Installing the Cisco 3504 Wireless Controller

This chapter describes how to install the Cisco 3504 Wireless Controller.

Warning IMPORTANT SAFETY INSTRUCTIONS

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

- Installation Guidelines and Safety Warnings, on page 1
- Unpacking and Inspecting the Controller, on page 3
- Package Contents, on page 3
- Requirements Tools and Information, on page 3
- Initial System Configuration Information, on page 4
- Configuring Management Interface, on page 5
- Choosing a Physical Location, on page 6
- Installing the Controller, on page 7

Installation Guidelines and Safety Warnings

This section includes the basic installation guidelines and safety warning statements. Read this section before you start the installation procedure. Translations of the warning statements appear in the RCSI guide on Cisco.com.

- This equipment is not suitable for use in locations where children are likely to be present.

Note The marking information is located at the bottom of the apparatus.

- The operating environment must be within the ranges listed in the "Environmental Specifications" section.
- Cabling is away from sources of electrical noise, such as radios, power lines, and fluorescent lighting fixtures. Make sure that the cabling is safely away from other devices that might damage the cables.

- Airflow around the device and through the vents is unrestricted
- Humidity around the device does not exceed 95 percent.
- Altitude at the installation site is not greater than 10,000 feet.
- Do not place any items on the top of the device.
- For 10/100/1000 fixed ports, the cable length from a switch to a connected device cannot exceed 328 feet (100 meters).
- Clearance to the switch front and rear panel 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.

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

Warning To prevent airflow restriction, allow clearance around the ventilation openings to be at least 50 mm (5 cm). **Statement 1076**

Warning Read the installation instructions before connecting the system to the power source. **Statement 1004**.

Warning Ultimate disposal of this product should be handled according to all national laws and regulations. **Statement 1040**.

Warning No user-serviceable parts inside. Do not open. **Statement 1073**.

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

Warning **Hot surface. Statement 1079.**

Unpacking and Inspecting the Controller

Follow these steps to unpack the Cisco 3504 Wireless Controller and prepare it for operation:

Procedure

Step 1 Remove the controller from its container and save all the packaging material.

Step 2 Compare the shipment to the equipment list provided by your Cisco customer service representative. Verify that you have all the items.

Step 3 Check for damage and report discrepancies or damage, if any, to your Cisco customer service representative. Before speaking to the representative, have the following information ready:

- Invoice number of shipper (see the packing slip)
- Model and serial number of the damaged unit
- Description of damage
- Effect of damage on the installation

Package Contents

Each Cisco 3504 Wireless Controller package contains the following items:

- One Cisco 3504 Wireless Controller
- One Power supply and power cord (power cord option configurable)
- Optional licenses will be pre-installed on controller at factory, if selected
- Cisco 3504 Wireless Controller software pre-loaded on the controller (software option configurable)
- Four adhesive rubber feet pieces

Requirements Tools and Information

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

- Wireless 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
  - Serial terminal emulator on CLI console (PC or laptop)

  - Mini-B USB console port
  - Use either RJ-45 console cable or Mini-B USB 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), such as controller. The system name can contain up to 32 printable ASCII characters.
- An administrative username and password, which can contain up to 24 printable ASCII characters.
- You must enter a username and password and the configured username and password cannot be the same.
- A management interface (DS Port or network interface port) IP address, such as 10.40.0.4.
- A management interface netmask address, such as 255.255.255.0.
- A management interface default router IP address, such as 10.40.0.5.
- A VLAN identifier if the management interface is assigned to a VLAN, such as 40 or 0 for an untagged VLAN.
- Configure the management interface port mapping to either of the following:
  - Port 5 if utilizing the mGig port to the DS
  - Appropriate Gigabit port number (1-4) to the DS
- A management interface DHCP server IP address, such as 10.40.0.6 (the IP address of the default DHCP server that will supply IP addresses to clients and the management interface.
- A virtual gateway IP address (a fictitious, unassigned IP address, such as 192.0.2.1, used by all Cisco wireless controller Layer 3 security and mobility managers).
- A Cisco wireless controller mobility or RF group name, such as rfgrp40 if required. An RF group name can contain up to 19 printable ASCII characters.
- An 802.11 network name (SSID), such as wlan1. An SSID can contain up to 32 printable, case-sensitive ASCII characters.
- DHCP bridging
- Whether or not to allow static IP addresses from clients, either Yes or No.
  - 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 devices.
- RADIUS server IP address, communications port, and secret if you are configuring a RADIUS server, such as 10.40.0.3, 1812, and mysecretcode.

- The country code for this installation. Enter help to see a list or refer to the Cisco Wireless LAN Controller Configuration Guide for country code information. This guide is available on Cisco.com.
- Status of the 802.11 networks, either enabled or disabled.
- Status of Radio Resource Management (RRM), either enabled or disabled.

Configuring Management Interface

When you save the controller's configuration, the controller stores it in XML format in flash memory. Controller software release 5.2 or later releases enable you to easily read and modify the configuration file by converting it to CLI format. When you upload the configuration file to a TFTP/FTP/SFTP server, the controller initiates the conversion from XML to CLI. You can then read or edit the configuration file in a CLI format on the server. When you are finished, you download the file back to the controller, where it is reconverted to an XML format and saved.

The controller does not support the uploading and downloading of port configuration CLI commands. If you want to configure the controller ports, enter these commands:

- **config port linktrap** {*port* | **all**} {**enable** | **disable**}—Enables or disables the up and down link traps for a specific controller port or for all ports.
- **configport adminmode** {*port* | **all**} {**enable** | **disable**}—Enables or disables the administrative mode for a specific controller port or for all ports.

The management interface is the default interface for in-band management of the controller and connectivity to enterprise services such as AAA servers. It is also used for communications between the controller and access points. The management interface has the only consistently “pingable” in-band interface IP address on the controller. You can access the GUI of the controller by entering the management interface IP address of the controller in the address field of either Internet Explorer or Mozilla Firefox browser.

Following are the steps to configure the management interface:

Procedure

Step 1 Enter the show interface detailed management command to view the current management interface settings.

Note The management interface uses the controller’s factory-set distribution system MAC address.

Step 2 Enter the **config wlan disable** *wlan-id* command to disable each WLAN that uses the management interface for distribution system communication.

Step 3 Enter these commands to define the management interface:

- **config interface address management** *ip-addr ip-netmask gateway*
- **config interface quarantine vlan** *management-interface vlan-id*

  Note Use the config interface quarantine vlan management vlan_id command to configure a quarantine VLAN on the management interface.

- **config interface vlan management** {*vlan-id* | *0*}

Note Enter 0 for an untagged VLAN or a nonzero value for a tagged VLAN. We recommend using tagged VLANs for the management interface.

- **config interface port management** *physical-ds-port-number*
- **config interface dhcp management primary** *ip-address-of-primary-dhcp-server* [**secondary** *ip-address-of-secondary-dhcp-server*]
- **config interface acl management** *access-control-list-name*

Step 4 Enter the **save config** command.

Step 5 Enter the **show interface detailed management** command to verify that your changes have been saved.

Step 6 If you made any changes to the management interface, enter the **reset system** command to reboot the controller for the changes to take effect.

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 while following these guidelines:

- 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.
- To prevent airflow restriction, allow clearance around the ventilation openings to be at least 50 mm (5 cm).
- Verify that the ambient temperature remains between 32° F to 104° F (0° C to 40° C).
- Make sure that the controller is within 328 ft. (100 m) of equipment connected to the 10/100/1000 Mbps Ethernet ports.
- Make sure that the power supply adapter and the power cord can reach a 100 to 240 VAC grounded electrical outlet.

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 This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than 20A. **Statement 1005**.

Installing the Controller

Mounting the Controller

This section describes the various mounting options for the controller:

Mounting the Controller on Desktop or Shelf

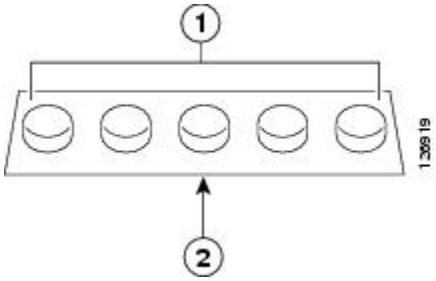
Before mounting the controller on a desktop or shelf, install the rubber feet located in accessory kit shipped with the controller.

To install the rubber feet to the controller, follow these steps:

Procedure

Step 1 Locate the rubber feet on the black adhesive strip that is shipped with the controller.

Figure 1: Identifying the Rubber Feet

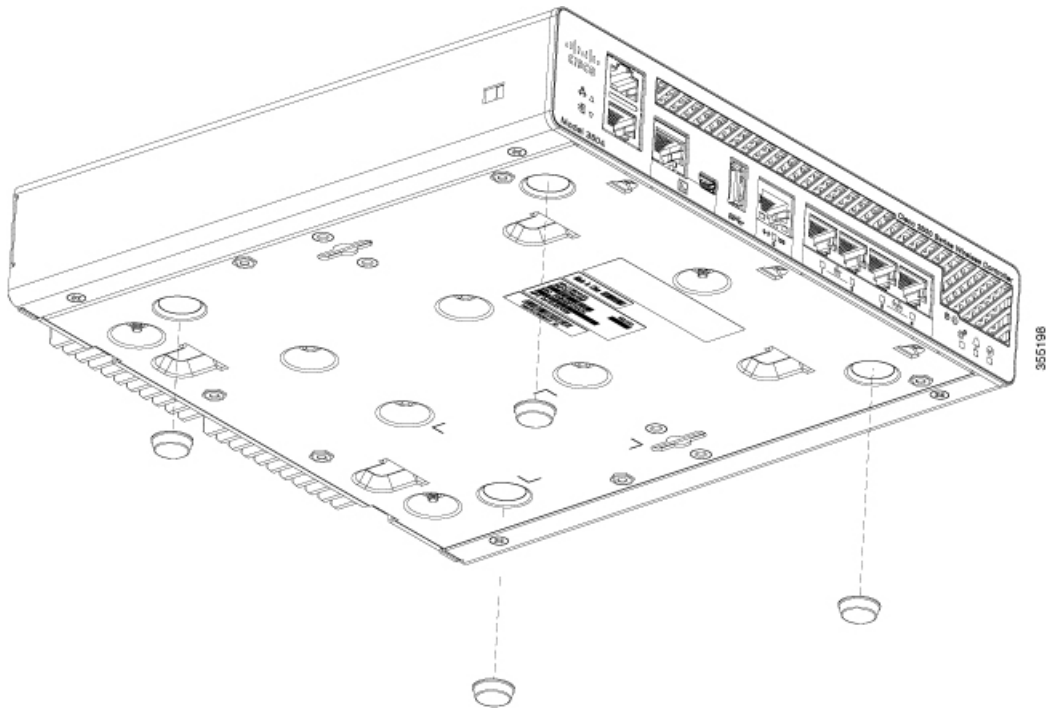


1	Rubber feet	2	Black adhesive strip

Step 2 Place the controller upside down, on a smooth, flat surface.

Step 3 Peel off the rubber feet from the black adhesive strip and press them adhesive-side down onto the bottom four corners of the controller, see the figure below:

Figure 2: Attaching the Rubber Feet



Step 4 Place the controller right-side up on a flat, smooth, secure surface.

Step 5 Connect the interface cables.

Mounting the Controller on a Wall

Note Do not wall-mount the device with its front panel facing up. Following safety regulations, wall-mount the device with its front panel facing down or to the side to prevent airflow restriction and to provide easier access to the cables.

Warning Read the wall-mounting carefully before beginning installation. Failure to use the correct hardware or to follow the correct procedures could result in a hazardous situation to people and damage to the system. **Statement 378**.

Note Wall mounting screws are not supplied with the product. We recommend that the installer supply appropriate screws in accordance with the local codes.

The controller wall-mount holes located at the bottom of the enclosure fit standard #6 or M3 pan head screw. The type of screw used to mount the controller to the wall must follow the local guidelines for wall type and material.

To mount the controller on a wall using mounting screws, follow these steps:

Procedure

Step 1 Mark the location of the mounting screws on the wall. Use the mount hole locations on the back of the controller for placement of the mounting screws.

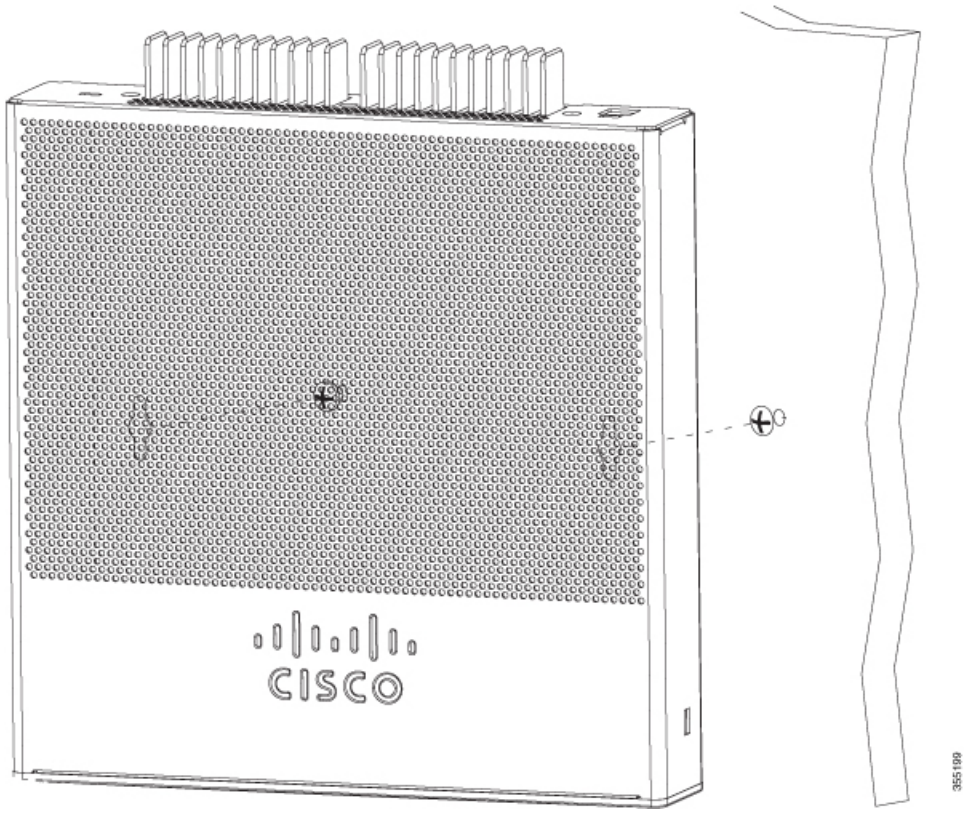
Mounting screw spacing is 5 7/16 inch (138 mm).

Step 2 Install two screws and tighten until the top of the screws are 1/8 inch (3 mm) from the wall (leaving enough room for the back panel to slide onto the screws firmly).

Step 3 Place the controller onto the mounting screws and slide it down until it lock into place, as shown in figure below:

Note The front panel of the controller should be facing down.

Figure 3: Place the Controller on the Mounting Screws



Step 4 After the controller is mounted on the wall, perform the following tasks to complete the installation

- Connecting the Controller Console Port
- Securing the Power Adapter Cable
- Connecting to the Network

Step 5 For configuration instructions about using the CLI setup program, see the (Link to Running the Bootup script section).

Rack Mounting the Controller

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

To mount the controller in a 19-inch equipment rack, you can order an optional Optional Rack Mount kit (AIR-CT3504-RMNT= Cisco 3504 Wireless Controller Rack Mount Tray).

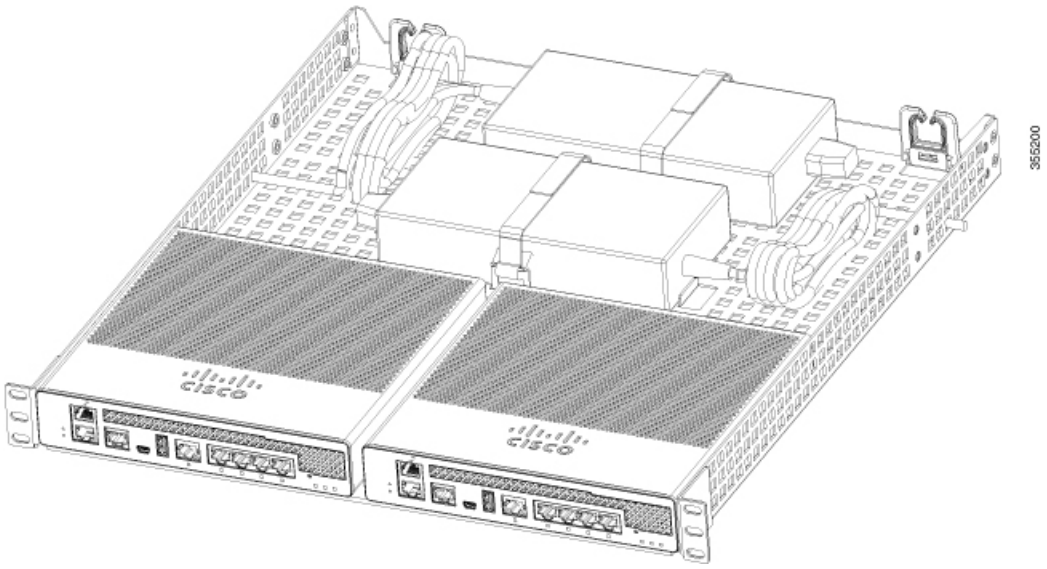
The rack-mount tray is designed for tool-less assembly. To rack-mount the controller, perform the following steps:

Procedure

Step 1 Remove the four rubber feet if previously installed.

Step 2 Slide the Cisco 3504 Wireless Controller in position such that the 4-tray tabs align and latch into the bottom of the unit as it is pushed in place. The front of the Cisco 3504 Wireless Controller should be flush against the front edge of the tray. A nylon latch in the center of the tray snaps into and locks the Cisco 3504 Wireless Controller in place.

Figure 4: Placing the Controller on the Rack Mount Tray

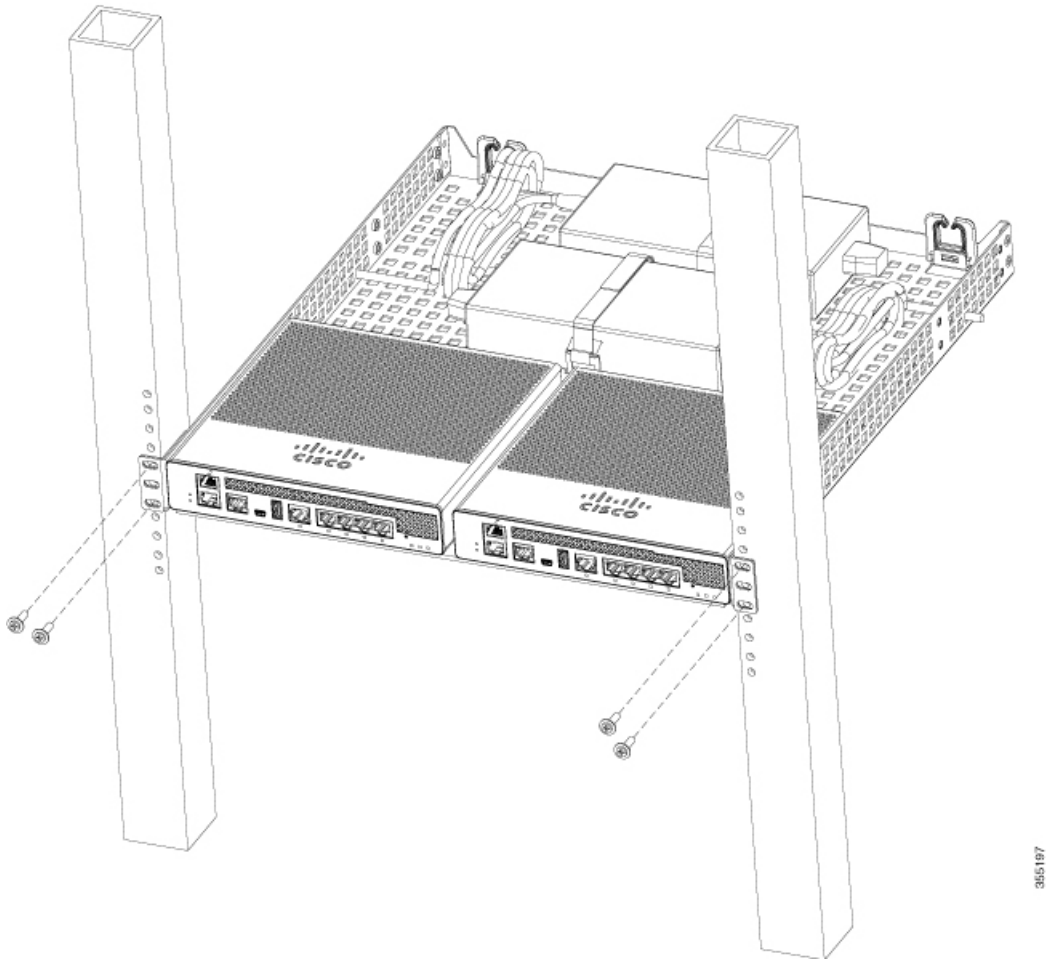


Step 3 Place the power adapters between either of the two tabs in the rear of the tray and use the provided velcro straps to secure them.

Step 4 Route the AC wiring through the cable management clips.

Step 5 Attach the rack mount tray to the rack using the supplied screws, as shown in figure below:

Figure 5: Attaching the Rack Mount Tray to the Rack



To remove the chassis from the rack, remove the screws that attach the chassis to the rack, and then remove the chassis.

Step 6 If required, install rear rack mount braces for additional stability.

Include optional orderable rear rack mount adapter kit: 53-3544-05 ACCKIT, SPARE PART, RKMNT, REAR, C4948E(-F).

Reuse 69-2237-05 or later, MECHKIT, ACCY,RKMNT, REAR, C4948E(-F) (or equivalent) mounting adapters to provide additional rear tray support when rack mounted in standard or deep 4-post rack.

Connecting the Controller Console Port

⚠

Caution Do not connect a Power over Ethernet (PoE) cable to the console port. Doing so might damage the controller.

Note Install the USB device driver before establishing a physical connection between the router and the PC using the USB Console cable plugged into the USB serial port, otherwise the connection will fail.

Procedure

Step 1 Perform either of the following tasks:

- Connect the end of the console cable with the RJ-45 connector to the console port on the controller.
- Connect a Mini-B USB cable to the Mini-B USB console port. If you are using the USB serial port for the first time on a Windows-based computer, ensure that you have installed the USB driver.

Note It is not possible to to use both the Mini-B USB console port and the CPU console port concurrently. If both the ports are connected, the USB port takes precedence over the CPU console port.

Step 2 Connect the end of the cable with the DB-9 connector (or USB Type-A) to the terminal or PC. If your terminal or PC has a console port that does not accommodate a DB-9 connector, you must provide an appropriate adapter for that port.

Step 3 To communicate with the controller, start a terminal emulator application. This software should be configured with the following parameters:

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

Installing a Security Lock

The controller has a security slot on the back panel. You can install an optional customer-supplied Kensington lock, such as the type that is used to secure a laptop computer, to secure the controller. See the "Cisco 3504 Wireless Controller Rear Panel" section for the location of the security lock.

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 CLI console on the controller as described in the Connecting to Console Port section.

To run the bootup script and conduct the power-on self test (POST), follow these steps:

Procedure

Step 1 Plug the external power supply into the power jack on the back of the controller.

Step 2 Plug a country-specific power cord into the external power supply, then plug the other end into 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 when the boot loader prompt appears. The Bootloader Options menu appears.

Note When the controller receives power, the green front panel multicolor system LED lights. If the system LED does not light, ensure that the electrical outlet is supplying power and that the power connections to the controller are correct.

Step 3 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 bootup display example:

```
Cisco bootloader . . SPI ID: xx:xx:xx:xx:xx
Header 1 found at offset 0x40000
Header 2 found at offset 0xb0000
Header 3 found at offset 0x400000
Header 4 found at offset 0x470000
failsafe value = 0
Set to Boot from Normal
Found bootloaders, booting bootloader 3 of 4 at offset 0x400000.
Starting next bootloader at 0xffffffff81000000
.

Cisco BootLoader Version : 8.5.1.88 (Development build)
(Build time: Mar 08 2017 - 20:32:41)

Octeon unique ID: 01800090c019f31e018f
N0.LMC0 Configuration Completed: 8192 MB
Warning: Board descriptor tuple not found in eeprom, using defaults
OCTEON CN7240-AAP pass 1.2, Core clock: 1500 MHz, IO clock: 800 MHz,
DDR clock: 1067 MHz (2134 Mhz DDR)
DRAM: 8 GiB
Clearing DRAM...... done
failsafe value = 0
Found valid SPI bootloader at offset: 0xb0000, size: 1571960 bytes
Found valid SPI bootloader at offset: 0x470000, size: 1571960 bytes
Loading bootloader from SPI offset 0x470000, size: 1571960 bytes

Cisco BootLoader Version : 8.5.1.88 (Development build)
(Build time: Mar 08 2017 - 20:32:06)

Octeon unique ID: 01800090c019f31e018f
OCTEON CN7240-AAP pass 1.2, Core clock: 1500 MHz,
IO clock: 800 MHz, DDR clock: 1067 MHz (2134 Mhz DDR)
DRAM: 8 GiB
Clearing DRAM...... done           CPLD Revision : a2
Reset Reason : Soft reset due to RST_SOFT_RST write
SF: Detected S25FL064P with page size 256 Bytes, erase size 64 KiB, total 8 MiB
MMC:   Octeon MMC/SD0: 0 (Type: MMC, Version: MMC v5.1, Manufacturer ID: 0x15,
Vendor: Man 150100 Snr 0739c2b4, Product: BJNB4R, Revision: 0.7)
Net:   octmgmt0, octmgmt1, octeth0, octeth1, octeth2, octeth3, octeth4,
octeth5, octeth6
SF: Detected S25FL064P with page size 256 Bytes, erase size 64 KiB,
total 8 MiB
```

```
Press <ESC> now to access the Boot Menu...


============================================================
Boot Loader Menu - Unlocked
============================================================

1. Run primary image (8.5.1.88) - Active
2. Run backup image (8.5.1.92)
3. Change active boot image
4. Clear configuration
5. Manually update images
6. Run network image via TFTP
7. Run diagnostic image from FLASH
8. Exit from menu system to boot loader prompt

------------------------------------------------------------
Enter selection:



Cisco bootloader . . SPI ID: xx:xx:xx:xx:xx
Header 1 found at offset 0x40000
Header 2 found at offset 0xb0000
Header 3 found at offset 0x400000
Header 4 found at offset 0x470000
failsafe value = 0
Set to Boot from Normal
Found bootloaders, booting bootloader 3 of 4 at offset 0x400000.
Starting next bootloader at 0xffffffff81000000.
Cisco BootLoader Version : 8.5.1.88 (Development build)
(Build time: Mar 08 2017 - 20:32:41)

Octeon unique ID: 01800090c019f31e018f
N0.LMC0 Configuration Completed: 8192 MB
Warning: Board descriptor tuple not found in eeprom, using defaults
OCTEON CN7240-AAP pass 1.2, Core clock: 1500 MHz, IO clock: 800 MHz,
DDR clock: 1067 MHz (2134 Mhz DDR)
DRAM: 8 GiB
Clearing DRAM..... done
failsafe value = 0
Found valid SPI bootloader at offset: 0xb0000, size: 1571960 bytes
Found valid SPI bootloader at offset: 0x470000, size: 1571960 bytes
Loading bootloader from SPI offset 0x470000, size: 1571960 bytes


Cisco BootLoader Version : 8.5.1.88 (Development build)
(Build time: Mar 08 2017 - 20:32:06)

Octeon unique ID: 01800090c019f31e018f
OCTEON CN7240-AAP pass 1.2, Core clock: 1500 MHz, IO clock: 800 MHz,
DDR clock: 1067 MHz (2134 Mhz DDR)
DRAM: 8 GiB
Clearing DRAM..... done
CPLD Revision : a2
Reset Reason : Soft reset due to RST_SOFT_RST write
SF: Detected S25FL064P with page size 256 Bytes, erase size 64 KiB, total 8 MiB
MMC:   Octeon MMC/SD0: 0 (Type: MMC, Version: MMC v5.1, Manufacturer ID: 0x15,
Vendor: Man 150100 Snr 0739c2b4, Product: BJNB4R, Revision: 0.7)
Net:   octmgmt0, octmgmt1, octeth0, octeth1, octeth2, octeth3, octeth4,
octeth5, octeth6
```

```
SF: Detected S25FL064P with page size 256 Bytes, erase size 64 KiB, total 8 MiB


Press <ESC> now to access the Boot Menu...

Loading primary image (8.5.1.88)
76661462 bytes read in 1805 ms (40.5 MiB/s)
Launching images...
PP0:~CONSOLE-> Using device tree
PP0:~CONSOLE-> Version: Cavium Inc. OCTEON SDK version 3.1.2-p7, build 591
PP2:~CONSOLE-> Version: Cavium Inc. OCTEON SDK version 3.1.2-p7, build 591
PP1:~CONSOLE-> Version: Cavium Inc. OCTEON SDK version 3.1.2-p7, build 591
PP3:~CONSOLE-> Version: Cavium Inc. OCTEON SDK version 3.1.2-p7, build 591
PP0:~CONSOLE-> Application in 64-bit mode (ptrsize= 8 bytes)
PP0:~CONSOLE-> # cvmcs: Cores are running at 1500000000 Hz
PP0:~CONSOLE-> # cvmcs: BOOT CORE: Core 0; DISPLAY CORE: Core 3
PP0:~CONSOLE-> SDK Build Number: 3.1.2-p7, build 591
PP0:~CONSOLE-> Platform Initialization... Platform board =24590
PP0:~CONSOLE-> # fp_hal_platform_init: WLC-Kukri core_mask=0xf
num_cores=4 pool=204800/102400/34794/128
PP0:~CONSOLE-> Octeon68xx/73xx found in init_irqs
PP0:~CONSOLE-> Done with all fp init functions
PP0:~CONSOLE-> Initializing Phy ports, queues
PP0:~CONSOLE-> Node 0 Interface 0 has 4 ports (SGMII)
PP0:~CONSOLE-> Node 0 Interface 1 has 4 ports (XFI)
PP0:~CONSOLE-> Node 0 Interface 2 has 2 ports (SGMII)
PP0:~CONSOLE-> Node 0 Interface 3 has 128 ports (NPI)
PP0:~CONSOLE-> Node 0 Interface 4 has 4 ports (LOOP)
PP0:~CONSOLE->
PP0:~CONSOLE->
PP0:~CONSOLE-> Active FP Cores in System = 04.
PP0:~CONSOLE->
PP0:~CONSOLE->
PP0:~CONSOLE-> Booting DP ID 0
INIT: version 2.88 booting
Configuring network interfaces... done.
Starting udev
cp: can't stat '/boot/rescue.ver': No such file or directory
PP0:~CONSOLE-> Warning: Enabling PKI when PKI already enabled.
INIT: Entering runlevel: 3
Detecting Hardware ...
Loading host drivers..
Starting DB Services...

Cryptographic library self-test....
Testing SHA1 Short Message 1
Testing SHA256 Short Message 1
Testing SHA384 Short Message 1
SHA1 POST PASSED
Testing HMAC SHA1 Short Message 1
Testing HMAC SHA2 Short Message 1
Testing HMAC SHA384 Short Message 1
passed!

XML config selected
Validating XML configuration
octeon_device_init: found 1 DPs
Cisco is a trademark of Cisco Systems, Inc.
Software Copyright Cisco Systems, Inc. All rights reserved.

Cisco AireOS Version 8.5.1.88
Initializing OS Services: ok
Initializing Serial Services: ok
Initializing Network Services: ok
```

```
Starting Statistics Service: ok
Starting ARP Services: ok
Starting Trap Manager: ok

Starting Data Externalization services: ok
Starting Network Interface Management Services: ok
Starting System Services:
 Read from Flash Completed ...
ok
Starting FIPS Features: ok : Not enabled
Starting SNMP services: ok
Starting Fastpath Hardware Acceleration: ok
Starting Fastpath DP Heartbeat : ok
Fastpath CPU0.00: Starting Fastpath Application. SDK-Cavium Inc.
OCTEON SDK version 3.1.2-p7, build 591. Flags-[DUTY CYCLE] : ok
Fastpath CPU0.00: Initializing last packet received queue. Num of cores(4)
Fastpath CPU0.00: Core 0 Initialization: ok
Fastpath CPU0.00: Initializing Timer...
Fastpath CPU0.00: Initializing Timer...done.
Fastpath CPU0.00: Initializing Timer...
Fastpath CPU0.00: Initializing NBAR AGING Timer...done.
Fastpath CPU0.00: Initializing Data Ports....done
Fastpath CPU0.01: Core 1 Initialization: ok
Fastpath CPU0.02: Core 2 Initialization: ok
Fastpath CPU0.03: Core 3 Initialization: ok
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 Client Troubleshooting Service: ok
Starting Certificate Database: ok
Starting VPN Services: ok
Starting Management Frame Protection: ok
Starting DNS Services: ok
ok
HBL initialization is successful
Starting Licensing Services: ok
Starting Redundancy: ok
Start rmgrPingTask: ok
Starting LWAPP: ok
Starting CAPWAP: ok
Starting LOCP: ok
Starting Security Services: ok
Starting OpenDNS Services: ok
Starting Policy Manager: ok
Starting TrustSec Services: ok
Starting Authentication Engine: ok
Starting Mobility Management: ok
Starting Capwap Ping Component: ok
Starting AVC Services: ok
Starting AVC Flex Services: ok
Starting Virtual AP Services: ok
Starting AireWave Director: ok
Starting Network Time Services: ok
Starting Cisco Discovery Protocol: ok
Starting Broadcast Services: ok
Starting Logging Services: ok
Starting DHCP Server: ok
Starting IDS Signature Manager: ok
Starting RFID Tag Tracking: ok
Starting RF Profiles: ok
```

```
Starting Environment Fan Status Monitoring Service: ok
Starting Mesh Services:  ok
Starting TSM: ok
Starting CIDS Services: ok
Starting Ethernet-over-IP: ok
Starting DTLS server:  enabled in CAPWAP
Starting CleanAir: ok
Starting WIPS: ok
Starting SSHPM LSC PROV LIST: ok
Starting RRC Services: ok
Starting SXP Services: ok
Starting Alarm Services: ok
Starting FMC HS: ok
Starting IPv6 Services: ok
Starting Config Sync Manager : ok
Starting Hotspot Services: ok
Starting Tunnel Services New: ok
Starting PMIP Services: ok
Starting Portal Server Services: ok
Starting mDNS Services: ok
Starting Management Services:
   Web Server:    CLI:    Secure Web: ok
Starting IPSec Profiles component: ok
Starting FEW Services: ok
Starting MS Agent Services: ok
Semaphore priority is larger than limit of 640
Starting Fabric Services: ok

(Cisco Controller)>
```

Step 4 If desired, press Esc key to interrupt the boot process and access the Boot menu.

Step 5 Continue booting the controller or press Esc to access the following menu:

```
1. Run primary image (8.5.1.88) - Active
2. Run backup image (8.5.1.92)
3. Change active boot image
4. Clear configuration
5. Manually update images
6. Run network image via TFTP
7. Run diagnostic image from FLASH
8. Exit from menu system to boot loader prompt

------------------------------------------------------------
Enter selection:
```

If you did not press Esc, the boot process continues and takes two to three minutes. Do not reboot the controller until the user login prompt appears.

```
Cisco bootloader . . SPI ID: xx:xx:xx:xx:xx
Header 1 found at offset 0x40000
Header 2 found at offset 0xb0000
Header 3 found at offset 0x400000
Header 4 found at offset 0x470000
failsafe value = 0
Set to Boot from Normal
Found bootloaders, booting bootloader 3 of 4 at offset 0x400000.
Starting next bootloader at 0xffffffff81000000.
Cisco BootLoader Version : 8.5.1.88 (Development build)
(Build time: Mar 08 2017 - 20:32:41)

Octeon unique ID: 01800090c019f31e018f
```

```
N0.LMC0 Configuration Completed: 8192 MB
Warning: Board descriptor tuple not found in eeprom, using defaults
OCTEON CN7240-AAP pass 1.2, Core clock: 1500 MHz, IO clock: 800 MHz,
DDR clock: 1067 MHz (2134 Mhz DDR)
DRAM: 8 GiB
Clearing DRAM...... done
failsafe value = 0
Found valid SPI bootloader at offset: 0xb0000, size: 1571960 bytes
Found valid SPI bootloader at offset: 0x470000, size: 1571960 bytes
Loading bootloader from SPI offset 0x470000, size: 1571960 bytes


Cisco BootLoader Version : 8.5.1.88 (Development build)
(Build time: Mar 08 2017 - 20:32:06)

Octeon unique ID: 01800090c019f31e018f
OCTEON CN7240-AAP pass 1.2, Core clock: 1500 MHz, IO clock: 800 MHz,
DDR clock: 1067 MHz (2134 Mhz DDR)
DRAM: 8 GiB
Clearing DRAM...... done
CPLD Revision : a2
Reset Reason : Soft reset due to RST_SOFT_RST write
SF: Detected S25FL064P with page size 256 Bytes, erase size 64 KiB, total 8 MiB
MMC:   Octeon MMC/SD0: 0 (Type: MMC, Version: MMC v5.1, Manufacturer ID: 0x15,
Vendor: Man 150100 Snr 0739c2b4, Product: BJNB4R, Revision: 0.7)
Net:   octmgmt0, octmgmt1, octeth0, octeth1, octeth2, octeth3, octeth4,
octeth5, octeth6
SF: Detected S25FL064P with page size 256 Bytes, erase size 64 KiB, total 8 MiB


Press <ESC> now to access the Boot Menu...

Loading primary image (8.5.1.88)
76661462 bytes read in 1805 ms (40.5 MiB/s)
Launching images...
PP0:~CONSOLE-> Using device tree
PP0:~CONSOLE-> Version: Cavium Inc. OCTEON SDK version 3.1.2-p7, build 591
PP2:~CONSOLE-> Version: Cavium Inc. OCTEON SDK version 3.1.2-p7, build 591
PP1:~CONSOLE-> Version: Cavium Inc. OCTEON SDK version 3.1.2-p7, build 591
PP3:~CONSOLE-> Version: Cavium Inc. OCTEON SDK version 3.1.2-p7, build 591
PP0:~CONSOLE-> Application in 64-bit mode (ptrsize= 8 bytes)
PP0:~CONSOLE-> # cvmcs: Cores are running at 1500000000 Hz
PP0:~CONSOLE-> # cvmcs: BOOT CORE: Core 0; DISPLAY CORE: Core 3
PP0:~CONSOLE-> SDK Build Number: 3.1.2-p7, build 591
PP0:~CONSOLE-> Platform Initialization... Platform board =24590
PP0:~CONSOLE-> # fp_hal_platform_init: WLC-Kukri core_mask=0xf num_cores=4
pool=204800/102400/34794/128
PP0:~CONSOLE-> Octeon68xx/73xx found in init_irqs
PP0:~CONSOLE-> Done with all fp init functions
PP0:~CONSOLE-> Initializing Phy ports, queues
PP0:~CONSOLE-> Node 0 Interface 0 has 4 ports (SGMII)
PP0:~CONSOLE-> Node 0 Interface 1 has 4 ports (XFI)
PP0:~CONSOLE-> Node 0 Interface 2 has 2 ports (SGMII)
PP0:~CONSOLE-> Node 0 Interface 3 has 128 ports (NPI)
PP0:~CONSOLE-> Node 0 Interface 4 has 4 ports (LOOP)
PP0:~CONSOLE->
PP0:~CONSOLE->
PP0:~CONSOLE-> Active FP Cores in System = 04.
PP0:~CONSOLE->
PP0:~CONSOLE->
PP0:~CONSOLE-> Booting DP ID 0
INIT: version 2.88 booting
Configuring network interfaces... done.
Starting udev
```

```
cp: can't stat '/boot/rescue.ver': No such file or directory
PP0:~CONSOLE-> Warning: Enabling PKI when PKI already enabled.
INIT: Entering runlevel: 3
Detecting Hardware ...
Loading host drivers..
Starting DB Services...

Cryptographic library self-test....
Testing SHA1 Short Message 1
Testing SHA256 Short Message 1
Testing SHA384 Short Message 1
SHA1 POST PASSED
Testing HMAC SHA1 Short Message 1
Testing HMAC SHA2 Short Message 1
Testing HMAC SHA384 Short Message 1
passed!

XML config selected
Validating XML configuration
octeon_device_init: found 1 DPs
Cisco is a trademark of Cisco Systems, Inc.
Software Copyright Cisco Systems, Inc. All rights reserved.

Cisco AireOS Version 8.5.1.88
Initializing OS Services: ok
Initializing Serial Services: ok
Initializing Network Services: ok
Starting Statistics Service: ok
Starting ARP Services: ok
Starting Trap Manager: ok

Starting Data Externalization services: ok
Starting Network Interface Management Services: ok
Starting System Services:
 Read from Flash Completed ...
ok
Starting FIPS Features: ok : Not enabled
Starting SNMP services: ok
Starting Fastpath Hardware Acceleration: ok
Starting Fastpath DP Heartbeat : ok
Fastpath CPU0.00: Starting Fastpath Application. SDK-Cavium Inc.
OCTEON SDK version 3.1.2-p7, build 591. Flags-[DUTY CYCLE] : ok
Fastpath CPU0.00: Initializing last packet received queue. Num of cores(4)
Fastpath CPU0.00: Core 0 Initialization: ok
Fastpath CPU0.00: Initializing Timer...
Fastpath CPU0.00: Initializing Timer...done.
Fastpath CPU0.00: Initializing Timer...
Fastpath CPU0.00: Initializing NBAR AGING Timer...done.
Fastpath CPU0.00: Initializing Data Ports....done
Fastpath CPU0.01: Core 1 Initialization: ok
Fastpath CPU0.02: Core 2 Initialization: ok
Fastpath CPU0.03: Core 3 Initialization: ok
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 Client Troubleshooting Service: ok
Starting Certificate Database: ok
Starting VPN Services: ok
Starting Management Frame Protection: ok
Starting DNS Services: ok
```

```
ok
HBL initialization is successful
Starting Licensing Services: ok
Starting Redundancy: ok
Start rmgrPingTask: ok
Starting LWAPP: ok
Starting CAPWAP: ok
Starting LOCP: ok
Starting Security Services: ok
Starting OpenDNS Services: ok
Starting Policy Manager: ok
Starting TrustSec Services: ok
Starting Authentication Engine: ok
Starting Mobility Management: ok
Starting Capwap Ping Component: ok
Starting AVC Services: ok
Starting AVC Flex Services: ok
Starting Virtual AP Services: ok
Starting AireWave Director: ok
Starting Network Time Services: ok
Starting Cisco Discovery Protocol: ok
Starting Broadcast Services: ok
Starting Logging Services: ok
Starting DHCP Server: ok
Starting IDS Signature Manager: ok
Starting RFID Tag Tracking: ok
Starting RF Profiles: ok
Starting Environment Fan Status Monitoring Service: ok
Starting Mesh Services:  ok
Starting TSM: ok
Starting CIDS Services: ok
Starting Ethernet-over-IP: ok
Starting DTLS server:  enabled in CAPWAP
Starting CleanAir: ok
Starting WIPS: ok
Starting SSHPM LSC PROV LIST: ok
Starting RRC Services: ok
Starting SXP Services: ok
Starting Alarm Services: ok
Starting FMC HS: ok
Starting IPv6 Services: ok
Starting Config Sync Manager : ok
Starting Hotspot Services: ok
Starting Tunnel Services New: ok
Starting PMIP Services: ok
Starting Portal Server Services: ok
Starting mDNS Services: ok
Starting Management Services:
   Web Server:    CLI:    Secure Web: ok
Starting IPSec Profiles component: ok
Starting FEW Services: ok
Starting MS Agent Services: ok
Semaphore priority is larger than limit of 640
Starting Fabric Services: ok

(Cisco Controller)>
```

Step 6 If the controller passes the POST, the bootup script runs the Startup Wizard, which prompts you for basic configuration information.

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_d9:16:24]:
```

Note The startup wizard runs the first time that you power on the controller. The second time you power it on, the controller prompts you for a login ID and password.

Using the Startup Wizard

Before you can use the startup wizard, you must obtain the information discussed in the (Link to Required Tools and Information section). The table below contains startup wizard information you can use to configure your controller for basic operation.

Note

- The available options appear in brackets after each configuration parameter. The default value appears in all uppercase letters.
- If you enter an incorrect response, the controller provides you with an appropriate error message such as invalid response, and returns to the wizard prompt.
- Press the hyphen key if you need to return to the previous command line.

Table 1: Startup Wizard Information

Wizard Setting	Action
System Name	Enter the system name, which is the name you want to assign to the controller. You can enter up to 31 ASCII characters.
Administrative user name	Enter the administrative user name to be assigned to this controller. You can enter up to 24 ASCII characters for each. The default administrative username is *admin*.
Administrative password	Enter the administrative password to be assigned to this controller. You can enter from 3 to 24 ASCII characters for each. **Note** There is no default administrative password, you must enter a password.
Service Interface IP Address	Enter the Service Interface IP address
Service Interface Netmask	Enter the Service Interface Netmask
Enable Link Aggregation (LAG)	Choose Yes or No

Wizard Setting	Action
Management Interface IP Address	Enter the IP address of the management interface. The management interface is the default interface for in-band management of the controller and connectivity to enterprise services such as AAA servers. You can access the controller GUI interface using the management interface IP address.
Management Interface Netmask	Enter the IP address of the management interface netmask.
Management Interface Default Router	Enter the IP address of the default router.
Management Interface VLAN Identifier	Enter the VLAN identifier of the management interface (a valid VLAN identifier or 0 for an untagged VLAN). The VLAN identifier should be set to match the switch interface configuration.
Management Interface Port Num [1 to 4]	Management Interface Port Num 1-5. Port 5 if using mGig port.
Management Interface DHCP Server IP Address	Enter the management interface DHCP server IP address.
Enable HA	Choose Yes or No to enable or disable High Availability
Virtual Gateway IP Address	Enter the IP address of the controller virtual interface. You should enter a fictitious, unassigned IP address, such as 192.0.2.1. 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.
Mobility/RF Group Name	If desired, 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 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.
Network Name (SSID)	Enter the network name, or service set identifier (SSID). This is the default SSID that the access points use when they join a controller.
Configure DHCP Bridging Mode	Enter yes to configure DHCP Bridging Mode. Values are yes or no. The following message appears: `Warning! The default WLAN security policy requires a RADIUS server. Please see documentation for more details.`

Wizard Setting	Action
Allow Static IP Addresses	Enter YES to allow clients to assign their own IP address or no to make clients request an IP address from a DHCP server. Values are YES or no. The default setting is YES.
Configure a RADIUS Server Now?	If you select YES, you are prompted to enter the following: • RADIUS Server IP address • RADIUS server port (default port is 1812) • RADIUS Server secret If you select no, the following message appears: `Warning! The default WLAN security policy requires a RADIUS server. Please see documentation for more details.`
Enter Country Code List	Enter the two letter country code. The default country code is the United States (US). Enter 'help' to see a list of countries.
Enable 802.11b Network	Choose YES to enable or no to disable the 802.11b radio network. The default is YES.
Enable 802.11a Network	Choose YES to enable or no to disable the 802.11a radio network. The default is YES.
Enable 802.11g Network	Choose YES to enable
Enable Auto-RF	Choose YES to enable or no to disable radio resource management. The default is YES.
Configure a NTP server now?	Enter YES to configure an NTP server. The values are YES or no. The default value is YES.
Enter the NTP server IP address	Enter the NTP server IP address. **Note** This prompt only displays if YES was entered in the "Configure a NTP Server Now?" prompt.
Enter a polling interval between 3600 and 604800 secs	Enter the polling interval between 3600 and 604800 seconds. **Note** This prompt only displays if YES was entered in the "Configure a NTP Server Now?" prompt.
Configure the system time now?	Enter YES to configure the system time.
Would you like to configure IPv6 parameters	Choose YES or No.
Configuration correct?	Enter yes if the configuration entered is correct. Values are yes and no. If yes is entered. the controller saves your configuration, reboots, and prompts you to log in.

Logging On to the Controller

To log into the controller, follow these steps:

Procedure

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)>
```

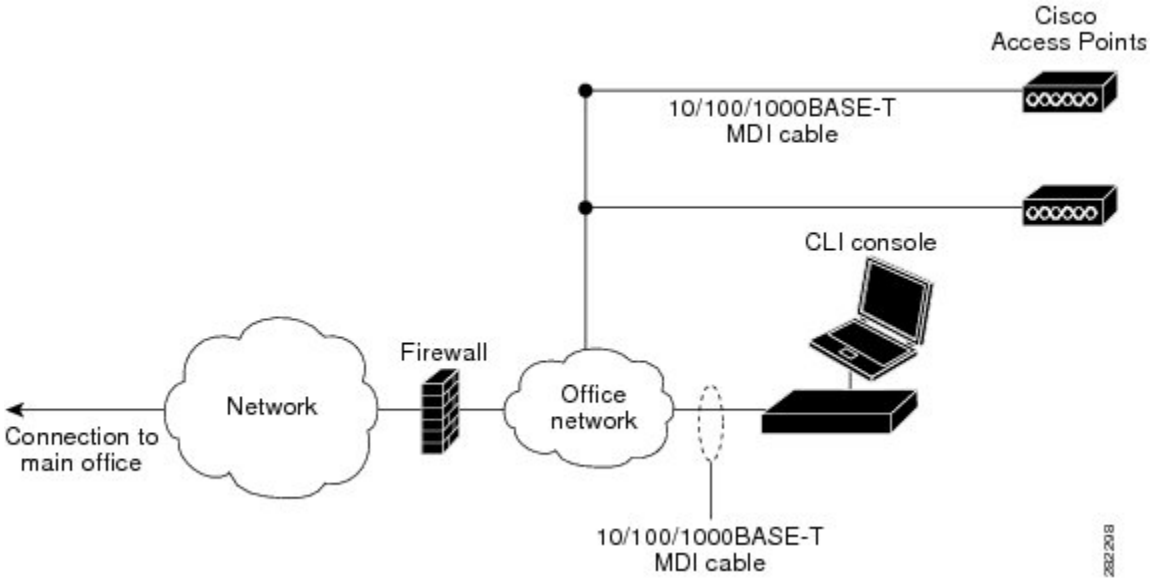
The system prompt can be any alphanumeric string up to 31 characters. You can change it by entering the config prompt command. For example, to change the system prompt to CISCO3504, enter config prompt "CISCO3504" and press Enter. Make sure you enter the new prompt using double quotation marks.

Note The CLI automatically logs 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.

Connecting to the Network

Figure below shows the connection from the network (802.11 distribution system) to the controller. The connection uses 10/100/1000BASE-T Ethernet (RJ-45 physical port, UTP, Category-5 or higher cable). Always use Category-5, Category-5e, Category-6, or Category-7 Ethernet cables to connect the office network equipment to the controller.

Figure 6: External Network Equipment Connection to the Controller



Note If the link does not activate, check the cable. When you are connecting to a hub or a switch, use a straight-through cable.

Connecting Access Points

After you have configured the controller, use Category-5, Category-5e, Category-6, or Category-7 Ethernet cables to connect up to 50 Cisco lightweight access points to the controller Ethernet ports or to the network (distribution system). The controller has an auto MDI feature, so you can use an MDI-X or MDI cable (crossover or straight-through) to make the connections.

As soon as the controller is operational, the controller is available to connect access that are scanning for a controller. When it detects an access point, it records the access point MAC address in its database. The controller Radio Resource Management (RRM) feature automatically configures the access point to start transmitting and allowing clients to associate.

Note Directly connected local mode APs via two PoE (Power over Ethernet) ports are supported. Directly connected APs were not supported before Release 7.4.

You have prepared the controller for basic operation. Refer to the Cisco Wireless Controller Configuration Guides for information about configuring the controller to meet the specific needs of your wireless network.

Troubleshooting the Controller

This section contains the following topics:

- *Checking the Controller LEDs*
- *Using the Reset Button*

Checking the Controller LEDs

If the 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 status of the unit. See the "Front Panel LEDs: Definitions of States" section for a description of the front panel LEDs.

The installation is complete. See the Cisco Wireless Controller Configuration Guide for more information about configuring your controller.

Using the Reset Button

The Reset button on the front panel of the controller becomes active after the controller boots. To reset the controller using the Reset button, follow these steps:

1. Connect a PC to the controller console point.
2. Press and hold the Reset button for at least 3 seconds using a pointed object.
3. After the controller reboots, enter your username and password at the prompts.

If you have configured the controller, it reboots and loads the configuration. If you have not configured the controller, the configuration wizard is displayed.