CHAPTER 1

Overview

This chapter describes the Cisco Unified Wireless Network Solution and the Cisco Wireless Control System (WCS). It contains these sections:

Overview of the Cisco Unified Wireless Network Solution

The Cisco Unified Wireless Network solution is designed to provide 802.11 wireless networking solutions for enterprises and service providers. It simplifies the deployment and management of 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 Unified Wireless Network Solution consists of Cisco Unified Wireless Network Controllers (hereafter called *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:

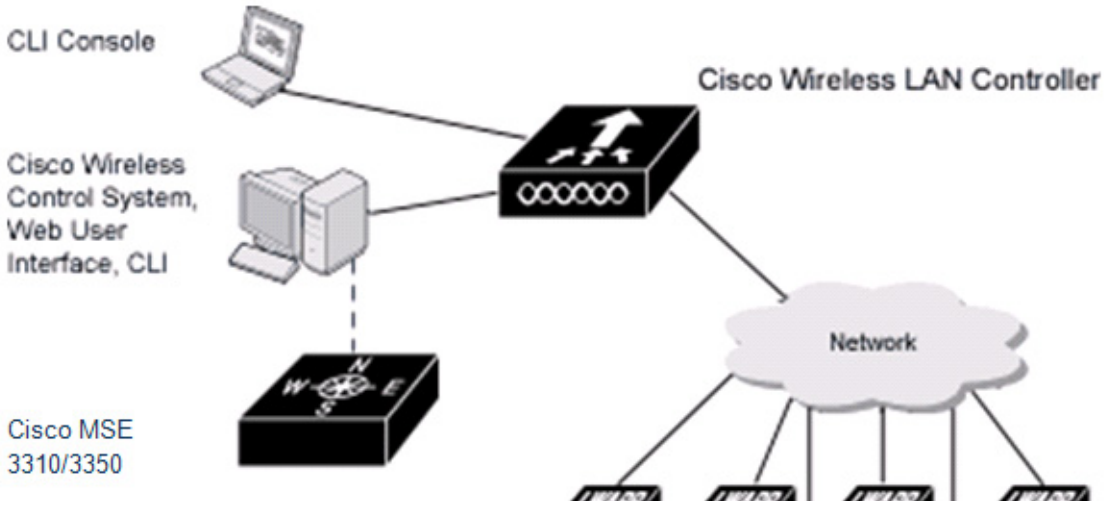
- An HTTPS full-featured web user interface hosted by Cisco controllers can be used to configure and monitor individual controllers.
- A full-featured command line interface (CLI) can be used to configure and monitor individual controllers.
- The Cisco Wireless Control System (WCS) can be used to configure and monitor one or more controllers and associated access points. WCS has tools to facilitate large-system monitoring and control. It runs on Windows 2003 and Red Hat Enterprise Linux ES/AS 4 servers.
- An industry-standard SNMP V1, V2c, and V3 interface can be used with any SNMP-compliant third-party network management system.

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

Note This document refers to controllers throughout. Unless specified otherwise, the descriptions herein apply to all Cisco Unified Wireless Network Controllers, including but not limited to Cisco 2000 and 2100 Series Unified Wireless Network Controllers, Cisco 4100 Series Unified Wireless Network Controllers, Cisco 4400 Series Unified Wireless Network Controllers, and controllers within the Cisco Wireless Services Module (WiSM) and Cisco 26/28/37/38*xx* Series Integrated Services Routers.

Figure 1-1 shows the Cisco Unified Wireless Network Solution components, which can be simultaneously deployed across multiple floors and buildings.

Figure 1-1 Cisco Unified Wireless Network Solution



Overview of WCS

The Cisco Wireless Control System (WCS) is a Cisco Unified Wireless Network Solution management tool that adds to the capabilities of the web user interface and command line interface (CLI), moving from individual controllers to a network of controllers. WCS includes the same configuration, performance monitoring, security, fault management, and accounting options used at the controller level and adds a graphical view of multiple controllers and managed access points.

WCS runs on Windows 2003 and Red Hat Enterprise Linux ES 5.1. On both Windows and Linux, WCS can run as a normal application or as a service, which runs continuously and resumes running after a reboot.

The WCS user interface enables operators to control all permitted Cisco Unified Wireless Network Solution configuration, monitoring, and control functions through Internet Explorer 6.0 or later. Operator permissions are defined by the administrator using the WCS user interface Administration menu, which enables the administrator to manage user accounts and schedule periodic maintenance tasks.

WCS simplifies controller configuration and monitoring while reducing data entry errors. WCS uses the industry-standard SNMP protocol to communicate with the controllers.

WCS Versions

You can install WCS with one of two capabilities: WCS Base or WCS Location. Regardless of whether you choose WCS Base or WCS Location, a license is required.

WCS Base

The WCS Base supports wireless client data access, rogue access point, and rogue ad hoc detection and containment functions (such as on-demand location of rogue access points that are mapped next to the detecting access point), and Cisco UWN Solution monitoring and control.

It also includes graphical views of the following:

- Autodiscovery of access points as they associate with controllers
- Autodiscovery and containment or notification of rogue access points
- Map-based organization of access point coverage areas, which is helpful when the enterprise spans more than one geographical area
- Adhoc rogue
- User-supplied campus, building, and floor plan graphics, which show the following:
  - Locations and status of managed access points
  - Locations of rogue access points based on the signal strength received by the nearest managed Cisco access points
  - Coverage hole alarm information for access points based on the received signal strength from clients. This information appears in a tabular rather than map format.
  - RF coverage maps

The WCS Base also provides system-wide control of the following:

  - Streamlined network, controller, and managed access point configuration using customer-defined templates
  - Network, controller, and managed access point status and alarm monitoring
  - Automated and manual data client monitoring and control functions
  - Automated monitoring of rogue access points, rogue ad hocs, coverage holes, security violations, controllers, and access points
  - Full event logs for data clients, rogue access points, coverage holes, security violations, controllers, and access points
  - Automatic channel and power level assignment by radio resource management (RRM)
  - User-defined automatic controller status audits, missed trap polling, configuration backups, and policy cleanups
  - Real-time location of rogue access points and rogue ad hocs to the nearest Cisco access point
  - Real-time and historical location of clients to the nearest Cisco access point

WCS Base + Location

The WCS Location includes all the features of the WCS Base as well as these enhancements:

- On-demand location of rogue access points and rogue ad hocs to within 33 feet (10 meters)
- On-demand location of clients to within 33 feet (10 meters)
- Ability to use location appliances to collect and return historical location data viewable in the WCS Location user interface

Mobility Services Enablement and HA

A Cisco WCS PLUS license is available that supports Cisco WCS base license features and the following capabilities:

- Location services
- High availability

A Cisco WCS PLUS license is backward compatible to existing Cisco WCS location and enterprise licenses. The process to provision a Cisco WCS PLUS license is the same as provisioning a current Cisco WCS license. A PLUS license is required in order to enable mobility services engines which are launched with the Motion campaign.

Relationship with Cisco Location Appliances

When WCS Location is used, end users can also deploy Cisco 2700 Series Location Appliances. The location appliance enhances the high-accuracy built-in WCS Location capabilities by computing, collecting, and storing historical location data, which can be displayed in WCS. In this role, the location appliance acts as a server to a WCS server by collecting, storing, and passing on data from its associated controllers.

After a quick command line interface (CLI) configuration, the remaining location appliance configuration can be completed using the WCS user interface. After each location appliance is configured, it communicates directly with its associated controllers to collect operator-defined location data. The associated WCS server operators can then communicate with each location appliance to transfer and display selected data.

The location appliance can be backed up to any WCS server into an operator-defined FTP folder, and the location appliance can be restored from that server at any time and at defined intervals. Also, the location appliance database can be synchronized with the WCS server database at any time. Operators can use the location appliance features and download new application code to all associated appliances from any WCS server.

When WCS is enhanced with a location appliance, it can display historical location data for up to 2,500 laptop clients, palmtop clients, VoIP telephone clients, radio frequency identifier (Wi-Fi tags) asset tags, rogue access points, rogue ad hocs, and rogue clients for each location appliance in the Cisco Unified Wireless Network Solution. Operators can configure location appliances to collect this data and statistics at defined intervals.

You can also use WCS to configure location appliance event notification parameters. *Event notification* is a feature that enables you to define conditions that cause the location appliance to send notifications to the listeners whom you have specified in WCS.

In this way, WCS acts as a notification listener. It receives notifications from the location appliance in the form of the locationNotifyTrap trap as part of the bsnwras.my MIB file. WCS translates the traps into user interface alerts and displays the alerts in the following format:

```
Absence:
- Absence of Tag with MAC 00:0c:cc:5b:e4:1b, last seen at 16:19:45 13 Oct 2005.

Containment:
- Tag with MAC 00:0c:cc:5b:fa:44 is In the Area 'WNBU > WNBU > 4th Floor > wcsDevArea'

Distance:
- Tag with MAC 00:0c:cc:5b:fa:47 has moved beyond the distance configured for the marker
'marker2'.
- Tag with MAC 00:0c:cc:5b:f9:b9 has moved beyond 46.0 ft. of marker 'marker2', located at
a range of 136.74526528595058 ft.
```

Note Refer to the *Cisco Location Application Configuration Guide* for more detailed information about the location appliance and its use with WCS.

Comparison of WCS Base and WCS Location

Table 1-1 compares the WCS Base and WCS Location features.

Table 1-1 WCS Base and WCS Location Features

Features	WCS Base	WCS Location
Location and tracking		
Low-resolution client location	Yes	—
High-resolution client location	—	Yes
Integration with location appliance	—	Yes
Low-resolution rogue access point location	Yes	—
High-resolution rogue access point location	—	Yes
Client data services, security, and monitoring		
Client access via access points	Yes	Yes
Multiple wireless LANs (individual SSIDs and policies)	Yes	Yes
Rogue access point detection and containment using access points	Yes	Yes
802.11a/b/g/n bands	Yes	Yes
Radio resource management		
Real-time channel assignment and rogue access point detection and containment	Yes	Yes
Real-time interference detection and avoidance, transmit power control, channel assignment, client mobility management, client load distribution, and coverage hole detection	Yes	Yes
Automated software and configuration updates	Yes	Yes
Wireless intrusion protection	Yes	Yes

Table 1-1 WCS Base and WCS Location Features (continued)

Features	WCS Base	WCS Location
Global and individual AP security policies	Yes	Yes
Controls Cisco Unified Wireless Network Controllers	Yes	Yes
Supported workstations		
Windows 2003	Yes	Yes
Red Hat Enterprise Linux ES 5.1	Yes	Yes
Mozilla Firefox 2.0.0.11 or later	Yes	Yes

Embedded Access Points

WCS software release 5.2 or later supports the AP801, which is the integrated access point on the Cisco 800 Series Integrated Services Routers (ISRs). This access point uses a Cisco IOS software image that is separate from the router Cisco IOS software image. It can operate as an autonomous access point that is configured and managed locally, or it can operate as a centrally managed access point using CAPWAP or LWAPP protocol. The AP801 is preloaded with both an autonomous Cisco IOS release and a recovery image for the unified mode.

When you want to use the AP801 with a controller, you must enable the recovery image for the unified mode on the access point by entering this CLI command on the router in privileged EXEC mode: **service-module wlan-ap 0 bootimage unified**.

Note If the **service-module wlan-ap 0 bootimage unified** command does not work, make sure that the software license is still current.

After enabling the recovery image, enter this CLI command on the router to shut down and reboot the access point: **service-module wlan-ap 0 reload**. After the access point reboots, it discovers the controller, downloads the full CAPWAP or LWAPP software release from the controller, and acts as a lightweight access point.

Note To use the CLI commands mentioned above, the router must be running Cisco IOS Release 12.4(20)T or later. If you experience any problems, refer to the "Troubleshooting an Upgrade or Reverting the AP to Autonomous Mode" section in the ISR configuration guide at this URL:

http://www.cisco.com/en/US/docs/routers/access/800/860-880-890/software/configuration/guide/admin_ap.html#wp1061143

In order to support CAPWAP or LWAPP, the router must be activated with at least the Cisco Advanced IP Services IOS license-grade image. A license is required to upgrade to this IOS image on the router. Refer to this URL for licensing information:

http://www.cisco.com/en/US/docs/routers/access/sw_activation/SA_on_ISR.html

After the AP801 boots up with the recovery image for the unified mode, it requires an IP address in order to communicate with the controller and to download its unified image and configuration from the controller. The router can provide DHCP server functionality, the DHCP pool to reach the controller, and setup option 43 for the controller IP address in the DHCP pool configuration. Use the following configuration to perform this task:

```
ip dhcp pool pool_name
    network ip_address subnet_mask
    dns-server ip_address
    default-router ip_address
    option 43 hex controller_ip_address_in_hex
Example:
ip dhcp pool embedded-ap-pool
    network 60.0.0.0 255.255.255.0
    dns-server 171.70.168.183
    default-router 60.0.0.1
    option 43 hex f104.0a0a.0a0f /* single WLC IP address (10.10.10.15) in hex format */
```

The AP801 802.11n radio supports lower power levels than the 802.11n radio in the Cisco Aironet 1250 series access points. The AP801 stores the radio power levels and passes them to the controller when the access point joins the controller. The controller uses the supplied values to limit the user's configuration.

The AP801 can be used in hybrid-REAP mode. Refer to Chapter 14 for more information on hybrid REAP.

Note For more information on the AP801, refer to the documentation for the Cisco 800 Series ISRs at this URL:

http://www.cisco.com/en/US/products/hw/routers/ps380/tsd_products_support_series_home.html.

Access Point Communication Protocols

In controller software release 5.2 or later, Cisco lightweight access points use the IETF standard Control and Provisioning of Wireless Access Points protocol (CAPWAP) to communicate between the controller and other lightweight access points on the network. Controller software releases prior to 5.2 use the Lightweight Access Point Protocol (LWAPP) for these communications.

CAPWAP, which is based on LWAPP, is a standard, interoperable protocol that enables a controller to manage a collection of wireless access points. CAPWAP is being implemented in controller software release 5.2 for these reasons:

- To provide an upgrade path from Cisco products that use LWAPP to next-generation Cisco products that use CAPWAP
- To manage RFID readers and similar devices
- To enable controllers to interoperate with third-party access points in the future

LWAPP-enabled access points are compatible with CAPWAP, and conversion to a CAPWAP controller is seamless. For example, the controller discovery process and the firmware downloading process when using CAPWAP are the same as when using LWAPP. The one exception is for Layer 2 deployments, which are not supported by CAPWAP.

Deployments can combine CAPWAP and LWAPP software on the controllers. The CAPWAP-enabled software allows access points to join either a controller running CAPWAP or LWAPP. The only exception is the Cisco Aironet 1140 Series Access Point, which supports only CAPWAP and therefore joins only controllers running CAPWAP.

Guidelines for Using CAPWAP

Keep these guidelines in mind when using CAPWAP:

- CAPWAP and LWAPP controllers cannot be used in the same mobility group. Therefore, client mobility between CAPWAP and LWAPP controllers is not supported.
- If your firewall is currently configured to allow traffic only from access points using LWAPP, you must change the rules of the firewall to allow traffic from access points using CAPWAP.
- Make sure that the CAPWAP ports are enabled and are not blocked by an intermediate device that could prevent an access point from joining the controller.
- Any access control lists (ACLs) in your network might need to be modified if CAPWAP uses different ports than LWAPP.

The Controller Discovery Process

In a CAPWAP environment, a lightweight access point discovers a controller by using CAPWAP discovery mechanisms and then sends it a CAPWAP join request. The controller sends the access point a CAPWAP join response allowing the access point to join the controller. When the access point joins the controller, the controller manages its configuration, firmware, control transactions, and data transactions.

Lightweight access points must be discovered by a controller before they can become an active part of the network. The lightweight access points support these controller discovery processes:

- **Layer 3 CAPWAP or LWAPP discovery—**Can occur on different subnets from the access point and uses IP addresses and UDP packets rather the MAC addresses used by Layer 2 discovery.
- **Over-the-air provisioning (OTAP)—**This feature is supported by Cisco 4400 series controllers. If this feature is enabled on the controller (on the controller General page), all associated access points transmit wireless CAPWAP or LWAPP neighbor messages, and new access points receive the controller IP address from these messages. This feature is disabled by default and should remain disabled when all access points are installed.
- **Locally stored controller IP address discovery—**If the access point was previously associated to a controller, the IP addresses of the primary, secondary, and tertiary controllers are stored in the access point's non-volatile memory. This process of storing controller IP addresses on access points for later deployment is called *priming the access point*.
- **DHCP server discovery—**This feature uses DHCP option 43 to provide controller IP addresses to the access points. Cisco switches support a DHCP server option that is typically used for this capability.
- **DNS discovery—**The access point can discover controllers through your domain name server (DNS). For the access point to do so, you must configure your DNS to return controller IP addresses in response to CISCO-CAPWAP-CONTROLLER.*localdomain* or CISCO-LWAPP-CONTROLLER.*localdomain*, where *localdomain* is the access point domain name. When an access point receives an IP address and DNS information from a DHCP server, it contacts

the DNS to resolve CISCO-CAPWAP-CONTROLLER.*localdomain* or CISCO-LWAPP-CONTROLLER.*localdomain*. When the DNS sends a list of controller IP addresses, the access point sends discovery requests to the controllers.

WCS User Interface

The WCS user interface enables the network operator to create and configure Cisco Unified Wireless Network Solution coverage area layouts, configure system operating parameters, monitor real-time Cisco Unified Wireless Network Solution operation, and perform troubleshooting tasks using an HTTPS web browser window. The WCS user interface also enables the WCS administrator to create, modify, and delete user accounts; change passwords; assign permissions; and schedule periodic maintenance tasks. The administrator creates new usernames and passwords and assigns them to predefined permissions groups.

Note Cisco recommends Internet Explorer 6.0, Internet Explorer 7.0, Mozilla Firefox 2.0, or Mozilla Firefox 3.0 for full access to WCS functionality.

Cisco WCS Navigator

The Cisco Wireless Control System Navigator (Cisco WCS Navigator) manages multiple Cisco WCSs (running the same version as Navigator) and provides a unified view of the network. It uses SOAP/XML over HTTPs to communicate with individual WCSs. With WCS Navigator, there is monitoring functionality and reporting capability across all WCSs. In addition, network wide searches are available. In Windows and Linux, Cisco WCS Navigator runs as a service, which runs continuously and resumes running after a reboot.

In order for the WCS Navigator to detect the regional WCSs, you must manually add them to the system using either the IP address or hostname and specify the login credentials for each of the regional WCSs. After being added, WCS Navigator provides summary information and links to the regional WCS systems.