



Overview

This chapter introduces the basic concepts, methodology, and general troubleshooting guidelines for problems that might occur when configuring and using the Cisco VSG.

This chapter includes the following sections:

- [Overview of the Troubleshooting Process, page 1-1](#)
- [Overview of Best Practices, page 1-1](#)
- [Troubleshooting Basics, page 1-2](#)
- [Overview of Symptoms, page 1-3](#)
- [System Messages, page 1-3](#)
- [Troubleshooting with Logs, page 1-5](#)
- [Troubleshooting Fragmentation/Jumbo Issues, page 1-6](#)
- [Contacting Cisco Customer Support, page 1-7](#)

Overview of the Troubleshooting Process

To troubleshoot your network, follow these steps:

-
- | | |
|---------------|---|
| Step 1 | Gather information that defines the specific symptoms. |
| Step 2 | Identify all potential problems that could be causing the symptoms. |
| Step 3 | Eliminate each potential problem (from most likely to least likely) until the symptoms disappear. |
-

Overview of Best Practices

Best practices are the recommended steps you should take to ensure the proper operation of your network. We recommend the following general best practices for most networks:

- Maintain a consistent Cisco VSG release across all network devices.
- Refer to the release notes for your Cisco VSG release for the latest features, limitations, and caveats.
- Enable system message logging. See the [“Overview of Symptoms” section on page 1-3](#).

- Verify and troubleshoot any new configuration changes after implementing the change.

Troubleshooting Basics

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

This section includes the following topics:

- [Troubleshooting Guidelines, page 1-2](#)
- [Gathering Information, page 1-2](#)

Troubleshooting Guidelines

By answering the questions in the following sections, you can determine the paths you must 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, too high latency, excessively long response time) or did the problem show up recently?
- What changed in the configuration or in the overall infrastructure immediately before the applications started to have problems?

To discover a network problem, follow these steps:

-
- Step 1** Gather information on problems in your system. See the [“Gathering Information” section on page 1-2](#).
 - Step 2** Verify the Layer 2 connectivity. See the [“Overview of Symptoms” section on page 1-3](#).
 - Step 3** Verify the configuration for your end devices (storage subsystems and servers).
 - Step 4** Verify end-to-end connectivity. See the [“Overview of Symptoms” section on page 1-3](#).
-

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 may use to troubleshoot your specific problem.

Each chapter in this guide may include additional tools and commands 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.

Enter the following commands and examine the outputs:

- `show vsg`
- `show version`

- **show running-config**
- **show logging log**
- **show interfaces brief**
- **show interface data 0**
- **show accounting log**
- **show tech support**
- **show vnm-pa status**
- **show ac-driver statistics**

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 serves users who might have identical problems that are perceived by different indicators. You can search this guide in PDF form, use the index, or rely on the symptoms and diagnostics listed in each chapter as entry points to access necessary information.

Using a given a set of observable symptoms on a network, you can 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 VSG troubleshooting tools.
- Obtain and analyze protocol traces using Switched Port Analyzer (SPAN) or Ethalyzer on the command line interface (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 Cisco Technical Assistance Center (TAC).
- Recover from switch upgrade failures.

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.

This section includes the following topics:

- [System Message Text, page 1-4](#)
- [Syslog Server Implementation, page 1-4](#)

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 vsg %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 NX-OS System Messages Reference*.

Each system message has an explanation and recommended action. The action might be as simple as no action required or it might involve a fix or a recommendation to contact technical support as shown in the following example:

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

Explanation VEM module inserted successfully on slot 3.

Recommended Action None. This is an information message. Use the **show module** command to verify the module in slot 3.

Syslog Server Implementation

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

The example provided in this section shows how to configure a Cisco VSG device to use the syslog facility on a Solaris platform. Although a Solaris host is being used, syslog configuration on all UNIX and Linux systems is very similar.

Syslog uses a facility to determine how the logging 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. The messages could be logged to different files or e-mailed to a particular user. Specifying a severity determines that all messages of that level and greater severity (lower number) will be acted upon by the syslog facility.



Note

You should configure the Cisco VSG messages to 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 VSG messages to: /var/adm/nxos_logs

To configure a syslog server, follow these steps:

Step 1 Configure the Cisco VSG syslog policy and server through the Cisco VNMC GUI. See the “Configuring Syslog Policy” section in the *Cisco Virtual Network Management Center GUI Configuration Guide*.

Step 2 Configure the syslog server as follows:

- a. Modify `/etc/syslog.conf` to handle local1 messages. For Solaris, there must be at least one tab 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 a log file.

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

- c. Restart the syslog function.

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

- d. Verify that the syslog function has started.

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

Step 3 Test the syslog server by creating an event in the Cisco VSG. This example shows that the system image messages generated are listed on the syslog server. Notice that the IP address of the Cisco VSG 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:
%AAA-6-AAA_ACCOUNTING_MESSAGE: update:171.70.212.30@pts/3:admin:configure terminal ; no
boot system (SUCCESS)
Sep 17 11:07:49 [172.22.36.142.2.2] : 2004 Sep 17 11:17:36 pacific:
%AAA-6-AAA_ACCOUNTING_MESSAGE: update:171.70.212.30@pts/3:admin:Boot Image list set to
bootflash:/nexus-1000v-mzg.VSG1.1.bin
Sep 17 11:07:51 [172.22.36.142.2.2] : 2004 Sep 17 11:17:39 pacific:
%AAA-6-AAA_ACCOUNTING_MESSAGE: update:171.70.212.30@pts/3:admin:configure terminal ; boot
system bootflash:/nexus-1000v-mzg.VSG1.1.bin (SUCCESS)
```

Troubleshooting with Logs

The Cisco VSG generates many types of system messages on the switch 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.

Viewing Logs

You can access and view logs in the Cisco VSG by entering the `show logging ?` command as follows:

```
vsg# 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

```

This example shows how to display the VSG server configuration logs:

```

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

```

Troubleshooting Fragmentation/Jumbo Issues

When the Cisco VSG, VEM, and ASA communicate with each other, in a service chain or otherwise, there may be issues related to fragmentation or jumbo frames. You need to make the correct MTU settings to ensure seamless traffic flow and better network performance.

Some of the likely scenarios and maximum transmission unit (MTU) setting recommendations for the Cisco VSG are as follows:

- When the VEM communicates with the Cisco VSG in the Layer 2 mode, an additional header with 62 bytes is added to the original packet. The VEM fragments the packet if it exceeds the uplink MTU. For better performance, increase the MTU of all links between the VEM and the Cisco VSG by 62 bytes to account for packet encapsulation, which occurs for communication between vPath and the Cisco VSG.
- When the VEM communicates with the Cisco VSG in the Layer 3 mode, an additional header with 82 bytes is added to the original packet. The VEM does not support fragmentation in Layer 3 mode and the ports/network elements (that carry the vPath-encapsulated packets) must be configured in a way that the vPath overhead is accommodated.
- If the jumbo frames are enabled in the network, make sure that the MTU of the client and server VMs are reduced by the vPath encapsulation size.
- If the Cisco VSG is deployed on a Virtual Extensible Local Area Network (VXLAN), an additional header with 50 bytes is added to the vPath encapsulation. Adjust the MTU by this value.

The recommended MTU settings for the Cisco ASA 1000V are as follows:

- For fragmentation, use these settings:
 - ASA Inside MTU 9000
 - ASA Outside MTU 9000
 - vPath Path-MTU 1500
- For jumbo frames, use these settings:
 - ASA Inside MTU 9000
 - ASA Outside MTU 9000

- vPath Path-MTU 8950

Contacting Cisco Customer Support

If you are unable to solve a problem after using the troubleshooting suggestions in this guide, 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:

- Version of the Cisco VSM/VSG and VNMC software
- Version of the ESX and vCenter Server software
- Contact phone number
- Brief description of the problem
- Brief explanation of the steps that you have already taken to isolate and resolve the problem

If you purchased the product and support contract from Cisco, contact Cisco for support. Cisco provides Layer 1, Layer 2, and Layer 3 support.

After you have collected this information, see the [“Obtaining Documentation and Submitting a Service Request”](#) section on page -xii.

For more information about the steps to take before calling technical support, see the [“Before Contacting Technical Support”](#) section on page 9-1.

