



Overview

This chapter describes the controller components and features. It contains these sections:

- [Cisco Wireless LAN Solution Overview, page 1-2](#)
- [Operating System Software, page 1-5](#)
- [Operating System Security, page 1-5](#)
- [Layer 2 and Layer 3 LWAPP Operation, page 1-7](#)
- [Cisco Wireless LAN Controllers, page 1-7](#)
- [Client Roaming, page 1-8](#)
- [External DHCP Servers, page 1-10](#)
- [Cisco WLAN Solution Wired Connections, page 1-11](#)
- [Cisco WLAN Solution Wireless LANs, page 1-11](#)
- [Access Control Lists, page 1-12](#)
- [Identity Networking, page 1-12](#)
- [File Transfers, page 1-13](#)
- [Power over Ethernet, page 1-14](#)
- [Pico Cell Functionality, page 1-14](#)
- [Intrusion Detection Service \(IDS\), page 1-15](#)
- [Wireless LAN Controller Platforms, page 1-15](#)
- [Rogue Access Points, page 1-24](#)
- [Web User Interface and the CLI, page 1-25](#)

Cisco Wireless LAN Solution Overview

The Cisco Wireless LAN Solution is designed to provide 802.11 wireless networking solutions for enterprises and service providers. The Cisco Wireless LAN Solution simplifies deploying and managing large-scale wireless LANs and enables a unique best-in-class security infrastructure. The operating system manages all data client, communications, and system administration functions, performs Radio Resource Management (RRM) functions, manages system-wide mobility policies using the operating system Security solution, and coordinates all security functions using the operating system security framework.

The Cisco Wireless LAN Solution consists of Cisco Wireless LAN Controllers and their associated lightweight access points controlled by the operating system, all concurrently managed by any or all of the operating system user interfaces:

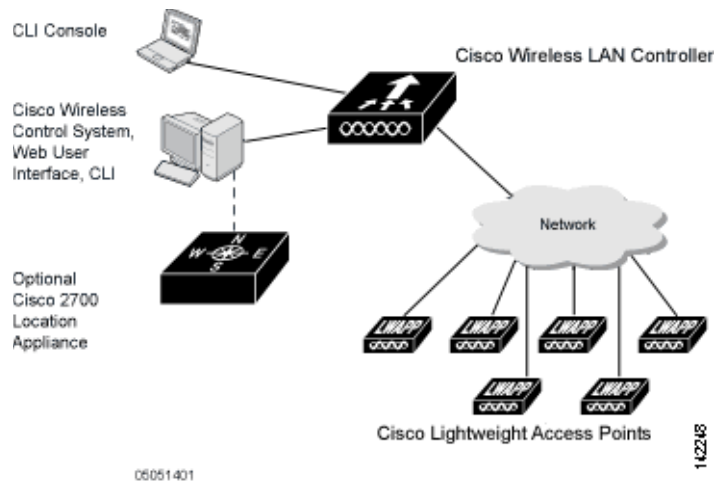
- An HTTP and/or HTTPS full-featured Web User Interface hosted by Cisco Wireless LAN Controllers can be used to configure and monitor individual controllers. See the [“Web User Interface and the CLI” section on page 1-25](#).
- A full-featured command-line interface (CLI) can be used to configure and monitor individual Cisco Wireless LAN Controllers. See the [“Web User Interface and the CLI” section on page 1-25](#).
- The Cisco Wireless Control System (WCS), which you use to configure and monitor one or more Cisco Wireless LAN Controllers and associated access points. WCS has tools to facilitate large-system monitoring and control. WCS runs on Windows 2000, Windows 2003, and Red Hat Enterprise Linux ES servers.
- An industry-standard SNMP V1, V2c, and V3 interface can be used with any SNMP-compliant third-party network management system.

The Cisco Wireless LAN Solution supports client data services, client monitoring and control, and all rogue access point detection, monitoring, and containment functions. The Cisco Wireless LAN Solution uses lightweight access points, Cisco Wireless LAN Controllers, and the optional Cisco WCS to provide wireless services to enterprises and service providers.

**Note**

This document refers to Cisco Wireless LAN Controllers throughout. Unless specifically called out, the descriptions herein apply to all Cisco Wireless LAN Controllers, including but not limited to Cisco 2000 Series Wireless LAN Controllers, Cisco 4100 Series Wireless LAN Controllers, Cisco 4400 Series Wireless LAN Controllers, and the controllers on the Wireless Services Module (WiSM).

[Figure 1-1](#) shows the Cisco Wireless LAN Solution components, which can be simultaneously deployed across multiple floors and buildings.

Figure 1-1 Cisco WLAN Solution Components

Single-Controller Deployments

A standalone controller can support lightweight access points across multiple floors and buildings simultaneously, and supports the following features:

- Autodetecting and autoconfiguring lightweight access points as they are added to the network.
- Full control of lightweight access points.
- Full control of up to 16 wireless LAN (SSID) policies for Cisco 1000 series access points.



Note LWAPP-enabled access points support up to 8 wireless LAN (SSID) policies.

- Lightweight access points connect to controllers through the network. The network equipment may or may not provide Power over Ethernet to the access points.

Note that some controllers use redundant Gigabit Ethernet connections to bypass single network failures.

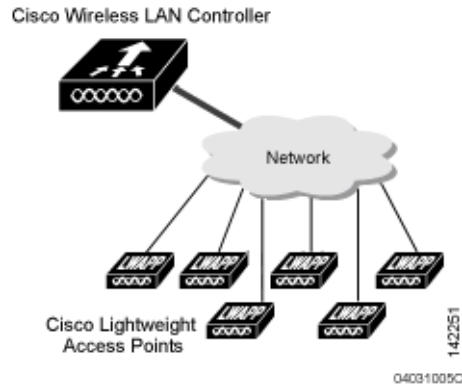


Note

Some controllers can connect through multiple physical ports to multiple subnets in the network. This feature can be helpful when Cisco WLAN Solution operators want to confine multiple VLANs to separate subnets.

Figure 1-2 shows a typical single-controller deployment.

Figure 1-2 Single-Controller Deployment



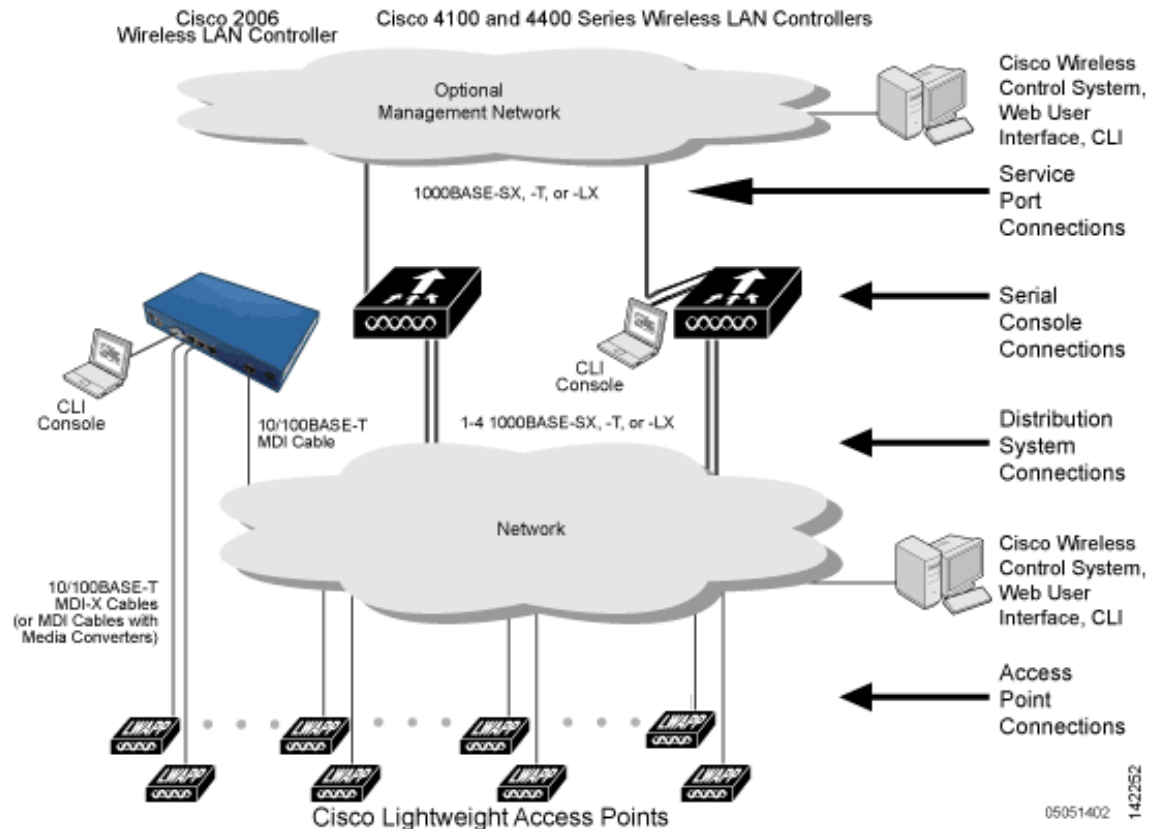
Multiple-Controller Deployments

Each controller can support lightweight access points across multiple floors and buildings simultaneously. However, full functionality of the Cisco Wireless LAN Solution is realized when it includes multiple controllers. A multiple-controller system has the following additional features:

- Autodetecting and autoconfiguring RF parameters as the controllers are added to the network.
- [Same-Subnet \(Layer 2\) Roaming](#) and [Inter-Subnet \(Layer 3\) Roaming](#).
- Automatic access point failover to any redundant controller with a reduced access point load (refer to the [“Cisco Wireless LAN Controller Failover Protection”](#) section on page 1-20).

The following figure shows a typical multiple-controller deployment. The figure also shows an optional dedicated Management Network and the three physical connection types between the network and the controllers.

Figure 1-3 Typical Multi-Controller Deployment



Operating System Software

The operating system software controls Cisco Wireless LAN Controllers and Cisco 1000 Series Lightweight Access Points. It includes full operating system security and Radio Resource Management (RRM) features.

Operating System Security

Operating system security bundles Layer 1, Layer 2, and Layer 3 security components into a simple, Cisco WLAN Solution-wide policy manager that creates independent security policies for each of up to 16 wireless LANs. (Refer to the [“Cisco WLAN Solution Wireless LANs”](#) section on page 1-11.)

The 802.11 Static WEP weaknesses can be overcome using robust industry-standard security solutions, such as:

- 802.1X dynamic keys with extensible authentication protocol (EAP).
- Wi-Fi protected access (WPA) dynamic keys. The Cisco WLAN Solution WPA implementation includes:
 - Temporal key integrity protocol (TKIP) + message integrity code checksum (Michael) dynamic keys, or
 - WEP keys, with or without Pre-Shared key Passphrase.

- RSN with or without Pre-Shared key.
- Cranite FIPS140-2 compliant passthrough.
- Fortress FIPS140-2 compliant passthrough.
- Optional MAC Filtering.

The WEP problem can be further solved using industry-standard Layer 3 security solutions, such as:

- Terminated and passthrough VPNs
- Terminated and passthrough Layer Two Tunneling Protocol (L2TP), which uses the IP Security (IPSec) protocol.
- Terminated and pass-through IPSec protocols. The terminated Cisco WLAN Solution IPSec implementation includes:
 - Internet key exchange (IKE)
 - Diffie-Hellman (DH) groups, and
 - Three optional levels of encryption: DES (ANSI X.3.92 data encryption standard), 3DES (ANSI X9.52-1998 data encryption standard), or AES/CBC (advanced encryption standard/cipher block chaining).

The Cisco WLAN Solution IPSec implementation also includes industry-standard authentication using:

- Message digest algorithm (MD5), or
- Secure hash algorithm-1 (SHA-1)
- The Cisco Wireless LAN Solution supports local and RADIUS MAC Address filtering.
- The Cisco Wireless LAN Solution supports local and RADIUS user/password authentication.
- The Cisco Wireless LAN Solution also uses manual and automated Disabling to block access to network services. In manual Disabling, the operator blocks access using client MAC addresses. In automated Disabling, which is always active, the operating system software automatically blocks access to network services for an operator-defined period of time when a client fails to authenticate for a fixed number of consecutive attempts. This can be used to deter brute-force login attacks.

These and other security features use industry-standard authorization and authentication methods to ensure the highest possible security for your business-critical wireless LAN traffic.

Cisco WLAN Solution Wired Security

Many traditional access point vendors concentrate on security for the Wireless interface similar to that described in the [“Operating System Security” section on page 1-5](#). However, for secure Cisco Wireless LAN Controller Service Interfaces, Cisco Wireless LAN Controller to access point, and inter-Cisco Wireless LAN Controller communications during device servicing and client roaming, the operating system includes built-in security.

Each Cisco Wireless LAN Controller and Cisco 1000 series lightweight access point is manufactured with a unique, signed X.509 certificate. This certificate is used to authenticate IPSec tunnels between devices. These IPSec tunnels ensure secure communications for mobility and device servicing.

Cisco Wireless LAN Controllers and Cisco 1000 series lightweight access points also use the signed certificates to verify downloaded code before it is loaded, ensuring that hackers do not download malicious code into any Cisco Wireless LAN Controller or Cisco 1000 series lightweight access point.

Layer 2 and Layer 3 LWAPP Operation

The LWAPP communications between Cisco Wireless LAN Controller and Cisco 1000 series lightweight access points can be conducted at ISO Data Link Layer 2 or Network Layer 3.

**Note**

The IPv4 network layer protocol is supported for transport through an LWAPP controller system. IPv6 (for clients only) and Appletalk are also supported but only on 4400 series controllers and the Cisco WiSM. Other Layer 3 protocols (such as IPX, DECnet Phase IV, OSI CLNP, and so on) and Layer 2 (bridged) protocols (such as LAT and NetBeui) are not supported.

Operational Requirements

The requirement for Layer 2 LWAPP communications is that the Cisco Wireless LAN Controller and Cisco 1000 series lightweight access points must be connected to each other through Layer 2 devices on the same subnet. This is the default operational mode for the Cisco Wireless LAN Solution. Note that when the Cisco Wireless LAN Controller and Cisco 1000 series lightweight access points are on different subnets, these devices must be operated in Layer 3 mode.

The requirement for Layer 3 LWAPP communications is that the Cisco Wireless LAN Controllers and Cisco 1000 series lightweight access points can be connected through Layer 2 devices on the same subnet, or connected through Layer 3 devices across subnets.

Note that all Cisco Wireless LAN Controllers in a mobility group must use the same LWAPP Layer 2 or Layer 3 mode, or you will defeat the Mobility software algorithm.

Configuration Requirements

When you are operating the Cisco Wireless LAN Solution in Layer 2 mode, you must configure a management interface to control your Layer 2 communications.

When you are operating the Cisco Wireless LAN Solution in Layer 3 mode, you must configure an AP-manager interface to control Cisco 1000 series lightweight access points and a management interface as configured for Layer 2 mode.

Cisco Wireless LAN Controllers

When you are adding Cisco 1000 series lightweight access points to a multiple Cisco Wireless LAN Controller deployments network, it is convenient to have all Cisco 1000 series lightweight access points associate with one master controller on the same subnet. That way, the operator does not have to log into multiple controllers to find out which controller newly-added Cisco 1000 series lightweight access points associated with.

One controller in each subnet can be assigned as the master controller while adding lightweight access points. As long as a master controller is active on the same subnet, all new access points without a primary, secondary, and tertiary controller assigned automatically attempt to associate with the master Cisco Wireless LAN Controller. This process is described in the [“Cisco Wireless LAN Controller Failover Protection”](#) section on page 1-20.

The operator can monitor the master controller using the WCS Web User Interface and watch as access points associate with the master controller. The operator can then verify access point configuration and assign a primary, secondary, and tertiary controller to the access point, and reboot the access point so it reassociates with its primary, secondary, or tertiary controller.

**Note**

Lightweight access points without a primary, secondary, and tertiary controller assigned always search for a master controller first upon reboot. After adding lightweight access points through the master controller, assign primary, secondary, and tertiary controllers to each access point. Cisco recommends that you disable the master setting on all controllers after initial configuration.

Primary, Secondary, and Tertiary Controllers

In multiple-controller networks, lightweight access points can associate with any controller on the same subnet. To ensure that each access point associates with a particular controller, the operator can assign primary, secondary, and tertiary controllers to the access point.

When a primed access point is added to a network, it looks for its primary, secondary, and tertiary controllers first, then a master controller, then the least-loaded controller with available access point ports. Refer to the [“Cisco Wireless LAN Controller Failover Protection” section on page 1-20](#) for more information.

Client Roaming

The Cisco Wireless LAN Solution supports seamless client roaming across Cisco 1000 series lightweight access points managed by the same Cisco Wireless LAN Controller, between Cisco Wireless LAN Controllers in the same Cisco WLAN Solution Mobility Group on the same subnet, and across controllers in the same Mobility Group on different subnets.

Same-Subnet (Layer 2) Roaming

Each Cisco Wireless LAN Controller supports same-controller client roaming across access points managed by the same controller. This roaming is transparent to the client as the session is sustained and the client continues using the same DHCP-assigned or client-assigned IP Address. The controller provides DHCP functionality with a relay function. Same-controller roaming is supported in single-controller deployments and in multiple-controller deployments.

Inter-Controller (Layer 2) Roaming

In multiple-controller deployments, the Cisco Wireless LAN Solution supports client roaming across access points managed by controllers in the same mobility group and on the same subnet. This roaming is also transparent to the client, as the session is sustained and a tunnel between controllers allows the client to continue using the same DHCP- or client-assigned IP Address as long as the session remains active. Note that the tunnel is torn down and the client must reauthenticate when the client sends a DHCP Discover with a 0.0.0.0 client IP Address or a 169.254.*.* client auto-IP Address, or when the operator-set session timeout is exceeded.

Note that the Cisco 1030 remote edge lightweight access points at a remote location must be on the same subnet to support roaming.

Inter-Subnet (Layer 3) Roaming

In multiple-controller deployments, the Cisco Wireless LAN Solution supports client roaming across access points managed by controllers in the same mobility group on different subnets. This roaming is transparent to the client, because the session is sustained and a tunnel between the controllers allows the client to continue using the same DHCP-assigned or client-assigned IP Address as long as the session remains active. Note that the tunnel is torn down and the client must reauthenticate when the client sends a DHCP Discover with a 0.0.0.0 client IP Address or a 169.254.*.* client auto-IP Address or when the operator-set user timeout is exceeded.

Note that the Cisco 1030 remote edge lightweight access points at a remote location must be on the same subnet to support roaming.

Special Case: Voice Over IP Telephone Roaming

802.11 VoIP telephones actively seek out associations with the strongest RF signal to ensure best Quality of Service (QoS) and maximum throughput. The minimum VoIP telephone requirement of 20 millisecond or shorter latency time for the roaming handover is easily met by the Cisco Wireless LAN Solution, which has an average handover latency of nine or fewer milliseconds.

This short latency period is controlled by Cisco Wireless LAN Controllers, rather than allowing independent access points to negotiate roaming handovers.

The Cisco Wireless LAN Solution supports 802.11 VoIP telephone roaming across Cisco 1000 series lightweight access points managed by Cisco Wireless LAN Controllers on different subnets, as long as the controllers are in the same mobility group. This roaming is transparent to the VoIP telephone, because the session is sustained and a tunnel between controllers allows the VoIP telephone to continue using the same DHCP-assigned IP Address as long as the session remains active. Note that the tunnel is torn down and the VoIP client must reauthenticate when the VoIP telephone sends a DHCP Discover with a 0.0.0.0 VoIP telephone IP Address or a 169.254.*.* VoIP telephone auto-IP Address or when the operator-set user timeout is exceeded.

Client Location

When you use Cisco WCS in your Cisco Wireless LAN Solution, controllers periodically determine client, rogue access point, rogue access point client, radio frequency ID (RFID) tag location and store the locations in the Cisco WCS database. For more information on location solutions, refer to the *Cisco Wireless Control System Configuration Guide* and the *Cisco Location Appliance Configuration Guide* at these URLs:

Cisco Wireless Control System Configuration Guide:

http://www.cisco.com/en/US/products/ps6305/products_installation_and_configuration_guides_list.html

Cisco Location Appliance Configuration Guide:

http://www.cisco.com/en/US/products/ps6386/products_installation_and_configuration_guides_list.html

External DHCP Servers

The operating system is designed to appear as a DHCP Relay to the network and as a DHCP Server to clients with industry-standard external DHCP Servers that support DHCP Relay. This means that each Cisco Wireless LAN Controller appears as a DHCP Relay agent to the DHCP Server. This also means that the Cisco Wireless LAN Controller appears as a DHCP Server at the virtual IP Address to wireless clients.

Because the Cisco Wireless LAN Controller captures the client IP Address obtained from a DHCP Server, it maintains the same IP Address for that client during same-Cisco Wireless LAN Controller, inter-Cisco Wireless LAN Controller, and inter-subnet client roaming.

Per-Wireless LAN Assignment

All Cisco WLAN Solution wireless LANs can be configured to use the same or different DHCP Servers, or no DHCP Server. This allows operators considerable flexibility in configuring their Wireless LANs, as further described in the [“Cisco WLAN Solution Wireless LANs” section on page 1-11](#).

Note that Cisco WLAN Solution wireless LANs that support management over wireless must allow the management (device servicing) clients to obtain an IP Address from a DHCP Server. See the [“Using Management over Wireless” section on page 5-6](#) for instructions on configuring management over wireless.

Per-Interface Assignment

You can assign DHCP servers for individual interfaces. The Layer 2 management interface, Layer 3 AP-manager interface, and dynamic interfaces can be configured for a primary and secondary DHCP server, and the service-port interface can be configured to enable or disable DHCP servers.

**Note**

Refer to [Chapter 3](#) for information on configuring the controller’s interfaces.

Security Considerations

For enhanced security, Cisco recommends that operators require all clients to obtain their IP Addresses from a DHCP server. To enforce this requirement, all wireless LANs can be configured with a DHCP Required setting and a valid DHCP Server IP Address, which disallows client static IP Addresses. If a client associating with a wireless LAN with DHCP Required set does not obtain its IP Address from the designated DHCP Server, it is not allowed access to any network services.

Note that if DHCP Required is selected, clients must obtain an IP address via DHCP. Any client with a static IP address will not be allowed on the network. The Cisco Wireless LAN Controller monitors DHCP traffic because it acts as a DHCP proxy for the clients.

If slightly less security is tolerable, operators can create wireless LANs with DHCP Required disabled and a valid DHCP Server IP Address. Clients then have the option of using a static IP Address or obtaining an IP Address from the designated DHCP Server.

Operators are also allowed to create separate wireless LANs with DHCP Required disabled and a DHCP Server IP Address of 0.0.0.0. These wireless LANs drop all DHCP requests and force clients to use a static IP Address. Note that these wireless LANs do not support management over wireless connections.

Cisco WLAN Solution Wired Connections

The Cisco Wireless LAN Solution components communicate with each other using industry-standard Ethernet cables and connectors. The following paragraphs contain details of the Cisco WLAN Solution wired connections.

- The Cisco 2000 Series Wireless LAN Controller connects to the network using from one to four 10/100BASE-T Ethernet cables.
- The Cisco 4100 Series Wireless LAN Controller connects to the network using one or two fiber-optic Gigabit Ethernet cables: two redundant Gigabit Ethernet connections to bypass single network failures.
- The Cisco 4402 Wireless LAN Controller connects to the network using one or two fiber-optic Gigabit Ethernet cables, and the 4404 Wireless LAN Controller connects to the network using up to four fiber-optic Gigabit Ethernet cables: two redundant Gigabit Ethernet connections to bypass single network failures.
- The controllers on the Wireless Services Module (WiSM), installed in a Cisco Catalyst 6500 Series Switch, connect to the network through switch ports on the switch.
- The Wireless LAN Controller Network Module, installed in a Cisco Integrated Services Router, connects to the network through the ports on the router.
- Cisco 1000 series lightweight access points connects to the network using 10/100BASE-T Ethernet cables. The standard CAT-5 cable can also be used to conduct power for the Cisco 1000 series lightweight access points from a network device equipped with Power over Ethernet (PoE) capability. This power distribution plan can be used to reduce the cost of individual AP power supplies and related cabling.

Cisco WLAN Solution Wireless LANs

The Cisco Wireless LAN Solution can control up to 16 Wireless LANs for lightweight access points. Each wireless LAN has a separate wireless LAN ID (1 through 16), a separate wireless LAN SSID (wireless LAN name), and can be assigned unique security policies. Using software release 3.2 and later you can configure both static and dynamic WEP on the same wireless LAN.

The Cisco 1000 series lightweight access points broadcast all active Cisco WLAN Solution wireless LAN SSIDs and enforce the policies defined for each wireless LAN.

**Note**

Cisco recommends that you assign one set of VLANs for wireless LANs and a different set of VLANs for management interfaces to ensure that controllers operate with optimum performance and ease of management.

If management over wireless is enabled across Cisco Wireless LAN Solution, the Cisco Wireless LAN Solution operator can manage the System across the enabled wireless LAN using CLI and Telnet, http/https, and SNMP.

To configure the Cisco WLAN Solution wireless LANs, refer to [Chapter 6, “Configuring WLANs.”](#)

Access Control Lists

The operating system allows you to define up to 64 Access Control Lists (ACLs), similar to standard firewall Access Control Lists. Each ACL can have up to 64 Rules (filters).

Operators can use ACLs to control client access to multiple VPN servers within a given wireless LAN. If all the clients on a wireless LAN must access a single VPN server, use the IPSec/VPN Gateway Passthrough setting, described in the [“Security Overview” section on page 5-2](#).

After they are defined, the ACLs can be applied to the management interface, the AP-Manager interface, or any of the operator-defined interfaces.

Refer to Access Control Lists > New in the *Web User Interface Online Help* for instructions on configuring Access Control Lists.

Identity Networking

Cisco Wireless LAN Controllers can have the following parameters applied to all clients associating with a particular wireless LAN: QoS, global or Interface-specific DHCP server, Layer 2 and Layer 3 Security Policies, and default Interface (which includes physical port, VLAN and ACL assignments).

However, the Cisco Wireless LAN Controller can also have individual clients (MAC addresses) override the preset wireless LAN parameters by using MAC Filtering or by Allowing AAA Override parameters. This configuration can be used, for example, to have all company clients log into the corporate wireless LAN, and then have clients connect using different QoS, DHCP server, Layer 2 and Layer 3 Security Policies, and Interface (which includes physical port, VLAN and ACL assignments) settings on a per-MAC Address basis.

When Cisco Wireless LAN Solution operators configure MAC Filtering for a client, they can assign a different VLAN to the MAC Address, which can be used to have operating system automatically reroute the client to the management interface or any of the operator-defined interfaces, each of which have their own VLAN, ACL, DHCP server, and physical port assignments. This MAC Filtering can be used as a coarse version of AAA Override, and normally takes precedence over any AAA (RADIUS or other) Override.

However, when Allow AAA Override is enabled, the RADIUS (or other AAA) server can alternatively be configured to return QoS and ACL on a per-MAC Address basis. Allow AAA Override gives the AAA Override precedence over the MAC Filtering parameters set in the Cisco Wireless LAN Controller; if there are no AAA Overrides available for a given MAC Address, the operating system uses the MAC Filtering parameters already in the Cisco Wireless LAN Controller. This AAA (RADIUS or other) Override can be used as a finer version of AAA Override, but only takes precedence over MAC Filtering when Allow AAA Override is enabled.

Note that in all cases, the Override parameters (Operator-Defined Interface and QoS, for example) must already be defined in the Cisco Wireless LAN Controller configuration.

In all cases, the operating system will use QoS and ACL provided by the AAA server or MAC Filtering regardless of the Layer 2 and/or Layer 3 authentication used.

Also note that the operating system will only move clients from the default Cisco WLAN Solution wireless LAN VLAN to a different VLAN when configured for MAC filtering, 802.1X, and/or WPA Layer 2 authentication.

To configure the Cisco WLAN Solution wireless LANs, refer to the [“Configuring Wireless LANs” section on page 6-2](#).

Enhanced Integration with Cisco Secure ACS

The identity-based networking feature uses authentication, authorization, and accounting (AAA) override. When the following vendor-specific attributes are present in the RADIUS access accept message, the values override those present in the wireless LAN profile:

- QoS level
- 802.1p value
- VLAN interface name
- Access control list (ACL) name

In this release, support is being added for the AAA server to return the VLAN number or name using the standard “RADIUS assigned VLAN name/number” feature defined in IETF RFC 2868 (RADIUS Attributes for Tunnel Protocol Support). To assign a wireless client to a particular VLAN, the AAA server sends the following attributes to the controller in the access accept message:

- IETF 64 (Tunnel Type): VLAN
- IETF 65 (Tunnel Medium Type): 802
- IETF 81 (Tunnel Private Group ID): VLAN # or VLAN Name String

This enables Cisco Secure ACS to communicate a VLAN change that may be a result of a posture analysis. Benefits of this new feature include:

- Integration with Cisco Secure ACS reduces installation and setup time
- Cisco Secure ACS operates smoothly across both wired and wireless networks

This feature supports 2000, 4100, and 4400 series controllers and 1000, 1130, 1200 and 1500 series lightweight access points.

File Transfers

The Cisco Wireless LAN Solution operator can upload and download operating system code, configuration, and certificate files to and from a Cisco Wireless LAN Controller using CLI commands, Web User Interface commands, or Cisco WCS.

- To use CLI commands, refer to the “[Transferring Files to and from a Controller](#)” section on [page 8-2](#).
- To use Cisco WCS to upgrade software, refer to the *Cisco Wireless Control System Configuration Guide*. Click this URL to browse to this document:
http://www.cisco.com/en/US/products/ps6305/products_installation_and_configuration_guides_list.html

Power over Ethernet

Lightweight access points can receive power via their Ethernet cables from 802.3af-compatible Power over Ethernet (PoE) devices, which can reduce the cost of discrete power supplies, additional wiring, conduits, outlets, and installer time. PoE also frees installers from having to mount Cisco 1000 series lightweight access points or other powered equipment near AC outlets, providing greater flexibility in positioning Cisco 1000 series lightweight access points for maximum coverage.

When you are using PoE, the installer runs a single CAT-5 cable from each lightweight access point to PoE-equipped network elements, such as a PoE power hub or a Cisco WLAN Solution Single-Line PoE Injector. When the PoE equipment determines that the lightweight access point is PoE-enabled, it sends 48 VDC over the unused pairs in the Ethernet cable to power the lightweight access point.

The PoE cable length is limited by the 100BASE-T or 10BASE-T specification to 100 m or 200 m, respectively.

Lightweight access points can receive power from an 802.3af-compliant device or from the external power supply.

Pico Cell Functionality

A Pico Cell is a small area of wireless provisioning provided by antenna, which allows for a dense high-bandwidth deployment for installations such as stock exchanges. Pico Cell wireless configurations require a specific supplicant to function correctly with Pico Cell environments. Off-the-shelf laptop supplicants are not supported.

**Note**

Do not attempt to configure Pico Cell functionality within your wireless LAN without consulting your sales team. Non-standard installation is not supported.

**Note**

Do not change the configuration database setting unless you are committing to a Pico Cell installation or without the advice of Cisco technical support.

Pico Cell functionality includes optimization of the operating system (operating system) to support this functionality as follows:

- The Cisco WCS Pico Cell Mode parameter reconfigures operating system parameters, allowing operating system to function efficiently in pico cell deployments. Note that when the operator is deploying a pico cell network the operating system must also have more memory allocated (512 to 2048 MB) using the **config database size 2048** CLI command.
- Client mobility between multiple mobility domains when such exist.
- Addition of a WPA2 VFF extension to eliminate the need to re-key after every association. This allows the re-use of existing PTK and GTK.
- With WPA2 PMK caching and VFF, the PMK cache is transferred as part of context transfer prior to the authentication phase. This allows expedited handoffs to work for both intra- and inter-Cisco Wireless LAN Controller roaming events.
- A beacon/probe response that allows a Cisco 1000 Series lightweight access point to indicate which Cisco Wireless LAN Controller it is attached to so that reauthorization events only occur when needed, minimizing inter-Cisco Wireless LAN Controller handoffs and thus reducing CPU usage.

- Allows changes to Cisco 1000 series lightweight access point sensitivity for pico cells.
- Allows control of Cisco 1000 series lightweight access point fallback behavior to optimize pico cell use.
- Supports heat maps for directional antennas.
- Allows specific control over blacklisting events
- Allows configuring and viewing basic LWAPP configuration using the Cisco 1000 series lightweight access point CLI.

Intrusion Detection Service (IDS)

Intrusion Detection Service includes the following:

- Sensing Clients probing for “ANY” SSID
- Sensing if Cisco 1000 series lightweight access points are being contained
- Notification of MiM Attacks, NetStumbler, Wellenreiter
- Management Frame Detection and RF Jamming Detection
- Spoofed Deauthentication Detection (AirJack, for example)
- Broadcast Deauthorization Detection
- Null Probe Response Detection
- Fake AP Detection
- Detection of Weak WEP Encryption
- MAC Spoofing Detection
- AP Impersonation Detection
- Honeypot AP Detection
- Valid Station Protection
- Misconfigured AP Protection
- Rogue Access Point Detection
- AD-HOC Detection and Protection
- Wireless Bridge Detection
- Asleep Detection / Protection

Wireless LAN Controller Platforms

Cisco controllers are enterprise-class high-performance wireless switching platforms that support 802.11a and 802.11b/802.11g protocols. They operate under control of the operating system, which includes the Radio Resource Management (RRM), creating a Cisco WLAN Solution that can automatically adjust to real-time changes in the 802.11 RF environment. The controllers are built around high-performance network and security hardware, resulting in highly-reliable 802.11 enterprise networks with unparalleled security.

Cisco 2000 Series Wireless LAN Controllers

The Cisco 2000 Series Wireless LAN Controller is part of the Cisco Wireless LAN Solution. Each 2000 series controller controls up to six Cisco 1000 series lightweight access points, making it ideal for smaller enterprises and low-density applications.

The Cisco 2000 Series Wireless LAN Controller is a slim 9.5 x 6.0 x 1.6 in. (241 x 152 x 41 mm) chassis that can be desktop or shelf mounted. The Cisco 2000 Series Wireless LAN 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 Cisco 2000 Series Wireless LAN Controller is shipped with four rubber desktop/shelf mounting feet.

Cisco 4100 Series Wireless LAN Controllers

The Cisco 4100 Series Wireless LAN Controllers are part of the Cisco Wireless LAN Solution. Each Cisco 4100 Series Wireless LAN Controller controls up to 36 Cisco 1000 series lightweight access points, making it ideal for medium-sized enterprises and medium-density applications.

Figure 1-4 shows the Cisco 4100 Series Wireless LAN Controller, which has two redundant front-panel SX/LC jacks. Note that the 1000BASE-SX circuit provides a 100/1000 Mbps wired connection to a network through an 850nm (SX) fiber-optic link using an LC physical connector.

Figure 1-4 4100 Series Controller



The Cisco 4100 Series Wireless LAN Controller can be factory-ordered with a VPN/Enhanced Security Module (Crypto Card) to support VPN, IPSec and other processor-intensive tasks, and contains two (Cisco 4100 Series Wireless LAN Controller) 1000BASE-SX network connectors that allow the Cisco 4100 Series Wireless LAN Controller to communicate with the network at Gigabit Ethernet speeds. The 1000BASE-SX network connectors provides 100/1000 Mbps wired connections to a network through 850nm (SX) fiber-optic links using LC physical connectors.

The two redundant Gigabit Ethernet connections on the Cisco 4100 Series Wireless LAN Controller allow the Cisco 4100 Series Wireless LAN Controller to bypass single network failures.

Cisco 4400 Series Wireless LAN Controllers

Cisco 4400 Series Wireless LAN Controllers are part of the Cisco Wireless LAN Solution. Each Cisco 4400 Series Wireless LAN Controller controls up to 100 Cisco 1000 series lightweight access points, making it ideal for large-sized enterprises and large-density applications.

The 4402 Cisco 4400 Series Wireless LAN Controller has one set of two redundant front-panel SX/LC/T SFP modules (SFP transceiver, or Small Form-factor Plug-in), and the 4404 Cisco 4400 Series Wireless LAN Controller has two sets of two redundant front-panel SX/LC/T SFP modules:

- 1000BASE-SX SFP modules provide a 1000 Mbps wired connection to a network through an 850nm (SX) fiber-optic link using an LC physical connector.
- 1000BASE-LX SFP modules provide a 1000 Mbps wired connection to a network through a 1300nm (LX/LH) fiber-optic link using an LC physical connector.
- 1000BASE-T SFP modules provide a 1000 Mbps wired connection to a network through a copper link using an RJ-45 physical connector.

The one or two sets of redundant Gigabit Ethernet connections on the Cisco 4400 Series Wireless LAN Controller allow the Cisco 4400 Series Wireless LAN Controller to bypass single network failures.

The Cisco 4400 Series Wireless LAN Controller can be equipped with one or two Cisco 4400 series power supplies. When the Cisco Wireless LAN Controller is equipped with two Cisco 4400 series power supplies, the power supplies are redundant and either power supply can continue to power the Cisco 4400 Series Wireless LAN Controller if the other power supply fails.

One Cisco 4400 series power supply is included standard with the Cisco Wireless LAN Controller, and is installed in Slot 1 at the factory. For redundancy, a second Cisco 4400 series power supply can be ordered from the factory and may be installed in Slot 2. The same power supply also fits in Slot 1 and can be used to replace a failed power supply in the field.

Cisco 2000 Series Wireless LAN Controller Model Numbers

Cisco 2000 Series Wireless LAN Controller model number is as follows:

- AIR-WLC2006-K9 — The Cisco 2000 Series Wireless LAN Controller communicates with up to six Cisco 1000 series lightweight access points.

**Note**

Cisco 2000 Series Wireless LAN Controllers come from the factory with tabletop mounting feet.

Cisco 4100 Series Wireless LAN Controller Model Numbers

Cisco 4100 Series Wireless LAN Controller model numbers are as follows:

- AIR-WLC4112-K9 — The Cisco 4100 Series Wireless LAN Controller uses two redundant Gigabit Ethernet connections to bypass single network failures, and communicates with up to 12 Cisco 1000 series lightweight access points. The 1000BASE-SX Network Adapters provide 100/1000 Mbps wired connections to a network through 850nm (SX) fiber-optic links using LC physical connectors.
- AIR-WLC4124-K9 — The Cisco 4100 Series Wireless LAN Controller uses two redundant Gigabit Ethernet connections to bypass single network failures, and communicates with up to 24 Cisco 1000 series lightweight access points.
- AIR-WLC4136-K9 — The Cisco 4100 Series Wireless LAN Controller uses two redundant Gigabit Ethernet connections to bypass single network failures, and communicates with up to 36 Cisco 1000 series lightweight access points.

**Note**

Cisco 4100 Series Wireless LAN Controller models come from the factory with 19-inch EIA equipment rack flush-mount ears.

The following upgrade module is also available:

- AIR-VPN-4100 — VPN/Enhanced Security Module: Supports VPN, L2TP, IPSec and other processor-intensive security options. This is a field-installable option for all Cisco 4100 Series Wireless LAN Controllers.

Cisco 4400 Series Wireless LAN Controller Model Numbers

Cisco 4400 Series Wireless LAN Controller model numbers are as follows:

- AIR-WLC4402-12-K9 — The 4402 Cisco 4400 Series Wireless LAN Controller uses two redundant Gigabit Ethernet connections to bypass single network failures, and communicates with up to 12 Cisco 1000 series lightweight access points.
- AIR-WLC4402-25-K9 — The 4402 Cisco Wireless LAN Controller uses two redundant Gigabit Ethernet connections to bypass single network failures, and communicates with up to 25 Cisco 1000 series lightweight access points.
- AIR-WLC4402-50-K9 — The 4402 Cisco Wireless LAN Controller uses two redundant Gigabit Ethernet connections to bypass single network failures, and communicates with up to 50 Cisco 1000 series lightweight access points.
- AIR-WLC4404-100-K9 — The 4404 Cisco Wireless LAN Controller uses four redundant Gigabit Ethernet connections to bypass one or two single network failures, and communicates with up to 100 Cisco 1000 series lightweight access points.

**Note**

Cisco 4400 Series Wireless LAN Controller models come from the factory with integral 19-inch EIA equipment rack flush-mount ears.

The 4402 Cisco 4400 Series Wireless LAN Controller uses one set of two redundant front-panel SX/LC/T SFP modules (SFP transceiver, or Small Form-factor Plug-in), and the 4404 Cisco 4400 Series Wireless LAN Controller uses two sets of two redundant front-panel SX/LC/T SFP modules:

- 1000BASE-SX SFP modules provide a 1000 Mbps wired connection to a network through an 850nm (SX) fiber-optic link using an LC physical connector.
- 1000BASE-LX SFP modules provide a 1000 Mbps wired connection to a network through a 1300nm (LX/LH) fiber-optic link using an LC physical connector.
- 1000BASE-T SFP modules provide a 1000 Mbps wired connection to a network through a copper link using an RJ-45 physical connector.

The following power supply module is also available:

- AIR-PWR-4400-AC — All Cisco 4400 series power supplies. One Cisco 4400 series power supply can power Cisco 4400 series power supplies, the Cisco 4400 series power supplies are redundant.

Startup Wizard

When an Cisco Wireless LAN Controller is powered up with a new factory operating system software load or after being reset to factory defaults, the bootup script runs the Startup Wizard, which prompts the installer for initial configuration. The Startup Wizard:

- Ensures that the Cisco Wireless LAN Controller has a System Name, up to 32 characters.
- Adds an Administrative username and password, each up to 24 characters.
- Ensures that the Cisco Wireless LAN Controller can communicate with the CLI, Cisco WCS, or Web User interfaces (either directly or indirectly) through the service port by accepting a valid IP configuration protocol (none or DHCP), and if none, IP Address and netmask. If you do not want to use the Service port, enter 0.0.0.0 for the IP Address and netmask.
- Ensures that the Cisco Wireless LAN Controller can communicate with the network (802.11 Distribution System) through the management interface by collecting a valid static IP Address, netmask, default router IP address, VLAN identifier, and physical port assignment.
- Prompts for the IP address of the DHCP server used to supply IP addresses to clients, the Cisco Wireless LAN Controller Management Interface, and optionally to the Service Port Interface.
- Asks for the LWAPP Transport Mode, described in the [“Layer 2 and Layer 3 LWAPP Operation” section on page 1-7](#).
- Collects the Virtual Gateway IP Address; any fictitious, unassigned IP address (such as 1.1.1.1) to be used by Layer 3 Security and Mobility managers.
- Allows you to enter the Mobility Group (RF Group) Name.
- Collects the wireless LAN 1 802.11 SSID, or Network Name.
- Asks you to define whether or not clients can use static IP addresses. 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 DHCP for an IP Address, works well for Windows XP devices.
- If you want to configure a RADIUS server from the Startup Wizard, the RADIUS server IP address, communication port, and Secret.
- Collects the Country Code.

- Enables and/or disables the 802.11a, 802.11b and 802.11g Cisco 1000 series lightweight access point networks.
- Enables or disables Radio Resource Management (RRM).

To use the Startup Wizard, refer to the [“Using the Configuration Wizard”](#) section on page 4-2.

Cisco Wireless LAN Controller Memory

The Cisco Wireless LAN Controller contain two kinds of memory: volatile RAM, which holds the current, active Cisco Wireless LAN Controller configuration, and NVRAM (non-volatile RAM), which holds the reboot configuration. When you are configuring the operating system in a Cisco Wireless LAN Controller, you are modifying volatile RAM; you must save the configuration from the volatile RAM to the NVRAM to ensure that the Cisco Wireless LAN Controller reboots in the current configuration.

Knowing which memory you are modifying is important when you are:

- [Using the Configuration Wizard](#)
- [Clearing the Controller Configuration](#)
- [Saving Configurations](#)
- [Resetting the Controller](#)
- [Logging Out of the CLI](#)

Cisco Wireless LAN Controller Failover Protection

Each Cisco Wireless LAN Controller has a defined number of communication ports for Cisco 1000 series lightweight access points. This means that when multiple controllers with unused access point ports are deployed on the same network, if one controller fails, the dropped access points automatically poll for unused controller ports and associate with them.

During installation, Cisco recommends that you connect all lightweight access points to a dedicated controller, and configure each lightweight access point for final operation. This step configures each lightweight access point for a primary, secondary, and tertiary controller, and allows it to store the configured WLAN Solution Mobility Group information.

During failover recovery, the configured lightweight access points obtain an IP address from the local DHCP server (only in Layer 3 Operation), attempt to contact their primary, secondary, and tertiary controllers, and then attempt to contact the IP addresses of the other controllers in the Mobility group. This prevents the access points from spending time sending out blind polling messages, resulting in a faster recovery period.

In multiple-controller deployments, this means that if one controller fails, its dropped access points reboot and do the following under direction of the Radio Resource Management (RRM):

- Obtain an IP address from a local DHCP server (one on the local subnet).
- If the Cisco 1000 series lightweight access point has a primary, secondary, and tertiary controller assigned, it attempts to associate with that controller.
- If the access point has no primary, secondary, or tertiary controllers assigned or if its primary, secondary, or tertiary controllers are unavailable, it attempts to associate with a master controller on the same subnet.

- If the access point finds no master controller on the same subnet, it attempts to contact stored Mobility Group members by IP address.
- Should none of the Mobility Group members be available, and if the Cisco 1000 series lightweight access point has no Primary, Secondary, and Tertiary Cisco Wireless LAN Controllers assigned and there is no master Cisco Wireless LAN Controller active, it attempts to associate with the least-loaded Cisco Wireless LAN Controller on the same subnet to respond to its discovery messages with unused ports.

This means that when sufficient controllers are deployed, should one controller fail, active access point client sessions are momentarily dropped while the dropped access point associates with an unused port on another controller, allowing the client device to immediately reassociate and reauthenticate.

Cisco Wireless LAN Controller Automatic Time Setting

Each controller can have its time manually set or can be configured to obtain the current time from one or more Network Time Protocol (NTP) servers. Each NTP server IP address is added to the controller database. Each controller searches for an NTP server and obtains the current time upon reboot and at each user-defined polling interval (daily to weekly).

Cisco Wireless LAN Controller Time Zones

Each Cisco Wireless LAN Controller can have its time zone manually set or can be configured to obtain the current time from one or more Network Time Protocol (NTP) servers. Each NTP server IP address is added to the Cisco Wireless LAN Controller database. Each Cisco Wireless LAN Controller can search for an NTP server and obtain the current time zone upon reboot and at each user-defined (daily to weekly) polling interval.

Network Connections to Cisco Wireless LAN Controllers

Regardless of operating mode, all Cisco Wireless LAN Controllers use the network as an 802.11 Distribution System. Regardless of the Ethernet port type or speed, each controller monitors and communicates with its related controllers across the network. The following sections give details of these network connections:

- [Cisco 2000 Series Wireless LAN Controllers, page 1-16](#)
- [Cisco 4100 Series Wireless LAN Controllers, page 1-16](#)
- [Cisco 4400 Series Wireless LAN Controllers, page 1-17](#)

**Note**

[Chapter 3](#) provides information on configuring the controller's ports and assigning interfaces to them.

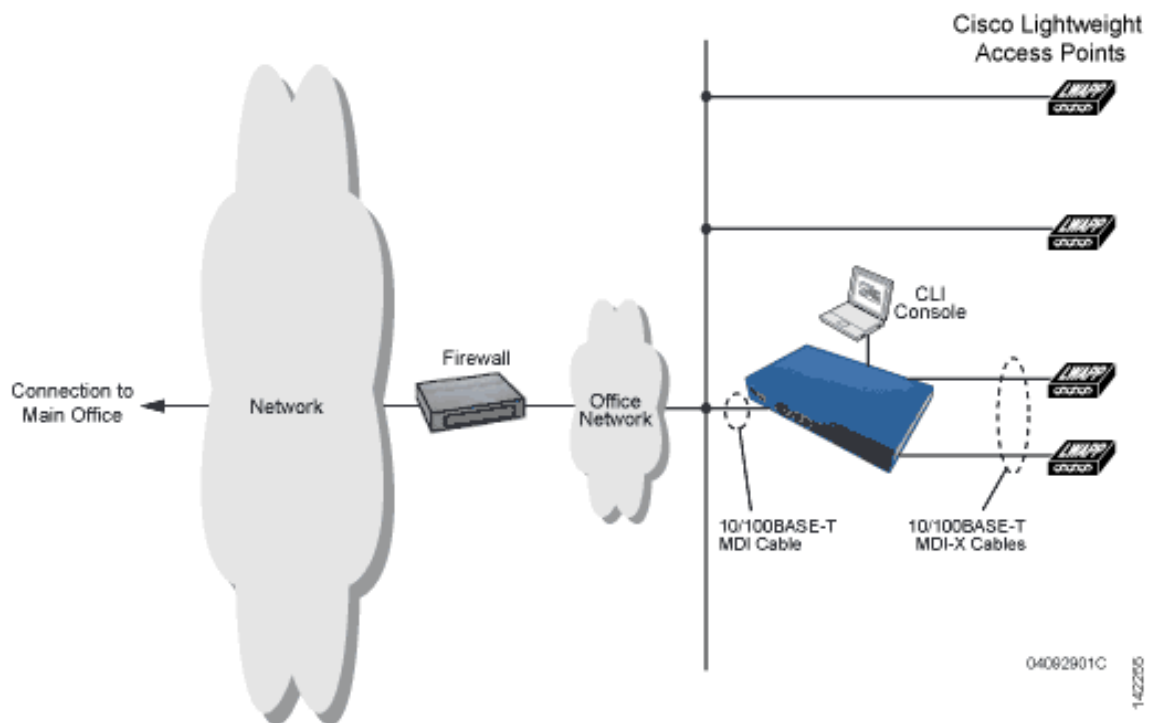
Cisco 2000 Series Wireless LAN Controllers

Cisco 2000 Series Wireless LAN Controllers can communicate with the network through any one of its physical data ports, as the logical management interface can be assigned to one of the ports. The physical port description follows:

- Up to four 10/100BASE-T cables can plug into the four back-panel data ports on the Cisco 2000 Series Wireless LAN Controller chassis.

Figure 1-5 shows connections to the 2000 series controller.

Figure 1-5 Physical Network Connections to the 2000 Series Controller



Cisco 4100 Series Wireless LAN Controllers

Cisco 4100 Series Wireless LAN Controllers can communicate with the network through one or two physical data ports, as the logical management interface can be assigned to one or both ports. The physical port description follows:

- Two Gigabit Ethernet 1000BASE-SX fiber-optic cables can plug into the LC connectors on the front of the Cisco 4100 Series Wireless LAN Controller, and they must be connected to the same subnet. Note that the two Gigabit Ethernet ports are redundant--the first port that becomes active is the master, and the second port becomes the backup port. If the first connection fails, the standby connection becomes the master, and the failed connection becomes the backup port.

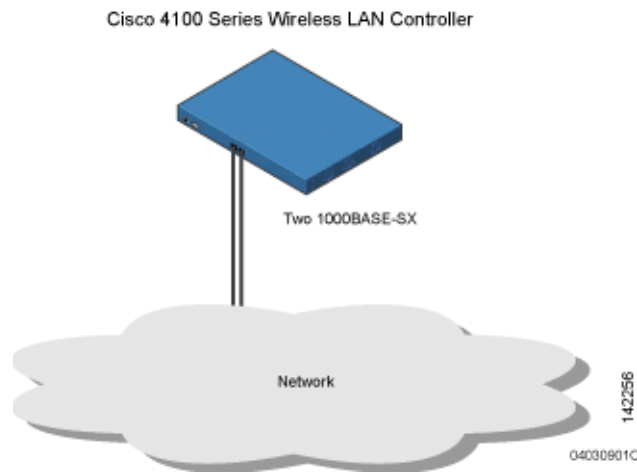


Note

The 1000BASE-SX circuits provide 100/1000 Mbps wired connections to the network through 850nm (SX) fiber-optic links using LC physical connectors.

Figure 1-6 shows connections to the 4100 series controller.

Figure 1-6 Physical Network Connections to the 4100 Series Controller



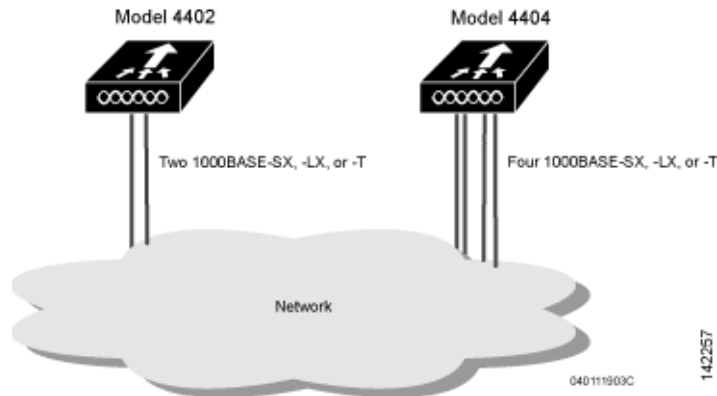
Cisco 4400 Series Wireless LAN Controllers

Cisco 4400 Series Wireless LAN Controllers can communicate with the network through one or two pairs of physical data ports, and the logical management interface can be assigned to the ports. The physical port descriptions follows:

- For the 4402 Cisco Wireless LAN Controller, up to two of the following connections are supported in any combination:
 - 1000BASE-T (Gigabit Ethernet, front panel, RJ-45 physical port, UTP cable).
 - 1000BASE-SX (Gigabit Ethernet, front panel, LC physical port, multi-mode 850nm (SX) fiber-optic links using LC physical connectors).
 - 1000BASE-LX (Gigabit Ethernet, front panel, LC physical port, multi-mode 1300nm (LX/LH) fiber-optic links using LC physical connectors).
- For the 4404 Cisco Wireless LAN Controller, up to four of the following connections are supported in any combination:
 - 1000BASE-T (Gigabit Ethernet, front panel, RJ-45 physical port, UTP cable).
 - 1000BASE-SX (Gigabit Ethernet, front panel, LC physical port, multi-mode 850nm (SX) fiber-optic links using LC physical connectors).
 - 1000BASE-LX (Gigabit Ethernet, front panel, LX physical port, multi-mode 1300nm (LX/LH) fiber-optic links using LC physical connectors).

Figure 1-7 shows connections to the 4400 series controller.

Figure 1-7 Physical Network Connections to 4402 and 4404 Series Controllers



VPN and Enhanced Security Modules for 4100 Series Controllers

All 4100 series controllers can be equipped with an optional module that slides into the rear panel of the controller. The 4100 Series VPN/Enhanced Security Module adds significant hardware encryption acceleration to the controller, which enables the following through the management interface:

- Provide a built-in VPN server for mission-critical traffic.
- Sustain up to 1 Gbps throughput with Layer 2 and Layer 3 encryption enabled.
- Support high-speed, processor-intensive encryption, such as L2TP, IPSec and 3DES.

Rogue Access Points

Because they are inexpensive and readily available, employees sometimes plug unauthorized rogue access points into existing LANs and build ad hoc wireless networks without IT department knowledge or consent.

These rogue access points can be a serious breach of network security because they can be plugged into a network port behind the corporate firewall. Because employees generally do not enable any security settings on the rogue access point, it is easy for unauthorized users to use the access point to intercept network traffic and hijack client sessions. Even more alarming, wireless users and war chalers frequently publish unsecure access point locations, increasing the odds of having the enterprise security breached.

Rather than using a person with a scanner to manually detect rogue access point, the Cisco Wireless LAN Solution automatically collects information on rogue access point detected by its managed access points, by MAC and IP Address, and allows the system operator to locate, tag and monitor them. The operating system can also be used to discourage rogue access point clients by sending them deauthenticate and disassociate messages from one to four Cisco 1000 series lightweight access points. Finally, the operating system can be used to automatically discourage all clients attempting to authenticate with all rogue access point on the enterprise subnet. Because this real-time detection is automated, it saves labor costs used for detecting and monitoring rogue access point while vastly improving LAN security. Note that peer-to-peer, or ad-hoc, clients can also be considered rogue access points.

Rogue Access Point Location, Tagging, and Containment

This built-in detection, tagging, monitoring, and containment capability allows system administrators to take required actions:

- Locate rogue access point as described in the *Cisco Wireless Control System Configuration Guide*.
- Receive new rogue access point notifications, eliminating hallway scans.
- Monitor unknown rogue access point until they are eliminated or acknowledged.
- Determine the closest authorized access point, making directed scans faster and more effective.
- Contain rogue access points by sending their clients deauthenticate and disassociate messages from one to four Cisco 1000 series lightweight access points. This containment can be done for individual rogue access points by MAC address, or can be mandated for all rogue access points connected to the enterprise subnet.
- Tag rogue access points:
 - Acknowledge rogue access point when they are outside of the LAN and do not compromise the LAN or wireless LAN security.
 - Accept rogue access point when they do not compromise the LAN or wireless LAN security.
 - Tag rogue access point as unknown until they are eliminated or acknowledged.
 - Tag rogue access point as contained and discourage clients from associating with the rogue access point by having between one and four Cisco 1000 series lightweight access points transmit deauthenticate and disassociate messages to all rogue access point clients. This function contains all active channels on the same rogue access point.

Rogue Detector mode detects whether or not a rogue access point is on a trusted network. It does not provide RF service of any kind, but rather receives periodic rogue access point reports from the Cisco Wireless LAN Controller, and sniffs all ARP packets. If it finds a match between an ARP request and a MAC address it receives from the Cisco Wireless LAN Controller, it generates a rogue access point alert to the Cisco Wireless LAN Controller.

To facilitate automated rogue access point detection in a crowded RF space, Cisco 1000 series lightweight access points can be configured to operate in monitor mode, allowing monitoring without creating unnecessary interference.

Web User Interface and the CLI

This section describes the controller GUI and CLI.

Web User Interface

The Web User Interface is built into each Cisco Wireless LAN Controller. The Web User Interface allows up to five users to simultaneously browse into the built-in Cisco Wireless LAN Controller http or https (http + SSL) Web server, configure parameters, and monitor operational status for the Cisco Wireless LAN Controller and its associated Access Points.

**Note**

Cisco recommends that you enable the https: and disable the http: interfaces to ensure more robust security for your Cisco WLAN Solution.

Because the Web User Interface works with one Cisco Wireless LAN Controller at a time, the Web User Interface is especially useful when you wish to configure or monitor a single Cisco Wireless LAN Controller and its associated Cisco 1000 series lightweight access points.

Refer to the [“Using the Web-Browser Interface” section on page 2-2](#) for more information on the Web User Interface.

Command Line Interface

The Cisco Wireless LAN Solution command line interface (CLI) is built into each Cisco Wireless LAN Controller. The CLI allows operators to use a VT-100 emulator to locally or remotely configure, monitor and control individual Cisco Wireless LAN Controllers, and to access extensive debugging capabilities.

Because the CLI works with one Cisco Wireless LAN Controller at a time, the command line interface is especially useful when you wish to configure or monitor a single Cisco Wireless LAN Controller.

The Cisco Wireless LAN Controller and its associated Cisco 1000 series lightweight access points can be configured and monitored using the command line interface (CLI), which consists of a simple text-based, tree-structured interface that allows up to five users with Telnet-capable terminal emulators to simultaneously configure and monitor all aspects of the Cisco Wireless LAN Controller and associated Cisco 1000 series lightweight access points.

Refer to [“Using the CLI” section on page 2-5](#) and the *Cisco Wireless LAN Solution CLI Reference* for more information.