Wireless Technology
Process Oriented Guided Inquiry learning

1. **Discuss the Cisco elements of UWN**
   The Cisco WCS includes tools for WLAN planning and design, RF management, basic location tracking, intrusion prevention systems, and WLAN systems configuration, monitoring, and management

2. **What are the benefits of Cisco UWN**
   Benefits of the Cisco UWN architecture include ease of deployment and upgrades, reliable connectivity through dynamic RF management, optimized per-user performance through user load balancing, guest networking, Layer 2 and 3 roaming, embedded wireless IDS, location services, voice over IP support, lowered total cost of ownership, and wired and wireless unification.

3. **Give the UWN Architecture**
   With the explosion of wireless solutions in and out of the enterprise, designers must create solutions that provide mobility and business services while maintaining network security. The Cisco Unified Wireless Network (UWN) architecture combines elements of wireless and wired networks to deliver scalable, manageable, and secure WLANs. As shown in Figure 4-2, the Cisco UWN architecture is composed of five network elements:

   A. **Client devices:** These include laptops, workstations, IP phones, PDAs, and manufacturing devices to access the WLAN.
   B. **Access points:** These devices provide access to the wireless network. APs are placed in strategic locations to minimize interference.
   C. **Network unification:** The WLAN system should be able to support wireless applications by providing security policies, QoS, intrusion prevention, and radio frequency (RF) management. Cisco WLAN controllers provide this functionality and integration into all major switching and routing platforms.

D. **Network management:** The Cisco Wireless Control System (WCS) provides a central management tool that lets us design, control, and monitor wireless networks.
E. **Mobility services:** These include guest access, location services, voice services, and threat detection and mitigation.

4. **What is LWAPP**

In the Cisco Unified Wireless Architecture, a wireless LAN controller (WLC) is used to manage the wireless access point configuration and firmware creating an LWAPP tunnel. LWAPP provides the control messaging protocol and data encapsulation. In other words, the wireless client data packets are encapsulated between the access point and the WLC.

5. **Explain layer 3 LWAPP**

Layer 3 LWAPP control and data messages are transported over the IP network in User Datagram Protocol (UDP) packets. Layer 3 LWAPP is supported on all Cisco WLC platforms and lightweight APs.

The only requirement is established IP connectivity between the APs and the WLC. The LWAPP tunnel uses the IP address of the AP and the AP-Manager interface IP address of the WLC as endpoints. On the AP side, both LWAPP control and data messages use an ephemeral port that is derived from a hash of the AP MAC address as the UDP port. On the WLC side, LWAPP data messages always use UDP port 12222, and LWAPP control messages always use UDP port 12223. The process of clients sending frames in Layer 3

6. **What are the different AP modes**

There are different Access Point Modes that we can configure on Cisco Access Points. These Wireless AP Modes are given below:

A. Client Mode
B. Local Mode
C. Sniffer
D. SE-Connect
E. Rogue Detector
F. Flexconnect
G. Bridge

H. Monitor
I. REAP/H-REAP

7. **What is CAPWAP and WLC**

The Control And Provisioning of Wireless Access Points (CAPWAP) protocol is a standard, interoperable networking protocol that enables a central wireless LAN Access Controller (AC) to manage a collection of Wireless Termination Points (WTPs), more commonly known as wireless access points.

A wireless LAN controller is used in combination with the Lightweight Access Point Protocol to manage light-weight access points in large quantities by the network administrator or network operations center. The wireless LAN controller is part of the Data Plane within the Cisco Wireless Model

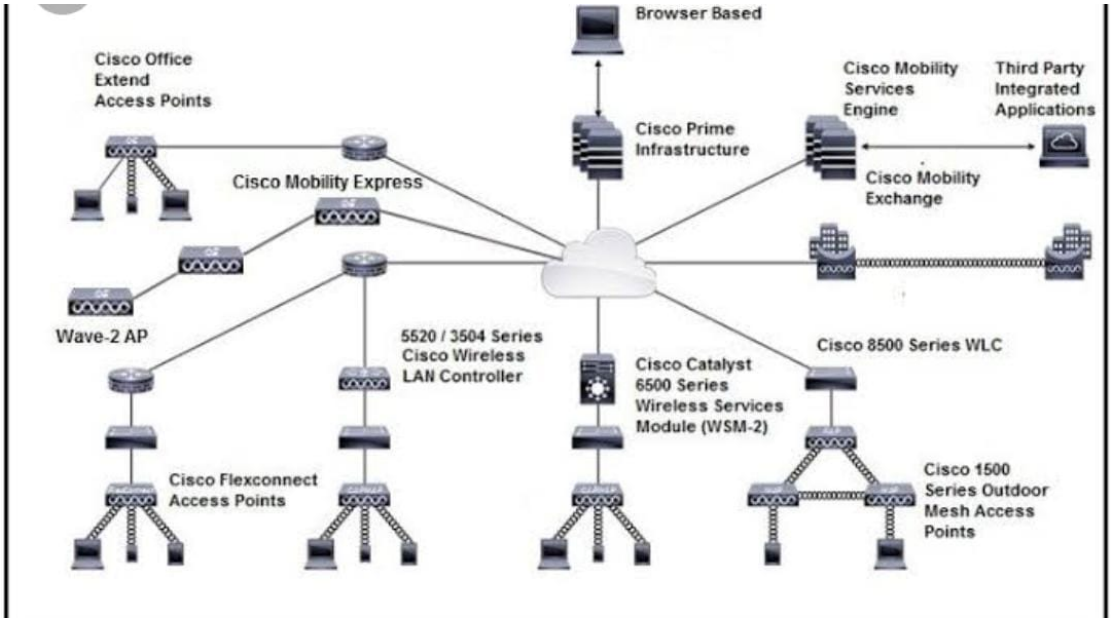
8. **Discuss LWAP MAC functions**

Lightweight Access Point Protocol (LWAPP) is the name of a protocol that can control multiple Wi-Fi wireless access points at once. This can reduce the amount of time spent on configuring, monitoring or troubleshooting a large network. The system will also allow network administrators to closely analyze the network.

9. **Discuss the major components of WLC**

A WLC interface is a logical connection that maps to a VLAN on the wired network. Each interface is configured with a unique IP address, default gateways, physical ports, VLAN tag, and DHCP server.

The port is a physical connection to the neighboring switch or router. By default, each port is an IEEE 802.1Q trunk port.



10. What are the five Interface types of WLC

Five different types of interfaces (Management, AP-Manager, Virtual, Service-Port, and Dynamic Interfaces), I figured I would just take some time to quickly touch on them.

A. **Management Interface:** As we can suspect this interface is for in-band management and handles any communication with AAA servers. This interface will also handle the layer 2 communication between the controller and any APs.

B. **AP-Manager:** If we want to have APs on different subnets other than the subnet the WLC is on then this interface must be configured, it's a requirement for Layer 3 LWAPP transport mode.

C. **Virtual Interface:** This interface handles any mobility management, VPN Termination, Web authentication, and is also a DHCP relay for WLAN clients.

D. **Service-Port:** This is also a physical port for out of band management, so its configuration is optional. (Note: This is only physical port that is active while the controller is booting)

E. **Dynamic Interface:** Now these are the interfaces we can create and use to link specific SSID to specific VLANs on the wire. So this is where and how we can separate our wireless client traffic, this interface will also double as the DHCP relay for it's subnet/VLAN