Cisco Catalyst Blade Switch 3030 Getting Started Guide

This guide provides instructions on how to install your Cisco Catalyst Blade Switch 3030—hereafter referred to as the *switch module*—in the Dell Modular Server Chassis and to set up and configure your switch module. The Dell Modular Server Chassis—hereafter referred to as the *server chassis*—is a system that supports up to ten server modules and up to four Ethernet switch modules. The switch module is installed in one of the chassis I/O module bays on the rear panel of the server chassis.

Also covered in this guide are switch management options and troubleshooting help for the switch module.

For details on the number, types, and the location of the module bays and for additional information on the entire modular server system, see the *Dell PowerEdge 1855 Systems User's Guide* and the *Dell PowerEdge 1855 Systems Installation and Troubleshooting Guide* at www.support.dell.com.

For additional installation and configuration information about the switch module, see the Cisco Catalyst Blade Switch 3030 documentation on Cisco.com. For system requirements, important notes, limitations, open and resolved caveats, and last-minute documentation updates about the switch module, see the release notes, also on Cisco.com.

When using the online publications, refer to the documents that match the Cisco IOS software version that is running on the switch. You can order printed copies of the manuals from the Cisco.com sites and from the telephone numbers listed in the "Obtaining Documentation" section on page 1-24.

For translations of the warnings that appear in this publication, see the *Regulatory Compliance and Safety Information for the Cisco Catalyst Blade Switch 3030 Getting Started Guide* that accompanies this guide.

Note Before proceeding, read the release notes for the server chassis. The release notes are available on the Dell support website at www.support.dell.com.

Contents

Taking Out What You Need

These items ship with your switch module:

- Console cable
- *Cisco Catalyst Blade Switch 3030 Getting Started Guide* (this book)

- *Regulatory Compliance and Safety Information for the Cisco Catalyst Blade Switch 3030*
- Registration card

Follow these steps:

1. Unpack and remove the switch module and the accessory kit from the shipping box.
2. Return the packing material to the shipping container, and save it for future use.

Note If the switch modules are ordered with the server chassis, the switch modules are already installed, and no unpacking is required. The unpacking procedure applies only if a switch module is ordered separately.

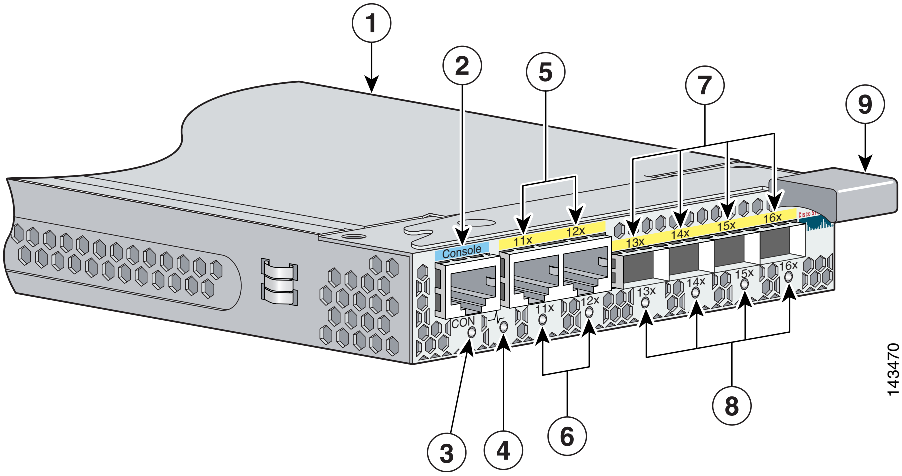
Cisco Gigabit Ethernet Switch Module Description

Figure 1 shows the switch module, which has these features:

- 10 internal Gigabit Ethernet 1000BASE-X ports
- 1 console port
- 2 external 10/100/1000BASE-T copper Gigabit Ethernet ports
- 4 external small form-factor pluggable (SFP) module uplink ports that support 1000BASE-SX fiber and 10/100/1000BASE-T copper (only Cisco SFP modules are supported)

Each port has an LED associated with it. Additionally, there is a System Status/ID LED that is controlled by the Dell Remote Access Controller/Modular Chassis (DRAC/MC) management board.

Figure 1 The Cisco Gigabit Ethernet Switch Module



1	Switch module	**6**	Gigabit Ethernet port LEDs
2	Console port	**7**	SFP module ports
3	Console port LED	**8**	SFP module port LEDs
4	System Status/ID LED	**9**	Release latch
5	Gigabit Ethernet ports		

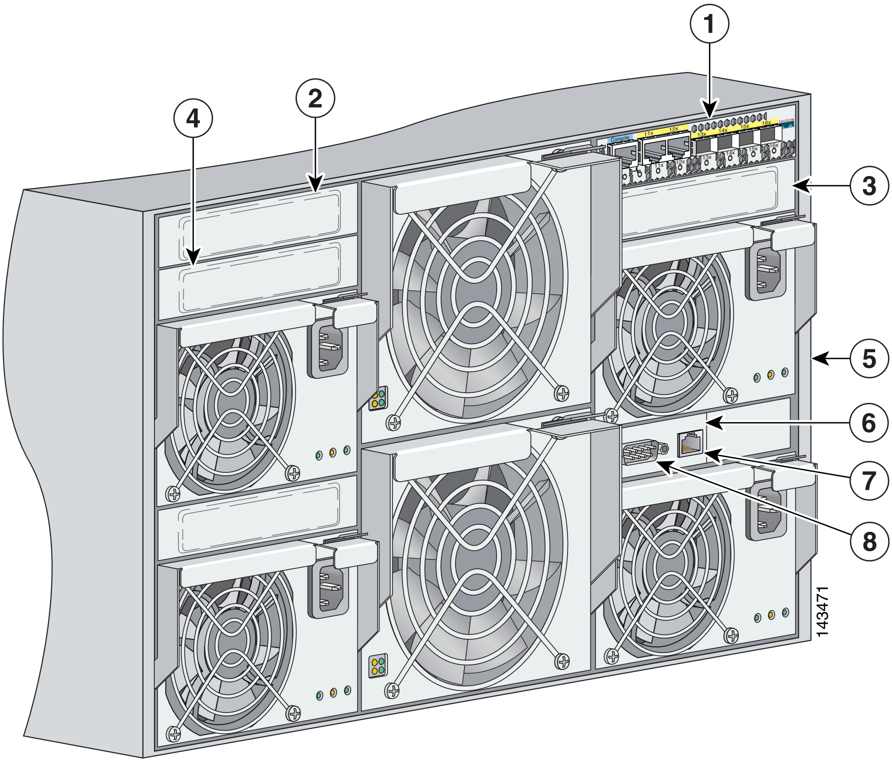
You need to supply this equipment to set up your switch module:

- PC
- Ethernet (Category 5) straight-through cable (as shown) or console cable

Dell Modular Server Chassis Architecture

The four chassis I/O module bays are on the rear panel (see Figure 2). You can insert switch modules into the chassis I/O module bays 1 and 2. Use bays 3 and 4 for switch modules only if a Gigabit Ethernet daughter card is installed on the server modules.

Figure 2 Dell Modular Server Chassis



1	Bay 1 (populated with switch module)	**5**	Rear panel of server chassis
2	Bay 2	**6**	DRAC/MC management board
3	Bay 3	**7**	Ethernet port
4	Bay 4	**8**	RS-232 port

Consider these prerequisites before installing your switch module:

- Bay 1 and bay 2 are a pair. Bay 1 must be populated before bay 2. If bay 2 is used, the I/O module in bay 2 must be the same type as the one in bay 1.
- Bay 3 and bay 4 are a pair. Bay 3 must be populated before bay 4. If bay 4 is used, the I/O module in bay 4 must be the same type as the one in bay 3.

For more information about the components of the information panel, see the *Dell PowerEdge 1855 Systems User's Guide* and the *Dell PowerEdge 1855 Systems Installation and Troubleshooting Guide*.

Installing the Switch Module in the Server Chassis

Before you install the switch module 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 and the *Regulatory Compliance and Safety Information for the Cisco Catalyst Blade Switch 3030* that accompanies this guide.
- 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 end-cap (blank plug).
  - When you remove a hot-swap module, you must replace it with an identical module or an end-cap (blank plug) within 1 minute of removal.

Caution To prevent electrostatic-discharge (ESD) damage when installing switch modules, follow your normal board and component handling procedures.

Note When you install a switch module, you do not need to power down the server modules or the switch.

Note The initial configuration assumes that the switch module was never configured, that it is in the same state as when it was received, and that it is not configured with a default username and password.

Follow these steps to install the switch module into the server chassis:

Step 1 Obtain and make note of this information from your network administrator before you begin the switch module 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)

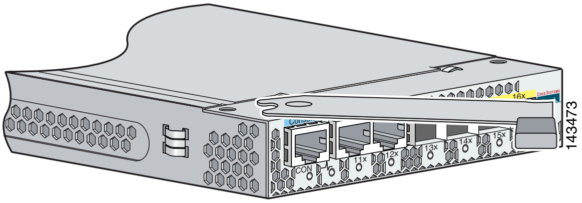
Step 2 Select a chassis I/O module bay in which to install the switch module. Follow the prerequisites listed in the "Dell Modular Server Chassis Architecture" section on page 1-5.

Step 3 Remove the end-cap (blank plug) from the selected bay. Store the end-cap (blank plug) for future use.

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

Step 5 Remove the switch module from its static-protective package.

Step 6 Ensure that the release latch on the switch module is in the open position (perpendicular to the module):

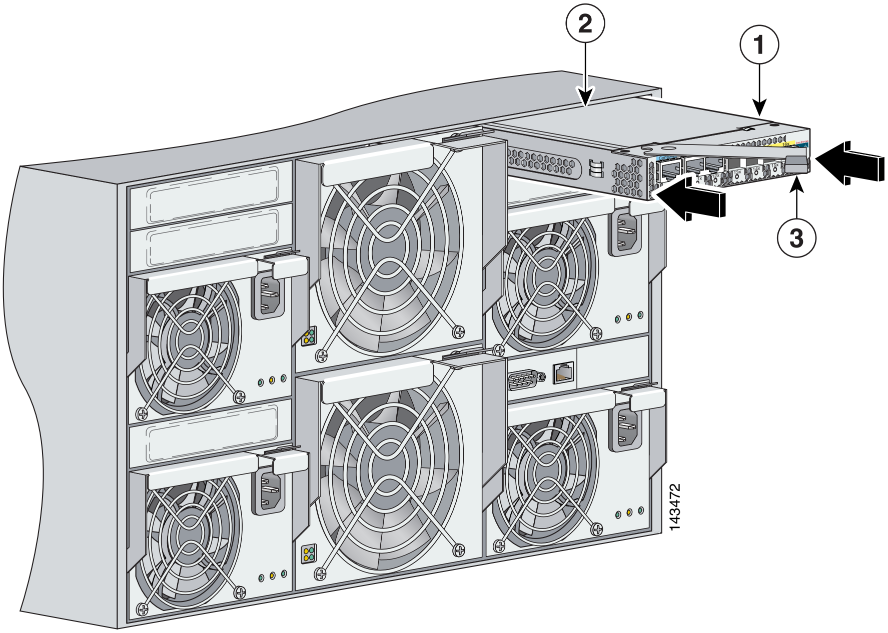


Step 7 Slide the switch module into the appropriate bay until it stops.

Step 8 Push the release latch on the front of the switch module to the closed position.

Figure 3 shows the switch module being inserted into the server chassis.

Figure 3 Inserting the Switch Module into the Server Chassis



1	Switch module	**3**	Release latch
2	Server chassis		

Configuring the Switch Module

Note To run the system configuration dialog, you must first connect the switch to a PC to run a terminal emulation program. There are two ways you can connect the PC to the switch: either through the switch console port or through the DRAC/MC console port. Instructions for these two procedures are included in this section.

If you connect to the switch through the DRAC/MC, 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. Type **logout** to log out of the switch, then type **~.** to disconnect the DRAC/MC from the switch.

Follow one of these procedures:

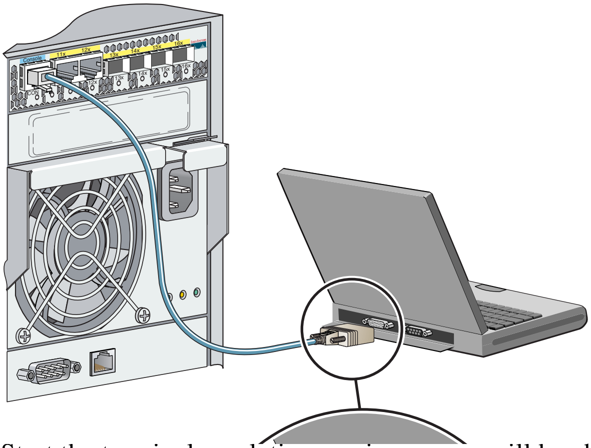
- To run the terminal emulation program through the switch module console port, go to "Connecting through the Switch Module Console Port" section on page 1-9.
- To run the terminal emulation program through the DRAC/MC port, go to "Connecting through the DRAC/MC" section on page 1-11.

Connecting through the Switch Module Console Port

Follow these steps when connecting through the switch module console port:

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

Figure 4 Connecting through the Switch Module Console Port



Step 2 Start the terminal emulation session so you will be able to 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)

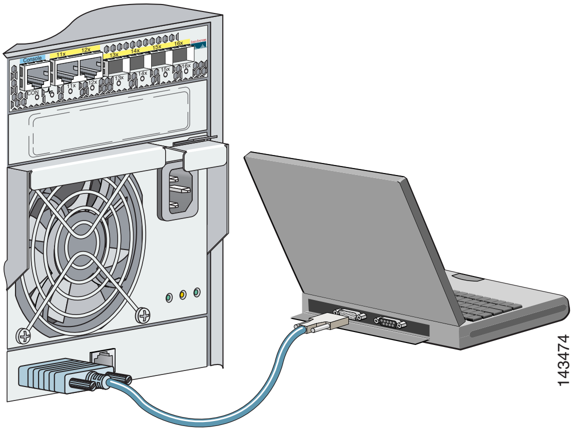
Step 3 Go to "Waiting for POST to Complete" section on page 1-13 to finish configuring the switch module.

Connecting through the DRAC/MC

Follow these steps when connecting through the DRAC/MC:

Step 1 Connect one end of a DB9 null-modem or crossover cable to the RS-232 console serial port of the DRAC/MC. Connect the other end of the cable to the RS-232 console serial port of the computer. (See Figure 5.)

Figure 5 Connecting through the DRAC/MC



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 for information on Windows 2000 service packs.

Step 3 On the console monitor, the DRAC/MC application displays a login screen. Log in by using these defaults:
username **root**
password **calvin**

The DRAC/MC command-line interface (CLI) command prompt **DRAC/MC:** appears.

Step 4 If the server chassis is off, use this command to power it on:

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

The switch module 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*.

Step 5 Power cycle the switch module by using this command:

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

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

Step 6 Redirect the DRAC/MC console to the switch module internal serial console interface. Enter this command at the DRAC/MC command prompt:

```
connect switch-N
```

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

To return to the command prompt, press this key sequence:
Enter ~.
First press **Enter**, press tilde ~ (remember to press the <Shift> key if the tilde character is located in the upper register of your keyboard), and then press period **.** (dot).

Step 7 Go to "Waiting for POST to Complete" section on page 1-13 to finish configuring the switch module.

Waiting for POST to Complete

Follow these steps:

Step 1 Wait for the switch to complete the power-on self test (POST). It might take several minutes for the switch to complete POST.

Step 2 Verify that POST has completed by confirming that the System Status/ID LED is off, and the Console LED is solid green or amber. If the switch fails POST because of a misconfiguration or error, the System Status/ID LED blinks green, and the Console LED is off.

Log into the DRAC/MC console to get more details about the failure mode.

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

See item 4 in Figure 1 on page 4 for the location of the System Status/ID LED and the Console LED.

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

Step 4 Make sure that the System Status/ID LED on the switch module is off and the Console LED is green or amber. This means that the switch module is operating properly.

Step 5 See the "Completing the Initial Configuration" section on page 1-13 for instructions on setting up and initially configuring the switch module.

Completing the Initial Configuration

Follow these steps to complete the setup program and to create an initial configuration for the switch.

Note For information about automatically configuring the switch, see the "Assigning the Switch IP Address and Default Gateway" chapter in the switch configuration guide.

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]:
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 on the Cisco Catalyst Blade Switch 3030.

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$e4LP91PNazfdADoNAZm6y0
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 GigabitEthernet0/1
!
interface GigabitEthernet0/2

. . . (output truncated)
```

```
interface GigabitEthernet0/16
!
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 1-16 for information about configuring and managing the switch.

If you need to rerun the initial configuration dialog, see the "Resetting the Switch Configuration" section on page 1-22.

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.

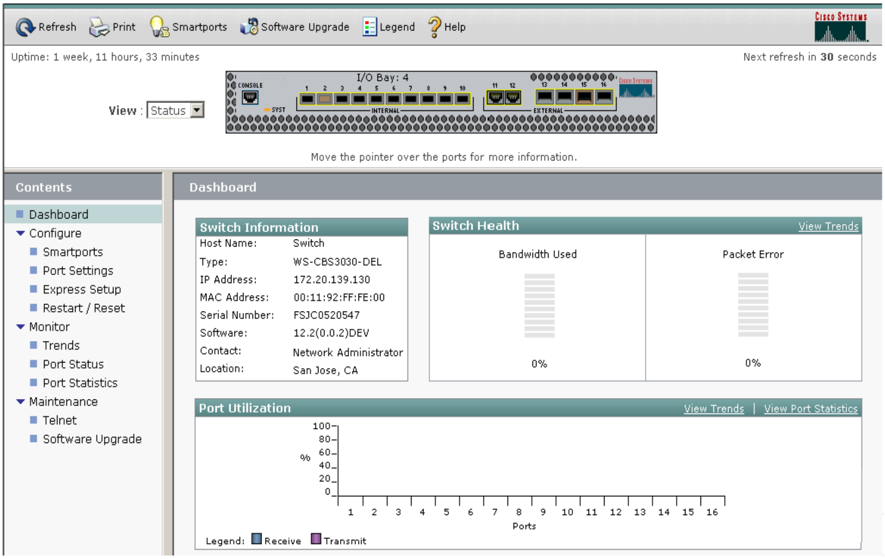
Using the CLI

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 console serial port (see "Configuring the Switch Module" section on page 1-9).

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 6.

Figure 6 Device Manager Dashboard



Uptime: 1 week, 11 hours, 33 minutes

Next refresh in **30** seconds

Move the pointer over the ports for more information.

Host Name:	Switch
Type:	WS-CBS3030-DEL
IP Address:	172.20.139.130
MAC Address:	00:11:92:FF:FE:00
Serial Number:	FSJC0520547
Software:	12.2(0.0.2)DEV
Contact:	Network Administrator
Location:	San Jose, CA

Follow these steps to access the device manager:

1. Launch a web browser on your PC or workstation.
2. Enter the switch IP address in the web browser, and press **Enter**. The device manager page appears.
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.

See the "Accessing Help Online" section on page 1-23 for a list of supporting documentation.

Installation Warning Statements

This section includes the basic installation warning statements. Translations of these warning statements appear in the *Regulatory Compliance and Safety Information for the Cisco Gigabit Ethernet Switch Module for the Dell Server Chassis* document that shipped with the switch.

Warning **To prevent the switch from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of 113°F (45°C). To prevent airflow restriction, allow at least 3 inches (7.6 cm) of clearance around the ventilation openings.** Statement 17B

Warning **Class 1 laser product.** Statement 1008

Warning **This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.** Statement 1024

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

Connect to the Switch Ports

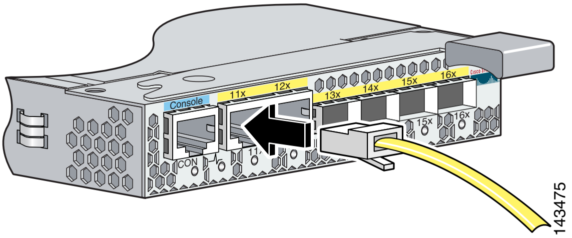
This section describes how to connect to the fixed switch ports and to the SFP module ports.

Connect to the 10/100/1000 Ports

Follow these steps:

Step 1 The automatic medium-dependent interface crossover (auto-MDIX) feature is enabled by default on the switch module. When the auto-MDIX feature is enabled, the switch detects the required cable type for copper Ethernet connections and configures the interfaces accordingly. (See Figure 7.)

Figure 7 Connecting to 10/100/1000 Ports



Use either a crossover or a straight-through cable for connections to a copper 10/100/1000 or 1000BASE-T SFP module port on the switch, regardless of the type of device on the other end of the connection.

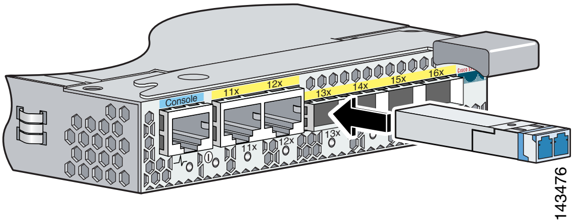
Step 2 Insert the other cable end into an RJ-45 connector on the other device.

Install the SFP Modules and Connect to the Ports

Follow these steps:

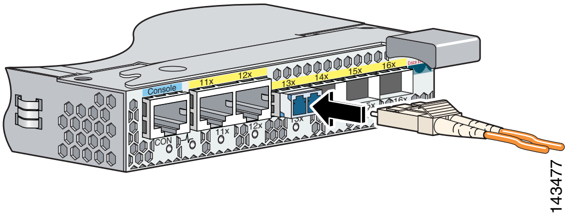
Step 1 Grasp the SFP module on the sides, and insert it into the switch slot until you feel the connector snap into place (see Figure 8).

Figure 8 Installing an SFP Module



Step 2 Insert an appropriate cable into the SFP module port. Insert the other cable end into the other device (see Figure 9).

Figure 9 Inserting the Cable into the SFP Module Port



For a list of supported modules, see the release notes on Cisco.com. For detailed instructions on installing, removing, and connecting to SFP modules, see the documentation that came with the SFP module.

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

Verify Port Connectivity

After you connect to the switch port, the port LED turns amber while the switch establishes a link. This process takes about 30 seconds, and then the LED turns green when the switch and the target device have an established link. If the LED is off, the target device might not be turned on, there might be a cable problem, or there might be a problem with the adapter installed in the target device. See the "In Case of Difficulty" section on page 1-22 for information about online assistance.

In Case of Difficulty

If you experience difficulty, help is available in this section and on Cisco.com. This section includes initial setup troubleshooting, how to reset the switch, how to access help online, and where to find more information.

Troubleshooting Initial Configuration Setup

If you have problems running the initial configuration dialog:

• Did you verify that POST successfully ran before running the initial configuration dialog?	POST errors are usually fatal. Call Cisco Customer Support immediately if your switch fails POST.
• Did you wait 30 seconds after connecting the switch and the PC before entering the IP address in your browser?	If not, wait 30 seconds, re-enter **10.0.0.1** in the browser, and press **Enter**.
• Did you lock yourself out and forget your password?	See the “Recovering from a Lost or Forgotten Password” section in the Troubleshooting appendix of the software configuration guide if you forget your password.

Resetting the Switch Configuration

This section describes how to reset the switch configuration by rerunning the initial configuration dialog (System Configuration Dialog). These are reasons why you might want to reset the switch:

- You installed the switch in your network and cannot connect to it because you assigned the wrong IP address.
- You want to clear all configuration from the switch and assign a new IP address.

⚠ **Caution** Resetting the switch deletes the configuration and reboots the switch.

To reset the switch:

- At the switch prompt, enter **enable** and press **Return or Enter**.
- At the Privileged EXEC prompt, `switch#`, enter **setup** and press **Return or Enter**.

The switch displays the prompt to run the initial configuration dialog. See the "Configuring the Switch Module" section on page 1-9 to re-enter the configuration information and set up your switch.

Accessing Help Online

First look for a solution to your problem in the troubleshooting sections of the hardware installation guide or the software configuration guide for your switch on Cisco.com. You can also go to the Cisco Technical Support and Documentation website for a list of known hardware problems and extensive troubleshooting documentation, including:

- Factory defaults and password recovery
- Recovery from corrupted or missing software
- Switch port problems
- Network interface cards
- Troubleshooting tools
- Field notices and security advisories

Follow these steps:

1. Open your browser, and go to http://www.cisco.com/.
2. Click **Technical Support and Documentation**.
3. Click **Product Support > Switches > LAN and ATM Switches > Cisco Gigabit Ethernet Switch Module > Troubleshooting**.
4. Click the subject that addresses the problem that you are experiencing.

For More Information

For more information about the switch, see these documents on Cisco.com:

- *Cisco Catalyst Blade Switch 3030 Hardware Installation Guide* (not orderable, but available on Cisco.com). This guide provides complete hardware descriptions and detailed installation procedures.
- *Regulatory Compliance and Safety Information for the Cisco Catalyst Blade Switch 3030* (order number DOC-7817053=). This guide contains agency approvals, compliance information, and translated warning statements.
- *Release Notes for the Cisco Catalyst Blade Switch 3030, Cisco IOS Release 12.2(25)SEE* (not orderable but available on Cisco.com)
- *Cisco Catalyst Blade Switch 3030 Software Configuration Guide* (order number DOC-7817261=). This guide provides a product overview and detailed descriptions and procedures of the switch software features.
- *Cisco Catalyst Blade Switch 3030 Command Reference* (order number DOC-7817262=). This reference provides detailed descriptions of the Cisco IOS commands specifically created or modified for the switch.
- *Cisco Catalyst Blade Switch 3030 System Message Guide* (order number DOC-7817263=). This guide provides descriptions of the system messages specifically created or modified for the switch.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupports

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

http://www.cisco.com/go/iqmagazine

or view the digital edition at this URL:

http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

Hardware Warranty Terms

This section describes the warranty terms for the switch.

Dell Hardware Warranty Terms

Note Important Note about Your Warranty: The limited warranty below reflects the extent of the Cisco warranty for the Cisco Catalyst Blade Switch 3030. If you purchased this product from Dell, Dell might provide an additional warranty that is different than the limited warranty terms below. See the Product Information Guide included with your Dell branded server product for the applicable warranty information. This additional warranty is provided by Dell and not by Cisco; please see your authorized Dell representative for any questions or claims related to this warranty. Cisco disclaims any warranty other than as specifically provided below.

Cisco 90-Day Limited Hardware Warranty Terms

There are special terms applicable to your hardware warranty and various services that you can use during the warranty period. Your formal Warranty Statement, including the warranties and license agreements applicable to Cisco software, is available on Cisco.com. Follow these steps to access and download the *Cisco Information Packet* and your warranty and license agreements from Cisco.com.

1. Launch your browser, and go to this URL:

   http://www.cisco.com/univercd/cc/td/doc/es_inpck/cetrans.htm

   The Warranties and License Agreements page appears.

2. To read the *Cisco Information Packet*, follow these steps:

   a. Click the **Information Packet Number** field, and make sure that the part number 78-5235-03A0 is highlighted.

   b. Select the language in which you would like to read the document.

   c. Click **Go**.

   The Cisco Limited Warranty and Software License page from the Information Packet appears.

d. Read the document online, or click the **PDF** icon to download and print the document in Adobe Portable Document Format (PDF).

Note You must have Adobe Acrobat Reader to view and print PDF files. You can download the reader from Adobe's website:

http://www.adobe.com

3. To read translated and localized warranty information about your product, follow these steps:

   a. Enter this part number in the Warranty Document Number field:

      78-5236-01C0

   b. Select the language in which you would like to read the document.

   c. Click **Go**.

      The Cisco warranty page appears.

   d. Review the document online, or click the **PDF** icon to download and print the document in Adobe Portable Document Format (PDF).

You can also contact the Cisco service and support website for assistance:

http://www.cisco.com/public/Support_root.shtml

Duration of Hardware Warranty

Ninety (90) days.

Replacement, Repair, or Refund Policy for Hardware

Cisco or its service center will use commercially reasonable efforts to ship a replacement part within ten (10) working days after receipt of a Return Materials Authorization (RMA) request. Actual delivery times can vary, depending on the customer location.

Cisco reserves the right to refund the purchase price as its exclusive warranty remedy.

To Receive a Return Materials Authorization (RMA) Number

Contact the company from whom you purchased the product. If you purchased the product directly from Cisco, contact your Cisco Sales and Service Representative.

Complete the information below, and keep it for reference:

Company product purchased from	
Company telephone number	
Product model number	
Product serial number	
Maintenance contract number	