

Installation and Startup

This chapter provides information you need to unpack, install, and set up your Micro Switch.



Timesaver You can also use the *Cisco 1548M Micro Switch 10/100 Cabling and Start Up* guide that came with your switch for quick instructions on how to install and configure your Micro Switch.

Safety Information

To ensure personal safety and protect the equipment, follow these guidelines:

- Read the safety information in Appendix C, “Translated Safety Warnings.”
- Keep the chassis area clear and dust-free during and after installation.
- Keep tools and chassis components away from walk areas.
- Do not wear loose clothing that could get caught in the chassis.
- Wear safety glasses when working under hazardous conditions.
- Do not perform any action that creates a hazard or makes the equipment unsafe.



Warning Read the installation instructions before you connect the system to its power source.

Safety Information



Warning Before working on equipment that is connected to power lines, remove jewelry (including rings, necklaces, and watches). Metal objects heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals.



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



Warning The device is designed to work with TN power systems.



Warning Do not work on the system or connect or disconnect cables during periods of lightening activity.



Warning The ports labeled “1X” through “8X,” and “console” are safety extra-low voltage (SELV) circuits. SELV circuits should only be connected to other SELV circuits. Avoid connecting these circuits to telephone network voltage (TNV) circuits.



Caution Do not place anything on top of the switch that could block the air flow from the vents on top of the switch. Products designed specifically to interoperate with the switch and stacked on top of the switch with the included stacking clip will not block the air flow from the vents.

EMC Regulatory Statements

U.S.A. FCC B Declaration of Conformity

Responsible party:

Manager, Corporate compliance
Cisco Systems Inc.
170 West Tasman Drive
San Jose, CA 95134
USA
(408) 526-4000

The following product:

Cisco 1548M Micro Switch 10/100 has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules.

The FCC B warning statement for this product is in the front matter of this manual.

Taiwan

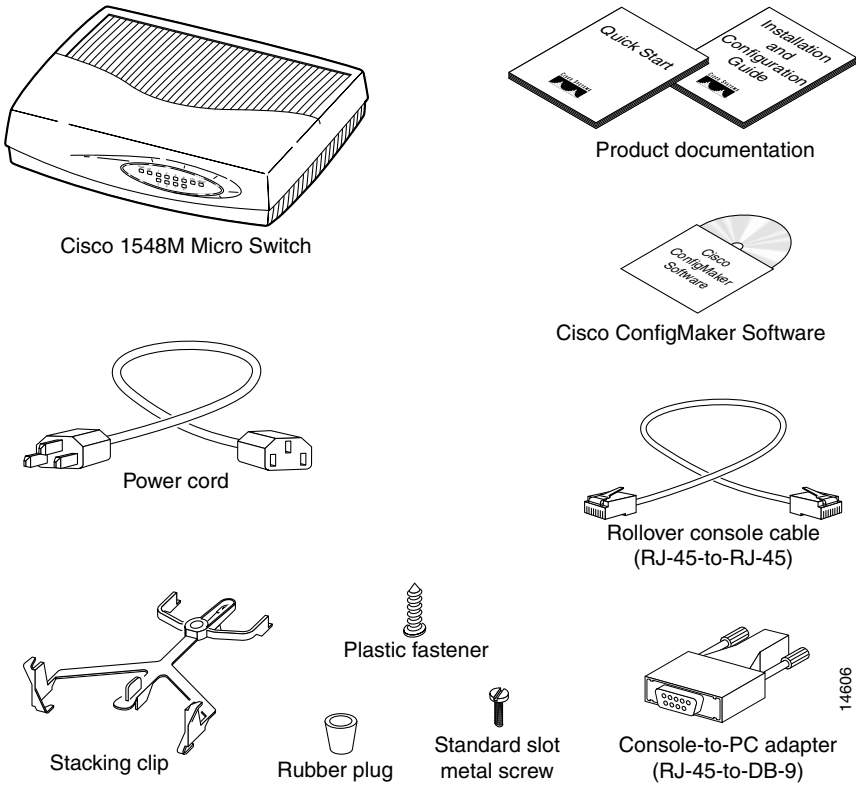
警告使用者：

這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Unpacking Your Switch

Make sure that you receive all the items shown in Figure 2-1. If any items are missing or damaged, contact your Cisco reseller.

Figure 2-1 Micro Switch Box Contents



Preinstallation

Before you begin installing the switch:

- Assemble the network devices you intend to connect to the switch. These devices must support either 10BaseT or 100BaseTX. For example, the Cisco 1538 series Micro Hub or any of the Cisco 1700 series routers are compatible devices.
- Select your cabling:
 - To connect a compatible router, server, PC, or workstation, you must provide straight-through Ethernet cables.

For information on cabling the switch to a compatible network device, see “Connecting Network Devices to the Micro Switch” section on page 2-12.
 - To connect a 10- or 100-Mbps hub without an MDI/MDI-X button, provide one 100BaseTX crossover Ethernet cable for each hub. To connect a compatible hub that has an MDI/MDI-X button, such as a Cisco 1538 series Micro Hub, provide a 100BaseTX straight-through Ethernet cable.
 - To connect a compatible switch such as another Micro Switch, provide one 100BaseTX crossover Ethernet cable for each switch you plan to connect.

Note If you plan to connect a PC or workstation that runs at 100 Mbps, make sure it has a 100 Mbps-capable network interface card (NIC) installed.

Installing the Switch

These are the major steps for installing your Micro Switch:

- Verify that the switch is operational by running the power-on self-test (POST).



Timesaver If you are installing more than one Micro Switch, complete the next step. If you are installing only one switch, go directly to “Connecting the Power Cord” on page 2-11.

- Install the switches in a stack configuration.
- Connect power to the switch.
- Connect other network devices to the switch.



Timesaver If you plan to use the Micro Switch management features, complete the next two steps. If you do not plan to manage your switch, skip these steps.

- Connect the console port of the Micro Switch to a terminal or PC to monitor and configure the switch.
- Access the Micro Switch management interface.

Using POST to Pretest the Switch Operation

Before installing and cabling the switch, you might want to power up the switch and verify that it is operational.

To power up the switch, connect one end of the AC power cord to the AC power connector on the switch and the other end of the cord to a power outlet (see Figure 2-5).

The switch begins the POST after power up. POST consists of the eight individual tests in Table 4-1. The port LEDs show which test the switch is executing. As each test executes, a port LED turns green. For example, if the LED for port 4 is green, the boot code test (test 1) is being executed. On the switch, the port LED for port 4 turns green first, followed by ports 3, 2, 1, 8, 7, and so on. The LED turns off after the test completes. The POWER LED is solid amber until POST completes.

When POST completes, the following conditions can exist (if other devices are not connected to the switch):

- All POST tests passed—If the POWER LED is green and all of the port LEDs are off, no problems were detected. The switch is fully operational.

Note After POST completes (and if there are devices connected to the switch ports), Spanning-Tree Protocol (if enabled) immediately turns the port LEDs green. The forwarding state is delayed to allow the Spanning-Tree Protocol to discover the network topology and to ensure no temporary loops are formed. Spanning-tree discovery takes approximately 30 seconds to complete, and no packet forwarding takes place during this time.

- Nonfatal failure(s) detected—If the POWER LED is amber and the switch is functional, POST detected one or more nonfatal failures. Although the switch is still operational and can forward packets, it might not operate optimally. Refer to the POST failure message displayed on the diagnostic console screen, identifying the nonfatal failure(s) detected (See “Understanding POST Results” on page 4-3).
- Fatal failure(s) detected—POST stops when it encounters a fatal failure. If the POWER LED is amber and a port LED is blinking green, POST detected a fatal failure. The switch is not operational, but the blinking port LED indicates which test failed.

You should inform your system administrator if one or more nonfatal failures are detected. Contact your Cisco representative or reseller for support if any fatal failures are detected.

The “Understanding POST Results” section on page 4-4 provides additional information, including the possible causes of nonfatal and fatal failures.

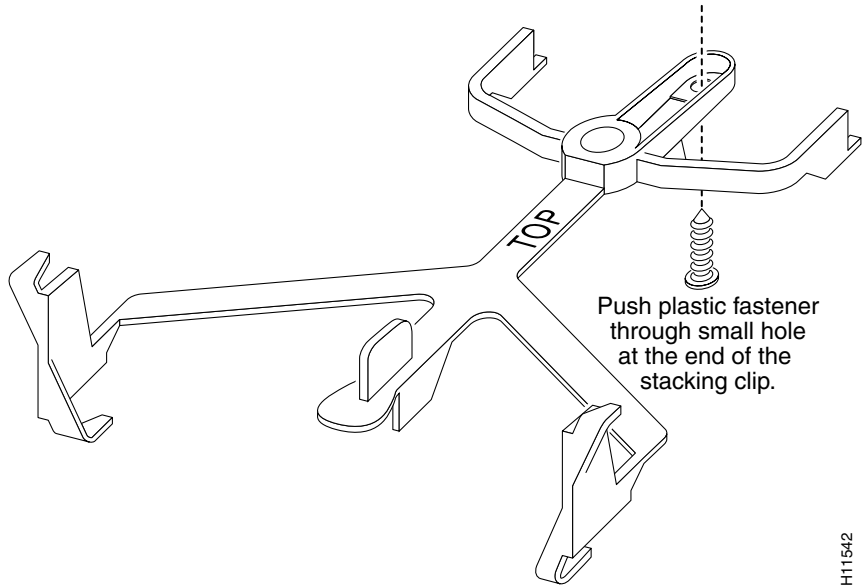
Installing the Switch in a Stack

Each switch comes with a stacking clip and a screw that are used to keep multiple devices together in a stack. Before using the clip, you must assemble the clip and the screw, as shown in Figure 2-2.



Timesaver If you are using only one switch and no other Cisco Networked Office devices, skip this step, and go to the “Connecting the Power Cord” section.

Figure 2-2 Assembling the Stacking Clip and Fastener



After pushing the fastener into the stacking clip, use the clip as shown in Figure 2-3.

Adding or Removing a Switch from a Stack

Figure 2-3 shows how to stack a Micro Switch with other Cisco Networked Office devices, and Figure 2-4 shows how to remove devices from the stack.



Warning Unplug the power cord before you work on a system that does not have an on/off switch.

Figure 2-3 Mounting Cisco Networked Office Switches

Step 1

Place the clip on top of the lower switch. Slide the clip forward so that the front tabs slide into the vent slots.

Step 2

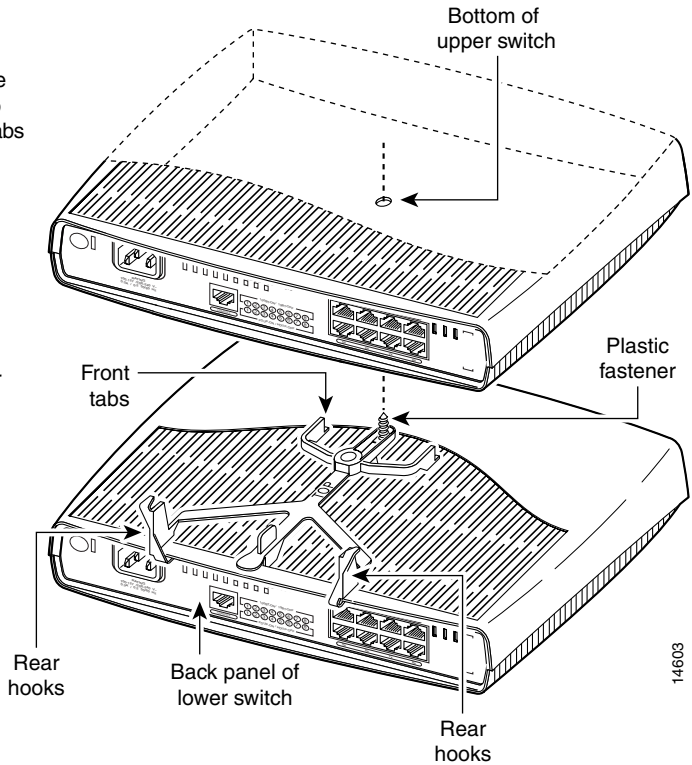
Make sure the rear hooks fit over the edge of the lower switch.

Step 3

Position the upper switch on the clip so that the rear hooks fit over the edge of the upper switch.

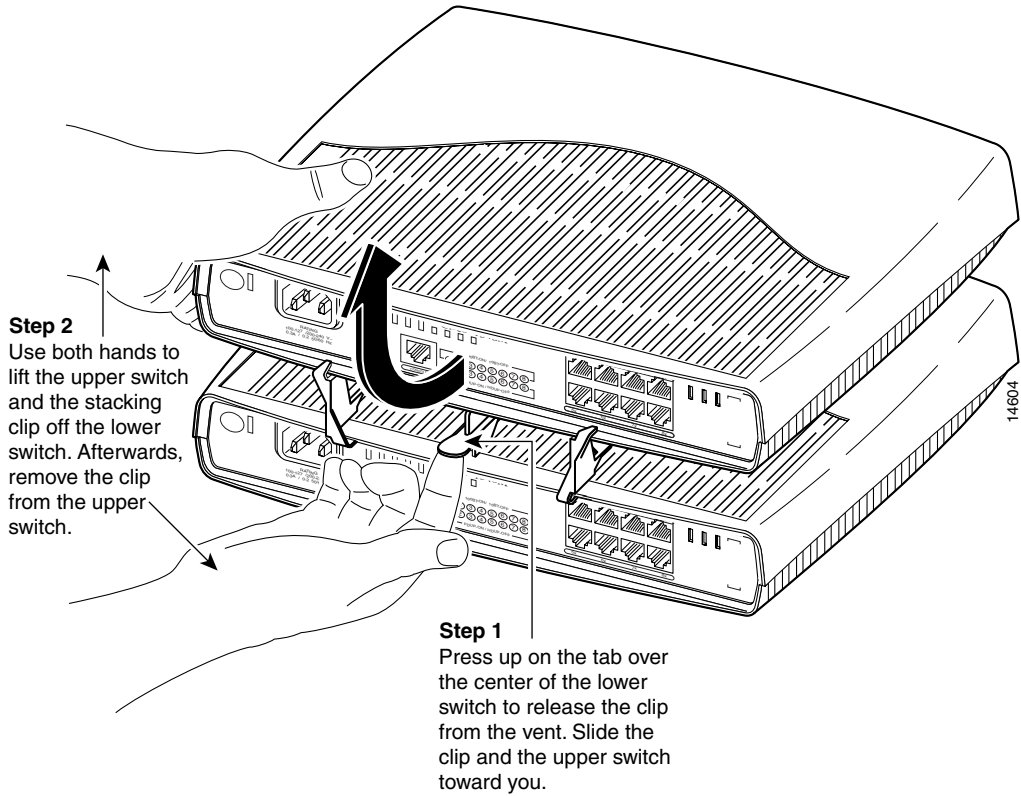
Step 4

Press down to snap the upper switch on the clip. Make sure the plastic fastener fits into the bottom of the upper switch.



14603

Figure 2-4 Removing a Device from the Stack



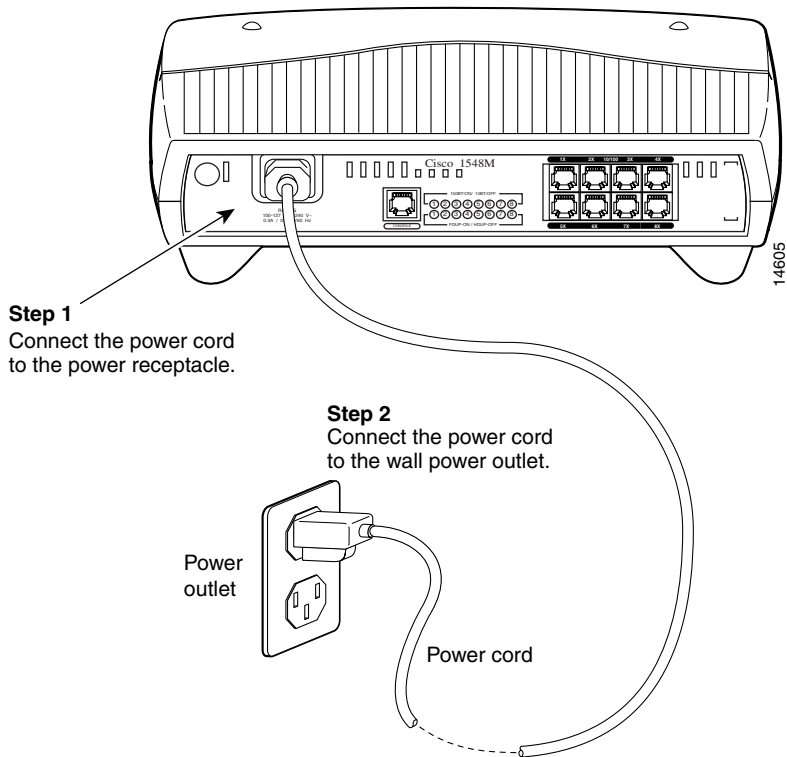
Connecting the Power Cord

Connect power and turn on the switch as shown in Figure 2-5.



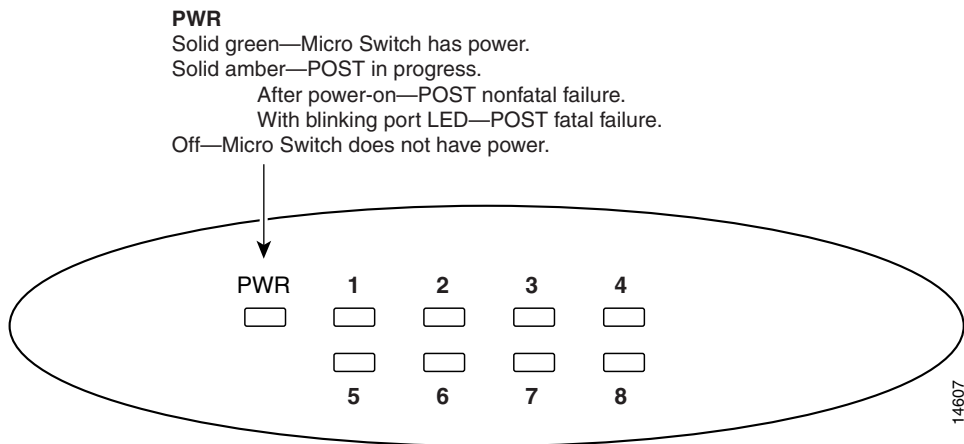
Warning This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15A U.S. (240 VAC, 10A international) is used on all current-carrying conductors.

Figure 2-5 Connecting the Power Cord



To verify correct operation, check the front panel to make sure that the PWR LED is on as shown in Figure 2-6.

Figure 2-6 **Checking the PWR LED**



Connecting Network Devices to the Micro Switch

You can connect the following types of compatible devices to the switch ports, labeled 1 through 8:

- Network devices such as a PC, workstation, router, or server
- A hub with or without a configurable MDI/MDI-X port
- Another switch

A compatible network device supports either 10BaseT or 100BaseTX. You can connect any combination of 10BaseT and 100BaseTX devices to the switch. Table 2-1 lists these devices that you can connect to the switch and summarizes the cable types needed.

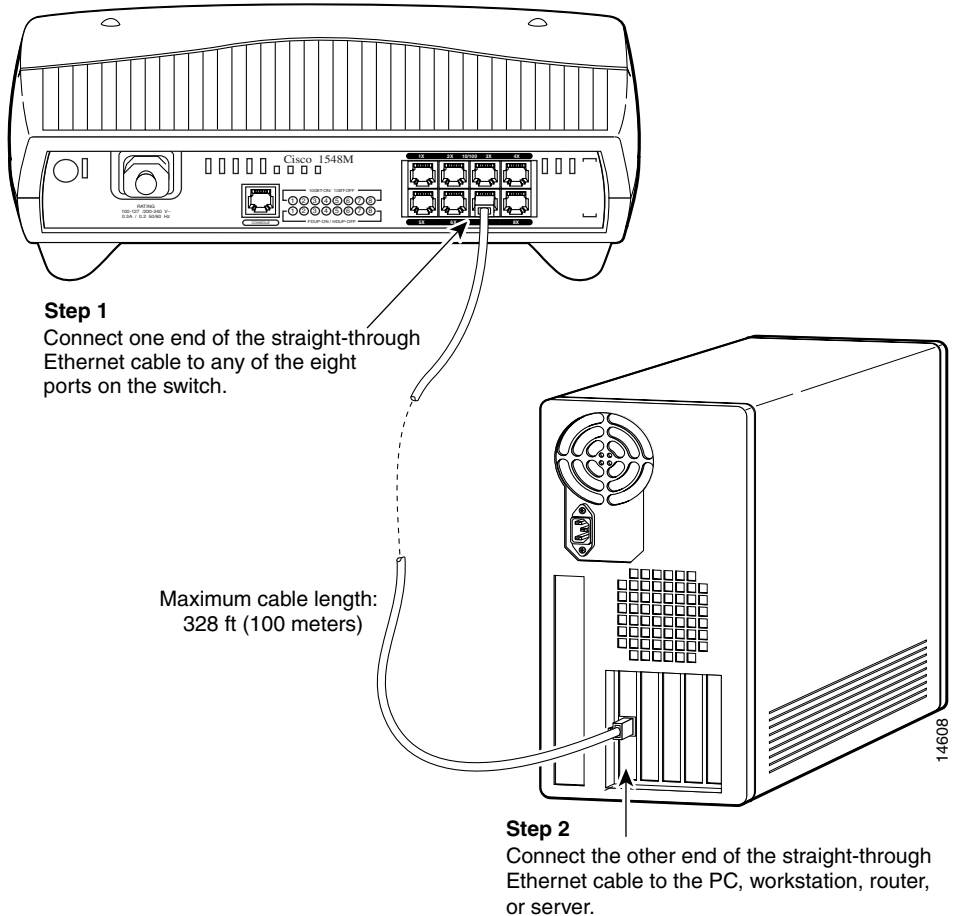
Table 2-1 Connecting Compatible Network Devices to the Switch

Network Device	Connecting Ports	Ethernet Cable Type
PC, workstation, router, or server	Ports 1 through 8	Straight-through
Hub without an MDI port option	Ports 1 through 8	Crossover
Hub with an MDI option such as the Cisco 1538M Micro Hub 10/100 or FastHub 400 10/100 series	Standard MDI-X ports	Crossover
	Port associated with MDI option on hub	Straight-through
Switch such as another Micro Switch	Ports 1 through 8	Crossover

Connecting a PC, Workstation, Router, or Server

Connect a PC, workstation, router, or server to the switch ports as shown in Figure 2-7.

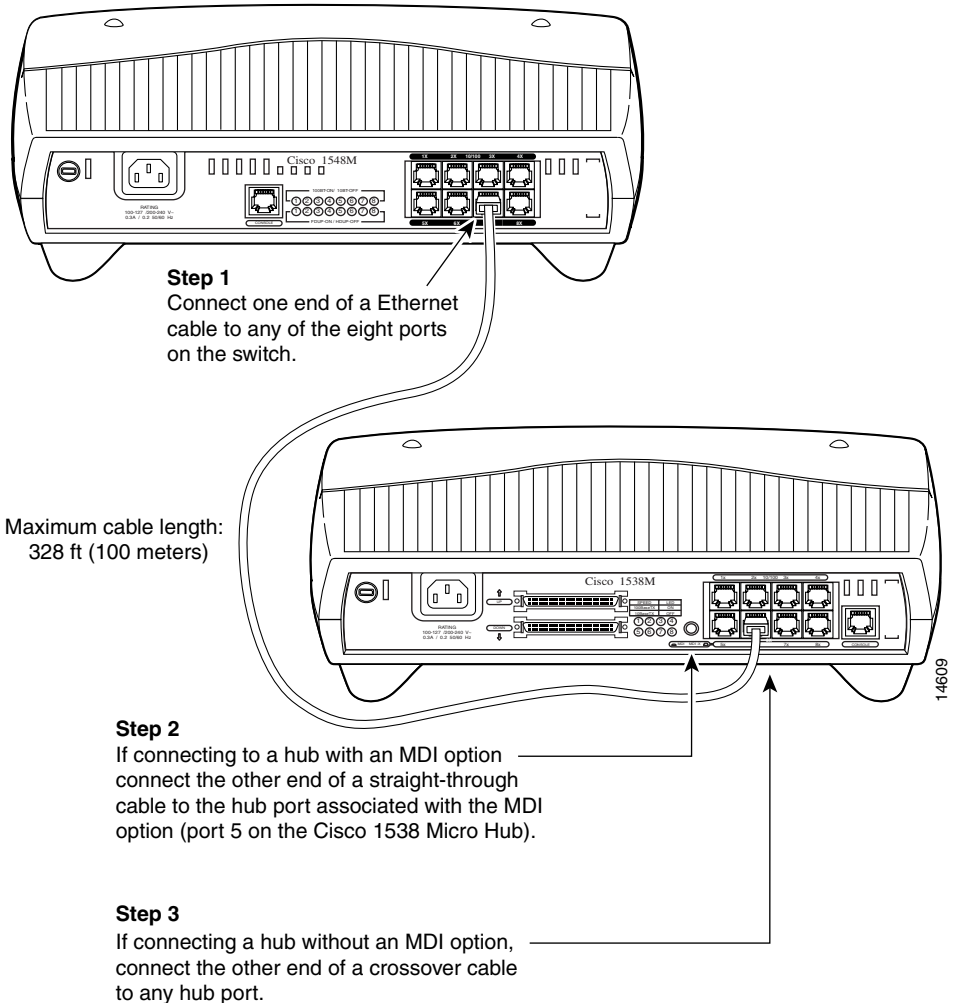
Figure 2-7 Connecting a PC, Workstation, Router, or Server



Connecting a Hub

Connect a compatible hub to the switch ports as shown in Figure 2-8.

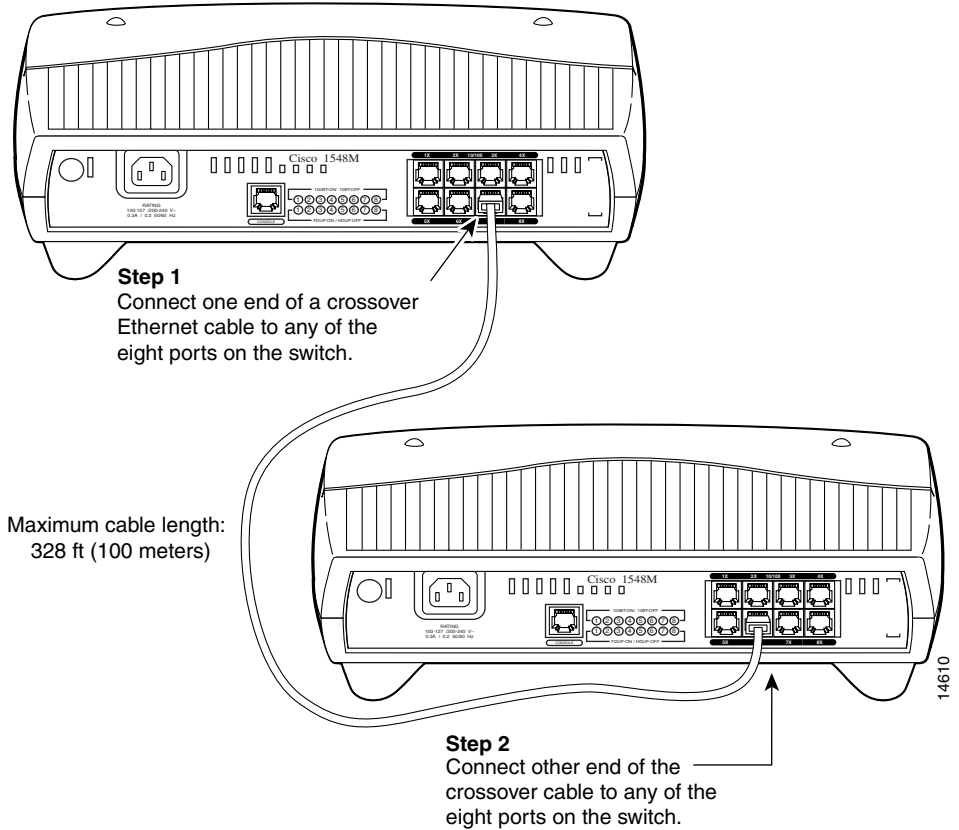
Figure 2-8 Cabling the Switch to a Compatible Hub



Connecting a Switch

Connect a compatible switch to the switch ports as shown in Figure 2-9.

Figure 2-9 Connecting the Micro Switch to a Compatible Switch



Verifying That Network Devices Are Connected

After connecting network devices to the switch ports, check the corresponding port LEDs (labeled 1 through 8) on the front and back panels. The color and blinking pattern of the LEDs indicate the activity for the corresponding switch port as shown in Figure 2-10 and Figure 2-11.

Figure 2-10 **Checking the Port LEDs**

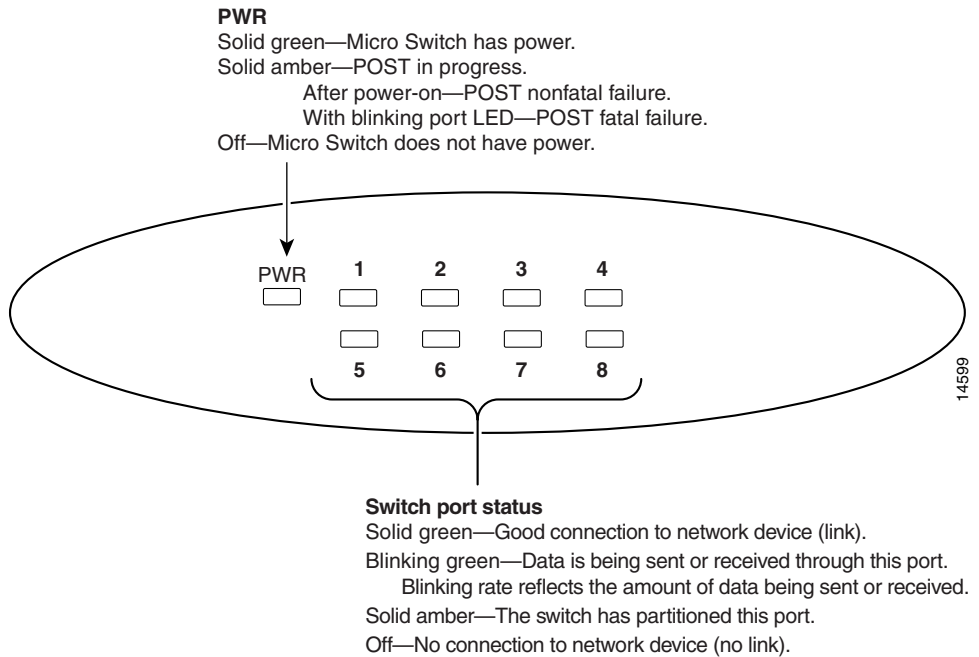
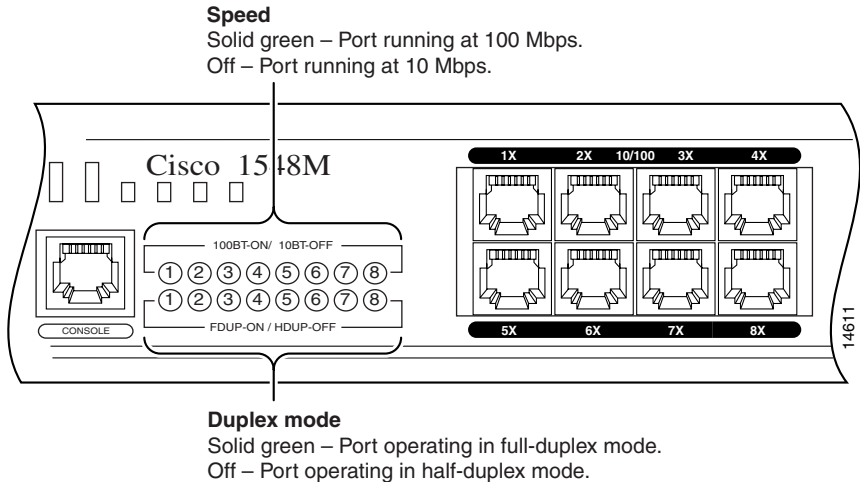


Figure 2-11 Verifying Running Speed Between Connected Ports



Connecting to the Console Port

To connect the RJ-45 console port of the Micro Switch to a management station or modem, you must use the supplied RJ-45-to-RJ-45 rollover console cable and the appropriate adapter and follow these steps.

Note The rollover console cable and a RJ-45-to-DB-9 female DTE adapter are supplied with the switch. If your management station requires a different adapter—such as a RJ-45-to-DB-25 female DTE or RJ-45-to-DB-25 male DCE adapter—you must provide it.

Step 1 Configure the switch console port settings to match the management station or modem. These are the default settings of the console port:

- 9600 baud
- 8 data bits
- 1 stop bit
- No parity
- No flow control

You can change the console port characteristics of the switch from the web-based System Configuration Page (see the “Changing the System Configuration” section on page 3-29) or by using the **terminal** command from the command-line interface (CLI).

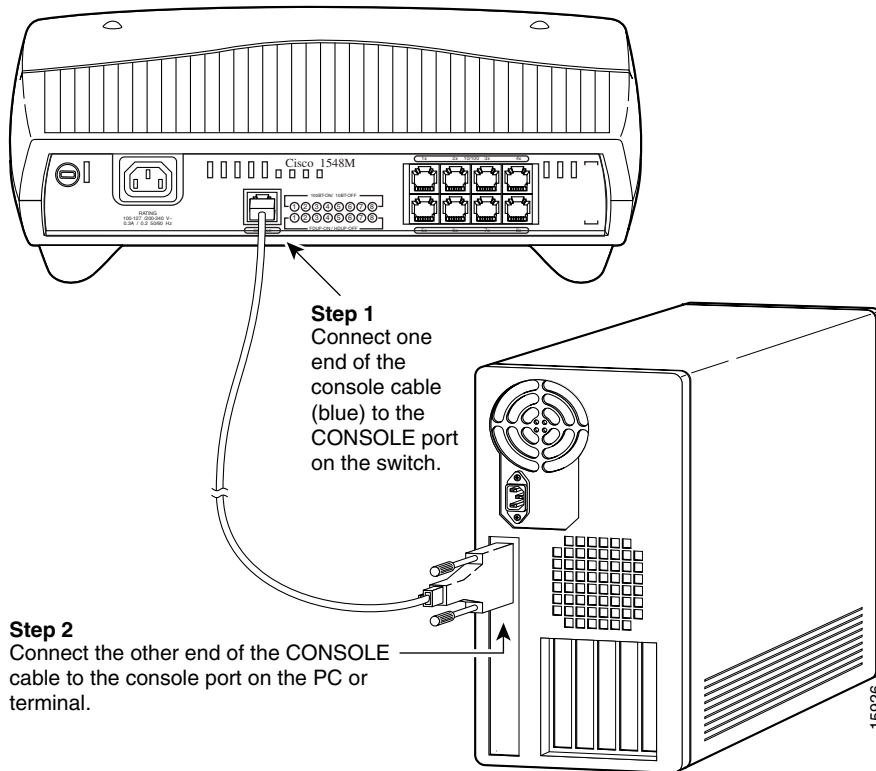
Note Make sure the settings of the console port and the management station or the modem match.

Step 2 Connect one end of the supplied rollover console cable to the console port, as shown in Figure 2-12.



Caution Do not connect an actual telephone line, an ISDN line, or an Ethernet cable to this console port. Damage to the switch can result. Make sure you use the supplied RJ-45-to-RJ-45 rollover cable and adapters to connect the console port to the management station or modem.

Figure 2-12 Connecting to the Console Port



Step 3 Attach the appropriate adapter, such as the supplied RJ-45-to-DB-9 female DTE adapter (labeled Terminal), to a management station or modem.

Note If you are connecting the switch to a Sun workstation (or to a management station with a female DB-25 serial connector), use a male-to-male gender changer to attach the supplied RJ-45-to-RJ-45 console cable and a RJ-45-to-DB-25 female DTE adapter to the management station.

Step 4 Connect the other end of the supplied console cable to the adapter.

Now that the switch is connected to a management station, you can now assign IP information to the switch (see “Assigning IP Information to the Switch” section on page 2-21).

Connector and cabling specifications for the console port are in the “Specifications for the Micro Switch” appendix.

Assigning IP Information to the Switch

After you install the switch and connect it to a management station, you can assign IP information to the switch. IP information identifies the switch to the network and is necessary to configure and monitor the switch through the Cisco 1548 Switch Manager, the CLI, or SNMP.

You can assign IP information to the switch by either:

- Following the switch start-up prompts displayed from a terminal emulation program on your management station. This section provides information on using these start-up prompts.

or

- Using Cisco ConfigMaker if your management station is a PC running Microsoft Windows 95, Windows 98, or Windows NT 4.0. For information about Cisco ConfigMaker, refer to the Cisco ConfigMaker software.

You should contact your system administrator for the following information:

- Switch IP address
- Subnet mask (netmask)
- Default gateway (router)

To assign IP information to the switch, follow these steps:

Step 1 From your management station, start the terminal emulation program.

Assigning IP Information to the Switch

After POST completes, the Continue with configuration dialog? prompt appears on the management station, and you can then follow the prompts to assign IP information to the switch. If the Continue with configuration dialog? prompt does not appear, see the “Troubleshooting” chapter.

Note After POST completes (and if there are devices connected to the switch ports), Spanning-Tree Protocol (if enabled) immediately turns the port LEDs green. The forwarding state is delayed to allow the Spanning-Tree Protocol to discover the network topology and to ensure no temporary loops are formed. Spanning-tree discovery takes approximately 30 seconds to complete, and no packet forwarding takes place during this time.

Step 2 From the terminal or PC, enter **Y**:

```
Continue with configuration dialog? [yes/no]: Y
```

Step 3 Enter the IP address (for example: 10.1.105.20):

```
Enter IP address: 10.1.105.20
```

Step 4 Enter the subnet mask (IP netmask) (for example: 255.255.255.0):

```
Enter IP netmask: 255.255.255.0
```

Step 5 Enter the IP address of the default gateway (for example: 10.1.105.254):

```
Enter IP default gateway: 10.1.105.254
```

Note If the management station from which the Cisco 1548 Switch Manager is used is not on the same IP subnet as the switch, you must also assign a default gateway (the router for the local subnet).

The following information is displayed:

```
The following configuration command script was created:
ip address 10.1.105.20 255.255.255.0
ip default-gateway 10.1.105.254
!
end
```

Step 6 Enter **Y**:

```
Use this configuration? [yes/no]: Y
```

The following information is displayed:

```
Building configuration...
Use the enabled mode 'configuration' command to modify this
configuration.
```

```
Press RETURN to get started.
```

Pressing **Return** opens a CLI session

Step 7 Exit from the terminal session.

Accessing the Management Interfaces

After you assign IP information to the switch, you can access the switch management interfaces. This section provides information for accessing the Cisco 1548 Switch Manager, the CLI, and SNMP and MIB files.

Accessing the Cisco 1548 Switch Manager

To access the switch manager, all you need is the IP information of the switch (and the password if one has been assigned). IP information for the switch is usually assigned when the switch is first started up after installation. (See the “Assigning IP Information to the Switch” section on page 2-21.)

Note You can access the switch manager from a PC connected to one of the 10/100 network ports. Therefore, make sure that you do not disable or otherwise misconfigure the port through which *you* are communicating with the switch. You might want to write down the port number you are connected to. Make changes to the switch IP information with care.

To access the switch manager, follow these steps:

- Step 1** Start Netscape Communicator (4.03 or higher) or Microsoft Internet Explorer (4.01 or higher).
- Step 2** Ensure that the following browser features are enabled:
- Java
 - JavaScript
 - Set the caching of pages to **Every time** in Communicator or **Every visit to the page** in Internet Explorer.
- Step 3** Enter the IP address of the switch in the Location field if you are using Communicator (the Address field if you are using Internet Explorer) to display the switch manager Home Page (Figure 2-13).

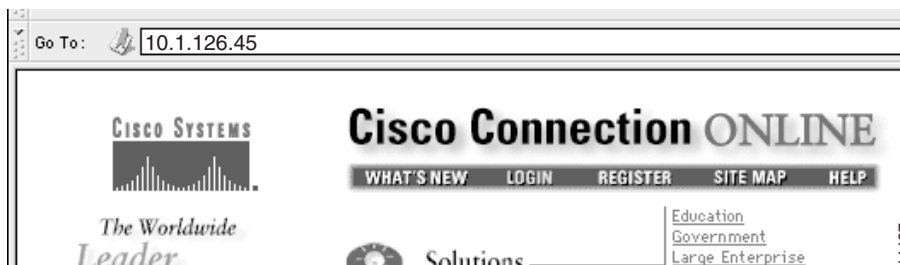


Figure 2-13 Home Page

Click Apply after making changes on a page.

Click Revert to discard unapplied changes on a page.

Click Help for procedures and detailed field descriptions.

Click these topics to move from page to page. On Netscape Communicator only, when the cursor is above a topic, a pop-up briefly describes the options on that particular page.

Click a port to display its settings, status, and statistics.

15531

Note You can bookmark the switch IP address to retrieve the switch manager for later use. If you are using Communicator, choose the **Communicator** menu option, and select **Bookmarks > Add Bookmark**. If you are using Internet Explorer, choose the **Favorites** menu option, and select **Add to Favorites**. Do not use the right mouse button to bookmark the switch IP address; doing so only saves the specific frame (image) of the switch manager page.

Accessing the CLI

You can access the CLI

- From a console terminal connected to the switch console port. For more information, see the “Connecting to the Console Port” section on page 2-18.
- Through a Telnet session from a remote host by entering the **telnet** command and the name or IP address of the switch.
- Through a Telnet session by clicking **Telnet** on the switch manager Home Page.

When you access the CLI and a password has been defined, the following prompt is displayed:

```
Cisco Systems Console
Enter Password:
```

Enter the password. The `hostname>` prompt is displayed after you enter the correct password.

For complete information about the CLI, refer to the *Cisco 1548M Micro Switch 10/100 Command Reference*.

Accessing the MIB Files through SNMP

You can access the switch MIB files through SNMP. The following MIB files contain variables that can be set or read to provide information about the switch and the traps generated by the switch.

- RFC1213-MIB.my contains the MIB II (RFC 1213).
- ETHERLIKE-MIB.my contains the Ethernet Transmission MIB (RFC 1643).
- BRIDGE-MIB.my contains the Bridge MIB (RFC 1493).
- CISCO-CDP-MIB-.my contains the CDP MIB.
- RMON-MIB.my contains the RFC 1757 RMON (Groups 1, 2, 3, and 9). More information about RMON and the RMON groups is provided in the “Remote Monitoring” section on page 2-28.
- CISCO-SIBU-SIMPLE-UPGRADE-MIB.my contains the MIB module for upgrading the firmware on Cisco low-end devices.

- CISCO-SIBU-MANAGERS-MIB.my contains the MIB module for management interfaces on the Micro Switch.
- CISCO-CNO-SWITCH-MIB.my contains the MIB module is for the management of Cisco Network Office (CNO) switch products.

If you are going to manage the switch by using SNMP and the MIB files, the Read and Write community strings need to be set. To do this, you can either

- Use the default community strings
 - Read community string. The default is public.
 - Write community string. The default is private.
- Assign community strings by using the SNMP Management Page or by using the **snmp-server community** command

Note Wait approximately 30 seconds for the changes to be saved to permanent storage before turning off the switch, or the changes might not be saved.

You can obtain a copy of the MIB files in the following ways:

- Using File Transfer Protocol (FTP) to access the ftp.cisco.com server.
- Using Cisco Connection Online (CCO) to access the cisco.com server.

Using FTP to Access the MIB Files

To obtain a MIB file, follow these steps:

- Step 1** Use FTP to access the server ftp.cisco.com.
- Step 2** Log in with the username anonymous.
- Step 3** Enter your e-mail name when prompted for the password.
- Step 4** At the ftp> prompt, change directories to /pub/MIBs.
- Step 5** Use the **get README** command to display the readme file listing available files.
- Step 6** Use the **get MIB_filename** command to get a copy of the MIB file.

Using CCO to Access the MIB Files

To access the MIB files from CCO, click **Software & Support** to display the Software Center site.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: <http://www.cisco.com>
- WWW: <http://www-europe.cisco.com>
- WWW: <http://www-china.cisco.com>
- Telnet: cco.cisco.com
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; data bits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

Remote Monitoring

The Remote Monitoring (RMON) MIB is used by network managers to monitor remote devices. An RMON implementation consists of a software probe that continually collects statistics about a LAN and a management station that communicates with the probe. The probe transfers information to the management station on request or when a predefined threshold is crossed.

The switch supports four RMON groups (Table 2-2) as defined in RFC 1757. Default statistic rows are created for each port when you start the switch. You can obtain information about the four supported groups by using any SNMP management application.

Table 2-2 **RMON Groups and Their Functions**

Group Name	Description
Statistics	<p>This group collects traffic and error statistics for a specific interface. For example, you could use this group to determine how many error packets have been seen on a given port.</p> <p>Statistics from this group can be used by the history group to record historical views of network performance. A statistics row is established by default for each switch port.</p>
History	<p>This group periodically samples the counters generated by the statistics group. This information can be used to establish baseline information regarding network activity. You can define the intervals you want to record information for, and you can define how many of the samples are to be stored.</p> <p>Note RMON statistics gathering has a maximum limit of 50 history buckets per historyControlTable entry.</p>
Alarm	<p>This group generates alarms according to user-defined thresholds. You could, for example, configure RMON to generate an alarm when alignment errors on a port exceeded a predefined limit. Rising and falling thresholds can be defined, and the events group can generate traps and automated responses based on the alarms.</p>
Event	<p>This group sends traps to the management station based on information (alarms) received from the alarm group.</p>

Where to Go Next

Now that you have installed and assigned IP information to the switch, continue to Chapter 3, “Configuring and Monitoring from the Hub Manager,” for configuration and monitoring information.

