Chapter 21

The Internet

Episode: **Beyond the LAN**

Objective(s): Core 1: 2.7 Compare and contrast Internet connection types, network types, and their features.

CompTIA A+ (220-110x)
Mike Meyers and Steve Nicholson

Episode Description

In this episode, Mike explores the crazy acronym soup around networking, explaining the differences among terms like LAN, WAN, MAN, PAN, and HAM. (Just kidding on the last term!) This helps minimize confusion in later networking episodes.

Key Terms

- 0:26 - Objective term - Local Area Network (LAN)
- 1:02 - Objective term - Wide Area Network (WAN)
- 1:25 - Objective term - Metropolitan Area Network (MAN)
- 1:42 - The Internet
- 2:19 - Objective term - Personal Area Network (PAN)

Quick Review

- Local area network (LAN) computers share the same network ID
- A wide area network (WAN) is two or more LANs interconnected by one or more routers
- A metropolitan area network (MAN) is a WAN that spans a city
- A personal area network (PAN) is a point-to-point connection used only in Bluetooth connections

Episode: **Internet Tiers**

Objective(s): Core 1: 2.7 Compare and contrast Internet connection types, network types, and their features.

CompTIA A+ (220-110x)
Mike Meyers and Steve Nicholson

Episode Description

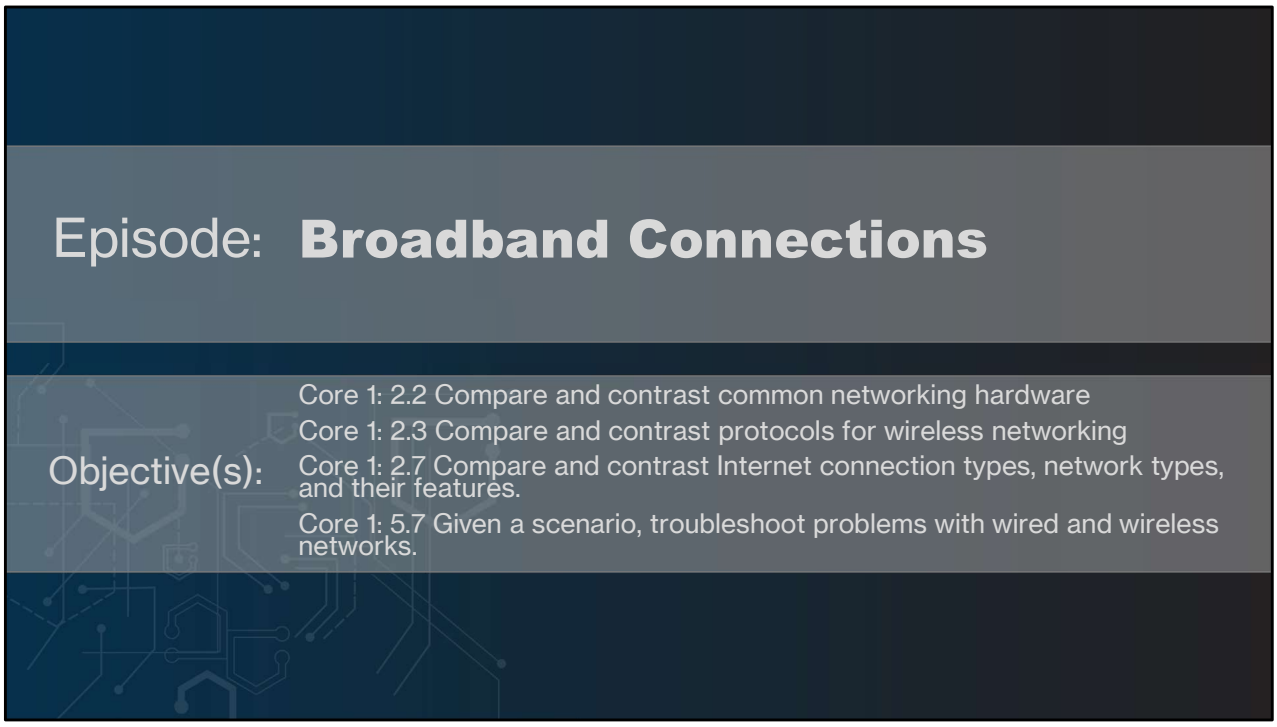
In this episode, Mike discusses the structure of the Internet. Starting with the Tier 1 carriers, he shows how carriers at each layer relate to their peers and also how they interact with Tiers above and customers below. This episode provides a good structure for layering your wide-area-networking knowledge.

Key Terms

- 0:21 - Tier 1
- 1:20 - Peering agreement
- 2:04 - Network Operation Centers (NOCs)
- 3:38 - Tier 2
- 4:31 - Tier 3

Quick Review

- The Internet is composed of many organizations that connect to each other
- Tier 1 are providers that do not pay anyone (peering)
- Tier 2 are providers that pay some Tier 1s but also peer with Tier 1 and Tier 2s
- Tier 3 providers pay Tier 1 or Tier 2 providers


Episode: Broadband Connections
Objective(s):
Core 1: 2.2 Compare and contrast common networking hardware
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 1: 5.7 Given a scenario, troubleshoot problems with wired and wireless networks.

Episode Description

In this episode, Mike explores common always-on broadband connections to the Internet. Starting with DSL, the episode looks also at fiber, cable, satellite, and 802.11 Wi-Fi.

Key Terms

- 0:14 - Broadband connection
- 0:42 - Objective term - Digital Subscriber Line (DSL)
- 1:34 - Modem
- 1:52 - Objective term - DSL/cable modem
- 2:10 - Asymmetric DSL (ADSL)
- 2:16 - Symmetric DSL (SDSL)
- 2:24 - Speeds: 768 Kbps - 3 Mbps upload, 1.5 - 7+ Mbps download

Key Terms

- 3:17 - Point-to-Point Protocol over Ethernet (PPPoE)
- 4:41 - Objective term - Cable
- 4:58 - Data Over Cable Service Interface Specification (DOCSIS)
- 5:17 - Speeds: Older 1.5 Mbps up/10 Mbps down, Today: 50 Mbps up/100+ Mbps down
- 6:29 - Objective term - Cable modem (usually includes router, WAP, switch, firewall)

Key Terms

- 7:38 - Objective term - Satellite
- 7:56 - Speeds: 3 Mbps upload/25+ Mbps download
- 8:17 - Objective term - Latency
- 8:45 - Objective term - 802.11
- 9:51 - Objective term - Wireless Internet Service Providers (WISPs)
- 10:14 - Objective term - Optical network terminal (ONT)

What's the Difference Between a Modem and a Router, Anyway?

- Check out this resource to help you understand the difference:
  - https://seeromega.com/whats-difference-cable-modem-router/#:~:text=In%20fact%2C%20cable%20modems%20contain%20a%20coax%20%28short,cable%20port%20which%20is%20located%20on%20a%20wall

Quick Review

- Broadband connections are high speed and always on
- Digital Subscriber Line (DSL) runs on top of a telephone service
- Cable runs through a modem supplied by your Internet Service Provider (ISP), or bought by the customer (often combined with a switch, router, WAP, and firewall)
- Satellites are handy for more remote locations
- Optical network terminals (ONTs) convert data to and from fiber light signals

Episode: **Firewalls and Servers**

Objective(s):

Core 1: 2.1 Compare and contrast Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports, protocols, and their purposes.

Core 1: 2.2 Compare and contrast common networking hardware.

Core 1: 2.4 Summarize services provided by networked hosts.

CompTIA A+ (220-110x)

Mike Meyers and Steve Nicholson

Episode Description

In this episode, Mike begins the discussion of Application-layer protocols. Starting with a review of the interaction between IP packets and servers, the episode analyzes the functions of local and server-based firewalls.

Key Terms

- 4:09 - Objective term - All web servers have a firewall
- 5:11 - Objective term - Home routers don't need to allow incoming port 80 (HTTP) or port 443 (HTTPS) traffic

Quick Review

- All Internet connections require a client and a server
- One of the primary functions of firewalls is to block ports
- Client and server networks use firewalls
- Firewalls block ports on an incoming vs. outgoing concept
- Servers must not block incoming ports on the ports to which they listen

Episode: **E-Mail**

Objective(s):

Core 1: 2.1 Compare and contrast Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports, protocols, and their purposes.

Core 1: 2.4 Summarize services provided by networked hosts.

Episode Description

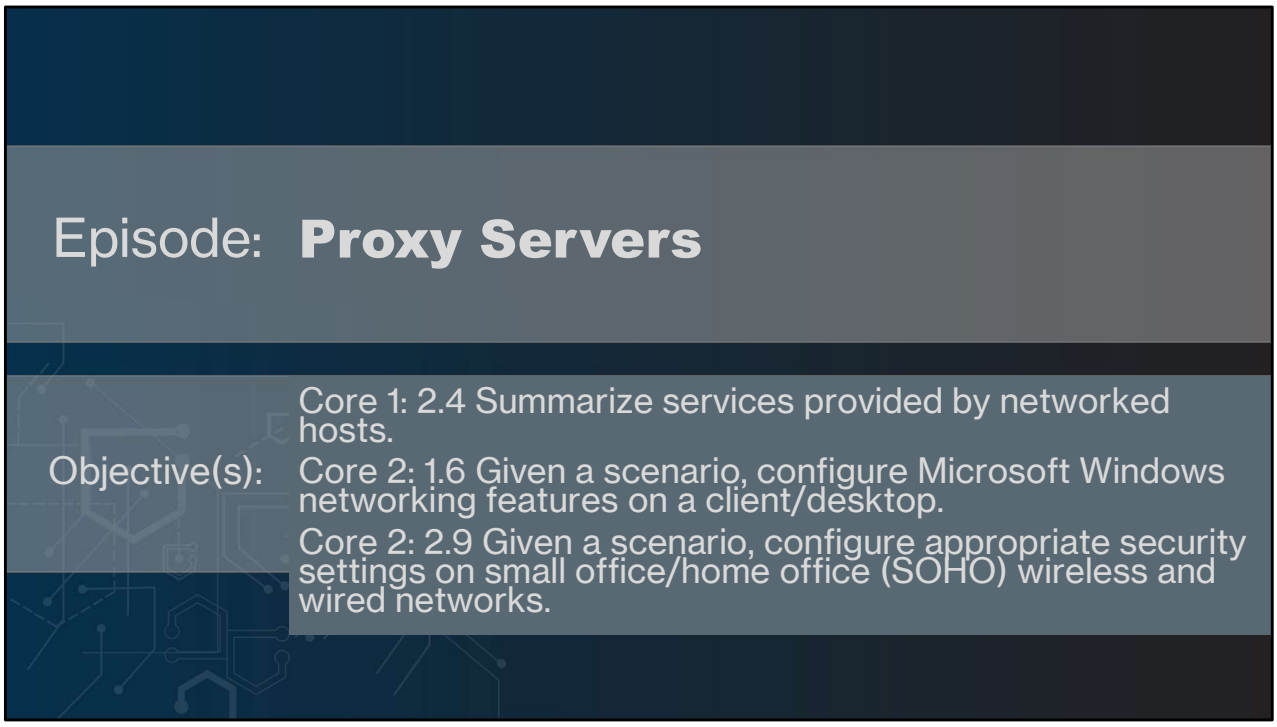
Continuing with the Application-layer protocols, this episode explores e-mail. Mike covers the three classic e-mail protocols, SMTP for sending and POP3 and IMAP4 for receiving. The episode covers typical client configuration using the classic protocols and port numbers.

Key Terms

- 0:38 - michaelm@totalsem.com
- 1:26 - Objective term - Simple Mail Transfer Protocol (SMTP) - port 25
- 1:26 - Objective term - Post Office Protocol 3 (POP3) - port 110
- 1:26 - Objective term - Internet Message Access Protocol (IMAP) - port 143
- 2:48 - POP3, IMAP4
- 4:36 - Objective term - The outgoing mail server will always be SMTP

Quick Review

- E-mail uses Simple Mail Transfer Protocol (SMTP) to send e-mail from a client to an e-mail server
- Use Post Office Protocol v3 (POP3) or Internet Message Access Protocol (IMAP) to pull e-mail down from an e-mail server
- SMTP uses TCP port 25; POP3 uses TCP port 110; IMAP uses port 143
- Setting up an e-mail account requires knowledge of the IP addresses or DNS name for the different servers


Episode: Proxy Servers
Objective(s):
Core 1: 2.4 Summarize services provided by networked hosts.
Core 2: 1.6 Given a scenario, configure Microsoft Windows networking features on a client/desktop.
Core 2: 2.9 Given a scenario, configure appropriate security settings on small office/home office (SOHO) wireless and wired networks.

Episode Description

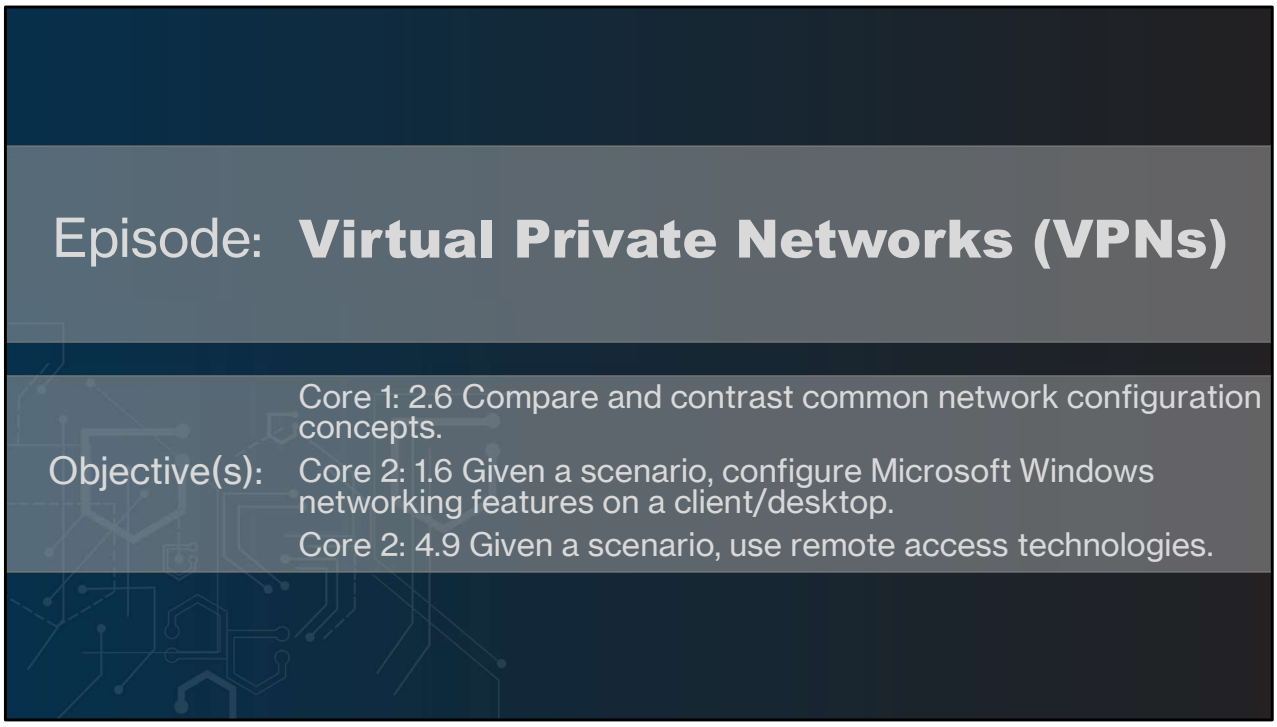
In this episode, Mike describes how proxy servers work to block certain web sites and filter outgoing or incoming content. The episode shows how to set up a browser to connect to a proxy server.

Key Terms

- 0:28 - Objective term - Proxy server
- 1:31 - Objective term - Proxy servers can filter like firewalls (based on web addresses, IP addresses, ports, etc.)
- 2:01 - Objective term - Proxy servers can also filter based on restricted content
- 2:39 - Objective term - Proxy settings
- 4:56 - Proxy servers can do caching

Quick Review

- A proxy server acts as a go-between (a proxy) between a client and a server
- Proxy servers are application-specific (e.g., a web proxy for HTTP and HTTPS)
- Proxy servers can provide firewalling, check for malware, and ban bad URLs
- Applications must know the address of the proxy server



CompTIA A+ (220-110x)

Mike Meyers and Steve Nicholson

Episode Description

In this episode, Mike shows how virtual private networking (VPN) work and why people use VPN connections. He discusses the types of protocols and clients that make this work today and walks through a generic VPN setup.

Key Terms

- 0:45 - Objective term - Virtual Private Network (VPN)
- 2:50 - VPN tunnel
- 3:51 - Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), IP security (IPsec)
- 7:21 - Split tunneling

Quick Review

- Virtual Private Networks (VPNs) use the Internet to create a private connection to a remote network
- We need a VPN client program that connects to a VPN server/endpoint at the remote network
- The VPN client needs to know the IP address of the VPN server to make the connection

Episode: **Internet of Things (IoT)**

Objective(s):
- Core 1: 2.3 Compare and contrast protocols for wireless networking.
- Core 1: 2.4 Summarize services provided by networked hosts.
- Core 2: 2.7 Explain common methods for securing mobile and embedded devices.

CompTIA A+ (220-110x)
Mike Meyers and Steve Nicholson

Episode Description

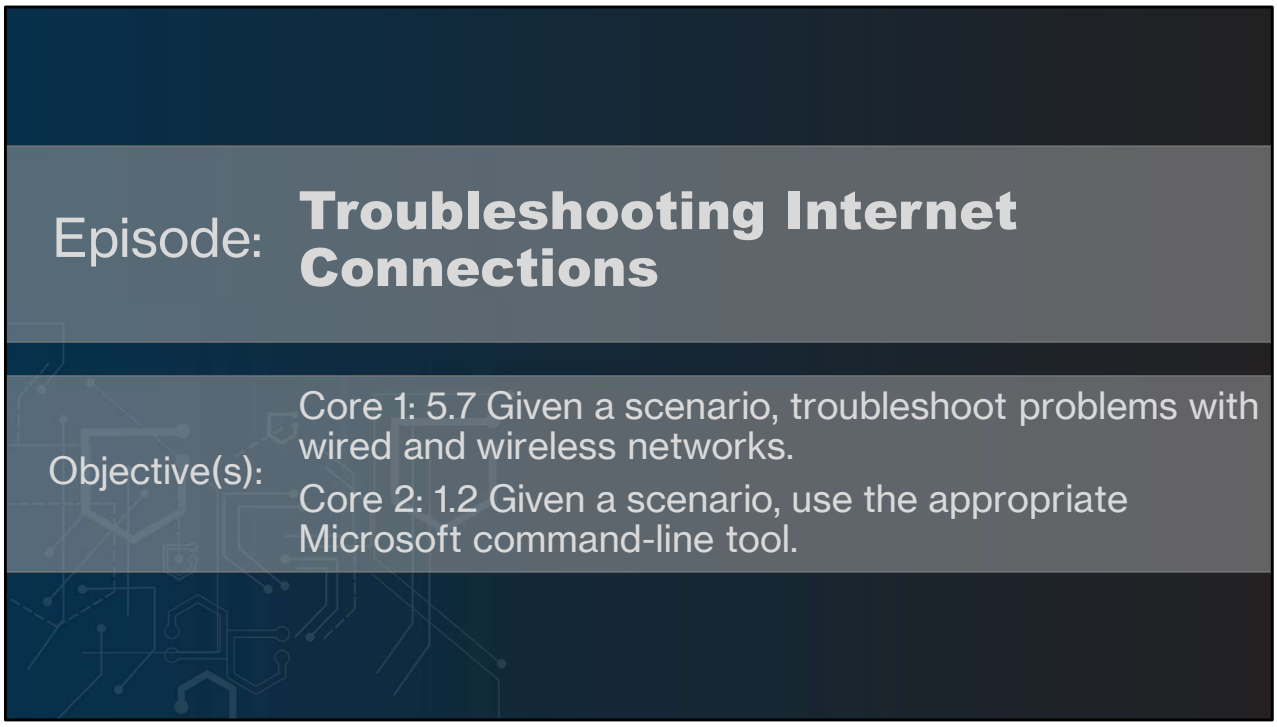
Mike explores some of the latest and greatest networking technologies with the Internet of Things (IoT). He describes the three common wireless technologies used to connect to IoT devices, 802.11, Zigbee, and Z-wave. Mike finishes with a discussion and demonstration of typical IoT set ups and configurations.

Key Terms

- 0:14 - Objective term - Internet of Things (IoT)
- 0:28 - Objective term - IoT devices like: Thermostats, light bulbs, refrigerators, hot water heaters, door locks, garage door openers, and more!
- 1:23 - Objective term - 802.11
- 1:25 - Zigbee
- 1:48 - Z-Wave

Quick Review

- Internet of Things (IoT) means giving Internet capability to devices not traditionally associated with the Internet (light bulbs, thermostats, refrigerators, etc.)
- The most common IoT connections are 802.11, Zigbee, and Z-wave
- IoT requires a hub to link to the IoT devices
- Google Home, Amazon Alexa, and Apple Siri add voice capabilities to IoT


Episode:
Troubleshooting Internet Connections
Objective(s):
Core 1: 5.7 Given a scenario, troubleshoot problems with wired and wireless networks.
Core 2: 1.2 Given a scenario, use the appropriate Microsoft command-line tool.

Episode Description

A+

The CompTIA A+ exams have many network troubleshooting scenario questions. The Great Mikestrami gives you a few rules to help you get through these questions. In addition, a few basic tools and preparation makes troubleshooting most problems easy if not trivial.

CompTIA

Key Terms

- 0:46 - Check your physical system first (link lights, cabling, ports, etc.)
- 1:07 - Know your network!
- 1:23 - ipconfig /all
- 2:09 - Know your Internet connectivity!
- 2:29 - Traceroute
- 2:37 - Windows: tracert, Linux/Mac: traceroute
- 5:00 - ping

Quick Review

- For network troubleshooting, check physical connectivity first
- Run ipconfig /all from the CLI to get important network information
- Run traceroute (Windows) or tracert (Linux/mac) to test Internet connectivity before you have problems
- Run ping to test connection between two systems (plus DNS)