Overview

This chapter introduces the basic concepts, methodology, and general troubleshooting guidelines for problems that might occur when configuring and using Cisco Nexus 1000V. This chapter contains the following sections:

Troubleshooting Process

To troubleshoot your network, follow these steps:

Procedure

Step 1 Gather information that defines the specific symptoms.

Step 2 Identify all potential problems that could be causing the symptoms.

Step 3 Systematically eliminate each potential problem (from most likely to least likely) until the symptoms disappear.

Step 4 If the problem still persists, get technical support. For more information, see Cisco Support Information and Gathering Information for Technical Support.

Best Practices

We recommend that you do the following to ensure the proper operation of your networks:

- Maintain a consistent Cisco Nexus 1000V release across all network devices.
- Refer to the release notes for your Cisco Nexus 1000V release for the latest features, limitations, and caveats.
- Enable system message logging. See Overview of Symptoms, on page 2.
- Verify and troubleshoot any new configuration changes after implementing the change.

Troubleshooting Basics

This section introduces questions to ask when troubleshooting a problem with the Cisco Nexus 1000V or connected devices. Use the answers to these questions to identify the scope of the problem and to plan a course of action.

Overview of Symptoms

The symptom-based troubleshooting approach provides multiple ways to diagnose and resolve problems. By using multiple entry points with links to solutions, this guide best serves users who may have identical problems that are perceived by different indicators.

Using a given a set of observable symptoms on a network, it is important to 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. These problems and corrective actions include the following:

- Identify key Cisco Nexus 1000V troubleshooting tools.
- Obtain and analyze protocol traces using SPAN 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.
- Obtain core dumps and other diagnostic data for use by the Technical Assistance Center (TAC).
- Recover from switch upgrade failures.

Troubleshooting Guidelines

By answering the following questions, you can determine the paths that you need to follow and the components that you should investigate further.

Answer the following questions to determine the status of your installation:

- Is this a newly installed system or an existing installation? It could be a new host, switch, or VLAN.
- Has the host ever been able to see the network?
- Are you trying to solve an existing application problem (too slow, high latency, excessively long response time) or did the problem show up recently?
- What was changed in the configuration or in the overall infrastructure immediately before the applications started to have problems?

Discovering a Network Problem

To discover a network problem, follow these steps:

Procedure

Step 1 Gather information about problems in your system. See Gathering Information, on page 3.

Step 2 Verify the Layer 2 connectivity. See Verifying Layer 2 Connectivity, on page 4.

Step 3 Verify the configuration for your end devices (storage subsystems and servers).

Step 4 Verify the end-to-end connectivity. See Verifying Layer 3 Connectivity, on page 4.

Gathering Information

This section highlights the tools that are commonly used to troubleshoot problems within your network. These tools are a subset of what you might use to troubleshoot your specific problem. Each chapter in this guide includes additional tools and commands that are specific to the symptoms and possible problems covered in that chapter. You should also have an accurate topology of your network to help isolate problem areas.

Use the following commands and examine the outputs:

- **show module**
- **show version**
- **show running-config**
- **show logging log**
- **show interfaces brief**
- **show vlan**
- **show accounting log**
- **show tech support svs**

Note To use commands with the **internal** keyword, you must log in with the network-admin role.

Verifying Ports

Answer the following questions to verify ports:

- Are you using the correct media copper or optical fiber type?
- Is the media broken or damaged?
- Are you checking a virtual Ethernet port? If yes, use the **show interface brief** command. The status should be up.
- Are you checking a physical Ethernet port? If yes, check the port by looking at the server or by looking at an upstream switch.

- Are the network adapters of the Virtual Supervisor Module (VSM) virtual machine (VM) assigned the right port groups? Are all of them connected from vSphere Client?

Verifying Layer 2 Connectivity

To verify Layer 2 connectivity, do the following:

1. Answer the following questions:
   - Are the necessary interfaces in the same VLANs?
   - Are all ports in the port channel configured for the same speed, duplex, and trunk mode?
2. Use the following commands:
   - Use the **show vlan brief** command to check the status. The status should be up.
   - Use the **show port-profile** command to check a port profile configuration.
   - Use the **show interface-brief** command to check the status of a virtual Ethernet port or a physical Ethernet port.

Verifying Layer 3 Connectivity

To verify Layer 3 connectivity, do the following:

1. Answer the following questions:
   - Have you configured a gateway of last resort?
   - Are any IP access lists, filters, or route maps blocking route updates?
2. Use the following commands:
   - Ping
   - Traceroute

System Messages

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

```
2009 Apr 29 12:35:51 switch
%KERN-1-SYSTEM_MSG: stun_set_domain_id : Setting domain ID (1024) -
kernel
```

Use this string to find the matching system message in the *Cisco Nexus 1000V Series and Cisco VSG NX-OS System Messages Reference Guide for VMware vSphere*.

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

```
Error Message 2009 Apr 29 14:57:23 switch
%MODULE-5-MOD_OK: Module 3 is online (serial:)

Explanation VEM module inserted successfully on slot 3
Use the show module command to verify the module in
slot 3.
```

syslog Server Implementation

The syslog facility allows the Cisco Nexus 1000V to send a copy of the message log to a host for more permanent storage. This feature can be useful if the logs need to be examined over a long period of time or when the Cisco Nexus 1000V is not accessible.

This section demonstrates how to configure a Cisco Nexus 1000V 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 concept of a facility to determine how it should be handled on the syslog server (the Solaris system in this example), and the message severity. Therefore, different message severities can be handled differently by the syslog server. They could be logged to different files or emailed to a particular user. Specifying a severity determines that all messages of that level and greater severity (lower number) will be acted upon.

Note The Cisco Nexus 1000V messages should be logged to a different file from the standard syslog file so that they cannot be confused with other non-Cisco syslog messages. The logfile should not be located on the / file system, to prevent log messages from filling up the / file system.

```
Syslog Client: switch1
Syslog Server: 172.22.36.211 (Solaris)
Syslog facility: local1
Syslog severity: notifications (level 5, the default)
File to log Cisco Nexus 1000V messages to: /var/adm/nxos_logs
```

Configuring a syslog Server

To configure a syslog server, follow these steps:

Procedure

Step 1 Configure the Cisco Nexus 1000V.

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch (config)# logging server 192.0.2.1 6 facility local1
```

Step 2 Display the configuration.

```
switch# show logging server
Logging server: enabled
{192.0.2.1}
server severity: notifications
server facility: local1
```

Step 3 Configure the syslog server.

a) Modify `/etc/syslog.conf` to handle local1 messages. For Solaris, at least one tab needs to be between the facility severity and the action (`/var/adm/nxos_logs`).

```
#Below is for the NX-OS logging
local1.notice /var/adm/nxos_logs
```

b) Create the log file.

```
#touch /var/adm/nxos_logs
```

c) Restart the syslog.

```
# /etc/init.d/syslog stop
# /etc/init.d/syslog start
syslog service starting.
```

d) Verify that the syslog has started.

```
# ps -ef |grep syslogd
root 23508 1 0 11:01:41 ? 0:00 /usr/sbin/syslogd
```

Step 4 Test the syslog server by creating an event in the Cisco Nexus 1000V. In this case, port e1/2 was bounced and the following was listed on the syslog server. Notice that the IP address of the switch is listed in brackets.

```
# tail -f /var/adm/nxos_logs
Sep 17 11:07:41 [172.22.36.142.2.2] : 2004 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] : 2004 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] : 2004 Sep 17 11:17:39 pacific:
%VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from pts/0
(dhcp-171-71-49-125.cisco.com)
```

Troubleshooting with Logs

Cisco Nexus 1000V generates many types of system messages on the switch and sends them to a syslog server. These messages can be viewed to determine the events that might have led up to the current problem condition that you are facing.

Viewing Logs

Use the following commands to access and view logs in Cisco Nexus 1000V.

```
switch# show logging ?

console Show console logging configuration
info Show logging configuration
internal syslog syslog internal information
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
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
| Pipe command output to filter
```

```
switch# show logging server
Logging server: enabled
{192.0.1.1}
server severity: critical
server facility: user
```