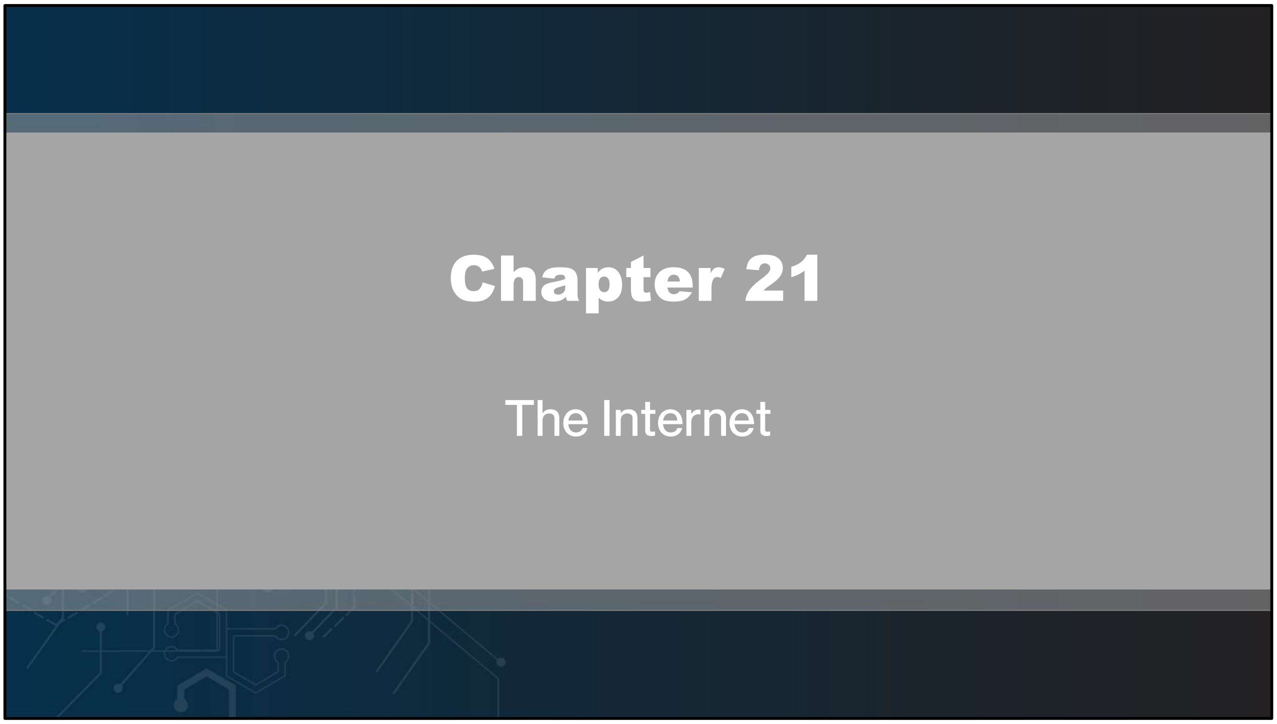
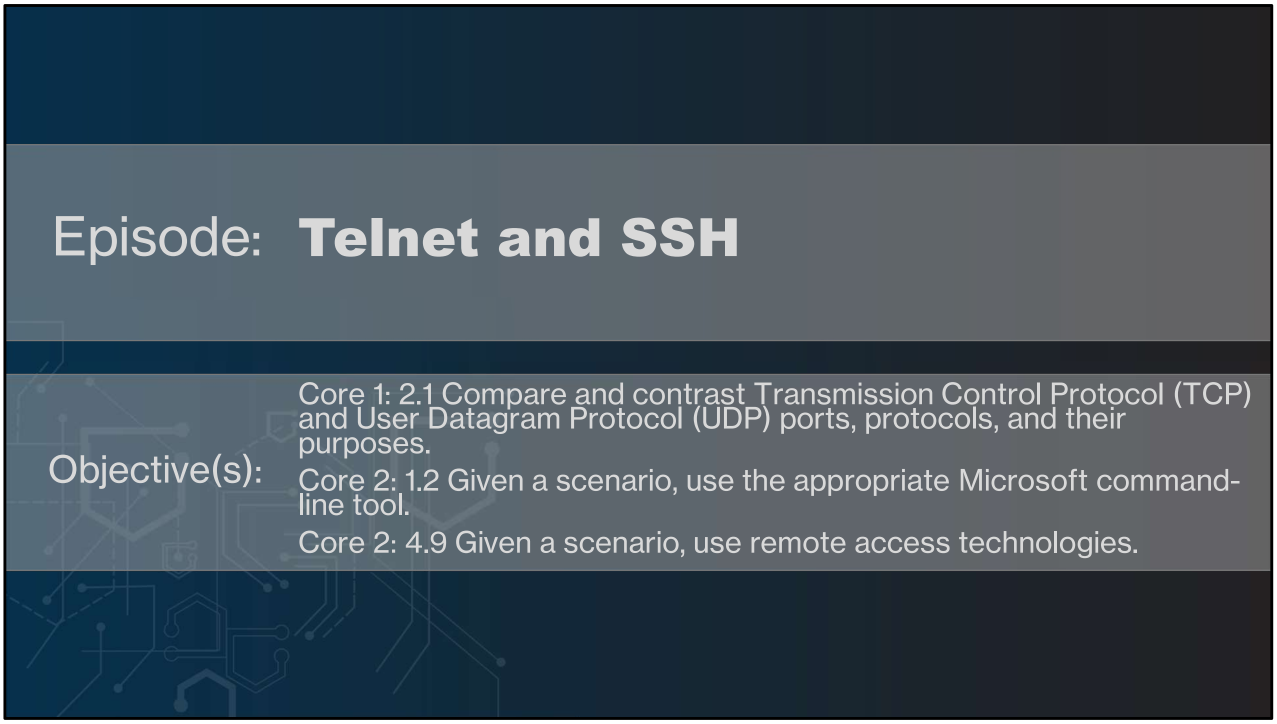


Chapter 21

The Internet



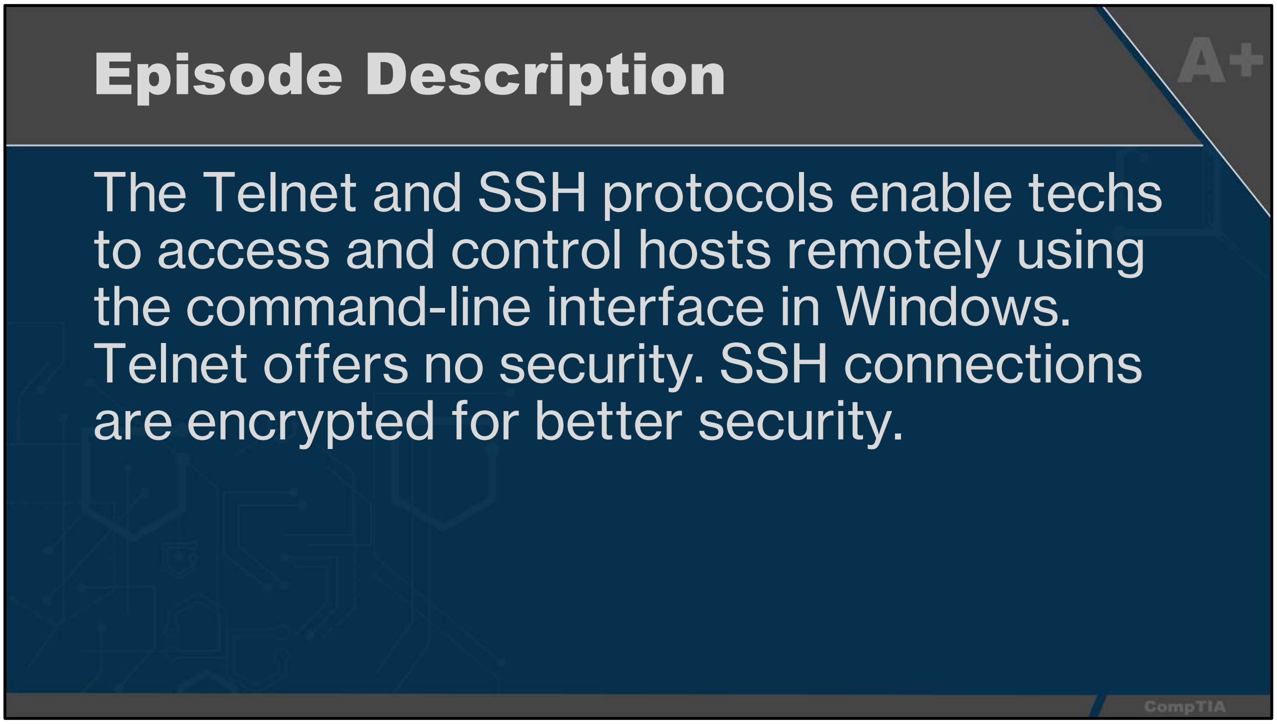
Episode: **Telnet and SSH**

Objective(s):

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

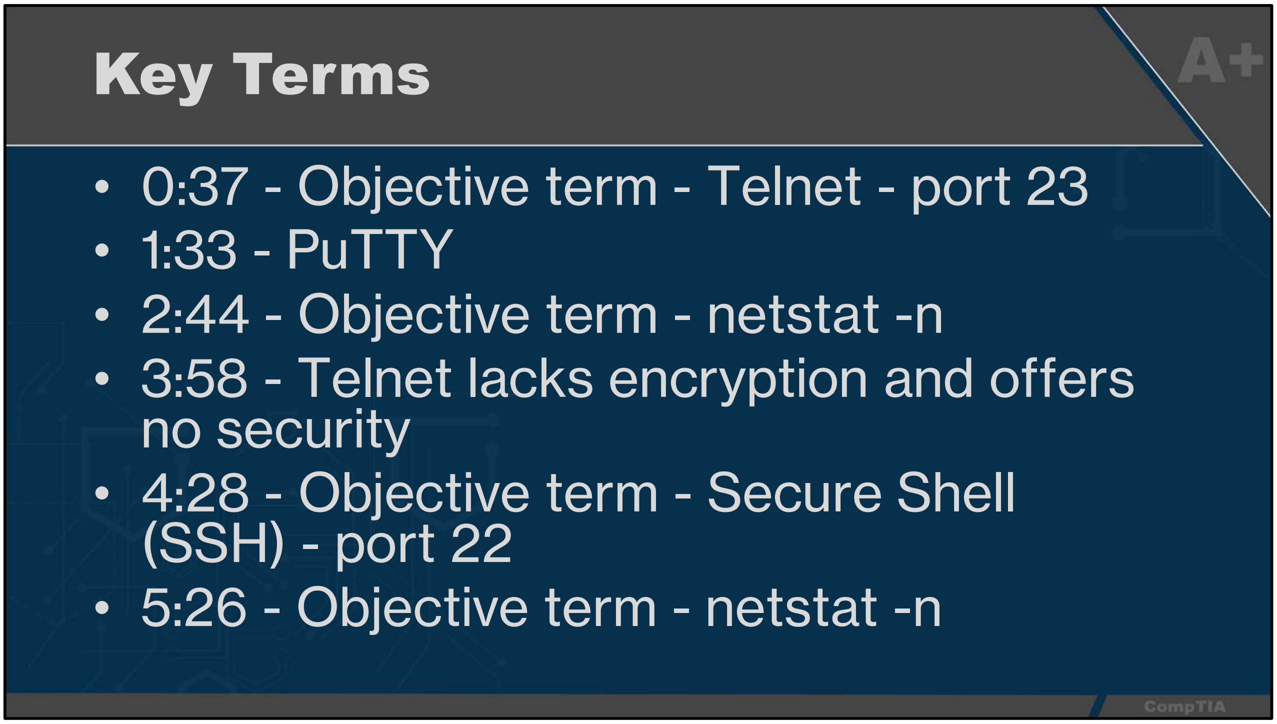
Core 2: 1.2 Given a scenario, use the appropriate Microsoft command-line tool.

Core 2: 4.9 Given a scenario, use remote access technologies.



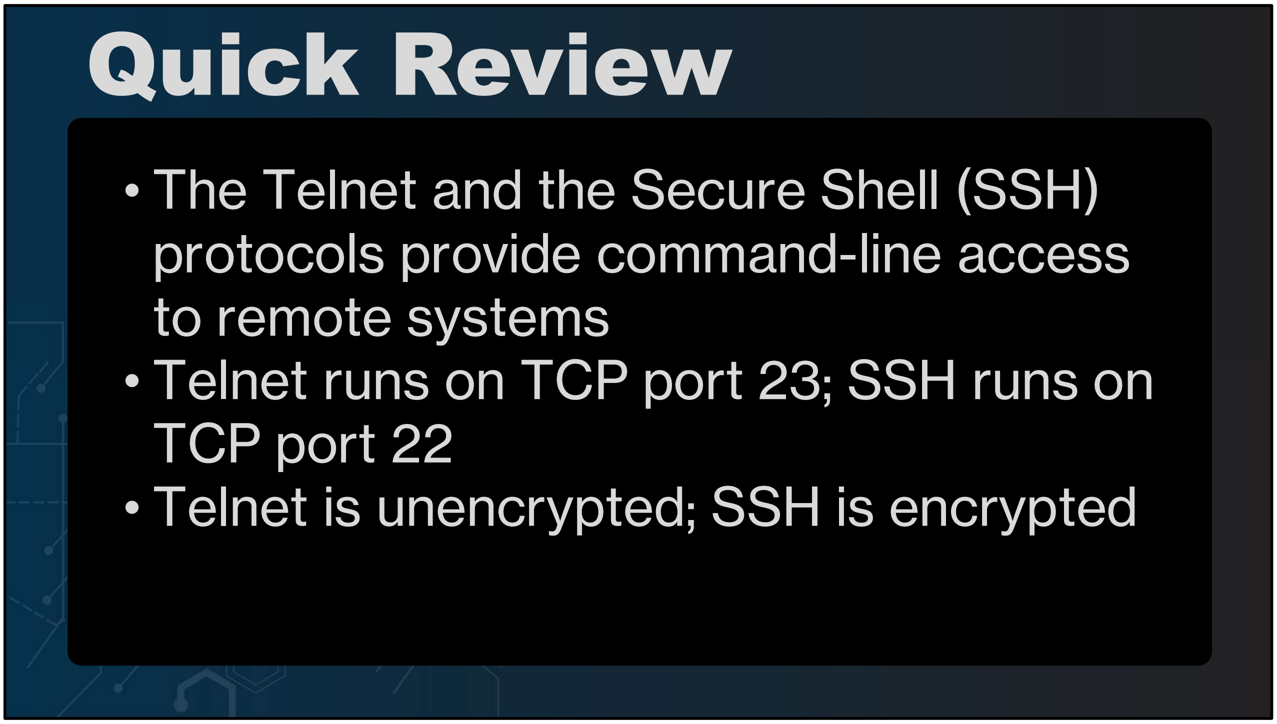
Episode Description

The Telnet and SSH protocols enable techs to access and control hosts remotely using the command-line interface in Windows. Telnet offers no security. SSH connections are encrypted for better security.



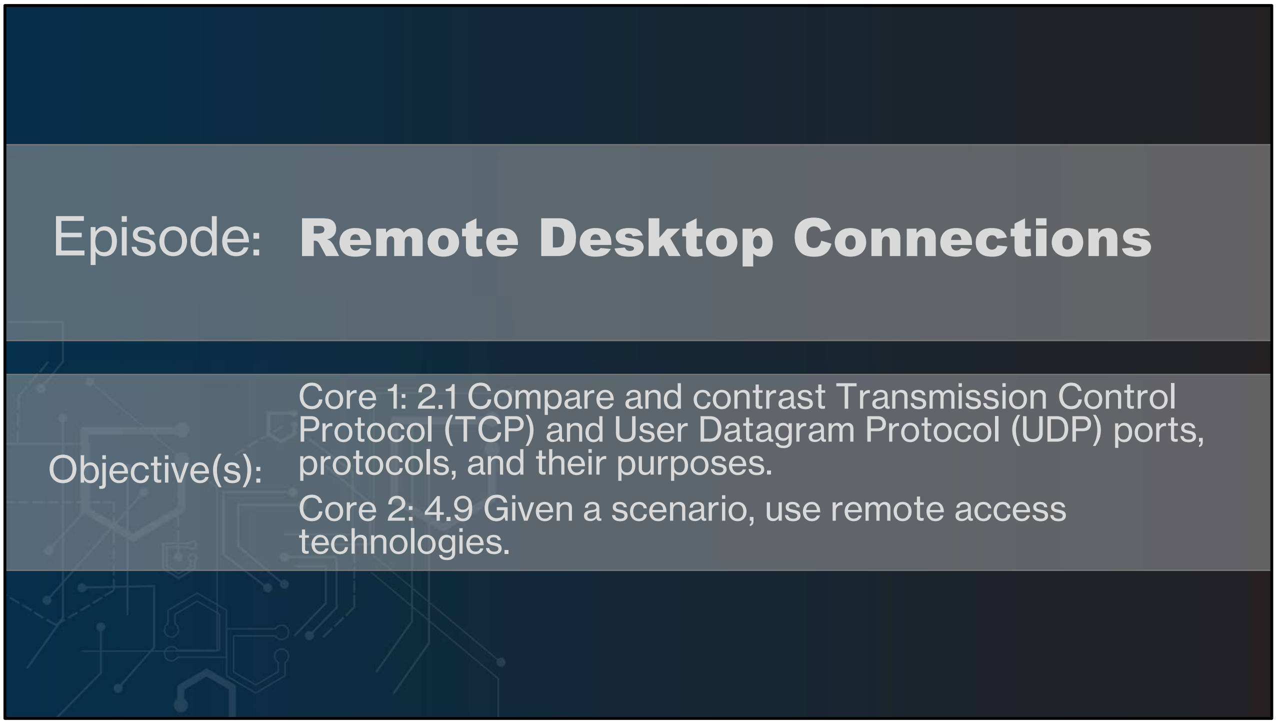
Key Terms

- 0:37 - Objective term - Telnet - port 23
- 1:33 - PuTTY
- 2:44 - Objective term - netstat -n
- 3:58 - Telnet lacks encryption and offers no security
- 4:28 - Objective term - Secure Shell (SSH) - port 22
- 5:26 - Objective term - netstat -n



Quick Review

- The Telnet and the Secure Shell (SSH) protocols provide command-line access to remote systems
- Telnet runs on TCP port 23; SSH runs on TCP port 22
- Telnet is unencrypted; SSH is encrypted

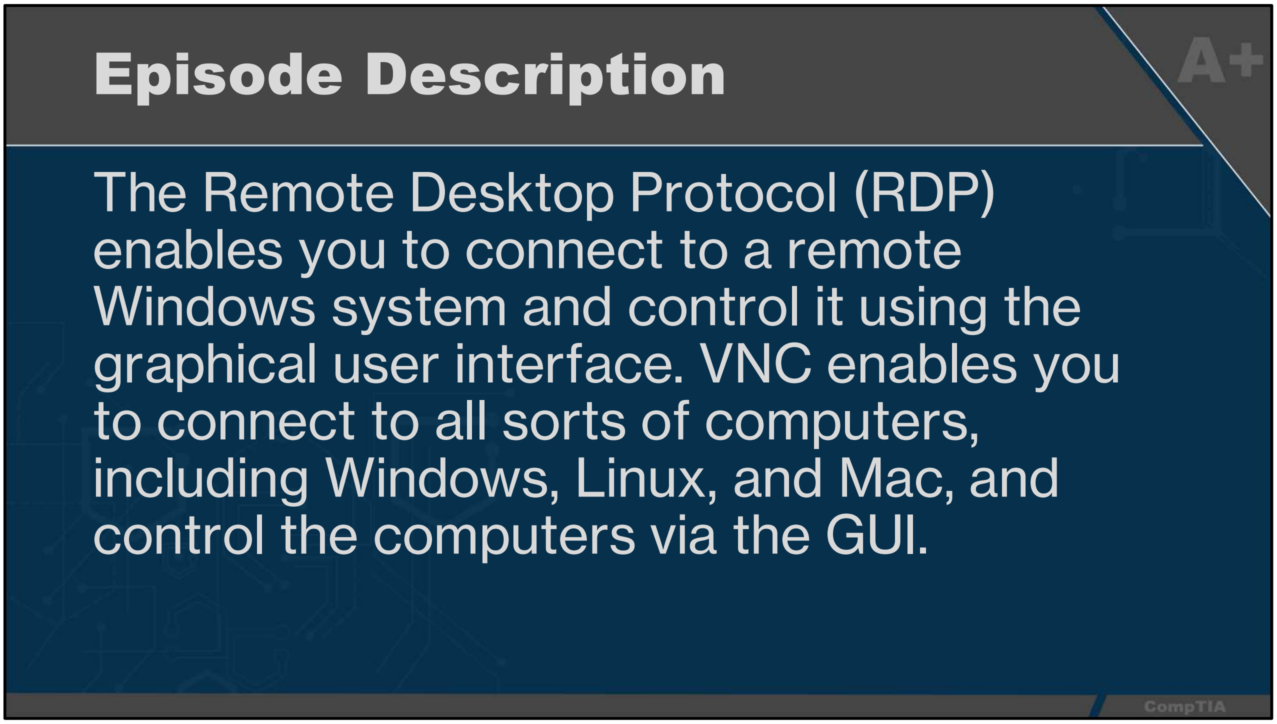


Episode: **Remote Desktop Connections**

Objective(s):

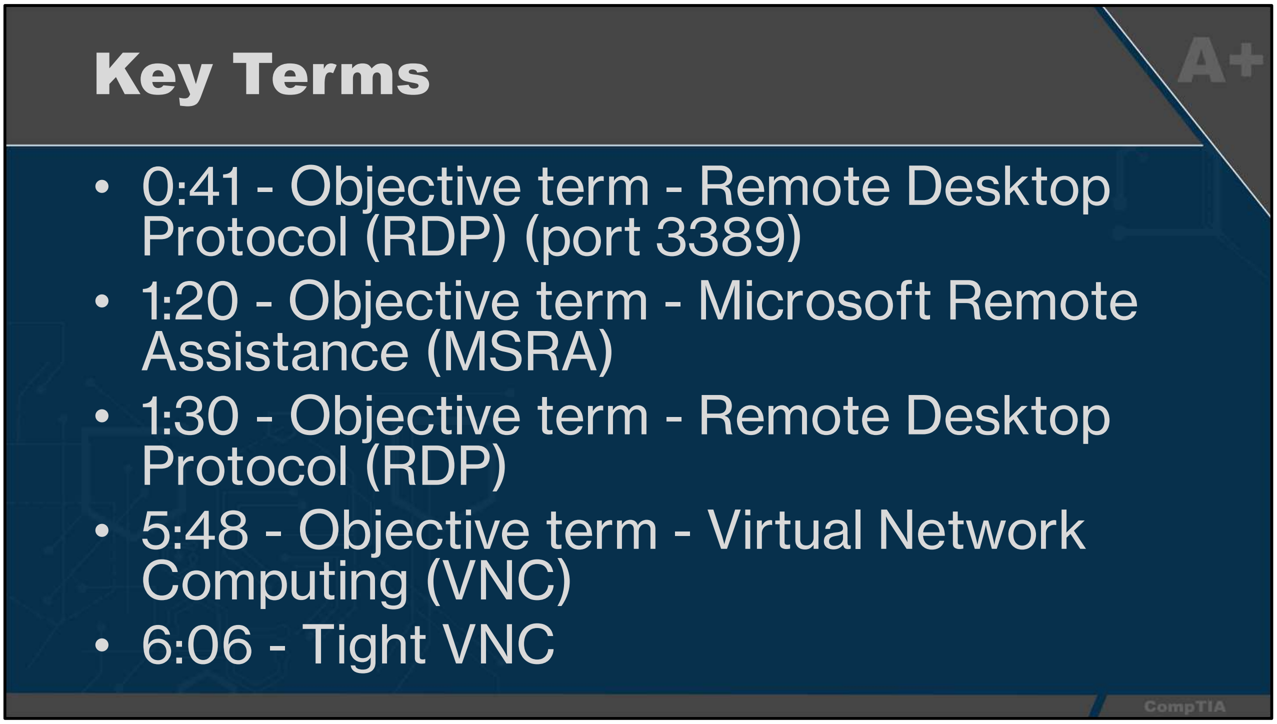
Core 1: 2.1 Compare and contrast Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports, protocols, and their purposes.

Core 2: 4.9 Given a scenario, use remote access technologies.



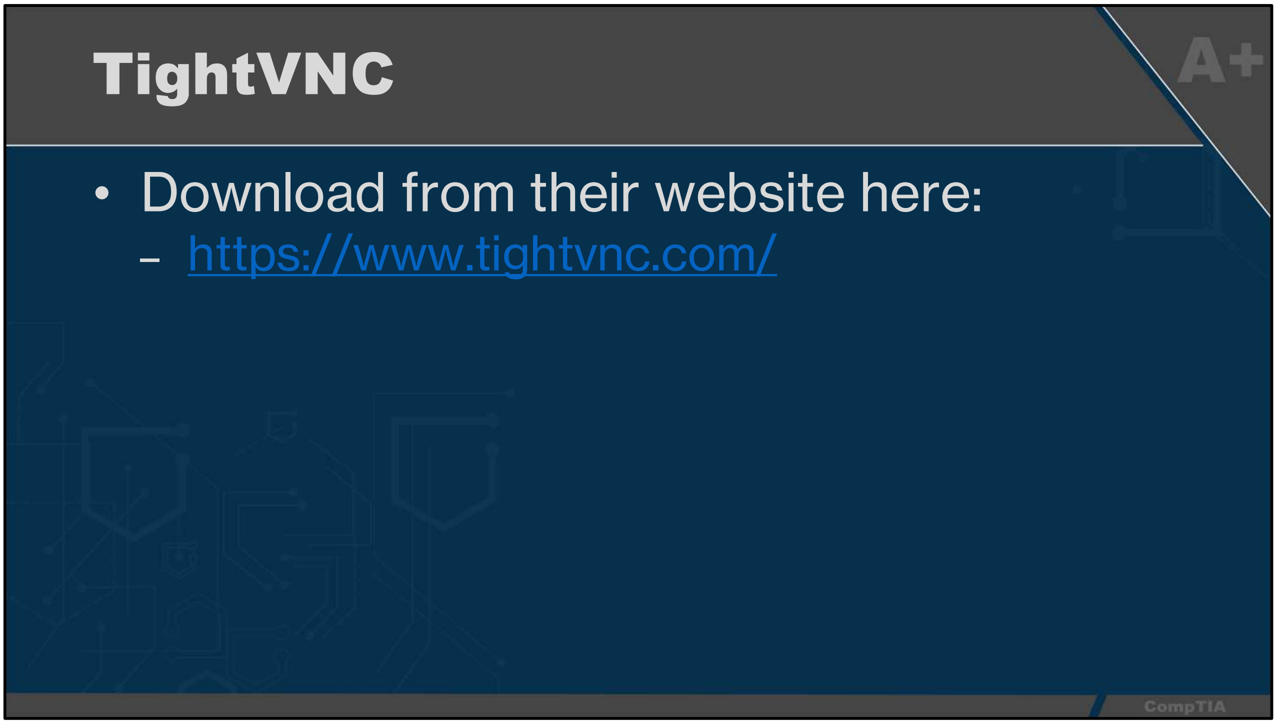
Episode Description

The Remote Desktop Protocol (RDP) enables you to connect to a remote Windows system and control it using the graphical user interface. VNC enables you to connect to all sorts of computers, including Windows, Linux, and Mac, and control the computers via the GUI.



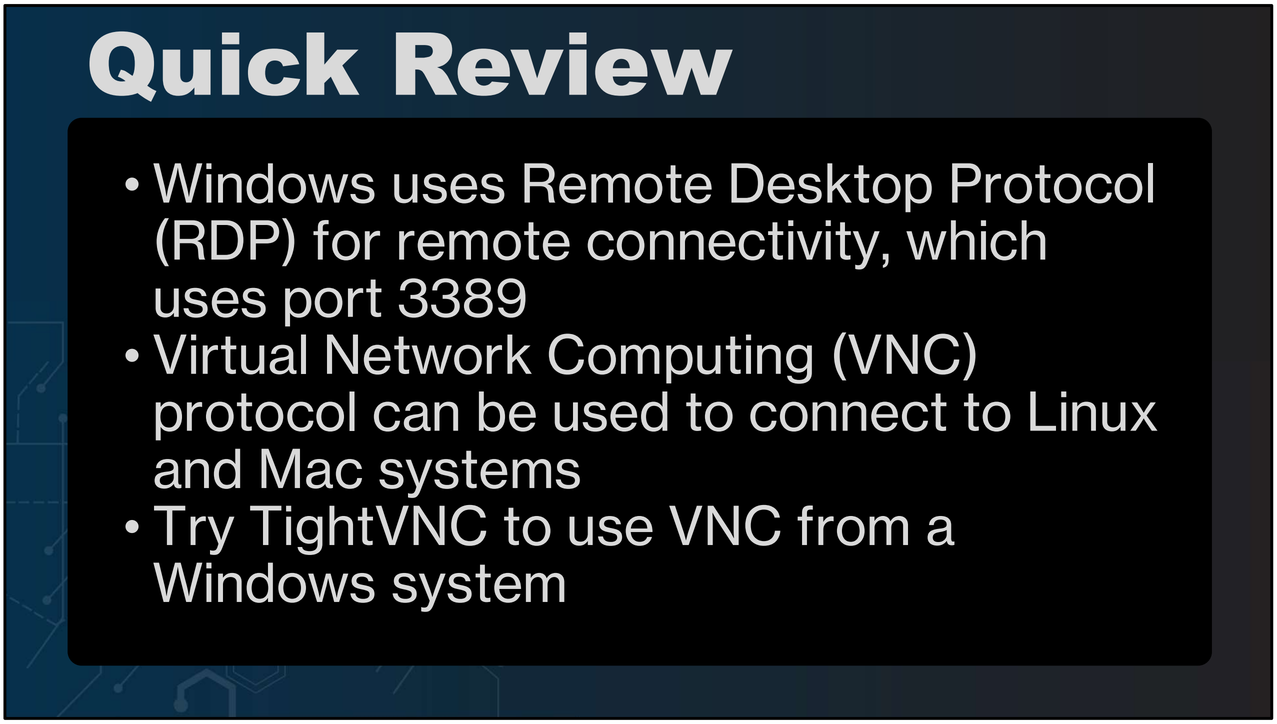
Key Terms

- 0:41 - Objective term - Remote Desktop Protocol (RDP) (port 3389)
- 1:20 - Objective term - Microsoft Remote Assistance (MSRA)
- 1:30 - Objective term - Remote Desktop Protocol (RDP)
- 5:48 - Objective term - Virtual Network Computing (VNC)
- 6:06 - Tight VNC



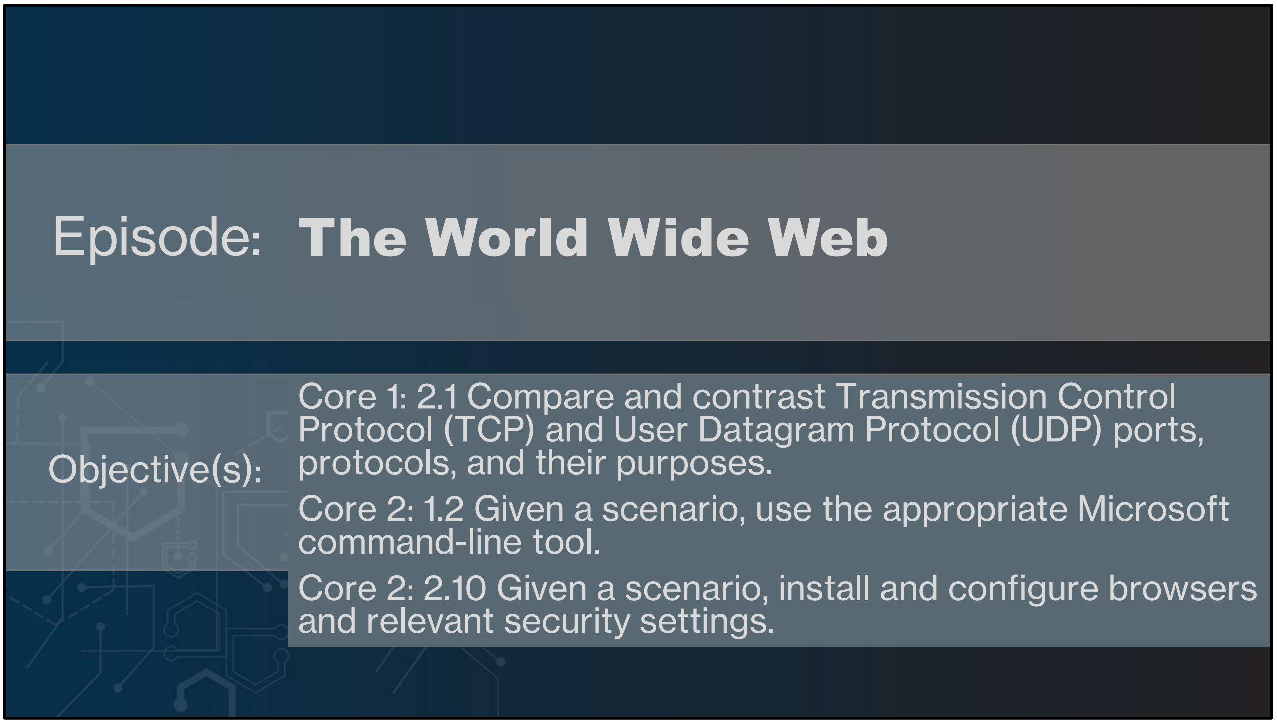
TightVNC

- Download from their website here:
  - https://www.tightvnc.com/



Quick Review

- Windows uses Remote Desktop Protocol (RDP) for remote connectivity, which uses port 3389
- Virtual Network Computing (VNC) protocol can be used to connect to Linux and Mac systems
- Try TightVNC to use VNC from a Windows system



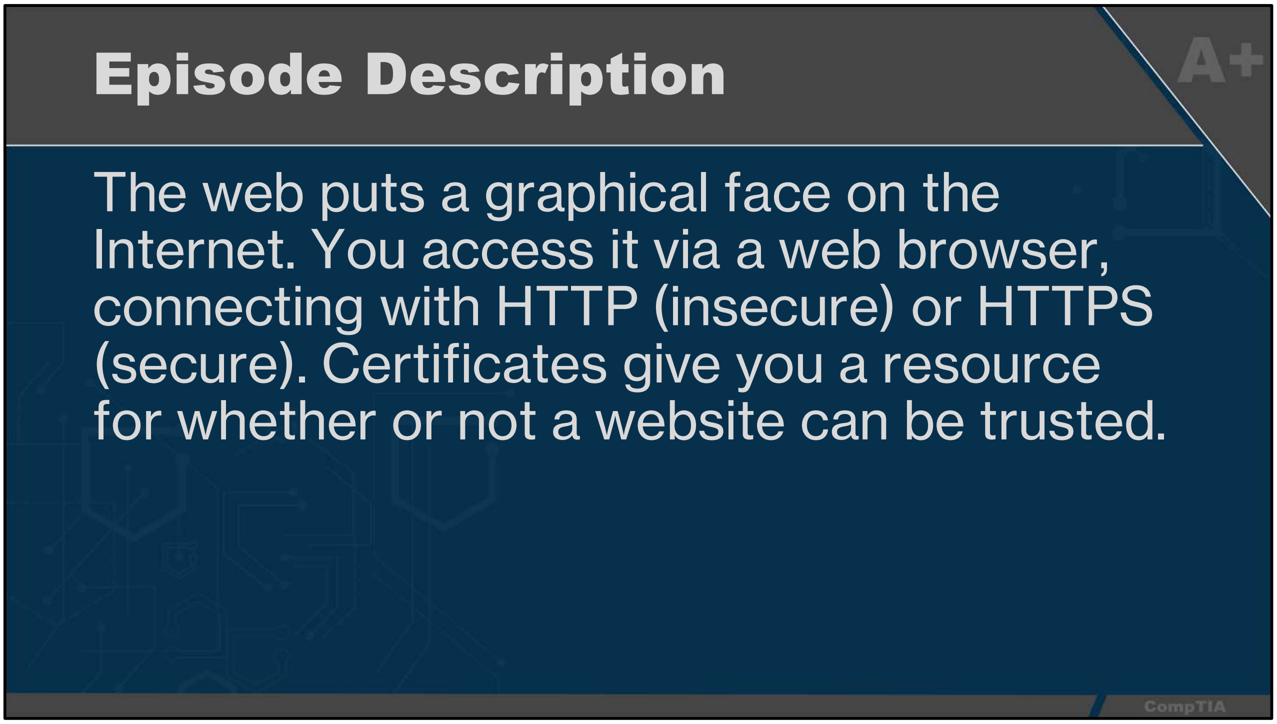
Episode: **The World Wide Web**

Objective(s):

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

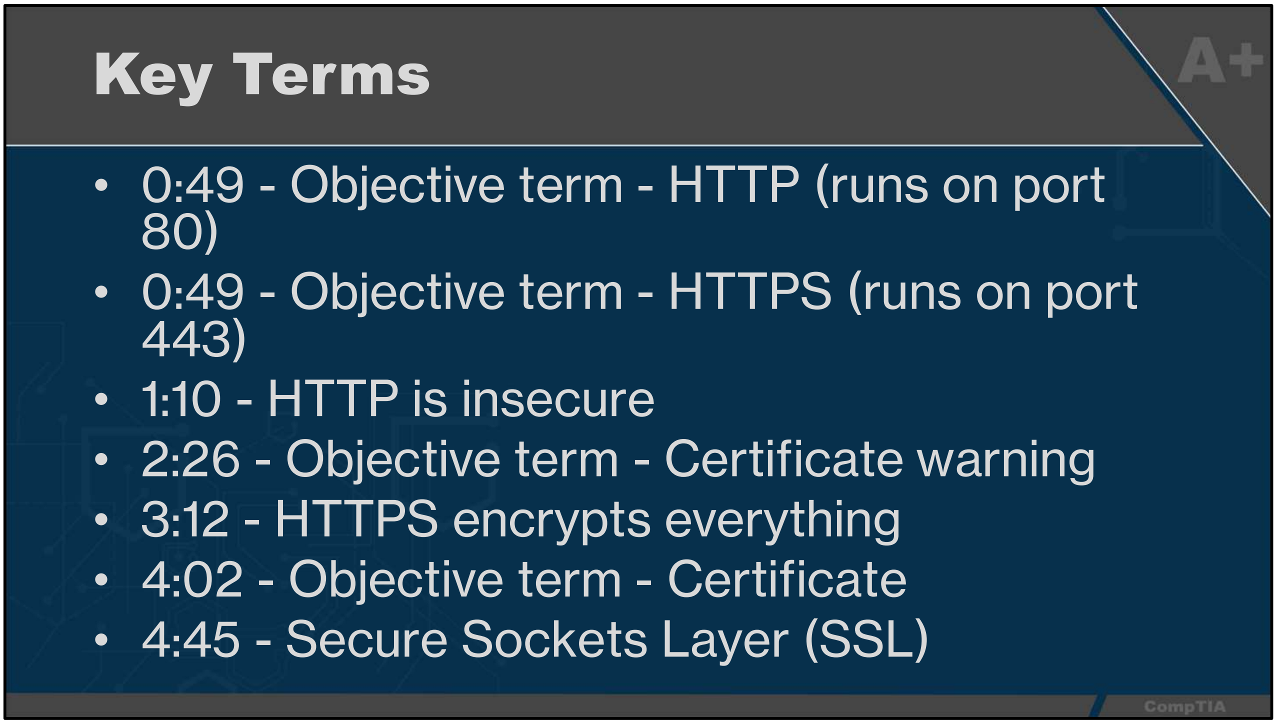
Core 2: 1.2 Given a scenario, use the appropriate Microsoft command-line tool.

Core 2: 2.10 Given a scenario, install and configure browsers and relevant security settings.



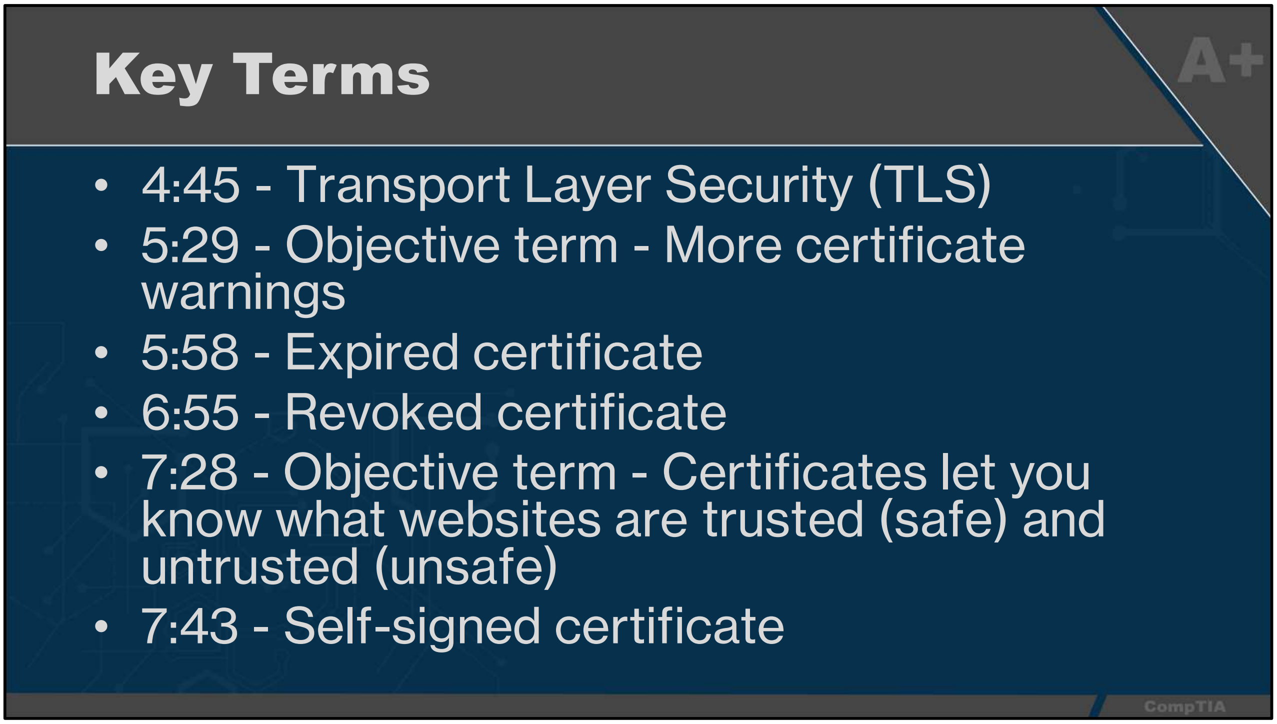
Episode Description

The web puts a graphical face on the Internet. You access it via a web browser, connecting with HTTP (insecure) or HTTPS (secure). Certificates give you a resource for whether or not a website can be trusted.



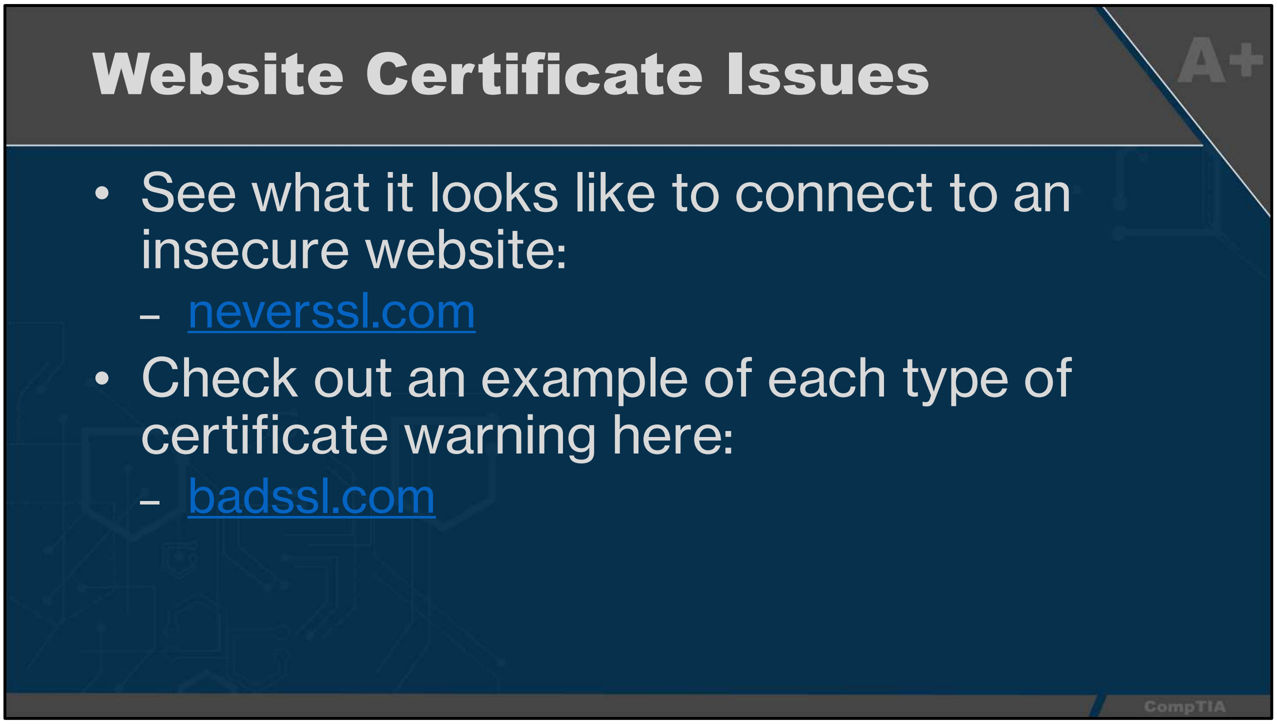
Key Terms

- 0:49 - Objective term - HTTP (runs on port 80)
- 0:49 - Objective term - HTTPS (runs on port 443)
- 1:10 - HTTP is insecure
- 2:26 - Objective term - Certificate warning
- 3:12 - HTTPS encrypts everything
- 4:02 - Objective term - Certificate
- 4:45 - Secure Sockets Layer (SSL)



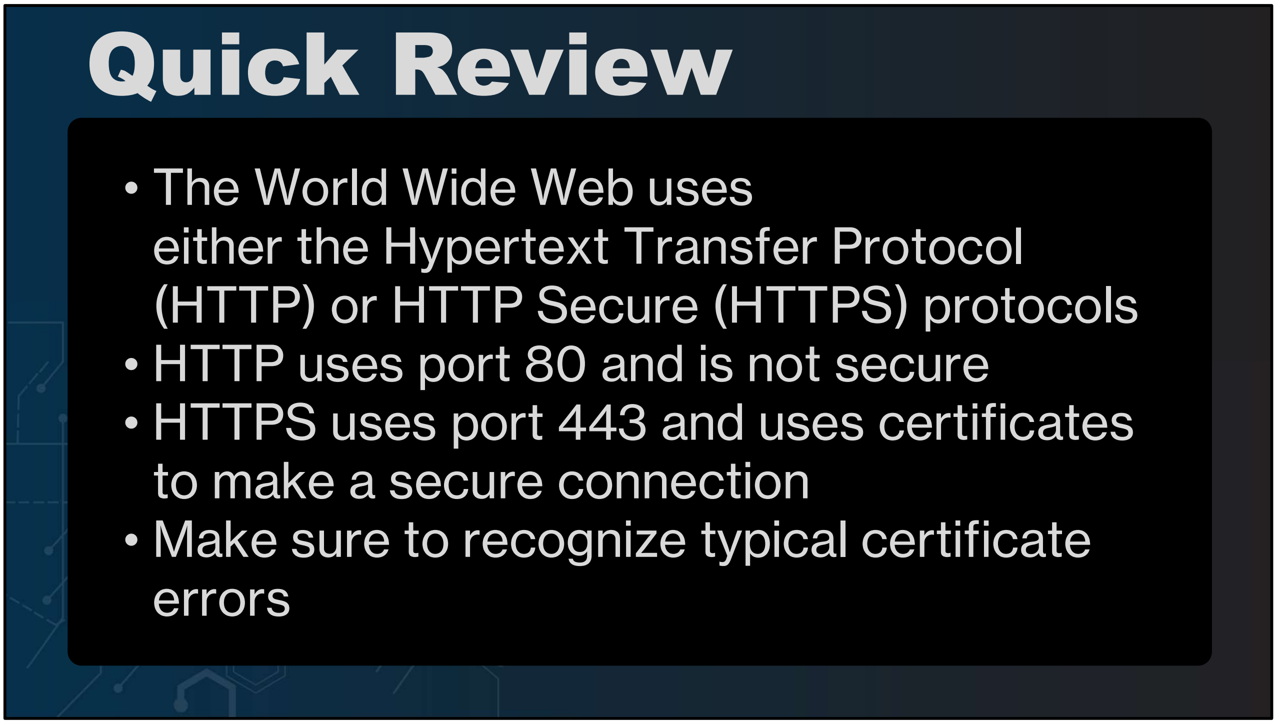
Key Terms

- 4:45 - Transport Layer Security (TLS)
- 5:29 - Objective term - More certificate warnings
- 5:58 - Expired certificate
- 6:55 - Revoked certificate
- 7:28 - Objective term - Certificates let you know what websites are trusted (safe) and untrusted (unsafe)
- 7:43 - Self-signed certificate



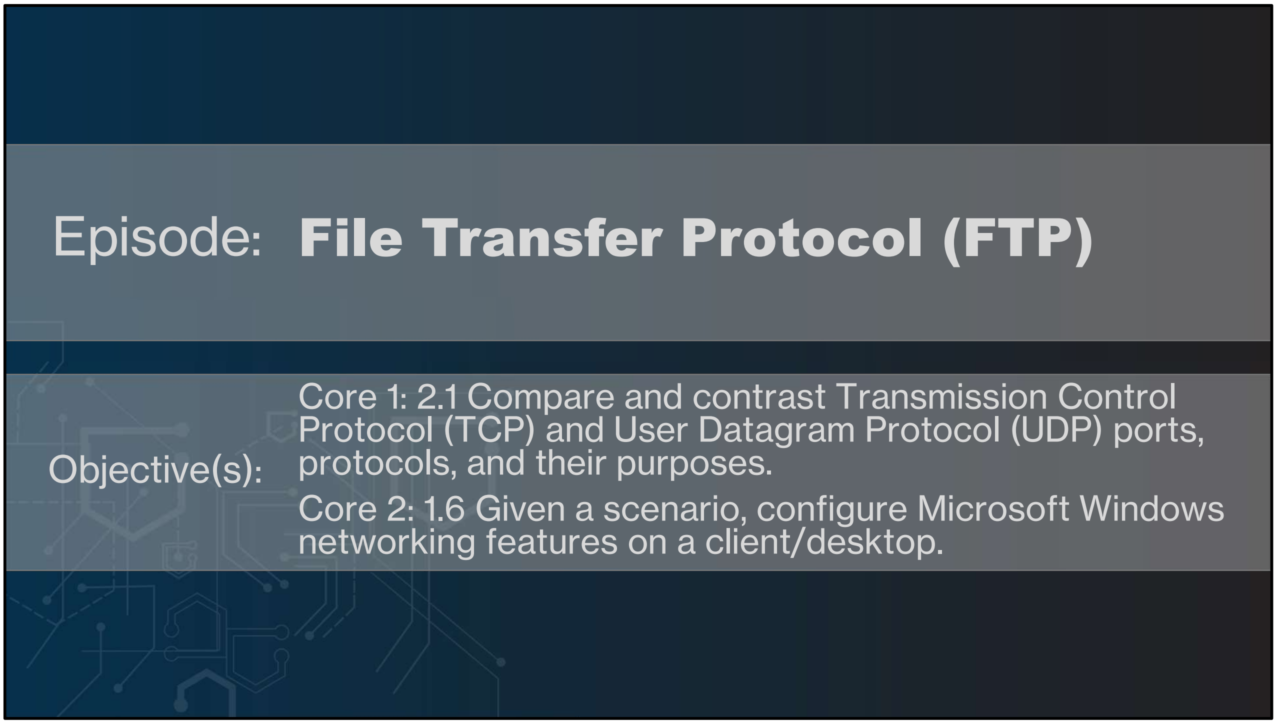
Website Certificate Issues

- See what it looks like to connect to an insecure website:
  - neverssl.com
- Check out an example of each type of certificate warning here:
  - badssl.com



Quick Review

- The World Wide Web uses either the Hypertext Transfer Protocol (HTTP) or HTTP Secure (HTTPS) protocols
- HTTP uses port 80 and is not secure
- HTTPS uses port 443 and uses certificates to make a secure connection
- Make sure to recognize typical certificate errors

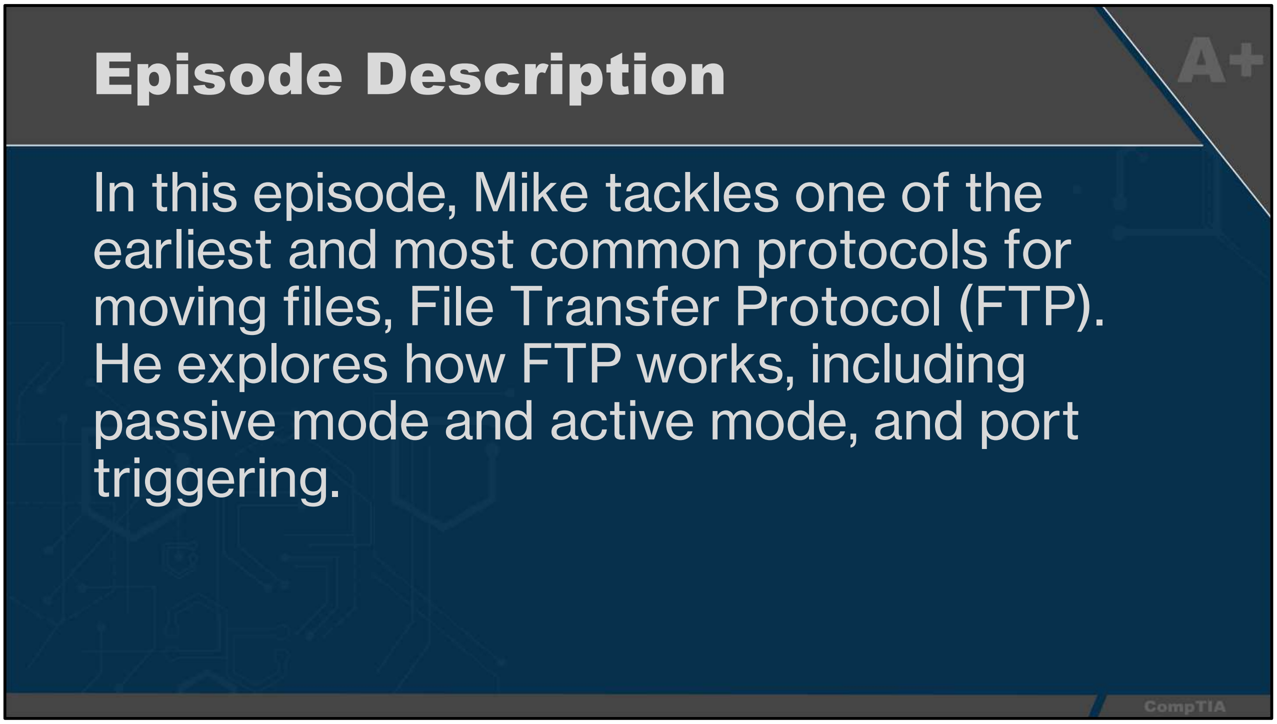


Episode: **File Transfer Protocol (FTP)**

Objective(s):

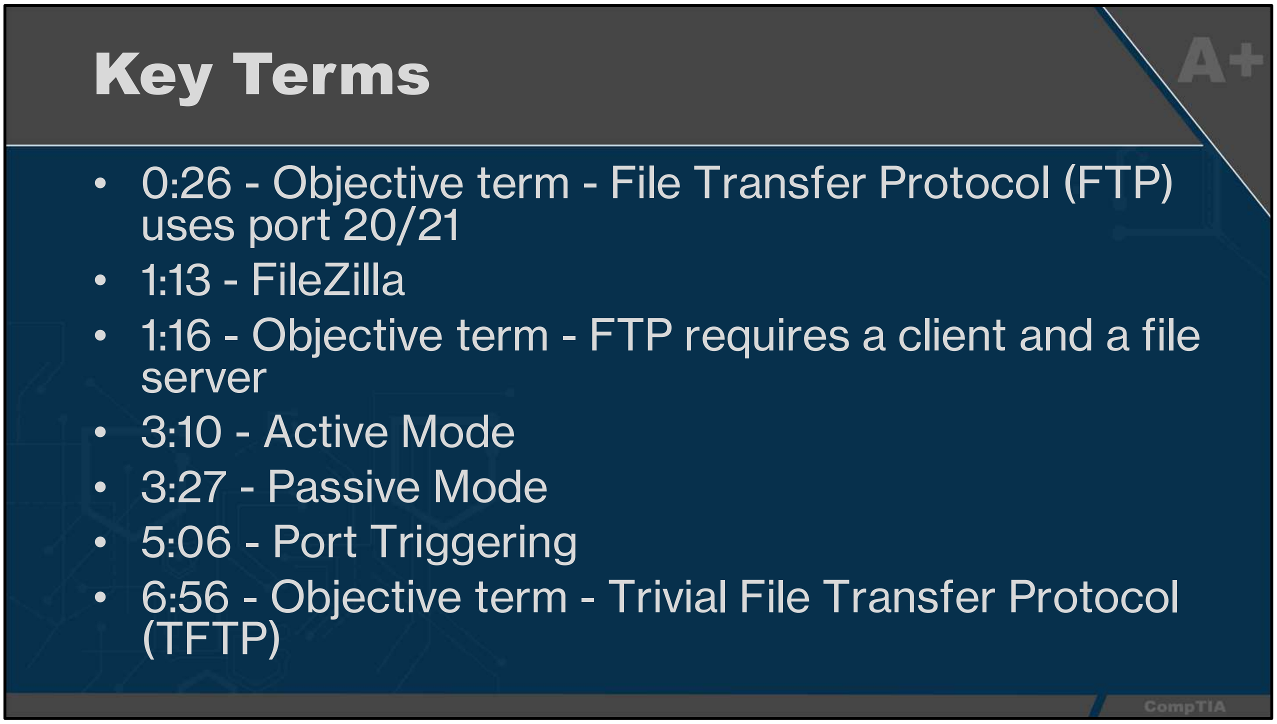
Core 1: 2.1 Compare and contrast Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports, protocols, and their purposes.

Core 2: 1.6 Given a scenario, configure Microsoft Windows networking features on a client/desktop.



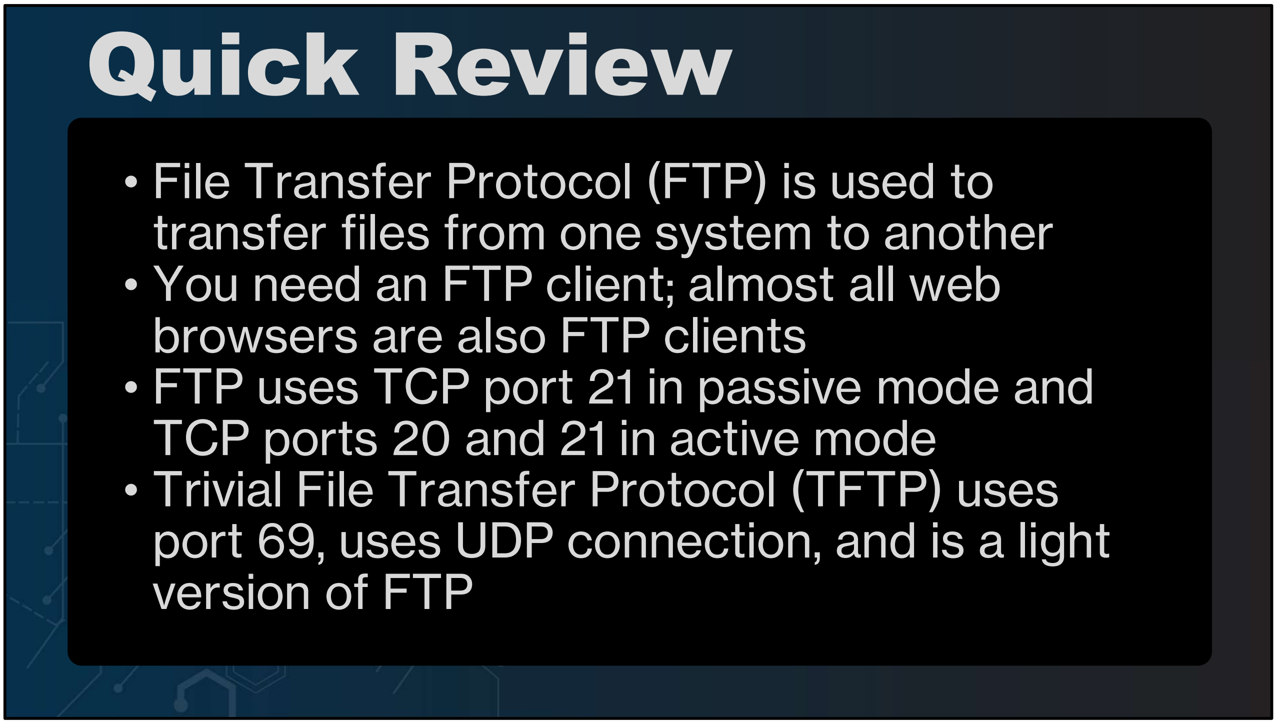
Episode Description

In this episode, Mike tackles one of the earliest and most common protocols for moving files, File Transfer Protocol (FTP). He explores how FTP works, including passive mode and active mode, and port triggering.



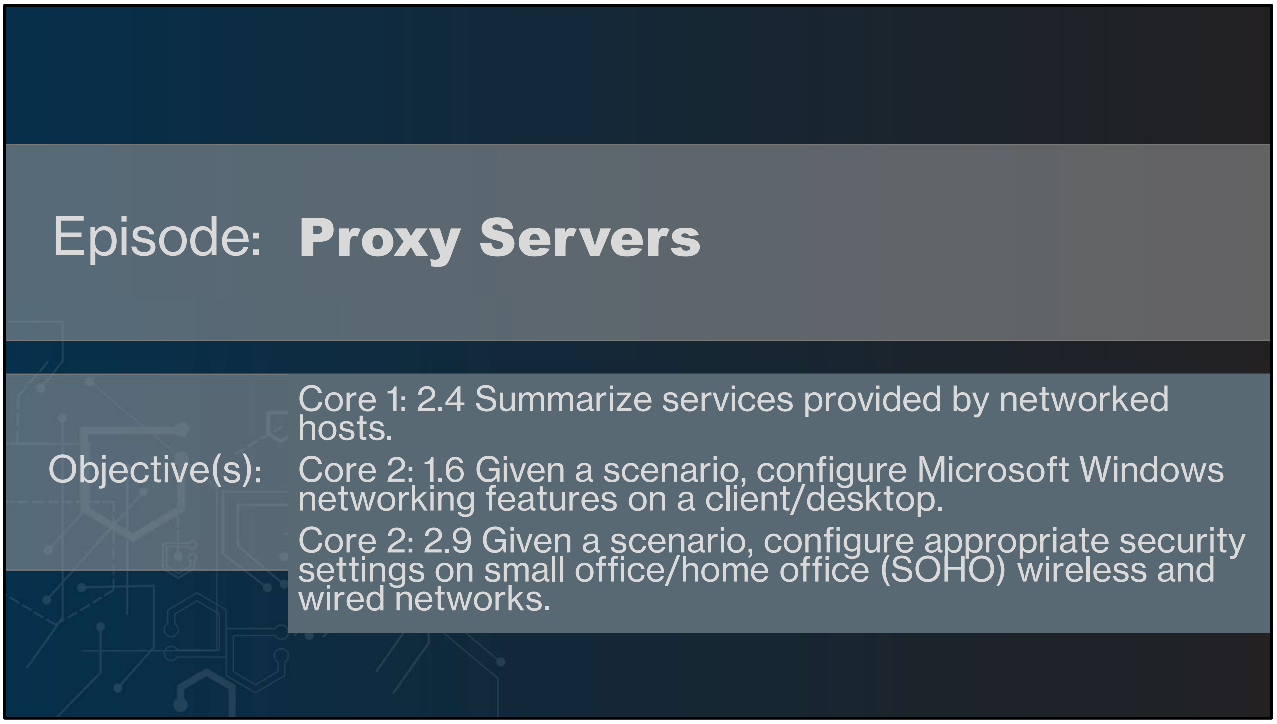
Key Terms

- 0:26 - Objective term - File Transfer Protocol (FTP) uses port 20/21
- 1:13 - FileZilla
- 1:16 - Objective term - FTP requires a client and a file server
- 3:10 - Active Mode
- 3:27 - Passive Mode
- 5:06 - Port Triggering
- 6:56 - Objective term - Trivial File Transfer Protocol (TFTP)



Quick Review

- File Transfer Protocol (FTP) is used to transfer files from one system to another
- You need an FTP client; almost all web browsers are also FTP clients
- FTP uses TCP port 21 in passive mode and TCP ports 20 and 21 in active mode
- Trivial File Transfer Protocol (TFTP) uses port 69, uses UDP connection, and is a light version of FTP



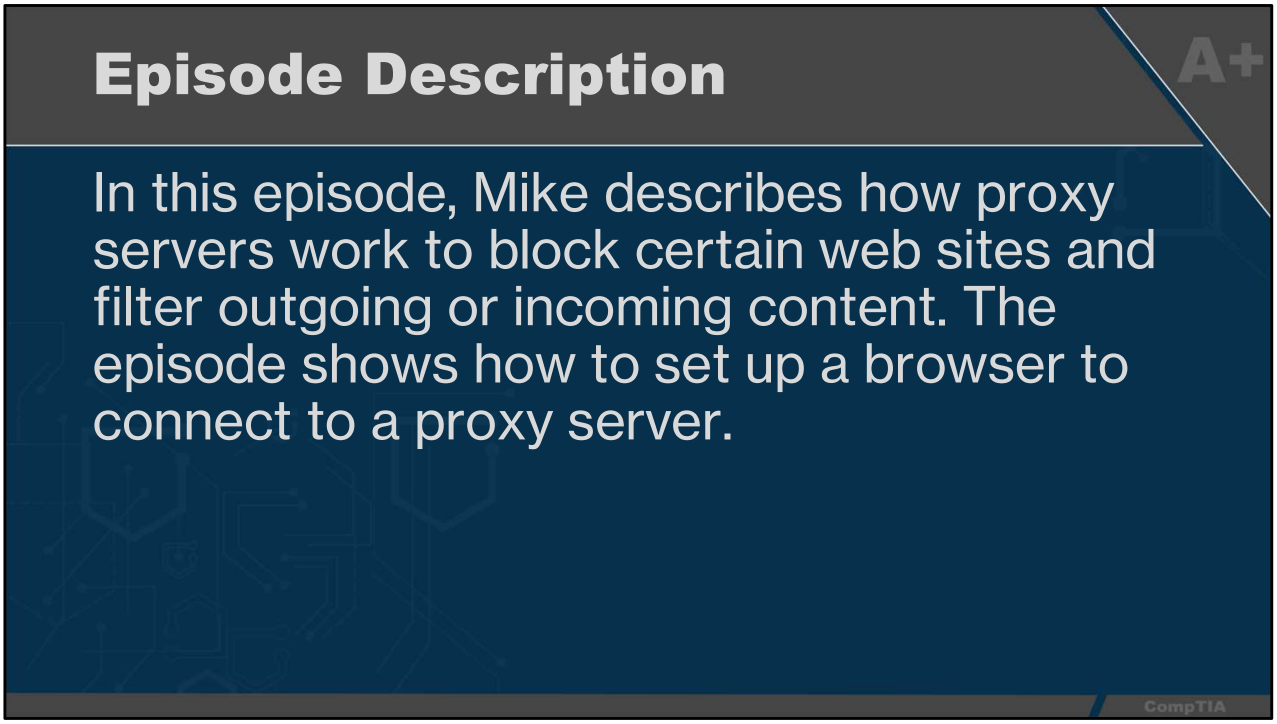
Episode: **Proxy Servers**

Objective(s):

Core 1: 2.4 Summarize services provided by networked hosts.

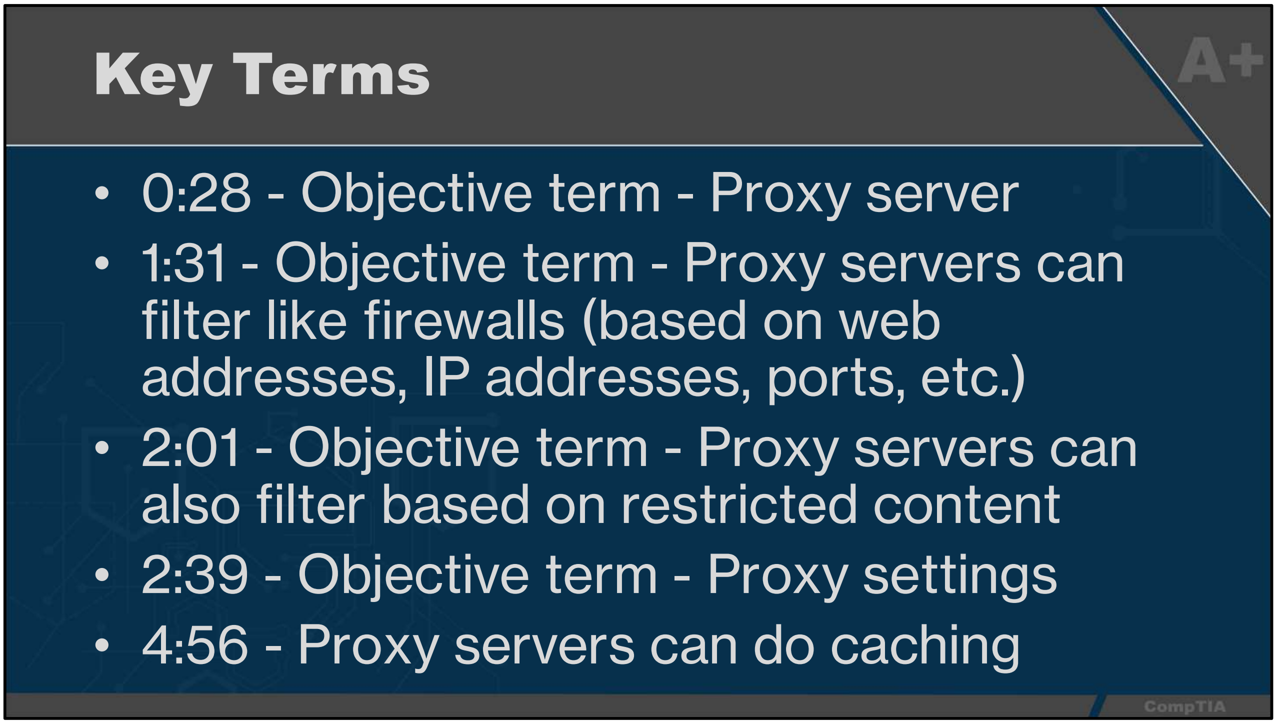
Core 2: 1.6 Given a scenario, configure Microsoft Windows networking features on a client/desktop.

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



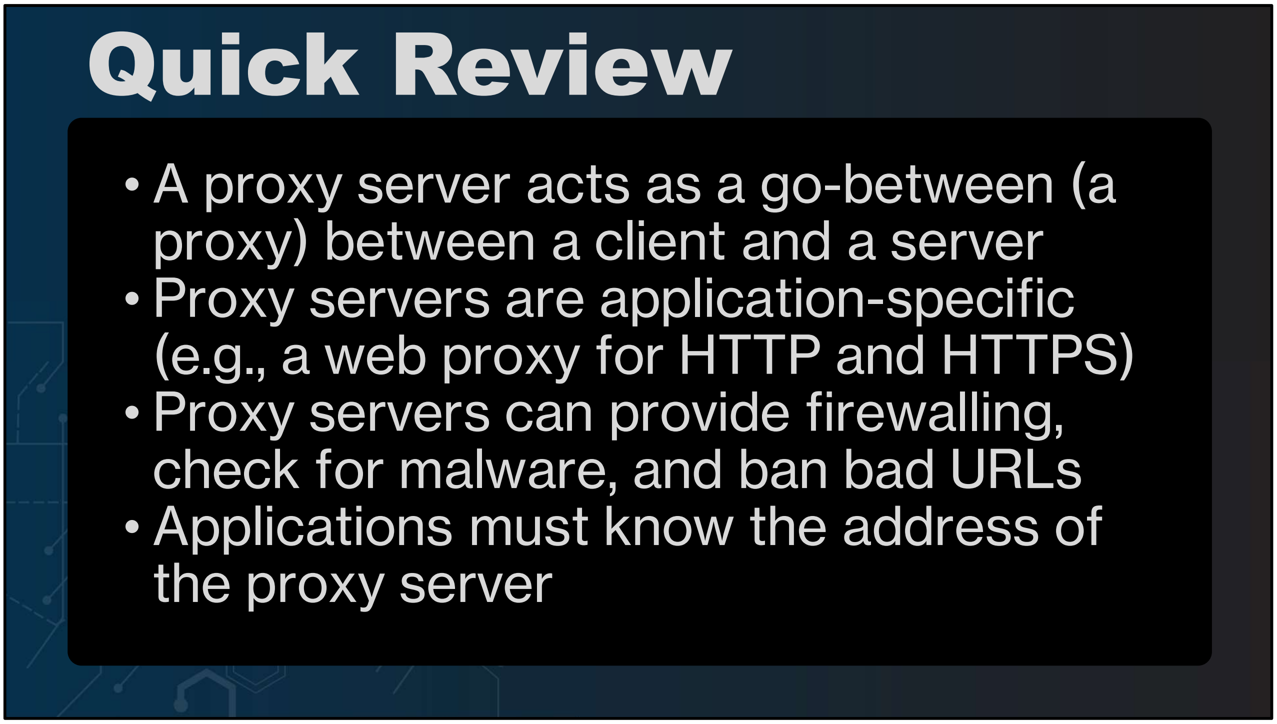
Episode Description

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.



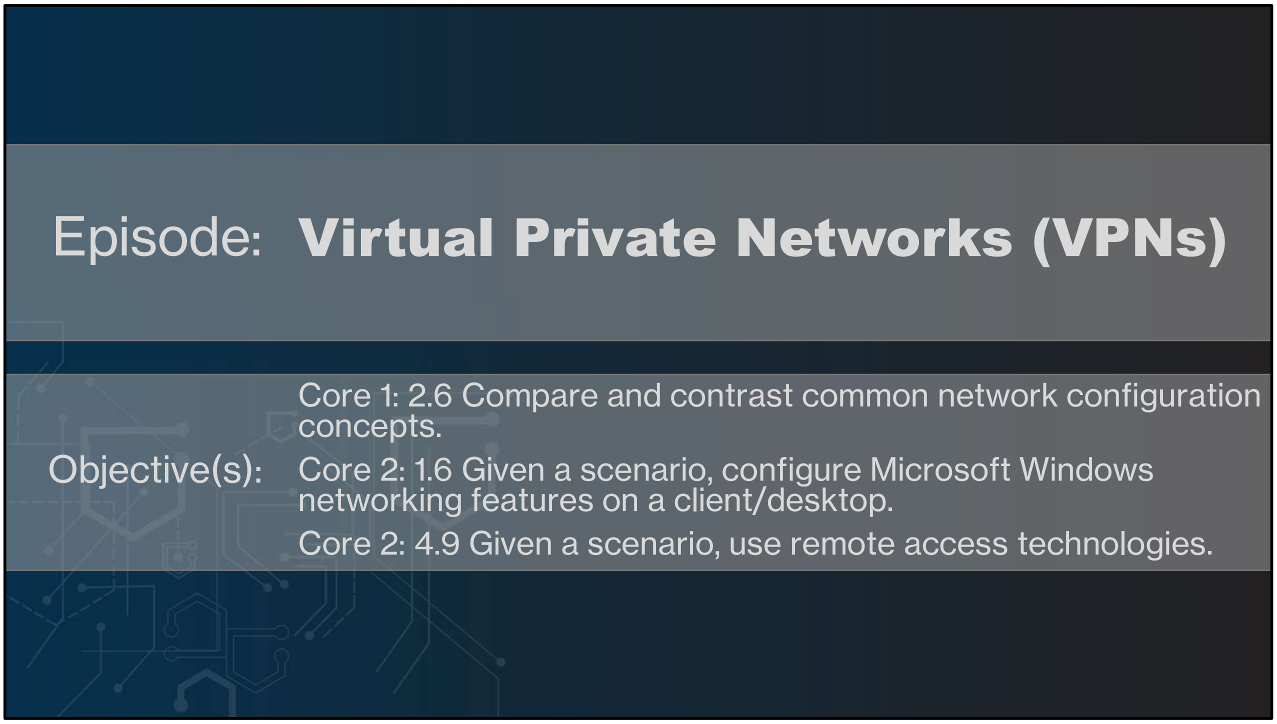
Key Terms

- 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



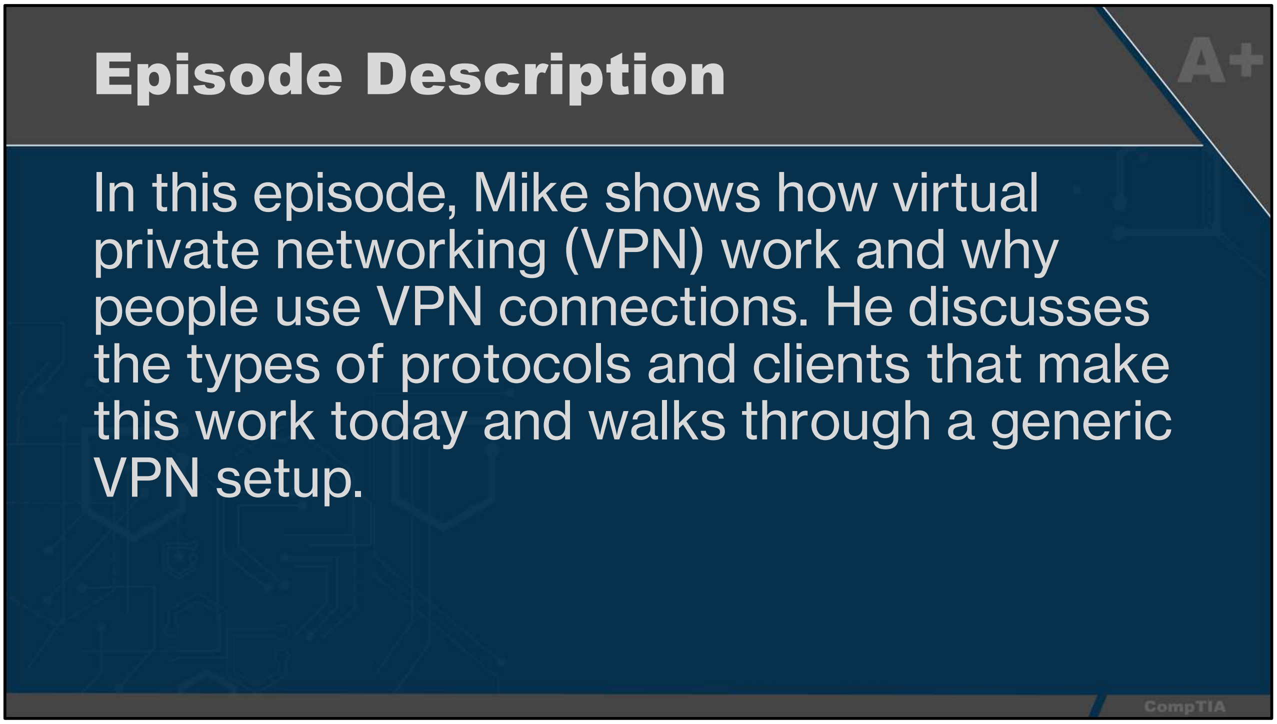
Episode: **Virtual Private Networks (VPNs)**

Objective(s):

Core 1: 2.6 Compare and contrast common network configuration concepts.

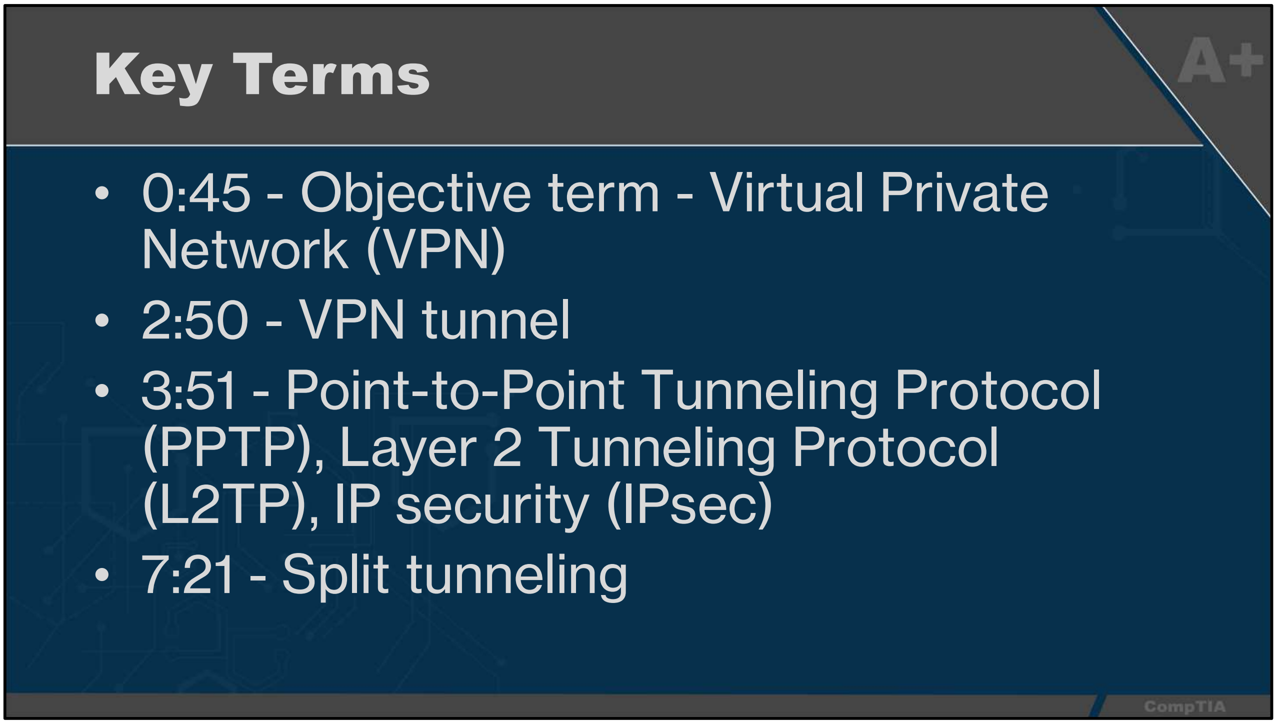
Core 2: 1.6 Given a scenario, configure Microsoft Windows networking features on a client/desktop.

Core 2: 4.9 Given a scenario, use remote access technologies.



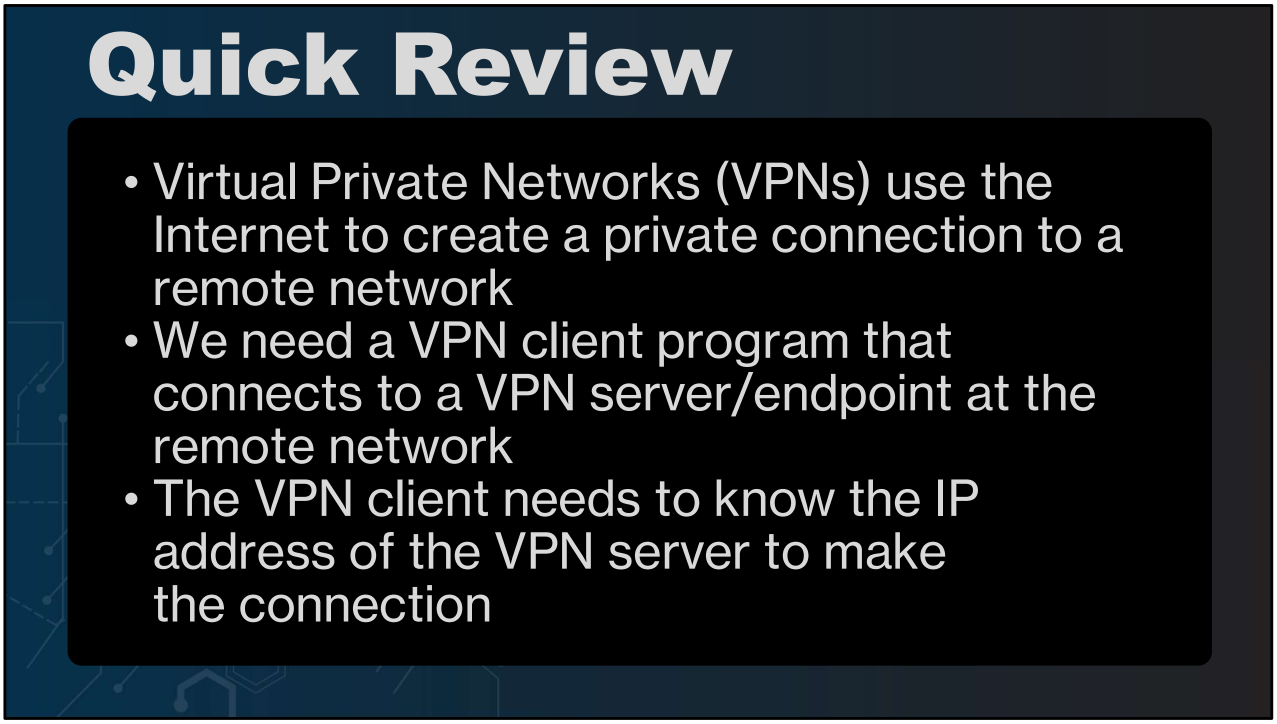
Episode Description

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.



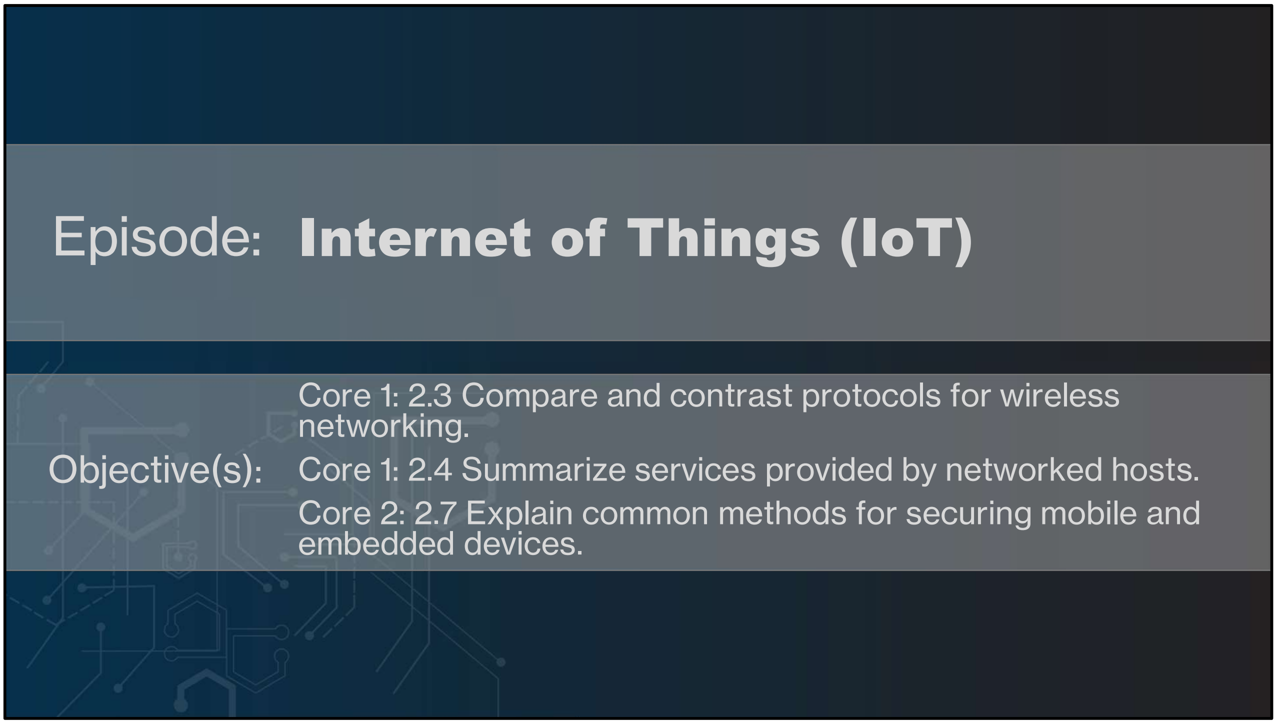
Key Terms

- 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



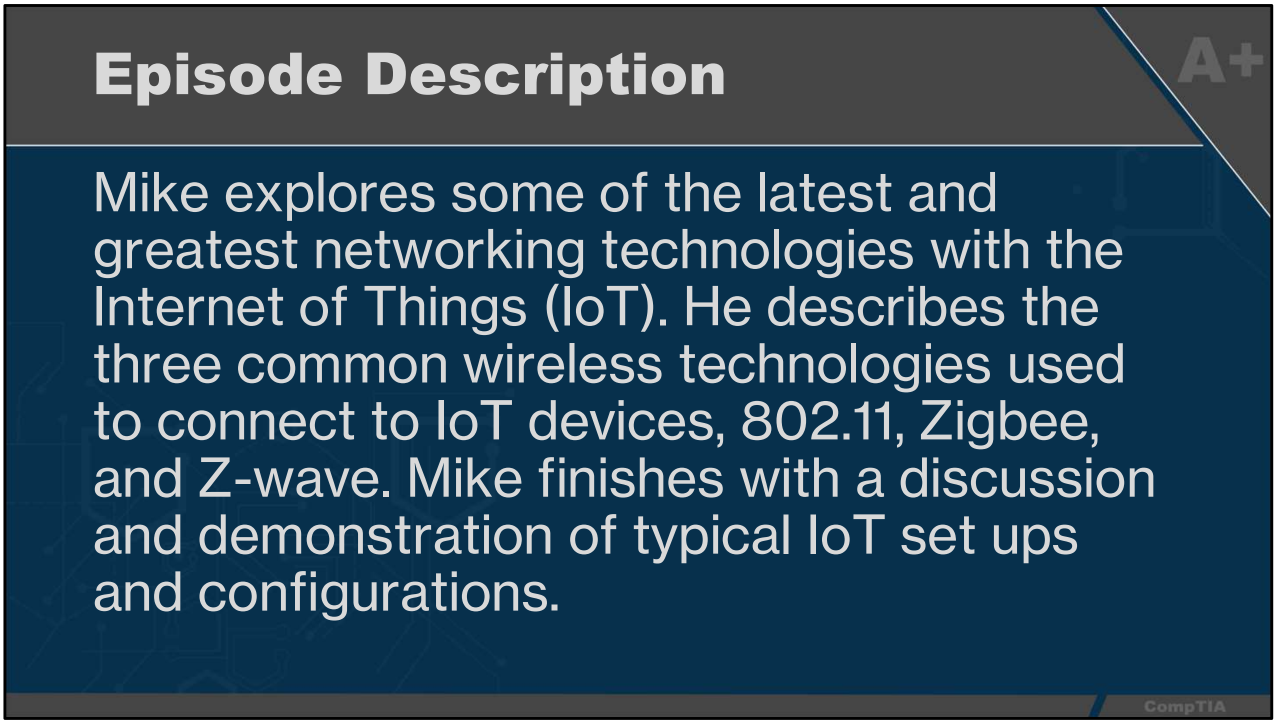
Episode: **Internet of Things (IoT)**

Objective(s):

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

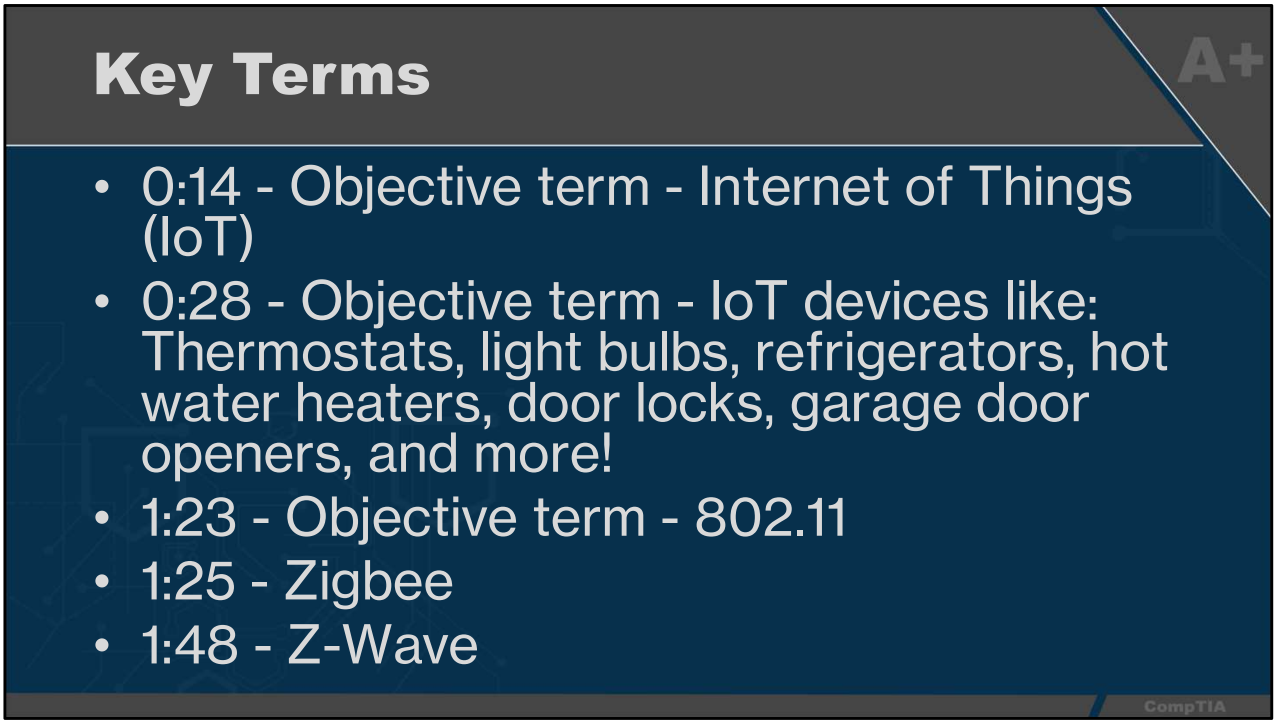
Core 1: 2.4 Summarize services provided by networked hosts.

Core 2: 2.7 Explain common methods for securing mobile and embedded devices.



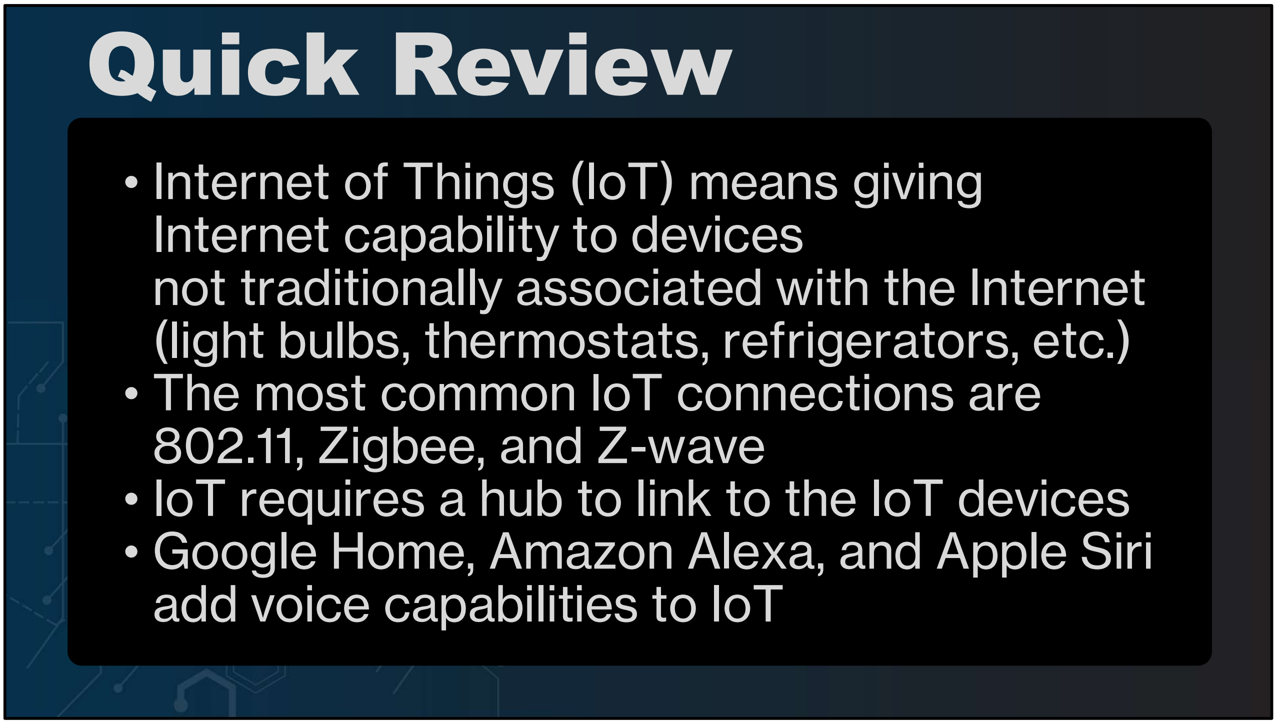
Episode Description

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.



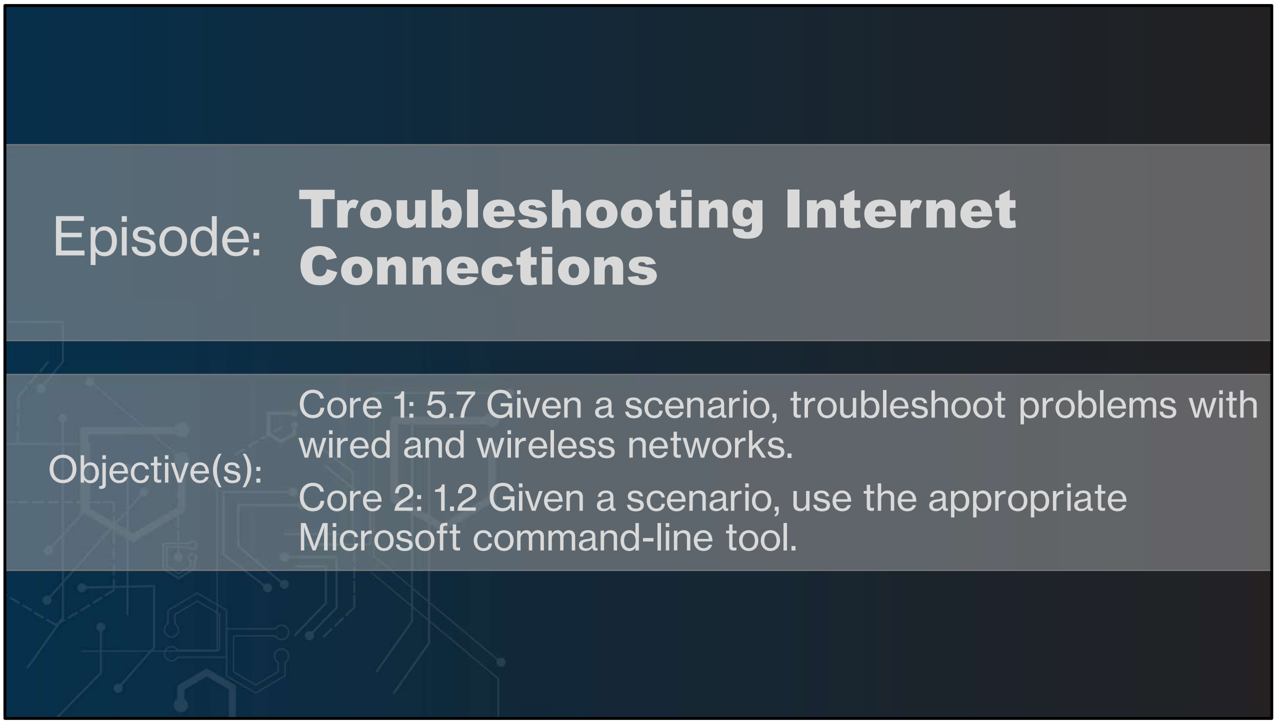
Key Terms

- 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

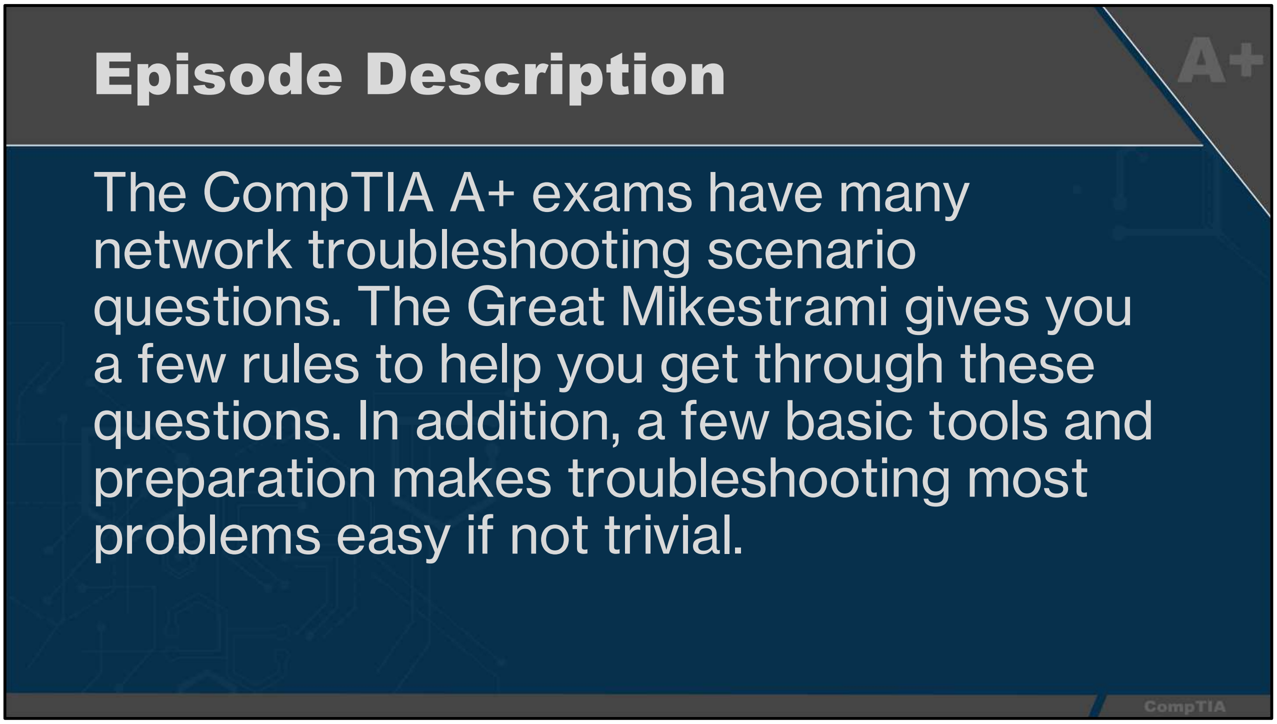


Episode: **Troubleshooting Internet Connections**

Objective(s):

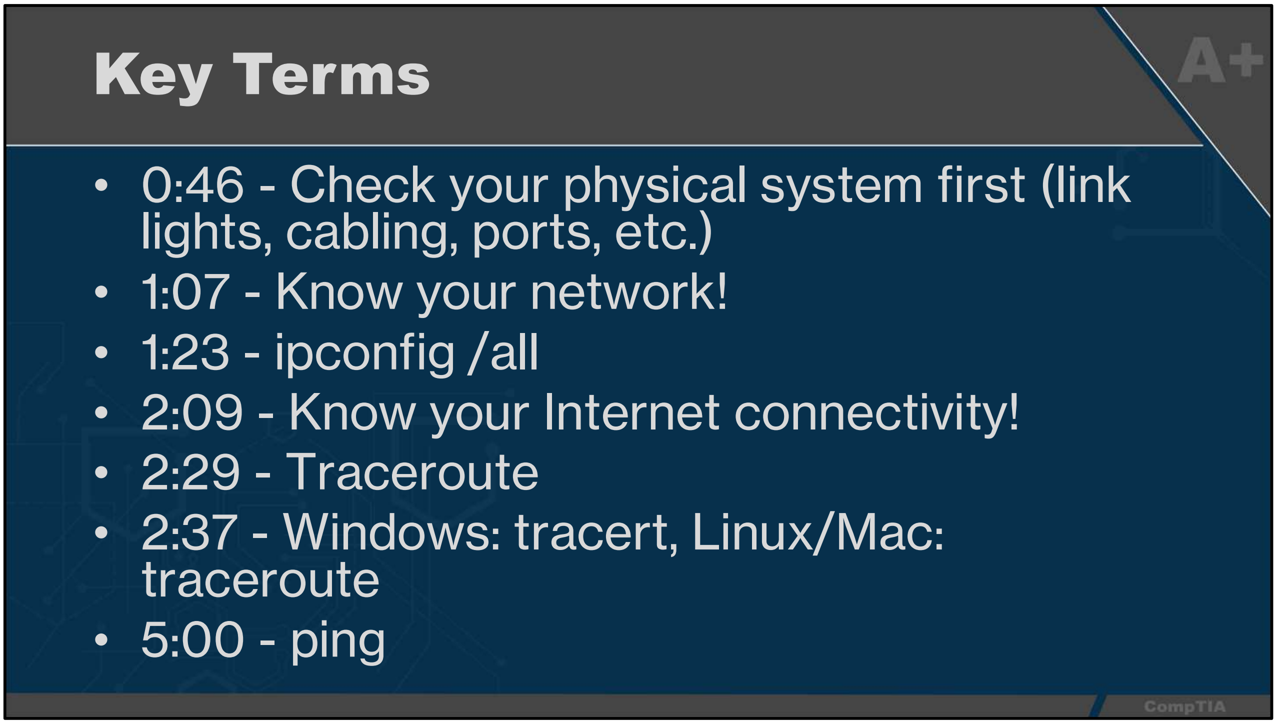
Core 1: 5.7 Given a scenario, troubleshoot problems with wired and wireless networks.

Core 2: 1.2 Given a scenario, use the appropriate Microsoft command-line tool.



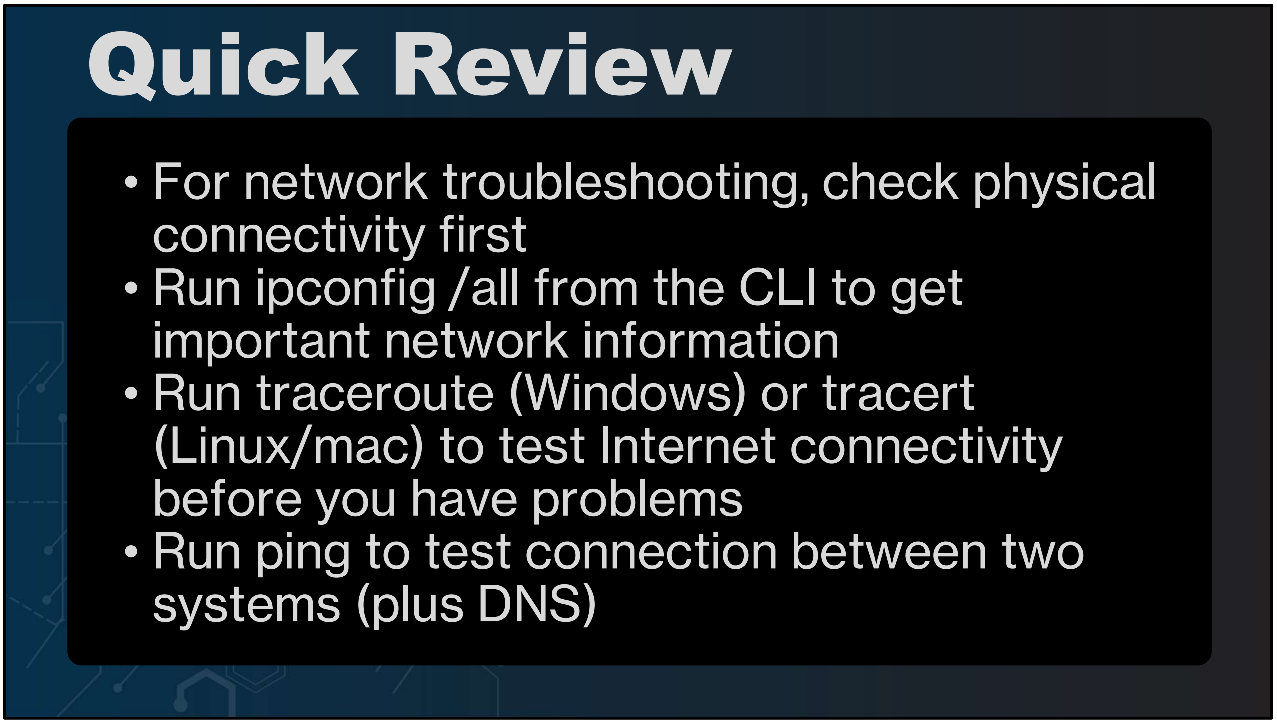
Episode Description

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.



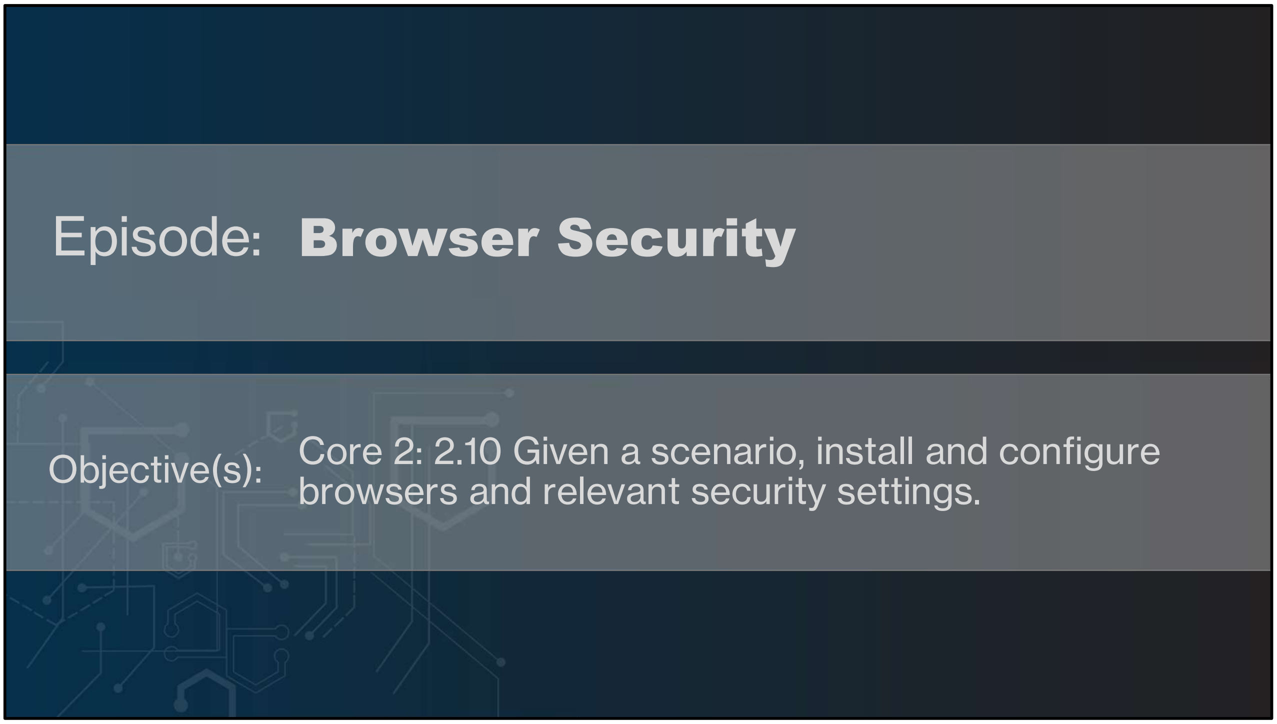
Key Terms

- 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



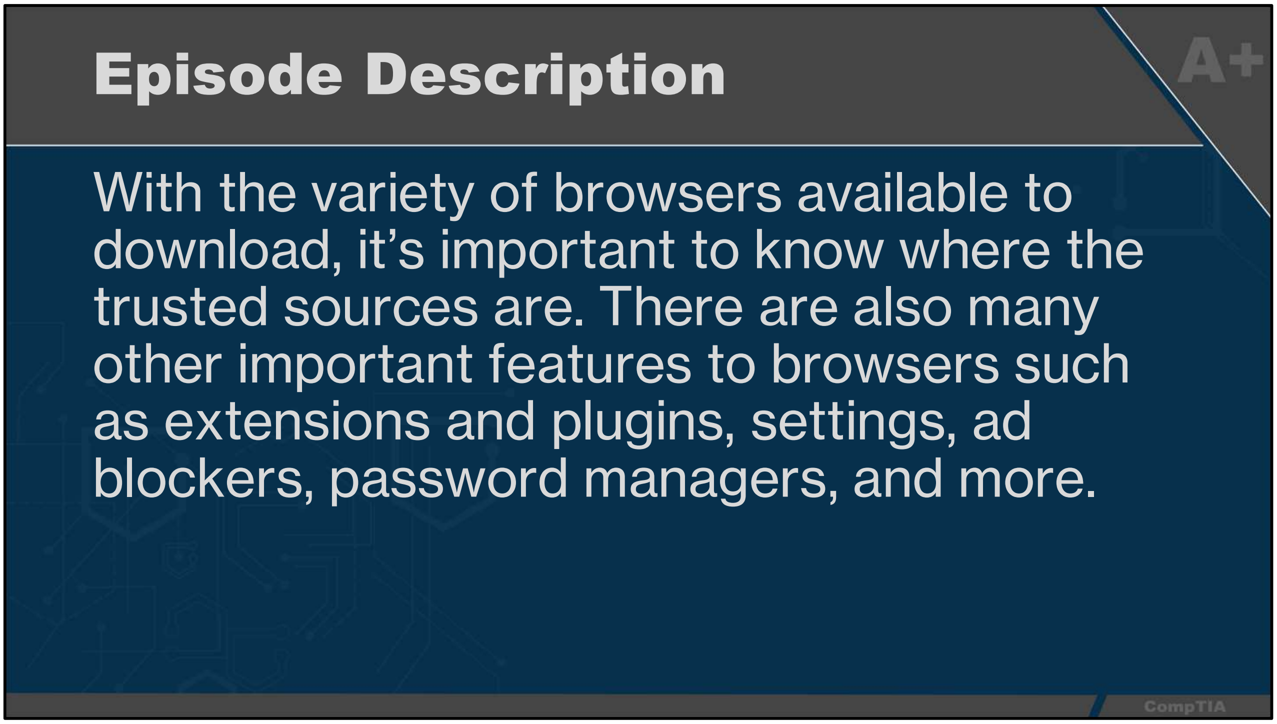
Quick Review

- 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)



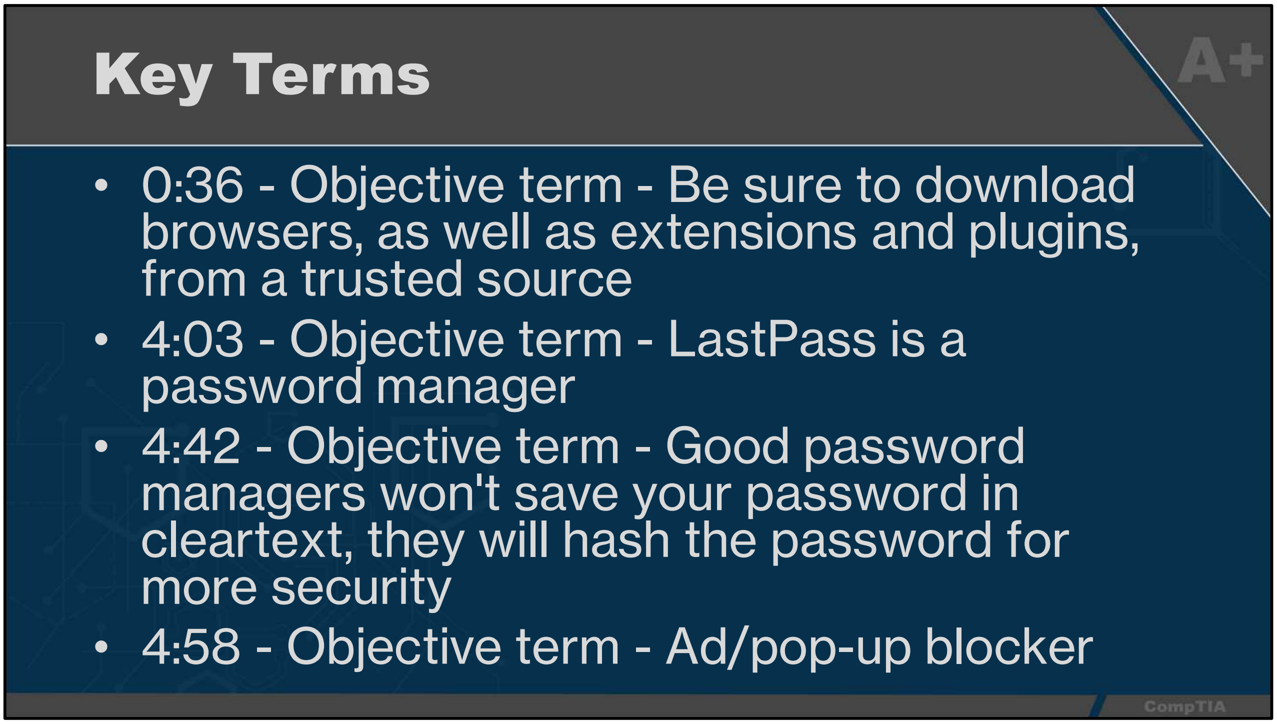
Episode: **Browser Security**

Objective(s): Core 2: 2.10 Given a scenario, install and configure browsers and relevant security settings.



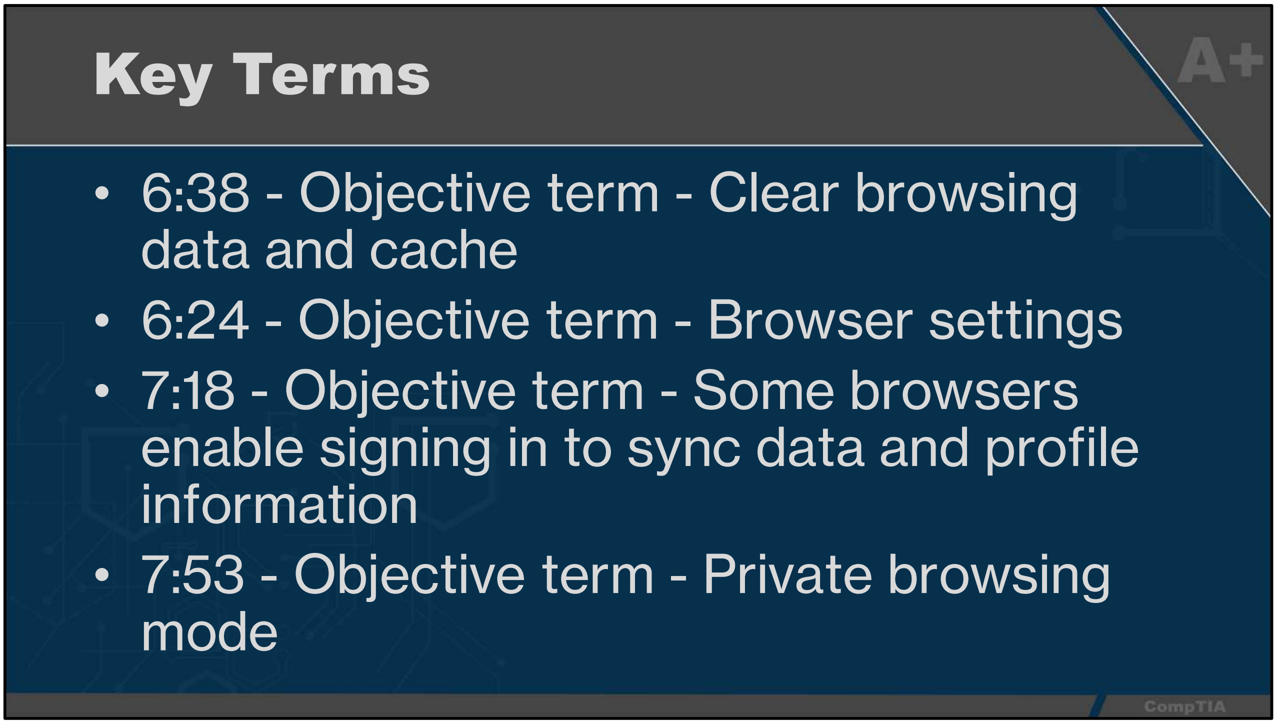
Episode Description

With the variety of browsers available to download, it’s important to know where the trusted sources are. There are also many other important features to browsers such as extensions and plugins, settings, ad blockers, password managers, and more.



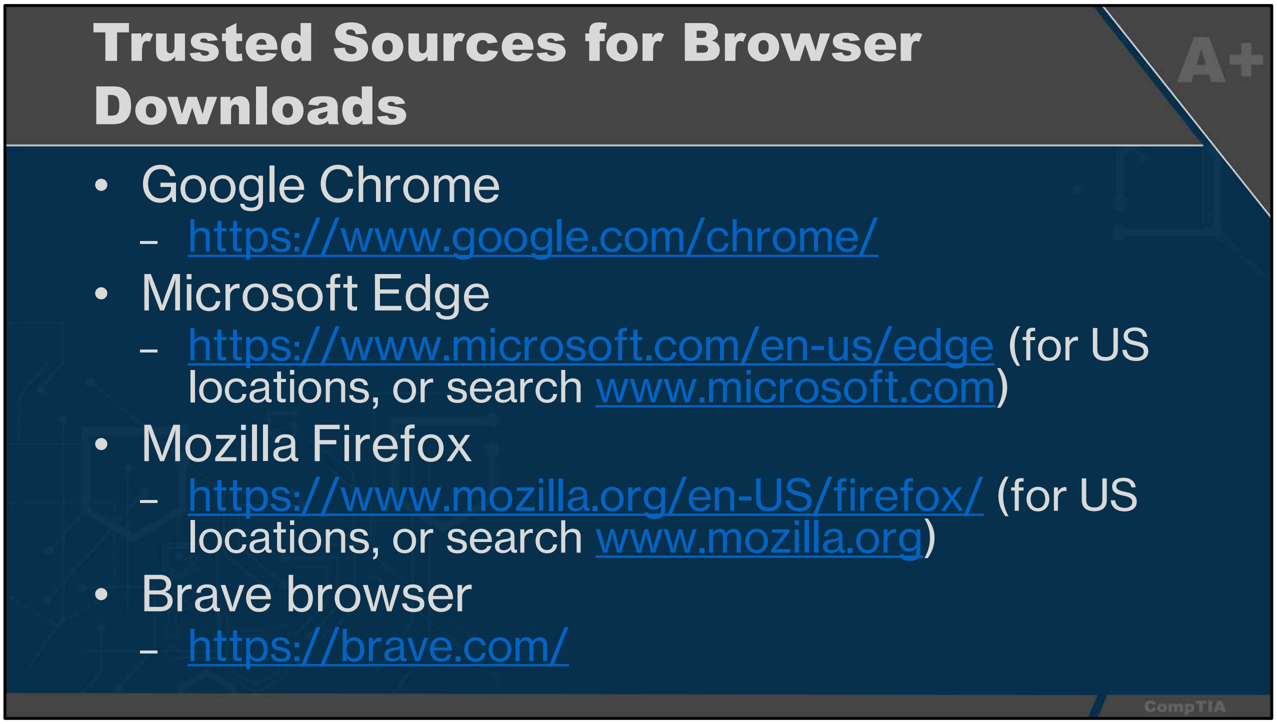
Key Terms

- 0:36 - Objective term - Be sure to download browsers, as well as extensions and plugins, from a trusted source
- 4:03 - Objective term - LastPass is a password manager
- 4:42 - Objective term - Good password managers won't save your password in cleartext, they will hash the password for more security
- 4:58 - Objective term - Ad/pop-up blocker



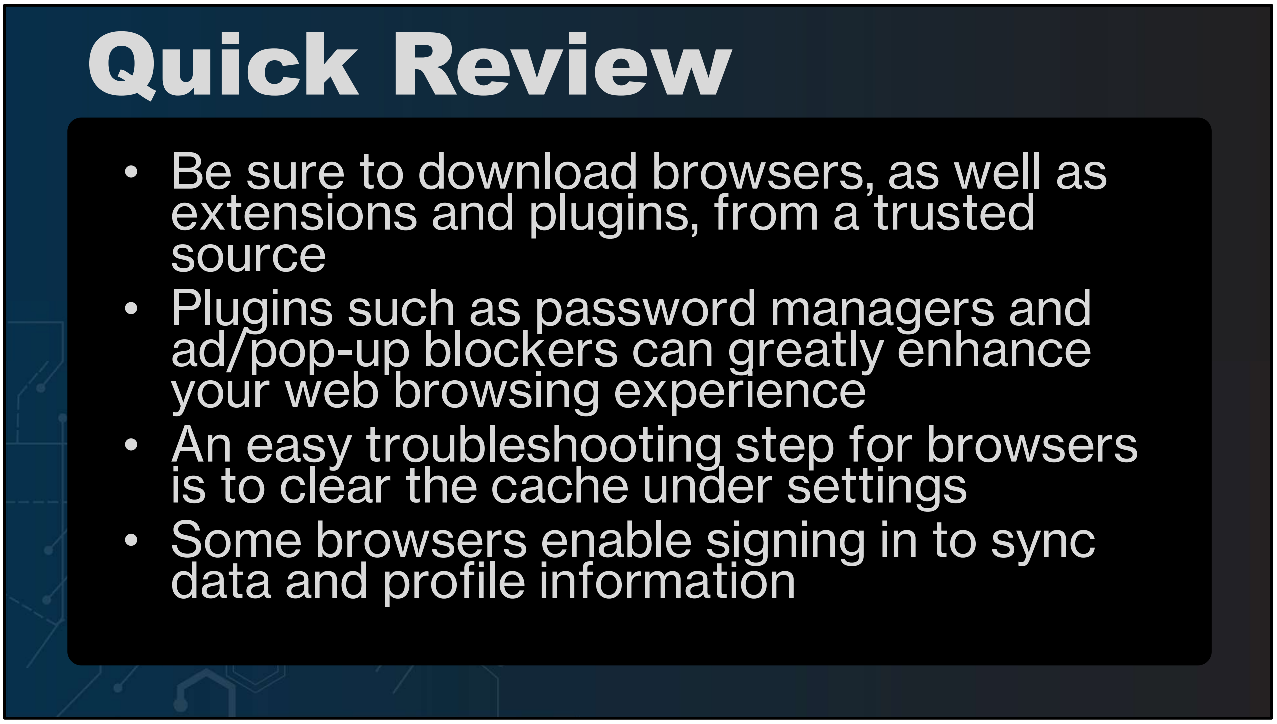
Key Terms

- 6:38 - Objective term - Clear browsing data and cache
- 6:24 - Objective term - Browser settings
- 7:18 - Objective term - Some browsers enable signing in to sync data and profile information
- 7:53 - Objective term - Private browsing mode



Trusted Sources for Browser Downloads

- Google Chrome
  - https://www.google.com/chrome/
- Microsoft Edge
  - https://www.microsoft.com/en-us/edge (for US locations, or search www.microsoft.com)
- Mozilla Firefox
  - https://www.mozilla.org/en-US/firefox/ (for US locations, or search www.mozilla.org)
- Brave browser
  - https://brave.com/



Quick Review

- Be sure to download browsers, as well as extensions and plugins, from a trusted source
- Plugins such as password managers and ad/pop-up blockers can greatly enhance your web browsing experience
- An easy troubleshooting step for browsers is to clear the cache under settings
- Some browsers enable signing in to sync data and profile information