         9/18         0    16375/32750     99    16384/32768
IPv6 Multicast:       5/20         0     2043/8172      99     2048/8192
```

NetFow TCAM Tables

This section contains information for verifying the NetFlow TCAM table utilization.

Utilization

Introduced: Cisco NX-OS Release 4.0(1)

The Cisco Nexus 7000 Series uses a distributed forwarding architecture in which each Ethernet M series module has a forwarding engine responsible for forwarding packets. A forwarding engine on an M series module is capable of storing 512,000 NetFlow entries. This value is the same for both non-XL and XL M series modules.

```
n7000# show hardware capacity forwarding | begin Netflow

n7000# show hardware capacity forwarding | begin Netflow
Netflow Resources
-----------------
Flow Table Usage:  Module  Util    Used    Free    Fail
                   1       0.00%   0       515090  0
                   2       0.00%   0       515090  0
ICAM Usage:        Module  Util    Used    Free
                   1       0.00%   0       16
                   2       0.00%   0       16
IPv4 Mask Usage:   Module  Util    Used    Free
                   1       0.00%   0       32
                   2       0.00%   0       32
IPv6 Mask Usage:   Module  Util    Used    Free
                   1       0.00%   0       32
                   2       0.00%   0       32
```

ACL or QoS TCAM Tables

This section contains information for verifying the ACL or QoS TCAM table utilization and enabling ACL TCAM chaining if required.

Utilization

Introduced: Cisco NX-OS Release 4.0(1)

The Cisco Nexus 7000 Series uses a distributed forwarding architecture in which each Ethernet M series module has a forwarding engine responsible for forwarding packets. A forwarding engine on an M series module is capable of storing 64,000 (non-XL) or 128,000 ACL QoS entries if it is an XL module with the Scalable Feature license installed.

```
n7000# show hardware capacity | begin ACL
         ACL Hardware Resource Utilization (Module 1)
         ---------------------------------------------
                           Used    Free    Percent
                                           Utilization
-----------------------------------------------------
Tcam 0, Bank 0             1       16383   0.00
Tcam 0, Bank 1             2       16382   0.01
Tcam 1, Bank 0             1       16383   0.00
Tcam 1, Bank 1             2       16382   0.01
```

```
LOU                       0       104     0.00
Both LOU Operands         0
Single LOU Operands       0
LOU L4 src port:          0
LOU L4 dst port:          0
LOU L3 packet len:        0
LOU IP tos:               0
LOU IP dscp:              0
LOU ip precedence:        0
TCP Flags                 0       16      0.00

Protocol CAM              0       7       0.00
Mac Etype/Proto CAM       0       14      0.00

Non L4op labels, Tcam 0   0       6143    0.00
Non L4op labels, Tcam 1   0       6143    0.00
L4 op labels, Tcam 0      0       2047    0.00
L4 op labels, Tcam 1      0       2047    0.00
```

ACL Resource Polling

Introduced: Cisco NX-OS Release 4.2(1)

This section is included for reference and may not be required.

The ACL TCAM is divided into four banks (16K per bank for non-XL and 32K per bank for XL modules) on the current M series forwarding engines. Prior to Cisco NX-OS Release 4.2(1) an ACL could only contain 1 bank of entries (16K or 32K entries depending on the module type). Starting in Cisco NX-OS Release 4.2(1) a single ACL can be programmed across multiple banks allowing up to 64, 000 entries in a single ACL per non-XL and 132,000 entries in an XL module. This feature should only be enabled on systems that require ACLs that contain more than 16,000 entries. This feature is configured in the default VDC(1) for all VDCs.

```
n7000(config)# hardware access-list resource pooling module 1

n7000# show hardware access-list resource pooling
  Module 1 enabled
```

Fabric Utilization

The fabric utilization can be monitored to verify the ingress and egress bandwidth utilization. The **show hardware fabric-utilization** commands are useful for verifying the high-level and detailed utilization. The **show hardware capacity fabric-utilization** is useful for verifying the peak utilization history.

```
n7000# show hardware fabric-utilization
------------------------------------------------
Slot        Total Fabric        Utilization
            Bandwidth      Ingress % Egress %
------------------------------------------------
1             138 Gbps          0.0       0.0
2             138 Gbps          0.0       0.0
4             138 Gbps          0.0       0.0
5              69 Gbps          0.0       0.0
7             138 Gbps          0.0       0.0
8             138 Gbps          0.0       0.0
9             138 Gbps          0.0       0.0
```

```
10            138 Gbps          0.0       0.0

n7000# show hardware fabric-utilization detail
--------------------------------------------------------------------------------
Fabric Planes:
A -- Unicast fabric interface
B -- Multicast/Multidestination fabric interface
--------------------------------------------------------------------------------
Unidirectional Fabric Bandwidth per Fab Link is 23 Ggps (A+B)
--------------------------------------------------------------------------------
I/O   Fab  Fab  Fab  Fab  Fab        Fabric Utilization
Slot  Mod  Ins  Chnl Link Plane    Ingress%     Egress%
--------------------------------------------------------------------------------
1     1    1    5    0    A          0            0
1     1    1    5    0    B          0            0
1     1    1    3    1    A          0            0
1     1    1    3    1    B          0            0
1     2    1    5    2    A          0            0
1     2    1    5    2    B          0            0
1     2    1    3    3    A          0            0
1     2    1    3    3    B          0            0
1     3    1    5    4    A          0            0
1     3    1    5    4    B          0            0
1     3    1    3    5    A          0            0
1     3    1    3    5    B          0            0

<Text omitted>

n7000# show hardware capacity fabric-utilization
--------------------------------------------------------------------------------
Fabric Planes:
A -- Unicast fabric interface
B -- Multicast/Multidestination fabric interface
-------------------------PEAK FABRIC UTILIZATION-------------------------
I/O  |-----FABRIC----|       Ingress           |       Egress
Slot |Mod Inst  Plane| Util           Time     | Util          Time
--------------------------------------------------------------------------------
1     1     1     A      0%     11-01@23:09:42    0%     11-01@23:09:42
1     1     1     B      0%     11-01@23:09:42    0%     11-01@23:09:42
1     1     1     A      0%     11-01@23:09:42    0%     11-01@23:09:42
1     1     1     B      0%     11-01@23:09:42    0%     11-01@23:09:42
1     2     1     A      0%     11-01@23:09:42    0%     11-01@23:09:42
1     2     1     B      0%     11-01@23:09:42    0%     11-01@23:09:42
1     2     1     A      0%     11-01@23:09:42    0%     11-01@23:09:42
1     2     1     B      0%     11-01@23:09:42    0%     11-01@23:09:42
1     3     1     A      0%     11-01@23:09:42    0%     11-01@23:09:42
```

VDC Resource Utilization

Introduced: Cisco NX-OS Release 4.0(1)

Global VDC resources can be verified with the **show vdc resource** command. This is useful to know, since VDCs can contend for common resources such as memory, SPAN sessions, etc.).

```
n7000# show vdc resource

  vlan                16 used    48 unused  16368 free  16320 avail  16384 total

  monitor-session      0 used     0 unused      2 free      2 avail      2 total
```

```
monitor-session-erspan-dst      0 used     0 unused     23 free     23 avail  23 total

vrf                             8 used     0 unused    992 free    992 avail   1000 total

port-channel                    0 used     0 unused    768 free    768 avail    768 total

u4route-mem                   120 used     0 unused    396 free    396 avail    516 total

u6route-mem                    36 used     0 unused    172 free    172 avail    208 total

m4route-mem                    82 used     0 unused    118 free    118 avail    200 total
```

CHAPTER 13

Collecting Data for the Cisco TAC

It is important to proactively attach troubleshooting information and logs when opening a TAC case to expedite problem resolution. This chapter contains the recommended procedures for collecting information for troubleshooting that should be attached to a TAC case. A Cisco TAC engineer may request additional data, but if the following actions are performed, the engineer will have data to review right away, which should reduce the problem resolution time.

This chapter includes the following sections:

Collecting Show Tech-Support Information

Introduced: Cisco NX-OS Release 4.0(1)

The **show tech–support** command is useful when diagnosing a potential problem or when collecting information to attach to a Cisco TAC case. The contents of a **show tech-support** are usually vary large and will vary in size depending on how long the system has been powered up. The **show tech-support** command supports feature options such as **hsrp**, **ospf**, etc. This is useful when troubleshooting, if you want to collect a subset of information for a specific feature.

When running a **show tech-support** for a specific feature, detailed information is collected by default. The **brief** option can be specified to collect less data for a feature, although this option is typically not recommended. When running a **show tech-support** for all features you have to specify the **details** option if you want to collect the additional data.

The first example captures detailed information for all features using the **space-optimized** option. The second example captures detailed information for **ospf** and redirects it to a file in flash (bootflash:).

```
n7000# show tech-support details space-optimized

n7000# show tech-support ospf > show-tech-ospf
```

Generating a TAC-PAC

Introduced: Cisco NX-OS Release 4.0(1)

When opening a TAC case, always generate a **tac-pac** and attach the file to the case. This allows the Cisco TAC engineers to obtain information about the issue without having to ask for a **show tech-support**. A **tac-pac** collects useful information that is stored in a compressed file, so it is easier to transfer than a **show tech-support** redirected to an uncompressed file. The following example saves the compressed file in flash (Slot0:).

```
n7000# tac-pac slot0:tac-pac-for-tac
```

Archiving or Compressing Multiple Files

Introduced: Cisco NX-OS Release 4.0(1)

Multiple files can be archived and compressed to simplify the transport process when saving data to a remote destination.

```
n7000# show tech hsrp > hsrp-detail.txt
n7000# show tech ospf > ospf-detail.txt

n7000# dir bootflash: | grep detail
    9855855    Nov 02 21:07:40 2010  hsrp-detail.txt
       2703    Nov 02 21:08:11 2010  ospf-detail.txt

n7000# tar create bootflash:tac-info gz-compress bootflash:hsrp-detail.txt
bootflash:ospf-detail.txt

n7000# dir bootflash:tac-info.tar.gz
     860311    Nov 02 21:12:51 2010  tac-info.tar.gz
```

Verifying and Collecting Core Files

Introduced: Cisco NX-OS Release 4.0(1)

When a process has an unexpected restart or failure, Cisco NX-OS saves a core file that contains details about the event. The content in a core file is useful for Cisco TAC engineers and software developers to diagnose the process failure. The core files should be copied and attached to the TAC case. The following commands determine if there are any core files and copies them to a remote destination. This example uses SCP, but other transport protocols such as SFTP, FTP or TFTP can be used.

```
n7000# show cores

VDC No Module-num       Process-name      PID     Core-create-time

------ ----------       ------------      ---     ----------------
1   8         acltcam     285     Oct 27 09:32


n7000# copy core://8/285 scp://username@x.x.x.x/acltcam-core
```