Cisco Prime Infrastructure Overview

The Cisco Prime Infrastructure is a network management tool that supports lifecycle management of your entire network infrastructure from one graphical interface. Prime Infrastructure provides network administrators with a single solution for provisioning, monitoring, optimizing, and troubleshooting both wired and wireless devices. Robust graphical interfaces make device deployments and operations simple and cost-effective.

Prime Infrastructure provides two different graphical user interfaces (from which you can switch back and forth by clicking the downward arrow next to your login name):

- Lifecycle view, which is organized according to home, design, deploy, operate, report and administer menus.
- Classic view, which closely corresponds to the graphical user interface in the Cisco Prime Network Control System 1.1 or Cisco Wireless Control System (WCS).

The Cisco Prime Infrastructure enables you to configure and monitor one or more controllers, switches and associated access points. Prime Infrastructure 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.

On Linux, the Prime Infrastructure runs as a service, which runs continuously and resumes running after a reboot.

Prime Infrastructure simplifies controller configuration and monitoring and reduces data entry errors. Prime Infrastructure uses the industry-standard SNMP protocol to communicate with the controllers.

Prime Infrastructure also includes the Floor Plan editor, which allows you to do the following:

- Access vectorized bitmap campus, floor plan, and outdoor area maps.
- Add and change wall types.
- Import the vector wall format maps into the database.

The vector files allow the Cisco Prime Infrastructure RF Prediction Tool to make better RF predictions based on more accurate wall and window RF attenuation values.

For information on browser requirment, see *Cisco Prime Infrastructure 2.0 Quick Start Guide.*

This chapter describes the different components in Cisco Unified Network and contains the following sections:

Cisco Unified Network Components

The Cisco Unified Wireless Network (CUWN) solution is based on Wireless LAN Controllers running Airespace Operating System. The wireless LAN controller models include 2100, 2500, 4400, WiSM/WiSM2 (6500 service module), 5500, 7500, 8500. In this solution, access points tunnel the wireless traffic to the controllers through CAPWAP.

The Cisco Unified Access (UA) Wireless Solution is new architecture that provides a converged model where you can manage your wired and wireless network configurations in the same place. This solution includes the 3850 series switch with integrated wireless support. The solution also includes the 5760 series wireless controller, which can act as an aggregation point for many 3850 switches. This platform is based on IOS-XE, so the command structure is similar to other IOS products. In this solution, the wireless traffic can terminate directly on the 3850 switch, so that it can be treated in a similar mode to a wired connection on the switch. This section describes the different components in the Cisco Unified Network and contains the following topics:

Cisco Wireless LAN Controller

The Cisco Wireless LAN Controllers are highly scalable and flexible platforms that enables system wide services for mission-critical wireless in medium to large-sized enterprises and campus environments. Designed for 802.11n performance and maximum scalability, the WLAN controllers offer enhanced uptime with the ability to simultaneously manage from 5000 access points to 250 access points; superior performance for reliable streaming video and toll quality voice; and improved fault recovery for a consistent mobility experience in the most demanding environments.

Prime Infrastructure supports the Cisco wireless controllers that help reduce the overall operational expense of Cisco Unified Networks by simplifying network deployment, operations, and management. The following WLAN controllers are supported in the Prime Infrastructure:

- Cisco 2106 Wireless LAN Controllers
- Cisco 2500 Series Wireless Controllers
- Cisco 4400 Series Wireless LAN Controllers
- Cisco 5508 Series Wireless Controllers
- Cisco Wireless Services Modules (WiSMs) for Cisco Catalyst 6500 Series Switches
- Cisco Wireless Services Module 2 (WiSM2) for Cisco Catalyst 6500 Series Switches
- Cisco Flex 7500 Series Wireless Controllers
- Cisco Flex 8500 Series Wireless Controllers
- Cisco Service Module Wireless Controllers
- Cisco Virtual Wirelesss Controllers
- Cisco 5760 Series Wireless LAN Controller
- Cisco Catalyst 3850 Series Ethernet Stackable Switch

Virtual LAN Controllers

The virtual wireless LAN controller is a software that can run on a hardware that is compliant with an industry standard virtualization infrastructure. Virtual Wireless LAN Controllers provide flexibility for users to select the hardware based on their requirement.

When you view or configure the properties of a virtual wireless LAN controller using the controller configuration page, the Prime Infrastructure displays the value of the Device Type as VWLC (Configure > Controllers > *IP address* > Properties > Settings).

Features Not Supported by Virtual LAN Controllers

Following is the list of features that are not supported by VLAN controllers:

- Data DTLS
- Cisco 600 Series OfficeExtend Access Points
- Wireless rate limiting
- Internal DHCP server
- Mobility/guest anchor
- Multicast-unicast mode
- PMIPv6
- Controller High Availability
- Outdoor mesh access points

Note Outdoor AP in FlexConnect mode is supported.

Access Points

Prime Infrastructure supports the industry-leading performance access points for highly secure and reliable wireless connections for both indoor and outdoor environments. Prime Infrastructure supports a broad portfolio of access points targeted to the specific needs of all industries, business types, and topologies.

The following access points are supported in the Prime Infrastructure:

- Cisco Aironet 801, 802, 1040, 1100, 1130, 1140, 1200, 1230, 1240, 1250, 1260, 1310, 1500, 1522, 1524, 1552, 2600i, 2600e, 3500i, 3500e, 3500p, 3600i, and 3600e Series Lightweight Access Points.
- Cisco Aironet 1040, 1100, 1130, 1141, 1142, 1200, 1240, 1250, and 1260.
- Cisco 600 Series OfficeExtend Access Points.
- Cisco Aironet Access Points running Lightweight Access Point Protocol (LWAPP) or Control and Provisioning of Wireless Access Points (CAPWAP) protocol.

Embedded Access Points

Prime Infrastructure 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 software 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 the **service-module wlan-ap 0 bootimage unified** command on the router in privileged EXEC mode.

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

After enabling the recovery image, enter the **service-module wlan-ap 0 reload** command on the router to shut down and reboot the access point. 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 previously, the router must be running Cisco IOS Release 12.4(20)T or later. If you experience any problems, see the "Troubleshooting an Upgrade or Reverting the AP to Autonomous Mode" section in the Integrated Services Router configuration guide at the following URL:
http://www.cisco.com/en/US/docs/routers/access/800/860-880-890/software/configuration/guide/admin_ap.html

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 Cisco IOS image on the router. See the following 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 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 209.165.200.224 255.255.255.224
    dns-server 209.165.200.225
    default-router 209.165.200.226
    option 43 hex f104.0a0a.0a0f /* single WLC IP address (209.165.201.0) in hex format */
```

The AP801 802.11n radio supports power levels lower 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 configuration.

The AP801 can be used in FlexConnect mode.

Note For more information about AP801, see the documentation for the Cisco 800 Series ISRs at the following 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 (CAPWAP) protocol 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 the following 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.

Note The Cisco Aironet 1140 series and 3500 series access points associate only with CAPWAP controllers that run WLC versions 7.0 or later.

This section contains the following topics:

Guidelines and Restrictions for 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.

WLAN Controller Autodiscovery

Controller Autodiscovery is limited to the Cisco WLAN Solution mobility group subnets defined by the operator.

The Cisco Wireless LAN Controller Autodiscovery:

- Allows operators to search for a single controller by IP address.
- Finds the controller on the network within the specified IP address range.
- Automatically enters the controller information into the Cisco Prime Infrastructure database.

Note Controller Autodiscovery can take a long time in a Class C address range. Because of the large number of addresses in a Class B or Class A range, we recommend that you do not attempt Autodiscovery across Class B or Class A ranges.

As access points associate with a controller, the controller immediately transmits the access point information to Cisco Prime Infrastructure, which automatically adds the access point to the database.

Once the access point information is added to the Cisco Prime Infrastructure database, operators can add the access point to the appropriate spot on a Cisco Prime Infrastructure user interface map.

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 the following 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 than 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 (in 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 non-volatile memory of an access point. 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.

Prime Infrastructure Services

The IT departments within organizations are tasked with meeting increased bandwidth and performance demands, managing a proliferation of new mobile devices, while guaranteeing network access, availability, and regulatory compliance.

Cisco and its partners can work with IT staff to assist with migration to the Cisco Unified Network, making it easier to manage a secure, high-performance, and integrated wired and wireless network that incorporates rich media and diverse mobile devices, including Wi-Fi-enabled phones and tablets.

This section describes the services provided by the Prime Infrastructure and contains the following topics:

Cisco Context-Aware Service Solution

Context-Aware Service (CAS) provides the capability for a Wi-Fi 802.11a/b/g/n network to determine the location of a person or object with an active Wi-Fi device, such as a wireless client or active RFID tag and/or associated data that can be passed by the end point through the wireless infrastructure to an upstream client.

Context-Aware Service (CAS) allows a mobility services engine (MSE) to simultaneously track thousands of mobile assets and clients by retrieving contextual information such as location and availability from Cisco access points.

The collected contextual information can be viewed in GUI format in the Prime Infrastructure User Interface, the centralized WLAN management platform. Prime Infrastructure is the management system that interfaces with the MSE and serves the user interface (UI) for the services that the MSE provides.

After the MSE installation and initial configurations are complete, the MSE can communicate with multiple Cisco wireless LAN controllers to collect operator-defined contextual information. You can then use the associated Prime Infrastructure to communicate with each MSE to transfer and display selected data.

You can configure the MSE to collect data for clients, switches, rogue access points, rogue clients, mobile stations, and active RFID asset tags.

With Context-Aware Location Services, administrators can determine the location of any 802.11-based device, as well as the specific type or status of each device. Clients (associated, probing, and so on.), rogue access points, rogue clients, and active tags can all be identified and located by the system. See the Context-Aware Mobility Solution Deployment Guide for more information.

Note One MSE can be managed by only one Prime Infrastructure, that is, a single MSE cannot be managed by more than one Prime Infrastructure, but a single Prime Infrastructure can manage multiple MSEs. When the number of devices to be managed exceeds the capacity of a single MSE, you need to deploy multiple, independent MSEs.

Cisco Identity Service Engine Solution

The Cisco Identity Services Engine (ISE) is a next-generation identity and policy-based network access platform that enables enterprises to enforce compliance, enhance infrastructure security, and streamline their service operations.

The Cisco ISE provides a single console where authentication, authorization, posture, guest, and profiling policies can be created and managed. In addition, policy elements can now be reused across all services, reducing the number of tasks and overhead and bringing consistency to the enterprise.

The Cisco ISE gathers information from devices, the infrastructure, and services to enable organizations to build richer contextual policies that can be enforced centrally across the network. The ISE tracks all clients and devices connected to the network, acting as a single source of information for connected user and device identity and location, as well as the health of the endpoint.

The ability to discover, identify, and monitor all IP-enabled endpoint devices gives IT teams complete visibility of both users and "headless" devices on the corporate network.

The Cisco ISE combines AAA, posture, profiling, and guest management capabilities in a single appliance to enforce dynamic access control. The Identity Services Engine can be deployed across the enterprise infrastructure, supporting 802.1x wired, wireless, and VPN networks.

Prime Infrastructure manages the wired and the wireless clients in the network. When Cisco ISE is used as a RADIUS server to authenticate clients, the Prime Infrastructure collects additional information about these clients from Cisco ISE and provides all client relevant information to the Prime Infrastructure to be visible in a single console.

When posture profiling is enforced in the network, the Prime Infrastructure talks to Cisco ISE to get the posture data for the clients and displays it along with other client attributes. When Cisco ISE is used to profile the clients or an endpoint in the network, the Prime Infrastructure collects the profiled data to determine what type of client it is, whether it is an iPhone, iPad, an Android device, or any other device.

Cisco ISE is assisting the Prime Infrastructure to monitor and troubleshoot client information, and displays all the relevant information for a client in a single console.

Cisco Adaptive Wireless Intrusion Prevention Service

Maintain a constant awareness of your RF environment to minimize legal liability, protect your brand reputation, and assure regulatory compliance.

Cisco Adaptive Wireless Intrusion Prevention System (IPS) offers advanced network security for dedicated monitoring and detection of wireless network anomalies, unauthorized access, and RF attacks. Fully integrated with the Cisco Unified Network, this solution delivers integrated visibility and control across the network, without the need for an overlay solution.

Cisco Adaptive Wireless Intrusion Prevention Service (wIPS) performs rogue access point, rogue client, and ad-hoc connection detection and mitigation, over-the-air wireless hacking and threat detection, security vulnerability monitoring, performance monitoring and self-optimization, network hardening for proactive prevention of threats and complete wireless security management and reporting.

Cisco wIPS is made up of the following components that work together to provide a unified security monitoring solution:

- Mobility services engine (MSE) running wIPS software—Serves as the central point of alarm aggregation for all controllers and their respective wIPS monitor mode access points. Alarm information and forensic files are stored on the mobility services engine for archival purposes.
- A wIPS monitor mode access point—Provides constant channel scanning with attack detection and forensics (packet capture) capabilities.
- Local mode access point—Provides wireless service to clients in addition to time-sliced rogue scanning.
- Wireless LAN Controller—Forwards attack information received from wIPS monitor mode access points to the mobility services engine and distributes configuration parameters to access points.
- Prime Infrastructure—Provides a centralized management platform for the administrator to configure the wIPS Service on the mobility services engine, push wIPS configurations to the controller, and configure access points in wIPS monitor mode. Prime Infrastructure is also used to view wIPS alarms, forensics, reporting, and to access the attack encyclopedia.