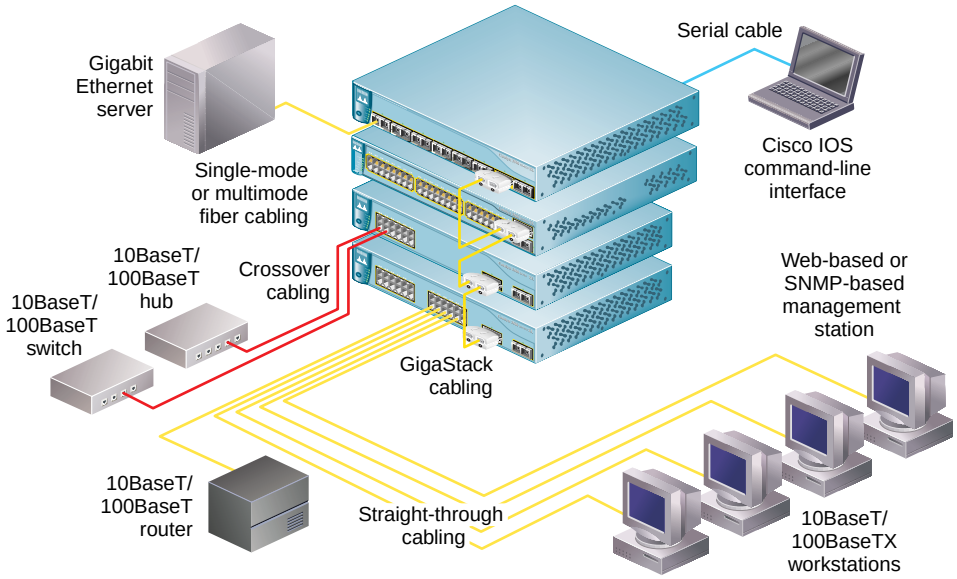
Quick Start Guide

CATALYST 3500 SERIES XL SWITCHES



1

TAKE OUT WHAT YOU NEED

2

CABLE THE SWITCH

3

ASSIGN IP INFORMATION TO THE SWITCH

4

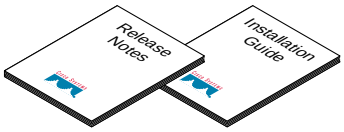
ACCESS THE SWITCH FROM YOUR BROWSER

CISCO SYSTEMS

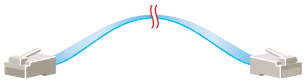
1 Take Out What You Need

Catalyst 3500 series XL switch

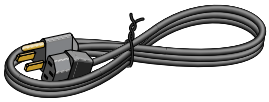
Catalyst 3500 *Installation Guide* and *Release Notes for the Catalyst 2900 Series XL and Catalyst 3500 Series XL Cisco IOS Release 12.0(5)XP.*



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



AC power cable

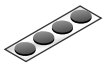


RJ-45-to-DB-9 serial connector

RJ-45-to-DB-25 terminal connector

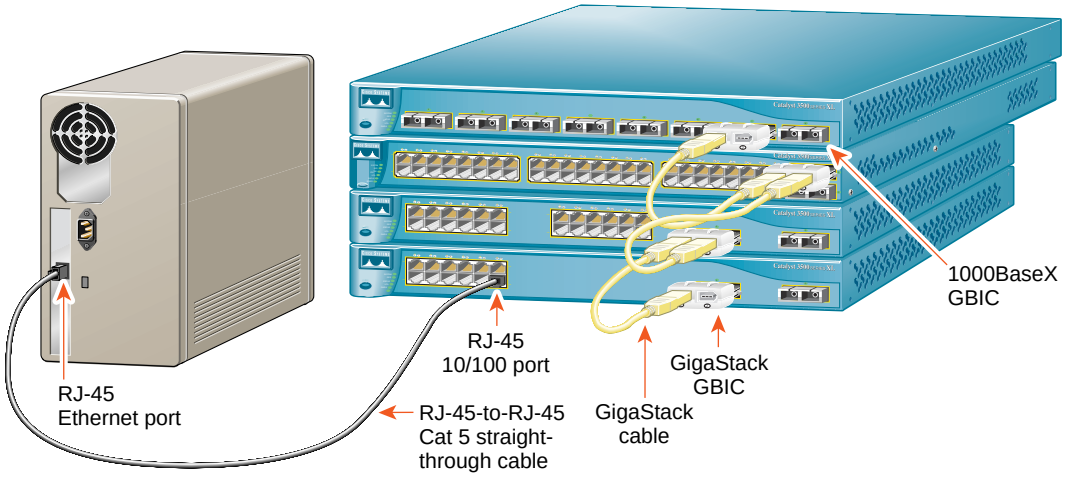
Rack-mount kit

Rubber feet



Note: You need to supply Category 5 straight-through or crossover cables to connect to Ethernet devices.

2 Cable the Switch



Connect PCs, Workstations, 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 PC, workstation, server, or router.

Connect Switches and Hubs

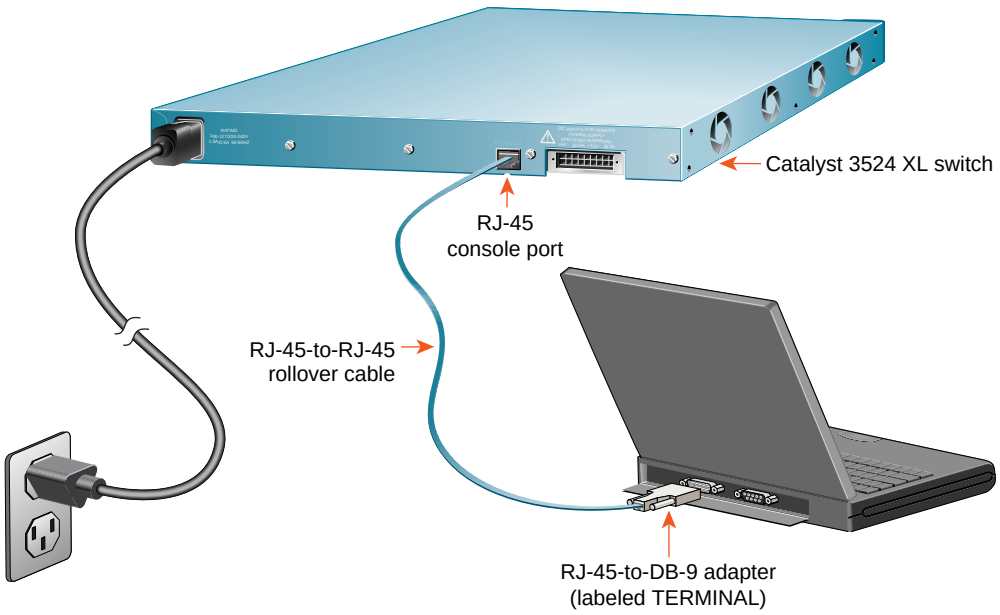
1. Connect a Category 5 **crossover** cable (not supplied) to a 10/100 port on the front panel of the switch.
2. Connect the other end of the cable to an RJ-45 port on the target switch or hub.

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 the Switches through GigaStack GBICs (Optional)

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

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 the AC Power Cord

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.

Connect the Console Cable

1. Connect the supplied flat, blue, rollover cable to the port marked CONSOLE on the rear panel of the switch.
2. Connect the other end of the cable to a terminal or PC with terminal-emulation software (such as ProComm Plus or HyperTerminal), using an adapter if necessary.

The terminal or emulation software must match the settings on the console port. Check your terminal or emulation software to be sure it matches the settings listed below, and reconfigure it if it does not.

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

3 Assign IP information to the Switch

The first time that you access the switch, it runs a setup program that prompts you for IP and other configuration information. This information is needed so that the switch can communicate with the local routers and the Internet. It is also required if you plan to use Cisco Visual Switch Manager (CVSM) to configure and manage the switch.

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

IP Information Requirements

Get the following IP information from your system administrator:

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

First-Time Startup

Use this procedure to assign IP information:

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

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

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

   ```
   Enter IP address:
   ```

3. Enter subnet mask, and press **Return**:

   ```
   Enter IP netmask:
   ```

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

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

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

   ```
   IP address of the default gateway?
   ```

6. Enter the host name, and press **Return**:

   ```
   Enter the host name:
   ```

7. Enter a secret password, and press **Return**:

   ```
   Enable secret password:
   ```

8 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 will appear as a candidate switch in Cluster Builder. In this case, the Step 9 message will not be displayed.

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

9 Assign a name to the cluster:

```
Enter cluster name? cls_name
```

10 The initial configuration displays as follows:

```
The following configuration command
script was created:
interface VLAN1
ip address 172.20.153.36 255.255.255.0
ip default-gateway 172.20.128.1
enable secret 5 $1$M3pS$cXtAlkyR3/6Cn8/
snmp community private rw
snmp community public ro
cluster enable cls_name
end

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

11 Verify that the addresses are correct.

12 Enter **Y**, and press **Return**. If the addresses are not correct, enter **N**, press **Return**, and begin again at Step 1.

When you see the message "Press RETURN to get started," the setup program is complete. You can use your browser, CVSM, or the command-line interface (CLI) to manage the switch.

4 Access the Switch from Your Browser

After you have assigned an IP address to the switch, you can use CVSM or the CLI to view or change configuration settings. If this is a command switch, you can also use the Cluster Management application to configure other switches. To use these Web-based tools, follow the procedures to set the appropriate browser options.

CVSM supports these platforms and network browsers:

Operating System	Minimum Operating System Requirements	Netscape Communicator	Microsoft Internet Explorer
Windows 95	Service Pack 1	4.5, 4.51, or 4.61	4.01a or 5.0
Windows 98	Second Edition	4.5, 4.51, or 4.61	4.01a or 5.0
Windows NT 4.0	Service Pack 3	4.5, 4.51, or 4.61	4.01a or 5.0
Solaris 2.5.1 or higher	SUN-recommended patch cluster for the OS and Motif library patch 103461-24	4.5, 4.51, or 4.61	Not supported

Note: Netscape Communicator version 4.6 is NOT supported.

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. Select **Every time.**
6. Click **OK**.

Configuring Internet Explorer (4.01a)

Note: For the procedure on configuring Internet Explorer 5.0, refer to the Cisco IOS Desktop Switching Software Configuration Guide.

1. From the menu bar, select **Tools>Internet Options**.
2. In the Internet Options window, click the **Advanced** tab.
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.**

Internet Explorer (continued)

4 Click the **General** tab. 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 the **Security** tab.

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 the **Edit Permissions** tab.

11 If the buttons under **Run Unsigned Content** are not available, select either **Medium** or **Low** security in the Reset Java Permissions list box. 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 the **Security** tab. 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 you plan to use Cluster Management for switch configuration, you must enter the IP address of the command switch. You can enter the addresses of the member switches, but they are not required. If you plan to use CVSM 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 site list if the switch later becomes a cluster member.

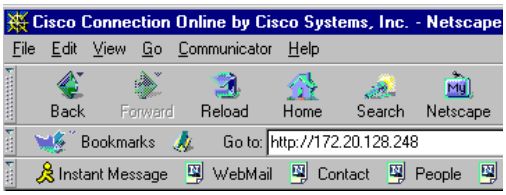
18 Click **Add,** and then click **OK**.

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

When the browser is configured, display the CVSM:

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 screen 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 **Visual Switch Manager** to display the CVSM home page.

For More Information

See the *Catalyst 3500 Series XL Installation Guide* for detailed installation instructions for the Cisco 3500 series XL switch. See the *Cisco IOS Desktop Switching Software Configuration Guide* for detailed instructions on using CVSM, the CLI, and the Cluster Management application to configure and manage switches. See *Release Notes for the Catalyst 2900 Series XL and Catalyst 3500 Series XL Cisco IOS Release 12.0(5)XP* for recent information about the Catalyst 3500 series XL switch.

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 s.a.r.l.
Parc Evolic, Batiment L1/L2
16 Avenue du Quebec
Villebon, BP 706
91961 Courtaboeuf Cedex
France
http://www-europe.cisco.com
Tel: 33 1 69 18 61 00
Fax: 33 1 69 28 83 26

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/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

Printed in the USA on recycled paper containing 10% postconsumer waste.

78-6458-02