This article introduces the basic concepts, methodology, and general troubleshooting guidelines for problems that may occur when configuring and using Cisco NX-OS.

Guide Contents
Troubleshooting Overview (this section)
Troubleshooting Installs, Upgrades, and Reboots
Troubleshooting Licensing
Troubleshooting VDCs
Troubleshooting CFS
Troubleshooting Ports
Troubleshooting vPCs
Troubleshooting VLANs
Troubleshooting STP
Troubleshooting Routing
Troubleshooting Unicast Traffic
Troubleshooting WCCP
Troubleshooting Memory
Troubleshooting Packet Flow Issues
Troubleshooting FCoE
Before Contacting Technical Support
Troubleshooting Tools and Methodology

Contents

Overview of the Troubleshooting Process

To troubleshoot your network, follow these general steps:

1. Maintain a consistent Cisco NX-OS release across all your devices.
2. See the Cisco NX-OS release notes for your Cisco NX-OS release for the latest features, limitations,

and caveats.
3. Enable system message logging. See System Messages.
4. Troubleshoot any new configuration changes after implementing the change.
5. Gather information that defines the specific symptoms. See Gathering Information.
6. Verify the physical connectivity between your device and end devices. See Verifying Ports.
7. Verify the Layer 2 connectivity. See Verifying Layer 2 Connectivity.
8. Verify the end-to-end connectivity and the routing configuration. See Verifying Layer 3 Connectivity.
9. After you have determined that your troubleshooting attempts have not resolved the problem, contact Cisco TAC or your technical support representative.

Note: View the Cisco Nexus 7000 instructional videos for an overview of Cisco NX-OS.

Gathering Information

This section describes the tools that are commonly used to troubleshoot problems within your network. Specific troubleshooting articles may include additional tools and commands specific to the symptoms and possible problems covered in that article.

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 in the correct VDC?

  Use the **show vdc membership** command to check which VDC that the interface is a member of. You must log into the device with the network-admin role to use this command.

- Is the interface operational?

  Use the **show interface brief** command. The status should be up.

See Troubleshooting Ports 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 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 no essential Layer 2 processes are in the error state.
- 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 is occurring at each node.

See Troubleshooting VLANs and Troubleshooting STP for more information on troubleshooting Layer 2 issues.

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 arp**
- **show ip routing**
- **show platform forwarding**

See Ping and Traceroute to verify Layer 3 connectivity. See Troubleshooting Routing for more information on troubleshooting Layer 3 issues.

Overview of Symptoms

This article 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 and RSPAN or Ethanalyzer 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

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.

Use this string to find the matching system message in the NX-OS System Messages Reference or in the Error Message Decoder. Each system message is followed by an explanation and recommended action. The action may be as simple as "No action is required." It may involve a fix or a recommendation to contact technical support as shown in the following example:

> **Error Message** 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 Cisco NX-OS 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 Cisco NX-OS device is not accessible.

This example shows how to configure a Cisco NX-OS 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.

Note: 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. switch1# **config terminal**
2. switch1(config)# **logging server 192.0.2.1 6 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

```
root 23508 1 0 11:01:41 ? 0:00 /usr/sbin/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 switch is listed in brackets.

tail -f /var/adm/MDS_logs

```
Sep 17 11:07:41 [172.22.36.142.2.2] : 2004 Sep 17 11:17:29 pacific: PORT-5-IF_DOWN_INITIALIZING: %

Sep 17 11:07:49 [172.22.36.142.2.2] : 2004 Sep 17 11:17:36 pacific: %PORT-5-IF_UP: %$VLAN 1%$ Inte

Sep 17 11:07:51 [172.22.36.142.2.2] : 2004 Sep 17 11:17:39 pacific: %VSHD-5-VSHD_SYSLOG_CONFIG_I:
```

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 may have led up to the current problem 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
pending       server address pending configuration
pending-diff  server address pending configuration diff
server        Show server logging configuration
session       Show logging session status
status        Show logging status
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**

```
2008 Sep 10 15:51:58 switch %$ VDC-1 %$ %SYSMGR-2-NON_VOLATILE_DB_FULL: System n
on-volatile storage usage is unexpectedly high at 99%.
2008 Sep 10 15:52:13 switch %$ VDC-1 %$ %PLATFORM-2-PFM_SYSTEM_RESET: Manual sys
tem restart from Command Line Interface
2008 Sep 10 15:57:49 switch %$ VDC-1 %$ %KERN-2-SYSTEM_MSG: Starting kernel... -
 kernel
2008 Sep 10 15:58:00 switch %$ VDC-1 %$ %CARDCLIENT-2-REG: Sent
2008 Sep 10 15:58:01 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG: R2D2: P1 SUP NO GMTL
 FOR P1 SUP  - r2d2
2008 Sep 10 15:58:01 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG: R2D2: P1 SUP NO GMTL
 FOR P1 SUP  - r2d2
2008 Sep 10 15:58:05 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG: R2D2: P1 SUP: Reset
Tx/Rx during QOS INIT  - r2d2
2008 Sep 10 15:58:16 switch %$ VDC-1 %$ %USER-2-SYSTEM_MSG: can't dlsym ssnmgr_i
s_session_command: please link this binary with ssnmgr.so! - svi
2008 Sep 10 15:58:16 switch %$ VDC-1 %$ %CARDCLIENT-2-SSE: LC_READY sent
2008 Sep 10 15:58:17 switch %$ VDC-1 %$ snmpd: load_mib_module :Error, while loa
ding the mib module /isan/lib/libpmsnmp_common.so (/isan/lib/libpmsnmp_common.so
: undefined symbol: sme_mib_get_if_info)
2008 Sep 10 15:58:17 switch %$ VDC-1 %$ %CARDCLIENT-2-SSE: MOD:6 SUP ONLINE
2008 Sep 10 15:58:17 switch %$ VDC-1 %$ %VDC_MGR-2-VDC_LIC_WARN: Service using g
race period will be shutdown in 9 day(s)
```

Contacting Customer Support

If you are unable to solve a problem after using the troubleshooting suggestions in these articles, 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 switch

- 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.

See Also

Before Contacting Technical Support

Further Reading

The following links contain further information on this topic from Cisco.com:

Cisco NX-OS System Messages Reference

External Links

External links contain content developed by external authors. Cisco does not review this content for accuracy.

Nexus: Hands on with NX-OS, Part#1