S50 Quick Reference

Version 2.3 **December 2006** **101-00173-01**

FORCE10™

Danger: To prevent electrical shock, make sure the S50 is grounded properly. If you do not ground your equipment correctly, excessive emissions may result. Use a qualified electrician to ensure the power cables meet your local electrical requirements.

Warning: As with all electrical devices of this type, take all the necessary safety precautions to prevent injury when installing this system. Electrostatic discharge (ESD) damage can occur if components are mishandled. Always wear an ESD-preventive wrist or heel ground strap when handling the S50 and its components.

Warning: For fan maintenance and proper ventilation, position the S50 in an equipment rack (or cabinet) with a minimum of five inches (12.7 cm) of clearance around the side intake and exhaust vents.

Warning: The site where the S50 is placed should be a dry, clean, well-ventilated and temperature-controlled room, away from heat sources such as hot air vents or direct sunlight and have an environmental temperature between 32° – 122°F (0° – 40°C).

Contents

Overview

Thank you for purchasing a Force10 Networks S50 switch!

This *S50 Quick Reference* document is printed and included in the S50 shipping box to provide you with a quick way to access basic installation and configuration instructions and to tell you how to get more information.

In addition to the S50 with its SFTOS operating system (basic Layer 2 package) loaded in its default configuration, the shipping box also contains the AC power cord, a DB9 to RJ45 connector, and a small bag with rack-mounting screws, plastic feet for table-top mounting, and the *S-Series Documentation and Software* CD-ROM (hereafter simply referred to as the "S-Series CD-ROM").
Other purchased components are shipped separately.

The hardware installation section (Installing the Hardware on page 6) in this guide contains a subset of the information in *Installing the S50 System*, a book stored as a PDF both on the S-Series CD-ROM and at the iSupport website.

The software configuration section here (see "Basic Software Configuration on page 10") contains a subset of the configuration information in the *SFTOS Configuration Guide*, which is also on the S-Series CD-ROM and at the iSupport website.

In fact, all of the S50 documentation that is on the S-Series CD-ROM is also available on the iSupport website.

For more information about the S-Series CD-ROM, see the next section, Contents of the S-Series CD-ROM on page 5.

For more information about the iSupport website (login required), see The iSupport Website on page 20.

Note: This *S50 Quick Reference* is specific to SFTOS Version 2.3 for the S50.

Contents of the S-Series CD-ROM

The S-Series CD-ROM launches a Web page from the CD-ROM containing the links described in the following sections.

Documentation

Force10 Literature: This is a link to the Force10 Literature folder on the CD-ROM. It contains links to data sheets for all Force10 products.

***Installing the S50 System*:** This book contains details of installation options.

***Release Notes*:** This document contains release notes for the SFTOS operating system and S-Series hardware. In addition to a list of open and closed caveats, the document contains a replication of the Secure Communications document listed above. It also contains a discussion of differences in the behavior between SFTOS for the S-Series and FTOS for the E-Series switches.

***SFTOS Command Reference*:** This book contains syntax statements for all SFTOS commands in the Layer 2 and Layer 3 software.

***SFTOS Configuration Guide*:** This book is designed to help you perform the most common configuration tasks, with examples of the most commonly used commands.

Software

Note: The software image is no longer on the CD-ROM. You can check the iSupport website of Force10 for the latest image. See The iSupport Website on page 20.

MIBs: This is a link to a folder on the CD-ROM containing the S-Series MIBs.

Secure Communications (SSH/SSL/HTTPS): This link opens an HTML page containing a link to the *S-Series Secure Management* application note on the CD-ROM, describing how to enable secure communications through SSH, SSL, and HTTP. The page also contains links to folders on the CD-ROM containing example keys and shell scripts that you can use to generate your own SSH keys and SSL certificates.

Training Material

The **Training Material** link on the CD-ROM home page is to a folder on the CD-ROM containing sets of slides, in PDF format, that are used in the S-Series training.

Installing the Hardware

To install the S50 system, Force10 Networks recommends that you complete the installation procedures in the order presented below, before attaching a power source:

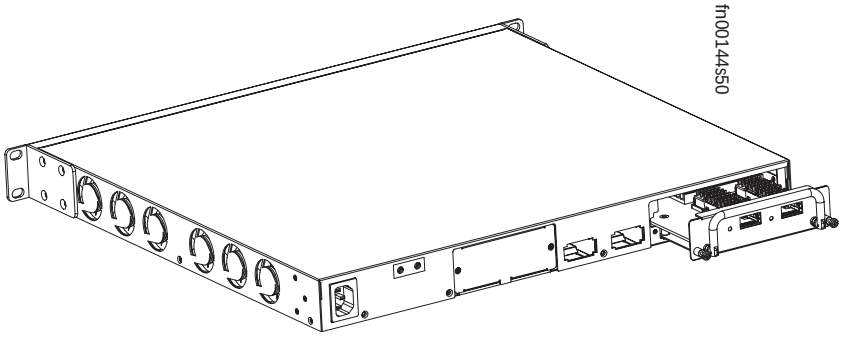
- Insert the 10-Gigabit Module (optional)
- Insert the DC Power Module (optional)
- Attach the S50 to the Rack
- Connect Stacking Ports (optional)

Warning: Before starting the installation, be sure that the installation conditions conform to those specified in Installing the S50 System.

Inserting the 10-Gigabit Module (optional)

The S50 has a slot at the right rear of the chassis, for which there are two types of 10-Gigabit module available—fiber (optical) and copper (10GBase-CX4). Both have two ports (the system numbers them 49 and 50). The fiber module requires additional XFP inserts (see Installing XFP Modules (optional) on page 9). The ports in the copper module use the same kind of stacking cable that you use for the stacking ports. To install a 10-Gigabit module, follow the steps below:

Step	Task
1.	Remove the 10-Gigabit module faceplate located at the far right rear of the S50.
2.	Remove the 10-Gigabit module from its packaging and slide the module into the 10-Gigabit slot.
3.	Secure the captive screws on either side of the module.



Inserting the DC Power Module (optional)

The S50 system includes an optional DC power module that you can install in the back of the S50 chassis. Connect it to your AC power source through an external S50 power converter module. To install these optional components, see Chapter 4 in *Installing the S50 System.* Force10 also supplies a power shelf for housing up to eight power converter modules, for use with an S50 stack.

Attaching the S50 to the Rack

The S50 is shipped with universal front-mounting brackets (rack ears) attached. The screws for attaching those ears to a standard 19-inch rack are in the bag that also contains the S-Series CD-ROM.

Ensure that there is adequate clearance surrounding the rack to permit access and airflow. If you are installing two S50 systems side-by-side, position the two S50 chassis at least 5 inches (12.7 cm) apart to permit proper airflow.

Position the S50 chassis in the rack. Secure the chassis with two screws through each bracket and onto the rack post.

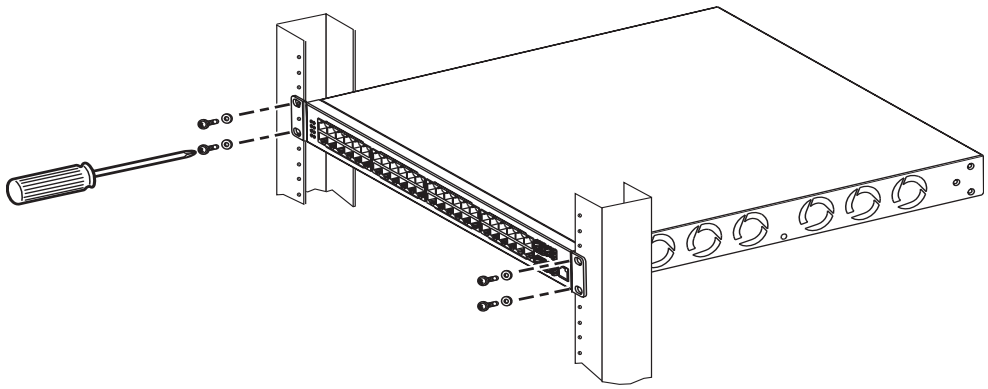


Figure 1 Front-mounting the S50

Note: The front-mounting installation above is one of several installation options contained in the book *Installing the S50 System*. Other options include rear mounting, four-post mounting, and table-mounting.

Connecting Stacking Ports (optional)

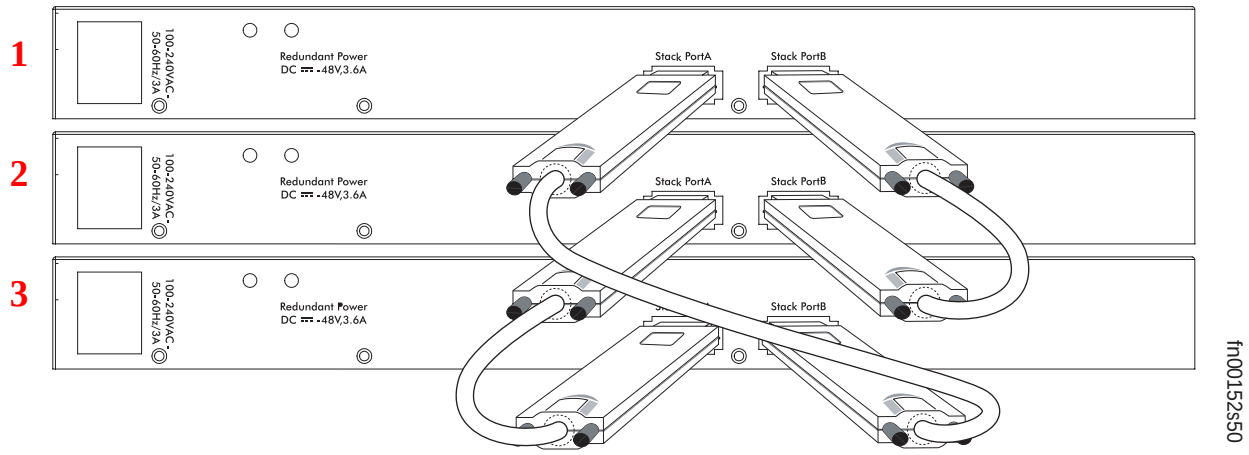
You can connect S50 systems together to configure them to act as a unified system.

Stack limitations — The number of S50s in a stack is limited by the number of S50s with 10Gb modules:

- If zero or one S50 has a 10Gb module, the stack is limited to seven S50s.
- If three S50s have a 10Gb module, the stack is limited to six S50s.
- If four or more S50s have 10Gb modules, only five S50s are allowed in the stack.

Use the optional stacking cables to connect the systems through Stack Ports A and B, as depicted below.

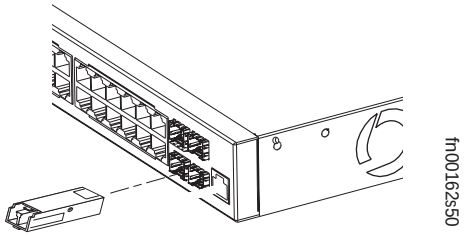
Note: The diagram shows a connection between the top and bottom S50s, from Stack Port A on unit 1 to Stack Port B on unit 3. That connection completes a topology called a ring. While that ring connection is not necessary, it provides redundancy in case of a failure of stacking cable or port.



Installing SFP Modules (optional)

To install SFPs (Small Form-factor Pluggable modules) into the four open ports at the right front of the S50:

1. Position the SFP so that the bail is closed and on top of the SFP.
2. Insert the SFP into the port until it gently snaps into place.



Note: The four SFP ports shown in the graphic, when populated, automatically preempt the four copper ports labeled 45 through 48.
In other words, while you use a particular optical port, you cannot use the equivalent copper port.

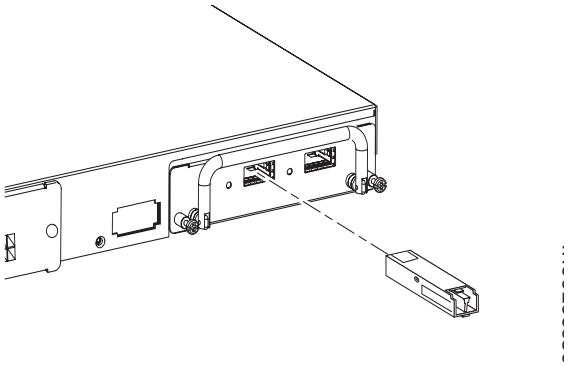
Installing XFP Modules (optional)

Warning: Do not look directly into any optical port. Failure to follow this warning could result in physical harm.

The two 10-Gigabit ports (identified by the system as ports 49 and 50) on the back of the S50 require the optional 10-Gigabit module. See Inserting the 10-Gigabit Module (optional) on page 6.

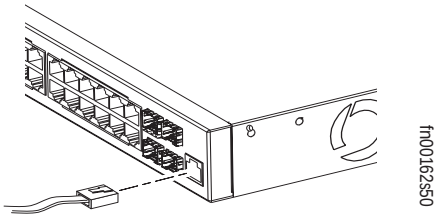
To install XFPs into the two open ports that are in the fiber (optical) version of the 10-Gigabit module:

1. Position the XFP so that the bail is closed and on top of the XFP.
2. Insert the XFP into the port until it gently snaps into place.



Connecting a Cable to the Console Port

Caution: Install a **straight-through RJ-45 copper cable** (a standard Ethernet cable) into the console port. This is different from many other implementations that require a crossover (rollover) cable. If connecting to a terminal server and using an Ethernet crossover cable, daisychain another crossover cable to effectively get a straight-through cable connection. Many console terminal servers use octopus cables that are crossover cables. As above, connect an additional crossover cable.

Connect the RJ-45/DB-9 adapter that is shipped with the S50 system to the RJ-45 cable. **Note:** The console port pinout: Pin 1 = NC Pin 2 = NC Pin 3 = RXD Pin 4 = GND Pin 5 = GND Pin 6 = TXD Pin 7 = NC Pin 8 = NC	 fn00162s50	Set your console terminal settings to: • 9600 baud rate • no parity • 8 data bits • 1 stop bit • no flow control

See the Getting Started chapter of the *SFTOS Configuration Guide* for other console port details, such as setting the console timeout and the baud rate.

Basic Software Configuration

This *S50 Quick Reference* contains a small subset of the information that is provided in the Getting Started chapter of the *SFTOS Configuration Guide*. That guide is available PDF format on the S-Series CD-ROM and on the Documents tab of the iSupport website.

This section discusses the following configuration topics for the S50:

Creating a User and Password

The S50 comes installed with one read/write user named “admin”, with no password. You can add that password, and also create up to five more read/write users with the **username** command in Global Config mode. The command edits the user name and password in one statement, as shown below. Usernames provide access to the S50 through both the CLI and the SFTOS Web User Interface (Web UI).

Note: Text boxes surrounded by oval lines, such as the following, are used throughout Force10 documentation to simulate the appearance of a terminal screen after logging in to the operating system of the switch through a console program. The hostname prompt, exemplified in the following example by “(Force10_S50)”, is configurable.
Note: In this guide, bold text highlights the commands that you enter.

```
(Force10_S50) >enable
(Force10_S50) #config
(Force10_S50) (Config)#username admin passwd apassword
User login name and password are set.
(Force10_S50) (Config)#exit
(Force10_S50) #exit
(Force10_S50) >
```

Setting the Enable Password

The Privileged Exec password (commonly called the “enable” password), is not set when the S50 starts the first time. To set the enable password, access the Privileged Exec mode (also called “enable mode”) and then the Global Config mode, as shown in the following example. Enter the command **enable passwd**, then press **Enter**.

At the prompts, enter the password that you want to use:

```
(Force10_S50) >enable
(Force10_S50) #enable passwd
Enter new password:*******
Confirm new password:*******
Password Changed!
(Force10_S50) #exit
```

Enabling Ports

When the S50 is first installed, all ports are disabled by default. To enable all ports, enter **no shutdown all** in Global Config mode, as shown here:

```
(Force10_S50) >enable
(Force10_S50) #config
(Force10_S50) (Config)#no shutdown all
(Force10_S50) (Config)#exit
```

Alternatively, you can use the **no shutdown** command at the specific interface level.

Note: The equivalent action on the Web UI is to select **Enable** in the Admin Mode field of the Port Configuration panel. See Enabling and Using the SFTOS Web User Interface on page 14.

Setting the Management IP Address

Note: SFTOS Version 2.3 replaces the **network parms** command with the commands shown below in steps 2, 3, and 4.

Use the following the procedure to set up a management IP interface to the switch. You will need this to access the switch through Telnet, SSH, TFTP, or the SFTOS Web User Interface.

Step	Command Syntax	Command Mode	Purpose
1.	**show interface managementethernet**	User Exec or Privileged Exec	Display current management IP configuration.
2.	**interface managementethernet**	Global Config	Invoke the (Config-if-ma)# prompt.
3.	**ip address** *ipaddr subnetmask*	(Config-if-ma)# prompt within the Global Config mode	Set the IP address and subnet mask of the management interface.
4.	**management route default** *gateway*	Global Config	Set the IP gateway of the management interface.

Note: The management address is reachable from VLAN 1. All physical ports are, by default, members of VLAN 1, so the management address will be reachable from all enabled physical ports by default.

Enabling Telnet to the Switch

Access to the switch through a Telnet server is disabled by default. If you want to access the switch through an SSH client, you would leave Telnet disabled and set up the SSH connection, as described in "Enabling Secure Management with Secure Shell or Secure Sockets Layer" in the *SFTOS Configuration Guide*.

To enable Telnet access, first assign the management IP address (see Setting the Management IP Address on page 12), then execute the **ip telnet server enable** command in Global Config mode.

Managing a Stack of S50 Switches

When you connect a set of previously unconfigured S50 switches, and you follow the instructions in Connecting Stacking Ports (optional) on page 8, a startup algorithm automatically designates a unit to be the management unit. You do not need to configure anything else specific to stack management.

If, on the other hand, you are modifying a stack, you will need to follow the directions that are in the Stacking chapter of the *SFTOS Configuration Guide*.

If you need to upgrade the software in the stack, see the following section.

Installing New Software

The S50 comes with the basic Layer 2 software package installed. If you purchased the extended Layer 3 software package, you will receive instructions under separate cover on how to access the software.

If you need to upgrade the software image that is installed on the S50, and you have downloaded the image to a TFTP server, issue the following command: **copy tftp://***ip_address/filename* **system:image**

Note: In command examples, such as the one above, a word in italics indicates a placeholder for a variable that you enter. For example, *ip_address* and *filename* in the case above should be replaced by the IP address of your TFTP server and the file name of the SFTOS software image to be downloaded.

You can use variations of the **copy** command to download or upload files to and from the switch. For details on the command syntax, see the **copy** command in the *SFTOS Command Reference*. More detailed instructions for upgrading or reinstalling the software or configuration files are available in the Getting Started chapter of the *SFTOS Configuration Guide*. The migration from SFTOS Version 2.2.1 to Version 2.3.1 is detailed in the S-Series and SFTOS Release Notes for Version 2.3.1.

Enabling and Using the SFTOS Web User Interface

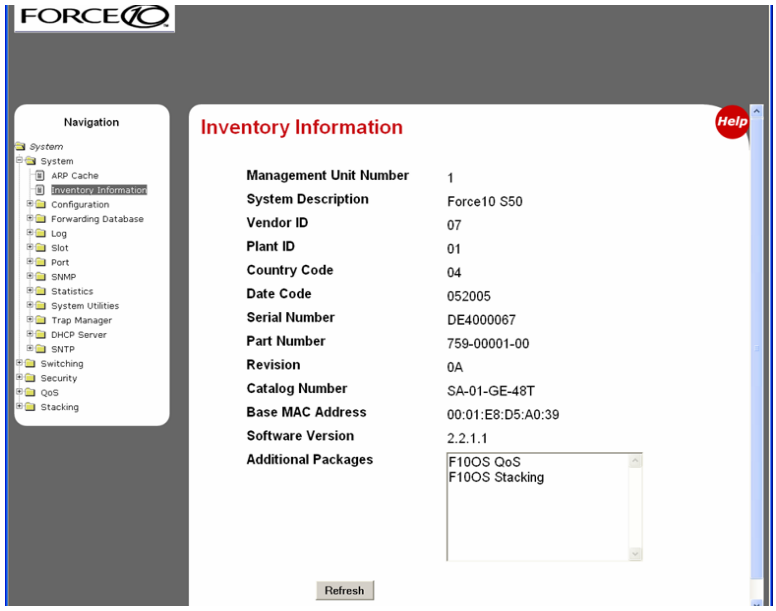
The SFTOS Web User Interface (Web UI), provided by the SFTOS operating system, provides much of the functionality provided by the CLI. Also, the CLI and Web UI can be used in combination to give you even better control.

1. To enable the Web UI, you first must give the S50 a management IP address. See Setting the Management IP Address on page 12.
2. Then, in Global Config mode, enter the command **ip http server enable**.

Note: Details on enabling an HTTPS secure server are in Chapter 7, “Security”, in the *SFTOS Configuration Guide,* and through the *Secure Communications* link on the S-Series CD-ROM.

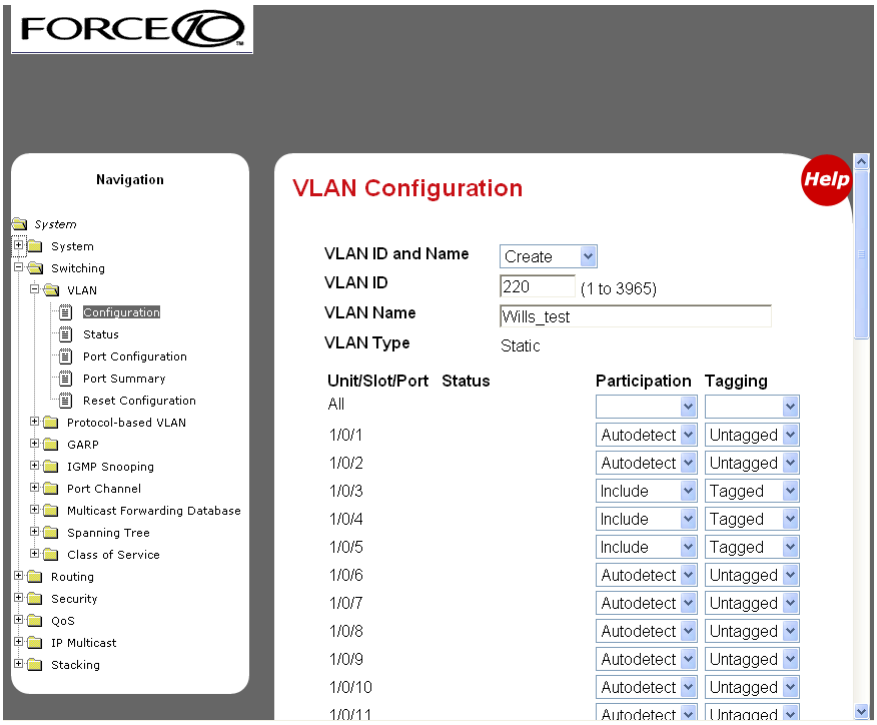
3. Launch a supported Web browser. The Web browser must support:
   - HTML version 4.0, or later
   - HTTP version 1.1, or later
   - JavaScript(TM) version 1.2, or later
4. Enter the URL of the switch (http://<IP address>) in the Web browser address field. The IP address is the management IP address that you assigned above.
5. When the Login panel is displayed, click the **Login** button.
6. Enter the admin username and password, or any other username and password that you created, as discussed above in Creating a User and Password.
7. The Navigation tree is displayed in the left frame, and the System Description panel is displayed in the right frame. Make your selection by clicking on the appropriate item in the Navigation tree.

   For example, the following screenshot shows that the Inventory Information panel opened when the user clicked the Inventory Information node in the tree. Notice that the Inventory Information panel displays the serial number of the S50. Notice also the large red Help button, which displays on every panel, and provides context help for the panels in the selected branch of the tree.



Creating a Simple Configuration using VLANs and STP

You can use the Web UI to create a VLAN. The following screenshot of the VLAN Configuration panel shows selection of a group of ports to add to a VLAN.



1. Access the VLAN Configuration panel by traversing the Navigation tree in this sequence: **System** >> **Switching** >> **VLAN** >> **Configuration.** The VLAN Configuration panel displays.
2. From the VLAN ID and Name list, either select an existing VLAN number, or click **Create**.
3. If the VLAN is new, enter a number in the **VLAN ID** field, and then, optionally, assign a name in the **VLAN Name** field.
4. Select the interfaces that you want to include in the VLAN, and whether you want them to participate in tagged or untagged mode.

   Note that, for new VLANs, the ports defaults are Autodetect (for Participation) and Untagged (for Tagging). (The Autodetect option in the Participation list is for dynamic VLANs created by GVRP.) If you select another option in the All list, that option is not reflected in the displayed port settings until you click **Submit**.
5. When you have finished, click the **Submit** button at the bottom of the panel.

If you have questions about VLAN configuration, click the red **Help** icon in the upper right corner of the panel.

Note: As noted in Enabling Ports on page 11, all ports are disabled by default. Enable them with **no shutdown all** (Global Config mode), or individually with the **no shutdown** command on each port. The equivalent action on the Web UI is to select **Enable** in the Admin Mode field on the Port Configuration panel.

If you prefer to use the command line interface (CLI) for the same purpose, here is an example of using the CLI to create a VLAN (55) and then add a tagged interface and an untagged interface to it (ports 5 and 6, respectively, in unit 1):

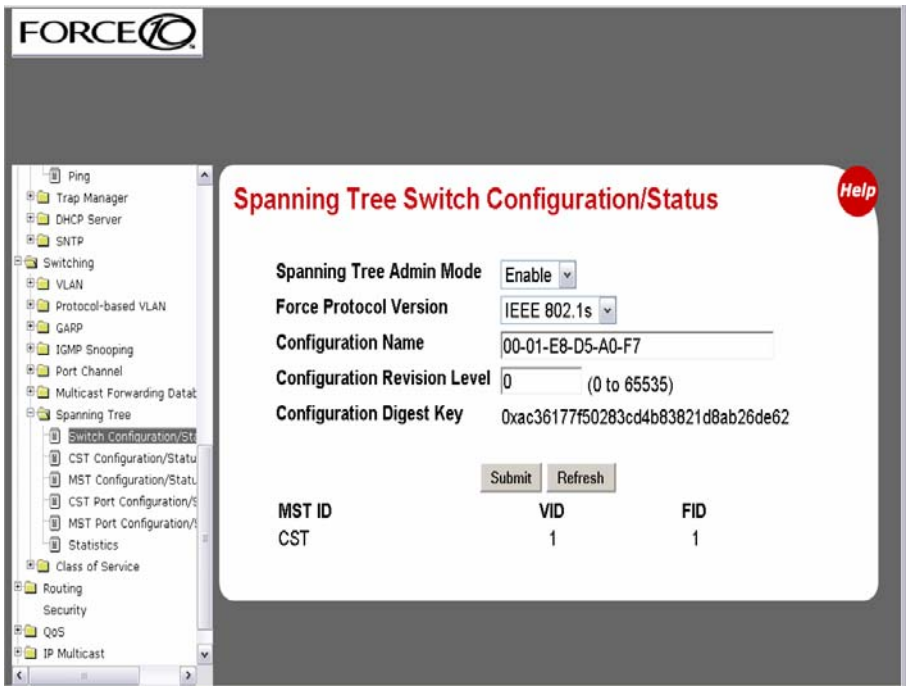
```
(Force10_S50) (Config)#interface vlan 55
(Force10_S50) (Conf-if-vl-55)#tagged 1/0/5
(Force10_S50) (Conf-if-vl-55)#untagged 1/0/6
(Force10_S50) (Config)#interface 1/0/1
```

In the above example, we use the Interface VLAN mode, which is new in SFTOS 2.3. The many VLAN commands in the Interface Config mode are deprecated.

The **tagged 1/0/5** command not only assigns the port to VLAN 55, it also sets the Port VLAN ID (PVID) to 55 (causing untagged frames to be assigned to VLAN 55) and causes frames transmitted by this port to be tagged as part of traffic for VLAN 55. These additional functions are handled by the VLAN Port Summary panel of the Web UI, and their Help screens can assist you in configuring them. For more on using the CLI to create VLANs, see the IEEE 802.1Q VLANs chapter in the *SFTOS Configuration Guide*.

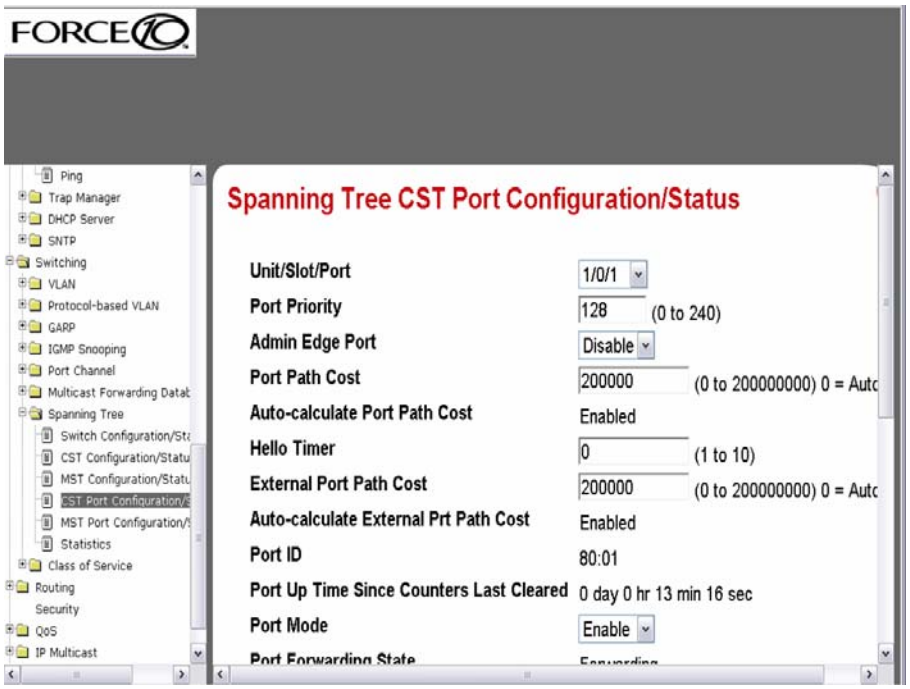
Enabling Spanning Tree Protocol

Spanning Tree Protocol (STP) is off by default. First, you must enable STP globally. To use the Web UI to enable it, navigate to the **Spanning Tree** branch, and then select the **Switch Configuration/Status** panel:



Select **Enable** next to **Spanning Tree Admin Mode**. Then click **Submit**.

Next, enable STP on the desired ports. To use the Web UI, select the **CST Port Configuration/Status** panel. Choose the port from the **Unit/Slot/Port** list, and then set **Port Mode** to **Enable**:



Alternatively, you can use the CLI to enable STP. It is possible to enable spanning tree globally, and on all the ports with just two commands:

```
(Force10 S50) #configure
(Force10 S50) (Config)#spanning-tree
(Force10 S50) (Config)#spanning-tree port mode all
(Force10 S50) (Config)#exit
(Force10 S50) #show spanning-tree summary

Spanning Tree Adminmode.......... Enabled
Spanning Tree Version............ IEEE 802.1s
Configuration Name............... 00-01-E8-D5-A0-F7
Configuration Revision Level..... 0
Configuration Digest Key..........
0xac36177f50283cd4b83821d8ab26de62
Configuration Format Selector..... 0
No MST instances to display.

(Force10 S50) #show spanning-tree interface 1/0/1
Hello Time..................................... 0
Port Mode...................................... Enabled
Port Up Time Since Counters Last Cleared....... 0 day 0 hr 19 min 38 sec
STP BPDUs Transmitted.......................... 2
STP BPDUs Received............................. 593
RSTP BPDUs Transmitted......................... 0
RSTP BPDUs Received............................ 0
MSTP BPDUs Transmitted......................... 4
MSTP BPDUs Received............................ 0

(Force10 S50) #write memory
![Your final step is to execute the write memory command to save the configuration.]!
```

Notable Differences between S-Series and E-Series

This section describes the major differences in how command usage on the S-Series differs from the E-Series. Users familiar with the E-Series CLI will notice enough similarities in the CLI environment on the S-Series that they can quickly learn the variations in syntax and usage.

Of course, there are more commands with more detailed options in FTOS than in SFTOS, because FTOS supports the E-Series switches, which are larger and more complex than the S50 (currently, the only switch in the S-Series line, supported by SFTOS).

Interface Nomenclature

The major difference between SFTOS and FTOS is that commands that contain a parameter in the form *slot/port* in FTOS use a *unit/slot/port* parameter in SFTOS for both physical and logical interfaces.

For physical identifiers, the unit is the stack member number in an S50 stack. For example, both FTOS and SFTOS have the **show interface** command, but the SFTOS equivalent of **show interface gigabitethernet 2/11** (slot 2, port 11 in FTOS) would be **show interface 1/0/11**, where 1/0/11 represents unit 1 in the stack, slot 0, port 11. If the port were in unit 2 of the S50 stack, the command would be **show interface 2/0/11**.

Logical interface identifiers are automatically generated by SFTOS. They also use the unit/slot/port convention, but system unit numbers are always 0, slot numbers are sequential, starting at 1, and the interface numbers (in the third position) are also sequential, starting at 1 per slot.

Other variations include:

- **Creating a static route**: The SFTOS command **ip route** supports only IP addresses for setting the next-hop router, while **ip route** in the FTOS also supports physical interfaces.
- **Setting the size of the logging buffer**: The FTOS command **logging buffered** has a parameter that enables you to set the size of the buffer, while SFTOS does not. Both FTOS and SFTOS invoke debug logging with the number 7 for the severity level parameter. The SFTOS command is **logging buffered 7**.
- **Displaying the MAC address table**: Both FTOS and SFTOS have the **show mac-address-table** command, but the SFTOS command **show mac-addr-table** provides more similar results to that FTOS command. The SFTOS syntax contains the *unit/slot/port* form cited above, for example, **show mac-addr-table interface 1/0/4**.
- **Displaying system information**: The FTOS command **show linecard** is similar to **show version** in SFTOS, which shows basic information, including the running software version and up time. Other similar commands in SFTOS are **show hardware** and **show sysinfo**, and **show tech-support** provides the results of a group of those similar commands.
- **service timestamps**: This FTOS command is not available in SFTOS. SFTOS sets timestamps automatically.
- **aaa authentication**: This FTOS command is available in SFTOS as **authentication**.

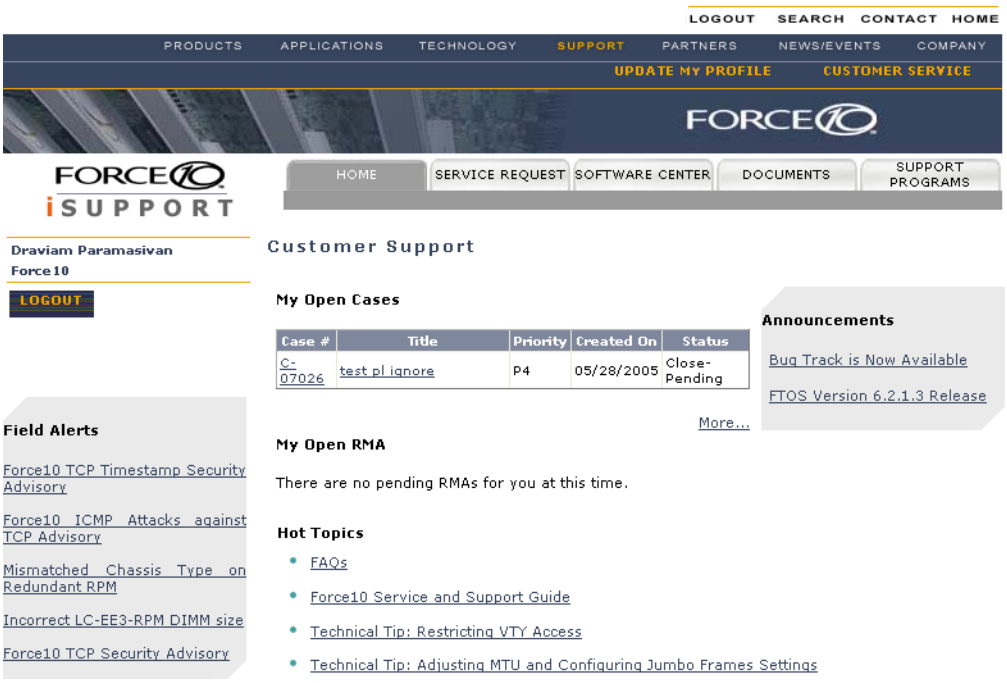
The iSupport Website

Access to some sections of the iSupport website do not require a password to access. However, if some section does require a password, you can request one at the website:

1. On the Force10 Networks website home page, http://www.force10networks.com, click the **Support** link.
2. Click the **Account Request** link.
3. Fill out the User Account Request form and click **Send**.
4. Click **Login**, and then enter the userid and password that you received by email.

The i-Support website (http://www.force10networks.com/support/) contains the following five tabs:

- **Home:** Summary of open cases, RMA management, and field notices (as shown below)
- **Service Request**: Case management
- **Software Center:** Software downloads, bug fixes, and bug tracking tool
- **Documents:** User documentation, FAQs, field notices, technical tips, and white papers
- **Support Programs:** Information on the complete suite of Force10 support and professional support services.



For more on using the iSupport website and accessing services, see the *Force10 Service and Support Guide*, available on the Home tab, as displayed above.

You can also contact the Force10 Technical Assistance Center (TAC) by email or phone. For details, click the **Contact Support** link on the **Support** page of **http://www.force10networks.com**.