
# Administrative Commands

This chapter documents the following commands:

# action

To execute predefined administrative functions on expansion modules (gateway cards), enter the **action** command in Card Configuration submode.

**action** {**delete-inactive-image** | **reset**}

## Syntax Description

| | |
|---|---|
| **delete-inactive-image** | Removes the inactive image from interface cards. Use the **action** command with the **delete-inactive-image** keyword after the **boot-config** command when you upgrade the system image on your Server Switch to clear the inactive image from the card(s) after a reboot. |
| **reset** | Resets the card(s) that you specify in a Cisco SFS 7008. |

## Command Modes

Card Configuration (config-card) mode.

## Defaults

This command has no default settings.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

Unrestricted or card-specific read-write user.

Currently, you can execute only one predefined administrative function on all platforms except the Cisco SFS 7008. The function (delete-inactive-image) deletes inactive images from one or more cards to provide more available memory on the card.

Before you use the **action** command with the **delete-inactive-images** keyword, enter the **boot-config** command with the **primary-image-source** keyword to install and activate the proper image on the card. When you execute this command, the previously-active image becomes inactive. You can now execute the **action** command to clear the inactive image from your card.

To execute this command, you require read-write administrative permissions for the type(s) of card(s) that you want to clear.

## Examples

The following example deletes inactive images from the card that resides in slot 2.

```
SFS-7000P(config-card-2)# action delete-inactive-images
```

The following example resets a management I/O card on a Cisco SFS 7008.

```
SFS-270(config-card-15)# action reset
```

## Related Commands

boot-config
copy
install
show card
shutdown

# addr-option

To configure the Ethernet Management port to

- use a static IP address,
- obtain an IP address from a DHCP server,
- automatically obtain an IP address from a hardware-designated controller,

enter the **addr-option** command in Ethernet Management Configuration submode.

**addr-option** {**auto** | **dhcp** | **static**}

## Syntax Description

| | |
|---|---|
| **auto** | Applies an IP address from an outside controller to the Ethernet Management port. |
| **dhcp** | Uses DHCP to configure the address for the Ethernet Management port. |
| **static** | Changes the address of the Ethernet management port from the DCHP address to the static address that you configure with the **ip** command. |

## Defaults

This command has no default settings.

## Command Modes

Ethernet Management Configuration (config-mgmt-ethernet) mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

Ethernet read-write user.

If you use the **static** keyword, configure the IP address of the Ethernet Management port with the "ip" section on page 5-8.

## Examples

The following example configures the Ethernet Management port to obtain an IP address from a DHCP server.

```
SFS-270(config-if-mgmt-ethernet)# addr-option dhcp
```

## Related Commands

**ip**

# authentication

To configure your Server Switch to use RADIUS server authentication in addition to local authentication (always active), and to configure the order in which your Server Switch authenticates, enter the **authentication** command in Global Configuration mode.

**authentication login** [**default** {**local** [**radius**] | **radius local**}]

## Syntax Description

| | |
|---|---|
| **login** | Enables local login authentication.<br>**Note** When you enter **authentication login**, the command behaves as though you had entered **authentication login default local**. |
| **default** | (Optional) Configures where and in what order your Server Switch authenticates logins. |
| **local** | (Optional) Authenticates the login with the local CLI user database. |
| **radius** | (Optional) Authenticates the login with the RADIUS server. |

## Defaults

CLI logins authenticate locally by default.

## Command Modes

Global Configuration (config) mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

Unrestricted read-write user.

If you enter the **local** keyword before the **radius** keyword, your Server Switch authenticates logins locally first, then on the RADIUS server if local authentication fails. If you enter the **radius** keyword before the **local** keyword, your Server Switch authenticates logins with the RADIUS server first, then on the local CLI user database.

## Examples

The following example configures the Server Switch to authenticate to the RADIUS server, then to the local database if server authentication fails.

```
SFS-7000P(config)# authentication login default radius local
```

## Related Commands

**configure terminal**
**radius-server**
**show authentication**

# auto-negotiate

To configure your Server Switch to

- dynamically determine the connection speed of direct-attached Fibre Channel devices,
- dynamically determine the connection speed of direct-attached Ethernet devices,
- dynamically determine the connection speed of direct-attached InfiniBand devices,

enter the **auto-negotiate** command in the appropriate Interface Configuration submode. To disable auto-negotiation, use the **no** form of this command.

**auto-negotiate**

**no auto-negotiate**

## Syntax Description

This command has no arguments or keywords

## Defaults

Fibre Channel and Ethernet ports auto-negotiate connection speeds by default.

## Command Modes

Fibre Channel Interface Configuration (config-if-fc) submode, Ethernet Interface Configuration (config-if-ether) submode, InfiniBand Interface Configuration (config-if-ib) submode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

Fibre Channel read-write user (for FC ports), Ethernet read-write user (for Ethernet ports), InfiniBand read-write user (for InfiniBand ports).

**Fibre Channel:**

Before you configure your FC port to auto-negotiate speed, perform the following steps to verify that the attached Fibre Channel device supports auto-negotiation:

**Step 1** Enter the **show interface fc** command in User Exec mode or Privileged Exec mode.

**Step 2** Verify that the **auto-negotiate-supported** field of the command output displays **yes**. If the field displays **no**, you must manually configure the connection speed of the port.

**Note** If you disable auto-negotiation in the CLI but leave it active on the attached Fibre Channel devices, the port manager for the Fibre Channel interface on your device does not negotiate speed and mode with the FC devices. The FC devices may choose a different duplex setting than the port manager and produce unexpected results.

**Ethernet:**

Before you enable auto-negotiation, perform the following steps to verify that the Ethernet host supports auto-negotiation:

**Step 1** Enter the **show interface ethernet** command in User Exec mode or Privileged Exec mode.

**Step 2** Verify that the **auto-negotiate-supported** field displays **yes**. If the field displays **no**, you must manually configure the connection speed of the port.

**InfiniBand:**

Before you enable auto-negotiation, perform the following steps to verify that the InfiniBand host supports auto-negotiation:

**Step 1** Enter the **show interface ib** command in User Exec mode or Privileged Exec mode.

**Step 2** Verify that the **auto-negotiate-supported** field displays **yes**. If the field displays **no**, you must manually configure the connection speed of the port.

## Examples

The following example disables auto-negotiation on ports 1 through 2 on Fibre Channel card 5. The result of this command appears in the **auto-negotiate** field of the **show interface fc** command.

```
SFS-7000P(config-if-fc-5/1-5/2)# no auto-negotiate
```

The following example disables auto-negotiation on ports 1 through 4 on Ethernet card 4. The result of this command appears in the **auto-negotiate-supported** field of the **show interface ethernet** command.

```
SFS-7000P(config-if-ether-4/1-4/4)# no auto-negotiate
```

The following example enables auto-negotiation on port 1 on a Cisco SFS 7000. The result of this command appears in the **auto-negotiate-supported** field of the **show interface ib** command.

```
SFS-120(config-if-ib-1/1)# auto-negotiate
```

## Related Commands

**link-trap**
**name**
**show fc srp initiator**
**show interface ethernet**
**show interface fc**
**show interface ib**
**shutdown**
**speed**

# boot-config

To specify the system image to run when your Server Switch boots, enter the **boot-config** command in Global Configuration mode.

**boot-config primary-image-source** *dir*

## Syntax Description

| | |
|---|---|
| **primary-image-source** | Specifies that you want to configure the boot image. |
| *dir* | Directory that contains the boot image. |

## Defaults

This command has no default settings.

## Command Modes

Global Configuration (config) mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

Unrestricted read-write user.

Specify an image *directory* as a boot image. Do not specify image files that end in ".img" since these are compressed archives that must be installed first.

**Note** Use the **dir** command with the image keyword to view a list of images on your device.

## Examples

The following example configures the Server Switch controller to use the sfsOS-1.1.0/build460 directory when the Server Switch boots. Without this directory, the system cannot boot successfully.

```
SFS-7000P(config)# boot-config primary-image-source sfsOS-1.1.0/build460
```

## Related Commands

**dir**
**install**
**radius-server**
**reload**
**show boot-config**
**show card**
**show card-inventory**

# broadcast

To send text messages to all other CLI users, enter the **broadcast** command in User Exec mode or Privileged Exec mode.

**broadcast** *message*

## Syntax Description

| | |
|---|---|
| *message* | Message to broadcast. This message may consist of one or more words and may include any alphanumeric character or symbol (except for quotation marks). |

## Defaults

This command has no default settings.

## Command Modes

User Execute mode, Privileged Execute mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

Unrestricted read-write user.

Multi-word messages must begin and end with quotation marks (“,”). Single-word messages do not require quotation marks.

You can broadcast a message to warn other CLI users about events that may impact their sessions, such as a network outage or major configuration change. A broadcast message appears on every active CLI session on the Server Switch, including the user who sends the message.

## Examples

The following example prints “FC card 5 going down in 10 minutes” to the terminal screens of all users on the Server Switch.

```
SFS-7000P# broadcast "FC card 5 going down in 10 minutes."
```

## Related Commands

**reload**
**who**
**write**

# card

To enter Card Configuration submode, enter the **card** command in Global Configuration mode.

**card** {*slot-list* | **all** | *digit* | *digit,digit* | *digit-digit*}

## Syntax Description

| | |
|---|---|
| *slot-list* | Card, list of cards, or range of cards to configure. |
| **all** | Configures all cards in the chassis. |
| *digit* \| *digit,digit* | Specifies the slot numbers for cards you want to configure in the chassis. |

## Defaults

This command has no default settings.

## Command Modes

Global Configuration (config) mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

Card-specific read-write user

Enter Card Configuration submode to enable, disable, configure, and reinitialize cards in your Server Switch.

## Examples

The following example enters Card Configuration submode for all cards on the Server Switch. Any commands that execute in this mode apply to all of the cards in the chassis.

```
SFS-7000P(config)# card all
SFS-7000P(config-card-1,6,11,15-16)#
```

## Related Commands

**clock set**
**delete**
**install**
**show card**
**show card-inventory**
**shutdown**

# cdp advertise-v2

To enable Cisco Discovery Protocol Version 2 (CDPv2) advertising functionality on a device, use the **cdp advertise-v2** command in global configuration mode. To disable advertising CDPv2 functionality, use the **no** form of the command.

**cdp advertise-v2**

**no cdp advertise-v2**

## Syntax Description

This command has no arguments or keywords

## Defaults

Enabled. CDP is running on chassis boot.

## Command Modes

Global Configuration (config) mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

Unrestricted and general read-write user.

Each device configured for CDP sends periodic messages, known as advertisements, to a multicast address. Each device advertises at least one address at which it can receive SNMP messages. The advertisements also contain time-to-live, or holdtime, information, which indicates the length of time a receiving device should hold CDP information before discarding it. Each device also listens to the periodic CDP messages sent by others in order to learn about neighboring devices and determine when their interfaces to the media go up or down.

CDP Version 2 is the most recent release of the protocol. With CDP Version-2, detailed information is provided on the VLAN Trunking Protocol (VTP) management domain and duplex modes of neighbor devices, CDP-related counters, and VLAN IDs of connecting ports. This can help the Ethernet gateway configuration. CDP is run on server switches over management-Ethernet interfaces. CDP Version 2 has three additional type-length values (TLVs): VTP Management Domain Name, Native VLAN, and full/half-Duplex.

**Note** CDP runs by default when a chassis boots up, but CDP is only learning in this mode. If any neighbors are advertisng, CDP will identify them.

## Examples

The following example sets the CDP advertisement for CDP version 2.

```
SFS-7000P(config)# cdp advertise-v2
```

**Related Commands**

cdp holdtime
cdp timer
show cdp
show cdp entry
show cdp neighbors
show clock

# cdp holdtime

To set the Cisco Discovery Protocol (CDP) transmission holdtime, enter the **cdp holdtime** command in Global Configuration mode.

**cdp holdtime** *seconds*

## Syntax Description

| | |
|---|---|
| *seconds* | Sets the number of seconds for transmission holdtime. |

## Defaults

This command has no default settings.

## Command Modes

Global Configuration (config) mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

Unrestricted and general read-write user.

CDP packets are sent with a time to live, or hold time, value. The receiving device will discard the CDP information in the CDP packet after the hold time has elapsed. You can set the hold time lower than the default setting of 180 seconds if you want the receiving devices to update their CDP information more rapidly. The CDP hold time must be set to a higher number of seconds than the time between CDP transmissions, which is set using the **cdp timer** command.

## Examples

The following example sets the CDP holdtime:

```
SFS-7000P(config)# cdp holdtime 120
```

## Related Commands

**cdp advertise-v2**
**cdp timer**
**show cdp**
**show cdp entry**
**show cdp neighbors**
**show clock**

# cdp run

To enable Cisco Discovery Protocol (CDP), use the **cdp run** command in global configuration mode. To disable CDP, use the **no** form of this command.

**cdp run**

**no cdp run**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Disabled

## Command Modes

Global Configuration (config) mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

Unrestricted and general read-write user.

CDP is enabled by default, which means the Cisco IOS software will receive CDP information. CDP also is enabled on supported interfaces by default. To disable CDP on an interface, use the **no cdp run** interface configuration command.

**Note** Because ODR (on demand routing) uses CDP, the **cdp enable**, **cdp timer**, and **cdp run** commands affect the operation of the **router odr** global configuration command. For more information on the router odr command, see the Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols document.

**Note** CDP is runs by default when a chassis boots up, but CDP is only learning in this mode. If any neighbors are advertisng, CDP will identify them.

## Examples

The following example starts CDP advertising on your chassis.

```
SFS-7000P(config)# cdp run
```

The following example starts CDP advertising on your chassis and specifies the CDP timer interval:

```
SFS-7000P# configure
SFS-7000P(config)# cdp run
SFS-7000P(config)# cdp timer 10
```

## Related Commands

cdp advertise-v2
cdp holdtime
cdp timer
show cdp
show cdp entry
show cdp neighbors
show clock

# cdp timer

To specify how often the Cisco IOS software sends Cisco Discovery Protocol (CDP) updates, use the **cdp timer** command in global configuration mode. To revert to the default setting, use the **no** form of this command.

**cdp timer** *seconds*

**no cdp timer**

## Syntax Description

| | |
|---|---|
| *seconds* | Sets the number of seconds for the transmission timer. |

## Defaults

80 seconds

## Command Modes

Global Configuration (config) mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

Unrestricted and general read-write user.

The trade-off with sending more frequent CDP updates to provide up-to-date information, is that bandwidth is used more often.

**Note** The c**dp timer**, and **cdp run** commands affect the operation of the IP on demand routing feature (that is, the router odr global configuration command). For more information on the **router odr** command, see the "On-Demand Routing Commands" chapter in the Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols document.

## Examples

The following example sets the CDP timer.

```
SFS-7000P(config)# cdp timer 120
```

## Related Commands

**cdp advertise-v2**
**cdp holdtime**
**cdp run**
**show cdp**
**show cdp entry**
**show cdp neighbors**
**show clock**

# clear cdp counters

To reset Cisco Discovery Protocol (CDP) traffic counters to zero, use the **clear cdp counters** command in privileged EXEC mode.

**clear cdp counters**

## Syntax Description

This command has no arguments or keywords.

## Defaults

This command has no default settings.

## Command Modes

Global Configuration (config) mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

Privileged EXEC mode.

## Examples

The following example sets the CDP counters to zero.

```
SFS-7000P(config)# clear cdp counters
```

## Related Commands

**cdp advertise-v2**
**cdp holdtime**
**cdp run**
**clear cdp table**
**show cdp**
**show cdp entry**
**show cdp neighbors**
**show clock**

# clear cdp table

To clear the table that contains Cisco Discovery Protocol (CDP) information about neighbors, use the **clear cdp table** command in privileged EXEC mode.

**clear cdp table**

## Syntax Description

This command has no arguments or keywords.

## Defaults

This command has no default settings.

## Command Modes

Privileged EXEC mode

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

Unrestricted and general read-write user.

## Examples

The following example sets the CDP counters to zero.

```
SFS-7000P(config)# clear cdp counters
```

## Related Commands

**cdp advertise-v2**
**cdp holdtime**
**cdp run**
**clear cdp counters**
**show cdp**
**show cdp entry**
**show cdp neighbors**
**show clock**

# clock set

To manually configure the time and date of the on-board Server Switch clock, enter the **clock set** command in Privileged Exec mode.

**clock set** *hh:mm:ss dd mm yy*

## Syntax Description

| | |
|---|---|
| *hh* | Hour to assign. |
| *mm* | Minute to assign. |
| *ss* | Second to assign. |
| *dd* | Day to assign. |
| *mm* | Month to assign. |
| *yy* | Year to assign. |

## Defaults

This command has no default settings.

## Command Modes

Privileged Execute mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

Unrestricted and general read-write user.

Your Server Switch uses one of the following means to maintain system time:

- an on-board system clock
- an external NTP server (recommended)

When you first power on your Server Switch, factory-default system clock settings run. To ensure accurate synchronization, we recommend that you use an external NTP server, as it will synchronize log dates with other management systems. To configure NTP servers, refer to the "ntp" section on page 2-53.

## Examples

The following example sets the clock time to 7:22 PM and 10 seconds on the 25th of May, 2015.

```
SFS-7000P# clock set 19:22:10 25 05 15
```

## Related Commands

**card**
**ntp**
**radius-server**
**show clock**

# configure system

To disable theIB port regular counter resetting feature, enter the **configure system** command in Privileged Exec mode. To reenable the IB port regular counter resetting feature, use the **no** form of this command.

**configure system ib-counter-reset**

**no configure system ib-counter-reset**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Counter resetting is enabled.

## Command Modes

Global Configuration mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

Unrestricted and general read-write user.

Use the **configure system** command to disable or enable the regular counter resetting. This is a global chassis-wide setting allowing you to disable or enable all IB port agents and all IB ports within a chassis.

## Examples

The following example enters Global Configuration mode.

```
SFS-7000P# configure system
SFS-7000P(config)#
```

# configure terminal

To enter Global Configuration mode, enter the **configure terminal** command in Privileged Exec mode.

**configure terminal**

## Syntax Description

This command has no arguments or keywords.

## Defaults

This command has no default settings.

## Command Modes

Privileged Execute mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

Unrestricted and general read-write user.

Use the **configure terminal** command to enter Global Configuration mode. From this mode, you can configure gateway and switch cards, subnet management, IP addressing, and various aspects of your Server Switch.

## Examples

The following example enters Global Configuration mode.

```
SFS-7000P# configure terminal
SFS-7000P(config)#
```

## Related Commands

**arp ethernet**
**authentication**
**boot-config**
**bridge-group**
**card**
**show diagnostic**
**exit**
**fc srp initiator**
**fc srp initiator-wwpn**
**fc srp it**
**fc srp itl**
**fc srp lu**
**fc srp target**
**fc srp-global gateway-portmask-policy restricted**
**fc srp-global itl**
**fc srp-global lun-policy restricted**
**ftp-server enable**

# copy

To copy files

- to your Server Switch from a remote location,
- from your Server Switch to a remote location,
- from one directory on your Server Switch to another,

enter the **copy** command in Privileged Exec mode.

**copy ftp**:*//user-id*:*password@host*[*/path*]/*file-name* [*slot-number*:]*file-system*[:*file-name*]

Downloads a file from a FTP server.

**copy scp**:*//user-id*:*password@host*[*/path*]/*file-name* [*slot-number*:]*file-system*[:*file-name*]

Securely transfers files from a remote server to the chassis.

**copy tftp**:*//remote-system*[*/path*]/*file-name* [*slot-number*:]*file-system*[:*file-name*]

Downloads a file from a remote TFTP server.

**copy** {[*slot-number*:]*file-system*:*file-name* | **startup-config** | **running-config**} **ftp**:*//user-id*:*password@host*[*/path*]/[*file-name*]

Uploads a file to a FTP server.

**copy running-config startup-config**

Saves the running configuration as the startup configuration.

**copy** [*slot-number*:]*file-system*:*file-name* **running-config**

Executes a configuration file without a system reboot.

## Syntax Description

| | |
|---|---|
| **ftp** | Identifies a remote system that runs file transfer protocol (FTP). |
| **scp** | Securely transfers files from a remote server to the chassis. |
| **tftp** | Identifies a remote system that runs trivial file transfer protocol (TFTP). |
| **remote-system** | IP address (or DNS name, if appropriate) of the remote host. |
| **running-config** | Refers to the active configuration running on your Server Switch. |
| **startup-config** | Refers to the configuration that your Server Switch runs when it boots. |
| *user-id* | User ID that you use to log in to the FTP server. |
| *password* | Password that you use to log in to the FTP server. |
| *host* | FTP server domain name or IP address. |
| *path* | (Optional) Directory path on the host from which or to which you want to copy a file. |
| *slot-number* | (Optional) Slot of the controller card (1 on the Cisco SFS 3001, Cisco SFS 7000, and IB Server Switch Module; 1 or 14 on the Cisco SFS 3012; 11 or 12 on the Cisco SFS 7008). |

| | |
|---|---|
| *file-name* | (Optional) Name of the file that you want to copy. |
| *file-system* | File system on your Server Switch. |

## Defaults

This command has no default settings.

## Command Modes

Privileged Execute mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

Unrestricted read-write user.

Use the **copy** command to save a running configuration as a boot-up configuration, to download image files to install, or to upload configurations that you want to propagate to other Server Switches. The **copy** command copies image, configuration, and log data locally as well as onto and off of the system chassis.

**Note** If an administrator has configured the system-mode to VFrame, the Server Switch does not apply SRP configuration changes to the startup configuration. For more information, refer to this command: system-mode, page 2-69.

The **copy** command can also execute the contents of a configuration file.

**Note** Configuration files that you upload from your Server Switch to a remote host contain plain text that you can read with any word processor. Log files also appear in plain text.

You may download image and configuration files from an FTP server to the system chassis. You may also upload log and configuration files from the system chassis to an FTP server.

Download image files to your Server Switch to upgrade system firmware. Download configuration files to quickly replicate a desired configuration. Upload configuration and log files to maintain back-ups and to troubleshoot your Server Switch.

Image files require additional processing. Your Server Switch can run an image only after you install the image file. For more information on how to install an image, refer to this command: install, page 2-40.

After you download a configuration file to your Server Switch, you can use the **boot-config** command to configure your Server Switch to load that configuration when you reboot the Server Switch.

The **copy** command recognizes **Ctrl-c** as a command to terminate a file transfer. Use **Ctrl-c** to cancel a transfer if the network hangs.

**Note** You can only download image and configuration files. Log files cannot be downloaded. You can only upload configuration and log files. System image data cannot be uploaded.

## Examples

The following example downloads an image file from a remote host to the Server Switch:

```
SFS-7000P# copy ftp://bob:mypassword@10.0.0.5/SFS-7000P-sfsOS-2.3.0-build497.img
image:SFS-7000P-2.3.0-build497.img

sfsOS-2.3.0-build497.img
operation completed successfully
```

The following example saves the running configuration as the startup configuration so the current configuration executes when the Server Switch reboots:

```
SFS-7000P# copy running-config startup-config
operation completed successfully

SFS-7000P
```

The following example copies the startup configuration image from the controller card in slot 1 on a Cisco SFS 3012 to the controller card in slot 14:

```
SFS-7000P# copy 1:config:startup-config 14:config:save.cfg
** operation completed successfully
```

## Related Commands

**action**
**boot-config**
**delete**
**dir**
**exec**
**ftp-server enable**
**history**
**install**
**show boot-config**
**show fan**

# delete

To remove image, configuration, or log files from your Server Switch, enter the **delete** command in Privileged Exec mode.

**delete** [*slot-number*:]*file-system*:*file*

## Syntax Description

| | |
|---|---|
| *file-system* | Server Switch file system. Your Server Switch displays this internal directory by name only. The file systems are config, images, and syslog. The specified file system must be appropriate to the type of file that you want to delete. For example, if you attempt to delete a configuration file from the syslog file system, an error occurs because the name of the file does not match the file system. A colon (:) always follows the file-system specification.<br>**Note** The startup configuration maps to config:startup-config. Therefore, you do not need to specify the file system at the CLI. |
| *slot-number* | (Optional) Slot of the controller card (1 on the Cisco SFS 3001 and Cisco SFS 7000, 1 or 14 on the Cisco SFS 3012). |
| *file* | Name of the configuration, image, or log file that you want to delete. |

## Defaults

This command has no default settings.

## Command Modes

Privileged Execute mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

Unrestricted read-write user.

You cannot delete an active image. To deactivate an active system image in order to delete it, install a new image using this command: (install, page 2-40) and configure your Server Switch to boot that image using this command: (boot-config, page 2-9), then delete the old image.

## Examples

The following example deletes the delete-me.cfg file from the controller card in slot 1 of a Cisco SFS 3012.

```
SFS-7000P# delete 1:config:delete-me.cfg
Delete file 1:delete-me.cfg? [yes(default) | no] yes
******
```

The following example deletes an image file from the controller card in slot 14 of a Cisco SFS 3012.

```
SFS-7000P# delete 14:image:sfs360-sfsOS-2.0.0-build488.img
Delete file 14:sfs360-sfsOS-2.0.0-build488.img? [yes(default) | no] yes
******
```

## Related Commands

boot-config
copy
dir
install

# dir

To list the configuration, log, and system image files on your Server Switch, enter the **dir** command in Privileged Exec mode.

**dir** [*slot-number*:]{**config** | **image** | **syslog**}

## Syntax Description

| | |
|---|---|
| *slot-number* | (Optional) Slot of the controller card (1 on the Cisco SFS 3001 and Cisco SFS 7000, 1 or 14 on the Cisco SFS 3012, 11 or 12 on the Cisco SFS 7008). |
| **config** | Lists all configuration files in the config directory. |
| **image** | Lists the current image files and system images in the image directory. Image files end with a .img extension. Installed system images look like path names.<br>**Note** You must unpack and install image files before they can boot the system. For more information, refer to this command: install, page 2-40. |
| **syslog** | Lists the log files in the syslog directory. |

## Defaults

This command has no default settings.

## Command Modes

Privileged Execute mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

General read-only user.

Use this command to list the files on your Server Switch. This command requires one of three arguments: **config**, **image**, or **syslog**. Files reside on the Server Switch in separate file systems. The CLI automatically tracks these file systems so you do not need to include file-path information to administer these files.

Use the **dir** command with the **image** keyword to see the installed image directories on your Server Switch.

On the Cisco SFS 3012, use the *slot-number* variable to view files on the controller card in slot 1 or slot 14. The **dir** command lists the files of the active controller by default.

## Examples

The following example displays the configuration files on the Server Switch:

```
SFS-7000P# dir config
==============================================================================
                        Existing Configurations on System
==============================================================================
slot    date-created                    size       file-name
```

```
---------------------------------------------------------------------------
1       Thu Oct 24 11:21:06 2002       58         check.cfg
1       Thu Dec  5 14:50:09 2002       39216      check2.cfg
1       Wed Dec 11 09:09:54 2002       1712       config_bc.cfg
1       Thu Dec  5 11:18:21 2002       1712       running_config.cfg
1       Wed Dec  4 07:10:23 2002       4407       running_config.cfg.backup
1       Thu Dec  5 12:04:53 2002       1712       running_config2.cfg
1       Thu Oct 24 11:19:53 2002       58         test.cfg
SFS-7000P#
```

The following example displays installed system images and image files on the Server Switch:

```
SFS-7000P# dir image
==============================================================
             Existing Boot-Images on System
==============================================================
slot    date-created                   size       file-name
---------------------------------------------------------------------------
1       Thu Jun 1 11:16:50 2003       23691613   TopspinOS-1.1.3-build548.img
1       Wed Jul 11 00:56:52 2002       1024       TopspinOS-1.1.3/build541
1       Thu Jul 1 00:10:40 2003       1024       TopspinOS-1.1.3/build548
SFS-7000P#
```

The following example displays the log files in the syslog directory on the Server Switch.

```
SFS-7000P# dir syslog
===========================================================================
                        Existing Syslog-files on System
===========================================================================
slot    date-created                   size       file-name
---------------------------------------------------------------------------
1       Thu Jun 12 12:13:06 2002       19636      ts_log
1       Wed Jun 11 13:28:54 2002       4978       ts_log.1.gz
1       Tue Jun 10 04:02:02 2002       30         ts_log.2.gz
1       Mon Jun 9 04:02:02 2002       30         ts_log.3.gz
1       Sun Jul 8 04:02:02 2002       30         ts_log.4.gz
1       Sat Jul 7 04:02:02 2002       30         ts_log.5.gz
1       Fri Jul 6 17:20:35 2002       16264      ts_log.6.gz
1       Thu Jul 5 15:14:57 2002       245        ts_log.7.gz
SFS-7000P#
```

The following example displays the files in the image directory on the controller in slot 14 of a Cisco SFS 3012.

```
SFS-7000P# dir 14:image


==============================================================================
                         Existing Boot-Images on System
==============================================================================
slot date-created              size      file-name
------------------------------------------------------------------------------
14   Thu Mar 18 14:59:06 2004  0         TopspinOS-2.0.0/build488
```

## Related Commands

**boot-config**
**copy**
**delete**
**install**
**more**

# disable

To exit Privileged Exec mode and return to User Exec mode, enter the **disable** command in Privileged Exec mode.

To disable a trunk group, enter the **disable** command in Trunk Interface Configuration submode.

**disable**

## Syntax Description

This command has no arguments or keywords.

## Defaults

This command has no default settings.

## Command Modes

Privileged Execute mode, Trunk Interface Configuration (config-if-trunk) submode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

General read-only user.

## Examples

The following example exits Privileged Exec mode and enters User Exec mode.

```
SFS-7000P# disable
SFS-7000P>
```

The following example deletes a trunk group.

```
SFS-7000P(config-if-trunk)# disable
```

## Related Commands

**enable**
**show interface ethernet**

# enable

To enter Privileged Exec mode from User Exec mode, enter the **enable** command in User Exec mode.

To enable a trunk group, enter the **enable** command in Trunk Interface Configuration submode.

**enable**

## Syntax Description

This command has no arguments or keywords.

## Defaults

This command has no default settings.

## Command Modes

User Execute mode, Trunk Interface Configuration (config-if-trunk) mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

General read-only user.

Enter the **enable** command in User Exec mode to make administrative configuration changes to your Server Switch. Enter the **enable** command in Trunk Interface Configuration submode to activate a trunk group.

## Examples

The following example enters Privileged Exec mode from User Exec mode.

```
SFS-7000P> enable
SFS-7000P#
```

The following example enables a new trunk group.

```
SFS-7000P(config-if-trunk)# enable
```

## Related Commands

**configure terminal**
**disable**
**exit**

# exec

To execute a file in the config file system on your Server Switch, enter the **exec** command in Privileged Exec mode.

**exec** *file-name*

## Syntax Description

| | |
|---|---|
| *file-name* | Name of the file that you want to execute. |

## Defaults

This command has no default settings.

## Command Modes

Privileged Execute mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

Unrestricted read-write user.

You can create command files on a management workstation and copy them to config file system on the switch using **copy** command. Then you can execute these files with **exec** command. Use the **save-log** command to save the latest commands that you have executed in the CLI to a file, then copy the file to the management station and use it as an example. See the **save-log** and **copy** commands for further details.

**Note** You can only run files from the config directory of your file system.

## Examples

The following example executes the test.cfg file in the config file system on the Server Switch.

```
SFS-7000P# exec test.cfg
```

## Related Commands

**configure terminal**
**copy**

# exit

To exit your current CLI mode and return to the previous mode, enter the **exit** command in any mode.

**exit** [**all**]

## Syntax Description

| | |
|---|---|
| **all** | (Optional) Returns you to User Execute mode from any other CLI mode. |

## Defaults

This command has no default settings.

## Command Modes

All modes.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

All users.

The **exit** command performs different functions in different modes.

*Table 2-1 Exit Command Modes and Functions*

| Mode(s) | Function |
|---|---|
| User Exec<br>Privileged Exec | Logs you out of the Server Switch. |
| Global Configuration | Returns you to Privileged Exec mode. |
| Configuration submode (any) | Returns you to Global Configuration mode. |

## Examples

The following example exits Card Configuration submode and enters User Exec mode.

```
SFS-7000P(config-card-1,2)# exit all
SFS-7000P>
```

## Related Commands

**enable**
**login**
**logout**

# ftp-server enable

To enable the FTP server on your Server Switch, enter the **ftp-server enable** command in Global Configuration mode. To disable this feature, use the **no** form of this command.

**ftp-server enable**

**no ftp-server enable**

## Syntax Description

This command has no arguments or keywords.

## Defaults

This command has no default settings.

## Command Modes

Global Configuration (config) mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

All users.

The FTP server feature provides read-only access to the file systems on the Server Switch, and complements the **copy** command. Use a FTP client on a management workstation to connect to the server via FTP protocol. You can download log files, configuration files or image files.

## Examples

The following example disables FTP services on the Server Switch.

```
SFS-7000P(config)# no ftp-server enable
```

## Related Commands

**show system-services**
**copy**
**telnet**

# gateway

To assign a default IP gateway to

- the Ethernet Management port,
- the virtual in-band InfiniBand port,

enter the **gateway** command in the appropriate Interface Configuration mode. To disassociate a port from a gateway, use the **no** form of this command.

**gateway** *gateway*

**no gateway**

## Syntax Description

| | |
|---|---|
| *gateway* | IP address of the gateway to assign to the port. |

## Defaults

The gateway address defaults to 0.0.0.0.

## Command Modes

Ethernet Management Interface Configuration (config-if-mgmt-ethernet) submode, InfiniBand Management Interface Configuration (config-if-mgmt-ib) submode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

Unrestricted read-write user.

The gateway that you assign connects the port to the InfiniBand backplane on your Server Switch. You must configure the gateway through the Serial Console port. Enter the IP address of the gateway when you configure the management interfaces.

## Examples

The following example assigns a default IP gateway to the Ethernet Management interface.

```
SFS-7000P(config-if-mgmt-ethernet)# gateway 10.3.0.94
```

The following example assigns a default IP gateway to the InfiniBand Management interface.

```
SFS-7000P(config-if-mgmt-ib)# gateway 10.3.0.2
```

## Related Commands

**show interface mgmt-ethernet**
**show interface mgmt-ib**
**snmp-server**

# help

To view the help options that the CLI provides, enter the **help** command in any mode.

**help**

## Syntax Description

This command has no arguments or keywords.

## Defaults

This command has no default settings.

## Command Modes

All modes.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

All users.

This command may be executed in any mode. It provides the methods for you to display the various types of available help. The **help** command provides the same instructions regardless of mode.

## Examples

The following example displays help options.

```
SFS-7000P(config-if-ib-16/1-16/12)# help
Help may be requested at any point in a command by entering
a question mark '?'. If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show pr?'.)
SFS-7000P360(config-if-ib-16/1-16/12)#
```

# history

To display a list of the commands that you executed during your CLI session, enter the **history** command in any mode.

**history**

## Syntax Description

This command has no arguments or keywords.

## Defaults

The **history** command stores the last 40 commands that you entered.

## Command Modes

All modes.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

All users.

The format of the history output and a configuration file are similar. You can cut and paste the contents of the history output to a text file and, with minor editing, use it as a configuration file.

This global command may be executed in any mode. To display just one screen of history data at a time, configure the terminal display length.

## Examples

The following example displays the recent command history.

```
SFS-7000P(config)# history
  1 history
  2 enable
  3 config
  4 arp
  5 boot-conf
  6 boot-config
  7 diagn
  8 interface ib all
  9 exit
  10 interface ethernet all
  11 ip
  12 history
SFS-7000P(config)#
```

## Related Commands

**copy**
**telnet**
**show fan**
**show system-services**

# hostname

To assign a hostname to your Server Switch, enter the **hostname** command in Global Configuration mode.

**hostname** *name*

## Syntax Description

| | |
|---|---|
| **name** | Name to assign to the system. |

## Defaults

This command has no default settings.

## Command Modes

Global Configuration (config) mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

Unrestricted read-write user.

When you enter the **hostname** command, you apply the new name to the following three areas:

**Step 1** Server Switch version information

**Step 2** CLI prompt

**Step 3** Server Switch network name

After you configure the host name, the name that you assigned appears in the **show version** command output. When you change modes, the new host name will appear in the CLI prompt.

## Examples

Note the change in the CLI prompt that occurs in the last line of example output.

```
SFS-7000P(config)# hostname samplename
SFS-7000P(config)# exit
samplename#
```

## Related Commands

**ip**
**ping**
**show version**

# install

To install an image file on your Server Switch, enter the **install** command in Privileged Exec mode.

**install** [*slot-number*:]**image:***file*

## Syntax Description

| | |
|---|---|
| *slot-number* | (Optional) Slot of the controller card (1 on the Cisco SFS 3001, Cisco SFS 7000, and IB Server Switch Module; 1 or 14 on the Cisco SFS 3012; 11 or 12 on the Cisco SFS 7008). |
| **image** | Specifies that the file resides in the image file-system. |
| *file* | The name of the image file to install. |

Image files must reside in the image file system and the file name must have the .img extension.

## Defaults

This command has no default settings.

## Command Modes

Privileged Execute mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

Unrestricted read-write user.

To run a new system image, you must perform the following steps:

**Step 1** Download an image file to your Server Switch (see this command: copy, page 2-24).

**Step 2** Bring up all cards in your chassis.

**Step 3** Install the image file with the **install** command.

**Step 4** Configure your Server Switch to run the new system image when it boots (see this command: boot-config, page 2-9).

**Step 5** (Optional) Execute the **action** command with the **delete-inactive-images** keyword for each card in your chassis to remove old images.

The **install** command performs everything necessary to install a new system image to flash memory. It automatically installs all necessary firmware and component images. The command updates all cards with an administrative status of **up**.

To update additional cards, re-enter the **install** and **boot-config** commands after you add the cards.

**Note** When you upgrade your Server Switch, your configuration file persists.

## Examples

The following example installs a new image on the Server Switch.

```
SFS-7000P# install image:SFS-7000P-sfsOS-2.3.0-build497.img
************************** operation completed successfully
SFS-7000P#
```

**Note** If you try to install an OS image designed for Anafa chips on a system with Anafa 2 chips, you will receive an error message.

```
TS120-1# install image:sfs120-sfsOS-2.2.0-build556.img
Proceed with install? [yes(default) | no]
****************************
Error: This image cannot be used with the Anafa2 chip(s) installed.
```

## Related Commands

**action**
**boot-config**
**card**
**dir**
**reload**
**show boot-config**
**show card**
**shutdown**

# ip http

To enable or configure HTTP and HTTPS services on your Server Switch, enter the **ip http** command in Global Configuration mode. To disable service or change a port number to the default value, use the **no** form of this command.

**ip http** {**polling** | **port** *number* | **secure-cert-common-name** {**useSysName** | **useMgmtEnetIpAddr** | **useMgmtIbIpAddr**} | **secure-port** | **secure-server** | **server**}

**no ip http** {**polling** | **port** | **secure-port** | **secure-server** | **server**}

## Syntax Description

| | |
|---|---|
| **polling** | Enables polling on the Server Switch. |
| **port** | Specifies the HTTP port that the HTTP server uses. Returns the port configuration to the default value (80) when you use the **no** form of the command. |
| **secure -cert-common-name** | Specifies where to get the common name used to generate a SSL certificate. |
| **server** | Enables the HTTP server on your Server Switch. Use this keyword with the **no** form of the command to disable the HTTP server. |
| **useSysName** | Configures your Server Switch to use its system name (that you configure with the **hostname** command) in SSL certificates. |
| **useMgmtEnetIpAddr** | Configures your Server Switch to use the IP address of its Ethernet Management Port in SSL certificates. |
| **useMgmtIbIpaddr** | Configures your Server Switch to use the IP address of its InfiniBand Management Port in SSL certificates. |
| **secure-port** | Specifies the HTTPS port that the HTTP server uses. Returns the port configuration to the default value (443) when you use the **no** form of the command. |
| **secure-server** | Enables HTTPS with Secure Sockets Layer (SSL) on your Server Switch. Use this keyword with the **no** form of the command to disable HTTPS. |
| *number* | HTTP port (integer) that the HTTP server uses. |

## Defaults

The HTTP port value defaults to 80.
HTTP services on your Server Switch run by default.
The HTTPS port value defaults to 443.
HTTPS services on your Server Switch run by default.

## Command Modes

Global Configuration (config) mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

Ethernet read-write user.

Configure the **ip http** command to run Chassis Manager. For more information, refer to the *Chassis Manager User Guide*.

## Examples

The following example enables the HTTP server on the Server Switch:

```
SFS-7000P(config)# ip http server
```

## Related Commands

**show ip http**
**show ip http server secure**

# link-trap

To configure internal and external ports to generate link-up and link-down SNMP traps when the operating status (oper-status) of the ports changes, enter the **link-trap** command in the appropriate Interface Configuration mode. To disable this function, use the **no** form of this command.

**link-trap**

**no link-trap**

## Syntax Description

This command has no arguments or keywords.

## Defaults

By default, ports do not generate link traps.

## Command Modes

All Interface Configuration submodes.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

Fibre Channel read-write user, Ethernet read-write user.

Ports generate link-up traps when the oper-status of the port changes to **up** and link-down traps when the oper-status of the port changes to **down**. Trap receivers (that you define with the **snmp-server** command) receive the traps. You can then perform link validation and checking with the receivers, or configure SNMP alerts.

## Examples

The following example enables link-trap generation for Fibre Channel interface ports 1and 2, on card 5.

```
SFS-7000P(config-if-fc-5/1-5/2)# link-trap
```

The following example enables link-trap generation for InfiniBand interface ports 1 through 5 on card 15. The resulting traps are sent to trap receivers, as defined by the **snmp-server** command.

```
SFS-7000P(config-if-ib-15/1-15/5)# link-trap
```

The following example enables link-trap generation for Ethernet interface port 1 on card 4. The resulting traps are sent to trap receivers, as defined by the **snmp-server** command.

```
SFS-7000P(config-if-ether-4/1)# link-trap
```

## Related Commands

**auto-negotiate**
**shutdown**
**show snmp**
**snmp-server**

# location

To assign a text-based location identifier to your Server Switch, enter the **location** command in Global Configuration mode. To reset the location to an empty string, use the **no** form of this command.

**location** "*string*"

**no location**

## Syntax Description

| | |
|---|---|
| *string* | Refers to an ASCII text string. Enclose multi-word strings within double-quotes (“,”). |

## Defaults

This command has no default settings.

## Command Modes

Global Configuration (config) mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

Unrestricted read-write user.

Use the **location** command to assign a readable identifier to your Server Switch. Use the location string to identify support providers, the Server Switch owner, the Server Switch itself, or the physical location of the Server Switch. Display the location with the **show location** command.

**Note** The **location** command configures the same parameter that the **snmp-server** command configures with the **location** and *location-string* arguments.

## Examples

The following example assigns a location to the Server Switch.

```
SFS-7000P(config)# location "515 Ellis Street, Mountain View, CA 94043"
```

## Related Commands

**snmp-server**
**show location**
**show version**

# logging

To identify a remote server as a server that accepts log messages from your Server Switch, enter the **logging** command in Global Configuration mode.

**logging** *ip-address*

## Syntax Description

| | |
|---|---|
| *ip-address* | IP address of the remote syslog server. |

## Defaults

This command has no default settings.

## Command Modes

Global Configuration (config) mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

All users.

Warnings, errors, notifications, and alerts occur once the system boots successfully. The **logging** command sends these occurrences to the remote server that you specify.

## Examples

The following example configures the Server Switch to send log messages to the host with an IP address of 10.3.0.60.

```
SFS-7000P(config)# logging 10.3.0.60
```

## Related Commands

**show logging**
**terminal**
**snmp-server**
**show snmp**

# login

To change user identity during a CLI session, enter the **login** command in User Exec mode or Privileged Exec mode.

**login** *userid*

## Syntax Description

| | |
|---|---|
| *userid* | User ID that you want to use to log in. |

## Defaults

This command has no default settings.

## Command Modes

User Execute mode, Privileged Execute mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

All users.

The **login** command allows you to assume the identity of another user without having to exit the CLI. The CLI prompts you for your password.

**Note** To change back to a previous login, do not use the **logout** command. Instead, use the **login** command again.

## Examples

In the following example, the user moves from the current login to the **super** login.

```
SFS-7000P> login super
Password: xxxxx
SFS-7000P>
```

## Related Commands

**exit**
**logout**
**username**
**show user**

# logout

To log out of the current CLI session, enter the **logout** command in User Exec mode or Privileged Exec mode.

**logout**

## Syntax Description

This command has no arguments or keywords.

## Defaults

This commandhas no default settings.

## Command Modes

User Execute mode, Privileged Execute mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

All users.

The **logout** command ends the current CLI session. If logged in through the Serial Console port, the CLI login prompt appears. If logged in through a Telnet connection, the Telnet session ends and you are returned to your operating system.

## Examples

The following example logs the user out of the CLI.

```
SFS-7000P# logout
SFS-7000P#
Connection to host lost.
```

## Related Commands

**exit**
**login**

# more

To view the contents of a text file on your terminal screen, enter the **more** command in Privileged Exec mode.

**more** [*slot-number*:]*file-system*:*file-name*

## Syntax Description

| | |
|---|---|
| *slot-number* | (Optional) Slot of the controller card (1 on the Cisco SFS 3001 and Cisco SFS 7000, 1 or 14 on the Cisco SFS 3012). |
| *file-system* | File system on your Server Switch in which the text file resides.<br>**Note** For the startup configuration file, you do not need to include the file system in the command syntax. |
| *file-name* | Name of the file to display. |

## Defaults

This command has no default settings.

## Command Modes

Privileged Execute mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

General read-write user.

The **more** command displays text data resident on the chassis in increments determined by the **terminal length** command. The specified file-system must be appropriate for the file. See also the **dir** command to list the names of files in the respective file-systems.

Press any key (except the **q** key) to display the next screen of text lines.

The *file-system* variable represents the file system that contains the file. The file system variable may be **config** or **syslog**. You cannot display image file data or compressed system log files. Only the currently active log file, ts_log, may be viewed.

## Examples

The following example displays the contents of the startup configuration file.

```
SFS-7000P# more config:startup-config
!   TopspinOS-2.3.0/build560
!   Fri Mar 15 18:06:10 1935
enable
config terminal
!
boot-config primary-image-source TopspinOS-2.3.0/build560
!
interface mgmt-ethernet
 ip address 10.3.106.25 255.255.0.0
 gateway 10.3.0.1
 no shutdown
```

```
!
SFS-7000P#
```

**Note** The lines beginning with an exclamation point (!) are comments ignored when the configuration file executes.

The following example displays the contents of the hwif_log file.

```
SFS-7000P# more 14:syslog:hwif_log
Mon Mar  1 00:32:10 2004: card_startup.x : card is starting up
Mon Mar  1 00:32:26 2004: POST: Tavor: Firmware rev 200000000 matches tavor_fw.A
1.200000000.bin: PASSED
Mon Mar  1 03:58:49 2004: card_startup.x : card is starting up
Mon Mar  1 03:59:05 2004: POST: Tavor: Firmware rev 200000000 matches tavor_fw.A
1.200000000.bin: PASSED
Mon Mar  1 04:01:37 2004: card_startup.x : card is starting up
Mon Mar  1 04:01:53 2004: POST: Tavor: Firmware rev 200000000 matches tavor_fw.A
1.200000000.bin: PASSED
Mon Mar  1 04:04:27 2004: card_startup.x : card is starting up
Mon Mar  1 04:04:43 2004: POST: Tavor: Firmware rev 200000000 matches tavor_fw.A
1.200000000.bin: PASSED
Mon Mar  1 04:07:10 2004: card_startup.x : card is starting up
Mon Mar  1 04:07:26 2004: POST: Tavor: Firmware rev 200000000 matches tavor_fw.A
1.200000000.bin: PASSED
Mon Mar  1 19:27:10 2004: card_startup.x : card is starting up
Mon Mar  1 19:27:26 2004: POST: Tavor: Firmware rev 200000000 matches tavor_fw.A
1.200000000.bin: PASSED
Mon Mar  1 19:30:39 2004: card_startup.x : card is starting up
Mon Mar  1 19:30:55 2004: POST: Tavor: Firmware rev 200000000 matches tavor_fw.A
1.200000000.bin: PASSED
Mon Mar  1 19:55:33 2004: card_startup.x : card is starting up
Mon Mar  1 19:55:50 2004: POST: Tavor: Firmware rev 200000000 matches tavor_fw.A
```

## Related Commands

**dir**
**telnet**
**terminal**

# mtu

To configure the maximum transmission unit on the chassis, enter the **mtu** command in InfiniBand Management Interface Configuration submode.

**mtu** *integer*

**no mtu**

## Syntax Description

| | |
|---|---|
| *integer* | Slot of the controller card (1 on the Cisco SFS 3001 and Cisco SFS 7000, 1 or 14 on the Cisco SFS 3012). |

## Defaults

The IB MTU value defaults to 1500.

## Command Modes

InfiniBand Management Interface Configuration submode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

General read-write user.

The maximum possible MTU for InfiniBand is higher than the MTU for Ethernet. To smoothly transition traffic through Ethernet gateways, the factory setting of IB MTU matches the maximum Ethernet setting. On an IB-only network, you can set the MTU as high as 2044

## Examples

The following example configures the IB MTU:

```
SFS-120(config-if-mgmt-ib)# mtu 1500
```

## Related Commands

**show interface mgmt-ib**

# name

To assign a user-defined name to an interface port, enter the **name** command in the appropriate Interface Configuration submode.

**name** *string*

## Syntax Description

| | |
|---|---|
| **string** | Alphanumeric ASCII text string (up to 20 characters, including spaces) to assign to one or more ports. |

## Defaults

By default, the name of a port appears as a slot#/port# pair.

## Command Modes

Interface Configuration (config-if-fc, config-if-ib, config-if-ether) submodes.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

Fibre Channel read-write user, InfiniBand read-write user, Ethernet read-write user.

The name can be used to simplify port identification and indicate port use. Assign the same name to multiple ports to identify the ports as a group with a uniform function. The name that you assign appears in the **name** field of the appropriate **show interface** command.

## Examples

The example below assigns the name “storage bank 3” to all the ports on Fibre Channel interface card 5, ports 1-2.

```
SFS-7000P(config-if-fc-5/1-5/4)# name "storage bank 3"
```

This example assigns the name “InfiniBand Group 1-6” to the first 6 ports of InfiniBand card 15.

```
SFS-7000P(config-if-ib-15/1-15/6)# name "InfiniBand Group 1-6"
```

## Related Commands

**auto-negotiate**
**show fc srp initiator**
**show ib sm configuration**
**show interface ethernet**
**show interface fc**
**show interface ib**

# ntp

To synchronize the clock on your Server Switch to primary, secondary, and tertiary NTP servers, enter the **ntp** command in Global Configuration mode. To reset an NTP configuration to the default value, use the **no** form of this command.

**ntp** {**server-one** | **server-two** | **server-three**} *ip-address*

**no ntp** {**server-one** | **server-two** | **server-three**}

## Syntax Description

This command has no arguments or keywords.

## Defaults

This command has no default settings.

## Command Modes

Global Configuration (config) mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

Unrestricted read-write user.

Use the **ntp** command to configure your Server Switch to take time information from up to three servers so that your Server Switch can identify a problem when one server sends faulty data packets. We strongly recommend that you configure all three servers for maximum precision.

## Examples

The following example assigns primary, secondary, and tertiary NTP servers to the Server Switch.

```
SFS-7000P(config)# ntp server-one 10.0.3.110
SFS-7000P(config)# ntp server-two 10.0.3.111
SFS-7000P(config)# ntp server-three 10.0.3.112
```

## Related Commands

**clock set**
**show clock**
**show ntp**
**snmp-server**

# ping

To verify that your Server Switch can reach a given host, enter the **ping** command from User Exec mode or Privileged Exec mode.

**ping** *host*

## Syntax Description

| | |
|---|---|
| *host* | IP address or hostname of the host, port, or expansion module that you want to reach. |

## Defaults

This command has no default settings.

## Command Modes

User Execute mode, Privileged Execute mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

General read-only user.

Use the **ping** command to verify connectivity between your Server Switch and a host or port. The reply packet tells you if the host received the ping and the amount of time it took to return the packet.

**Note** You must configure a DNS server on your network to use hostnames as an argument in the **ping** command.

## Examples

The following example verifies that the Server Switch can contact the device with an IP address of 10.3.102.24.

```
SFS-7000P# ping 10.3.102.24
Sending 5 ICMP Echoes to 10.3.102.24, 56 data bytes
!!!!!
Success rate is 100 percent (5/5)
round-trip min/avg/max = 0.000000/0.000000/0.000000 ms
SFS-7000P#
```

## Related Commands

**hostname**
**ip**

# power-supply

To enter Power Supply Configuration submode, enter the **power-supply** command from Global Configuration mode.

**power-supply** [**all** | *selection*]

## Syntax Description

| | |
|---|---|
| **all** | (Optional) Configures all power supplies. |
| *selection* | (Optional) Selection of power supplies to configure. |

## Defaults

This command has no default settings.

## Command Modes

Global Configuration mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 7000, Cisco SFS 7008

**Privilege Level:**

General read-write user.

Use the **shutdown** or **no shutdown** commands to bring down and bring up power supplies. The command will only let you bring down one power supply at a time.

## Examples

The following example enters Power Supply Configuration submode for all power supplies.

```
SFS-120(config)# power-supply all
```

## Related Commands

**show power-supply**

# radius-server

To configure the RADIUS server that your Server Switch uses to authenticate CLI user logins, enter the **radius-server** command in Global Configuration mode. To remove a RADIUS server from the configuration, use the **no** form of this command.

**radius-server host** *ip-address* [**auth-port** *udp-port*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *encryption-key*]

**no radius-server host** *ip-address*

## Syntax Description

| | |
|---|---|
| **host** | Specifies the IP address of the RADIUS server. |
| *ip-address* | IP address of the RADIUS server. |
| **auth-port** | (Optional) Specifies the user datagram protocol (UDP) authentication port of the RADIUS server. |
| *udp-port* | (Optional) UDP authentication port of the RADIUS server. |
| **timeout** | (Optional) Specifies the amount of time that your Server Switch waits for a reply from the server before the login request times out. |
| *seconds* | (Optional) Amount of time, in seconds, that your Server Switch waits for a reply from the server before the login request times out. |
| **retransmit** | (Optional) Specifies the number of times that your Server Switch tries to authenticate after a timeout. |
| *retries* | (Optional) Number of times that your Server Switch tries to authenticate after a timeout. |
| **key** | (Optional) Specifies the authentication key that the client and radius server use. |
| *encryption-key* | (Optional) Authentication key that the client and radius server use. |

## Defaults

The RADIUS server IP address defaults to 0.0.0.0, which assigns no server, and the Server Switch authenticates locally by default.

The *udp-port* variable defaults to 1812. Use the **show authentication** command to display the configuration of the radius server.

## Command Modes

Global Configuration (config) mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

Unrestricted read-write access.

Configure a RADIUS server to authenticate CLI user logins. Enter the **authentication** command to enable authentication and to configure your Server Switch to authenticate with the RADIUS server. Use the **show authentication** command to display the configuration of the radius server.

## Examples

The following example assigns the RADIUS server that the Server Switch can use to validate logins.

```
SFS-7000P(config)# radius-server host 10.5.0.100
```

## Related Commands

**authentication**
**boot-config**
**clock set**
**show authentication**
**snmp-server**

# reload

To reboot your Server Switch, enter the **reload** command in Privileged Exec mode.

**reload** [**no-failover**]

## Syntax Description

| | |
|---|---|
| **no-failover** (Cisco SFS 3012 only) | (Optional) Forces a Cisco SFS 3012 to run from the same controller card when it reboots. By default, Cisco SFS 3012 Server Switches swap active controller cards when they reboot. |

## Defaults

This command has no default settings.

## Command Modes

Privileged Execute mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

General read-write user.

At stages of chassis and interface setup, you need to reinitialize chassis firmware or restore interface card configurations. Use the **reload** command because it allows the chassis to close files and prepare for shutdown. The **reload** command brings down the entire Server Switch and restarts all of the cards in the Server Switch.

The Server Switch prompts you to verify the reload. If you have not already saved configuration changes, and the Server Switch detects the changes, it prompts you to save. To store the new configuration as the startup configuration, enter **yes** at the prompt. To store the configuration elsewhere under a different file name, enter the new file name and press **Enter**.

The system reinitializes itself and then loads the active system image and the startup configuration file. Wait a few minutes and attempt to log onto the chassis.

**Note** If your Server Switch includes a second controller card, the CLI will prompt you to save changes to the backup controller as well as to the primary controller.

## Examples

The following example reloads the Server Switch.

```
SFS-7000P# reload
System configuration has been modified. Save?
[yes(default)/no/*.cfg] yes
Proceed with reload? [confirm]
SFS-7000P#
Connection to host lost.
#
```

## Related Commands

boot-config
broadcast
install
who
show boot-config

# save-log

To save a log file of the last 40 commands that you entered, enter the **save-log** command in Privileged Exec mode.

**save-log** [*filename*]

## Syntax Description

| | |
|---|---|
| *filename* | (Optional) Name of the file you create to store your command history. |

## Defaults

If you do not provide a name for the log file, your Server Switch assigns a name with the following format:

**savelog.***mmddhhmmss*

where *mmddhhmmss* represents the system UTC time.

## Command Modes

Privileged Execute mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

General read-write user.

Your Server Switch stores save-log files to the syslog directory. To execute the commands in the save-log file, copy the file to a host, edit it appropriately, and copy it to the config file system on a Server Switch and run the **exec** command.

## Examples

The following example saves the last 40 commands as a file called mylog.log.

```
SFS-7000P# save-log mylog.log
```

## Related Commands

**exec**
**history**

# shutdown

To disable

- a specific interface card or port,
- the Ethernet Management port,
- the InfiniBand Management port,
- a power supply

enter the **shutdown** command in the appropriate Configuration submode. To enable any of these elements, use the **no** form of this command.

**shutdown**

**no shutdown**

## Syntax Description

This command has no arguments or keywords.

## Defaults

This command has no default settings.

## Command Modes

Card Configuration (config-card) submode, Ethernet Management Interface Configuration (config-int-mgmt-ethernet) submode, InfiniBand Management Interface Configuration (config-int-mgmt-ib) submode, Ethernet Interface Configuration (config-if-ether) submode, InfiniBand Interface Configuration (config-if-ib) submode, Fibre Channel Interface Configuration (config-if-fc) submode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

Unrestricted or card-specific read-write user.

Enabling/Disabling a card:

Before you use the **action** command on a card, you must enable (bring up) the card. To enable or disable a card, perform the following steps:

**Step 1** In User Exec mode, enter the **enable** command to enter Privileged Exec mode.

**Step 2** Enter the **configure terminal** command to enter Global Configuration mode.

**Step 3** Enter the **card** command and specify the card or cards that you want to enable.

**Step 4** Enter the **shutdown** command or the **no shutdown** command to disable or enable the cards that you specified in <Link>Step Step 3<Link>

When you use the **shutdown** command to disable a card, the card stops processing packets and powers down.

**Note** You cannot update or delete the active system image on a card when you disable the card. Before you update the active system image on your Server Switch, enable all cards that you want to update.

Enabling/Disabling an interface port:

To enable or disable a port, perform the following steps:

**Step 1** In User Exec mode, enter the **enable** command to enter Privileged Exec mode.

**Step 2** Enter the **configure terminal** command to enter Global Configuration mode.

**Step 3** Enter the **interface** command and appropriate keyword (**ethernet**, **fc**, or **ib**), then specify the port or ports that you want to enable.

**Step 4** Enter the **shutdown** command or the **no shutdown** command to disable or enable the cards that you specified in Step 3

Enabling/Disabling the Ethernet Management Port:

To enable or disable the Ethernet Management port, perform the following steps:

**Step 1** In User Exec mode, enter the **enable** command to enter Privileged Exec mode.

**Step 2** Enter the **configure terminal** command to enter Global Configuration mode.

**Step 3** Enter the **interface mgmt-ethernet** command to enter Ethernet Management Interface Configuration submode.

**Step 4** Enter the **shutdown** command or the **no shutdown** command to disable or enable the port.

You must enable the Ethernet Management port before you can configure it. Use the **no shutdown** command to bring up the Ethernet Management port before you assign IP and gateway addresses to the port.

When you disable the Ethernet Management port, the current configuration of the port remains intact. If you experience problems configuring the Ethernet Management port, first check that the admin-status field in the **show interface mgmt-ethernet** command output displays **up**.

Enabling/Disabling the Infiniband Management port:

To enable or disable the InfiniBand Management port, perform the following steps:

**Step 1** In User Exec mode, enter the **enable** command to enter Privileged Exec mode.

**Step 2** Enter the **configure terminal** command to enter Global Configuration mode.

**Step 3** Enter the **interface mgmt-ib** command to enter InfiniBand Management Interface Configuration submode.

**Step 4** Enter the **shutdown** command or the **no shutdown** command to disable or enable the port.

The InfiniBand Management port provides Telnet, SSH, and Element Manager access to InfiniBand hosts that run IPoIB and connect to any of the InfiniBand ports on your Server Switch. With the IB management port, you can run management applications over IPoIB.

**Note** You must configure the IP address and gateway of the Infiniband Management port through the Serial Console terminal. Use the **ip** and **gateway** commands.

## Examples

The following example enables interface card 12.

```
SFS-7000P(config-card-12)# no shutdown
```

The following example enables the interface Management Ethernet port.

```
SFS-7000P(config-if-mgmt-ethernet)# no shutdown
```

The following example enables the interface Management IB port.

```
SFS-7000P360(config-if-mgmt-ib)# no shutdown
```

The following example sets the admin-status field for ports 1 through 6 on InfiniBand card 15 to **up**.

```
SFS-7000P(config-if-ib-15/1-15/6)# no shutdown
```

## Related Commands

**action**
**auto-negotiate**
**card**
**gateway**
**ip**
**link-trap**
**show card**
**show fc srp initiator**
**show interface mgmt-serial**
**type**

# snmp-server

To store contact and location information and to configure the SNMP notification host and SNMPv3 user, enter the **snmp-server** command in Global Configuration mode. To replace these values with empty strings, enter the **no** form of this command.

**snmp-server** {**contact** "*contact-string*" | **engineID local** *engine-string* | **host** *dest* [*community-string*] [**recv-event-traps**] | **location** "*location-string*" | **enable traps authentication**}

**snmp-server user** *username* {**disable** | **enable** | **privilege** *privileges* | **v3** [**encrypted**] **auth** {**md5** | **sha**} *password* [**priv des56** *privacy*]}

**no snmp-server** {**contact** | **host** *ip-address* [**recv-event-traps**] | **location** | **user** ***username*** **v3** | **enable traps authentication**}

## Syntax Description

| | |
|---|---|
| **contact** | Stores the contact information for your Server Switch. This contact information appears in the **show version** command output. |
| **host** | Configures your Server Switch to communicate with the host that receives SNMP traps from your Server Switch. |
| **engineID** | Configures a SNMPv3 engine ID. |
| **local** | Configures the engine ID of the local agent. |
| *engine-string* | Engine ID, as a 15-octet string. |
| **location** | Stores location information about your Server Switch. This contact information appears in the **show version** command output. |
| *contact-string* | ASCII text string of contact information. |
| *dest* | IP address or DNS name of an SNMP server. |
| *community-string* | (Optional) SNMP community string that authenticates your Server Switch to the SNMP server. |
| **recv-event-traps** | (Optional) Configures the Server Switch to send SNMP traps to the receiver. If you configure this keyword, the remote host receives SNMP events as well as traps. |
| *location-string* | ASCII text string of location information. |
| **user** | Specifies the user ID that you want to configure. |
| *username* | User ID that you want to configure. |
| **disable** | Disables the SNMP user. |
| **enable** | Enables the SNMP user. |
| **privilege** | Assigns privileges to the user. |
| **enable traps authentication** | Generates a trap each time a user is blocked from accessing the system. |

| | |
|---|---|
| *privileges* | Privileges to apply to the user. The privileges may be any combination of<br>• ib-ro<br>• ib-rw<br>• ip-ethernet-ro<br>• ip-ethernet-rw<br>• fc-ro<br>• fc-rw<br>• unrestricted-rw<br>and you must enter whatever privileges you include in the order that they appear above. |
| **v3** | Configures a user with the SNMPv3 security model. |
| **encrypted** | (Optional) Specifies passwords as digests |
| **auth** | Configures authentication parameters for the user. |
| **md5** | Specifies md5 authentication. |
| **sha** | Specifies sha authentication. |
| *password* | Authentication password to assign to the user. |
| **priv** | (Optional) Configures privacy for the user and assigns a privacy password. |
| **des56** | (Optional) Configures the privacy type |
| *privacy* | Privacy password. |

## Defaults

This command has no default settings.

## Command Modes

Global Configuration (config) mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

Unrestricted read-write user.

The snmp-server contact string appears when you view system version or SNMP information.

The snmp-server host string appears in the **show snmp** command output.

The **host** keyword configures the IP address of the host that you want to receive traps.

**Note** SNMPv3 configurations are not portable across Server Switches. You must configure SNMPv3 individually on each chassis. If you migrate a configuration file from one chassis to another, the SNMPv3 section does not appear.

## Examples

The following example stores contact information on your Server Switch and assigns a SNMP server to your Server Switch.

```
SFS-7000P(config)# snmp-server contact "support@cisco.com"
SFS-7000P(config)# snmp-server host 10.3.106.99 secret
```

The following example inputs user “dog” with the SNMPv3 security model, assigns md5 authentication, a password of “cat,” and des56 privacy with a password of “fish” in the configuration.

```
SFS-270(config)# snmp-server user dog v3 auth md5 cat priv des56 fish
```

## Related Commands

**gateway**
**radius-server**
**ntp**
**location**
**logging**

# speed

To configure the connection speed between Fibre Channel interface ports on your Server Switch and Fibre Channel devices, enter the **speed** command in Fibre Channel Interface Configuration submode.

To assign an Ethernet connection speed to a port or ports, enter the **speed** command in Ethernet Interface Configuration submode.

**speed** *speed*

## Syntax Description

| | |
|---|---|
| *speed* | Integer value that configures the speed (in Mbps) of the connection between your Server Switch and a Fibre Channel device or Ethernet device. For Fibre Channel, enter **1000** for 1 Gbps or **2000** for 2 Gbps. |

## Defaults

By default, Fibre Channel connections run at 2000 Mbps (2 Gbps).

## Command Modes

Fibre Channel Interface Configuration (config-if-fc) mode, Ethernet Interface Configuration (config-if-ether) submode, InfiniBand Interface Configuration (config-if-ib) submode (select Server Switches).

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

Unrestricted read-write user, Fibre Channel read-write user, Ethernet read-write user, InfiniBand read-write user.

Fibre Channel:

The speed of a connection does not necessarily match the speed that you configure. If your connection cannot physically connect at the speed that you specify, the connection runs at a slower speed that your Server Switch automatically detects. As soon as a physical change makes your speed setting possible, the connection will run at the speed that you specified.

**Note** You cannot manually configure connection speed you enable auto-negotiation. Enter the **no auto-negotiate** command before you manually configure connection speed.

Ethernet:

The **speed** command sets the administrative speed (the speed that you want) only. Self-detection determines the actual speed, which depends on the capabilities of the connection. You must disable the auto-negotiation feature to manually configure speed.

InfiniBand:

The **speed** command sets the administrative speed only. Self-detection determines the actual speed, which depends on the capabilities of the connection. You must disable the auto-negotiation feature to manually configure speed.

## Examples

The following example sets the preferred speed to 1,000 Mbps (1 Gbps). The results of this command may be viewed in the admin-speed field for Fibre Channel interfaces using the **show interface fc** command.

```
SFS-7000P(config-if-fc-5/4)# speed 1000
```

The following example sets the ethernet interface (slot 4, port 1) to a speed of 100 Mbps.

```
SFS-7000P(config-if-ether-4/1)# speed 100
```

The following example sets all InfiniBand interfaces on a Cisco SFS 7000 to a speed of 4x.

```
SFS-120(config-if-ib-1/1-1/24)# speed 4x
```

## Related Commands

**auto-negotiate**
**half-duplex**
**show fc srp initiator**
**show interface ethernet**

# system-mode

To configure your Server Switch to deny changes to SRP configuration to preserve VFrame-authorized configurations, enter the system-mode command in Global Configuration mode.

**system-mode** {**normal** | **vframe-210**}

## Syntax Description

| | |
|---|---|
| **normal** | Grants all users with appropriate access levels to configure SRP on the Server Switch. |
| **vframe-210** | Prevents changes to the SRP configuration on the Server Switch so as to preserve the VFrame SRP configuration. |

## Defaults

By default, authorized users can manually alter the SRP configuration.

## Command Modes

Global Configuration mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

Unrestricted read-write user, Fibre Channel read-write user

Configure the system-mode of all switches in a VFrame environment to vframe-210 to avoid manual SRP configuration changes that interfere with the VFrame SRP configuration.

## Examples

The following example "locks" the SRP configuration for VFrame purposes.

```
SFS-7000P(config)# system-mode normal
```

## Related Commands

**fc srp initiator**
**fc srp initiator-wwpn**
**fc srp it**
**fc srp itl**
**fc srp lu**
**fc srp target**
**fc srp-global gateway-portmask-policy restricted**
**fc srp-global itl**
**fc srp-global lun-policy restricted**

# telnet

To enable or disable telnet services on your Server Switch, enter the **telnet** command in Privileged Exec mode.

**telnet** {**enable** | **disable**}

## Syntax Description

This command has no arguments or keywords.

## Defaults

By default, telnet services run on your Server Switch.

## Command Modes

Global Configuration (config) mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

Unrestricted read-write access.

Disable the telnet feature to restrict access to your Server Switch to SSH only. Your Server Switch supports two concurrent telnet log-ins (in addition to the Serial log-in, if applicable).

## Examples

The following example enables telnet access to the Server Switch.

```
SFS-7000P(config)# telnet enable
```

## Related Commands

**ftp-server enable**
**history**
**more**
**show interface mgmt-ib**
**show system-services**

# terminal

To configure

- the maximum number of lines that appear on the terminal screen when you enter commands that display multiple lines of output,
- the duration of idle time that triggers your Server Switch to automatically log you out and end your CLI session

enter the **terminal length** command in User Exec mode or Privileged Exec mode. To restore these settings to default values, use the **no** form of this command.

**terminal** {**length** *number-of-**lines*** | **time-out** *minutes*}

**terminal no** {**length** | **time-out**}

## Syntax Description

| | |
|---|---|
| **length** | Specifies the number of lines that appear on the screen when you run commands such as the **more** command an on-line help (**?**). |
| *number-of-lines* | Number (integer) of lines that appear on the screen when you run commands such as the **more** command. Enter **0** to disable paging and display all output at once. |
| **time-out** | Specifies the amount of idle time that your Server Switch allows before it logs a user out of the CLI. |
| *minutes* | Number of minutes (integer ranging from 1 to 100000) of idle time that prompts your Server Switch to end your CLI session and log you out. |

## Defaults

By default, the CLI displays 24 lines per screen.

By default, your Server Switch logs you out after 15 minutes of inactivity.

## Command Modes

User Execute mode, Privileged Execute mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

General read-only user.

- length

  A *number-of-lines* value of 0 turns off paging and displays data on the screen without stopping until completed. We recommend that you set the terminal page length to 0 when you use the **show logging** command with the **end** argument. Otherwise, you will have to keep pressing the space bar to continue each time the maximum display length prints. The **no** form of this command resets the terminal length to the default.

  The number of lines specified only applies to the current CLI session. Other users are unaffected by changes to the display length.

NOTE: If you set the page length to 0 to disable paging, do not change the terminal window size. Changing window size restores the terminal length to that of the window and re-enables paging.

- time-out

  Changes to this parameter apply immediately to all users and continue to apply to users who log in after you configure the timeout value. Enter **0** to disable timeouts.

  NOTE: System timeouts apply if you use Telnet or SSH to connect to your Server Switch.

## Examples

The following example configures the CLI to display 66 lines of display output at a time.

```
SFS-7000P# terminal length 66
```

The following example configures the CLI to time out after 60 minutes.

```
SFS-7000P# terminal time-out 60
```

## Related Commands

**logging**
**more**
**show logging**
**show system-services**

# trace

To track internal Server Switch program modules that specific interface cards call, enter the **trace** command in Global Configuration mode.

**Note** Use this command only under the direction of support personnel for program debug purposes.

**trace app** *app* **module** *mod* **level** {**no-display** | **very-terse** | **terse** | **verbose** | **very-verbose** | **scream**} **flowmask** *val* [**card** *slot*]

## Syntax Description

| | |
|---|---|
| **app** | Identifies an internal application to trace. |
| **module** | Identifies a program module to trace within the specified application. |
| **level** | Specifies the verbosity level of the **trace** command output. |
| **flowmask** | Masks modules that you do not want to display. |
| **card** | (Optional) Identifies the card to trace. |
| **no-display** | Disables tracing when you also set the *val* variable to 0x00. |
| **very-terse** | Contact technical support for details. |
| **terse** | Contact technical support for details. |
| **verbose** | Contact technical support for details. |
| **very-verbose** | Contact technical support for details. |
| **scream** | Contact technical support for details. |
| *app* | Integer that indicates the internal application to trace. |
| *mod* | Program module within the application. |
| *val* | Decimal or hexadecimal value of modules to mask. A value of 0xFFFFFFFF masks all modules. A value of 0x00 displays all modules. |
| *slot* | (Optional) Slot number of the card to trace. |

## Defaults

This command has no default settings.

## Command Modes

Global Configuration (config) mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

General read-write user.

Use this command to debug your system.

The number of applications and modules may change between releases. The numbers assigned to applications and modules may also change. Check application and module number assignments using CLI help (**?**) before you execute this command, as shown in the example below.

## Examples

The following example displays the applications that you can trace (output abridged).

```
SFS-7000P(config)# trace app ?
app <1-25>
app numbers:
APP_ID_CLI        = 1
APP_ID_OSPF       = 2
APP_ID_RIP        = 3
…
…
APP_ID_IP_AGENT   = 22
APP_ID_FIB_AGENT  = 23
APP_ID_KERNEL     = 24
APP_ID_CARD_AGENT = 25
APP_ID_SM         = 26
```

The following example enables tracing for application 4, module 36.

```
SFS-7000P(config)# trace app 4 module 36 level very-verbose flowmask 0x12 card 2
```

## Related Commands

**help**
**show trace**

# type

To assign an administrative card-type to a slot into which you want to install a card, enter the **type** command in Card Configuration submode.

**type** *card-type*

## Syntax Description

| | |
|---|---|
| *card-type* | Type of card in the slot. See Table 2-2 for available card types. |

## Defaults

This command has no default settings.

## Command Modes

Configuration Card (config-card) mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

Unrestricted or card-specific read-write user.

Use the **type** command to reserve slots for particular card types. For instance, if you want a slot to run only Fibre Channel gateway cards, configure the type of the slot to "fc2port2G" so that only that card type will function in the slot. Any other card that you place in the slot will not function. Table 2-2 lists and describes available card types.

***Table 2-2 Card Types***

| Type | Description |
|---|---|
| controller | Configures the slot for a Cisco SFS 3012 controller card. |
| controllerIb12port4x | Configures the slot for a Cisco SFS 3001 controller card with 12 4x InfiniBand ports. |
| controllerIb24port4x | Configures the slot for a Cisco SFS 7000 controller card with 24 4x InfiniBand ports. |
| en4port1G | Configures the slot for a 4-port, 1Gbps Ethernet gateway. |
| en6port1G | Configures the slot for a 6-port, 1Gbps Ethernet gateway. |
| fabric12x | Configures a slot in a Cisco SFS 7008 for a fabric controller module (FCM). |
| fc2port2G | Configures the slot for a 2-port, 2Gbps Fibre Channel gateway. |
| fc4port2G | Configures the slot for a 4-port, 2Gbps Fibre Channel gateway. |
| ib12port4x | Configures the slot for a 12-port, 4X InfiniBand switch card. |
| ib12port4xTX | Configures a slot in a Cisco SFS 7008 for a line interface module (LIM) with twelve 4x InfiniBand ports. |

*Table 2-2 Card Types*

| Type | Description |
|---|---|
| ib14port1x4port4x | Configures a IB Server Switch Module to run four 4x ports and not one 4x port and one 12x port. |
| ib24port4x | Configures the slot for a 24-port, 4X InfiniBand switch card. |
| mgmtIO | Configures the slot for a Cisco SFS 7008 management I/O card. |

## Examples

The following example assigns a card-type to the expansion module slot on a Cisco SFS 3001.

```
SFS-7000P(config-card-2)# type en4port1G
```

The following example assigns a card-type to expansion modules 2 through 4 on a Cisco SFS 3012.

```
SFS-7000P(config-card-2-4)# type en4port1G
```

## Related Commands

**shutdown**
**show card**

# username

To reconfigure or create and configure user accounts, enter the **username** command in Global Configuration mode. To delete a user account, use the **no** form of this command.

**username** *user* **password** *passwd*

Creates a new user account.

**username** *user* {[**disable** | **enable**] | [**community-string** *string* | **no-community-string**] | **privilege** *priv*[***priv priv...***]}

Reconfigures an existing user account

**no username** *user*

Deletes an existing user account.

## Syntax Description

| | |
|---|---|
| **password** | Configures the password for the user account. |
| **disable** | (Optional) Disables the user account. |
| **enable** | (Optional) Enables the user account. |
| **community-string** | (Optional) Assigns a SNMP community string to the user account. |
| **no-community-string** | (Optional) Clears the SNMP community string of the user. |
| **privilege** | Assigns access privileges to the user.<br>**Note** When you assign privileges, new privileges completely overwrite your previous privilege settings. If you omit an access privilege, the user account will lose this privilege even if you previously assigned it to the account. |
| *user* | Account login name (up to 20 alphanumeric characters). |
| *passwd* | Account password (5 to 34 alphanumeric characters). |
| *string* | SNMP community string. |
| *priv* | (Optional) Access privilege. The *priv* variable may be any of the following:<br>• **ib-ro**, for InfiniBand read-only access<br>• **ib-rw**, for InfiniBand read-write access<br>• **ip-ethernet-ro**, for Ethernet read-only access<br>• **ip-ethernet-rw**, for Ethernet read-write access<br>• **fc-ro**, for Fibre Channel read-only access<br>• **fc-rw**, for Fibre Channel read-write access<br>• **unrestricted-rw**, for universal read-write access |

## Defaults

Guest user accounts are disabled by default. All other user accounts are enabled.

## Command Modes

Global Configuration (config) mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

Unrestricted read-write user or general read-write user (change own password only).

The **username** command

- Creates and remove user accounts. The default CLI user accounts are guest, admin, and super.
- Changes user password. A user with read-write access may change their own password.
- Assigns access levels based upon functional areas, such as Fibre Channel, Ethernet, and InfiniBand administrative areas. Access levels may be unrestricted or read-only or read-write for the various administrative areas. Unrestricted indicates super user.
- Enables or disables the account.
- Associates user accounts with SNMP community strings. This community string serves as the password for Element Manager access.

You must create the user account with the **password** keyword before you can configure the account. By default, the Server Switch provides the unrestricted user login **super** (that uses a default password of **super**). This login uses **secret** as its default SNMP community string. SNMP community strings provide the user credentials necessary to access Management Information Base (MIB) object.

Each user login uses one unique community string and one password. A login must use a community string to launch an Element Manager session. To restrict a deny a user access to SNMP, do not provide the login with a community string.

**Note** SNMP community strings are sent across the network in UDP packets with no encryption.

By default, new user accounts have read-only access. You may grant write privileges to a user for functional areas, such as InfiniBand, Ethernet, and Fibre Channel. Privileges are order-dependent. You must enter multiple access privileges in the following order:

**Step 1** ib-ro

**Step 2** ib-rw

**Step 3** ip-ethernet-ro

**Step 4** ip-ethernet-rw

**Step 5** fc-ro

**Step 6** fc-rw

**Step 7** unrestricted-rw

When changing the privileges of an existing user, specify all the privileges allowed to the user (including re-entering existing privileges), because the privilege argument removes all existing privileges and replaces them with them with the new ones.

For security purposes, since multiple users exist on the system, we recommend that you change the default passwords after initial configuration. The default user accounts are listed in the table below.

*Table 2-3 Default User Accounts*

| User Name | Password | Privilege |
|---|---|---|
| super | By default, the password is **super**. The default community string is **secret**. | The super user has unrestricted privileges. Use this account to manage any part of the system. This user may view and modify a configuration, as well as administer user accounts and access privileges. This user configures the console and management ports for initial chassis setup. |
| admin | By default, the password is **admin**. The default community string is "**private**". | The admin user has general read-write privileges. This user may view and modify the current configuration. However, the admin user can change only its own user information, such as the admin password. |
| guest | The default password is **guest**. The default community string is **public**. | The guest user has read-only privileges. This user may only view the current configuration. The guest user cannot make any changes during the CLI session. |

## Examples

The following example creates a user with InfiniBand and Fibre Channel administrative privileges, as well as an SNMP community-string.

```
SFS-7000P(config)# username ib-fc_admin password ibFcAdmin
SFS-7000P(config)# username ib-fc_admin community-string ibFc-commStr
SFS-7000P(config)# username ib-fc_admin privilege ib-rw ip-ethernet-ro fc-rw
SFS-7000P(config)# username ib-fc_admin enable
SFS-7000P(config)# exit
SFS-7000P# show user ib-fc_admin
================================================================
                        User Information
================================================================
                 username : ib-fc_admin
                 password : $1$JwcI/25k$3aCHn3BAQcTF3V2PGv1m7.
           snmp-community : ibFc-commStr
         permission-level : ib-rw, ip-ethernet-ro, fc-rw
             admin-status : enabled
               num-logins : 0
  num-unsuccessful-logins : 0
               last-login :
  last-unsuccessful-login :
SFS-7000P#
```

The following example disables a user account but does not delete it.

```
SFS-7000P(config)# username ib-fc_admin disable
```

The following example deletes a user account.

```
SFS-7000P(config)# username ib-fc_admin no
```

## Related Commands

**show user**

# who

To display

- the users currently connected to your Server Switch,
- the host system from which each connected user logged in,

enter the **who** command in User Exec mode or Privileged Exec mode.

**who**

## Syntax Description

This command has no arguments or keywords.

## Defaults

This command has no default settings.

## Command Modes

User Execute mode, Privileged Execute mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

General read-only user.

Use this command before you reboot the Server Switch so you can broadcast a message about impending reboots if other users have sessions open to the Server Switch.

## Examples

The following example displays the users on the Server Switch.

```
SFS-7000P# who
super               Console
super               10.10.253.47
admin               10.10.196.8
SFS-7000P#
```

## Related Commands

**broadcast**
**reload**
**write**

# write

To send a text message to another CLI user, enter the **write** command in User Exec mode or Privileged Exec mode.

**write** *user* "*string*"

## Syntax Description

| | |
|---|---|
| *user* | User account to which you want to send a message. |
| *string* | Text that you want to send to the other user. |

## Defaults

This command has no default settings.

## Command Modes

User Execute mode, Privileged Execute mode.

## Usage Guidelines

**Platform Availability:**

Cisco SFS 3001, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 3012, IB Server Switch Module

**Privilege Level:**

General read-only user.

Use the **write** command to send messages about administrative functions that impact individual users.

## Examples

The following example sends a message to the admin user.

```
SFS-7000P# write admin "Please reconnect ib1 to the switch card."
```

## Related Commands

**broadcast**
**who**