



# CHAPTER 1

## Overview

---

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

- [Cisco Unified Wireless Network 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 1-6](#)
- [Cisco Wireless LAN Controllers, page 1-7](#)
- [Controller Platforms, page 1-8](#)
- [Cisco UWN Solution Wired Connections, page 1-12](#)
- [Cisco UWN Solution WLANs, page 1-13](#)
- [Identity Networking, page 1-13](#)
- [File Transfers, page 1-14](#)
- [Power over Ethernet, page 1-14](#)
- [Startup Wizard, page 1-15](#)
- [Cisco Wireless LAN Controller Memory, page 1-16](#)
- [Cisco Wireless LAN Controller Failover Protection, page 1-16](#)
- [Network Connections to Cisco Wireless LAN Controllers, page 1-17](#)
- [Rogue Access Points, page 1-19](#)

# Cisco Unified Wireless Network Solution Overview

The Cisco Unified Wireless Network (Cisco UWN) Solution is designed to provide 802.11 wireless networking solutions for enterprises and service providers. The Cisco UWN 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 UWN 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 [Chapter 2](#).
- A full-featured command-line interface (CLI) can be used to configure and monitor individual Cisco Wireless LAN Controllers. See [Chapter 2](#).
- 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.



---

**Note** WCS software release 4.2 must be used with controllers running controller software release 4.2. Do not attempt to use older versions of WCS software with controllers running controller software release 4.2.

---

- An industry-standard SNMP V1, V2c, and V3 interface can be used with any SNMP-compliant third-party network management system.

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

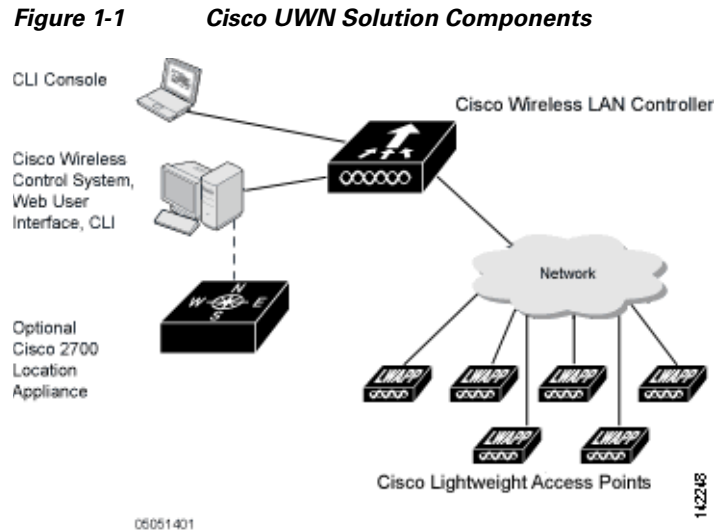
**Note**

---

Unless otherwise noted, all of the Cisco wireless LAN controllers are hereafter referred to as *controllers*, and all of the Cisco lightweight access points are hereafter referred to as *access points*.

---

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



## 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.



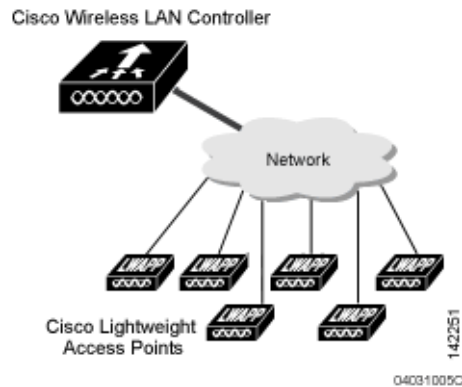
**Note**

---

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

---

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

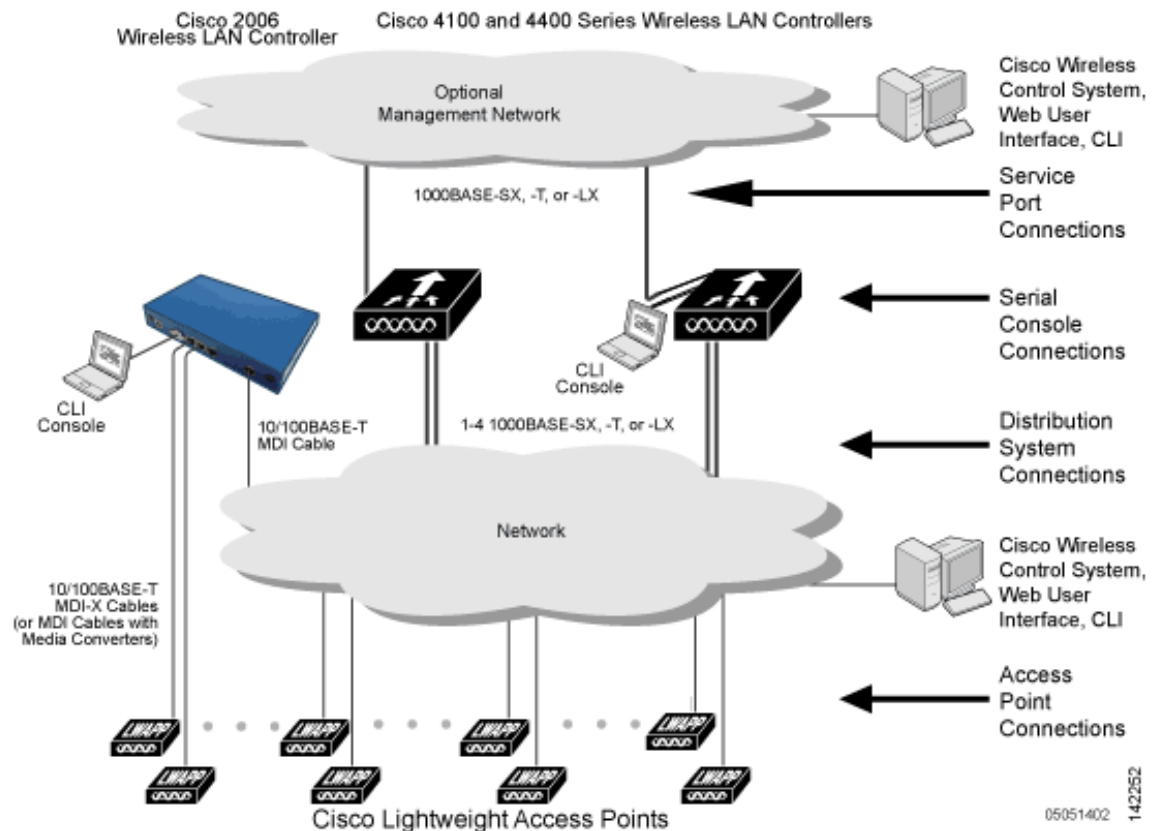
**Figure 1-2 Single-Controller Deployment**

## 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 1-16).

[Figure 1-3](#) 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 UWN Solution WLANs”](#) section on page 1-13.)

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.
- Optional MAC filtering.

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

- Passthrough VPNs
- 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. These signed certificates are used 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.

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. Another requirement is that the IP addresses of access points should be either statically assigned or dynamically assigned through an external DHCP server.

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 1-16.

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 1-16 for more information.

## 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](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](http://www.cisco.com/en/US/products/ps6386/products_installation_and_configuration_guides_list.html)

## Controller Platforms

Controllers are enterprise-class high-performance wireless switching platforms that support 802.11a/n and 802.11b/g/n protocols. They operate under control of the operating system, which includes the radio resource management (RRM), creating a Cisco UWN 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.

The following controllers are supported for use with software release 4.2:

- Cisco 2000 series controllers
- Cisco 2100 series controllers
- Cisco 4400 series controllers
- Catalyst 6500 Series Wireless Services Module (WiSM)
- Cisco 7600 Series Router Wireless Services Module (WiSM)
- Cisco 28/37/38xx Series Integrated Services Router with Controller Network Module
- Catalyst 3750G Integrated Wireless LAN Controller Switch

The first three controllers are stand-alone platforms. The remaining four controllers are integrated into Cisco switch and router products.

## Cisco 2000 and 2100 Series Controllers

The Cisco 2000 and 2100 Series Wireless LAN Controllers work in conjunction with Cisco lightweight access points and the Cisco Wireless Control System (WCS) to provide system-wide wireless LAN functions. Each 2000 and 2100 series controller controls up to six lightweight access points for multi-controller architectures typical of enterprise branch deployments. It may also be used for single controller deployments for small and medium-sized environments.

**Caution**

Do not connect a power-over-Ethernet (PoE) cable to the controller's console port. Doing so may damage the controller.

**Note**

Wait at least 20 seconds before reconnecting an access point to the controller. Otherwise, the controller may fail to detect the device.

## Features Not Supported

These hardware features are not supported on 2000 and 2100 series controllers:

- Power over Ethernet (PoE) [2000 series controllers only]

**Note**

Ports 7 and 8 on 2100 series controllers are PoE ports.

- Service port (separate out-of-band management 10/100-Mbps Ethernet interface)

These software features are not supported on 2000 and 2100 series controllers:

- VPN termination (such as IPSec and L2TP)
- Termination of guest controller tunnels (origination of guest controller tunnels is supported)
- External web authentication web server list
- Layer 2 LWAPP
- Spanning tree
- Port mirroring
- Cranite
- Fortress
- AppleTalk
- QoS per-user bandwidth contracts
- IPv6 pass-through
- Link aggregation (LAG)

## Cisco 4400 Series Controllers

The Cisco 4400 Series Wireless LAN Controller is available in two models: 4402 and 4404. The 4402 supports up to 50 lightweight access points while the 4404 supports up to 100, making it ideal for large-sized enterprises and large-density applications.

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

## Catalyst 6500 Series Wireless Services Module

The Catalyst 6500 Series Wireless Services Module (WiSM) is an integrated Catalyst 6500 switch and two Cisco 4404 controllers that supports up to 300 lightweight access points. The switch has eight internal Gigabit Ethernet ports that connect the switch and the controller. The switch and the internal controller run separate software versions, which must be upgraded separately.

**Note**

The Catalyst 6500 Series Switch chassis can support up to six Cisco WiSMs without any other service module installed. If one or more service modules are installed, the chassis can support up to a maximum of four service modules (WiSMs included).

**Note**

The Cisco WiSM controllers do not support port mirroring.

Refer to the following documents for additional information:

- *Catalyst 6500 Series Switch Installation Guide*
- *Catalyst 6500 Series Switch Wireless Services Module Installation and Configuration Note*
- *Release Notes for Catalyst 6500 Series Switch Wireless LAN Services Module*
- *Configuring a Cisco Wireless Services Module and Wireless Control System*
- *Catalyst 6500 Series Switch and Cisco 7600 Series Router Wireless Services Module Installation and Verification Note*

You can find these documents at these URLs:

[http://www.cisco.com/en/US/products/hw/switches/ps708/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html)

<http://www.cisco.com/en/US/docs/wireless/technology/wism/technical/reference/appnote.html>

[http://www.cisco.com/en/US/docs/wireless/technology/wism/installation/note/78\\_17121.html](http://www.cisco.com/en/US/docs/wireless/technology/wism/installation/note/78_17121.html)

## Cisco 7600 Series Router Wireless Services Module

The Cisco 7600 Series Router Wireless Services Module (WiSM) is an integrated Cisco 7600 router and two Cisco 4404 controllers that supports up to 300 lightweight access points. The router has eight internal Gigabit Ethernet ports that connect the router and the controller. The router and the internal controller run separate software versions, which must be upgraded separately.

**Note**

The WiSM is supported on Cisco 7600 series routers running only Cisco IOS Release 12.2(18)SXF5 or later.

**Note**

The Cisco 7600 series router chassis can support up to six Cisco WiSMs without any other service module installed. If one or more service modules are installed, the chassis can support up to four service modules (WiSMs included).

**Note**

The Cisco WiSM controllers do not support port mirroring.

Refer to the following documents for additional information:

- *Cisco 7600 Series Router Installation Guide*
- *Cisco 7600 Series Router Software Configuration Guide*
- *Cisco 7600 Series Router Command Reference*
- *Configuring a Cisco Wireless Services Module and Wireless Control System*
- *Catalyst 6500 Series Switch and Cisco 7600 Series Router Wireless Services Module Installation and Verification Note*

You can find these documents at these URLs:

[http://www.cisco.com/en/US/products/hw/routers/ps368/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/hw/routers/ps368/tsd_products_support_series_home.html)

<http://www.cisco.com/en/US/docs/wireless/technology/wism/technical/reference/appnote.html>

[http://www.cisco.com/en/US/docs/wireless/technology/wism/installation/note/78\\_17121.html](http://www.cisco.com/en/US/docs/wireless/technology/wism/installation/note/78_17121.html)

## Cisco 28/37/38xx Series Integrated Services Router

The Cisco 28/37/38xx Series Integrated Services Router is an integrated 28/37/38xx router and Cisco controller network module that supports up to 6, 8, or 12 lightweight access points, depending on the version of the network module. The versions that support 8 and 12 access points feature a high-speed processor and more on-board memory. An internal Fast Ethernet port (on the 6-access point version) or an internal Gigabit Ethernet port (on the 8- and 12-access point versions) connects the router and the integrated controller. The router and the internal controller run separate software versions, which must be upgraded separately. Refer to the following documents for additional information:

- *Cisco Wireless LAN Controller Network Module Feature Guide*
- *Cisco 28/37/38xx Series Hardware Installation Guide*

You can find these documents at this URL:

<http://www.cisco.com/en/US/products/hw/wireless/index.html>

**Note**

The controller network module does not support port mirroring.

**Note**

The Cisco 2801 Integrated Services Router does not support the controller network module.

## Catalyst 3750G Integrated Wireless LAN Controller Switch

The Catalyst 3750G Integrated Wireless LAN Controller Switch is an integrated Catalyst 3750 switch and Cisco 4400 series controller that supports up to 25 or 50 lightweight access points. The switch has two internal Gigabit Ethernet ports that connect the switch and the controller. The switch and the internal controller run separate software versions, which must be upgraded separately. Refer to the following documents for additional information:

- *Catalyst 3750G Integrated Wireless LAN Controller Switch Getting Started Guide*
- *Catalyst 3750 Switch Hardware Installation Guide*
- *Release Notes for the Catalyst 3750 Integrated Wireless LAN Controller Switch, Cisco IOS Release 12.2(25)FZ*

You can find these documents at this URL:

[http://www.cisco.com/en/US/products/hw/switches/ps5023/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/hw/switches/ps5023/tsd_products_support_series_home.html)

## Cisco UWN Solution Wired Connections

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

- The 2000 series controller connects to the network using from one to four 10/100BASE-T Ethernet cables.
- The 2100 series controller connects to the network using from one to six 10/100BASE-T Ethernet cables.
- The 4402 controller connects to the network using one or two fiber-optic Gigabit Ethernet cables, and the 4404 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 in the Wireless Services Module (WiSM), installed in a Cisco Catalyst 6500 Series Switch or a Cisco 7600 Series Router, connect to the network through ports on the switch or router.
- The Wireless LAN Controller Network Module, installed in a Cisco Integrated Services Router, connects to the network through the ports on the router.
- The controller in the Catalyst 3750G Integrated Wireless LAN Controller Switch connects to the network through the ports on the switch.
- Cisco 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 UWN Solution WLANs

The Cisco UWN Solution can control up to 16 WLANs for lightweight access points. Each WLAN has a separate WLAN ID (1 through 16), a separate WLAN SSID (WLAN 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 WLAN.

The lightweight access points broadcast all active Cisco UWN Solution WLAN SSIDs and enforce the policies defined for each WLAN.

**Note**

Cisco recommends that you assign one set of VLANs for WLANs 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 the Cisco UWN Solution, the operator can manage the system across the enabled WLAN using CLI and Telnet, http/https, and SNMP.

To configure WLANs, refer to [Chapter 6](#).

## Identity Networking

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 controllers 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 UWN 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, access control list (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 controller; if there are no AAA Overrides available for a given MAC Address, the operating system uses the MAC Filtering parameters already in the 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 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 only moves clients from the default Cisco UWN Solution WLAN VLAN to a different VLAN when configured for MAC filtering, 802.1X, and/or WPA Layer 2 authentication. To configure WLANs, refer to [Chapter 6](#).

## 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, 2100, and 4400 series controllers and 1000, 1130, 1200, and 1500 series lightweight access points.

## File Transfers

The Cisco UWN Solution operator can upload and download operating system code, configuration, and certificate files to and from controller using the GUI, CLI commands, or Cisco WCS.

- To use CLI commands, refer to the “[Transferring Files to and from a Controller](#)” section on [page 8-8](#).
- 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](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.

## Startup Wizard

When a 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 controller has a System Name, up to 32 characters.
- Adds an Administrative username and password, each up to 24 characters.
- Ensures that the controller can communicate with the GUI, CLI, or Cisco WCS (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 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 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 1-6](#).
- 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 or disables the 802.11a/n and 802.11b/g/n 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 controller contains two kinds of memory: volatile RAM, which holds the current, active controller configuration, and NVRAM (non-volatile RAM), which holds the reboot configuration. When you are configuring the operating system in controller, you are modifying volatile RAM; you must save the configuration from the volatile RAM to the NVRAM to ensure that the 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 controller has a defined number of communication ports for 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 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 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 lightweight access point has no primary, secondary, and tertiary controllers assigned and there is no master controller active, it attempts to associate with the least-loaded 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.

## Network Connections to Cisco Wireless LAN Controllers

Regardless of operating mode, all 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 and 2100 Series Wireless LAN Controllers, page 1-17](#)
- [Cisco 4400 Series Wireless LAN Controllers, page 1-18](#)



**Note**

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

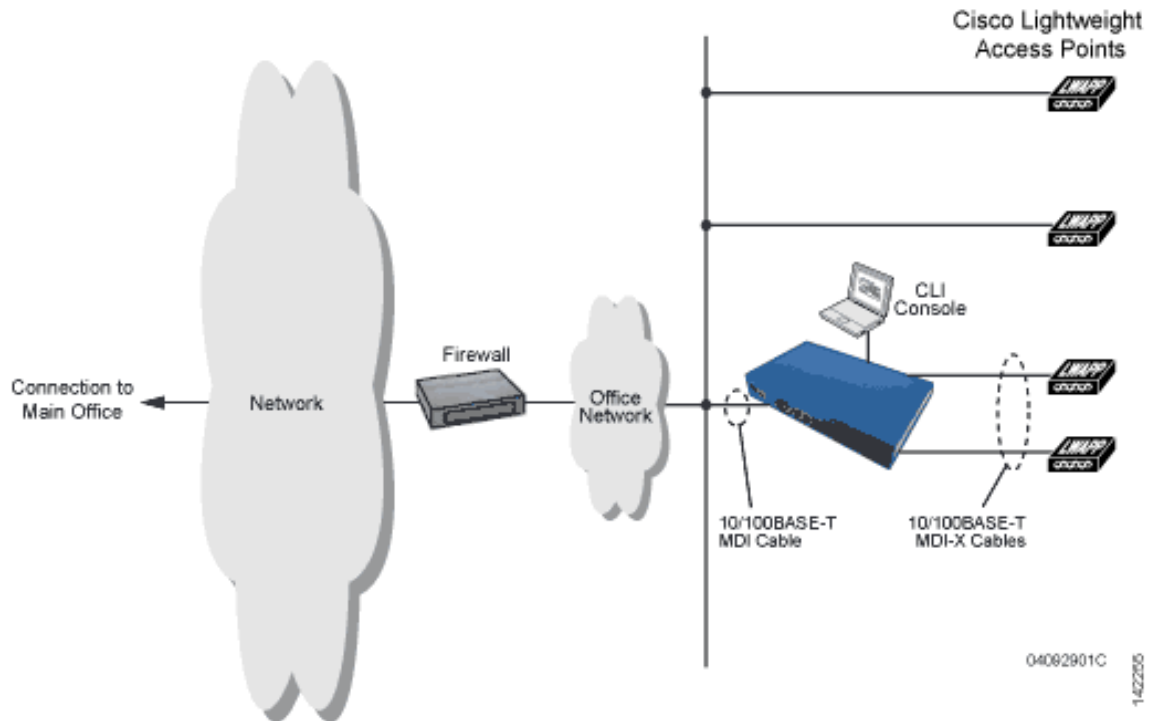
### Cisco 2000 and 2100 Series Wireless LAN Controllers

Cisco 2000 and 2100 series controllers can communicate with the network through any one of their physical data ports, as the logical management interface can be assigned to one of the ports. The physical port descriptions follow:

- Up to four 10/100BASE-T cables can plug into the four back-panel data ports on the 2000 series controller chassis.
- Up to six 10/100BASE-T cables can plug into the six back-panel data ports on the 2100 series controller chassis. The 2100 series also has two PoE ports (ports 7 and 8).

[Figure 1-4](#) shows connections to the 2000 and 2100 series controllers.

**Figure 1-4** Physical Network Connections to the 2000 and 2100 Series Controller



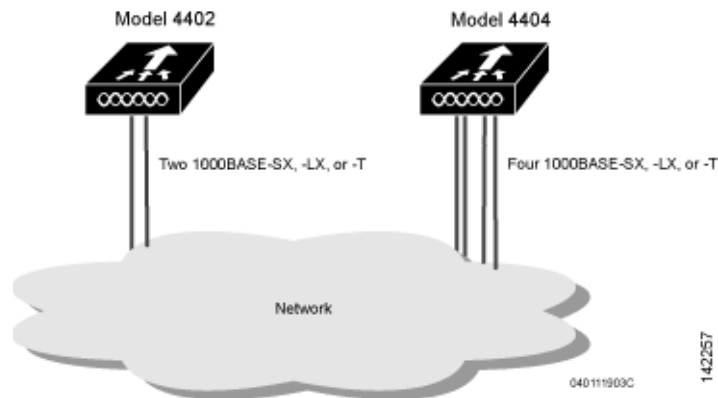
## Cisco 4400 Series Wireless LAN Controllers

Cisco 4400 series 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 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 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 1-5 shows connections to the 4400 series controller.

**Figure 1-5 Physical Network Connections to 4402 and 4404 Series Controllers**



## 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 chasers 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 UWN 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 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 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 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 controller, and sniffs all ARP packets. If it finds a match between an ARP request and a MAC address it receives from the controller, it generates a rogue access point alert to the controller.

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