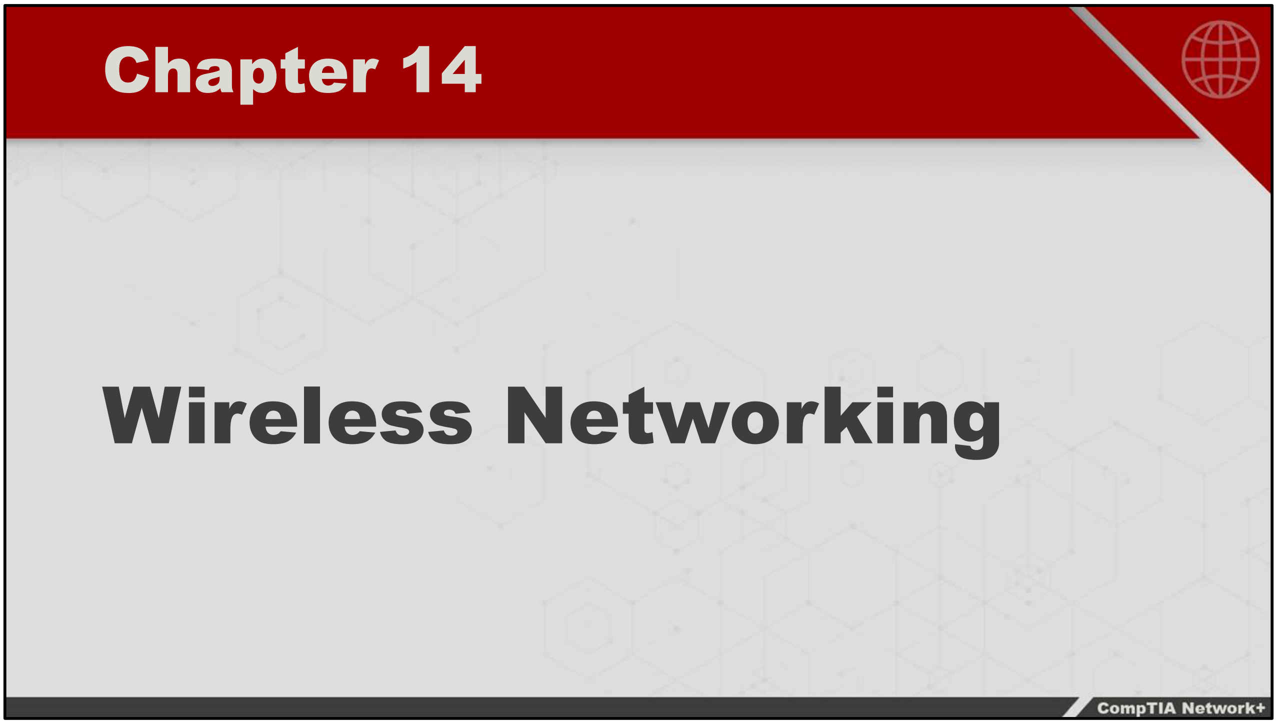
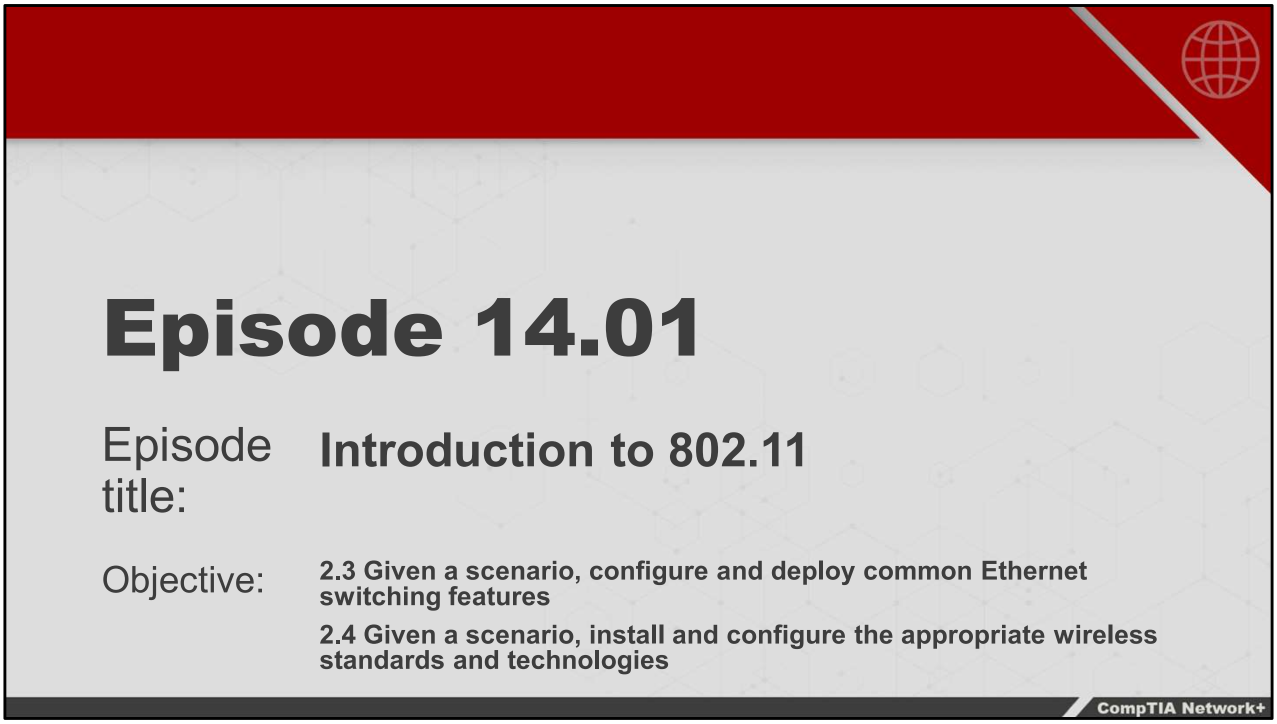


Chapter 14

Wireless Networking



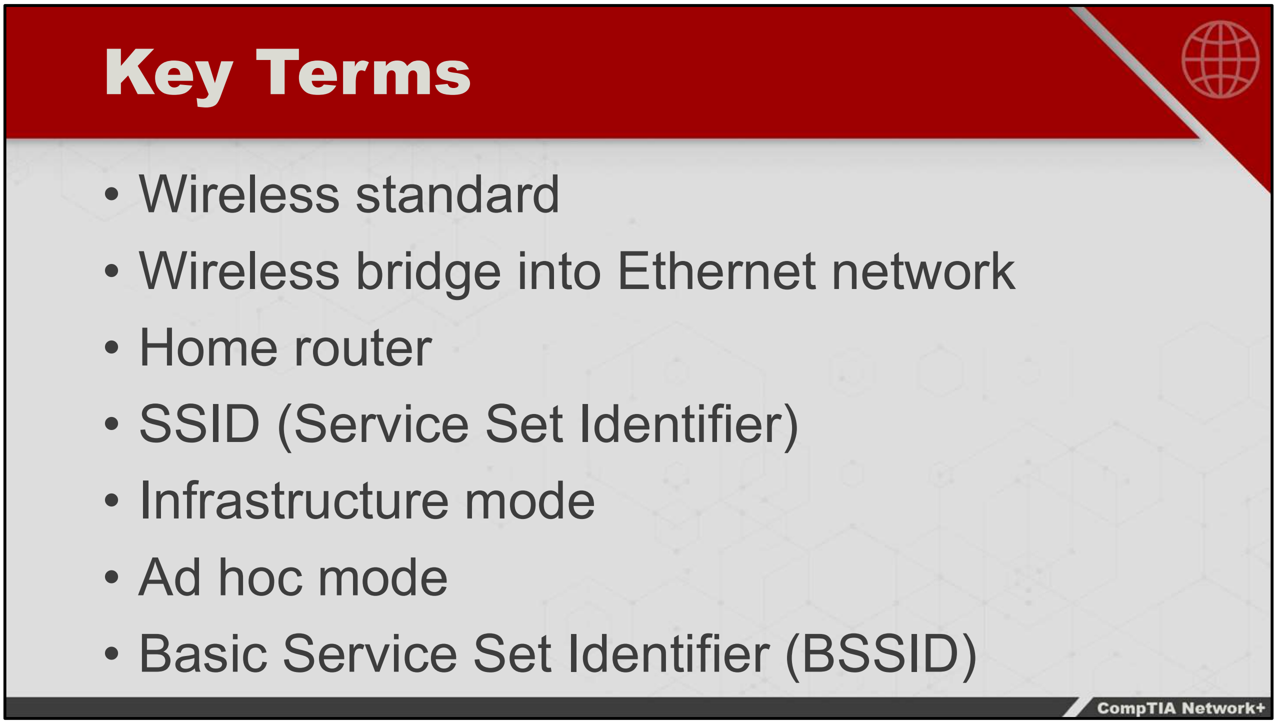
Episode 14.01

Episode title: **Introduction to 802.11**

Objective: **2.3 Given a scenario, configure and deploy common Ethernet switching features**

2.4 Given a scenario, install and configure the appropriate wireless standards and technologies

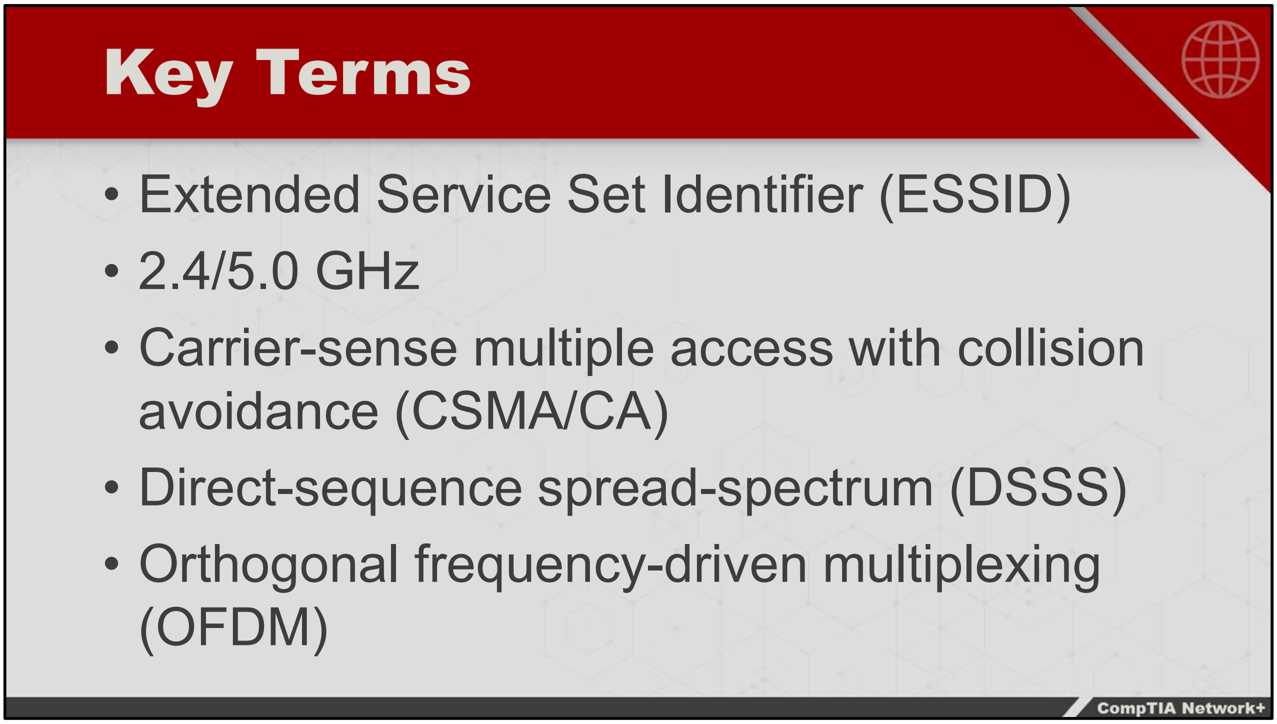
CompTIA Network+



Key Terms

- Wireless standard
- Wireless bridge into Ethernet network
- Home router
- SSID (Service Set Identifier)
- Infrastructure mode
- Ad hoc mode
- Basic Service Set Identifier (BSSID)

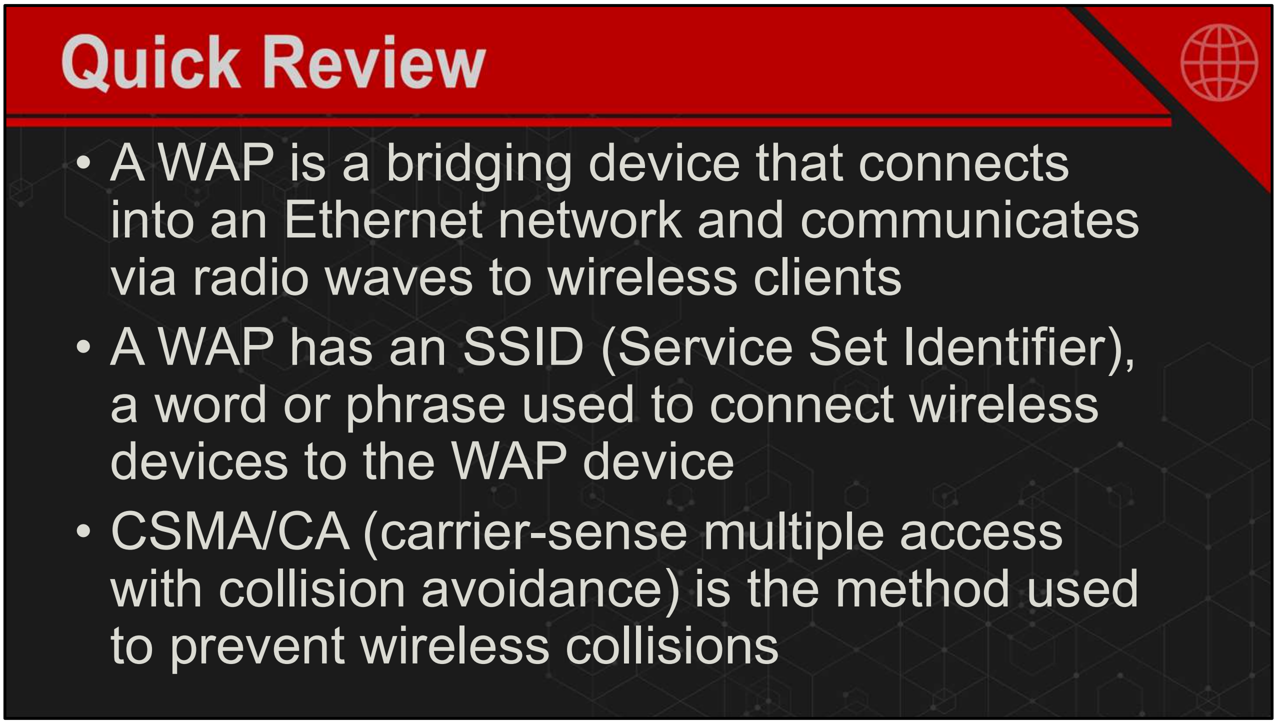
CompTIA Network+



Key Terms

- Extended Service Set Identifier (ESSID)
- 2.4/5.0 GHz
- Carrier-sense multiple access with collision avoidance (CSMA/CA)
- Direct-sequence spread-spectrum (DSSS)
- Orthogonal frequency-driven multiplexing (OFDM)

CompTIA Network+



Quick Review

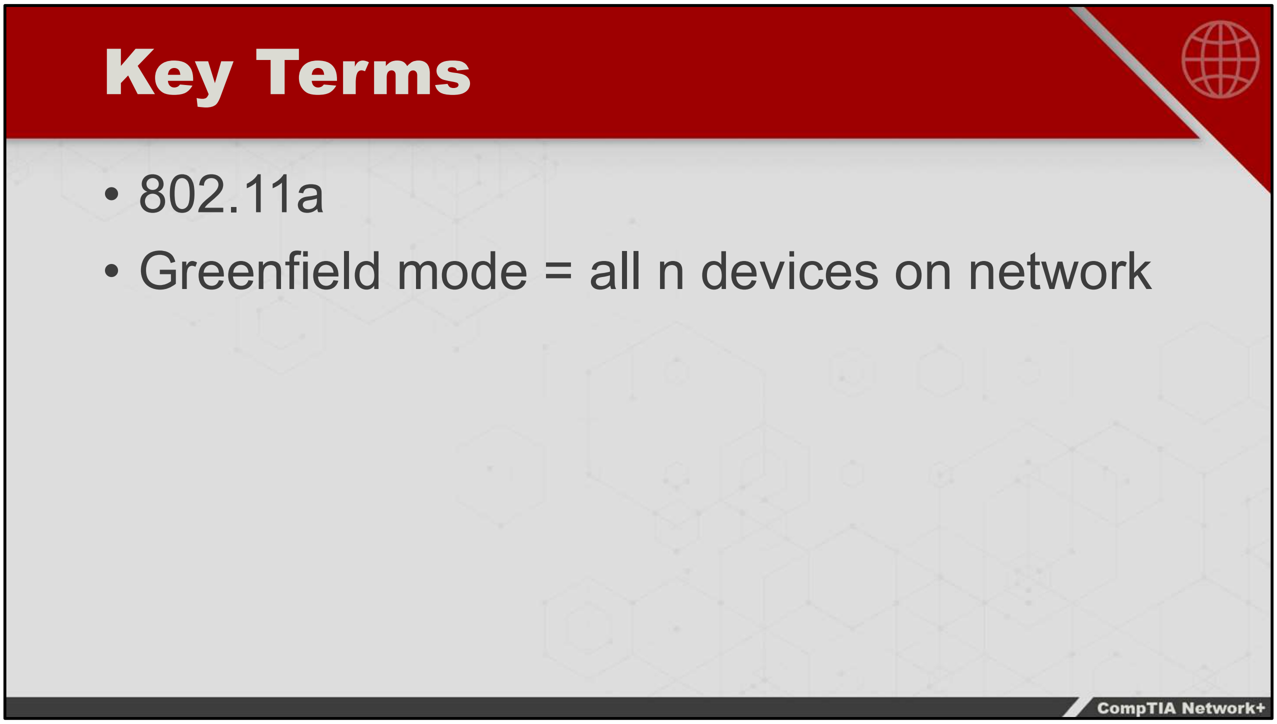
- A WAP is a bridging device that connects into an Ethernet network and communicates via radio waves to wireless clients
- A WAP has an SSID (Service Set Identifier), a word or phrase used to connect wireless devices to the WAP device
- CSMA/CA (carrier-sense multiple access with collision avoidance) is the method used to prevent wireless collisions

Episode 14.02

Episode title: **802.11 Standards**

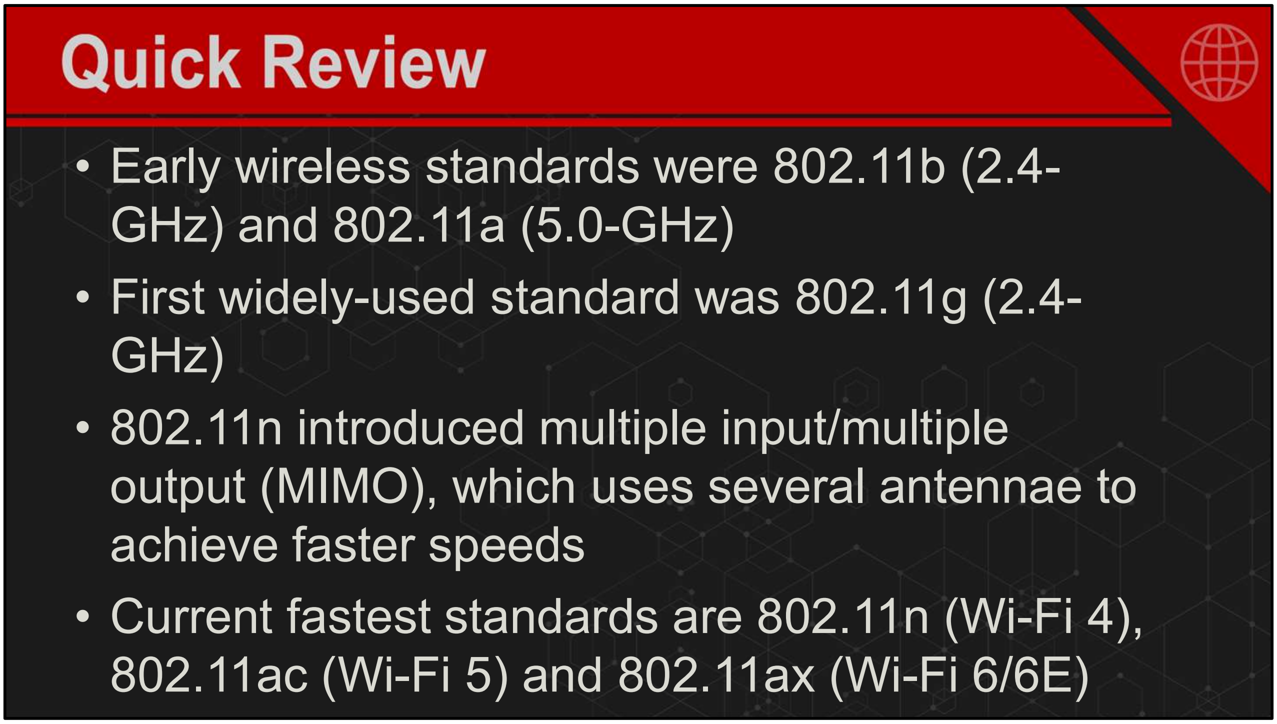
Objective: **2.4 Given a scenario, install and configure the appropriate wireless standards and technologies**

CompTIA Network+



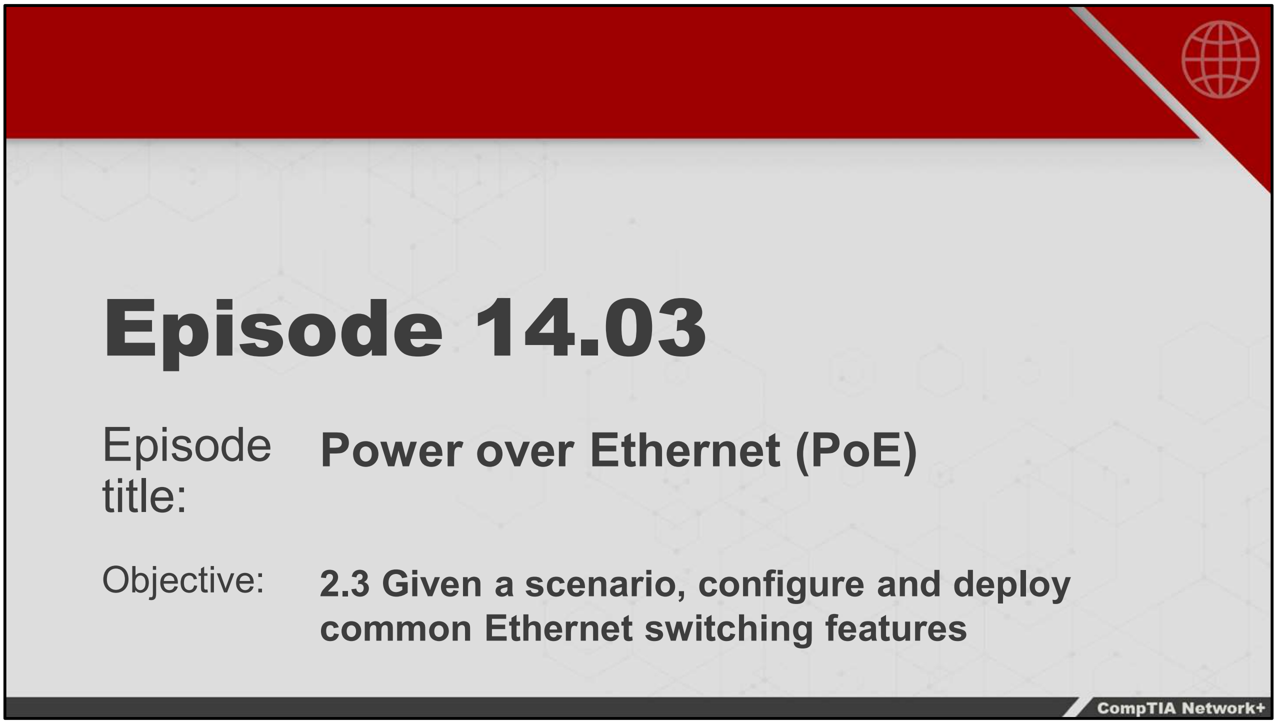
Key Terms

- 802.11a
- Greenfield mode = all n devices on network



Quick Review

- Early wireless standards were 802.11b (2.4-GHz) and 802.11a (5.0-GHz)
- First widely-used standard was 802.11g (2.4-GHz)
- 802.11n introduced multiple input/multiple output (MIMO), which uses several antennae to achieve faster speeds
- Current fastest standards are 802.11n (Wi-Fi 4), 802.11ac (Wi-Fi 5) and 802.11ax (Wi-Fi 6/6E)

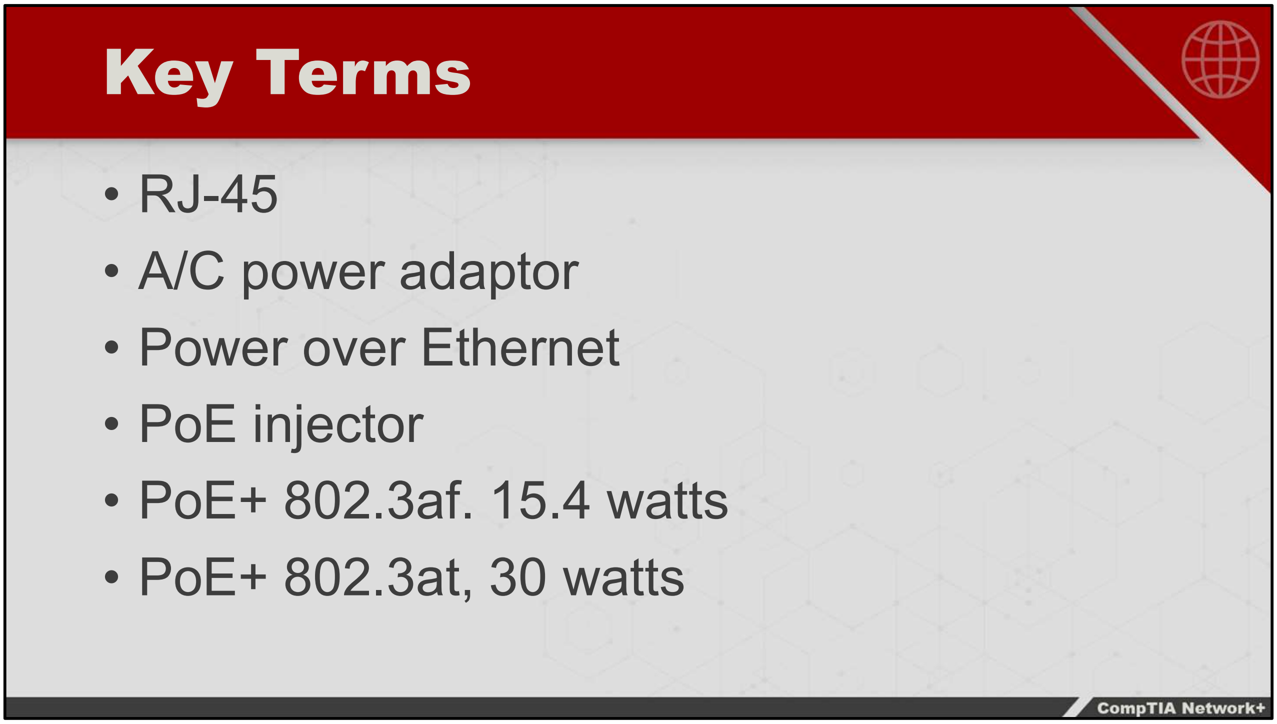


Episode 14.03

Episode title: **Power over Ethernet (PoE)**

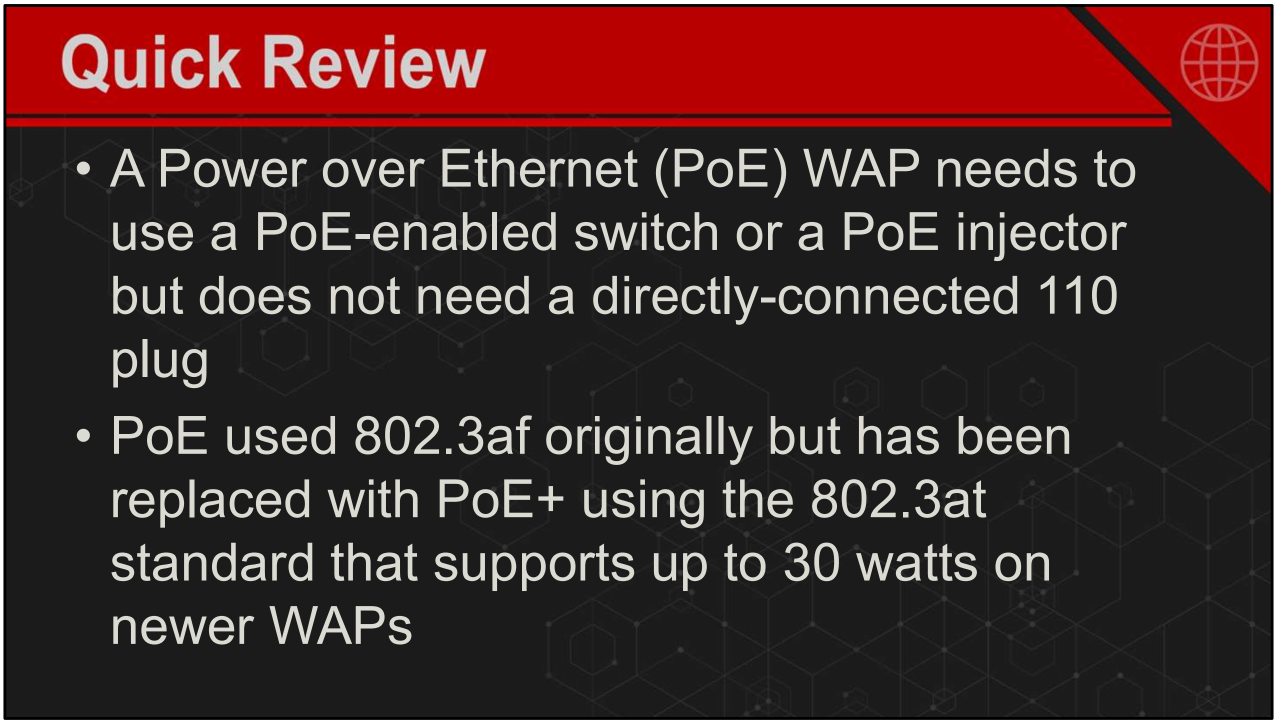
Objective: **2.3 Given a scenario, configure and deploy common Ethernet switching features**

CompTIA Network+



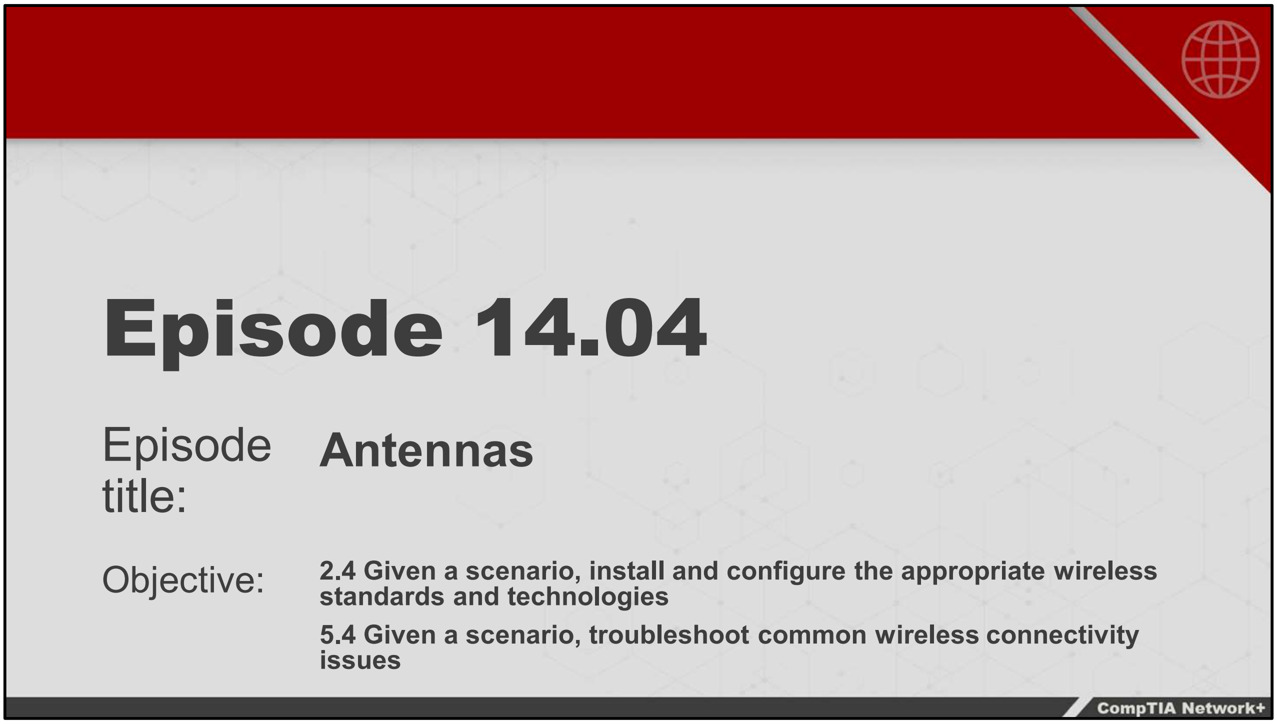
Key Terms

- RJ-45
- A/C power adaptor
- Power over Ethernet
- PoE injector
- PoE+ 802.3af. 15.4 watts
- PoE+ 802.3at, 30 watts



Quick Review

- A Power over Ethernet (PoE) WAP needs to use a PoE-enabled switch or a PoE injector but does not need a directly-connected 110 plug
- PoE used 802.3af originally but has been replaced with PoE+ using the 802.3at standard that supports up to 30 watts on newer WAPs



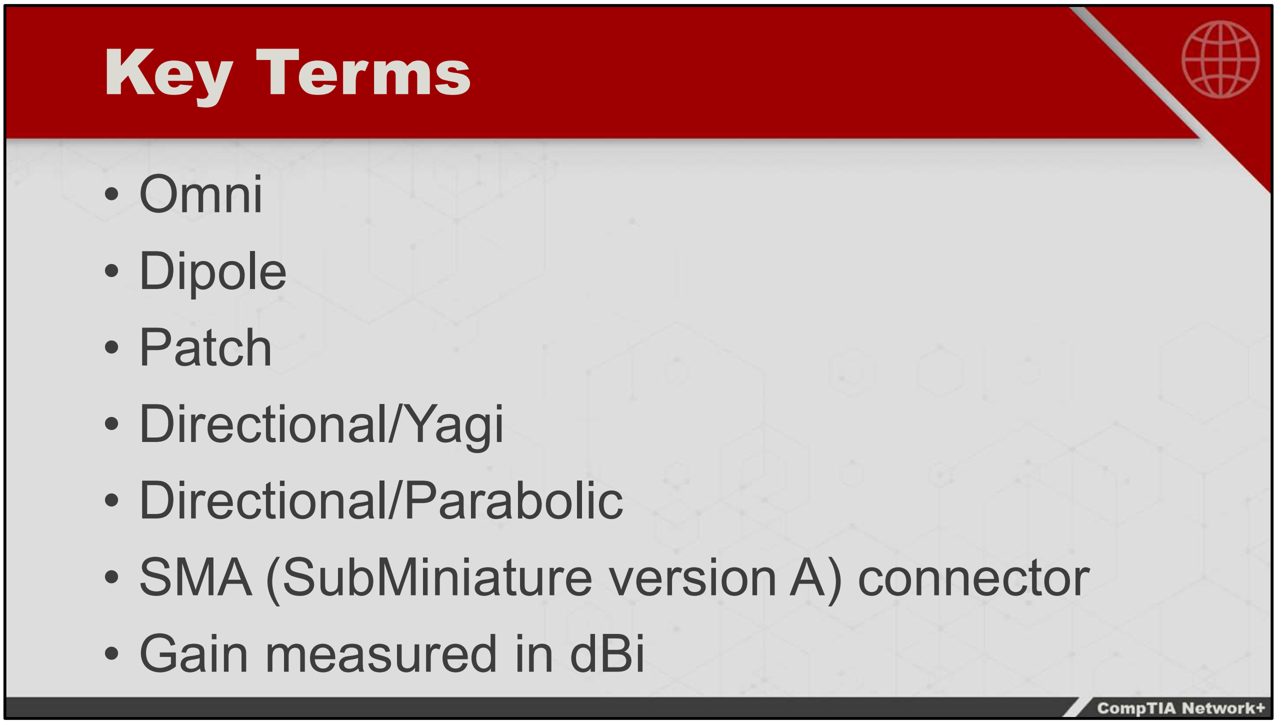
Episode 14.04

Episode title: **Antennas**

Objective: **2.4 Given a scenario, install and configure the appropriate wireless standards and technologies**

5.4 Given a scenario, troubleshoot common wireless connectivity issues

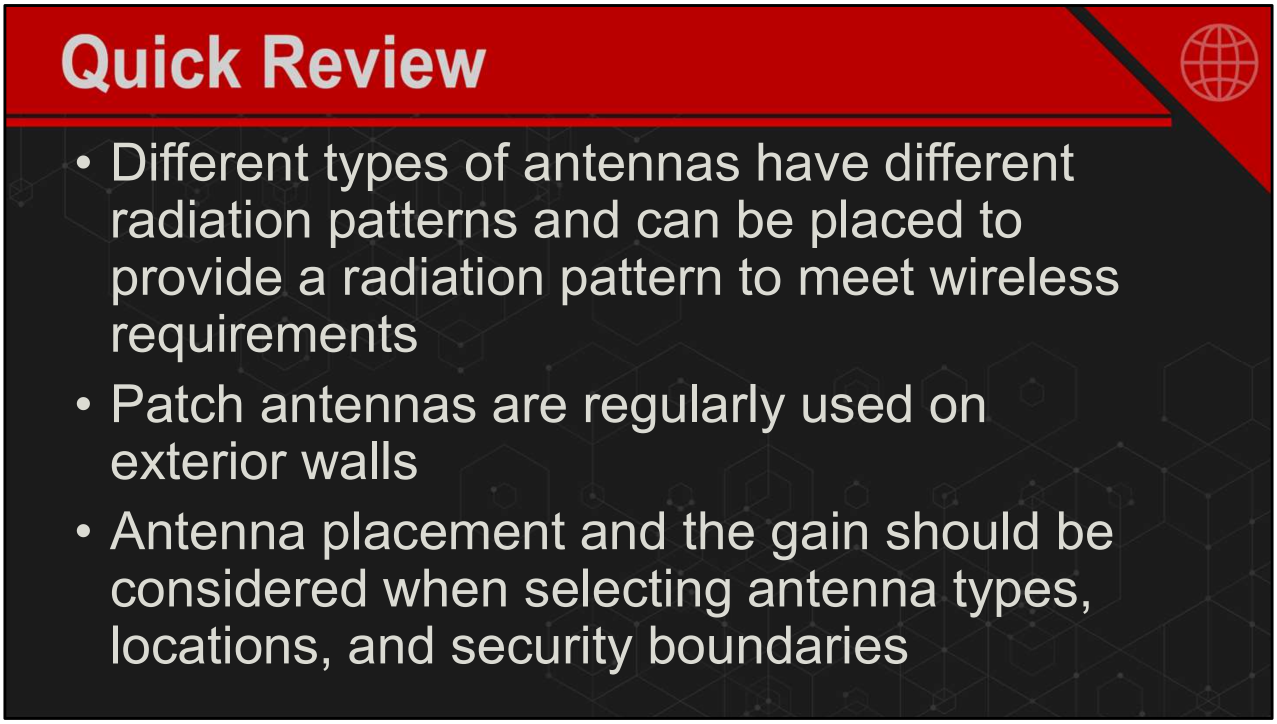
CompTIA Network+



Key Terms

- Omni
- Dipole
- Patch
- Directional/Yagi
- Directional/Parabolic
- SMA (SubMiniature version A) connector
- Gain measured in dBi

CompTIA Network+



Quick Review

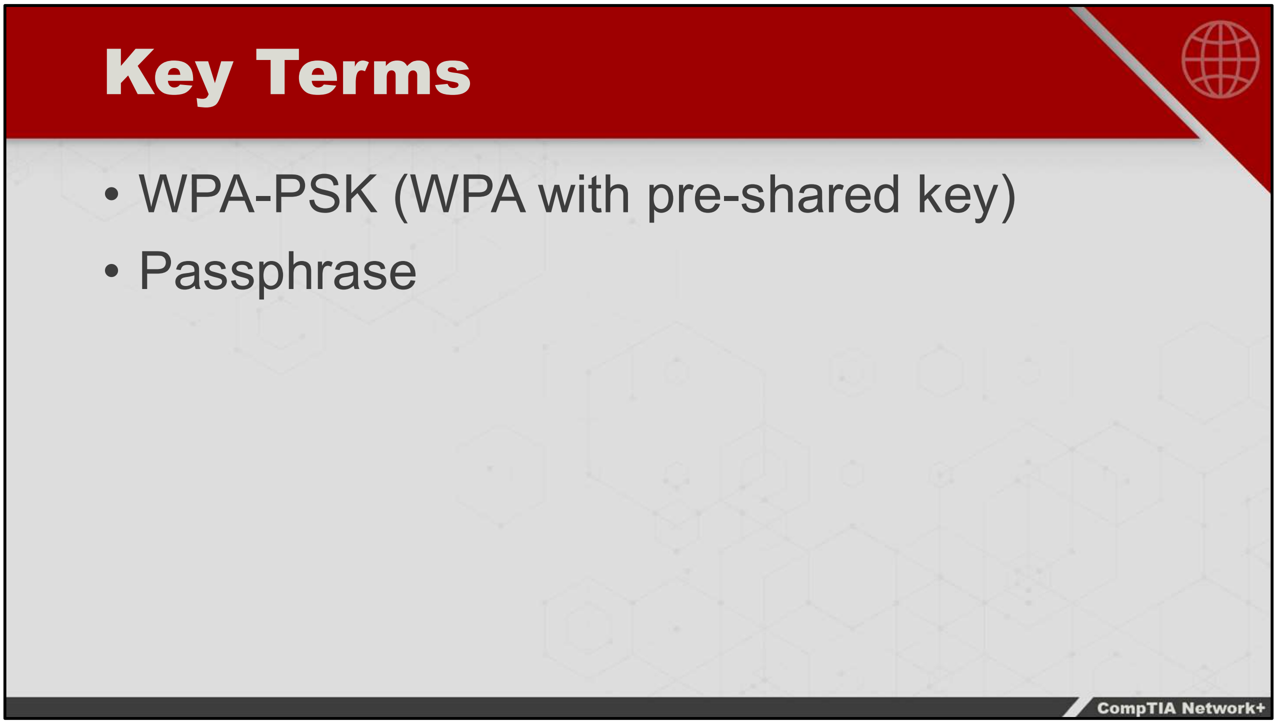
- Different types of antennas have different radiation patterns and can be placed to provide a radiation pattern to meet wireless requirements
- Patch antennas are regularly used on exterior walls
- Antenna placement and the gain should be considered when selecting antenna types, locations, and security boundaries

Episode 14.05

Episode title: **Wireless Security Standards**

Objective: **2.4 Given a scenario, install and configure the appropriate wireless standards and technologies**

CompTIA Network+

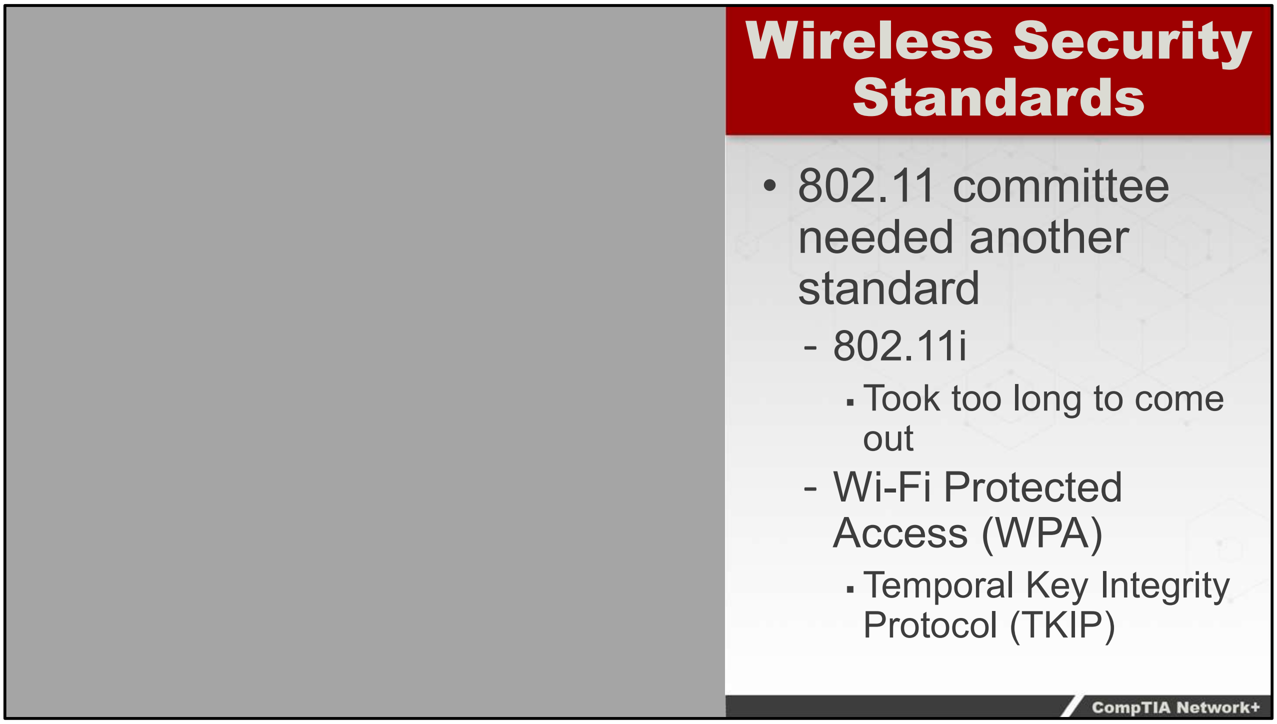


Key Terms

- WPA-PSK (WPA with pre-shared key)
- Passphrase

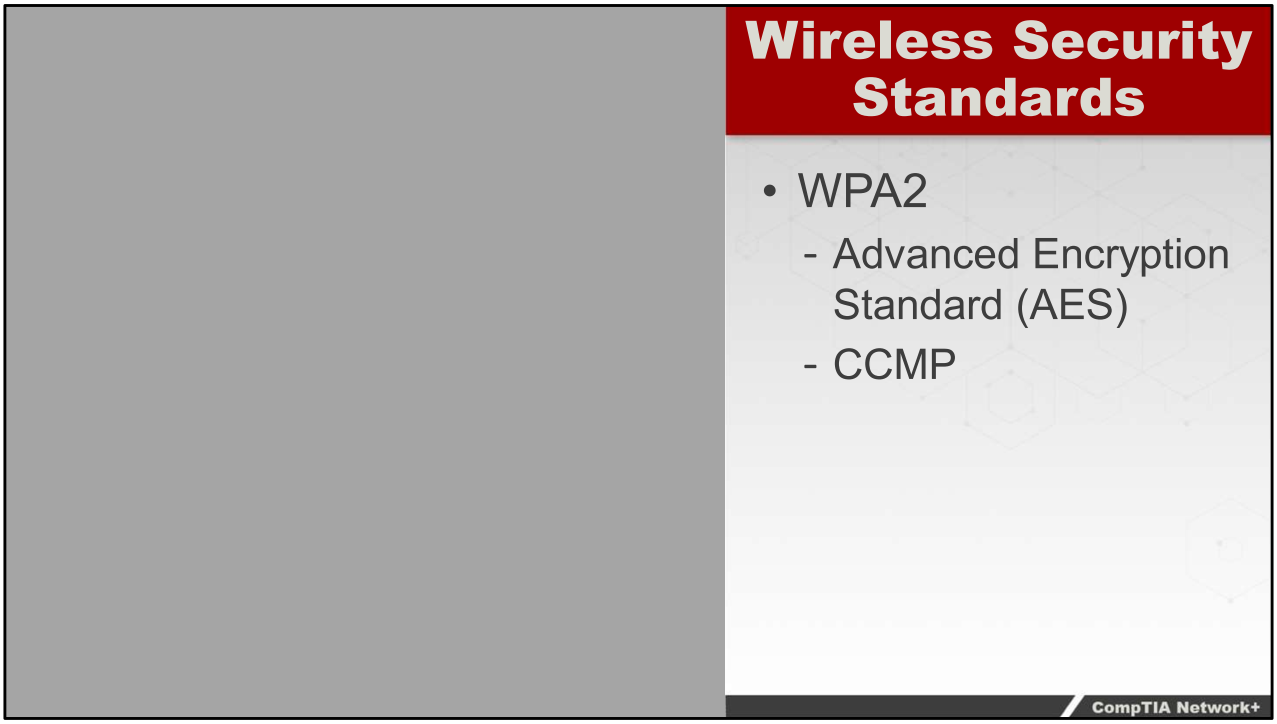
Wireless Security Standards

- Wired Equivalent Privacy (WEP)
  - Used 64- and 128-bit keys
  - Crackable



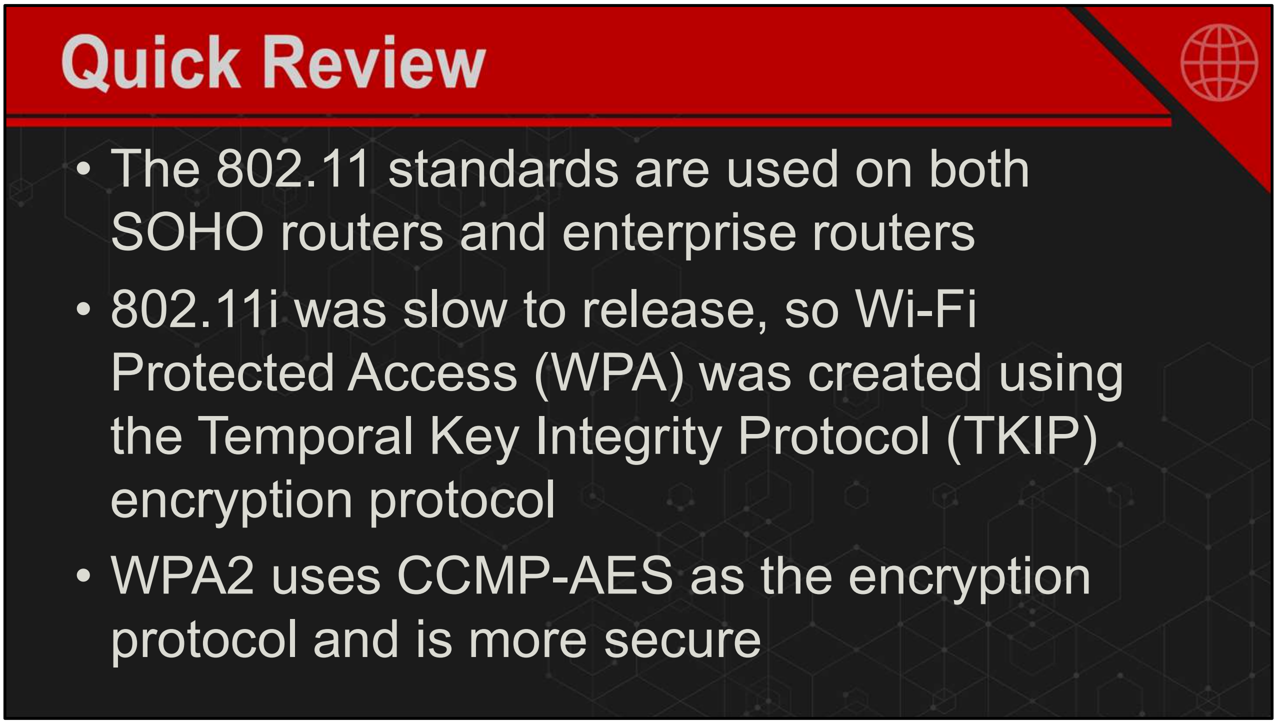
Wireless Security Standards

- 802.11 committee needed another standard
  - 802.11i
    - Took too long to come out
  - Wi-Fi Protected Access (WPA)
    - Temporal Key Integrity Protocol (TKIP)



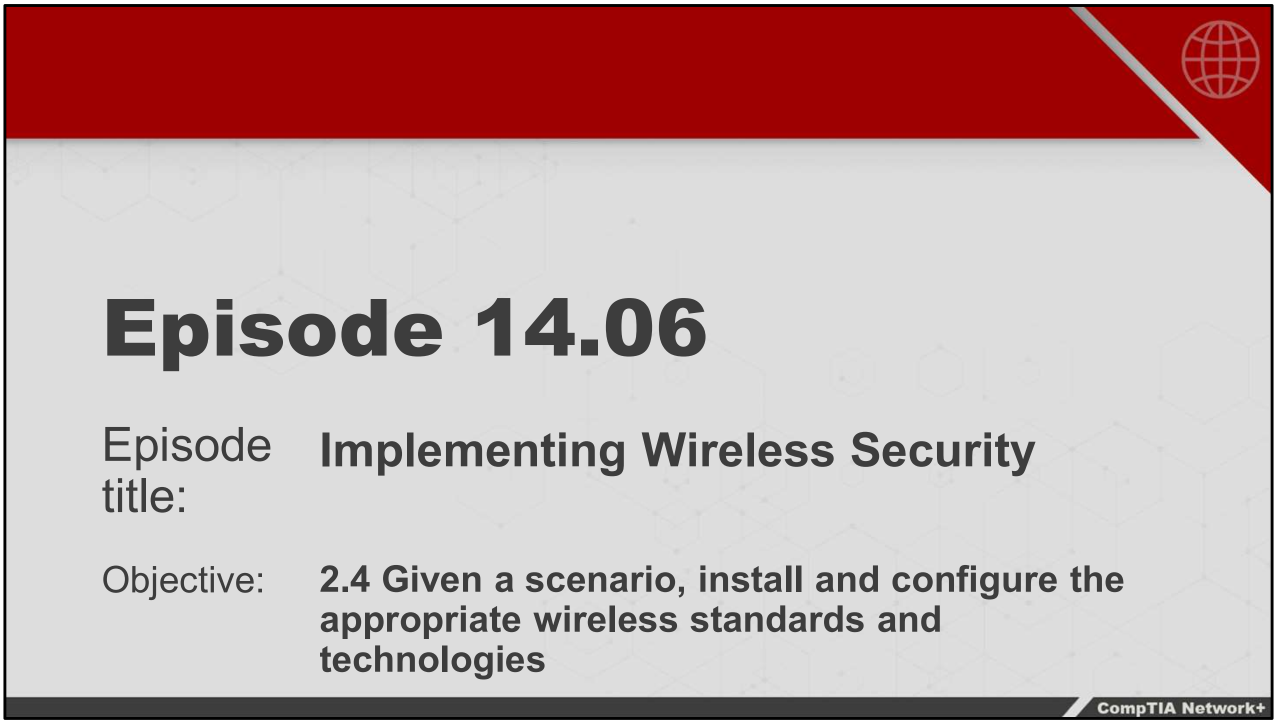
Wireless Security Standards

- WPA2
  - Advanced Encryption Standard (AES)
  - CCMP



Quick Review

- The 802.11 standards are used on both SOHO routers and enterprise routers
- 802.11i was slow to release, so Wi-Fi Protected Access (WPA) was created using the Temporal Key Integrity Protocol (TKIP) encryption protocol
- WPA2 uses CCMP-AES as the encryption protocol and is more secure

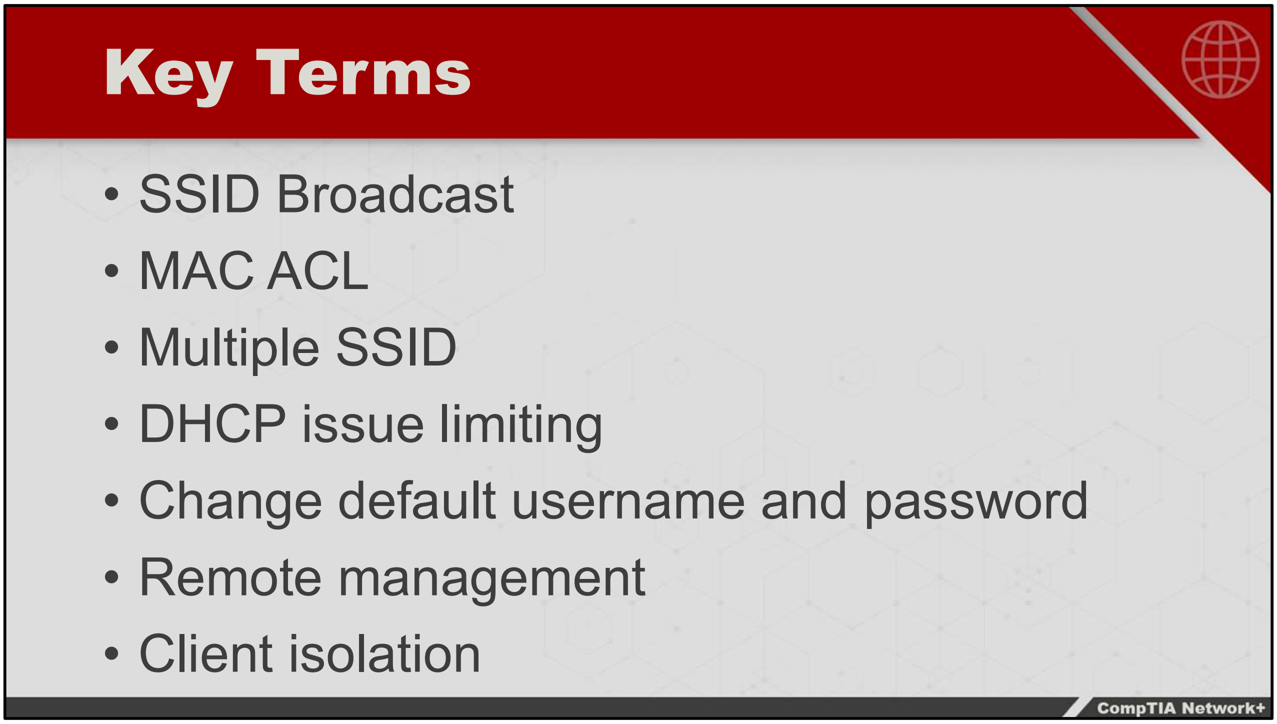


Episode 14.06

Episode title: **Implementing Wireless Security**

Objective: **2.4 Given a scenario, install and configure the appropriate wireless standards and technologies**

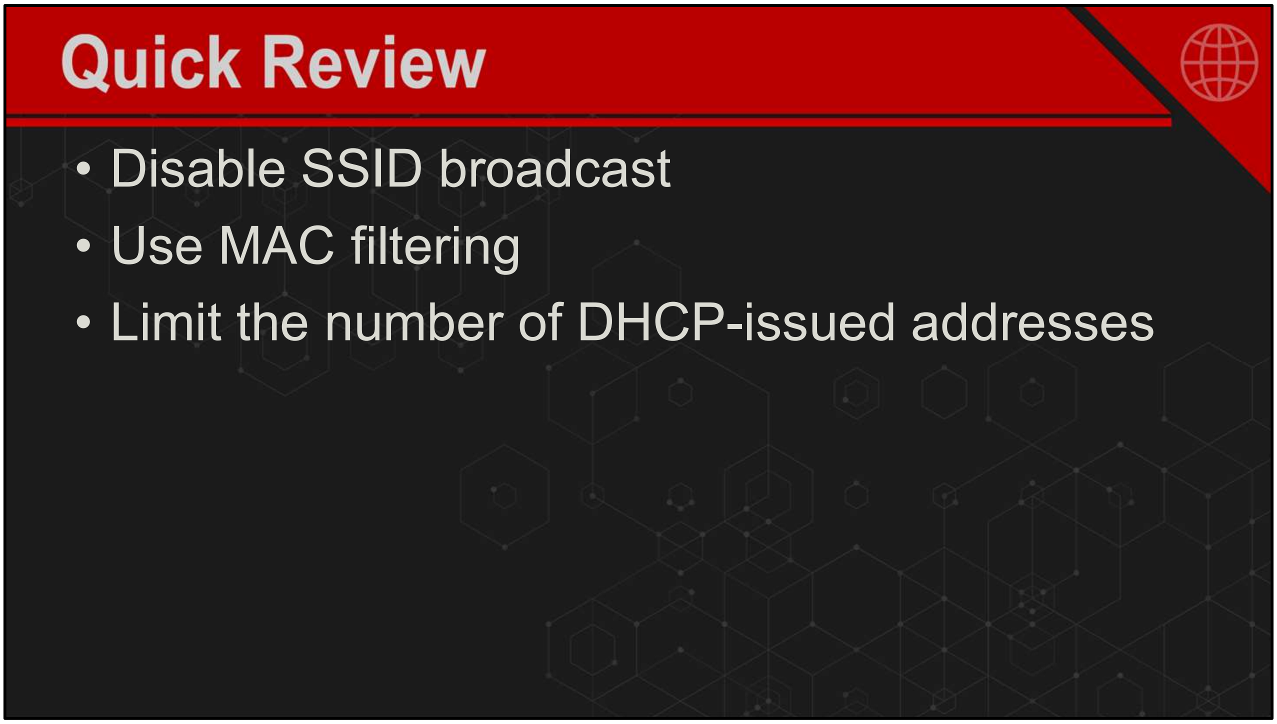
CompTIA Network+



Key Terms

- SSID Broadcast
- MAC ACL
- Multiple SSID
- DHCP issue limiting
- Change default username and password
- Remote management
- Client isolation

CompTIA Network+



Quick Review

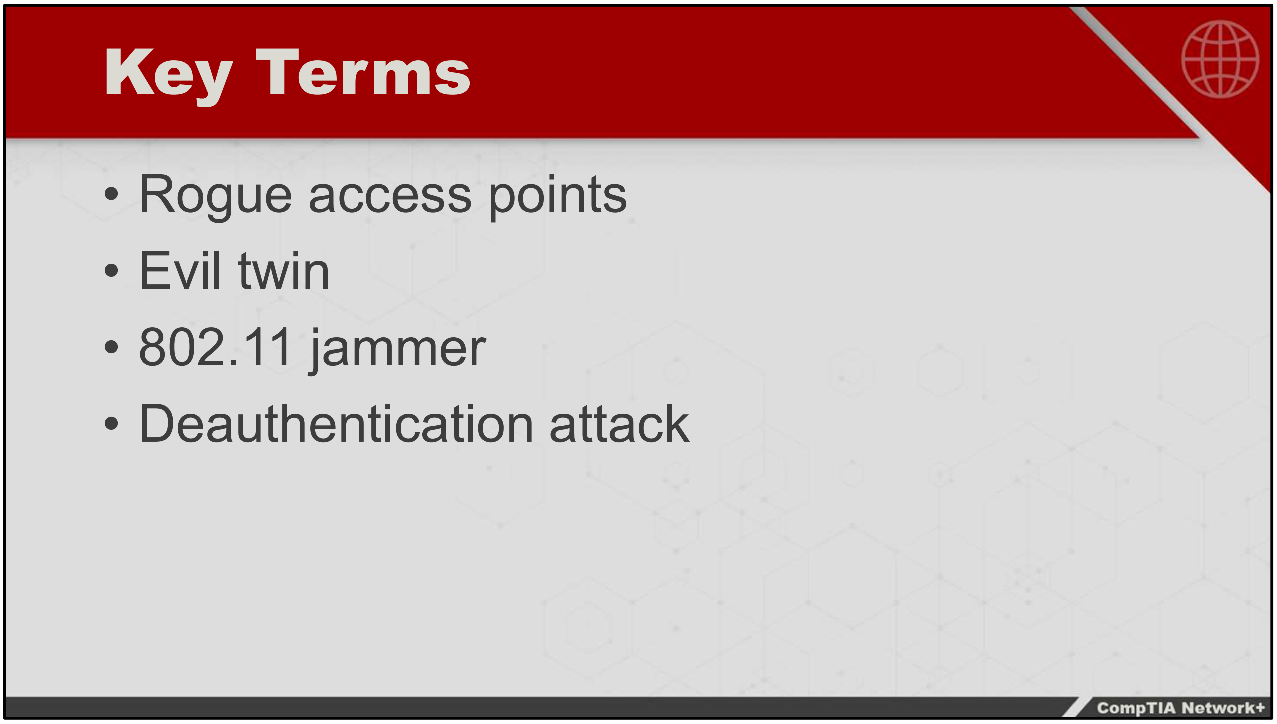
- Disable SSID broadcast
- Use MAC filtering
- Limit the number of DHCP-issued addresses

Episode 14.07

Episode title: **Threats to Your Wireless Network**

Objective: **4.2 Compare and contrast common types of attacks**

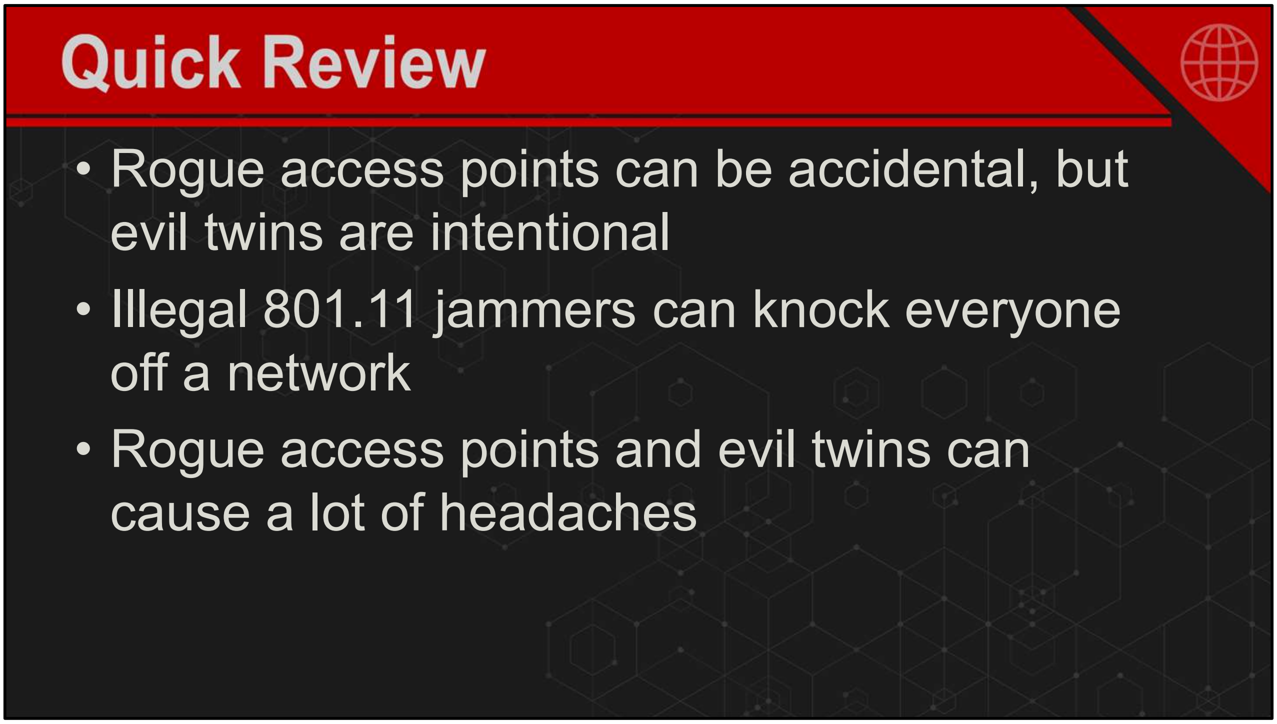
CompTIA Network+



Key Terms

- Rogue access points
- Evil twin
- 802.11 jammer
- Deauthentication attack

CompTIA Network+



Quick Review

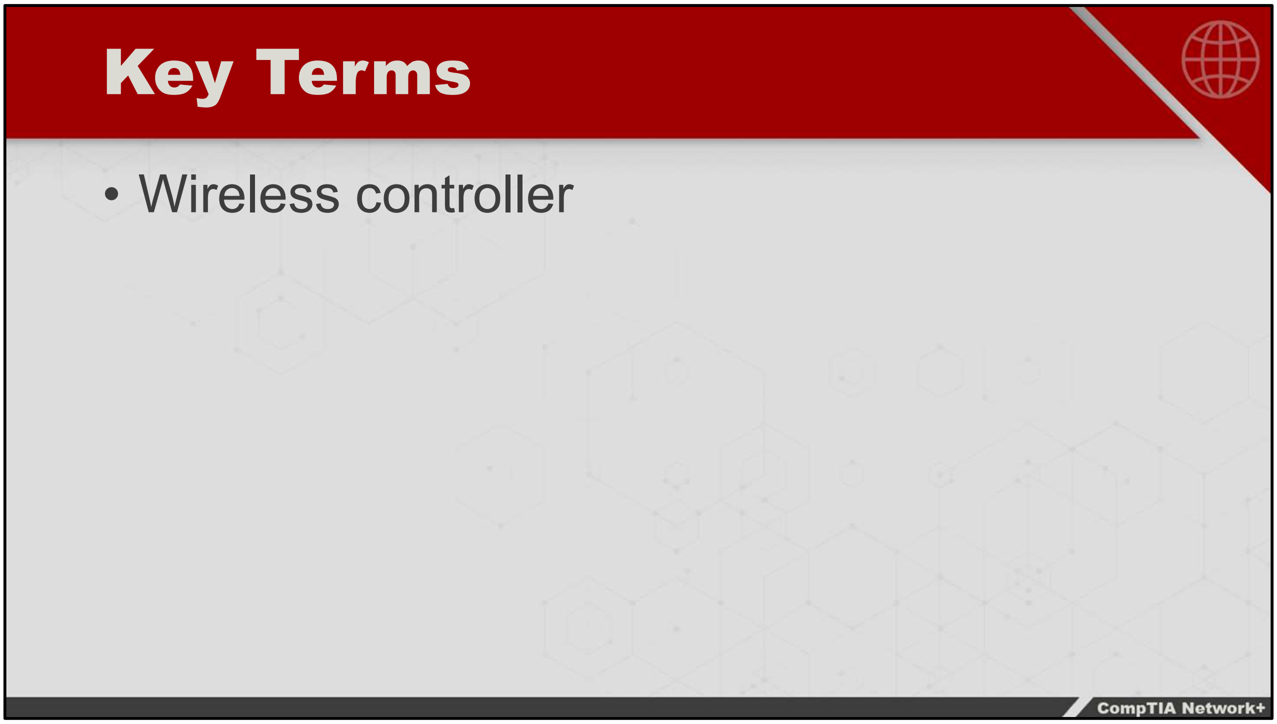
- Rogue access points can be accidental, but evil twins are intentional
- Illegal 801.11 jammers can knock everyone off a network
- Rogue access points and evil twins can cause a lot of headaches

Episode 14.08

Episode title: **Enterprise Wireless**

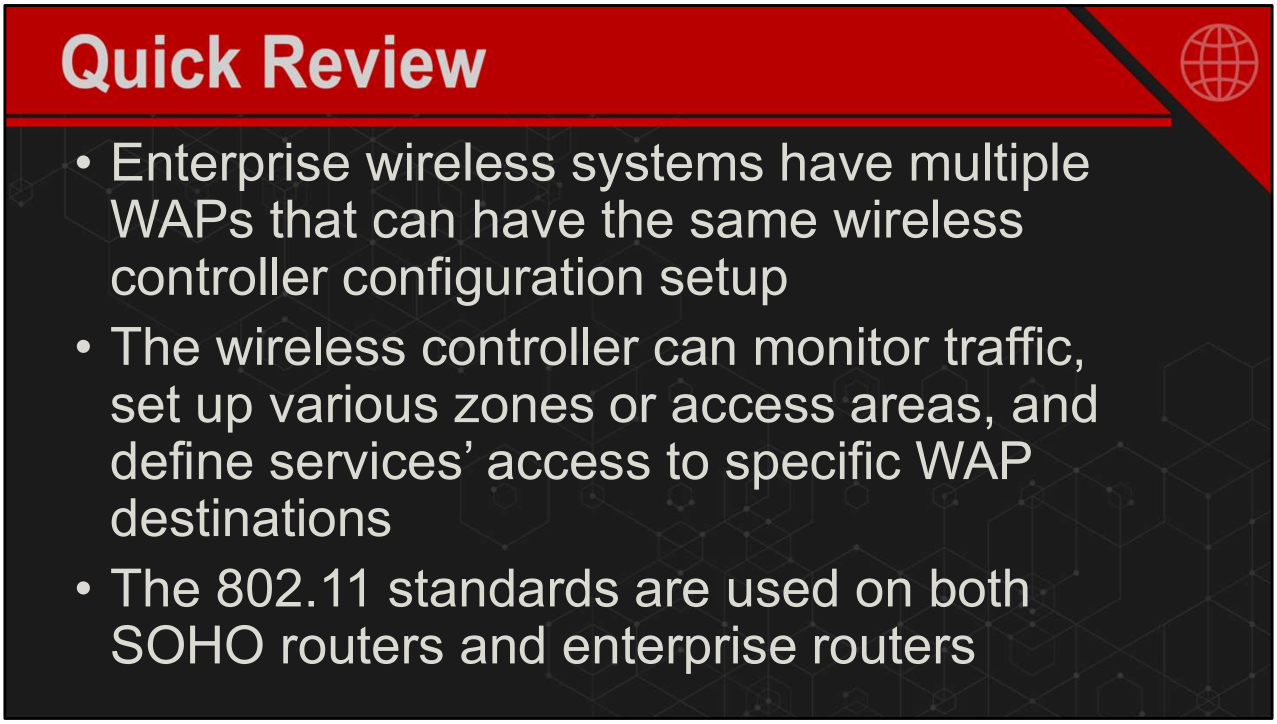
Objective: **2.1 Compare and contrast various devices, their features, and their appropriate placement on the network**

CompTIA Network+



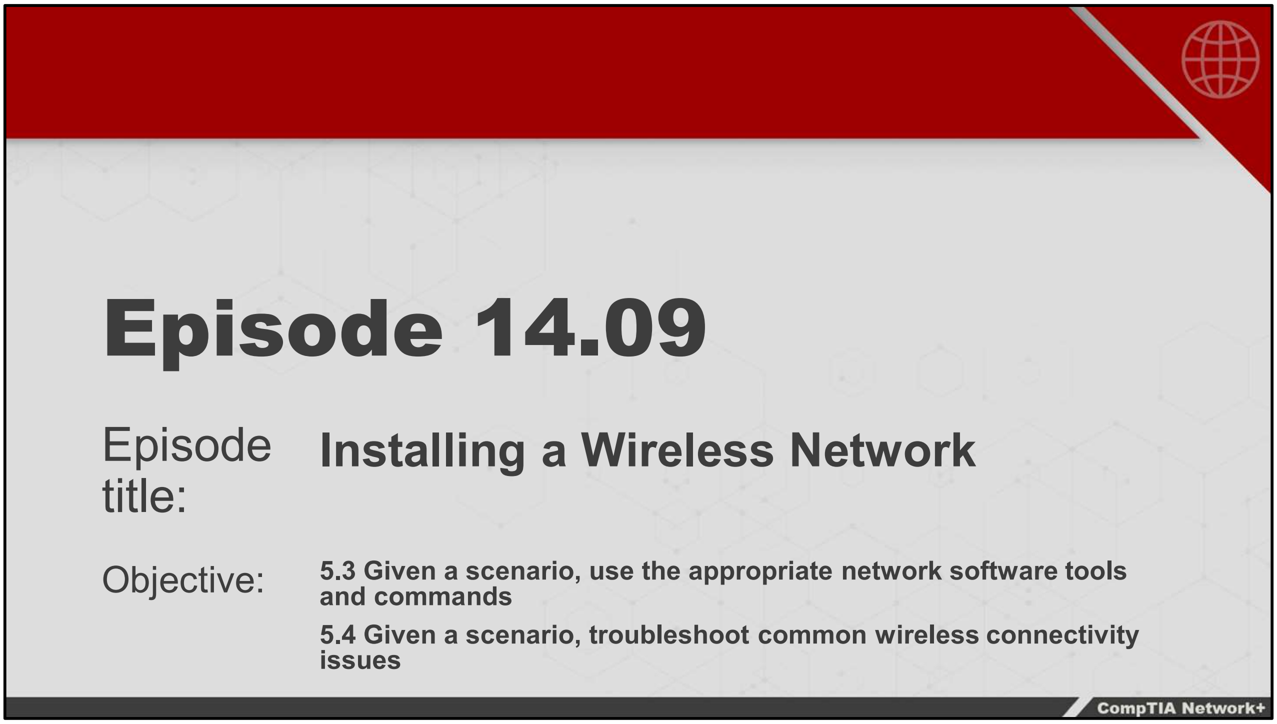
Key Terms

- Wireless controller



Quick Review

- Enterprise wireless systems have multiple WAPs that can have the same wireless controller configuration setup
- The wireless controller can monitor traffic, set up various zones or access areas, and define services' access to specific WAP destinations
- The 802.11 standards are used on both SOHO routers and enterprise routers



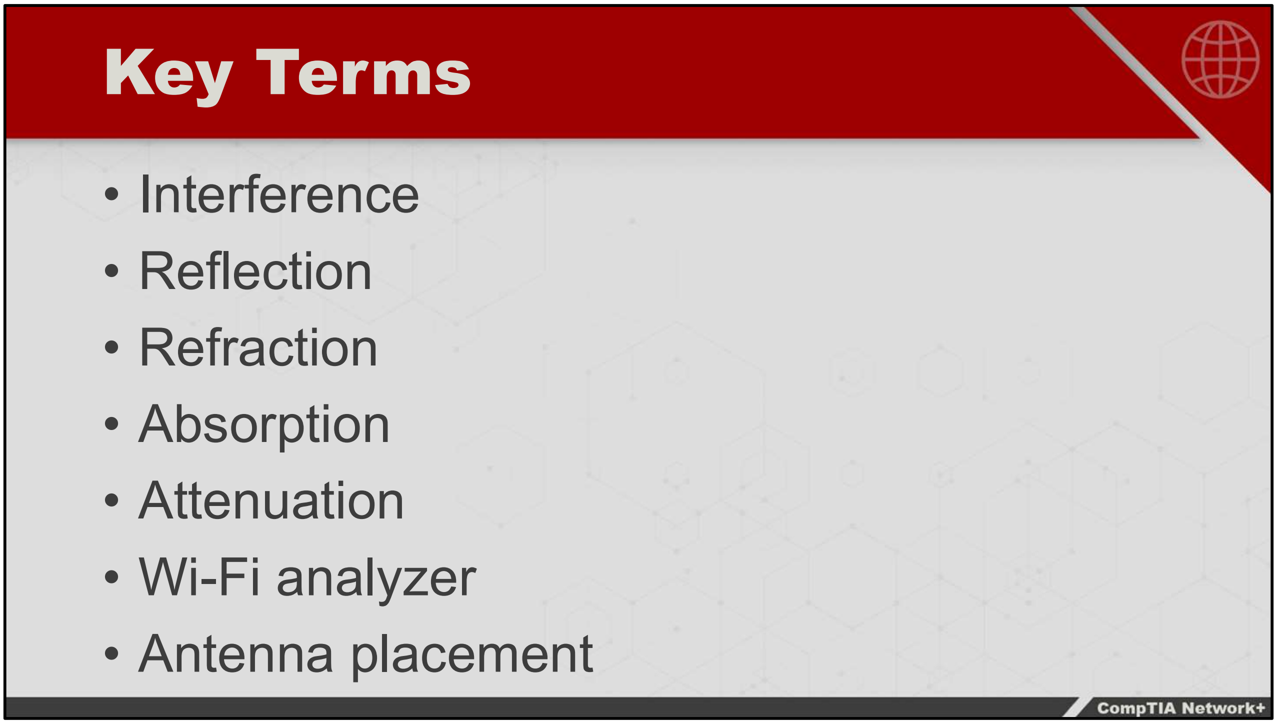
Episode 14.09

Episode title: **Installing a Wireless Network**

Objective: **5.3 Given a scenario, use the appropriate network software tools and commands**

5.4 Given a scenario, troubleshoot common wireless connectivity issues

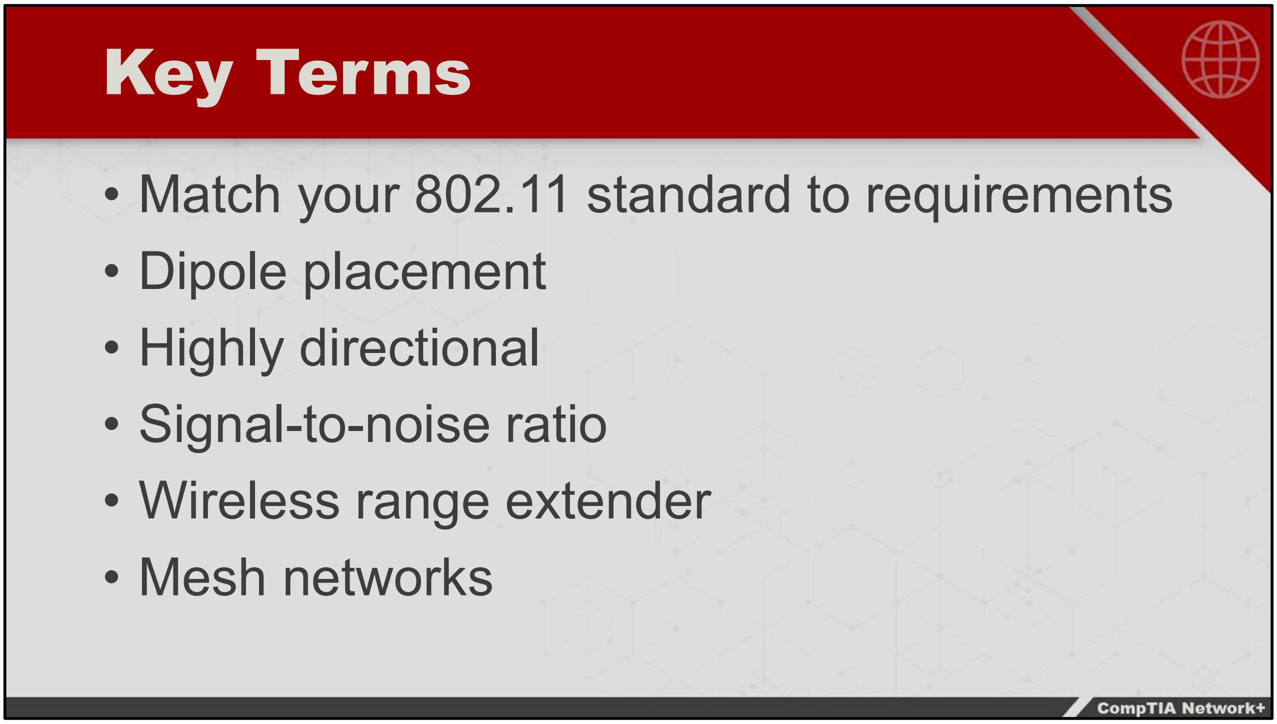
CompTIA Network+



Key Terms

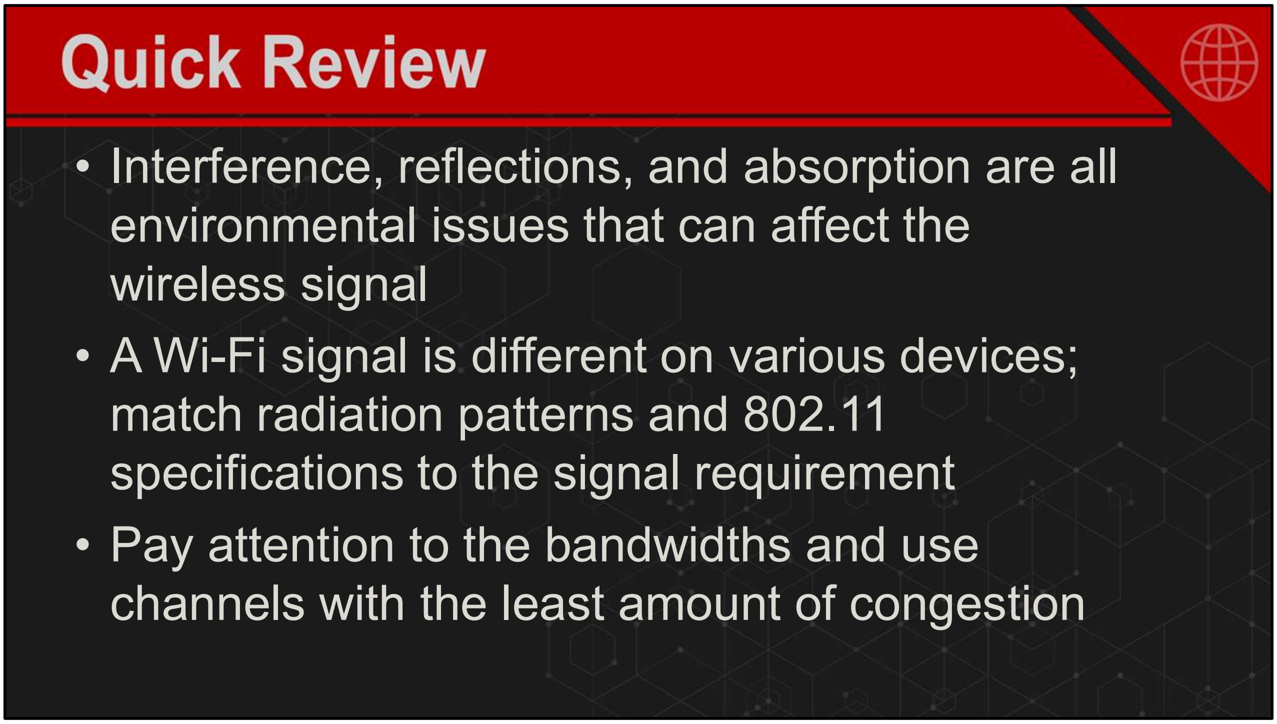
- Interference
- Reflection
- Refraction
- Absorption
- Attenuation
- Wi-Fi analyzer
- Antenna placement

CompTIA Network+



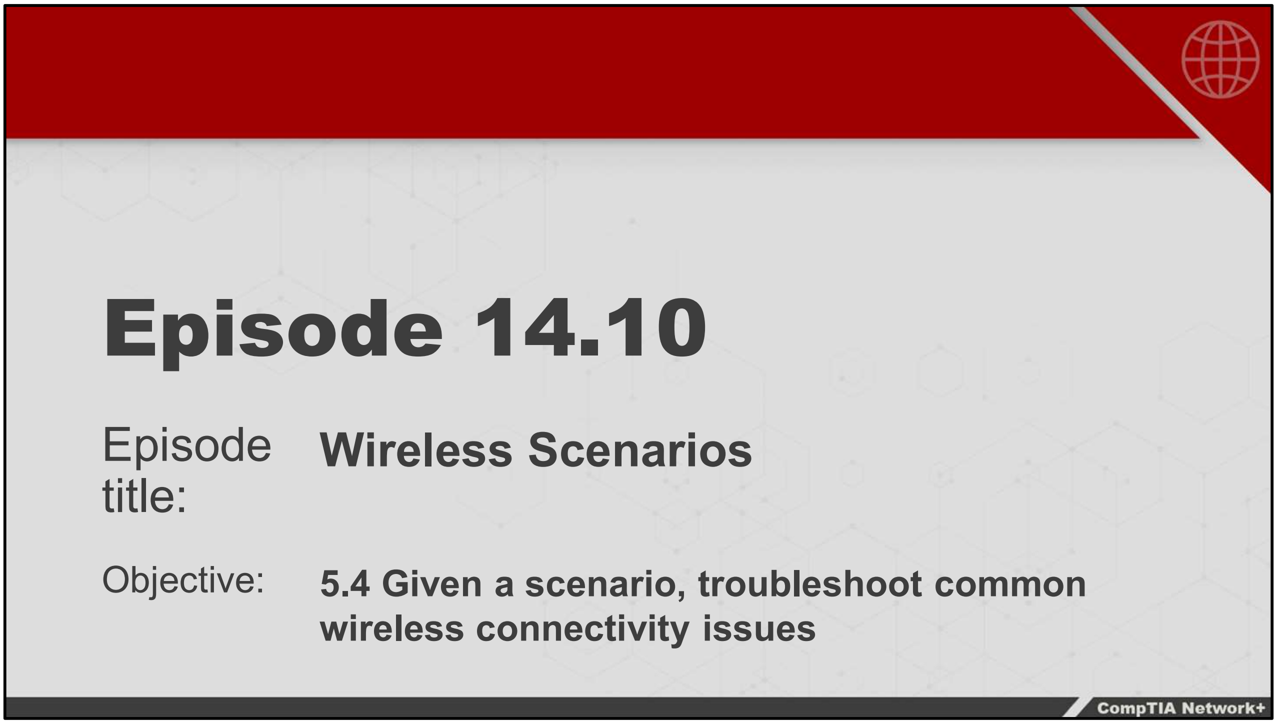
Key Terms

- Match your 802.11 standard to requirements
- Dipole placement
- Highly directional
- Signal-to-noise ratio
- Wireless range extender
- Mesh networks



Quick Review

- Interference, reflections, and absorption are all environmental issues that can affect the wireless signal
- A Wi-Fi signal is different on various devices; match radiation patterns and 802.11 specifications to the signal requirement
- Pay attention to the bandwidths and use channels with the least amount of congestion

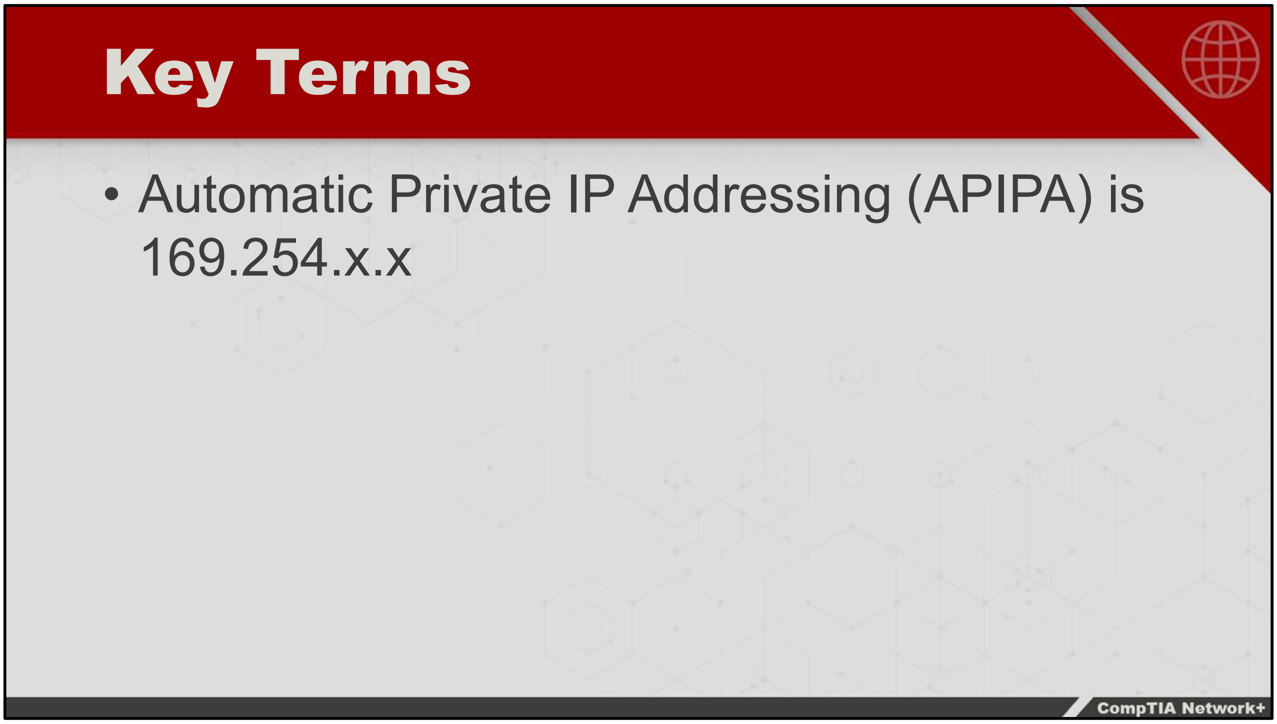


Episode 14.10

Episode title: **Wireless Scenarios**

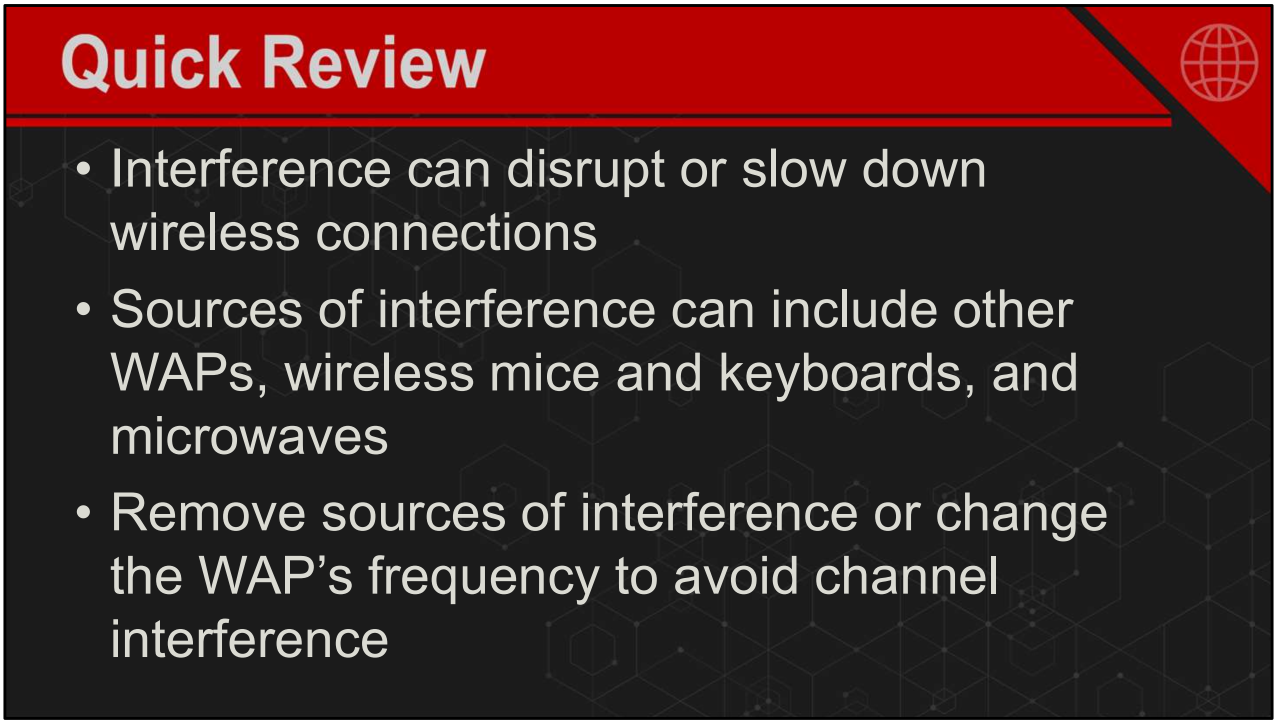
Objective: **5.4 Given a scenario, troubleshoot common wireless connectivity issues**

CompTIA Network+



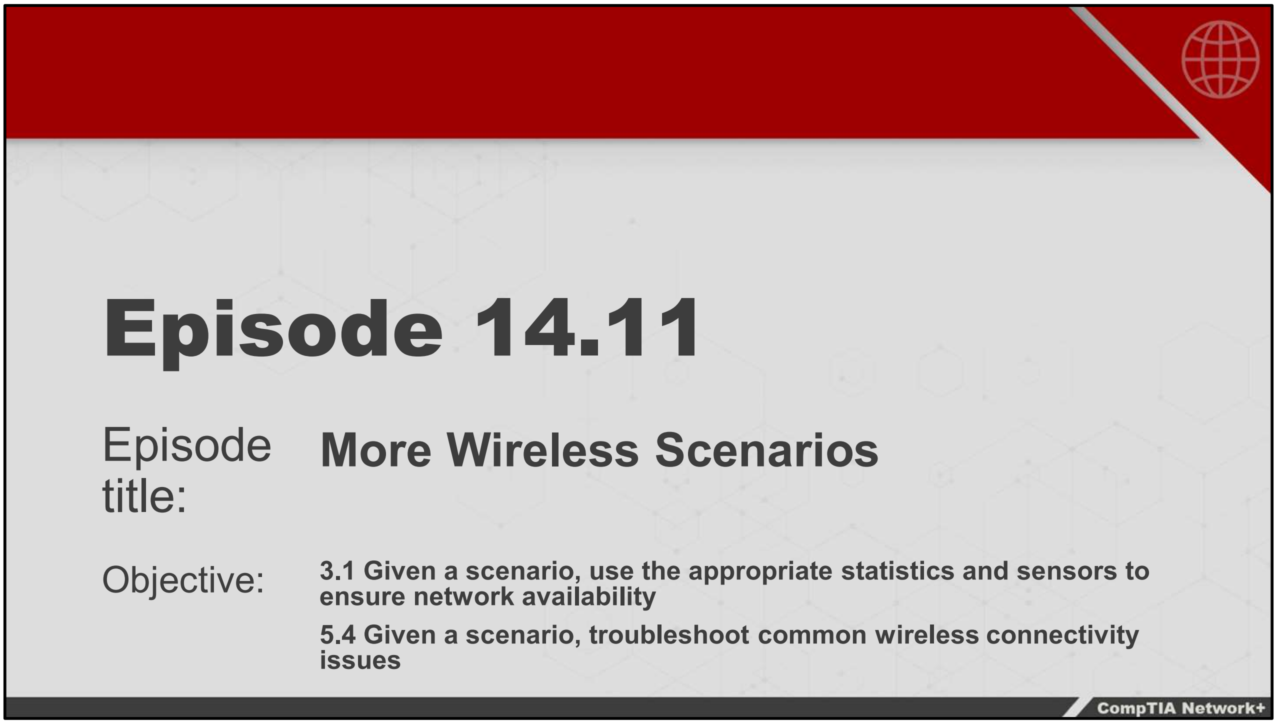
Key Terms

- Automatic Private IP Addressing (APIPA) is 169.254.x.x



Quick Review

- Interference can disrupt or slow down wireless connections
- Sources of interference can include other WAPs, wireless mice and keyboards, and microwaves
- Remove sources of interference or change the WAP’s frequency to avoid channel interference



Episode 14.11

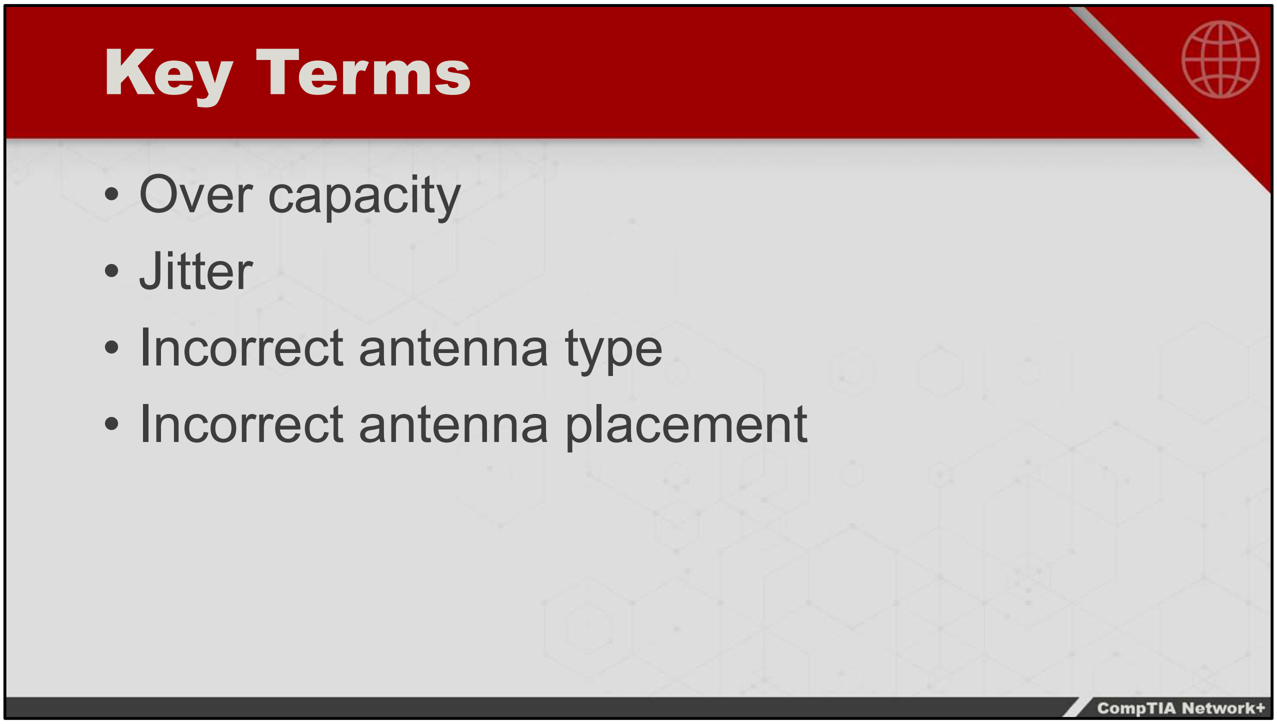
Episode title: **More Wireless Scenarios**

Objective:

3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability

5.4 Given a scenario, troubleshoot common wireless connectivity issues

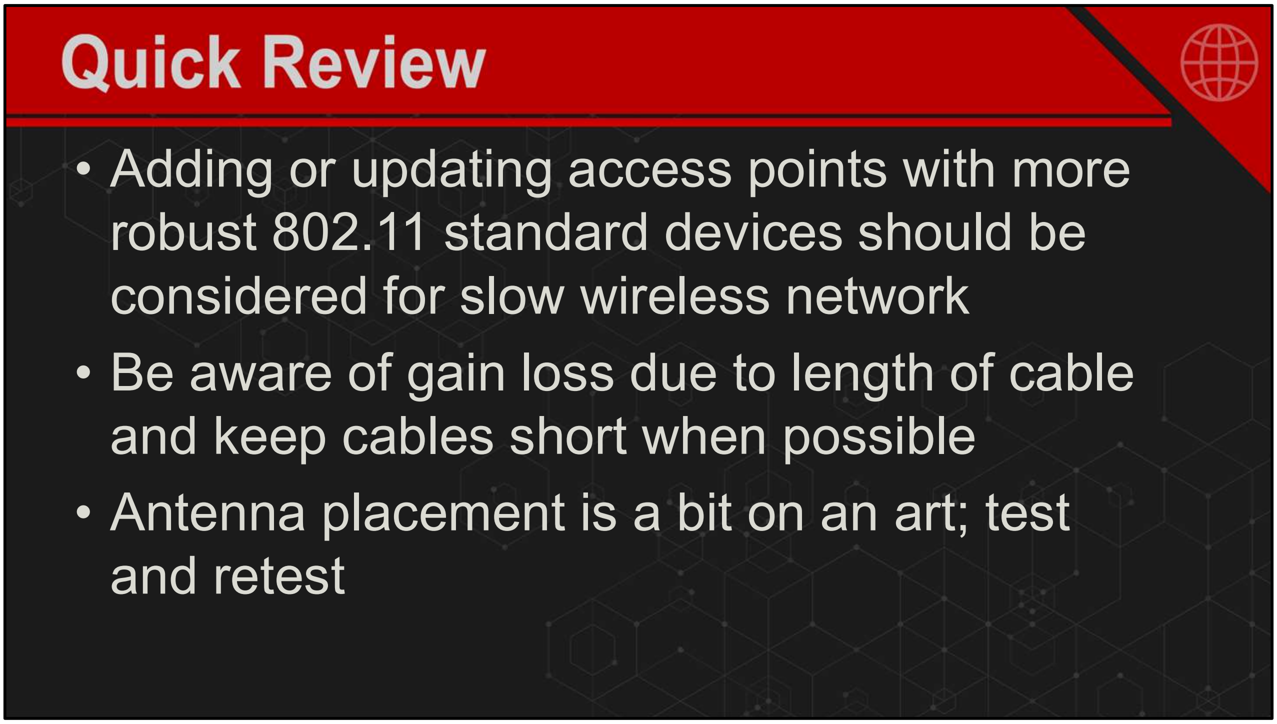
CompTIA Network+



Key Terms

- Over capacity
- Jitter
- Incorrect antenna type
- Incorrect antenna placement

CompTIA Network+



Quick Review

- Adding or updating access points with more robust 802.11 standard devices should be considered for slow wireless network
- Be aware of gain loss due to length of cable and keep cables short when possible
- Antenna placement is a bit on an art; test and retest