Chapter 20

Wireless Networking

Episode: **Wireless Network Hardware**

Objective(s):

Core 1: 1.2 Compare and contrast the display components of mobile devices.

Core 1: 2.2 Compare and contrast common networking hardware.

Core 1: 2.3 Compare and contrast protocols for wireless networking.

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

Episode Description

The 802.11 standard has had a number of improvements over the years, but every version shares common devices and functions that haven't changed in over 20 years. This episode explores wireless access points (WAPs), home routers, and the antennas that make them work.

Key Terms

- 0:30 - Objective term - IEEE 802.11
- 1:05 - Objective term - Wireless access point (WAP)
- 1:35 - Objective term - Wireless home router
- 2:36 - Infrastructure Mode
- 3:10 - Objective term - Wireless network card
- 4:14 - Objective term - Laptop wireless antennas are usually run around the monitor
- 4:50 - Objective term - Service set identifier (SSID)

Key Terms

- 5:14 - Ad hoc mode
- 6:15 - Antennas
- 6:36 - Omni-directional
- 7:16 - Dipole
- 8:12 - Patch
- 8:43 - Highly directional
- 8:46 - Yagi

Quick Review

- A wireless access point (WAP) bridges 802.11 and Ethernet networks and only has one Ethernet port
- A home router has multiple Ethernet ports to give Internet access to multiple devices; it is a router, switch, and WAP all in one
- Wireless clients connect to WAPs
- 802.11 works in one of two modes: infrastructure mode or ad hoc mode
- Use the correct antenna for the job

Episode: **Wi-Fi Standards**

Objective(s): Core 1: 2.3 Compare and contrast protocols for wireless networking.

Episode Description

Since the original 802.11 standard back in 1999, there have been five major and hundreds of minor revisions. It's impossible to support an 802.11 network without a working understanding of these standards.

Key Terms

- 1:06 - Industrial, scientific, and medical (ISM) radio bands
- 1:20 - Objective term - Frequencies: 2.4 GHz and 5 GHz band
- 2:06 - Objective term - 2.4 GHz band: 2.412 - 2.4884 GHz
- 2:36 - Objective term - Channels
- 3:18 - Objective term - 5 GHz band: 5.150 - 5.875 GHz
- 4:17 - Objective term - 802.11a
- 4:34 - Objective term - 802.11b

Key Terms

- 4:58 - Objective term - 802.11g
- 5:58 - Objective term - 802.11n (Wi-Fi 4)
- 6:37 - MIMO (multiple in/multiple out)
- 7:10 - Objective term - 802.11ac (Wi-Fi 5)
- 7:23 - Multiuser MIMO (MU-MIMO)
- 8:19 - Objective term - 802.11n (Wi-Fi 4) 802.11ac (Wi-Fi 5)

IEEE 802.11 Standards

Standard	Speed	Band
802.11a	54 Mbps	5 GHz
802.11b	11 Mbps	2.4 GHz
802.11g	54 Mbps	2.4 GHz
802.11n (Wi-Fi 4)	150 Mbps	2.4GHz 5 GHz
802.11ac (Wi-Fi 5)	1+ Gbps	5 GHz
802.11ax (Wi-Fi 6)	9+ Gbps	2.4 GHz 5 GHz 6 GHz

Quick Review

- 802.11 uses the 2.4- and 5-GHz ISM bands (and now 802.11ax Wi-Fi 6 uses the 6-GHz band)
- 802.11 uses premade channels
- Memorize the band usage and relative speeds of the 802.11 extensions

Episode: **It's a Huge Mesh**

Objective(s): Core 1: 2.5 Given a scenario, install and configure basic wired/wireless small office/home office (SOHO) networks.

Episode Description

Mesh networking is here and gaining in popularity daily. But what does mesh networking do for your 802.11 network? Where do you use it and how is it deployed?

Key Terms

- 0:23 - Wireless Mesh Network (WMN)

Quick Review

- Mesh networks are often a great wireless solution for SOHO environments
- Mesh networks have a base station and beacon devices that connect to the base station
- Mesh networks use their own encryption
- Mesh networks are universally easy to configure

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: **Beyond Wi-Fi**

Objective(s):

- Core 1: 1.3 Given a scenario, set up and configure accessories and ports of mobile devices.
- Core 1: 1.4 Given a scenario, configure basic mobile-device network connectivity and application support.
- Core 1: 2.3 Compare and contrast protocols for wireless networking.
- Core 1: 2.7 Compare and contrast Internet connection types, network types, and their features.
- Core 2: 3.4 Given a scenario, troubleshoot common mobile OS and application issues.

Episode Description

The 802.11 standard isn't the only wireless out there today. Standards such as Bluetooth, RFID, and NFC also need the support of good techs.

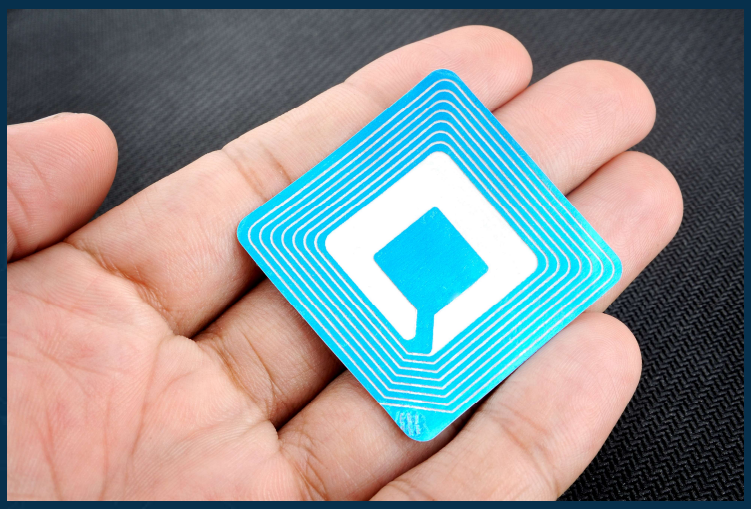
Key Terms

- 0:22 - Objective term - Radio Frequency Identification (RFID)
- 1:21 - Objective term - Near Field Communication (NFC)
- 1:30 - Tap-to-print
- 2:06 - Tap-to-pay
- 2:22 - Objective term - Bluetooth

Key Terms

- 2:56 - Objective term - Personal Area Network (PAN)
- 4:15 - Objective term - Bluetooth pairing
- 5:20 - Objective term - Some Bluetooth pairing requires a PIN code

RFID

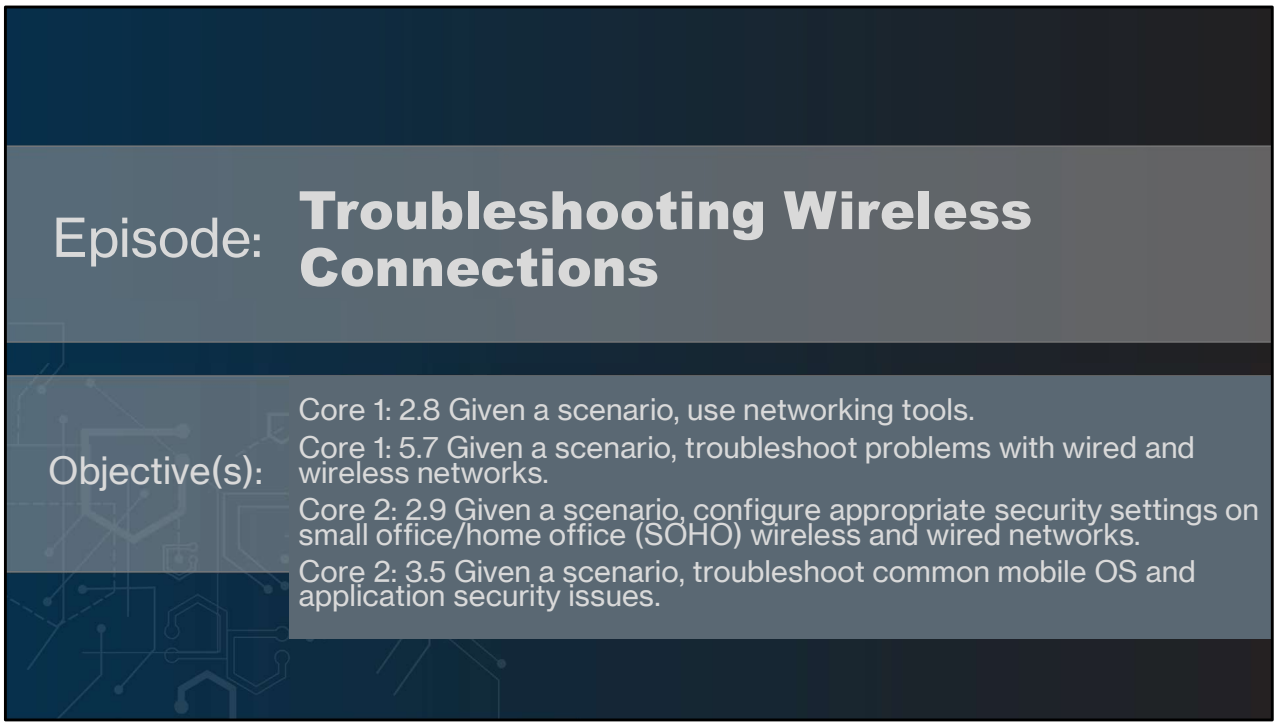


Bluetooth Classes

Class	Power	Range
Class 1	100 mW	100 m
Class 2	2.5 mW	10 m
Class 3	1 mW	1 m

Quick Review

- RFID uses tiny radios activated by the energy of the scanning device
- NFC requires extremely close proximity to function
- Bluetooth is like 802.11 but pairs with devices to function as point-to-point


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