Switch Installation

This chapter provides instructions on how to install your Cisco Catalyst Blade Switch 3130 for Dell and the Cisco Catalyst Blade Switch 3032 for Dell, referred to as the switch. The switch modules are installed in the Dell Modular Server Chassis, referred to as the server chassis, a system that supports up to sixteen server modules and up to six Ethernet switches. You install the switch in one of the chassis I/O module bays on the rear panel of the server chassis.

This chapter also describes how to interpret the power-on self-test (POST) that ensures proper operation and how to make connections to the switch module.

Read the topics and perform the procedures in this order:

- Safety Warnings, page 2-1
- Dell Modular Server Chassis Architecture, page 2-3
- Installing the Switch in the Server Chassis, page 2-4
- Configuring the Switch, page 2-7
- Managing the Switch, page 2-15
- Planning and Creating a Switch Stack (Only 3130G-S and 3130X-S Switches), page 2-17
- Installing Devices in the 10-Gigabit Ethernet Slots, page 2-21
- Connecting to 10/100/1000 Ethernet Ports, page 2-27
- Where to Go Next, page 2-27

Safety Warnings

These warnings are translated into several languages in the Regulatory Compliance and Safety Information for the Cisco Catalyst Blade Switch 3000 Series for Dell that ships with the product. The EMC regulatory statements are also included in that guide.

**Warning**

To prevent the switch from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of 104°F (40°C). To prevent airflow restriction, allow at least 3 inches (7.6 cm) of clearance around the ventilation openings. Statement 17B
Warning: Before working on equipment that is connected to power lines, remove jewelry (including rings, necklaces, and watches). Metal objects will heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals. Statement 43

Warning: Ethernet cables must be shielded when used in a central office environment. Statement 171

Warning: Do not work on the system or connect or disconnect cables during periods of lightning activity. Statement 1001

Warning: Read the installation instructions before connecting the system to the power source. Statement 1004

Warning: Class 1 laser product. Statement 1008

Warning: Only trained and qualified personnel should be allowed to install, replace, or service this equipment. Statement 1030

Warning: Ultimate disposal of this product should be handled according to all national laws and regulations. Statement 1040

Warning: For connections outside the building where the equipment is installed, the following ports must be connected through an approved network termination unit with integral circuit protection. 10/100/1000 Ethernet Statement 1044

Warning: Installation of the equipment must comply with local and national electrical codes. Statement 1074
Dell Modular Server Chassis Architecture

The six chassis I/O module bays are on the rear panel (see Figure 2-1).

Figure 2-1  Dell Modular Server Chassis Rear Panel

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Dell server chassis</td>
</tr>
<tr>
<td>2</td>
<td>Primary CMC(^1) module</td>
</tr>
<tr>
<td>3</td>
<td>Switch installed in I/O module bay A1</td>
</tr>
<tr>
<td>4</td>
<td>I/O module bay B1</td>
</tr>
<tr>
<td>5</td>
<td>I/O module bay C1</td>
</tr>
<tr>
<td>6</td>
<td>Optional iKVM(^3) module</td>
</tr>
<tr>
<td>7</td>
<td>I/O module bay C2</td>
</tr>
<tr>
<td>8</td>
<td>I/O module bay B2</td>
</tr>
<tr>
<td>9</td>
<td>I/O module bay A2</td>
</tr>
<tr>
<td>10</td>
<td>Secondary CMC module(^2)</td>
</tr>
<tr>
<td>11</td>
<td>Fan modules</td>
</tr>
<tr>
<td>12</td>
<td>Power supplies</td>
</tr>
</tbody>
</table>

1. CMC: Chassis Management Controller.
2. This module is optional.
3. iKVM: integrated keyboard video mouse.
Installing the Switch in the Server Chassis

See the getting started guide that ships on CD-ROM with the product for information about what ships with your switch.

Before you install the switch in the server chassis, consider these points:

- Review and become familiar with the safety and handling guidelines specified in the Product Information Guide.
- Review the Regulatory Compliance and Safety Information for the Cisco Catalyst Blade Switch 3000 Series for Dell that ships with this product.
- If you plan to create a switch stack, review the “Planning and Creating a Switch Stack (Only 3130G-S and 3130X-S Switches)” section on page 2-17 before you install the switch and run the initial configuration setup program.
- To help ensure proper cooling and system reliability, keep these points in mind:
  - Each chassis I/O module bay must contain either a module or an input/output module (IOM) blank.
  - Fan modules must be operating in the fan module bays to ensure proper cooling of the switch modules. See the Dell server chassis documentation for information about how to ensure that the modules are properly cooled.
  - When you remove a hot-swap module, you must replace it with an identical module or an IOM blank within 1 minute of removal.
  - You can install the switch into any of the module bays. If you install a switch in the B or C module bay, the Ethernet mezzanine cards must be installed in the blade server.
  - The dust covers should always remain in place unless a module is installed in the slot.

⚠️ **Caution**

To prevent electrostatic-discharge (ESD) damage when you install the switch, follow your normal board and component handling procedures.

When you install a switch, you do not need to power down the server chassis.

Be sure to observe these requirements:

- For copper Ethernet ports, cable lengths from the switch module to connected devices can be up to 328 feet (100 meters).
- See the documentation for the SFP module for more information about cable specifications for the SFP module connections. Also see the “SFP Module Cable Specifications” section on page B-6. Each port must match the wave-length specifications on the other end of the cable, and the cable must not exceed the stipulated cable length for reliable communications.
  When you use shorter lengths of single-mode fiber-optic cable, you might need to insert an inline optical attenuator in the link to avoid overloading the receiver.
- Operating environment is within the ranges listed in Appendix A, “Technical Specifications.”
- Cabling is away from sources of electrical noise, such as radios, power lines, and fluorescent lighting fixtures. Make sure the cabling is safely away from other devices that might damage the cables.
Follow these steps to install the switch into the server chassis:

**Step 1** Obtain and make note of this information from your network administrator before you begin the switch installation:
- Switch IP address
- Subnet mask (IP netmask)
- Default gateway (router)
- Enable secret password (encrypted)
- Enable password (not encrypted)
- Telnet password
- SNMP community strings (optional)

**Step 2** Select a chassis I/O module bay in which to install the switch. Follow the prerequisites listed in the “Dell Modular Server Chassis Architecture” section on page 2-3.

**Step 3** Remove the IOM blank from the selected bay, and store it for future use.

**Step 4** If you have not already done so, touch the static-protective package that contains the switch to an unpainted metal part of the server chassis for at least 2 seconds.

**Step 5** Remove the switch from its static-protective package.
**Step 6** Ensure that the release latch on the switch is in the open position or perpendicular to the module (see Figure 2-2):

![Release Latch in Open Position](image)

**Step 7** Slide the switch into the appropriate bay until it stops.

**Step 8** Push the release latch on the front of the switch to the closed position.
Figure 2-3 shows the switch being inserted into the server chassis.

Figure 2-3 Inserting the Switch into the Server Chassis

Configuring the Switch

To run the system configuration dialog, you must first connect the switch to a PC to run a terminal emulation program. You can connect the switch to the PC either through the switch console port or through the CMC console port. Instructions for these procedures are included in this section.

If you connect to the switch through the CMC, the switch console port is disabled. After you have completed the configuration procedure, you must use the disconnect command to close the active console port and re-enable the switch console port. Enter `logout` to log out of the switch, then enter `Ctrl \` to disconnect the CMC from the switch.
Follow one of these procedures:

- To run the terminal emulation program through the switch console port, go to “Connecting through the Switch Console Port” section on page 2-8.
- To run the terminal emulation program through the CMC port, go to “Connecting through the CMC” section on page 2-9.

**Connecting through the Switch Console Port**

Follow these steps when connecting through the switch console port:

**Step 1** Connect one end of the console cable to the switch console port. Connect the other end of the cable to the serial port of the PC that is running the terminal emulation application. (See Figure 2-4.)

*Figure 2-4  Connecting To the Switch Console Port*

**Step 2** Start the terminal emulation session so that you can see the output display from the power-on self-test (POST). The terminal-emulation software—a PC application such as Hyperterminal or ProcommPlus—makes communication between the switch and your PC or terminal possible.

Configure the baud rate and character format of the PC or terminal to match these console port default characteristics:

- 9600 baud
- 8 data bits
- 1 stop bit
- No parity
- None (flow control)

**Step 3** Go to the “Waiting for POST to Complete” section on page 2-10 to finish configuring the switch.
## Configuring the Switch

### Connecting through the CMC

Follow these steps when connecting through the CMC:

**Step 1**
Connect one end of a DB-9 null-modem or crossover cable to the RS-232 console serial port of the CMC. Connect the other end of the cable to the RS-232 console serial port of the PC.

**Step 2**
On the PC terminal emulation program:

a. Set the data format to 8 data bits, 1 stop bit, and no parity.

b. Set the terminal emulation speed to 115200 baud.

c. Set **Flow Control** to none.

d. Under **Properties**, select **VT100** for Emulation mode.

e. Select Terminal keys for Function, Arrow, and Ctrl keys. Ensure that the setting is for Terminal keys (not Windows keys).

When using HyperTerminal with Microsoft Windows 2000, ensure that you have Windows 2000 Service Pack 2 or later installed. With Windows 2000 Service Pack 2, the arrow keys function properly in the HyperTerminal VT100 emulation. Go to [www.microsoft.com](http://www.microsoft.com) for information on Windows 2000 service packs.

**Step 3**
On the console monitor, the CMC application displays a login screen. Log in by using these defaults:

- **username** root
- **password** calvin

The CMC command-line interface (CLI) command prompt **CMC:** appears.

**Note**
If the server chassis is off, use this command to power it on:

```
racadm chassisaction -m chassis powerup
```

The switch inserted into the chassis I/O bay automatically powers on when the server chassis powers on. For more information on configuring the server chassis by using the CLI, see the *Dell Remote Access Controller/Modular Chassis User's Guide*.

Power-cycle the switch by using this command:

```
racadm chassisaction -m switch-N powercycle
```

where *N* is the chassis I/O module bay number in which the switch is inserted.

<table>
<thead>
<tr>
<th>Module Bay</th>
<th>Substitute for <em>N</em></th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>1</td>
</tr>
<tr>
<td>A2</td>
<td>2</td>
</tr>
<tr>
<td>B1</td>
<td>3</td>
</tr>
<tr>
<td>B2</td>
<td>4</td>
</tr>
<tr>
<td>C1</td>
<td>5</td>
</tr>
<tr>
<td>C2</td>
<td>6</td>
</tr>
</tbody>
</table>
Step 4 Redirect the CMC console to the switch internal serial console interface. Enter this command at the CMC command prompt:

```
connect switch-N
```

where \(N\) is the chassis I/O module bay number in which the switch is inserted.

To return to the command prompt, press this key sequence:
```
Enter Ctrl \ (Press Enter, and press the Control key and the backslash key together.)
```

Step 5 Go to the “Waiting for POST to Complete” section on page 2-10 to finish configuring the switch.

---

**Waiting for POST to Complete**

Follow these steps to verify that POST completes successfully:

---

**Step 1** Wait for the switch to complete the POST. During POST, the LEDs blink while tests verify that the switch functions properly. Wait for the switch to complete POST, which can take several minutes.

**Step 2** Verify that POST has completed by confirming that the SYST LED remains green. If the switch fails POST, the SYST LED turns amber. See Figure 1-1 on page 1-2 for the location of the SYST LED.

POST errors are usually fatal. Call Cisco Customer Support immediately if your switch fails POST.

**Step 3** Wait for the switch to complete flash initialization. When you see the prompt `Press Return to Get Started!`, press `Return` or `Enter`.

If you do not see the prompt `Press Return to Get Started!`, be sure that you have set the baud rate on the terminal to 9600 baud.

**Step 4** Make sure that the System Status/ID LED on the switch is off. This means that the switch is operating properly.

**Step 5** See the “Completing the Initial Configuration” section on page 2-10 for instructions on setting up and initially configuring the switch.

**Step 6** If the switch obtains an IP address through the Fa0 port, you can use the device manager to configure the switch. See the “Using the Device Manager to Configure the Switch” section on page 2-13.

---

**Completing the Initial Configuration**

Follow these steps to complete the setup program and to create an initial configuration for the switch. For information about automatically configuring the switch, see the “Assigning the Switch IP Address and Default Gateway” chapter in the switch configuration guide on Cisco.com.

---

**Step 1** After you have pressed `Enter` or `Return` after the prompt to start the initial configuration setup program, enter `yes` at these prompts:

```
Would you like to terminate autoinstall? [yes]: yes
--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: yes
```
At any point you may enter a question mark '?' for help. Use ctrl-c to abort configuration dialog at any prompt. Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity for management of the system, extended setup will ask you to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: yes

Configuring global parameters:

Step 2 Enter a hostname for the switch after the prompt, and press Return.

The hostname is limited to 20 characters. Do not use -n, where n is a number, as the last character in a host name for any switch.

Step 3 Enter an enable secret password, and press Return.

The password can be from 1 to 25 alphanumeric characters, can start with a number, is case sensitive, allows spaces, but ignores leading spaces. The secret password is encrypted, and the enable password is in plain text.

Step 4 Enter an enable password, and press Return.

Step 5 Enter a virtual terminal (Telnet) password, and press Return.

The password can be from 1 to 25 alphanumeric characters, is case sensitive, allows spaces, but ignores leading spaces.

Step 6 (Optional) Configure Simple Network Management Protocol (SNMP) by responding to the prompts.

1. To configure SNMP later, press Return (which applies the default of no). If you accept the default, you can configure SNMP later through the CLI.

   Configure SNMP Network Management? [no]:

2. To configure SNMP now, enter yes.

   Configure SNMP Network Management? [no]: yes

   Community string [public]: public

Step 7 Enter the interface name (physical interface or VLAN name) of the interface that connects to the management network, and press Return.

Enter vlan1 for the interface name at this prompt.

Step 8 To configure the interface, enter Yes after the prompt, and then enter the switch IP address and subnet mask. Press Return.

The IP address and subnet mask shown here are examples:

   Configuring interface Vlan1:
   Configure IP on this interface? [yes]:
   IP address for this interface [10.0.0.1]: 10.0.0.1
   Subnet mask for this interface [255.255.255.0]: 255.255.255.0
   Class A network is 10.0.0.1, 21 subnet bits; mask is /21

Step 9 Enter no when the prompt asks you if you would like to enable the switch as a cluster command switch. This switch will be a standalone switch.

Would you like to enable as a cluster command switch? [yes/no]: no

Note Clustering is not supported.
You have now completed the initial configuration of the switch, and the switch displays its initial configuration. An example of the output is shown here:

```
The following configuration command script was created:
hostname switch1
enable secret 5 $1$cagJ$e4LP91PNazfADoNAZm6y0
enable password enable_password
line vty 0 15
password terminal-password
snmp-server community public

! interface Vlan1
no shutdown
ip address 10.0.0.1 255.255.255.0

! interface FastEthernet0
shutdown
no ip address

! interface GigabitEthernet1/0/1

! interface GigabitEthernet1/0/2

. . . (output truncated)

! interface TenGigabitEthernet1/0/1

! interface TenGigabitEthernet1/0/2

end
```

**Step 10** These choices appear:

- [0] Go to the IOS command prompt without saving this config.
- [1] Return back to the setup without saving this config.
- [2] Save this configuration to nvram and exit.

If you want to save the configuration and use it the next time the switch reboots, save it in NVRAM by selecting option 2.

Enter your selection [2]: 2

Make your selection, and press Return.

**Step 11** Disconnect the server chassis serial port or the switch console port from the PC. See the “Managing the Switch” section on page 2-15 for information about configuring and managing the switch.
Using the Device Manager to Configure the Switch

Follow these steps to set up the switch through the device manager. In a browser window, enter the IP address that the Fa0 port assigned to the switch. Before you complete the setup program, obtain the default gateway IP address and the switch password from your system administrator. You can configure these optional parameters through the Express Setup program:

- Telnet access password
- Names of the SNMP read and write community strings if you are going to use a network-management program like CiscoWorks
- Host name, system contact, and system location
- System time, time zone, Daylight Savings Time enable

Step 1

On the left side of the device manager GUI, choose Configuration > Express Setup. The Express Setup page appears (see Figure 2-5 and Figure 2-6). (Close or minimize the device manager Help window.)

Figure 2-5 Express Setup Page

Step 2

Enter this information in the Network Settings fields.

- In the Default Gateway field, enter the IP address for the default gateway (router).
- In the Switch Password field, enter your password. The password can be from 1 to 25 alphanumeric characters, can start with a number, is case sensitive, allows embedded spaces, but does not allow spaces at the beginning or end.

In the Confirm Switch Password field, enter your password again.
You can enter the **Optional Settings** information now or enter it later by using the device manager interface.

**Figure 2-6 Advanced Settings Tab**

![Advanced Settings Tab Image]

**Step 3** In the **Host Name** field, enter a name for the switch module. The host name is limited to 31 characters; embedded spaces are not allowed.

**Step 4** In the **System Date** and **System Time** fields, enter the current date and time, or use the down arrows to select them.

**Step 5** In the **Time Zone** field, use the down arrow to choose your time zone.

**Step 6** Click **Enable** in the **Daylight Savings Time** field to enable this feature.

**Step 7** In the **Telnet Access** field, click **Enable** if you are going to use Telnet to manage the switch module by using the CLI. If you enable Telnet access, you must enter a Telnet password.

**Note** If you plan to create a switch stack, enable Telnet access so that you can use the CLI to set this switch to the highest priority (usually 15). See the “Planning and Creating a Switch Stack (Only 3130G-S and 3130X-S Switches)” section on page 2-17 for more information about creating a switch stack.

**Step 8** In the **Telnet Password** field, enter a password. The Telnet password can be from 1 to 25 alphanumeric characters, is case sensitive, allows embedded spaces, but does not allow spaces at the beginning or end. In the **Confirm Telnet Password** field, re-enter the Telnet password.

**Step 9** In the **SNMP** field, click **Enable** to enable Simple Network Management Protocol (SNMP). Enable SNMP only if you plan to manage switches by using CiscoWorks 2000 or another SNMP-based network-management system.

**Step 10** If you enable SNMP, you must enter a community string in the **SNMP Read Community** field, the **SNMP Write Community** field, or both. SNMP community strings authenticate access to MIB objects. Embedded spaces are not allowed in SNMP community strings. When you set the SNMP read community, you can access SNMP information, but you cannot change it. When you set the SNMP write community, you can both access and change SNMP information.
Step 11 In the System Contact field, enter the name of the person who is responsible for the switch module. In the System Location field, enter the wiring closet, floor, or building where the switch module is located.

Step 12 Depending on which software license you choose, you can enable IPv6 in the IPv6 Settings area.
- Click Enable IPv6 to enable it.
- In the Interface column, choose the interface for which you want to set an IPv6 address, and complete the other fields in this table.

Step 13 Click Submit to save your settings, or click Cancel to clear your settings.
You can close this window.

Configuring the Switch Stack Master

If you plan to create a switch stack, we recommend that you set the first configured switch as the stack master. To do this, you must assign the highest priority value to that switch. To assign a priority value after you have installed and initially configured the first switch, follow these steps:

Step 1 Launch a Telnet session.
Step 2 Enter enable.
Step 3 Enter configure terminal.
Step 4 Enter switch 1 priority 15.
Step 5 At the prompt, press Return.
Step 6 Enter end to exit this mode.
Step 7 Enter copy running-configuration startup-configuration to save this setting.
Step 8 At the prompt, press Return.
Step 9 To verify that this switch is set as the master, enter the show switch user EXEC command.

For more information about creating switch stacks, see the “Planning and Creating a Switch Stack (Only 3130G-S and 3130X-S Switches)” section on page 2-17.

Managing the Switch

After completing the initial setup and configuration steps, use the CLI, the device manager, or other management options described in this section for further configuration.

Using the CLI

After setting up and installing the switch in your network, you can enter Cisco IOS commands and parameters through the CLI. Access the CLI either by connecting your PC directly to the switch console port or through a Telnet session from a remote PC or workstation. You can also access the CLI through the server chassis serial console port of the active Dell CMC. For more information, see the hardware installation guide on Cisco.com.
Using the Device Manager

The simplest way to manage the switch is by using the device manager that is in the switch memory. This is an easy-to-use web interface that offers quick configuration and monitoring. You can access the device manager from anywhere in your network through a web browser. The device manager dashboard is shown in **Figure 2-7**.

**Figure 2-7  Device Manager Dashboard**

Follow these steps to access the device manager:

1. **Step 1**  Launch a web browser on your PC or workstation.
2. **Step 2**  Enter the switch IP address in the web browser, and press **Enter**. The device manager page appears.
3. **Step 3**  Use the device manager to perform basic switch configuration and monitoring. See the device manager online help for more information.

**Other Management Options**

You can use SNMP management applications such as CiscoWorks. You also can manage it from an SNMP-compatible workstation that is running platforms such as SunNet Manager.
Planning and Creating a Switch Stack (Only 3130G-S and 3130X-S Switches)

A switch stack is a set of up to nine stacking-capable switches that are connected through their StackWise Plus ports. One switch controls the operation of the stack and is called the stack master. The stack master and the other switches in the stack are stack members. Layer 2 and Layer 3 protocols present the entire switch stack as a single entity to the network. Stacking is optional.

When switches are not stacked, each acts as a standalone switch. For general concepts and procedures to manage switch stacks, see the switch software configuration guide and command reference on Cisco.com.

Caution

The Cisco Catalyst Blade Switch 3130 for Dell does not support switch stacks with other types of blade switches as members. Combining the Cisco Catalyst Blade Switch 3130 for Dell with other types of blade switches in a switch stack might cause the switch to work improperly or to fail.

Before you connect the switches in a stack, keep in mind these stacking guidelines:

- You should install the stack master switch and run the initial setup program on that switch before you connect the StackWise Plus cables to other stack members. We recommend that you assign the highest priority value to the switch that you prefer to be the stack master. This ensures that the switch is re-elected as stack master if a re-election occurs. As you add new switches to the stack, they automatically become stack members.

- When you connect the StackWise Plus cables and create a stack, you can communicate with the master switch internal Ethernet management port (Fa0) port, but not the Fa0 ports of the member switches. Only one Fa0 interface can be active, and that interface is the one on the active stack master.

- For conditions that might cause a stack master re-election or to manually elect the stack master, see the “Managing Switch Stacks” chapter in the switch software configuration guide on Cisco.com.

- You can stack any combination of up to nine Catalyst 3130G-S and 3130X-S switches. You can stack only the Catalyst 3130 switches; other switches cannot be stacked.

- Before installation, verify the StackWise Plus cable length. Depending on your configuration, you might need different sized cables. If you do not specify the length of the StackWise Plus cable when you order your product, the 1-meter cable is supplied. If you need the 0.5-meter cable or the 3-meter cable, you can order these StackWise Plus cables from your sales representative:
  - CAB-STK-E-0.5M= (0.5-meter cable)
  - CAB-STK-E-1M= (1-meter cable)
  - CAB-STK-E-3M= (3-meter cable)

For switch dimensions and additional stacking guidelines, see the switch hardware installation guide on Cisco.com. For concepts and procedures to manage switch stacks, see the switch software configuration guide on Cisco.com.

To create a switch stack:

Step 1
Install the member switches if you have not already done so.
Step 2  Connect the StackWise Plus cables as described in the “Planning and Creating a Switch Stack (Only 3130G-S and 3130X-S Switches)” section on page 2-17.

Step 3  Configure the member switches through the master switch by using the CLI.

Stack Cabling Configurations

This section describes the recommended configurations for stacking the switches by using the supplied 1-meter StackWise cable.

In this example, the stack uses the 1-meter StackWise Plus cable to make redundant connections between two Catalyst 3130 switches in a single chassis (see Figure 2-8).

Figure 2-8  Stacking Two Switch Modules in a Single Blade Server to Create One Stack
Figure 2-9 is an example of a recommended configuration in which eight switch modules create a switch stack in four blade servers.

**Figure 2-9**  
*Stacking Eight Switch Modules in Four Blade Servers to Create One Stack*
Figure 2-10 is an example of a recommended configuration in which eight switch modules create two separate switch stacks in four blade servers. This configuration provides redundant connections.

*Figure 2-10  Stacking up to Eight Switch Modules in Four Server Chassis to Create Two Stacks*
Connecting the StackWise Plus Cables

Follow these steps to connect the StackWise Plus cables:

**Step 1** Remove the dust covers from the StackWise Plus cables, and store them for future use.

**Step 2** Verify that cables are aligned as shown in Figure 2-11.

*Figure 2-11  Inserting the StackWise Plus Cable*

**Step 3** Insert one end of the cable into the StackWise Plus port on the front panel of the switch. Insert the other end of the cable into the connector on the other switch (see Figure 2-11).

Always use a Cisco-approved StackWise Plus cable to connect the switches.

When you remove the StackWise Plus cables from the connectors, replace the dust covers to protect them from dust.

**Caution** Removing and installing the StackWise Plus cable can shorten its useful life. Do not remove and insert the cable more often than is absolutely necessary.

Installing Devices in the 10-Gigabit Ethernet Slots

These sections describe how to install and remove X2 transceiver modules, Cisco TwinGig Converter Modules (also known as converter modules), and SFP modules:

- Installing X2 Transceiver Modules and Cisco Converter Modules, page 2-22
- Installing SFP Modules, page 2-25

**Caution** Do not remove the dust plugs from the fiber-optic X2 transceiver modules or SFP modules or the rubber caps from the fiber-optic cable until you are ready to connect the cable. The plugs and caps protect the module ports and cables from contamination and ambient light.
Caution
Do not install or remove an X2 or SFP module with the cables attached because of the potential damage to the cables, the cable connectors, or the optical interfaces in the modules. Disconnect all cables before removing or installing the module.

Caution
Removing and installing an X2 or SFP module can shorten its useful life. Do not remove and insert any X2 or SFP module more often than is absolutely necessary.

Caution
To prevent ESD damage, follow your normal board and component handling procedures when connecting cables to the switch and other devices.

Installing X2 Transceiver Modules and Cisco Converter Modules

These sections describe how to install and remove X2 transceiver modules and the converter modules in the switch module 10-Gigabit Ethernet module slots.

Note
Do not remove the dust cover from the converter module until you are ready to install an X2 transceiver or SFP modules. A module or dust cover must be installed in the slot at all times.

The Cisco Catalyst Blade Switch 3032G and 3130G support only the Cisco TwinGig Converter Modules, not the X2 transceiver modules.

Use only Cisco X2 transceiver modules and Cisco TwinGig Converter Modules with the switch module. Each Cisco transceiver and converter module has an internal serial EEPROM that is encoded with security information. This encoding provides a way for Cisco to identify and validate that the module meets the requirements for the switch.

For more information about installing, removing, cabling, and troubleshooting X2 transceiver modules, see the module documentation that shipped with your device. For module cable specifications, see Appendix B, “Connector and Cable Specifications.”

Installing a Transceiver or Converter Module

When you install or remove the converter module, the mode on the switch changes from 10-Gigabit Ethernet to Gigabit Ethernet or the reverse. During this mode change, data traffic on the other switch module uplink ports (X2 transceiver or SFP module ports) might temporarily stop. When you install or remove an X2 transceiver or SFP module, traffic delay does not occur.

To insert an X2 transceiver module or a converter module, follow these steps:

Step 1
Attach an ESD-preventive wrist strap to your wrist and to a bare metal surface.

Step 2
Remove the transceiver or converter module from its protective packaging.

Step 3
Align the transceiver module in the module slot (Figure 2-12 and Figure 2-13).
Caution
Verify the correct orientation of your module before inserting it into the slot. Incorrect insertion can damage the module.

Step 4
Slide the transceiver or converter module into the opening until the back of its faceplate is flush with the switch module faceplate.

Caution
Do not install the converter module with SFP modules or cables installed. Always remove any cables and modules before installing the converter module in the slot.
Removing a Module

To remove an X2 transceiver module or a converter module, follow these steps:

**Step 1**  Attach an ESD-preventive wrist strap to your wrist and to a bare metal surface.

**Step 2**  For X2 transceiver modules, disconnect the cables from the module. For fiber-optic modules, install the optical bore dust plugs.

**Step 3**  For converter modules, disconnect the cables from the SFP module. Remove the SFP modules from the converter module.

**Caution**  Do not remove the converter module with SFP modules or cables installed. Always remove any cables and modules before removing the converter module from the slot.

**Step 4**  Carefully pull on the X2 module sleeve, or pinch the tabs on the converter module to disengage it from the slot. Grasp the edges of the module, and carefully slide it out of the slot.

**Step 5**  Reinstall the dust cover in the 10-Gigabit Ethernet slot.

**Caution**  The dust covers should always remain in place unless a module is installed in the slot.

**Step 6**  Place the module in an antistatic bag or other protective environment.
Installing SFP Modules

This section describes how to install and remove SFP modules in the 10-Gigabit Ethernet slots. To use SFP modules in the switch, you must have a converter module installed in a 10-Gigabit Ethernet slot.

Caution

To avoid damage to the converter module, first install the converter module in the switch 10-Gigabit Ethernet slot before installing the SFP modules.

See the switch module release notes on Cisco.com for the list of SFP modules that the switch module supports. Use only Cisco SFP modules on the switch. Each Cisco module has an internal serial EEPROM that is encoded with security information. This encoding provides a way for Cisco to identify and validate that the SFP module meets the requirements for the switch.

For more information about installing, removing, cabling, and troubleshooting SFP modules, see the module documentation that shipped with your device. For module cable specifications, see Appendix B, “Connector and Cable Specifications.”

Installing an SFP Module

To insert an SFP module into a converter module slot, follow these steps:

| Step 1 | Attach an ESD-preventive wrist strap to your wrist and to a bare metal surface. |
| Step 2 | Remove the Cisco TwinGig Converter Module dust cover and save. |
| Note | The dust cover is an integral part of the airflow function. If you remove the SFP module, you must replace it with the saved dust cover. |
| Step 3 | Install the converter module in the 10-Gigabit Ethernet module slot as described in “Installing a Transceiver or Converter Module” section on page 2-22. |
| Step 4 | Find the send (TX) and receive (RX) markings that identify the top side of the SFP module. |
| | On some SFP modules, the send and receive (TX and RX) markings might be replaced by arrows that show the direction of the connection, either send or receive (TX or RX). |
| Step 5 | If the SFP module has a bale-clasp latch, move it to the open, unlocked position. |
| Step 6 | Align the SFP module in the converter module opening. When installing a module in the upper module slot (slot 1), position the SFP module face up. When using the lower module slot (slot 2), position the SFP module face down. |
| Step 7 | Slide the SFP module into the opening until you feel the connector on the module snap into place (Figure 2-14). |
| Step 8 | If the module has a bale-clasp latch, close it to lock the SFP module in place. |
| Step 9 | Remove the SFP dust plugs and save. Install the SFP cables. |
Removing an SFP Module

To remove an SFP module from a module slot, follow these steps:

**Step 1**  Attach an ESD-preventive wrist strap to your wrist and to a bare metal surface.

**Step 2**  Disconnect the cable from the SFP module. For reattachment, note which cable connector plug is send (TX) and which is receive (RX).

**Step 3**  Insert a dust plug into the optical ports of the SFP module to keep the optical interfaces clean.

**Step 4**  If the module has a bale-clasp latch, pull the bale out and down to eject the module. If the bale-clasp latch is obstructed and you cannot use your index finger to open it, use a small, flat-blade screwdriver or other long, narrow instrument to open the bale-clasp latch.

**Step 5**  Grasp the SFP module, and carefully remove it from the module slot.

**Step 6**  Place the removed SFP module in an antistatic bag or other protective environment.

---

**Caution**  Category 5e and Category 6 cables can store high levels of static electricity. Always ground the cables to a suitable and safe earth ground before connecting them to the switch or other devices.
Connecting to 10/100/1000 Ethernet Ports

The 10/100/1000 Ethernet ports use standard RJ-45 connectors with Ethernet pinouts. The maximum cable length is 328 feet (100 meters). The 100BASE-TX and 1000BASE-T traffic requires Category 5, Category 5e, or Category 6 UTP cable. The 10BASE-T traffic can use Category 3 or Category 4 cable.

The autonegotiation feature is enabled by default on the switch. At this setting, the switch ports configure themselves to operate at the speed of attached device. If the attached device does not support autonegotiation, you can explicitly set the switch port speed and duplex parameters. To maximize performance, either let the ports autonegotiate both speed and duplex, or set the port speed and duplex parameters on both ends of the connection.

For simplified cabling, the automatic medium-dependent interface crossover (auto-MDIX) feature is enabled by default on the switch. With auto-MDIX enabled, the switch detects the required cable type for copper Ethernet connections and configures the interface accordingly. Therefore, you can use either a crossover or a straight-through cable for connections to a switch 10/100/1000 Ethernet port regardless of the type of device on the other end of the connection.

See the switch software configuration guide or the switch command reference on Cisco.com for more information about enabling or disabling autonegotiation and auto-MDIX.

If auto-MDIX is disabled, use the guidelines in Table 2-1 to select the correct cable for connecting the switch 10/100/1000 Ethernet ports to other devices. See the “Cable and Adapter Specifications” section on page B-4 for cable-pinout descriptions.

<table>
<thead>
<tr>
<th>Device</th>
<th>Crossover Cable</th>
<th>Straight-Through Cable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch to switch</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Switch to hub</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Switch to computer or server</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Switch to router</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Switch to IP phone</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

1. 100BASE-TX and 1000BASE-T traffic requires twisted four-pair, Category 5, Category 5e, or Category 6 cable. 10BASE-T traffic can use Category 3 or Category 4 cable.

Where to Go Next

If the default configuration is satisfactory, the switch module does not need further configuration. You can use any of these management options to change the default configuration:

- **Using the Device Manager**
  Access the device manager through a web browser from anywhere in your network. See “Using the Device Manager” section on page 2-16 for instructions.

- **Using the Command-Line Interface**
  The switch module CLI is based on Cisco IOS software and enhanced to support desktop-switching features. You can fully configure and monitor the switch module from the CLI. You can access the CLI either by connecting your management station directly to the switch module console port or by using Telnet from a remote management station. Refer to the switch module command reference on Cisco.com for more information.
- Using SNMP
  You can use SNMP management applications such as CiscoWorks Small Network Management Solution (SNMS) to configure and manage the switch module. You also can manage it from an SNMP-compatible workstation that is running platforms such as HP OpenView or SunNet Manager.

- Using the Dell CMC
  See the Dell documentation for more information.