Using the Cisco NX-OS Setup Utility

This chapter contains the following sections:

Configuring the Switch

Image Files on the Switch

The Cisco Nexus devices have the following images:

- BIOS and loader images combined in one file
- Kickstart image
- System image that includes a BIOS image that can be upgraded

The switch has flash memory that consists of two separate flash parts:

- A 2 MB flash part holds two BIOS and loader images.
- A 1 GB flash part holds configuration files, kickstart images, systems images, and other files.

The upgradeable BIOS and the golden BIOS are programmed onto the 2 MB flash part. You cannot upgrade the golden BIOS.

When you download a new pair of kickstart and system images, you also get a new BIOS image because it is included in the system image. You can use the **install all** command to upgrade the kickstart, system, and upgradeable BIOS images.

Starting the Switch

A Cisco Nexus switch starts its boot process as soon as its power cord is connected to an A/C source. The switch does not have a power switch.

Boot Sequence

When the switch boots, the golden BIOS validates the checksum of the upgradeable BIOS. If the checksum is valid, then control is transferred to the upgradeable BIOS image. The upgradeable BIOS launches the kickstart image, which then launches the system image. If the checksum of the upgradeable BIOS is not valid, then the golden BIOS launches the kickstart image, which then launches the system image.

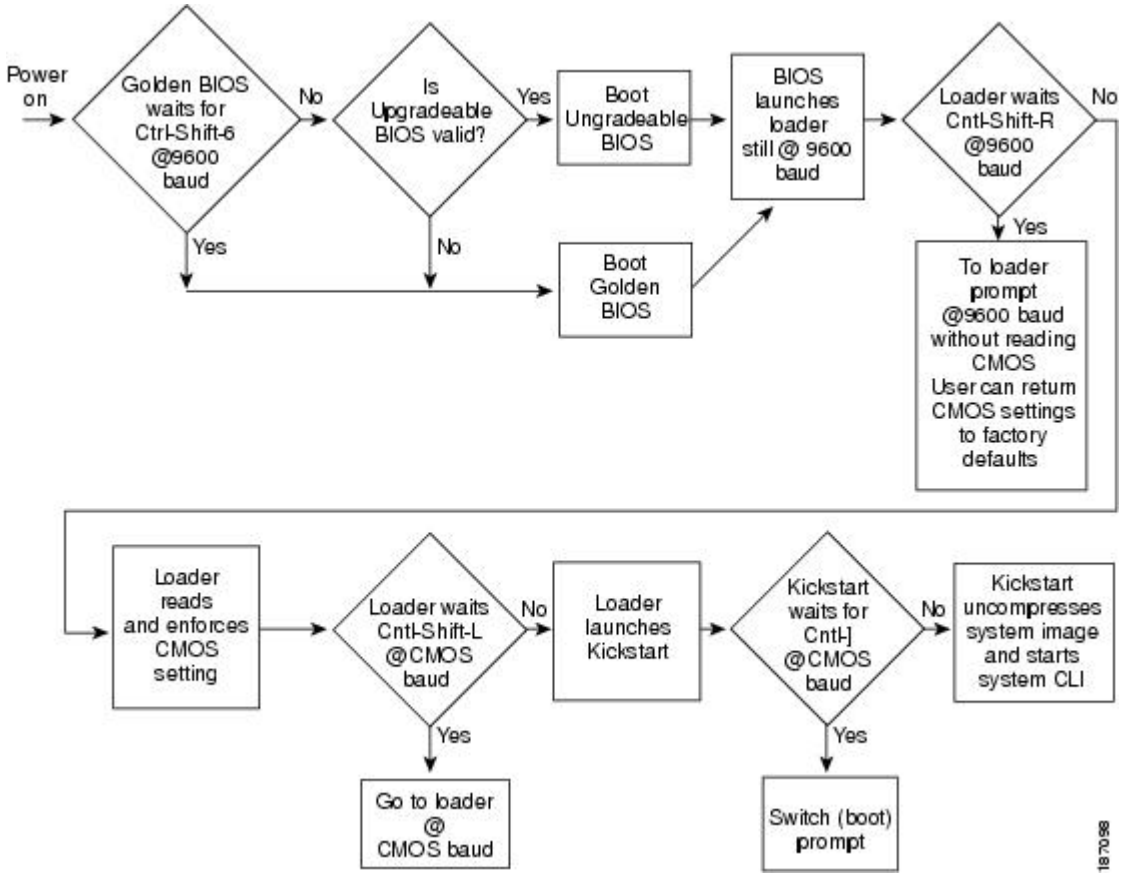
You can force the switch to bypass the upgradeable BIOS and use the golden BIOS instead. If you press **Ctrl-Shift-6** within two seconds of when power is supplied to the switch, the golden BIOS will be used to launch the kickstart image, even if the checksum of the upgradeable BIOS is valid.

Note When you press **Ctrl-Shift-6**, the console settings must be set to their defaults: 9600 baud, 8 data bits, no parity, and 1 stop bit.

Before the boot sequence starts, the BIOS performs internal tests on the switch. If the tests fail, then the loader does not gain control. Instead, the BIOS image retains control and prints a message to the console at 9600 baud every 30 seconds that indicates a failure.

The following figure shows the normal and recovery boot sequence.

Figure 1: Boot Sequence



For additional information, see *Troubleshooting*.

Console Settings

The loader, kickstart, and system images have the following factory default console settings:

- Speed—9600 baud
- Databits—8 bits per byte
- Stopbits—1 bit
- Parity—none

These settings are stored on the switch, and all three images use the stored console settings.

To change a console setting, use the **line console** command in configuration mode. The following example configures a line console and sets the options for that terminal line:

```
switch# configure terminal
switch(config)# line console
switch(config-console)# databits 7
switch(config-console)# exec-timeout 30
switch(config-console)# parity even
switch(config-console)# stopbits 2
```

You cannot change the BIOS console settings. These are the same as the default console settings.

Upgrading the Switch Software

Note You must have the network-admin role before you can upgrade the software image on the switch.

You must log in to the switch on its console port connection.

To upgrade the software on the switch, follow these steps:

SUMMARY STEPS

1. Log in to Cisco.com to access the Software Download Center. To log in to Cisco.com, go to the URL http://www.cisco.com/ and click **Log In** at the top of the page. Enter your Cisco username and password.
2. Access the Software Download Center using this URL: http://www.cisco.com/cisco/web/download/index.html
3. Navigate to the software downloads for Cisco Nexus devices.
4. Read the release notes for the related image file.
5. Select and download the kickstart and system software files to a local server.
6. Ensure that the required space is available in the bootflash: directory for the image file(s) to be copied.
7. If you need more space on the active supervisor module bootflash, delete unnecessary files to make space available.
8. Copy the kickstart and system images to the switch bootflash using a transfer protocol. You can use **ftp**, **tftp**, **scp**, or **sftp**. The examples in this procedure use **scp**.
9. Install the new images, specifying the new image names that you downloaded in the previous step.
10. After the switch completes the installation, log in and verify that the switch is running the required software version.

DETAILED STEPS

Step 1 Log in to Cisco.com to access the Software Download Center. To log in to Cisco.com, go to the URL http://www.cisco.com/ and click **Log In** at the top of the page. Enter your Cisco username and password.

Note Unregistered Cisco.com users cannot access the links provided in this document.

Step 2 Access the Software Download Center using this URL: http://www.cisco.com/cisco/web/download/index.html

Step 3 Navigate to the software downloads for Cisco Nexus devices.
You see links to the download images for the switch.

Step 4 Read the release notes for the related image file.

Step 5 Select and download the kickstart and system software files to a local server.

Step 6 Ensure that the required space is available in the bootflash: directory for the image file(s) to be copied.

Example:

Caution We recommend that you keep the kickstart and system image files for at least one previous software release to use if the new image files do not load successfully.

Step 7 If you need more space on the active supervisor module bootflash, delete unnecessary files to make space available.

Example:

Step 8 Copy the kickstart and system images to the switch bootflash using a transfer protocol. You can use **ftp**, **tftp**, **scp**, or **sftp**. The examples in this procedure use **scp**.

Example:

Step 9 Install the new images, specifying the new image names that you downloaded in the previous step.

Example:

The **install all** command performs the following actions:

- Performs compatibility checks (equivalent to the **show incompatibility** command) for the images that you have specified. If there are compatibility issues, an error message is displayed and the installation does not proceed.
- Displays the compatibility check results and displays whether the installation is disruptive.
- Provides a prompt to allow you to continue or abort the installation.

  Caution After completing the installation, all traffic through the switch is disrupted while the switch reboots.

- Updates the boot variables to reference the specified images and saves the configuration to the startup configuration file.

Step 10 After the switch completes the installation, log in and verify that the switch is running the required software version.

Example:

Downgrading from a Higher Release

The procedure to downgrade the switch is identical to a switch upgrade, except that the image files to be loaded are for an earlier release than the image currently running on the switch.

Note Prior to downgrading to a specific release, check the release notes for the current release installed on the switch, to ensure that your hardware is compatible with the specific release. There are special caveats you must be aware of before you downgrade the switch software to a 4.0(0)-based release. See the Cisco Nexus release notes for your device for details.

SUMMARY STEPS

1. Locate the image files you will use for the downgrade by entering the **dir bootflash:** command.
2. Install the new images.
3. After the switch completes the installation, log in and verify that the switch is running the required software version.

DETAILED STEPS

Step 1 Locate the image files you will use for the downgrade by entering the **dir bootflash:** command.
If the image files are not stored on the bootflash memory, download the files from Cisco.com:

a) Log in to Cisco.com to access the Software Download Center. To log in to Cisco.com, go to the URL http://www.cisco.com/ and click **Log In** at the top of the page. Enter your Cisco username and password.
Note Unregistered Cisco.com users cannot access the links provided in this document.

b) Access the Software Download Center using this URL: http://www.cisco.com/cisco/web/download/index.html

c) Navigate to the software downloads for Cisco Nexus Series switches.
You see links to the download images for the switch.

d) Read the release notes for the related image file then select and download the kickstart and system software files to a local server

e) Ensure that the required space is available in the bootflash: directory for the image file(s) to be copied.

Caution We recommend that you keep the kickstart and system image files for at least one previous software release to use if the new image files do not load successfully.

f) Copy the kickstart and system images to the switch bootflash using a transfer protocol. You can use **ftp**, **tftp**, **scp**, or **sftp**.

Step 2 Install the new images.

Example:
The **install all** command performs the following actions:

- Performs compatibility checks (equivalent to the **show incompatibility** command) for the images that you have specified. If there are compatibility issues, an error message is displayed and the installation does not proceed.
- Displays the compatibility check results and displays whether the installation is disruptive.
- Provides a prompt to allow you to continue or abort the installation.

  Note A disruptive installation causes traffic disruption while the switch reboots.

- Updates the boot variables to reference the specified images and saves the configuration to the startup configuration file.

Step 3 After the switch completes the installation, log in and verify that the switch is running the required software version.

Example:
```
switch# show version
```

Initial Configuration

Configuration Prerequisites

The following procedure is a review of the tasks you should have completed during hardware installation. These tasks must be completed before you can configure the switch.

SUMMARY STEPS

1. Verify the following physical connections for the new Cisco Nexus device:
2. Verify that the default console port parameters are identical to those of the computer terminal (or terminal server) attached to the switch console port:

DETAILED STEPS

Step 1 Verify the following physical connections for the new Cisco Nexus device:

- The console port is physically connected to a computer terminal (or terminal server).
- The management Ethernet port (mgmt0) is connected to an external hub, switch, or router.

Refer to the Cisco Nexus Hardware Installation guide for your device for more information.

Tip Save the host ID information for future use (for example, to enable licensed features). The host ID information is provided in the Proof of Purchase document that accompanies the switch.

Step 2 Verify that the default console port parameters are identical to those of the computer terminal (or terminal server) attached to the switch console port:

- 9600 baud
- 8 data bits
- No parity
- 1 stop bit

Initial Setup

The first time that you access a switch in your Cisco Nexus series, it runs a setup program that prompts you for the IP address and other configuration information necessary for the switch to communicate over the Ethernet interface. This information is required to configure and manage the switch.

Note The IP address can only be configured from the CLI. When the switch powers up for the first time, you should assign the IP address. After you perform this step, the Cisco MDS 9000 Family Fabric Manager can reach the switch through the console port.

Preparing to Configure the Switch

Before you configure Cisco Nexus device for the first time, you need the following information:

- Administrator password.

Note If a password is weak (short, easy-to-decipher), your password configuration is rejected. Be sure to configure a strong password.

- If you are using an IPv4 address for the management interface, you need the following information:
  - IPv4 subnet mask for the switch's management interface.

    - IPv4 address of the default gateway (optional).

- SSH service on the switch (optional).

  To enable this service, select the type of SSH key (dsa/rsa/rsa1) and number of SSH key bits (768 to 2048).

- NTP server IPv4 address (optional).
- SNMP community string (optional).
- Switch name (optional).

  This is your switch prompt.

- An additional login account and password (optional).

Note If you are using IPv4, be sure to configure the IPv4 route, the IPv4 default network address, and the IPv4 default gateway address to enable SNMP access.

Default Login

The switch has the network administrator as a default user (admin). You cannot change the default user at any time.

There is no default password so you must explicitly configure a strong password. If a password is trivial (short, easy-to-decipher), your password configuration is rejected. Be sure to configure a strong password. If you configure and subsequently forget this new password, you have the option to recover this password.

Note If you enter the **write erase** command and reload the switch, you must reconfigure the default user (admin) password using the setup procedure.

Configuring the Switch

This section describes how to initially configure the switch.

Note Press **Ctrl-C** at any prompt to skip the remaining configuration options and proceed with what you have configured up to that point. However, entering the new password for the administrator is a requirement and cannot be skipped.

Tip If you do not want to answer a previously configured question, or if you want to skip answers to any questions, press **Enter**. If a default answer is not available (for example, switch name), the switch uses what was previously configured and skips to the next question.

To configure the switch for first time, follow these steps:

SUMMARY STEPS

1. Ensure that the switch is on. Switches in the Cisco Nexus series boot automatically.
2. Enter the new password for the administrator.
3. Enter yes to enter the setup mode.
4. Enter the new password for the administrator (admin is the default).
5. Enter yes (no is the default) to create additional accounts.
6. Enter yes (yes is the default) to create an SNMP read-only community string.
7. Enter a name for the switch.
8. Enter yes (yes is the default) to configure out-of-band management and enter the mgmt0 IPv4 address.
9. Enter yes (yes is the default) to configure the IPv4 default gateway (recommended) and enter the IPv4 address for the default gateway.
10. Enter yes (yes is the default) to enable the Telnet service.
11. Enter yes (no is the default) to enable the SSH service.
12. Enter yes (no is the default) to configure the NTP server and enter the IPv4 address for the NTP server.
13. Enter yes (yes is the default) to configure basic Fibre Channel configurations.
14. Enter shut (shut is the default) to configure the default Fibre Channel switch port interface to the shut (disabled) state.
15. Enter on (on is the default) to configure the switch port trunk mode.
16. Enter permit (deny is the default) to deny a default zone policy configuration.
17. Enter yes (no is the default) to enable a full zone set distribution.
18. You see the new configuration. Review and edit the configuration that you have just entered. Enter no (no is the default) if you are satisfied with the configuration.
19. Enter yes (yes is default) to use and save this configuration:

DETAILED STEPS

Step 1 Ensure that the switch is on. Switches in the Cisco Nexus series boot automatically.

Step 2 Enter the new password for the administrator.

Example:
```
Enter the password for admin: <password>
```

Note Clear text passwords cannot contain dollar signs ($) or spaces anywhere in the password. Also, they cannot include these special characters at the beginning of the password: quotation marks (" or '), vertical bars (|), or right angle brackets (>).

Tip If a password is weak (short, easy-to-decipher), your password configuration is rejected. Be sure to configure a strong password. Passwords are case-sensitive.

Step 3 Enter yes to enter the setup mode.

Example:
```
This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

*Note: setup is mainly used for configuring the system initially,
```

```
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): yes
```

The setup utility guides you through the basic configuration process. Press **Ctrl-C** at any prompt to end the configuration process.

Step 4 Enter the new password for the administrator (admin is the default).

Example:
```
Enter the password for admin: admin
```

Step 5 Enter yes (no is the default) to create additional accounts.

Example:
```
Create another login account (yes/no) [n]: yes
```

While configuring your initial setup, you can create an additional user account (in the network-admin role) besides the administrator's account.

a) Enter the user login ID.

Example:
```
Enter the user login ID: user_name
```

b) Enter the user password.

Example:
```
Enter the password for user_name: user-password
```

Step 6 Enter yes (yes is the default) to create an SNMP read-only community string.

Example:
```
Configure read-only SNMP community string (yes/no) [n]:yes
SNMP community string: snmp_community
```

Step 7 Enter a name for the switch.

Note Starting with Cisco NX-OS Release 7.3(0)N1(1), the character limit of a switch name is increased from 32 to 63 alphanumeric characters. Also, 63 characters is the maximum length limit for setting hostname using SNMP. The default name is switch.

Example:
```
Enter the switch name: switch_name
```

Step 8 Enter yes (yes is the default) to configure out-of-band management and enter the mgmt0 IPv4 address.

Example:
```
Continue with Out-of-band (mgmt0) management configuration? [yes/no]: yes
Mgmt0 IPv4 address: ip_address
```

Step 9 Enter yes (yes is the default) to configure the IPv4 default gateway (recommended) and enter the IPv4 address for the default gateway.

Example:
```
Configure the default-gateway: (yes/no) [y]: yes
IPv4 address of the default-gateway: default_gateway
```

Step 10 Enter yes (yes is the default) to enable the Telnet service.

Example:
```
Enable the telnet service? (yes/no) [y]: yes
```

Step 11 Enter yes (no is the default) to enable the SSH service.

Example:
```
Enabled SSH service? (yes/no) [n]: yes
```

a) Enter the SSH key type that you would like to generate.

Example:
```
Type the SSH key you would like to generate (dsa/rsa/rsa1)? dsa
```

b) Enter the number of key bits within the specified range.

Example:
```
Enter the number of key bits? (768 to 2048): 768
```

Step 12 Enter yes (no is the default) to configure the NTP server and enter the IPv4 address for the NTP server.

Example:
```
Configure NTP server? (yes/no) [n]: yes
NTP server IP address: ntp_server_IP_address
```

Step 13 Enter yes (yes is the default) to configure basic Fibre Channel configurations.

Example:
```
Enter basic FC configurations (yes/no) [n]: yes
```

Step 14 Enter shut (shut is the default) to configure the default Fibre Channel switch port interface to the shut (disabled) state.

Example:
```
Configure default physical FC switchport interface state (shut/noshut) [shut]: shut
```

Step 15 Enter on (on is the default) to configure the switch port trunk mode.

Example:
```
Configure default physical FC switchport trunk mode (on/off/auto) [on]: on
```

Step 16 Enter permit (deny is the default) to deny a default zone policy configuration.

Example:
```
Configure default zone policy (permit/deny) [deny]: permit
```

Permits traffic flow to all members of the default zone.

Note If you are executing the setup script after entering a **write erase** command, you explicitly must change the default zone policy to permit for VSAN 1 after finishing the script using the following command:

```
Configure read-only SNMP community string (yes/no) [n]: zone default-zone permit vsan 1
```

Step 17 Enter yes (no is the default) to enable a full zone set distribution.

Example:
```
Enable full zoneset distribution (yes/no) [n]: yes
```

Overrides the switch-wide default for the full zone set distribution feature.

Step 18 You see the new configuration. Review and edit the configuration that you have just entered. Enter no (no is the default) if you are satisfied with the configuration.

Example:
```
The following configuration will be applied:
  username admin password <user-password> role network-admin
  snmp-server community snmp_community ro
  switchname switch
  feature telnet
  ssh key dsa 768 force
  feature ssh
  system default switchport shutdown san
  system default switchport trunk mode on
  system default zone default-zone permit
  system default zone distribute full
Would you like to edit the configuration? (yes/no) [n]: no
```

Step 19 Enter yes (yes is default) to use and save this configuration:

Example:
```
Use this configuration and save it? (yes/no) [y]: yes
```

Caution If you do not save the configuration at this point, none of your changes are updated the next time the switch is rebooted. Type yes to save the new configuration. This operation ensures that the kickstart and system images are also automatically configured.

Changing the Initial Configuration

To make changes to the initial configuration at a later time, enter the **setup** command in EXEC mode:

```
switch# setup
---- Basic System Configuration Dialog ----
This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.
*Note: setup is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.
Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
```

```
to skip the remaining dialogs.
Would you like to enter the basic configuration dialog (yes/no): yes
```

The setup utility guides you through the basic configuration process.

Management Interface Configuration

The management interface on the switch allows multiple simultaneous Telnet, SSH, or SNMP sessions. You can remotely configure the switch through the management interface (mgmt0), but first you must configure some IP parameters so that the switch is reachable. You can manually configure the management interface from the CLI through the console port.

About the mgmt0 Interface

The mgmt0 interface on a Cisco Nexus device provides out-of-band management, which enables you to manage the switch by its IPv4 or IPv6 address. The mgmt0 interface is a 10/100/1000 Ethernet port.

Note Before you begin to configure the management interface manually, obtain the switch's IP address and subnet mask. Also make sure that the console cable is connected to the console port.

Configuring the Management Interface

To configure the management (mgmt0) Ethernet interface to connect over IP, perform this task:

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface mgmt 0**
3. Configure the IP address for IPv4 or IPv6:
4. switch(config-if)# **no shutdown**
5. switch(config-if)# **exit**
6. switch(config)# **vrf context management**
7. Configure the IP address (IPv4 or IPv6) for the next hop:
8. switch(config-vrf)# **end**
9. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

Step 1 switch# **configure terminal**
Enters configuration mode.

Step 2 switch(config)# **interface mgmt 0**
Selects the management Ethernet interface on the switch and enters interface configuration submode.

Step 3 Configure the IP address for IPv4 or IPv6:

a) switch(config-if)# **ip address** *ipv4-address*[/ *length*]
Configures the IPv4 address and its subnet mask.

b) switch(config-if)# **ip address** *ipv4-address* [*subnet-mask*]
An alternative method that configures the IPv4 address and its subnet mask.

c) switch(config-if)# **ipv6 address** *ipv6-address*[/ *length*]
Configures the IPv6 address and its subnet mask.

Step 4 switch(config-if)# **no shutdown**
Enables the interface.

Step 5 switch(config-if)# **exit**
Returns to configuration mode.

Step 6 switch(config)# **vrf context management**
Enters VRF context management configuration mode.

Step 7 Configure the IP address (IPv4 or IPv6) for the next hop:

a) switch(config-vrf)# **ip route** *ipv4-prefix*[/ *length*] *ipv4-nexthop-address*
Configures the IPv4 address of the next hop.

b) switch(config-vrf)# **ipv6 route** *ipv6-prefix*[/ *length*] *ipv6-nexthop-address*
Configures the IPv6 address of the next hop.

Step 8 switch(config-vrf)# **end**
Returns to EXEC mode.

Step 9 (Optional) switch# **copy running-config startup-config**
Saves your configuration changes to the file system.

In some cases, a switch interface might be administratively shut down. You can check the status of an interface at any time by using the **show interface mgmt 0** command.

Displaying Management Interface Configuration

To display the management interface configuration, use the **show interface mgmt 0** command.

```
switch# show interface mgmt0

mgmt0 is up
    Hardware is GigabitEthernet, address is 000d.ec8f.cb00 (bia 000d.ec8f.cb00)
    Internet Address is 172.16.131.202/24
    MTU 1500 bytes, BW 0 Kbit, DLY 0 usec,
       reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation ARPA
    full-duplex, 1000 Mb/s
    Input flow-control is off, output flow-control is off
    8540 packets input, 2835036 bytes
    5202 multicast frames, 0 compressed
    0 input errors, 0 frame, 0 overrun, 0 fifo
    570 packets output, 85555 bytes
    0 underrun, 0 output errors, 0 collisions
    0 fifo, 0 carrier errors
```

Shutting Down the Management Interface

To shut down the management interface (mgmt0), you use the **shutdown** command. A system prompt requests you confirm your action before it executes the command. You can use the force option to bypass this confirmation.

The following example shuts down the interface without using the force option:

```
switch# configure terminal
switch(config)# interface mgmt 0
switch(config-if)# shutdown
Shutting down this interface will drop all telnet sessions.
Do you wish to continue (y/n)? y
```

The following example shuts down the interface using the force option:

```
switch# configure terminal
switch(config)# interface mgmt 0
switch(config-if)# shutdown force
```