CHAPTER 1

Using the CLI

This chapter provides a general overview of the Cisco server switch command line interface (CLI). It describes how to start a CLI session, how to enter commands, and how to view online help. Details about individual commands appear later in this document.

The following sections appear in this chapter:

Setting up the Switch

The first time that you access your Cisco SFS 3001, Cisco SFS 3012, Cisco SFS 3012R, Cisco SFS 7000, Cisco SFS 7000P, Cisco SFS 7008, or Cisco SFS 7008P Server Switch, you must connect a management station, such as a PC or Linux terminal, to the serial console port on your server switch. After you establish this connection you can configure the management ports on your server switch so that you can perform configuration tasks with a Telnet session, Element Manager, or Chassis Manager.

This procedure is not necessary on a Cisco SFS 7000D Server Switch because DHCP is enabled by default.

To configure a server switch through the serial console port, perform the following steps:

Step 1 Connect a PC or terminal to the serial console port. For detailed instructions, see the appropriate hardware guide for your server switch model.

Step 2 Open a terminal emulation program (such as HyperTerminal for Windows), and configure session parameters as follows:

- Baud: 9600 b/s
- Data Bits: 8
- Parity: None
- Stop Bits: 1
- Flow control: None

Step 3 Attach a power cord to each power supply on the server switch chassis to power up the server switch. The CLI login prompt appears on the management station terminal.

Starting A CLI Session

The CLI login prompt automatically appears in a terminal window when you connect the serial port of a computer to the Serial Console port. It also appears when you launch a Telnet or Secure Shell (SSH) session to an Ethernet Management port. The user account that you use to log in determines your level of access. By default, you can log in as "super," "admin," or "guest." Table 1-1 lists and describes user login privileges.

Table 1-1 Privilege Levels

User Log-in	Privileges
super	The super user has unrestricted privileges. Use this account for initial configuration. This user can view and modify a configuration, as well as administer user accounts and access privileges. This user configures the console and management ports for initial server switch setup. This login uses "super" as the default password.
admin	The admin user has general read-write privileges. This user can view and modify the current configuration. However, the admin user can change only its own user information, such as the admin password. This login uses "admin" as the default password.
guest	The guest user has read-only privileges. This user can only view the current configuration. The guest user cannot make any changes during the CLI session. When you first bring up your server switch, you must enable this login. (See the "username" section on page 3-400). This login uses "guest" as the default password.

Note Cisco SFS Server Switch product configurations with operating system release 2.3.x and higher use a 128-bit MD5-based hashing scheme to store passwords.

In addition to the default user accounts described above, there are administrative *roles* that can be assigned to individual user accounts. Roles allow granular levels of privileges. For example, you can create separate Fibre Channel, Ethernet, or InfiniBand administrators who need access to specific subsystems only. The server switch combines multiple roles with read and read-write access for flexible control.

Note If a user does not have access to particular functionality, that functionality will not appear in the CLI, on-line help, or any GUI management windows.

The unrestricted (super) administrator assigns these roles. Table 1-2 lists and describes these access levels.

Table 1-2 Access Levels

Role	Description
ib-ro	InfiniBand read-only access.
ib-rw	InfiniBand read-write access.
ip-ethernet-ro	Ethernet read-only access.
ip-ethernet-rw	Ethernet read-write access.
fc-ro	Fibre Channel read-only access.
fc-rw	Fibre Channel read-write access.
unrestricted-rw	Read-write access to all network configuration commands.

To configure accounts, see the **username** command in the "username" section on page 3-400.

Logging In

At the CLI prompt, enter the appropriate username and password to log in as the super user.

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

You are now logged in as an administrator and can view and configure the CLI configuration.

Note Cisco SFS Server Switches support up to three concurrent CLI sessions.

Authentication

You can authenticate users against information stored on a local database on the server switch itself, a RADIUS server, or a TACACS+ server. You can use any of the authentication methods shown in Table 1-3.

Table 1-3 Authentication Methods for Logging In

Authentication	How it Works
local	Authenticates user logins against the chassis database.
local and then RADIUS	Authenticates user logins against the chassis database. Upon failure, authenticates with up to three configured RADIUS servers. Upon failure to authenticate the user or failure to reach any configured RADIUS server, the user is denied access.
RADIUS and then local	Authenticates user logins with up to three configured RADIUS servers. Upon failure to authenticate the user or failure to access any configured RADIUS server, authenticates against the chassis database. If authentication against the chassis database fails, then the user is denied access.
local and then TACACS	Authenticates user logins against the chassis database. Upon failure, authenticates with up to three configured TACACS+ servers. Upon failure to authenticate the user or failure to access any configured TACACS+ server, the user is denied access.
TACACS and then local	Authenticates user logins with up to three configured TACACS+ servers. Upon failure to authenticate the user or failure to access any configured TACACS+ server, authenticates against the chassis database. If authentication against the chassis database fails, then the user is denied access.
RADIUS	Authenticates user logins with up to three configured RADIUS servers. Upon failure to authenticate the user, the user is denied access. The authentication process checks against the chassis database only if it cannot access any RADIUS server.
TACACS	Authenticates user logins with up to three configured TACACS+ servers. Upon failure to authenticate the user, the user is denied access. The authentication process checks against the chassis database only if it cannot access any TACACS+ server.

User Authentication Against the Chassis Database

When local authentication is in effect and a user logs in, the user must be configured as a CLI user. The login username and password are verified against the local CLI user database. If a match is found, the login succeeds, and the user is assigned a pre-configured privilege level.

User Authentication with a RADIUS Server

When authentication against a RADIUS server is in effect, the login username and password are passed to the RADIUS server for verification. The RADIUS server verifies the login username and password, and it sends back a reply. No RADIUS user information is stored locally. The **show user all** command shows local users only.

The **radius-server** command (see the "radius-server" section on page 3-146) configures the IP address of RADIUS servers. You can configure up to three RADIUS servers. The first configured server is queried. The second server is queried if the first server is not reachable, and the third server is queried if both of the other servers are not reachable.

No privilege level is verified against the Radius server. All users authenticated by the Radius server are given unrestricted rights. If a Radius user makes changes to system configuration, the log will include the Radius username and the configuration information, just as it does for a local user.

RADIUS users do not have associating SNMP community strings. There are no SNMP logins for RADIUS users.

User Authentication with a TACACS+ Server

When authentication against a TACACS+ server is in effect, the login username and password are passed to the TACACS+ server for verification. The TACACS+ server verifies the login username and password, and it sends back a reply. No TACACS+ user information is stored locally. The **show user all** command shows local users only.

The **tacacs-server** command (see the "tacacs-server" section on page 3-387) configures the IP address of TACACS+ servers. Up to three TACACS+ servers can be configured. The first configured server is queried. The second server is queried if the first server is not reachable, and the third server is queried if both of the other servers are not reachable.

No privilege level is verified against the TACACS+ server. All users authenticated by the TACACS+ server are given unrestricted rights. If a TACACS+ user makes changes to system configuration, the log will include the TACACS+ username and the config information, just as it does for a local user.

Like RADIUS users, the TACACS+ users do not have associating SNMP community strings. There are no SNMP logins for TACACS+ users.

Note The following are limitations to TACACS+ authentication:

- TACACS+ authorization and accounting are not supported.
- TACACS+ single-connection not supported. Each login authentication makes its own connection to the TACACS+ server.
- TACACS+ user privilege level is always unrestricted.

Customizing the Login Prompt

The CLI checks the file **login-banner** for customized text to include in the prompt. Use the copy command with FTP to place a file named **login-banner** in the config directory of the switch:

copy ftp://user:xxx.x.x.x/my-banner config:login-banner

Note The length of the text is restricted to 512 characters.

Entering CLI Modes

The CLI uses the following three command modes:

- User EXEC mode
- Privileged EXEC mode
- Global configuration mode

Note Global configuration mode includes a number of submodes.

The commands that you can execute depend upon the current command mode and your user login. You can enter a question mark (?) at the CLI prompt to list the commands available to the current user identity in the current mode.

Using User EXEC Mode

All CLI sessions begin in user EXEC mode. This mode provides commands for viewing some of the system configuration and some user information. Guest users can work only in user EXEC mode. From user EXEC mode, authorized users can access privileged EXEC mode.

Using Privileged EXEC Mode

When you enter the **enable** command in user EXEC mode, you enter privileged EXEC mode. From privileged EXEC mode you can view the entire system configuration and all user information. From this mode you can perform certain high-level administrative tasks, such as save the current configuration and set the system clock. You can also access global configuration mode. You must enter privileged EXEC mode before you can enter global configuration mode. Only administrative and unrestricted users are allowed to enter privileged EXEC mode.

```
# telnet SFS-7000P
Login: super
Password: xxxx
SFS-7000P> enable
SFS-7000P#
```

Mode changes are reflected in changes to the CLI prompt. When you transition from user EXEC mode to privileged EXEC mode, the prompt changes from `SFS-7000P>` to `SFS-7000P#`.

Using Global Configuration Mode

You enter global configuration mode from privileged EXEC mode. Global configuration (config) mode configures system-level attributes, such as SNMP, SNMP agents, and networks. To enter config mode, enter either the **configure terminal** or the **configure** command in privileged EXEC mode.

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

When you transition from privileged EXEC to global configuration mode, the prompt changes from `SFS-7000P#` to `SFS-7000P(config)#`.

To configure particular elements of the server switch, you must enter a configuration submode specific to that element. All Ethernet, Fibre Channel, and InfiniBand configuration occurs in submodes. In submodes, you can assign IP addresses to interface gateway ports, set connection speeds, set connection types, and so on.

To enter the Ethernet interface configuration (config-if-ether) submode from global configuration mode, enter the **interface** command, specify the interface type, and specify the port(s) to configure.

```
SFS-7000P(config)# interface ethernet 4/1-4/4
SFS-7000P(config-if-ether-4/1-4/4)#
```

The commands that you enter in a configuration submode apply to the specified modules and ports. The Ethernet Management port, however, does not require you to specify a port number because there is only one active Ethernet Management port during a system session.

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

Exiting CLI Modes

Most commands are mode-dependent. For example, you can configure clock settings in global configuration mode only. To configure the system, you must enter and exit CLI modes. The **exit** command returns you to the previous mode.

```
SFS-3001(config-if-fc-5/1)# exit
SFS-3001(config)# exit
SFS-3001#
```

Note If you enter the **exit** command in user EXEC mode or privileged EXEC mode, your Telnet session ends.

You can also enter the **exit** command with the **all** keyword to return to user EXEC mode in one step.

```
SFS-3001(config-if-fc-5/1)# exit all
SFS-3001>
```

To return to user EXEC mode from privileged EXEC mode, enter the **disable** command.

```
SFS-3001# disable
SFS-3001>
```

Quick Help

You can enter the question mark (?) at the CLI prompt to display one of three types of user information.

Step 1 Enter a question mark (?) at the CLI prompt at any time to display the commands that you can enter. Only those commands that are appropriate to the current mode and user login appear.

```
 SFS-7000P> ?
Exec Commands:
 broadcast            - Write message to all users logged in
 enable               - Turn on privileged commands
 exit                 - Exit current mode
 help                 - Show command help
 history              - Show command history
```

```
 login                - Login as a different user
 logout               - Logout of this system
 ping                 - Send echo messages
 show                 - Show running system information
 terminal             - Set terminal line parameters
 who                  - Display users currently logged in
 write                - Write text to another user
```

Step 2 Enter part of a command string, and end it with a question mark (?) to display options that you can use to complete the string.

```
SFS-7000P> b?
 broadcast
```

Step 3 Enter a command (or enough of a command for the CLI to uniquely identify it), and then enter a space and a question mark (?) to display available arguments to follow the command.

```
SFS-7000P> broadcast ?
 String               - Message to broadcast. Enclose multi-word strings within
                        double-quotes.

SFS-7000P> broadcast
```

After the CLI displays the help information, the server switch prints the command string up to the question mark on the input line and waits for you to complete the string. You do not have to retype the string.

Command Abbreviation

To facilitate command entry, you do not need to enter CLI commands in their entirety. You can enter just enough of each command or argument to make it uniquely identifiable.

When enough characters have been entered to uniquely identify a command or keyword in a command string, you can leave the partially-typed command or keyword, enter a space, and then add additional keywords or arguments, or you can press the **Tab** key to complete the commands or keywords to improve readability.

```
SFS-7000P(config)# fc ?
 srp                  - Configure FC SRP
 srp-global           - Configure FC SRP-global parameters
SFS-7000P(config)# fc srp- ?
 enable               - Enable FC SRP
 gateway-portmask-pol - Configure FC SRP-global gateway-portmask-policy
 itl                  - Configure FC SRP-global ITL
 lun-policy           - Configure FC SRP-global lun-policy
 target-portmask-poli - Configure FC SRP-global target portmask policy
SFS-7000P(config)# fc srp- gate ?
 restricted           - Configure FC SRP gateway-portmask-policy restricted
SFS-7000P(config)# fc srp- gate res ?
<cr>
SFS-7000P(config)# fc srp- gate res
```

In the preceding example, **srp-** is short for srp-global, **gate** is short for gateway-portmask-policy, and **res** is short for restricted.

Correcting Commands

The CLI responds to invalid command input by identifying the first error with an arrow cursor immediately below the error, followed by text describing the error. The first example shows a misspelled command:

```
SFS-7000D> enabll
           ^
% Error: Invalid input detected at '^' marker
SFS-7000D>
```

In the next example, part of the command is correct. The carat indicates that the **node** keyword cannot immediately follow the **ib** keyword in this command.

```
SFS-7000D> enable
SFS-7000D# show ib node subnet-prefix fe:80:00:00:00:00:00:00
                    ^
% Error: Invalid input detected at '^' marker
SFS-7000D#
```

The system response to command line errors is different when you use the question mark (?) to obtain help for a command. In this case, the system repeats your input following the subsequent prompt for ease of editing, as shown in the following example:

```
SFS-7000P# show interfce ?
                 ^
% Error: Unrecognized command
SFS-7000P# show interfce
```

Editing the CLI

Command-line editing lets you modify a command line command that you have just entered or a command line that you entered previously in the CLI session. The CLI supports a variety of ways to move about and edit the currently displayed command line. Table 1-4 lists and describes these options.

Table 1-4 Key Stroke Shortcuts

Key Strokes	Description
Ctrl-A	Moves the cursor to the beginning of the line.
Ctrl-B	Moves the cursor left (back) one character.
Ctrl-D	Deletes the current character.
Ctrl-E	Moves the cursor to the end of the line.
Ctrl-F	Moves the cursor to the right (forward) one character.
Ctrl-K	Deletes text from cursor to the end of the line.
Ctrl-L	Refreshes the input line.
Ctrl-N	Displays the next command in the history queue.
Ctrl-P	Displays the previous command in the history queue.
Ctrl-Q	Returns to user EXEC mode. **Note** If a command is entered on the command line, execute the command before returning to user EXEC mode.

Table 1-4 Key Stroke Shortcuts (continued)

Key Strokes	Description
Ctrl-T	Transposes the current and previous characters.
Ctrl-U	Deletes all text to the left of the cursor.
Ctrl-W	Deletes the text of a word up to cursor.
Ctrl-Z	Returns you to privileged EXEC mode.
Esc-B	Moves the cursor left (back) one word.
Esc-C	Converts characters, from the cursor to the end of the word, to upper case.
Esc-D	Deletes characters from the cursor through remainder of the word.
Esc-F	Moves the cursor right (forward) one word.
Esc-L	Converts characters, from the cursor to the end of the word, to lower case.
down-arrow	Displays the next command in the history queue.
up-arrow	Displays the previous command in the history queue.
left-arrow	Moves the cursor left (back) one character.
right-arrow	Moves the cursor right (forward) one character.

Exiting the CLI Session

To exit the CLI session, return to user EXEC mode or privileged EXEC mode, and enter the **logout** command or the **exit** command. The CLI session ends.

```
SFS-3001(config-if-fc-5/1)# exit all
SFS-3001> logout
Login:
```

Note If you use Telnet or SSH to run a remote CLI session, the connection closes when you log out. Conversely, when you terminate a Telnet or SSH session, you log out of the server switch.

Specifying Modules and Ports

To configure one or more ports on one or more modules, specify the ports when you enter the configuration submode. Many CLI commands allow you to enter the following:

- A slot#/port# pair.
- A range of pairs.
- A list of pairs.
- The **all** keyword.

Slot#/Port# Pairs

A slot#/port# pair (sometimes referred to as the card#/port# pair) is a slash-separated (/) pair of numbers. The first number indicates the slot in which the interface module resides, and the second number represents a port on that module. See your hardware documentation to identify slot numbers and port numbers.

Note With hardware platforms with no removable modules, such as the Cisco 4x InfiniBand Switch Module for IBM BladeCenter, or the Cisco SFS 7000, the slot number defaults to 1.

Ranges

A range is a dash-separated (-) set of two slot#/port# pairs. A range can span multiple modules of the same interface type. Module and port numbers in a range must both appear in ascending order. That is, specify the lower module and port number in the first slot#/port# pair and the higher module and port number in the second slot#/port# pair.

Note Do not insert spaces between elements in the range.

The range 3/2-4/3 indicates all ports starting with module 3, port 2, up to and including module 4, and port 3. (This example assumes that modules 3 and 4 are of the same interface type.)

Lists

A list is a comma-separated (,) series of slot#/port# pairs and/or ranges. Sequencing of pairs in the list is not important. You can specify pairs in any order you wish; however, the data returned is displayed in numerical sequence with the lowest slot#/port# pair first. Do not insert spaces between elements in the list. For example, 3/1,3/3,4/3 indicates ports 1 and 3 on interface module 3 and port 3 on interface module 4. (This example assumes that modules 3 and 4 are of the same interface type.) You can include ranges in lists.

3/1,4/1-4/4,5/1

The preceding example assumes that modules 3, 4, and 5 are of the same interface type.

The “all” Keyword

The **all** keyword indicates all the ports of all the modules of a specific type of interface. That is, all Ethernet, Fibre Channel, or InfiniBand interface modules. The subsequent prompt will appear as though you entered the ports as a list.

Using the Documentation

The command descriptions in this book provide quick access to the information about each command. This book divides each command description into subsections, so you can go directly to the desired information.

Each command description begins with a brief, high-level description of the command, followed by the command syntax.

The following conventions apply to command syntax:

- Text in **bold** font represents text that you enter exactly as it appears.
- Text in *italicized* font represents variables that you replace with actual values when you enter a command at the command line.
- Square brackets ([,]) enclose optional syntax. Do not enter square brackets in the CLI.
- Braces ({,}) enclose required syntax choices. Do not enter braces in the CLI.
- The pipe character (|) delineates between selections in syntax. That is, if command X requires argument Y *or* argument Z, but not both at the same time, the syntax will appear as follows:

  X {**Y** | **Z**}

Note Input strings, such as device names and descriptions, must be contiguous without any intervening spaces or blanks. In the event that you wish to enter a multi-word string, enclose the string within double-quotes (**“,”**) ; otherwise, the CLI parses each word as a separate argument, which results in a syntax violation.

Syntax Description

The Syntax Description subsection provides a table that describes all syntax arguments.

Platform Availability

The Platform Availability subsection indicates the platform or platforms (such as Cisco SFS 3001, Cisco SFS 3012, Cisco SFS 3012R, Cisco SFS 7000, Cisco SFS 7000P, Cisco SFS 7008, Cisco SFS 7008P, Cisco SFS 7000D, and Cisco 4x InfiniBand Switch Module for IBM Blade Center) on which you can execute the command.

Command Modes

The Command Modes subsection indicates the command mode or submode that you must enter to execute the command.

Privilege Level

The Privilege Level subsection indicates the user permissions that are required to execute the command. For example, there are commands that only an unrestricted read-write user (for example, a super user) can execute that a user with general read-write permissions (admin) cannot.

Usage Guidelines

The Usage Guidelines subsection supplies additional information and details to help you use a command to its full potential.

Examples

The Examples subsection shows actual command entry and CLI output.

```
SFS-7000P# show interface gateway 5
============================Gateway Information================================
                  gateway : 5
                     name : 5/0
                     type : fc-gateway
                     desc : 5/0 (320)
              last-change : none
                      mtu : 0
             admin-status : up
              oper-status : up
SFS-7000P#
```

Defaults

The Defaults subsection lists command default behavior or values.

Related Commands

The Related Commands subsection provides hypertext links to related CLI commands.