Overview

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

- Introduction, page 1
- Operating System Software, page 3
- Operating System Security, page 4
- Layer 2 and Layer 3 Operation, page 4
- Cisco Wireless Controllers, page 5
- Cisco Wireless Solution WLANs, page 6
- File Transfers, page 6
- Power over Ethernet, page 6
- Cisco Wireless Controller Memory, page 7
- Cisco Wireless Controller Failover Protection, page 7

Introduction

Cisco Wireless is designed to provide 802.11 wireless networking solutions for enterprises and service providers. Cisco Wireless 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.

Cisco Wireless solution consists of Cisco wireless controllers (Cisco WLCs) 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 WLCs can be used to configure and monitor individual Cisco WLCs.
- A full-featured command-line interface (CLI) can be used to configure and monitor individual Cisco WLCs.
The Cisco Prime Infrastructure, which you use to configure and monitor one or more Cisco WLCs and associated access points. The Prime Infrastructure has tools to facilitate large-system monitoring and control. For more information about Cisco Prime Infrastructure, see http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/tsd-products-support-series-home.html.

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

The Cisco Wireless 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 WLCs, and the optional Cisco Prime Infrastructure to provide wireless services to enterprises and service providers.


**Single-Controller Deployments**

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

- Autodetecting and autoconfiguring lightweight access points as they are added to the network.
- Full control of lightweight access points.
- Lightweight access points connect to controllers through the network. The network equipment may or may not provide Power over Ethernet (PoE) to the access points.

Some controllers use redundant Gigabit Ethernet connections to bypass single network failures.

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

This figure shows a typical single-controller deployment.

*Figure 1: 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 occurs 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.

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 2: Typical Multiple-Controller Deployment*

Operating System Software

The operating system software controls controllers and 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.

The 802.11 Static WEP weaknesses can be overcome using the following robust industry-standard security solutions:

- 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) and message integrity code checksum dynamic keys
  - WEP keys, with or without a preshared key passphrase
- RSN with or without a preshared key
- Optional MAC filtering

The WEP problem can be further solved using the following industry-standard Layer 3 security solutions:

- Passthrough VPNs
- Local and RADIUS MAC address filtering
- Local and RADIUS user/password authentication
- Manual and automated disabling to block access to network services. In manual disabling, you block access using client MAC addresses. In automated disabling, which is always active, the operating system software automatically blocks access to network services for a user-defined period of time when a client fails to authenticate for a fixed number of consecutive attempts. This feature 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.

Layer 2 and Layer 3 Operation

Lightweight Access Point Protocol (LWAPP) communications between the controller and lightweight access points can be conducted at Layer 2 or Layer 3. Control and Provisioning of Wireless Access Points protocol (CAPWAP) communications between the controller and lightweight access points are conducted at Layer 3. Layer 2 mode does not support CAPWAP.

Note

The IPv4 network layer protocol is supported for transport through a CAPWAP or LWAPP controller system. IPv6 (for clients only) and AppleTalk are also supported but only on Cisco 5500 Series Controllers and the Cisco WiSM2. 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 3 LWAPP communications is that the controller and 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.

The requirement for Layer 3 CAPWAP communications is that the controller and lightweight access points can be connected through Layer 2 devices on the same subnet or connected through Layer 3 devices across subnets.

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 lightweight access points and a management interface as configured for Layer 2 mode.

Cisco Wireless Controllers

When you are adding lightweight access points to a multiple-Cisco WLC deployment network, it is convenient to have all lightweight access points associate with one master Cisco WLC on the same subnet. That way, the you do not have to log into multiple Cisco WLCs to find out which controller newly-added lightweight access points associated with.

One Cisco WLC in each subnet can be assigned as the master Cisco WLC while adding lightweight access points. As long as a master Cisco WLC 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 WLC.

You can monitor the master Cisco WLC using the Cisco Prime Infrastructure Web User Interface and watch as access points associate with the master Cisco WLC. You can then verify the access point configuration and assign a primary, secondary, and tertiary Cisco WLC to the access point, and reboot the access point so it reassociates with its primary, secondary, or tertiary Cisco WLC.

Note

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

Client Location

When you use Cisco Prime Infrastructure in your Cisco wireless LAN solution, controllers periodically determine the client, rogue access point, rogue access point client, radio frequency ID (RFID) tag location and store the locations in the Cisco Prime Infrastructure database.
Cisco WLC Platforms

Cisco WLCs 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 Wireless solution that can automatically adjust to real-time changes in the 802.11 RF environment. Cisco WLCs are built around high-performance network and security hardware, resulting in highly reliable 802.11 enterprise networks with unparalleled security.

The following Cisco WLCs are supported:

- Cisco 2504 Wireless Controller
- Cisco 5508 Wireless Controller
- Cisco Flex 7510 Wireless Controller
- Cisco 8510 Wireless Controller
- Cisco Virtual Wireless Controller
- Catalyst Wireless Services Module (WiSM2)

Cisco Wireless Solution WLANs

The Cisco Wireless solution can control up to 512 WLANs for lightweight access points. Each WLAN has a separate WLAN ID (1 through 512), a separate profile name, and a WLAN SSID and can be assigned with unique security policies. The lightweight access points broadcast all active Cisco Wireless solution WLAN SSIDs and enforce the policies defined for each WLAN.

Note

We recommend 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 Wireless solution, you can manage the system across the enabled WLAN using CLI and Telnet, HTTP/HTTPS, and SNMP.

File Transfers

You can upload and download operating system code, configuration, and certificate files to and from the controller using the GUI, CLI, or Cisco Prime Infrastructure.

Power over Ethernet

Lightweight access points can receive power through 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 installation time. PoE frees you from having to mount lightweight access points or other powered equipment near AC outlets, which provides greater flexibility in positioning the access points for maximum coverage.
When you are using PoE, you run 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 access point.

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

Cisco Wireless Controller Memory

The controller contains two kinds of memory: volatile RAM, which holds the current, active controller configuration, and NVRAM (nonvolatile RAM), which holds the reboot configuration. When you are configuring the operating system in the 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 doing the following tasks:

- Using the configuration wizard
- Clearing the controller configuration
- Saving configurations
- Resetting the controller
- Logging out of the CLI

Cisco Wireless Controller Failover Protection

During installation, we recommend 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 the failover recovery, the following tasks are performed:

- The configured access point attempts to contact the primary, secondary, and tertiary controllers, and then attempts to contact the IP addresses of the other controllers in the mobility group.
- DNS is resolved with the controller IP address.
- DHCP servers get the controller IP addresses (vendor-specific option 43 in DHCP offer).

In multiple-controller deployments, if one controller fails, the access points perform the following tasks:

- 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.
- If the access point finds no master controller, it attempts to contact stored mobility group members by the IP address.
• If the mobility group members are 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 to respond to its discovery messages.

When controllers are deployed, if one controller fails, active access point client sessions are momentarily dropped while the dropped access point associates with another controller, allowing the client device to immediately reassociate and reauthenticate.