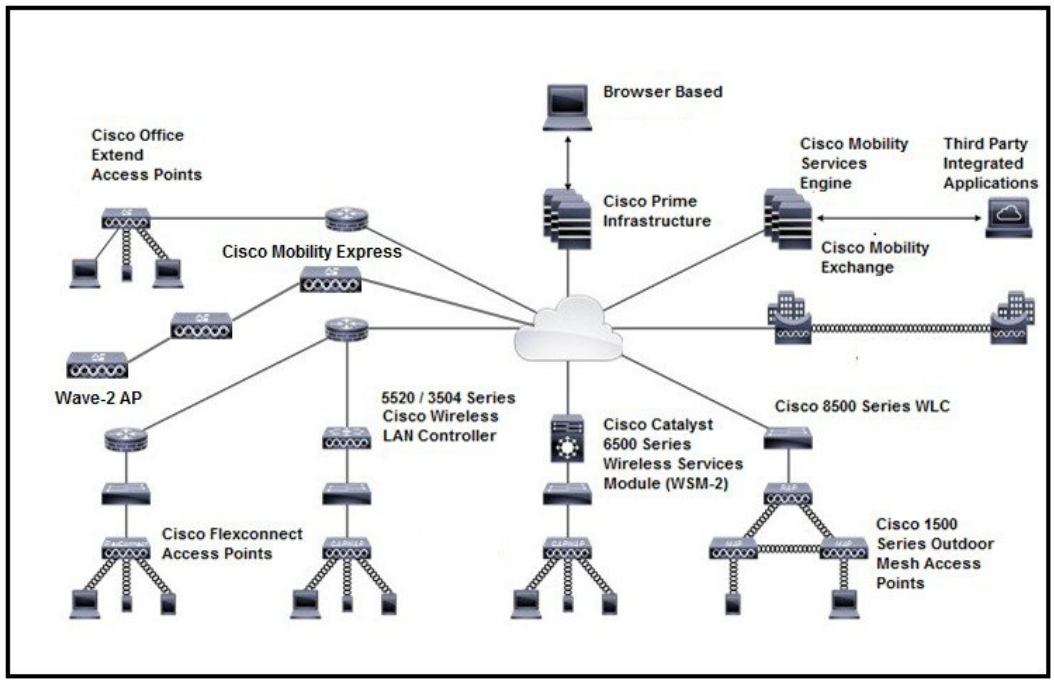
Cisco Wireless Solution Overview

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

This figure shows a sample architecture of a Cisco Wireless Enterprise Network:

Figure 1: Sample Cisco Wireless Enterprise Network Architecture



The interconnected elements that work together to deliver a unified enterprise-class wireless solution include the following:

- Client devices
- Access points (APs)

- Network unification through Cisco Wireless Controllers (controllers)
- Network management
- Mobility services

Beginning with a base of client devices, each element adds capabilities as the network needs to evolve and grow, interconnecting with the elements above and below it to create a comprehensive, secure wireless LAN (WLAN) solution.

Core Components

A Cisco Wireless network consists of the following core components:

- Cisco Wireless Controllers: Cisco Wireless Controllers (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 AireOS 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 radio frequency (802.11 RF) environment. 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:

  - 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 2 (WiSM2)

- Cisco Access Points: Cisco access points (APs) can be deployed in a distributed or centralized network for a branch office, campus, or large enterprise. For more information about APs, see https://www.cisco.com/c/en/us/products/wireless/access-points/index.html
- Cisco Prime Infrastructure (PI): Cisco Prime Infrastructure can be used to configure and monitor one or more controllers and associated APs. Cisco PI has tools to facilitate large-system monitoring and control. When you use Cisco PI in your Cisco wireless 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 PI database. For more information about Cisco PI, see https://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/series.html.

- Cisco Connected Mobile Experiences (CMX): Cisco Connected Mobile Experiences (CMX) acts as a platform to deploy and run Cisco Connected Mobile Experiences (Cisco CMX). Cisco Connected Mobile Experiences (CMX) is delivered in two modes—the physical appliance (box) and the virtual appliance (deployed using VMware vSphere Client) . Using your Cisco wireless network and location intelligence from Cisco MSE, Cisco CMX helps you create personalized mobile experiences for end users and gain operational efficiency with location-based services. For more information about Cisco CMX, see https://www.cisco.com/c/en/us/support/wireless/connected-mobile-experiences/series.html.
- Cisco DNA Spaces: Cisco DNA Spaces is a multichannel engagement platform that enables you to connect, know, and engage with visitors at their physical business locations. It covers various verticals of business such as retail, manufacturing, hospitality, healthcare, education, financial services, enterprise work spaces, and so on. Cisco DNA Spaces also provides solutions for monitoring and managing the assets in your premises.

  The Cisco DNA Spaces: Connector enables Cisco DNA Spaces to communicate with multiple Cisco Wireless Controller (controller) efficiently by allowing each controller to transmit high intensity client data without missing any client information.

  For information about how to configure Cisco DNA Spaces and the Connector, see https://www.cisco.com/c/en/us/support/wireless/dna-spaces/products-installation-and-configuration-guides-list.html.

For more information about design considerations for enterprise mobility, see the *Enterprise Mobility Design Guide* at:

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/Enterprise-Mobility-8-5-Design-Guide/Enterprise_Mobility_8-5_Deployment_Guide.html

Overview of Cisco Mobility Express

The Cisco Mobility Express wireless network solution comprises of at least one Cisco Wave 2 AP with an in-built software-based wireless controller managing other Cisco APs in the network.

The AP acting as the controller is referred to as the primary AP while the other APs in the Cisco Mobility Express network, which are managed by this primary AP, are referred to as subordinate APs.

In addition to acting as a controller, the primary AP also operates as an AP to serve clients along with the subordinate APs.

Cisco Mobility Express provides most features of a controller and can interface with the following:

- Cisco Prime Infrastructure: For simplified network management, including managing AP groups
- Cisco Identity Services Engine: For advanced policy enforcement
- Connected Mobile Experiences (CMX): For providing presence analytics and guest access using Connect & Engage

For more information about using Cisco Mobility Express, see the user guide for relevant releases at: https://www.cisco.com/c/en/us/support/wireless/mobility-express/products-installation-and-configuration-guides-list.html

Single-Controller Deployments

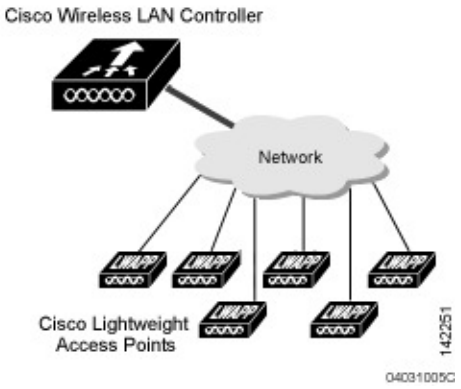
A standalone controller can support lightweight access points across multiple floors and buildings simultaneously and support the following features:

- 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.

Note 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.

Figure 2: Single-Controller Deployment



This figure shows a typical single-controller deployment.

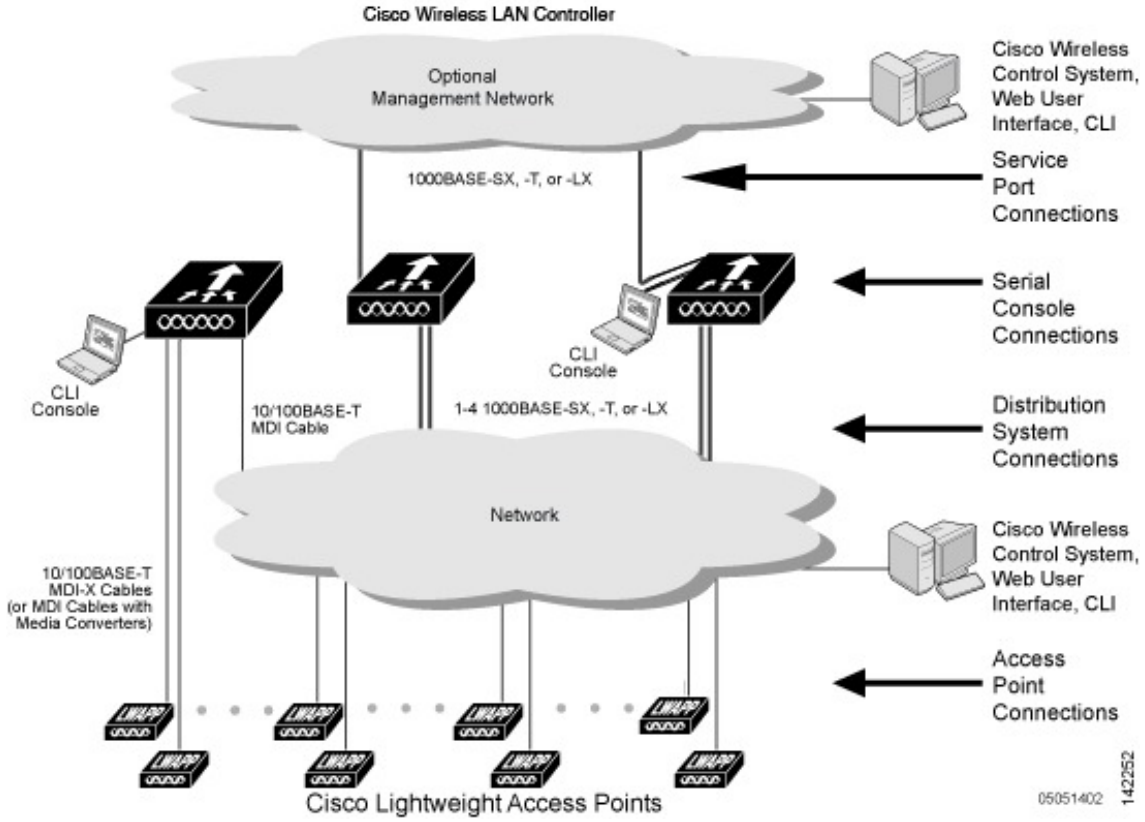
Multiple-Controller Deployments

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.

Figure 3: Typical Multiple-Controller Deployment

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.



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 p assphrase
- 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 across subnets is that the controller and lightweight access points are connected through Layer 3 devices. Another requirement is that the IP addresses of access points should be either statically assigned or dynamically assigned through an external DHCP server.

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 primary Cisco WLC on the same subnet. That way, you do not have to log into multiple Cisco WLCs to find out which controller the newly-added lightweight access points associated with.

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

You can monitor the primary Cisco WLC using the Cisco Prime Infrastructure and watch as access points associate with the primary 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 primary Cisco WLC first upon reboot. After adding lightweight access points through the primary Cisco WLC, you should assign primary, secondary, and tertiary Cisco WLCs to each access point. We recommend that you disable the primary setting on all Cisco WLCs after initial configuration.

Client Location

When you use Cisco Prime Infrastructure in your Cisco wireless LAN solution, Cisco WLCs 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 Mobility Services Engine (Cisco MSE) acts as a platform to deploy and run Cisco Connected Mobile Experiences (Cisco CMX). Cisco MSE is delivered in two modes—the physical appliance (box) and the virtual appliance (deployed using VMware vSphere Client) . Using your Cisco wireless network and location intelligence from Cisco MSE, Cisco CMX helps you create personalized mobile experiences for end users and gain operational efficiency with location-based services. For more information about Cisco CMX, see

https://www.cisco.com/c/en/us/support/wireless/connected-mobile-experiences/tsd-products-support-series-home.html.

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 2 (WiSM2)

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 2 (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 .

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 primary controller.
- If the access point finds no primary 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 primary 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.

To know more about high availability, see http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/107250-ha-wlc.html.