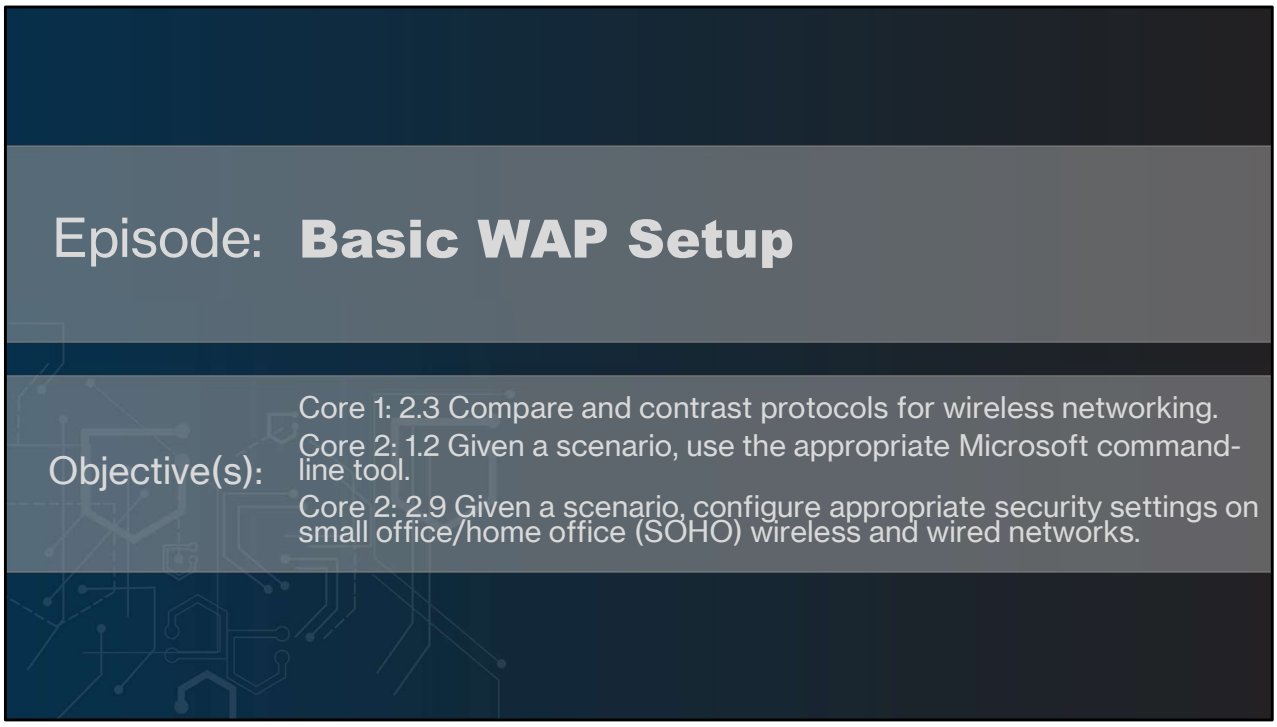
Chapter 20

Wireless Networking


Episode: Basic WAP Setup
Objective(s):
Core 1: 2.3 Compare and contrast protocols for wireless networking.
Core 2: 1.2 Given a scenario, use the appropriate Microsoft command-line tool.
Core 2: 2.9 Given a scenario, configure appropriate security settings on small office/home office (SOHO) wireless and wired networks.

Episode Description

The standard wireless access point (WAP) doesn't just work out of the box. It's important to understand how to perform a basic setup for a WAP to make sure it operates properly in your network.

Key Terms

- 0:37 - Site survey
- 0:45 - WiFiman
- 1:02 - 2.4 GHz band site survey
- 2:06 - 5 GHz band site survey
- 2:30 - Objective term - The best practice is to have the WAP set the channels automatically
- 3:09 - Objective term - ipconfig
- 3:14 - The default gateway is your router!

Key Terms

- 2:30 - Objective term - Changing channels
- 4:57 - Objective term - Service set identifier (SSID) (It's the name of your wireless network)
- 6:20 - Objective term - Hide/disable SSID broadcast

Quick Review

- A site survey shows available channels in an ISM band
- You must create a service set identifier (SSID)
- Most WAPs support multiple SSIDs
- You can hide SSID broadcasts
- You can define extensions to support channels and channel width

Episode: **Wireless Encryption**

Objective(s):

Core 2: 2.2 Compare and contrast wireless security protocols and authentication methods.

Core 2: 2.9 Given a scenario, configure appropriate security settings on small office/home office (SOHO) wireless and wired networks.

CompTIA A+ (220-110x)

Mike Meyers and Steve Nicholson

Episode Description

Everything on an unencrypted (open) wireless network is easily intercepted by anyone with the right capture tools. Over the years, 802.11 has developed three different encryption standards, each with its own idiosyncrasies, strengths, and weaknesses.

Key Terms

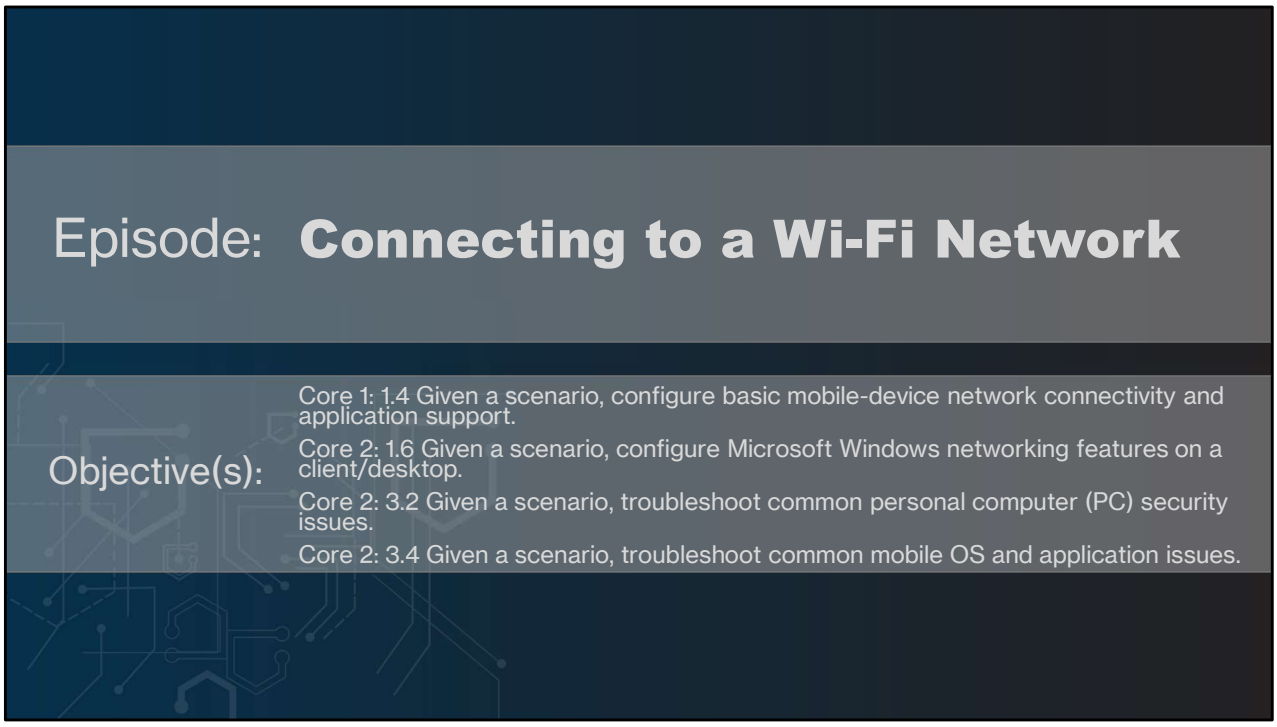
- 0:46 - WEP (Wired Equivalent Privacy)
- 1:48 - RC-4
- 2:49 - Objective term - TKIP (Temporal Key Integrity Protocol)
- 3:03 - Objective term - AES (Advanced Encryption Standard)
- 3:58 - Personal/Pre-shared key (PSK)
- 4:17 - Objective term - Remote Authentication Dial-In User Service (RADIUS) server

Key Terms

- 4:53 - WPA (Wi-Fi Protected Access)
- 5:18 - Objective term - WPA2
- 6:21 - WPA-PSK (personal/pre-shared key)
- 7:10 - WPA uses TKIP; WPA2 uses AES
- 7:44 - WPS (Wi-Fi Protected Setup)

Quick Review

- The obsolete WEP encryption is easily cracked today and is never used
- WPA introduced TKIP-personal shared key and RADIUS authentication
- WPA2 added AES encryption
- WPS automates encryption, but is easily crackable


Episode: Connecting to a Wi-Fi Network
Objective(s):
Core 1: 1.4 Given a scenario, configure basic mobile-device network connectivity and application support.
Core 2: 1.6 Given a scenario, configure Microsoft Windows networking features on a client/desktop.
Core 2: 3.2 Given a scenario, troubleshoot common personal computer (PC) security issues.
Core 2: 3.4 Given a scenario, troubleshoot common mobile OS and application issues.

Episode Description

The best 802.11 network is useless unless your users can connect to it. Smartphones, desktops, IoT devices, and other networked gizmos need to be individually configured to access your 802.11 network.

Key Terms

- 1:31 - Establish wireless network connection on laptop
- 2:10 - Unable to access the network due to disables wireless NIC
- 3:42 - Network profile
- 6:06 - Enable mobile wireless network

Issues Connecting to an SSID

- The NIC is setup as a DHCP client
  - If you get an APIPA address (169.254.x.x), it's a clue that you have a bad password
- Passwords can change
- Set wireless NIC to a static IP address to avoid some of these issues

Quick Review

- All wireless clients can scan the 802.11 spectrum, finding available SSIDs
- You must know the SSID and password to connect
- Clients create profiles that store the SSIDs and their passwords

Episode: **Enterprise Wireless**

Objective(s):

Core 1: 2.2 Compare and contrast common networking hardware.

Core 2: 2.2 Compare and contrast wireless security protocols and authentication methods.

Core 2: 2.9 Given a scenario, configure appropriate security settings on small office/home office (SOHO) wireless and wired networks.

Episode Description

There's a big difference between the 802.11 network in your home and small office vs. 802.11 in larger organization such as businesses, schools and government offices. Multiple SSIDS, advanced technologies, and more aggressive authentication and encryption are common in every enterprise.

Key Terms

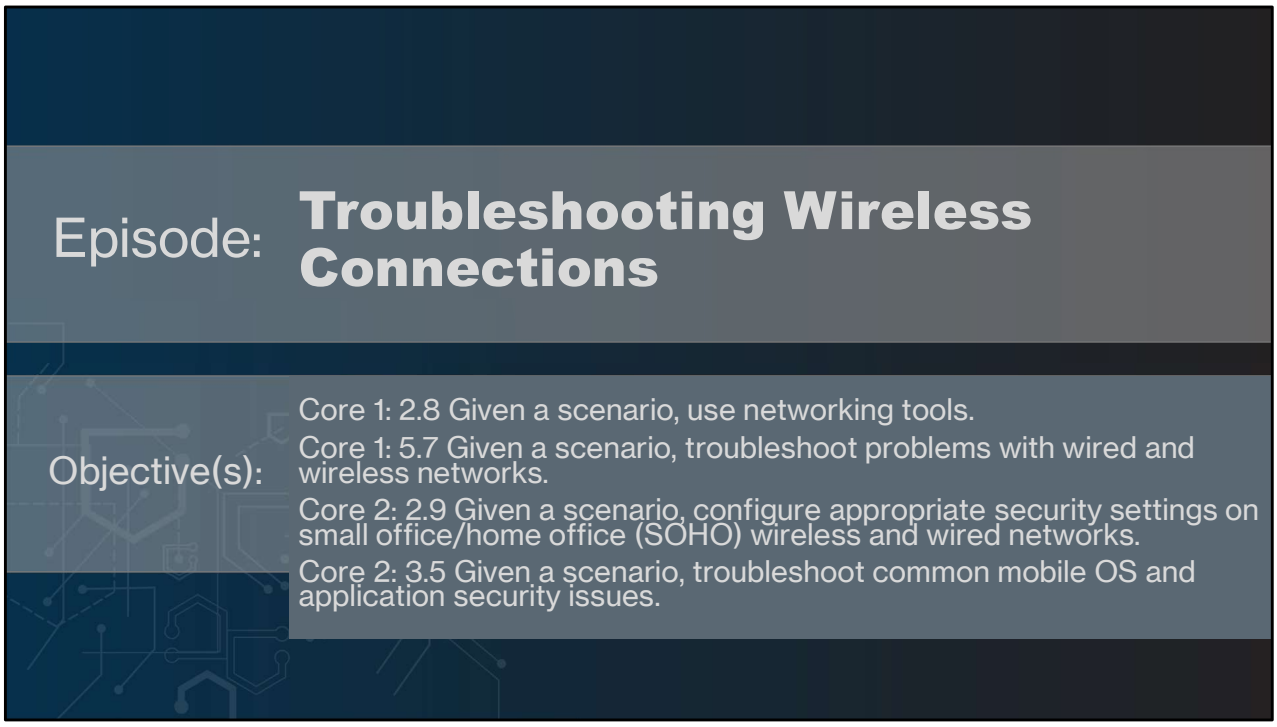
- 1:06 - Objective term - Power over Ethernet (PoE)
- 1:24 - Objective term- PoE (1st generation) and PoE
- 1:42 - Objective term - PoE switch
- 2:12 - Objective term - PoE injector
- 4:52 - AAA – authorization, authentication, accounting
- 5:12 - Objective term - RADIUS or TACACS+
- 7:09 - Objective term - Change default usernames and passwords!

Key Terms

- 8:22 - Extended SSID (ESSID)
- 11:18 - Objective term - Separate SSIDs can be enabled or disabled easily for guest access
- 12:55 - Rate limit
- 13:34 - Captive portal
- 14:23 - Objective term - Special enterprise wireless LAN (WLAN) switch

Quick Review

- Enterprise WAPs often use Power over Ethernet (PoE)
- Use powerful wireless analysis tools to determine WAP location
- Enterprise networks often use RADIUS or TACACS+ protocols for authentication
- Two or more WAPs sharing the same SSID are known as extended SSIDs (ESSIDs)


Episode:
Troubleshooting Wireless Connections
Objective(s):
Core 1: 2.8 Given a scenario, use networking tools.
Core 1: 5.7 Given a scenario, troubleshoot problems with wired and wireless networks.
Core 2: 2.9 Given a scenario, configure appropriate security settings on small office/home office (SOHO) wireless and wired networks.
Core 2: 3.5 Given a scenario, troubleshoot common mobile OS and application security issues.

Episode Description

There are few worse feelings than a wireless connection that just doesn't... connect. In situations like this, good techs will have the right tools and skills to diagnose and repair the issue.

Key Terms

- 0:32 - Objective term - Wi-Fi analyzer
- 1:11 - Objective term - No connectivity
- 1:45 - Objective term - Low RF signal can lead to no, low, slow, or intermittent connectivity
- 3:19 - Objective term - Disabling SSID broadcast can also cause connectivity problems
- 3:46 - Objective term - Limited connectivity

Key Terms

- 4:11 - Objective term - External interference (like a wall, baby monitor, microwave, etc) can interfere with wireless signals
- 4:20 - Objective term - Slow transfer/network speeds or high latency
- 4:24 - Objective term - Change the physical placement of the WAP or move interfering objects
- 5:05 - Objective term - Intermittent connectivity

Quick Review

- Wi-Fi analyzers are helpful to diagnose wireless problems
- No connectivity can be caused by low RF signal or disabled SSID broadcast
- Limited connectivity can be caused by low RF signal or external interferences
- Intermittent connectivity is usually caused by too many people on the Wi-Fi network