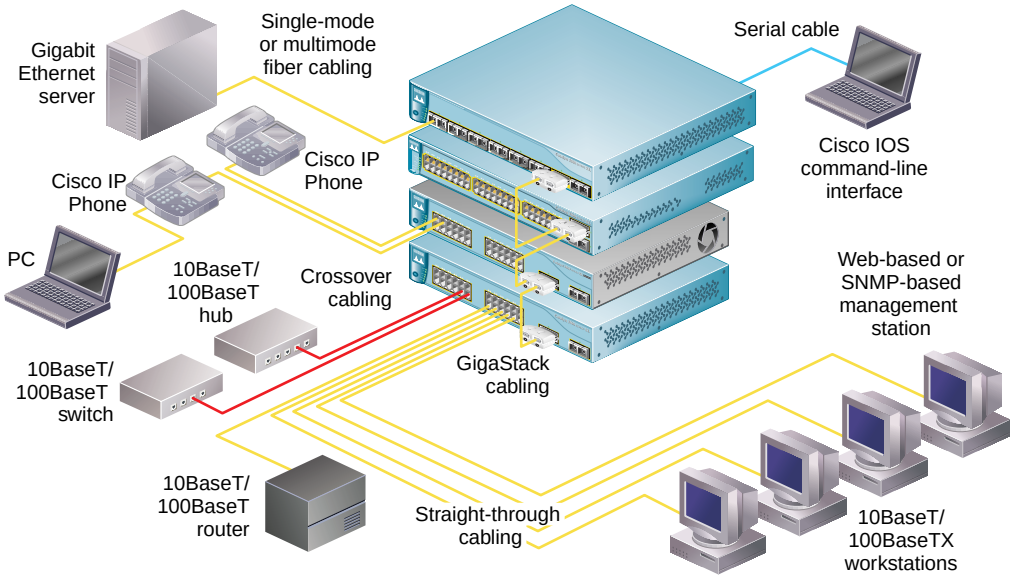
Quick Start Guide

CATALYST 3500 SERIES XL SWITCHES



1

TAKE OUT WHAT YOU NEED

2

CABLE THE SWITCH

3

ASSIGN SWITCH INFORMATION

4

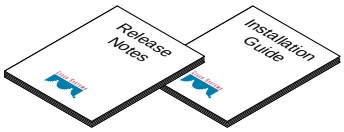
ACCESS THE SWITCH FROM YOUR BROWSER

CISCO SYSTEMS

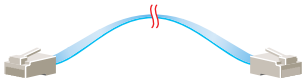
1 Take Out What You Need

Catalyst 3500 series XL switch

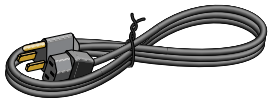
Hardware installation guide and release notes



RJ-45-to-RJ-45 rollover console cable



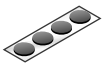
AC power cable



RJ-45-to-DB-9 serial adapter

Rack-mount kit

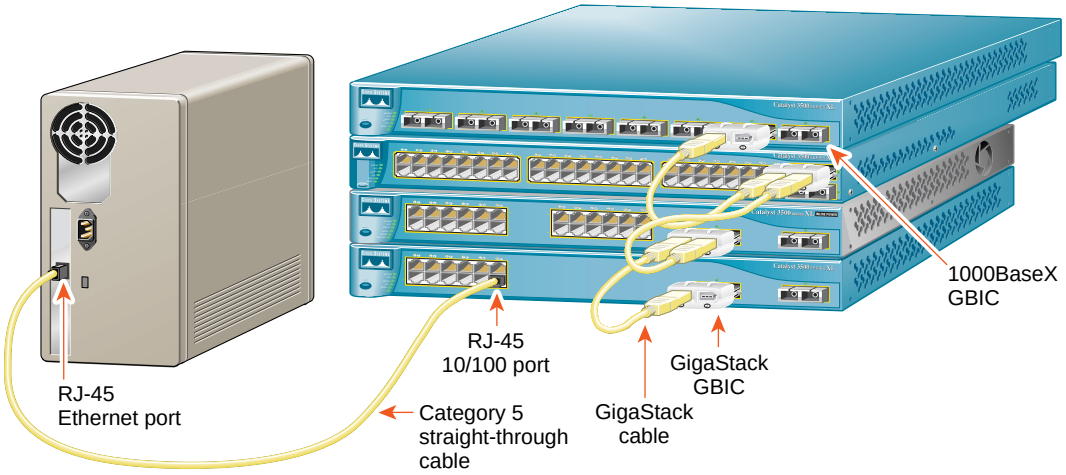
Rubber feet



Note If any item is missing or damaged, contact your Cisco representative or reseller for support.

Note You need to provide the Category 5 straight-through and crossover cables to connect the switch ports to other Ethernet devices. In addition, the supplied RJ-45-to-DB-9 serial adapter is for connecting the switch console port to a PC. You need to provide a RJ-45-to-DB-25 female DTE adapter if you want to connect the switch console port to a terminal. You can order a kit (part number ACS-DSBUASYN=) containing that adapter from Cisco.

2 Cable the Switch



Connect to Workstations, PCs, Servers, and Routers

1. Connect a Category 5 **straight-through** cable (not supplied) to a 10/100 port on the front panel of the switch.
2. Connect the other end of the cable to the RJ-45 port of the workstation, PC, server, or router.

Connect to Hubs and Other Switches

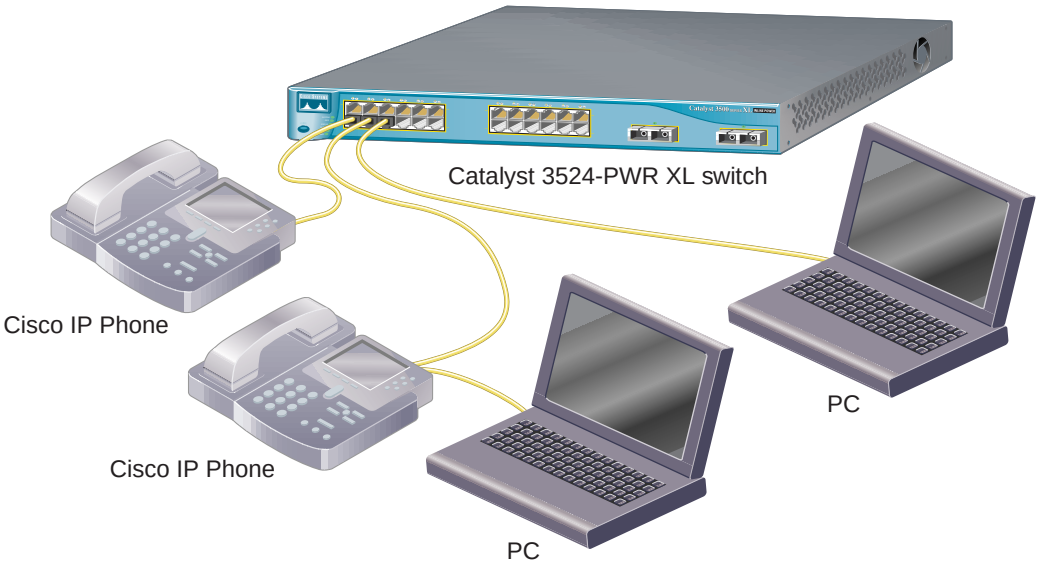
1. Connect a Category 5 **crossover** cable (not supplied) to a 10/100 port on the front panel of the switch.
2. Connect the other end of the cable to an RJ-45 port on the target switch or hub.

Note Use a straight-through cable to connect two ports when one of the port numbers is designated with an **X**. Use a crossover cable to connect two ports when both port numbers are designated with an **X** or when both ports do not have an **X**.

Connect through the GigaStack GBICs (Optional)

1. Insert GigaStack Gigabit Interface Convertors (GBICs) in the GBIC module slots on the switches.
2. Connect the GigaStack GBICs with the Cisco GigaStack cables.

Note The GigaStack GBICs are orderable separately. Refer to the *Catalyst GigaStack Gigabit Interface Convertor Installation Guide* for details on installing and cabling the GigaStack GBICs.

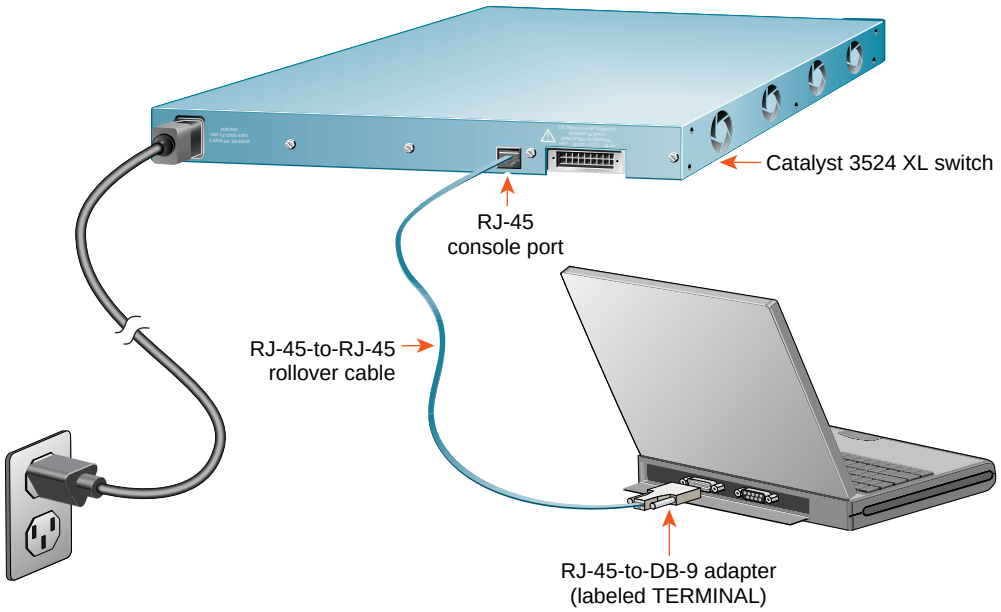


Connect to Cisco IP Phones

The Catalyst 3524-PWR XL 10/100 ports also can provide inline power to Cisco IP Phones.

1. Connect a Category 5 **straight-through** cable (not supplied) to a 10/100 port on the front panel of the switch.
2. Connect the other end of the cable to the LAN-to-phone jack on the Cisco IP Phone.

Note The rear panel of the Cisco IP Phone might have more than one RJ-45 jack. Use the LAN-to-phone jack to connect the phone to the Catalyst 3524-PWR XL switch. Refer to the documentation that came with your Cisco IP Phone for information about connecting devices to it.



Connect to a Power Source

1. Connect one end of the supplied AC power cord to the power connector on the switch rear panel.
2. Connect the other end of the power cable to a grounded AC outlet.

Note If you are connecting the switch to a Cisco Redundant Power System (RPS), refer to the documentation that shipped with your RPS. Specific Cisco RPS models support specific Catalyst 3500 XL switches:

- Cisco RPS 600 (model PWR600-AC-RPS) supports the Catalyst 3512, 3524, 3548, and 3508 XL switches.
- Cisco RPS 300 (model PWR300-AC-RPS) supports the Catalyst 3524-PWR XL switch.

Connect to a PC or Terminal

1. Connect the blue rollover cable to the port marked CONSOLE on the rear panel of the switch.
2. If necessary, attach the RJ-45-to-DB-9 adapter to the PC, or attach the appropriate adapter to a terminal. You can order a kit (part number ACS-DSBUASYN=) containing the terminal adapter from Cisco.
3. Connect the other end of the cable to the PC or terminal running terminal-emulation software, such as ProComm Plus or HyperTerminal.
4. If necessary, reconfigure the terminal-emulation software to match the console port settings (default settings are 9600 baud, no parity, 8 data bits, and 1 stop bit).

3 Assign Switch Information

The first time that you access the switch, it runs a setup program that prompts you for IP and other configuration information necessary for the switch to communicate with the local routers and the Internet. This information also is required if you plan to use the Cluster Management Suite of applications to configure and manage the switch.

Note If the switch will be a cluster member managed through the IP address of the command switch, it is not necessary to assign IP information or a password. If you are configuring the switch as a standalone switch or as a command switch, you must assign IP information. Refer to the *Cisco IOS Desktop Switching Software Configuration Guide* for more information.

IP Information Requirements

You will need the following information from your system administrator:

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

First-Time Setup

Use this procedure to create an initial configuration for the switch:

1. Enter **Y** at the prompt:

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

   If this prompt does not appear, enter enable, and press **Return**. Enter setup, and press **Return** to restart the setup program.

2. Enter the switch IP address, and press **Return**:

   ```
   Enter IP address: ip_address
   ```

3. Enter the subnet mask (IP netmask) address, and press **Return**:

   ```
   Enter IP netmask: ip_netmask
   ```

4. Enter **Y** to enter a default gateway (router):

   ```
   Would you like to enter a default
   gateway address? [yes]: y
   ```

5. Enter the IP address of the default gateway, and press **Return**:

   ```
   IP address of the default gateway:
   ip_address
   ```

6 Enter the host name for the switch, and press **Return**.

Note On a command switch, the host name is limited to 28 characters and on a member switch to 31 characters. Do not use *-n*, where *n* is a number, as the last characters in a host name for any switch.

```
Enter the host name: host_name
```

7 Enter a secret password (which ensures switch security), and press **Return**:

Note The secret password can be from 1 to 25 alphanumeric characters, can start with a number, is case-sensitive, and allows spaces but ignores leading spaces.

```
Enter enable secret:
secret_password
```

8 Enter **Y** to enter a Telnet password:

```
Would you like to configure a
Telnet password? [yes]: y
```

9 Enter the Telnet password, and press **Return**:

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

```
Enter Telnet password:
telnet_password
```

10 Enter **Y** to configure this switch as the cluster command switch. Enter **N** to configure it as a member switch or as a standalone switch.

Note If you enter **N** to configure the switch as a member switch or as a standalone switch, it appears as a candidate switch in Cluster Builder, and the Step 11 message is not displayed.

```
Would you like to enable as a
cluster command switch? y
```

11 Assign a name to the cluster, and press **Return**:

Note The cluster name can be 1 to 31 alphanumeric characters, dashes, or underscores.

```
Enter cluster name: cls_name
```

12 Verify that the addresses are correct in the initial configuration displayed:

```
The following configuration command
script was created:

ip subnet-zero
interface VLAN1
ip address ip_address ip_netmask
ip default-gateway ip_address
hostname host_name
enable secret 5
$1$M3pS$cXtAlkyR3/6Cn8/
line vty 0 15
password telnet_password
snmp community private rw
snmp community public ro
cluster enable cls_name
!
end
!
Use this configuration? [yes/no]:
```

13 If the information is correct, enter **Y** at the prompt, and press **Return** to use the displayed configuration. When you see the message "Press RETURN to get started," the setup program is complete. You can use your browser and the Cluster Management Suite or use the command-line interface (CLI) to manage the switch.

If the information is not correct, enter **N** at the prompt, press **Return**, and begin again at Step 1.

Where to Go Next

After you complete the setup program, the switch can run the created default configuration. If you want to change this configuration or want to perform other management tasks, use one of these tools:

- CLI
- Cluster Management Suite from your browser

To use the CLI, enter commands at the switch> prompt. Refer to the *Cisco IOS Desktop Switching Software Configuration Guide* or the *Cisco IOS Desktop Switching Command Reference* (online only) for configuration information.

To use the Cluster Management Suite, go to the "Access the Switch from Your Browser" section on page 8.

4 Access the Switch from Your Browser

Downloading the Required Plug-In

A Java browser plug-in is required to access the HTML interface. You can download the plug-in from Cisco Connection Online (CCO). If you have a SmartNet support contract, you can log in to the following URL and download the plug-in:

- http://www.cisco.com/cgi-bin/tablebuild.pl/cat3500XL

If you do not have a SmartNet contract, you can download the plug-in from the following URL:

- http://www.cisco.com/pcgi-bin/tablebuild.pl/cat3500XL

Follow the instructions that accompany the plug-in to install it on your computer.

Supported Operating Platforms and Network Browsers

After you have assigned an IP address to the switch and installed the plug-in, you can access the switch from your browser and use the Cluster Management Suite to view or change configuration settings. If this is a command switch, you also can use the Cluster Management application to configure other switches. To use web-based tools, follow the procedure to set the appropriate browser options.

The web-based tools support the following platforms and network browsers:

Operating System	Minimum Operating System Requirements	Netscape Communicator	Microsoft Internet Explorer
Windows 95	Service Pack 1	4.61 or 4.7	4.01a or 5.0
Windows 98	Second Edition	4.61 or 4.7	4.01a or 5.0
Windows NT	Service Pack 3	4.61 or 4.7	4.01a or 5.0
Solaris 2.5.1 or higher	SUN-recommended patch cluster for the OS and Motif library patch 103461-24	4.61 or 4.7	Not supported

Note Netscape Communicator version 4.60 is NOT supported.

The switch checks the browser version when starting a session to ensure that the browser is supported. If the browser is not supported, the switch displays a warning message.

Note Refer to the release notes for additional requirements for setting up your browser.

Configuring Netscape Communicator (All Versions)

1. From the menu bar, select **Edit>Preferences**.
2. In the Preferences window, click **Advanced**.
3. Select the **Enable Java**, the **Enable JavaScript**, and the **Enable Style Sheets** check boxes.
4. From the **Advanced** drop-down list, select **Cache**.
5. Under **Document in cache is compared to document on network**, select **Every time**.
6. Click **OK**.

Configuring Internet Explorer (4.01a)

Note For the procedure to configure Internet Explorer 5.0, refer to the *Cisco IOS Desktop Switching Software Configuration Guide*.

1. From the menu bar, select **View>Internet Options**.
2. In the Internet Options window, click **Advanced**.
3. Scroll through the list of options to Java VM, select the **Java JIT compiler enabled** and the **Java logging enabled** check boxes, and click **Apply**.
4. Click **General**. In the Temporary Internet Files section, click **Settings**. The Settings window opens.
5. Select **Every visit to the page**, and click **OK**.
6. In the Internet Options window, click **Security**.
7. In the Zone drop-down list, select **Trusted Sites Zone**, and click **Custom**.
8. Click **Settings**.
9. In the **Java>Java permissions** section, select **Custom**. Click the **Java Custom Setting**, which appears at the bottom of the window.
10. In the Trusted Sites Zone window, click **Edit Permissions**.
11. If the buttons under **Run Unsigned Content** are not available, select either **Medium** or **Low** security in the Reset Java Permissions list box, and click **Reset**.
12. Under **Run Unsigned Content**, select **Enable**, and click **OK**.
13. In the Security Settings window, click **OK**.
14. In the Internet Options window, click **Security**. Verify that the Zone drop-down list is set to Trusted Sites Zone.
15. In the Trusted Sites Zone section, click **Add Sites**.

16 In the Trusted Sites Zone window, deselect the **Require server verification** check box.

17 In the Add this Web site to the Zone field, enter the IP address of the switch.

Note If the you plan to use Cluster Management for switch configuration, you must enter the address of the cluster command switch. You also can enter the addresses of the member switches, but they are not required. If you plan to use Visual Switch Manager (VSM) for switch configuration, you must enter the IP address of each switch that you want to manage. You do not need to delete the address from the Trusted Sites list if the switch later becomes a cluster member. Refer to the *Cisco IOS Desktop Switching Software Configuration Guide* for more information.

18 Click **Add**, and then click **OK**.

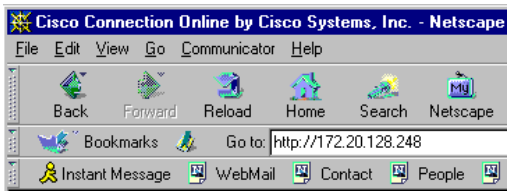
19 In the Internet Options window, click **Apply**, and then click **OK**.

Displaying the Access Page

After the browser is configured, display the Cluster Management Suite access page:

1 Enter the switch IP address in the Location field if you are using Netscape (the Address field if you are using Internet Explorer).

Note You can cut and paste the switch IP address from the window that you use to complete the setup program.



2 Press **Return**. The universal access page for your switch displays.

Note You are prompted with a message if your browser version is not supported.

3 Click **Cluster Management Suite or Visual Switch Manager** to display the appropriate Cluster Management application.

For More Information

See the *Catalyst 3500 Series XL Hardware Installation Guide* for detailed installation instructions for the Catalyst 3500 series XL switch. See the *Cisco IOS Desktop Switching Software Configuration Guide* for detailed instructions on using the Cluster Management Suite and the CLI to configure and manage switches. See the release notes for recent information about the Catalyst 3500 series XL switches.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe
11, Rue Camille Desmoulins
92782 Issy Les Moulineaux
Cedex 9
France
http://www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Headquarters
Nihon Cisco Systems K.K.
Fuji Building, 9th Floor
3-2-3 Marunouchi
Chiyoda-ku, Tokyo 100
Japan
http://www.cisco.com
Tel: 81 3 5219 6250
Fax: 81 3 5219 6001

Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the Cisco Connection Online Web site at http://www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE Finland • France • Germany • Greece • Hong Kong • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Singapore Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela

Access Registrar, AccessPath, Any to Any, AtmDirector, Browse with Me, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, the Cisco logo, Cisco Certified Internetwork Expert logo, CiscoLink, the Cisco Management Connection logo, the Cisco NetWorks logo, the Cisco Powered Network logo, Cisco Systems Capital, the Cisco Systems Capital logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, the Cisco Technologies logo, ConnectWay, Fast Step, FireRunner, Follow Me Browsing, FormShare, GigaStack, IGX, Intelligence in the Optical Core, Internet Quotient, IP/VC, Kernel Proxy, MGX, Natural Network Viewer, NetSonar, Network Registrar, the Networkers logo, Packet, PIX, Point and Click Internetworking, Policy Builder, Precept, RateMUX, ScriptShare, Secure Script, ServiceWay, Shop with Me, SlideCast, SMARTnet, SVX, The Cell, TrafficDirector, TransPath, ViewRunner, Virtual Loop Carrier System, Virtual Voice Line, VlanDirector, Voice LAN, Wavelength Router, Workgroup Director, and Workgroup Stack are trademarks; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, The Internet Economy, and The New Internet Economy are service marks; and Aironet, ASIST, BPX, Catalyst, Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, the Cisco Systems logo, the Cisco Systems Cisco Press logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, FastSwitch, GeoTel, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any of its resellers. (0004R)

Printed in the USA on recycled paper containing 10% postconsumer waste.
78-6458-03