CompTIA N+ (N10-009) Day 4

Chapter 5 WiFi Signaling

Effective Isotropic Radiated Power (EIRP)

- **Definition:** The total power radiated by a theoretical isotropic antenna in a single direction. EIRP = Transmit Power + Antenna Gain − Cable Loss.
- **Purpose:** Used to calculate maximum legal wireless output power for compliance with regional regulations.

Received Signal Strength Indicator (RSSI)

- **Definition:** A measure of the signal strength received by a client device.

RSSI Reference Table

(for general Wi-Fi signal quality — values in dBm, where closer to 0 is stronger)

RSSI (dBm)	Signal Quality	Typical Use Case / Impact
-30 to -40	Excellent / Max Strength	Ideal conditions, often right next to the AP.
-50 to -60	Very Good	Strong connection, suitable for all applications.
-60 to -67	Good	Still supports VoIP, video, and most tasks reliably.
-67 to -70	Fair	Minimum for VoIP and HD streaming.
-70 to -80	Poor	Connection unstable; low-speed apps may still work.
< -80	Very Poor / Unusable	Likely drops, very slow speeds, or total loss.

Note: Closer to zero (less negative) is better.

Attenuation / Absorption vs Frequency

- **Concept:** Wireless signals absorb or reflect off surrounding objects (walls, doors, metals, etc.).
- **Interference Source:**
  - Reflections can be caused by flat metal surfaces like elevator shafts, filing cabinets, ducts, and refrigerators.
  - These reflections can lead to **multipath interference**.

Band Steering

- **Definition:** A feature that directs dual-band clients to connect to 5 GHz when signal is strong, and fall back to 2.4 GHz when weak.

Antennas and Polarization

- **Omnidirectional Antenna:** Radiates signal in all horizontal directions equally; best for general coverage.
- **Directional Antenna:** Focuses the signal in one direction for longer range and higher gain; ideal for point-to-point links.
- **Example Use:** Two buildings with directional antennas aimed at each other can form a **wireless bridge**.

Client Disassociation

- **Definition:** When a client device is disconnected from an AP due to certain conditions.
- **Common Causes:**
  - High channel utilization
  - Excessive interference
  - Poor signal strength

Site Survey & Heat Maps

- **Purpose:** To plan and optimize AP placement based on measured signal strength and coverage.
- **Checks:**
  - RSSI readings (not EIRP — EIRP is fixed by AP hardware settings)
  - AP placement
  - Antenna type selection
  - Adjusting power settings to limit unwanted coverage
- **Tools:**
  - CLI example (Linux):

    ```
    iwlist wlan0 scanning | grep -i signal
    ```

  - GUI example: WiFi Analyzer apps for Android, or Ekahau/Acrylic WiFi on PC.

ESS and Roaming

- **Extended Service Set (ESS):** A group of interconnected APs sharing the same SSID and credentials.
- **Benefit:** Supports seamless roaming between APs.
- **Roaming Trigger Thresholds:**
  - macOS: -75 dBm
  - iOS: -70 dBm

Exam Note: Seamless roaming is a byproduct of ESS, not a separate feature.

WiFi MIMO & Channel Bonding

MIMO Types

- **SU-MIMO (Single User):**
  - Increases throughput using multiple antennas.
  - Only one client communicates at a time.
- **MU-MIMO (Multi-User):**
  - Introduced in 802.11ac Wave 2.
  - Uses **beamforming** to allow multiple clients to transmit/receive simultaneously.

Channel Bonding

- **Definition:** Combines two 20 MHz channels into a 40 MHz channel to increase throughput.
- **Pros:** ~38–85% speed increase.
- **Cons:** Reduces available channels.
- **Notes:**
  - Not recommended for 2.4 GHz due to overlap.
  - In 5 GHz, channels do not overlap.

Wi-Fi Security

MAC Filtering (Not Recommended)

- **Definition:** Allowing/denying specific MAC addresses at the WLAN level.
- **Weakness:** Easily bypassed via MAC spoofing.

Wi-Fi Security Protocols

Protocol	Authentication	Encryption	Transition Mode	KRACK Resilience	Offline Dictionary Attack Resilience
WPA2 Personal	PSK	AES-CCMP	No	No	No
WPA2 Enterprise	802.1X (RADIUS)	AES-CCMP	No	No	Yes (if EAP-TLS used)
WPA3-OWE (Enhanced Open)	None (Opportunistic)	AES-CCMP	Yes	Yes	Yes
WPA3-SAE (Personal)	SAE	AES-CCMP	Yes	Yes	Yes
WPA3 Enterprise (AES-CCMP)	802.1X (RADIUS)	AES-CCMP	Yes	Yes	Yes
WPA3 Enterprise (GCMP-256)	802.1X (RADIUS)	GCMP-256	No	Yes	Yes

Key Definitions

- **AES** – Advanced Encryption Standard, a symmetric block cipher widely used to secure data transmissions.
- **AES-CCMP** – Counter Mode with Cipher Block Chaining Message Authentication Code Protocol; ensures confidentiality and data integrity in WPA2 and WPA3.
- **OWE** – Opportunistic Wireless Encryption; an open authentication method that encrypts data without requiring a pre-shared key.
- **GCMP-256** – Galois/Counter Mode Protocol with a 256-bit key, providing stronger encryption and authentication than AES-CCMP.
- **SAE** – Simultaneous Authentication of Equals; a secure password-based authentication protocol used in WPA3-Personal to protect against offline dictionary attacks and improve handshake security.

Exam Note: Transition Mode

- **Transition Mode** allows an access point to support **both WPA2 and WPA3 simultaneously**, easing the migration to WPA3 while maintaining compatibility with older devices.
- **Security tradeoff:** Transition Mode may lower overall security because attackers might force connections over WPA2 instead of WPA3.
- **WPA3 Enterprise (GCMP-256)** does **not support Transition Mode** since it is designed for high-security environments requiring strict compliance (e.g., FIPS 140-3).

802.1X Authentication - LAN and WLAN NAC

Enterprise Mode Authentication

- **Enterprise Mode** uses **802.1X authentication** combined with **EAP-TLS** and **RADIUS** servers.
- **EAP-TLS** (Extensible Authentication Protocol - Transport Layer Security) uses **digital certificates** (X.509 PKI certificates) for mutual authentication between client and server, providing strong security.

Evil Twin WLANs

- **Evil Twin** is a type of **rogue access point attack** where an attacker sets up a Wi-Fi access point mimicking a legitimate AP’s SSID and settings to trick users into connecting.
- Once connected, the attacker can intercept data, steal credentials, or launch man-in-the-middle attacks.

Disassociation Attacks

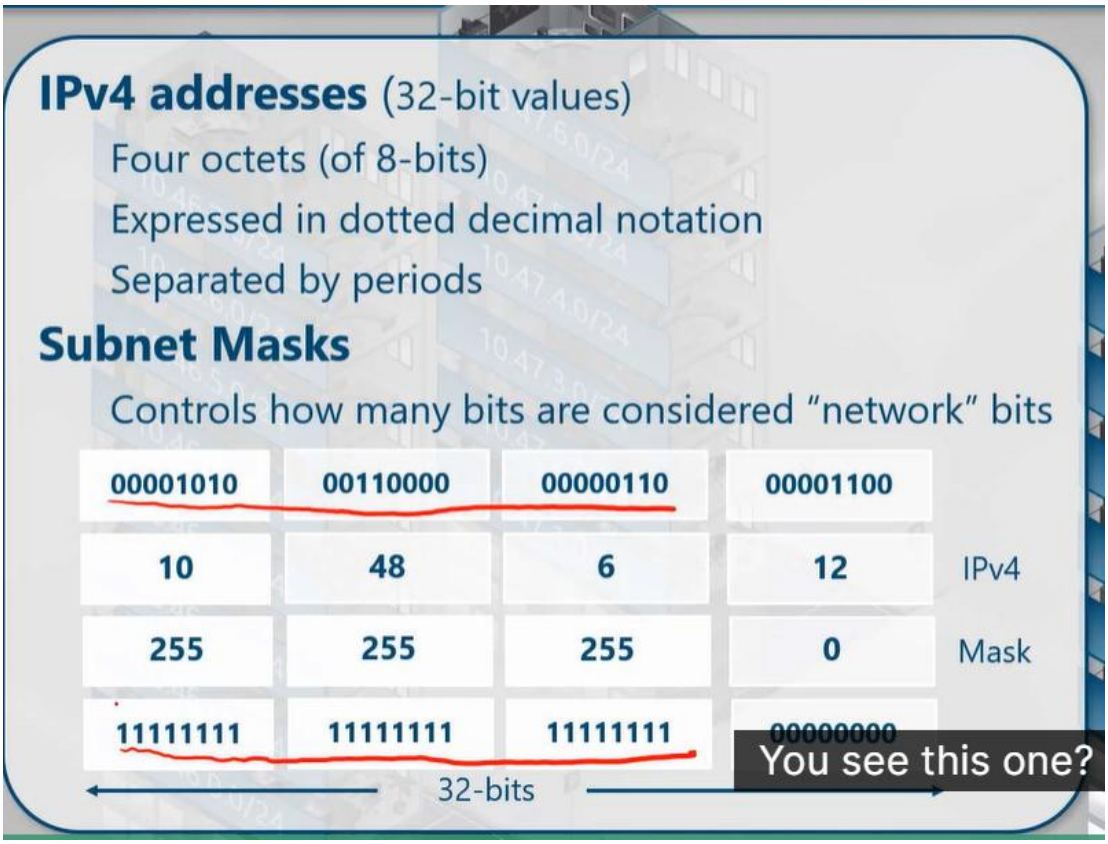
- A **Disassociation Attack** involves an attacker sending forged disassociation frames to clients or access points, forcing clients to disconnect from the legitimate Wi-Fi network.
- This causes denial of service, forcing users to reconnect or potentially connect to a rogue AP.

Network+ CompTIA (N10-009) Day 4

Chapter 6: IP Masks and Subnetting

IP Subnet Masks

- A **Subnet Mask** is a 32-bit number used to divide an IP address into **network** and **host** portions.
- It determines which part of the IP address identifies the network and which part identifies the host.
- Written in **dotted decimal** notation (e.g., 255.255.255.0).



Prefix Notation	Decimal Notation	Binary Notation	Host Bits = h	Hosts Per Subnet 2^h-2
/8	255.0.0.0	11111111.00000000.00000000.00000000	24	16777214
/9	255.128.0.0	11111111.10000000.00000000.00000000	23	8388606
/10	255.192.0.0	11111111.11000000.00000000.00000000	22	4194302
/11	255.224.0.0	11111111.11100000.00000000.00000000	21	2097150
/12	255.240.0.0	11111111.11110000.00000000.00000000	20	1048574
/13	255.248.0.0	11111111.11111000.00000000.00000000	19	524286
/14	255.252.0.0	11111111.11111100.00000000.00000000	18	262142
/15	255.254.0.0	11111111.11111110.00000000.00000000	17	131070
/16	255.255.0.0	11111111.11111111.00000000.00000000	16	65534
/17	255.255.128.0	11111111.11111111.10000000.00000000	15	32766
/18	255.255.192.0	11111111.11111111.11000000.00000000	14	16382
/19	255.255.224.0	11111111.11111111.11100000.00000000	13	8190
/20	255.255.240.0	11111111.11111111.11110000.00000000	12	4094
/21	255.255.248.0	11111111.11111111.11111000.00000000	11	2046
/22	255.255.252.0	11111111.11111111.11111100.00000000	10	1022
/23	255.255.254.0	11111111.11111111.11111110.00000000	9	510
/24	255.255.255.0	11111111.11111111.11111111.00000000	8	254
/25	255.255.255.128	11111111.11111111.11111111.10000000	7	126
/26	255.255.255.192	11111111.11111111.11111111.11000000	6	62
/27	255.255.255.224	11111111.11111111.11111111.11100000	5	30
/28	255.255.255.240	11111111.11111111.11111111.11110000	4	14
/29	255.255.255.248	11111111.11111111.11111111.11111000	3	6
/30	255.255.255.252	11111111.11111111.11111111.11111100	2	2
/31	255.255.255.254	11111111.11111111.11111111.11111110	1	2 (RFC 3021)
/32	255.255.255.255	11111111.11111111.11111111.11111111	0	1

How Many Devices Can We Have in Each Subnet?

To determine the number of usable hosts in a subnet, use the following formula:

Hosts per subnet = 2^h – 2

- Where **h** = number of bits allocated for hosts (number of zeros in the subnet mask's binary form).
- For example, in a **/24 subnet mask** (255.255.255.0), the host bits are:
  32 (total bits) – 24 (network bits) = 8 host bits
- So, usable hosts = 2^8 – 2 = 254

Why Subtract 2?

- The **first address** in the subnet is reserved as the **network address** (all host bits are 0).
- The **last address** is reserved as the **directed broadcast address** (all host bits are 1).
- These two addresses cannot be assigned to hosts.

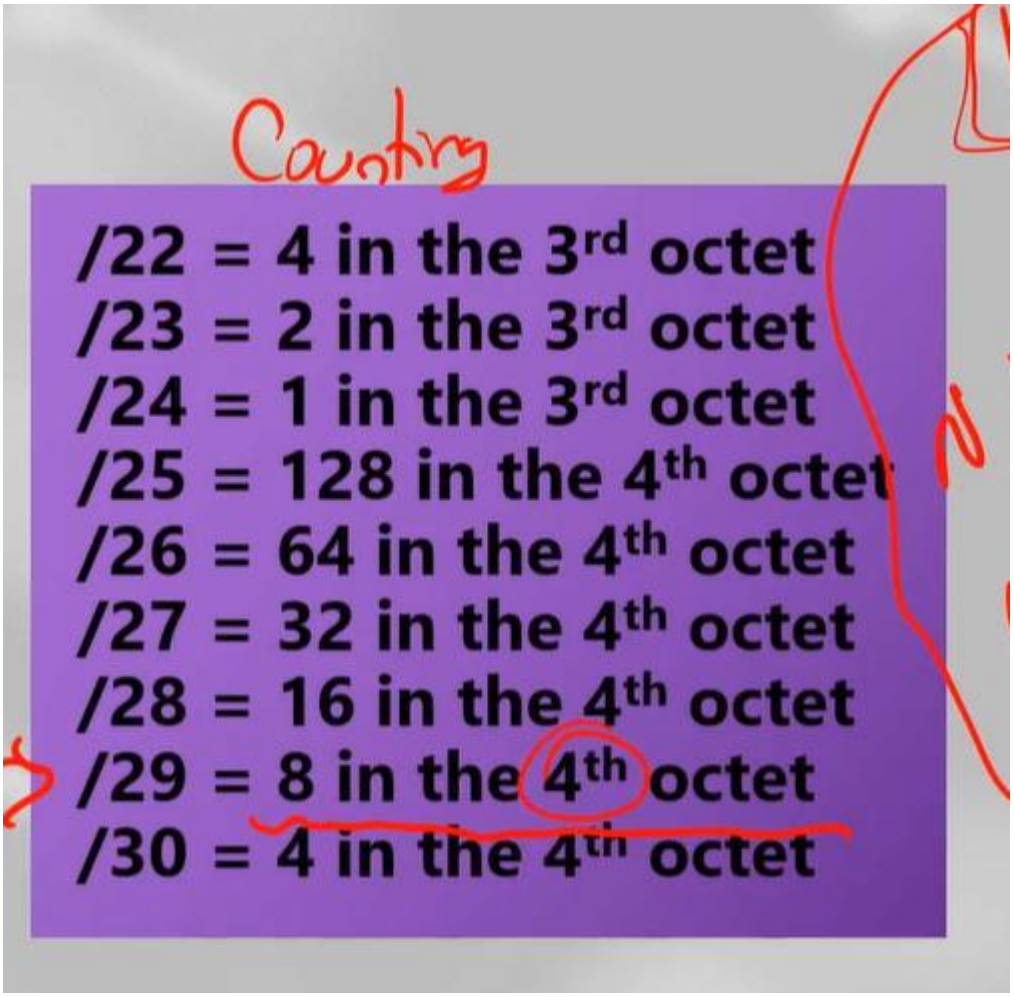
Exam Note:

- The best subnet to use for **point-to-point links** between routers is **/30** (255.255.255.252), which provides exactly 2 usable host addresses.

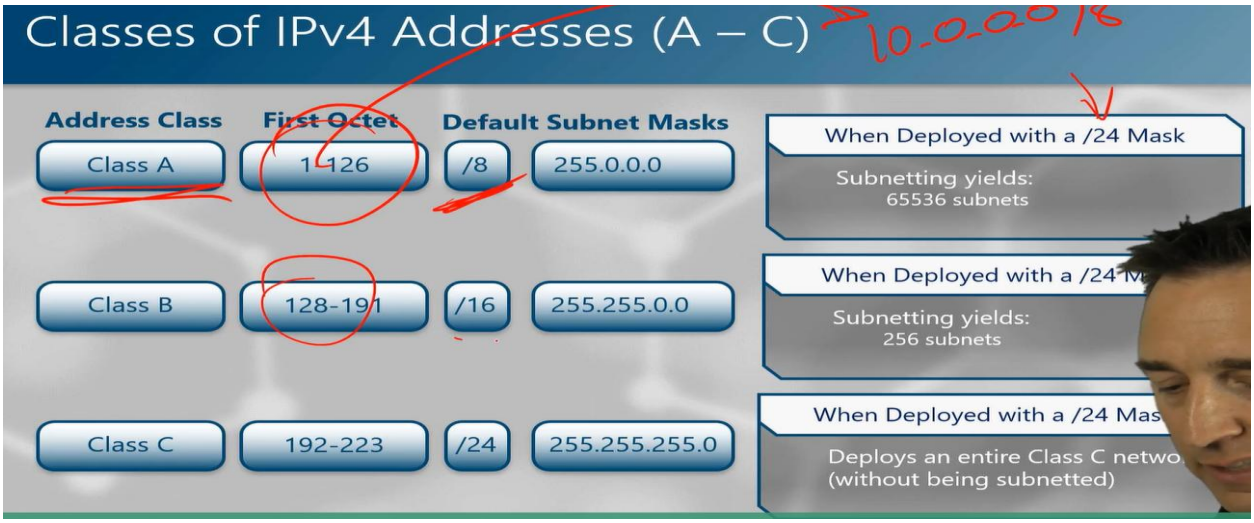
Addressing a VLAN with SVIs

- **SVI (Switched Virtual Interface)**: A virtual interface on a Layer 3 switch that allows the switch to route traffic for a VLAN.
- SVIs provide Layer 3 processing (routing) for all devices in a VLAN.
- SVIs are assigned IP addresses that act as the default gateway for hosts in the VLAN.

Determining Network ID



Subnet Created Calculations



Formula for Number of Subnets Created

Number of subnets = 2^n

- **n** = Number of bits borrowed from the host portion to create subnet bits

---

Example: Class C Network

- Default Class C subnet mask: 255.255.255.0 (/24)
- Host bits originally: 8 (last octet)
- Suppose you borrow **3 bits** from the host portion to create subnets.
- New subnet mask becomes: 255.255.255.224 (/27)
    - Because 3 bits borrowed → 11100000 in the last octet → 224 in decimal
- Calculate number of subnets:
    - 2^3 = **8 subnets**
- Number of hosts per subnet:
    - Remaining host bits: 8 – 3 = 5
    - Hosts = 2^5 – 2 = 30 usable hosts per subnet

Summary

- Borrowing bits reduces hosts per subnet but increases number of subnets.
- Always subtract 2 from hosts to account for network and broadcast addresses.