Troubleshooting Installations, Upgrades, and Reboots

- About Upgrades and Reboots, on page 1
- Upgrade and Reboot Checklist, on page 1
- Verifying Software Upgrades, on page 2
- Verifying a Nondisruptive Upgrade, on page 2
- Troubleshooting Software Upgrades and Downgrades, on page 3
- Troubleshooting Software System Reboots, on page 4
- Changing the Administrator Password, on page 22

About Upgrades and Reboots

Upgrades and reboots are ongoing network maintenance activities. You should try to minimize the risk of disrupting the network when performing these operations in production environments and to know how to recover quickly when something does go wrong.

Note This publication uses the term upgrade to refer to both Cisco NX-OS upgrades and downgrades.

Upgrade and Reboot Checklist

Use the following checklist to prepare for an upgrade or reboot:

Checklist	Done
Read the Release Notes for the release to which you are upgrading or downgrading.	
Ensure that an FTP or TFTP server is available to download the software image.	
Copy the new image onto your supervisor modules in bootflash: or slot0:.	
Use the **show install all impact** command to verify that the new image is healthy and the impact that the new load will have on any hardware with regard to compatibility. Check for compatibility.	

Checklist	Done
Copy the startup-config file to a snapshot configuration in NVRAM. This step creates a backup copy of the startup configuration file.	
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 network.	

After you have completed the checklist, you are ready to upgrade or reboot the systems in your network.

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

Note Up to 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 by entering the **show logging nvram** command.

Verifying Software Upgrades

You can use the **show install all status** command to watch the progress of your software upgrade or to view the ongoing **install all** command or the log of the last installed **install all** command from a console, SSH, or Telnet session. This command shows the **install all** output on both the active and standby supervisor module even if you are not connected to the console terminal.

Verifying a Nondisruptive Upgrade

When you initiate a nondisruptive upgrade, Cisco NX-OS notifies all services that an upgrade is about to start and determines whether the upgrade can proceed. If a service cannot allow the upgrade to proceed, the service aborts the upgrade, and you are 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.<---prompt
 failure-reason
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: "xxx" failed to respond within the given time period.
```

If a failure occurs for any reason (such as a save runtime state failure or a module upgrade failure) after the upgrade is in progress, the device reboots disruptively because the changes cannot be rolled back. In such cases, the upgrade has failed.

If you need further assistance to determine why an upgrade is unsuccessful, you should collect the details from the **show tech-support** [**issu**] command output and the console output from the installation, if available, before you contact your technical support representative.

Troubleshooting Software Upgrades and Downgrades

Software Upgrade Ends with Error

Problem	Possible Cause	Solution
The upgrade ends with an error	The standby supervisor module bootflash: file system does not have sufficient space to accept the updated image.	Use the **delete** command to remove unnecessary files from the file system.
	The **install all** command is entered 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.
	The system experienced a power disruption while the upgrade was in progress.	Restart the installation.
	An incorrect software image path was specified.	Specify the entire path for the remote location accurately.
	Another upgrade is already in progress.	Verify the state of the system at every stage and restart the upgrade after 10 seconds. If you restart the upgrade within 10 seconds, the command is rejected. An error message displays, indicating that an upgrade is currently in progress.
	A module failed to upgrade.	Restart the upgrade or use the **install module** command to upgrade the failed module.

Upgrading the Cisco NX-OS Software

You can perform an automated software upgrade on any system from the CLI.

The image filename begins with "nxos" [beginning with Cisco NX-OS Release 7.0(3)I2(1)] or "n9000" (for example, nxos.7.0.3.I2.1.bin or n9000-dk9.7.0.3.I1.1.bin).

Before you begin

Log into the system through the console, Telnet, or SSH port of the active supervisor.

Create a backup of your existing configuration file, if required.

SUMMARY STEPS

1. **install all** [**nxos bootflash:***filename*]
2. **show module**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**install all** [**nxos bootflash:***filename*]	Performs the upgrade. **Note** If the configuration meets all guidelines when the **install all** command is used, all modules (supervisor and switching) are upgraded. **Note** If you enter the **install all** command without specifying a filename, the command performs a compatibility check, notifies you of the modules that will be upgraded, and confirms that you want to continue with the installation. If you choose to proceed, it installs the NXOS software image that is currently running on the switch and upgrades the BIOS of various modules from the running image if required.
Step 2	**show module**	Exits the system console and opens a new terminal session to view the upgraded supervisor module.

Troubleshooting Software System Reboots

Power-On or Switch Reboot Hangs

Problem	Possible Cause	Solution
A power-on or switch reboot hangs for a dual supervisor configuration	The bootflash is corrupted.	See Corrupted Bootflash Recovery, on page 5.
	The BIOS is corrupted.	Replace this module. Contact your customer support representative to return the failed module.
	The nx-os image is corrupted.	Power cycle the switch if required and press **Ctrl-C** when the switch displays the "Loading Boot Loader" message to interrupt the boot process at the >loader prompt.
	Boot parameters are incorrect.	Verify and correct the boot parameters and reboot.

Corrupted Bootflash Recovery

All device 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 system boot goes through the following sequence:

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

If the nx-os image on your system is corrupted and you cannot proceed (error state), you can interrupt the system 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.

Caution 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 sequence goes through three phases between the time that you turn on the system and the time that the system prompt appears on your terminal—BIOS, boot loader, and nx-os image. The following table describes the steps in the recovery interruption process.

Table 1: Recovery Interruption

Phase	Normal Prompt (appears at the end of each phase)	Recovery Prompt (appears when the system cannot progress to the next phase)	Description
BIOS	loader>	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 nx-os	loader>	The boot loader uncompresses the loaded software to boot an image using its filename as a reference. The image is made available through bootflash. When the memory test is over, press **Esc** to enter the boot loader prompt.

Phase	Normal Prompt (appears at the end of each phase)	Recovery Prompt (appears when the system cannot progress to the next phase)	Description
nx-os image	Uncompressing system	switch(boot)#	When the boot loader phase is over, press **Ctrl-]** (Control key plus right bracket key) to enter the switch(boot)# prompt. Depending on your Telnet client, these keys might be reserved, and you might need to remap the keystroke. See the documentation provided by your Telnet client. If the corruption causes the console to stop at this prompt, copy the nx-os image and reboot the system. The nx-os image then loads the configuration file of the last saved running configuration and returns a switch login prompt.

Recovery from the loader> Prompt

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.

Before you begin

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# or switch(boot)# prompt. The CLI command completion feature does not work at the loader> prompt and might result in undesired errors. You must type the command exactly as you want the command to appear.

If you boot over TFTP from the loader> prompt, you must supply the full path to the image on the remote server.

SUMMARY STEPS

1. loader> **set ip** *ip-address*
2. loader> **set gw** *gw-address*
3. loader> **cmdline recoverymode=1**
4. loader> **boot tftp:** *tftp-path*
5. switch(boot)# **init system**
6. switch(boot)# **load-nxos**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	loader> **set ip** *ip-address* **Example:** `loader> set ip 172.21.55.213 255.255.255.224`	Specifies the local IP address and the subnet mask for the system.
Step 2	loader> **set gw** *gw-address* **Example:** `loader> set gw 172.21.55.193`	Specifies the IP address of the default gateway.
Step 3	loader> **cmdline recoverymode=1** **Example:** `loader> cmdline recoverymode=1`	Configures the boot process to stop at the switch(boot)# prompt.
Step 4	loader> **boot tftp:** *tftp-path* **Example:** `loader> boot tftp://172.28.255.18/tftpboot/n9000-dk9.6.1.2.I1.1.bin`	Boots the nx-os image file from the required server. The switch(boot)# prompt indicates that you have a usable nx-os image.
Step 5	switch(boot)# **init system** **Example:** `switch(boot)# init system`	Enters the nx-os system. **Caution** Be sure that you have made a backup of the configuration files before you enter this command.
Step 6	switch(boot)# **load-nxos** **Example:** `switch(boot)# load-nxos`	Completes the upload of the nx-os image file.

Example

This example shows how to configure the local IP address and the subnet mask for the system:

```
loader> set ip 172.21.55.213 255.255.255.224
set ip 172.21.55.213 255.255.255.224
Correct - ip addr is 172.21.55.213, mask is 255.255.255.224
Found Intel 82546GB [2:9.0] at 0xe040, ROM address 0xf980
Probing...[Intel 82546GB]
Management interface
Link UP in 1000/full mode
Ethernet addr: 00:1B:54:C1:28:60
Address: 172.21.55.213
Netmask: 255.255.255.224
Server: 0.0.0.0
Gateway: 172.21.55.193
```

This example shows how to configure the IP address of the default gateway:

```
loader> set gw 172.21.55.193
Correct gateway addr 172.21.55.193
Address: 172.21.55.213
Netmask: 255.255.255.224
Server: 0.0.0.0
Gateway: 172.21.55.193
```

This example shows how to boot the nx-os image from the server:

```
loader> boot tftp://172.28.255.18/tftpboot/n9000-dk9.6.1.2.I1.1.bin
 Address: 172.21.55.213
 Netmask: 255.255.255.224
 Server: 172.28.255.18
 Gateway: 172.21.55.193
  Filesystem type is tftp, using whole disk
 Booting: /tftpboot/n9000-dk9.6.1.2.I1.1.gbin console=ttyS0,9600n8nn quiet loader
 _ver="3.17.0"....
 ..............................................................................Im
 age verification OK

 Starting kernel...
 INIT: version 2.85 booting
 Checking all filesystems..r.r.r.. done.
 Setting kernel variables: sysctlnet.ipv4.ip_forward = 0
 net.ipv4.ip_default_ttl = 64
 net.ipv4.ip_no_pmtu_disc = 1
 .
 Setting the System Clock using the Hardware Clock as reference...System Clock set. Local
time: Wed Oct  1
 11:20:11 PST 2013
 WARNING: image sync is going to be disabled after a loader netboot
 Loading system software
 No system image Unexporting directories for NFS kernel daemon...done.
 INIT: Sending processes the KILL signal
 Cisco Nexus Operating System (NX-OS) Software
 TAC support: http://www.cisco.com/tac
 Copyright (c) 2013, Cisco Systems, Inc. All rights reserved.
 The copyrights to certain works contained in this software are
 owned by other third parties and used and distributed under
 license. Certain components of this software are licensed under
 the GNU General Public License (GPL) version 2.0 or the GNU
 Lesser General Public License (LGPL) Version 2.1. A copy of each
 such license is available at
 http://www.opensource.org/licenses/gpl-2.0.php and
 http://www.opensource.org/licenses/lgpl-2.1.php
 switch(boot)#
```

System or Process Restarts

When a recoverable or nonrecoverable error occurs, the system or a process on the system might reset. This table lists possible causes and solutions.

Problem	Possible Cause	Solution
The system or a process on the system resets.	A recoverable error occurred on the system or on a process in the system.	The system has automatically recovered from the problem. See Recovering System Restarts, on page 9.
	A nonrecoverable error occurred on the system.	The system cannot recover automatically from the problem. See Recovering System Restarts, on page 9 to determine the cause.
	A clock module failed.	Verify that a clock module failed. Replace the failed clock module during the next maintenance window.

Recovering 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 a service interruption.

Note After following the steps, determine the cause and resolution for the restart condition by contacting your technical support representative and asking the representative to review your core dump.

Before you begin

The following conditions apply:

- The system automatically copies the core files to a TFTP server every 4 minutes. This time interval is not configurable.
- The copy of a specific core file to a TFTP server can be manually triggered by using the **copy core:***//module#/pid# tftp://tftp_ip_address/file_name* command.
- If a supervisor failover occurs, the cores might be in the secondary logflash rather than the primary logflash.
- The maximum number of times that a process can be restarted is part of the high-availability (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.)

SUMMARY STEPS

1. **show log | include error**
2. **show processes**
3. **show process log**
4. **show process log pid** *pid*

5. **show system uptime**
6. **show cores**
7. **copy core:**//*module#*/*pid#* **tftp:**//*tftp_ip_address*/*file_name*
8. **show processes log pid** *pid*
9. **system cores tftp:** *tftp-path*

DETAILED STEPS

Procedure

	Command or Action	Purpose

Step 1	**show log | include error**
	Example:
	`switch# show log logfile | include error`
	`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, ad`
	`dr 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, ad`
	`dr 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, ad`
	`dr 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, ad`
	`dr 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`
	`or not-connected)`
	`switch#`
		Displays the syslog file so you can see which process restarted and why it restarted.

	Command or Action	Purpose

Step 2	**show processes**
	Example:
	`switch# show processes`
	`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`
		Displays the processes that are running and the status of each process.
		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 = not running
		• ER = should be running but currently not running
		Note
		ER usually is the state that a process enters if it has been restarted too many times and has been detected as faulty by the system and disabled.

Step 3	**show process log**
	Example:
	`switch# show process log`
	`Process PID Normal-exit Stack-trace Core Log-create-time`
	`------- --- ----------- ----------- ---- ---------------`
	`ntp 919 N N N Jan 27 04:08`
	`snsm 972 N Y N Jan 24 20:50`
		Displays the processes that have had abnormal exits and if there is a stack-trace or core dump.

Step 4	**show process log pid** *pid*
	Example:
	`switch# show processes log pid 898`
	`Service: idehsd`
	`Description: ide hotswap handler Daemon`
	`Started at Mon Sep 16 14:56:04 2013 (390923 us)`
	`Stopped at Thu Sep 19 14:18:42 2013 (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`
		Displays detailed information about a specific process that has restarted.

	Command or Action	Purpose

	`BRK 0804E9A0 - 08050000`
	`STACK 7FFFFD10`
	`Register Set:`
	`EBX 00000003 ECX 0804E994 EDX 00000008`
	`ESI 00000005 EDI 7FFFFC9C EBP 7FFFFCAC`
	`EAX 00000008 XDS 0000002B XES 0000002B`
	`EAX 00000003 (orig) EIP 2ABF5EF4 XCS 00000023`
	`EFL 00000246 ESP 7FFFFC5C XSS 0000002B`
	`Stack: 128 bytes. ESP 7FFFFC5C, TOP 7FFFFD10`
	`0x7FFFFC5C: 0804F990 0804C416 00000003 0804E994 ................`
	`0x7FFFFC6C: 00000008 0804BF95 2AC451E0 2AAC24A4 .........Q.*.$.*`
	`0x7FFFFC7C: 7FFFFD14 2AC2C581 0804E6BC 7FFFFCA8 .......*........`
	`0x7FFFFC8C: 7FFFFC94 00000003 00000001 00000003 ................`
	`0x7FFFFC9C: 00000001 00000000 00000068 00000000 ........h.......`
	`0x7FFFFCAC: 7FFFFCE8 2AB4F819 00000001 7FFFFD14 .......*........`
	`0x7FFFFCBC: 7FFFFD1C 0804C470 00000000 7FFFFCE8 ....p...........`
	`0x7FFFFCCC: 2AB4F7E9 2AAC1F00 00000001 08048A2C ...*...*....,...`
	`PID: 898`
	`SAP: 0`
	`UUID: 0`
	`switch#`	

Step 5	**show system uptime**
	Example:
	`switch# show system uptime`
	`Start Time: Fri Sep 13 12:38:39 2013`
	`Up Time: 0 days, 1 hours, 16 minutes, 22 seconds`
		Displays if the restart recently occurred.
		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.

Step 6	**show cores**
	Example:
	`switch# show cores`
	`VDC Module Instance Process-name PID Date(Year-Month-Day Time)`
	`--- ------ -------- --------------- -------- -------------------------`
	`1 1 1 nginx 29017 2025-03-26 23:31:54`
		Displays all cores that are presently available for upload from the active supervisor.

Step 7	**copy core:**//*module#*/*pid#* **tftp:**//*tftp_ip_address*/*file_name* **Example:** `switch# copy core://1/29017 tftp://1.1.1.1/example`	Copies the FSPF core dump to a TFTP server with an IP address.
Step 8	**show processes log pid** *pid* **Example:**	Displays the file named zone_server_log.889 in the log directory,

Command or Action	Purpose
switch# show processes log pid 1473 ========== Service: ips Description: IPS Manager Started at Tue Jan 8 17:07:42 2013 (757583 us) Stopped at Thu Jan 10 06:16:45 2013 (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: 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 .	

	Command or Action	Purpose
	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	
Step 9	**system cores tftp:** *tftp-path* **Example:** `switch(config)# system cores tftp://10.1.1.1/cores`	Configures the system to use TFTP to send the core dump to a TFTP server. This command causes the system to enable the automatic copy of core files to a TFTP server.

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. An unrecoverable reset might cause functionality loss, the active supervisor to restart, a supervisor switchover, or the system to restart.

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

- The last four reset-reason codes for a specific module in a given slot. If a module is absent, the reset-reason codes for that module are not displayed.
- The overall history of when and why expected and unexpected reloads occur.
- The time stamp of when the reset or reload occurred.
- The 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.

```
switch# show system reset-reason module 27
----- reset reason for Supervisor-module 27 (from Supervisor in slot 27) ---
1) At 281000 usecs after Wed Jun 26 20:16:34 2013
    Reason: Reset Requested by CLI command reload
    Service:
```

```
    Version: 6.1(2)I1(1)
2) At 791071 usecs after Wed Jun 26 20:04:50 2013
    Reason: Reset Requested by CLI command reload
    Service:
    Version: 6.1(2)I1(1)
3) At 70980 usecs after Wed Jun 26 19:55:52 2013
    Reason: Reset Requested by CLI command reload
    Service:
    Version: 6.1(2)I1(1)
4) At 891463 usecs after Wed Jun 26 23:44:48 2013
    Reason: Reset Requested by CLI command reload
    Service:
    Version: 6.1(2)I1(1)
```

Standby Supervisor Fails to Boot

The standby supervisor does not boot after an upgrade. You may see the following system message:

```
SYSMGR-2-STANDBY_BOOT_FAILED
```

This message is printed if the standby supervisor does not complete its boot procedure (does not reach the login prompt on the local console) 3 to 6 minutes after the loader has been loaded by the BIOS. This message is usually caused by boot variables not properly set for the standby supervisor. This message can also be caused by a user intentionally interrupting the boot procedure at the loader prompt (by pressing ESC).

Connect to the local console of the standby supervisor. If the supervisor is at the loader prompt, try to use the **boot** command to continue the boot procedure. Otherwise, enter the **reload** command for the standby supervisor from a vsh session on the active supervisor, specifying the **force-dnld** option. Once the standby is online, fix the problem by setting the boot variables appropriately.

Symptom	Possible Cause	Solution
Standby supervisor does not boot.	Active supervisor nx-os image booted from TFTP.	Reload the active supervisor from bootflash:.

Recovering the Administrator Password

See Recovering the Administrator Password topic in Password Recovery Procedure for Cisco NX-OS guide to know how to recover administrator password.

- From the CLI with a username that has network-admin privileges
- By power cycling the device
- By reloading the device

Using the CLI with Network-Admin Privileges to Recover the Administrator Password

SUMMARY STEPS

1. switch# **show user-account**
2. switch# **config terminal**
3. switch(config)# **username admin password** *new-password*
4. switch(config)# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

Step 1	switch# **show user-account**
	Example:
	`switch# show user-account`
	`user:admin`
	`this user account has no expiry date`
	`roles:network-admin`
	`user:dbgusr`
	`this user account has no expiry date`
	`roles:network-admin network-operator`
		Shows that your username has network-admin privileges.

Step 2	switch# **config terminal**
	Example:
	`switch# config terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 3	switch(config)# **username admin password** *new-password* **Example:** `switch(config)# username admin password egBdf`	Assigns a new network administrator password if your username has network-admin privileges. **Note** The *new-password* does not allow the $ character.
Step 4	switch(config)# **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Power Cycling the Device to Recover the Administrator Password

If you cannot start a session on the device that has network-admin privileges, you can recover the network administrator password by power cycling the device.

Caution The password recovery procedure disrupts all traffic on the device. All connections to the device will be lost for 2 to 3 minutes.

Note You cannot recover the administrator password from a Telnet or Secure Shell (SSH) session to the management interface. You must have access to the local console connection.

Note Password recovery updates the new administrator password only in the local user database and not on the remote AAA servers. The new password works only if local authentication is enabled; it does not work for remote authentication. When a password is recovered, local authentication is enabled for logins through a console so that the admin user can log in with a new password from a console.

Note If you need to recover the password because the username was not specified in the configuration file when you performed a **copy** *configuration-file* **startup-config** followed by the **fast-reload** or **reload** command, you will need to perform a **write erase** in Step 12 below.

Before you begin

On a device with two supervisor modules, you must perform the password recovery procedure on the supervisor module that will become the active module after you complete the recovery procedure. To ensure that the other supervisor module does not become active, perform one of the following tasks:

- Remove the other supervisor module from the chassis.
- Change the console prompt of the other supervisor module to one of the following two prompts until the recovery procedure completes:
  - loader >
  - switch(boot)#

Procedure

	Command or Action	Purpose
Step 1	Establish a terminal session on the console port of the active supervisor module.	— **Note** If you are using a non-U.S. keymap, the key sequence that you need to press to generate the break sequence might not work. In this case, we recommend that you set your terminal to a U.S. keymap. You can enter **Ctrl-C** instead of **Ctrl-]** (right square bracket) due to keyboard mapping.
Step 2	If you use SSH or a terminal emulator to access the console port, go to Step 6.	—
Step 3	If you use Telnet to access the console port, press **Ctrl-]** (right square bracket) to verify that it does not conflict with the Telnet escape sequence. **Example:** `switch login: Ctrl-]`	— **Note** If the Cisco NX-OS login prompt remains and the Telnet prompt does not appear, go to Step 6.

	Command or Action	Purpose

Step 4	If the Telnet prompt appears, change the Telnet escape sequence to a character sequence other than Ctrl-] (right square bracket).
	Example:
	`telnet> set escape ^\`
	`Escape Character is 'CTRL+\'`
		The example shows how to set Ctrl-\ as the escape key sequence in Microsoft Telnet.
		Note
		If the Cisco NX-OS login prompt remains and the Telnet prompt does not appear, go to Step 6.

Step 5	Press **Enter** one or more times to return to the Cisco NX-OS login prompt.
	Example:
	`telnet> <Enter>`
	`switch login:`
		—

Step 6	Power cycle the device.	—

Step 7	Press **Ctrl-C** to access the loader> prompt.
	Example:
	`Ctrl-C`
	`loader>`
		—

Step 8	loader> **cmdline recoverymode=1** **Example:** `loader> cmdline recoverymode=1`	Enters recovery mode.

Step 9	loader> **boot n9000-dk9.x.x.x.bin**
	Example:
	`loader> boot n9000-dk9.x.x.x.bin`
	`Booting iash`
	`Trying diskboot`
	`Filesystem type is ext2fs, partition type 0x83`
	`Image valid`
	`MD5Sum mismatch`
	
	`INIT: Loading IGB driver ... Signature Envelope.(36)Invalid Tag in Signature Envelope`
	`Installing SSE module ... done`
	`Creating the sse device node ... done`
	`Installing CCTRL driver for card_type 3 ...`
	
	`Checking all filesystems.......`
	`Installing SPROM driver ...`
	`Installing default sprom values ...`
	`done.Configuring network ...`
	`Installing psdev ...`
	`Installing veobc ...`
	`Installing OBFL driver ...`
	`Starting portmap daemon...`
	`creating NFS state directory: done`
		Restarts the device with the nx-os image to reach the switch(boot)# prompt.

	Command or Action	Purpose
	starting 8 nfsd kernel threads: done starting mountd: done starting statd: done Loading system software No system image is specified INIT: Sending processes the TERM signal INIT: Sending processes the KILL signal Bad terminal type: "linux". Will assume vt100. Cisco Nexus Operating System (NX-OS) Software TAC support: http://www.cisco.com/tac Copyright (c) 2002-2013, Cisco Systems, Inc. All rights reserved. The copyrights to certain works contained in this software are owned by other third parties and used and distributed under license. Certain components of this software are licensed under the GNU General Public License (GPL) version 2.0 or the GNU Lesser General Public License (LGPL) Version 2.1. A copy of each such license is available at http://www.opensource.org/licenses/gpl-2.0.php and http://www.opensource.org/licenses/lgpl-2.1.php switch(boot)#	
Step 10	Press **Enter** one or more times to return to the Cisco NX-OS login prompt. **Example:** telnet> <Enter> switch login:	—
Step 11	switch(boot)# **config terminal** **Example:** switch(boot)# config terminal Enter configuration commands, one per line. End with CNTL/Z. switch(boot)(config)#	Enters boot configuration mode.
Step 12	switch(boot)(config)# **admin-password** *new-password* **Example:** switch(boot)(config)# admin-password egBdf WARNING! Remote Authentication for login through console has been disabled	Resets the network administrator password. **Note** If you are performing this password recovery procedure because the username was not specified in the configuration file when you performed a **copy** *configuration-file* **startup-config** followed by the **fast-reload** or **reload** command, skip this step, enter the **write erase** command instead, and then go to the next step. **Important** If your switch is running Cisco NX-OS Release 7.0(3)I2(2), skip Steps 12 through 14, perform a write erase, and reload the device. Make sure that the

	Command or Action	Purpose
		configurations are backed up before attempting the password recovery. This workaround pertains only to Cisco NX-OS Release 7.0(3)I2(2).

Step 13	switch(boot)(config)# **exit**
	Example:
	`switch(boot)(config)# exit`
	`switch(boot)#`
		Exits boot configuration mode.

Step 14	switch(boot)# **load-nxos** **Example:** `switch(boot)# load-nxos`	Loads the nx-os image. You must enter the **load-nxos** command exactly as shown. Do not enter the image filename with this command.

Step 15	Log into the device using the new administrator password.
	Example:
	`switch login: admin`
	`Password: egBdf`
		The running configuration indicates that local authentication is enabled for logins through a console. You should not change the running configuration in order for the new password to work for future logins. You can enable remote authentication after you reset and remember the administrator password that is configured on the AAA servers.
		`switch# show running-config aaa`
		`!Command: show running-config aaa`
		`!Time: Fri Jun 7 02:39:23 2013`
		`version 6.1(2)I1(1)`
		`logging level aaa 5`
		`aaa authentication login ascii-authentication`

Step 16	switch# **config terminal**
	Example:
	`switch# config terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 17	switch(config)# **username admin password** *new-password* **Example:** `switch(config)# username admin password egBdf`	Resets the new password to ensure that it is also the Simple Network Management Protocol (SNMP) password.

Step 18	switch(config)# **exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 19	Insert the previously removed standby supervisor module into the chassis, if necessary.	—

	Command or Action	Purpose
Step 20	Boot the nx-os image on the standby supervisor module, if necessary.	—
Step 21	switch(config)# **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Reloading the Device to Recover the Administrator Password

You can reset the network administrator password by reloading the device.

Caution This procedure disrupts all traffic on the device. All connections to the device will be lost for 2 to 3 minutes.

Note You cannot recover the administrator password from a Telnet or Secure Shell (SSH) session to the management interface. You must have access to the local console connection.

Note Password recovery updates the new administrator password only in the local user database and not on the remote AAA servers. The new password works only if local authentication is enabled; it does not work for remote authentication. When a password is recovered, local authentication is enabled for logins through a console so that the admin user can log in with a new password from a console.

SUMMARY STEPS

1. Establish a terminal session on the console port of the active supervisor module.
2. switch# **reload**
3. loader> **cmdline recoverymode=1**
4. loader> **boot n9000-dk9.x.x.x.bin**
5. Reset the network administrator password by following Steps 6 through 20 in Power Cycling the Device to Recover the Administrator Password, on page 16.

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	Establish a terminal session on the console port of the active supervisor module.	—

	Command or Action	Purpose

Step 2	switch# **reload**
	Example:
	`switch# reload`
	`This command will reboot the system. (y/n)?  [n]`
	`Y`
	`2013 Jun  7 13:09:56 switch %$ VDC-1 %$`
	`%PLATFORM-2-PFM_SYSTEM_RESET:`
	`Manual system restart from Command Line Interface`
	`writing reset reason 9,`
	`..`
	`..`
	`GNU GRUB  version 0.97`
	`Autobooting bootflash:/n9000-dk9.x.x.x.bin`
	`bootflash:/n...`
	`Filesystem type is ext2fs, partition type 0x83`
	`Booting nx-os image:`
	`bootflash:/n9000-dk9.x.x.x.bin....(---->`
	`Press Ctrl + C)`
	`....Aborting Image Boot`
	`GNU GRUB  version 0.97`
	`Loader Version 3.22.0`
	`loader>`
		Reloads the device to reach the loader prompt. You need to press **Ctrl-C** when the following appears:
		`Booting nx-os image:`
		`bootflash:/n9000-dk9.x.x.x.bin....`

Step 3	loader> **cmdline recoverymode=1** **Example:** `loader> cmdline recoverymode=1`	Configure the boot process to stop at the switch(boot)# prompt.

Step 4	loader> **boot n9000-dk9.x.x.x.bin**
	Example:
	`loader> boot n9000-dk9.x.x.x.bin`
	`Filesystem type is ext2fs, partition type 0x83`
	`Booting nx-os image: n9000-dk9.6.1.2.I1.1.gbin....`
	`.....`
	`.....Image verification OK`
	`..`
	`..`
	`Lesser General Public License (LGPL) Version 2.1.`
	`A copy of each such license is available at`
	`http://www.opensource.org/licenses/gpl-2.0.php and`
	`http://www.opensource.org/licenses/lgpl-2.1.php`
	`switch(boot)#`
		Restarts the device with only the nx-os image to reach the switch boot prompt.

Step 5	Reset the network administrator password by following Steps 6 through 20 in Power Cycling the Device to Recover the Administrator Password, on page 16.	—

Changing the Administrator Password

You must be logged in as admin to change the network administrator password.

Guidelines and Limitations for Changing the Administrator Password

Follow these guidelines and limitations to change an administrator password:

- You must be an admin to enable or disable the CLI command, no service password-recovery.
- You must be logged in as admin to change the admin password.
- You cannot change the admin password from a boot prompt if the CLI was disabled by the admin on a previous boot.

Note If you are not logged in as admin, you see an error.

Granting the Change Admin Password to Admin User Only

SUMMARY STEPS

1. switch# **show user-account**
2. switch# **configure terminal**
3. switch(config)# **no service password-recovery**

DETAILED STEPS

Procedure

	Command or Action	Purpose

Step 1	switch# **show user-account**
	Example:
	`switch# show user-account`
	`user:admin`
	`this user account has no expiry date`
	`roles:network-admin`
	`user:dbgusr`
	`this user account has no expiry date`
	`roles:network-admin network-operator`
		Shows that your username has network-admin privileges.

Step 2	switch# **configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 3	switch(config)# **no service password-recovery** **Example:**	Enables/disables password recovery. **Note**

	Command or Action	Purpose
	`switch(config)# no service password-recovery` `WARNING: executing this command will disable the password recovery mechanism. Do not execute this command without another plan for password recovery. Are you sure you want to continue? (y/n) : [y] y`	To allow another user to change the Admin password, run **service password-recovery** when logged in as admin with network admin privileges.