



Catalyst 3750G Integrated Wireless LAN Controller Switch Getting Started Guide

INCLUDING LICENSE AND WARRANTY

- 1** About this Guide
- 2** Taking Out What You Need
- 3** Running Express Setup
- 4** Managing the Switch
- 5** Preparing the Wireless LAN Controller for Operation
- 6** Planning Switch Stacks
- 7** Rack-Mounting
- 8** In Case of Difficulty
- 9** Obtaining Documentation
- 10** Cisco Limited Lifetime Hardware Warranty Terms



1 About this Guide

This guide provides instructions on how to use Express Setup to initially configure your Catalyst 3750G Integrated Wireless LAN Controller switch. It also covers switch management options, the configuration procedures for the controller, basic rack-mounting procedures, stacking, port and module connections, power connection procedures, and any troubleshooting help.

The Catalyst 3750G Integrated Wireless LAN Controller switch has an integrated Cisco wireless LAN controller that can support Cisco Lightweight Access Points. The switch also has two internal Gigabit Ethernet ports (ports 27 and 28) that connect the switch and the controller. The integrated wireless LAN controller centralizes and simplifies network management of a wireless LAN. It collapses large numbers of managed lightweight access points and client devices into a single unified system.

For additional installation and configuration information for wireless LAN controller switches, see the Catalyst 3750 documentation on Cisco.com. For more information on the controller, see the *Cisco Wireless LAN Controller Configuration Guide, Release 4.0* or later on Cisco.com. For system requirements, important notes, limitations, open and resolved caveats, and last-minute documentation updates, see the release notes, also on Cisco.com.

When using the online publications, refer to the documents that match the Cisco IOS software version running on the switch. The software version is on the Cisco IOS label on the switch rear panel.

For translations of the warnings that appear in this publication, see the *Regulatory Compliance and Safety Information for the Catalyst 3750 Switch* that accompanies this guide.

2 Taking Out What You Need

Follow these steps:

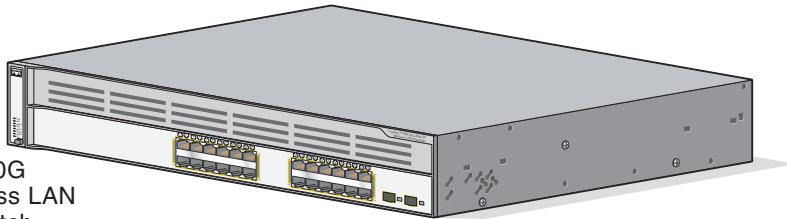
1. Unpack and remove the switch and the accessory kit from the shipping box.
2. Return the packing material to the shipping container, and save it for future use.
3. Verify that you have received the items shown on page 3. If any item is missing or damaged, contact your Cisco representative or reseller for instructions.



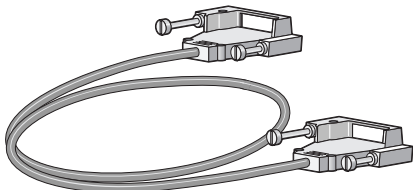
Note

If you do not specify the length of the StackWise cable, the 0.5-meter cable is supplied.

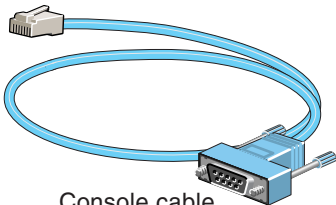
Shipping Box Contents



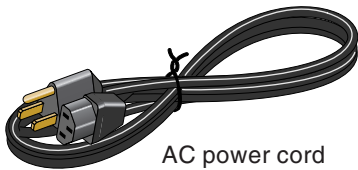
Catalyst 3750G
Integrated Wireless LAN
Controller switch



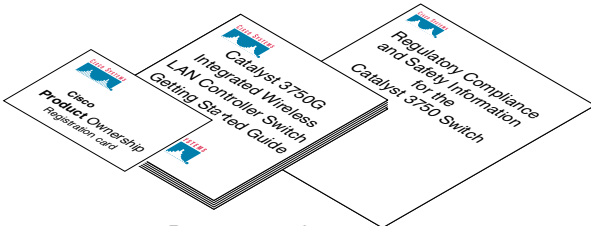
0.5-meter, 1-meter or 3-meter
StackWise cable



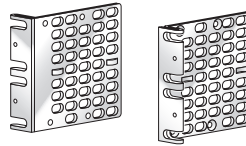
Console cable



AC power cord



Documentation



Two 19-inch
mounting brackets

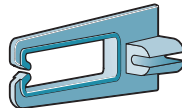
Four number-12 Phillips machine screws

Four number-8 Phillips truss-head screws

Six number-8 Phillips flat-head screws

Connector cover for redundant
power system (RPS)

Two number-4 pan-head screws



Cable guide

One black Phillips machine screw



Four rubber mounting feet

Equipment that You Supply to Run Express Setup

You need to supply this equipment to run Express Setup:

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



3 Running Express Setup

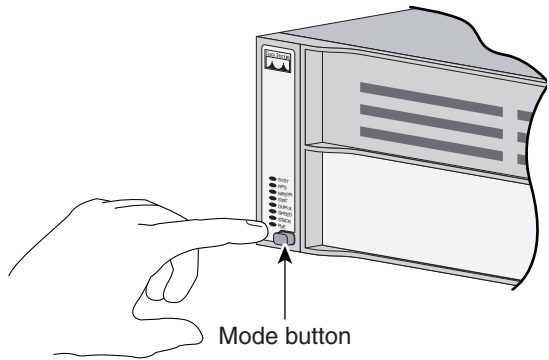
When you first set up the switch, you should use Express Setup to enter the initial IP information. Doing this enables the switch to connect to local routers and the Internet. You can then access the switch through the IP address for further configuration.

To run Express Setup:

-
- | | |
|---------------|---|
| Step 1 | Verify that no devices are connected to the switch. During Express Setup, the switch acts as a DHCP server. If your PC has a static IP address, before you begin, change your PC settings to temporarily use DHCP. |
| <hr/> | |
| Step 2 | Connect the AC power cord to the switch and to a grounded AC outlet. The power-on self-test (POST) begins. During POST, the LEDs blink while a series of tests verify that the switch functions properly. |
| <hr/> | |
| Step 3 | Wait for the switch to complete POST. It might take several minutes for the switch to complete POST. |
| <hr/> | |
| Step 4 | Verify that POST has completed by confirming that the SYST LED remains green. If the switch fails POST, the SYST LED turns amber.
POST errors are usually fatal. Call Cisco Systems immediately if your switch fails POST. |
-

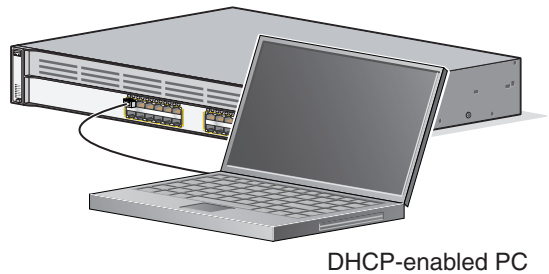
Step 5 Press and hold the Mode button for 3 seconds. When all of the LEDs above the Mode button turn green, release the Mode button.

If the LEDs above the Mode button begin to blink after you press the button, release it. Blinking LEDs mean that the switch has already been configured and cannot go into Express Setup mode. For more information, see the “Resetting the Switch” section on page 35.



Step 6 Verify that the switch is in Express Setup mode by confirming that all LEDs above the Mode button are green. (On some switch models, the RPS LED remains off.)

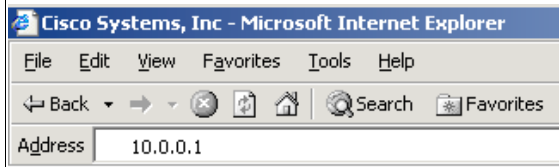
Step 7 Connect a straight-through Category 5 Ethernet cable (not provided) to any 10/100/1000 Ethernet port on the switch front panel and to the Ethernet port on the PC.



Step 8 Verify that the LEDs on both Ethernet ports are green.

Step 9 Wait 30 seconds.

Step 10 Launch a web browser on your PC. Enter the IP address 10.0.0.1 in the web browser, and press Enter.



Step 11

The Express Setup page appears. If it does not appear, see the “In Case of Difficulty” section on page 34 for help.

The screenshot shows the Express Setup page with three main sections:

- Network Settings:** Management Interface (VLAN ID): 1, IP Address: . . . , Subnet Mask: 255.255.255.0, Default Gateway: . . . , Switch Password: , Confirm Switch Password: .
- Wireless Controller Settings:** A table with columns: Stack Number, Management VLAN ID, IP Address, Subnet Mask, Default Gateway. Row 1: 1, 1, . . . , 255.255.255.0, . . .
- Optional Settings:** Host Name: Switch, Telnet Access: Enable Disable, Telnet Password: , Confirm Telnet Password: ., SNMP: Enable Disable, SNMP Read Community: , SNMP Write Community: ., System Contact: , System Location: .

Buttons: Submit, Cancel

Step 12

Enter this information in the **Network Settings** fields:

- In the **Management Interface (VLAN ID)** field, the default is 1. Enter a new VLAN ID only if you want to change the management interface through which you manage the switch and to which you assign IP information. The VLAN ID range is 1 to 1001.
 - In the **IP Address** field, enter the IP address of the switch. In the **IP Subnet Mask** field, click the drop-down arrow, and select an **IP Subnet Mask**.
 - In the **Default Gateway** field, enter the IP address for the default gateway (router).
 - Enter your password in the **Switch Password** field. The password can be from 1 to 25 alphanumeric characters, can start with a number, is case sensitive, allows embedded spaces, but does not allow spaces at the beginning or end. In the **Confirm Switch Password** field, enter your password again.
-

Step 13

In the **Wireless Controller Settings** area (see the Figure in Step 11), the stack number displays the stack-member number of the switch.

Enter this information:

- In the **Management Interface (VLAN ID)** field, the default is 0. Enter a new VLAN ID only if you want to change the management interface through which you manage the controller and to which you assign IP information. If you entered a VLAN ID other than 1 in Step 12, then enter the same VLAN ID for the controller. The VLAN ID range is 0 to 1001.
- In the **IP Address** field, enter the IP address of the controller.
- In the **IP Subnet Mask** field, click the drop-down arrow, and select an **IP Subnet Mask**.
- In the **Default Gateway** field, enter the IP address for the default gateway (router).



Note

If you are connecting more than one wireless controller switch, multiple rows appear in the wireless controller settings area.

Step 14 (Optional) You can enter the **Optional Settings** information now or enter it later by using the device manager interface:

- In the **Host Name** field, enter a name for the switch. The host name is limited to 31 characters; embedded spaces are not allowed.
- In the **Telnet Access** field, click **Enable** if you are going to use Telnet to manage the switch by using the command-line interface (CLI). If you enable Telnet access, you must enter a Telnet password.
- In the **Telnet Password** field, enter a password. The Telnet password can be from 1 to 25 alphanumeric characters, is case sensitive, allows embedded spaces, but does not allow spaces at the beginning or end. In the **Confirm Telnet Password** field, re-enter the Telnet password.
- In the **SNMP** field, click **Enable** to enable Simple Network Management Protocol (SNMP). Enable SNMP only if you plan to manage switches by using CiscoWorks 2000 or another SNMP-based network-management system.

If you enable SNMP, you must enter a community string in the **SNMP Read Community** field, the **SNMP Write Community** field, or both. SNMP community strings authenticate access to MIB objects. Embedded spaces are not allowed in SNMP community strings. When you set the SNMP read community, you can access SNMP information, but you cannot modify it. When you set the SNMP write community, you can both access and modify SNMP information.

- In the **System Contact** field, enter the name of the person who is responsible for the switch. In the **System Location** field, enter the wiring closet, floor, or building where the switch is located.

Step 15 Click **Submit** to save your settings, or click **Cancel** to clear your settings.

When you click **Submit**, the switch is configured and exits Express Setup mode. The PC displays a warning message and then tries to connect with the new switch IP address. If you configured the switch with an IP address that is in a different subnet from the PC, connectivity between the PC and the switch is lost.

Step 16 Disconnect the switch from the PC, and install the switch in your network. See the “Managing the Switch” section on page 9 for information about configuring and managing the switch.

If you need to rerun Express Setup, see the “Resetting the Switch” section on page 35.

Refreshing the PC IP Address

After you complete Express Setup, you should refresh the PC IP address:

- For a dynamically assigned IP address, disconnect the PC from the switch, and reconnect it to the network. The network DHCP server assigns a new IP address to the PC.
- For a statically assigned IP address, change it to the previously configured IP address.

4 Managing the Switch

After you complete Express Setup and install the switch in your network, use the device manager or other management options described in this section for further configuration.

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.

Follow these steps:

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. Refer to the device manager online help for more information.
4. For more advanced configuration, download and run the Cisco Network Assistant, which is described in the next section.

Downloading Cisco Network Assistant

Cisco Network Assistant is a software program that you download from Cisco.com and run on your PC. It offers advanced options for configuring and monitoring multiple devices, including switches, switch clusters, switch stacks, routers, and access points. Network Assistant is free—there is no charge to download, install, or use it.

Follow these steps:

1. Go to this Web address: <http://www.cisco.com/go/NetworkAssistant>.
You must be a registered Cisco.com user, but you need no other access privileges.
2. Find the Network Assistant installer.

3. Download the Network Assistant installer, and run it. (You can run it directly from the Web if your browser offers this choice.)
4. When you run the installer, follow the displayed instructions. In the final panel, click **Finish** to complete the Network Assistant installation.

Refer to the Network Assistant online help and the getting started guide for more information.

Command-Line Interface

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.

Follow these steps:

1. Connect the supplied RJ-45-to-DB-9 adapter cable to the standard 9-pin serial port on the PC. Connect the other end of the cable to the switch console port.
2. Start a terminal-emulation program on the PC.
3. Configure the PC terminal emulation software for:
 - 9600 baud
 - 8 data bits
 - No parity
 - 1 stop bit
 - No flow control
4. Use the CLI to enter commands to configure the switch. See the software configuration guide and the command reference for more information.

Other Management Options

You can use SNMP management applications such as CiscoWorks Small Network Management Solution (SNMS) and HP OpenView to configure and manage the switch. You also can manage it from an SNMP-compatible workstation that is running platforms such as HP OpenView or SunNet Manager.

The Cisco IE2100 Series Configuration Registrar is a network management device that works with embedded Cisco Networking Services (CNS) agents in the switch software. You can use IE2100 to automate initial configurations and configuration updates on the switch.

See the “Accessing Help Online” section on page 36 for a list of supporting documentation.

5 Preparing the Wireless LAN Controller for Operation

Follow these major steps to prepare the integrated wireless LAN controller for operation.

- Using the Configuration Wizard to Configure the Controller
- Logging into the Controller
- Verifying Interface Settings and Port Operation
- Connecting Access Points

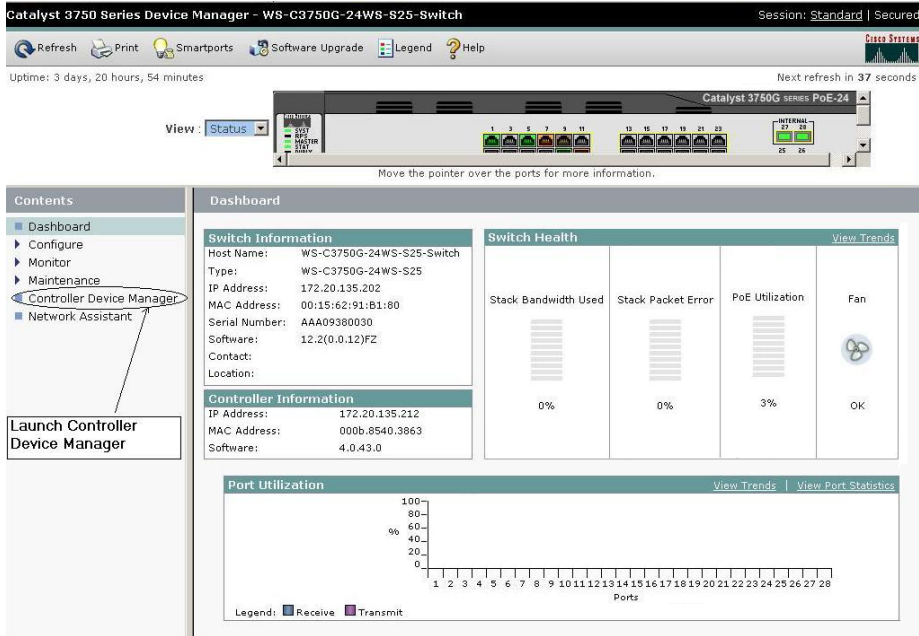
Using the Configuration Wizard to Configure the Controller

Follow these steps to use the Configuration Wizard to configure the controller for basic operation:

Step 1	Get the initial configuration parameter settings for the controller from your wireless LAN planner.
Step 2	Launch a web browser on your PC.
Step 3	If you have not already done so, assign a static IP address to your PC from the same subnet as the switch; otherwise, the web browser cannot establish a connection with the switch.

Step 4

Enter the management IP address of the switch (which you set in Step 12 of the Express Setup) in the web browser, and press **Enter**. The Catalyst 3750 Device Manager page appears.



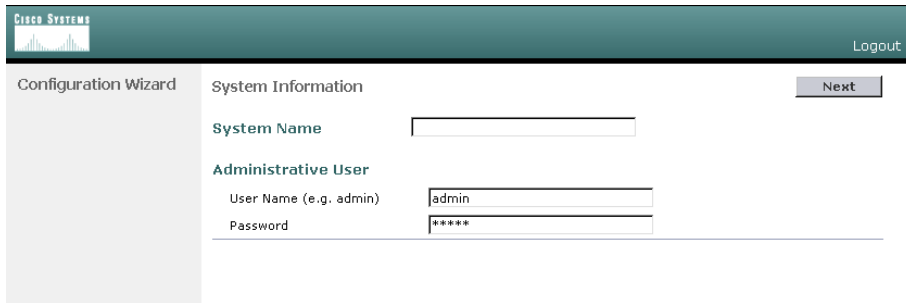
155493

Step 5

Under Contents, click **Controller Device Manager**.

Step 6

When prompted for a username and password, enter **admin** in each field. The first page of the Configuration Wizard appears.



155494

Step 7 In the **System Name** field, enter the system name, which is the name that you want to assign to the controller. You can enter up to 32 ASCII characters.

Step 8 In the **User Name** and **Password** fields, enter the administrative username and password for this controller. You can enter up to 24 ASCII characters for each. The default administrative username and password are both *admin*.

Step 9 Click **Next**. The Service Interface Configuration page appears.

CISCO SYSTEMS
Logout

Configuration Wizard Service Interface Configuration < Back Next

General Information

Interface Name service-port

MAC Address 00:16:9d:ca:e0:21

Interface Address

DHCP Protocol Enabled

IP Address 192.168.1.1

Netmask 255.255.255.0

155496

Step 10 If you want the controller service-port interface to get an IP address from a DHCP server, check the **DHCP Protocol Enabled** check box. If you do not want to use the service port or if you want to assign a static IP address to the service-port interface, leave the check box unchecked.

The service-port interface controls communications through the service port, which is reserved for out-of-band management of the controller and for system recovery and maintenance in the event of a network failure. Its IP address must be on a different subnet from the management and AP-manager interfaces. You can use this configuration to manage the controller directly or through a dedicated management network to ensure service access during network downtime.

Step 11 If you did not check the DHCP Protocol Enabled check box in Step 10, leave the IP address and the netmask for the service-port interface as they are, or change them as necessary. If you do not want to use the service port, enter **0.0.0.0** for both the IP address and the netmask.

Step 12

Click **Next**. The Management Interface Configuration page appears.

CISCO SYSTEMS

Logout

Configuration Wizard Management Interface Configuration < Back Next

General Information

Interface Name management

MAC Address 00:16:9d:ca:e0:20

Interface Address

VLAN Identifier 0

IP Address 20.20.20.2

Netmask 255.255.255.0

Gateway 20.20.20.1

Physical Information

The interface is attached to a LAG.

DHCP Information

Primary DHCP Server 20.20.20.1

Secondary DHCP Server 0.0.0.0

155677

Step 13

Enter the VLAN identifier zero (0) if the VLAN ID set on the switch management interface is 1. If you entered a VLAN ID other than 1 on the switch management interface (see Step 12 of the Running Express Setup section), enter the same VLAN ID for the controller. Enter the IP address, the netmask, and the gateway for the management interface.

The management interface is the default interface for in-band management of the controller and for connectivity to enterprise services such as authentication, authorization, and accounting (AAA) servers.

Step 14

Enter the IP addresses of the primary and the optional secondary DHCP servers that supply IP addresses to clients, the controller management interface, and, optionally, the service-port interface.

Step 15

Click **Next**. The Miscellaneous Configuration page appears.

Configuration Wizard Miscellaneous Configuration

LWAPP Transport Mode

RF Mobility Domain Name

Enter the country code where the system is currently operating. A table of supported country codes is provided below.

Country Code

Country Code - Name	Supported Protocols		
	802.11a	802.11b	802.11g
AR	NO	YES	YES
AT	YES	YES	YES
AU	YES	YES	YES
BR	NO	YES	YES
BE	YES	YES	YES
CA	YES	YES	YES
CH	YES	YES	YES
CL	NO	YES	YES
CN	YES	YES	YES
CO	NO	YES	YES
CY	YES	YES	YES
CZ	YES	YES	NO
DE	YES	YES	YES
DK	YES	YES	YES
EE	YES	YES	YES
ES	YES	YES	YES
FI	YES	YES	YES
FR	YES	YES	YES
GB	YES	YES	YES
GR	NO	YES	YES
GI	YES	YES	YES
HK	YES	YES	YES
HU	YES	YES	YES
ID	NO	YES	YES
IE	YES	YES	YES
IN	YES	YES	YES
IL	YES	YES	YES
ILO	NO	YES	YES
IS	YES	YES	YES
IT	YES	YES	YES
JP	YES	YES	YES
J2	YES	YES	YES
KR	YES	YES	YES
KE	YES	YES	YES
LI	YES	YES	YES
LT	YES	YES	YES
LU	YES	YES	YES
LV	YES	YES	YES
MC	YES	YES	YES
MT	YES	YES	YES
MX	YES	YES	YES
MY	YES	YES	YES
NL	YES	YES	YES

155499

Step 16 From the **LWAPP Transport Mode** drop-down box, choose **Layer 3**. The controller operates only in Layer 3 mode.

Step 17 (Optional) In the **RF Mobility Domain Name** field, enter the name of the mobility group/RF group to which you want the controller to belong.

Although the name that you enter here is assigned to both the mobility group and the RF group, these groups are not identical. Both groups define clusters of controllers, but they have different purposes. All of the controllers in an RF group are usually also in the same mobility group and the reverse. However, a mobility group facilitates scalable, system-wide mobility and controller redundancy, while an RF group facilitates scalable, system-wide dynamic RF management.

Step 18 In the **Country Code** field, enter the code for the country in which the controller will be used. See the table below the Country Code field for the list of available country codes.

Step 19 Click **Next**. The AP Manager Interface Configuration page appears.

The screenshot shows the 'AP Manager Interface Configuration' page within a 'Configuration Wizard'. The page has a dark green header with the Cisco Systems logo and a 'Logout' link. Below the header, the page title 'AP Manager Interface Configuration' is displayed, along with '< Back' and 'Next >' buttons. The configuration is organized into sections: 'General Information' with an 'Interface Name' field set to 'ap-manager'; 'Interface Address' with fields for 'VLAN Identifier' (0), 'IP Address' (20.20.20.3), 'Netmask' (255.255.255.0), and 'Gateway' (20.20.20.1); 'Physical Information' with a note 'The interface is attached to a LAG.'; and 'DHCP Information' with fields for 'Primary DHCP Server' (20.20.20.1) and 'Secondary DHCP Server' (0.0.0.0). A vertical ID number '155500' is visible on the right side of the page.

Step 20 Enter the VLAN identifier, the IP address, the netmask, and the gateway for the controller AP-manager interface.

The AP-manager interface is used for Layer 3 communications between the controller and lightweight access points and must have a unique IP address. It is usually configured on the same VLAN or IP subnet as the management interface, but this is not a requirement.

Step 21 Enter the IP addresses of the primary and the optional secondary DHCP servers that supply IP addresses to the controller AP-manager interface. If the AP-manager interface is on the same subnet as the management interface, the AP-manager interface uses the same DHCP server IP address as the management interface.

Step 22 Click **Next**. The Virtual Interface Configuration page appears.

The screenshot shows the 'Virtual Interface Configuration' page in the Cisco Configuration Wizard. The page is divided into two main sections: 'General Information' and 'Interface Address'. In the 'General Information' section, the 'Interface Name' field is populated with the value 'virtual'. In the 'Interface Address' section, the 'IP Address' field is populated with '1.1.1.1', and the 'DNS Host Name' field is currently empty. At the top right of the page, there is a 'Logout' link. Below the main content area, the number '155501' is printed vertically. Navigation buttons for '< Back' and 'Next >' are located at the top right of the configuration area.

Step 23 In the **IP Address** field, enter the IP address of the controller virtual interface to be used by all controller Layer 3 security and mobility managers. You should enter a fictitious, unassigned IP address, such as 1.1.1.1.

The virtual interface is used to support mobility management, DHCP relay, and embedded Layer 3 security such as guest web authentication and VPN termination. All controllers within a mobility group must be configured with the same virtual interface IP address.

Step 24 In the **DNS Host Name** field, enter the DNS host name if your controller uses an externally generated web authentication ID certificate that includes a DNS hostname.

Step 25

Click **Next**. The WLAN Policy Configuration page appears.

Configuration Wizard WLAN Policy Configuration < Back Next

WLAN ID 1
WLAN SSID WLAN

General Policies

Radio Policy All
Admin Status Enabled
Session Timeout 1800
Quality of Service (QoS) Silver (best effort)
Allow AAA Override Enabled
Blacklist Timeout Enabled ** 60
Timeout Value(secs)
DHCP Server Override
DHCP Addr. Assignment Required
Interface Name management

Security Policies

Layer 2 Security 802.1X
 MAC Filtering
Layer 3 Security None
 Web Authentication *

** When enabled, a blacklist timeout value of zero means infinity (will require administrative override to reset blacklisted clients).

802.1X Parameters

802.11 Data Encryption	Type	Key Size
<input checked="" type="radio"/>	WEP	104 bits

155678

Step 26

In the **WLAN SSID** field, enter the network name or service set identifier (SSID). This is the default SSID that the access points use when they join a controller.

Step 27

Under **General Policies**, check the **DHCP Address Assignment Required** check box to make clients request an IP address from a DHCP server, or uncheck this check box to allow clients to assign their own IP addresses.

Step 28

Leave the rest of the parameters on this page at their default values, or change them to meet your deployment needs. Refer to the online help for additional information on specific parameters.

Step 29 Click **Next**. The RADIUS Server Configuration page appears.

The screenshot shows the 'RADIUS Server Configuration' page within the Cisco Configuration Wizard. The page has a dark green header with the Cisco Systems logo and a 'Logout' link. Below the header, the title 'RADIUS Server Configuration' is displayed, followed by '< Back', 'Apply', and 'Skip' buttons. The main content area contains several configuration fields: 'Server IP Address' (text input), 'Shared Secret Format' (dropdown menu set to 'ASCII'), 'Shared Secret' (text input), 'Confirm Shared Secret' (text input), 'Port Number' (text input set to '1812'), and 'Server Status' (dropdown menu set to 'Disabled'). A vertical ID number '155503' is visible on the right side of the page.

Step 30 To configure a RADIUS server now, enter the IP address, the shared secret, and the communication port of the RADIUS server, and click **Apply**. Otherwise, click **Skip**. The IEEE 802.11 Configuration page appears.

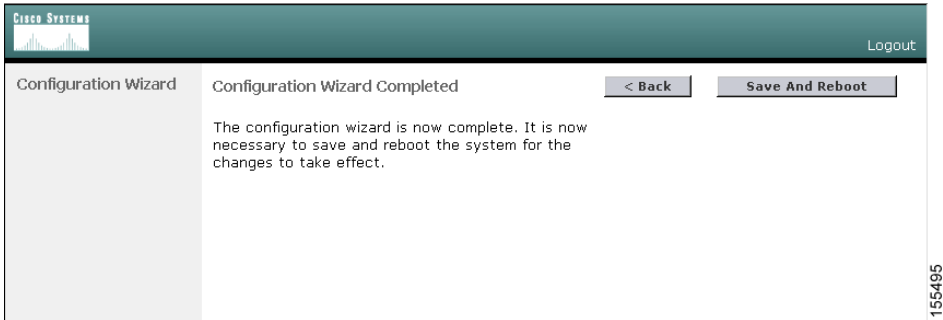
The screenshot shows the '802.11 Configuration' page within the Cisco Configuration Wizard. The page has a dark green header with the Cisco Systems logo and a 'Logout' link. Below the header, the title '802.11 Configuration' is displayed, followed by '< Back' and 'Next' buttons. The main content area contains four configuration items, each with a checkbox and the text 'Enabled': '802.11a Network Status', '802.11b Network Status', '802.11g Network Status', and 'Auto RF'. A vertical ID number '155505' is visible on the right side of the page.

Step 31 Check or uncheck the **802.11a**, **802.11b**, and **802.11g Network Status** check boxes to enable or disable each of the IEEE 802.11a, IEEE 802.11b, and IEEE 802.11g lightweight access point networks.

Step 32 Check or uncheck the **Auto RF** check box to enable or disable the controller radio resource management (RRM) auto-RF feature.

The auto-RF feature enables the controller to automatically form an RF group with other controllers. The group dynamically elects a leader to optimize RRM parameter settings, such as channel and send power assignments, for the group.

Step 33 Click **Next**. The Configuration Wizard Completed page appears.



Step 34 Click **Save and Reboot**.

Step 35 When prompted, click **OK** to confirm the reboot. The controller saves your configuration and reboots. The reboot process can take several minutes, so you might need to wait before accessing your web browser again.

Logging into the Controller

Follow these steps to log into the controller from the switch.

Step 1 Telnet to the switch by using the switch IP address.

Step 2 At the switch system prompt, enter **session 1 processor 1**, and press **Enter**. The session number is linked to the controller. If there are two switches and you want to access controller number 2, you would enter **session 2 processor 1**.

Step 3 When prompted, enter a valid username and password to log into the controller, and press **Enter**. The administrative username and password were assigned in the Configuration Wizard and are case sensitive.

Verifying Interface Settings and Port Operation

Follow these steps to verify that your interface configurations have been set properly and that the controller ports are operational.

Step 1 Enter **show interface summary**, and press **Enter**. This display shows the controller interface configurations:

Interface Name	Port	Vlan Id	IP Address	Type	Ap Mgr
ap-manager	LAG	10	10.91.104.99	Static	Yes
management	LAG	10	10.91.104.93	Static	No
service-port	N/A	N/A	10.10.0.9	Static	No
virtual	N/A	N/A	1.1.1.1	Static	No

Link aggregation (LAG) is always enabled for the integrated wireless LAN controller and cannot be disabled. LAG bundles all of the controller distribution system ports into a single IEEE 802.3ad port channel. See the *Cisco Wireless LAN Controller Configuration Guide 4.0* or later for more information.

Step 2 Enter **show port summary**, and press **Enter**. This display shows the status of the controller distribution system ports, which serve as the data path between the controller and the Cisco lightweight access points and to which the controller management and AP-manager interfaces are mapped.

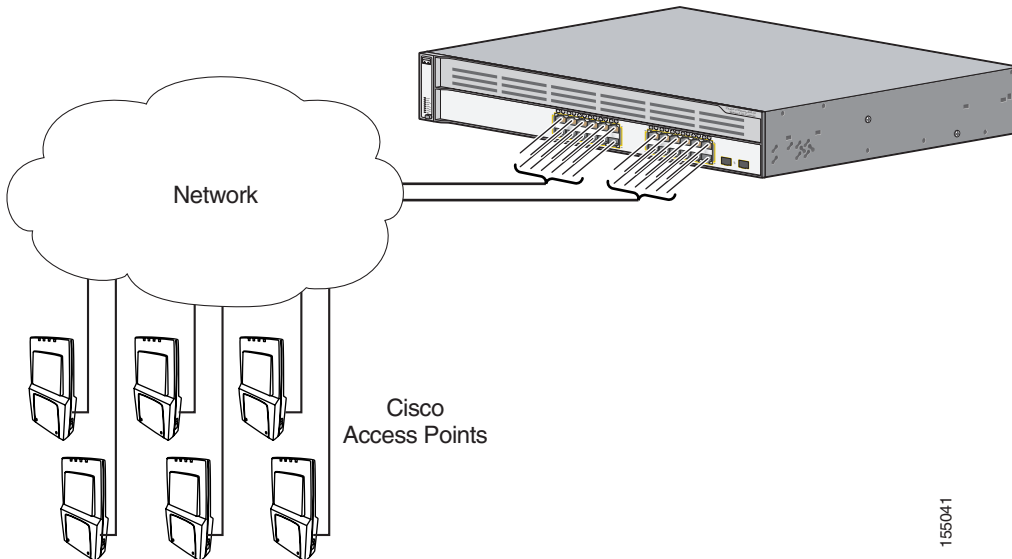
Pr	Type	STP Stat	Admin Mode	Physical Mode	Physical Status	Link Status	Link Trap	Mcast Appliance	POE
1	Normal	Forw	Enable	Auto	1000 Full	Up	Enable	Enable	N/A
2	Normal	Forw	Enable	Auto	1000 Full	Up	Enable	Enable	N/A

A link status of *Up* means that the controller ports are fully operational.

Connecting Access Points

After you have configured the controller, use Category-5, -5e, -6, or -7 Ethernet cables to connect Cisco lightweight access points to the network.

As soon as the controller is operational, it starts to scan for access points. When it detects one, it records the its MAC address in its database. The controller RRM feature then automatically configures the access point to start sending and allowing clients to associate.



For the integrated wireless LAN controller, access points can operate only in Layer 3 Lightweight Access Point Protocol (LWAPP) mode.

You have prepared the controller for basic operation. See the *Cisco Wireless LAN Controller Configuration Guide, Release 4.0* or later, for information on configuring the controller to meet the specific needs of your wireless network.

6 Planning Switch Stacks

Before connecting the Catalyst 3750 switches in a stack, keep in mind these planning considerations:

- The size of the switch—See the “Technical Specifications” appendix of the *Catalyst 3750 Switch Hardware Installation Guide* for the switch dimensions. Stacking together switches of the same size makes it easier to cable the switches.
- Length of cable—Depending on the configuration of your switch stack, you might need different-sized cables. If you do not specify the length of the StackWise cable, the 0.5-meter cable is supplied. If you require the 1-meter cable or 3-meter cable, you can order it from your Cisco supplier. For cable numbers, see the *Catalyst 3750 Switch Hardware Installation Guide*.



Note For concepts and procedures for managing switch stacks, refer to the switch software configuration guide.

Powering Considerations

Consider these guidelines before you power the switches in a stack:

- The sequence in which the switches are initially powered on might affect the switch that becomes the stack master.
- If you want a particular switch to become the stack master, power on that switch first. This switch becomes the stack master and remains the stack master until a master re-election is required. After 20 seconds, power on the remaining switches in the stack.
- If you have no preference for which switch becomes the stack master, power on all the switches in the stack within a 20-second timeframe. These switches participate in the stack master election. Switches powered on after the 20-second timeframe do not participate in the election.
- Power off a switch before you add it to or remove it from an existing switch stack.



Note Stack master elections occur over a 10-second timeframe on switches running releases earlier than Cisco IOS Release 12.2(20)SE3.

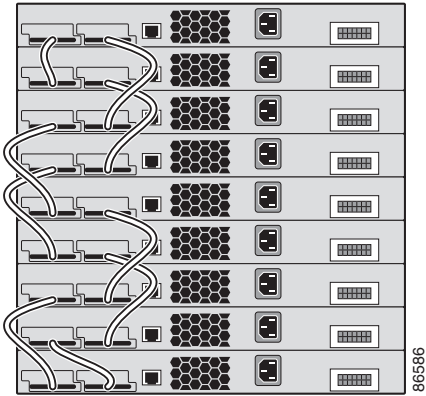
For more information on stack master elections, see the “Managing Switch Stacks” chapter in the switch software configuration guide.

Cabling Considerations

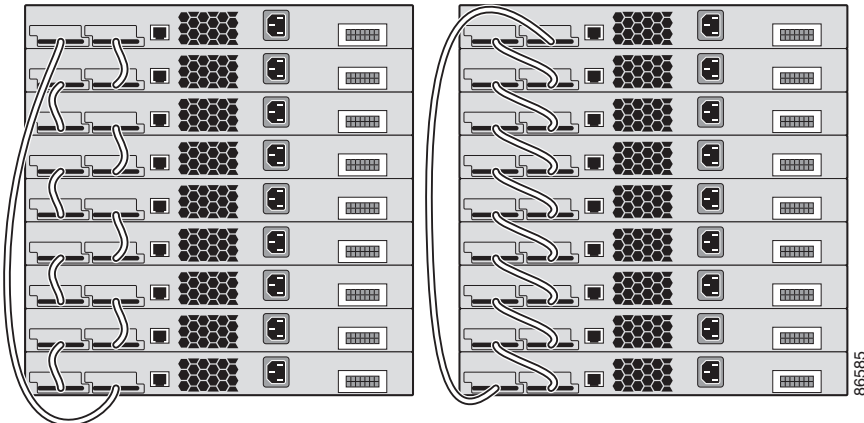
These illustrations show the recommended Catalyst 3750 switch stack configurations with redundant StackWise cabling connections for optimized stack bandwidth. For more configuration examples, see the *Catalyst 3750 Switch Hardware Installation Guide* on Cisco.com.

Vertical Stacking

In this example, the stack uses the 0.5-meter StackWise cable to make redundant connections.

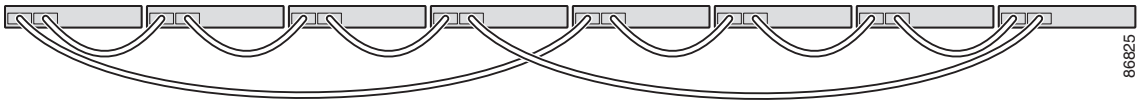


In this example, the stacks use both 0.5- and 3-meter StackWise cables to make redundant connections.

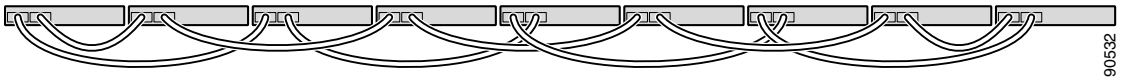


Side-By-Side Stacking

In this example, eight switches are stacked side-by-side with redundant connections by using 0.5- and 3-meter StackWise cables.



In this example, nine switches are stacked side-by-side with redundant connections by using 0.5- and 3-meter StackWise cables.



7 Rack-Mounting

This section covers basic 19-inch rack-mounting and switch port connections. For additional cabling information, see the *Catalyst 3750 Switch Hardware Installation Guide* on Cisco.com.

Equipment That You Supply

You need to supply a number-2 Phillips screwdriver to rack-mount the switch.

Before You Begin

When determining where to install the switch, verify that these guidelines are met:

- Airflow around the switch and through the vents is unrestricted.
- Temperature around the switch does not exceed 113°F (45°C).
- Humidity around the switch does not exceed 85 percent.
- Altitude at the installation site is not greater than 10,000 feet.
- Clearance to the switch front and rear panels meets these conditions:
 - Front-panel LEDs can be easily read.
 - Access to ports is sufficient for unrestricted cabling.
 - AC power cord can reach from the AC power outlet to the connector on the switch rear panel.
 - Access to the rear of the rack is sufficient for connecting StackWise cables to stacked switches.
- Cabling is away from sources of electrical noise, such as radios, power lines, and fluorescent lighting fixtures.
- For 10/100/1000 ports, the cable length from a switch to an attached device cannot exceed 328 feet (100 meters).
- For cable lengths for small form-factor pluggable (SFP) modules, see the documentation that shipped with the module.

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 Catalyst 3750 Switch* document that shipped with the switch and is also available on Cisco.com.



Warning

Only trained and qualified personnel should be allowed to install, replace, or service this equipment. Statement 148



Warning

Installation of the equipment must comply with local and national electrical codes. Statement 1074



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

To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:

- **This unit should be mounted at the bottom of the rack if it is the only unit in the rack.**
 - **When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.**
 - **If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.** Statement 1006
-



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

If a redundant power system (RPS) is not connected to the switch, install an RPS connector cover on the back of the switch. Statement 265



Warning

Class 1 laser product. Statement 1008



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

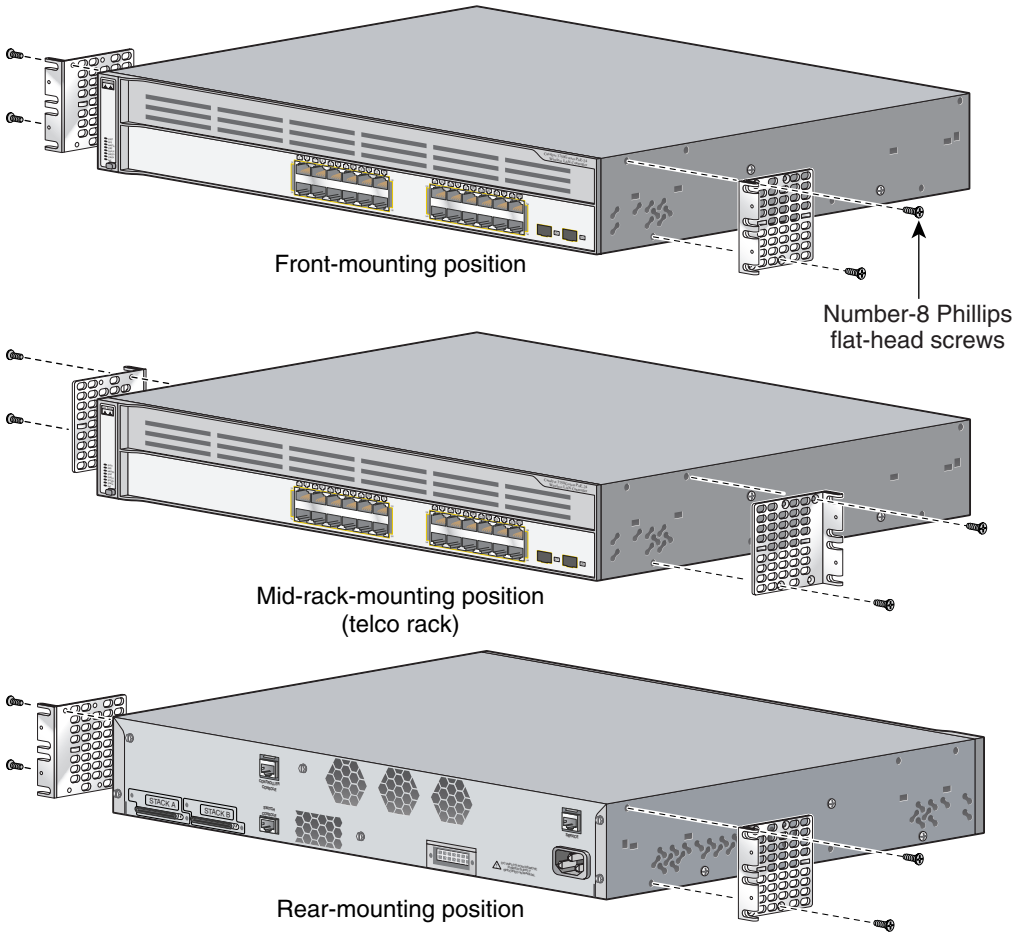


Warning

Voltages that present a shock hazard may exist on Power over Ethernet (PoE) circuits if interconnections are made using uninsulated exposed metal contacts, conductors, or terminals. Avoid using such interconnection methods, unless the exposed metal parts are located within a restricted access location and users and service people who are authorized within the restricted access location are made aware of the hazard. A restricted access area can be accessed only through the use of a special tool, lock and key or other means of security. Statement 1072

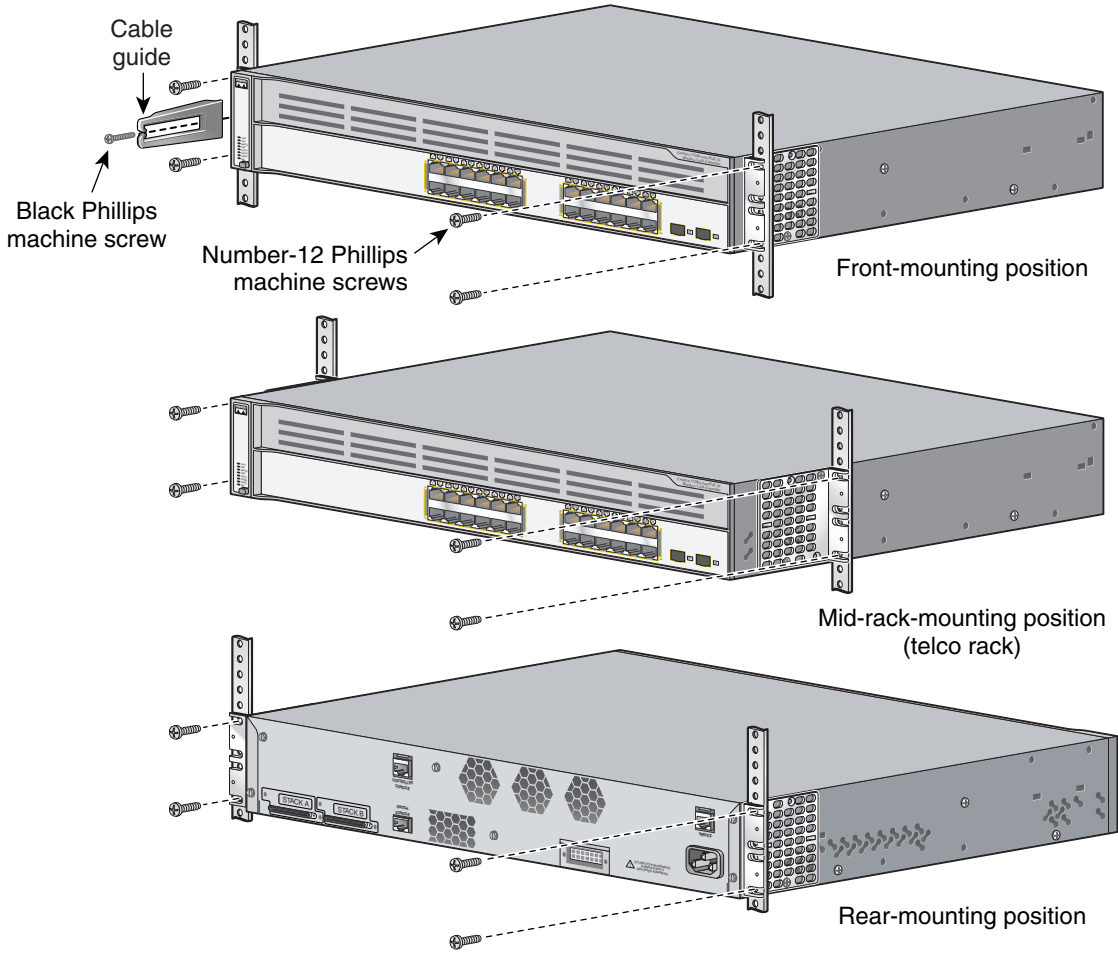
Attaching the Brackets

Use four Phillips flat-head screws to attach the long side of the brackets to wireless controller LAN switches in one of three mounting positions.



Rack-Mount the Switch

Use the black Phillips machine screw to attach the cable guide to the left or right bracket. Use the four number-12 Phillips machine screws to attach the brackets to the rack.

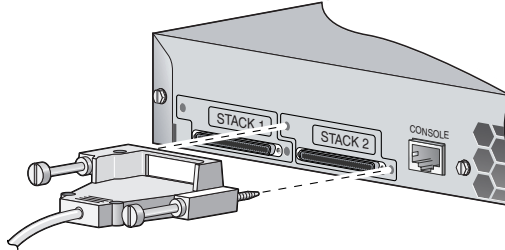


Connect the StackWise Cables

Follow these steps to connect the StackWise cable to the StackWise ports:

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

Step 2 Insert one end of the StackWise cable into the StackWise port on the back of the switch.



Step 3 Use the window in the StackWise cable to align the connector correctly. Secure the screws tightly.

Step 4 Insert the other end of the cable into the connector of the other switch, and secure the screws tightly.



Caution

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



Note

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

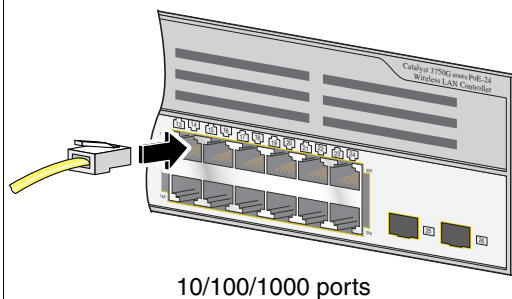
Connect to the Switch Ports

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

Connect to 10/100/1000 Ports

Follow these steps:

- Step 1** When you connect to servers, workstations, IP phones, wireless access points, and routers, insert a straight-through, twisted four-pair, Category 5 cable in a switch 10/100/1000 port.
- Use a crossover, twisted four-pair, Category 5 cable when you connect to other switches, hubs, or repeaters.



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

The fixed ports on the Catalyst 3750 Power over Ethernet (PoE) switches provide PoE support for IEEE 802.3af-compliant devices. They also provide Cisco pre-standard PoE support for Cisco IP Phones and Cisco Aironet Access Points.

Each of the 24 10/100/1000 switch ports can deliver up to 15.4 W of PoE. Any combination of the ports can deliver an average of 7.7 W of PoE at the same time, up to a maximum switch power output of 370 W.

By default, a Catalyst 3750 switch PoE port automatically provides power when a valid powered device is connected to it. For information about configuring and monitoring PoE ports, see the switch software configuration guide. For information about troubleshooting PoE problems, see the *Catalyst 3750 Switch Hardware Installation Guide* on Cisco.com.

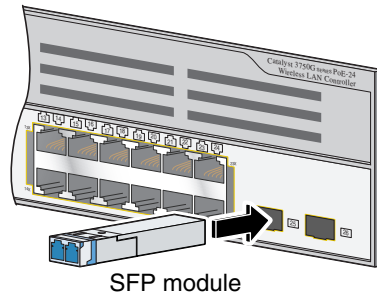


Note The automatic medium-dependent interface crossover (auto-MDIX) feature is enabled by default on switches running Cisco IOS Release 12.2(18)SE or later. When the auto-MDIX feature is enabled, the switch detects the required cable type for copper Ethernet connections and configures the interfaces accordingly. Therefore, you can use either a crossover or a straight-through cable for connections to a copper 10/100, 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.

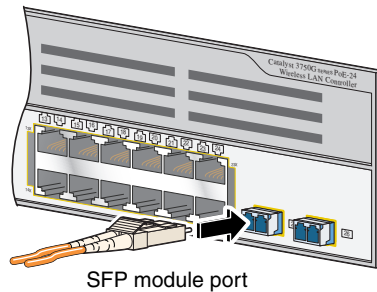
Install the SFP Modules and Connect to the Ports

Follow these steps:

- Step 1** Grasp the module on the sides, and insert it into the switch slot until you feel the connector snap into place.



- Step 2** Insert an appropriate cable into the module port. Insert the other cable end into the other device.



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 inserting 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. 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 34 for information about online assistance.

8 In Case of Difficulty

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

Troubleshooting Express Setup

If Express Setup does not run, or if the Express Setup page does not appear in your browser:

- Did you verify that POST successfully ran before starting Express Setup? If not, make sure that only the SYST and STAT LEDs are green before pressing the Mode button to enter the Express Setup mode.
- Did you press the Mode button while the switch was still running POST? If yes, wait until POST completes. Power cycle the switch. Wait until POST completes. Confirm that the SYST and STAT LEDs are green. Press the Mode button to enter Express Setup mode.
- Did you try to continue without confirming that the switch was in Express Setup mode? Verify that all LEDs above the Mode button are green. (The RPS LED is off.) If necessary, press the Mode button to enter Express Setup mode.
- Does your PC have a static IP address? If yes, before connecting to the switch, change your PC settings to temporarily use DHCP.
- Did you connect a crossover cable instead of a straight-through Ethernet cable between a switch port and the Ethernet port of the PC? If yes, connect a straight-through cable to an Ethernet port on the switch and the PC. Wait 30 seconds before you enter 10.0.0.1 in the browser.
- Did you connect the Ethernet cable to the console port instead of to a 10/100/1000 Ethernet port on the switch? If yes, disconnect the cable from the console port. Then connect the cable to an Ethernet port on the switch and the PC. Wait 30 seconds before you enter 10.0.0.1 in the browser.

- Did you wait 30 seconds after you connected the switch and the PC before you entered 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 enter the wrong address in the browser, or is there an error message? If yes, re-enter **10.0.0.1** in the browser, and press **Enter**.

Resetting the Switch

This section describes how to reset the switch by rerunning Express Setup. 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 incorrect IP address.
- You want to clear all configuration from the switch and assign a new IP address.
- You are trying to enter Express Setup mode, and the switch LEDs start blinking when you press the Mode button (which means that the switch is already configured with IP information).



Caution

Resetting the switch deletes the configuration and reboots the switch.

To reset the switch:

Press and hold the Mode button. The switch LEDs begin blinking after about 3 seconds. Continue holding down the Mode button. The LEDs stop blinking after 7 more seconds, and then the switch reboots.

The switch now behaves like an unconfigured switch. You can enter the switch IP information by using Express Setup as described in the “Running Express Setup” section on page 4.

Troubleshooting the Wireless Controller

You can troubleshoot the controller by using the **show platform wireless-controller** privileged EXEC command.

It displays information about the internal wireless controller in a Catalyst 3750G Integrated Wireless LAN Controller Switch. You can use it to determine the stack number of a switch or switches in the stack that contain the integrated wireless LAN controller. The command output also displays the MAC address and IP address of the controller.

```
show platform wireless-controller [management-info | status | summary] [switch-number]
[ | {begin | exclude | include} expression]
```

Accessing Help Online

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

9 Obtaining Documentation

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the What's New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

For More Information

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

- *Catalyst 3750 Switch 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 Catalyst 3750 Switch* (order number DOC-7816664=). This guide contains agency approvals, compliance information, and translated warning statements.
- *Release Notes for the Catalyst 3750 Switch* (not orderable but available on Cisco.com)
- *Release Notes for the Catalyst 3750G Integrated Wireless LAN Controller Switch* (not orderable but available on Cisco.com)
- *Catalyst 3750 Switch Software Configuration Guide* (not orderable but available on Cisco.com). This guide provides a product overview and detailed descriptions and procedures of the switch software features.
- *Catalyst 3750 Switch Command Reference* (not orderable but available on Cisco.com). This reference provides detailed descriptions of the Cisco IOS commands specifically created or modified for the switch.
- *Catalyst 3750 Switch System Message Guide* (not orderable but available on Cisco.com). This guide provides descriptions of the system messages specifically created or modified for the switch.
- *Cisco Wireless LAN Controller Configuration Guide, Release 4.0* or later (not orderable but available on Cisco.com). This guide provides setup and configuration information for Cisco Wireless LAN Controllers.

10 Cisco Limited Lifetime 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/en/US/products/prod_warranties_listing.html

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:
78-6310-02C0
 - b. Select the language in which you would like to view the document.
 - c. Click **Go**.
The Cisco warranty page appears.
 - d. Read 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/cisco/web/support/index.html>

Duration of Hardware Warranty

A Cisco product hardware warranty is supported for as long as the original end user continues to own or use the product, provided that the fan and power supply warranty is limited to five (5) years. In the event of a discontinuance of product manufacture, the Cisco warranty support is limited to five (5) years from the announcement of the discontinuance.

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 the 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	



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

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

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

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the **Cisco Website at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE
Finland • France • Germany • Greece • Hong Kong SAR • 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 • Scotland • Singapore
Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2006 Cisco Systems, Inc. All rights reserved.

♻️ Printed in China
78-17540-01
DOC-7817540=