



Installation and Configuration

The Cisco 2000 Series Wireless LAN Controller (referred to as the *controller* hereafter) is a slim 9.5 x 6.0 x 1.6 in. (241 x 152 x 41 mm) chassis that can be mounted on a desktop or on a shelf. controller front panel has one POWER LED and four sets of Ethernet LAN port status LEDs, which indicate 10 MHz or 100 MHz connections and transmit/receive activity for the four corresponding back-panel Ethernet LAN connectors. The controller is shipped with four rubber feet for mounting. [Figure 1](#) shows the controller back panel, which has one Power Input Connector (PWR), one Serial Console Port Connector (CONSOLE), one Reset Switch (RST), and four 10/100BASE-T Ethernet LAN Port Connectors (1 through 4).

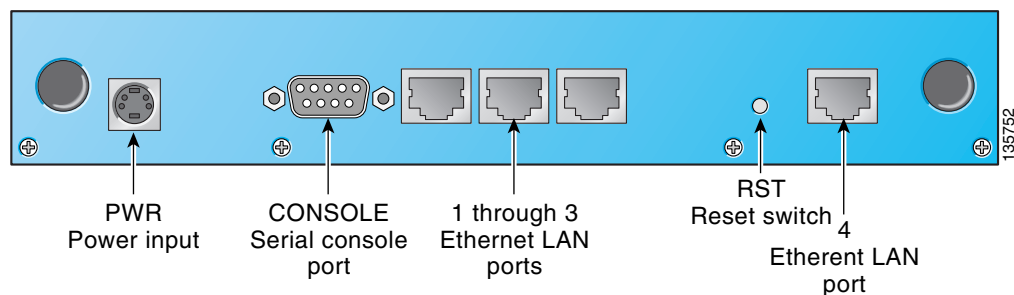


Note

These ports are MDI ports, requiring straight-through MDI cables to other network devices, and requiring crossover MDI-X cables to access points.

All external connections are made to the controller back panel.

Figure 1 Controller Back Panel



The controller is powered by an external power supply that accepts power from an electrical outlet (100-VAC to 240-VAC, 50-Hz to 60-Hz).



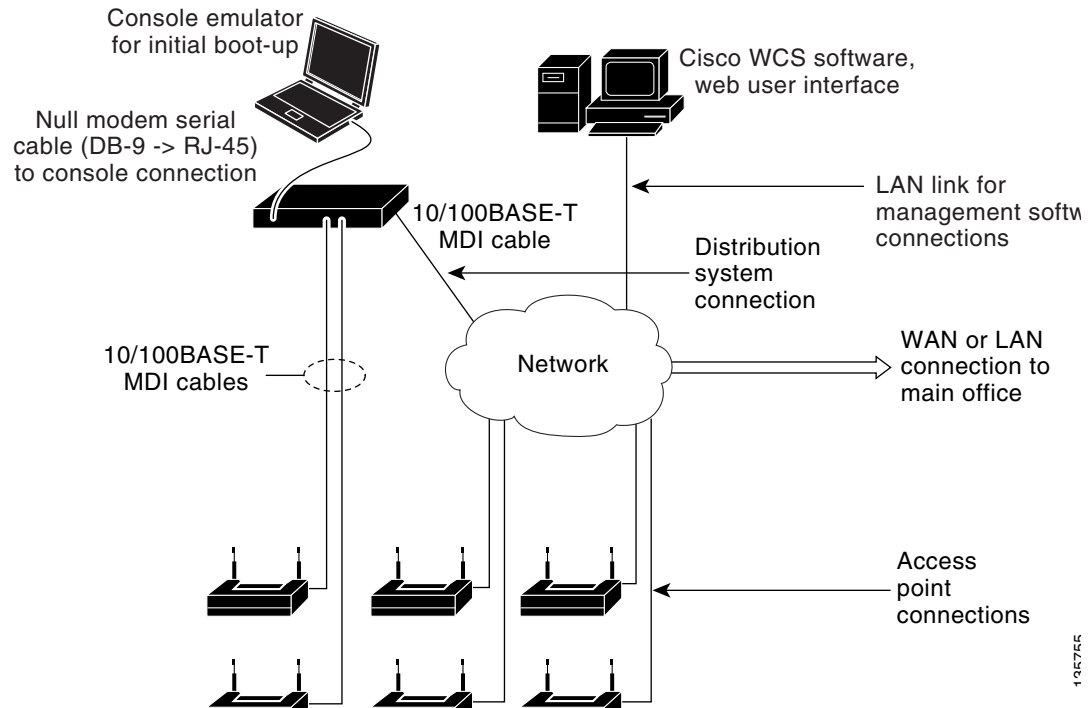
Note

The controller can be ordered with country-specific power cords; be sure to include the proper country suffix when ordering to ensure that you receive the correct power cord.

This document is written assuming that you have already determined the 802.11 topology. Because the Radio Resource Management (RRM) automatically detects and configures the access points as they appear on the network, it is not necessary to have any access points on the network to install and configure the controller.

The following figure shows a typical controller network topology and network connections, showing the MDI (straight-through) and MDI-X (crossover) ethernet LAN cables required for the controller.

Figure 2 Typical Controller Topology and Network Connections



Note

The controller does not supply Power over Ethernet (PoE). To use PoE to power access points, you must use a Cisco or external third-party PoE injector. Contact Cisco Technical Assistance Center (TAC) for recommended external PoE equipment.

Collecting Required Tools and Information

This section provides details on the tools and information that you should have before installing the controller.

Controller Hardware

You need the following controller-related hardware:

- Controller (ships with factory-supplied power cord and external power supply).
- Network, management network, and access point cables, as required.



Note

You must use MDI-X crossover Ethernet cables for Direct-Connect access points, and you must use MDI straight-through Ethernet cables for hubs and controllers.

CLI Console

To setup the CLI console, you need the following:

- VT-100 terminal emulator on CLI console laptop or palmtop.
- Null modem serial cable to connect CLI console and controller male DB-9 console port.

Local TFTP Server

This is required for software updates. (Contact Cisco Technical Assistance Center (TAC) for software updates.)

**Note**

The Cisco Wireless Control System (Cisco WCS) uses an integral TFTP server. This means that third-party TFTP servers cannot run on the same workstation as Cisco WCS because Cisco WCS and the third-party TFTP servers use the same communication port.

**Note**

The Cisco 2000 Series Wireless LAN Controller does not have a Service Port like those on other Cisco Wireless LAN Controllers. This means that Cisco WCS Servers and TFTP servers must be on the same subnet or must be connected by network devices that pass SNMP and TFTP messages, respectively.

Initial System Configuration Information

Enter the following information from the console CLI after you have completed all external connections to the controller:

- System (Controller) name.
- Administrative username and password. (Default administrative username and password are *admin* and *admin*, respectively.)
- Management interface—Management interface port IP Address, or DS (802.11 distribution system) port.

**Note**

This logical port can be assigned to any physical back-panel port.

- Management interface netmask.
- Management Interface default router IP address.
- DHCP server IP address.
- VLAN identifier, if the management interface is assigned to a VLAN, or '0' for an untagged VLAN.
- AP manager interface IP address, netmask, default router, optional VLAN identifier, Physical port number, and default DHCP server IP Address. The AP manager interface which manages layer 3 LWAPP communications between the controller and its associated access points. This AP Manager Interface requires a fixed IP address which is different from the Management Interface IP address.
- Virtual gateway IP address: one fictitious, unassigned IP address (such as 1.1.1.1) to be used by all Cisco WLAN Solution layer 3 security and mobility managers.
- Controller Mobility Group (RF Group) name, if required.

- 802.11 Network Name (SSID) for WLAN 1. This is the default SSID that the access points broadcast when they associate with the controller.
- Whether or not to allow Static IP Addresses for clients.
 - * Yes = more convenient, but lower security (session can be hijacked), clients can supply their own IP Address, better for devices that cannot use DHCP.
 - * No = less convenient, higher security, clients must use DHCP for an IP Address, works well for Windows XP devices.
- If you are configuring a RADIUS server, enter the server IP address, communication port, and Secret.
- Country Code for this installation.
- 802.11a network enabled or disabled?
- 802.11b network enabled or disabled?
- 802.11g network enabled or disabled?
- Radio Resource Management (Auto-RF) enabled or disabled?

Determining a Physical Location

The controller can be installed almost anywhere, but it is more secure and reliable if installed in a secure equipment room or wiring closet.

For maximum reliability, mount the controller using the following constraints:

- Be sure you can reach the controller and all cables.
- Be sure that water or excessive moisture cannot get into the controller.
- Ensure that airflow through the controller is not obstructed. Leave at least 4 in. (10 cm) clear on both sides of the controller chassis.
- Verify that the ambient temperature remains between 0 to 40° C (32 to 104° F).
- Be sure that the controller is within 100 m (328 ft.) of any equipment connected to the 10/100BASE-T ports.
- Ensure that the power cord can reach a 110 or 220 VAC grounded electrical outlet.

Installing the Chassis

This section describes how to install the controller chassis.



Warning

Only trained and qualified personnel should be allowed to install, replace, or service this equipment. Statement 1030

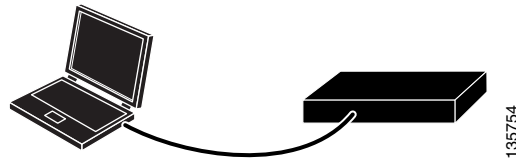
The controller is shipped with rubber feet for mounting. Place the controller chassis on any secure horizontal surface.

You have installed the controller chassis.

Connecting and Using the CLI Console

For initial system configuration, use the CLI console. As shown in the following figure, the CLI console connects to the controller back-panel Console port.

Figure 3 CLI Console Connection to a Cisco 2000 Series Wireless LAN Controller



Follow these steps to connect the CLI console to the controller:

Step 1 Use a null-modem serial cable to connect the CLI console to the controller console port.



Note The controller end of the cable is female DB-9. The other end should be any kind of connector that plugs into your VT-100 terminal emulator (usually a laptop or palmtop computer).

Step 2 Be sure that the VT-100 terminal emulator (HyperTerminal, ProComm, minicom, tip, or other) is configured for the following parameters:

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

Performing 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. Follow these steps to perform power on self test (POST) and to initialize operating system software:



Note This procedure is written assuming that you have connected the CLI console to the controller as described in [“Connecting and Using the CLI Console.”](#)

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

Step 2 Plug a country-specific power cord into the external power supply and the other end into a grounded 100 to 240 VAC 50/60 Hz electrical outlet.

**Note**

Cisco supplies the country-specific power cord if ordered with the controller.

**Note**

In order to run a previous version of the controller code, press the <ESC> key immediately after the Model and S/N line. This will take you to the *Bootloader Boot Options* menu.

Step 3 When the controller receives power, the green front-panel POWER LED lights. If the POWER LED does not light, contact Cisco Technical Assistance Center (TAC) for technical support.

Step 4 Monitor the controller bootup using the CLI screen.

During Bootup, operating system software displays code download and POST verification messages similar to the following:

```
.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

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

(If desired, press <ESC> now to display the Bootloader Boot Options Menu.)

```
Boot Options
Please choose an option from below:
 1. Run active image (version 3.0.80.0)
 2. Run backup image (version 3.0.57.0)
 3. Manually perform system upgrade
 4. Clear Configuration
Please enter your choice:
```

(Enter 1 to run the current Code, enter 2 to run the previous Code, enter 4 to run the current Code and clear the Cisco 2000 Series Wireless LAN Controller configuration to factory defaults. Do not enter 3 unless directed to do so by Cisco Technical Assistance Center (TAC).)

Booting 'Run primary image (version 3.3)'

```
root (hd0,1)
Filesystem type is ext2fs, partition type 0x83
kernel /bzImage-primary root=/dev/ram ramdisk_size=28672 console=ttyS0,9600
[Linux-bzImage, setup=0xa00, size=0xac47b]
initrd (hd0,1)/initrd-primary
[Linux-initrd @ 0x6eb5000, 0x92a717 bytes]
init started: BusyBox v1.00-pre7 (2004.03.22-23:05+0000) multi-call binary
Starting pid 14, console /dev/ttyS0: '/etc/init.d/rcS'
Using /lib/modules/2.4.17_mvl21-pc_target/broff.o
Using /lib/modules/2.4.17_mvl21-pc_target/sshquicksec.o
Warning: loading /lib/modules/2.4.17_mvl21-pc_target/sshquicksec.o will taint the kernel:
no license
cp: unable to open `/mnt/bootsys/root/*/Entries': No such file or directory
cp: unable to open `/mnt/bootsys/root/*/Repository': No such file or directory
cp: unable to open `/mnt/bootsys/root/*/Root': No such file or directory
cp: unable to open `/mnt/bootsys/root/*/clear-config': No such file or directory
cp: unable to open `/mnt/bootsys/root/*/switch-images': No such file or directory
cp: unable to open `/mnt/bootsys/root/*/system-upgrade': No such file or directory
```

```
OS Version 3.0.37.0
Initializing OS Services: ok
Initializing Serial Services: ok
Initializing Network Services: ok
Starting ARP Services: ok
Starting Network Interface Management Services: ok
Starting System Services: ok
Starting Fast Path Hardware Acceleration: broffu_UserInit: ioctl broff0 file opened,
BROFFU_IOCTL_FD=11
broffu_UserInit: ctlpkt broff1 file opened, fd=0xc
broffu_UserInit: allpkts broff2 file opened, fd=0xd
ok
Starting Switching Services: ok
Starting QoS Services: ok
Starting Data Transport Link Layer: ok
Starting Access Control List Services: ok
Starting System Interfaces: ok
Starting LWAPP: ok
Starting Crypto Accelerator: Not Present
Starting Certificate Database: ok
Starting VPN Services: modprobe: Can't locate module /tmp/sshquicksec.o
ok
Starting Security Services: ok
Starting Policy Manager: ok
Starting Authentication Engine: ok
Starting Mobility Management: ok
Starting Virtual AP Services: ok
Starting 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 Management Services:
  Web Server: ok
  CLI: ok
  Secure Web: Web Authentication Certificate not found (error).
(Cisco WLAN Solution switch)
Enter User Name (or 'Recover-Config' to reset configuration to factory defaults)
```

Step 5 At this point, the controller has passed the POST test.

- If this is the first time a controller has been powered up, or if you previously entered *Recover-Config* command at the User: prompt, the bootup script runs the Startup Wizard, which prompts you for basic configuration input. Continue with “[Using the Startup Wizard](#).”
 - If this is atleast the second time you have powered up a controller, the bootup script prompts you for a login and password. Enter the login and password as described in “[Logging In](#)”, or enter *Recover-Config* to reset the controller configuration to factory defaults.
-

Using the Startup Wizard

The first time you power up the controller with a new factory-default operating system configuration, use the **Startup Wizard** to do the following:


Note

Use the information you collected in “[Collecting Required Tools and Information](#)” for this process.

-
- Step 1** Enter the system (controller) name, up to 32 printable ASCII characters.
 - Step 2** Enter the administrative username and password, each up to 24 printable ASCII characters. The default administrative user login and password are *admin* and *admin*, respectively.
 - Step 3** Enter the management interface IP address, netmask, default router IP address, and optional VLAN identifier (a valid VLAN identifier, or ‘0’ for untagged).
 - Step 4** Enter the IP address of the default DHCP server that will supply IP addresses to Cisco WLAN Solution clients. When planning to use the built-in OS DHCP server, enter the management interface IP address.
 - Step 5** Enter the AP manager interface IP address, netmask, default router IP address, optional VLAN identifier (a valid VLAN identifier, or ‘0’ for untagged), and default DHCP server IP address.


Note

The AP manager interface IP address **MUST** be different than the management interface IP address.

-
- Step 6** Enter the virtual gateway IP address; one fictitious, unassigned IP address (such as 1.1.1.1) to be used by all Cisco WLAN Solution layer 3 security and mobility managers.
 - Step 7** Enter the Controller Mobility Group (RF Group) name, if required.
 - Step 8** Enter the WLAN 1 network name, or SSID. This is the default SSID that the access points broadcast when they associate with the controller.
 - Step 9** Allow or disallow static IP addresses for clients. (Yes = clients can supply their own IP Address. No = clients must request an IP address from a DHCP server.)
 - Step 10** If you are configuring a RADIUS server now, enter YES, and then enter the RADIUS Server IP address, communication port, and Secret. Otherwise, enter NO.
 - Step 11** Enter the Country Code for this installation.
 - Step 12** Independently enable and/or disable the 802.11b, 802.11a, and 802.11g access point networks.
 - Step 13** Enable or disable the Radio Resource Management (Auto RF).

The controller saves your configuration, reboots with your changes, and prompts you to log in or enter **Recover-Config** to repeat this step.

Logging In

To log into the controller, perform these steps:

Step 1 Enter a valid login and password to enter the CLI.

```
User:
Password:
```



Note

The login and password functions are case sensitive. The default **Administrative User login** and **password** are *admin* and *admin*, respectively.

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 following command:

```
(system prompt)>config prompt
```

Because this is a user-defined variable, it is omitted from the rest of this documentation.

Step 3 The CLI automatically logs you out without saving any changes after five minutes of inactivity. This automatic logout can be set from 0 (never log out) to 160 minutes entering the following command:

```
(system prompt)>config serial timeout
```

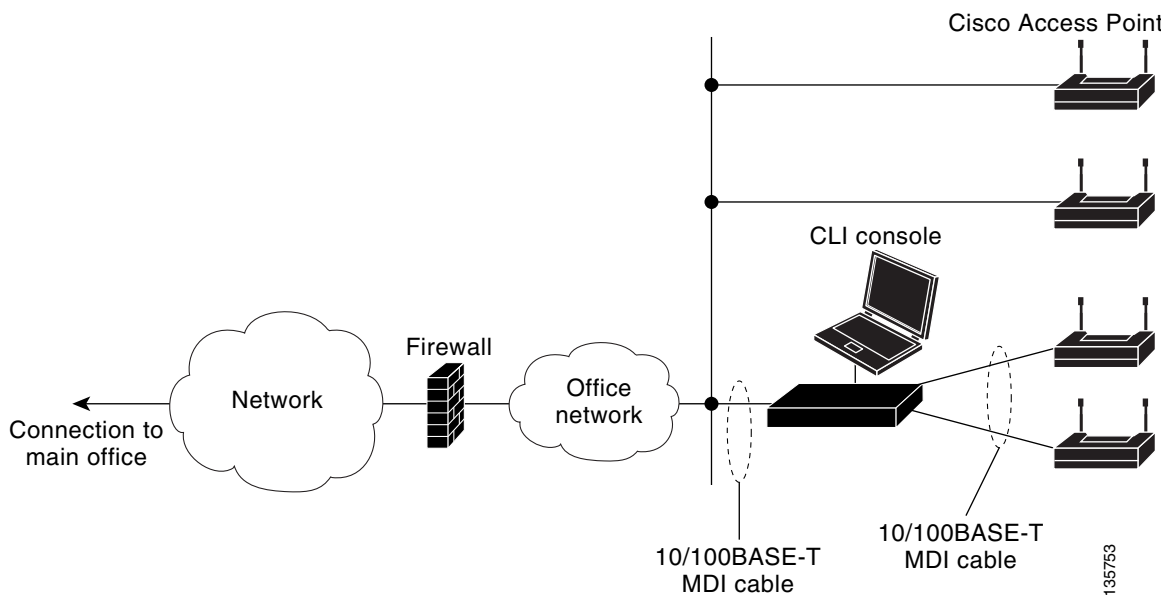
You have logged into the controller.

Connecting the Network (Distribution System)

Refer to [Figure 4](#) for the connection from the network (802.11 Distribution System) to the controller. The connection uses a 10/100BASE-T Ethernet (RJ-45 physical port, UTP, CAT-5 or higher cable).

Always use CAT-5, CAT-5e, CAT-6, or CAT-7 Ethernet cables to connect the office network equipment to the controller.

Figure 4 External Network Equipment Connection to the Controller



Note

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

Connecting Access Points

After you have installed and configured the controller, use CAT-5, CAT-5e, CAT-6, or CAT-7 Ethernet cables to connect up to six access points either to the controller back panel 10/100BASE-T Ethernet ports or to the Network (Distribution System) as shown in the following figures.



Note

As soon as the controller is activated, it starts listening for access points on all connected ports. As it detects access points, it records their MAC addresses in its database. The Radio Resource Management function then automatically configures the access points to start transmitting and start allowing clients to connect through the Cisco WLAN Solution.



Note

If the link does not come up, check the cable. When you are connecting an access point to the controller, use a crossover cable.

Figure 5 Access Points Connected to a Controller Back Panel using MDI-X Crossover Cables

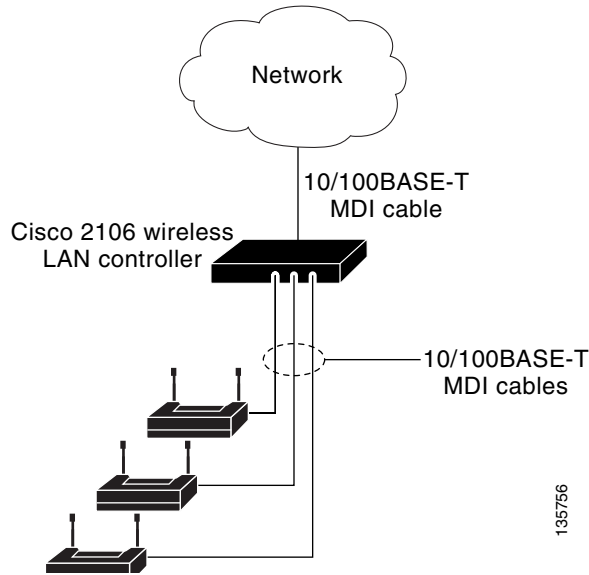
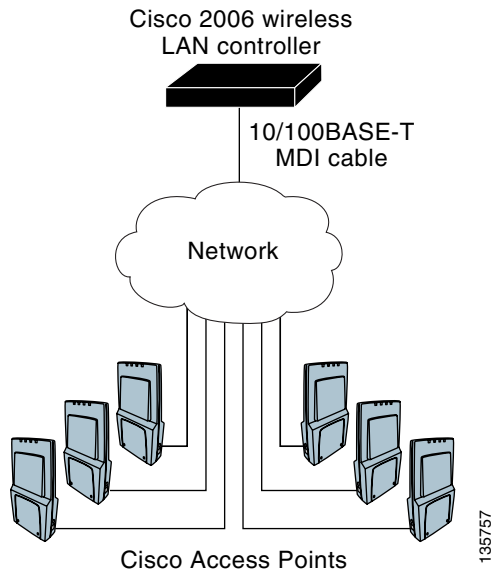


Figure 6 Access Points Connected to a Controller through the Network using an MDI Straight-Through Cable



Where to Go from Here

You have completely installed the controller hardware.

- Register your controller.
- Refer to the *Cisco WLAN Controller Web User Interface User Guide* for more information on configuring the controller.

**Note**

The Cisco 2000 Series Wireless LAN Controller uses a subset of the commands available on the Cisco 4100 Series Wireless LAN Controller.
