

CompTIA Network+ Exam N10-008

Lesson 15



Deploying and Troubleshooting Wireless Networks

Objectives

- Summarize wireless standards
- Install wireless networks
- Troubleshoot wireless networks
- Configure and troubleshoot wireless security

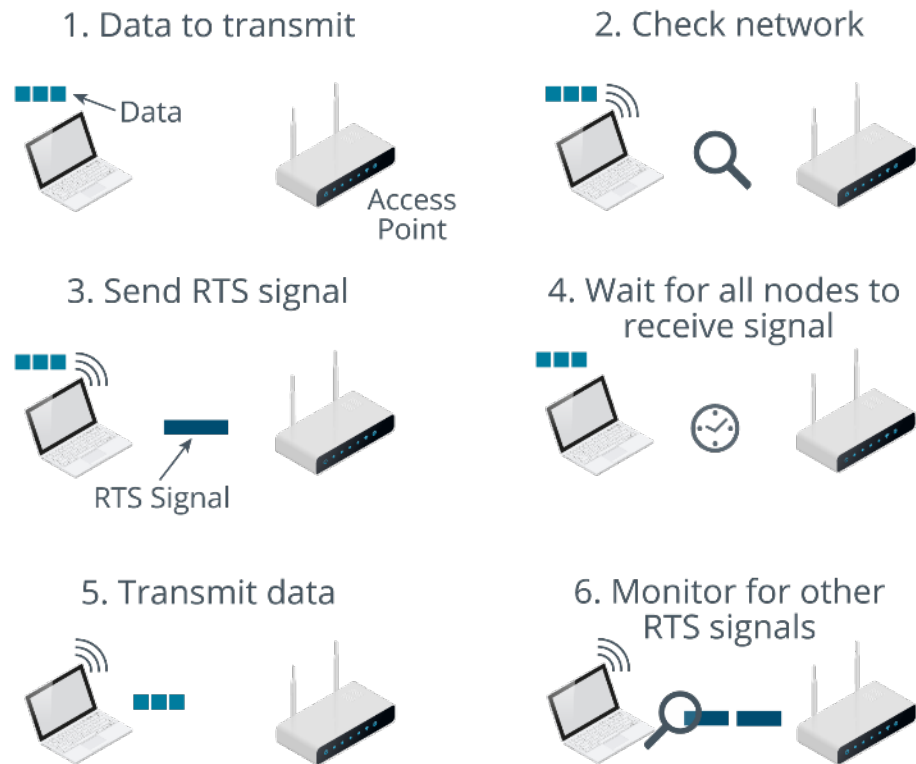
Lesson 15

Topic 15A

Summarize Wireless Standards

IEEE 802.11 Wireless Standards

- Wi-Fi modulation and carrier methods
- Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
 - Ack undamaged frames
 - Request to Send/Clear to Send
- Original data rate just 1 Mbps

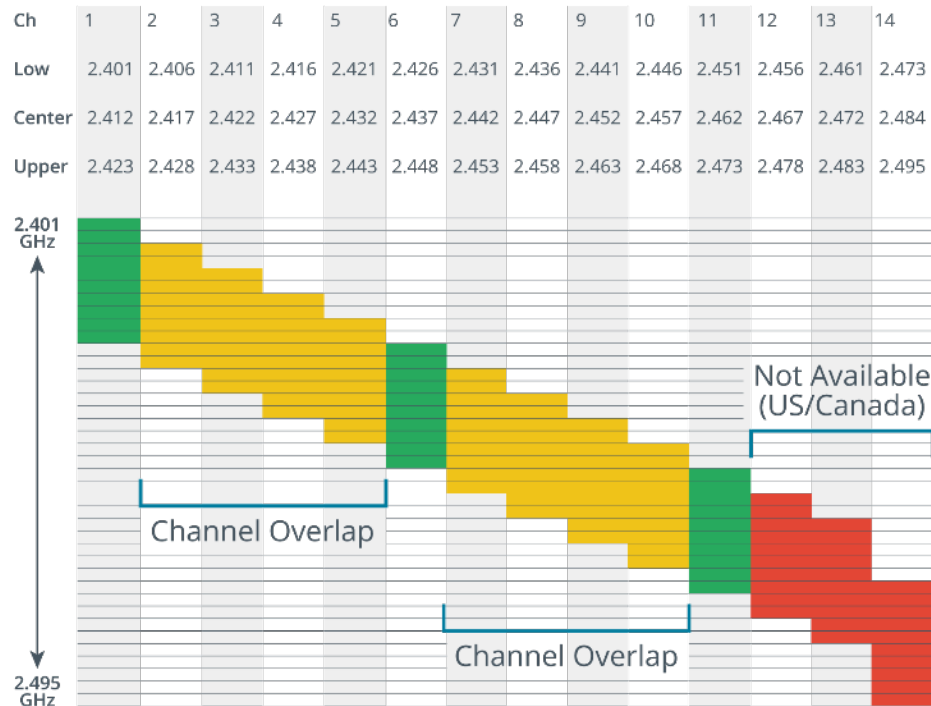


IEEE 802.11a and 5 GHz Channel Bandwidth

- 2.4 GHz
 - Better propagation, but fewer channels and greater interference risk
- 5 GHz
 - Lower range, but less congested
- IEEE 802.11a (54 Mbps)
 - Orthogonal Frequency Division Multiplexing (OFDM)
 - 23 x non-overlapping 20 Mhz channels
 - Dynamic Frequency Selection (DFS) and regulatory impacts

IEEE 802.11b/g and 2.4 GHz Channel Bandwidth

2.4 GHz Wi-Fi Frequencies (in GHz)



- IEEE 802.11b (11 Mbps)
 - Direct Sequence Spread Spectrum (DSSS), along with Complementary Code Keying (CCK) signal encoding
 - 14 x 5 MHz channels
 - Wi-Fi still needs 20 MHz channel bandwidth
 - Channels require careful configuration to avoid overlap
- IEEE 802.11g (54 Mbps)
 - OFDM
 - 802.11b compatibility mode

IEEE 802.11n, MIMO, and Channel Bonding

- Single User Multiple Input Multiple Output (SU-MIMO)
 - AxB:C transmit and receive antennas plus maximum simultaneous streams
 - Spatial multiplexing and spatial diversity
- Can use 5 GHz or 2.4 GHz bands with channel bonding
- High Throughput (HT)/greenfield
 - 288.8 Mbps for a single channel and 600 Mbps for bonded channels
 - HT mixed mode for compatibility with older standards
- Wi-Fi 4

	U-NII-1	U-NII-2	U-NII-2 Extended	U-NII-3
20 MHz	36 40 44 48	52 56 60 64	100 104 108 112 116 120 124 128 132 136 140	149 153 157 161
40 MHz	38 46	54 62	102 110 118 126 134	151 159
80 MHz	42	58	106 122	155
160 MHz	50		114	

Dynamic Frequency Selection (DFS) Range

Wi-Fi 5 and Wi-Fi 6

- Wi-Fi 5 (802.11ac)
 - 5 GHz only
 - 80 or 160 MHz channel bonding
 - Up to 8 spatial streams
- Wi-Fi 6 (802.11ax)
 - High Efficiency (HE)
 - 2.4 GHz or 5 GHz (plus new 6 GHz band)
 - Enhancements to support Internet of Things (IoT) devices
 - OFDM with multiple access (OFDMA)
 - Not so much throughput, but reduced latency

Multiuser MIMO

- Beamforming
- Downlink MU-MIMO (DL MU-MIMO)
 - Separate signals by alignment
 - Up to 4 in Wi-Fi 5 and up to 8 in Wi-Fi 6
- Uplink MU-MIMO (UL MU-MIMO)

2G and 3G Cellular Technologies

- 2G cellular radio
 - Global System for Mobile Communication (GSM)
 - Initially used Time Division Multiple Access (TDMA)
 - Subscriber Identity Module (SIM) allows number portability between handsets
 - Code Division Multiple Access (CDMA)/IS-95
 - Circuit Switched Data (CSD)
- 3G packet radio for cellular networks
 - General Packet Radio Services/Enhanced Data Rates for GSM Evolution (GPRS/EDGE) for 2.5G on GSM
 - Universal Mobile Telecommunications System (UMTS)/Evolved High Speed Packet Access (HSPA+) for 3G on GSM networks (now using a form of CDMA)
 - CDMA2000 Evolution Data Optimized (EV-DO) for 3G on CDMA networks

4G and 5G Cellular Technologies

- Long Term Evolution (LTE) for 4G
 - Convergence between the GSM and “CDMA” camps – uses Orthogonal Frequency Division Multiple Access (OFDMA)
 - 150 Mbps downlink (nominally)
 - 20 Mbps more typical of actual conditions
- Long Term Evolution (Advanced) (LTE-A)
 - 300 Mbps downlink (nominally)
 - 90 Mbps more typical of actual conditions
- 5G
 - Aims for 1 Gbps but achieves 50 – 300 Mbps
 - Uses hundreds of small antennas in different frequency bands, unlike with current wireless cells
 - Fixed-wireless broadband solutions

Review Activity: Wireless Standards

- IEEE 802.11 Wireless Standards
- IEEE 802.11a and 5 GHz Channel Bandwidth
- IEEE 802.11b/g and 2.4 GHz Channel Bandwidth
- IEEE 802.11n, MIMO, and Channel Bonding
- Wi-Fi 5 and Wi-Fi 6
- Multiuser MIMO
- 2G and 3G Cellular Technologies
- 4G and 5G Cellular Technologies

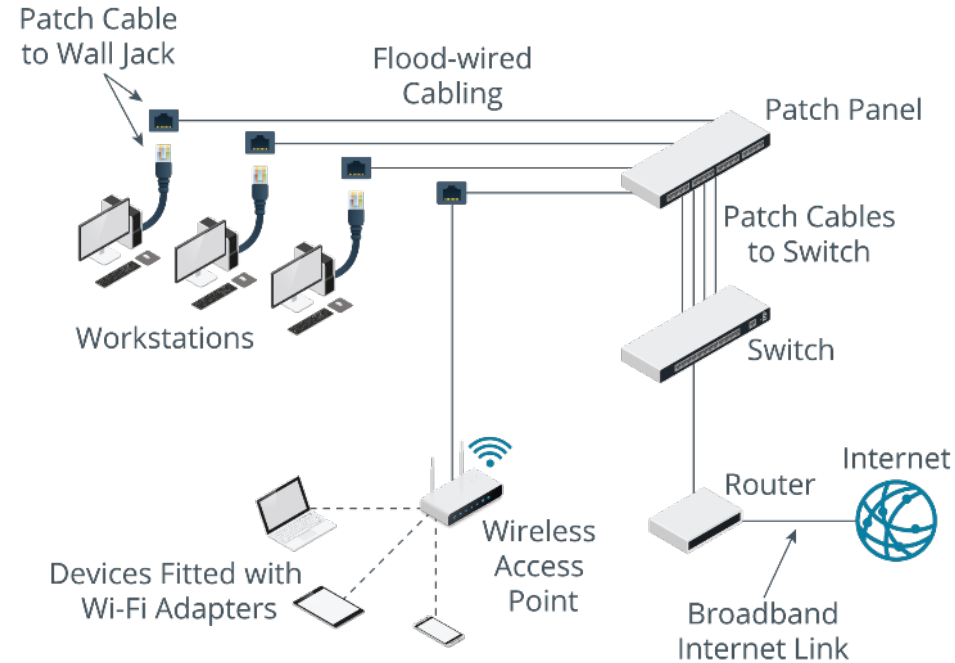
Lesson 15

Topic 15B

Install Wireless Networks

Infrastructure Topology and Wireless Access Points

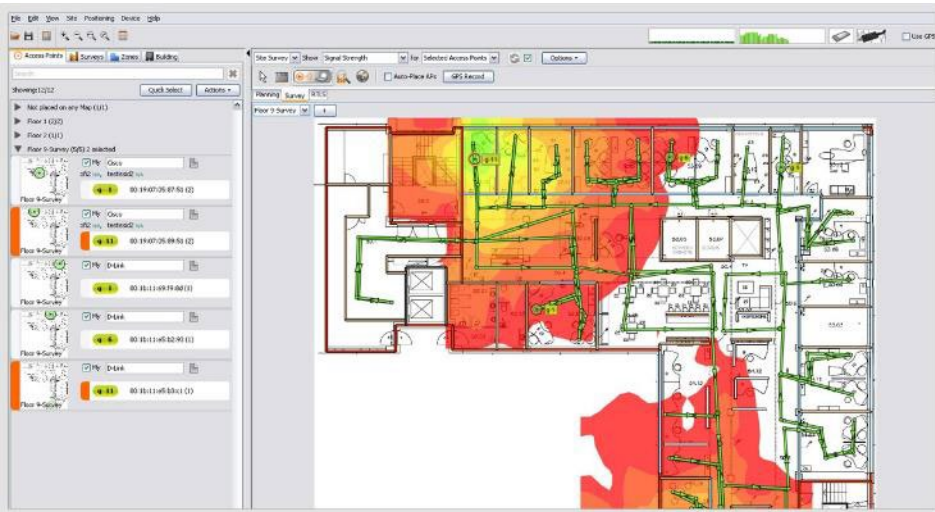
- Access point (AP)
 - Bridges wireless stations (STA) and cabled network
- Basic Service Set (BSS)
 - MAC address of AP is used as Basic Service Set Identifier (BSSID)
 - More than one BSS can be grouped together in Extended Service Set (ESS)



Wireless Site Design

- Service Set Identifier (SSID)
 - Multiple BSSs with the same SSID form an extended service set (ESS)
- SSID broadcast and beacon frame
- Speed and distance requirements
 - Maximum indoor and outdoor ranges
 - Dynamic Rate Switching/Selection (DRS)
 - Built environment obstructions
 - Radio source interference
 - Competing wireless networks
 - Other devices/standards

Site Surveys and Heat Maps



- Inspect floor plan and rooms to identify obstructions
- Plan cells to provide good coverage of the area
 - Device density
 - Bandwidth per device (uplink/downlink)
- Use wireless survey tools to identify signal strength and channel utilization (heat map)

Wireless Roaming and Bridging

- Extended service area (ESA)
 - Distribution System (DS) where wired network connects access points via switches
 - Access points use different channels to avoid interference
 - Access points all use the same SSID (Extended SSID/ESSID) and security configuration
- Disassociation/reassociation
- Wireless Distribution System (WDS)
 - Repeater mode
- Wireless bridges

Wireless LAN Controllers

- Manage tens or hundreds of access points
- Appliance or software solution
- Access point governed by controller is “thin” or “lightweight”
- Lightweight Access Point Protocol (LWAPP)
- VLAN pooling
- Power over Ethernet

Ad Hoc and Mesh Topologies

- Ad hoc
 - Peer-to-peer or Independent Basic Service Set (IBSS)
- Mesh
 - Self-forming network with path discovery and routing

Review Activity: Wireless Network Installation

- Infrastructure Topology and Wireless Access Points
- Wireless Site Design
- Site Surveys and Heat Maps
- Wireless Roaming and Bridging
- Wireless LAN Controllers
- Ad Hoc and Mesh Topologies

Lesson 15

Topic 15C

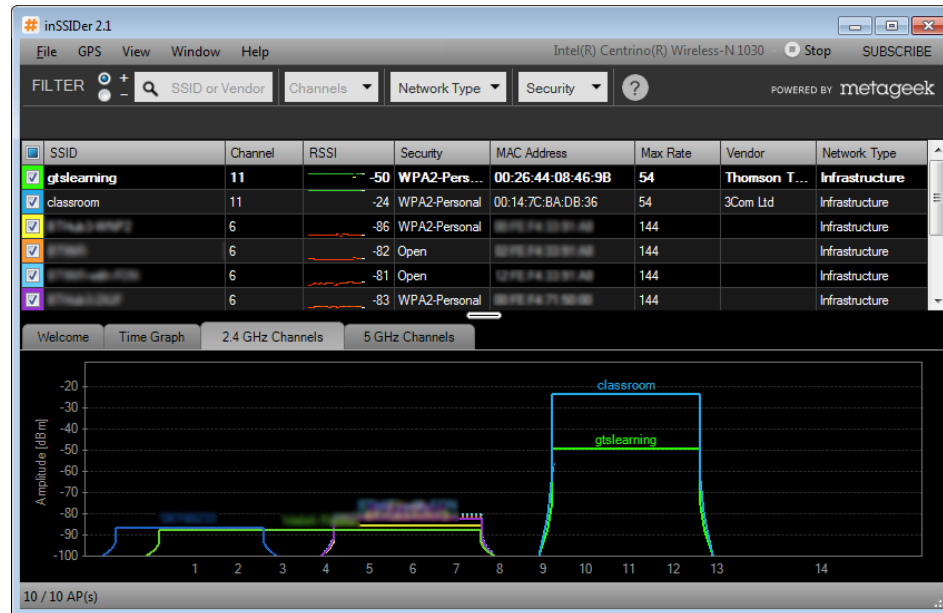
Troubleshoot Wireless Networks

Wireless Performance Assessment

- Specifications and limitations
- Speed versus throughput
- Distance
 - Radio frequency (RF) attenuation or free space path loss
 - Doubling distance quadruples signal loss
 - dBm measures signal strength as ratio to 1 milliwatt (mw)
 - $1 \text{ mw} = 0 \text{ dBm}$
 - Negative dBm represents fractional mw values

Signal Strength

- Received Signal Strength Indicator (RSSI)
 - Up to -65 dBm is a good signal
 - 80 dBm is at the limit
- Signal-to-noise ratio (SNR)
- Wi-Fi analyzers



Antenna Types



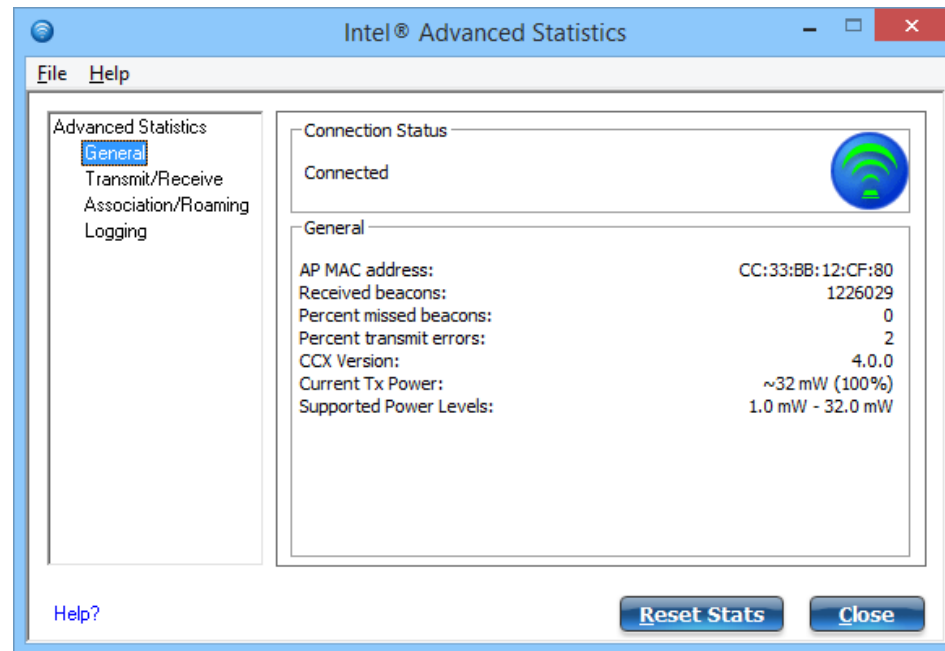
- Omnidirectional
 - Same signal in all directions - torus (donut) shape
- Unidirectional (Yagi and parabolic)
 - Signal can be focused in one direction to increase signal strength
 - Gain measured in dBi (decibel isotropic) units
 - Beamwidth
- Polarization

Insufficient Wireless Coverage Issues

- Insufficient wireless coverage
 - Add access point
 - Configure wireless bridge
- Antenna placement
- Antenna cable attenuation
- Effective isotropic radiated power (EIRP)
 - $\text{Transmit Power} + \text{Cable Loss} + \text{Antenna Gain}$
 - Maximum transmit power and regulatory limitations
 - Client must be able to transmit back

Channel Utilization and Overlap Issues

- Co-channel interference (CCI)
- Adjacent channel interference (ACI)
- Channel layout
- Transmit power and site survey
- Overlap for roaming
 - Access point association time



Overcapacity Issues

- High number of stations overwhelming access point
- Manage client density
- Analyze associations through controller

Interference Issues

- Reflection/bounce
- Refraction
- Absorption/environmental factors
- Electromagnetic interference (EMI)
 - Spectrum analyzers

Review Activity: Wireless Network Troubleshooting

- Wireless Performance Assessment
- Signal Strength
- Antenna Types
- Insufficient Wireless Coverage Issues
- Channel Utilization and Overlap Issues
- Overcapacity Issues
- Interference Issues

Lesson 15

Topic 15D

Configure and Troubleshoot Wireless Security

Wi-Fi Encryption Standards

- Cryptographic protocols and authentication mechanism
- Wi-Fi Protected Access (WPA)
 - Based on RC4 cipher from Wired Equivalent Privacy (WEP)
 - Adds Temporal Key Integrity Protocol (TKIP)
 - Both WEP and WPAv1 are too weak to use safely
- WPA2
 - Uses strong Advanced Encryption Standard (AES) cipher
 - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)
- WPA3

Personalize settings for each band or enable Smart Connect to configure the same settings for all bands.

OFDMA: ☒ Enable ?

Smart Connect: ☐ Enable ?

2.4GHz: ☒ Enable [Sharing Network](#)

Network Name (SSID): ☐ Hide SSID

Security:

Version:

Encryption:

Password:

Transmit Power:

Channel Width:

Channel:

Mode:

5GHz: ☒ Enable [Sharing Network](#)

Network Name (SSID): ☐ Hide SSID

Security:

Version:

Password:

Transmit Power:

Channel Width:

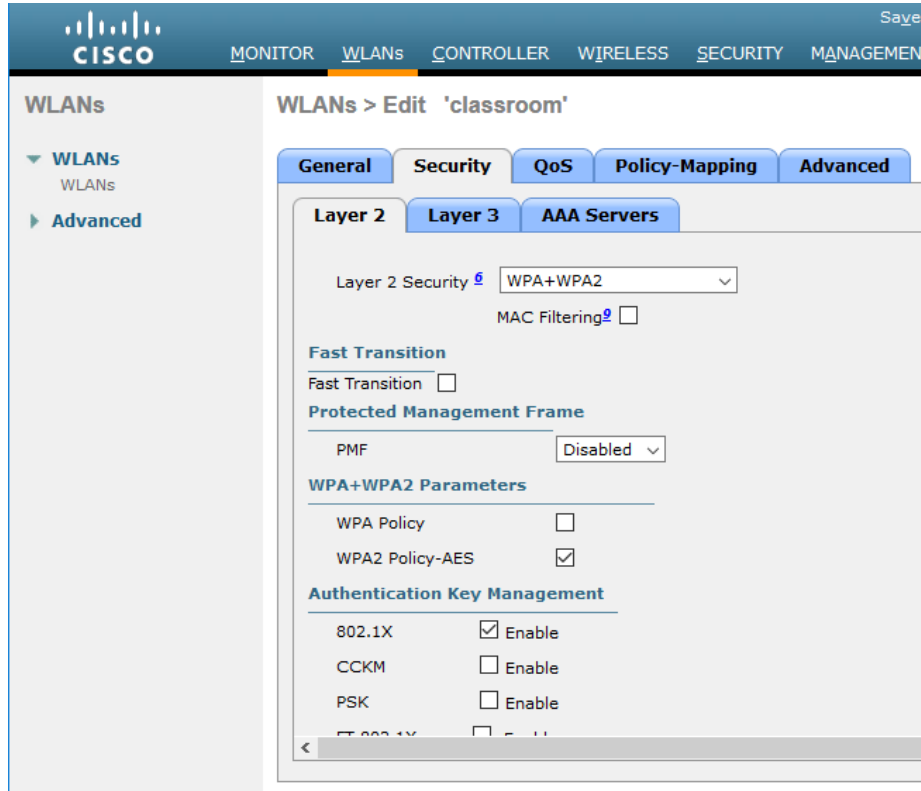
Channel:

Mode:

Personal Authentication

- WPA2 Pre-Shared Key Authentication
 - Group authentication
 - All stations configured with same passphrase
 - Passphrase used to generate master encryption key
 - 4-way handshake generates session keys
- WPA3 Personal Authentication
 - Still based on group passphrase
 - Key generation improved by Password Authenticated Key Exchange (PAKE)
 - Simultaneous Authentication of Equals (SAE) generates session keys

Enterprise/IEEE 802.1X Authentication



- Uses Extensible Authentication Protocol (EAP) to authenticate to a network server
- IEEE 802.1X allows only EAP over Wireless (EAPoW) until station is authenticated
- User's network credential is used to generate session keys

Wi-Fi Security Configuration Issues

- Wrong SSID and incorrect passphrase issues
 - Incorrect manual configuration of SSID
 - Selecting wrong SSID
- Encryption protocol mismatch issues
 - Check client support for WPA version

Client Disassociation Issues

- Disassociation and deauthentication
 - AP or station can initiate
 - Station might be roaming
- Malicious attacks
 - Spoof frames to disconnect station from WLAN
 - Try to force new connection to rogue AP
 - Sniff authentication process

Open Authentication and Captive Portal Issues

- Access point configured with no security
- No encryption
- Secondary authentication mechanisms
 - Captive portal
- Connection security
 - Use SSL/TSL-protected services (HTTPS and secure email)
 - Use a secured VPN

Review Activity: Wireless Security

- Wi-Fi Encryption Standards
- Personal Authentication
- Enterprise/IEEE 802.1X Authentication
- Wi-Fi Security Configuration Issues
- Client Disassociation Issues
- Open Authentication and Captive Portal Issues

CompTIA Network+ Exam N10-008

Lesson 15



Summary