Before Contacting Technical Support

This chapter describes the steps to take before calling for technical support.

This chapter includes the following sections:

Note If you purchased Cisco support through a Cisco reseller, contact the reseller directly. If you purchased support directly from Cisco, contact Cisco Technical Support at this URL: http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

Gathering Information for Technical Support

Use this procedure to gather information about your network that you will provide to your customer support representative or Cisco TAC.

Note Required logs and counters are part of volatile storage and do not persist through a reload. Do not reload the module or the switch until you have completed this procedure.

DETAILED STEPS

Step 1 Configure your Telnet or Secure Shell (SSH) application to log screen output to a text file.

Step 2 Set the number of lines that appear on the screen so that pausing is disabled:

terminal length 0

Step 3 Display the configuration information needed to troubleshoot your network by entering the **show tech-support** command.

Step 4 Capture the error codes that appear in your message logs by entering the following commands:

- **show logging logfile**—Displays the contents of the logfile.
- **show logging last** *number*—Displays the last few lines of the logfile.

Step 5 Gather your answers to the following questions:

- On which Cisco VSG is the problem occurring?
- Are Cisco Virtual Security Gateway (VSG) software, driver versions, operating systems versions, and storage device firmware in your fabric?
- Are you running ESX and vCenter Server software?
- What is your network topology?
- Did you make any changes to the environment (VLANs, adding modules or upgrades) before 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 switch 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 tried? Which, if any, of the following tools were used?
  - Ethanalyzer, local or remote SPAN
  - CLI debug commands
  - traceroute, ping
- Is your problem related to a software upgrade attempt?
  - What was the original Cisco VSG version?
  - What is the new Cisco VSG version?

Obtaining a File of Core Memory Information

Cisco customer support engineers often use files from your system for analysis. One such file that contains memory information is referred to as a core dump. The file is sent to a TFTP server or to a flash card in slot0: of the local switch. You should set up your switch to generate this file under the instruction of your TAC representative, and send it to a TFTP server so that it can be e-mailed to TAC.

This example shows how to generate a file of core memory information or a core dump:

```
vsg(config)# system cores tftp://10.91.51.200/svr15svc_cores
vsg(config)# show system cores
Cores are transferred to tftp://10.91.51.200/svr15svc_cores
vsg(config)#
```

Note The filename (indicated by svr15svc_cores) must exist in the TFTP server directory.

Copying Files

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

The Cisco VSG always acts as a client. For example, an FTP/SCP/TFTP session always originates from the switch 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** CLI command supports 4 transfer protocols and 12 different sources for files.

This example shows the results of the command:

```
vsg# copy ?
    bootflash:      Select source filesystem
    core:           Select source filesystem
    debug:          Select source filesystem
    ftp:            Select source filesystem
    log:            Select source filesystem
    modflash:       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
    volatile:       Select source filesystem
vsg#
```

This example shows how to use secure copy (SCP) as the transfer mechanism:

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

This example shows how to copy /etc/hosts from 172.22.36.10 using the user user1, where the destination is hosts.txt:

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

This example shows how to back up the startup configuration to an SFTP server:

```
vsg# 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:
vsg#
```

Tip You should back up the startup-configuration file to a server daily and before you make any changes. You could use a short script to be run on the Cisco VSG to perform a save and a backup of the configuration. The script must 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.