- Cisco 802.11 Implementations -

Cisco Unified Wireless Network

The **Cisco Unified Wireless Network (UWN)** is a platform for simplifying and centralizing the management of an enterprise Wireless LAN (WLAN) solution. It addresses the following aspects of WLAN environments:

- WLAN security
- WLAN deployment
- WLAN management
- WLAN control

The Cisco Unified Wireless Network is comprised of five elements:

- **Client Devices** – includes all wireless-enabled VoIP, handheld, notebook, and appliance hardware. The **Cisco Compatible Extensions (CCX)** program ensures that wireless clients are compatible with Cisco WLAN equipment.

- **Mobility Platform** – includes all Cisco **Aironet** Wireless Access Point (WAP) and Lightweight WAP (LWAP) product families.

- **Network Unification** – includes Cisco Wireless LAN Controllers (WLCs) to integrate the wireless environment into the wired infrastructure.

- **Network Management** – includes the software tools to centrally manage WLAN security and configuration, using **Cisco Wireless Control System (WCS)**.

- **Unified Advanced Services –** includes mobility applications, Intrusion Detection/Prevention Systems (IDS/IPS), and the Cisco Wireless Location Appliance.

(Reference: CCNP BCMSN Official Exam Certification Guide 4th Edition. David Hucaby. Pages 503-504
http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps430/prod_brochure09186a0080184925.html)

Cisco Compatible Extensions (CCX)

A large number of vendors have released wireless client software and hardware. **Cisco Compatible Extensions (CCX)** is a certification program to identify the interoperability of these clients with Cisco WAPs and LWAPs, and the capabilities and features supported by each client.

There are currently five categories of CCX. Each successive category supports the features and capabilities of the preceding categories. The following is a brief list of the features supported by each CCX specification:

- **CCXv1** – Standard 802.11 features, 802.1X with LEAP
- **CCXv2** – WPA, 802.1X with PEAP
- **CCXv3** – WPA2, 802.1X with EAP-FAST
- **CCXv4** – Network Admission Control (NAC), Call Admission Control for VoIP
- **CCXv5 –** Advanced troubleshooting and client reporting functionality

A comprehensive breakdown of the supported features of each CCX specification can be found here:

http://www.cisco.com/web/partners/pr46/pr147/program_additional_information_new_release_features.html

A list of CCX-compliant wireless clients can be found here:

http://www.cisco.com/web/partners/pr46/pr147/partners_pgm_partners_0900aecd800a7907.html

Autonomous vs. Lightweight WAPs

There are two categories of Wireless Access Points (WAPs):

- **Autonomous WAPs**
- **Lightweight WAPs (LWAPs)**

Autonomous WAPs operate independently, and each contains its own configuration file and security policy. Autonomous WAPs suffer from scalability issues in enterprise environments, as a large number of independent WAPs can quickly become difficult to manage.

Centralized management of Autonomous WAPs is still possible using products like CiscoWorks Wireless LAN Solution Engine (WLSE).

Lightweight WAPs (LWAPs) are centrally controlled using one or more **Wireless LAN Controllers (WLCs)**, providing a more scalable solution than Autonomous WAPs.

Each LWAP performs the real-time RF functions between the client and the LWAP, but is otherwise *completely dependent* on a WLC to operate. The WLC provides a variety of functions for the LWAP, including:

- **Intelligent Channel Assignment –** preventing channel overlap with other LWAPs in the vicinity.
- **Intelligent Power Optimization –** ensuring full wireless coverage, and providing self-healing if a LWAP fails.
- **Fast Roaming** – allowing clients to quickly roam between LWAPs.
- **User Authentication** and **Security Policy Management**

Distributing the 802.11 functions between the LWAP and WLC is known as a **Split MAC** approach.

A single WLC can control multiple LWAPs (the exact number is dependent on the WLC model). In larger environments, multiple WLCs may be necessary. WLCs and their corresponding LWAPs can be centrally managed using Cisco Wireless Control System (WCS).

LWAPs and WLCs authenticate each other using pre-installed X.509 digital certificates. This prevents rogue LWAPs and WLCs from disrupting or invading the wireless network.

(Reference: CCNP BCMSN Official Exam Certification Guide 4th Edition. David Hucaby. Pages 501-510; http://tools.ietf.org/html/rfc5412)

LWAP and WLC Functionality

LWAPs and WLCs communicate using the **Lightweight Access Point Protocol (LWAPP)**. LWAPP was developed by Airespace, which was bought out by Cisco. LWAPP has been submitted to the IETF for standardization.

LWAPP can operate at either the Layer-2 or Layer-3 layers. This guide will focus on Layer-3 LWAPP operations.

Before a LWAP can become functional, it must follow a specific process during bootup:

1. The LWAP is assigned an IP address via DHCP.
2. The LWAP discovers the IP address of a WLC, or a list of WLCs.
3. The LWAP sends a *join request* to the first WLC in the list, and will continue down the list until it receives a *join reply* from a WLC.
4. (Optional) The WLC will forward an updated software image to the LWAP, if the LWAP is out of date. The LWAP will then reboot and restart this process.
5. The LWAP and WLC create a secure tunnel for management traffic.
6. The LWAP and WLC create a non-secure tunnel for client data traffic.

LWAPs can discover the WLC(s) one of two ways:

- Via DHCP, using option 43 to identify WLCs.
- By broadcasting a *join request* message. This requires that the WLC is on the same IP subnet as the LWAP.

LWAPP **Control Messages** are used to configure and manage the LWAP, and are passed between the LWAP and WLC via the secure tunnel. The secure tunnel is encrypted using AES, and the control messages operate on **UDP destination port 12223**.

LWAPP **client data** is passed via the non-secure tunnel. If an encryption mechanism like WPA-TKIP or WPA-AES is used, the data traffic is *only* encrypted between the wireless client and the LWAP, not the LWAP and the WLC. LWAPP client data operates on **UDP destination port 12222**.

If a LWAP loses contact with its WLC, it will reboot and attempt to bind with another WLC. A LWAP can only be bound to one WLC at a time.

(Reference: http://www.cisco.com/en/US/docs/wireless/controller/4.0/configuration/guide/c40ovrv.html; http://tools.ietf.org/html/rfc5412)

CiscoWorks Wireless LAN Solution Engine (WLSE)

CiscoWorks Wireless LAN Solution Engine (WLSE) is a hardware appliance used to centrally manage *autonomous* WAPs. WLSE provides the following centralized features:

- Configuration of WAPs (individually or in groups).
- Monitoring and reporting of WAPs.
- Firmware upgrades for WAPs.
- Intrusion Detection System (IDS) functionality.

Implementing WLSE provides the following benefits:

- **Improved Security** – through the use of IDS to mitigate rogue WAPs, and the reporting of misconfigured security policies on WAPs.
- **Simplified WAP Deployment** – through the use of deployment wizards to quickly configure new WAPs.
- **Improved RF Management** – through the use of wireless coverage maps, and the use of self-healing functions if a WAP or WAPs fail.
- **Simplified Management and Reporting –** through the use of threshold-based monitoring, centralized firmware upgrades, and advanced reporting.

WLSE is supported by most Cisco Aironet WAPs, and is designed for large environments with up to 2500 managed devices. Cisco also provides **WLSE Express** for smaller environments with up to 100 managed devices. WLSE Express includes built-in AAA services.

(Reference: CCNP ONT Official Exam Certification Guide. Amir Ranjbar. Pages 295-299; http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6380/ps6563/ps3915/ps6688/prod_qas0900aecd80410bb5.html)

Cisco Wireless Control System (WCS)

Cisco Wireless Control System (WCS) is a software solution used to centrally manage *lightweight* WAPs (LWAPs) and Wireless LAN Controllers (WLCs).

There are three versions of Cisco WCS:

- WCS Base
- WCS Location
- WCS Location with Wireless Location Appliance.

The base product supports the following features:

- Auto-discovery of LWAPs as they bind with WLCs.
- Mitigation of rogue WAPs.
- Wireless coverage maps over custom floor-plan graphics.
- Centralized configuration of all LWAPs and WLCs.
- Advanced monitoring and logging of all devices, security violations, and gaps in wireless coverage.

WCS Location provides highly-detailed location tracking of a single LWAP (or rogue WAP), accurate to within 10 meters using **Received Signal Strength Indicators (RSSI)**. A Wireless Location Appliance enhances this capability to up to 1500 LWAPs simultaneously.

WCS is designed to support up to 50 WLCs and 1500 LWAPs, and is supported on Windows 2000/2003 and Red Hat Linux platforms. WCS is configured using a web interface via HTTPS.

(Reference: CCNP ONT Official Exam Certification Guide. Amir Ranjbar. Pages 299-313; http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps6301/ps6305/product_data_sheet0900aecd802570d0.html)

802.11 QoS

If two 802.11 wireless devices transmit simultaneously, their signals will mix resulting in unusable noise (essentially a *wireless collision*).

802.11 devices have no method of *detecting* a collision, beyond the failure of the receiving device to send an **acknowledgement**. Instead, 802.11 devices attempt to avoid collisions using **Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA).** Devices will listen before attempting to transmit, and will *only* transmit if no other device is currently transmitting.

If another device *is* transmitting, other devices must wait until that transmission is finished, using a process called **Distributed Coordination Function (DCF)**. The currently transmitting device includes a **duration value** within the 802.11 header, informing other devices of the estimated time-length of its transmission.

Other 802.11 devices will not only wait out this duration value, but will wait an additional random amount of time (referred to as the **DCF interframe space (DIFS)**), before beginning their own transmissions. The random DIFS was implemented to prevent devices from transmitting simultaneously after waiting out another device's transmission duration. DIFS is often referred to as a **random back-off timer.**

DCF provides no QoS mechanism to service higher priority traffic before lower priority traffic. The IEEE developed the **802.11e amendment** to address this shortcoming. While 802.11e was still in draft, the Wi-Fi Alliance released a comparable specification for QoS called the **Wi-Fi Multimedia (WMM).**

802.11e defines **eight** *priority levels* for RF traffic, while WMM defines for **four.** Packets **marked** with a higher priority level are given preference for RF transmission, by providing shorter random back-off timers for that traffic. The prioritized back-off timer is part of 802.11e/WMM's **Enhanced Distributed Coordination Function (EDCF).**

802.11e/WMM Priority Levels

The following table defines the priority levels employed by 802.11e and WMM, and how they relate to Ethernet 802.1p CoS and IP DSCP values:

WMM Priority	***802.11e Priority***	***802.1p CoS***	***IP DSCP***	***General Application***
Silver (Best-Effort)	0 or 3	0	0	*Best effort* forwarding
Bronze (Background)	1	1	AF11	Medium priority forwarding
	2	2	AF21	High priority forwarding
Gold (Video)	4	3	AF31	VoIP call signaling forwarding
	5	4	AF41	Video conferencing forwarding
Platinum (Voice)	6	5	EF	VoIP forwarding
	7	6	48	Inter-network control (*Reserved*)
	7	7	56-62	Network control (*Reserved*)

802.1p CoS and IP DSCP are covered extensively in another guide.

An LWAP that receives a client packet marked with an 802.11e/WMM priority will map the 802.11e/WMM value to a DSCP value, and then pass the packet to the WLC using LWAPP. If there is no 802.11e/WMM mark on a packet, the traffic will be forwarded on a best-effort basis.

The LWAPP can be configured with one of three settings relating to 802.11e/WMM compatibility:

- **Disabled** – ignores 802.11e/WMM priority marks within traffic headers.
- **Allowed** – provides appropriate priority service to 802.11e/WMM marked traffic. Client traffic that is not 802.11e/WMM compliant will be forwarded on a best-effort basis.
- **Required** – requires that all wireless clients be WMM/802.11e compliant.

(Reference: CCNP ONT Official Exam Certification Guide. Amir Ranjbar. Pages 235-246)

* * *