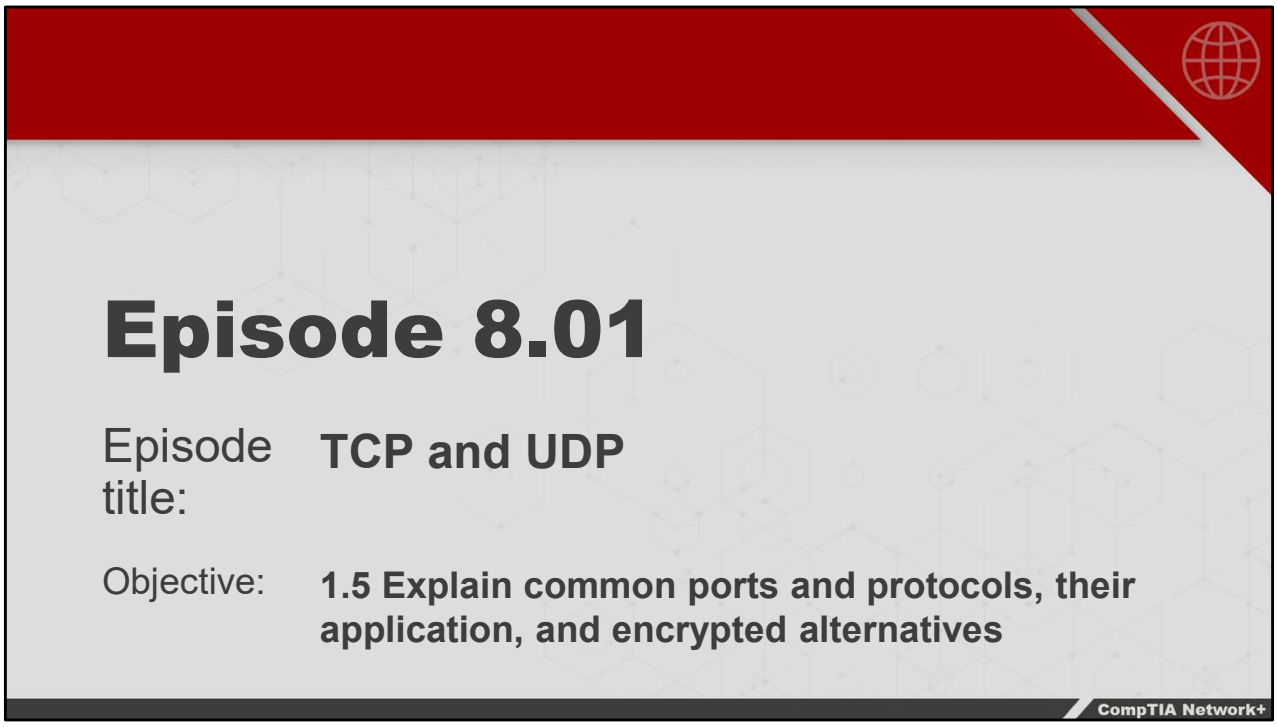
Chapter 8

Chapter 8


Episode 8.01
Episode title:
TCP and UDP
Objective:
1.5 Explain common ports and protocols, their application, and encrypted alternatives
CompTIA Network+

NOTE TO EDITORS

- Ethernet frame
- Protocol Data Units (PDU)
- TCP segment
- UDP datagram
- TCP connection-oriented
- UDP NOT connection-oriented
- TFTP uses UDP
- Internet uses TCP
- TCP 3-way handshake

Quick Review

- Ethernet frames are used by switches and routers
- PDU is the information used by the different protocols provided in frame segments
- TCP is connection-oriented; 2-way communication initiated by a 3-way handshake process (syn, syn-ack, ack)
- UDP is NOT a connection-oriented protocol, and has low overhead with one-way communication


Episode 8.02
Episode title:
ICMP and IGMP
Objective:
1.5 Explain common ports and protocols, their application, and encrypted alternatives
CompTIA Network+

NOTE TO EDITORS

- ICMP (Internet Control Message Protocol)
- IGMP (Internet Group Management Protocol)
- Multicast
- 224.ANYTHING
- ICMP & IGMP work with the internet layer (2) in the TCP/IP model

Quick Review

- ICMP is works at the Internet (2) layer in the TCI/IP model and the network (3) in the OSI model
- IGMP provides multicasting support
- Multicast addresses always start with 224


Episode 8.03
Episode title:
Handy Tools
Objective:
5.3 Given a scenario, use the appropriate network software tools and commands
CompTIA Network+

NOTE TO EDITORS

- Tracert (Windows) = traceroute (Linux)
- Pathping
- Bandwidth speedtester

Quick Review

- Both tracert (Windows) and traceroute (Linux) commands display the hops through a router to reach a destination
- Using the alternative command pathping can get a quicker ping response from the routers
- Bandwidth speed testing helps verify the upload and download speeds to an individual computer

Episode 8.04

Episode title: **Introduction to Wireshark**

Objective: **5.3 Given a scenario, use the appropriate network software tools and commands**

CompTIA Network+

NOTE TO EDITORS

- Protocol analyzer
- Alternative capture tool – tcpdump

Quick Review

- Wireshark is a protocol analyzer, integrated with a frame capture tool
- Wireshark displays the traffic flow of Ethernet frames, and can drill down into the frame-viewing various protocols, ports, timelines, and services
- Wireshark can segment and organize the data into consumable information to help in troubleshooting


8.05
Episode title:
Introduction to netstat
Objective:
5.3 Given a scenario, use the appropriate network software tools and commands
CompTIA Network+

NOTE TO EDITORS

- Netstat lists all the open ports and connections on your computer
- Netstat –n presents the results numerically
- Netstat –b shows the executable for every connection
- Netstat –o shows the executable and process id for every connection
- Netstat –a shows all the active ports
- Port 445 is also referred to as SMB 445
- Netstat –r shows the local routing table

Quick Review

- The netstat command lists all open ports and network connections on a computer
- Run netstat at the command prompt
- Make sure to know the netstat switches displayed in this episode


Episode 8.06
Episode title:
Web Servers
Objective:
1.5 Explain common ports and protocols, their application, and encrypted alternatives
CompTIA Network+

Key Terms

- Hypertext Transfer Protocol (HTTP)
- HTTP uses TCP port 80
- Primary Web server software:
- Microsoft IIS
- Apache (open source)
- Run netstat –a to check if a web server is running
- Network+ is more interested in web clients than servers

Key Terms

- Internet Explorer
- Chrome
- Firefox
- Safari
- HTTP Secure (HTTPS)
- HTTPS uses TCP port 443

Quick Review

- Web servers host Web sites: Web clients access Web servers
- HTTP uses TCP port 80 by default
- HTTPS uses TCP port 443 by default

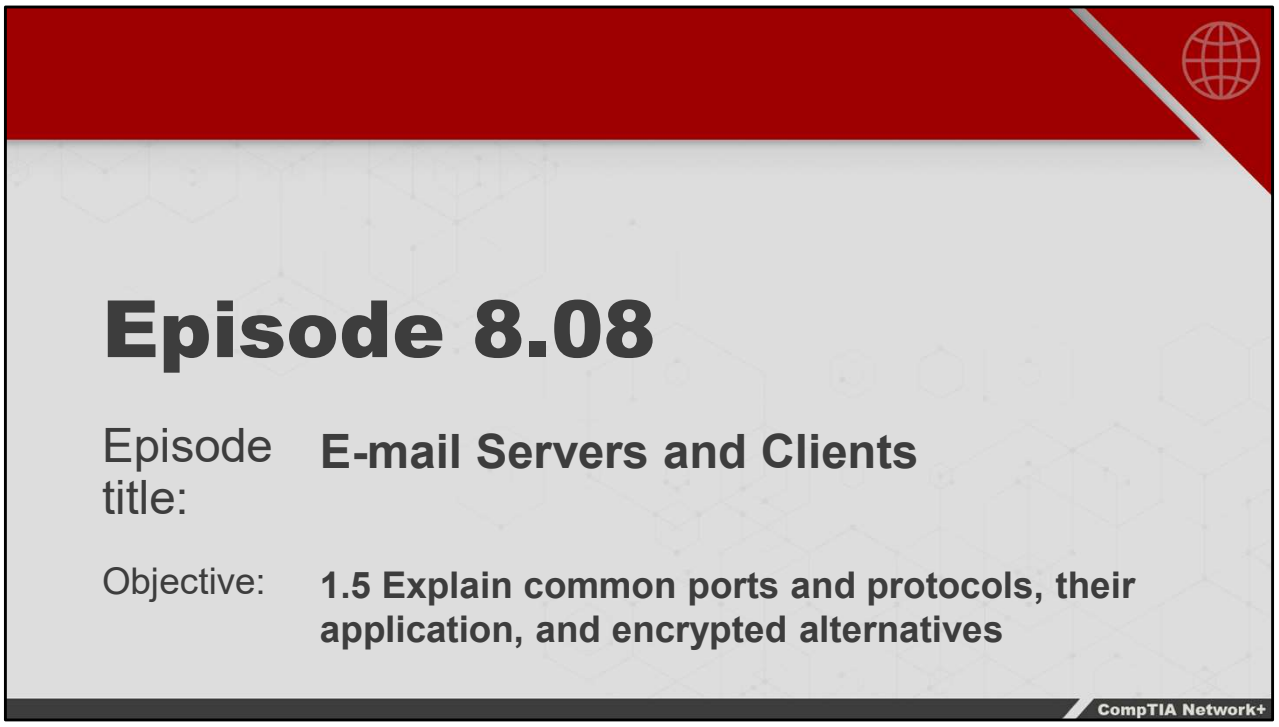

Episode 8.07
Episode title:
File Transfer Protocol (FTP)
Objective:
1.5 Explain common ports and protocols, their application, and encrypted alternatives
CompTIA Network+

NOTE TO EDITORS

- File Transfer Protocol
- FTP uses ports 21 and 20
- Anonymous accounts enable public access to FTP servers
- The GET command downloads and the PUT command uploads
- FTP is not an encrypted protocol
- SFTP (secure FTP) uses SSL and TLS
- TFTP (trivial FTP) uses UDP port 69

Quick Review

- FTP is a file transfer protocol, consider SFTP as a more secure method
- FTP servers listen on port 21 and send data back to the clients on port 20
- FTP is NOT encrypted so all passwords and data are sent in the clear


Episode 8.08
Episode title:
E-mail Servers and Clients
Objective:
1.5 Explain common ports and protocols, their application, and encrypted alternatives
CompTIA Network+

NOTE TO EDITORS

- SMTP (Simple Mail Transfer Protocol) – port 25
- POP3 (Post Office Protocol v3) – port 110
- IMAP (Internet Message Access Protocol v4) – port 143
- SMTP, POP3, and IMAP are not encrypted protocols

Quick Review

- SMTP uses port 25
- POP3 uses port 110
- IMAP uses port 143


Episode 8.09
Episode title:
Securing E-mail
Objective:
1.5 Explain common ports and protocols, their application, and encrypted alternatives
CompTIA Network+

Encrypting E-mail

- Traditional e-mail
  - SMTP port 25 – unencrypted
  - POP3 port 110 – unencrypted
  - IMAP port 143 – unencrypted

Encrypting E-mail

- Implementing TLS
  - IMAP 143 -> 993 encrypted
  - POP 110 -> 995 encrypted
  - SMTP 25 -> 465 encrypted

Encrypting E-mail

- STARTTLS
  - IMAP, POP3, SMTP – Port 465
  - TLS/STARTTLS conflicted with Port 465
  - STARTTLS changed to Port 587

Quick Review

- SMTP, POP3, and IMAP are unencrypted e-mail protocols
- Implementing unencrypted e-mail protocols with TLS has complex port assignments
- The STARTTLS extension uses only one port (587) for encrypted communication

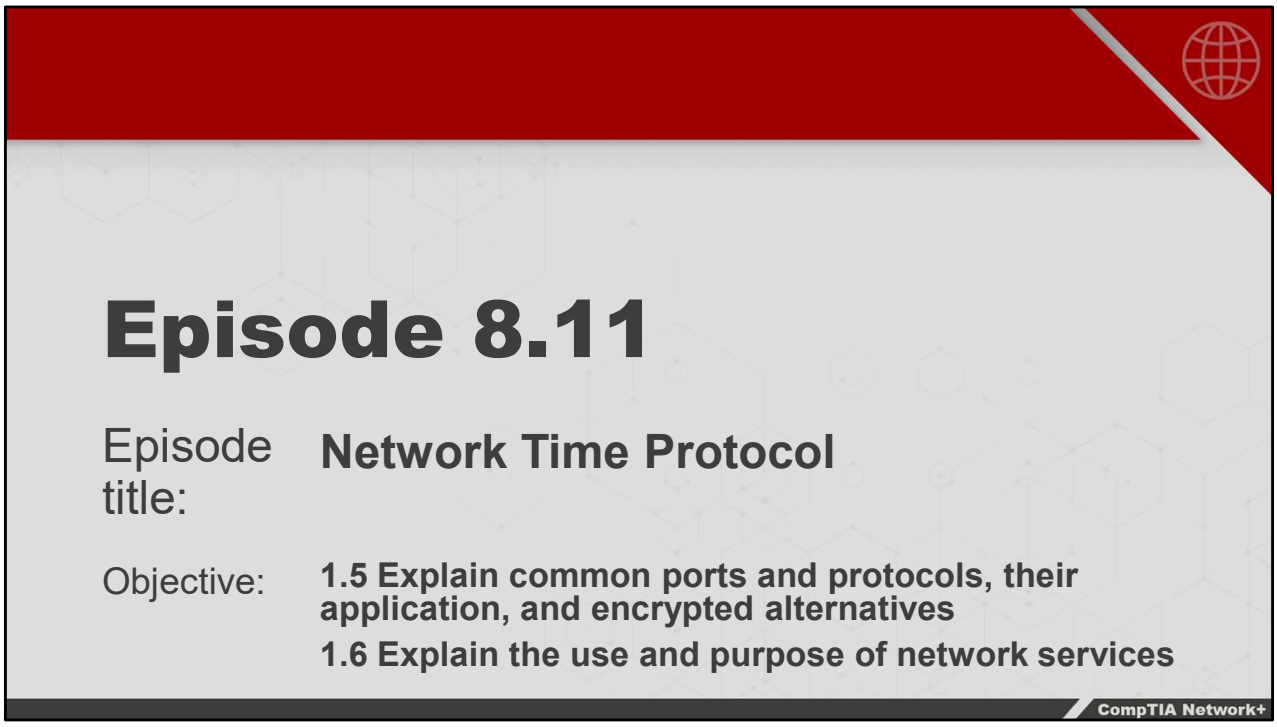

Episode 8.10
Episode title:
Telnet and SSH
Objective:
1.5 Explain common ports and protocols, their application, and encrypted alternatives
CompTIA Network+

NOTE TO EDITORS

- Telnet enables you to access a remote computer
- Telnet runs on TCP port 23
- PuTTY is a free, robust telnet/SSH client
- Telnet (unsecure) and SSH (secure) are both terminal emulators
- SSH (secure shell)
- SSH runs on TCP port 22
- SSH uses an authentication key
- Rlogin is not secure uses port 513 – replaced with SSH

Quick Review

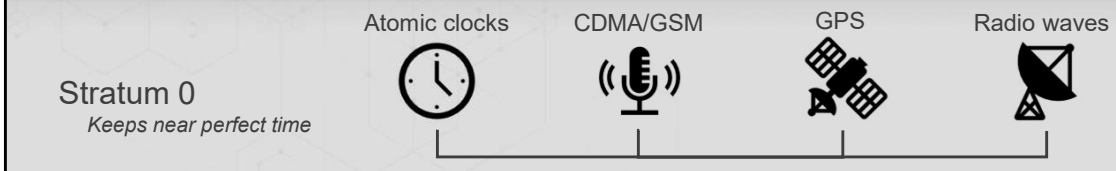
- Telnet is unencrypted and runs over TCP port 23
- SSH runs over port TCP port 22
- SSH is fully encrypted and has almost completely replaced telnet


Episode 8.11
Episode title:
Network Time Protocol
Objective:
1.5 Explain common ports and protocols, their application, and encrypted alternatives
1.6 Explain the use and purpose of network services
CompTIA Network+

Key Terms

- Network Time Protocol (NTP)
- Simple Network Time Protocol (SNTP)
- NTP/SNTP uses port 123
- NTP operates in a hierarchical fashion (clock strata)

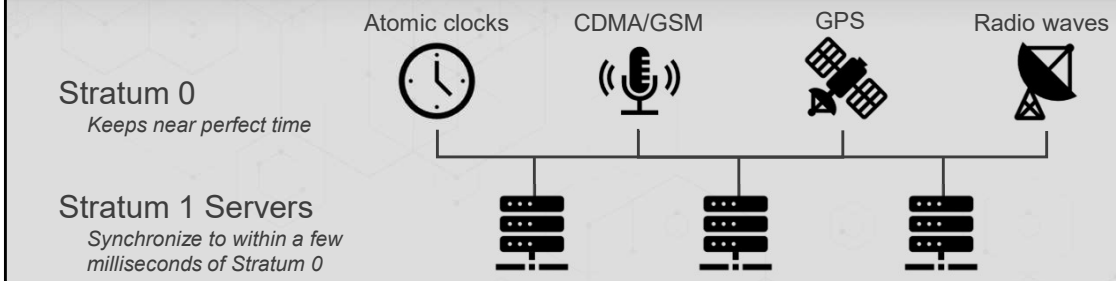
Network Time Protocol Strata



Stratum 0

Keeps near perfect time

Network Time Protocol Strata



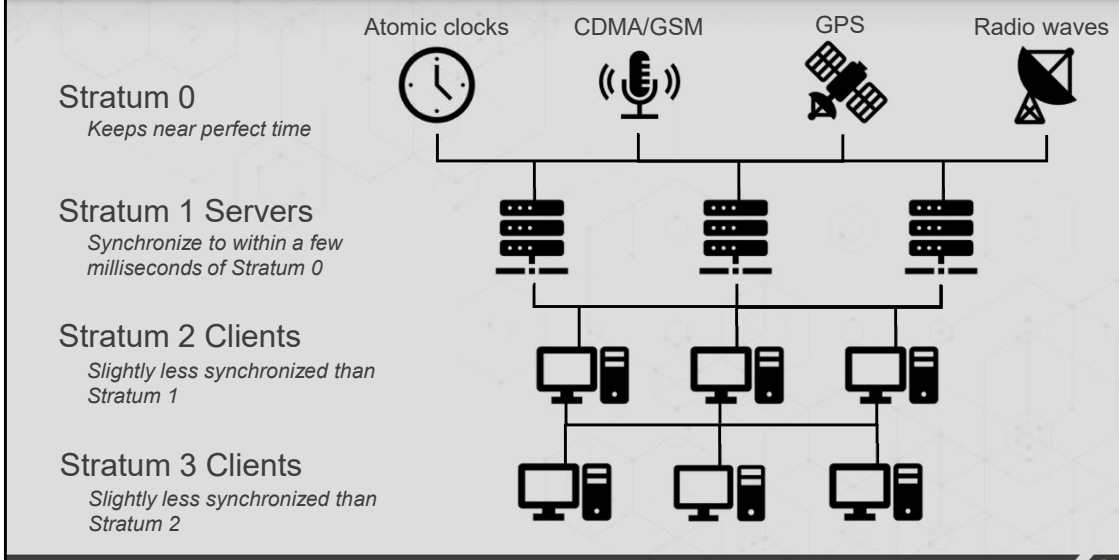
Stratum 0

Keeps near perfect time

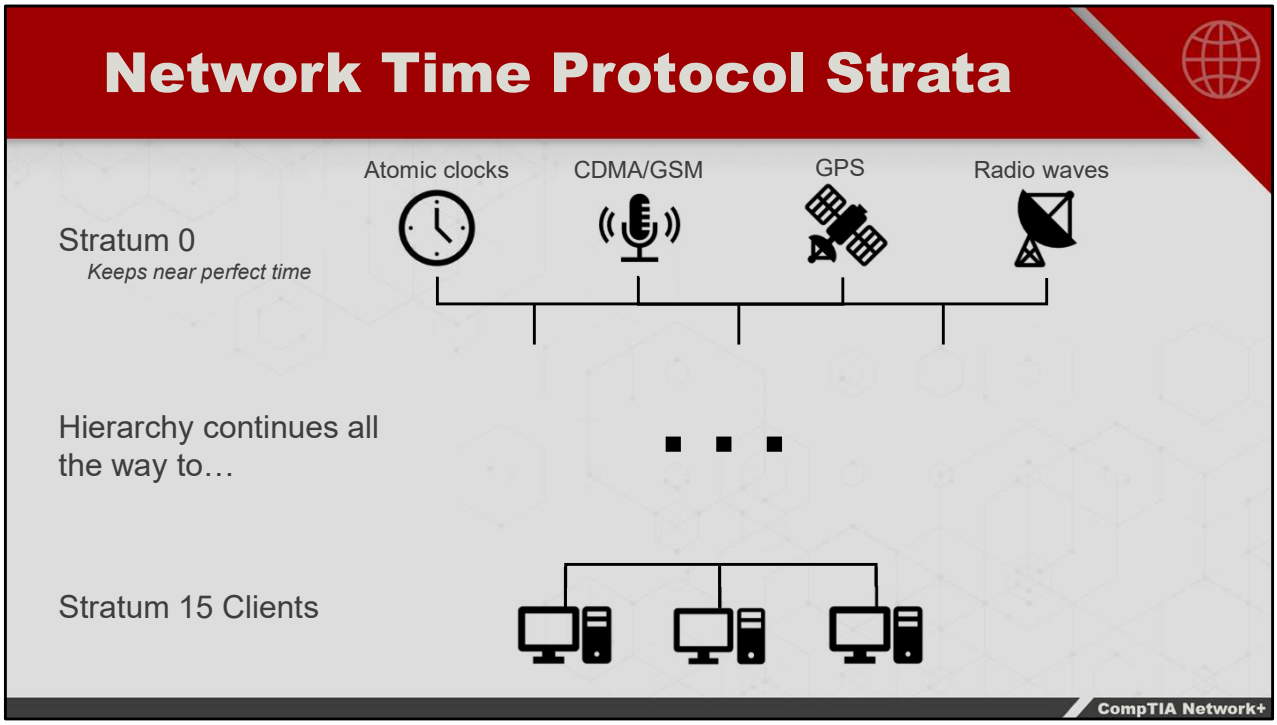
Stratum 1 Servers

Synchronize to within a few milliseconds of Stratum 0

Network Time Protocol Strata

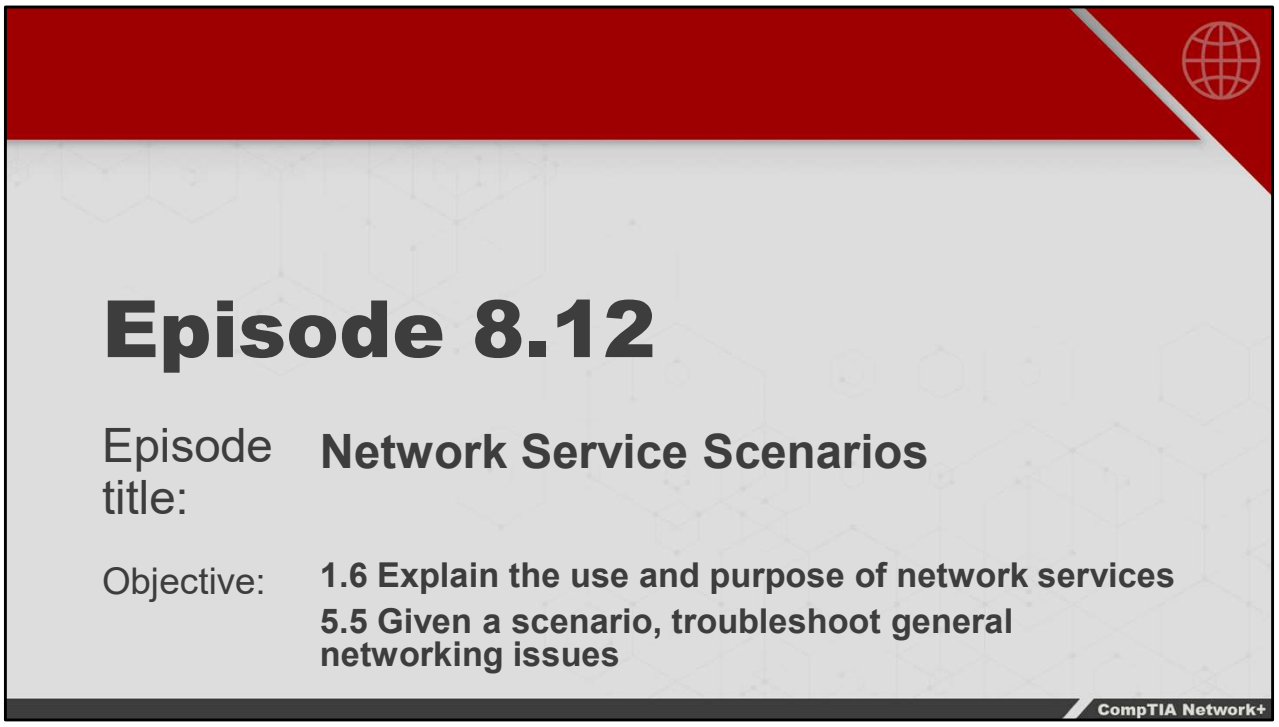


Network Time Protocol Strata



Quick Review

- Network Time Protocol (NTP) and Simple Network Time Protocol (SNTP) use UDP to allow devices to synchronize their clocks
- NTP operates in a hierarchical fashion or clock strata
- NTP uses port 123


Episode 8.12
Episode title:
Network Service Scenarios
Objective:
1.6 Explain the use and purpose of network services
5.5 Given a scenario, troubleshoot general networking issues
CompTIA Network+

NOTE TO EDITORS

- DHCP issues
- IP reservation
- MAC reservation
- Exhausted DHCP scope
- IPAM

Quick Review

- DHCP scope ranges need to consider gateway, printers, and other types of hosts to provide for IP reservations
- MAC reservations can be used to define devices that have top priority for address assignment
- IPAM tools track and manage allotted IP addresses, keeping address requirement available for server and VM farms