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

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

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

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

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2013-2014 Cisco Systems, Inc. All rights reserved.
CONTENTS

Preface ix

Audience ix

Document Conventions ix

Related Documentation for Cisco Nexus 9000 Series Switches x

Documentation Feedback x

Obtaining Documentation and Submitting a Service Request xi

CHAPTER 1

New and Changed Information 1

New and Changed Information 1

CHAPTER 2

Overview 3

Software Image 3

About the Troubleshooting Process 3

Verifying Ports 4

Verifying Layer 2 Connectivity 4

Verifying Layer 3 Connectivity 5

Symptoms 5

System Messages 6

Syslog Server Implementation 6

Troubleshooting with Logs 8

Troubleshooting Modules 8

Viewing NVRAM Logs 8

Contacting Customer Support 9

CHAPTER 3

Troubleshooting Installations, Upgrades, and Reboots 11

About Upgrades and Reboots 11

Upgrade and Reboot Checklist 11
Verifying Software Upgrades 12
Troubleshooting Software Upgrades and Downgrades 13
  Software Upgrade Ends with Error 13
  Upgrading the Cisco NX-OS Software 13
Troubleshooting Software System Reboots 14
  Power-On or Switch Reboot Hangs 14
  Corrupted Bootflash Recovery 14
  Recovery from the loader> Prompt 16
System or Process Restarts 18
Recovering System Restarts 18
Unrecoverable System Restarts 23
Standby Supervisor Fails to Boot 24
Recovering the Administrator Password 24
  Using the CLI with Network-Admin Privileges to Recover the Administrator Password 24
  Power Cycling the Device to Recover the Administrator Password 25
  Reloading the Device to Recover the Administrator Password 30

CHAPTER 4
Troubleshooting Licensing Issues 33
  About Troubleshooting Licensing Issues 33
  Guidelines and Limitations for Licensing 33
  Initial Troubleshooting Checklist for Licensing 34
  Displaying License Information Using the CLI 34
  Licensing Installation Issues 35
    Serial Number Issues 35
    RMA Chassis Errors or License Transfers Between Systems 36
    License Listed as Missing 36

CHAPTER 5
Troubleshooting Ports 37
  About Troubleshooting Ports 37
  Guidelines and Limitations for Troubleshooting Ports 37
  Initial Port Troubleshooting Checklist 38
  Viewing Port Information 38
  Viewing Port Errors 39
  Troubleshooting Port Statistics from the CLI 39
Troubleshooting Port-Interface Issues 40
   The Interface Configuration Has Disappeared 40
   You Cannot Enable an Interface 40
   You Cannot Configure a Dedicated Port 41
   A Port Remains in a Link Failure or Not Connected State 41
   An Unexpected Link Flapping Occurs 42
   A Port Is in the ErrDisabled State 43
   Verifying the ErrDisable State Using the CLI 43

CHAPTER 6
Troubleshooting vPCs 45
   About Troubleshooting vPCs 45
   Initial Troubleshooting vPCs Checklist 45
   Verifying vPCs Using the CLI 46
   Received Type 1 Configuration Element Mismatch 47
   Cannot Enable the vPC Feature 48
   vPCs in Blocking State 48
   VLANs on a vPC Moved to Suspend State 48
   Hosts with an HSRP Gateway Cannot Access Beyond Their VLAN 49

CHAPTER 7
Troubleshooting VLANs 51
   About Troubleshooting VLANs 51
   Guidelines and Limitations for Troubleshooting VLANs 51
   Initial Troubleshooting VLANs Checklist 52
   Troubleshooting VLAN Issues 52
   You Cannot Create a VLAN 52
   You Cannot Create a PVLAN 53
   The VLAN Interface is Down 53

CHAPTER 8
Troubleshooting STP 55
   About Troubleshooting STP 55
   Initial Troubleshooting STP Checklist 55
   Troubleshooting STP Data Loops 56
   Troubleshooting Excessive Packet Flooding 59
   Troubleshooting Convergence Time Issues 60
   Securing the Network Against Forwarding Loops 61
CHAPTER 9

Troubleshooting Routing 63
  About Troubleshooting Routing Issues 63
  Initial Troubleshooting Routing Checklist 63
  Troubleshooting Routing 64
  Troubleshooting Policy-Based Routing 66

CHAPTER 10

Troubleshooting Memory 69
  About Troubleshooting Memory 69
  General/High Level Assessment of Platform Memory Utilization 70
  Detailed Assessment of Platform Memory Utilization 70
    Page Cache 72
    Kernel 72
  User Processes 73
    Determining Which Process Is Using a Lot of Memory 74
    Determining How a Specific Process Is Using Memory 75
  Built-in Platform Memory Monitoring 76
    Memory Thresholds 77
    Memory Alerts 77

CHAPTER 11

Troubleshooting Packet Flow Issues 79
  Packet Flow Issues 79
    Packets Dropped Because of Rate Limits 79
    Packets Dropped Because of CoPP 80
  Monitoring Inband Packet Statistics 80
  Fabric Connectivity Commands 81

CHAPTER 12

Troubleshooting PowerOn Auto Provisioning 85
  Switch Does Not Come Up in Time for POAP to Complete 85
  POAP Fails 85

CHAPTER 13

Troubleshooting the Python API 87
  Receiving Python API Errors 87

CHAPTER 14

Troubleshooting NX-API 91
NX-API Guidelines 91
NX-API Is Not Responding 91
Configuration Fails 92
Permission Is Denied for Bash 92
Output Cannot Be Retrieved from the Browser Sandbox 92
CLI Command Errors Are Appearing 92
Error Messages Are Appearing 92
Temporary Files Are Disappearing 93
Chunks of the Command Output Are Not Being Delivered 93

CHAPTER 15

Troubleshooting Service Failures 95
Identifying Memory Allocations for Processes 95
Identifying CPU Utilization for Processes 96
Monitoring Process Core Files 97
Processing the Crash Core Files 97
Clearing the Core 97
Enabling Auto-Copy for Core Files 98

CHAPTER 16

Before Contacting Technical Support 99
Steps to Perform Before Calling TAC 99
Copying Files to or from Cisco NX-OS 101
Using Core Dumps 102

CHAPTER 17

Troubleshooting Tools and Methodology 103
Command-Line Interface Troubleshooting Commands 103
Consistency Checker Commands 104
Configuration Files 105
CLI Debug 105
Debug Filters 106
Ping and Traceroute 106
Using Ping 106
Using Traceroute 107
Monitoring Processes and CPUs 108
Using the show processes cpu Command 109
Using the show system resources Command 110
Preface

This preface includes the following sections:

- Audience, page ix
- Document Conventions, page ix
- Related Documentation for Cisco Nexus 9000 Series Switches, page x
- Documentation Feedback, page x
- Obtaining Documentation and Submitting a Service Request, page xi

Audience

This publication is for network administrators who install, configure, and maintain Cisco Nexus switches.

Document Conventions

Command descriptions use the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bold</strong></td>
<td>Bold text indicates the commands and keywords that you enter literally as shown.</td>
</tr>
<tr>
<td><em>Italic</em></td>
<td>Italic text indicates arguments for which the user supplies the values.</td>
</tr>
<tr>
<td>[x]</td>
<td>Square brackets enclose an optional element (keyword or argument).</td>
</tr>
<tr>
<td>[x</td>
<td>y]</td>
</tr>
<tr>
<td>{x</td>
<td>y}</td>
</tr>
</tbody>
</table>
### Convention

- **[x {y | z}]**: Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.

- **variable**: Indicates a variable for which you supply values, in context where italics cannot be used.

- **string**: A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

---

### Examples use the following conventions:

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

---

### Related Documentation for Cisco Nexus 9000 Series Switches

The entire Cisco Nexus 9000 Series switch documentation set is available at the following URL:


### Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to nexus9k-docfeedback@cisco.com. We appreciate your feedback.
Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to What's New in Cisco Product Documentation, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.
New and Changed Information

This chapter provides release-specific information for each new and changed feature in the Cisco Nexus 9000 Series NX-OS Troubleshooting Guide, Release 6.x.

- New and Changed Information, page 1

### Table 1: New and Changed Features for Cisco NX-OS Release 6.x

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Changed in Release</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private VLANs (PVLANs)</td>
<td>Introduced this feature.</td>
<td>6.1(2)I3(4)</td>
<td>Troubleshooting VLANs, on page 51</td>
</tr>
<tr>
<td>Traceroute</td>
<td>Added source interface support.</td>
<td>6.1(2)I3(3)</td>
<td>Troubleshooting Tools and Methodology, on page 103</td>
</tr>
<tr>
<td>Policy-based routing</td>
<td>Introduced this feature.</td>
<td>6.1(2)I3(1)</td>
<td>Troubleshooting Routing, on page 63</td>
</tr>
<tr>
<td>Consistency checker commands</td>
<td>Added commands for Layer 2 and VLANs.</td>
<td>6.1(2)I2(1)</td>
<td>Consistency Checker Commands, on page 104</td>
</tr>
<tr>
<td>DCNM</td>
<td>Introduced this feature.</td>
<td>6.1(2)I2(1)</td>
<td>Before Contacting Technical Support, on page 99</td>
</tr>
<tr>
<td>Layer 2</td>
<td>Added support for Layer 2 connectivity.</td>
<td>6.1(2)I2(1)</td>
<td>Overview, on page 3</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Changed in Release</td>
<td>Where Documented</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------------------</td>
<td>--------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Software upgrades</td>
<td>Added support for software upgrades.</td>
<td>6.1(2)I2(1)</td>
<td>Troubleshooting Installations, Upgrades, and Reboots, on page 11</td>
</tr>
<tr>
<td>Spanning Tree Protocol</td>
<td>Introduced this feature.</td>
<td>6.1(2)I2(1)</td>
<td>Troubleshooting STP, on page 55</td>
</tr>
<tr>
<td>Trunk ports</td>
<td>Introduced this feature.</td>
<td>6.1(2)I2(1)</td>
<td>Overview, on page 3</td>
</tr>
<tr>
<td>VLANs</td>
<td>Introduced this feature.</td>
<td>6.1(2)I2(1)</td>
<td>Troubleshooting VLANs, on page 51</td>
</tr>
<tr>
<td>vPCs</td>
<td>Introduced this feature.</td>
<td>6.1(2)I2(1)</td>
<td>Troubleshooting vPCs, on page 45</td>
</tr>
</tbody>
</table>
Overview

This chapter contains the following sections:

- Software Image, page 3
- About the Troubleshooting Process, page 3
- Symptoms, page 5
- Troubleshooting with Logs, page 8
- Troubleshooting Modules, page 8
- Viewing NVRAM Logs, page 8
- Contacting Customer Support, page 9

Software Image

The Cisco NX-OS software consists of one NXOS software image (for example, n9000-dk9.6.1.2.I1.1.bin). This image runs on all Cisco Nexus 9000 Series switches.

About the Troubleshooting Process

To troubleshoot your network, follow these general guidelines:

- Maintain a consistent Cisco NX-OS release across all your devices.
- See the Cisco NX-OS release notes for your Cisco NX-OS release for the latest features, limitations, and caveats.
- Enable system message logging.
- Troubleshoot any new configuration changes after implementing the change.
- Gather information that defines the specific symptoms.
- Verify the physical connectivity between your device and end devices.
- Verify the Layer 2 connectivity.
- Verify the end-to-end connectivity and the routing configuration.
- After you have determined that your troubleshooting attempts have not resolved the problem, contact Cisco TAC or your technical support representative.

This section describes the tools that are commonly used to troubleshoot problems within your network.

**Note**
You should have an accurate topology of your network to isolate problem areas. Contact your network architect for this information. Use the following commands to gather general information on your device:

- `show module`
- `show version`
- `show running-config`
- `show logging log`
- `show interfaces brief`
- `show vlan`
- `show spanning-tree`
- `show {ip | ipv6} routing`
- `show processes | include ER`
- `show accounting log`

**Verifying Ports**

Answer the following questions to verify that your ports are connected correctly and are operational:

- Are you using the correct media (copper, optical, fiber type)?
- Is the media broken or damaged?
- Is the port LED green on the module?
- Is the interface operational?

See [Troubleshooting Ports, on page 37](#) for more troubleshooting tips for ports.

**Verifying Layer 2 Connectivity**

Use the following commands to verify Layer 2 connectivity:

- Use the `show vlan all-ports` command to verify that all the necessary interfaces are in the same VLAN. The status should be active for the VLAN.
- Use the `show port-channel compatibility-parameters` command to verify that all of the ports in a port channel are configured the same for the speed, the duplex, and the trunk mode.
• Use the `show running-config spanning-tree` command to verify that the Spanning Tree Protocol (STP) is configured the same on all devices in the network.

• Use the `show processes | include ER` command to verify that nonessential Layer 2 processes are in the error state.

• Use the `show mac address-table dynamic vlan` command to determine if learning or aging is occurring at each node.

### Verifying Layer 3 Connectivity

Answer the following questions to verify Layer 3 connectivity:

- Have you configured a default gateway?
- Have you configured the same dynamic routing protocol parameters throughout your routing domain or configured static routes?
- Are any IP access lists, filters, or route maps blocking route updates?

Use the following commands to verify your routing configuration:

- `show ip arp`
- `show ip routing`

See **Troubleshooting Tools and Methodology, on page 103** to verify Layer 3 connectivity. See **Troubleshooting Routing, on page 63** for more information on troubleshooting Layer 3 issues.

### Symptoms

This document uses a symptom-based troubleshooting approach that allows you to diagnose and resolve your Cisco NX-OS problems by comparing the symptoms that you observed in your network with the symptoms listed in each chapter.

By comparing the symptoms in this publication to the symptoms that you observe in your own network, you should be able to diagnose and correct software configuration issues and inoperable hardware components so that the problems are resolved with minimal disruption to the network. Those problems and corrective actions include the following:

- Identify key Cisco NX-OS troubleshooting tools.
- Obtain and analyze protocol traces using SPAN or Ethalyzer on the CLI.
- Identify or rule out physical port issues.
- Identify or rule out switch module issues.
- Diagnose and correct Layer 2 issues.
- Diagnose and correct Layer 3 issues.
- Recover from switch upgrade failures.
- Obtain core dumps and other diagnostic data for use by Cisco TAC or your customer support representative.
System Messages

The system software sends syslog (system) messages to the console (and, optionally, to a logging server on another device). Not all messages indicate a problem with your device. Some messages are purely informational, while others might help diagnose problems with links, internal hardware, or the device software.

System message text is a text string that describes the condition. This portion of the message might contain detailed information about the event, including terminal port numbers, network addresses, or addresses that correspond to locations in the system memory address space. Because the information in these variable fields changes from message to message, it is represented here by short strings enclosed in square brackets ([ ]). A decimal number, for example, is represented as [dec ].

PORT-3-IF_UNSUPPORTED_TRANSCEIVER: Transceiver for interface [chars] is not supported.

Each system message is followed by an explanation and recommended action. The action may be as simple as "No action is required." It might involve a fix or a recommendation to contact technical support as shown in the following example:

**ErrorMessage** PORT-3-IF_UNSUPPORTED_TRANSCEIVER: Transceiver for interface [chars] is not supported.

**Explanation** Transceiver (SFP) is not from an authorized vendor.

**Recommended Action** Enter the show interface transceiver CLI command or similar DCNM command to determine the transceiver being used. Please contact your customer support representative for a list of authorized transceiver vendors.

Syslog Server Implementation

The syslog facility allows the device to send a copy of the message log to a host for more permanent storage. This feature allows you to examine the logs over a long period of time or if the device is not accessible.

This example shows how to configure the device to use the syslog facility on a Solaris platform. Although a Solaris host is being used, the syslog configuration on all UNIX and Linux systems is very similar.

Syslog uses the facility to determine how to handle a message on the syslog server (the Solaris system in this example) and the message severity. Different message severities are handled differently by the syslog server. They could be logged to different files or e-mailed to a particular user. Specifying a severity level on the syslog server determines that all messages of that level and greater severity (lower number) will be acted upon as you configure the syslog server.
You should configure the syslog server so that the Cisco NX-OS messages are logged to a different file from the standard syslog file so that they cannot be confused with other non-Cisco syslog messages. Do not locate the logfile on the / file system. You do not want log messages to fill up the / file system. This example uses the following values:

- syslog client: switch1
- syslog server: 172.22.36.211
- (Solaris) syslog facility: local1
- syslog severity: notifications (level 5, the default)
- File to log Cisco NX-OS messages to: /var/adm/nxos_logs

To configure the syslog feature on Cisco NX-OS, follow these steps:

1. switch# config terminal
2. switch(config)# logging server 192.0.2.16 facility local1

Use the `show logging server` command to verify the syslog configuration.

switch1# show logging server
Logging server: enabled
{172.22.36.211}
    server severity: notifications
    server facility: local1
    server VRF: management

To configure a syslog server, follow these steps:

1. Modify /etc/syslog.conf to handle local1 messages. For Solaris, you must allow at least one tab between the facility.severity and the action (/var/adm/nxos_logs).
   
   local1.notice /var/adm/nxos_logs

2. Create the log file.
   
   touch /var/adm/nxos_logs

3. Restart the syslog process.
   
   /etc/init.d/syslog stop
   /etc/init.d/syslog start
   
   syslog service starting.

4. Verify that the syslog process has started.
   
   ps -ef | grep syslogd

Test the syslog server by creating an event in Cisco NX-OS. In this case, port e1/2 was shut down and reenabled, and the following was listed on the syslog server. The IP address of the device is listed in brackets.

```
tail -f /var/adm/MDS_logs
Sep 17 11:07:41 (172.22.36.142.2.2) : 2013 Sep 17 11:17:29 pacific:
PORT-5-IF_DOWN_INITIALIZING: %VLAN 1%$ Interface e 1/2 is down (Initializing)
Sep 17 11:07:49 (172.22.36.142.2.2) : 2013 Sep 17 11:17:36 pacific: %PORT-5-IF_UP: %VLAN 1%$ Interface e 1/2 is up in mode access
Sep 17 11:07:51 (172.22.36.142.2.2) : 2013 Sep 17 11:17:39 pacific:
```
Troubleshooting with Logs

Cisco NX-OS generates many types of system messages on the device and sends them to a syslog server. You can view these messages to determine what events might have led up to the current condition that you are facing.

Use the following commands to access and view logs in Cisco NX-OS:

```
switch# show logging ?
console Show console logging configuration
info Show logging configuration
internal syslog syslog internal information
ip IP configuration
last Show last few lines of logfile
level Show facility logging configuration
logfile Show contents of logfile
loopback Show logging loopback configuration
module Show module logging configuration
monitor Show monitor logging configuration
nvram Show NVRAM log
onboard show logging onboard
server Show server logging configuration
source-interface Show logging source-interface configuration
timestamp Show logging timestamp configuration
```

This example shows the output of the `show logging server` command:

```
switch# show logging server
Logging server: enabled
{172.28.254.254}
server severity: notifications
server facility: local7
server VRF: management
```

Troubleshooting Modules

You can directly connect to a module console port to troubleshoot module bootup issues. Use the `attach console module` command to connect to the module console port.

Viewing NVRAM Logs

System messages that are priority 0, 1, or 2 are logged into NVRAM on the supervisor module. After a switch reboots, you can display these syslog messages in NVRAM by using the `show logging nvram` command:

```
switch# show logging nvram
2013 Sep 10 15:51:58 switch %$ VDC-1 %$ %SYSMGR-2-NON_VOLATILE_DB_FULL: System non-volatile storage usage is unexpectedly high at 99%.
2013 Sep 10 15:52:13 switch %$ VDC-1 %$ %PLATFORM-2-PFM_SYSTEM_RESET: Manual system restart from Command Line Interface
2013 Sep 10 15:57:49 switch %$ VDC-1 %$ %KERN-2-SYSTEM_MSG: Starting kernel... - kernel
2013 Sep 10 15:58:00 switch %$ VDC-1 %$ %CARDCLIENT-2-REG: Sent
2013 Sep 10 15:58:01 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG: R2D2: P1 SUP NO GMTL FOR P1 SUP - r2d2
2013 Sep 10 15:58:01 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG: R2D2: P1 SUP NO GMTL FOR P1 SUP - r2d2
2013 Sep 10 15:58:05 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG: R2D2: P1 SUP: Reset Tx/Rx during QOS INIT - r2d2
```
Contacting Customer Support

If you are unable to solve a problem after using the troubleshooting suggestions in this document, contact a customer service representative for assistance and further instructions. Before you call, have the following information ready to help your service provider assist you as quickly as possible:

• Date that you received the device
• Chassis serial number (located on a label on the right side of the rear panel of the chassis)
• Type of software and release number
• Maintenance agreement or warranty information
• Brief description of the problem
• Brief explanation of the steps that you have already taken to isolate and resolve the problem

For more information on steps to take before calling Technical Support, see Before Contacting Technical Support, on page 99.
Troubleshooting Installations, Upgrades, and Reboots

This chapter contains the following sections:

- About Upgrades and Reboots, page 11
- Upgrade and Reboot Checklist, page 11
- Verifying Software Upgrades, page 12
- Troubleshooting Software Upgrades and Downgrades, page 13
- Troubleshooting Software System Reboots, page 14

About Upgrades and Reboots

Upgrades and reboots are ongoing network maintenance activities. You should try to minimize the risk of disrupting the network when performing these operations in production environments and to know how to recover quickly when something does go wrong.

Note

This publication uses the term upgrade to refer to both Cisco NX-OS upgrades and downgrades.

Upgrade and Reboot Checklist

Use the following checklist to prepare for an upgrade or reboot:

<table>
<thead>
<tr>
<th>Checklist</th>
<th>Done</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read the Release Notes for the release to which you are upgrading or downgrading.</td>
<td></td>
</tr>
<tr>
<td>Ensure that an FTP or TFTP server is available to download the software image.</td>
<td></td>
</tr>
<tr>
<td>Copy the new image onto your supervisor modules in bootflash: or slot0:</td>
<td></td>
</tr>
</tbody>
</table>
Verifying Software Upgrades

You can use the `show install all status` command to watch the progress of your software upgrade or to view the ongoing `install all` command or the log of the last installed `install all` command from a console, SSH, or Telnet session. This command shows the `install all` output on both the active and standby supervisor module even if you are not connected to the console terminal.
Troubleshooting Software Upgrades and Downgrades

Software Upgrade Ends with Error

<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The upgrade ends with an error</td>
<td>The standby supervisor module bootflash: file system does not have sufficient space to accept the updated image.</td>
<td>Use the delete command to remove unnecessary files from the file system.</td>
</tr>
<tr>
<td></td>
<td>The <strong>install all</strong> command is entered on the standby supervisor module.</td>
<td>Enter the command on the active supervisor module only.</td>
</tr>
<tr>
<td></td>
<td>A module was inserted while the upgrade was in progress.</td>
<td>Restart the installation.</td>
</tr>
<tr>
<td></td>
<td>The system experienced a power disruption while the upgrade was in progress.</td>
<td>Restart the installation.</td>
</tr>
<tr>
<td></td>
<td>An incorrect software image path was specified.</td>
<td>Specify the entire path for the remote location accurately.</td>
</tr>
<tr>
<td></td>
<td>Another upgrade is already in progress.</td>
<td>Verify the state of the system at every stage and restart the upgrade after 10 seconds. If you restart the upgrade within 10 seconds, the command is rejected. An error message displays, indicating that an upgrade is currently in progress.</td>
</tr>
<tr>
<td></td>
<td>A module failed to upgrade.</td>
<td>Restart the upgrade or use the <strong>install module</strong> command to upgrade the failed module.</td>
</tr>
</tbody>
</table>

Upgrading the Cisco NX-OS Software

You can perform an automated software upgrade on any system from the CLI.

**Before You Begin**

Log into the system through the console, Telnet, or SSH port of the active supervisor.
Create a backup of your existing configuration file, if required.
### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>install all [nxos bootflash:filename]</strong></td>
</tr>
</tbody>
</table>

**Note** If the configuration meets all guidelines when the `install all` command is used, all modules (supervisor and switching) are upgraded.

**Note** If you enter the `install all` command without specifying a filename, the command performs a compatibility check, notifies you of the modules that will be upgraded, and confirms that you want to continue with the installation. If you choose to proceed, it installs the NXOS software image that is currently running on the switch and upgrades the BIOS of various modules from the running image if required.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td><code>show module</code></td>
</tr>
</tbody>
</table>

### Troubleshooting Software System Reboots

#### Power-On or Switch Reboot Hangs

<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>A power-on or switch reboot hangs for a dual supervisor configuration</td>
<td>The bootflash is corrupted.</td>
<td>See Recovering Both Supervisor Modules with Corrupted Bootflash.</td>
</tr>
<tr>
<td></td>
<td>The BIOS is corrupted.</td>
<td>Replace this module. Contact your customer support representative to return the failed module.</td>
</tr>
<tr>
<td></td>
<td>The nx-os image is corrupted.</td>
<td>Power cycle the switch if required and press Ctrl-C when the switch displays the &quot;Loading Boot Loader&quot; message to interrupt the boot process at the &gt;loader prompt. See Recovery From the loader&gt; Prompt on Supervisor Modules to update the nx-os image.</td>
</tr>
<tr>
<td></td>
<td>Boot parameters are incorrect.</td>
<td>Verify and correct the boot parameters and reboot.</td>
</tr>
</tbody>
</table>

### Corrupted Bootflash Recovery

All device configurations reside in the internal bootflash. If you have a corrupted internal bootflash, you could potentially lose your configuration. Be sure to save and back up your configuration files periodically. The regular system boot goes through the following sequence:
The basic input/output system (BIOS) loads the loader.

The loader loads the nx-os image into RAM and starts the image.

The nx-os image reads the startup configuration file.

If the nx-os image on your system is corrupted and you cannot proceed (error state), you can interrupt the system boot sequence and recover the image by entering the BIOS configuration utility described in the following section. Access this utility only when needed to recover a corrupted internal disk.

Caution
The BIOS changes explained in this section are required only to recover a corrupted bootflash.

Recovery procedures require the regular sequence to be interrupted. The internal sequence goes through three phases between the time that you turn on the system and the time that the system prompt appears on your terminal—BIOS, boot loader, and nx-os image. The following table describes the steps in the recovery interruption process.

Table 2: Recovery Interruption

<table>
<thead>
<tr>
<th>Phase</th>
<th>Normal Prompt (appears at the end of each phase)</th>
<th>Recovery Prompt (appears when the system cannot progress to the next phase)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIOS</td>
<td>loader&gt;</td>
<td>No bootable device</td>
<td>The BIOS begins the power-on self test, memory test, and other operating system applications. While the test is in progress, press Ctrl-C to enter the BIOS configuration utility and use the netboot option.</td>
</tr>
<tr>
<td>Boot loader</td>
<td>Starting nx-os</td>
<td>loader&gt;</td>
<td>The boot loader uncompresses the loaded software to boot an image using its filename as a reference. The image is made available through bootflash. When the memory test is over, press Esc to enter the boot loader prompt.</td>
</tr>
<tr>
<td>nx-os image</td>
<td>Uncompressing system</td>
<td>switch(boot)#</td>
<td>When the boot loader phase is over, press Ctrl-[ (Control key plus right bracket key) to enter the switch(boot)# prompt. Depending on your Telnet client, these keys might be reserved, and you might need to remap the keystroke. See the documentation provided by your Telnet client. If the corruption causes the console to stop at this prompt, copy the nx-os image and reboot the system. The nx-os image then loads the configuration file of the last saved running configuration and returns a switch login prompt.</td>
</tr>
</tbody>
</table>
Recovery from the loader> Prompt

Use the `help` command at the loader> prompt to display a list of commands available at this prompt or to obtain more information about a specific command in that list.

### Before You Begin

This procedure uses the `init system` command, which reformats the file system of the device. Be sure that you have made a backup of the configuration files before you begin this procedure.

The loader> prompt is different from the regular switch# or switch(boot)# prompt. The CLI command completion feature does not work at the loader> prompt and might result in undesired errors. You must type the command exactly as you want the command to appear.

If you boot over TFTP from the loader> prompt, you must supply the full path to the image on the remote server.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>loader&gt; set ip ip-address</code></td>
<td>Specifies the local IP address and the subnet mask for the system.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>loader&gt; set ip 172.21.55.213 255.255.255.224</code></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>loader&gt; set gw gw-address</code></td>
<td>Specifies the IP address of the default gateway.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>loader&gt; set gw 172.21.55.193</code></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>loader&gt; cmdline recoverymode=1</code></td>
<td>Configures the boot process to stop at the switch(boot)# prompt.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>loader&gt; cmdline recoverymode=1</code></td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>loader&gt; boot tftp: tftp-path</code></td>
<td>Boots the nx-os image file from the required server.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>loader&gt; boot tftp://172.28.255.18/tftpboot/n9000-dk9.6.1.2.I1.1.bin</code></td>
</tr>
<tr>
<td><strong>Step 5</strong> <code>switch(boot)# init system</code></td>
<td>Enters the nx-os system.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>switch(boot)# init system</code></td>
</tr>
</tbody>
</table>

**Caution**

Be sure that you have made a backup of the configuration files before you enter this command. See the [Recovery from the switch(boot)# Prompt](#) procedure.
**Purpose**

Command or Action

<table>
<thead>
<tr>
<th>Step 6</th>
<th>switch(boot)# load-nxos</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>switch(boot)# load-nxos</td>
</tr>
</tbody>
</table>

Completes the upload of the `nx-os` image file.

This example shows how to configure the local IP address and the subnet mask for the system:

```
loader> set ip 172.21.55.213 255.255.255.224
Correct - ip addr is 172.21.55.213, mask is 255.255.255.224
Found Intel 82546GB [2:9.0] at 0xe040, ROM address Ox980
Probing...[Intel 82546GB]
Management interface
Link UP in 1000/full mode
Ethernet addr: 00:1B:54:C1:28:60
Address: 172.21.55.213
Netmask: 255.255.255.224
Server: 0.0.0.0
Gateway: 172.21.55.193
```

This example shows how to configure the IP address of the default gateway:

```
loader> set gw 172.21.55.193
Correct gateway addr 172.21.55.193
Address: 172.21.55.213
Netmask: 255.255.255.224
Server: 0.0.0.0
Gateway: 172.21.55.193
```

This example shows how to boot the `nx-os` image from the server:

```
loader> boot tftp://172.28.255.18/tftpboot/n9000-dk9.6.1.2.I1.1.bin
Address: 172.21.55.213
Netmask: 255.255.255.224
Server: 172.28.255.18
Gateway: 172.21.55.193
Filesystem type is tftp, using whole disk
Booting: /tftpboot/n9000-dk9.6.1.2.I1.1.globin console=ttyS0,9600n8n quiet loader
_ver="3.17.0"....
..........................................................................
Image verification OK
Starting kernel...
INIT: version 2.85 booting
Checking all filesystems..r.r.. done.
Setting kernel variables: sysctlnet.ipv4.ip_forward = 0
net.ipv4.ip_default_ttl = 64
net.ipv4.ip_no_pmtu_disc = 1
Setting the System Clock using the Hardware Clock as reference...System Clock set. Local
time: Wed Oct 1
11:20:11 PST 2013
WARNING: image sync is going to be disabled after a loader netboot
Loading system software
No system image Unexporting directories for NFS kernel daemon...done.
INIT: Sending processes the KILL signal
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2013, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
System or Process Restarts

When a recoverable or nonrecoverable error occurs, the system or a process on the system might reset. This table lists possible causes and solutions.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The system or a process on the system resets.</td>
<td>A recoverable error occurred on the system or on a process in the system.</td>
<td>The system has automatically recovered from the problem. See Recovering System Restarts, on page 18.</td>
</tr>
<tr>
<td>A nonrecoverable error occurred on the system.</td>
<td>The system cannot recover automatically from the problem. See Recovering System Restarts, on page 18 to determine the cause.</td>
<td></td>
</tr>
<tr>
<td>A clock module failed.</td>
<td>Verify that a clock module failed. Replace the failed clock module during the next maintenance window.</td>
<td></td>
</tr>
</tbody>
</table>

Recovering System Restarts

Every process restart generates a syslog message and a Call Home event. Even if the event does not affect service, you should identify and resolve the condition immediately because future occurrences could cause a service interruption.

Note

After following the steps, determine the cause and resolution for the restart condition by contacting your technical support representative and asking the representative to review your core dump.

Before You Begin

The following conditions apply:

- The system automatically copies the core files to a TFTP server every 4 minutes. This time interval is not configurable.
- The copy of a specific core file to a TFTP server can be manually triggered by using the `copy core://module#//pid# //tftp://tftp_ip_address/file_name` command.
- If a supervisor failover occurs, the cores might be in the secondary logflash rather than the primary logflash.
• The maximum number of times that a process can be restarted is part of the high-availability (HA) policy for any process. (This parameter is not configurable.) If the process restarts more than the maximum number of times, the older core files are overwritten.

• The maximum number of core files that can be saved for any process is part of the HA policy for any process. (This parameter is not configurable, and it is set to three.)

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> switch# show log</td>
<td>Displays the syslog file so you can see which process restarted and why it restarted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch# show log logfile</td>
<td>include error</td>
</tr>
<tr>
<td>Sep 10 23:31:31 dot-6 % LOG_SYSMGR-3-SERVICE TERMINATED: Service &quot;sensor&quot; (PID 704) has finished with error code SYSMGR_EXITCODE SY.</td>
<td></td>
</tr>
<tr>
<td>switch# show logging logfile</td>
<td>include fail</td>
</tr>
<tr>
<td>Jan 27 04:08:42 88 %LOG_DAEMON-3-SYSTEM_MSG: bind() fd 4, family 2, port 123, ad dr 0.0.0.0, in_classd=0 flags=1 fails: Address already in use</td>
<td></td>
</tr>
<tr>
<td>Jan 27 04:08:42 88 %LOG_DAEMON-3-SYSTEM_MSG: bind() fd 4, family 2, port 123, ad dr 127.0.0.1, in_classd=0 flags=0 fails: Address already in use</td>
<td></td>
</tr>
<tr>
<td>Jan 27 04:08:42 88 %LOG_DAEMON-3-SYSTEM_MSG: bind() fd 4, family 2, port 123, ad dr 127.1.1.1, in_classd=0 flags=1 fails: Address already in use</td>
<td></td>
</tr>
<tr>
<td>Jan 27 04:08:42 88 %LOG_DAEMON-3-SYSTEM_MSG: bind() fd 4, family 2, port 123, ad dr 172.22.93.88, in_classd=0 flags=1 fails: Address already in use</td>
<td></td>
</tr>
<tr>
<td>Jan 27 23:18:59 88 % LOG_PORT-5-IF_DOWN: Interface fc1/13 is down (Link failure or not-connected)</td>
<td></td>
</tr>
<tr>
<td>Jan 27 23:18:59 88 % LOG_PORT-5-IF_DOWN: Interface fc1/14 is down (Link failure or not-connected)</td>
<td></td>
</tr>
<tr>
<td>Jan 27 00:55:12 88 % LOG_PORT-5-IF_DOWN: Interface fc1/1 is down (Link failure or not-connected)</td>
<td></td>
</tr>
<tr>
<td>Jan 28 00:58:06 88 % LOG_ZONE-2-ZS_MERGE_FAILED: Zone merge failure, Isolating port fc1/1 (VSAN 100)</td>
<td></td>
</tr>
<tr>
<td>Jan 28 00:58:44 88 % LOG_ZONE-2-ZS_MERGE_FAILED: Zone merge failure, Isolating port fc1/1 (VSAN 100)</td>
<td></td>
</tr>
<tr>
<td>Jan 28 03:26:38 88 % LOG_ZONE-2-ZS_MERGE_FAILED: Zone merge failure, Isolating port fc1/1 (VSAN 100)</td>
<td></td>
</tr>
<tr>
<td>Jan 29 19:01:34 88 % LOG_PORT-5-IF_DOWN: Interface fc1/1 is down (Link failure or not-connected)</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> switch# show processes</td>
<td>Displays the processes that are running and the status of each process.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>The following codes are used in the system output for the state (process state):</td>
</tr>
<tr>
<td>switch# show processes</td>
<td></td>
</tr>
<tr>
<td>PID State PC Start_cnt TTY Process</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>S</td>
<td>2ab8e33e</td>
<td>1</td>
<td>-</td>
<td>init</td>
</tr>
<tr>
<td>2</td>
<td>S</td>
<td>0</td>
<td>1</td>
<td>-</td>
<td>keventd</td>
</tr>
<tr>
<td>3</td>
<td>S</td>
<td>0</td>
<td>1</td>
<td>-</td>
<td>ksoftirqd_CPU0</td>
</tr>
<tr>
<td>4</td>
<td>S</td>
<td>0</td>
<td>1</td>
<td>-</td>
<td>kswapd</td>
</tr>
<tr>
<td>5</td>
<td>S</td>
<td>0</td>
<td>1</td>
<td>-</td>
<td>bflush</td>
</tr>
<tr>
<td>6</td>
<td>S</td>
<td>0</td>
<td>1</td>
<td>-</td>
<td>kupdater</td>
</tr>
<tr>
<td>71</td>
<td>S</td>
<td>0</td>
<td>1</td>
<td>-</td>
<td>kjournald</td>
</tr>
<tr>
<td>136</td>
<td>S</td>
<td>0</td>
<td>1</td>
<td>-</td>
<td>kjournald</td>
</tr>
<tr>
<td>140</td>
<td>S</td>
<td>0</td>
<td>1</td>
<td>-</td>
<td>kjournald</td>
</tr>
<tr>
<td>431</td>
<td>S</td>
<td>2ab333e</td>
<td>1</td>
<td>-</td>
<td>httpd</td>
</tr>
<tr>
<td>443</td>
<td>S</td>
<td>2abf33e</td>
<td>1</td>
<td>-</td>
<td>httpd</td>
</tr>
<tr>
<td>446</td>
<td>S</td>
<td>2ace33e</td>
<td>1</td>
<td>-</td>
<td>sysmgr</td>
</tr>
<tr>
<td>452</td>
<td>S</td>
<td>2ab91a2</td>
<td>1</td>
<td>-</td>
<td>httpd</td>
</tr>
<tr>
<td>453</td>
<td>S</td>
<td>2ab91a2</td>
<td>1</td>
<td>-</td>
<td>httpd</td>
</tr>
<tr>
<td>454</td>
<td>S</td>
<td>2ac7a19</td>
<td>1</td>
<td>-</td>
<td>vsh</td>
</tr>
<tr>
<td>469</td>
<td>S</td>
<td>2ab91a2</td>
<td>1</td>
<td>-</td>
<td>httpd</td>
</tr>
<tr>
<td>470</td>
<td>S</td>
<td>2ab91a2</td>
<td>1</td>
<td>-</td>
<td>httpd</td>
</tr>
</tbody>
</table>

### Purpose

- **D** = uninterruptible sleep (usually I/O)
- **R** = runnable (on run queue)
- **S** = sleeping
- **T** = traced or stopped
- **Z** = defunct (zombie) process
- **NR** = not running
- **ER** = should be running but currently not running

**Note**: **ER** usually is the state that a process enters if it has been restarted too many times and has been detected as faulty by the system and disabled.

### Step 3

**switch# show process log**  
Displays the processes that have had abnormal exits and if there is a stack-trace or core dump.

#### Example:

```plaintext
switch# show process log
Process PID Normal-exit Stack-trace Core Log-create-time
----- --- ----------- ----------- ---- -------------
ntp  919 N    N    N    Jan 27 04:08
snsm 972 N    Y    N    Jan 24 20:50
```

### Step 4

**switch# show process log pid pid**  
Displays detailed information about a specific process that has restarted.

#### Example:

```plaintext
switch# show processes log pid 898
Service: idehsd
Description: ide hotswap handler Daemon
Started at Mon Sep 16 14:56:04 2013 (390923 us)
Stopped at Thu Sep 19 14:18:42 2013 (639239 us)
Uptime: 2 days 23 hours 22 minutes 22 seconds
Start type: SRV_OPTION_RESTART_STATELESS (23)
Death reason: SYSMGR_DEATH_REASON_FAILURE_SIGTERM (3)
Exit code: signal 15 (no core)
CWD: /var/sysmgr/work
Virtual Memory:
CODE 08048000 - 0804D660
DATA 0804E660 - 0804E924
BRK 0804E9A0 - 08050000
STACK 7FFFFD10
Register Set:
EDX 00000003  ECX 0804E994  EDX 00000008
   ESI 00000005  EDI 7FFFFC9C  EBP 7FFFFCAC
   EAX 00000008  XDS 0000002B  XES 0000002B
```
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAX 00000003 (orig) EIP 2ABF5EF4 XCS 00000023</td>
<td></td>
</tr>
<tr>
<td>EFL 00000246 ESP 7FFFC5C XSS 0000002B</td>
<td>Stack: 128 bytes. ESP 7FFFC5C, TOP 7FFFD10 0x7FFFC5C: 804F990 804C416 00000003 804F994 .......................... 0x7FFFC6C: 00000008 0804BF95 2AC451E0 2AAC24A4 ..............Q.<em>:</em>.* 0x7FFFC7C: 7FFFD14 2AC2C581 804E6BC 7FFFC8A .......................... 0x7FFFC8C: 7FFFC94 00000003 00000001 00000003 .......................... 0x7FFFC9C: 00000001 00000000 00000068 00000000 ............h........ 0x7FFFCAC: 7FFFCB4 2AB4F819 00000001 7FFFD14 .......................... 0x7FFFCBC: 7FFFD1C 804C470 00000000 7FFFCBE .......................... 0x7FFFCDC: 2AB4F7E9 2AAC1F00 00000001 8048A2C .......................... PID: 898 SAP: 0 UUID: 0 switch#</td>
</tr>
</tbody>
</table>

#### Step 5

**switch# show system uptime**

**Example:**

```bash
switch# show system uptime
Start Time: Fri Sep 13 12:38:39 2013
Up Time: 0 days, 1 hours, 16 minutes, 22 seconds
```

#### Step 6

**switch# show cores**

**Example:**

```bash
switch# show cores
Module Instance Process-name PID Date(Year-Month-Day Time)
--------- -------- ------------ ----
28 1 bgp-64551 5179 2013-09-13 23:51:26
```

#### Step 7

**switch# copy core: core path**

**Example:**

```bash
switch# copy core://5/1524 tftp::/1.1.1.1/abcd
```

#### Step 8

**switch# show processes log pid pid**

**Example:**

```bash
switch# "show processes log pid 1473"
Service: ips
Description: IPS Manager

Started at Tue Jan  8 17:07:42 2013 (757583 us)
Stopped at Thu Jan 10 06:16:45 2013 (83451 us)
```
### Command or Action
- Uptime: 1 days 13 hours 9 minutes 9 seconds
- Start type: SRV_OPTION_RESTART_STATELESS (23)
- Death reason: SYSMGR_DEATH_REASON_FAILURE_SIGNAL (2)
- Exit code: signal 6 (core dumped)
- CWD: /var/sysmgr/work

### Virtual Memory:
- CODE: 08048000 - 080FB060
- DATA: 080FC060 - 080FCBA8
- BRK: 081795C0 - 081EC000
- STACK: 7FFFFFFF0
- TOTAL: 20952 KB

### Register Set:
- EBX: 000005C1
- ECX: 00000006
- EDX: 2AD721E0
- ESI: 2AD701A8
- EDI: 08109308
- EBP: 7FFFF2EC
- EAX: 00000000
- XDS: 000002B
- XES: 0000002B
- EAX: 0000025 (orig)
- EIP: 2AC8CC71
- EFL: 00000207
- ESP: 7FFFF2C0
- XSS: 0000002B

### Stack:
- 2608 bytes. ESP 7FFFFFFC0, TOP 7FFFFFFF0

```plaintext
0x7FFFFFFC0: 2AC8C944 000005C1 00000006 2AC735E2
0x7FFFFFFD0: 2AC8C92C 2AD721E0 2AAB76F0 00000000
0x7FFFFFFE0: 7FFFFFFF0 2AC8C920 2AC513F8 7FFFFFFF42C ...
0x7FFFFFFF20: 2AC8E0BB 00000000 7FFFFFFF320 00000000 ...*
0x7FFFFFFF30: 2AC8DF88 2AD721E0 08109308 2AC65AFC ...
0x7FFFFFFF40: 00000039 2AC6A49C 2AC621CC 2AC513F8 ...
0x7FFFFFFF50: 00000020 00000000 00000000 00000000 ...
0x7FFFFFFF60: 00000000 00000000 00000000 00000000 ...
0x7FFFFFFF70: 00000000 00000000 00000000 00000000 ...
0x7FFFFFFF80: 00000000 00000000 00000000 00000000 ...
0x7FFFFFFF90: 00000000 00000000 00000000 00000000 ...
0x7FFFFFFFA0: 00000002 7FFFFFFF4 2AAB752D 2AC5154C ...
```

### Stack:
- 128 bytes. ESP 7FFFFFF830, TOP 7FFFFFFF0

```plaintext
... output abbreviated ...
Stack: 128 bytes. ESP 7FFFFFFF30, TOP 7FFFFFFF0
```
### Unrecoverable System Restarts

An unrecoverable system restart might occur in the following cases:

- A critical process fails and is not restartable.
- A process restarts more times than is allowed by the system configuration.
- A process restarts more frequently than is allowed by the system configuration.

The effect of a process reset is determined by the policy configured for each process. An unrecoverable reset might cause functionality loss, the active supervisor to restart, a supervisor switchover, or the system to restart.

The `show system reset-reason` command displays the following information:

- The last four reset-reason codes for a specific module in a given slot. If a module is absent, the reset-reason codes for that module are not displayed.
- The overall history of when and why expected and unexpected reloads occur.
- The time stamp of when the reset or reload occurred.
- The reason for the reset or reload of a module.
- The service that caused the reset or reload (not always available).
- The software version that was running at the time of the reset or reload.

```bash
switch# show system reset-reason module 27
----- reset reason for Supervisor-module 27 (from Supervisor in slot 27) ---
1) At 281000 usecs after Wed Jun 26 20:16:34 2013
   Reason: Reset Requested by CLI command reload
   Service:
   Version: 6.1(2)I1(1)
2) At 791071 usecs after Wed Jun 26 20:04:50 2013
   Reason: Reset Requested by CLI command reload
   Service:
   Version: 6.1(2)I1(1)
   Reason: Reset Requested by CLI command reload
   Service:
   Version: 6.1(2)I1(1)
4) At 891463 usecs after Wed Jun 26 23:44:48 2013
   Reason: Reset Requested by CLI command reload
   Service:
   Version: 6.1(2)I1(1)
```
Standby Supervisor Fails to Boot

The standby supervisor does not boot after an upgrade. You may see the following system message:

SYSMGR-2-STANDBY_BOOT_FAILED

This message is printed if the standby supervisor does not complete its boot procedure (does not reach the login prompt on the local console) 3 to 6 minutes after the loader has been loaded by the BIOS. This message is usually caused by boot variables not properly set for the standby supervisor. This message can also be caused by a user intentionally interrupting the boot procedure at the loader prompt (by pressing ESC).

Connect to the local console of the standby supervisor. If the supervisor is at the loader prompt, try to use the **boot** command to continue the boot procedure. Otherwise, enter the **reload** command for the standby supervisor from a vsh session on the active supervisor, specifying the **force-dnld** option. Once the standby is online, fix the problem by setting the boot variables appropriately.

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Possible Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standby supervisor does not boot</td>
<td>Active supervisor nx-os image booted from TFTP.</td>
<td>Reload the active supervisor from bootflash:.</td>
</tr>
</tbody>
</table>

Recovering the Administrator Password

You can recover the network administrator password using one of these methods:

- From the CLI with a username that has network-admin privileges
- By power cycling the device
- By reloading the device

Using the CLI with Network-Admin Privileges to Recover the Administrator Password

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>switch# show user-account</td>
<td>Shows that your username has network-admin privileges.</td>
</tr>
</tbody>
</table>

**Example:**

```
switch# show user-account
user:admin
  this user account has no expiry date
  roles:network-admin
user:dbgusr
  this user account has no expiry date
  roles:network-admin network-operator
```
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>&lt;br&gt;switch# configure terminal&lt;br&gt;switch(config)#</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>switch(config)# username admin password new-password</td>
<td>Assigns a new network administrator password if your username has network-admin privileges.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>&lt;br&gt;switch(config)# username admin password egBdf</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>switch(config)# copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>&lt;br&gt;switch(config)# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

### Power Cycling the Device to Recover the Administrator Password

If you cannot start a session on the device that has network-admin privileges, you can recover the network administrator password by power cycling the device.

#### Caution
The password recovery procedure disrupts all traffic on the device. All connections to the device will be lost for 2 to 3 minutes.

#### Note
You cannot recover the administrator password from a Telnet or Secure Shell (SSH) session to the management interface. You must have access to the local console connection.

#### Note
Password recovery updates the new administrator password only in the local user database and not on the remote AAA servers. The new password works only if local authentication is enabled; it does not work for remote authentication. When a password is recovered, local authentication is enabled for logins through a console so that the admin user can log in with a new password from a console.

#### Note
If you need to recover the password because the username was not specified in the configuration file when you performed a `copy configuration-file startup-config` followed by the `fast-reload` or `reload` command, you will need to perform a `write erase` in Step 12 below.
Before You Begin

On a device with two supervisor modules, you must perform the password recovery procedure on the supervisor module that will become the active module after you complete the recovery procedure. To ensure that the other supervisor module does not become active, perform one of the following tasks:

- Remove the other supervisor module from the chassis.
- Change the console prompt of the other supervisor module to one of the following two prompts until the recovery procedure completes:
  - loader >
  - switch(boot)#

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Establish a terminal session on the console port of the active supervisor module.</td>
<td>Note: If you are using a non-U.S. keymap, the key sequence that you need to press to generate the break sequence might not work. In this case, we recommend that you set your terminal to a U.S. keymap. You can enter Ctrl-C instead of Ctrl-[ (right square bracket) due to keyboard mapping.</td>
</tr>
</tbody>
</table>

| Step 2 | If you use SSH or a terminal emulator to access the console port, go to Step 6. | — |
|        | If you use Telnet to access the console port, press Ctrl-[ (right square bracket) to verify that it does not conflict with the Telnet escape sequence. | — |

**Example:**
```bash
switch login: Ctrl-]
```

| Step 3 | If the Cisco NX-OS login prompt remains and the Telnet prompt does not appear, go to Step 6. | — |

**Note:** If the Cisco NX-OS login prompt remains and the Telnet prompt does not appear, go to Step 6.

**Example:**
```bash
telnet> set escape ^\nEscape Character is 'CTRL+' 
```

| Step 4 | Press Enter one or more times to return to the Cisco NX-OS login prompt. | — |

**Note:** If the Cisco NX-OS login prompt remains and the Telnet prompt does not appear, go to Step 6.
### Command or Action

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong> Power cycle the device.</td>
</tr>
<tr>
<td><strong>Step 7</strong> Press Ctrl-C to access the loader&gt; prompt.</td>
</tr>
<tr>
<td><strong>Step 8</strong> loader&gt; cmdline recoverymode=1</td>
</tr>
<tr>
<td><strong>Step 9</strong> loader&gt; boot n9000-dk9.x.x.x.bin</td>
</tr>
</tbody>
</table>

**Example:**

```
Example:
telnet> <Enter>
switch login:

Step 6
Power cycle the device.

Step 7
Press Ctrl-C to access the loader> prompt.

Example:
Ctrl-C
loader>

Step 8
loader> cmdline recoverymode=1

Example:
loader> cmdline recoverymode=1

Step 9
loader> boot n9000-dk9.x.x.x.bin

Example:
loader> boot n9000-dk9.x.x.x.bin
Bootling lash
Trying diskboot
Filesystem type is ext2fs, partition type 0x83
Image valid
MD5sum mismatch
INIT: Loading IGB driver ... Signature Envelope.(36)Invalid Tag in Signature Envelope Installing SSE module ... done
Creating the sse device node ... done
Installing CCTRL driver for card_type 3 ...
Checking all filesystems....... Installing SPROM driver ...
Installing default sprom values ... done.Configuring network ...
Installing psdev ...
Installing veobc ...
Installing OBFL driver ...
Starting portmap daemon ...
creating NFS state directory: done
starting 8 nfsd kernel threads: done
starting mountd: done
starting statd: done
Loading system software
No system image is specified
INIT: Sending processes the TERM signal
INIT: Sending processes the KILL signal
Bad terminal type: "linux". Will assume vt100.
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2013, Cisco Systems, Inc. All rights reserved. The copyrights to certain works contained in this software are owned by other third parties and used
```
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>and distributed under license. Certain components of this software are licensed under the GNU General Public License (GPL) version 2.0 or the GNU Lesser General Public License (LGPL) Version 2.1. A copy of each such license is available at <a href="http://www.opensource.org/licenses/gpl-2.0.php">http://www.opensource.org/licenses/gpl-2.0.php</a> and <a href="http://www.opensource.org/licenses/lgpl-2.1.php">http://www.opensource.org/licenses/lgpl-2.1.php</a></td>
<td></td>
</tr>
<tr>
<td>switch(boot)#</td>
<td></td>
</tr>
</tbody>
</table>

**Step 10**  
Press Enter one or more times to return to the Cisco NX-OS login prompt.  
**Example:**  
telnet> <Enter>  
switch login:  

**Step 11**  
switch(boot)# config terminal  
**Example:**  
switch(boot)# config terminal  
Enter configuration commands, one per line.  
End with CNTL/Z.  
switch(boot)(config)#  

**Step 12**  
switch(boot)(config)# admin-password new-password  
**Example:**  
switch(boot)(config)# admin-password egBdf  
WARNING! Remote Authentication for login through console has been disabled  

**Step 13**  
switch(boot)(config)# exit  
**Example:**  
switch(boot)(config)# exit  
switch(boot)#  

**Step 14**  
switch(boot)# load-nxos  
**Example:**  
switch(boot)# load-nxos  

---
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 15</strong></td>
<td>Log into the device using the new administrator password.</td>
</tr>
</tbody>
</table>
| **Example:**  | switch login: admin  
|               | Password: egBdf |
|                | The running configuration indicates that local authentication is enabled for logins through a console. You should not change the running configuration in order for the new password to work for future logins. You can enable remote authentication after you reset and remember the administrator password that is configured on the AAA servers. switch# show running-config aaa  
|                | !Command: show running-config aaa  
|                | !Time: Fri Jun 7 02:39:23 2013  
|                | version 6.1(2)I1(1)  
|                | logging level aaa 5  
|                | aaa authentication login  
|                | ascii-authentication |
| **Step 16**  | switch# configure terminal  
| **Example:**  | switch# configure terminal  
|               | switch(config)# |
|                | Enters global configuration mode. |
| **Step 17**  | switch(config)# username admin password  
|               | new-password  
| **Example:**  | switch(config)# username admin password egBdf |
|                | Resets the new password to ensure that it is also the Simple Network Management Protocol (SNMP) password. |
| **Step 18**  | switch(config)# exit  
| **Example:**  | switch(config)# exit  
|               | switch# |
|                | Exits global configuration mode. |
| **Step 19**  | Insert the previously removed standby supervisor module into the chassis, if necessary. |
| **Step 20**  | Boot the nx-os image on the standby supervisor module, if necessary. |
| **Step 21**  | switch(config)# copy running-config startup-config  
| **Example:**  | switch(config)# copy running-config  
|               | startup-config |
|                | Copies the running configuration to the startup configuration. |
Reloading the Device to Recover the Administrator Password

You can reset the network administrator password by reloading the device.

**Caution**
This procedure disrupts all traffic on the device. All connections to the device will be lost for 2 to 3 minutes.

**Note**
You cannot recover the administrator password from a Telnet or Secure Shell (SSH) session to the management interface. You must have access to the local console connection.

**Note**
Password recovery updates the new administrator password only in the local user database and not on the remote AAA servers. The new password works only if local authentication is enabled; it does not work for remote authentication. When a password is recovered, local authentication is enabled for logins through a console so that the admin user can log in with a new password from a console.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Establish a terminal session on the console port of the active supervisor module.</td>
<td>—</td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>switch# reload</code></td>
<td>Reloads the device to reach the loader prompt. You need to press Ctrl-C when the following appears: Booting nx-os image: bootflash:/n9000-dk9.x.x.x.bin...</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>switch# reload</code> This command will reboot the system. (y/n)? [n] y 2013 Jun 7 13:09:56 switch %$ VDC-1 %$ %PLATFORM-2-PFM_SYSTEM_RESET: Manual system restart from Command Line Interface writing reset reason 9, ... GNU GRUB version 0.97 Autobothing bootflash:/n9000-dk9.x.x.x.bin bootflash:/n... Filesystem type is ext2fs, partition type 0x83 Booting nx-os image: bootflash:/n9000-dk9.x.x.x.bin....(---) Press Ctrl + C) ....Aborting Image Boot GNU GRUB version 0.97 Loader Version 3.22.0 loader&gt;</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>loader&gt; boot n9000-dk9.x.x.x.bin</code></td>
<td>Restarts the device with only the nx-os image to reach the switch boot prompt.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>loader&gt; boot n9000-dk9.x.x.x.bin</code> Filesystem type is ext2fs, partition type 0x83 Booting nx-os image: n9000-dk9.6.1.2.II.1.gbin.... ................................. Image verification OK</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

Command or Action | Purpose
--- | ---
.. .. Lesser General Public License (LGPL) Version 2.1. A copy of each such license is available at http://www.opensource.org/licenses/gpl-2.0.php and http://www.opensource.org/licenses/lgpl-2.1.php switch(boot)\

**Step 4** Reset the network administrator password by following Steps 6 through 20 in Power Cycling the Device to Recover the Administrator Password, on page 25.
Troubleshooting Licensing Issues

This chapter contains the following sections:

• About Troubleshooting Licensing Issues, page 33
• Guidelines and Limitations for Licensing, page 33
• Initial Troubleshooting Checklist for Licensing, page 34
• Displaying License Information Using the CLI, page 34
• Licensing Installation Issues, page 35

About Troubleshooting Licensing Issues

Cisco NX-OS requires licenses for select features. The licenses enable those features on your system. You must purchase a license for each system on which you want to enable the licensed features.

Chassis Serial Numbers

Licenses are created using the serial number of the chassis where the license file is to be installed. Once you order a license based on a chassis serial number, you cannot use this license on any other system.

Swapping out a Chassis

If you swap out a chassis which included licenses, you must contact TAC to generate a new license. The old license was based on the chassis serial number and will not work with the new chassis.

Guidelines and Limitations for Licensing

Follow these guidelines when dealing with licenses for Cisco NX-OS:

• Carefully determine the license(s) that you require based on the features that require a license.
• Order your license accurately, as follows:
  • Enter the Product Authorization Key that appears in the Proof of Purchase document that comes with your system.
Enter the correct chassis serial number when ordering the license. The serial number must be for the same chassis on which you plan to install the license. Use the `show license host-id` command to obtain your chassis serial number.

Enter serial numbers accurately. Do not use the letter "O" instead of a zero in the serial number.

Order the license that is specific to your chassis.

- Back up the license file to a remote, secure place. Archiving your license files ensures that you will not lose the licenses in the case of a failure on your system.
- Install the correct licenses on each system, using the licenses that were ordered using that system's serial number. Licenses are serial-number specific and platform specific.
- Use the `show license usage` command to verify the license installation.
- Never modify a license file or attempt to use it on a system for which it was not ordered. If you return a chassis, contact your customer support representative to order a replacement license for the new chassis.

## Initial Troubleshooting Checklist for Licensing

Begin troubleshooting license issues by checking the following issues first:

<table>
<thead>
<tr>
<th>Checklist</th>
<th>Done</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify the chassis serial number for all licenses ordered.</td>
<td></td>
</tr>
<tr>
<td>Verify the platform or module type for all licenses ordered.</td>
<td></td>
</tr>
<tr>
<td>Verify that the Product Authorization Key that you used to order the licenses comes from the same chassis from which you retrieved the chassis serial number.</td>
<td></td>
</tr>
<tr>
<td>Verify that you have installed all licenses on all systems that require the licenses for the features you enable.</td>
<td></td>
</tr>
</tbody>
</table>

### Displaying License Information Using the CLI

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>`show license [host-id</td>
<td>usage [package]]`</td>
</tr>
</tbody>
</table>
This example displays all installed license key files and contents:

```
switch# show license
entp.lic:
SERVER this_host ANY
VENDOR cisco
INCREMENT LAN_ENTERPRISE_SERVICES_PKG cisco 1.0 permanent uncounted \ 
  VENDOR_STRING=\<LIC_SOURCE>MDS_SWIFT</LIC_SOURCE><SKU>N95-LAN1K9=</SKU> \ 
  HOSTID=VDH=TBC10412106 \ > 
  NOTICE="\LicFileID>20071025133322456</LicFileID>LicLineID>1/LicLineID>
```

This example displays information about current license usage:

```
switch# show license usage
Feature      Ins  Lic Status  Expiry Date  Comments  Count
--------------------------------------------------------------------------------------------------------
LAN_ENTERPRISE_SERVICES_PKG  No  -  In use
--------------------------------------------------------------------------------------------------------
```

This example displays a list of features in a specified package:

```
switch# show license usage LAN_ENTERPRISE_SERVICES_PKG
Application
-----------
bgp
pim
msdp
ospf
ospfv3
-----------
```

This example displays the host ID for the license:

```
switch# show license host-id
License hostid: VDH=FOX0646S017
```

Use the entire ID that appears after the colon (:). The VHD is the Vendor Host ID.

---

**Licensing Installation Issues**

### Serial Number Issues

Make sure that you use the correct chassis serial number when ordering your license. Use the `show license host-id` command to obtain the correct chassis serial number for your system using the CLI.

If you use a license meant for another chassis, you might see the following system message:

**Error Message:** LICMGR-3-LOG_LIC_INVALID_HOSTID: Invalid license hostid VDH=[chars] for feature [chars].

**Explanation:** The feature has a license with an invalid license Host ID. This can happen if a supervisor module with licensed features for one system is installed on another system.

**Recommended Action:** Reinstall the correct license for the chassis where the supervisor module is installed.
Note
When entering the chassis serial number during the license ordering process, do not use the letter "O" instead of any zeros in the serial number.

RMA Chassis Errors or License Transfers Between Systems

A license is specific to the system for which it is issued and is not valid on any other system. If you need to transfer a license from one system to another, contact your technical support representative.

License Listed as Missing

After a license is installed and operating properly, it might show up as missing if you modify your system hardware or encounter a bootflash: issue.

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Possible Causes</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>A license is listed as missing.</td>
<td>The supervisor module was replaced after the license was installed.</td>
<td>See Corrupted Bootflash Recovery, on page 14 to recover from the corrupted bootflash:. Reinstall the license.</td>
</tr>
<tr>
<td></td>
<td>The supervisor bootflash: is corrupted.</td>
<td></td>
</tr>
</tbody>
</table>
Troubleshooting Ports

This chapter contains the following sections:

- About Troubleshooting Ports, page 37
- Guidelines and Limitations for Troubleshooting Ports, page 37
- Initial Port Troubleshooting Checklist, page 38
- Viewing Port Information, page 38
- Viewing Port Errors, page 39
- Troubleshooting Port Statistics from the CLI, page 39
- Troubleshooting Port-Interface Issues, page 40

About Troubleshooting Ports

Before a device can relay frames from one data link to another, the characteristics of the interfaces through which the frames are received and sent must be defined. The configured interfaces can be Ethernet interfaces, VLAN interfaces (SVIs), or the management interface (mgmt0).

Each interface has an associated administrative configuration and operational status as follows:

- The administrative configuration does not change unless you modify it. This configuration has various attributes that you can configure in administrative mode.

- The operational status represents the current status of a specified attribute such as the interface speed. This status cannot be changed and is read-only. Some values may not be valid when the interface is down (such as the operation speed).

For a complete description of port modes, administrative states, and operational states, see the Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide.

Guidelines and Limitations for Troubleshooting Ports

Follow these guidelines when you configure a port interface:
• Before you begin configuring a device, make sure that the modules in the chassis are functioning as designed. Use the `show module` command to verify that a module is OK or active before continuing the configuration.

• When configuring dedicated ports in a port group, follow these port mode guidelines:
  • You can configure only the one port in each four-port group in dedicated mode. The other three ports are not usable and remain shut down.
  • If any of the other three ports are enabled, you cannot configure the remaining port in dedicated mode. The other three ports continue to remain enabled.

• There are no licensing requirements for port configuration in Cisco NX-OS.

### Initial Port Troubleshooting Checklist

Begin troubleshooting the port configuration by checking the following issues:

<table>
<thead>
<tr>
<th>Checklist</th>
<th>Done</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check the physical media to ensure that there are no damaged parts.</td>
<td></td>
</tr>
<tr>
<td>Verify that the SFP (small form-factor pluggable) devices in use are those authorized by Cisco and that they are not faulty.</td>
<td></td>
</tr>
<tr>
<td>Verify that you have enabled the port by using the <code>no shutdown</code> command.</td>
<td></td>
</tr>
<tr>
<td>Use the <code>show interface</code> command to verify the state of the interface. See the <em>Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide</em> for reasons why a port might be in a down operational state.</td>
<td></td>
</tr>
<tr>
<td>Verify that you have configured a port as dedicated and make sure that you have not connected to the other three ports in the port group.</td>
<td></td>
</tr>
</tbody>
</table>

### Viewing Port Information

You can use the `show interface counters` command to view port counters. Typically, you only observe counters while actively troubleshooting, in which case you should first clear the counters to create a baseline. The values, even if they are high for certain counters, can be meaningless for a port that has been active for an extended period. Clearing the counters provides a better idea of the link behavior as you begin to troubleshoot.

Use one of the following commands to clear all port counters or the counters for specified interfaces:

- `clear counters interface all`
- `clear counters interface range`

The counters can identify synchronization problems by displaying a significant disparity between received and transmitted frames.

Use the following commands to gather more information about ports:
Viewing Port Errors

You can use the `show hardware internal errors {module module-number | all}` command to display hardware internal errors for a single module or for all modules.

In the output for this command, the first number in the Ports column is the port number. For example, "1 -" is port 1 for module 27, which is the Ethernet 6/27 interface. Internal ports are shown as "--".

```
switch# show hardware internal errors module 27
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Device:Forwarding ASIC Role:MAC Mod: 27</td>
</tr>
<tr>
<td>Last cleared @ Fri Nov 8 14:13:39 2013</td>
</tr>
<tr>
<td>Device Statistics Category :: ERROR</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Instance:0 ID Name Value Ports</td>
</tr>
<tr>
<td>777 snmpIfInDiscards 00000000000000034 -- --</td>
</tr>
<tr>
<td>778 snmpIfInDiscards 00000000000000011 -- --</td>
</tr>
<tr>
<td>779 snmpIfInDiscards 00000000000000023 -- --</td>
</tr>
<tr>
<td>780 snmpIfInDiscards 00000000000000022 -- --</td>
</tr>
<tr>
<td>781 snmpIfInDiscards 00000000000000002 1 --</td>
</tr>
<tr>
<td>783 snmpIfInDiscards 00000000000000006 3 --</td>
</tr>
<tr>
<td>784 snmpIfInDiscards 00000000000000006 4 --</td>
</tr>
<tr>
<td>785 snmpIfInDiscards 00000000000000005 5 --</td>
</tr>
<tr>
<td>786 snmpIfInDiscards 00000000000000004 6 --</td>
</tr>
<tr>
<td>787 snmpIfInDiscards 00000000000000005 7 --</td>
</tr>
<tr>
<td>788 snmpIfInDiscards 00000000000000005 8 --</td>
</tr>
<tr>
<td>789 snmpIfInDiscards 00000000000000004 9 --</td>
</tr>
<tr>
<td>791 snmpIfInDiscards 00000000000000005 11 --</td>
</tr>
<tr>
<td>792 snmpIfInDiscards 00000000000000005 12 --</td>
</tr>
<tr>
<td>2305 snmpIfOutDiscards 00000000000000012 -- --</td>
</tr>
</tbody>
</table>

...............
```

```
| Instance:2 ID Name Value Ports                                      |
| 780 snmpIfInDiscards 00000000000000001 25 --                       |
| 781 snmpIfInDiscards 00000000000000000 31 --                       |
| 787 snmpIfInDiscards 00000000000000004 32 --                       |
| 789 snmpIfInDiscards 00000000000000001313 33 --                    |
| 790 snmpIfInDiscards 00000000000000002 34 --                       |
| 791 snmpIfInDiscards 00000000000000002 35 --                       |
| 792 snmpIfInDiscards 00000000000000001 36 --                       |
```

Troubleshooting Port Statistics from the CLI

To display complete information for an interface, use the `show interface` command. In addition to the state of the port, this command displays the following:

- Speed
• Trunk VLAN status
• Number of frames sent and received
• Transmission errors, including discards, errors, and invalid frames

switch# show interface ethernet 2/45
Ethernet2/45 is down (Administratively down)
Hardware is 10/100/1000 Ethernet, address is 0019.076c.4dd8 (bia 0019.076c.4dd8)
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA
auto-duplex, auto-speed
Beacon is turned off
Auto-Negotiation is turned on
Input flow-control is off, output flow-control is off
Auto-mdix is turned on
Last clearing of "show interface" counters never
1 minute input rate 0 bytes/sec, 0 packets/sec
1 minute output rate 0 bytes/sec, 0 packets/sec
L3 Switched:
  input: 0 pkts, 0 bytes - output: 0 pkts, 0 bytes
Rx
  0 input packets 0 unicast packets 0 multicast packets
  0 broadcast packets 0 jumbo packets 0 storm suppression packets
  0 bytes
Tx
  0 output packets 0 multicast packets
  0 broadcast packets 0 jumbo packets
  0 bytes
  0 input error 0 short frame 0 watchdog
  0 no buffer 0 runt 0 CRC 0 ecc
  0 overrun 0 underrun 0 ignored 0 bad etype drop
  0 bad proto drop 0 if down drop 0 input with dribble
  0 output error 0 collision 0 deferred
  0 late collision 0 lost carrier 0 no carrier
  0 babble
  0 Rx pause 0 Tx pause 0 reset
Receive data field Size is 2112

Troubleshooting Port-Interface Issues

The Interface Configuration Has Disappeared

You may have a problem where your interface configuration disappears.

<table>
<thead>
<tr>
<th>Symptoms</th>
<th>Possible Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The interface configuration has disappeared.</td>
<td>The interface mode has changed to or from the switchport mode.</td>
<td>Cisco NX-OS removes the interface configuration when you switch between Layer 2 and Layer 3 port mode. You must reconfigure the interface.</td>
</tr>
</tbody>
</table>

You Cannot Enable an Interface

You might have a problem when enabling an interface.
### You Cannot Configure a Dedicated Port

You may have a problem when trying to configure a port as dedicated.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>You cannot configure a dedicated port.</td>
<td>The other three ports in the port group are not shut down.</td>
<td>Use the <code>shutdown</code> command in interface configuration mode to disable the other three ports in the port group.</td>
</tr>
<tr>
<td></td>
<td>The port is not the first port in the port group.</td>
<td>You can set only the first port in a port group to the dedicated mode.</td>
</tr>
</tbody>
</table>

### A Port Remains in a Link Failure or Not Connected State

You may have a problem with ports or links becoming operational.

<table>
<thead>
<tr>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>You cannot enable the other three ports in a port group if one port is dedicated. Use the <code>show running-config interface</code> CLI command to verify the rate mode setting.</td>
</tr>
<tr>
<td>Use the <code>show interface capabilities</code> command on both ports to determine if both ports have the same capabilities. Modify the configuration as needed to make the ports compatible.</td>
</tr>
<tr>
<td>Use the <code>show interface brief</code> command to see if the interface is configured in a VLAN. Use the <code>show vlan brief</code> command to determine the status of the VLAN. Use the <code>state active</code> command in VLAN configuration mode to configure the VLAN as active.</td>
</tr>
<tr>
<td>Use the <code>show interface brief</code> command to see if you are using an incorrect transceiver. Replace with a Cisco-supported SFP.</td>
</tr>
<tr>
<td>Problem</td>
</tr>
<tr>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>A port remains in a link-failure state.</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

An Unexpected Link Flapping Occurs

When a port is flapping, it cycles through the following states, in this order, and then starts over again:

1. Initializing—The link is initializing.
2. Offline—The port is offline.
3. Link failure or not connected—The physical layer is not operational, and there is no active device connection.

When you are troubleshooting an unexpected link flapping, you should know the following information:

- Who initiated the link flap.
- The actual link down reason.
A Port Is in the ErrDisabled State

The ErrDisabled state indicates that the switch detected a problem with the port and disabled the port. This state could be caused by a flapping port or a high amount of bad frames (CRC errors), which could indicate a problem with the media.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>An unexpected link flapping occurs.</td>
<td>The bit rate exceeds the threshold and puts the port into the errDisabled state.</td>
<td>Use the shutdown command followed by the no shutdown command to return the port to the normal state.</td>
</tr>
<tr>
<td></td>
<td>A problem in the system triggers the link flap action by the end device.</td>
<td>Determine the link flap reason as indicated by the MAC driver. Use the debug facilities on the end device to troubleshoot the problem. An external device might choose to reinitialize the link when it encounters the error. In such cases, the method of reinitializing the link varies by device.</td>
</tr>
<tr>
<td></td>
<td>Some of the causes are as follows:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• A packet drop in the device occurs because of either a hardware failure or an intermittent hardware error such as an X-bar sync loss.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• A packet drop results from a software error.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• A control frame is erroneously sent to the device.</td>
<td></td>
</tr>
</tbody>
</table>

A Port Is in the ErrDisabled State

The ErrDisabled state indicates that the switch detected a problem with the port and disabled the port. This state could be caused by a flapping port or a high amount of bad frames (CRC errors), which could indicate a problem with the media.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>A port is in the ErrDisabled state.</td>
<td>The port is flapping.</td>
<td>See Verifying the ErrDisable State Using the CLI, on page 43 to verify the SFP, cable, and connections.</td>
</tr>
<tr>
<td></td>
<td>The device detected a high amount of bad frames (CRC errors), which might indicate a problem with the media.</td>
<td></td>
</tr>
</tbody>
</table>

Verifying the ErrDisable State Using the CLI

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
</tr>
<tr>
<td>switch# show interface interface slot/port</td>
<td>Verifies that the device detected a problem and disabled the port.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# show interface ethernet 1/14 e1/7 is down (errDisabled)</td>
<td>After verifying the port is disabled, check cables, SFPs, and optics.</td>
</tr>
</tbody>
</table>
### Command or Action

#### Step 2

```
switch# show system internal ethpm
event-history interface interface slot/port
```

**Example:**

```
switch# show system internal ethpm
event-history interface ethernet 1/7
```

#### Step 3

```
switch# show logging logfile
```

**Example:**

```
switch# show logging logfile
```

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td>Displays information about the internal state transitions of the port.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Displays the switch log file and view a list of port state changes.</td>
</tr>
</tbody>
</table>

This example shows how view information about the internal state transitions of the port. The port ethernet 1/7 entered the ErrDisabled state because of a capability mismatch, or "CAP MISMATCH":

```
switch# show system internal ethpm event-history interface ethernet 1/7
>>>><FSM: <e1/7> has 86 logged transitions<<<<
1) FSM:<e1/7> Transition at 647054 usecs after Tue Jan  1 22:44..
   Previous state: [ETH_PORT_FSM_ST_NOT_INIT]
   Triggered event: [ETH_PORT_FSM_EV_MODULE_INIT_DONE]
   Next state: [ETH_PORT_FSM_ST_IF_INIT_EVAL]
2) FSM:<e1/7> Transition at 647114 usecs after Tue Jan  1 22:43..
   Previous state: [ETH_PORT_FSM_ST_IF_INIT_EVAL]
   Triggered event: [ETH_PORT_FSM_EV_IE_ERR_DISABLED_CAP_MISMATCH]
   Next state: [ETH_PORT_FSM_ST_IF_DOWN_STATE]
```

This example shows how to display the switch log file and view a list of port state changes. An error was recorded when someone attempted to add port e1/7 to port channel 7. The port was not configured identically to port channel 7, so the attempt failed:

```
switch# show logging logfile
Jan  4 06:54:04 switch %PORT_CHANNEL-5-CREATED: port-channel 7 created
Jan  4 06:54:24 switch %PORT-5-IF_DOWN_PORT_CHANNEL_MEMBERS_DOWN: Interface port-channel 7 is down (No operational members)
Jan  4 06:54:40 switch %PORT_CHANNEL-5-PORT_ADDED: e1/8 added to port-channel 7
Jan  4 06:54:56 switch %PORT-5-IF_DOWN_ADMIN_DOWN: Interface e1/7 is down (Administratively down)
Jan  4 06:54:59 switch %PORT_CHANNEL-3-COMPAT_CHECK_FAILURE: speed is not compatible
Jan  4 06:55:59 switch %PORT_CHANNEL-5-PORT_ADDED: e1/7 added to port-channel 7
```
Troubleshooting vPCs

This chapter contains the following sections:

- About Troubleshooting vPCs, page 45
- Initial Troubleshooting vPCs Checklist, page 45
- Verifying vPCs Using the CLI, page 46
- Received Type 1 Configuration Element Mismatch, page 47
- Cannot Enable the vPC Feature, page 48
- vPCs in Blocking State, page 48
- VLANs on a vPC Moved to Suspend State, page 48
- Hosts with an HSRP Gateway Cannot Access Beyond Their VLAN, page 49

About Troubleshooting vPCs

A vPC allows links that are physically connected to two different devices to appear as a single port channel by a third device.

Initial Troubleshooting vPCs Checklist

Begin troubleshooting vPC issues by checking the following issues first:

<table>
<thead>
<tr>
<th>Checklist</th>
<th>Done</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is the vPC keepalive link mapped to a separate VRF? If not, it will be mapped to the management VRF by default. In this case, do you have a management switch connected to the management ports on both vPC peer devices?</td>
<td></td>
</tr>
<tr>
<td>Verify that both the source and destination IP addresses used for the peer-keepalive messages are reachable from the VRF associated with the vPC peer-keepalive link.</td>
<td></td>
</tr>
<tr>
<td>Verify that the peer-keepalive link is up. Otherwise, the vPC peer link will not come up.</td>
<td></td>
</tr>
</tbody>
</table>
Verifying vPCs Using the CLI

To verify vPCs using the CLI, perform one of these tasks:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show running-config vpc</code></td>
<td>Verifies the vPC configuration.</td>
</tr>
<tr>
<td><code>show vpc</code></td>
<td>Checks the status of the vPCs.</td>
</tr>
<tr>
<td><code>show vpc peer-keepalive</code></td>
<td>Checks the status of the vPC peer-keepalive link.</td>
</tr>
<tr>
<td><code>show vpc consistency-parameters</code></td>
<td>Verifies that the vPC peers have the identical type-1 parameters.</td>
</tr>
<tr>
<td><code>show tech-support vpc</code></td>
<td>Displays detailed technical support information for vPCs.</td>
</tr>
<tr>
<td><code>show port-channel summary</code></td>
<td>Verifies that the members in the port channel are mapped to the vPC.</td>
</tr>
<tr>
<td><code>show spanning-tree</code></td>
<td>Verifies that the following STP parameters are identical when STP is enabled:</td>
</tr>
<tr>
<td></td>
<td>• BPDU filter</td>
</tr>
<tr>
<td></td>
<td>• BPDU guard</td>
</tr>
<tr>
<td></td>
<td>• Cost</td>
</tr>
<tr>
<td></td>
<td>• Link type</td>
</tr>
<tr>
<td></td>
<td>• Priority</td>
</tr>
<tr>
<td></td>
<td>• VLANs (PVRST+)</td>
</tr>
</tbody>
</table>
The following example shows sample output for the `show vpc` command:

Legend:

(*) - local vPC is down, forwarding via vPC peer-link

<table>
<thead>
<tr>
<th>vPC domain id</th>
<th>: 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer status</td>
<td>: peer link is down</td>
</tr>
<tr>
<td>vPC keep-alive status</td>
<td>: Suspended (Destination IP not reachable)</td>
</tr>
<tr>
<td>Configuration consistency status</td>
<td>: failed</td>
</tr>
<tr>
<td>Per-vlan consistency status</td>
<td>: success</td>
</tr>
<tr>
<td>Configuration inconsistency reason</td>
<td>Consistency Check Not Performed</td>
</tr>
<tr>
<td>Type-2 inconsistency reason</td>
<td>Consistency Check Not Performed</td>
</tr>
<tr>
<td>vPC role</td>
<td>none established</td>
</tr>
</tbody>
</table>

Number of vPCs configured : 2
Peer Gateway : Enabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Disabled (due to peer configuration)
Auto-recovery status | Disabled
vPC Peer-link status
-------------------------------------------------------
<table>
<thead>
<tr>
<th>id</th>
<th>Port</th>
<th>Status</th>
<th>Active vlans</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Po10</td>
<td>down</td>
<td>-</td>
</tr>
</tbody>
</table>

vPC status
-------------------------------------------------------
<table>
<thead>
<tr>
<th>id</th>
<th>Port</th>
<th>Status</th>
<th>Consistency Reason</th>
<th>Active vlans</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Po20</td>
<td>down</td>
<td>failed</td>
<td>Peer-link is down</td>
</tr>
<tr>
<td>50</td>
<td>Po50</td>
<td>down</td>
<td>failed</td>
<td>Peer-link is down</td>
</tr>
</tbody>
</table>

Received Type 1 Configuration Element Mismatch

You might have a problem where you cannot bring up a vPC link because of a type 1 configuration element mismatch.

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Possible Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Received a type 1 configuration element mismatch.</td>
<td>The vPC peer ports or membership ports do not have identical configurations.</td>
<td>Use the <code>show vpc consistency-parameters interface</code> command to determine where the configuration mismatch occurs.</td>
</tr>
</tbody>
</table>

This example shows how to display the vPC consistency parameters on a port channel:

```
switch# show vpc consistency-parameters interface po 10

Legend:
Type 1 : vPC will be suspended in case of mismatch

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Local Value</th>
<th>Peer Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>STP Mode</td>
<td>1</td>
<td>Rapid-PVST</td>
<td>Rapid-PVST</td>
</tr>
<tr>
<td>STP Disabled</td>
<td>1</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>STP MST Region Name</td>
<td>1</td>
<td>&quot;&quot;</td>
<td>&quot;&quot;</td>
</tr>
<tr>
<td>STP MST Region Revision</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

Cisco Nexus 9000 Series NX-OS Troubleshooting Guide, Release 6.x

47
Cannot Enable the vPC Feature

You might receive an error when you enable the vPC feature.

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Possible Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cannot enable the vPC feature.</td>
<td>The hardware is incompatible with the vPC.</td>
<td>Use the <code>show module</code> command to determine the hardware version of each Ethernet module.</td>
</tr>
</tbody>
</table>

This example shows how to display the module hardware version:

```
switch# show module
```

```
<table>
<thead>
<tr>
<th>Mod</th>
<th>Ports</th>
<th>Module-Type</th>
<th>Model</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>0</td>
<td>Fabric Module</td>
<td>N9K-C9508-FM</td>
<td>ok</td>
</tr>
<tr>
<td>24</td>
<td>0</td>
<td>Fabric Module</td>
<td>N9K-C9508-FM</td>
<td>ok</td>
</tr>
<tr>
<td>26</td>
<td>0</td>
<td>Fabric Module</td>
<td>N9K-C9508-FM</td>
<td>ok</td>
</tr>
<tr>
<td>27</td>
<td>0</td>
<td>Supervisor Module</td>
<td>N9K-SUP-A</td>
<td>active*</td>
</tr>
<tr>
<td>29</td>
<td>0</td>
<td>System Controller</td>
<td>N9K-SC-A</td>
<td>active</td>
</tr>
<tr>
<td>30</td>
<td>0</td>
<td>System Controller</td>
<td>N9K-SC-A</td>
<td>standby</td>
</tr>
</tbody>
</table>
```

vPCs in Blocking State

vPCs might be in the blocking state because of bridge assurance (BA).

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Possible Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>vPC is in blocking state.</td>
<td>BPDUs only send on a single link of a port channel. If a BA dispute is detected, the entire vPC will be in the blocking state.</td>
<td>Do not enable BA on the vPC.</td>
</tr>
</tbody>
</table>

VLANs on a vPC Moved to Suspend State

VLANs on a vPC might move to the suspend state.
Hosts with an HSRP Gateway Cannot Access Beyond Their VLAN

When HSRP is enabled on both vPC peer devices on a VLAN and hosts on that VLAN set the HSRP as their gateway, they might not able to reach anything outside their own VLAN.

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Possible Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLANs on a vPC are moved to the suspend state.</td>
<td>VLANs allowed on the vPC have not been allowed on the vPC peer link.</td>
<td>All VLANs allowed on a vPC must also be allowed on the vPC peer link. Also, we recommend that only vPC VLANs are allowed on the vPC peer link.</td>
</tr>
<tr>
<td>Hosts with an HSRP gateway cannot access beyond their VLAN.</td>
<td>If the host gateway MAC address is mapped to the physical MAC address of any one of the vPC peer devices, packets might get dropped due to the loop prevention mechanism in the vPC.</td>
<td>Map the host gateway's MAC address to the HSRP MAC address and not the physical MAC address of any one of the vPC peer devices. The peer gateway can be a workaround for this scenario. Read the configuration guide for more information about the peer gateway before you implement it.</td>
</tr>
</tbody>
</table>
Troubleshooting VLANs

This chapter contains the following sections:

• About Troubleshooting VLANs, page 51
• Guidelines and Limitations for Troubleshooting VLANs, page 51
• Initial Troubleshooting VLANs Checklist, page 52
• Troubleshooting VLAN Issues, page 52

About Troubleshooting VLANs

VLANs provide a method of isolating devices that are physically connected to the same network but are logically considered to be part of different LANs that do not need to be aware of one another.

You should use only the following characters in a VLAN name:

• a through z or A through Z
• 0 through 9
• - (hyphen) or _ (underscore)

Guidelines and Limitations for Troubleshooting VLANs

Follow these guidelines when configuring VLANs:

• Keep user traffic off the management VLAN; keep the management VLAN separate from user data.
• You can apply different quality of service (QoS) configurations to primary, isolated, and community VLANs.
• VACLs that apply to the Layer 3 VLAN interface of a primary VLAN automatically apply to the associated isolated and community VLANs.
• If you do not map the secondary VLAN to the Layer 3 VLAN interface of the primary VLAN, you can have different VACLs for primary and secondary VLANs.
• IGMP runs only on the primary VLAN and uses the configuration of the primary VLAN for all secondary VLANs.
• Any IGMP join request in the secondary VLAN is treated as if it is received in the primary VLAN.
• A destination SPAN port cannot be an isolated port. (However, a source SPAN port can be an isolated port.)
• You can configure SPAN to span both primary and secondary VLANs or, alternatively, to span either one if you are interested only in ingress or egress traffic.
• A MAC address learned in a secondary VLAN is placed in the shared table of the primary VLAN. When the secondary VLAN is associated to the primary VLAN, its MAC address tables are merged into one shared MAC table.
• You can configure a private VLAN (PVLAN) port as a SPAN source port.
• A PVLAN host or promiscuous port cannot be a SPAN destination port.

**Initial Troubleshooting VLANs Checklist**

Troubleshooting a VLAN problem involves gathering information about the configuration and connectivity of individual devices and the entire network. Begin your troubleshooting VLAN issues by checking the following issues first:

<table>
<thead>
<tr>
<th>Checklist</th>
<th>Done</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify the physical connectivity for any problem ports or VLANs.</td>
<td></td>
</tr>
<tr>
<td>Verify that you have both end devices in the same VLAN.</td>
<td></td>
</tr>
</tbody>
</table>

The following CLI commands are used to display VLAN information:

- `show vlan vlan-id`
- `show vlan all-ports`
- `show tech-support vlan`
- `show vlan private-vlan [type]`
- `show interface vlan vlan-id private-vlan mapping`

**Troubleshooting VLAN Issues**

**You Cannot Create a VLAN**

You may have a problem when creating a VLAN.
### You Cannot Create a PVLAN

You may experience issues when creating a private VLAN (PVLAN).

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Possible Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>You cannot create a PVLAN</td>
<td>The PVLAN feature is not enabled.</td>
<td>Use the <code>feature private-vlan</code> command to enable the PVLAN feature.</td>
</tr>
</tbody>
</table>

### The VLAN Interface is Down

You might have a problem when configuring VLAN interfaces.

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Possible Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The VLAN interface is down.</td>
<td>The VLAN does not exist.</td>
<td>Use the <code>show vlan</code> command to determine if the VLAN exists. Use the <code>vlan</code> command to create the VLAN.</td>
</tr>
<tr>
<td></td>
<td>No interfaces on the VLAN are in the STP forwarding state.</td>
<td>Use the <code>show vlan internal vlan-info</code> command to check the operating state of the Spanning Tree Protocol (STP). Configure STP so that at least one interface goes into the STP forwarding state.</td>
</tr>
<tr>
<td></td>
<td>One or more services prevented the VLAN interface from coming up.</td>
<td>Use the <code>show vlan internal vlan-info</code> command to determine the state of the VLAN interface. If the state is oper-es, use the <code>show tech-support interface vlan</code> command to gather more information.</td>
</tr>
<tr>
<td></td>
<td>The VLAN is a secondary VLAN.</td>
<td>Use the <code>show vlan internal vlan-info</code> command to determine the state of the VLAN interface. Change the VLAN to a primary or user VLAN.</td>
</tr>
<tr>
<td></td>
<td>The interface is in the wrong VRF.</td>
<td>Use the <code>show vrf interface</code> command to determine the interface to which the VLAN interface is assigned.</td>
</tr>
</tbody>
</table>
The VLAN Interface is Down
Troubleshooting STP

This chapter contains the following sections:

- About Troubleshooting STP, page 55
- Initial Troubleshooting STP Checklist, page 55
- Troubleshooting STP Data Loops, page 56
- Troubleshooting Excessive Packet Flooding, page 59
- Troubleshooting Convergence Time Issues, page 60
- Securing the Network Against Forwarding Loops, page 61

About Troubleshooting STP

STP provides a loop-free network at the Layer 2 level. Layer 2 LAN ports send and receive STP frames at regular intervals. Network devices do not forward these frames but use the frames to construct a loop-free path. For more information on Layer 2, see the Cisco Nexus 9000 Series Layer 2 Configuration Guide.

Initial Troubleshooting STP Checklist

Troubleshooting an STP problem involves gathering information about the configuration and connectivity of individual devices and the entire network.

Begin troubleshooting STP issues by checking the following issues first:

<table>
<thead>
<tr>
<th>Checklist</th>
<th>Done</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify the type of spanning tree configured on your device.</td>
<td></td>
</tr>
<tr>
<td>Verify the network topology including all interconnected ports and switches. Identify all redundant paths on the network and verify that the redundant paths are blocking.</td>
<td></td>
</tr>
</tbody>
</table>
Use the `show spanning-tree summary totals` command to verify that the total number of logical interfaces in the Active state are less than the maximum allowed. For information on these limits, see the *Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide*.

Verify the primary and secondary root bridge and any configured Cisco extensions.

Use the following commands to view STP configuration and operational details:

- `show running-config spanning-tree`
- `show spanning-tree summary`
- `show spanning-tree detail`
- `show spanning-tree bridge`
- `show spanning-tree mst`
- `show spanning-tree mst configuration`
- `show spanning-tree interface interface-type slot/port [detail]`
- `show tech-support stp`
- `show spanning-tree vlan`

Use the `show spanning-tree blockedports` command to display the ports that are blocked by STP.

Use the `show mac address-table dynamic vlan` command to determine if learning or aging occurs at each node.

**Troubleshooting STP Data Loops**

Data loops are a common problem in STP networks. Some of the symptoms of a data loop are as follows:

- High link utilization, up to 100 percent
- High CPU and backplane traffic utilization
- Constant MAC address relearning and flapping
- Excessive output drops on an interface

When the l2fm logging level is greater than or equal to 4, the switch logs occurrences of host MAC address flapping to help you locate STP data loops. If it detects a MAC address move within less than 1 second and if 10 consecutive moves occur, the switch disables learning on the VLAN for one of the ports between which the MAC address is moving. Learning is disabled for 120 seconds and reenabled automatically. Syslogs are generated while learning is disabled and enabled. You can configure the logging level using the `logging level l2fm log-level` command.
## Troubleshooting STP

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> switch# show interface interface-type slot/port include rate</td>
<td>Identifies the ports involved in the loop by looking at the interfaces with high link utilization.</td>
</tr>
<tr>
<td>Example: switch# show interface ethernet 2/1 include rate</td>
<td></td>
</tr>
<tr>
<td>1 minute input rate 19968 bits/sec, 0 packets/sec</td>
<td></td>
</tr>
<tr>
<td>1 minute output rate 39520 bits/sec, 957312 packets/sec</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> switch(config)# interface interface-type slot/port</td>
<td>Configures the interface type and location.</td>
</tr>
<tr>
<td>Example: switch(config)# interface ethernet 2/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> switch(config-if)# shutdown</td>
<td>Shuts down or disconnects the affected ports. After disconnecting the affected ports, locate every switch in the redundant paths using your network topology diagram.</td>
</tr>
<tr>
<td>Example: switch(config-if)# shutdown</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> switch(config-if)# show spanning-tree vlan vlan-id</td>
<td>Verifies that the switch lists the same STP root bridge as the other nonaffected switches.</td>
</tr>
<tr>
<td>Example: switch(config-if)# show spanning-tree vlan 9</td>
<td></td>
</tr>
<tr>
<td>VLAN0009</td>
<td></td>
</tr>
<tr>
<td>Spanning tree enabled protocol rstp</td>
<td></td>
</tr>
<tr>
<td>Root ID Priority 32777'' Address 0018.bad7.db15''</td>
<td></td>
</tr>
<tr>
<td>Cost 4</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> switch(config-if)# show spanning-tree interface interface-type slot/port detail</td>
<td>Verify that the root port and alternate ports are regularly receiving BPDUs.</td>
</tr>
<tr>
<td>Example: switch(config-if)# show spanning-tree interface ethernet 3/1 detail</td>
<td></td>
</tr>
<tr>
<td>Port 385 (Ethernet3/1) of VLAN0001 is root forwarding</td>
<td></td>
</tr>
<tr>
<td>Port path cost 4, Port priority 128, Port Identifier 128.385</td>
<td></td>
</tr>
<tr>
<td>Designated root has priority 32769, address 0018.bad7.db15</td>
<td></td>
</tr>
<tr>
<td>Designated bridge has priority 32769, address 0018.bad7.db15</td>
<td></td>
</tr>
<tr>
<td>Designated port id is 128.385, designated path cost 0</td>
<td></td>
</tr>
<tr>
<td>Timers: message age 16, forward delay 0, hold 0</td>
<td></td>
</tr>
<tr>
<td>Number of transitions to forwarding state: 1</td>
<td></td>
</tr>
<tr>
<td>The port type is network by default</td>
<td></td>
</tr>
<tr>
<td>Link type is point-to-point by default</td>
<td></td>
</tr>
<tr>
<td>BPU: sent 1265, received 1269</td>
<td></td>
</tr>
</tbody>
</table>
### Troubleshooting STP

**Command or Action**

<table>
<thead>
<tr>
<th>Step 6</th>
<th>switch(config-if)# show system internal pktmgr interface interface-type slot/port</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(Optional) Checks if the BPDUs are received by the internal packet manager.</td>
</tr>
</tbody>
</table>

**Example:**

```bash
switch(config-if)# show system internal pktmgr interface ethernet 3/1
Ethernet3/1, ordinal: 36
SUP-traffic statistics: (sent/received)
  Packets: 120210 / 15812
  Bytes: 8166401 / 1083056
  Instant packet rate: 5 pps / 5 pps
  Average packet rates (1min/5min/15min/EWMA):
  Packet statistics:
    Tx: Unicast 0, Multicast 120210
    Rx: Unicast 0, ** Multicast 15812 **
    Broadcast 0
```

**Step 7**

<table>
<thead>
<tr>
<th>switch(config-if)# show system internal pktmgr client client-id</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Optional) Checks if the BPDUs are received by the client.</td>
</tr>
</tbody>
</table>

**Example:**

```bash
switch(config-if)# show system internal pktmgr client 303
Client uuid: 303, 2 filters
Filter 0: EthType 0x4242, Dmac 0180.c200.0000
Filter 0: EthType 0x010b, Snap 267, Dmac 0100.0ccc.cccd
Options: TO 0, Flags Ox1, AppId 0, Epid 0
Ctrl SAP: 171, Data SAP 177 (1)
Rx: 28356632, Drop: 0, Tx: 35498365, Drop: 0
```

**Step 8**

<table>
<thead>
<tr>
<th>switch(config-if)# show interface counters errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Optional) Checks the hardware packet statistic (error drop) counters.</td>
</tr>
</tbody>
</table>

**Example:**

```bash
switch(config-if)# show interface counters errors
--------------------------------------------------------------
Port Align-Err FCS-Err Xmit-Err Rcv-Err UnderSize OutDiscards
--------------------------------------------------------------
mgmt0  --  --  --  --  --  --
Eth1/1  0  0  0  0  0  0
Eth1/2  0  0  0  0  0  0
Eth1/3  0  0  0  0  0  0
Eth1/4  0  0  0  0  0  0
Eth1/5  0  0  0  0  0  0
Eth1/6  0  0  0  0  0  0
Eth1/7  0  0  0  0  0  0
Eth1/8  0  0  0  0  0  0
```

This example shows that the designated port is regularly sending BPDUs:

```bash
switch# show spanning-tree interface ethernet 3/1 detail
Port 385 (Ethernet3/1) of VLAN0001 is root forwarding
  Port path cost 4, Port priority 128, Port Identifier 128.385
  Designated root has priority 32769, address 0018.bad7.db15
  Designated bridge has priority 32769, address 0018.bad7.db15
  Designated port id is 128.385, designated path cost 0
  Timers: message age 16, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  The port type is network by default
  Link type is point-to-point by default
```
BPDU: sent 1265, received 1269

This example shows how to check if BPDUs are transmitted by the packet manager:

```
switch# show system internal pktmgr interface ethernet 3/1
Ethernet3/1, ordinal: 36
SUP-traffic statistics: (sent/received)
Packets: 120210 / 15812
Bytes: 8166401 / 1083056
Instant packet rate: 5 pps / 5 pps
Average packet rates(1min/5min/15min/EWMA):
  Tx: Unicast 0, Multicast 120210
  Rx: Unicast 0, Multicast 15812

switch# show system internal pktmgr client 303
Client uuid: 303, 2 filters
  Filter 0: EthType 0x4242, Dmac 0180.c200.0000
  Filter 0: EthType 0x010b, Snap 267, Dmac 0100.0ccc.cccd
Options: TO 0, Flags 0x1, AppId 0, Epid 0
Ctrl SAP: 171, Data SAP 177 (1)
Rx: 28356632, Drop: 0, Tx: 35498365, Drop: 0
```

This example shows how to check the hardware packet statistic counters for a possible BPDU error drop:

```
switch# show interface counters errors
--------------------------------------------------------------
Port | Align-Err | FCS-Err | Xmit-Err | Rcv-Err | UnderSize | OutDiscards
-----------------------------------------------
mgmt0 | -- | -- | -- | -- | -- | --
Eth1/1 | 0 | 0 | 0 | 0 | 0 | 0
Eth1/2 | 0 | 0 | 0 | 0 | 0 | 0
Eth1/3 | 0 | 0 | 0 | 0 | 0 | 0
Eth1/4 | 0 | 0 | 0 | 0 | 0 | 0
Eth1/5 | 0 | 0 | 0 | 0 | 0 | 0
Eth1/6 | 0 | 0 | 0 | 0 | 0 | 0
Eth1/7 | 0 | 0 | 0 | 0 | 0 | 0
Eth1/8 | 0 | 0 | 0 | 0 | 0 | 0
```

## Troubleshooting Excessive Packet Flooding

Unstable STP topology changes can trigger excessive packet flooding in your STP network. With Rapid STP or Multiple STP (MST), a change of the port's state to forwarding, as well as the role change from designated to root, can trigger a topology change. Rapid STP immediately flushes the Layer 2 forwarding table. 802.1D shortens the aging time. The immediate flushing of the forwarding table restores connectivity faster but causes more flooding.

In a stable topology, a topology change should not trigger excessive flooding. Link flaps can cause a topology change, so continuous link flaps can cause repetitive topology changes and flooding. Flooding slows the network performance and can cause packet drops on an interface.

### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch# show spanning-tree vlan vlan-id detail</td>
<td>Determines the source of the excessive topology change.</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bridge Identifier has priority 32768, sysid 9, address 0018.bad8.27ad</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configured hello time 2, max age 20, forward delay 15</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Current root has priority 32777, address 0018.bad7.db15</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Root port is 385 (Ethernet3/1), cost of root path is 4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Topology change flag not set, detected flag not set</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of topology changes 8 last change occurred 1:32:11 ago</td>
<td></td>
<td></td>
</tr>
<tr>
<td>' from Ethernet3/1'</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Times: hold 1, topology change 35, notification 2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Step 2** switch# show spanning-tree vlan vlan-id detail

**Example:**

```plaintext
switch# show spanning-tree vlan 9 detail
VLAN0009 is executing the rstp compatible Spanning Tree protocol
Bridge Identifier has priority 32768, sysid 9, address 0018.bad8.27ad
Configured hello time 2, max age 20, forward delay 15
Current root has priority 32777, address 0018.bad7.db15
Root port is 385 (Ethernet3/1), cost of root path is 4
Topology change flag not set, detected flag not set
Number of topology changes 8 last change occurred 1:32:11 ago
'' from Ethernet3/1''
Times: hold 1, topology change 35, notification 2
```

**Troubleshooting Convergence Time Issues**

STP convergence can take longer than expected or result in an unexpected final network topology.

To troubleshoot convergence issues, check the following issues:

- Errors in the documented network topology diagram.
- Misconfiguration of the timers; diameter; Cisco extension features such as bridge assurance, root guard, and BPDU guard; and so on.
- Overloaded switch CPU during convergence that exceeds the recommended logical port (port-vlan) limit.
- Software defects that affect STP.
Securing the Network Against Forwarding Loops

To handle the inability of STP to deal correctly with certain failures, Cisco has developed a number of features and enhancements to protect the networks against forwarding loops.

Troubleshooting STP helps to isolate and find the cause for a particular failure, while the implementation of these enhancements is the only way to secure the network against forwarding loops.

Before You Begin

- Enable the Cisco-proprietary Unidirectional Link Detection (UDLD) protocol on all the switch-to-switch links. For information, see the Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide.

- Set up the bridge assurance feature by configuring all the switch-to-switch links as the spanning tree network port type.

  Note
  You should enable the bridge assurance feature on both sides of the links. Otherwise, Cisco NX-OS will put the port in the blocked state because of a bridge assurance inconsistency.

- Set up all the end-station ports as a spanning tree edge port type.
  You must set up the STP edge port to limit the amount of topology change notices and subsequent flooding that can affect the performance of the network. Use this command only with ports that connect to end stations. Otherwise, an accidental topology loop can cause a data-packet loop and disrupt the device and network operation.

- Enable the Link Aggregation Control Protocol (LACP) for port channels to avoid any port-channel misconfiguration issues. For information, see the Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide.

  Do not disable autonegotiation on the switch-to-switch links. Autonegotiation mechanisms can convey remote fault information, which is the quickest way to detect failures at the remote side. If failures are detected at the remote side, the local side brings down the link even if the link is still receiving pulses.

  Caution
  Be careful when you change STP timers. STP timers are dependent on each other, and changes can impact the entire network.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>switch(config)# spanning-tree loopguard default</td>
<td>(Optional) Secures the network STP perimeter with root guard. Root guard and BPDV guard allow you to secure STP against influence from the outside.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enables BPDU guard on STP edge ports to prevent STP from being affected by unauthorized network devices (such as hubs, switches, and bridging routers) that are connected to the ports.</td>
<td></td>
</tr>
<tr>
<td>switch(config)# spanning-tree bpduguard enable</td>
<td>Root guard prevents STP from outside influences. BPDU guard shuts down the ports that are receiving any BPDUs (not only superior BPDUs).</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Short-living loops are not prevented by root guard or BPDU guard if two STP edge ports are connected directly or through the hub.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configures separate VLANs and avoids user traffic on the management VLAN. The management VLAN is contained to a building block, not the entire network.</td>
<td></td>
</tr>
<tr>
<td>switch(config)# vlan vlan-range</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> switch(config)# vlan 9</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Configures a predictable STP root.</td>
<td></td>
</tr>
<tr>
<td>switch(config)# spanning-tree vlan vlan-range root primary</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> switch(config)# spanning-tree vlan 9 root primary</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Configures a predictable backup STP root placement. You must configure the STP root and backup STP root so that convergence occurs in a predictable way and builds optimal topology in every scenario. Do not leave the STP priority at the default value.</td>
<td></td>
</tr>
<tr>
<td>switch(config)# spanning-tree vlan vlan-range root secondary</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> switch(config)# spanning-tree vlan 12 root secondary</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Troubleshooting Routing

This chapter contains the following sections:

- About Troubleshooting Routing Issues, page 63
- Initial Troubleshooting Routing Checklist, page 63
- Troubleshooting Routing, page 64
- Troubleshooting Policy-Based Routing, page 66

About Troubleshooting Routing Issues

Layer 3 routing involves determining optimal routing paths and packet switching. You can use routing algorithms to calculate the optimal path from the router to a destination. This calculation depends on the algorithm selected, route metrics, and other considerations such as load balancing and alternate path discovery.

Cisco NX-OS supports multiple virtual routing and forwarding (VRF) instances and multiple routing information bases (RIBs) to support multiple address domains. Each VRF is associated with a RIB, and this information is collected by the Forwarding Information Base (FIB).

See the following documents for more information on routing:

- Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide
- Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide

Initial Troubleshooting Routing Checklist

You can troubleshoot routing issues by checking these items first:

<table>
<thead>
<tr>
<th>Checklist</th>
<th>Done</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that the routing protocol is enabled.</td>
<td></td>
</tr>
<tr>
<td>Verify that the address family is configured if necessary.</td>
<td></td>
</tr>
<tr>
<td>Verify that you have configured the correct VRF for your routing protocol.</td>
<td></td>
</tr>
</tbody>
</table>
Use the following commands to display routing information:

- show ip arp
- show ip traffic
- show ip static-route
- show ip client
- show ip fib
- show ip process
- show ip route
- show vrf
- show vrf interface

## Troubleshooting Routing

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | switch# show ospf | Verifies that the routing protocol is enabled.  
**Example:**
```bash
switch# show ospf
% invalid command detected at '^' marker.
```
| | | If the feature is not enabled, Cisco NX-OS reports that the command is invalid. |
| Step 2 | switch# show running-config eigrp all | Verifies the configuration for this routing protocol.  
**Example:**
```bash
switch# show running-config eigrp all
```
| Step 3 | switch# show running-config eigrp | Verifies the VRF configuration for this routing protocol.  
**Example:**
```bash
switch# show running-config eigrp
certification 6.1(2)I1(1)
feature eigrp
router eigrp 99
  address-family ipv4 unicast
  router-id 192.0.2.1
  vrf red
  stub
```
| Step 4 | switch# show processes memory | include isis | Checks the memory utilization for this routing protocol.  
**Example:**
```bash
switch# show processes memory | include isis
8913 9293824 bfffe1d0/bfffe0d0 isis
32243 8609792 bfffe0c0/bfffd9c0 isis
```
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>switch# show ip client pim</td>
<td>Verifies that the routing protocol is receiving packets.</td>
</tr>
</tbody>
</table>
|      | **Example:** switch# show ip client pim  
|      | Client: pim, uuid: 284, pid: 3839, extended pid: 3839  
|      | Protocol: 103, client-index: 10, routing VRF id: 255  
|      | Data MTS-SAP: 1519  
|      | Data messages, send successful: 2135, failed: 0 | |
| 6    | switch# show ip interface loopback-interface | Verifies that the routing protocol is enabled on an interface. |
|      | **Example:** switch# show ip interface loopback0  
|      | loopback0, Interface status:  
|      | protocol-up/link-up/admin-up, iod: 36,  
|      | Context:"default"  
|      | IP address: 1.0.0.1, IP subnet: 1.0.0.0/24  
|      | ...  
|      | IP multicast groups locally joined:  
|      | 224.0.0.2 224.0.0.1 224.0.0.13 | |
| 7    | switch# show vrf interface loopback-interface | Verifies that the interface is in the correct VRF. |
|      | **Example:** switch# show vrf interface loopback 99  
|      | Interface VRF-ID  
|      | loopback99 1 | default  |
| 8    | switch# show routing unicast clients | Verifies that the routing protocol is registered with the RIB. |
|      | **Example:** switch# show routing unicast clients | |
| 9    | switch# show forwarding distribution multicast client | Verifies that the RIB is interacting with the forwarding plane. |
|      | **Example:** switch# show forwarding distribution multicast client  
|      | Number of Clients Registered: 3  
|      | Client-name Client-id Shared Memory Name  
|      | igmp 1 N/A  
|      | mrib 2 /procket/shm/mrib-mfdm | |
timers nsf signal 20
distance 90 170
metric weights 0 1 0 1 0 0
metric maximum-hops 100
default-metric 100000 100 255 1 1500
maximum-paths 16
address-family ipv4 unicast
log-neighbor-warnings
log-neighbor-changes
log-adjacency-changes
graceful-restart
router-id 192.0.2.1
nsf
timers nsf signal 20
distance 90 170
metric weights 0 1 0 1 0 0
metric maximum-hops 100
default-metric 100000 100 255 1 1500
maximum-paths 16

This example shows how to display that the unicast routing protocol is registered with the RIB:

switch# show routing unicast clients
CLIENT: am
index mask: 0x00000002
epid: 3908  MTS SAP: 252  MRU cache hits/misses:  2/1
Routing Instances:
  VRF: management  table: base
Messages received:
  Register     : 1  Add-route     : 2  Delete-route     : 1
Messages sent:
  Add-route-ack : 2  Delete-route-ack : 1
CLIENT: rpm
index mask: 0x00000004
epid: 4132  MTS SAP: 348  MRU cache hits/misses:  0/0
Messages received:
  Register     : 1
Messages sent:

CLIENT: eigrp-99
index mask: 0x000002000
epid: 3148  MTS SAP: 63775  MRU cache hits/misses:  0/1
Routing Instances:
  VRF: default  table: base  notifiers: self
Messages received:
  Register     : 1  Delete-all-routes : 1
Messages sent:

Troubleshooting Policy-Based Routing

• Make sure the ACLs match the incoming traffic.

• Make sure the route is available:
  • For IP network routes, use the show ip route command to make sure the IP network route is available for the next hop specified in the set ip next-hop command.
  • For IP host routes, use the show ip arp command to make sure the IP host route is available for the next hop specified in the set ip next-hop command.
  • For IPv6 network routes, use the show ipv6 route command to make sure the IPv6 network route is available for the next hop specified in the set ipv6 next-hop command.
For IPv6 host routes, use the **show ipv6 neighbor** command to make sure the IPv6 host route is available for the next hop specified in the **set ipv6 next-hop** command.

- Make sure the policy is active in the system (using the **show ip policy** command).
- Check the statistics for the entry (using the **show route-map map-name pbr-statistics** command).
Troubleshooting Memory

This chapter contains the following sections:

- About Troubleshooting Memory, page 69
- General/High Level Assessment of Platform Memory Utilization, page 70
- Detailed Assessment of Platform Memory Utilization, page 70
- User Processes, page 73
- Built-in Platform Memory Monitoring, page 76

About Troubleshooting Memory

Dynamic random access memory (DRAM) is a limited resource on all platforms and must be controlled or monitored to ensure utilization is kept in check.

Cisco NX-OS uses memory in the following three ways:

- **Page cache**—When you access files from persistent storage (CompactFlash), the kernel reads the data into the page cache, which means that when you access the data in the future, you can avoid the slow access times that are associated with disk storage. Cached pages can be released by the kernel if the memory is needed by other processes. Some file systems (tmpfs) exist purely in the page cache (for example, /dev/sh, /var/sysmgr, /var/tmp), which means that there is no persistent storage of this data and that when the data is removed from the page cache, it cannot be recovered. tmpfs-cached files release page-cached pages only when they are deleted.

- **Kernel**—The kernel needs memory to store its own text, data, and Kernel Loadable Modules (KLMs). KLMs are pieces of code that are loaded into the kernel (as opposed to being a separate user process). An example of kernel memory usage is when an inband port driver allocates memory to receive packets.

- **User processes**—This memory is used by Cisco NX-OS or Linux processes that are not integrated in the kernel (such as text, stack, heap, and so on).

When you are troubleshooting high memory utilization, you must first determine what type of utilization is high (process, page cache, or kernel). Once you have identified the type of utilization, you can use additional troubleshooting commands to help you figure out which component is causing this behavior.
General/High Level Assessment of Platform Memory Utilization

You can assess the overall level of memory utilization on the platform by using two basic CLI commands: `show system resources` and `show processes memory`.

From these command outputs, you might be able to tell that platform utilization is higher than normal/expected, but you will not be able to tell what type of memory usage is high.

**Note**

The `show system resources` command displays platform memory statistics.

```
switch# show system resources
Load average: 1 minute: 0.43 5 minutes: 0.30 15 minutes: 0.28
Processes : 884 total, 1 running
CPU states : 2.0% user, 1.5% kernel, 96.5% idle
Memory usage: 4135780K total, 3423272K used, 712508K free
0K buffers, 1739356K cache
```

This output is derived from the Linux memory statistics in `/proc/meminfo`.

- **total**—The amount of physical RAM on the platform.
- **free**—The amount of unused or available memory.
- **used**—The amount of allocated (permanent) and cached (temporary) memory.

The cache and buffers are not relevant to customer monitoring.

This information provides a general representation of the platform utilization only. You need more information to troubleshoot why memory utilization is high.

The `show processes memory` command displays the memory allocation per process.

```
switch# show processes memory
Load average: 1 minute: 0.43 5 minutes: 0.30 15 minutes: 0.28
Processes : 884 total, 1 running
CPU states : 2.0% user, 1.5% kernel, 96.5% idle
PID MemAlloc MemLimit MemUsed StackBase/Ptr Process
---- -------- --------- --------- ----------------- ----------------
4662 52756480 562929945 150167552 bfffdf00/bfffd970 netstack
```

Detailed Assessment of Platform Memory Utilization

Use the `show system internal memory-alerts-log` or the `show system internal kernel` command for a more detailed representation of memory utilization in Cisco NX-OS.

```
switch# show system internal kernel meminfo
MemTotal: 4135780 kB
MemFree: 578032 kB
Buffers: 5312 kB
Cached: 1926296 kB
RAMCached: 1803020 kB
Allowed: 1033945 Pages
Free: 144508 Pages
Available: 177993 Pages
SwapCached: 0 kB
Active: 1739400 kB
```
Inactive: 1637756 kB
HighTotal: 3287760 kB
HighFree: 640 kB
LowTotal: 848020 kB
LowFree: 577392 kB
SwapTotal: 0 kB
SwapFree: 0 kB
Dirty: 0 kB
Writeback: 0 kB
Mapped: 1903768 kB
Slab: 85392 kB
CommitLimit: 2067888 kB
Committed_AS: 3479912 kB
PageTables: 20860 kB
VmallocTotal: 131064 kB
VmallocUsed: 128216 kB
VmallocChunk: 2772 kB

In the output above, the most important fields are as follows:

- **MemTotal (kB)**—Total amount of memory in the system.
- **Cached (kB)**—Amount of memory used by the page cache (includes files in tmpfs mounts and data cached from persistent storage /bootflash).
- **RamCached (kB)**—Amount of memory used by the page cache that cannot be released (data not backed by persistent storage).
- **Available (Pages)**—Amount of free memory in pages (includes the space that could be made available in the page cache and free lists).
- **Mapped (Pages)**—Memory mapped into page tables (data being used by nonkernel processes).
- **Slab (Pages)**—Rough indication of kernel memory consumption.

---

**Note**

One page of memory is equivalent to 4 kB of memory.

The `show system internal kernel memory global` command displays the memory usage for the page cache and kernel/process memory.

```
switch# show system internal kernel memory global
Total memory in system : 4129600KB
Total Free memory : 1345232KB
Total memory in use : 2784368KB
Kernel/App memory : 1759856KB
RAM FS memory : 1018616KB
```

---

**Note**

In Cisco NX-OS, the Linux kernel monitors the percentage of memory that is used (relative to the total RAM present) and platform manager generates alerts as utilization passes default or configured thresholds. If an alert has occurred, it is useful to review the logs captured by the platform manager against the current utilization.

By reviewing the output of these commands, you can determine if the utilization is high as a result of the page cache, processes holding memory, or kernel.
Page Cache

If Cached or RAMCached is high, you should check the file system utilization and determine what kind of files are filling the page cache.

The `show system internal flash` command displays the file system utilization (the output is similar to `df -hT` included in the memory alerts log).

```
switch# show system internal flash
Mount-on 1K-blocks Used Available Use% Filesystem
/ 409600 43008 367616 11 /dev/root
/proc 0 0 0 0 /dev/root
/sys 0 0 0 0 none
/lsan 409600 269312 140288 66 none
/var/tmp 307200 876 306324 1 none
/var/sysmgr 1048576 999424 49152 96 none
/var/sysmgr/ftp 307200 24576 282624 8 none
/dev/shm 1048576 412672 635904 40 none
/volatile 204800 0 204800 0 none
/debug 2048 16 2032 1 none
/dev/mqueue 0 0 0 0 none
/mnt/cfg/0 76099 5674 76096 8 /dev/hda5
/mnt/cfg/1 75605 5674 75604 8 /dev/hda6
/boothash 1796768 629784 1075712 37 /dev/hda3
/var/sysmgr/startup-cfg 409600 27536 382064 7 none
/mnt/plog 56192 6682 56192 19 /dev/hda4
/slot0 2026608 4 2026604 1 /dev/hdc1
/logflash 7997912 219408 7372232 3 127.1.1.6:/mnt/logflash/
/logflash_sup-remote 1767480 1121784 555912 67 127.1.1.6:/mnt/bootflash/
/logflash_sup-remote 7953616 554976 6994608 8 127.1.1.6:/mnt/logflash/
```

When reviewing this output, the value of none in the Filesystem column means that it is a tmpfs type.

In this example, utilization is high because the `/var/sysmgr` (or subfolders) is using a lot of space. `/var/sysmgr` is a tmpfs mount, which means that the files exist in RAM only. You need to determine what type of files are filling the partition and where they came from (cores/debugs/etc). Deleting the files will reduce utilization, but you should try to determine what type of files are taking up the space and what process left them in tmpfs.

Use the following commands to display and delete the problem files from the CLI:

- The `show system internal dir full directory path` command lists all the files and sizes for the specified path (hidden command).
- The `filesys delete full file path` command deletes a specific file (hidden command).

Kernel

Kernel issues are less common, but you can determine the problem by reviewing the slab utilization in the `show system internal kernel meminfo` command output. Generally, kernel troubleshooting requires Cisco customer support assistance to isolate why the utilization is increasing.

If slab memory usage grows over time, use the following commands to gather more information:
• The `show system internal kernel malloc-stats` command displays all the currently loaded KLMs, malloc, and free counts.

```
switch# show system internal kernel malloc-stats
Kernel Module Memory Tracking
================================================================================================
Module       kmalloc kcalloc kfree diff
klm_usd      00318846 00007000 00318825 00000021
klm_eobcmon  08366981 00000000 08366981 00000000
klm_utaker   00001306 00000000 00001306 00000000
klm_sysmgr-hb 00000540 00000000 00000540 00000000
klm_idehs    00000001 00000000 00000001 00000000
klm_sup_ctrl_mc 02095800 00000000 02095800 00000000
klm_sup_config 00000003 00000000 00000003 00000000
klm_mts      03357731 00000000 03344979 00012752
klm_kadb     00000368 00000000 00000368 00000000
klm_aipc     00850300 00000000 00850272 00000028
klm_pss      04090498 00000000 04043260 00047238
klm_rwsem    00000001 00000000 00000001 00000000
klm_vdc      00000126 00000000 00000126 00000000
klm_modlock  00000016 00000000 00000016 00000000
klm_e1000    00000024 00000000 00000024 00000000
klm_dc_sprom 00000123 00000000 00000123 00000000
klm_sdwrap   00000024 00000000 00000024 00000000
klm_obfl     00000050 00000000 00000050 00000000
```

By comparing several iterations of this command, you can determine if some KLMs are allocating a lot of memory but are not freeing/returning the memory back (the differential value will be very large compared to normal).

• The `show system internal kernel skb-stats` command displays the consumption of SKBs (buffers used by KLMs to send and receive packets).

```
switch# show system internal kernel skb-stats
Kernel Module skbuff Tracking
================================================================================================
Module  alloc free diff
klm_shreth 00028632 00028625 00000007
klm_eobcmon 02798915 02798829 0000086
klm_mts    00420053 00420047 0000006
klm_aipc   00373467 00373450 000017
klm_pss    00420053 00420047 0000006
klm_rwsem  00000001 00000000 00000001
klm_vdc    00000126 00000000 00000126
klm_modlock 00000016 00000000 00000016
klm_e1000  00000024 00000024 00000000
klm_dc_sprom 00000123 00000123 00000000
klm_sdwrap 00000024 00000024 00000000
klm_bobr   00000050 00000050 00000000
```

Compare the output of several iterations of this command to see if the differential value is growing or very high.

• The `show hardware internal proc-info slabinfo` command dumps all of the slab information (memory structure used for kernel management). The output can be large.

## User Processes

If page cache and kernel issues have been ruled out, utilization might be high as a result of some user processes taking up too much memory or a high number of running processes (due to the number of features enabled).

**Note**

Cisco NX-OS defines memory limits for most processes (rlimit). If this rlimit is exceeded, sysmgr will crash the process, and a core file is usually generated. Processes close to their rlimit may not have a large impact on platform utilization but could become an issue if a crash occurs.
Determining Which Process Is Using a Lot of Memory

The following commands can help you identify if a specific process is using a lot of memory:

- **The `show process memory` command** displays the memory allocation per process.

  ```
  switch# show processes memory
  PID MemAlloc MemLimit MemUsed StackBase/Ptr Process
  ----- -------- ---------- ---------- ----------------- ---------
  4662 52756480 562929945 150167552 bfffd00/bfffd970 netstack
  ```

  **Note** The output of the `show process memory` command might not provide a completely accurate picture of the current utilization (allocated does not mean in use). This command is useful for determining if a process is approaching its limit.

- **The `show system internal processes memory` command** displays the process information in the memory alerts log (if the event occurred).

  To determine how much memory the processes are really using, check the Resident Set Size (RSS). This value will give you a rough indication of the amount of memory (in KB) that is being consumed by the processes. You can gather this information by using the `show system internal processes memory` command.

  ```
  switch# show system internal processes memory
  PID TTY STAT TIME MAJFLT TRS RSS VSZ %MEM COMMAND
  4811 ? Ssl 00:00:16 0 0 49772 361588 0.3 /isan/bin/routing-sw/cli
  -cli /isan/etc/routing-sw/cli
  4928 ? Ssl 00:18:41 0 0 44576 769512 0.2 /isan/bin/routing-sw/netstack
  /isan/etc/routing-sw/pm.cfg
  4897 ? Ssl 00:00:18 0 0 42604 602216 0.2 /isan/bin/routing-sw/arp
  4791 ? Ss 00:00:00 0 0 34384 318856 0.2 /isan/bin/pixm_vl
  4957 ? Sal 00:00:26 0 0 30440 592348 0.1 /isan/bin/snmpd -f -s udp:161
  udp6:161 tcp:161 tcp6:161
  5097 ? Ssl 00:06:53 0 0 28052 941880 0.1 /isan/bin/routing-sw/pim -t
  5062 ? Ss 00:01:00 0 0 27300 310596 0.1 /isan/bin/diag_port_lb
  5087 ? Sal 00:03:53 0 0 24988 992756 0.1 /isan/bin/routing-sw/bgp -t
  65001
  4792 ? Ss 00:00:00 0 0 24080 309024 0.1 /isan/bin/pixm_gl
  5063 ? Ss 00:00:01 0 0 21940 317440 0.1 /isan/bin/ethpm
  5044 ? Ss 00:00:00 0 0 21700 304032 0.1 /isan/bin/eltm
  5049 ? Ss 00:00:14 0 0 20592 306156 0.1 /isan/bin/ipqosmgr
  5042 ? Ssl 00:00:05 0 0 20580 672640 0.1 /isan/bin/routing-sw/igmp
  5082 ? Ssl 00:00:25 0 0 19948 914088 0.1 /isan/bin/routing-sw/mrib
  -m 4
  5091 ? Sal 00:01:58 0 0 19192 729500 0.1 /isan/bin/routing-sw/ospfv3
  -t 8893
  5092 ? Ssl 00:01:55 0 0 18988 861556 0.1 /isan/bin/routing-sw/ospf
  -t 6464
  5083 ? Ss 00:00:06 0 0 18876 309516 0.1 /isan/bin/mfdm
  ```

  If you see an increase in the utilization for a specific process over time, you should gather additional information about the process utilization.
Determining How a Specific Process Is Using Memory

If you have determined that a process is using more memory than expected, it is helpful to investigate how the memory is being used by the process.

- The `show system internal sysmgr service pid PID-in-decimal` command dumps the service information running the specified PID.

```
switch# show system internal sysmgr service pid 4727
Service "pixm" ("pixm", 109):
  UUID = 0x133, PID = 4727, SAP = 176
  State: SRV_STATE_HANDSHAKED (entered at time Fri May 10 01:42:01 2013).
  Restart count: 1
The service never crashed since the last reboot.
  Tag = N/A
  Plugin ID: 1
```

Convert the UUID from the above output to decimal and use in the next command.

**Note**

If you are troubleshooting in a lab, you can use Cisco NX-OS hexadecimal/decimal conversion using the following hidden commands:

- `hex<decimal to convert>`
- `dec<hexadecimal to convert>`

- The `show system internal kernel memory uuid uuid-in-decimal` command displays the detailed process memory usage including its libraries for a specific UUID in the system (convert UUID from the sysmgr service output).

```
switch# show system internal kernel memory uuid 307
Note: output values in KiloBytes
<table>
<thead>
<tr>
<th>Name</th>
<th>ras</th>
<th>shrd</th>
<th>drt</th>
<th>map</th>
<th>heap</th>
<th>ro</th>
<th>dat</th>
<th>bss</th>
<th>stk</th>
<th>misc</th>
</tr>
</thead>
<tbody>
<tr>
<td>/isan/bin/pixm</td>
<td>7816</td>
<td>5052</td>
<td>2764</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>52</td>
<td></td>
</tr>
<tr>
<td>/isan/plugin/1/isan/bin/pixm</td>
<td>115472</td>
<td>0</td>
<td>115472</td>
<td>0</td>
<td>109176</td>
<td>752</td>
<td>28</td>
<td>6268</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>/lib/ld-2.3.3.so</td>
<td>84</td>
<td>76</td>
<td>8</td>
<td>2</td>
<td>0</td>
<td>76</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>/usr/lib/libbz.so.1.2.1.1</td>
<td>16</td>
<td>12</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>122</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/libstdc++.so.6.0.3</td>
<td>296</td>
<td>272</td>
<td>24</td>
<td>1</td>
<td>0</td>
<td>272</td>
<td>20</td>
<td>4</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>/lib/libgcc_s.so.1</td>
<td>1824</td>
<td>12</td>
<td>1812</td>
<td>1</td>
<td>1808</td>
<td>12</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>/isan/plugin/1/isan/lib/libtmifdb.so.0</td>
<td>12</td>
<td>8</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>8</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>/isan/plugin/0/isan/lib/libtmifdb_stub</td>
<td>12</td>
<td>8</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>8</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>/dev/mts</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>/isan/plugin/1/isan/lib/libpcm_sdb.so.0</td>
<td>16</td>
<td>12</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>12</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
```

Cisco Nexus 9000 Series NX-OS Troubleshooting Guide, Release 6.x
This output helps you to determine if a process is holding memory in a specific library and can assist with memory leak identification.

- The `show system internal service mem-stats detail` command displays the detailed memory utilization including the libraries for a specific service.

```plaintext
switch# show system internal pixm mem-stats detail
Private Mem stats for UUID : Malloc track Library(103) Max types: 5
-----------------------------------------------------------------------------
TYPE NAME ALLOCS BYTES
CURR MAX CURR MAX
2 MT_MEM_mtrack_hdl 35 35 132132 149940
3 MT_MEM_mtrack_info 598 866 9568 13856
4 MT_MEM_mtrack_lib_name 593 866 15860 22970
-----------------------------------------------------------------------------
Total bytes: 157560 (153k)
-----------------------------------------------------------------------------
Private Mem stats for UUID : Non mtrack users(0) Max types: 15?
-----------------------------------------------------------------------------
TYPE NAME ALLOCS BYTES
CURR MAX CURR MAX
1 [0x41000000]ld-2.15.so 283 283 48255 48256
2 [0x41024000]libc-2.15.so 142 144 4979 5587
8 [0x41241000]libglib-2.0.so.0.3200.3 500 771 10108 15588
39 [0xf68af000]libindxobj.so 7 7 596 596
45 [0xf68ca000]libavl.so 73 73 1440 1440
67 [0xf71b3000]libsdb.so 56 58 3670 73278
75 [0xf7313000]libmpmts.so 35 37 280 380
86 [0xf7441000]libutils.so 23 28 3283 5766
89 [0xf74bf000]libpss.so 59 60 8564 483642
90 [0xf750b000]libmts.so 7 8 828 828
92 [0xf754c000]libacfg.so 4 4 0 51337
-----------------------------------------------------------------------------
Total bytes: 82817 (80k)
-----------------------------------------------------------------------------
remaining output omitted
```

These outputs are usually requested by the Cisco customer support representative when investigating a potential memory leak in a process or its libraries.

**Built-in Platform Memory Monitoring**

Cisco NX-OS has built-in kernel monitoring of memory usage to help avoid system hangs, process crashes, and other undesirable behavior. The platform manager periodically checks the memory utilization (relative to the total RAM present) and automatically generates an alert event if the utilization passes the configured threshold values. When an alert level is reached, the kernel attempts to free memory by releasing pages that are no longer needed (for example, the page cache of persistent files that are no longer being accessed), or if critical levels are reached, the kernel will kill the highest utilization process. Other Cisco NX-OS components have introduced memory alert handling, such as the Border Gateway Protocol's (BGP's) graceful low memory handling, that allows processes to adjust their behavior to keep memory utilization under control.
Memory Thresholds

When many features are deployed, baseline memory requires the following thresholds:

- 85% MINOR
- 90% SEVERE
- 95% CRITICAL

The thresholds are configurable using the system memory-thresholds minor percentage severe percentage critical percentage command.

The `show system internal memory-status` command allows you to check the current memory alert status.

```
switch# show system internal memory-status
MemStatus: OK
```

Memory Alerts

When a memory threshold has been passed (OK -> MINOR, MINOR -> SEVERE, SEVERE -> CRITICAL), the Cisco NX-OS platform manager captures a snapshot of memory utilization and logs an alert to syslog. This snapshot is useful in determining why memory utilization is high (process, page cache, or kernel). The log is generated in the Linux root path (/) and copy is moved to OBFL (/mnt/plog) if possible. This log is very useful for determining if memory utilization is high due to the memory that was consumed by the page cache, kernel, or Cisco NX-OS user processes.

The `show system internal memory-alerts-log` command displays the memory alerts log.

The memory alerts log consists of the following outputs:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cat /proc/memory_events</code></td>
<td>Provides a log of time stamps when memory alerts occurred.</td>
</tr>
<tr>
<td><code>cat /proc/meminfo</code></td>
<td>Shows the overall memory statistics including the total RAM, memory consumed by the page cache, slabs (kernel heap), mapped memory, available free memory, and so on.</td>
</tr>
<tr>
<td><code>cat /proc/memtrack</code></td>
<td>Displays the allocation/deallocation counts of the KLMs (Cisco NX-OS processes running in kernel memory).</td>
</tr>
<tr>
<td><code>df -hT</code></td>
<td>Displays file system utilization information (with type).</td>
</tr>
<tr>
<td><code>du --si -La /tmp</code></td>
<td>Displays file information for everything located in /tmp (symbolic link to /var/tmp).</td>
</tr>
<tr>
<td><code>cat /proc/memory_events</code></td>
<td>Dumped a second time to help determine if utilization changed during data gathering.</td>
</tr>
<tr>
<td><code>cat /proc/meminfo</code></td>
<td>Dumped a second time to help determine if utilization changed during data gathering.</td>
</tr>
</tbody>
</table>
Memory Alerts
Troubleshooting Packet Flow Issues

This chapter contains the following sections:

- Packet Flow Issues, page 79
- Monitoring Inband Packet Statistics, page 80
- Fabric Connectivity Commands, page 81

Packet Flow Issues

Packets could be dropped for the following reasons:

- Software-switched packets could be dropped because of Control Plane Policing (CoPP).
- Hardware-switched packets could be dropped by the hardware because of a bandwidth limitation.

Packets Dropped Because of Rate Limits

Use the `show hardware rate-limit` command to determine if packets are being dropped because of a rate limit.

```
switch(config)# show hardware rate-limit module 1
```

Units for Config: packets per second
Allowed, Dropped & Total: aggregated since last clear counters

<table>
<thead>
<tr>
<th>Rate Limiter Class</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list-log</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Config : 100</td>
</tr>
<tr>
<td></td>
<td>Allowed : 0</td>
</tr>
<tr>
<td></td>
<td>Dropped : 0</td>
</tr>
<tr>
<td></td>
<td>Total : 0</td>
</tr>
</tbody>
</table>
Packets Dropped Because of CoPP

Use the `show policy-map interface control-plane` command to determine if packets are being dropped because of CoPP.

```bash
switch# show policy-map interface control-plane
class-map copp-system-p-class-exception (match-any)
  match exception ip option
  match exception ip icmp unreachable
  match exception ttl-failure
  match exception ipv6 option
  match exception ipv6 icmp unreachable
  match exception mtu-failure
  set cos 1
  police cir 200 pps , bc 32 packets

module 27 :
  transmitted 0 packets;
  dropped 0 packets;
module 28 :
  transmitted 0 packets;
  dropped 0 packets;
```

Monitoring Inband Packet Statistics

Use the `show hardware internal cpu-mac inband counters` command to display inband packet statistics for supervisor modules, fabric modules, and line cards.

```bash
switch# show hardware internal cpu-mac inband counters
eth2 counters:
  eth2  Link encap:Ethernet  HWaddr 00:00:00:01:1b:01
        BROADCAST MULTICAST  MTU:9400  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

eth3 counters:
  eth3  Link encap:Ethernet  HWaddr 00:00:00:01:1b:01
        inet6 addr: fe80::200:ff:fe01:1b01/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:9400  Metric:1
        RX packets:425432 errors:0 dropped:0 overruns:0 frame:0
        TX packets:352432 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:253284953 (241.5 MiB) TX bytes:249647978 (238.0 MiB)

ps-inb counters:
  ps-inb Link encap:Ethernet  HWaddr 00:00:00:01:1b:01
        inet6 addr: fe80::200:ff:fe01:1b01/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:9400  Metric:1
        RX packets:129086 errors:0 dropped:0 overruns:0 frame:0
        TX packets:129761 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:221538103 (211.2 MiB) TX bytes:227158091 (216.6 MiB)

switch# slot 22 show hardware internal cpu-mac inband counters
inband0 counters:
  inband0 Link encap:Ethernet  HWaddr 00:00:00:01:16:03
        inet addr:127.2.2.22  Bcast:127.2.255.255  Mask:255.255.0.0
        inet6 addr: fe80::200:ff:fe01:1603/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:9676  Metric:1
        RX packets:147425 errors:0 dropped:0 overruns:0 frame:0
        TX packets:147470 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:532
```
Fabric Connectivity Commands

Cisco NX-OS provides the following commands to display information and statistics related to fabric connectivity:

- `show system internal fabric connectivity [module module-number]`—Displays connectivity information for all fabric modules or a single module.

```
switch# show system internal fabric connectivity
HiGIG Link-info Linecard slot:4
-------------------------------------------------------------------------------------
<table>
<thead>
<tr>
<th>LC-Slot</th>
<th>LC-Unit</th>
<th>LC-HGLink</th>
<th>FM-Slot</th>
<th>FM-Unit</th>
<th>FM-HGLink</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>0</td>
<td>HG02</td>
<td>22</td>
<td>0</td>
<td>HG09</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>HG03</td>
<td>22</td>
<td>1</td>
<td>HG09</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>HG06</td>
<td>24</td>
<td>0</td>
<td>HG09</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>HG07</td>
<td>24</td>
<td>1</td>
<td>HG09</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>HG02</td>
<td>22</td>
<td>0</td>
<td>HG10</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>HG03</td>
<td>22</td>
<td>1</td>
<td>HG10</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>HG06</td>
<td>24</td>
<td>0</td>
<td>HG10</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>HG07</td>
<td>24</td>
<td>1</td>
<td>HG10</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>HG02</td>
<td>22</td>
<td>0</td>
<td>HG11</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>HG03</td>
<td>22</td>
<td>1</td>
<td>HG11</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>HG06</td>
<td>24</td>
<td>0</td>
<td>HG11</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>HG07</td>
<td>24</td>
<td>1</td>
<td>HG11</td>
</tr>
</tbody>
</table>

HiGIG Link-info Fabriccard slot:22
-------------------------------------------------------------------------------------
<table>
<thead>
<tr>
<th>FM-Slot</th>
<th>FM-Unit</th>
<th>FM-HGLink</th>
<th>LC-Slot</th>
<th>LC-Unit</th>
<th>LC-HGLink</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>0</td>
<td>HG09</td>
<td>4</td>
<td>0</td>
<td>HG02</td>
</tr>
<tr>
<td>22</td>
<td>0</td>
<td>HG10</td>
<td>4</td>
<td>1</td>
<td>HG02</td>
</tr>
<tr>
<td>22</td>
<td>1</td>
<td>HG11</td>
<td>4</td>
<td>2</td>
<td>HG02</td>
</tr>
<tr>
<td>22</td>
<td>1</td>
<td>HG09</td>
<td>4</td>
<td>0</td>
<td>HG03</td>
</tr>
<tr>
<td>22</td>
<td>1</td>
<td>HG10</td>
<td>4</td>
<td>1</td>
<td>HG03</td>
</tr>
<tr>
<td>22</td>
<td>1</td>
<td>HG11</td>
<td>4</td>
<td>2</td>
<td>HG03</td>
</tr>
</tbody>
</table>

HiGIG Link-info Fabriccard slot:24
-------------------------------------------------------------------------------------
<table>
<thead>
<tr>
<th>FM-Slot</th>
<th>FM-Unit</th>
<th>FM-HGLink</th>
<th>LC-Slot</th>
<th>LC-Unit</th>
<th>LC-HGLink</th>
</tr>
</thead>
<tbody>
<tr>
<td>24</td>
<td>0</td>
<td>HG09</td>
<td>4</td>
<td>0</td>
<td>HG06</td>
</tr>
<tr>
<td>24</td>
<td>0</td>
<td>HG10</td>
<td>4</td>
<td>1</td>
<td>HG06</td>
</tr>
<tr>
<td>24</td>
<td>1</td>
<td>HG11</td>
<td>4</td>
<td>2</td>
<td>HG06</td>
</tr>
<tr>
<td>24</td>
<td>1</td>
<td>HG09</td>
<td>4</td>
<td>0</td>
<td>HG07</td>
</tr>
<tr>
<td>24</td>
<td>1</td>
<td>HG10</td>
<td>4</td>
<td>1</td>
<td>HG07</td>
</tr>
</tbody>
</table>
```
• show system internal interface counters module module-number [nz]—Displays the rates for HG or fabric links on a module. The nz option displays only non-zero counters.

```plaintext
switch# show system internal interface counters module 22 nz
Internal Port Counters (150 secs rate) for Slot: 22
----------------------------------------------------------------------------------
Interface ASIC ASIC BCM TxBitRate(BwUtil) TxPktRate RxBitRate(BwUtil) RxPktRate
Port Inst Port (bps) (pps) (bps) (pps)
----------------------------------------------------------------------------------
i12/1/10 HG9 0 10 0( 0.00) 0 33064( 0.00) 17
```

```plaintext
switch# show system internal interface counters module 22
Internal Port Counters (150 secs rate) for Slot: 22
----------------------------------------------------------------------------------
Interface ASIC ASIC BCM TxBitRate(BwUtil) TxPktRate RxBitRate(BwUtil) RxPktRate
Port Inst Port (bps) (pps) (bps) (pps)
----------------------------------------------------------------------------------
i12/1/2 HG1 0 1 0( 0.00) 0 0( 0.00) 0
i12/1/3 HG2 0 2 0( 0.00) 0 0( 0.00) 0
i12/1/4 HG3 0 4 0( 0.00) 0 0( 0.00) 0
i12/1/5 HG4 0 5 0( 0.00) 0 0( 0.00) 0
i12/1/6 HG5 0 6 0( 0.00) 0 0( 0.00) 0
i12/1/7 HG6 0 7 0( 0.00) 0 0( 0.00) 0
i12/1/8 HG7 0 8 0( 0.00) 0 0( 0.00) 0
i12/1/9 HG8 0 9 0( 0.00) 0 0( 0.00) 0
i12/1/10 HG9 0 10 0( 0.00) 0 30888( 0.00) 12
```

Cisco Nexus 9000 Series NX-OS Troubleshooting Guide, Release 6.x
show system internal interface counters detail module module-number—Displays detailed statistics for all HG or fabric links on a single module.

show system internal interface counters detail module 4

---------
Interface: ii4/1/3  ASIC Inst# 0/Port# 3/Name HG2
---------
Last Cleared @ Thu Jan 1 00:00:00 2013
(0)

Tx/Rx Rates (per second):
segs  tx bytes  tx packets  rx bytes  rx packets
[0] - 10  0         0         0         0
[1] - 150 9448      60        0         0
[2] - 300 9448      60        0         0

Mac Pktflow:
Rx Counters:
Ingress Packets : 0x0000000000000000/0
Unicast Packets : 0x0000000000000000/0
Multicast Packets: 0x0000000000000000/0
Broadcast Packets: 0x0000000000000000/0
Jumbo Packets : 0x0000000000000000/0
Total Bytes : 0x0000000000000000/0

Rx Bytes by Packet Size:
  64: 0x0000000000000000/0
  65 - 127: 0x0000000000000000/0
  128 - 255: 0x0000000000000000/0
  256 - 511: 0x0000000000000000/0
  512 - 1023: 0x0000000000000000/0
  1024 - 1518: 0x0000000000000000/0
  1519 - 1548: 0x0000000000000000/0

Tx Counters:
Egress Packets : 0x0000000000001351/4945
Unicast Packets: 0x0000000000001351/4945
Multicast Packets: 0x0000000000000000/0
Broadcast Packets: 0x0000000000000000/0
Jumbo Packets : 0x0000000000000000/0
Total Bytes : 0x000000000008e756/583510

Tx Bytes by Packet Size:
  64: 0x0000000000000000/0
  65 - 127: 0x0000000000001351/4945
  128 - 255: 0x0000000000000000/0
  256 - 511: 0x0000000000000000/0
  512 - 1023: 0x0000000000000000/0
  1024 - 1518: 0x0000000000000000/0
  1519 - 1548: 0x0000000000000000/0
  trunk: 0x0000000000000000/0

Mac Control:
Rx Pause: 0x0000000000000000/0
Tx Pause: 0x0000000000000000/0
Reset: 0x0000000000000000/0

Mac Errors:
Undersize: 0x0000000000000000/0
Runt: 0x0000000000000000/0
Crc: 0x0000000000000000/0
Input Errors: 0x0000000000000000/0
In Discard: 0x0000000000000000/0
Giants: 0x0000000000000000/0
Output Errors: 0x0000000000000000/0
Output Discard: 0x0000000000000000/0
Bad Proto: 0x0000000000000000/0
Collision: 0x0000000000000000/0
Late Collision: 0x0000000000000000/0
No Carrier: 0x0000000000000000/0
Troubleshooting PowerOn Auto Provisioning

This chapter contains the following sections:

- Switch Does Not Come Up in Time for POAP to Complete, page 85
- POAP Fails, page 85

Switch Does Not Come Up in Time for POAP to Complete

If the switch does not come up in a reasonable duration for POAP to complete, connect to the switch through the serial line and check to see if it is stuck at the following prompt:

```
Waiting for system online status before starting POAP ...
Waiting for system online status before starting POAP ...
Waiting for system online status before starting POAP ...
```

System is not fully online. Skip POAP? (yes/no){n}:

You can continue with POAP by entering no at the prompt. If POAP does not start properly on the second attempt, proceed with the normal setup by entering yes at the prompt when it returns.

POAP Fails

Take these actions if PowerOn Auto Provisioning (POAP) fails for any reason:

- Stop the POAP process to continue with the normal switch bring-up steps. It might take a few minutes for a full stop of POAP, so be patient.

```
2013 Oct 29 22:24:59 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: Assigned IP address: 172.23.40.221
2013 Oct 29 22:24:59 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: Netmask: 255.255.255.0
2013 Oct 29 22:24:59 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: Default Gateway: 172.23.40.1
2013 Oct 29 22:24:59 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: Script Server: 172.23.40.6
2013 Oct 29 22:24:59 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: Script Name: /pxelinux.0
2013 Oct 29 22:25:09 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: The POAP Script download has started
2013 Oct 29 22:25:09 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: The POAP Script is being downloaded from [copy tftp://172.23.40.6//pxelinux.0 bootflash://scripts/script.sh vrf management ]
```
2013 Oct 29 22:25:10 switch %$ VDC-1 %$ %POAP-2-POAP_FAILURE: POAP DHCP discover phase failed
2013 Oct 29 22:25:12 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: Abort Power On Auto Provisioning and continue with normal setup ?(yes/no)[n]:
2013 Oct 29 22:25:46 switch %$ VDC-1 %$ %POAP-2-POAP_DHCP_DISCOVER_START: POAP DHCP Discover phase started
2013 Oct 29 22:25:46 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: Abort Power On Auto Provisioning and continue with normal setup ?(yes/no)[n]:

Abort Auto Provisioning and continue with normal setup ?(yes/no)[n]: yes

- Check the failure reason in the log files. Two POAP log files are saved on the bootflash. Logs from the POAP process are stored in the file that ends with `poap_pid_init.log` as shown below. The failure reason should appear toward the end of this file.

```
bash-4.2# tail 20131029_222312_poap_5367_init.log -n 3
Tue Oct 29 22:27:41 2013:poap_net_rx_pkt:Droppping the pakcet due to Ethernet hdrparsing error on if_index - 5000000
Tue Oct 29 22:27:41 2013:DEST IP is not Broadcast
Tue Oct 29 22:27:41 2013:poap_net_rx_pkt:Droppping the pakcet due to Ethernet hdrparsing error on if_index - 5000000
```

- Check to see if the POAP script file that is downloaded from your DHCP or TFTP server fails in the process of running. Depending on the stage of the failure, the device might proceed with the normal setup or reboot.

```
2013 Oct 29 22:42:34 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: Assigned IP address: 172.23.40.181
2013 Oct 29 22:42:34 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: Netmask: 255.255.255.0
2013 Oct 29 22:42:34 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: Default Gateway: 172.23.40.1
2013 Oct 29 22:42:34 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: Script Server: 172.23.40.6
2013 Oct 29 22:42:45 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: Script Name: poap.py
2013 Oct 29 22:42:45 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: The POAP Script download has started
2013 Oct 29 22:42:45 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: The POAP Script is being downloaded from [copy tftp://172.23.40.6/poap.py bootflash:scripts/script.sh vrf management ]
2013 Oct 29 22:42:46 switch %$ VDC-1 %$ %POAP-2-POAP_SCRIPT_DOWNLOADED: Successfully downloaded POAP script file
2013 Oct 29 22:42:46 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: Script file size 21965, MD5 checksum 1bd4b86892439c5785a20a3e3ac2b0de
2013 Oct 29 22:42:46 switch %$ VDC-1 %$ %POAP-2-POAP_SCRIPT_STARTED_MD5_NOT_VALIDATED: POAP script execution started(MD5 not validated)
2013 Oct 29 22:47:57 switch %$ VDC-1 %$ %POAP-2-POAP_FAILURE: POAP script execution aborted
```

- The POAP script file logs are written to a file under the bootflash scheme. The filename starts with `poap.log`. If there are multiple file logs, look at the one with the most recent time stamp for any errors.

```
bash-4.2# tail poap.log.22_42_46
CLI : show file volatile:poap.cfg.md5.poap_md5 | grep -v "^#" | head lines 1 | sed 's/\n.*/\n/'
INFO: md5sum 46684d8f8b7c5ffacc3b37ac8560928e5 (.md5 file)
CLI : show file volatile:poap.cfg md5sum
INFO: md5sum 46684d8f8b7c5ffacc3b37ac8560928e5 (recalculated)
CLI : show system internal platform internal info | grep box_online | sed 's/[^0-9]*//g'
INFO: Setting the boot variables
CLI : config terminal | boot nxos bootflash:poap/system.img
CLI : copy running-config startup-config
CLI : copy volatile:poap.cfg & scheduled-config
INFO: Configuration successful
```
Troubleshooting the Python API

This chapter contains the following sections:

- Receiving Python API Errors, page 87

Receiving Python API Errors

Take these actions if any of the following Python API errors appear:
## Receiving Python API Errors

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Solution</th>
<th>Example</th>
</tr>
</thead>
</table>
| The Python cli API throws a NameError. | Import the cli module into the global namespace. | ```
>>> cli('show clock')
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
NameError: name 'cli' is not defined

>>> from cli import *
>>> cli('show clock')
'20:23:33.967 UTC Fri Nov 01 2013\n'
``` |
| The Python clid API throws a `structured_output_not_supported_error`. | Use the cli or clid API. The clid API works only with commands that support structured data output. | ```
>>> clid('show clock')
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
  File "/isan/python/scripts/cli.py", line 45, in clid
    raise
  structured_output_not_supported_error(cmd)
errors.structured_output_not_supported_error: 'show clock'
``` |
| The cli API and cisco objects throw a `Permission denied error`. | Make sure your login ID has sufficient permissions to access the command or resource. If necessary, ask your network administrator for additional permissions. | ```
>>> from cli import *
>>> cli('clear counters')
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
  File "/isan/python/scripts/cli.py", line 20, in cli
    raise cmd_exec_error(msg)
errors.cmd_exec_error: '% Permission denied for the role
  File "/isan/python/scripts/cli.py", line 20, in cli
    raise cmd_exec_error(msg)
errors.cmd_exec_error: '% Permission denied for the role

Cmd exec error.
``` |
| The urllib2 or socket connection is not processed. | Make sure you are using the correct virtual routing context. If not, switch to the correct one. | ```
>>> import os
>>> os.system('whoami')
test
``` |
## Receiving Python API Errors

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Solution</th>
<th>Example</th>
</tr>
</thead>
</table>
| >>> import urllib2  
>>> u=urllib2('http://172.23.40.211:8000/welcome.html')  
Traceback (most recent call last):  
  File "<stdin>", line 1, in <module>  
  TypeError: 'module' object is not callable  
>>> u=urllib2.urlopen('http://172.23.40.211:8000/welcome.html')  
Traceback (most recent call last):  
  File "<stdin>", line 1, in <module>  
  File "/isan/python/python2.7/urllib2.py", line 127, in urlopen  
    return _opener.open(url, data, timeout)  
  File "/isan/python/python2.7/urllib2.py", line 404, in open  
    response = self._open(req, data)  
  File "/isan/python/python2.7/urllib2.py", line 422, in _open  
    'open', req)  
  File "/isan/python/python2.7/urllib2.py", line 382, in _call_chain  
    result = func(*args)  
  File "/isan/python/python2.7/urllib2.py", line 1214, in http_open  
    return self.do_open(httplib.HTTPConnection, req)  
  File "/isan/python/python2.7/urllib2.py", line 1184, in do_open  
    raise URLError(err)  
urllib2.URLError: <urlopen error [Errno 113] No route to host>  
>>> from cisco.vrf import *  
>>> VRF.get_vrf_name_by_id(get_global_vrf())  
'default' |
Troubleshooting NX-API

This chapter contains the following sections:

- NX-API Guidelines, page 91
- NX-API Is Not Responding, page 91
- Configuration Fails, page 92
- Permission Is Denied for Bash, page 92
- Output Cannot Be Retrieved from the Browser Sandbox, page 92
- CLI Command Errors Are Appearing, page 92
- Error Messages Are Appearing, page 92
- Temporary Files Are Disappearing, page 93
- Chunks of the Command Output Are Not Being Delivered, page 93

NX-API Guidelines

NX-API performs authentication through a programmable authentication module (PAM) on the switch. Use cookies to reduce the number of PAM authentications and thus reduce the load on PAM.

NX-API Is Not Responding

Take these actions if NX-API is not responding:

- Make sure that NX-API is enabled by using the `show feature | grep nxapi` command.
- Make sure that HTTP or HTTPs is enabled by using the `show nxapi` command.
- Make sure that NX-API is listening on the expected port by using the `show nxapi` command.
- Check for a long running command. Currently NX-API runs on a single worker process and is single threaded. If one command takes a long time to complete, it will block other commands. NX-API caches the request. When the current request completes, the others will be served.
Configuration Fails

Take these actions if the user cannot execute configuration commands:

• Make sure that the user has the correct privileges to execute the commands.

Permission Is Denied for Bash

Take these actions if users receive a "Permission Denied" message for Bash:

• Make sure that Bash is enabled by using the `show feature | grep bash` command.
• Make sure that the current user has the correct privileges to access Bash.
• For more information on Bash, see the Cisco Nexus 9000 Series NX-OS Programmability Guide.

Output Cannot Be Retrieved from the Browser Sandbox

Take these actions if you cannot retrieve the output from the browser sandbox:

• When the output is large or the command execution takes a long time, the browser might not be able to handle the load and might time out. Try using the Python client to access the NX-API. For instructions, see the Cisco Nexus 9000 Series NX-OS Programmability Guide.

Note The recommended browser is Mozilla Firefox.

CLI Command Errors Are Appearing

Take these actions if CLI command errors appear when the user runs multiple commands:

• Check to see how multiple commands are separated. Show and configure commands must be separated by a [space]. Bash commands must be separated by a semicolon (;).

Error Messages Are Appearing

Take these actions if error messages are appearing in the output:

• Follow the instructions in the error message.
If the Bash commands do not go through, make sure that Bash is enabled by using the `show feature | grep bash` command. For more information on Bash, see the Cisco Nexus 9000 Series NX-OS Programmability Guide.

- Make sure that the user has the correct privileges to execute the command.
- Follow the instructions in NX-API Is Not Responding, on page 91.

Temporary Files Are Disappearing

For every request, a temporary file is created in /volatile to store the command output that is sent back to the client. If the chunk parameter on the request is 0, the file is deleted right before the command output is sent back to the client. If the request does have chunk = 1, the file is retained so that the chunks can be extracted from it and sent to the client. That file will be cleaned up on a periodic basis. Currently that cleanup is set to occur once every 100 requests. Files are cleaned up if they are not accessed within 60 seconds of being created or are not modified or their status is not updated within 600 seconds.

Chunks of the Command Output Are Not Being Delivered

For requests where chunk = 1, if the sid is set to the same value, you will get the same chunk of the command output. This functionality allows for situations where a client requests a specific chunk and does not receive it in a timely manner because it is dropped or blocked somewhere in the network. The clients can request the same chunk again, and they will receive the correct data as long as the temporary file has not been cleaned up (as described in Temporary Files Are Disappearing, on page 93).
Chunks of the Command Output Are Not Being Delivered
Troubleshooting Service Failures

This chapter contains the following sections:

- Identifying Memory Allocations for Processes, page 95
- Identifying CPU Utilization for Processes, page 96
- Monitoring Process Core Files, page 97
- Processing the Crash Core Files, page 97
- Clearing the Core, page 97
- Enabling Auto-Copy for Core Files, page 98

Identifying Memory Allocations for Processes

You can identify the allocation, limit, memory allocation, and usage for each process in the memory. The following is a sample output from the `show processes memory` command. This output has been abbreviated to make the example more concise.

```
switch# show processes memory
PID MemAlloc MemLimit MemUsed StackBase/Ptr Process
--- -------- -------- ------- ----------------- -----------
1 159744 0 2027520 ff808d30/ffffffff init
2 0 0 0 0/0 kthread
3 0 0 0 0/0 migration/0
4 0 0 0 0/0 watchdog/0
5 0 0 0 0/0 migration/1
6 0 0 0 0/0 ksoftirqd/1
7 0 0 0 0/0 watchdog/1
8 0 0 0 0/0 migration/2
9 0 0 0 0/0 ksoftirqd/2
10 0 0 0 0/0 watchdog/2
11 0 0 0 0/0 migration/3
12 0 0 0 0/0 ksoftirqd/3
13 0 0 0 0/0 watchdog/3
14 0 0 0 0/0 migration/4
15 0 0 0 0/0 ksoftirqd/4
16 0 0 0 0/0 watchdog/4
17 0 0 0 0/0 migration/5
18 0 0 0 0/0 ksoftirqd/5
19 0 0 0 0/0 watchdog/5
20 0 0 0 0/0 migration/6
21 0 0 0 0/0 ksoftirqd/6
22 0 0 0 0/0...```
Identifying CPU Utilization for Processes

You can identify the CPU utilization for running processes in the memory. The following is a sample output from the `show processes cpu` command. This output has been abbreviated to make the example more concise.

```
switch# show processes cpu
CPU utilization for five seconds: 0%/0%; one minute: 1%; five minutes: 2%

   PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
--- ------------------ ----- ----- ----- ----- --- ----------
  1  28660 405831 70 0.00% 0.00% 0.00% - init
  2    21  1185 18 0.00% 0.00% 0.00% - kthreadd
  3    468  36439 12 0.00% 0.00% 0.00% - migration/0
  4    79725 8804385 9 0.00% 0.00% 0.00% - ksoftirqd/0
  5       0    4  65 0.00% 0.00% 0.00% - watchdog/0
  6   472  35942 13 0.00% 0.00% 0.00% - migration/1
  7  33967  95376 35 0.00% 0.00% 0.00% - ksoftirqd/1
  8       0    11  3 0.00% 0.00% 0.00% - watchdog/1
  9   424  35558 11 0.00% 0.00% 0.00% - migration/2
 10  58084  763251  7 0.00% 0.00% 0.00% - ksoftirqd/2
 11       0     3  1 0.00% 0.00% 0.00% - watchdog/2
 12    381  29760 12 0.00% 0.00% 0.00% - migration/3
 13  17258  265864 64 0.00% 0.00% 0.00% - ksoftirqd/3
 14       0     2  0 0.00% 0.00% 0.00% - watchdog/3
 15  46558 1300598 35 0.00% 0.00% 0.00% - migration/4
 16 1332913 4354439 306 0.00% 0.00% 0.00% - ksoftirqd/4
 17       0     6  2 0.00% 0.00% 0.00% - watchdog/4
 18  45808 1283581 35 0.00% 0.00% 0.00% - migration/5
 19  981030 1973423 497 0.00% 0.00% 0.00% - ksoftirqd/5
 20       0    16  3 0.00% 0.00% 0.00% - watchdog/5
 21  48019 1334683 35 0.00% 0.00% 0.00% - migration/6
 22 1084448 2520990 430 0.00% 0.00% 0.00% - ksoftirqd/6
 23       0     3  3 0.00% 0.00% 0.00% - watchdog/6
 24  46490 1306203 35 0.00% 0.00% 0.00% - migration/7
 25 1187547 2867126 414 0.00% 0.00% 0.00% - ksoftirqd/7
 26       0    16  3 0.00% 0.00% 0.00% - watchdog/7
```
The `show processes cpu` command includes the following keywords:

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&gt;</code></td>
<td>Redirects the output to a file.</td>
</tr>
<tr>
<td><code>&gt;&gt;</code></td>
<td>Adds the output to an existing file.</td>
</tr>
<tr>
<td><code>history</code></td>
<td>Displays information about the CPU utility.</td>
</tr>
<tr>
<td><code>sort</code></td>
<td>Sorts the list based on the memory usage.</td>
</tr>
</tbody>
</table>

### Monitoring Process Core Files

You can monitor the process core files by using the `show cores` command.

```
switch# show cores
Module Instance Process-name PID Date(Year-Month-Day Time)
------ -------- --------------- -------- -------------------------
28 1 bgp-64551 5179 2013-11-08 23:51:26
```

The output shows all cores that are presently available for upload from the active supervisor.

### Processing the Crash Core Files

You can process the crash core files by using the `show processes log` command.

```
switch# show processes log
Process PID Normal-exit Stack-trace Core Log-create-time
------- ------ ----------- ----------- ------- ---------------
ntp 919 N N N Jun 27 04:08
snsm 972 N N Y N Jun 24 20:50
```

### Clearing the Core

You can clear the core by using the `clear cores` command.

```
switch# clear cores
```
Enabling Auto-Copy for Core Files

You can enter the `system cores` command to enable the automatic copy of core files to a TFTP server, the flash drive, or a file.

```
switch(config)# system cores tftp://10.1.1.1/cores
```
CHAPTER 16

Before Contacting Technical Support

This chapter contains the following sections:

- Steps to Perform Before Calling TAC, page 99
- Copying Files to or from Cisco NX-OS, page 101
- Using Core Dumps, page 102

Steps to Perform Before Calling TAC

At some point, you might need to contact your technical support representative or Cisco TAC for some additional assistance. This section outlines the steps that you should perform before you contact your next level of support in order to reduce the amount of time spent resolving the issue.

To prepare for contacting your customer support representative, follow these steps:

1. Collect the system information and configuration. You should collect this information before and after the issue has been resolved. Use one of the following three methods to gather this information:

   - Configure your Telnet or Secure Shell (SSH) application to log the screen output to a text file. Use the `terminal length 0` command and then use the `show tech-support details` command.
   - Use the `tac-pac filename` command to redirect the output of the `show tech-support details` command to a file, and then gzip the file.
     
     switch# tac-pac bootflash://showtech.switch1
   - If you do not specify a filename, Cisco NX-OS creates the file as volatile:show_tech_out.gz. Copy the file from the device using the procedure in Copying Files to or from Cisco NX-OS, on page 101.

2. If an error occurs in DCNM, take a screen shot of the error. In Windows, press Alt+PrintScreen to capture the active window, or press PrintScreen to capture the entire desktop. Paste the screenshot into a new Microsoft Paint (or similar program) session and save the file.

3. Capture the exact error codes that you see in the message logs from either DCNM or the CLI.

   - Choose Event Browser in DCNM to see the recent list of messages generated.
• Copy the error from the message log, which you can display by using either the `show logging logfile` or the `show logging last number` command to view the last lines of the log.

4 Answer the following questions before you contact your technical support representative:
   • On which device or port is the problem occurring?
   • Which Cisco NX-OS software, driver versions, operating systems versions, and storage device firmware are in your network?
   • What is the network topology? (In DCNM, choose Topology > Save layout.)
   • Were any changes made to the environment (VLANs, upgrades, or adding modules) prior to or at the time of this event?
   • Are there other similarly configured devices that could have this problem but do not?
   • Where was this problematic device connected (which device and interface)?
   • When did this problem first occur?
   • When did this problem last occur?
   • How often does this problem occur?
   • How many devices have this problem?
   • Were any traces or debug output captured during the problem time? What troubleshooting steps have you attempted? Which, if any, of the following tools were used?
     • Ethalyzer, local or remote SPAN
     • CLI debug commands
     • traceroute, ping
     • DCNM tools

5 Answer the following questions if your problem is related to a software upgrade attempt:
   • What was the original Cisco NX-OS version?
   • What is the new Cisco NX-OS version?
   • Collect the output from the following commands and forward them to your customer support representative:
     • `show install all status`
     • `show system internal log install`
     • `show system internal log install details`
     • `show log nvram`
Copying Files to or from Cisco NX-OS

You might need to move files to or from the device. These files may include the log, configuration, or firmware files.

Cisco NX-OS offers protocols to use for copying to or from the device. The device always acts as a client, so that an FTP, SCP, or TFTP session always originates from Cisco NX-OS and either pushes files to an external system or pulls files from an external system.

File Server: 172.22.36.10
File to be copied to the switch: /etc/hosts

The `copy` command supports the FTP, SCP, SFTP, and TFTP transfer protocols and many different sources for copying files.

```
switch# copy ?
bootflash: Select source filesystem
core: Select source filesystem
dev: Select source filesystem
ftp: Select source filesystem
http: Select source filesystem
licenses Backup license files
log: Select source filesystem
logflash: Select source filesystem
nvram: Select source filesystem
running-config Copy running configuration to destination
scp: Select source filesystem
sftp: Select source filesystem
startup-config Copy startup configuration to destination
system: Select source filesystem
tftp: Select source filesystem
usb1: Select source filesystem
usb2: Select source filesystem
volatile: Select source filesystem
```

You can use secure copy (SCP) as the transfer mechanism, as follows:

```
scp://[username@]server[/path]
```

This example copies /etc/hosts from 172.22.36.10 to hosts.txt, for user user1:

```
switch# copy scp://user1@172.22.36.10/etc/hosts bootflash:hosts.txt
user1@172.22.36.10's password:
hosts 100% |*****************************| 2035 00:00
```

This example backs up the startup configuration to an SFTP server:

```
switch# copy startup-config sftp://user1@172.22.36.10/test/startup-configuration.bak1
Connecting to 172.22.36.10...
User1@172.22.36.10's password:
switch#
```

Note

You should backup the startup configuration to a server on a daily basis and prior to any changes. You could write a short script to run on Cisco NX-OS to perform a save and then a backup of the configuration. The script needs to contain two commands: `copy running-configuration startup-configuration` and `copy startup-configuration tftp://server/name`. To execute the script, use the `run-script` filename command.
Using Core Dumps

Core dumps contain detailed information about the system and software status prior to a crash. Use core dumps in situations where unknown problems exist. You can send core dumps to a TFTP server or to a Flash card in slot0: of the local system. You should set up your system to generate core dumps under the instruction of your technical support representative. Core dumps are decoded by technical support engineers.

Set up core dumps to go to a TFTP server so that you can e-mail these core dumps directly to your technical support representative.

Use the `system cores` command to set up core dumps on your system as follows:

```bash
switch# system cores tftp://10.91.51.200/jsmith_cores
switch# show system cores
Cores are transferred to tftp://10.91.51.200/jsmith_cores
```

**Note**

The filename (indicated by `jsmith_cores`) must exist in the TFTP server directory.
Troubleshooting Tools and Methodology

This chapter contains the following sections:

- Command-Line Interface Troubleshooting Commands, page 103
- Configuration Files, page 105
- CLI Debug, page 105
- Ping and Traceroute, page 106
- Monitoring Processes and CPUs, page 108
- Using Onboard Failure Logging, page 110
- Using Diagnostics, page 111
- Using Embedded Event Manager, page 112
- Using Ethalyzer, page 112
- SNMP and RMON Support, page 114
- Using RADIUS, page 114
- Using syslog, page 115
- Using SPAN, page 116
- Using the Blue Beacon Feature, page 117
- Additional References for Troubleshooting Tools and Methodology, page 117

Command-Line Interface Troubleshooting Commands

The command-line interface (CLI) allows you to configure and monitor Cisco NX-OS using a local console or remotely using a Telnet or Secure Shell (SSH) session. The CLI provides a command structure similar to Cisco IOS software, with context-sensitive help, show commands, multiuser support, and roles-based access control.

Each feature has show commands that provide information about the feature configuration, status, and performance. Additionally, you can use the following command for more information:
• **show system**—Provides information about system-level components, including cores, errors, and exceptions. Use the **show system error-id** command to find details on error codes.

```
switch# copy running-config startup-config
2013 May 16 09:59:29 zoom %$ VDC-1 %$ %BOOTVAR-2-AUTOCOPY_FAILED: Autocopy of file /bootflash/n9000-dk9.6.1.2.I1.1.bin to standby
```

```
switch# show system error-id 0x401e0008
Error Facility: sysmgr
Error Description: request was aborted, standby disk may be full
```

## Consistency Checker Commands

Cisco NX-OS provides consistency checker commands to validate the software state with the hardware state. The result of the consistency checker is logged as either PASSED or FAILED.

2013 Nov 1 16:31:39 switch vshd: CC_LINK_STATE:
Consistency Check: PASSED

Cisco NX-OS supports the following consistency checker commands:

- **show consistency-checker l2 module module-number**—Verifies that learned MAC addresses are consistent between the software and the hardware. It also shows extra entries that are present in the hardware but not in the software and missing entries in the hardware.

- **show consistency-checker l3-interface module module-number**—Checks for Layer 3 settings of an interface in the hardware and for the following configuration in the hardware: L3 VLAN, CML Flags, IPv4 Enable, VPN ID. This command works for physical interfaces and interfaces that are part of a port channel. It does not validate subinterfaces.

- **show consistency-checker link-state module module-number**—Verifies the software link state of all the interfaces in the module against its hardware link state.

- **show consistency-checker membership port-channels [interface port-channel channel-number]**—Checks for port-channel membership in the hardware in all modules and validates it with the software state.

- **show consistency-checker membership vlan vlan-id**—Determines that the VLAN membership in the software is the same as programmed in the hardware. It also ignores the interfaces that are in the STP BLK state.

- **show consistency-checker acl [module module-number] [port-channels [interface port-channel channel-number]]**—Validates the IPv4 RAACL programming consistency between the hardware and software and verifies if <label, entry-location> pairs are consistent between the hardware and software. When invoked per module, this command verifies IPv4 ACL consistency for all the physical interfaces in that module.

When invoked on a specific port channel, this command verifies for all the member ports.

When invoked on all port channels, this command verifies for each port channel that has an ACL applied.

---

**Note**
Currently, this command does not verify IPv4 and IPv6 ACLs, does not verify on subinterfaces, and does not verify if qualifiers and actions are matching.
- `show consistency-checker stp-state vlan vlan-id`—Determines whether the spanning tree state in the software is the same as programmed in the hardware. This command is run only on interfaces that are operational (up).

**Configuration Files**

Configuration files contain the Cisco NX-OS commands used to configure the features on a Cisco NX-OS device. Cisco NX-OS has two types of configuration files: running configuration and startup configuration. The device uses the startup configuration (startup-config) during the device startup to configure the software features. The running configuration (running-config) contains the current changes that you make to the startup-configuration file. You should create a backup version of your configuration files before modifying that configuration. You can back up the configuration files to a remote server. See the configuration file information in the *Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide*. You can also create a checkpoint copy of the configuration file that you can roll back to if problems occur. See the rollback feature in the *Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*.

Cisco NX-OS features can create internal locks on the startup configuration file. In rare cases, these locks might not be removed by the features. Use the `show system internal symsmgr startup-config locks` command to determine if any locks remain on the startup configuration file. Use the `system startup-config unlock` command to remove these locks.

**CLI Debug**

Cisco NX-OS supports an extensive debugging feature set for actively troubleshooting a network. Using the CLI, you can enable debugging modes for each feature and view a real-time updated activity log of the control protocol exchanges. Each log entry has a time stamp and is listed chronologically. You can limit access to the debug feature through the CLI roles mechanism to partition access on a per-role basis. While the `debug` commands show real-time information, you can use the `show` commands to list historical and real-time information.

⚠️ **Caution**

Use the `debug` commands only under the guidance of your Cisco technical support representative because some `debug` commands can impact your network performance.

📝 **Note**

You can log debug messages to a special log file, which is more secure and easier to process than sending the debug output to the console.

By using the `?` option, you can see the options that are available for any feature. A log entry is created for each entered command in addition to the actual debug output. The debug output shows a time-stamped account of the activity that occurred between the local device and other adjacent devices.

You can use the debug facility to track events, internal messages, and protocol errors. However, you should be careful when using the debug utility in a production environment because some options might prevent access to the device by generating too many messages to the console or creating CPU-intensive events that could seriously affect network performance.
We recommend that you open a second Telnet or SSH session before you enter any `debug` commands. If the debug session overpowers the current output window, you can use the second session to enter the `undebug all` command to stop the debug message output.

### Debug Filters

You can filter out unwanted debug information by using the `debug-filter` command. The `debug-filter` command allows you to limit the debug information produced by related `debug` commands.

The following example limits EIGRP hello packet debug information to Ethernet interface 2/1:

```plaintext
switch# debug-filter ip eigrp interface ethernet 2/1
switch# debug eigrp packets hello
```

### Ping and Traceroute

Use the ping and traceroute features to troubleshoot problems with connectivity and path choices. Do not use these features to identify or resolve network performance issues.

The `ping` and `traceroute` commands are two of the most useful tools for troubleshooting TCP/IP networking problems. The ping utility generates a series of echo packets to a destination across a TCP/IP internetwork. When the echo packets arrive at the destination, they are rerouted and sent back to the source.

The traceroute utility operates in a similar fashion but can also determine the specific path that a frame takes to its destination on a hop-by-hop basis.

### Using Ping

Use the `ping` command to verify connectivity and latency to a particular destination across an IPv4 routed network.

Use the `ping6` command to verify connectivity and latency to a particular destination across an IPv6 routed network.

The ping utility allows you to send a short message to a port or end device. By specifying the IPv4 or IPv6 address, you can send a series of frames to a target destination. Once these frames reach the target, they are looped back to the source and a time stamp is taken.

We do not recommend using the Ping utility to test network performance with the IP address configured on the system.

```plaintext
switch# ping 172.28.230.1 vrf management
PING 172.28.230.1 (172.28.230.1): 56 data bytes
64 bytes from 172.28.230.1: icmp_seq=0 ttl=254 time=1.095 ms
```
Using Traceroute

Use traceroute to do the following:

- Trace the route followed by the data traffic.
- Compute the interswitch (hop-to-hop) latency.

The traceroute utility identifies the path taken on a hop-by-hop basis and includes a time stamp at each hop in both directions. You can use traceroute to test the connectivity of ports along the path between the generating device and the device closest to the destination.

Use the `traceroute {dest-ipv4-addr | hostname} [vrf vrf-name]` command for IPv4 networks and the `traceroute6 {dest-ipv6-addr | hostname} [vrf vrf-name]` command for IPv6 networks. If the destination cannot be reached, the path discovery traces the path up to the point of failure.

```
switch# traceroute 172.28.254.254 vrf management
traceroute to 172.28.254.254 (172.28.254.254), 30 hops max, 40 byte packets
  1  172.28.230.1 (172.28.230.1)    0.941 ms  0.676 ms  0.585 ms
  2  172.24.114.213 (172.24.114.213) 0.733 ms  0.70 ms  0.69 ms
  3  172.20.147.46 (172.20.147.46)   0.671 ms  0.628 ms  0.615 ms
  4  172.28.254.254 (172.28.254.254) 0.613 ms  0.628 ms  0.61 ms
```

Press Ctrl-C to terminate a running traceroute.

You can use the following commands to specify a source interface for the traceroute:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`traceroute {dest-ipv4-addr</td>
<td>hostname} [source {dest-ipv4-addr</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch# traceroute 112.112.112.1 source vlan 10</td>
<td></td>
</tr>
<tr>
<td>`traceroute6 {dest-ipv6-addr</td>
<td>hostname} [source {dest-ipv6-addr</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch# traceroute6 2010:11:22:0:1000::1 source ethernet 2/2</td>
<td></td>
</tr>
</tbody>
</table>
### Command

**Purpose**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>[no] ip traceroute source-interface interface [vrf vrf-name]</td>
<td>Generates traceroute or traceroute6 packets with the source IP address from the configured interface.</td>
</tr>
</tbody>
</table>

**Example:**

```
switch(config)# ip traceroute source-interface loopback 1
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip traceroute source-interface [vrf vrf-name]</td>
<td>Displays the configured source interface for the traceroute.</td>
</tr>
</tbody>
</table>

**Example:**

```
switch# show ip traceroute source-interface vrf all
VRF Name Interface
default loopback 1
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip icmp-errors source-interface interface</td>
<td>Generates ICMP error packets with the source IPv4 or IPv6 address from the configured interface.</td>
</tr>
</tbody>
</table>

**Example 1:**

```
switch(config)# ip icmp-errors source-interface loopback 1
```

**Example 2:**

```
switch(config)# vrf context vrf-blue
switch(config-vrf)# ip icmp-errors source-interface loopback 2
```

---

### Monitoring Processes and CPUs

Use the `show processes` command to identify the processes that are running and the status of each process.  
The command output includes the following:

- **PID** = process ID.
- **State** = process state.
- **PC** = current program counter in hexadecimal format.
- **Start_cnt** = how many times a process has been started (or restarted).
- **TTY** = terminal that controls the process. A - (hyphen) usually means a daemon not running on any particular TTY.
- **Process** = name of the process.

**Process states are as follows:**

- **D** = uninterruptible sleep (usually I/O).
- **R** = runnable (on run queue).
• S = sleeping.
• T = traced or stopped.
• Z = defunct (zombie) process.
• NR = not-running.
• ER = should be running but currently not-running.

Note: Typically, the ER state designates a process that has been restarted too many times, causing the system to classify it as faulty and disable it.

Typically, the ER state designates a process that has been restarted too many times, causing the system to classify it as faulty and disable it.

```
switch# show processes?
cpu    Show processes CPU Info
log    Show information about process logs
memory Show processes Memory Info
switch# show processes

<table>
<thead>
<tr>
<th>PID</th>
<th>State</th>
<th>PC</th>
<th>Start_cnt</th>
<th>TTY</th>
<th>Type</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>S</td>
<td>b7f9e468</td>
<td></td>
<td>1</td>
<td>-</td>
<td>init</td>
</tr>
<tr>
<td>2</td>
<td>S</td>
<td>0</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>migration/0</td>
</tr>
<tr>
<td>3</td>
<td>S</td>
<td>0</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>ksoftirqd/0</td>
</tr>
<tr>
<td>4</td>
<td>S</td>
<td>0</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>desched/0</td>
</tr>
<tr>
<td>5</td>
<td>S</td>
<td>0</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>migration/1</td>
</tr>
<tr>
<td>6</td>
<td>S</td>
<td>0</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>ksoftirqd/1</td>
</tr>
<tr>
<td>7</td>
<td>S</td>
<td>0</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>desched/1</td>
</tr>
<tr>
<td>8</td>
<td>S</td>
<td>0</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>events/0</td>
</tr>
<tr>
<td>9</td>
<td>S</td>
<td>0</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>events/1</td>
</tr>
<tr>
<td>10</td>
<td>S</td>
<td>0</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>khelper</td>
</tr>
<tr>
<td>15</td>
<td>S</td>
<td>0</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>kthread</td>
</tr>
<tr>
<td>24</td>
<td>S</td>
<td>0</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>kacpid</td>
</tr>
<tr>
<td>103</td>
<td>S</td>
<td>0</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>kblockd/0</td>
</tr>
<tr>
<td>104</td>
<td>S</td>
<td>0</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>kblockd/1</td>
</tr>
<tr>
<td>117</td>
<td>S</td>
<td>0</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>khubd</td>
</tr>
<tr>
<td>184</td>
<td>S</td>
<td>0</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>pdflush</td>
</tr>
<tr>
<td>185</td>
<td>S</td>
<td>0</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>pdflush</td>
</tr>
<tr>
<td>186</td>
<td>S</td>
<td>0</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>aio/0</td>
</tr>
<tr>
<td>188</td>
<td>S</td>
<td>0</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>aio/1</td>
</tr>
<tr>
<td>189</td>
<td>S</td>
<td>0</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>SerrLogKthread</td>
</tr>
</tbody>
</table>

...```

**Using the show processes cpu Command**

Use the `show processes cpu` command to display CPU utilization. The command output includes the following:

• Runtime(ms) = CPU time that the process has used, expressed in milliseconds.
• Invoked = Number of times that the process has been invoked.
• uSecs = Average CPU time, in microseconds, for each process invocation.
• 1Sec = Percentage of CPU utilization for the last 1 second.

```
switch# show processes cpu

<table>
<thead>
<tr>
<th>PID</th>
<th>Runtime (ms)</th>
<th>Invoked</th>
<th>uSecs</th>
<th>1Sec</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2264</td>
<td>108252</td>
<td>0</td>
<td>0</td>
<td>init</td>
</tr>
<tr>
<td>2</td>
<td>950</td>
<td>211341</td>
<td>4</td>
<td>0</td>
<td>migration/0</td>
</tr>
<tr>
<td>3</td>
<td>1154</td>
<td>32833341</td>
<td>0</td>
<td>0</td>
<td>ksoftirqd/0</td>
</tr>
<tr>
<td>4</td>
<td>609</td>
<td>419568</td>
<td>1</td>
<td>0</td>
<td>desched/0</td>
</tr>
</tbody>
</table>
```

Cisco Nexus 9000 Series NX-OS Troubleshooting Guide, Release 6.x
Using the show system resources Command

Use the `show system resources` command to display system-related CPU and memory statistics. The output includes the following:

- Load average is defined as the number of running processes. The average reflects the system load over the past 1, 5, and 15 minutes.
- Processes displays the number of processes in the system and how many are actually running when the command is issued.
- CPU states show the CPU usage percentage in user mode, kernel mode, and idle time in the last 1 second.
- Memory usage provides the total memory, used memory, free memory, memory used for buffers, and memory used for cache in kilobytes. Buffers and cache are also included in the used memory statistics.

```bash
switch# show system resources
Load average: 1 minute: 0.00 5 minutes: 0.02 15 minutes: 0.05
Processes : 355 total, 1 running
CPU states : 0.0% user, 0.2% kernel, 99.8% idle
    CPU0 states : 0.0% user, 1.0% kernel, 99.0% idle
    CPU1 states : 0.0% user, 0.0% kernel, 100.0% idle
    CPU2 states : 0.0% user, 0.0% kernel, 100.0% idle
    CPU3 states : 0.0% user, 0.0% kernel, 100.0% idle
Memory usage: 16402560K total, 2664308K used, 13738252K free
Current memory status: OK
```

Using Onboard Failure Logging

Cisco NX-OS provides the facility to log failure data to the persistent storage, which can be retrieved and displayed for analysis. This onboard failure logging (OBFL) feature stores failure and environmental information in nonvolatile memory on the module. This information will help you analyze failed modules.

The data stored by the OBFL facility includes the following:

- Time of initial power on
- Slot number of the module in the chassis
- Initial temperature of the module
- Firmware, BIOS, FPGA, and ASIC versions
Using Diagnostics

Generic online diagnostics (GOLD) define a common framework for diagnostic operations across Cisco platforms. The GOLD implementation checks the health of hardware components and verifies proper operation of the system data and control planes. Some tests take effect when the system is booting up; other tests take effect when the system is operational. A booting module goes through a series of checks before coming online to allow the system to detect faults in the hardware components at bootup and to ensure that a failing module is not introduced in a live network.

Defects are also diagnosed during system operation or runtime. You can configure a series of diagnostic checks to determine the condition of an online system. You must distinguish between disruptive and nondisruptive diagnostic tests. Although nondisruptive tests occur in the background and do not affect the system data or control planes, disruptive tests do affect live packet flows. You should schedule disruptive tests during special maintenance windows. The `show diagnostic content module` command output displays test attributes such as disruptive or nondisruptive tests.

You can configure runtime diagnostic checks to run at a specific time or to run continually in the background. Health-monitoring diagnostic tests are nondisruptive, and they run in the background while the system is in operation. The role of online diagnostic health monitoring is to proactively detect hardware failures in the live network environment and inform you of a failure.

GOLD collects diagnostic results and detailed statistics for all tests including the last execution time, the first and last test pass time, the first and last test failure time, the total run count, the total failure count, the consecutive failure count, and the error code. These test results help administrators determine the condition of a system and understand the reason for a system failure. Use the `show diagnostic result` command to view diagnostic results.

For more information about configuring GOLD, see the Cisco Nexus 9000 Series NX-OS System Management Configuration Guide.
Using Embedded Event Manager

Embedded Event Manager (EEM) is a policy-based framework that allows you to monitor key system events and then act on those events through a set policy. The policy is a preprogrammed script that you can load that defines actions that the device should invoke based on set events occurring. The script can generate actions, including, but not limited to, generating custom syslog or SNMP traps, invoking CLI commands, forcing a failover, and much more.

For more information about configuring EEM, see the Cisco Nexus 9000 Series NX-OS System Management Configuration Guide.

Using Ethanalyzer

Ethanalyzer is a Cisco NX-OS protocol analyzer tool based on the Wireshark (formerly Ethereal) open source code. Ethanalyzer is a command-line version of Wireshark that captures and decodes packets. You can use Ethanalyzer to troubleshoot your network and analyze the control-plane traffic.

To configure Ethanalyzer, use the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethanalyzer local interface</td>
<td>Captures packets sent or received by the supervisor and provides detailed protocol information.</td>
</tr>
<tr>
<td>ethanalyzer local interface inband</td>
<td>Captures packets sent or received by the supervisor and provides detailed protocol information in the inband and outband interfaces.</td>
</tr>
<tr>
<td>ethanalyzer local interface mgmt</td>
<td>Captures packets sent or received by the supervisor and provides detailed protocol information in the management interfaces.</td>
</tr>
<tr>
<td>ethanalyzer local interface {inband</td>
<td>mgmt}</td>
</tr>
<tr>
<td>ethanalyzer local interface {inband</td>
<td>mgmt} limit-captured-frames</td>
</tr>
<tr>
<td>ethanalyzer local interface {inband</td>
<td>mgmt} limit-frame-size</td>
</tr>
<tr>
<td>ethanalyzer local interface {inband</td>
<td>mgmt} capture-filter</td>
</tr>
<tr>
<td>ethanalyzer local interface {inband</td>
<td>mgmt} display-filter</td>
</tr>
<tr>
<td>ethanalyzer local interface {inband</td>
<td>mgmt} write</td>
</tr>
<tr>
<td>ethanalyzer local read</td>
<td>Opens the captured data file and analyzes it.</td>
</tr>
</tbody>
</table>

Ethanalyzer does not capture data traffic that Cisco NX-OS forwards in the hardware.
Ethanalyzer uses the same capture filter syntax as `tcpdump` and uses the Wireshark display filter syntax.

This example shows captured data (limited to four packets) on the management interface:

```
switch(config)# ethanalyzer local interface mgmt limit-captured-frames 4
Capturing on eth1
Win=64475 Len=0
2013-05-18 13:21:21.850463 00:13:5f:1c:ee:80 -> ab:00:00:02:00:00 0x6002 DEC DN
```

Remote Console
4 packets captured

This example shows detailed captured data for one HSRP packet:

```
switch(config)# ethanalyzer local interface mgmt capture-filter "udp port 1985"
limit-captured-frames 1
Capturing on eth1
Frame 1 (62 bytes on wire, 62 bytes captured)
Arrival Time: May 18, 2013 13:29:19.961280000
[Time delta from previous captured frame: 1203341359.961280000 seconds]
[Time delta from previous displayed frame: 1203341359.961280000 seconds]
[Time since reference or first frame: 1203341359.961280000 seconds]
Frame Number: 1
Frame Length: 62 bytes
Capture Length: 62 bytes
[Frame is marked: False]
```

```
Ethernet II, Src: 00:00:0c:07:ac:01 (00:00:0c:07:ac:01), Dst: 01:00:5e:00:00:02 (01:00:5e:00:00:02)
Destination: 01:00:5e:00:00:02 (01:00:5e:00:00:02)
Address: 01:00:5e:00:00:02 (01:00:5e:00:00:02)
.... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
.... ...0 .... .... .... .... = LG bit: Globally unique address (factory default)
Source: 00:00:0c:07:ac:01 (00:00:0c:07:ac:01)
Address: 00:00:0c:07:ac:01 (00:00:0c:07:ac:01)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
.... ...0 .... .... .... .... = LG bit: Globally unique address (factory default)
```

```
Type: IP (0x0800)
Internet Protocol, Src: 172.28.230.3 (172.28.230.3), Dst: 224.0.0.2 (224.0.0.2)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x0 (DSCP 0x0: Class Selector 6; ECN: 0x0)
1100 00.. = Differentiated Services Codepoint: Class Selector 6 (0x0)
.... ...0 = ECN-Capable Transport (ECT): 0
.... ...0 = ECN-CE: 0
```

```
Total Length: 48
Identification: 0x0000 (0)
Flags: 0x00
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 1
Protocol: UDP (0x11)
Header checksum: 0x46db [correct]
[Good: True]
[Bad : False]
```

```
Source: 172.28.230.3 (172.28.230.3)
Destination: 224.0.0.2 (224.0.0.2)
Source port: 1985 (1985)
```
SNMP and RMON Support

Cisco NX-OS provides extensive SNMPv1, v2, and v3 support, including Management Information Bases (MIBs) and notifications (traps and informs).

The SNMP standard allows any third-party applications that support the different MIBs to manage and monitor Cisco NX-OS.

SNMPv3 provides extended security. Each device can be selectively enabled or disabled for SNMP service. In addition, each device can be configured with a method of handling SNMPv1 and v2 requests.

Cisco NX-OS also supports Remote Monitoring (RMON) alarms and events. RMON alarms and events provide a mechanism for setting thresholds and sending notifications based on changes in network behavior.

The *Alarm Group* allows you to set alarms. Alarms can be set on one or multiple parameters within a device. For example, you can set an RMON alarm for a specific level of CPU utilization on a device. The *Event Group* allows you to configure events that are actions to be taken based on an alarm condition. The types of events that are supported include logging, SNMP traps, and log-and-trap.

For more information about configuring SNMP and RMON, see the *Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*.

Using RADIUS

The RADIUS protocol is used to exchange attributes or credentials between a head-end RADIUS server and a client device. These attributes relate to three classes of services:

- Authentication
- Authorization
• Accounting

Authentication refers to the authentication of users for access to a specific device. You can use RADIUS to manage user accounts for access to a Cisco NX-OS device. When you try to log into a device, Cisco NX-OS validates you with information from a central RADIUS server.

Authorization refers to the scope of access that you have once you have been authenticated. Assigned roles for users can be stored in a RADIUS server with a list of actual devices that the user should have access to. Once the user has been authenticated, the device can then refer to the RADIUS server to determine the access that the user will have.

Accounting refers to the log information that is kept for each management session in a device. You can use this information to generate reports for troubleshooting purposes and user accountability. You can implement accounting locally or remotely (using RADIUS).

This example shows how to display accounting log entries:

```
switch# show accounting log
Sun May 12 04:02:27 2007:start:/dev/pts/0_1039924947:admin
Sun May 12 04:02:28 2007:stop:/dev/pts/0_1039924947:admin:vsh exited normally
Sun May 12 04:02:33 2007:start:/dev/pts/0_1039924953:admin
Sun May 12 04:02:34 2007:stop:/dev/pts/0_1039924953:admin:vsh exited normally
Sun May 12 05:02:08 2007:start:snmp_1039928528_172.22.95.167:public
Sun May 12 05:02:08 2007:update:snmp_1039928528_172.22.95.167:public:Switchname
```

Note: The accounting log shows only the beginning and end (start and stop) for each session.

---

### Using syslog

The system message logging software saves messages in a log file or directs the messages to other devices. This feature provides the following capabilities:

- Logging information for monitoring and troubleshooting
- Selection of the types of logging information to be captured
- Selection of the destination of the captured logging information

You can use syslog to store a chronological log of system messages locally or to send this information to a central syslog server. The syslog messages can also be sent to the console for immediate use. These messages can vary in detail depending on the configuration that you choose.

The syslog messages are categorized into seven severity levels from debug to critical events. You can limit the severity levels that are reported for specific services within the device. For example, you might want to report debug events only for the OSPF service but record all severity level events for the BGP service.

Log messages are not saved across system reboots. However, a maximum of 100 log messages with a severity level of critical and below (levels 0, 1, and 2) are saved in NVRAM. You can view this log at any time with the `show logging nvram` command.
Logging Levels

Cisco NX-OS supports the following logging levels:

- 0-emergency
- 1-alert
- 2-critical
- 3-error
- 4-warning
- 5-notification
- 6-informational
- 7-debugging

By default, the device logs normal but significant system messages to a log file and sends these messages to the system console. Users can specify which system messages should be saved based on the type of facility and the severity level. Messages have a time stamp to enhance real-time debugging and management.

Enabling Logging for Telnet or SSH

System logging messages are sent to the console based on the default or configured logging facility and severity values.

- To disable console logging, use the `no logging console` command in configuration mode.
- To enable logging for Telnet or SSH, use the `terminal monitor` command in EXEC mode.
- When logging to a console session is disabled or enabled, that state is applied to all future console sessions. If a user exits and logs in again to a new session, the state is preserved. However, when logging to a Telnet or SSH session is enabled or disabled, that state is applied only to that session. The state is not preserved after the user exits the session.

The `no logging console` command disables console logging and is enabled by default.

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

The `terminal monitor` command enables logging for Telnet or SSH and is disabled by default.

```
switch# terminal monitor
```

For more information about configuring syslog, see the *Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*.

Using SPAN

You can use the Switched Port Analyzer (SPAN) utility to perform detailed troubleshooting or to take a sample of traffic from a particular application host for proactive monitoring and analysis.
When you have a problem in your network that you cannot solve by fixing the device configuration, you typically need to take a look at the protocol level. You can use `debug` commands to look at the control traffic between an end node and a device. However, when you need to focus on all the traffic that originates from or is destined to a particular end node, you can use a protocol analyzer to capture protocol traces.

To use a protocol analyzer, you must insert the analyzer inline with the device under analysis, which disrupts input and output (I/O) to and from the device.

In Ethernet networks, you can solve this problem by using the SPAN utility. SPAN allows you to take a copy of all traffic and direct it to another port within the device. The process is nondisruptive to any connected devices and is facilitated in the hardware, which prevents any unnecessary CPU load.

SPAN allows you to create independent SPAN sessions within the device. You can apply a filter to capture only the traffic received or the traffic transmitted.

For more information about configuring SPAN, see the *Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*.

### Using the Blue Beacon Feature

On some platforms, you can cause the platform LEDs to blink. This feature is a useful way to mark a piece of hardware so that a local administrator can quickly identify the hardware for troubleshooting or replacement.

To flash the LEDs on a hardware entity, use the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>blink chassis</code></td>
<td>Flashes the chassis LED.</td>
</tr>
<tr>
<td><code>blink fan number</code></td>
<td>Flashes one of the fan LEDs.</td>
</tr>
<tr>
<td><code>blink module slot</code></td>
<td>Flashes the selected module LED.</td>
</tr>
<tr>
<td><code>blink powersupply number</code></td>
<td>Flashes one of the power supply LEDs.</td>
</tr>
</tbody>
</table>

### Additional References for Troubleshooting Tools and Methodology

#### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>System management tools</td>
<td><em>Cisco Nexus 9000 Series NX-OS System Management Configuration Guide</em></td>
</tr>
<tr>
<td>MIBs</td>
<td><em>Cisco Nexus 7000 Series and 9000 Series NX-OS MIB Quick Reference</em></td>
</tr>
</tbody>
</table>
INDEX

B
blue beacon feature 117
troubleshooting 117

calling TAC 99
troubleshooting steps 99
cli debug 105
troubleshooting 105
configuration files 105
troubleshooting 105
convergence time 60
troubleshooting 60
copying files 101
troubleshooting 101
core dumps 102
troubleshooting 102
corrupted bootflash recovery 14
troubleshooting 14
customer support 9
troubleshooting 9

d
debug filters 106
troubleshooting 106
dedicated port, configuring 41
troubleshooting 41
diagnostics 111
troubleshooting 111
dropped packets 80
troubleshooting 80

e
Embedded Event Manager 112
troubleshooting 112
errdisable state 43
cli troubleshooting 43
ErrDisabled state 43	port troubleshooting 43
ethanalyzer 112
troubleshooting 112

i
initial routing checklist 63
troubleshooting 63
initial troubleshooting checklist 38
ports 38
interface configuration disappeared 40
troubleshooting 40
interface enabling 40
troubleshooting 40
iSTP 55
troubleshooting checklist 55

k
kernel 72
memory troubleshooting 72

l
Layer 2 connectivity 4
Layer 3 connectivity 5
troubleshooting 5
license 34, 36
displaying information 34
missing 36
transfer between systems 36
Index

licensing 33, 34, 35
  guidelines and limitations 33
  serial number issues 35
  troubleshooting 33
  troubleshooting checklist 34
loader> prompt 16
  recovery 16
logging for SSH, enabling 116
  troubleshooting 116
logging for Telnet, enabling 116
  troubleshooting 116
logging levels 116
  troubleshooting 116
logs 8
  troubleshooting 8

M
memory alerts 77
  troubleshooting 77
memory thresholds 77
  troubleshooting 77
memory, troubleshooting 69
modules 8
  troubleshooting 8

N
network forwarding loops 61
  troubleshooting 61
nvram logs 8
  troubleshooting 8

O
onboard failure logging 110
  troubleshooting 110

P
packet flooding 59
  troubleshooting 59
packet flow 79
  issue troubleshooting 79
page cache 72
  memory troubleshooting 72
ping 106
  troubleshooting 106
ping use 106
  troubleshooting 106
platform memory 76
  monitoring 76
platform memory utilization 70
  detailed assessment 70
  high level assessment 70
port information 38
  troubleshooting 38
port link failure 41
  troubleshooting 41
port statistics, cli 39
  troubleshooting 39
ports, troubleshooting 37
power-on 14
  switch reboot hangs 14
  troubleshooting 14
process memory use 74, 75
  troubleshooting 74, 75
processes and cpu, monitoring 108
  troubleshooting 108
pvlan, creating 53
  troubleshooting 53

R
radius 114
  troubleshooting 114
reboots 11
  troubleshooting 11
RMA chassis errors 36
RMON 114
  troubleshooting 114
routing 63, 64
  troubleshooting 63, 64

S
show processes cpu command 109
  troubleshooting 109
show system resources command 110
  troubleshooting 110
SNMP support 114
  troubleshooting 114
software image 3
  description 3
software upgrade 13
  troubleshooting 13
software upgrade error 13
  troubleshooting 13
SPAN 116
  troubleshooting 116
standby supervisor 24
  boot fail 24
STP data loops 56
  troubleshooting 56
STP, troubleshooting 55
  symptoms 5
  troubleshooting 5
syslog 115
  troubleshooting 115
system messages 6
  troubleshooting 6
system restarts 18, 23
  troubleshooting 18
  unrecoverable 23
  system restarts, recovering 18

U
  upgrades 11
    troubleshooting 11
user processes 73
    memory troubleshooting 73

V
  VLAN guidelines 51
    troubleshooting 51
  vlan interface 53
    troubleshooting 53
  VLAN, creating 52
    troubleshooting 52
  VLANs 51
    troubleshooting 51
  vPC blocking state 48
    troubleshooting 48
  vPC checklist 45
    troubleshooting 45
  vPC feature 48
    troubleshooting 48
  vPC information 45
    troubleshooting 45
  vPC moved to suspend state
    VLAN troubleshooting 48
  vPCs, verifying 46
    troubleshooting 46

T
  traceroute 106
    troubleshooting 106
  traceroute use 107
    troubleshooting 107
  troubleshooting process 3
  type 1 element mismatch 47
    troubleshooting 47

Cisco Nexus 9000 Series NX-OS Troubleshooting Guide, Release 6.x