Before Contacting Technical Support

This chapter describes the steps to take before calling for technical support and includes the following sections:

- Cisco Support Communities, page 17-1
- Gathering Information for Technical Support, page 17-1
- Obtaining a File of Core Memory Information, page 17-2
- Copying Files, page 17-3

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/warp/public/687/Directory/DirTAC.shtm

Cisco Support Communities

For additional information, visit one of the following support communities:

- Cisco Support Community for Server Networking
- Cisco Communities: Nexus 1000V

Gathering Information for Technical Support

At some point, you may need to contact your customer support representative or Cisco TAC for some additional assistance. This section outlines the steps that the you should perform prior to contacting your next level of support, so you can reduce the amount of time that you spend resolving the issue.

Note Do not reload the module or the switch at least until you have completed Step 1. Some logs and counters are kept in volatile storage and will not survive a reload.

Step 1 Collect switch information and configuration before and after the issue has been resolved.

Configure your Telnet or SSH application to log the screen output to a text file. Use the **terminal length 0** CLI command and then use the **show tech-support details** CLI command.

Step 2 Capture the exact error codes you see in CLI message logs.

- **show logging log** CLI (displays the error messages)
- **show logging last** *number* (displays the last lines of the log)

Step 3 Answer the following questions before calling for technical support:

- On which switch or port is the problem occurring?
- Which Cisco Nexus 1000V software, driver versions, operating systems versions and storage device firmware are in your fabric?
- ESX and vCenter Server software that you are running?
- What is the network topology?
- Were any changes being made to the environment (VLANs, adding modules, upgrades) 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 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 attempted? Which, if any, of the following tools were used?
  - Ethanalyzer, local, or remote SPAN
  - CLI debug commands
  - traceroute, ping

Obtaining a File of Core Memory Information

Cisco customer support engineers often use files from your system for analysis. One such file contains memory information and 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 customer support representative and send it to a TFTP server so that it can be emailed to them.

To generate a file of core memory information, or a core dump, use the command in the following example.

```
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.

Copying Files

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

The Cisco Nexus 1000V always acts as a client. An ftp/scp/tftp session will always originate from the switch and either push files to an external system or pull 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 four transfer protocols and 12 different sources for files.

```
switch# copy ?
    bootflash: Select source filesystem
    core: Select source filesystem
    debug: Select source filesystem
    ftp: Select source filesystem
    licenses Backup license files
    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
    slot0: Select source filesystem
    startup-config Copy startup configuration to destination
    system: Select source filesystem
    tftp: Select source filesystem
    volatile: Select source filesystem
```

Use the following syntax to use secure copy (scp) as the transfer mechanism:

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

Copy `/etc/hosts` from 172.22.36.10 using the user `user1`, where the destination would be `hosts.txt`.

```
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
```

Back 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#
```

Tip Back up the startup configuration to a server daily before you make any changes. You can write a short script to be run on the Cisco Nexus 1000V to perform a save and then back up the configuration. The script only needs to contain two commands: **copy running-configuration startup-configuration** and **copy startup-configuration tftp://***server/name*. To execute the script, enter the **run-script** *filename* command.