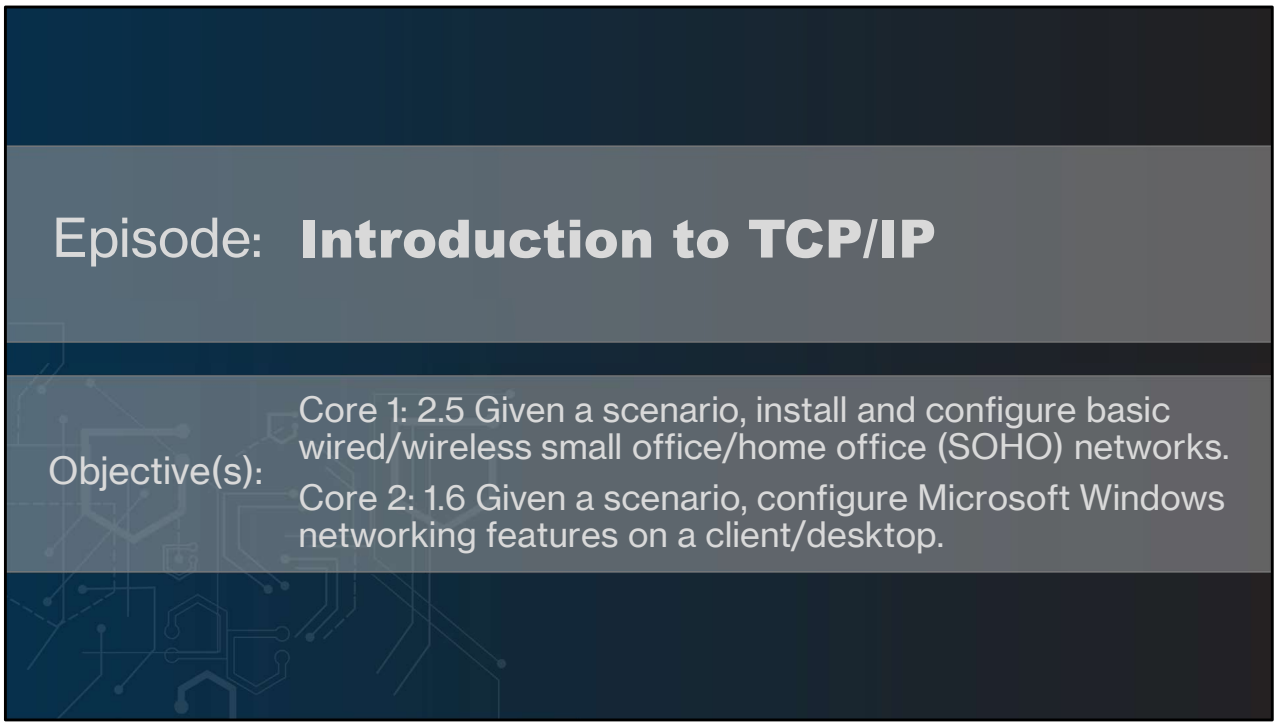
Chapter 19

Local Area Networking


Episode: Introduction to TCP/IP
Objective(s):
Core 1: 2.5 Given a scenario, install and configure basic wired/wireless small office/home office (SOHO) networks.
Core 2: 1.6 Given a scenario, configure Microsoft Windows networking features on a client/desktop.

Episode Description

A+

The Transmission Control Protocol/Internet Protocol (TCP/IP) is the cornerstone of Internet addressing and routing. It's important to understand IP addressing schemes and to see how TCP and IP work together to make the Internet work.

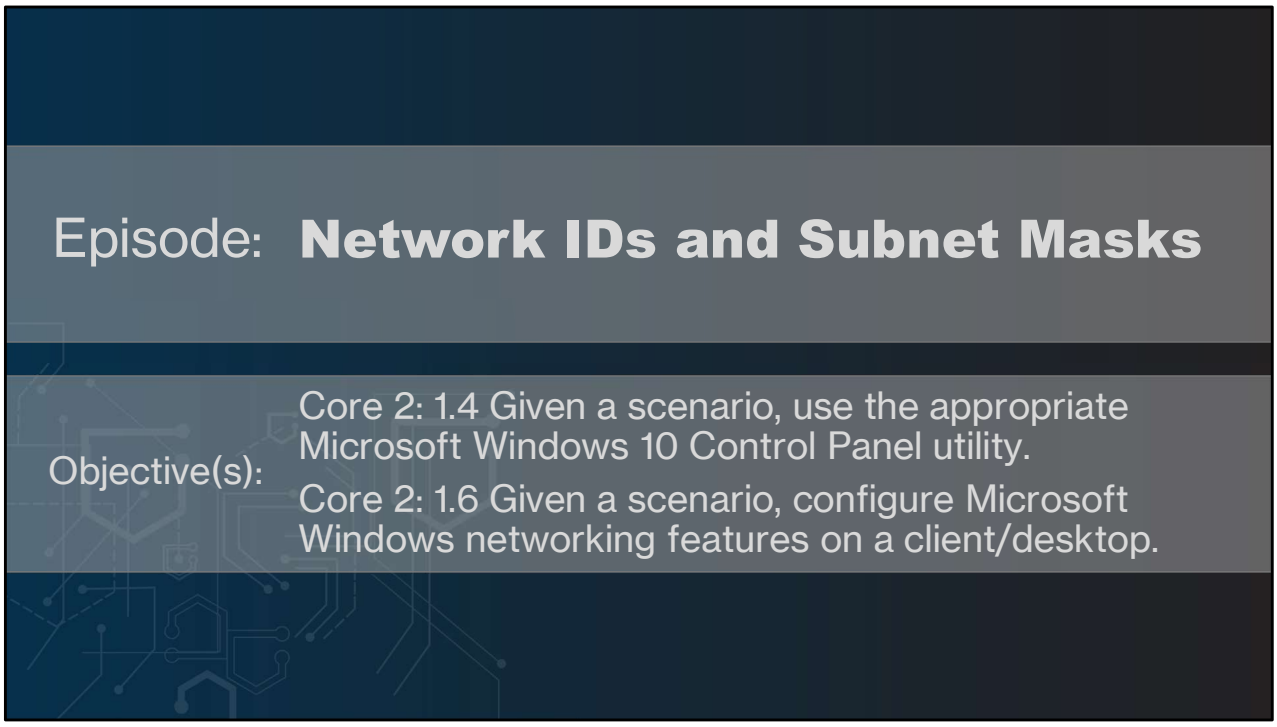
CompTIA

Key Terms

- 0:13 - 192.168.5.10
- 2:06 - Advanced Research Projects Agency Network (ARPANET)
- 11:41 - Objective term - Subnet mask
- 13:32 - Objective term - Default gateway

Quick Review

- TCP/IP was adopted as a protocol for ARPANET and what was to become the Internet
- IP addresses have four octets between 0-255
- Subnet masks are used to differentiate IP addresses on local LANs vs. outside traffic, and are only used for IPv4 addresses


Episode: Network IDs and Subnet Masks
Objective(s):
Core 2: 1.4 Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility.
Core 2: 1.6 Given a scenario, configure Microsoft Windows networking features on a client/desktop.

Episode Description

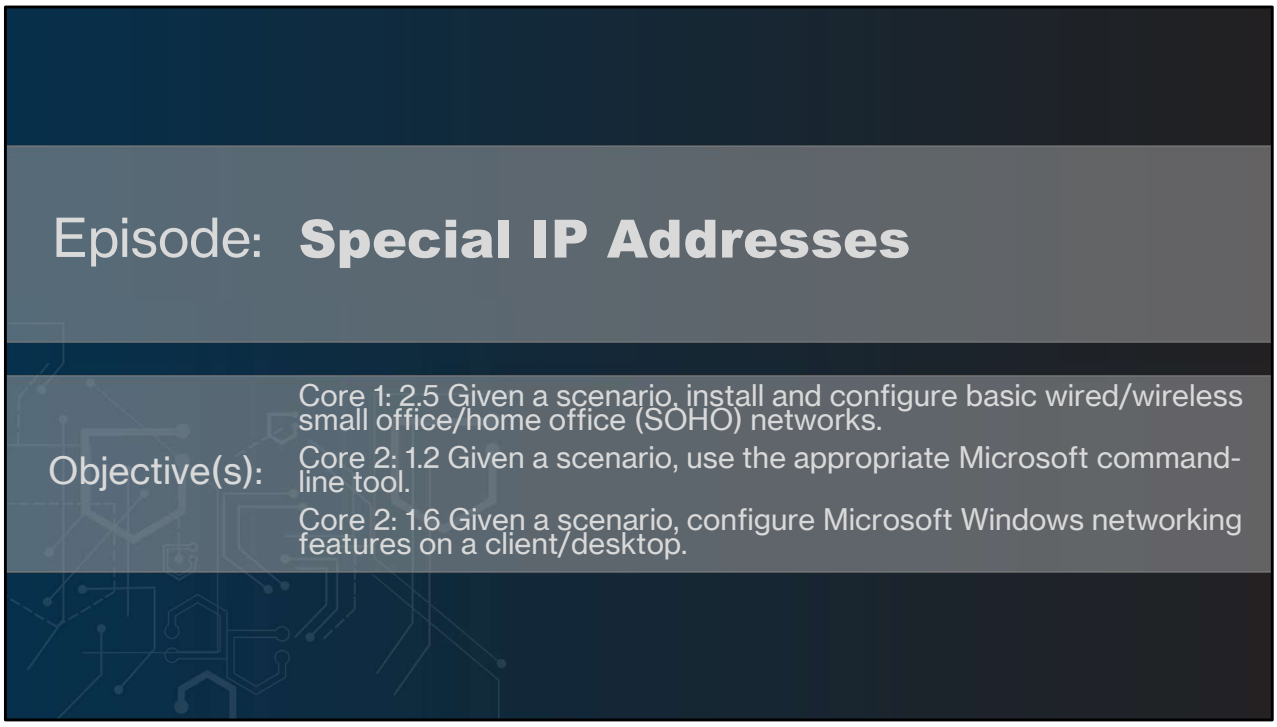
IP addressing was designed from the ground up for flexibility in supporting LANs and WANs of any size. The first step towards understanding this flexibility is to understand Network IDs and how they interact with a subnet mask to get packets delivered to the right system.

Key Terms

- 0:22 - Objective term - Network and Sharing Center
- 1:49 - Objective term - IPv4
- 2:20 - Objective term - Subnet mask
- 3:15 - Objective term - Default gateway
- 3:47 - Objective term - Static IP address

Quick Review

- Use Network and Sharing Center for setting up network information
- Set IP address, subnet mask, and gateway in Ethernet Properties
- When you manually set the IP address, it's called a static IP address


Episode: Special IP Addresses
Objective(s):
Core 1: 2.5 Given a scenario, install and configure basic wired/wireless small office/home office (SOHO) networks.
Core 2: 1.2 Given a scenario, use the appropriate Microsoft command-line tool.
Core 2: 1.6 Given a scenario, configure Microsoft Windows networking features on a client/desktop.

Episode Description

The designers of IP addressing reserved many IP addresses for special uses. From loopback to private IP addresses, a good tech understands these special addresses as well as when and how to use them.

Key Terms

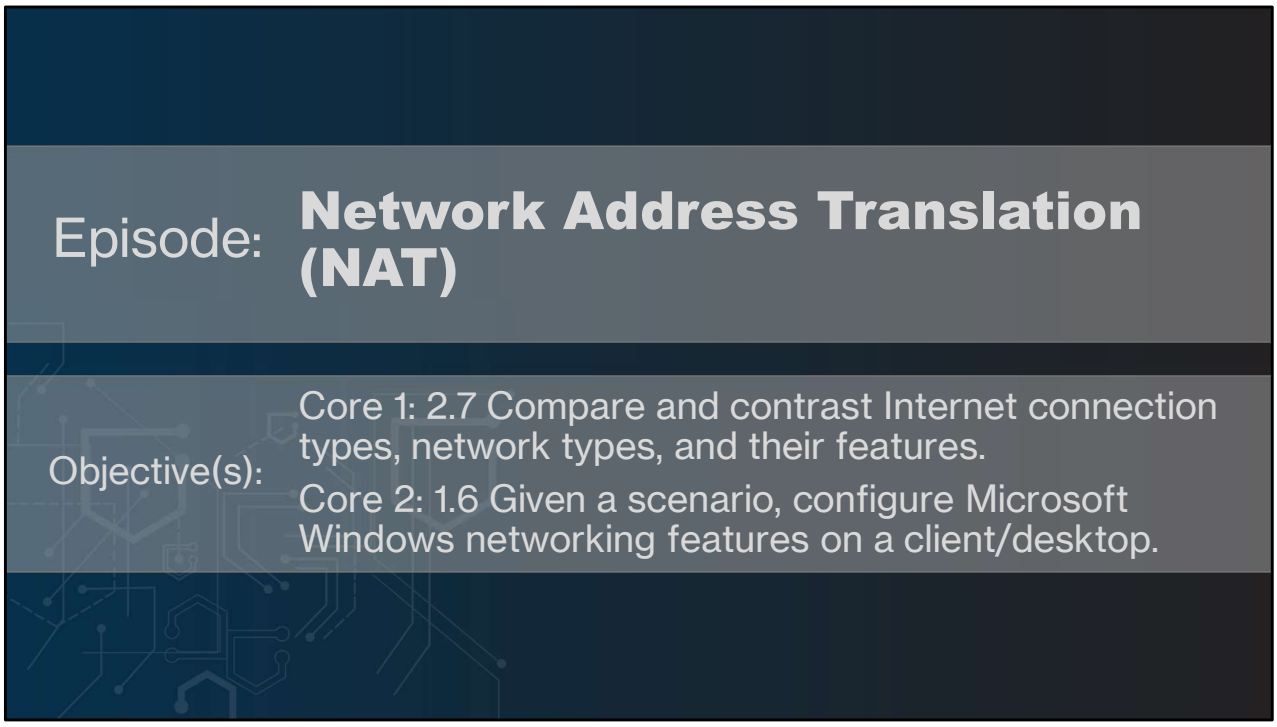
- 0:47 - Objective term - Class A
- 1:09 - Objective term - Class B
- 1:26 - Objective term - Class C
- 2:31 - Objective term - Class D (multicast)
- 2:55 - Objective term - Class E (reserved)
- 3:14 - Objective term - Private IP address
- 3:30 - Objective term - Class A private IP addresses
- 3:40 - Objective term - Class B private IP addresses
- 3:57 - Objective term - Class C private IP addresses

Key Terms

- 4:35 - Objective term - Loopback IP address
- 4:52 - Objective term - ping 127.0.0.1
- 5:09 - Ping packet
- 5:45 - Objective term - ipconfig
- 6:38 - Objective term - ping 192.168.4.1
- 7:20 - Objective term - ipconfig /all
- 7:56 - Objective term - ping -t 192.168.4.1

Quick Review

- Class D addresses are for multicast (224.x.x.x)
- Class E addresses are reserved (240.x.x.x)
- There are three sets of private IP addresses (Class A: 10.x.x.x, Class B: 172.16-172.31.x.x, Class C: 192.168.x.x)
- Loopback addresses are used to ping your own router (127.0.0.1)


Episode:
Network Address Translation (NAT)
Objective(s):
Core 1: 2.7 Compare and contrast Internet connection types, network types, and their features.
Core 2: 1.6 Given a scenario, configure Microsoft Windows networking features on a client/desktop.

Episode Description

A+

You'd be hard pressed to find a home or small office router that isn't using Network Address Translation (NAT). NAT provides some amazing benefits but also has some serious limitations.

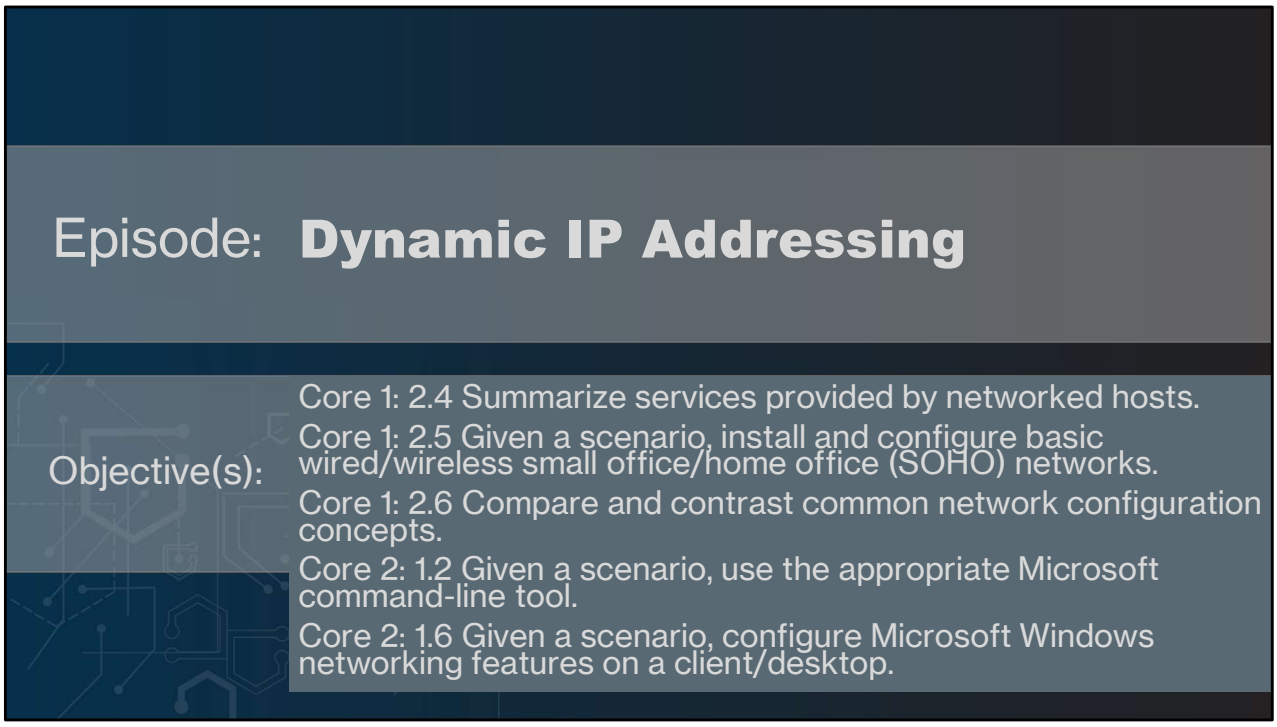
CompTIA

Key Terms

- 0:44 - Network Address Translation (NAT)
- 1:50 - Local area network (LAN)
- 1:22 - Objective term - Gateway router

Quick Review

- Network address translation (NAT) saves IP addresses
- With NAT, internal networks use private IP addresses and share a public address
- All gateway routers are NAT-enabled by default
- Networks that use NAT are invisible to the public Internet


Episode: Dynamic IP Addressing
Objective(s):
Core 1: 2.4 Summarize services provided by networked hosts.
Core 1: 2.5 Given a scenario, install and configure basic wired/wireless small office/home office (SOHO) networks.
Core 1: 2.6 Compare and contrast common network configuration concepts.
Core 2: 1.2 Given a scenario, use the appropriate Microsoft command-line tool.
Core 2: 1.6 Given a scenario, configure Microsoft Windows networking features on a client/desktop.

Episode Description

Manually entering IP addresses into all our devices is an administrative nightmare. To avoid this mess, smart techs use the Dynamic Host Configuration Protocol (DHCP) to automatically provide IP addressing to individual hosts.

Key Terms

- 0:24 - Objective term - Dynamic IP addressing via Dynamic Host Configuration Protocol (DHCP)
- 3:50 - Objective term - Automatic Private IP Addressing (APIPA)
- 4:22 - APIPA will always give 169.254.X.X address
- 4:34 - Class B address

Key Terms

- 5:48 - Objective term - ipconfig
- 6:34 - Objective term - ipconfig /renew
- 6:50 - Objective term - ipconfig
- 6:55 - Objective term - ipconfig /release
- 7:03 - Objective term - ipconfig /renew

Quick Review

- Dynamic Host Configuration Protocol (DHCP) automatically and dynamically assigns IP information to hosts
- Gateway routers commonly are DHCP servers for their internal LANs
- If a DHCP client can't find the DHCP server, it will use an APIPA address
- Use the ipconfig /renew command to force a new connection to the DHCP server

Episode: **Working with Connections**

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

Episode Description

When two computers begin the process of sharing data, they create what we call a connection (or session). A good tech knows how to use common utilities to observe these connections and diagnose issues.

Key Terms

- 0:28 - Objective term - netstat
- 0:51 - Objective term - netstat
- 1:17 & 3:13 - Objective term - netstat -n
- 3:25 - Windows folder sharing (port 445)
- 3:51 - Objective term - netstat -a -n
- 4:43 - Loopback address 127.0.0.1
- 7:29 - TCPView

Sysinternals TCPView

- https://learn.microsoft.com/en-us/sysinternals/downloads/tcpview

Quick Review

- The netstat command shows important information about connections
- Use netstat switches –n and –a as needed
- Consider a third-party tool such as TCPView as an alternative to netstat

Episode: **Understanding DNS**

Objective(s):

Core 1: 2.4 Summarize services provided by networked hosts.

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

Episode Description

Individual hosts use IP addresses, but humans are terrible at memorizing long strings of numbers. To make our lives easier, most TCP/IP networks (and certainly the Internet) use the Domain Name System (DNS) to apply more human-friendly names to systems. DNS can also make use of various spam management protocols such as DKIM, SPF, and DMARC.

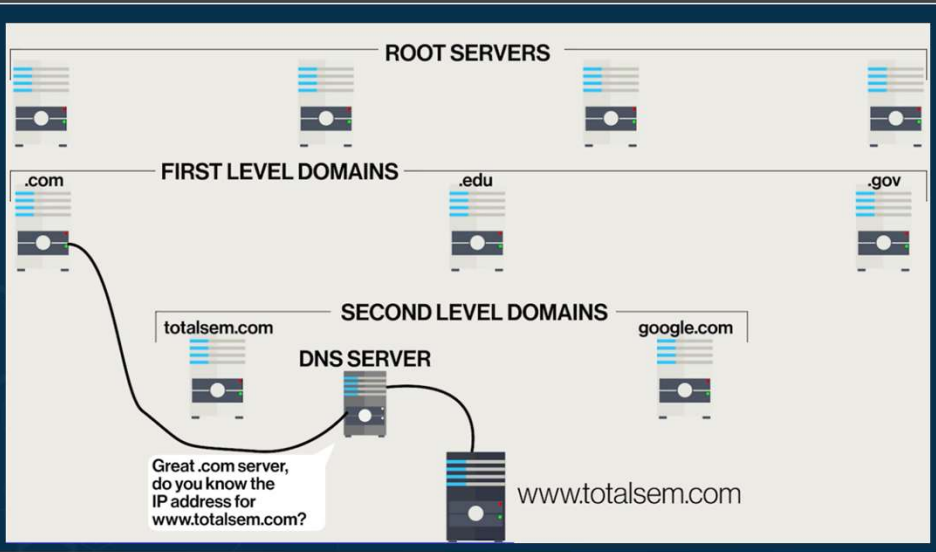
Key Terms

- 1:05 - www.totalsem.com (175.16.44.3)
- 1:10 - www.totalsem.com
- 1:20 - Objective term - Domain Name System (DNS)
- 1:26 - Fully Qualified Domain Name (FQDN)
  Example: www.totalsem.com
- 1:56 - Hosts file
- 8:15 - FQDNs have a 256-character limit

Key Terms

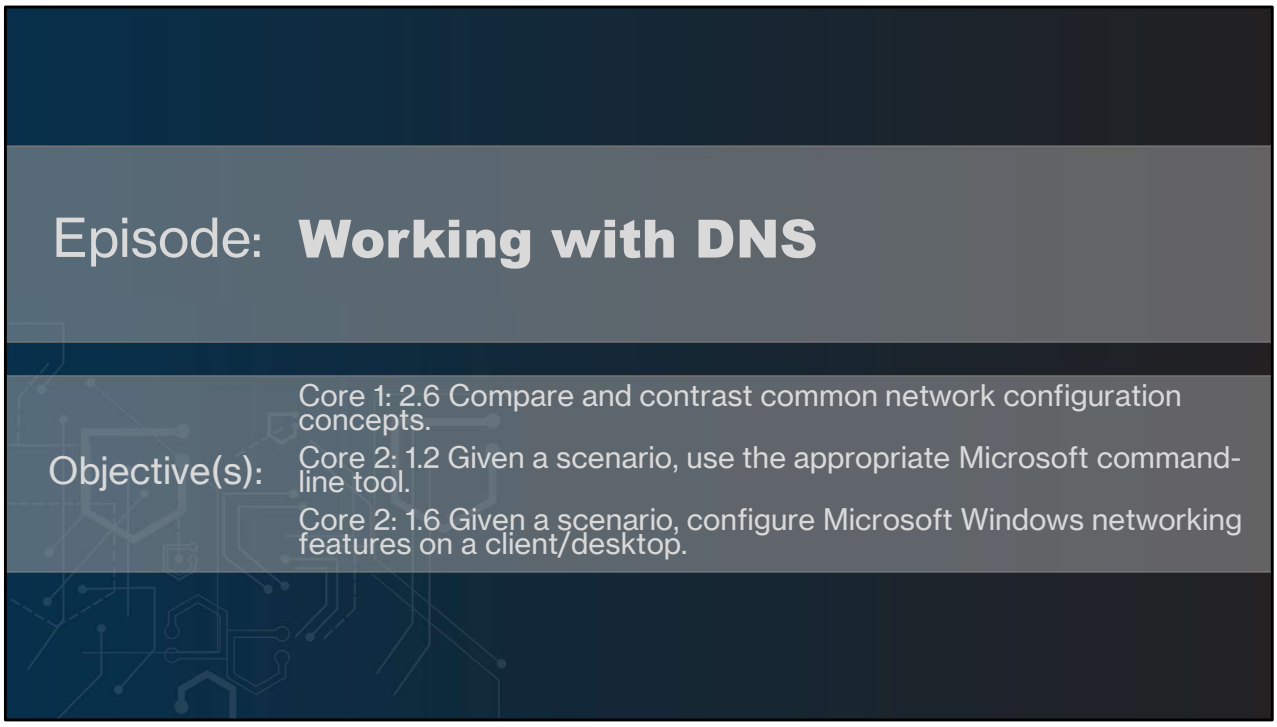
- 8:33 - Objective term - Spam gateway/spam management
- 9:17 - Objective term - Domain-based Message Authentication, Reporting, and Conformance (DMARC)
- 9:55 - Objective term - DomainKeys Identified Mail (DKIM)
- 10:28 - Objective term - Sender Policy Framework (SPF)

DNS Servers


ROOT SERVERS
FIRST LEVEL DOMAINS
.com
.edu
.gov
SECOND LEVEL DOMAINS
totalsem.com
google.com
DNS SERVER
Great .com server, do you know the IP address for www.totalsem.com?
www.totalsem.com

Quick Review

- The Domain Name System (DNS) resolves Fully Qualified Domain Names (FQDNs) to IP addresses
- Domain-based Message Authentication, Reporting, and Conformance (DMARC) enters records of domains to avoid spoofing
- DomainKeys Identified Mail (DKIM) enables the sender to sign their message and verify their identity
- Sender Policy Framework (SPF) detects fraudulent e-mail addresses


Episode: Working with DNS
Objective(s):
Core 1: 2.6 Compare and contrast common network configuration concepts.
Core 2: 1.2 Given a scenario, use the appropriate Microsoft command-line tool.
Core 2: 1.6 Given a scenario, configure Microsoft Windows networking features on a client/desktop.

Episode Description

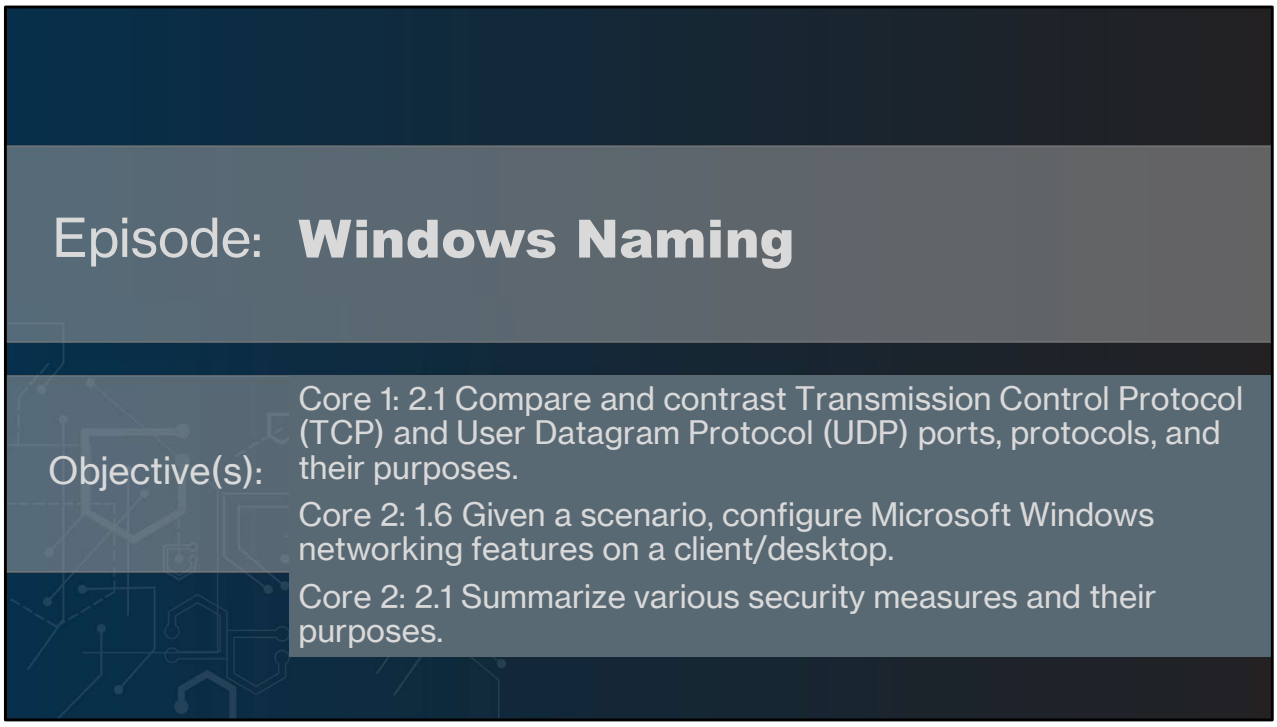
When a user complains the Internet is down, what's often happening is that DNS isn't working. There are a few simple tools and procedures to diagnose and repair DNS problems.

Key Terms

- 0:26 - Objective term - ipconfig /all
- 2:16 - Objective term - 1. Manually configure DNS
- 2:27 - Google's DNS servers: 8.8.8.8 or 8.8.4.4
- 3:25 & 3:56 - Objective term - nslookup
- 4:20 - Objective term - An A record tracks IPv4 address system names (AAAA records track IPv6)
- 4:29 - Objective term - MX records are used by mail servers
- 4:37 - Canonical Name (CNAME) record

Quick Review

- Use ipconfig /all to see a system's DNS servers
- You can statically configure DNS and still use DHCP for IP addressing
- Have an alternative public DNS server in case your DNS server is down
- Use nslookup to verify a DNS server is running


Episode: Windows Naming
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.
Core 2: 2.1 Summarize various security measures and their purposes.

Episode Description

Microsoft introduced a series of naming protocols, some of which predate the Internet. Interestingly, these protocols (or at least their modern versions) are still alive and well not only on Windows systems, but on Linux and macOS systems as well.

Key Terms

- 0:33 - Objective term - NetBIOS/NetBT
- 1:38 - Objective term - Every Windows system is a member of a Workgroup or Active Directory Domain
- 3:35 - Objective term - Workgroup vs. Domain
- 3:55 - Objective term - Domain
- 4:12 - Objective term - Active Directory Domain

Quick Review

- Windows naming is designed for LANs
- When you install Windows, you will need to give the computer a name
- All Windows systems will be a member of either a Workgroup or an Active Directory Domain
- Active Directory is set up on a specialized Windows server with proprietary software


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

Episode Description

Microsoft developed the concept of Workgroups for small networks to work with their naming system. Workgroups are simple and provide no security, but they're a part of every small Windows network.

Key Terms

- 0:29 - Objective term - NetBIOS/NetBEUI
- 1:10 - Objective term - NetBT (NetBIOS over TCP/IP)
- 1:44 - Common Internet File System (CIFS)
- 1:49 - Objective term - Server Message Block (SMB)
- 2:06 - Samba (Linux and macOS SMB protocol)
- 3:18 - Objective term - Sharing within a Workgroup
- 3:28 - whoami

Quick Review

- Server Message Block (SMB) is the common way Windows file and folder sharing is handled over TCP/IP
- All Windows computers on a single LAN will automatically see each other if they are in the same Workgroup
- You must have an account on a remote system to access shared folders
- We set share permissions when we share a folder

Episode: **Working with Active Directory**

Objective(s): Core 2: 2.1 Summarize various security measures and their purposes.

Episode Description

More advanced Windows networks use Active Directory Domains instead of Workgroups. These Domains, especially Microsoft's Active Directory-enabled Domains, provide powerful services for larger networks.

Key Terms

- 0:18 - Objective term - Active Directory requires: Domain controller (dedicated server) and Windows Server software
- 2:35 - Objective term - Organizational Units (OUs)
- 3:16 - <name>.local
- 4:38 - Windows Server
- 5:50 - Domain admin has the power to add any computer to the domain

Key Terms

- 8:06 - Objective term - Groups can be useful for security purposes
- 8:29 - Forest
- 11:22 - Objective term - Home folder (can be specified through folder redirection)
- 11:40 - Objective term - Login script

Quick Review

- An Active Directory Domain requires a dedicated Domain controller with Windows Server software installed
- We use Organizational Units (OUs) and Forests to organize members of a Domain
- Domains support many security policies, login scripts and home folder redirection
- Windows Domains support single sign-on

Episode: **Windows Sharing with macOS and Linux**

Objective(s):

Core 1: 2.4 Summarize services provided by networked hosts.

Core 2: 1.10 Identify common features and tools of the macOS/desktop OS.

Core 2: 1.11 Identify common features and tools of the Linux client/desktop OS.

Episode Description

Both macOS and Linux systems know how to use Windows naming functions to connect using Workgroups and Domains and share resources using Samba. The trick is to understand how they do it and to configure them to work with an existing Windows network.

Key Terms

- 0:50 - LAN manager
- 1:00 - Objective term - Server Message Block (SMB)
- 1:10 - Samba
- 1:54 - Objective term - Sharing

Quick Review

- Server Message Block (SMB) is the Windows method for network sharing
- Samba comes with Linux and macOS to connect to Windows networks
- You need to know the Workgroup or Domain name as well as give the system a computer name


Episode: The net Command
Objective(s):
Core 2: 1.2 Given a scenario, use the appropriate Microsoft command-line tool.
Core 2: 1.6 Given a scenario, configure Microsoft Windows networking features on a client/desktop.

Episode Description

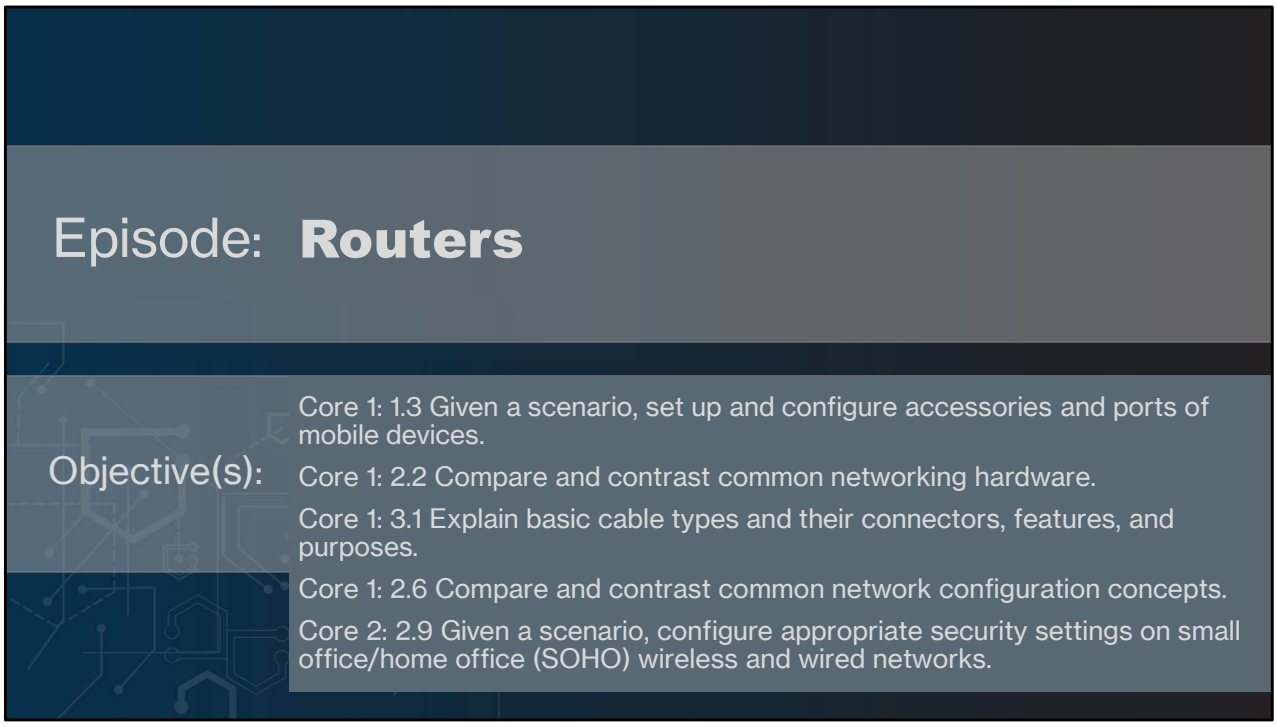
The Windows net command has so many features that it deserves its own episode. We use the net command for everything from querying the network to accessing shares.

Key Terms

- 0:42 - Objective term - net
- 0:51 - net view
- 1:05 - net view mikewin10pc
- 1:30 - net share shareit=c:\stuff
- 2:01 - net share
- 2:24 - Objective term - Drive mapping
- 2:37 - Objective term - net use v: \\mikewin10pc\mike
- 2:59 - Objective term - net user
- 3:11 - Objective term - net user tammy total /add
- 3:34 - Objective term - net user tammy delete

Quick Review

- The net command has many switches
- net view shows the systems and the shares in a workgroup or domain
- net share shares folders or views shared folders
- The net use command accesses shared folders
- net user creates and deletes user accounts


Episode: Routers
Objective(s):
Core 1: 1.3 Given a scenario, set up and configure accessories and ports of mobile devices.
Core 1: 2.2 Compare and contrast common networking hardware.
Core 1: 3.1 Explain basic cable types and their connectors, features, and purposes.
Core 1: 2.6 Compare and contrast common network configuration concepts.
Core 2: 2.9 Given a scenario, configure appropriate security settings on small office/home office (SOHO) wireless and wired networks.

Episode Description

A+

The CompTIA A+ exams challenge test takers to perform many configurations of a typical home router. But what does a router do for a SOHO network?

CompTIA

Key Terms

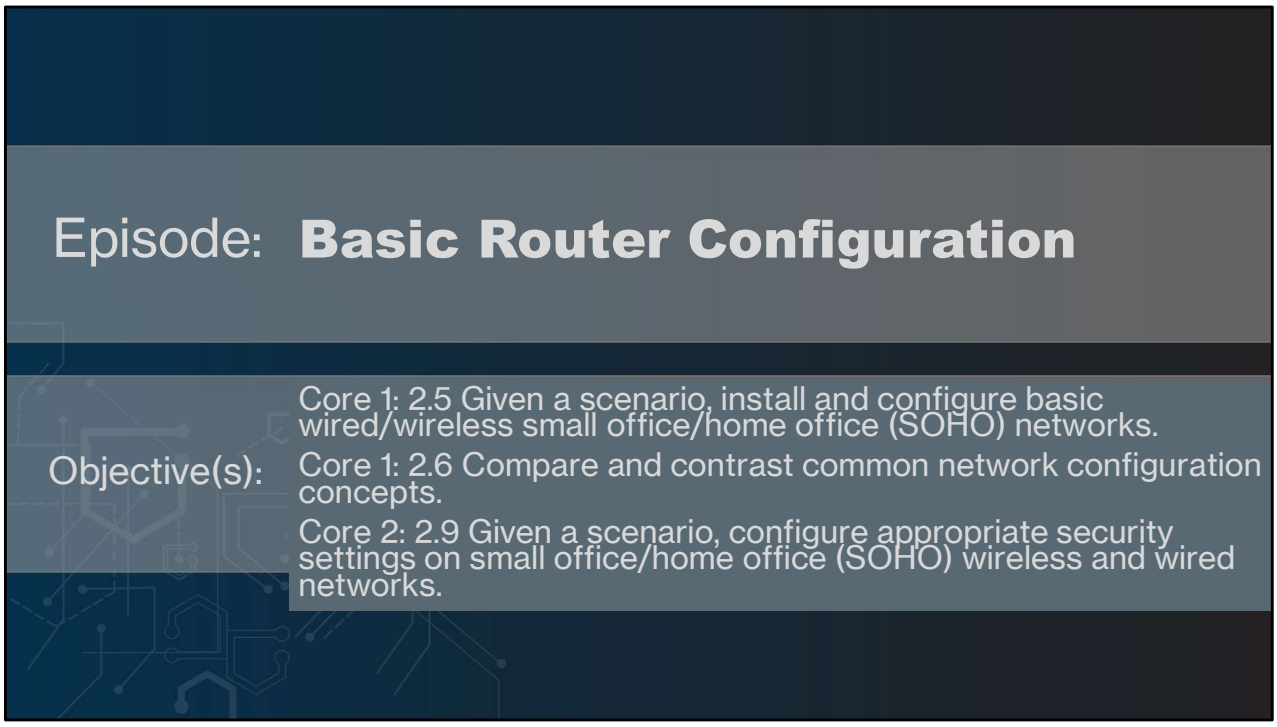
- 0:19 - Objective term - Routers filter and forward traffic based on IP traffic and connect systems on a LAN
- 4:15 - Router/switch with WAP
- 4:52 - DOCSIS
- 5:32 - Console port
- 5:35 - Objective term - Serial port
- 6:30 - Objective term - DB-9 connector

Key Terms

- 7:06 - Yost/Rollover cable
- 7:41 - Objective term - Small Office/Home Office (SOHO) router
- 7:59 - Objective term - DCHP range (scope)
- 8:24 - Default username and password
- 8:29 - Objective term - Change the default username and password!

Quick Review

- Routers filter and forward traffic based on IP addresses
- A routing table determines where to filter or forward IP packets
- Every routing table has a default gateway that sends all data unless otherwise specified
- A SOHO router is usually far more than a router


Episode: Basic Router Configuration
Objective(s):
Core 1: 2.5 Given a scenario, install and configure basic wired/wireless small office/home office (SOHO) networks.
Core 1: 2.6 Compare and contrast common network configuration concepts.
Core 2: 2.9 Given a scenario, configure appropriate security settings on small office/home office (SOHO) wireless and wired networks.

Episode Description

All routers share some basic configuration steps every tech must know. From router passwords to LAN IDs, this is the place to learn about these settings.

Key Terms

- 2:07 - Objective term - Static IP can be set on your WAN if required by your Internet Service Provider (ISP)
- 5:10 - Objective term - DHCP servers must be configured to hand out a pool (or scope) of IP addresses
- 5:38 - Objective term - DHCP lease limits the amount of time a client can use an IP address
- 6:53 - Objective term - DHCP reservations keep IP addresses for statically assigned clients
- 9:12 - Objective term - Firmware upgrade/update

Quick Review

- Configure both the WAN and LAN connections on your router
- Avoid default settings for basic configurations (IP, SSID, password, etc.)
- Static IP can be set on your WAN if required by your Internet Service Provider (ISP)
- Don't create too large of a DHCP pool
- DHCP reservations set aside IP addresses in the DHCP pool/scope

Episode: **Firewall Configuration**

Objective(s):

- Core 1: 2.2 Compare and contrast common networking hardware.
- Core 2: 1.6 Given a scenario, configure Microsoft Windows networking features on a client/desktop.
- Core 2: 2.1 Summarize various security measures and their purposes.
- Core 2: 2.5 Given a scenario, manage and configure basic security settings in the Microsoft Windows OS.
- Core 2: 2.9 Given a scenario, configure appropriate security settings on small office/home office (SOHO) wireless and wired networks.

Episode Description

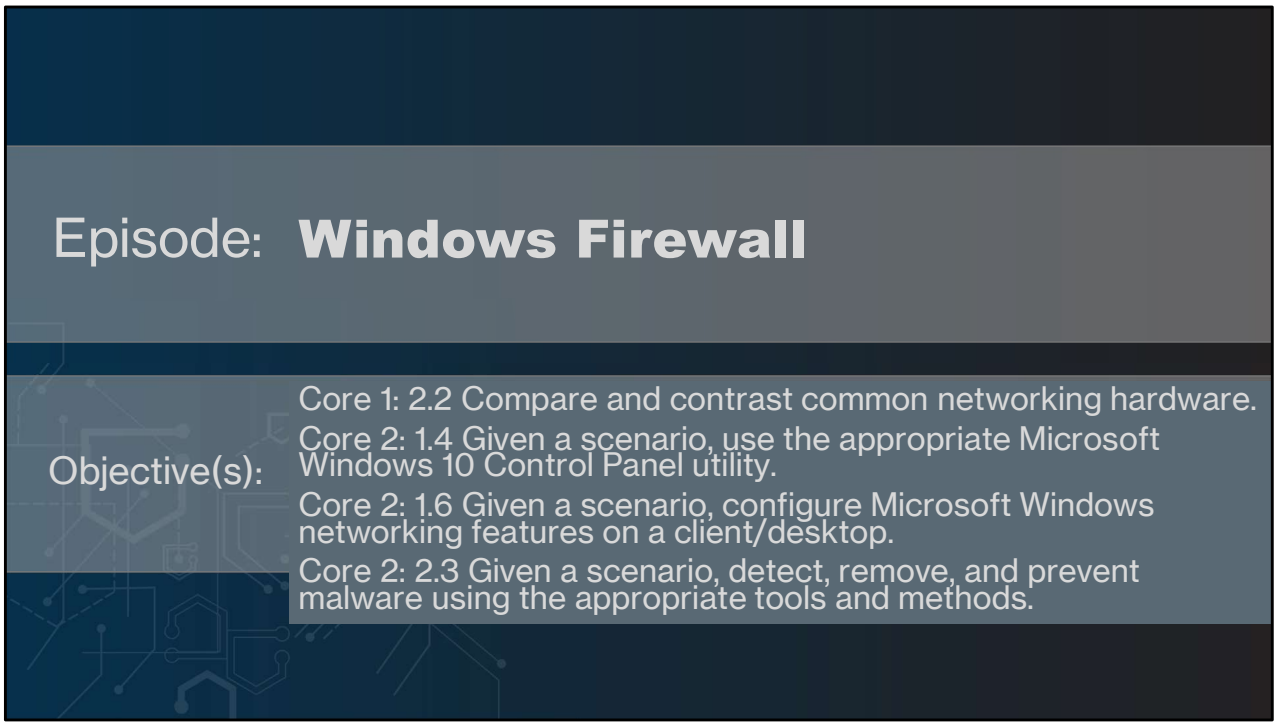
Setting up a hardware firewall is an obvious first step to making sure your network is protected. Even the most basic router has several different types of firewall settings – without proper configuration you'll either leave your network wide open, or so restricted no one can get work done.

Key Terms

- 0:23 - Objective term - Firewall
- 1:23 - Objective term - Access control list (ACL)
- 1:34 - Objective term - Principle of least privilege
- 1:56 - Objective term - Content filtering with deny list (blacklist) and allow list (whitelist)
- 3:13 - Stateless firewalls Stateful firewalls
- 5:17 - Access policy
- 7:14 - Objective term - Firewalls can be configured to block specific ports and applications
- 7:33 - Demilitarized zone (DMZ) or screened subnet
- 8:05 Real DMZ

Quick Review

- Firewalls are common on gateway routers
- The firewall's access control list (ACL) defines what may or may not forward or filter
- Stateless firewalls block on fixed criteria such as port number, time of day, URL, etc.
- Stateful firewalls block based on actions taking place at that moment (e.g., too may pings)


Episode: Windows Firewall
Objective(s):
Core 1: 2.2 Compare and contrast common networking hardware.
Core 2: 1.4 Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility.
Core 2: 1.6 Given a scenario, configure Microsoft Windows networking features on a client/desktop.
Core 2: 2.3 Given a scenario, detect, remove, and prevent malware using the appropriate tools and methods.

Episode Description

Like all operating systems, Windows comes with a built-in software firewall. Unlike the firewall on your router, this firewall only protects a single system. It's important for techs – and the users they support – to understand how to use the Windows firewall.

Key Terms

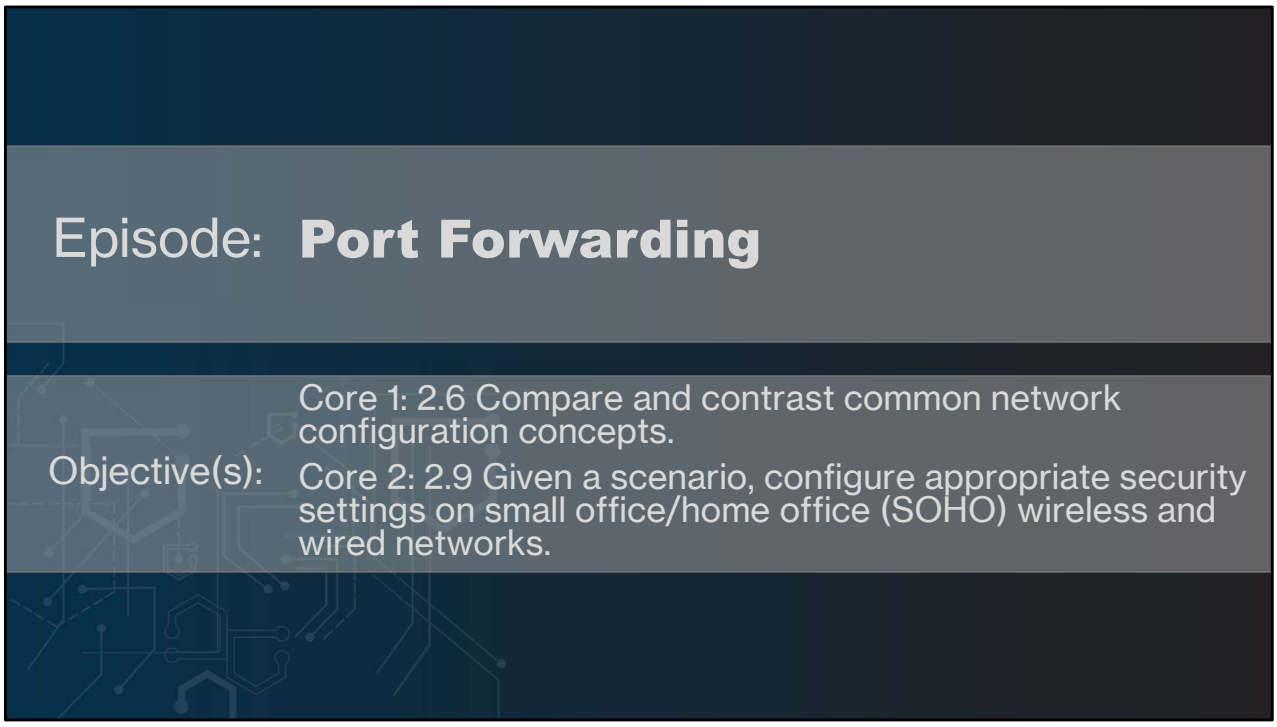
- 0:18 - Host firewall
- 0:21 - Network/edge firewall
- 1:17 - Objective term - Windows Defender Firewall (host-based software firewall)
- 1:40 - Active Directory domain network

Key Terms

- 1:44 - Objective term - Private network
- 1:52 - Objective term - Private/guest network
- 2:07 - Network discovery
- 5:54 - Objective term - Exception

Quick Review

- Windows Defender Firewall is a host-based software firewall that comes with Windows
- Host firewalls protect systems using host features such as file names or process IDs
- Defender Firewall has three settings: Domain, Public, and Private
- You can create exceptions manually if needed


Episode: Port Forwarding
Objective(s):
Core 1: 2.6 Compare and contrast common network configuration concepts.
Core 2: 2.9 Given a scenario, configure appropriate security settings on small office/home office (SOHO) wireless and wired networks.

Episode Description

NAT is a handy tool but comes with a huge drawback: no servers behind the firewall are accessible to the outside world. Port forwarding allows opening specific ports on your NAT-enabled router to provide access to servers behind it.

Key Terms

- 1:14 - Objective term - Port forwarding
- 4:52 - Objective term - Dynamic DNS

Quick Review

- A port forward is when a NAT router opens incoming traffic on a certain port access to a single system on the internal network
- You configure port forwarding on the NAT router
- We often use nonstandard port numbers for security reasons
- We use Dynamic DNS to give DNS names to port forwarded devices


Episode: Advanced Router Configuration
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: 2.9 Given a scenario, configure appropriate security settings on small office/home office (SOHO) wireless and wired networks.

Episode Description

Even the most basic router has setting beyond the basic setup. Protocols such as Quality of Service (QoS), Universal Plug and Play (UPnP), and Simple Network Management Protocol (SNMP) give extra features to enhance the capabilities of your router.

Key Terms

- 0:29 - Quality of Service (QoS)
- 3:55 - Objective term - Universal Plug and Play (UPnP)
- 5:04 - Link Layer Discovery Protocol
- 5:21 - Objective term - Simple Network Management Protocol (SNMP)

Quick Review

- Quality of service (QoS) gives control of network bandwidth by many different criteria
- Link Layer Discovery Protocol (LLDP) and Universal Plug and Play (UPnP) help with network device identification
- Simple Network Management Protocol (SNMP) enables querying of network devices

Episode: **VLANs**

Objective(s):

Core 1: 2.2 Compare and contrast common networking hardware.

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

Core 2: 2.5 Given a scenario, manage and configure basic security settings in the Microsoft Windows OS.

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

Episode Description

Virtual LANs (VLANs) are common features built into almost all switches. VLANs provide superb control of your LAN but have their own quirks that a good tech understands.

Key Terms

- 0:46 - Objective term- Virtual Local Area Network (VLAN)
- 1:55 - Objective term - Managed vs. unmanaged switch
- 5:59 - Objective term - Port security
- 6:35 - Objective term - Port security can disable ports
- 7:08 - Objective term - Software-defined networking (SDN)

Quick Review

- Virtual LANs (VLANs) enable network segmentation without adding hardware
- Configure VLAN-capable switches via IP address and web browser
- Use firmware interface for managing VLANs and enabling port security
- Software-defined networking (SDN) can lessen human error