Wireless

Definitions

- Radio wave hits an uneven surface and it scatters in random directions — **Scattering**
- Radio wave hits a surface causing it to go in different directions creating a blind spot — **Diffraction**
- Radio wave passes through an object which affects its speed. Commonly when a wave passes through **glass or water**. — **Refraction**
- Radio wave get reflected causing a weak signal. Very common when a wave tries to go through a **metal**. — **Reflection**
- Radio wave gets absorbed by an object weaking the signal. Very commonly when a radio wave tries to go through a **wall**. — **Absorption**

- Carrier Sense Multiple Access/Collision Avoidance is used in — **CSMA/CA**
- Basic Service Set describe a wireless LAN being offered by an — **BSS**
- Basic Service Area describes the area of coverage for a given — **BSA**
- Service Set Identifier is readable human name given to a wireless network being offered by an Access Point (AP). The SSID does not — **SSID**
- Basic Service Set Identifier a unique address (based on the MAC address of the AP) to identify a BSS being offered by an Acces — **BSSID**
- Root Access Point mesh-capable access point that is set up with a wired connection to your network and provides Internet — **RAP**
- Distribution System is used to identified the wired portion of a network which the wireless Access point connects to. — **DS**
- Being able to move freely between different BSA (Basic Service Area) without a disruption in service. — **Roaming**

Amplitude / Frequency / Period
- **Amplitude**: Measures the strength of the signal.
- **Frequency**: Measures how many cycle during a specific time frame.
- **Period**: Measures how long it takes for the wave to do one full cycle.

WiFi Bands
- **2.4 Ghz**: Offers better penetration, longer distances, but has overlapping channels and lower speeds in comparison.
- **5 Ghz**: Shorter distances, but offers faster speeds and no overlapping channels.

Standards

802.11	802.11b	802.11a	803.11g	802.11n "Wifi 4"	802.11ac "Wifi 5"	802.11ax "Wifi 6"
2.4 GHz	2.4 GHz	5 GHz	2.4 GHz	2.4 / 5 GHz	5 GHz	2.4 / 5 / 6 GHz
2 Mbps	11 Mbps	54 Mbps	54 Mbps	600 Mbps	6.93 Gbps	4*802.11ac

Infrastructure

Service Sets

Independent
- Also referred to as an **ad-hoc network**, and it allows two more wireless clients to communicate directly via wireless **without an AP**.

Infrastructure
- **BSS**: Infrastructure that relies on a **single AP**. It can offer multiple WLANs but it is *limited in scope(coverage area)* due using only a single AP.
- **ESS**: Wireless infrastructure composed of multiple APs. APs work together so that it create coverage so that it cover an entire floor or building.
- **Mesh**: We create a backhaul traffic of mesh network APs referred to as a Mesh Basic Service Set (MBSS). One radio is for the backhaul traffic, and another radio is to maintain the BSS for wireless clients on another channel.

Access Points
Lets look at some of the architectures for Wireless Access Points.

Autonomous
- Every single AP has to be manually configured (i.e QoS, transmit channels, associations, roaming, power levels, etc).
- Every devices need a remote management IP, and this is hard to scale for medium/large corportations.

Lightweight
- This typic of architecture relies heavily on the WLC; also known as Split-MAC-architecture.
- AP handles real time traffic ; WLC handles the management (Association, Security,QoS,authentication,etc).
- WLC centrally manages the APs that bind to it; WLC and APs authenticate each other using certificates.
- WLC use CAPWAP tunnels to communicate (frames are encapsulated with an IP header).
- CAPWAP Tunnel UDP 5246 : Control (encrypted by default using DTLS). CAPWAP Tunnel UDP 5247: Data (not encrypted by default, but can be encrypted using DTLS).
- CAPWAP Tunnel UDP 5246 : Control (encrypted by default using DTLS) CAPWAP Tunnel UDP 5247: Data (not encrypted by default, but can be encrypted using DTLS).

AP Modes
A lightweight AP has extra modes exclusive to it. It also offers other basic modes such as Repeater, WBG (WorkBridge Group), and Outdoor Brdieg).

Lightweight AP modes
- **Local**: default mode which offers a BSS or multiple BSS.
- **Flexconnect**: allows the APs to switch to autonomous if the WLC connection fails. ALso offers a BSS
- **Sniffer**: captures 802.11 frames and sends them to a device running software such as wireshark.
- **Monitor**: dedicated to receiving 802.11 frames. Main goal is to find rogue devices. If a rogue device is found, the AP can de-
- **Rogue Detector**: does not use wireless radio. It listens to ARP traffic in the wired network. Based on the info sent by the WLC and what it captures in the wired network, it can detect rogue devices. DOes not offer a BSS.
- **SE-Connect**: Dedicated to RF Spectrum analysis on all channels. It can send info to a device on the network to anyalyze and collect data. Does not offer a BSS.
- **Mesh/Bridge**: Similar to the Autonomous Outdoor Bridge mode, can create a bridge between two remote sites over long distances. A mesh can be created between the APs.
- **Flex Plus Bridge**: adds FlexConnect functionality to the Bridge/Mesh mode.

Extra modes
- **Repeater**: offers a BSS; main purpose is to extend the BSA (Basic Service Area) of the wireless
- **Workgroup Bridge (WBG)**: allows devices who lack wireless capabilities to connect to the
- **Outdoor Bridge**: allows remote sites to communicate; APs used a special antenna to be able to communicate

WLC Deployment
Lets look at the different WLC Deployments we
- **Unified**: hardware appliance in a *central location* of the network. Can support up to **6000 APs**.
- **Cloud-based**: a Virtual Machine usually in a data center. Can support up to **3000 APs**.
- **Cloud-based**: integrated within a switc. Supports up to **200 APs**.
- **Express Mobility**: integrated within an AP. Supports up to **100 APs**.

Cloud-based
- It is a mixture of Autonomous and Lightweight AP. Meraki is a dashboard used to configure APs from a cloud-based site.
- Management traffic gets sent to the cloud, while use data goes straight into the wired network as needed.

Wireless Configuration and additional notes
I wanted to use this portion to briefly go over some WLC concepts, and ideas that werent discussed enough in other sections.

WLC QoS Profiles
- **Platinum**: Voice
- **Gold**: Video
- **Silver**: Best Effort
- **Bronze**: Background

WLC Ports vs Interfaces
- **Service port**: physical ports on the WLC for out of band management. Can be used during boot up process, recovery, etc.
- **Distribution system port**: physical ports on the WLC which conects to the wired network and used for data traffic. Connected using LAG (static LAG only) and using trunk ports
- **Console port**: physical port on the WLC, which is either an RJ45 or USB.
- **Redundancy port**: physical port on the WLC used for HA (High availability).

- **Management interface**: logical interfaced in the WLC used management traffic (ie TELENT,SSH,HTTP/HTTPS, RADIUS authentication, NTP, Syslog,CAPWAP Tunnels.
- **Dynamic interfaces**: logical interfaces in the WLC,they map WLANs to VLANs.
- **Redundancy Management interface**: logical interface in the WLC uses to manage the standby WLC using the assigned IP Address.
- **Virtual interface**: logical interface in the WLC used to communicate with wireless clients to relay DHCP requests, peform client web authentication, etc.

AP Binding Algorithm

AP boots up
- AP tries to get an **IP** from a **DHCP server**.
- AP discovers WLC using **discover messages**, using **multicast** addresses or using **option 43** which would be provided by the DHCP server.
- AP might receive an image from an AP and/or configuration information from the WLC (SSID to offer, channel,etc).
- **CAPWAP tunnel is fomed, and the AP will ask if it can bind to the WLC.**
- AP and WLC will authenticated each other using certificates.
- AP will now start offering BSSs. Note: AP will likely have restarted during some of the previous step.

Issues
Wireless comes with plenty of issues we must dealwith such as security, encryption, integrity, half dupllex nature, channel restrictions, and interference.

Half-duplex
- CSMA/CA helps with the half duplex nature of wireless. The AP listens and waits for the channel to not be in use before sending anything. Additionally, the AP can send RTS (Request to Send) messages and wait for a CTS (Clear to Send) message.

Channel restriction
- Due to the channel band 2.4 Ghz having overlapping channels, in North America it is suggested to use channels 1, 6 and 11 to avoid overlaps.

Security
We will break down Security into two main components , authentication and encryption/integrity. The

Authentication

Open Authentication
- The deive here is authenticated. No questions asked. However it is possible to implement other security methods to make this better such as some Layer 3 authentication methods (note that these methods should be used for guest WLANs, not infrastructure)
- **Web Authentication**: Before granting full access to the network, the user must login to a website using a username/password. The client is provided with basic connectivity to be able to accomplish this task.

WEP
- Note that this one also provides encryption using the RC4 algorithm.
- Uses a shared key, keys can be 40 bits (64 bits with the Initlization vector being 24 bits in length) or 104 (128 bits with the initlization vector).
- AP sends a challenge phrase, challenge phrase is encrypted using the WEP key by the client and send to the AP. AP then compares the the phrase sent by the client, if it matches the AP knows the client has the same WEP key.
- **DO NOT USE**. This method was found to be vulnerable and easily cracked.
- **Web Authentication**: Before granting full access to the network, the user musty agree to some sort of terms and conditions through a webister the client was

EAP
EAP is more of a framework on how encryption should work. See the actual protocols below.
- **LEAP**: Created by Cisco. Similar to WEP with some main differences: –It uses **Dynamic WEP keys** per data packet. –AP and Client send **each other** challenge phrases. *Like WEP, it shouldnt be used.*
- **EAP Fast**: Created by Cisco. - AP sends a PAC (Protected Access Cr edential. - A TLS tunnel is established using the PAC. - The Client is then authenticated within the
- **PEAP**: – Works similar to EAP FAST but instead of a PAC, the AP instead sends a certificated. - TLS tunnel is created using the certificated. - Client is then authenticated within the tunnel using something like MS-CHAP (Microsoft Challenge Handshake Protocol).
- **EAP-TLS**: – Works similar to PEAP but instead both the client and AP have a certificated. - TLS tunnel is created using the certificated. - Since both the AP and Client authenticated each other usign the certificated, the tunnel is still used for the purpose of exhcnaging encryption keys. –This is the most secure version of EAP though it requires more work due to needed certificates for both clients and APs.

WPA Standards

- **WPA:**
  - Uses **TKIP** for encryption/MIC.
  - Supports both Enterpises:(**802.1X**) and Personal Mode (**PSK**).
  - Note: uses four-way handshake for authentication, and then the PSK is used to generate encryotion keys for personal mode.
- **WPA2:**
  - Uses **CCMP** for encryption (**AES counter**)/MIC (**CMAC**)
  - Supports both Enterpises(**802.1X**) and Personal Mode(**PSK**).
- **WPA3:**
  - Uses **GCMP** for encryption (**AES Counter**)/MIC (**GMAC**).
  - Supports both Enterpises(**802.1X**) and Personal Mode(**PSK**).
  - Additional features: Protected Management Frame (cant eavesdrop, and is is required in WPA3 although option in WPA2), Simultatneous AUthentication of Equals (protects the 4-way handshake in personal mode), Forward secrecy (frames arent allowed to be unencrypted

Encryption/Integrity
We will break down Security into two main components , authentication and encryption/integrity. The

- **GMCP**: Used in WPA3. Uses AES counter mode for encryption. Uses GMAC for MIC (Message integrity check).
- **CCMP**: Used in WPA2 (developed after TKIP). Uses AES counter mode for encryption. Uses CMAC for MIC (Message integrity check).
- **TKIP**: Uses as temporary solution to WEP. Still uses RC4 for encryption buts added extra security with TKIP (see below) Initlization vector increased to 48 bits, each packet has their own key. Added extra bits of info such as MAC, timestamps and TKIP sequence numbers to stop relay attacks.
- **WEP**: This one was already described on the authentication portion.