

This section describes how to identify and resolve problems that might occur when installing, upgrading, or restarting Cisco MDS 9000 Family products.

Contents

- [1 Generating a PDF of this section](#)
- [2 Overview](#)
- [3 Guidelines](#)
 - ◆ [3.1 Guidelines for Installations](#)
 - ◆ [3.2 Guidelines for Upgrading](#)
 - ◆ [3.3 Guidelines for Reboots](#)
- [4 Disruptive Module Upgrades](#)
- [5 Troubleshooting a Nondisruptive Upgrade on a Fabric Switch](#)
- [6 Troubleshooting Fabric Manager Installations](#)
- [7 Verifying Cisco SAN-OS Software Installations](#)
- [8 Troubleshooting Cisco SAN-OS Software Upgrades and Downgrades](#)
 - ◆ [8.1 Software Installation Reports an Incompatibility](#)
 - ◆ [8.2 Diagnosing Compatibility Issues](#)
 - ◆ [8.3 Software Installation Ends with Error](#)
 - ◇ [8.3.1 Installing SAN-OS Software Using Fabric Manager](#)
 - ◇ [8.3.2 Installing Cisco SAN-OS Software from the CLI](#)
- [9 Troubleshooting Cisco SAN-OS Software System Reboots](#)
 - ◆ [9.1 Power On or Switch Reboot Hangs](#)
 - ◆ [9.2 Corrupted Bootflash Recovery](#)
 - ◆ [9.3 Recovery Using BIOS Setup for Supervisor-1](#)
 - ◆ [9.4 Recovery from the loader> Prompt on Supervisor-2 Modules](#)
 - ◆ [9.5 Recovery from the loader> Prompt on Supervisor-1 Modules](#)
 - ◆ [9.6 Recovery from the switch\(boot\)# Prompt](#)
 - ◆ [9.7 Recovery for Switches with Dual Supervisor Modules](#)
 - ◇ [9.7.1 Recovering One Supervisor Module with Corrupted Bootflash](#)
 - ◇ [9.7.2 Recovering Both Supervisor Modules With Corrupted Bootflash](#)
 - ◆ [9.8 Recognizing Error States](#)
 - ◆ [9.9 Switch or Process Resets](#)
 - ◆ [9.10 Recoverable System Restarts](#)
 - ◆ [9.11 Unrecoverable System Restarts](#)
- [10 Recovering the Administrator Password](#)
- [11 Miscellaneous Software Image Issues](#)
 - ◆ [11.1 All Ports Down Because of System Health Failure](#)
 - ◆ [11.2 Switch Reboots after FCIP Reload](#)
 - ◆ [11.3 FCIP Link Fails to Come Up](#)
 - ◆ [11.4 Cannot Create, Modify, or Delete Admin Role](#)
 - ◆ [11.5 FC IDs Change after Link Reset](#)
 - ◆ [11.6 Switch Displays Wrong User](#)


Generating a PDF of this section

[Cisco MDS SanOS Troubleshooting Guide -- Troubleshooting Installs, Upgrades, and Reboots PDF](#)

Overview

Each Cisco MDS 9000 switch ships with an operating system (Cisco SAN-OS) that consists of two images: the kickstart image and the system image. There is also a module image if the Storage Services Module (SSM) is present.

Installations, upgrades, and reboots are ongoing parts of SAN maintenance activities. It is important to minimize the risk of disrupting ongoing operations when performing these operations in production environments and to know how to recover quickly when something does go wrong.

 **Note:** For documentation purposes, we use the term *upgrade* in this document. The term upgrade refers to both upgrading and downgrading your switch, pertaining to the context.

Guidelines

This section lists general guidelines for performing Cisco SAN-OS software installations, image upgrade and downgrade procedures, and reboots.

Guidelines for Installations

Follow these guidelines when installing Cisco SAN-OS software images:


- Ensure that an FTP or TFTP server is available and can be accessed via the IP address of the default gateway (rather than any other IP address on the defined subnet).
- Use the **show install all impact** CLI command to verify that the new image is healthy and the impact that new load will have on any hardware with regards to compatibility. Check for compatibility.
- Choose **Admin > Show Image Version** in the Device Manager to view information on images in the directories of the MDS file system.

Guidelines for Upgrading

Not all images need to be updated during an upgrade. Use the following checklist to prepare for an upgrade:

Checklist	Check off
Copy the new Cisco SAN-OS image onto your supervisor modules in bootflash: or slot0:.	
Save your running configuration to the startup configuration.	
Back up a copy of your configuration to a remote TFTP server.	
Schedule your upgrade during an appropriate maintenance window for your fabric.	
Verify that you have the correct image for your supervisor module type.	
Verify that no SSM ports are configured in auto mode.	

After you have completed the checklist, you are ready to upgrade the switches in your fabric.

 **Note:** It is normal for the active supervisor to become the standby supervisor during an upgrade.

Follow these guidelines when upgrading or downgrading Cisco SAN-OS software images:

- Read the Cisco SAN-OS Release Notes for the release you are upgrading or downgrading to. Cisco SAN-OS Release Notes are available at the following website:
http://cisco.com/en/US/products/ps5989/prod_release_notes_list.html
- Ensure that an FTP or TFTP server is available.
- Copy the startup-config to a snapshot config in NVRAM. This step creates a backup copy of the startup-config.
 - ◆ In Device Manager, choose **Admin > Copy Configuration** and select the startupConfig radio button for the From: field and the serverFile radio button for the To: field. Set the other fields, and click **Apply**.
 - ◆ From the CLI, use the **copy nvram:startup-config nvram-snapshot-config** command.
- Where possible, choose to do a nondisruptive upgrade. In general, you can nondisruptively upgrade to Cisco SAN-OS Release 3.x software from any Cisco SAN-OS software Release 2.x or later.
 - ◆ Review the upgrade table in the Cisco SAN-OS Release Notes for the version you will be installing.
 - ◆ Use the **show install all impact upgrade-image** CLI command to determine if your upgrade will be nondisruptive.
- Establish a PC serial connection to each supervisor console to record upgrade activity to a file. This serial connection catches any error messages or problems during bootup.
- In Fabric Manager, choose **Tools > Other > Software Install** or click the **Software Install** icon on the toolbar to use the Software Install Wizard.
- From the CLI, use the **install all [{asm-sfn | kickstart | ssi | system} URL]** command to run a complete script, test the images, and verify the compatibility with the hardware. See the "Installing Cisco SAN-OS Software from the CLI" section. Using the **install all** command offers the following advantages:
 - ◆ You can upgrade the entire switch using the least disruptive procedure with just one command.
 - ◆ You can receive descriptive information on the intended changes to your system before you continue with the command.
 - ◆ You have the option to cancel the command. Once the results of the command are shown, you can continue or cancel when you see this question (the default is no):

```
Do you want to continue (y/n) [n] :y
```

- - ◆ You can view the progress of this command on the console, Telnet, and SSH screens.
 - ◆ The image integrity is automatically checked, including the running kickstart and system images.
 - ◆ The command performs a platform validity check to verify that a wrong image is not used. For example, the command verifies that an MDS 9500 Series image is not used inadvertently to upgrade an MDS 9200 Series switch.
 - ◆ After entering the **install all** command, if any step in the sequence fails, the command completes the step in progress and ends. For example, if a switching module fails to be updated for any reason (for example, due to an unstable fabric state), then the command sequence disruptively updates that module and ends. In such cases, you can verify the problem on the affected switching module and upgrade the other switching modules.


- If you run the setup script after entering a **write erase** CLI command, you must set the default zone policy for VSAN 1 after the setup script completes. In Fabric Manager, choose **Fabricxx > VSAN 1 > Default Zone**, select the **Policies** tab and set the **Default Zone Behavior** drop-down menu to permit or deny. In the CLI, use the **zone default-zone** command.

Guidelines for Reboots

Cisco SAN-OS allows for three different types of system restarts:

- Recoverable ? A process restarts and service is not affected.
- Unrecoverable ? A process has restarted more than the maximum restart times within a fixed period of time (seconds) and will not be restarted again.
- System hung/crashed ? No communications of any kind is possible with the system.

Schedule the reboot to avoid possible disruption of services during critical business hours.

 **Note:** Log messages are not saved across system reboots. However, a maximum of 100 log messages with a severity level of critical and below (levels 0, 1, and 2) are saved in NVRAM. You can view this log at any time with the **show logging nvram** CLI command.

Disruptive Module Upgrades

Software upgrades for the SSM, MPS-14/2, MSM-18/4 module, or the IP Storage (IPS) services modules are disruptive. These modules use a rolling upgrade install mechanism where the modules are upgraded in sequence. After the first module upgrade finishes, and before the next module upgrade begins, Cisco SAN-OS introduces a time delay to ensure that all applications in the module reach a steady state. The IPS modules require a five-minute delay before the next IPS module upgrade can guarantee a stable state.

SSM supports nondisruptive upgrades for the Layer 1 and Layer 2 protocols under the following conditions:

- SSM is running Cisco SAN-OS Release 2.1(2) or later and upgrading to a later release.
- The SSM hardware has the ELPD image for Release 2.1(2) installed. Use the **show version module module number epld** CLI command, and verify that the EPLD version is 0x07 or later.
- You have turned off all Layer 3 services on the SSM by deprovisioning the DPPs for Layer 3 service.

Troubleshooting a Nondisruptive Upgrade on a Fabric Switch

When a nondisruptive upgrade begins, the system notifies all services that an upgrade is about to start, and finds out whether or not the upgrade can proceed. If a service cannot allow the upgrade to proceed at this time (for example, FSPF timers are not configured to the default value, or a CFS operation is in progress), then the service will abort the upgrade. If this occurs, you will be prompted to enter the **show install all failure-reason** command to determine the reason why the upgrade cannot proceed.

```
...
Do you want to continue with the installation (y/n)? [n] y
Install is in progress, please wait.
Notifying services about the upgrade.
[#           ] 0% -- FAIL. Return code 0x401E0066 (request timed out).
Please issue "show install all failure-reason" to find the cause of the failure.<---system
prompt to enter the show all failure-reason command.
Install has failed. Return code 0x401E0066 (request timed out).
Please identify the cause of the failure, and try 'install all' again.
```

```
switch# show install all failure-reason
```

Service: "cfs" failed to respond within the given time period.

switch#

Enter **show install all failure-reason** to find the cause of the failure.

Troubleshooting Fabric Manager Installations

This section describes possible problems and solutions for a Fabric Manager installation failure. Fabric Manager requires that the appropriate version of Sun JAVA JRE be installed, based on the Fabric Manager release. Table 2-1 shows the recommended JRE for Fabric Manager 2.x and later releases.

Table 2-1 Fabric Manager and Recommended JRE Version

Fabric Manager Release	Recommended JRE Version
2.0(1b) through 2.1(1b)	1.4.2_05
2.1(2) through 3.3(1)1	1.5.x

Fabric Manager and Device Manager do not operate properly with JRE 1.4.2_03 on Windows 2003.

Symptom: Fabric Manager or Device Manager will not start. Table 2-2 lists the scenarios and the solutions.

Table 2-2 Fabric Manager or Device Manager Will Not Start

Symptom	Possible Cause	Solution
Device Manager will not start.	Device Manager proxied through Fabric Manager Server.	Uncheck Proxy SNMP in the FM Server check box in the Device Manager startup dialog box, and restart Device Manager.
Fabric Manager will not start.	Using incorrect Fabric Manager Server.	Verify that you are choosing the appropriate Fabric Manager Server from the FMServer pull-down menu. If you have not already done so, download Fabric Manager Server.
	Fabric Manager Server not running.	On a Windows PC, choose Start > Control Panel > Administrative Tools > Services to verify that Fabric Manager Server and Fabric Manager database have started. The default setting for the Fabric Manager Server is that the server is automatically started when the PC is rebooted.
	Incompatible JRE version.	Verify that you have the correct JRE version installed for the Fabric Manager release you installed. Refer to the release notes for the software version you installed to determine which JRE version is compatible.
	Improperly installed.	If the problem remains, remove the application using the Cisco MDS 9000/Uninstall program, and then reinstall Fabric Manager.

Verifying Cisco SAN-OS Software Installations

In Fabric Manager you can watch the progress of your software installation using the Software Install Wizard. From the CLI, you can use the **show install all status** command to watch the progress of your software installation.

You can also use the **show install all status** CLI command to view the current **install all** command or the log of the last installed **install all** command from a console, SSH, or Telnet session.

This command presents the install all output on both the active and standby supervisor module even if you are not connected to the console terminal. It only displays the status of an **install all** command that is issued from the CLI (not the GUI). See the following example:

```
switch# show install all status
There is an on-going installation... <----- in progress installation
Enter Ctrl-C to go back to the prompt.
Verifying image bootflash:/b-1.3.0.104
-- SUCCESS
Verifying image bootflash:/i-1.3.0.104
-- SUCCESS
Extracting "system" version from image bootflash:/i-1.3.0.104.
-- SUCCESS
Extracting "kickstart" version from image bootflash:/b-1.3.0.104.
-- SUCCESS
Extracting "loader" version from image bootflash:/b-1.3.0.104.
-- SUCCESS
switch# show install all status
This is the log of last installation. <----- log of last install
Verifying image bootflash:/b-1.3.0.104
-- SUCCESS
Verifying image bootflash:/i-1.3.0.104
-- SUCCESS
Extracting "system" version from image bootflash:/i-1.3.0.104.
-- SUCCESS
Extracting "kickstart" version from image bootflash:/b-1.3.0.104.
-- SUCCESS
Extracting "loader" version from image bootflash:/b-1.3.0.104.
-- SUCCESS
```

Troubleshooting Cisco SAN-OS Software Upgrades and Downgrades

This section discusses possible causes and solutions for a software installation upgrade or downgrade failure.

Software Installation Reports an Incompatibility

This table describes the scenario and the solutions.

Symptom	Possible Cause	Solution
The software installation reports an incompatibility.	The running image may have a feature enabled that is not compatible with the proposed new image.	Review the incompatibility issues displayed by either the Fabric Manager Software Install Wizard or the install all CLI command. Correct any problems and retry the installation. See the

	<p>"Diagnosing Compatibility Issues" section.</p> <p>Verify which features are enabled on your switch and disable any features that may not be compatible with your new image. Refer to the appropriate release notes for both images.</p>
--	--

Diagnosing Compatibility Issues

To view the results of a dynamic compatibility check, use the **show incompatibility system bootflash:filename** CLI command. Use the **show incompatibility** CLI command for diagnosis when the **install all** CLI command warns of compatibility issues. During an attempted upgrade, the **install all** CLI command may return the following warning:

Warning: The startup config contains commands not supported by the system image; as a result, some resources might become unavailable after an install.

Do you wish to continue? (y/ n) [y]: ''n''

Use the **show incompatibility** CLI command to identify the problem.

Message 1 indicates that the remote SPAN (RSPAN) feature is in use, but it is not supported by the image that was installed. The incompatibility is strict because continuing the upgrade might cause the switch to move into an inconsistent state; that is, configured features might stop working.

```
switch# show incompatibility system bootflash:new-image
```

The following configurations on active are incompatible with the system image

```
1) Feature Index : 67 , Capability : CAP_FEATURE_SPAN_FC_TUNNEL_CFG
```

```
Description : SPAN - Remote SPAN feature using fc-tunnels
```

```
Capability requirement : STRICT
```

Message 2 indicates that the Fibre Channel tunnel feature is not supported in the new image. The RSPAN feature uses Fibre Channel tunnels.

```
2) Feature Index : 119 , Capability : CAP_FEATURE_FC_TUNNEL_CFG
```

```
Description : fc-tunnel is enabled
```

```
Capability requirement : STRICT
```

Software Installation Ends with Error

Symptom The software installation ends with an error. This table describes the scenarios and the solutions.

Problem	Possible Cause	Solution

The installation ends with an error.	The standby supervisor module bootflash: file system does not have sufficient space to accept the updated image.	Remove unnecessary files from the file system. In Device Manager, choose Admin > Flash Files and delete unnecessary files. From the CLI, use the delete command.
	The specified system and kickstart images are not compatible.	Check the output of the installation process for details on the incompatibility. Possibly update the kickstart image before updating the system image.
	The install all command is issued on the standby supervisor module.	Enter the command on the active supervisor module only.
	A module was inserted while the upgrade was in progress.	Restart the installation. See the "Installing SAN-OS Software Using Fabric Manager" section or the "Installing Cisco SAN-OS Software from the CLI" section.
	The fabric or switch was configured while the upgrade was in progress.	Wait until the upgrade is complete before configuring the switch. In Device Manager, choose Admin > CFS or from the CLI, use the show cfs lock command to check that there are no CFS commit operations in progress.
	The switch experienced a power disruption while the upgrade was in progress.	Restart the installation. See the "Installing SAN-OS Software Using Fabric Manager" section or the "Installing Cisco SAN-OS Software from the CLI" section.
	Incorrect software image path specified.	Specify the entire path for the remote location accurately.
	Another installation is already in progress.	Verify the state of the switch at every stage and restart the installation after 10 seconds. If you restart the installation within the 10-second span, the command is rejected with an error message indicating that an installation is currently in progress.
	Module failed to upgrade.	Restart the installation. See the "Installing SAN-OS Software Using Fabric Manager" section or the "Installing Cisco SAN-OS Software from the CLI" section.

	Or, use the install module CLI command to upgrade the failed module.
--	---

Installing SAN-OS Software Using Fabric Manager


To use the Software Install Wizard to install a new software image using Fabric Manager, follow these steps:

1. Open the Software Install Wizard by clicking its icon in the toolbar (see Figure 2-1).

Figure 2-1 Software Install Wizard Icon



2. Select the switches you want to install images on. You must select at least one switch in order to proceed. Click **Next**.
3. (Optional) Check the **Skip Image Download** check box and click **Next** to use images that are already downloaded (the file is already on the bootflash: file system). Proceed to Step 7.
4. Click the row under the System, Kickstart, Asm-sfn, or ssi columns to enter image URIs. You must specify at least one image for each switch to proceed.
5. Check the active (and standby, if applicable) bootflash: file system on each switch to see if there is enough space for the new images. You can see this information in the Flash Space column.
6. Click **Next**. You see the Select Download Image screen.
7. Double-click the table cell under System, Kickstart, Asm-sfn, or Ssi and select from a drop-down list of images available in the bootflash: file system on each switch. You must select at least one image for each switch to proceed.
8. Click **Next**. You see the final verification screen.
9. Click **Finish** to start the installation or click **Cancel** to leave the installation wizard without installing new images.

 **Note:** * This screen shows the active (and standby, if applicable) bootflash: memory space on each switch, and shows the status (whether there is enough space for the new images). If any switch has insufficient space, you cannot proceed. Deselect the switch without enough bootflash: memory by going back to the first screen and unchecking the check box for that switch.

* There is no limit on the number of switches you can upgrade. However, the upgrade is a serial process; that is, only a single switch is upgraded at a time.

* On hosts where the TFTP server cannot be started, a warning is displayed. The TFTP server may not start because an existing TFTP server is running or because access to the TFTP port 69 has been denied for security reasons (the default setting on LINUX). In these cases, you cannot transfer files from the local host to the switch.

* Before exiting the session, be sure that the upgrade process is complete. The wizard displays


status messages as the upgrade proceeds. Check the lower left-hand corner of the wizard for the status messages. The wizard first displays the message Success, followed a few seconds later by InProgress Polling. The wizard displays a second message Success, before displaying the final Upgrade Finished message.

Installing Cisco SAN-OS Software from the CLI

To perform an automated software upgrade on any switch from the CLI, follow these steps:

1. Log into the switch through the console, Telnet, or SSH port of the active supervisor.
2. Create a backup of your existing configuration file, if required.
3. Perform the upgrade by issuing the **install all** command.

The example that follows demonstrates upgrading from SAN-OS 2.0(2b) to 2.1(1a) using the **install all** command with the source images located on a SCP server.

 **Note:** Always carefully read the output of install all compatibility check. This compatibility check tells you exactly what needs to be upgraded (BIOS, loader, firmware) and what modules are not hitless. If there are any questions or concerns about the results of the output, select n to stop the installation and contact the next level of support.

```
ca-9506# install all system scp://testuser@dino/tftpboot/rel/qa/2_1_1a/final/m9500-sflek9-mz.2.1.1a.bin kickstart scp://testuser@dino/tftpboot/rel/qa/2_1_1a/final/m9500-sflek9-kickstart-mz.2.1.1a.bin
```

```
For scp://testuser@dino, please enter password:
```

```
For scp://testuser@dino, please enter password:
```

```
Copying image from scp://testuser@dino/tftpboot/rel/qa/2_1_1a/final/m9500-sflek9-kickstart-mz.2.1.1a.bin to bootflash:///m9500-sflek9-kickstart-mz.2.1.1a.bin.
```

```
[#####] 100% -- SUCCESS
```

```
Copying image from scp://testuser@dino/tftpboot/rel/qa/2_1_1a/final/m9500-sflek9-mz.2.1.1a.bin to bootflash:///m9500-sflek9-mz.2.1.1a.bin.
```

```
[#####] 100% -- SUCCESS
```

```
Verifying image bootflash:///m9500-sflek9-kickstart-mz.2.1.1a.bin
```

```
[#####] 100% -- SUCCESS
```

```
Verifying image bootflash:///m9500-sflek9-mz.2.1.1a.bin
```

```
[#####] 100% -- SUCCESS
```

Cisco_MDS_SanOS_Troubleshooting_Guide_--_Troubleshooting_Installs,_Upgrades,_and_Reboots

Extracting "slc" version from image bootflash:///m9500-sflek9-mz.2.1.1a.bin.

[#####] 100% -- SUCCESS

Extracting "ips" version from image bootflash:///m9500-sflek9-mz.2.1.1a.bin.

[#####] 100% -- SUCCESS

Extracting "svclc" version from image bootflash:///m9500-sflek9-mz.2.1.1a.bin.

[#####] 100% -- SUCCESS

Extracting "system" version from image bootflash:///m9500-sflek9-mz.2.1.1a.bin.

[#####] 100% -- SUCCESS

Extracting "kickstart" version from image bootflash:///m9500-sflek9-kickstart-mz.2.1.1a.bin.

[#####] 100% -- SUCCESS

Extracting "loader" version from image bootflash:///m9500-sflek9-kickstart-mz.2.1.1a.bin.

[#####] 100% -- SUCCESS

Compatibility check is done:

Module	bootable	Impact	Install-type	Reason
1	yes	non-disruptive	rolling	
2	yes	non-disruptive	rolling	
3	yes	disruptive	rolling	Hitless upgrade is not supported
4	yes	disruptive	rolling	Hitless upgrade is not supported
5	yes	non-disruptive	reset	
6	yes	non-disruptive	reset	

Images will be upgraded according to following table:

Module	Image	Running-Version	New-Version	Upg-Required
--------	-------	-----------------	-------------	--------------

Cisco_MDS_SanOS_Troubleshooting_Guide_--_Troubleshooting_Installs,_Upgrades,_and_Reboots

-----	-----	-----	-----	-----
1	slc	2.0(2b)	2.1(1a)	yes
1	bios	v1.1.0(10/24/03)	v1.1.0(10/24/03)	no
2	slc	2.0(2b)	2.1(1a)	yes
2	bios	v1.1.0(10/24/03)	v1.1.0(10/24/03)	no
3	ips	2.0(2b)	2.1(1a)	yes
3	bios	v1.1.0(10/24/03)	v1.1.0(10/24/03)	no
4	svclc	2.0(2b)	2.1(1a)	yes
4	svcsb	1.3(5m)	1.3(5m)	no
4	svcsb	1.3(5m)	1.3(5m)	no
4	bios	v1.1.0(10/24/03)	v1.1.0(10/24/03)	no
5	system	2.0(2b)	2.1(1a)	yes
5	kickstart	2.0(2b)	2.1(1a)	yes
5	bios	v1.1.0(10/24/03)	v1.1.0(10/24/03)	no
5	loader	1.2(2)	1.2(2)	no
6	system	2.0(2b)	2.1(1a)	yes
6	kickstart	2.0(2b)	2.1(1a)	yes
6	bios	v1.1.0(10/24/03)	v1.1.0(10/24/03)	no
6	loader	1.2(2)	1.2(2)	no

Do you want to continue with the installation (y/n)? [n] y

Install is in progress, please wait.

Syncing image bootflash:///m9500-sf1ek9-kickstart-mz.2.1.1a.bin to standby.

[#####] 100% -- SUCCESS

Syncing image bootflash:///m9500-sf1ek9-mz.2.1.1a.bin to standby.

[#####] 100% -- SUCCESS

Setting boot variables.

[#####] 100% -- SUCCESS

Performing configuration copy.

```
[#####] 100% -- SUCCESS
```

Module 5: Waiting for module online.

```
2005 May 20 15:46:03 ca-9506 %KERN-2-SYSTEM_MSG: mts: HA communication with standby terminated. Please check the standby supervisor.
```

```
-- SUCCESS
```

"Switching over onto standby".

Step 4 Exit the switch console and open a new terminal session to view the upgraded supervisor module using the **show module** command.

If the configuration meets all guidelines when the **install all** command is entered, all modules (supervisor and switching) are upgraded.

Troubleshooting Cisco SAN-OS Software System Reboots

This section lists possible problems and solutions for software reboots.

Power On or Switch Reboot Hangs

Symptom Power on or switch reboot hangs. This table describes the scenarios and solutions.

Problem	Possible Cause	Solution
Power on or switch reboot hangs for dual supervisor configuration.	The bootflash is corrupted.	See the "Recovery for Switches with Dual Supervisor Modules" section.
Power on or switch reboot hangs for single supervisor configuration.	The loader is corrupted.	Interrupt the boot process and reconfigure the BIOS through the console port to load a new kickstart image that updates to BIOS image. See the "Recovery Using BIOS Setup for Supervisor-1" section.
	The BIOS is corrupted.	Replace this module. Contact your customer support representative to return the failed module.
	The kickstart image is corrupted.	Interrupt the boot process at the >loader prompt. Update the kickstart image. See the "Recovery from the loader > Prompt on Supervisor-2 Modules" section.
	Boot parameters are incorrect.	Verify and correct the boot parameters and reboot.

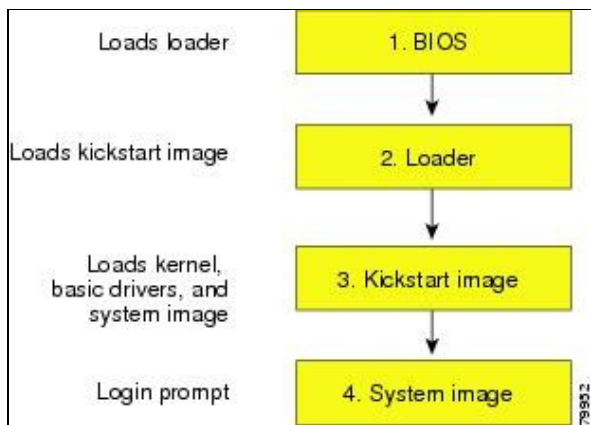
The system image is corrupted.	Interrupt the boot process at the switch#boot prompt. Update the system image. See the "Recovery from the switch(boot)# Prompt" section.
--------------------------------	--

Corrupted Bootflash Recovery


All switch configurations reside in the internal bootflash. If you have a corrupted internal bootflash you could potentially lose your configuration. Be sure to save and back up your configuration files periodically. The regular switch boot goes through the following sequence:

1. The basic input/output system (BIOS) loads the loader.
2. The loader loads the kickstart image into RAM and starts the kickstart image.
3. The kickstart image loads and starts the system image.
4. The system image reads the startup configuration file.

Figure 2-2 Regular Boot Sequence



If the images on your switch are corrupted and you cannot proceed (error state), you can interrupt the switch boot sequence and recover the image by entering the BIOS configuration utility described in the following section. Access this utility only when needed to recover a corrupted internal disk.

 **Note:** The BIOS changes explained in this section are required only to recover a corrupted bootflash.

Recovery procedures require the regular sequence to be interrupted. The internal switch sequence goes through four phases between the time you turn on the switch and the time the switch prompt appears on your terminal?BIOS, boot loader, kickstart, and system. Table 2-6 provides more information.

Table 2-6 Recovery Interruption

Phase

Normal Prompt1

Recovery Prompt2

Description

BIOS

loader>

Power On or Switch Reboot Hangs

No bootable

device

The BIOS begins the power-on self test, memory test, and other operating system applications. While the test is in progress, press **Ctrl-C** to enter the BIOS configuration utility and use the netboot option.

Boot loader

Starting

kickstart

loader>

The boot loader uncompresses loaded software to boot an image using its file name as reference. These images are made available through bootflash. When the memory test is over, press **Esc** to enter the boot loader prompt.

Kickstart

Uncompressing

system

switch(boot)#

When the boot loader phase is over, press **Ctrl-]3** (Control key plus right bracket key) to enter the switch(boot)# prompt. If the corruption causes the console to stop at this prompt, copy the system image and reboot the switch.

System

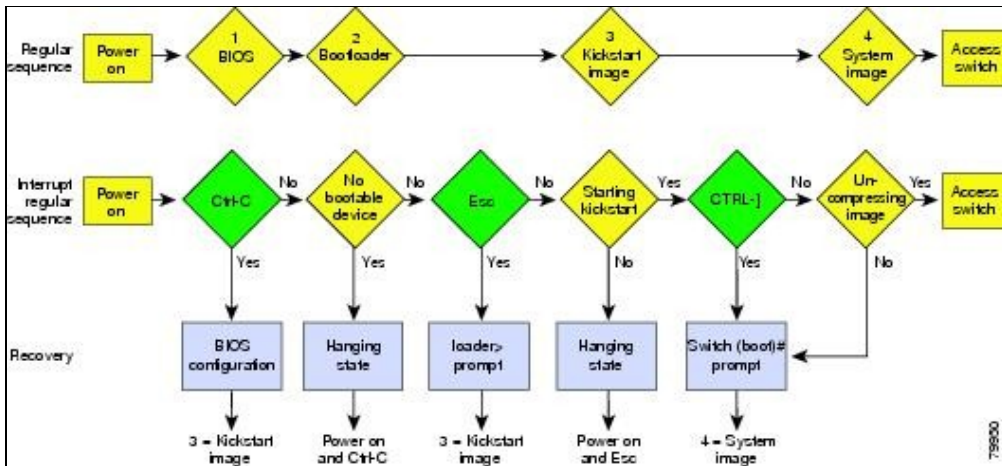
Login:

—


The system image loads the configuration file of the last saved running configuration and returns a switch login prompt.


- This prompt or message appears at the end of each phase.
- This prompt or message appears when the switch cannot progress to the next phase.
- Depending on your Telnet client, these keys may be reserved, and you need to remap the keystroke. Refer to the documentation provided by your Telnet client.

Figure 2-3 Regular and Recovery Sequence



Recovery Using BIOS Setup for Supervisor-1

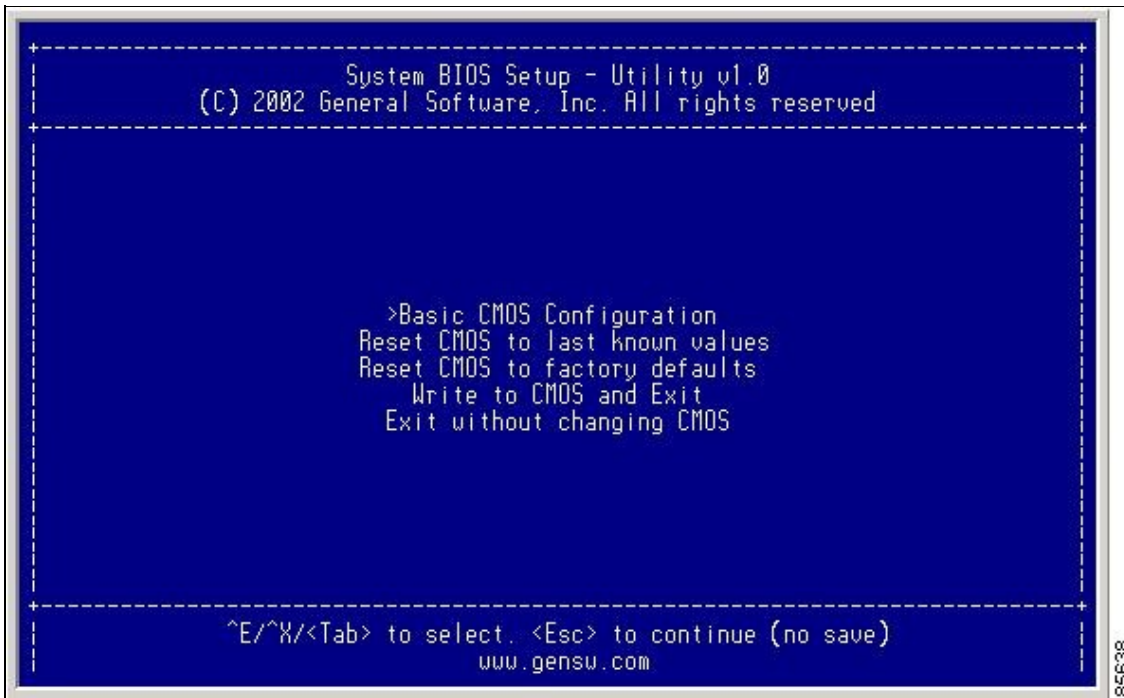
 **Note:** Supervisor-2 modules do not provide access to the BIOS.

 **Caution:** This procedure uses the **init system** command, which reformats the file system of the device. Be sure that you have made a backup of the configuration files before you begin this procedure.

To recover a corrupted bootflash: device (no bootable device found message) for a switch with a single supervisor-1 module, follow these steps:

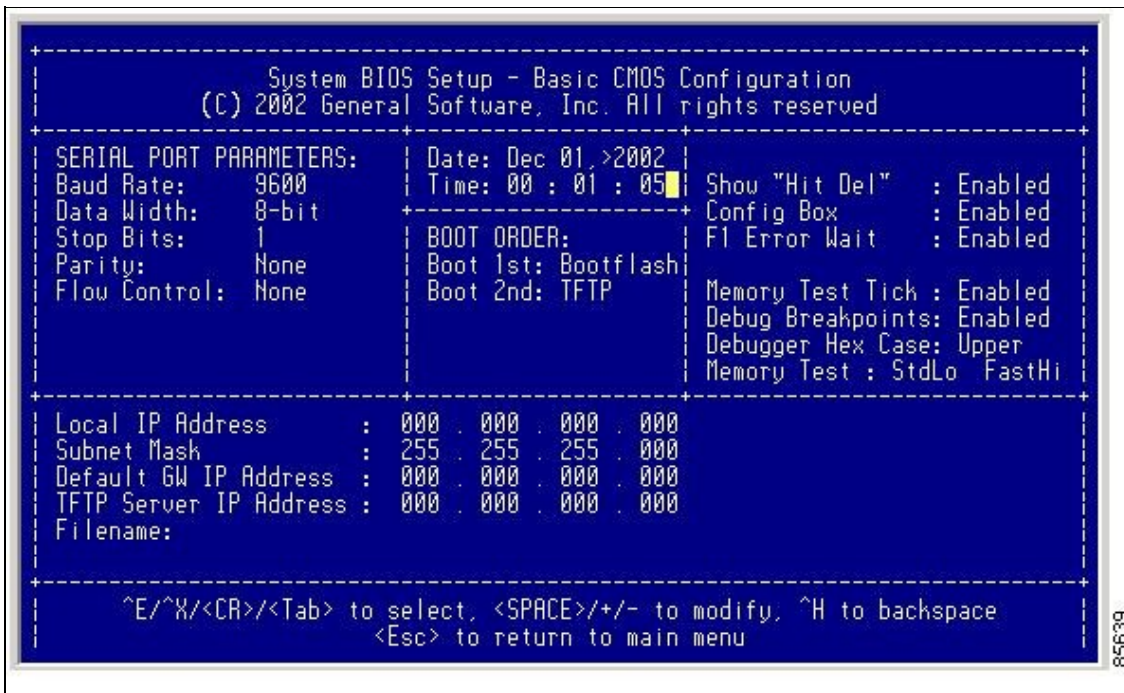
1. Connect to the console port of the required switch.
2. Boot or reboot the switch.
3. Press **Ctrl-C** to interrupt the BIOS setup during the BIOS memory test.

Figure 2-4 BIOS Setup Utility



4. Press the **Tab** key to select the Basic CMOS Configuration.

Figure 2-5 BIOS Setup Configuration (CMOS)



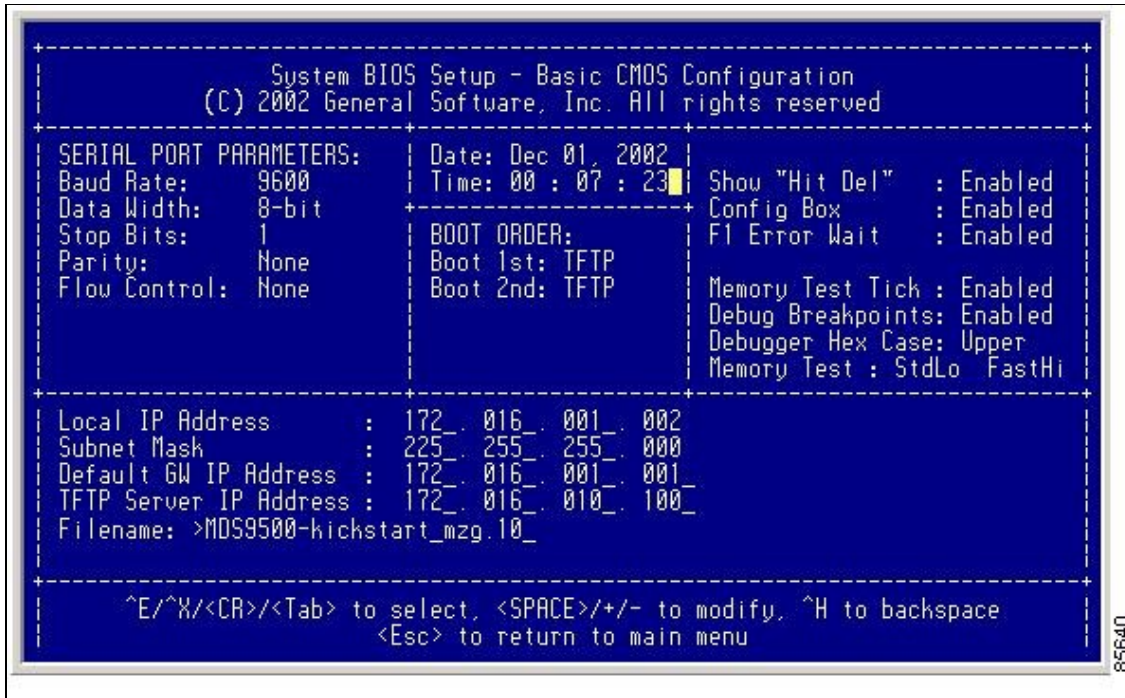
5. Change the Boot 1st: field to TFTP.

6. Press the **Tab** key until you reach the Local IP Address field.


7. Enter the local IP address for the switch, and press the **Tab** key.

8. Enter the subnet mask for the IP address, and press the **Tab** key.


9. Enter the IP address of the default gateway, and press the **Tab** key.
10. Enter the IP address of the TFTP server, and press the **Tab** key.
11. Enter the image name (kickstart), and press the **Tab** key. Use the full directory path from the TFTP server root directory.

Figure 2-6 BIOS Setup Configuration (CMOS) Changes


12. Press the **Esc** key to return to the main menu.
13. Choose Write to CMOS and Exit from the main screen to save your changes. You see the following prompt: switch(boot)#.
14. Enter the **init system** command at the switch(boot)# prompt, and press **Enter** to reformat the file system.
15. Enter switch(boot)# init system.
16. Follow the procedure specified in the "Recovery from the switch(boot)# Prompt" section.


 **Note:** Your navigating options are provided at the bottom of the screen:


- * Tab = Jump to next field
- * Ctrl-E = Down arrow
- * Ctrl-X = Up arrow
- * Ctrl-H = Erase. Backspace might not work if your terminal is not configured properly.

 **Caution:** The filename must be entered exactly as it is displayed on your TFTP server. For example, if you have a file named MDS9500-kiskstart_mzg.10, then enter this name using the exact


uppercase characters and file extensions as shown on your TFTP server.

 **Caution:** The switch must have IP connectivity to reboot using the newly configured values.

 **Note:** The **init system** command also installs a new loader from the existing (running) kickstart image.


 **Caution:** Be sure that you have made a backup of the configuration files before you issue this command.

Recovery from the loader> Prompt on Supervisor-2 Modules

 **Caution:** This procedure uses the **init system** command, which reformats the file system of the device. Be sure that you have made a backup of the configuration files before you begin this procedure.

The loader> prompt is different from the regular switch# prompt.

- The CLI command completion feature does not work at this prompt and may result in undesired errors. You must type the command exactly as you want the command to appear.
- The ICMP stack is not supported, so you cannot ping the TFTP server.
- The TFTP server must be configured with the IP address of the default gateway (rather than any other IP address on the defined subnet).

 **Note:** Use the **help** command at the loader> prompt to display a list of commands available at this prompt or to obtain more information about a specific command in that list.

To recover a corrupted kickstart image (system error state) for a switch with a single supervisor module, follow these steps:

1. Enter the local IP address for the switch at the loader> prompt, and press **Enter**.

```
loader> net --ip=172.16.1.2
```

2. Specify the subnet mask.

```
loader> net --nm= 255.255.255.0
```

3. Specify the IP address of the default gateway.

```
loader> net --gw=172.16.1.1
```


4. Boot the kickstart image file from the required server.

```
loader> boot tftp://172.16.10.100/m9500-kickstart-3.0.bin
```

In this example, 172.16.10.100 is the IP address of the TFTP server, and m9500-kickstart-3.0.bin is the name of the kickstart image file that exists on that server. The switch(boot)# prompt indicates that you have a usable kickstart image.


5. Issue the **init system** command at the switch(boot)# prompt.

```
switch(boot)# init system
```

 **Caution:** Be sure that you have made a backup of the configuration files before you issue this command.


6. Follow the procedure specified in the "Recovery from the switch(boot)# Prompt" section.

Recovery from the loader> Prompt on Supervisor-1 Modules

 **Caution:** This procedure uses the **init system** command, which reformats the file system of the device. Be sure that you have made a backup of the configuration files before you begin this procedure.

The loader> prompt is different from the regular switch# prompt.

- The CLI command completion feature does not work at this prompt and may result in undesired errors. You must type the command exactly as you want the command to appear.
 - The ICMP stack is not supported, so you cannot ping the TFTP server.
 - The TFTP server must be configured with the IP address of the default gateway (rather than any other IP address on the defined subnet).
-

 **Note:** Use the **help** command at the loader> prompt to display a list of commands available at this prompt or to obtain more information about a specific command in that list.

To recover a corrupted kickstart image (system error state) for a switch with a single supervisor module, follow these steps:

1. Enter the local IP address and the subnet mask for the switch at the loader> prompt, and press **Enter**.

```
loader> ip address 172.16.1.2 255.255.255.0
```

```
Found Intel EtherExpressPro100 82559ER at 0xe800, ROM address 0xc000
```

```
Probing...[Intel EtherExpressPro100 82559ER]Ethernet addr: 00:05:30:00:52:27
```

```
Address: 172.16.1.2
```

```
Netmask: 255.255.255.0
```

```
Server: 0.0.0.0
```

```
Gateway: 0.0.0.0
```

2. Specify the IP address of the default gateway.

```
loader> ip default-gateway 172.16.1.1
```

```
Address: 172.16.1.2
```

```
Netmask: 255.255.255.0
```

```
Server: 0.0.0.0
```

```
Gateway: 172.16.1.1
```

3. Boot the kickstart image file from the required server.

```
loader> boot tftp://172.16.10.100/kickstart-image1
Address: 172.16.1.2
Netmask: 255.255.255.0
Server: 172.16.10.100
Gateway: 172.16.1.1
Booting: /kick-282 console=ttyS0,9600n8nn quiet loader_ver= "2.1(2)"....
.....Image verification OK
Starting kernel...
INIT: version 2.78 booting
Checking all filesystems..... done.
Loading system software
INIT: Sending processes the TERM signal
Sending all processes the TERM signal... done.
Sending all processes the KILL signal... done.
Entering single-user mode...
INIT: Going single user
INIT: Sending processes the TERM signal
switch(boot) #
```

The switch(boot)# prompt indicates that you have a usable Kickstart image.

4. Issue the **init system** command at the switch(boot)# prompt.

```
switch(boot) # init system
```



Caution: Be sure that you have made a backup of the configuration files before you issue this command.

5. Follow the procedure specified in the "Recovery from the switch(boot)# Prompt" section.

Recovery from the switch(boot)# Prompt

To recover a system image using the kickstart image for a switch with a single supervisor module, follow these steps:

1. Change to configuration mode.

```
switch(boot) #config t
```

```
switch(boot) (config)#
```

2. Follow this step if you entered the **init system** command. Otherwise, skip to next step.

a. Enter the **ip default-gateway** command to configure the IP address of the default gateway.

```
switch(boot) (config)#ip default-gateway 209.165.200.226
```

b. Configure the IP address of the mgmt0 interface.

```
switch(boot) (config)#interface mgmt 0
```

```
switch(boot) (config-if)#ip address 209.165.200.227 255.255.255.0
```

3. Enter the **no shutdown** command to enable the mgmt0 interface on the switch.

```
switch(boot) (config-mgmt0)# no shutdown
```

4. Enter **end** to exit to EXEC mode.

```
switch(boot) (config-mgmt0)# end
```

5. If you believe there are file system problems, issue the **init system check-filesystem** command. As of Cisco MDS SAN-OS Release 2.1(1a), this command checks all internal file systems and fixes any errors that are encountered. This command takes considerable time to complete.

```
switch(boot)# init system check-filesystem
```

6. Copy the system image from the required TFTP server.

```
switch(boot)# copy tftp://172.16.10.100/system-image1 bootflash:system-image1
```

7. Copy the kickstart image from the required TFTP server.

```
switch(boot)# copy tftp://172.16.10.100/kickstart-image1 bootflash:kickstart-image1
```

8. Verify that the system and kickstart image files are copied to your bootflash: file system.

```
switch(boot)# dir bootflash:
```

```
  46080      Nov 11 21:48:55 2008  lost+found/
```

```
14753280    Nov 11 21:39:49 2008  kickstart-image1
```

```
78473925    Nov 11 21:37:12 2008  system-image1
```

```
Usage for bootflash://sup-local
```

```
 107465728 bytes used
```

```
  78619648 bytes free
```

```
 186085376 bytes total
```


9. Load the system image from the bootflash: files system.

```
switch(boot)# load bootflash:system-image1

Uncompressing system image: bootflash:/system-image1

CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC

Would you like to enter the initial configuration mode? (yes/no): yes
```

 **Note:** If you enter no, you will return to the switch# login prompt, and you must manually configure the switch.

10. Log in to the switch using the password configured in Step 9.

```
switch login:admin

Password:

Cisco Storage Area Networking Operating System (SAN-OS) Software

TAC support: http://www.cisco.com/tac

Copyright (c) 2002-2008, Cisco Systems, Inc. All rights reserved.

The copyrights to certain works contained herein are owned by

other third parties and are used and distributed under license.

Some parts of this software may be covered under the GNU Public

License or the GNU Lesser General Public License. A copy of

each such license is available at

http://www.gnu.org/licenses/gpl.html and

http://www.gnu.org/licenses/lgpl.html

switch#
```

11. Configure the boot variable.

```
switch #config t

switch(config)#boot kickstart bootflash:kickstart-image1

switch(config)#boot system bootflash:system-image1

switch(config)#end

switch#
```

12. Save the configuration.

```
switch# copy running-config startup-config

[#####] 100%
```

```
switch#
```

Recovery for Switches with Dual Supervisor Modules


This section describes how to recover when one or both supervisor modules in a dual supervisor switch have corrupted bootflash.

Recovering One Supervisor Module with Corrupted Bootflash

If one supervisor module has functioning bootflash and the other has corrupted bootflash, follow these steps:

1. Boot the functioning supervisor module and log on to the switch.
2. At the switch# prompt on the booted supervisor module, issue the **reload module slot force-dnld** command, where slot is the slot number of the supervisor module with the corrupted bootflash.

The supervisor module with the corrupted bootflash performs a netboot and checks the bootflash for corruption. When the bootup scripts discover that the bootflash is corrupted, it generates an **init system** command, which fixes the corrupt bootflash. The supervisor boots as the HA standby.

 **Caution:** If your system has an active supervisor module currently running, you must issue the **system standby manual-boot** command in EXEC mode on the active supervisor module before issuing the **init system** command on the standby supervisor module to avoid corrupting the internal bootflash. After the **init system** command completes on the standby supervisor module, issue the **system no standby manual-boot** command in EXEC mode on the active supervisor module.


Recovering Both Supervisor Modules With Corrupted Bootflash


If both supervisor modules have corrupted bootflash, follow these steps:

1. Boot the switch and press the **Esc** key after the BIOS memory test to interrupt the boot loader.

Press **Esc** immediately after you see the following message:

```
00000589K Low Memory Passed
00000000K Ext Memory Passed
Hit ^C if you want to run SETUP....
Wait.....
If you wait too long, you will skip the boot loader phase and enter the kickstart phase.
You see the loader> prompt.
```

 **Caution:** The loader> prompt is different from the regular switch# or switch(boot)# prompt. The CLI command completion feature does not work at this prompt and may result in undesired errors. You must type the command exactly as you want the command to appear.

 **Note:** Use the **help** command at the loader> prompt to display a list of commands available at this prompt or to obtain more information about a specific command in that list.

2. Specify the local IP address and the subnet mask for the switch.

```
loader> ip address 172.16.1.2 255.255.255.0
```


Cisco_MDS_SanOS_Troubleshooting_Guide_--_Troubleshooting_Installs,_Upgrades,_and_Reboots

Found Intel EtherExpressPro100 82559ER at 0xe800, ROM address 0xc000

Probing...[Intel EtherExpressPro100 82559ER]Ethernet addr: 00:05:30:00:52:27

Address: 172.16.1.2

Netmask: 255.255.255.0

Server: 0.0.0.0

Gateway: 0.0.0.0

3. Specify the IP address of the default gateway.

```
loader> ip default-gateway 172.16.1.1
```

Address: 172.16.1.2

Netmask: 255.255.255.0

Server: 0.0.0.0

Gateway: 172.16.1.1

4. Boot the kickstart image file from the required server.

```
loader> boot tftp://172.16.10.100/kickstart-latest
```

Address: 172.16.1.2

Netmask: 255.255.255.0

Server: 172.16.10.100

Gateway: 172.16.1.1

Booting: /kick-282 console=ttyS0,9600n8nn quiet loader_ver= "2.1(2)"....

.....Image verification OK

Starting kernel...

INIT: version 2.78 booting

Checking all filesystems..... done.

Loading system software

INIT: Sending processes the TERM signal

Sending all processes the TERM signal... done.

Sending all processes the KILL signal... done.

Entering single-user mode...


INIT: Going single user

```
INIT: Sending processes the TERM signal
```

```
switch(boot)#
```

The switch(boot)# prompt indicates that you have a usable kickstart image.

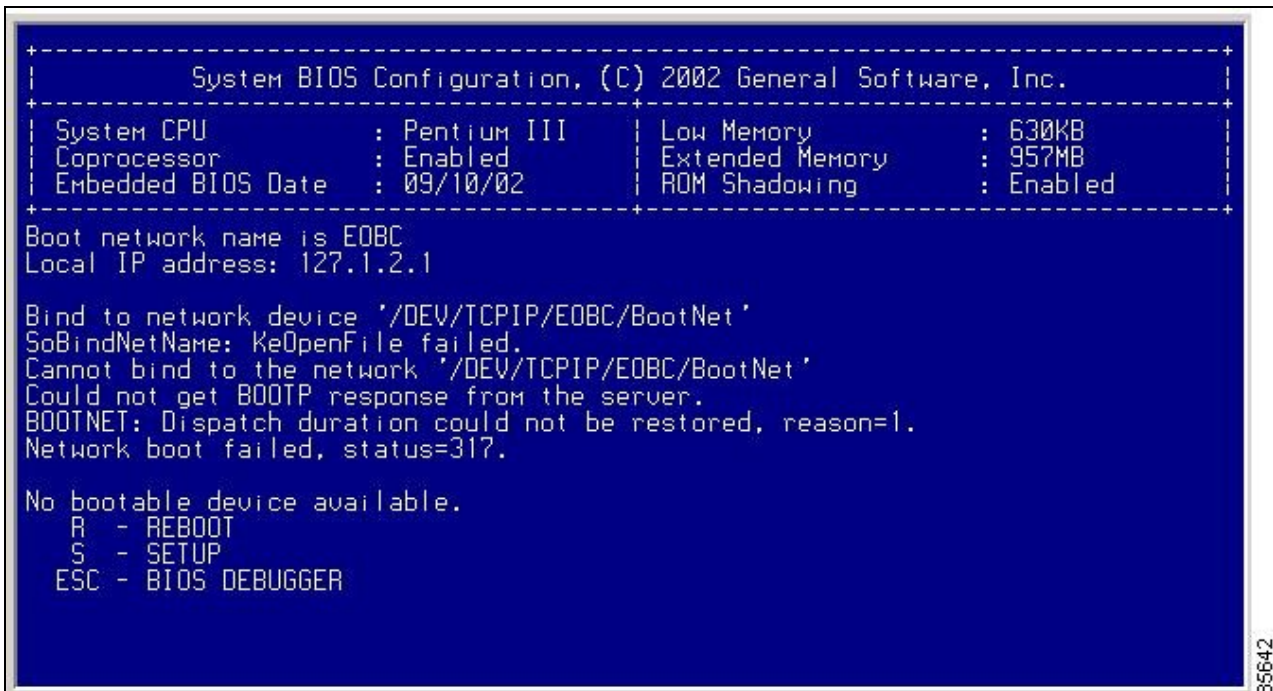
- Issue the **init-system** command to repartition and format the bootflash.
- Perform the procedure specified in the "Recovery from the switch(boot)# Prompt" section.
- Perform the procedure specified in the "Recovering One Supervisor Module With Corrupted Bootflash" section to recover the other supervisor module.

 **Note:** If you do not issue the **reload module** command when a boot failure has occurred, the active supervisor module automatically reloads the standby supervisor module within 3 to 6 minutes after the failure.

Recognizing Error States

If you see one or both of the error messages displayed in Figure 2-7 or Figure 2-8, follow the procedure specified in the "Recovery Using BIOS Setup for Supervisor-1" section.

Figure 2-7 Error State if Powered On and Ctrl-C Is Entered

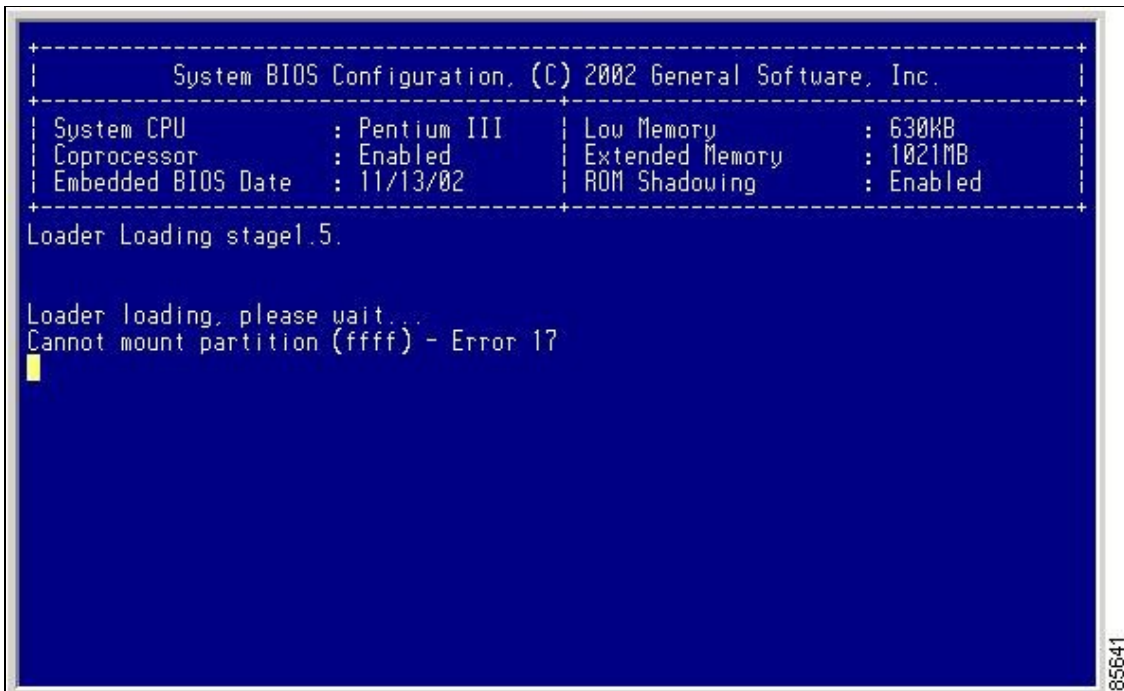


```
+-----+
|           System BIOS Configuration, (C) 2002 General Software, Inc.           |
+-----+
| System CPU       : Pentium III           | Low Memory       : 630KB          |
| Coprocessor     : Enabled                | Extended Memory  : 957MB          |
| Embedded BIOS Date : 09/10/02          | ROM Shadowing   : Enabled        |
+-----+
Boot network name is EOBC
Local IP address: 127.1.2.1

Bind to network device '/DEV/TCPIP/EOBC/BootNet'
SoBindNetName: KeOpenFile failed.
Cannot bind to the network '/DEV/TCPIP/EOBC/BootNet'
Could not get BOOTP response from the server.
BOOTNET: Dispatch duration could not be restored, reason=1.
Network boot failed, status=317.

No bootable device available.
R - REBOOT
S - SETUP
ESC - BIOS DEBUGGER
```

Figure 2-8 Error State if Powered On and Esc Is Pressed



Switch or Process Resets

When a recoverable or nonrecoverable error occurs, the switch or a process on the switch may reset.

Symptom The switch or a process on the switch reset. See the table below for the scenarios and solution:

Problem	Possible Cause	Solution
The switch or a process on the switch resets.	A recoverable error occurred on the system or on a process in the system.	Cisco SAN-OS automatically recovered from the problem. See the "Recoverable System Restarts" section and the "Switch or Process Resets" section.
	A nonrecoverable error occurred on the system.	Cisco SAN-OS cannot recover automatically from the problem. See the "Unrecoverable System Restarts" section to determine the cause.
	A clock module failed.	Verify that a clock module failed. See the "Troubleshooting Clock Module Issues" section. Replace the failed clock module during the next maintenance window.

Recoverable System Restarts

Every process restart generates a syslog message and a Call Home event. Even if the event does not affect service, you should identify and resolve the condition immediately because future occurrences could cause service interruption.

To respond to a recoverable system restart, follow these steps:

Cisco_MDS_SanOS_Troubleshooting_Guide_--_Troubleshooting_Installs,_Upgrades,_and_Reboots

1. Enter the following command to check the syslog file to see which process restarted and why it restarted:

```
switch# show log logfile | include error
```

For information about the meaning of each message, refer to the *Cisco MDS 9000 Family System Messages Reference*.

The system output resembles the following example:

```
Sep 10 23:31:31 dot-6 % LOG_SYSMGR-3-SERVICE_TERMINATED: Service "sensor" (PID 704) has finished with error code SYSMGR_EXITCODE_SY.
```

```
switch# show logging logfile | include fail
```

```
Jan 27 04:08:42 88 %LOG_DAEMON-3-SYSTEM_MSG: bind() fd 4, family 2, port 123, address 0.0.0.0, in_classd=0 flags=1 fails: Address already in use
```

```
Jan 27 04:08:42 88 %LOG_DAEMON-3-SYSTEM_MSG: bind() fd 4, family 2, port 123, address 127.0.0.1, in_classd=0 flags=0 fails: Address already in use
```

```
Jan 27 04:08:42 88 %LOG_DAEMON-3-SYSTEM_MSG: bind() fd 4, family 2, port 123, address 127.1.1.1, in_classd=0 flags=1 fails: Address already in use
```

```
Jan 27 04:08:42 88 %LOG_DAEMON-3-SYSTEM_MSG: bind() fd 4, family 2, port 123, address 172.22.93.88, in_classd=0 flags=1 fails: Address already in use
```

```
Jan 27 23:18:59 88 % LOG_PORT-5-IF_DOWN: Interface fc1/13 is down (Link failure or not-connected)
```

```
Jan 27 23:18:59 88 % LOG_PORT-5-IF_DOWN: Interface fc1/14 is down (Link failure or not-connected)
```

```
Jan 28 00:55:12 88 % LOG_PORT-5-IF_DOWN: Interface fc1/1 is down (Link failure or not-connected)
```

```
Jan 28 00:58:06 88 % LOG_ZONE-2-ZS_MERGE_FAILED: Zone merge failure, Isolating port fc1/1 (VSAN 100)
```

```
Jan 28 00:58:44 88 % LOG_ZONE-2-ZS_MERGE_FAILED: Zone merge failure, Isolating port fc1/1 (VSAN 100)
```

```
Jan 28 03:26:38 88 % LOG_ZONE-2-ZS_MERGE_FAILED: Zone merge failure, Isolating port fc1/1 (VSAN 100)
```

```
Jan 29 19:01:34 88 % LOG_PORT-5-IF_DOWN: Interface fc1/1 is down (Link failure o
```

r not-connected)


switch#

1. Enter the following command to identify the processes that are running and the status of each process.

```
switch# show processes
```

The following codes are used in the system output for the State (process state):

- D = uninterruptible sleep (usually I/O)
- R = runnable (on run queue)
- S = sleeping
- T = traced or stopped
- Z = defunct ("zombie") process
- NR = notrunning
- ER = should be running but currently notrunning

 **Note:** ER usually is the state a process enters if it has been restarted too many times and has been detected as faulty by the system and disabled.

The system output resembles the following example. (The output has been abbreviated to be more concise.)

PID	State	PC	Start_cnt	TTY	Process
1	S	2ab8e33e	1	-	init
2	S	0	1	-	keventd
3	S	0	1	-	ksoftirqd_CPU0
4	S	0	1	-	kswapd
5	S	0	1	-	bdflush
6	S	0	1	-	kupdated
71	S	0	1	-	kjournald
136	S	0	1	-	kjournald
140	S	0	1	-	kjournald
431	S	2abe333e	1	-	httpd

```

443      S  2abfd33e          1    -  xinetd
446      S  2ac1e33e          1    -  sysmgr
452      S  2abe91a2          1    -  httpd
453      S  2abe91a2          1    -  httpd
456      S  2ac73419          1   S0  vsh
469      S  2abe91a2          1    -  httpd
470      S  2abe91a2          1    -  httpd
    
```

1. Enter the following command to show the processes that have had abnormal exits and to show if there is a stack-trace or core dump:

```
switch# show process log
```

Process	PID	Normal-exit	Stack-trace	Core	Log-create-time
ntp	919	N	N	N	Jan 27 04:08
snsn	972	N	Y	N	Jan 24 20:50

1. Enter the following command to show detailed information about a specific process that has restarted:

```
switch# show processes log pid 898
```

Service: idehsd

Description: ide hotswap handler Daemon

Started at Mon Sep 16 14:56:04 2002 (390923 us)

Stopped at Thu Sep 19 14:18:42 2002 (639239 us)

Uptime: 2 days 23 hours 22 minutes 22 seconds

Start type: SRV_OPTION_RESTART_STATELESS (23)

Death reason: SYSMGR_DEATH_REASON_FAILURE_SIGTERM (3)

Exit code: signal 15 (no core)

CWD: /var/sysmgr/work

Virtual Memory:

CODE 08048000 - 0804D660

DATA 0804E660 - 0804E824

BRK 0804E9A0 - 08050000

STACK 7FFFFFFD10

Register Set:

```

EBX 00000003      ECX 0804E994      EDX 00000008
ESI 00000005      EDI 7FFFFFFC9C     EBP 7FFFFFFCAC
EAX 00000008      XDS 0000002B      XES 0000002B
EAX 00000003 (orig) EIP 2ABF5EF4      XCS 00000023
EFL 00000246      ESP 7FFFFFFC5C     XSS 0000002B

```

Stack: 128 bytes. ESP 7FFFFFFC5C, TOP 7FFFFFFD10

```

0x7FFFFFFC5C: 0804F990 0804C416 00000003 0804E994 .....
0x7FFFFFFC6C: 00000008 0804BF95 2AC451E0 2AAC24A4 .....Q.*.$.*
0x7FFFFFFC7C: 7FFFFFFD14 2AC2C581 0804E6BC 7FFFFFFCA8 .....*.....
0x7FFFFFFC8C: 7FFFFFFC94 00000003 00000001 00000003 .....
0x7FFFFFFC9C: 00000001 00000000 00000068 00000000 .....h.....
0x7FFFFFFCAC: 7FFFFFFCE8 2AB4F819 00000001 7FFFFFFD14 .....*.....
0x7FFFFFFCBC: 7FFFFFFD1C 0804C470 00000000 7FFFFFFCE8 ....p.....
0x7FFFFFFCCC: 2AB4F7E9 2AAC1F00 00000001 08048A2C ...*...*.....,....

```

PID: 898

SAP: 0

UUID: 0

switch#

1. Enter the following command to determine if the restart recently occurred:

```
switch# show system uptime
```

Start Time: Fri Sep 13 12:38:39 2002

Up Time: 0 days, 1 hours, 16 minutes, 22 seconds

To determine if the restart is repetitive or a one-time occurrence, compare the length of time that the system has been up with the timestamp of each restart.

1. Enter the following command to view the core files:

```
switch# show cores
```

Module-num	Process-name	PID	Core-create-time
5	fspf	1524	Jan 9 03:11
6	fcc	919	Jan 9 03:09
8	acltcam	285	Jan 9 03:09
8	fib	283	Jan 9 03:08

The output shows all cores that are presently available for upload from the active supervisor. The module-num column shows the slot number on which the core was generated. In the previous example, an FSPF core was generated on the active supervisor module in slot 5. An FCC core was generated on the standby supervisory module in slot 6. Core dumps generated on the module in slot 8 include ACLTCAM and FIB.

To copy the FSPF core dump in this example to a TFTP server with the IP address 1.1.1.1, enter the following command:

```
switch# copy core://5/1524 tftp://1.1.1.1/abcd
```

The following command displays the file named zone_server_log.889 in the log directory:

```
switch# show pro log pid 1473
=====
Service: ips
Description: IPS Manager

Started at Tue Jan  8 17:07:42 1980 (757583 us)
Stopped at Thu Jan 10 06:16:45 1980 (83451 us)
Uptime: 1 days 13 hours 9 minutes 9 seconds

Start type: SRV_OPTION_RESTART_STATELESS (23)
Death reason: SYSMGR_DEATH_REASON_FAILURE_SIGNAL (2)
Exit code: signal 6 (core dumped)
CWD: /var/sysmgr/work

Virtual Memory:
```


Cisco_MDS_SanOS_Troubleshooting_Guide_--_Troubleshooting_Installs,_Upgrades,_and_Reboots

CODE 08048000 - 080FB060
DATA 080FC060 - 080FCBA8
BRK 081795C0 - 081EC000
STACK 7FFFFCF0
TOTAL 20952 KB

Register Set:

EBX 000005C1 ECX 00000006 EDX 2AD721E0
ESI 2AD701A8 EDI 08109308 EBP 7FFFF2EC
EAX 00000000 XDS 0000002B XES 0000002B
EAX 00000025 (orig) EIP 2AC8CC71 XCS 00000023
EFL 00000207 ESP 7FFFF2C0 XSS 0000002B

Stack: 2608 bytes. ESP 7FFFF2C0, TOP 7FFFFCF0

0x7FFFF2C0: 2AC8C944 000005C1 00000006 2AC735E2 D..*.....5.*
0x7FFFF2D0: 2AC8C92C 2AD721E0 2AAB76F0 00000000 ,...*!.*.v.*....
0x7FFFF2E0: 7FFFF320 2AC8C920 2AC513F8 7FFFF42C*...*,...
0x7FFFF2F0: 2AC8E0BB 00000006 7FFFF320 00000000 ...*....
0x7FFFF300: 2AC8DFF8 2AD721E0 08109308 2AC65AFC ...*!.*.....Z.*
0x7FFFF310: 00000393 2AC6A49C 2AC621CC 2AC513F8*!.*...*
0x7FFFF320: 00000020 00000000 00000000 00000000
0x7FFFF330: 00000000 00000000 00000000 00000000
0x7FFFF340: 00000000 00000000 00000000 00000000
0x7FFFF350: 00000000 00000000 00000000 00000000
0x7FFFF360: 00000000 00000000 00000000 00000000
0x7FFFF370: 00000000 00000000 00000000 00000000
0x7FFFF380: 00000000 00000000 00000000 00000000
0x7FFFF390: 00000000 00000000 00000000 00000000
0x7FFFF3A0: 00000002 7FFFF3F4 2AAB752D 2AC5154C .

... output abbreviated ...

Stack: 128 bytes. ESP 7FFFF830, TOP 7FFFFCD0

1. Enter the following command to configure the switch to use TFTP to send the core dump to a TFTP server:

```
system cores tftp:[//servername][/path]
```

This command causes the switch to enable the automatic copy of core files to a TFTP server. For example, the following command sends the core files to the TFTP server with the IP address 10.1.1.1:

```
switch(config)# system cores tftp://10.1.1.1/cores
```

The following conditions apply:

- The core files are copied every 4 minutes. This time interval is not configurable.
- The copy of a specific core file to a TFTP server can be manually triggered, using the command `copy core://module#/pid# tftp://tftp_ip_address/file_name`.
- The maximum number of times a process can be restarted is part of the HA policy for any process. (This parameter is not configurable.) If the process restarts more than the maximum number of times, the older core files are overwritten.
- The maximum number of core files that can be saved for any process is part of the HA policy for any process. (This parameter is not configurable, and it is set to three.)

1. Determine the cause and resolution for the restart condition by contacting your customer support representative and asking the representative to review your core dump.

See also the "Troubleshooting Supervisor Issues" section on page 4-14 or the "Troubleshooting Switching and Services Modules" section on page 4-21.

Unrecoverable System Restarts

An unrecoverable system restart might occur in the following cases:

- A critical process fails and is not restartable.
- A process restarts more times than is allowed by the system configuration.
- A process restarts more frequently than is allowed by the system configuration.

The effect of a process reset is determined by the policy configured for each process. Unrecoverable reset may cause loss of functionality, restart of the active supervisor, a supervisor switchover, or restart of the switch.

To respond to an unrecoverable reset, see the "Troubleshooting Cisco SAN-OS Software System Reboots" section.

The **show system reset-reason** CLI command displays the following information:

- In a Cisco MDS 9500 Series switch, the last four reset-reason codes for the supervisor module in slot 5 and slot 6 are displayed. If either supervisor module is absent, the reset-reason codes for that

supervisor module are not displayed.

- In a Cisco MDS 9200 Series switch, the last four reset-reason codes for the supervisor module in slot 1 are displayed.
- The **show system reset-reason module number** command displays the last four reset-reason codes for a specific module in a given slot. If a module is absent, then the reset-reason codes for that module are not displayed.
- The overall history of when and why expected and unexpected reloads occur.
- Timestamp of when the reset or reload occurred
- Reason for the reset or reload of a module
- The service that caused the reset or reload (not always available)
- The software version that was running at the time of the reset or reload

Example:

```
switch# show system reset-reason module 5

----- reset reason for module 5 -----

1) At 224801 usecs after Fri Jan 21 16:36:40 2005

Reason: Reset Requested by CLI command reload

Service:

Version: 2.1(2)

2) At 922828 usecs after Fri Jan 21 16:02:48 2005

Reason: Reset Requested by CLI command reload

Service:

Version: 2.1(2)

3) At 318034 usecs after Fri Jan 21 14:03:36 2005

Reason: Reset Requested by CLI command reload

Service:

Version:2.1(2)

4) At 255842 usecs after Wed Jan 19 00:07:49 2005

Reason: Reset Requested by CLI command reload

Service:

Version: 2.1(2)
```

Recovering the Administrator Password

You can access the switch if you forget the administrator password by following the directions in the below table. **Symptom** You forgot the administrator password for accessing a switch.


Problem	Solution
You forgot the administrator password for accessing a Cisco MDS 9000 Family switch.	You can recover the password using a local console connection. For the latest instructions on password recovery, refer to the <i>Cisco MDS 9000 CLI Family Configuration Guide</i> at the following website: http://cisco.com/en/US/products/ps5989/products_installation_and_configuration_guides_list.html

If you can access Device Manager, recover the administrator password by following these steps:

1. Create a text file on the TFTP server containing the desired user name and password:

```
"username admin password 0 admin123"
```

1. Choose **Admin > Copy Configuration** to copy the file from the TFTP server to the running configuration on the switch.

 **Note:** The clear text password "admin123" will be copied over the existing password and encrypted in the running configuration.

1. Choose **Device > Command Line Interface** to log into the switch and verify the new password.

1. Choose **Admin > Save Configuration** to save the running configuration to the startup configuration.

Miscellaneous Software Image Issues

This section includes software image issues reported by the relevant release notes.

All Ports Down Because of System Health Failure

Symptom Console reports all ports on a module are down because of a system health failure. The table describes the scenarios and solution:

Symptom	Possible Cause	Solution
The system console reports that the module's ports are down because of a system health failure.	An incorrect process on the Cisco MDS 9000 modules might have been reinitialized from an error recovery mechanism, leaving the module in an unusable state. In some cases, the module may reboot.	Downgrade to a Cisco SAN-OS Release 2.0(x) version supported by your OSM.
		Upgrade to Cisco SAN-OS Release 2.1.2 or 2.1(1b). Resetting the module will clear the problem, but the problem could reoccur unless you are using a SAN-OS version with the bug fix.

Switch Reboots after FCIP Reload

Symptom Switch rebooted after FCIP module was reloaded, upgraded, or downgraded. The table describes the scenarios and solution:

Symptom	Possible Cause	Solution
Switch rebooted after FCIP module was reloaded, upgraded, or downgraded.	If an IPS module with operational FCIP PortChannels is reloaded, upgraded, or downgraded, the supervisor module might reload and cause the system to reboot.	Before reloading, upgrading, or downgrading an IPS module, shut down all FCIP PortChannels on the module.

FCIP Link Fails to Come Up

Symptom A newly configured FCIP link may fail to come up when running on an MPS-14/2 module. The table describes the scenarios and solution:

Symptom	Possible Cause	Solution
A newly configured FCIP link may fail to come up when running on an MPS-14/2 module.	This symptom may occur following an upgrade from Cisco MDS SAN-OS Release 2.0(1b) to Release 2.0(3) and following the configuration of a new FCIP link.	Reload the MPS-14/2 module using the reload module module-number command, where module-number is a specific module.

Cannot Create, Modify, or Delete Admin Role

Symptom Cannot create, modify, or delete the admin role. The table describes the scenarios and solution:

Symptom	Possible Cause	Solution
Cannot create, modify, or delete the admin role.	After upgrading to Cisco SAN-OS Release 2.0, you cannot create, modify, or delete the admin role.	Create the admin role before upgrading to Cisco SAN-OS Release 2.0.

FC IDs Change after Link Reset

Symptom FC IDs change after a link resets. The table describes the scenarios and solution:

Symptom	Possible Cause	Solution

FC IDs change after a link resets.	Following an upgrade from Cisco SAN-OS Release 1.1 to Cisco SAN-OS Release 1.3 or later, with persistent FC ID enabled, the FC IDs for the storage arrays might change after a link flap.	Reconfigure the FC IDs as necessary.
------------------------------------	---	--------------------------------------

Switch Displays Wrong User

Symptom Switch displays the wrong user with the show running-config CLI command. The table describes the scenarios and solution:

Symptom	Possible Cause	Solution
Switch displays the wrong user with the show running-config CLI command.	When you perform a nondisruptive upgrade from Cisco SAN-OS Release 1.3(x) to Cisco SAN-OS Release 2.0(x) and then issue the show running-config command, the switch displays the wrong user. The user shown after the nondisruptive upgrade is different from the user shown when you issue the show user-account command.	Recreate the user.

Back to Main Page: [Cisco MDS SAN-OS Troubleshooting Guide](#)
