



## **QUICK START GUIDE**



### **Cisco 4400 Series Wireless LAN Controllers INCLUDING LICENSE AND WARRANTY**

- 1** About this Guide
- 2** Introduction to the Controller
- 3** Unpacking and Preparing the Controller for Operation
- 4** Using the Startup Wizard
- 5** Obtaining Documentation
- 6** Documentation Feedback
- 7** Cisco Product Security Overview
- 8** Obtaining Technical Assistance
- 9** Obtaining Additional Publications and Information
- 10** Cisco 90-Day Limited Hardware Warranty Terms

# 1 About this Guide

This guide is designed to help you install and minimally configure your Cisco 4400 Series Wireless LAN Controller. This guide covers the following controller models: 4402-25, 4402-50, 4404-25, 4404-50, and 4404-100.

## FCC Safety Compliance Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on.

Try to correct the interference by one or more of the following measures:

- Verify that the ambient temperature remains between 32 to 104• F (0 to 40• C), taking into account the elevated temperatures when installed in a rack or enclosed space.
- When multiple Cisco 4400 series controllers are mounted in an equipment rack, be sure that the power source is sufficiently rated to safely run all the equipment in the rack.
- Verify the integrity of the electrical ground before installing the controller.

## Safety Information

Safety warnings appear throughout this guide in procedures that may harm you if performed incorrectly. A warning symbol precedes each warning statement. The warnings below are general warnings that are applicable to the entire guide. Translated versions of the safety warnings in this guide are provided in the *Safety Warnings for Cisco 4400 Wireless LAN Controllers* document that accompanies this guide.



### Warning

---

**This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.** Statement 1071

---

**SAVE THESE INSTRUCTIONS**

---



## 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

---

## Statement 371—Power Cable and AC Adapter

接続ケーブル、電源コード、ACアダプタなどの部品は、必ず添付品または指定品をご使用ください。添付品・指定品以外の部品をご使用になると故障や動作不良、火災の原因となります。また、電気用品安全法により、当該法の認定（PSEとコードに表記）でなくUL認定（ULとコードに表記）の電源ケーブルは弊社が指定する製品以外の電気機器には使用できないためご注意ください。

## Statement 191—VCCI Class A Warning for Japan

### Warning

---

**This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.**

### 警告

---

VCCI 準拠クラスA機器（日本）

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

## 2 Introduction to the Controller

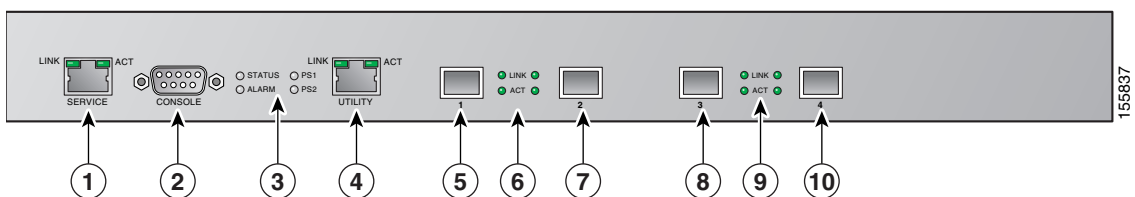
Cisco 4400 series wireless LAN controllers offer the highest level of performance and scalability for large scale enterprise wireless LAN deployments. In addition, these controllers deliver wireless LAN services over an existing Ethernet or IP infrastructure, thereby protecting existing network investments while providing the best in class wireless services. A core component of the Cisco unified wireless solution, these controllers deliver wireless security, intrusion detection, radio management, quality of service (QoS), and mobility across an entire enterprise. The controllers work in conjunction with other controllers, Cisco Wireless Control System (WCS), and access points to provide network managers with a robust wireless LAN solution.

In order to best use this guide, you should have already designed the wireless topology of your network. Because the radio resource management (RRM) feature automatically detects and configures access points as they appear on the network, it is not necessary to have any access points on the network to install and configure a controller.

Two versions of the 4400 series controller are available: 4402 and 4404 series controllers. Cisco 4402 controllers have two gigabit Ethernet distribution system ports, each of which is capable of managing up to 48 access points. However, Cisco recommends no more than 25 access points per port due to bandwidth constraints. The 4402-25 and 4402-50 models allow a total of 25 or 50 access points to join the controller. Cisco 4404 controllers have four gigabit Ethernet distribution system ports, each of which is capable of managing up to 48 access points. However, Cisco recommends no more than 25 access points per port due to bandwidth constraints. The 4404-25, 4404-50, and 4404-100 models allow a total of 25, 50, or 100 access points to join the controller.

Figure 1 shows the front panel layout of the 4400 series controller.

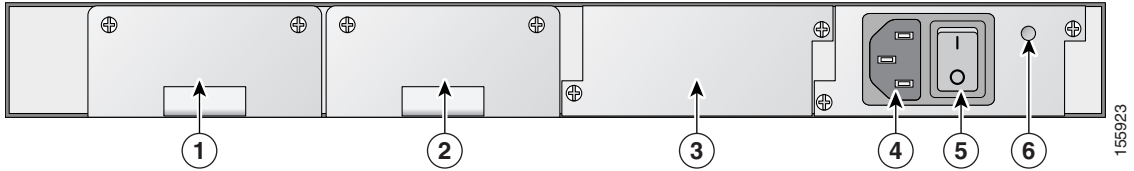
**Figure 1 Front Panel Layout**



<b>1</b>	Service port (RJ-45)	<b>6</b>	Distribution port 1 & 2 Link and Activity LEDs
<b>2</b>	Console port (DB-9 female)	<b>7</b>	Distribution port 2
<b>3</b>	Status, alarm, and power supply LEDs	<b>8</b>	Distribution port 3
<b>4</b>	Utility port (RJ-45)	<b>9</b>	Distribution port 3 & 4 Link and Activity LEDs
<b>5</b>	Distribution port 1	<b>10</b>	Distribution port 4

Figure 2 shows the back panel layout with a power supply unit installed in power supply slot 2.

**Figure 2 Back Panel Layout**



<b>1</b>	VPN termination module Slot 1	<b>4</b>	Slot 2 power supply power receptacle
<b>2</b>	VPN termination module slot 0	<b>5</b>	Slot 2 power supply switch
<b>3</b>	Power supply slot 1	<b>6</b>	Slot 2 power supply LED

## Checking the Controller LEDs

If your controller is not working properly, check the LEDs on the front panel of the unit. You can use the LED indications to quickly assess the unit’s status. The LED indicators are described in

**Table 1 LED Indicators**

Front Panel LEDs	
LED	Description
Service Port link	Solid green indicates service port link is established.
Service Port activity	Blinking green indicates link data transmission over the service port.
PS1 and PS2	Solid green indicates power supply # is operational.
Alarm	Solid red indicates an undervoltage condition detected on one of the DC/DC converters. Off indicates normal operation. This LED behavior may also be defined by the controller software.
Status	Solid green followed by blinking green indicates controller is rebooting or loading software. Off indicates normal operation. After the controller resets, the LED behavior is defined by the controller software.
Ethernet link	Solid green indicates Ethernet link to wired network is established.
Ethernet activity	Blinking green indicates data transmission over the Ethernet link
Distribution port link	Solid green indicates link established on distribution port # link.

**Table 1**     *LED Indicators (continued)*

<b>Front Panel LEDs</b>	
Distribution port activity	Blinking green indicates data transmission on distribution port # link.
<b>Rear Panel LEDs</b>	
<b>LED</b>	<b>Description</b>
Power supply unit	Solid white indicates normal operation. Solid red indicates a fault.

## 3 Unpacking and Preparing the Controller for Operation

Follow these steps to unpack the 4400 series controller and prepare it for operation:

- 
- Step 1**    Open the shipping container and carefully remove the contents.
  - Step 2**    Return all packing materials to the shipping container and save it.
  - Step 3**    Ensure that all items listed in the “Package Contents” section are included in the shipment. Check each item for damage. If any item is damaged or missing, notify your authorized Cisco sales representative.
- 

### Package Contents

Each access point package contains the following items:

- Cisco 4400 series wireless LAN controller and power cord
- Mounting hardware kit
- Translated Safety Warnings for Cisco 4400 Series Wireless LAN Controllers
- This guide
- Cisco product registration and Cisco documentation feedback cards

## Required Tools and Information

You will need the following tools and information before you can install the controller:

- Wireless LAN controller hardware
  - Controller with factory-supplied power cord and mounting hardware
  - Network, operating system service network, and access point cables as required
- Command-line interface (CLI) console
  - VT-100 terminal emulator on CLI console (PC, laptop, or palmtop)
  - Null modem serial cable to connect CLI console and controller
- Local TFTP server (required for downloading operating system software updates). Cisco uses an integral TFTP server. This means that third-party TFTP servers cannot run on the same workstation as the Cisco WCS because Cisco WCS and third-party TFTP servers use the same communication port.

## Initial System Configuration Information

Obtain the following initial configuration parameters from your wireless LAN or network administrator:

- A system (controller name).
- An administrative username and password. The default administrative username and password are *admin* and *admin*, respectively.
- A service port interface IP address configuration protocol (none or DHCP).
- A management interface (DS Port or network interface port) IP address.



---

**Note** The service port interface and management interface must be on different subnets.

---

- A management interface netmask address.
- A management interface default router IP address.
- A VLAN identifier if the management interface is assigned to a VLAN, or 0 for an untagged VLAN.
- Distribution system physical port number
  - 4402: 1–2 for front panel GigE ports
  - 4404: 1–4 for front panel GigE ports
- IP address of the default DHCP server that will supply IP addresses to clients.
- The lightweight access point protocol (LWAPP) transport mode (Layer 2 or Layer 3).

- A virtual gateway IP address (a fictitious, unassigned IP address, such as 1.1.1.1, used by all Cisco wireless LAN controller Layer 3 security and mobility managers).
- A Cisco wireless LAN controller mobility group name, if required.
- An 802.11 network name (SSID) for WLAN 1. This is the default SSID that the access points use when they join with the controller.
- Whether or not to allow static IP addresses from clients.
  - Yes is more convenient, but has lower security (session can be hijacked).
  - No is less convenient, but has higher security and works well for Windows XP devices.
- RADIUS server IP address, communications port, and secret (if you are configuring a RADIUS server).
- The country code for this installation. Refer to the *Cisco Wireless LAN Controller Configuration Guide* for country code information. This guide is available at [cisco.com](http://cisco.com).
- Status of the 802.11a, 802.11b, and 802.11g networks (enabled or disabled).
- Status of radio resource management (RRM) (enabled or disabled).

## Choosing a Physical Location

You can install the controller almost anywhere, but it is more secure and reliable if you install it in a secure equipment room or wiring closet. For maximum reliability, mount the controller using the following guidelines:



### Warning

---

**To prevent the system from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of:  
104• F (40• C)** Statement 1047

---



### Warning

---

**To prevent airflow restriction, allow clearance around the ventilation openings to be at least:  
4-in (10.16 cm)** Statement 1076

---



### Warning

---

**Take care when connecting units to the supply circuit so that wiring is not overloaded.** Statement 1018

---

- Make sure you can reach the controller and all cables attached to it.
- Make sure that water or excessive moisture cannot get into the controller.

- Make sure that the controller is within 328 ft. (100 m) of equipment connected to a 1000BASE-T port.
- Make sure the controller is within one of the following distances of equipment connected to the optional 1000BASE-SX or -LX port:
  - 722 ft. (220 m) when using 160 MHz-km rated 62.5/125 um multimode fiber.
  - 902 ft. (275 m) when using 200 MHz-km rated 62.5/125 um multimode fiber.
  - 1312 ft. (400 m) when using 400 MHz-km rated 50/125 um multimode fiber.
  - 1641 ft. (500 m) when using 500 MHz-km rated 50/125 um multimode fiber.



---

**Note** These distances depend on the small form factor pluggable (SFP) gigabit converter being used. Refer to the Gigabit Interface Converter (GBIC) Module and Small Form-Factor Pluggable (SFP) GBIC Module Install. Info. and Specifications, at [http://www.cisco.com/en/US/products/hw/routers/ps341/prod\\_module\\_installation\\_guid\\_e09186a00801cc731.html](http://www.cisco.com/en/US/products/hw/routers/ps341/prod_module_installation_guid_e09186a00801cc731.html)

---

The 1000BASE-SX SFP modules provide 1000 Mbps wired connections to a network through 850nm (SX) fiber-optic links using LC physical connectors. The 1000BASE-LX SFP modules provide 1000 Mbps wired connections to a network through 1300nm (LX/LH) fiber-optic links using LC physical connectors.

## Installing the Chassis

The controller ships with rack mounting ears attached and the desktop or shelf mounting rubber feet in a separate bag. Follow these guidelines when mounting the controller:

- When mounting the controller on a desktop or shelf, attach the rubber feet to the bottom of the controller chassis, and place the chassis on any secure horizontal surface. If desired, you can remove the rack mounting ears from the controller.
- When mounting the controller in an EIA standard rack, attach the ears to the equipment rack using the factory supplied fasteners.



---

**Caution** The controller weighs 15.2 lbs (6.95 kg). For safety, two or more people must work together to perform the rack mount installation.

---

- Install the SFP modules as described in the *1000BASE-SX, 1000BASE-LX, and 1000BASE-T SFP Module Quick Start Guide*.
- If you have purchased an extra power supply module or enhanced security modules, refer to the *Cisco 4400 Series Power Supply Quick Start Guide* for information about installing these devices.

**Warning**

**This unit might have more than one power supply connection. All connections must be removed to de-energize the unit.** Statement 1028

---

## Connecting the Controller's Console Port

Before you can configure the controller for basic operations, you need to connect it to a PC that uses a VT-100 terminal emulator (such as HyperTerminal, ProComm, Minicom, or Tip).

Follow these steps to connect the PC to the controller's console port:

- 
- Step 1** Plug the RJ-45 connector on a null-modem serial cable into the controller's console port and the other end of the cable into the PC's serial port.
- Step 2** Start the PC's terminal emulation program.
- Step 3** Configure the terminal emulation program for the following parameters:
- 9600 baud
  - 8 data bits
  - No flow control
  - 1 stop bit
  - No parity
- 

## Running the Bootup Script and Power-On Self Test

When you plug the controller into an AC power source, the bootup script initializes the system, verifies the hardware configuration, loads its microcode into memory, verifies its operating system software load, and initializes itself with its stored configurations. Before performing this test, you should have connected your PC to the controller's CLI console as described in the "Connecting the Controller's Console Port" section on page 10. Follow these steps to run the bootup script and conduct the power-on self test (POST).

- 
- Step 1** Plug an AC power cord into the back of the controller and connect the other end to a grounded 100 to 240 VAC, 50/60 Hz electrical outlet.

**Note**

If you wish to run a previous release of the controller code, press Esc immediately after the Model and S/N line appears. The Bootloader Options menu appears.

**Step 2** Observe the bootup using the CLI screen.

The bootup script displays operating system software initialization (code download and POST verification) and basic configuration as shown in the following sample bootup display:

```
Bootloader 3.4.0.0. (Feb 2 2006 - 19:14:47)

Motorola PowerPC ProcessorID=00000000 Rev. PVR=80200020
Cisco Systems INC., 4400 Wireless LAN Switch Board
  CPU: 833 MHz
  CCB: 333 MHz
  DDR: 166 MHz
  LBC: 41 MHz
L1 D-cache 32KB, L1 I-cache 32KB enabled.
I2C: ready
DTT: 1 is 22 C
DRAM: DDR module detected, total size: 512MB.
512MB
8540 in PCI Host Mode.
8540 is the PCI Arbiter.

Memory Test PASS

FLASH:
  Flash Bank 0: portsize = 2, size 8 MB in 142 Sectors
  8 MB
L2 cache enabled: 256KB
Card Id: 1541
Card Revision Id: 1
Card CPU Id: 1725
Number of MAC addresses: 32
Number of Slots supported: 4
Serial Number: 12345678-12345678-1244
Manufacturers ID: 30464
Board Maintenance Level: 00
Number of supported APs: 24
In: serial
Out: serial
Err: serial
```

```
.o88b. d888888b .d8888. .o88b. .d88b.
d8P Y8 `88' 88' YP d8P Y8 .8P Y8.
8P      88  `8bo. 8P      88  88
8b      88  `Y8b. 8b      88  88
Y8b d8  .88.  db  8D Y8b d8 `8b d8'
`Y88P' Y888888P `8888Y' `Y88P' `Y88P'
Model WS-C3750G-24PS-W24 S/N: 12345678-12345678-12345
```

Net:

```
PHY DEVICE: Found Intel LXT971A at 0x01
FEC ETHERNET
IDE: Bus 0: OK
    Device 0: Model: TOSHIBA THNCF256MBA Firm: 2.20
    Type: Removable Hard Disk
    Capacity: 244.5 MB = 0.2 GB (500736 x 512)
Device 1: not available
```

Booting Primary Image...

Press <ESC> now for additional boot options...

### Step 3 If desired, press Esc to display the Bootloader Boot Options menu.

```
Boot Options
Please choose an option from below:
 1. Run primary image
 2. Run backup image
 3. Manually update images
 4. Change active boot image
 5. Clear Configuration
Please enter your choice:
```



---

**Note** Enter 1 to run the current software, enter 2 to run the previous software, or enter 5 to run the current software and set the controller configuration to factory defaults. Do not enter 3 or 4 unless directed to do so.

---

Detecting Hardware . . .

### Step 4 The rest of the is process takes two to three minutes. Do not reboot the controller until the user login prompt appears.

```
Cisco is a trademark of Cisco Systems, Inc.
Software Copyright Cisco Systems, Inc. All rights reserved.
```

```
Cisco AireOS Version 3.4.0.0
Initializing OS Services: ok
```

```
Initializing Serial Services: ok
Initializing Network Services: ok
Starting ARP Services: ok
Starting Trap Manager: ok
Starting Network Interface Management Services: ok
policyBuildDefaultConfigData: Setting default LWAPP MODE to L3
policySysReadConfig: policySystemLwappModeSet(L3)
Starting System Services: ok
Starting Fast Path Hardware Acceleration: ok
Starting Switching Services: ok
Starting QoS Services: ok
Starting Policy Manager: ok
Starting Data Transport Link Layer: ok
Starting Access Control List Services: ok
Starting System Interfaces: ok
Starting LWAPP: ok
Starting Crypto Accelerator[s]: None Present
Starting Certificate Database: ok
Starting VPN Services: ok
Starting Security Services: ok
Starting Policy Manager: ok
Starting Authentication Engine: ok
Starting Mobility Management: ok
Starting Virtual AP Services: ok
Starting AireWave Director: ok
Starting Network Time Services: ok
Starting Broadcast Services: ok
Starting Logging Services: ok
Starting DHCP Server: ok
Starting IDS Signature Manager: ok
Starting External Policy Interface: ok
Starting RFID Tag Tracking: ok
Starting Power Supply and Fan Status Monitoring Service: ok
Starting WLAN Control Protocol (WCP): wcpSysInit: Out of factory boot:
Initialize ports and IP address for interfaces
wcpSysInit: Setting IP address for MGMT interface OK
wcpSysInit: Setting LAG for MGMT interface OK
wcpSysInit: Setting IP address for AP_MGR interface OK
wcpSysInit: Setting IP address for OOB interface OK
wcpSysInit: simInterfacePortSet for OOB at LAG port successful
wcpTask: osapiSetsockopt for AF_BSNET_OPTS success
wcpTask: Shrunk loopback interface's range to 127.0.0.0/24
Set status line to 1
wcpSysInit: wcpSysInit(): initializing wcp...Done
ok
```

```
Starting Management Services:
Web Server: ok
CLI: ok
Secure Web: ok
```

- Step 5** If the controller passes the power-on self test, the bootup script runs the Startup Wizard, which prompts you for basic configuration inputs.
- 

## 4 Using the Startup Wizard

Before you can use the startup wizard, you must obtain the information discussed in the “Required Tools and Information” section on page 7. Follow these steps to use the Startup Wizard to configure the controller for basic operation.



**Note** The available options appear in brackets after each configuration parameter. The default value appears in all uppercase letters.

---



**Note** Press the hyphen key if you ever need to return to the previous command line.

---

- Step 1** Enter the system name, which is the name you want to assign to the controller. You can enter up to 32 ASCII characters.
- Step 2** Enter the administrative username and password to be assigned to this controller. You can enter up to 24 ASCII characters for each. The default administrative username and password are *admin* and *admin*, respectively.
- Step 3** If you want the controller’s service-port interface to obtain an IP address from a DHCP server, enter **DHCP**. 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, enter **none**.



**Note** The *service-port interface* controls communications through the service port. Its IP address must be on a different subnet from the management and AP-manager interfaces. This configuration enables you to manage the controller directly or through a dedicated management network to ensure service access during network downtime.

---

- Step 4** If you entered **none** in Step 3, enter the IP address and netmask for the service-port interface on the next two lines.

**Step 5** Enter the IP address, netmask, default router IP address, and optional VLAN identifier (a valid VLAN identifier or 0 for an untagged VLAN) for the management interface.



---

**Note** The VLAN identifier should be set to match the switch interface configuration.

---

**Step 6** Enter the IP address of the default DHCP server that will supply IP addresses to clients, the controller's management interface, and optionally the service-port interface.



---

**Note** The *management interface* is the default interface for in-band management of the controller and connectivity to enterprise services such as AAA servers.

---

**Step 7** Enter the IP address of the controller's AP-manager interface.



---

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

---



---

**Note** 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 8** Enter the IP address of the controller's virtual interface, which will 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.



---

**Note** 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 9** If desired, enter the name of the mobility group/RF group to which you want the controller to belong.

**Note**

---

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 vice versa. However, a *mobility group* facilitates scalable, system-wide mobility and controller redundancy while an *RF group* facilitates scalable, system-wide dynamic RF management.

---

- Step 10** Enter the network name, or *service set identifier (SSID)*. The initial SSID enables basic functionality of the controller and allows access points that have joined the controller to enable their radios.
- Step 11** Enter **yes** to allow clients to assign their own IP address or **no** to make clients request an IP address from a DHCP server.
- Step 12** To configure a RADIUS server now, enter **yes** and then enter the IP address, communication port, and secret key of the RADIUS server. Otherwise, enter **no**.
- Step 13** Enter the code for the country in which the controller will be used.

**Note**

---

Enter **help** to view the list of available country codes.

---

- Step 14** Enter **yes** to enable or **no** to disable each of the 802.11b, 802.11a, and 802.11g lightweight access point networks.
- Step 15** Enter **yes** to enable or **no** to disable the controller's radio resource management (RRM) auto RF feature.

**Note**

---

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 transmit power assignment, for the group.

---

The controller saves your configuration, reboots, and prompts you to log in.

---

## Logging into the Controller

Follow these steps to log into the controller.

---

- Step 1** Enter a valid username and password to log into the controller CLI.

**Note**

The administrative username and password you created in the Startup Wizard are case sensitive.

**Step 2** The CLI displays the root level system prompt:

```
 #(system prompt) >
```

The system prompt can be any alphanumeric string up to 31 characters. You can change it by entering the **config prompt** command.

**Note**

The CLI automatically logs you out without saving any changes after 5 minutes of inactivity. You can set the automatic logout from 0 (never log out) to 160 minutes using the **config serial timeout** command.

**Note**

Cisco Aironet lightweight access points do not connect to the 4400 series controller if the date and time are not set properly. Set the current date and time on the controller before allowing the access points to connect to it.

## Verifying Interface Settings and Port Operation

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

**Step 1** Enter **show interface summary**. The controller's current interface configurations appear:

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

**Note**

Link aggregation (LAG) is enabled by default on the integrated wireless LAN controller. LAG bundles all of the controller's distribution system ports into a single IEEE 802.3ad port channel. Refer to the *Cisco Wireless LAN Controller Configuration Guide* for more information.

**Step 2** Enter **show port summary**. The following information appears, showing the status of the controller's distribution system ports, which serve as the data path between the controller and Cisco lightweight access points and to which the controller's 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* indicates that the controller's ports are fully operational.

## Connecting the Network (Distribution System)

### Model 4402 Controllers

Up to two of the following connections are supported in any combination:

- 1000BASE-T (GigE, front panel, RJ-45 physical port, UTP cable).
- 1000BASE-SX (GigE, front panel, LC physical port, multi-mode 850nm (SX) fiber-optic links using LC physical connectors).
- 1000BASE-LX (GigE, front panel, LC physical port, multi-mode 1300nm (LX/LH) fiber-optic links using LC physical connectors).

### Model 4404 Controllers

Up to four of the following connections are supported in any combination:

- 1000BASE-T (GigE, front panel, RJ-45, physical port, UTP cable).
- 1000BASE-SX (GigE, front panel, LC physical port, multi-mode 850nm (SX) fiber-optic links using LC physical connectors).
- 1000BASE-LX (GigE, front panel, LX physical port, multi-mode 1300nm (LX/LH) fiber optic links using LC physical connectors).

Depending on the distribution system physical port to be assigned, use Ethernet Category 5 or higher cables or SX/LX/LH compatible fiber-optic cables to connect the network equipment to the controller.

## Connecting the Switch's Service Port (Optional)

The service port is controlled by the service-port interface and is reserved for out-of-band management of the controller and system recovery and maintenance in the event of a network failure. The service-port interface enables the controller to be managed on an interface different from the one used for your network traffic. Use of the service port is optional.

You can perform out-of-band controller management from a PC running a terminal emulation program or a PC running Cisco WCS, a network management tool that enables you to configure and monitor a network of controllers, or the controller GUI. However, you must first connect the PC to the switch's service port in one of two ways:

- Use a shielded, twisted-pair cross-over cable to connect the PC directly to the switch's service port.
- For a remote connection (using Telnet or SSH) through a dedicated management network, use a Category 5, Category 5e, Category 6, or Category 7 Ethernet cable to connect the management network to the switch's service port and the appropriate cable to connect the PC to the management network.

## Connecting Access Points

After you have configured the controller, use Category-5, Category-5e, Category-6, or Category-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 an access point, it records the access-point MAC address in its database. The controller radio resource management (RRM) feature then automatically configures the access point to start sending and allowing clients to associate.

You have prepared the controller for basic operation. Refer to the *Cisco Wireless LAN Controller Configuration Guide, Release 3.4*, for information on configuring the controller to meet the specific needs of your wireless network.

## Installing a Power Supply Unit

The controller can be powered using one or two power supply units. When the controller is equipped with two power supply units, the power supplies are redundant. Either power supply continues to power the controller should the other power supply unit fail. Also, the power supplies are hot swappable; you do not need to remove power from the controller to replace one or both power supplies.

One power supply unit is installed in slot 2 at the factory. You can order a second power supply unit and install it in slot 1.

## Tools and Equipment Required

To install a power supply unit, you need the following tools and equipment:

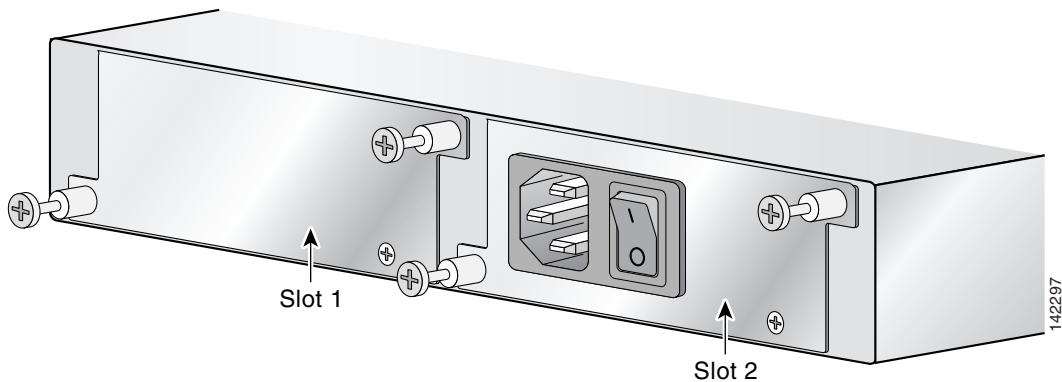
- A power supply unit
- A number 1 Phillips screwdriver

Follow these steps to install a power supply unit.

---

**Step 1** Locate the empty power supply slot on the controller's back panel. See Figure 3.

**Figure 3** Controller Power Supply Slots



---

**Note** The power supply units are hot swappable.

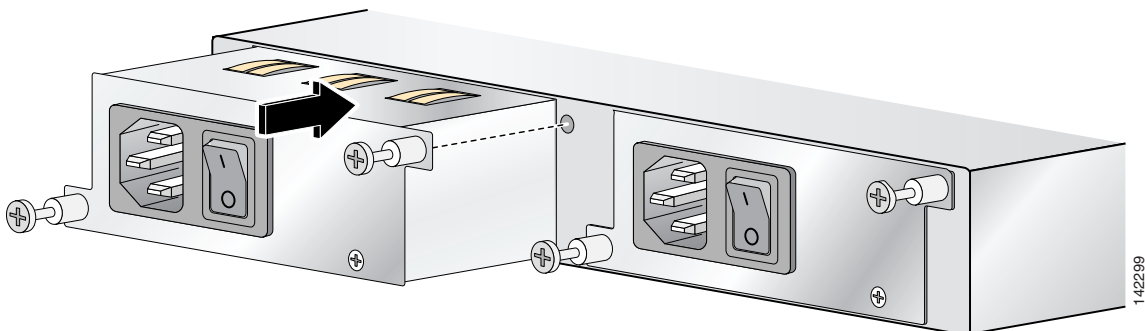
---

**Step 2** Use a Phillips screwdriver to loosen the captive screws on the slot cover.

**Step 3** Remove the slot cover and store it in a safe place for future use.

**Step 4** Align the power supply unit with the slot so that the unit's power input receptacle is on the left side of the slot. See Figure 4.

**Figure 4** *Inserting the Power Supply*



- Step 5** Gently but firmly push the power supply unit into the slot until it is firmly seated in the card electrical connector.
- Step 6** Use a Phillips screwdriver to tighten the captive screws. Do not overtighten.
- Step 7** Plug the power cord into the power supply unit and the other end into a grounded 95 to 260 VAC 50/60 Hz electrical outlet.
- Step 8** Make sure that both power supply units are turned on.
- 

## Installing a VPN Termination Module

VPN termination modules provide extra processing power needed to support the termination of client VPN sessions on the controller. You can order these modules and install them in all 4400 series controllers.

### Required Tools and Equipment

To install a VPN termination module, you need the following tools and equipment:

- One or two VPN termination modules.
- A standard screwdriver or a number 2 Phillips screwdriver.

Follow these steps to install a VPN termination module.



#### **Caution**

If you are installing a VPN termination module in a model 4402 controller, install the module in slot 0. On the model 4404 controller, you can install the module in either slot.

---

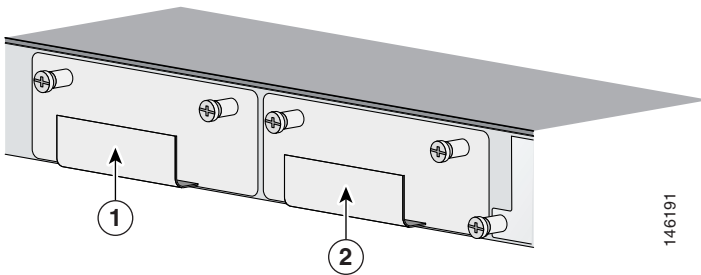
- Step 1** Remove all power from the controller.
- Turn the power switch off.
  - Remove the power cord from the power supply unit power receptacle.



**Caution** If your controller is equipped with two power supply units, remove both power cords.

- Step 2** Locate the VPN termination module slot on the rear panel of the controller. See Figure 5.

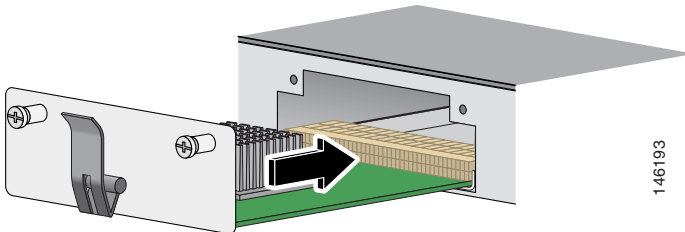
**Figure 5** VPN Termination Module Slots



<b>1</b>	VPN termination module slot 1	<b>2</b>	VPN termination module slot 0
----------	-------------------------------	----------	-------------------------------

- Step 3** Use a standard or Phillips screwdriver to unscrew the captive screws on the slot cover.
- Step 4** Remove the slot cover and store it in a safe place for future use.
- Step 5** Insert the module into the slot as shown in Figure 6.

**Figure 6** Inserting the VPN Termination Module



- Step 6** Gently but firmly push the module into the slot until it seats in the card electrical connector.

**Step 7** Use a standard or Phillips screwdriver to tighten the captive screws. Do not overtighten.

**Step 8** Restore all power to the controller.

- a. Insert the power cord into the controller power supply unit. If your controller is equipped with two power supply units, insert both power cords.
  - b. Plug the power cords into a grounded 95 to 260 VAC 50/60 Hz electrical outlet.
  - c. Turn the power supply units on.
- 

## 5 Obtaining Documentation

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

### Cisco.com

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

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

### Product Documentation DVD

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

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

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

## Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

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

## 6 Documentation Feedback

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

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

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

We appreciate your comments.

## 7 Cisco Product Security Overview

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

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

From this site, you will find information about how to:

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

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

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

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](http://www.cisco.com/en/US/products/products_psirt_rss_feed.html)

## Reporting Security Problems in Cisco Products

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

- For Emergencies only—[security-alert@cisco.com](mailto:security-alert@cisco.com)

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

- For Nonemergencies—[psirt@cisco.com](mailto:psirt@cisco.com)

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

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



### Tip

---

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

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

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

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

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

---

## 8 Obtaining Technical Assistance

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

### Cisco Technical Support & Documentation Website

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

<http://www.cisco.com/techsupport>

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

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



#### Note

---

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

---

### Submitting a Service Request

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

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

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

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

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

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

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

## Definitions of Service Request Severity

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

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

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

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

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

## 9 Obtaining Additional Publications and Information

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

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

<http://www.cisco.com/go/guide>

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:  
<http://www.cisco.com/go/marketplace/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:  
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:  
<http://www.cisco.com/packet>

## 10 Cisco 90-Day Limited Hardware Warranty Terms

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

1. Launch your browser, and go to this URL:  
[http://www.cisco.com/univercd/cc/td/doc/es\\_inpk/cetrans.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpk/cetrans.htm)  
The Warranties and License Agreements page appears.
2. To read the *Cisco Information Packet*, follow these steps:
  - a. Click the **Information Packet Number** field, and make sure that the part number 78-5235-03B0 is highlighted.
  - b. Select the language in which you would like to read the document.
  - c. Click **Go**.

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

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



### Note

You must have Adobe Acrobat Reader to view and print PDF files. You can download the reader from Adobe's website: <http://www.adobe.com>

3. To read translated and localized warranty information about your product, follow these steps:
  - a. Enter this part number in the Warranty Document Number field:  
78-5236-01C0
  - b. Select the language in which you would like to read the document.
  - c. Click **Go**.  
The Cisco warranty page appears.
  - d. Review the document online, or click the **PDF** icon to download and print the document in Adobe Portable Document Format (PDF).

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

[http://www.cisco.com/public/Support\\_root.shtml](http://www.cisco.com/public/Support_root.shtml).

### **Duration of Hardware Warranty**

Ninety (90) days.

### **Replacement, Repair, or Refund Policy for Hardware**

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

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

### **To Receive a Return Materials Authorization (RMA) Number**

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

Complete the information below, and keep it for reference:

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







**Americas Headquarters**  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://www.cisco.com)  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
168 Robinson Road  
#28-01 Capital Tower  
Singapore 068912  
[www.cisco.com](http://www.cisco.com)  
Tel: +65 6317 7777  
Fax: +65 6317 7799

**Europe Headquarters**  
Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
[www-europe.cisco.com](http://www-europe.cisco.com)  
Tel: 31 0 800 020 0791  
Fax: 31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0809R)

© 2008 Cisco Systems, Inc. All rights reserved.

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