TestOut®

TestOut Network Pro - English 6.0.x

LESSON PLAN

Modified: 2021-11-12

Powered by LABSIM

Table of Contents

Introduction

1.1: Network Pro Introduction

Lecture Focus Questions:

- What are the course prerequisites?
- Which major topics are covered in the course?
- Which certification does this course prepare you for?

Video/Demo	Time
1.1.1 Network Pro Introduction	4:15
Total Video Time	**4:15**

Total Time
About 5 minutes

1.2: Use the Simulator

Summary

In this section, you will learn to:

- Read simulated component documentation and view components to make appropriate choices and meet the scenario's requirements.
- Add and remove simulated computer components.
- Change views and navigate between floors and buildings to view and add simulated components.
- Use the zoom feature to view additional image details.
- Use the simulation interface to identify where simulated cables connect to the computer.
- Attach simulated cables.
- Configure services on Hyper-V guest servers.

Video/Demo	Time
1.2.1 Use the Simulator	14:56
Total Video Time	**14:56**

Lab/Activity

- 1.2.2 Explore a Single Location in a Lab
- 1.2.3 Explore Multiple Locations in a Lab

Fact Sheets

- 1.2.4 Networking Rack Facts

Total Time

About 39 minutes

Networking Basics

2.1: Networking Overview

Lecture Focus Questions:

- Why are protocols important for networking?
- What are the advantages of a client-server network as compared to a peer-to-peer network?
- What is defined by the logical topology?
- How does the logical topology differ from the physical topology?
- Why can a single physical topology support multiple logical topologies?
- Why is a physical mesh topology normally an impractical solution?

Key terms for this section include the following:

Term	Definition
Internet Protocol address (IP address)	An address that identifies the network and host address assigned to a device.
Subnet address	The portion of the IP address that identifies the network the device is assigned to.
Local area network (LAN)	A group of computers and associated devices that share a common communications line or wireless link, typically to a server.
Metropolitan area network (MAN)	Computer users and resources within a geographic area the size of a metropolitan area that are connected.
Wide area network (WAN)	A network that connects several LANs. WANs are often limited to a corporation or an organization but are sometimes accessible to the public.
Software-defined wide area network (SDWAN)	A WAN that uses software to control connectivity.
Multipoint Generic Routing Encapsulation (mGRE)	A tunnel interface.
Internet	A collection of many networks owned by many entities that share information and communicate together.
Intranet	A local or restricted communications network, especially a private network created using World Wide Web software.

Extranet	An intranet that can be partially accessed by authorized outside users, enabling businesses to exchange information over the internet securely.
Topology	The term used to describe how devices are connected and how messages flow from device to device. The physical topology describes the way the network is wired. The logical topology describes the way messages are sent.
Terminator	A device that is connected to absorb signals and prevent them from reflecting repeatedly back and forth on the cable. Terminators are used with bus topology.

This section helps you prepare for the following certification exam objectives:

Exam	Objective

CompTIA Network+ N10-008	1.2 Explain the characteristics of network topologies and network types.
	
	• 1.2.1 Mesh
	• 1.2.2 Star/hub-and-spoke
	• 1.2.3 Bus
	• 1.2.4 Ring
	• 1.2.5 Hybrid
	• 1.2.6 Network types and characteristics
	  ○ Peer-to-peer
	  ○ Client-server
	  ○ Local area network (LAN)
	  ○ Metropolitan area network (MAN)
	  ○ Wide area network (WAN)
	  ○ Wireless local area network (WLAN)
	  ○ Personal area network (PAN)
	  ○ Campus area network (CAN)
	  ○ Storage area network (SAN)
	  ○ Software-defined wide area network (SDWAN)
	  ○ Multipoint generic routing encapsulation (mGRE)

Video/Demo	Time
2.1.1 Introduction to Networking	5:17
2.1.2 Network Types	9:02
2.1.3 Networking Terms	9:28
2.1.5 Network Topologies	7:09
Total Video Time	**30:56**

Fact Sheets

2.1.4 Networking Facts

2.1.6 Network Topology Facts

Number of Exam Questions
10 questions

Total Time
About 51 minutes

2.2: OSI Model and Data Encapsulation

Lecture Focus Questions:

- What is the OSI model? Why is it important for understanding networking?
- What are the advantages of using a theoretical model to describe networking?
- What is the name of Layer 3 in the OSI model? Layer 5?
- Which OSI model layers typically correspond to the network architecture?
- How does the session ID differ from the port number?
- Which OSI model layer would you find a frame at?
- What is the difference between connectionless and connection-oriented services?

The key terms for this section include:

Term	Definition
Open Systems Interconnection (OSI) Model	A reference model for how applications communicate over a network without regard to its underlying internal structure and technology.

This section helps you prepare for the following certification exam objectives:

Exam	Objective

CompTIA Network+ N10-008	1.1 Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts.
	• 1.1.1 OSI model
	  ○ Layer 1 - Physical
	  ○ Layer 2 - Data link
	  ○ Layer 3 - Network
	  ○ Layer 4 - Transport
	  ○ Layer 5 - Session
	  ○ Layer 6 - Presentation
	  ○ Layer 7 - Application

Video/Demo	Time
2.2.1 The OSI Model	3:03
2.2.3 OSI Model Layers	7:58
2.2.4 OSI Model Communications	3:16
Total Video Time	**14:17**

Fact Sheets

- 2.2.2 OSI Model Facts
- 2.2.5 OSI Layers Facts

Number of Exam Questions

10 questions

Total Time
About 35 minutes

2.3: Data Encapsulation

Lecture Focus Questions:

- How does data encapsulation facilitate data transmission?
- What are the TCP/IP encapsulation process steps on a sending host?
- What are the TCP/IP de-encapsulation process steps?
- What are TCP flags?
- How do packets and frames work?

Key terms for this section include the following:

Term	Definition
Transmission Control Protocol (TCP)	TCP is one of the main internet protocols. It allows computing devices and application devices to exchange messages over a network.
Address Resolution Protocol (ARP)	ARP is used to determine the MAC address of the host using the destination IP address.
Maximum transmission unit (MTU)	MTU is the largest size data unit that can be transmitted through the network.

This section helps you prepare for the following certification exam objectives:

Exam	Objective

CompTIA N10-008	1.1 Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts.
	• 1.1.2 Data encapsulation and decapsulation within the OSI model context
	  ○ Ethernet header
	  ○ Internet Protocol (IP) header
	  ○ Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) headers
	  ○ TCP flags
	  ○ Payload
	  ○ Maximum transmission unit (MTU)
	2.3 Given a scenario, configure and deploy common Ethernet switching features.
	• 2.3.8 Address Resolution Protocol (ARP)

Video/Demo	Time
2.3.1 Data Encapsulation	5:21

2.3.3 Address Resolution Protocol (ARP)	4:26
2.3.4 Packets and Frames	5:58
2.3.6 Three-Way Handshake and TCP Flags	3:28
Total Video Time	**19:13**

Fact Sheets

- 2.3.2 Data Encapsulation Facts
- 2.3.5 Network Communication Process Facts
- 2.3.7 Three-Way Handshake and TCP Flags Facts

Number of Exam Questions

10 questions

Total Time

About 45 minutes

2.4: Network Protocols

Lecture Focus Questions:

- How does a protocol suite differ from a protocol?
- How does TCP differ from UDP?
- What are the differences between the three email protocols (IMAP4, POP3, and SMTP)?
- How does SSH differ from Telnet? How does HTTPS differ from HTTP?

In this section, you will learn to:

- Explore network services

The key terms for this section include:

Term	Definition
Protocol	A protocol is a set of standards for communication between network hosts.
Internet Protocol suite	The Internet Protocol suite (frequently referred to as TCP/IP) is a conceptual model and set of communications protocols used on the internet and similar computer networks. The foundational protocols in this suite are Transmission Control Protocol (TCP) and Internet Protocol.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Network+ N10-008	1.5 Explain common ports and protocols, their application, and encrypted alternatives. • 1.5.1 File Transfer Protocol (FTP) 20/21 • 1.5.2 Secure Shell (SSH) 22 • 1.5.3 Secure File Transfer Protocol (SFTP) 22 • 1.5.4 Telnet 23 • 1.5.5 Simple Mail Transfer Protocol (SMTP) 25 • 1.5.6 Domain Name System (DNS) 53 • 1.5.7 Dynamic Host Configuration Protocol (DHCP) 67/68 • 1.5.8 Trivial File Transfer Protocol (TFTP) 69 • 1.5.9 Hypertext Transfer Protocol (HTTP) 80 • 1.5.10 Post Office Protocol v3 (POP3) 110 • 1.5.11 Network Time Protocol (NTP) 123 • 1.5.12 Internet Message Access Protocol (IMAP) 143 • 1.5.13 Simple Network Management Protocol (SNMP) 161/162 • 1.5.14 Lightweight Directory Access Protocol (LDAP) 389

- 1.5.15 Hypertext Transfer Protocol Secure (HTTPS) [Secure Sockets Layer (SSL)] 443
- 1.5.16 HTTPS [Transport Layer Security (TLS)] 443
- 1.5.17 Server Message Block (SMB) 445
- 1.5.18 Syslog 514
- 1.5.19 SMTP TLS 587
- 1.5.20 Lightweight Directory Access Protocol (over SSL) (LDAPS) 636
- 1.5.21 IMAP over SSL 993
- 1.5.22 POP3 over SSL 995
- 1.5.23 Structured Query Language (SQL) Server 1433
- 1.5.24 SQLnet 1521
- 1.5.25 MySQL 3306
- 1.5.26 Remote Desktop Protocol (RDP) 3389
- 1.5.27 Session Initiation Protocol (SIP) 5060/5061

Video/Demo	Time
2.4.1 TCP/IP Protocols	7:58
2.4.2 Common Network Services	5:59
2.4.3 Explore Network Services	8:43
Total Video Time	**22:40**

Fact Sheets

- 2.4.4 Network Port and Protocol Facts
- 2.4.5 Common Ports

Number of Exam Questions

10 questions

Total Time

About 43 minutes

Network Cabling and Hardware Devices

3.1: Copper Cables and Connectors

Lecture Focus Questions:

- Why are wires twisted together in twisted pair cables?
- What is the difference between STP cabling and UTP cabling?
- What is the difference between Cat 3, Cat 5e, and Cat 6a cables?
- How can you tell the difference between RJ11 and RJ45 connectors?
- You have an installation that requires Cat 5 cabling. Which cable ratings could you use for the installation?

In this section, you will learn to:

- Connect to an Ethernet network.
- Connect a cable modem.

The key terms for this section include:

Term	Definition
Crosstalk	An unwanted transfer of signals between communication channels.
Unshielded twisted pair (UTP)	Two twisted wires that carry the data signals (one conductor carries a positive signal; one carries a negative signal). Twisting the cables reduces the effects of electromagnetic interference (EMI) and crosstalk.
Shielded twisted pair (STP)	Shielded twisted pair (STP) has a grounded outer copper shield around the bundle of twisted pairs or around each pair. This provides added protection against EMI.
Plenum space	A plenum space is a part of a building that provides a pathway for the airflow needed by heating and air conditioning systems, such as above a dropped ceiling or below a raised floor.
Riser space	An area that connects multiple floors where cables can be run. This area cannot be a plenum space.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Network+ N10-008	1.3 Summarize the types of cables and connectors and explain which is the appropriate type for a solution. • 1.3.1 Copper ○ Twisted pair

        - Cat 5
        - Cat 5e
        - Cat 6
        - Cat 6a
        - Cat 7
        - Cat 8
    - Coaxial/RG-6
    - Twinaxial
    - Termination standards
        - TIA/EIA-568A
        - TIA/EIA-568B
- 1.3.3 Connector types
    - RJ11
    - RJ45
    - F-type connector

1.2 Explain the characteristics of network topologies and network types.

- 1.2.7 Service-related entry point
    - Demarcation point
    - Smartjack

Video/Demo	Time
3.1.1 Twisted Pair	11:30
3.1.4 Coaxial	4:56
Total Video Time	**16:26**

Lab/Activity

- 3.1.3 Connect to an Ethernet Network
- 3.1.6 Connect a Cable Modem

Fact Sheets

- 3.1.2 Twisted Pair Facts
- 3.1.5 Coaxial Cable Facts

Number of Exam Questions

10 questions

Total Time

About 61 minutes

3.2: Fiber Optic Cables and Connectors

Lecture Focus Questions:

- How do light waves within a fiber optic cable travel around corners?
- What advantages do fiber optic cables offer over twisted-pair cables and other media choices? What are the disadvantages of implementing fiber optic cables?
- What is the difference between single-mode and multi-mode cables?
- How can you tell the difference between an ST connector and an SC connector?
- Which connector types combine two strands of fiber into a single connector?
- What are media converters used for?

In this section, you will learn to:

- Connect fiber optic cables

The key terms for this section include:

Term	Definition
Light-emitting diode (LED)	A light-emitting diode is a two-lead semiconductor light source that emits visible light when an electric current passes through it.
Wavelength division multiplexing (WDM)	WDM joins several light wavelengths (colors) onto a single strand of fiber by using different wavelengths of laser light.

This section helps you prepare for the following certification exam objectives:

Exam	Objective

CompTIA Network+ N10-008	1.3 Summarize the types of cables and connectors and explain which is the appropriate type for a solution.
	• 1.3.2 Fiber
	  ○ Single-mode
	  ○ Multi-mode
	• 1.3.3 Connector types
	  ○ Local connector (LC), straight tip (ST), subscriber connector (SC), mechanical transfer (MT), registered jack (RJ)

Video/Demo	Time
3.2.1 Fiber Optic	10:53
Total Video Time	**10:53**

Lab/Activity

- 3.2.3 Connect Fiber Optic Cables

Fact Sheets

- 3.2.2 Fiber Optic Facts

Number of Exam Questions

10 questions

Total Time

About 38 minutes

3.3: Wiring Implementation

Lecture Focus Questions:

- What is the difference between the T568A and T568B standards? When should you use both standards?
- What type of cable would you use to connect two hosts together in a back-to-back configuration using twisted pair cable?
- When should you use stranded core twisted pair cable instead of solid core twisted pair?
- What is the difference between the MDF and an IDF?
- What type of cable connects an IDF to the MDF?
- Who is typically responsible for installing a demarc extension?
- What is the difference between a 25-pair block and a 50-pair block? What can you use to make the 50-pair block function like a 25-pair block?
- When you use a punch down tool, which way should the blade be facing?
- For what purpose is a patch panel used?

In this section, you will learn to:

- Use punch down blocks
- Connect patch panel cables

The key terms for this section include:

Term	Definition
Krone LSA-PLUS	A krone is an European-style telecommunications connector.
Building Industry Cross-Connect (BIX)	BIX is a cross-connect system. It consists of various sizes of punch down blocks, cable distribution accessories, and a punch down tool to terminate wires on the punch down block.
Power over Ethernet (PoE)	PoE is a technology that allows a single cable to provide both data and electrical power to devices such as wireless access points, IP cameras, and VoIP phones.
Pinout	When connecting two devices using twisted-pair cabling, the pinout determines which wire goes to which pin of the connector.
Local exchange carrier (LEC)	In the United States, LEC is a term used for a public telephone company that provides local services. LECs are sometimes called telcos.
Demarcation point (demarc)	The demarc is the line that marks the boundary between the telecommunications (telco) equipment and your private network or telephone system.
Main distribution	A frame or rack that is used to interconnect and manage telecommunication wiring in a building. It functions like an old-time

frame (MDF)	telephone switchboard, where operators used connecting wires to route telephone calls. MDF can also refer to the room that houses the traditional MDF along with networking patch panels.
Punch down block	A device that connects one group of wires to another through a system of metal pegs.
Patch panel	Patch panels permit circuits to be arranged and rearranged by plugging and unplugging respective patch cords on a mounted hardware assembly.

This section helps you prepare for the following certification exam objectives:

Exam	Objective

CompTIA Network+ N10-008	1.3 Summarize the types of cables and connectors and explain which is the appropriate type for a solution.
	
	• 1.3.4 Cable management
	  ○ Patch panel/patch bay
	  ○ Fiber distribution panel
	  ○ Punch down block
	  ▪ 66
	  ▪ 110
	  ▪ Krone
	  ▪ BIX

Video/Demo	Time
3.3.1 Twisted-Pair Cable Construction	9:16
3.3.3 Wiring Distribution	5:07
3.3.4 Use Punchdown Blocks	5:33
Total Video Time	**19:56**

Lab/Activity

- 3.3.6 Connect Patch Panel Cables 1
- 3.3.7 Connect Patch Panel Cables 2

Fact Sheets

- 3.3.2 Cable Construction Facts
- 3.3.5 Wiring Distribution Facts

Number of Exam Questions

10 questions

Total Time

About 64 minutes

3.4: Troubleshoot Network Media

Lecture Focus Questions:

- How do you prevent back reflection and optical return loss?
- What is the difference between a short circuit and an open circuit?
- What happens when you connect a single mode fiber to multimode fiber?
- What is the difference between a time-domain reflectometer and an optical time-domain reflectometer?
- Which tool would you use to test the bandwidth of an internet connection?
- Which cable types are immune to the effects of EMI?
- How does distance affect attenuation? How does distance affect impedance?
- What is the single best method to reduce the effects of an impedance mismatch?
- What is the difference between a regular cable tester and a cable certifier?
- Which tool would you use to find the end of a specific cable within a wiring closet?

The key terms for this section include:

Term	Definition
Electromagnetic interference (EMI)	An external signal that interferes with normal network communications. Common sources of EMI include nearby generators, motors (such as elevator motors), radio transmitters, welders, transformers, and fluorescent lighting. When working with the radio frequency spectrum, this is known as radio frequency interference (RFI).
Crosstalk	Interference caused by signals within twisted pairs of wires. For example, current flow on one twisted pair causing a current flow on an adjacent pair.
Attenuation	The loss of signal strength from one end of a cable to the other. This is also known as dB loss.
Electrical short	A situation in which an electrical signal takes a path other than the intended path. In the case of twisted pair wiring, a short means that a signal sent on one wire arrives on a different wire.
Open circuit	A condition that results from a cut in the wire preventing the original signal from reaching the end of the wire. An open circuit is different from a short in that the signal stops with an open circuit. Electricity cannot flow because the path is disconnected.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Network Pro	1.1 Place objective here • Place sub objectives here ○ And here if needed

CompTIA Network+ N10-008	5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.
	• 5.2.1 Specifications and limitations
	  ○ Throughput
	  ○ Speed
	  ○ Distance
	• 5.2.2 Cable considerations
	  ○ Shielded and unshielded
	  ○ Plenum and riser-rated
	• 5.2.3 Cable application
	  ○ Rollover cable/console cable
	  ○ Crossover cable
	  ○ Power over Ethernet
	• 5.2.4 Common issues
	  ○ Attenuation
	  ○ Interference
	  ○ Decibel (dB) loss
	  ○ Incorrect pinout
	  ○ Bad ports
	  ○ Open/short
	  ○ Light-emitting diode (LED) status indicators
	  ○ Incorrect transceivers
	  ○ Duplexing issues
	  ○ Transmit and receive (TX/RX) reversed
	  ○ Dirty optical cables
	• 5.2.5 Common tools
	  ○ Cable crimper
	  ○ Punch down tool
	  ○ Tone generator
	  ○ Loopback adapter
	  ○ Optical time-domain reflectometer (OTDR)
	  ○ Multimeter
	  ○ Cable tester
	  ○ Wire map
	  ○ Tap
	  ○ Fusion splicers
	  ○ Spectrum analyzers
	  ○ Snips/cutters
	  ○ Cable stripper
	  ○ Fiber light meter

Video/Demo	Time
3.4.1 Troubleshoot Copper Wiring Issues	13:53
3.4.3 Troubleshoot Fiber Optic Wiring Issues	7:23

3.4.5 Troubleshooting Tools	6:09
Total Video Time	**27:25**

Fact Sheets

- 3.4.2 Copper Wiring Troubleshooting Facts
- 3.4.4 Fiber Optic Wiring Troubleshooting Facts
- 3.4.6 Troubleshooting Tools Facts

Number of Exam Questions

10 questions

Total Time

About 53 minutes

3.5: Network Adapters

Lecture Focus Questions:

- What are two major differences between a modem and an Ethernet network interface card (NIC)?
- How can you identify a network card manufacturer from the MAC address on the NIC?
- What is the function of a transceiver?
- What is the purpose of the cyclic redundancy check (CRC)?
- At which OSI layer does a network adapter card operate? At which layer does a media converter work?
- Can you use a media converter to connect network segments that use different architecture types? Why or why not?
- How does a computer find the MAC address of another device on the same subnet?
- What does the MAC address FF-FF-FF-FF-FF-FF indicate?

In this section, you will learn to:

- Select and install a network adapter
- Connect a media converter

The key terms for this section include:

Term	Definition
Network interface card	A hardware device that connects a computer to the network medium. It is responsible for converting binary data into a format that can be sent on the network medium. A NIC is also called a network adapter.
Gigabit interface converter (GBIC)	A transceiver that converts electrical signals to optical signals and vice versa in fiber optic and Ethernet systems.
Small form-factor pluggable (SFP)	A transceiver that is similar to a GBIC but is smaller in size. An SFP is sometimes called a mini-GBIC.
XFP	A 10-Gigabit small form-factor pluggable transceiver that is similar to an SFP in size but is used for 10-Gigabit networking.
QSFP	A quad (4-channel) small form-factor compact hot-pluggable transceiver that is also used for data communication applications.
Media access control (MAC)	A unique identifier burned into the ROM of every Ethernet NIC. The first half of the MAC address (the first six digits) is assigned to each manufacturer. The manufacturer determines the rest of the address, assigning a unique value that identifies the host address.

Address Resolution Protocol (ARP)	A protocol that hosts use to discover the MAC address of a device from its IP address.
Reverse Address Resolution Protocol (RARP)	A protocol that hosts use to find the IP address of a host with a known MAC address.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Network Pro	1.1 Place objective here • 1.1.1 Place sub objectives here ○ And here if needed

CompTIA Network+ N10-008	1.3 Summarize the types of cables and connectors and explain which is the appropriate type for a solution.
	• 1.3.3 Connector types
	  ○ Transceivers/media converters
	  ○ Transceiver type
	  ▪ Small form-factor pluggable (SFP)
	  ▪ Enhanced form-factor pluggable (SFP+)
	  ▪ Quad small form-factor pluggable (QSFP)
	  ▪ Enhanced quad small form-factor pluggable (QSFP+)
	2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.
	• 2.2.1 Networking devices
	  ○ Media converter

Video/Demo	Time
3.5.1 Network Adapters	8:35
Total Video Time	**8:35**

Lab/Activity

- 3.5.3 Select and Install a Network Adapter
- 3.5.4 Connect a Media Converter

Fact Sheets

3.5.2 Network Adapter Facts

Number of Exam Questions
10 questions

Total Time
About 48 minutes

3.6: Networking Devices

Lecture Focus Questions:

- A host on a network sends a frame to the hub. Which other devices on the network will see this frame?
- A host on a network sends a frame to a switch. Which other devices on the network will see this frame?
- What are the similarities and differences between a bridge and a switch?
- What are the advantages of using switches instead of hubs?
- At which OSI model layer do wireless access points operate?
- What type of device do you use to translate from one network architecture to another?

In this section, you will learn to:

- Install a switch
- Select a networking device
- Select a home router

The key terms for this section include:

Term	Definition
Hub	The central connecting point of a physical star. It uses a logical bus topology.
Bridge	A device that connects two (or more) media segments on the same subnet. It filters traffic between both segments based on the MAC address in the frame.
Switch	A multi-port bridge that performs filtering based on MAC addresses and provides additional features not found in a bridge.
Router	A device that connects two or more network segments or subnets.
Wireless access point (AP)	A hub for a wireless network. As with a hub, a message sent to any wireless host connected to the AP can be received by all other wireless hosts.
Firewall	A network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
Layer 3 switch	A switch capable of reading Layer 3 (network) addresses and routing packets between subnets.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Network Pro	1.2 Implement wired and wireless devices • 1.2.3 Create a home wireless network

CompTIA Network+ N10-008	• 1.2.5 Connect network components
	
	2.2 Configure routers and switches
	
	• 2.2.1 Configure switches
	
	2.1 Compare and contrast various devices, their features, and their appropriate placement on the network
	
	• 2.1.1 Networking devices
	  ○ Layer 2 switch
	  ○ Layer 3 capable switch
	  ○ Router
	  ○ Hub
	  ○ Access point
	  ○ Bridge
	  ○ Wireless LAN controller
	  ○ Load balancer
	  ○ Proxy server
	  ○ Cable modem
	  ○ DSL modem
	  ○ Repeater
	  ○ VPN headend
	
	3.2 Explain the purpose of organizational documents and policies
	
	• 3.2.3 Common documentation
	  ○ Physical network diagram
	  ▪ Physical network diagram - floor plan
	  ▪ Physical network diagram - rack diagram
	  ▪ Physical network diagram - intermediate distribution frame (IDF)/main distribution frame (MDF) documentation
	  ○ Logical network diagram
	  ○ Wiring diagram

Video/Demo	**Time**
3.6.1 Networking Devices	10:11
3.6.5 Internetwork Devices	6:29
3.6.8 Data Center Device Installation	7:40
Total Video Time	**24:20**

Lab/Activity

- 3.6.3 Install a Switch

- 3.6.4 Select a Networking Device
- 3.6.7 Configure a Home Router

Fact Sheets

- 3.6.2 Network Device Facts
- 3.6.6 Internetwork Device Facts
- 3.6.9 Data Center Device Installation Facts

Number of Exam Questions

10 questions

Total Time

About 86 minutes

Network Addressing and Services

4.1: IP Addressing

Lecture Focus Questions:

- What is the format of an IPv4 address?
- What is the purpose of a subnet mask?
- What are the different classes of IPv4 addresses?
- What is the purpose of subnetting?
- What formula is used to calculate the number of hosts per subnet?
- What does /14 mean in the following IP address: 199.78.11.12/14?

In this section, you will learn to:

- Configure IP addresses on a workstation
- Configure IP addresses on an iPad
- Configure IP addresses on mobile devices

The key terms for this section include:

Term	Definition
Octet	An 8-bit binary number. An IPv4 address consists of four octets separated by a dot.
Subnet mask	A 32-bit number that defines which portion of an IPv4 address identifies the network address and which portion of the address defines the host address.
Internet Assigned Numbers Authority (IANA)	A nonprofit, private American corporation that oversees global IP address allocation, autonomous system number allocation, root zone management in the Domain Name System, media types, and other Internet Protocol-related symbols and internet numbers.
Public IP	An IP address that is used to access the internet.
Private IP	An IP address that is used only on an internal network. These IP addresses do not go out on the internet.
Automatic Private IP Addressing (APIPA)	A feature that allows a device to automatically assign itself an IP address on the 169.254.0.0 network when a DHCP server or manual configuration is unavailable.
Loopback address	This special address is also known as home or localhost. This address is reserved by each network interface card (NIC) and is used for testing purposes. Ping requests can be sent to this address and if returned means that the NIC is capable of sending and receiving data packets.

Broadcast address	The last valid IP address on a network. It is reserved for broadcast functions. Any packet sent to this address will be sent to all devices on the network.
Network address	The first valid IP address on the network. This address is used for routing purposes to identify the network.
Subnetting	The process of dividing a large network into smaller networks.
Fixed-length subnet mask (FLSM)	Subnetting method in which each created subnet has an equal number of addresses.
Variable-length subnet mask (VLSM)	Subnetting method in which each subnet can be a different size.
Classless Inter-Domain Routing (CIDR)	A method for allocating IP addresses and for IP routing. CIDR notation is a simplified method of writing a network address with a slash followed by the number of bits in the network ID.
ANDing	The process used to determine the network address/ID.
Supernetting	The process of combining two or more networks.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Network Pro	2.1 Configure IP addressing • 2.1.1 - Configure IP addresses 1.4 Given a scenario, configure a subnet and use appropriate IP addressing schemes.

CompTIA Network+ N10-008	• 1.4.1 Public vs. Private
	  ○ RFC1918
	• 1.4.3 IPv4 subnetting
	  ○ Classless (variable-length subnet mask)
	  ○ Classful
	  ▪ A
	  ▪ B
	  ▪ C
	  ▪ D
	  ▪ E
	  ○ Classless Inter-Domain Routing (CIDR) notation

Video/Demo	Time
4.1.1 Numbering Systems	9:31
4.1.3 IP Addresses	8:55
4.1.5 Subnets Part 1	9:44

4.1.6 Subnets Part 2	6:10
4.1.8 IP Address Assignment	6:43
4.1.10 Configure IP Settings on Workstation	2:24
4.1.12 Configure IP Address on iPad	2:23
Total Video Time	**45:50**

Lab/Activity

- 4.1.11 Configure IP Addresses
- 4.1.13 Configure IP Addresses on Mobile Devices

Fact Sheets

- 4.1.2 Numbering System Facts
- 4.1.4 IP Address Facts
- 4.1.7 Subnet Facts
- 4.1.9 IP Address Assignment Facts

Number of Exam Questions

10 questions

Total Time

About 100 minutes

4.2: APIPA and Alternate Addressing

Lecture Focus Questions:

- How do you know if a host is using an Automatic Private IP Addressing (APIPA) address?
- Which IP configuration parameters are set when APIPA is used? Which parameters are not set?
- In which scenarios would an alternate IP configuration simplify IP configuration?

In this section, you will learn to:

- Set up alternate addressing
- Configure alternate addressing

The key terms for this section include:

Term	Definition
APIPA	The Windows function that provides DHCP autoconfiguration addressing. APIPA is enabled by default on most modern operating systems, including Windows and Linux.
Alternate IP configuration	A manual configuration of a computer's IP address, default gateway, DNS server address, and WINS address. This configuration is used if the DHCP server fails to provide this similar information.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Network Pro	1.1 Place objective here • Place sub objectives here ○ And here if needed
CompTIA Network+ N10-008	1.4 Given a scenario, configure a subnet and use appropriate IP addressing schemes. • 1.4.2 IPv4 vs. IPv6 ○ Automatic Private IP Addressing (APIPA)

Video/Demo	Time
4.2.1 APIPA	4:04
4.2.2 Set Up Alternate Addressing	3:32
Total Video Time	**7:36**

Lab/Activity

- 4.2.4 Configure Alternate Addressing

Fact Sheets

- 4.2.3 APIPA and Alternate IP Addressing Facts

Number of Exam Questions

10 questions

Total Time

About 35 minutes

4.3: DHCP

Lecture Focus Questions:

- What type of configuration parameters can be delivered using DHCP?
- What is a DHCP scope?
- What type of devices can be used as a DHCP server?
- What are the advantages of static IP address assignments?
- When would you use static IP addressing?

In this section, you will learn to:

- Configure a DHCP server
- Configure DHCP options
- Create DHCP exclusions
- Create DHCP client reservations

The key terms for this section include:

Term	Definition
IP range	The range of IP addresses that the DHCP server can assign.
Subnet mask	The structure of an IP address that defines the network ID and host ID.
Exclusions	IP addresses that the DHCP server will not assign.
Reservations	Static IP addresses that are not dynamically assigned by the DHCP server.
DHCP lease time	The specified amount of time that an IP configuration assigned by DHCP is valid. It is specified when a device is assigned an IP configuration.
Default gateway	The gateway where data packets that are leaving the network should go to be routed.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Network Pro	3.1 Manage DHCP services • 3.1.1 Implement a DHCP server • 3.1.2 Configure DHCP options

CompTIA Network+ N10-008	1.6 Explain the use and purpose of network services.
	• 1.6.1 DHCP
	  ○ Scope
	  ○ Exclusion ranges
	  ○ Reservation

- Dynamic assignment
- Static assignment
- Lease time
- Scope options
- Available leases
- DHCP relay
- IP helper/UDP forwarding

Video/Demo	Time
4.3.1 DHCP	6:50
4.3.3 Configure a DHCP Server	10:45
4.3.5 DHCP Options	10:40
4.3.9 Configure Client Addressing	2:21
4.3.10 Troubleshoot DHCP Exhaustion	4:09
Total Video Time	**34:45**

Lab/Activity

- 4.3.4 Configure a DHCP Server
- 4.3.6 Configure DHCP Options
- 4.3.7 Create DHCP Exclusions
- 4.3.8 Create DHCP Client Reservations

Fact Sheets

- 4.3.2 DHCP Facts

Number of Exam Questions

10 questions

Total Time

About 98 minutes

4.4: DHCP Relay

Lecture Focus Questions:

- What is the purpose of a DHCP relay agent?
- What is the purpose of an IP helper? How does it differ from a DHCP relay agent?
- What is a DHCP Discover packet?

In this section, you will learn to:

- Configure a DHCP relay agent
- Add a DHCP server on another subnet

The key terms for this section include:

Term	Definition
DHCP relay agent	A network device used to forward DHCP requests to a DHCP server located on another network.
IP helper	A command that performs the same actions as a DHCP relay agent except that it does so for other UDP-based protocols, such as NTP.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Network Pro	3.1 Manage DHCP services • 3.1.1 Implement a DHCP server • 3.1.2 Configure DHCP options

CompTIA Network+ N10-008	1.6 Explain the use and purpose of network services.
	• 1.6.1 DHCP
	  ○ DHCP relay
	  ○ IP helper/UDP forwarding

Video/Demo	Time
4.4.1 DHCP Relay	4:21
4.4.2 Configure DHCP Relay	5:52
Total Video Time	**10:13**

Lab/Activity

- 4.4.4 Configure a DHCP Relay Agent
- 4.4.5 Add a DHCP Server on Another Subnet

Fact Sheets

- 4.4.3 DHCP Relay Facts

Number of Exam Questions

10 questions

Total Time

About 50 minutes

4.5: DNS

Lecture Focus Questions:

- How are hostnames organized in Domain Name Service (DNS)?
- What is the difference between a forward lookup zone and a reverse lookup zone?
- What is the role of the root servers in DNS?
- In DNS, what is the difference between a zone and a domain?
- What is the difference between an A record and a PTR record?

In this section, you will learn to:

- Configure DNS addresses
- Create standard DNS zones
- Create host records
- Create CNAME records
- Troubleshoot DNS records

The key terms for this section include:

Term	Definition
Fully qualified domain name (FQDN)	A domain name that spells out each level of the hierarchy separated by periods. The final period (which is for the root domain) is often omitted and only implied.
DNS zone	The administrative portion of the DNS namespace used to maintain and define the domain namespace.
Forward lookup zone	The portion of the DNS namespace that resolves the hostname to the IP address.
Reverse lookup zone	The portion of the DNS namespace that resolves the IP address to the hostname.
Records	Database entries that store information. For DNS, the records store hostnames, IP addresses, etc., in the zone database. Each host has at least one record in the DNS database that maps the hostname to the IP address.
Root server	Servers that hold information for the root zone (.). Root servers answer name resolution requests by supplying the address of the corresponding top-level DNS server.
Top-level domain (TLD) server	Servers that contain the information for all websites that share a common domain extension, such as .com or .org.
Authoritative name server	A server that contains the DNS information for a site. The server is authoritative because it doesn't have to ask any other DNS server for help because it holds the information already.
Recursive server	A server that handles the DNS name resolution process.

HOSTS file	A local text file on each computer that maps hostnames to IP addresses.
Dynamic DNS (DDNS)	A method that enables clients or the DHCP server to update records in the zone database. Without dynamic updates, all A (host) and PTR (pointer) records must be configured manually. With dynamic updates, host records are created and deleted automatically whenever the DHCP server creates or releases an IP address lease.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Network Pro	3.2 Manage DNS services • 3.2.1 Configure DNS addresses • 3.2.2 Create standard DNS zones 5.1 Troubleshoot configuration and services • 5.1.3 Troubleshoot DNS records

CompTIA Network+ N10-008	1.6 Explain the use and purpose of network services.
	
	• 1.6.2 DNS
	  ○ Record Types
	  ▪ Address (A)
	  ▪ Canonical name (CNAME)
	  ▪ Mail exchange (MX)
	  ▪ Authentication, authorization, accounting, auditing (AAAA)
	  ▪ Start of authority (SOA)
	  ▪ Pointer (PTR)
	  ▪ Text (TXT)
	  ▪ Service (SRV)
	  ▪ Name server (NS)
	
	  ○ Global hierarchy
	  ▪ Root DNS servers
	  ▪ Internal vs. external
	  ▪ Zone transfers
	  ▪ Authoritative name servers
	  ▪ Time to live (TTL)
	  ▪ DNS caching
	  ▪ Reverse DNS/reverse lookup/forward lookup

- Recursive lookup/iterative lookup

Video/Demo	Time
4.5.1 DNS - Record Types	14:20
4.5.3 Configure DNS	11:36
4.5.9 Configure DNS Caching on Linux	4:23
Total Video Time	**30:19**

Lab/Activity

- 4.5.4 Configure DNS Addresses
- 4.5.5 Create Standard DNS Zones
- 4.5.6 Create Host Records
- 4.5.7 Create CNAME Records
- 4.5.8 Troubleshoot DNS Records

Fact Sheets

- 4.5.2 DNS Facts

Number of Exam Questions

10 questions

Total Time

About 106 minutes

4.6: NTP

Lecture Focus Questions:

- How does Network Time Protocol (NTP) handle time drift?
- What type of devices are authoritative time sources?
- How does slam differ from slew in correcting time?
- How is the concept of stratum implemented by NTP?

In this section, you will learn to:

- Configure NTP

The key terms for this section include:

Term	Definition
NTP	A protocol that uses UDP packets to send time data to connected devices to keep time synced across a network.
Stratum levels	Hierarchical representation of the time servers in a NTP network. Stratum level 0 is the authoritative time source. Stratum level 1 is the server connected directly to the time source. Each subsequent server increases the stratum level.
Time drift	When a system's clock is no longer accurate and is off by a few seconds or minutes.
Slam	A method of fixing time drift by immediately resetting the time to the correct time.
Slew	A method of fixing time drift by incrementally fixing the time a few milliseconds at a time.

This section helps you prepare for the following certification exam objectives:

Exam	Objective

CompTIA Network+ N10-00	1.6 Explain the use and purpose of network services.
	• 1.6.3 NTP
	  ○ Stratum
	  ○ Clients
	  ○ Servers

Video/Demo	Time
4.6.1 NTP	4:28
4.6.2 Configure NTP on Windows 2019	2:37
4.6.3 Configure NTP on Linux	6:27
Total Video Time	**13:32**

Lab/Activity

- 4.6.5 Configure NTP

Fact Sheets

- 4.6.4 NTP Facts

Number of Exam Questions

10 questions

Total Time

About 41 minutes

4.7: IP Version 6

Lecture Focus Questions:

- Why is IPv6 needed?
- What is the format of a IPv6 address?
- How can an IPv6 address be simplified?
- What are the two parts of an IPv6 address?
- What allows IPv6 hosts to communicate over a IPv4 network?
- What is the difference between stateful autoconfiguration and stateless autoconfiguration?

In this section, you will learn to:

- Configure IPv6 addresses
- Configure a DHCP6 server

The key terms for this section include:

Term	Definition
Prefix ID	The first 64 bits of the IPv6 address. The prefix can be divided into various parts that identify things such as geographic region, ISP, network, and subnet.
Interface ID	The last 64 bits of the IPv6 address. This is a unique identifier for each device, similar to a MAC address.
Tunneling	Allows IPv6 hosts or sites to communicate over the existing IPv4 infrastructure.
Unicast address	An address assigned to a single interface for the purpose of allowing one host to send and receive data. Packets sent to a unicast address are delivered to the interface identified by that address.
Multicast address	An address that represents a dynamic group of hosts.
Anycast address	A unicast address assigned to more than one interface, typically belonging to different hosts.
Loopback address	A special IP address that can be used to verify that the TCP/IP protocol stack is properly installed on the host. The local loopback address is not assigned to an interface.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Network Pro	2.1 Configure IP addressing • 2.1.2 Configure an IPv6 address

CompTIA Network+
N10-008
	1.4 Given a scenario, configure a subnet and use appropriate “3 addressing schemes.
	
	• 1.4.2 IPv4 vs. IPv6
	  ○ Automatic Private lP Addressing (APIPA)
	  ○ Extended unique identifier (EUl-64)
	  ○ Multicast
	  ○ Unicast
	  ○ Anycast
	  ○ Broadcast
	  ○ Link local
	  ○ Loopback
	  ○ Default gateway
	• 1.4.4 IPv6 Concepts
	  ○ Tunneling
	  ○ Dual stack
	  ○ Shorthand notation
	  ○ Router advertisement
	  ○ Stateless address autoconfiguration (SLAAC)

Video/Demo	Time
4.7.1 IP Version 6	8:22
4.7.4 IPv6 Address Assignment	9:40
4.7.5 Configure IPv6 Addresses	9:30
4.7.6 Configure a DHCP6 Server	5:01
Total Video Time	**32:33**

Lab/Activity

- 4.7.8 Configure an IPv6 Address

Fact Sheets

- 4.7.2 IPv6 Facts
- 4.7.3 IPv4 to IPv6 Migration
- 4.7.7 IPv6 Address Assignment Facts

Number of Exam Questions

10 questions

Total Time

About 70 minutes

4.8: Multicast

Lecture Focus Questions:

- How does multicast differ from unicast and broadcast?
- What is the IP address range reserved for multicast groups?
- What does a regular switch do when it receives a multicast frame?
- Which device would you configure to prevent multicast traffic from being sent to non-group members?

The key terms for this section include:

Term	Definition
Unicast	A transmission type that sends messages to a specific host address. The sending device must know the IP address of all recipients and must create a separate packet for each destination device.
Broadcast	A single packet that, when sent, is processed by all hosts. Broadcast packets are not typically forwarded by routers, so broadcast traffic is limited to within a single subnet.
IGMP	A protocol used to identify group members and to forward multicast packets on to the segments where group members reside.

This section helps you prepare for the following certification exam objectives:

Exam	Objective

CompTIA Network+ N10-008	1.4 Given a scenario, configure a subnet and use appropriate IP addressing schemes.
	• 1.4.2 IPv4 vs. IPv6
	  ○ Multicast
	  ○ Unicast
	  ○ Anycast
	  ○ Broadcast

Video/Demo	Time
4.8.1 Multicast	8:44
Total Video Time	**8:44**

Fact Sheets

4.8.2 Multicast Facts

Number of Exam Questions

10 questions

Total Time

About 24 minutes

4.9: Troubleshoot IP Configuration Issues

Lecture Focus Questions:

- Which IP configuration issues should you be aware of?
- How can an incorrect subnet mask cause IP communication issues?
- Which issues can prevent a Dynamic Host Configuration Protocol (DHCP) server from properly issuing an IP address to a host?
- What does the /release switch do when used with ipconfig?
- How can you tell if a rogue DHCP server is active on a network?
- How do you know if a host is using Automatic Private IP Addressing (APIPA)?

In this section, you will learn to:

- Use ipconfig
- Use the ip command
- Explore IP configuration
- Troubleshoot IP configuration

The key terms for this section include:

Term	Definition
APIPA	A Windows function that provides DHCP autoconfiguration addressing.
DHCP	A protocol used to centrally manage the distribution of IP addresses within a network.
Domain Name System (DNS)	A naming system for computers. The main function of DNS is to translate domain names into IP addresses, which computers can understand.
Rogue DHCP server	An unauthorized DHCP server on the network.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Network Pro	5.1 Troubleshooting configuration and services. • 5.1.2 Troubleshoot IP configuration • 5.1.3 Troubleshoot DNS records 5.3 Given a scenario, use the appropriate network software tools and commands.

CompTIA Network+ N10-008	• 5.3.2 Command line tool
	  ○ ping
	  ○ ipconfig/ifconfig/ip

5.5 Given a scenario, troubleshoot general networking issues.

- 5.5.2 Common issues
  - Duplicate MAC address
  - Rogue DHCP server

Video/Demo	Time
4.9.1 IP Configuration Troubleshooting	8:17
4.9.2 Use ipconfig	6:40
4.9.3 Use the ip Command	5:31
Total Video Time	**20:28**

Lab/Activity

- 4.9.5 Explore IP Configuration
- 4.9.6 Troubleshoot IP Configuration 1
- 4.9.7 Troubleshoot IP Configuration 2
- 4.9.8 Troubleshoot IP Configuration 3

Fact Sheets

- 4.9.4 IP Configuration Troubleshooting Facts

Number of Exam Questions

10 questions

Total Time

About 84 minutes

4.10: Troubleshoot IP Communications

Lecture Focus Questions:

- What is the difference between netstat and ARP?
- What does a failed ping test signify?
- When should you use tracert?
- What does TCPdump do?

In this section, you will learn to:

- Use ping and tracert
- Use ARP and netstat
- Explore network communications

The key terms for this section include:

Term	Definition
ping	A command-line utility that sends an ICMP echo request/reply packet to a remote host. A response from the remote host indicates that both hosts are correctly configured and a connection exists between them.
Address Resolution Protocol (ARP)	A protocol that hosts can use to discover the media access control (MAC) address of a device.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Network Pro	2.1 Configure IP addressing • 2.1.1 Configure IP addresses 5.3 Given a scenario, use the appropriate network software tools and commands.

CompTIA Network+ N10-008	• 5.3.2 Command line tool
	  ○ ping
	  ○ ipconfig/ifconfig/ip
	  ○ traceroute/tracert
	  ○ arp
	  ○ netstat

Video/Demo	Time
4.10.1 Network Communication Troubleshooting	11:10

4.10.2 Use ping and tracert	9:06
4.10.4 Use arp and netstat	8:29
Total Video Time	**28:45**

Lab/Activity

- 4.10.6 Explore Network Communications

Fact Sheets

- 4.10.3 Network Communication Troubleshooting Facts
- 4.10.5 arp and netstat Facts

Number of Exam Questions

10 questions

Total Time

About 61 minutes

4.11: Troubleshoot DNS

Lecture Focus Questions:

- What are the symptoms of name resolution problems?
- What is the difference between nslookup and dig?

In this section, you will learn to:

- Examine DNS attacks
- Use nslookup
- Use dig

This section helps you prepare for the following certification exam objectives:

Exam	Objective

TestOut Network Pro	3.2 Manage DNS services
	• 3.2.3 Explore nslookup
	
	5.3 Given a scenario, use the appropriate network software tools and commands.
	• 5.3.2 Command line tool
	  ○ ping
	  ○ nslookup/dig
	  ○ traceroute/tracert
	  ○ hostname

CompTIA Network+ N10-008	5.5 Given a scenario, troubleshoot common network service issues. • 5.5.2 Common issues ○ DNS issues

Video/Demo	Time
4.11.1 DNS Troubleshooting	4:47
4.11.3 Examining DNS Attacks	11:57
4.11.4 Use nslookup	3:38
4.11.5 Use dig	5:29
Total Video Time	**25:51**

Lab/Activity

- 4.11.6 Explore nslookup

Fact Sheets

- 4.11.2 DNS Troubleshooting Facts

Number of Exam Questions

10 questions

Total Time

About 53 minutes

Ethernet

5.1: Ethernet

Lecture Focus Questions:

- Which logical topologies are supported on an Ethernet network?
- What is the differences between a physical and logical topology?
- What is the purpose of the back-off on Ethernet networks?
- How can you eliminate collisions on an Ethernet network?
- Which device is used to enable full-duplex communications with Ethernet?

In this section, you will learn to:

- Reconnect to an Ethernet network

The key terms for this section include:

Term	Definition
Frame	A unit of data that is ready to be sent on the network medium.
Media access control (MAC) address	A unique identifier (address) that is burned into every network interface card (NIC).

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Network Pro	1.1 Implement Components and Cabling solutions • 1.1.1 Connect and reconnect Ethernet networks 1.2 Explain the characteristics of network topologies and network types. • 1.2.2 Star/hub-and-spoke • 1.2.3 Bus

CompTIA Network+ N10-008	1.3 Summarize the types of cable and connectors and explain which is the appropriate type for a solution.
	• 1.3.1 Copper
	• 1.3.5 Ethernet standards
	  ○ Copper
	  ▪ 10BASE-T
	  ▪ 100BASE-TX
	  ▪ 1000BASE-T

        - 10GBASE-T
        - 40GBASE-T
    - Fiber
        - 100BASE-FX
        - 100BASE-SX
        - 1000BASE-SX
        - 1000BASE-LX
        - 10GBASE-SR
        - 10GBASE-LR1.3

2.3 Given a scenario, configure and deploy common Ethernet switching features.

- 2.3.7 Carrier-sense multiple access with collision detection (CSMA/CD)

Video/Demo	Time
5.1.1 Ethernet Architecture	10:03
5.1.3 Ethernet Specifications	3:59
Total Video Time	**14:02**

Lab/Activity

- 5.1.5 Reconnect to an Ethernet Network

Fact Sheets

- 5.1.2 Ethernet Facts
- 5.1.4 Ethernet Specifications Facts

Number of Exam Questions

10 questions

Total Time

About 47 minutes

5.2: Connect Network Devices

Lecture Focus Questions:

- Which cable type would you use to connect a workstation to a regular port on a hub or a switch?
- Which cable type would you use to connect a router to the uplink port on a switch?
- Which cable type would you use to connect two switches together using their uplink ports?
- Which switch feature makes choosing crossover or straight-through cables easier?
- When would you use a rollover cable?

In this section, you will learn to:

- Connect network devices

The key terms for this section include:

Term	Definition
Straight-through cable	A cable that connects each wire to the same pin on each connector (pin 1 to pin 1, pin 2 to pin 2, etc.). You use a straight-through cable when a crossover is performed with a hub or a switch.
Crossover cable	A cable that matches the transmit (Tx) wires on one connector with the receive (Rx) wires on the other connector. Use a crossover cable when crossing is not performed automatically or when crossover is performed twice.
Rollover	A type of null-modem cable that is used to connect a computer terminal to a router's console port. A rollover cable might also have an RJ45 connector on both ends, requiring an adapter to convert from the RJ45 connector to the serial cable.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Network Pro	1.1 Implement Components and Cabling solutions • 1.1.1 Connect computer and network components 5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.

CompTIA Network+ N10-008	• 5.2.3 Cable application
	  ○ Rollover cable/console cable
	  ○ Crossover cable

Video/Demo	Time
5.2.1 Connect Devices	7:20
Total Video Time	**7:20**

Lab/Activity

- 5.2.3 Connect Network Devices

Fact Sheets

- 5.2.2 Device Connection Facts

Number of Exam Questions

10 questions

Total Time

About 35 minutes

5.3: Troubleshoot Physical Connectivity

Lecture Focus Questions:

- What happens if a host goes down in a star topology? What happens if a host goes down in a token-ring topology?
- What happens if there is a cable break on a bus topology? What happens if there is a cable break on a dual-ring topology?
- What is indicated by a flashing green link light?
- What might be the problem if none of the NIC lights are working?

In this section, you will learn to:

- Connect a network cable
- Replace the patch cable
- Replace a faulty cable
- Troubleshoot a faulty cable
- Reconnect a switch
- Troubleshoot a switch
- Connect an unplugged cable
- Troubleshoot an unplugged cable

The key terms for this section include:

Term	Definition
Network topology	A description of how computers and links are connected in a network (physical topology) and the flow of data (logical topology).
Link light	LED light, or lights on network adapters or switches, that indicate the status of the physical link.
Bus topology	A network topology where all nodes in the network are connected to a cable (called a bus).
Star topology	A network topology in which every node in the network is connected to a central node (either a hub or a switch) in a spoke-and-hub organization.
Ring topology	A network topology in which every node is connected to two other nodes in a closed circular organization where data travels through every node.
Mesh topology	A network topology in which every node is connected to every other node in the network to create redundancy.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Network Pro	2.2 Configure routers and switches • 2.2.5 Configure routers 5.2 Troubleshooting wired and wireless connectivity

	• 5.2.1 Explore physical connectivity • 5.2.2 Troubleshoot physical connectivity
CompTIA Network+ N10-008	1.2 Explain the characteristics of network topologies and network types. • 1.2.1 Mesh • 1.2.2 Star/hub-and-spoke • 1.2.3 Bus • 1.2.4 Ring • 1.2.5 Hybrid

Video/Demo	Time
5.3.1 Troubleshoot Physical Network Topology	5:33
5.3.3 Troubleshoot the Link Status	4:50
Total Video Time	**10:23**

Lab/Activity

- 5.3.5 Explore Physical Connectivity 1
- 5.3.6 Explore Physical Connectivity 2
- 5.3.7 Troubleshoot Physical Connectivity 1
- 5.3.8 Troubleshoot Physical Connectivity 2
- 5.3.9 Troubleshoot Physical Connectivity 3
- 5.3.10 Troubleshoot Physical Connectivity 4

Fact Sheets

- 5.3.2 Physical Network Topology Troubleshooting Facts
- 5.3.4 Link Status Troubleshooting Facts

Number of Exam Questions

10 questions

Total Time

About 103 minutes

Firewalls and Intrusion Detection

6.1: Firewalls

Lecture Focus Questions:

- How is a packet-filtering firewall different from a circuit-level gateway?
- Why is a packet-filtering firewall a stateless device?
- Which types of criteria can an Application layer gateway use for filtering?
- What is the difference between a proxy and a reverse proxy?

In this section, you will learn to:

- Configure Windows Firewall
- Configure Linux iptables
- Configure a host firewall

The key terms for this section include:

Term	Definition
Firewall	A software- or hardware-based network security system that allows or denies network traffic according to a set of rules.
Access control list (ACL)	A list of filtering rules that firewalls use to identify allowed and blocked traffic.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Network Pro	1.1 Place objective here • Place sub objectives here ○ And here if needed

CompTIA Network+ N10-008	2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.
	• 2.1.1 Networking devices
	  ○ Firewall
	4.3 Given a scenario, apply network hardening techniques.
	• 4.3.1 Best practices
	  ○ Firewall rules

Video/Demo **Time**

6.1.1 Firewalls	3:16
6.1.2 Firewall Types	11:04
6.1.4 Configure Windows Firewall	4:07
6.1.5 Configure Linux Firewall	5:35
Total Video Time	**24:02**

Lab/Activity

- 6.1.7 Configure a Host Firewall

Fact Sheets

- 6.1.3 Firewall Facts
- 6.1.6 Linux Firewall Facts

Number of Exam Questions

10 questions

Total Time

About 57 minutes

6.2: Firewall Design and Implementation

Lecture Focus Questions:

- What are the benefits of a unified threat management (UTM) system?
- What is the difference between a stateful and a stateless firewall?
- What is the difference between a standard access control list (ACL) and an extended ACL?
- Which filtering rules do firewalls use to identify the traffic to allow and the traffic to block?

In this section, you will learn to:

- Configure network security appliance access
- Configure a security appliance
- Configure a perimeter firewall
- Create firewall ACLs

The key terms for this section include:

Term	Definition
UTM	An appliance, also known as an all-in-one appliance, that combines several layers of security and networking services into one solution.
Screened subnet	A buffer network (or subnet) that sits between the private network and an untrusted network (such as the internet). It was previously known as a demilitarized zone.
ACL	Filtering rules that firewalls use to identify the traffic to allow and the traffic to block.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Network Pro	2.1 Compare and contrast various devices, their features, and their appropriate placement on the network. • 2.1.1 Networking devices ○ Firewall

CompTIA Network+ N10-008	4.3 Given a scenario, apply network hardening techniques.
	• 4.3.1 Best Practices
	  ○ Firewall rules
	  ▪ Explicit deny
	  ▪ Implicit deny

Video/Demo	Time
6.2.1 Unified Threat Management (UTM) Appliances	3:24
6.2.3 Firewall Network Design Principles	5:20
6.2.4 Configure Network Security Appliance Access	7:48
6.2.7 Configure Firewall Rules	6:50
6.2.9 Firewall ACLs	3:08
6.2.10 Create Firewall ACLs	5:50
6.2.11 Configure a Proxy Server	5:00
Total Video Time	**37:20**

Lab/Activity

- 6.2.5 Configure Network Security Appliance Access
- 6.2.6 Configure a Security Appliance 5.1.7
- 6.2.8 Configure a Perimeter Firewall

Fact Sheets

- 6.2.2 Unified Threat Management (UTM) Appliances Facts (update was 8.2.2)
- 6.2.12 Firewall Design and Configuration Facts

Number of Exam Questions

10 questions

Total Time

About 94 minutes

6.3: Screened Subnets (DMZ)

Lecture Focus Questions:

- What is the typical configuration for a screened subnet implemented as a dual-homed gateway?
- What are the functions of the two firewalls in a screened subnet?
- Which type of computer might exist inside a screened subnet?

In this section, you will learn to:

- Configure a screened subnet

The key terms for this section include:

Term	Definition
Screened subnet	A buffer network (or subnet) that is located between a private network and an untrusted network, such as the internet.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Network Pro	1.1 Place objective here • Place sub objectives here ○ And here if needed
CompTIA Network+ N10-008	4.1 Explain common security concepts • 4.1.8 Defense in depth ○ Screened subnet (previously known as demilitarized zone (DMZ))

Video/Demo	Time
6.3.1 Screened Subnets	3:57
6.3.2 Configure a Screened Subnet	3:28
Total Video Time	**7:25**

Lab/Activity

6.3.4 Configure a Screened Subnet (DMZ)

Fact Sheets

6.3.3 Screened Subnet Facts

Number of Exam Questions

10 questions

Total Time

About 35 minutes

6.4: Intrusion Detection and Prevention

Lecture Focus Questions:

- What is an intrusion detection system?
- How is an intrusion detection system different from an intrusion prevention system?
- What is the difference between anomaly-based and signature-based monitoring?

In this section, you will learn to:

- Implement intrusion detection
- Implement intrusion prevention

The key terms for this section include:

Term	Definition
Intrusion detection system (IDS)	A device or software that monitors, logs, and detects security breaches, but takes no action to stop or prevent the attack.
Intrusion prevention system (IPS)	A device that monitors, logs, detects, and reacts to stop or prevent security breaches.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Network Pro	1.1 Place objective here • Place sub objectives here ○ And here if needed
CompTIA Network+ N10-008	2.1 Compare and contrast various devices, their features, and their appropriate placement on the network. • 2.1.1 Networking devices ○ Intrusion prevention system (IPS)/intrusion detection system (IDS)

Video/Demo	Time
6.4.1 Intrusion Detection and Prevention	4:38
6.4.2 Implement Intrusion Detection and Prevention	6:18
Total Video Time	**10:56**

Lab/Activity

- 6.4.4 Implement Intrusion Prevention

Fact Sheets

- 6.4.3 Intrusion Detection and Prevention Facts

Number of Exam Questions

10 questions

Total Time

About 38 minutes

Switching and Routing

7.1: Switching

Lecture Focus Questions:

- What is the difference between a managed and an unmanaged switch?
- What is the difference between in-band and out-of-band management?
- What is the difference between a Layer 2 and a Layer 3 switch?

In this section, you will learn to:

- Connect a switch with SSH
- Connect to and secure a switch with a GUI
- Secure a switch

The key terms for this section include:

Term	Definition
Switch	A communication device that connects other network devices and receives and forwards data to a specified destination within a LAN.
MAC address	A unique identifier given to every device that connects to a network and is comprised of a 48-bit number separated into six 2-byte numbers.
Local area network (LAN)	A set of computers and devices connected in one physical location.
Virtual local area network (VLAN)	A logical grouping of computers through segmentation in a LAN.

This section helps you prepare for the following certification exam objectives:

Exam	Objective

CompTIA Network+ N10-008	2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.
	• 2.1.1 Networking devices
	  ○ Layer 2 switch
	  ○ Layer 3 capable switch
	4.4 Compare and contrast remote access methods and security implications.
	• 4.4.9 In-band vs. out-of-band management

Video/Demo	Time
7.1.1 Switch Features	8:14
7.1.2 Switch Access	3:58
7.1.3 Connect to a Switch with SSH	2:42
7.1.5 Connect to and Secure a Switch - GUI	2:57
7.1.7 Cisco IoS Basics	8:35
Total Video Time	**26:26**

Lab/Activity

- 7.1.6 Secure a Switch

Fact Sheets

- 7.1.4 Switching Facts

Number of Exam Questions

10 questions

Total Time

About 54 minutes

7.2: Basic Switch Configuration

Lecture Focus Questions:

- How do VLANs work?
- How do voice VLANs help VoIP work effectively?
- How can automatic-medium dependent interface crossover help with connecting devices?

In this section, you will learn to:

- Configure Switch IP and VLAN - GUI
- Create VLANs - GUI
- Configure Switch IP Settings - CLI
- Configure Management VLAN Settings - CLI

The key terms for this section include:

Term	Definition
Trunk port	A port configuration that allows multiple VLANs to connect through a single port and is also known as a tagged port.
Access port	A port that allows traffic from only one VLAN.
Automatic-medium dependent interface crossover (auto-MDIX)	A line sensing port configured to automatically detect the needed cable connection type and then configure the connection accordingly.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Network Pro	x.x Place objective here • x.x.x Place sub objectives here ○ And here if needed
CompTIA Network+ N10-008	2.3 Given a scenario, configure and deploy common Ethernet switching features. • 2.3.1 Data virtual local area network (VLAN) • 2.3.2 Voice VLAN ○ Auto-medium dependent interface crossover (MDIX) • 2.3.4 Media access control (MAC) address tables • 2.3.7 Carrier-sense multiple access with collision detection (CSMA/CD) • 2.3.8 Address Resolution Protocol (ARP)

- 2.3.9 Neighbor Discovery Protocol (NDP)

Video/Demo	Time
7.2.1 VLAN Overview	11:23
7.2.3 Configure Switch IP and VLAN - GUI	3:59
7.2.5 Create VLANs - GUI	3:26
7.2.7 Configure Switch IP and VLAN - CLI	4:43
Total Video Time	**23:31**

Lab/Activity

- 7.2.4 Configure Switch IP and VLAN - GUI
- 7.2.6 Create VLANs - GUI
- 7.2.9 Configure Switch IP Settings - CLI
- 7.2.10 Configure Management VLAN Settings - CLI

Fact Sheets

- 7.2.2 VLAN Facts
- 7.2.8 CLI Switch IP Configuration Facts

Number of Exam Questions

10 questions

Total Time

About 92 minutes

7.3: Switch Ports

Lecture Focus Questions:

- How do duplex, speed, and flow control affect port configurations?
- What are the benefits of link aggregation?
- What protocol can be used to prevent looping and broadcast storms in your network, and how does it work?
- What are the options and benefits of integrating PoE devices in your network?
- Why would you consider configuring switches in your network to handle jumbo frames?

In this section, you will learn to:

- Configure trunking
- Configure port aggregation
- Enable jumbo frame support
- Configure port mirroring
- Configure PoE
- Configure Spanning Tree Protocol

The key terms for this section include:

Term	Definition
Bridge Protocol Data Unit (BPDU)	To avoid switching loops, switches use BPDU frames to determine the network topology. BPDU frames contain such things as the switch ID, its MAC address and switch port cost. BPDU is an important function used by Spanning Tree Protocol (STP), which is used to prevent these switching loops.
Power over Ethernet (PoE)	The process of providing electrical power to a device by means of a copper Ethernet cable.
VoIP Phone	A telephone with hardware or software that allows phone calls to be made over an IP network.
Port Tagging	A technique of adding a VLAN ID into an Ethernet frame. The tag identifies which VLAN the frame is coming from or going to. A tagged frame is called an 802.1q frame or a Dot1q frame.
Sticky MAC	A switch port security feature that adds the MAC addresses of known devices to the Content Addressable Memory (CAM) table, or MAC address table. These MAC addresses can be dynamically learned or entered manually. Unless saved to the startup configuration, these address will be lost when the switch is rebooted.
Jumbo Frames	Ethernet frames that exceed the IEEE 802.3 limit of a 1,500 byte payload and can carry a payload of up to 9,000 bytes.

This section helps you prepare for the following certification exam objectives:

Exam	Objective

CompTIA Network+ N10-008	2.3 Given a scenario, configure and deploy common Ethernet switching features.
	
	• 2.3.3 Port configurations
	  ○ Port tagging/802.1q
	  ○ Port aggregation
	  ▪ Link Aggregation Control Protocol (LACP)
	  ○ Duplex
	  ○ Speed
	  ○ Flow control
	  ○ Port mirroring
	  ○ Port security
	  ○ Jumbo frames
	• 2.3.5 Power over Ethernet (PoE)/Power over Ethernet plus (PoE+)
	• 2.3.6 Spanning Tree Protocol

Video/Demo	Time
7.3.1 Switch Port Configurations	6:57
7.3.3 Configure Trunking	2:56
7.3.5 Configure Port Aggregation	2:50
7.3.7 Enable Jumbo Frame Support	2:36
7.3.9 Switch Port Features	10:24
7.3.11 Configure Port Mirroring	2:20
7.3.13 Configure PoE	2:33
7.3.15 Configure Spanning Tree	2:37
Total Video Time	**33:13**

Lab/Activity

- 7.3.4 Configure Trunking
- 7.3.6 Configure Port Aggregation
- 7.3.8 Enable Jumbo Frame Support
- 7.3.12 Configure Port Mirroring
- 7.3.14 Configure PoE

Fact Sheets

- 7.3.2 Switch Port Configuration Facts
- 7.3.10 Switch Port Feature Facts

Number of Exam Questions

10 questions

Total Time

About 114 minutes

7.4: Switch Security

Lecture Focus Questions:

- How are switches indirectly involved in Address Resolution Protocol (ARP) poisoning?
- How does the attacker hide their identity when performing media access control (MAC) spoofing?
- What is the function of a trunk port?
- What is required for devices to communicate between VLANs?
- How is port security different from port filtering?

In this section, you will learn to:

- Disable switch ports
- Harden a switch
- Secure access to a switch

The key terms for this section include:

Term	Definition
Virtual LAN (VLAN)	A logical grouping of computers based on switch port.
MAC filtering/port security	A switch feature that restricts connection to a given port based on the MAC address.
Port authentication	A switch feature that follows the 802.1x protocol to allow only authenticated devices to connect.
Content Addressable Memory (CAM) table	A table maintained by a switch that contains MAC addresses and their corresponding port locations.
Dynamic Host Configuration Protocol (DHCP) snooping	A security feature on some switches that filters out untrusted DHCP messages.
Dynamic ARP inspection (DAI)	A security feature on some switches that verifies that each ARP request has a valid IP-to-MAC binding.
MAC flooding	An attack that overloads a switch's MAC forwarding table to make the switch function like a hub.
ARP spoofing	An attack in which the attacker's MAC address is associated with the IP address of a target's device.
VLAN hopping	An attack in which the source MAC address is changed on frames sent by the attacker.
Double tagging	An attack in which the attacking host adds two VLAN tags instead of one to the header of the frames that it transmits.
MAC spoofing	An attack in which the source MAC address is changed in the header of a frame.

Dynamic Trunking Protocol (DTP)	An unsecure protocol that could allow unauthorized devices to modify a switch's configuration.

This section helps you prepare for the following certification exam objectives:

Exam	Objective

TestOut Network Pro	2.2 Configure routers and switches
	• 2.2.1 Configure switches
	4.2 Secure switches and wireless networks
	• 4.2.2 Disable switch ports
	2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.
	• 2.1.1 Networking devices
	  ○ Layer 2 switch
	  ○ layer 3 capable switch
	2.3 Given a scenario, configure and deploy common Ethernet switching features.
	• 2.3.1 Data virtual local area network (VLAN)
	• 2.3.2 Voice VLAN

CompTIA Network+ N10-008	4.1 Explain common security concepts.
	• 4.1.9 Authentication methods
	  ○ 802.1X
	4.2 Compare and contrast common types of attacks.
	• 4.2.1 Technology-based
	  ○ VLAN hopping
	  ○ ARP spoofing
	  ○ MAC spoofing
	4.3 Given a scenario, apply network hardening techniques.
	• 4.3.2 Wireless security
	  ○ MAC filtering

Video/Demo	Time
7.4.1 Securing Network Switches	7:29

7.4.3 Switch Attacks	11:50
7.4.5 Disable Switch Ports - GUI	2:09
7.4.7 Hardening a Switch	10:38
Total Video Time	**32:06**

Lab/Activity

- 7.4.6 Disable Switch Ports - GUI
- 7.4.8 Harden a Switch
- 7.4.9 Secure Access to a Switch
- 7.4.10 Secure Access to a Switch 2

Fact Sheets

- 7.4.2 Switch Security Facts
- 7.4.4 Switch Attack Facts

Number of Exam Questions

10 questions

Total Time

About 101 minutes

7.5: Routing

Lecture Focus Questions:

- What is the function of a routing table?
- What is the difference between static and dynamic routing?
- What network link characteristics are used by routing protocols when computing a metric value or cost?
- What are the most common routing protocols? Which protocol is best for each situation?

In this section, you will learn to:

- Configure QoS

The key terms for this section include:

Term	Definition
Classful Routing Protocol	A routing protocol that does not have subnet mask information in the routing updates.
Classless Routing Protocol	A routing protocol that does include subnet mask information in the routing updates.
Distance Vector Routing	A routing technique in which every router sends a complete topography of the routers in the network out to directly connected routers.
Link State Routing	A routing technique in which every router sends information about directly connected links to all the routers in the network.

This section helps you prepare for the following certification exam objectives:

Exam	Objective

CompTIA Network+ N10-008	1.4 Given a scenario, configure a subnet and use appropriate IP addressing schemes.
	• 1.4.5 Virtual IP (VIP)
	
	2.2 Compare and contrast routing technologies and bandwidth management concepts.
	• 2.2.1 Routing
	  ○ Dynamic routing
	  ▪ Protocols [Routing Internet Protocol (RIP), Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), Border Gateway Protocol (BGP)]
	  ▪ Link state vs. distance vector vs. hybrid
	  ▪ Static routing

- Dynamic routing
- Administrative distance
- Exterior vs. interior
- Time to live

- 2.2.2 Bandwidth management
  - Traffic shaping
  - Quality of service (QoS)

Video/Demo	Time
7.5.1 Routing	9:36
7.5.3 Routing Protocol Characteristics	12:41
7.5.5 Routing Protocols	6:59
7.5.7 Routing High Availability	11:56
7.5.9 Configure QoS	7:39
Total Video Time	**48:51**

Lab/Activity

- 7.5.10 Configure QoS

Fact Sheets

- 7.5.2 Routing Facts
- 7.5.4 Routing Protocol Characteristics Facts
- 7.5.6 Routing Protocol Facts
- 7.5.8 Routing High Availability Facts

Number of Exam Questions

10 questions

Total Time

About 91 minutes

7.6: Network Address Translation

Lecture Focus Questions:

- How does NAT work?
- What is the difference between static NAT and dynamic NAT?
- What is port forwarding?
- What is the difference between NAT and PAT?
- Which IP addresses are considered private and guaranteed not to be used on the internet?

In this section, you will learn to:

- Configure NAT

The key terms for this section include:

Term	Definition
IP address (Internet Protocol address)	A numerical identifier assigned to each device on the internet or local network. It is used for communication between devices.
IPv4 (Internet Protocol version 4)	A 32-bit numerical addressing method. It contains It has 12 header fields and checksum fields, supports broadcast and variable length subnet masking, and uses ARP.
IPv6 (Internet Protocol version 6)	A 128-bit alphanumeric addressing method that contains eight header fields and uses NDP, but does not contain checksum fields or support broadcast or variable length subnet mask.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Network Pro	2.1 Configure IP addressing • 2.1.3 Deploy NAT

CompTIA Network+ N10-008	1.4 Given a scenario, configure a subnet and use appropriate IP addressing schemes.
	• 1.4.1 Public vs. private
	  ○ Network address translation (NAT)
	  ○ Port address translation (PAT)

Video/Demo **Time**

7.6.1 Network Address Translation	9:53
7.6.3 Configure NAT	9:39
Total Video Time	**19:32**

Lab/Activity

- 7.6.4 Configure NAT

Fact Sheets

- 7.6.2 NAT Facts

Number of Exam Questions

10 questions

Total Time

About 47 minutes

7.7: Switching and Routing Troubleshooting

Lecture Focus Questions:

- How can you see if your interfaces are up and connected?
- How can VLAN assignment cause network communication problems?
- What causes broadcast storms?
- How can duplicate IP addresses happen?
- What is a rogue DHCP server? How can you protect your system from one?
- What can help prevent routing loops in multicast flooding?
- What is asymmetrical routing, and when does it cause a problem?

In this section, you will learn to:

- Troubleshoot routing

The key terms for this section include:

Term	Definition
Subnet mask	A 32-bit dot decimal notation that distinguishes which part of the IP address refers to the host and which part refers to the subnet. It also limits the IP addresses and the number of hosts that can exist within the subnet.
IP address (Internet Protocol address)	An identifying number assigned to a device on a network. IP addresses allow devices to find and communicate with each other.
Gateway address	A router that connects a local network to other networks and is also called the default gateway.
DNS (Domain Name System)	A naming system that converts human readable domain names into IP addresses.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Network Pro	5.1 Troubleshoot configuration and services • 5.1.1 Explore IP configuration • 5.1.2 Troubleshoot IP configuration • 5.1.3 Troubleshoot DNS records

CompTIA Network+ N10-008	5.5 Given a scenario, troubleshoot general networking issues.
	• 5.5.1 Considerations
	  ○ Device configuration review
	  ○ Routing tables

- Interface status
- VLAN assignment
- Network performance baselines

- 5.1.2 Common issues
  - Collisions
  - Broadcast storms
  - Duplicate MAC address
  - Duplicate IP address
  - Multicast flooding
  - Asymmetrical routing
  - Switching loops
  - Routing loops
  - Rogue DHCP server
  - DHCP scope exhaustion
  - IP setting issues
    - Incorrect gateway
    - Incorrect subnet mask
    - Incorrect IP address
    - Incorrect DNS
  - Missing route

Video/Demo	Time
7.7.1 Switching and Routing Troubleshooting (Part 1)	6:14
7.7.2 Switching and Routing Troubleshooting (Part 2)	6:50
7.7.3 Troubleshoot Routing	7:07
Total Video Time	**20:11**

Fact Sheets

7.7.4 Switching and Routing Troubleshooting Facts

Number of Exam Questions

9 questions

Total Time

About 35 minutes

Specialized Networks

8.1: Corporate and Datacenter Networks

Lecture Focus Questions:

- What is a corporate data center?
- What does the core switch do?
- How do the distribution and access layer switches work?
- What is the access layer switch?

In this section, you will learn to:

- Configure an iSCSI target
- Configure an iSCSI initiator

Key terms for this section include the following:

Term	Definition
Storage Area Network (SAN)	Dedicated block-based storage, leveraging a high-speed architecture that interconnects and delivers shared pools of storage devices to multiple servers. A SAN makes its data act as if it were locally attached.
Initiator	A server that connects to the shared storage device. They run initiator software that connects to and communicates with the SAN target.
Target	All SAN storage devices are called targets.
Internet Small Computer Systems Interface (iSCSI)	A protocol used in TCP/IP networks' data storage solutions. The advantage is the speed of data flow.
Software-Defined Network (SDN)	SDN is an approach to network management that lets you centrally control (or program) a network intelligently using a software application. This helps make the management of the entire network consistent regardless of the underlying network technology.

This section helps you prepare for the following certification exam objectives:

Exam	Objective

CompTIA Network+ N10-008	1.7. Explain basic corporate and data center network architecture.
	• 1.7.1 Three-tiered
	  ○ Core
	  ○ Distribution/aggregation layer

- Access/edge

Video/Demo	Time
8.1.1 Storage Area Networks	10:43
8.1.2 Configure an iSCSI SAN	5:55
8.1.6 Software-defined Networking	2:33
8.1.7 Configure Software Defined Networking (SDN)	5:53
Total Video Time	**25:04**

Lab/Activity

- 8.1.3 Configure an iSCSI Target
- 8.1.4 Configure an iSCSI Initiator

Fact Sheets

- 8.1.5 SAN Facts
- 8.1.8 Software-defined Networking Facts

Number of Exam Questions

10 questions

Total Time

About 70 minutes

8.2: Voice over IP (VoIP)

Lecture Focus Questions:

- How does VoIP differ from traditional phone service?
- What are the functions of a VoIP server? What are other names for a VoIP server?
- What is the difference between a hard VoIP phone and a soft VoIP phone?
- How is a VoIP gateway used?
- What is the most common open source VoIP protocol?
- What is the function of a codec?
- Why is quality of service (QoS) important for VoIP?
- What happens if there is too much latency in a VoIP call?
- What is jitter? How does it affect VoIP calls?

In this section, you will learn to:

- Configure VoIP

The key terms for this section include:

Term	Definition
Voice over IP (VoIP)	Voice over IP (VoIP) is a protocol optimized for the transmission of voice data (telephone calls) through a packet-switched IP network. VoIP routes phone calls through an IP network, including the internet. VoIP solutions can integrate with the public switched telephone network (PSTN) to allow VoIP customers to make and receive external calls.
VoIP gateway	A voice over IP (VoIP) gateway converts voice and fax calls between the PSTN and your IP network in real time.
Sampling	In VoIP, audio is converted from an analog signal to digital data through a technique called sampling.
Codec	A special algorithm called a codec compresses VoIP data to reduce bandwidth consumption. On the receiving end, the same algorithm is used to decompress the data.
Network latency	Network latency is a measure of delay as a packet of data travels from one point to another. Too much latency causes VoIP callers to talk over each other.
Jitter	Jitter is a variation in the delay or latency of received packets. Latency going up and down during a call can cause unusual sound effects (minor pauses, jumps, choppiness).
Unified communications	Appliances that plug directly into your network and provide a wide variety of communication services, such as voice, voicemail, instant messaging, and faxing.

This section helps you prepare for the following certification exam objectives:

Exam	Objective

CompTIA Network+ N10-008	2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.
	• 2.1.1 Networking devices
	  ○ Voice gateway
	• 2.1.2.Networked devices
	  ○ Voice over Internet Protocol (VoIP) phone

Video/Demo	Time
8.2.1 Voice over IP (VoIP)	11:14
8.2.5 Configure VoIP Server	8:44
8.2.6 Configure VoIP Phone	4:45
Total Video Time	**24:43**

Lab/Activity

- 8.2.3 Connect VoIP 1
- 8.2.4 Connect VoIP 2

Fact Sheets

- 8.2.2 VoIP Facts

Number of Exam Questions

10 questions

Total Time

About 64 minutes

8.3: Virtualization

Lecture Focus Questions:

- What is the relationship between the host and the guest operating systems?
- What is the function of the hypervisor?
- What is the main difference between Type 1 and Type 2 hypervisors?
- What are the differences between a virtual machine and a virtual hard disk?
- Which type of virtualization allows applications to run within the virtual machine and without being modified?
- What is paravirtualization?
- What is the difference between full and partial virtualization?

In this section, you will learn to:

- Create a virtual machine

Key terms for this section include the following:

Term	Definition
Virtualization	Virtualization is the ability to install and run multiple operating systems simultaneously on a single physical machine.
Hypervisor	A hypervisor is a thin layer of software that resides between the virtual operating system(s) and the hardware. A hypervisor allows virtual machines to interact with the hardware without going through the host operating system. A hypervisor also manages access to the CPU, storage, and RAM.
Virtual machine	A virtual machine is a software implementation of a computer that executes programs like a physical machine. The virtual machine appears to be a self-contained and autonomous system, but it runs on a host computer and functions through a hypervisor.
Virtual hard disk (VHD)	A virtual hard disk is a file created within the host operating system that simulates a hard disk for the virtual machine.
Paravirtualization	In paravirtualization, the hardware is not virtualized. All of the guest operating systems running on the hypervisor directly access various hardware resources on the physical device. Components are not virtual. The guest operating systems run in isolated domains on the same physical hardware. Operating systems and applications must be modified before they can run in a paravirtualization environment.
Partial virtualization	In partial virtualization, only some of the components of the virtual machine are virtualized. The guest operating systems use some virtual components and some real physical hardware components on the actual device where the hypervisor is running. Operating

	systems or applications must be modified before they can run in a partial virtualization environment.
Full virtualization	In full virtualization, the virtual machine completely simulates a real physical host. This allows most operating systems and applications to run within the virtual machine without being modified in any way.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
Comptia Network+ N10-008	1.2 Explain the characteristics of network topologies and network types. • 1.2.8 Virtual network concepts ○ Hypervisor

Video/Demo	Time
8.3.1 Virtualization Overview	9:26
8.3.2 Create a Virtual Machine	6:47
Total Video Time	**16:13**

Fact Sheets

8.3.3 Virtualization Facts

Number of Exam Questions

10 questions

Total Time

About 32 minutes

8.4: Virtual Networking

Lecture Focus Questions:

- How is Network as a Service (NaaS) similar to an offsite data center? How is it different?
- What can you do to protect virtual hosts from network exploits?
- How does a virtual router differ from a physical router?
- What is the best way to set up a virtual firewall?
- What is the difference between a physical switch and a virtual switch?
- Where can you configure a custom MAC address for a virtual network interface?

In this section, you will learn to:

- Configure virtual network devices

The key terms for this section include:

Term	Definition
Virtual network interface	A software version of a physical network adapter. It is used in a virtual machine. Virtual network interfaces can connect to either a physical or virtual network.
Virtual switches	A switch that allows one virtual machine to communicate with another in much the same way that a physical switch allows physical hosts to communicate with each other.
Virtual VLANs	A subnetwork collection of devices that may be on separate physical LANs. Most virtual switch implementations support VLANs. You can define VLANs within the virtual switch and associate specific hosts with a specific VLAN. Because virtual hosts are not physically connected to the switch with cables, VLAN membership is defined within the configuration of each virtual machine.
Virtual router	A software-based routing framework that allows the host machine to perform as a typical hardware router over a local area network.
Virtual firewall	A firewall within the hypervisor. It lets you monitor and filter traffic on the virtual network as it flows between virtual machines. It is also seen in cloud environments as well as defense in depth tools.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Network+ Network 10-008	1.2 Explain the characteristics of network topologies and network types. • 1.2.8 Virtual network concepts ○ vSwitch

- Virtual network interface card (vNIC)
- Network function virtualization (NFV)
- Hypervisor

Video/Demo	Time
8.4.1 Virtual Networking Implementations	6:40
8.4.2 Virtual Network Devices	5:47
8.4.3 Configure Virtual Network Devices	3:05
Total Video Time	**15:32**

Fact Sheets

- 8.4.4 Virtual Networking Facts
- 8.4.5 Virtualization Implementation Facts

Number of Exam Questions

10 questions

Total Time

About 36 minutes

8.5: Cloud Concepts and Connectivity

Lecture Focus Questions:

- What is the difference between a hybrid cloud and a community cloud?
- What is the difference between IaaS and PaaS?
- What is a multi-cloud?
- What services does cloud computing provide?
- Which cloud computing model allows the client to run software without purchasing servers, data center space, or network equipment?
- What is the difference between multitenancy and non-multitenancy?

The key terms for this section include:

Term	Definition
Cloud computing	Cloud computing is a combination of software, data access, computation, and storage services provided to clients through the internet. The term cloud is a metaphor for the internet based on the basic cloud drawing used to represent the telephone network
Public cloud	Cloud-based computing resources such as platforms, applications, and storage are made available to the general public by a cloud service provider (such as Google's Gmail). A public cloud can be accessed by anyone, although some may require a fee.
Private cloud	A private cloud provides resources to a single organization. Private clouds can be hosted internally, behind a firewall. The majority are hosted by the company, while some maybe assisted by a cloud service provider (CSP).
Community cloud	A community cloud is a model that offers free applications to the public. Many times, these are segmented into business verticals. Social Community Clouds would include Facebook, Reddit and Twitter for example. These Community Clouds just require username and password and allows for the use of aliases. Technical Community Cloud includes services like GitHub.
Hybrid cloud	A hybrid cloud is a combination of public (sometimes multiple) and, private clouds that are leveraged for certain kinds of apps.
Multi-cloud	When multiple public clouds are used by a company because of cost or team preferences. This requires extra vigilance in managing the use of multiple public cloud platforms.
Infrastructure as a Service (IaaS)	IaaS delivers infrastructure to the client, such as processing, storage, networks, and virtualized environments. The client deploys and runs software without purchasing servers, data center space, or network equipment. The client is still responsible to secure their networks and data. The provider handles any updates.

Platform as a Service (PaaS)	PaaS delivers everything a developer needs to build an application. The deployment comes without the cost and complexity of buying and managing the underlying hardware and software layers. It also provides the services that an OS normally provides without developers needing to worry about specific operating systems. Client is in charge of securing data. The provider handles all updates.
Software as a Service (SaaS)	SaaS delivers software applications to the client either over the internet or on a local area network. This is by far the most used model.

This section helps you prepare for the following certification exam objectives:

Exam	Objective

CompTIA Network+ N10-008	1.8 Summarize cloud concepts and connectivity options.
	
	• 1.8.1 Development models
	  ○ Private
	  ○ Public
	  ○ Hybrid
	  ○ Community
	• 1.8.2 Service models
	  ○ Software as a service (SaaS)
	  ○ infrastructure as a service (IaaS)
	  ○ Platform as a service (PaaS)
	  ○ Desktop as a service (DaaS)
	• 1.8.3 Infrastructure as code
	  ○ Automation/orchestration
	• 1.8.4 Connectivity options
	  ○ Virtual private network (VPN)
	• 1.8.5 Multitenancy
	• 1.8.6 Elasticity
	• 1.8.7 Scalability
	• 1.8.8 Security implications

Video/Demo	Time
8.5.1 Cloud Models	3:47
8.5.2 Cloud Delivery Methods	6:33
8.5.4 Virtual Private Networks	8:27
Total Video Time	**18:47**

Fact Sheets

- 8.5.3 Cloud Facts
- 8.5.5 Virtual Private Networks Facts
- 8.5.6 IPsec Virtual Private Networks Facts

Number of Exam Questions
10 questions

Total Time
About 44 minutes

8.6: Internet of Things (IoT)

Lecture Focus Questions:

- How can IoT help you manage several aspects of a home environment remotely?
- What makes devices (such as light switches, thermostats, and door locks) smart ? Which one would best suit your needs?
- What is a smart speaker/home assistant? What can it connect to?
- How can you determine if a hub is compatible with Z-Wave or Zigbee?

In this section, you will learn to:

- Scan for IoT devices
- Configure smart devices
- Identify IoT protocols

Key terms for this section include the following:

Term	Definition
IoT	The internet of things.
Digital assistant	A smart speaker that controls smart appliances and performs other actions through voicecommands.
Zigbee	A protocol used by wireless mesh networks for communication with smart devices.
Z-Wave	An IoT standards-based protocol similar to Zigbee but simpler and less expensive.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Network Pro	2.3 Configure wireless and VoIP • 2.3.2 Connect smart devices 3.3 Manage device discovery and VLANs • 3.3.1 Scan for IoT devices

CompTIA Network+ N10-008	2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.
	• 2.1.2 Networked devices
	  ○ Internet of Things (IoT)
	  ▪ Refrigerator
	  ▪ Smart speakers
	  ▪ Smart thermostats
	  ▪ Smart doorbells

- Industrial control systems/supervisory control and data acquisition (SCADA)

Video/Demo	Time
8.6.1 Internet of Things	11:01
8.6.2 Smart Devices	7:03
8.6.5 Iot Security Challenges	7:53
8.6.6 Scan for IoT with Nmap	3:24
Total Video Time	**29:21**

Lab/Activity

- 8.6.4 Configure Smart Devices
- 8.6.7 Scan for IoT Devices

Fact Sheets

- 8.6.3 Internet of Things Facts

Number of Exam Questions

10 questions

Total Time

About 69 minutes

Wireless Networking

9.1: Wireless Concepts and Standards

Lecture Focus Questions:

- Under what circumstances might you choose an ad hoc wireless network?
- What device is used to create an infrastructure wireless network?
- How do wireless networks control media access?
- What is the difference between a BSS and an ESS?
- What do wireless clients use to identify a specific wireless access point?
- How do multiple access points identify themselves as part of the same network?

The key terms for this section include:

Term	Definition
Station	A *station* is a wireless NIC in an end device such as a laptop or wireless PDA. STA often refers to the device itself, not just the NIC. A station is often abbreviated as STA.
Access Point (AP)	An AP is the device that coordinates all communications between wireless devices, as well as the connection to the wired network. An AP is sometimes called a wireless AP (WAP).
Basic Service Set (BSS)	A BSS is the smallest unit of a wireless network. All devices in the BSS can communicate with each other. A BSS is also called a cell.
Independent Basic Service Set (IBSS)	An IBSS is a set of stations (STAs) configured in ad hoc mode.
Extended Service Set (ESS)	An ESS consists of multiple BSSs with a distribution system (DS). In an ESS, BSSs that have an overlapping transmission range use different frequencies.
Distribution System (DS)	The LAN that connects multiple APs (and BSSs) together. The DS allows wireless clients to communicate with the wired network and with wireless clients in other cells.
Service Set Identifier (SSID)	A case-sensitive name that specifies a service set (network) to which a wireless device can join or connect to.
Basic Service Set Identifier (BSSID)	The BSSID is a 48-bit value that identifies an AP in an infrastructure network or an STA in an ad hoc network. The BSSID allows devices to find a specific AP within an ESS that has multiple access points, and STAs use it to keep track of APs as they roam between BSSs. The BSSID is the MAC address of the AP and is set automatically.

Ad Hoc	A wireless network that works in peer-to-peer mode without an access point. The wireless NICs in each host communicate directly with one another.

This section helps you prepare for the following certification exam objectives:

Exam	Objective

CompTIA Network+ N10-008	2.4 Given a scenario, install and configure the appropriate wireless standards and technologies.
	• 802.11 standards
	  ○ - a
	  ○ - b
	  ○ - g
	  ○ - n (WiFi 4)
	  ○ - ac (WiFi 5)
	  ○ - ax (WiFi 6)
	• Frequencies and range
	  ○ 2.4GHz
	  ○ 5GHz
	• Channels
	  ○ Regulatory impacts
	• Channel bonding
	• Service set identifier (SSID)
	  ○ Basic service set
	  ○ Extended service set
	  ○ Independent basic service set (Ad-hoc)
	  ○ Roaming
	• Multiple input, multiple output (MIMO) and multi-user MIMO (MU-MIMO)
	
	2.5 Compare and contrast WAN technologies.
	• Transmission mediums
	  ○ Wireless

Video/Demo	Time
9.1.1 Radio Frequency Wireless	11:28
9.1.2 Wireless Architecture	7:52
9.1.5 Wireless Standards	12:55
Total Video Time	**32:15**

Fact Sheets

- 9.1.3 Wireless Architecture Facts
- 9.1.4 Wireless Infrastructure Facts
- 9.1.6 Wireless Standards Facts

Number of Exam Questions
10 questions

Total Time
About 58 minutes

9.2: Wireless Configuration

Lecture Focus Questions:

- What information does the wireless profile contain?
- What is the strongest encryption method?
- How does a MAC access list help keep a network secure?
- What is the purpose of a beacon?
- How are wireless networks listed in the notification area?

In this section, you will learn to:

- Create a home wireless network
- Secure a home wireless network
- Configure wireless profiles

The key terms for this section include:

Term	Definition
Access point (AP)	A device that allows for Wi-Fi connectivity on a wired network.
Wi-Fi Protected Access (WPA)	A security certification program that was developed by the Wi-Fi Alliance to secure wireless signals between devices.
Temporal Key Integrity Protocol (TKIP)	Encryption that implements a key-mixing feature that only the receiver can unlock.
Advanced Encryption Standard (AES)	Encryption that uses 128-, 192-, or 256-bit key lengths to encrypt and decrypt block-sized messages over a wireless transmission.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Network Pro	1.2 Implement Wired and Wireless devices • 1.2.3 Create a home wireless network 2.3 Configure wireless and VolP • 2.3.2 Connect mobile devices 4.2 Secure switches and wireless networks • 4.2.4 Secure a home wireless network

CompTIA Network+ N10-008	2.4 Given a scenario, install and configure the appropriate wireless standards and technologies.
	• 2.4.7 Encryption standards
	  ○ WiFi Protected Access (WPA)/WPA2 Personal [Advanced Encryption Standard (AES)/Temporal Key Integrity Protocol (TKIP)
	  ○ WPA/WPAZ Enterprise (AES/TKIP)
	• 2.4.5 Service set identifier (SSID)
	  ○ Basic service set

Video/Demo	Time
9.2.1 Wireless Network Configuration	9:31
9.2.3 Configure Wireless Networks	8:39
9.2.4 Configure a Wireless Client	4:28
Total Video Time	**22:38**

Lab/Activity

- 9.2.5 Create a Home Wireless Network
- 9.2.6 Secure a Home Wireless Network
- 9.2.7 Configure Wireless Profiles

Fact Sheets

- 9.2.2 Wireless Configuration Tasks

Number of Exam Questions

10 questions

Total Time

About 74 minutes

9.3: Wireless Network Design

Lecture Focus Questions:

- What is device density?
- What is the difference between received signal length and signal to noise ratio?
- Which implementation automatically partitions a single broadcast domain into multiple VLANs?
- What information is specified in a logical network diagram?
- How do you measure the signal strength at a given distance from the access point?

In this section, you will learn to:

- Design an indoor wireless network
- Design an outdoor wireless network

The key terms for this section include:

Term	Definition
Radio frequency (RF)	The rate of oscillation of electromagnetic radio waves in the range of 3 kHz to 300 GHz, as well as the alternating currents carrying the radio signals. This is the frequency band that is used for communications transmission and broadcasting.
Spectrum analyzer	A device that displays signal amplitude (strength) as it varies by signal frequency. The frequency appears on the horizontal axis; the amplitude is displayed on the vertical axis.
Site survey	A process of planning and designing a wireless network that includes network capacity, coverage, data rates, and quality of service.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Network Pro	1.2 Implement Wired and Wireless devices • 1.2.1 Design indoor and outdoor wireless networks 2.4 Given a scenario, install and configure the appropriate wireless standards and technologies.

CompTIA Network+ N10-008	• 2.4.6 Antenna types
	  ○ Omni
	  ○ Directional
	
	5.4 Given a scenario, troubleshoot common wireless connectivity issues.

- 5.4.1 Specifications and limitations
  - Throughput
  - Speed
  - Distance
  - Received signal strength indication (RSSI) signal strength
  - Effective isotropic radiated power (EIRP)/power settings
- 5.4.2 Considerations
  - Antennas
  - Antennas - Placement
  - Antennas - Type
  - Antennas - Polarization
  - Channel utilization
  - AP association time
  - Site survey

Video/Demo	Time
9.3.1 Wireless Network Design	5:48
9.3.2 Site Survey	7:16
9.3.3 Wireless Antenna Types	6:11
9.3.5 Conduct a Wireless Survey	4:40
Total Video Time	**23:55**

Lab/Activity

- 9.3.7 Design an Indoor Wireless Network
- 9.3.8 Design an Outdoor Wireless Network

Fact Sheets

- 9.3.4 Wireless Network Design Facts
- 9.3.6 Wireless Site Survey Facts

Number of Exam Questions

10 questions

Total Time

About 68 minutes

9.4: Wireless Network Implementation

Lecture Focus Questions:

- What is the difference between a hub-and-spoke infrastructure and a distributed wireless mesh infrastructure?
- What is a lightweight access point (AP) used for?
- Which protocol is used to route frames back and forth between the wireless network and the wired LAN?
- Which enterprise deployment has limited mobility and is difficult to manage?

In this section, you will learn to:

- Implement an enterprise wireless network

The key terms for this section include:

Term	Definition
Independent access points	Access points that separate wireless networks by using independent configuration. Each AP stands alone.
Hub and spoke	A wireless topology that connects to all APs through wired links. The individual APs contain very little embedded intelligence and are sometimes referred to as lightweight access points (LWAPs).
Distributed wireless mesh infrastructure	A wireless topology that moves some of the network intelligence from the controller to the individual APs. Newer wireless networks can be deployed using a distributed wireless mesh architecture.
Wireless bridges	Bridges used to connect wired or wireless networks.
Service set identifier (SSID)	The name of the wireless network. Client devices see a list of available networks when trying to connect to a wireless network.
Roaming	The ability of devices to connect from one access point to another while maintaining connection to the same network. For example, a laptop moved from one building to another stays connected to the same network.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Network Pro	1.2 Implement Wired and Wireless devices • 1.2.2 Implement an enterprise wireless network
CompTIA Network+ N10-008	2.4 Given a scenario, install and configure the appropriate wireless standards and technologies.

- 2.4.5 Service set identifier (SSID)
  - Basic service set
  - Extended service set
  - Independent basic service set (Ad-hoc)
  - Roaming
- 2.4.7 Encryption Standards
  - WiFi Protected Access (WPA)/WPA2 Personal [Advanced Encryption Standard (AES)/Temporal Key Integrity Protocol (TKIP)]
  - WPA/WPA2 Enterprise (AES/TKlP)

Video/Demo	Time
9.4.1 Enterprise Wireless Equipment	7:46
9.4.2 Configure Enterprise Wireless Networks	6:22
Total Video Time	**14:08**

Lab/Activity

9.4.4 Implement an Enterprise Wireless Network

Fact Sheets

9.4.3 Enterprise Wireless Facts

Number of Exam Questions

10 questions

Total Time

About 42 minutes

9.5: Wireless Security

Lecture Focus Questions:

- What does open authentication use to authenticate a device?
- Why is open authentication an unsecure solution?
- Which two additional components are required to implement 802.1x authentication?
- What is the difference between WPA Personal and WPA Enterprise?
- How can geofencing protect a network?
- Which default values should you always change on a wireless network?

In this section, you will learn to:

- Secure an enterprise wireless network

The key terms for this section include:

Term	Definition
Open authentication	An authentication method that requires clients to provide a MAC address to connect to the wireless network.
Shared key authentication	An authentication method that configures clients and access points with a shared key (called a secret or a passphrase). Only devices with the correct shared key can connect to the wireless network.
802.1x authentication	An authentication method that uses usernames and passwords, certificates, or devices such as smart cards to authenticate wireless clients.
Rogue access point	Any unauthorized access point added to a network.
Data emanation	The electromagnetic field generated by a network cable or network device (such as wireless router) that can be manipulated in order to eavesdrop on conversations or steal data.
Packet sniffing	The interception and decoding of wireless transmissions. It is also known as eavesdropping.
Interference	A signal that corrupts or destroys the wireless signal sent by APs and other wireless devices. Interference affects the availability of a network because normal communications are made impossible.
Jamming	Signal interference created intentionally by an attacker to make a wireless network impossible to use.
Deauthentication attack	An attack that spoofs the MAC address and then disconnects the device from the wireless network. Attackers can use a deauthentication attack to stage evil twin or on-path attacks.

Bluetooth	The standard for short-range wireless interconnection. It is designed to allow devices to communicate within a personal area network (PAN) of close proximity. PAN devices include cell phones, personal digital assistants (PDAs), printers, mouses, and keyboards.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Network Pro	4.1 Secure firewalls and security appliances • 4.1.3 Configure a screened subnet 4.2 Secure switches and wireless networks • 4.2.3 Secure an enterprise wireless network • 4.2.5 Secure email accounts on mobile devices 2.3 Configure wireless and VoIP • 2.3.2 Connect mobile devices

CompTIA Network+ N10-008	4.2 Compare and contrast common types of attacks.
	• 4.2.1 Technology-based
	  ○ Rogue access point (AP)
	  ○ Evil twin
	  ○ Deauthentication
	
	4.3 Given a scenario, apply network hardening techniques.
	• 4.3.2 Wireless security
	  ○ MAC filtering
	  ○ Antenna placement
	  ○ Power levels
	  ○ Wireless client isolation
	  ○ Guest network isolation
	  ○ Preshared keys (PSKs)
	  ○ EAP
	  ○ Geofencing
	  ○ Captive portal
	• 4.3.3 IoT access considerations
	
	5.5 Given a scenario, troubleshoot general networking issues.

- 5.5.2 Common issues
  - BYOD challenges

Video/Demo	Time
9.5.1 Wireless Security Part 1	8:10
9.5.2 Wireless Security Part 2	6:56
9.5.4 Wireless Attacks	9:40
9.5.6 Secure a Wireless Network	5:41
9.5.9 Configuring a Captive Portal	6:21
9.5.11 Creating a Guest Network for BYOD	7:30
Total Video Time	**44:18**

Lab/Activity

- 9.5.7 Secure an Enterprise Wireless Network
- 9.5.8 Enable Wireless Intrusion Prevention
- 9.5.10 Configuring a Captive Portal
- 9.5.12 Creating a Guest Network for BYOD
- 9.5.13 Configure a Secure Email Account on Mobile Device

Fact Sheets

- 9.5.3 Wireless Security Facts
- 9.5.5 Wireless Attack Facts

Number of Exam Questions

10 questions

Total Time

About 125 minutes

9.6: Wireless Troubleshooting

Lecture Focus Questions:

- Where is the best place to situate a wireless access point?
- What types of objects might obstruct radio frequency wireless transmissions?
- How many channels should separate two wireless networks?
- Which types of wireless networks require line-of-sight connections?
- How do range and antenna placement affect wireless networks?
- How does refraction affect an RF signal?

In this section, you will learn to:

- Optimize a wireless network
- Explore wireless network problems
- Troubleshoot wireless network problems

The key terms for this section include:

Term	Definition
Directional antenna	An antenna that creates a narrow, focused signal, which increases the signal strength and transmission distance. It provides a stronger point-to-point connection and is better equipped to handle obstacles.
Omnidirectional antenna	An antenna that disperses the radio frequency wave in an equal 360-degree pattern. This provides access to many clients in a radius.
Bandwidth saturation	The point at which all the available bandwidth on a connection has achieved maximum capacity and cannot pass any more data through the connection.
Device saturation	The point at which bandwidth utilization for the device is close to 100%.
Frequency mismatch	Devices on the network are not broadcasting on the same frequency.
Absorption	A signal passes through objects and the signal loses power.
Refraction	Radio waves pass through objects of different densities, causing the signal to bend or change speeds.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Network Pro	4.2 Secure switches and wireless networks • 4.2.3 Secure an enterprise wireless network 5.2 Troubleshoot wired and wireless connectivity

CompTIA Network+ N10-008	• 5.2.3 Troubleshoot wireless network problems
	
	5.4 Given a scenario, troubleshoot common wireless connectivity and performance issues.
	
	• 5.4.1 Specifications and limitations
	  ○ Throughput
	  ○ Speed
	  ○ Distance
	  ○ Received signal strength indication (RSSI) signal strength
	  ○ Effective isotropic radiated power (EIRP)/power settings
	• 5.4.2 Considerations
	  ○ Antennas
	  ○ Antennas - Placement
	  ○ Antennas - Type
	  ○ Antennas - Polarization
	  ○ Channel utilization
	  ○ AP association time
	  ○ Site survey
	• 5.4.3 Common issues
	  ○ Interference
	  ○ Interference - Channel overlap
	  ○ Antenna cable attenuation/signal loss
	  ○ RF attenuation/signal loss
	  ○ Wrong SSID
	  ○ Incorrect passphrase
	  ○ Encryption protocol mismatch
	  ○ Insufficient wireless coverage
	  ○ Captive portal issues
	  ○ Client disassociation issues

Video/Demo	Time
9.6.1 Wireless Communications Troubleshooting Part 1	7:56
9.6.2 Wireless Communications Troubleshooting Part 2	14:52
9.6.3 Troubleshoot Wireless Connections	6:24
9.6.5 Optimize Wireless Networks	4:39
Total Video Time	**33:51**

Lab/Activity

- 9.6.6 Optimize a Wireless Network
- 9.6.7 Explore Wireless Network Problems

- 9.6.8 Troubleshoot Wireless Network Problems

Fact Sheets

- 9.6.4 Wireless Network Troubleshooting Facts

Number of Exam Questions

10 questions

Total Time

About 85 minutes

Wide Area Networks (WANs)

10.1: WAN Concepts

Lecture Focus Questions:

- What is the optical carrier specification base rate? Why is the base rate significant?
- What are the differences between T1 and T3? E1 and E3?
- Concerning wide area network (WAN) technologies, what is a channel? Why are channels important?
- What is the difference between a packet-switched network and a circuit-switched network?
- What are the three types of wavelength-division multiplexing (WDM)? What are these types used for?
- Which characteristics of the different mobile WAN technologies determine the potential bandwidth?
- In which deployment scenario would a full tunnel virtual private network be preferrable to a split tunnel?
- Which WAN technology is a transport technology for carrying signals over fiber optic cables?
- How does Multiprotocol Label Switching (MPLS) add labels to packets? What are these labels used for?

The key terms for this section include:

Term	Definition
WAN cloud	The collection of equipment that makes up the WAN network. The WAN cloud is owned and maintained by telecommunications companies.
Central office (CO)	A switching facility connected to the WAN. It is the nearest point of presence for the WAN provider. It provides WAN cloud entry and exit points.
Local loop	The cable that extends from the central office to the customer location. The local loop is owned and maintained by the WAN service provider.
Demarcation point (Demarc)	The point that marks the boundary between the telco equipment and an organization's network or telephone system. When you contract with a local exchange carrier (LEC) for data or telephone services, the carrier installs a physical cable and a termination jack onto the organization's premises.
Customer premises equipment (CPE)	The devices physically located on the subscriber's premises. CPE includes both the wiring and devices that the subscriber owns and

	the equipment leased from the WAN provider. CPE can include the smart jack, demarc, local loop, copper line drivers, and repeaters.
Wavelength-division multiplexing	A WAN technology that allows multiple signals to be carried along a single fiberoptic cable in both directions using different wavelengths of light for each signal. WDM types include coarse and dense. Both coarse and dense WDM can be single- or bi-directional.
Digital Subscriber Line (DSL)	A line that enables digital signals to be transmitted over telephone wiring. A limitation is that the endpoint must be within a certain distance of the nearest network repeating device.
Virtual private network (VPN)	A virtual network that creates an encrypted connection between a device, such as a laptop or mobile phone, and a secure network. The encrypted connection allows secure communication between the device and the network.
Integrated Services Digital Network (ISDN)	A WAN technology that provides increased bandwidth within the local loop. The two forms of ISDN are ISDN basic rate interface (BRI) and ISDN primary rate interface (PRI).
Distributed switching	An architecture in which multiple processor-controlled switching units are distributed. There is often a hierarchy of switching elements with a centralized host switch and remote switches located close to concentrations of users.
Multiprotocol Label Switching (MPLS)	MPLS is a WAN data classification and data carrying mechanism. MPLS is a packet switching technology that supports variable-length frames.

This section helps you prepare for the following certification exam objectives:

Exam	Objective

CompTIA Network+ N10-008	1.2 Explain the characteristics of network topologies and network types.
	
	• 1.2.6 Network types and characteristics
	  ○ Multiprotocol label switching (MPLS)
	• 1.2.9 Provider links
	  ○ Satellite
	  ○ Digital subscriber line (DSL)
	  ○ Cable
	  ○ Leased line
	  ○ Metro-optical
	
	1.3 Summarize the types of cables and connectors and explain which is the appropriate type for a solution.
	
	• 1.3.5 Ethernet standards
	  ○ Coarse wavelength division multiplexing (CWDM)
	  ○ Dense wavelength division multiplexing (DWDM)

- Bidirectional wavelength division multiplexing (WDM)

Video/Demo	Time
10.1.1 WAN Concepts	11:26
Total Video Time	**11:26**

Fact Sheets

10.1.2 WAN Concept Facts

Number of Exam Questions

10 questions

Total Time

About 27 minutes

10.2: Internet Connectivity

Lecture Focus Questions:

- Which connection speeds should you expect from various types of internet connectivity?
- What is multiplexing? How does it increase the bandwidth of a connection?
- How does DSL enable you to talk on the phone and connect to the internet at the same time?
- What are the requirements for qualifying for DSL service?
- Which DSL service does not support simultaneous voice and data transmissions?
- What are the advantages and disadvantages of the different mobile connectivity technologies?
- Which features of an optical (fiber connection) enable superior bandwidth to other connectivity technologies?
- What are the disadvantages of a satellite internet connection?

In this section, you will learn to:

- Connect to a DSL network

The key terms for this section include:

Term	Definition
Digital Subscriber Line (DSL)	A high-speed digital bandwidth connection from a phone wall jack on an existing telephone network. With DSL, data and voice are both sent on the same copper wire with data using one frequency and voice using another.
Cellular networking	A digital mobile network that can provide internet access. It is commonly used by phones, tablets, laptops, and mobile hot spots.
Cable	Internet access provided by companies that offer cable TV service using the same lines.
Satellite	Internet access by using signals transmitted to and received from orbiting satellites.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Network Pro	1.1 Implement Components and Cabling solutions • 1.1.4 Connect computer and network components
CompTIA Network+ N10-008	1.2 Explain the characteristics of network topologies and network types. • 1.2.9 Provider links

- Satellite
- Digital subscriber line (DSL)
- Cable
- Leased line
- Metro-optical

2.4 Given a scenario, install and configure the appropriate wireless standards and technologies.

- 2.4.8 Cellular technologies
  - Code-division multiple access (CDMA)
  - Global System for Mobile Communications (GSM)
  - Long-Term Evolution (LTE)
  - 3G, 4G, 5G

Video/Demo	Time
10.2.1 Traditional Internet Connectivity	14:57
10.2.2 Mobile Internet Connectivity	10:50
Total Video Time	**25:47**

Lab/Activity

10.2.4 Connect to a DSL Network

Fact Sheets

10.2.3 Internet Services Facts

Number of Exam Questions

10 questions

Total Time

About 53 minutes

10.3: Remote Access

Lecture Focus Questions:

- What is the difference between authentication and authorization?
- What is an advantage of using Remote Authentication Dial-in User Service (RADIUS) or Terminal Access Controller Access-Control System Plus (TACACS+) in a remote access solution?
- How does RADIUS differ from TACACS+?

In this section, you will learn to:

- Configure a RADIUS solution.

The key terms for this section include:

Term	Definition
Authentication	The process of proving identity where logon credentials are exchanged and logon is allowed or denied.
Authorization	The process of identifying the resources that a user can access over the remote access connection.
Accounting	An activity that tracks or logs the use of the remote access connection.
AAA Server	A server used to centralize authentication, authorization, and accounting for multiple remote access servers. Connection requests from remote clients are received by the remote access server and are forwarded to the AAA server to be approved or denied. Policies defined on the AAA server apply to all clients connected to all remote access servers.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Network Pro	4.4 Secure remote connections and VPNs • 4.4.2 Configure a remote access VPN

CompTIA Network+ N10-008	3.2 Explain the purpose of organizational documents and policies.
	• 3.2.2 Hardening and security policies
	  ○ Remote access policy
	4.1 Explain common security concepts.
	• 4.1.9 Authentication methods
	  ○ Terminal Access Controller Access-Control System Plus (TACACS+)

- Remote Authentication Dial-in User Service (RADIUS)

Video/Demo	Time
10.3.1 Remote Access	5:02
10.3.2 Configuring a RADIUS Solution	2:52
Total Video Time	**7:54**

Fact Sheets

10.3.3 Remote Access Facts

Number of Exam Questions

10 questions

Total Time

About 23 minutes

10.4: Virtual Private Networks

Lecture Focus Questions:

- What are the ways a virtual private network (VPN) can be implemented?
- What is a VPN concentrator?
- Which function do VPN endpoints provide?
- What is the difference between a full tunnel and split tunnel?
- What is inverse split tunneling?

In this section, you will learn to:

- Configure a VPN
- Configure a VPN client
- Configure a remote access VPN
- Configure a VPN connection iPad

The key terms for this section include:

Term	Definition
Virtual private network (VPN)	A type of network that uses encryption to allow IP traffic to travel securely over the TCP/IP network. A VPN is used primarily to support secure communications over an untrusted network.
Tunneling	Communication method that encrypts packet contents and encapsulates them for routing though a public network.
Internet Protocol Security (IPsec)	A set of protocols that provides security for Internet Protocol (IP) which can be used to set up a VPN solution.
Secure Sockets Layer (SSL)	A protocol to secure IP protocols such as HTTP and FTP. It is now largely unused.
Transport Layer Security (TLS)	A protocol that evolved from SSL and provides privacy and data integrity between two communicating applications.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Network Pro	4.4 Secure remote connections and VPNs • 4.4.2 Configure a remote access VPN • 4.4.3 Configure a mobile device VPN connection

CompTIA Network+ N10-008	4.4 Compare and contrast remote access methods and security implications.
	• 4.4.1 Site-to-site VPN
	• 4.4.2 Client-to-site VPN
	  ○ Clientless VPN
	  ○ Split tunnel vs. full tunnel

- Authentication and authorization considerations

Video/Demo	Time
10.4.1 Virtual Private Networks	8:32
10.4.2 Configuring a VPN	9:13
10.4.4 Configuring a VPN Client	2:40
Total Video Time	**20:25**

Lab/Activity

- 10.4.3 Configure a Remote Access VPN
- 10.4.5 Configure a VPN Connection iPad

Fact Sheets

- 10.4.6 VPN Protocol Facts
- 10.4.7 VPN Facts

Number of Exam Questions

10 questions

Total Time

About 65 minutes

Network Operations and Management

11.1: Performance Metrics

Lecture Focus Questions:

- What is the difference in bandwidth, throughput, and latency?
- How is a baseline established?
- What happens when a CPU overheats?

The key terms for this section include:

Term	Definition
Bottleneck	The condition that occurs when a system is unable to keep up with the demands placed on it.
Latency	The speed that data packets travel from source to destination and back. All packets experience some level of latency.
Bandwidth	The amount of data that could be transferred from one place to another in a specific amount of time.
Throughput	The amount of data that is transferred from one place to another in a specific amount of time.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Network Pro	1.1 Place objective here • Place sub objectives here ○ And here if needed 3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability. • 3.1.1 Performance metrics/sensors

CompTIA Network+ N10-008	○ Device/chassis
	  ▪ Temperature
	  ▪ Central processing unit (CPU) usage
	  ▪ Memory
	○ Network metrics
	  ▪ Bandwidth
	  ▪ Latency

- Jitter

Video/Demo	Time
11.1.1 Performance Metrics	5:17
Total Video Time	**5:17**

Fact Sheets

11.1.2 Performance Metrics

Number of Exam Questions

10 questions

Total Time

About 21 minutes

11.2: Network Management with SNMP

Lecture Focus Questions:

- What is SNMP?
- What is the role of the MIB when using SNMP?
- How is a trap used in network administration?
- Why doesn't the community name provide security for SNMP devices?

In this section, you will learn to:

- Configure an SNMP system on a router
- Monitor a switch with SNMP
- Configure an SNMP trap

The key terms for this section include:

Term	Definition
Simple Network Management Protocol (SNMP)	A protocol designed for managing complex networks. SNMP lets network hosts exchange configuration and status information. This information is gathered by management software to monitor and manage the network and network events.
Manager	A computer used to perform management tasks. The manager queries agents and gathers responses by sending messages.
Agent	A software process that runs on managed network devices. The agent communicates information to the manager and can send dynamic messages to it as well.
Trap	An event configured on an agent. When the event occurs, the agent logs details regarding the event.
Management information base (MIB)	A database of host configuration information. Agents report data to the MIB. The manager can view information by requesting data from the MIB.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Network Pro	1.1 Place objective here • Place sub objectives here ○ And here if needed
CompTIA Network+ N10-008	3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability. • 3.1.2 SNMP

- Traps
- Object identifiers (OIDs)
- Management information bases (MIBs)

Video/Demo	Time
11.2.1 Network Management with SNMP	5:14
11.2.2 Configure an SNMP System on a Router	2:38
11.2.3 Monitor Switch with SNMP	1:55
11.2.4 Configure SNMP Trap	5:40
Total Video Time	**15:27**

Fact Sheets

11.2.5 SNMP Facts

Number of Exam Questions

10 questions

Total Time

About 31 minutes

11.3: Log File Management

Lecture Focus Questions:

- Where are most log files stored by default?
- What is a System Logging Protocol (Syslog) server?
- What are the Syslog security levels?

In this section, you will learn to:

- Configure a Syslog server on a router
- Configure remote logging on Linux
- Log events on pfSense
- Audit device logs on a Cisco switch
- Configure logging on pfSense

The key terms for this section include:

Term	Definition
System Logging Protocol	A standard for system logging. Using syslog, any device can send messages about the status of events that are occurring on the device, operating system, or applications. Syslog operates using UDP on ports 514 and 601.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Network Pro	1.1 Place objective here • Place sub objectives here ○ And here if needed 3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.

CompTIA Network+ N10-008	• 3.1.3 Network device logs
	  ○ Log reviews
	  ▪ Traffic logs
	  ▪ Audit logs
	  ▪ Syslog
	  ○ Logging levels/security levels

Video/Demo **Time**

11.3.1 Log File Management	6:50
11.3.2 Configure a Syslog Server on a Router	3:21
11.3.3 Configuring Remote Logging on Linux	6:31
11.3.4 Logging Events on pfSense	6:00
11.3.7 Auditing Device Logs on a Cisco Switch	3:58
Total Video Time	**26:40**

Lab/Activity

- 11.3.6 Configure Logging on pfSense
- 11.3.8 Auditing Device Logs on a Cisco Switch

Fact Sheets

- 11.3.5 Log File Management Facts

Number of Exam Questions

10 questions

Total Time

About 66 minutes

11.4: Monitoring

Lecture Focus Questions:

- What is the goal of network monitoring?
- Why would a network administrator need to use a protocol analyzer?
- What measures can be taken to reduce temperatures in a server room?
- What impact can high temperatures have on computer equipment?

In this section, you will learn to:

- View event logs
- Use Wireshark to sniff traffic
- Monitor utilization
- Monitor interface statistics
- Configure Netflow on pfSense
- Monitor throughput with iperf

The key terms for this section include:

Term	Definition
Throughput tester	A device that measures the amount of data that can be transferred through a network or processed by a device (such as the amount of data that can be retrieved from a disk in a specific period).
Packet sniffer	A device that captures data that is being transmitted on a network and saves it for later analysis.

This section helps you prepare for the following certification exam objectives:

Exam	Objective

CompTIA Network+ N10-008	3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.
	• 3.1.4 Interface statistics/status
	  ○ Link state (up/down)
	  ○ Speed/duplex
	  ○ Send/receive traffic
	  ○ Cyclic redundancy checks (CRCs)
	  ○ Protocol packet and byte counts
	• 3.1.5 Interface errors or alerts
	  ○ CRC errors
	  ○ Giants
	  ○ Runts
	  ○ Encapsulation errors
	• 3.1.6 Environmental factors and sensors
	  ○ Temperature
	  ○ Humidity
	  ○ Electrical

    - Flooding
- 3.1.7 Baselines
- 3.1.8 NetFlow data
- 3.1.9 Uptime/downtime

5.3 Given a scenario, use the appropriate network software tools and commands.

- 5.3.1 Software tools
    - Protocol analyzer/packet capture
    - Bandwidth speed tester
    - Port scanner
    - iperf
    - NetFlow analyzers
    - IP scanner

Video/Demo	Time
11.4.1 Network Monitoring	4:01
11.4.2 Protocol Analyzers	3:46
11.4.3 View Event Logs	5:17
11.4.4 Use Wireshark to Sniff Traffic	6:47
11.4.5 Monitor Utilization	7:12
11.4.6 Monitor Interface Statistics	5:09
11.4.7 Configure Netflow on pfSense	3:23
11.4.8 Monitor Throughput with iperf	3:58
11.4.10 Environmental Monitoring	8:25
Total Video Time	**47:58**

Fact Sheets

- 11.4.9 Network Monitoring Facts
- 11.4.11 Environmental Monitoring Facts

Number of Exam Questions

10 questions

Total Time

About 68 minutes

11.5: Organization Policies

Lecture Focus Questions:

- What are onboarding and offboarding policies?
- What does a password policy include?
- What information is needed to create a network diagram?
- What is the difference between a policy and procedure?

The key terms for this section include:

Term	Definition
Policy	A policy describes the overall goals and requirements for a network. A policy identifies what should be done, but may not necessarily define how it should be done.
Procedure	A procedure is a step-by-step process outlining how to implement a specific action. The design of a procedure is guided by goals defined in a policy, but it is more detailed than a policy; it must identify the specific steps you must execute.
Standard operating procedure (SOP)	Documentation that provides detailed instructions for performing a complex business activity. A standard operating procedure is carefully designed with a specific outcome in mind and should be detailed.
Security incident	A security incident is an event or series of events that result from a security policy violation that has adverse effects on a company's ability to proceed with normal business.
Incident response	Incident response is the actions taken to deal with an incident during and after its occurrence. Prior planning helps people know what to do when a security incident takes place.

This section helps you prepare for the following certification exam objectives:

Exam	Objective

CompTIA Network+ N10-008	3.2 Explain the purpose of organizational documents and policies.
	• 3.2.1 Plans and procedures
	  ○ Change management
	  ○ Incident response plan
	  ○ Disaster recovery plan
	  ○ Business continuity plan
	  ○ System life cycle
	  ○ Standard operating procedure
	• 3.2.2 Hardening and security policies
	  ○ Password policy
	  ○ Acceptable use policy
	  ○ Bring your own device (BYOD) policy

    - Remote access policy
    - Onboarding and offboarding policy
    - Security policy
    - Data loss prevention
- 3.2.3 Common documentation
    - Physical network diagram
        - Floor plan
        - Rack diagram
        - Intermediate distribution frame (IDF/main distribution frame (MDF) documentation
    - Logical network diagram
    - Wiring diagram
    - Site survey report
    - Audit and assessment report
    - Baseline configurations
- 3.2.4 Common agreements
    - Non-disclosure agreement (NDA)
    - Service-level agreement (SLA)
    - Memorandum of understanding (MOU)

Video/Demo	Time
11.5.1 Plans and Procedures	5:49
11.5.3 Security Policies	4:14
11.5.5 Documentation and Agreements	8:41
Total Video Time	**18:44**

Fact Sheets

- 11.5.2 Plans and Procedure Facts
- 11.5.4 Security Policy Facts
- 11.5.6 Documentation and Agreements Facts

Number of Exam Questions

10 questions

Total Time

About 44 minutes

11.6: Redundancy and High Availability

Lecture Focus Questions:

- Which feature would you use to configure a device with two connections to the same network?
- How does a brownout differ from a blackout?
- What is the difference between an SPS and a UPS?
- Why is redundancy important to network security?
- Why would a network administrator want to use load balancing?
- What is the difference between active/active and active/passive?

In this section, you will learn to:

- Configure UPS settings
- Set up NIC teaming
- Configure NIC teaming
- Configure Linux Network Bonding
- Configure a load balancing server

The key terms for this section include:

Term	Definition
High availability	A term meaning that a network or a service is up and accessible most of the time.
Redundancy	A method for providing fault tolerance by using duplicate or multiple components that perform the same function.
Uptime	The percentage of time the network or service is up and accessible.
Fault tolerance	The ability to respond to an unexpected hardware or software failure without loss of data or loss of operation.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Network Pro	3.4 Manage backup and restore tasks • 3.4.1 Back up files with File History
CompTIA Network+ N10-008	3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution. • 3.3.1 Load balancing • 3.3.2 Multipathing • 3.3.3 Network interface card (NIC) teaming • 3.3.4 Redundant hardware/clusters

- Switches
- Routers
- Firewalls

- 3.3.5 Facilities and infrastructure support
  - Uninterruptible power supply (UPS)
  - Power distribution units (PDUs)
  - Generator
- 3.3.6 Redundancy and high availability concepts
  - Cold site
  - Warm site
  - Hot site
  - Cloud site
  - Active-active vs. active-passive
    - Multiple Internet service providers (ISPs)/diverse paths
    - Virtual Router Redundancy Protocol (VRRP)/First Hop Redundancy Protocol (FHRP)
  - Mean time to repair (MTTR)
  - Mean time between failure (MTBF)
  - Recovery time objective (RTO)
  - Recovery point objective (RPO)

Video/Demo	Time
11.6.1 High Availability	7:35
11.6.2 Redundancy Solutions	3:09
11.6.4 Power Management	11:37
11.6.6 Configure UPS Settings	5:38
11.6.7 Hardware Clustering	7:53
11.6.8 Set Up NIC Teaming	3:09
11.6.10 Configure Linux Network Bonding	8:02
11.6.12 Configure Load a Balancing Server	6:12
Total Video Time	**53:15**

Lab/Activity

- 11.6.9 Configure NIC Teaming

Fact Sheets

- 11.6.3 Redundancy and High Availability Facts
- 11.6.5 Power Management Facts
- 11.6.11 NIC Teaming Facts

Number of Exam Questions

10 questions

Total Time
About 91 minutes

11.7: Data Backup and Storage

Lecture Focus Questions:

- Why are there different backup types?
- How often should you run a full backup?
- What is the difference between an incremental and differential backup?

In this section, you will learn to:

- Configure an NAS for data backups
- Back up data
- Implement file backups
- Back up files with File History
- Recover files
- Recover a file from File History

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Network Pro	1.1 Implement Components and Cabling solutions • 1.1.6 Configure a load balancing server 1.2 Implement Wired and Wireless devices • 1.2.6 Configure NIC teaming 3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution.

CompTIA Network+ N10-008	• 3.3.7 Network device backup/restore
	  ○ State
	  ○ Configuration

Video/Demo	Time
11.7.1 Data Backups	10:16
11.7.2 Backup Storage Options	3:23
11.7.4 Configure a NAS for Data Backups	5:15
11.7.5 Implementing File Backups	7:42
11.7.7 Recover Files	3:37
Total Video Time	**30:13**

Lab/Activity

- 11.7.6 Back Up Files with File History
- 11.7.8 Recover a File from File History

Fact Sheets

- 11.7.3 Data Backup and Storage Facts

Number of Exam Questions

10 questions

Total Time

About 70 minutes

11.8: Remote Management

Lecture Focus Questions:

- How does remote desktop software differ from terminal emulation software?
- How can you use remote desktop solutions for troubleshooting and technical support within your organization?
- Under what circumstances would you want to install a remote gateway?

In this section, you will learn to:

- Use remote desktop
- Allow remote desktop connections

The key terms for this section include:

Term	Definition
Remote desktop	A remote desktop utility displays the graphical user interface of a remote device. Remote desktop solutions are used to remotely manage a computer or allow support personnel to view and troubleshoot a remote user's system.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Network Pro	4.4 Secure remote connections and VPNs • 4.4.1 Allow remote desktop connections
CompTIA Network+ N10-008	4.4 Compare and contrast remote access methods and security implications. • 4.4.3 Remote desktop connection • 4.4.4 Remote desktop gateway • 4.4.5 SSH • 4.4.6 Virtual network computing (VNC)

Video/Demo	Time
11.8.1 Remote Management	7:18
11.8.2 Use Remote Desktop	10:05
Total Video Time	**17:23**

Lab/Activity

- 11.8.3 Allow Remote Desktop Connections

Fact Sheets

11.8.4 Remote Management Facts

Number of Exam Questions
10 questions

Total Time
About 45 minutes

Network Security

12.1: Security Concepts

Lecture Focus Questions:

- How can you use the CIA triad to help create a strong security plan that also provides accessibility?
- Which are more difficult to prevent and detect, internal or external threats?
- What is the CVE list and how can it benefit network security?
- What is the attacker's window of opportunity in a zero-day attack?
- Which common protocols are secure and which ones are not?
- How can role-based access control simplify application of the principle of least privilege in your network?
- What are important components to a defense in-depth strategy?
- Why is a layered approach to network security important?

In this section, you will learn to:

- Configure permissions
- Scan for unsecure protocols
- Configure a honeypot

The key terms for this section include:

Term	Definition
Vulnerability	A weak area of a network that could result in a security breach.
Exploit	The breaching of security through a weakness in systems, software, hardware, policies, or human behavior.
Principle of least privilege	The idea that rights and permissions for each user or system are limited to only what is necessary for the user or system to accomplish their tasks or responsibilities.
Role-based access control (RBAC)	A method of limiting network access levels through assignment of permissions and rights based on the role of the user.
Confidentiality	A set of rules and practices that protect data and resources from unauthorized access.
Integrity	The protection of data and resources from unauthorized manipulation or alteration, keeping the data secure, accurate, and trustworthy, including data at rest and data in transit.
Availability	The timely and reliable access for authorized users to the resources and data in a network.
Zero trust	A security strategy based on the concept that no users or devices should be allowed access to the network's sensitive data

	without proper authentication and authorization within the network.

This section helps you prepare for the following certification exam objectives:

Exam	Objective

CompTIA Network+ N10-008	4.1 Explain common security concepts.
	• 4.1.1 Confidentiality, integrity, availability (CIA)
	• 4.1.2 Threats
	  ○ Internal
	  ○ External
	• 4.1.3 Vulnerabilities
	  ○ Common vulnerabilities and exposures (CVE)
	  ○ Zero-day
	• 4.1.4 Exploits
	• 4.1.5 Least privilege
	• 4.1.6 Role-based access
	• 4.1.7 Zero trust
	• 4.1.8 Defense in depth
	  ○ Network segmentation enforcement
	  ○ Separation of duties
	  ○ Network access control
	  ○ Honeypot
	• 4.1.9 Authentication methods
	  ○ Multifactor
	  ○ Terminal Access Controller Access-Control System Plus (TACACS+)
	  ○ Single sign-on (SSO)
	  ○ Remote Authentication Dial-in User Service (RADIUS)
	  ○ LDAP
	  ○ Kerberos
	  ○ Local authentication
	  ○ 802.1X
	  ○ Extensible Authentication Protocol (EAP)

Video/Demo	Time
12.1.1 Security Concepts	7:39
12.1.3 Configure Permissions	9:39
12.1.4 Secure Protocols	8:03
12.1.5 Scan for Unsecure Protocols	4:52

12.1.7 Defense in Depth	9:40
12.1.9 Configure a Honeypot	3:24
Total Video Time	**43:17**

Fact Sheets

- 12.1.2 Security Concepts Facts
- 12.1.6 Secure Protocol Facts
- 12.1.8 Defense in Depth Facts

Number of Exam Questions

10 questions

Total Time

About 69 minutes

12.2: Risk Management

Lecture Focus Questions:

- What is a risk assessment?
- What is a posture assessment?
- What are the four basic categories for managing risk?
- What is the difference between penetration testing and a vulnerability assessment?
- What is a SIEM system and how does it work?
- What is a process assessment?
- What is a vendor assessment?

In this section, you will learn to:

- Explore penetration testing tools
- Conduct a vulnerability scan

The key terms for this section include:

Term	Definition
Asset	A resource that has value to the organization. Assets take many forms, including information, infrastructure, physical devices, or support services.
Threat	Any potential danger to the confidentiality, integrity, or availability of information or systems.
Vulnerability	The possibility of an asset being exploited due to the absence or weakness of an asset safeguard.
Cybersecurity posture	The overall state and effectiveness of the security in a network's hardware, software, databases, transmissions, or processes.
Process	A sequence of events or activities which produces an expected result.

This section helps you prepare for the following certification exam objectives:

Exam	Objective

CompTIA Network+ N10-008	4.1 Explain common security concepts.
	
	• 4.1.10 Risk Management
	  ○ Security risk assessment
	  ▪ Threat assessment
	  ▪ Vulnerability assessment
	  ▪ Penetration testing
	  ▪ Posture assessment
	  ○ Business risk assessment
	  ▪ Process assessment
	  ▪ Vendor assessment

- 4.1.11 Security information and event management (SIEM)

4.5 Explain the importance of physical security.

- 4.5.3 Asset disposal
  - Factory reset/wipe configuration
  - Sanitize devices for disposal

Video/Demo	Time
12.2.1 Risk Management	6:54
12.2.3 Penetration Testing	2:41
12.2.5 Security Information and Event Management	4:35
12.2.7 Vulnerability Assessment	5:10
12.2.8 Conduct a Vulnerability Scan	3:17
Total Video Time	**22:37**

Fact Sheets

- 12.2.2 Risk Management Facts
- 12.2.4 Penetration Testing Facts
- 12.2.6 Security Information and Event Management Facts
- 12.2.9 Vulnerability Assessment Facts

Number of Exam Questions

10 questions

Total Time

About 53 minutes

12.3: Physical Security

Lecture Focus Questions:

- What are the basic categories of a multi-barrier system?
- What are physical control measures you can implement to protect your network?
- What are important considerations in physical security?
- What types of equipment are available to aid in physical security?

In this section, you will learn to:

- Implement physical security

The key terms for this section include:

Term	Definition
Infrared detector	An electronic device that can sense infrared radiation that emanates from living things and hot things.
Biometric scanner	Hardware that scans something physical on a person (such as a fingerprint, iris, face, or heart rate) and compares the information to its database for authentication purposes.
Proximity alarm	A sensor that detects the presence of an object within a set distance.
Smartcard reader	A device that reads a plastic badge that contains a memory chip and can be used for authentication purposes.

This section helps you prepare for the following certification exam objectives:

Exam	Objective

TestOut Network Pro	1.1 Implement Components and Cabling solutions
	• 1.1.2 Implement physical security
	
	4.5 Explain the importance of physical security.
	• 4.5.1 Detection methods
	  ○ Camera
	  ○ Motion detection
	  ○ Asset tags
	  ○ Tamper detection
	• 4.5.2 Prevention methods
	  ○ Employee training
	  ○ Access control hardware
	  ▪ Badge readers
	  ▪ Biometrics
	  ○ Locking racks
	  ○ Locking cabinets

CompTIA Network+ N10-008	

- Access Control vestibule
- Smart lockers

Video/Demo	Time
12.3.1 Physical Security	8:14
Total Video Time	**8:14**

Lab/Activity

- 12.3.3 Implement Physical Security

Fact Sheets

- 12.3.2 Physical Security Facts

Number of Exam Questions

10 questions

Total Time

About 36 minutes

12.4: Social Engineering

Lecture Focus Questions:

- What is social engineering?
- How can you verify that a website is using HTTPS?
- Why are social engineering attacks so common and effective?
- How can you protect your organization from social engineering attacks?
- How can you investigate a social engineering attack?

In this section, you will learn to:

- Use the Social Engineering Toolkit
- Investigate a social engineering attack
- Respond to social engineering exploits

The key terms for this section include:

Term	Definition
Masquerading	When a person presents themselves as a trustworthy person that plays on the victim's emotions to obtain information or access.
Malicious insiders	People that have authorized access to be inside the organization's facility (such as employees, contractors, or vending machine technicians) but take advantage of the trust given them to perform attacks against the organization. These can be passive attacks or active attacks.
Access control vestibule	A security buffer zone created through two interlocking doors that require the person wanting to pass through to provide authentication. This can be used to detain an intruder if proper authentication is not provided.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Network Pro	4.5 Secure network exploits • 4.5.2 Respond to social engineering exploits

CompTIA Network+ N10-008	4.2 Compare and contrast common types of attacks.
	• 4.2.2 Human and environmental
	  ○ Social engineering
	  ▪ Phishing
	  ▪ Tailgating
	  ▪ Piggybacking
	  ▪ Shoulder surfing

Video/Demo	Time
12.4.1 Social Engineering	9:13
12.4.3 Use the Social Engineer Toolkit	4:25
12.4.4 Investigating a Social Engineering Attack	6:31
Total Video Time	**20:09**

Lab/Activity

- 12.4.5 Respond to Social Engineering Exploits

Fact Sheets

- 12.4.2 Social Engineering Facts

Number of Exam Questions

10 questions

Total Time

About 48 minutes

12.5: Network Threats and Attacks

Lecture Focus Questions:

- What is the main goal in a denial-of-service (DoS) attack?
- How do DDoS and DrDoS attacks differ?
- What is the difference between a virus and a worm?
- In addition to implementing virus scanning software, what must you do to ensure that you are protected from the latest virus variations?
- Why is employee training so important in network protection?

In this section, you will learn to:

- Launch a DoS and DDoS attack
- Crack passwords
- Crack password-protected files
- Crack a password with John the Ripper

The key terms for this section include:

Term	Definition
Malware	Malware is a type of software designed to take over or damage a computer without the user's knowledge or approval.
DoS and DDoS	Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks impact system availability by flooding the target system with traffic or requests or by exploiting a system or software flaw.
Permanent denial of service (PDoS)	A permanent denial of service (PDoS) is an attack that damages a system so badly that it requires the replacement or re-installation of hardware.
Virus	A virus is a program that attempts to damage a computer system and replicate itself to other computer systems.
Worm	A worm is a self-replicating program.
Trojan horse	A Trojan horse is a malicious program that is disguised as legitimate or desirable software.
Zombie	A zombie is a computer that is infected with malware that allows remote software updates and control through a command and control center called a zombie master.
Botnet	A botnet refers to a group of zombie computers that are commanded from a central control infrastructure.
Rootkit	A rootkit is a set of programs that allow attackers to maintain permanent and hidden administrator-level access to a computer.
Logic bomb	A logic bomb is designed to execute only under predefined conditions and lies dormant until the predefined condition is met.

Spyware	Spyware is software that is installed without the user's consent or knowledge. Spyware is designed to intercept or take partial control of the user's interaction with the computer.
Adware	Adware monitors actions that denote personal preferences and then sends pop-ups and ads that match those preferences.
Ransomware	Ransomware denies access to a computer system until the user pays a ransom.
Scareware	Scareware is a scam that fools users into thinking they have some form of malware on their system. The intent of the scam is to sell the user fake antivirus software to remove malware they don't have.
Crimeware	Crimeware is designed to facilitate identity theft by gaining access to a user's online financial accounts, such as banks and online retailers.
Ping flood	A ping flood is a simple DoS attack where the attacker overwhelms the victim with ICMP Echo Request (ping) packets.
Ping of death	The ping of death is a DoS attack that uses the ping utility to send oversized ICMP packets.
Smurf	A smurf attack is a form of DrDoS attack that spoofs the source address in ICMP packets. A smurf attack requires an attacker system, an amplification network, and a victim computer or network.
SYN flood	The SYN flood exploits the TCP three-way handshake. So many resources are allocated that the victim cannot process a legitimate inbound request for a TCP/IP session.
LAND	A LAND attack is when an attacker floods the victim's system with packets that have forged headers.
Christmas (Xmas) tree	A Christmas (Xmas) tree attack (also known as Christmas tree scan, nastygram, kamikaze, or lamp test segment) uses an IP packet with every option turned on for the protocol being used. Christmas tree packets can be used to conduct reconnaissance by scanning for open ports and a DoS attack if sent in large numbers.
On-path attack	An on-path attack is used to intercept information between two communication partners.
TCP/IP (session) hijacking	TCP/IP hijacking is an extension of an on-path attack where the attacker steals an open and active communication session from a legitimate user.
HTTP (session) hijacking	HTTP (session) hijacking is a real-time attack in which the attacker hijacks a legitimate user's cookies and uses the cookies to take over the HTTP session.
Replay attack	In a replay attack, the attacker uses a protocol analyzer or sniffer to capture authentication information going from the client to the server. The attacker then uses this information to connect at a later time and pretend to be the client.

IP spoofing	IP spoofing changes the IP address information within a packet. It can be used to hide the origin of the attack by spoofing the source address. It can also amplify attacks by sending a message to a broadcast address and then redirecting responses to a victim who is overwhelmed with responses.
MAC spoofing	MAC spoofing is when an attacking device spoofs the MAC address of a valid host in the MAC address table of the switch. The switch then forwards frames destined for that valid host to the attacking device.
ARP spoofing	ARP spoofing (also known as ARP poisoning) uses spoofed ARP messages to associate a different MAC address with an IP address. ARP spoofing can also be used to perform denial-of-service (DoS) attacks by redirecting communications to fake or nonexistent MAC addresses.
DNS spoofing	DNS spoofing (also known as DNS poisoning or pharming) takes advantage of the DNS server's ability to resolve a domain into its respective IP address. This attack exploits DNS vulnerabilities, resolving a domain typed on a browser into a fake IP address. It also redirects connections to a potentially malicious server.

This section helps you prepare for the following certification exam objectives:

Exam	Objective

TestOut Network Pro	4.5 Secure network exploits
	• 4.5.4 Crack a password
	
	4.2 Compare and contrast common types of attacks.
	• 4.2.1 Technology-based
	  ○ DoS
	  ▪ Botnet/command and control
	  ○ Ransomware
	  ○ Password attacks
	  ▪ Brute-force
	  ▪ Dictionary
	  ○ Malware

CompTIA Network+ N10-008	

Video/Demo	Time
12.5.1 Malware	10:55
12.5.3 Denial of Service (DoS)	6:33
12.5.4 Launch a DoS and DDoS Attack	5:44
12.5.6 Password Attacks	7:26
12.5.7 Crack Passwords	8:03
12.5.8 Crack Password Protected Files	3:22

Total Video Time **42:03**

Lab/Activity

- 12.5.10 Crack a Password with John the Ripper

Fact Sheets

- 12.5.2 Malware Facts
- 12.5.5 Denial of Service
- 12.5.9 Password Attack Facts

Number of Exam Questions

11 questions

Total Time

About 81 minutes

12.6: Spoofing Attacks

Lecture Focus Questions:

- What are some common attacks that use IP spoofing?
- How does DNS poisoning work?
- Is it possible to be a victim of an on-path attack and not know it?
- How can a MAC address be spoofed if it is hard-coded on the NIC?
- How can an attacker manipulate an ARP cache to redirect frames to capture all outbound data?
- What kinds of problems can a rogue DHCP server cause in your network?

In this section, you will learn to:

- Poison ARP
- Poison ARP and Analyze with Wireshark
- Poison DNS
- Use SMAC to spoof MAC addresses
- Perform an on-path DHCP attack
- Perform a DHCP spoofing on-path attack
- Detect a rogue DHCP server
- Set up DHCP snooping
- Configure DHCP snooping

The key terms for this section include:

Term	Definition
Session	A temporary, interactive communication between two or more systems, such as a client and a server, or between personal computers.
Spoofing	The process of masquerading as another identity.
IPv4 (Internet Protocol version 4)	A standard-based protocol widely used to route internet traffic that defines endpoint device addresses in a 32-bit format.
IPv6 (Internet Protocol version 6)	A standard-based protocol designed to replace IPv4 with more secure 128-bit alpha-numeric value addresses that are assigned to endpoint devices.
TCP (Transmission Control Protocol)	An unsecure communication protocol that allows a client and server to communicate and guarantees data packets will be delivered in the order sent.
DNS (Domain Name System)	A system that converts alphabetic hostnames to the associated IP addresses that are stored in a database.

This section helps you prepare for the following certification exam objectives:

Exam	Objective

TestOut Network Pro	3.1 Manage DHCP services • 3.1.3 Configure DHCP snooping 4.5 Secure network exploits • 4.5.3 Perform on-path attacks • 4.5.5 Indentify poisoning attacks

CompTIA Network+ N10-008	4.2 Compare and contrast common types of attacks.
	• 4.2.1 Technology-based
	  ○ On-path attack (previously known as man-in-the-middle)
	  ○ DNS poisoning
	  ○ ARP spoofing
	  ○ Rogue DHCP
	  ○ MAC spoofing
	4.3 Given a scenario, apply network hardening techniques.
	• 4.3.1 Best practices
	  ○ Enable DHCP snooping

Video/Demo	Time
12.6.1 Session and Spoofing Attacks	8:15
12.6.3 Poison ARP	5:44
12.6.5 Poison DNS	6:18
12.6.7 Use SMAC to Spoof MAC Addresses	3:46
12.6.8 Perform a On-Path DHCP Attack	6:57
12.6.10 Detect a Rogue DHCP Server	5:54
12.6.11 Set Up DHCP Snooping	1:45
12.6.13 Respond to Network Attacks	4:24
Total Video Time	**43:03**

Lab/Activity

- 12.6.4 Poison ARP and Analyze with Wireshark
- 12.6.6 Poison DNS
- 12.6.9 Perform an DHCP Spoofing On-Path Attack
- 12.6.12 Configure DHCP Snooping

Fact Sheets

- 12.6.2 Session and Spoofing Attack Facts

Number of Exam Questions
10 questions

Total Time
About 107 minutes

Hardening and Update Management

13.1: Network Hardening

Lecture Focus Questions:

- How does SecureDynamic differ from SecureSticky?
- How does DAI validate ARP packets on the network?
- What are the differences between enforcement and remediation servers?
- How does a port violation occur? How can you resolve it?
- What does DHCP snooping do on your network?

In this section, you will learn to:

- View Windows services
- Disable network services
- View Linux services
- Enable and disable Linux services

The key terms for this section include:

Term	Definition
SecureConfigured address	A MAC address that has been manually identified as an allowed address.
SecureDynamic address	A MAC address that has been dynamically learned and allowed by the switch. SecureDynamic addresses are only saved in the MAC address table in RAM and are not added to the configuration file.
SecureSticky address	A MAC address that is manually configured or dynamically learned and saved.
Port violation	Occurs when the maximum number of MAC addresses has been seen on the port and an unknown MAC address is detected.
Network access protection (NAP)	A collection of components that allow administrators to regulate network access and communication based on a computer's compliance with health requirement policies.
NAP client	A client that has NAP-aware software, either through the operating system or through other components. Client software generates a Statement of Health (SoH) that reports the client configuration for health requirements.
NAP server	The server responsible for keeping track of health requirements and verifying that clients meet those requirements before gaining access. A Windows server running the Network Protection Service role is a NAP server.

Enforcement server (ES)	The connection point for clients into the network (also called an enforcement point). The ES allows or denies network access.
Remediation server	A set of resources that a non-compliant computer can access on a limited-access network.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Network Pro	4.1 Secure firewalls and security appliances • 4.1.3 Configure a screened subnet 4.3 Configure security for a switch • 4.3.2 Enable and disable Linux services

CompTIA Network+	4.3 Given a scenario, apply network hardening techniques.
	• 4.3.1 Best practices
	  ○ Secure SNMP
	  ○ Router Advertisement (RA) Guard
	  ○ Port security
	  ○ Dynamic ARP inspection
	  ○ Control plane policing
	  ○ Private VLANs
	  ○ Disable unneeded switchports
	  ○ Disable unneeded network services
	  ○ Change default passwords
	  ○ Password complexity/length
	  ○ Enable DHCP snooping
	  ○ Change default VLAN
	  ○ Patch and firmware management
	  ○ Access control list
	  ○ Role-based access
	  ○ Firewall rules
	  ▪ Explicit deny
	  ▪ Implicit deny

Video/Demo	Time
13.1.1 Network Hardening Techniques	8:06
13.1.3 View Windows Services	5:15
13.1.5 View Linux Services	4:16
Total Video Time	**17:37**

Lab/Activity

- 13.1.4 Disable Network Service
- 13.1.6 Enable and Disable Linux Services

Fact Sheets

- 13.1.2 Network Hardening Techniques Facts

Number of Exam Questions

10 questions

Total Time

About 57 minutes

13.2: Authentication

Lecture Focus Questions:

- What is the role of a CA in a PKI?
- What is the subject name within a certificate?
- What does an authentication protocol do?
- Which authentication protocol would you choose if you needed to use smart cards?
- What are the two ticket types used with Kerberos? How do tickets make authentication and authorization more efficient?
- Which device is required to implement 802.1X authentication?

The key terms for this section include:

Term	Definition
False negative	A false negative (or Type I error) occurs when a person who should be allowed access is denied access. The false rejection rate (FRR) is a measure of the probability that a false negative will occur.
False positive	A false positive (or Type II error) occurs when a person who should be denied access is allowed access.
Crossover error rate	The crossover error rate, also called the equal error rate, is the point where the number of false positives matches the number of false negatives in a biometric system.
Processing rate	The processing rate, or system throughput, identifies the number of subjects or authentication attempts that can be validated. An acceptable rate is ten subjects per minute or above.
Kerberos	Kerberos is a free protocol that provides strong authentication for client/server applications using a secret-key cryptography. With Kerberos, the client can prove its identity even across an unsecure network connection.
IEEE 802.1X	IEEE 802.1X is a port-based authentication service where the client initiates the authentication, a network device negotiates the authentication, and an authentication server is accessed after the supplicant is authenticated.
Captive portal	A captive portal is a web page that pops up when you access public Wi-Fi. This portal usually summarizes terms disclosing types of activities the Wi-Fi provider is not liable for during public access.
Certificate	A certificate is a digital document that identifies a user or a computer. The certificate includes a subject name, which is the name of the user or the computer.

This section helps you prepare for the following certification exam objectives:

Exam	Objective

CompTIA Network+ N10-008	3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.
	• 3.1.3 Network device logs
	  ○ Log reviews
	  ○ Audit logs
	
	4.1 Explain common security concepts.
	• 4.1.9 Authentication methods
	  ○ Multifactor
	  ○ Single sign-on (SSO)
	  ○ User Service (RADIUS)
	  ○ Kerberos
	  ○ Local authentication
	  ○ 802.1X
	  ○ Extensible Authentication Protocol (EAP
	
	5.5 Given a scenario, troubleshoot general networking issues.
	• 5.5.2 Common issues
	  ○ Certificate issues

Video/Demo	Time
13.2.1 Authentication	10:35
13.2.3 Authentication Protocols	11:13
13.2.4 Authentication Issues	4:15
13.2.5 Digital Certificates	5:26
Total Video Time	**31:29**

Fact Sheets

- 13.2.2 Authentication Facts
- 13.2.6 Authentication Protocol Facts

Number of Exam Questions

10 questions

Total Time

About 52 minutes

13.3: Hardening Authentication

Lecture Focus Questions:

- What defines a complex password?
- What does the minimum password age setting prevent?
- What is a drawback to account lockout for failed password attempts?
- What are the advantages of a self-service password reset management system?

In this section, you will learn to:

- Configure multifactor authentication
- Configure Windows user account restrictions
- Configure account policies and UAC settings
- Configure account password policies
- Configure account password policies
- Manage Linux users
- Change your Linux password
- Change a user's Linux password

The key terms for this section include:

Term	Definition
Multifactor authentication	Using more than one method to authenticate users.

This section helps you prepare for the following certification exam objectives:

Exam	Objective

CompTIA Network+ N10-008	4.1 Explain common security concepts.
	
	• 4.1.9 Authentication methods
	  ○ Multifactor
	  ○ Single sign-on (SSO)
	
	4.3 Given a scenario, apply network hardening techniques.
	
	• 4.3.1 Best practices
	  ○ Change default passwords

Video/Demo	Time
13.3.1 Hardening Authentication	12:05
13.3.2 Configure Multifactor Authentication	3:11
13.3.3 Configure Windows User Account Restrictions	4:21
13.3.4 Configuring Account Policies and UAC Settings	6:07
13.3.6 Manage Linux Users	8:00

Total Video Time **33:44**

Lab/Activity

- 13.3.5 Configure Account Password Policies
- 13.3.8 Change Your Linux Password
- 13.3.9 Change a User's Linux Password

Fact Sheets

- 13.3.7 Linux User Commands and Files Facts

Number of Exam Questions

10 questions

Total Time

About 85 minutes

13.4: Update Management

Lecture Focus Questions:

- What are the benefits of deployment rings?
- What is the difference between quality updates and feature updates?
- What is the Windows Insider Program?

In this section, you will learn to:

- Configure an update server
- Update firmware
- Update deployment and management facts

This section helps you prepare for the following certification exam objectives:

Exam	Objective

CompTIA Network+ N10-008	3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution.
	• 3.3.7 Network device backup/restore
	  ○ State
	  ○ Configuration
	4.3 Given a scenario, apply network hardening techniques.
	• 4.3.1 Best practices
	  ○ Patch and firmware management

Video/Demo	Time
13.4.1 Update Deployment and Management	5:39
13.4.2 Configure an Update Server	7:31
13.4.3 Update Firmware	3:06
Total Video Time	**16:16**

Lab/Activity

- 13.4.4 Update Firmware

Fact Sheets

- 13.4.5 Update Deployment and Management Facts

Number of Exam Questions

10 questions

Total Time

About 44 minutes

Network Optimization and Troubleshooting

14.1: Optimization

Lecture Focus Questions:

- Which feature would you use to configure a device with two connections to the same network?
- What is the purpose of spanning tree in a switched network?
- How does spanning tree compare to Ethernet bonding?
- Why doesn't spanning tree provide improved performance?
- How does a caching server improve network performance?
- When should quality of service (QoS) be a major concern on a network?
- What is the difference between a collision domain and a broadcast domain?
- A network uses hubs as connection devices. What happens to the number of collisions on the network as you add devices?
- Which device provides guaranteed bandwidth between devices?
- Which device can you use to filter broadcast traffic?
- A network uses switches as connection devices. All devices have a dedicated switch port. What happens to the number of collisions on the network as you add devices?

The key terms for this section include:

Term	Definition
NIC teaming	NIC Teaming (also called Ethernet bonding) logically groups two or more physical connections to the same network. Data is divided and sent on multiple interfaces, effectively increasing the speed at which the device can send and receive on the network.
Spanning tree	A protocol on a switch that allows the switch to maintain multiple paths between switches within a subnet. The spanning tree protocol (STP) runs on each switch and is used to select a single path between any two switches.
Load balancing	A process that configures a group of servers in a logical group called a server farm. Incoming requests to the group are distributed to individual members within the group. Incoming requests can be distributed evenly or unevenly between group members based on additional criteria, such as server capacity.
Caching engine	The mechanism used to save previously acquired data for quick retrieval at a later time. Caching stores data in memory or on disk within a network device, where it can quickly be retrieved when needed.

Quality of Service (QoS)	A set of mechanisms that try to guarantee timely delivery or minimal delay of important or time-sensitive communications.
Traffic Shaper	A device that can modify the flow of data through a network in response to network traffic conditions.
Multilayer switch	A multilayer switch, or content switch, that operates at OSI model layers above Layer 2 and can use other information within a packet to make forwarding decisions.
Screened Subnet	A subnetwork placed between the LAN and untrusted networks, such as the internet. External network nodes can access only what you choose to expose in the screened subnet. The rest of the network is protected by firewalls. A screened subnet was previously known as a demilitarized zone (DMZ).
Port Aggregation (PAgP)	A Cisco protocol that lets you combine Ethernet ports to improve the speed of aggregated, or related, file transfers. This protocol is also called link aggregation, teaming ports, and port trunking.
Differentiated Services (Diffserv)	A Layer 3 protocol QoS uses to classify IP packets. Each IP packet header has a DiffServ field. DiffServ inserts a differentiated services code point (DSCP) value in this field to prioritize data flow. Routers forward packets according to the value in this field.
Collision and broadcast domains	A collision domain identifies the devices that share the same network segment and have the potential to send colliding signals. A broadcast domain identifies all the devices that will see a broadcast frame sent on the network. The two work together to minimize collisions.
Common Address Redundancy Protocol (CARP)	A fault tolerance implementation that allows multiple firewalls and/or routers on the same local network to share a set of IP addresses. If one of the firewalls or routers fails, the shared IP address allows hosts to continue communicating with the firewall or router without interruption.
Switch dependent	A type of teaming that requires that the adapters in a team are connected to the same switch.
Switch independent	A type of teaming that allows the adapters in a team to connect to different switches.

This section helps you prepare for the following certification exam objectives:

Exam	Objective

CompTIA Network+ N10-008	2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.
	• 2.1.1 Networking devices
	  ○ Layer 2 switch
	  ○ Layer 3 capable switch
	  ○ Router

- Hub

2.3 Given a scenario, configure and deploy common Ethernet switching features.

- 2.3.7 Carrier-sense multiple access with collision detection (CSMA/CD)

4.2 Compare and contrast common types of attacks.

- 4.2.1 Technology-based
  - On-path attack (previously known as man-in-the-middle attack)

5.5 Given a scenario, troubleshoot general networking issues.

- 5.5.2 Common issues
  - Network performance issues

Video/Demo	Time
14.1.1 Optimization	7:59
14.1.2 Network Segmentation	11:05
Total Video Time	**19:04**

Fact Sheets

14.1.3 Optimization Facts

Number of Exam Questions

10 questions

Total Time

About 35 minutes

14.2: General Network Issues

Lecture Focus Questions:

- What happens when an unauthorized router is added to the network?
- What are some things you can do if the network is experiencing DHCP exhaustion?
- What is the biggest concern when employees use their own laptops on the network?
- What are the symptoms of having an incorrect virtual local area network (VLAN)?

The key terms for this section include:

Term	Definition
Hardware failure	A malfunction within the electronic circuits or electromechanical components (disks or tapes) of a computer system.
Rogue Dynamic Host Configuration Protocol (DHCP)	A Dynamic Host Configuration Protocol (DHCP) server that is not controlled by the network administration or staff.
DHCP exhaustion	A situation in which there are more host requests for IP addresses and related configuration information than the DHCP server can provide. DHCP servers that use IPv4 have a finite set of addresses specific to a single network. The pool of addresses can become exhausted, and the server can no longer provide every machine with an IP address and configuration information.
Untrusted SSL certificate	Certificates that are misconfigured or not stored in a certificate authority list. Untrusted SSL certificates can block connectivity to certain sites. These certificates can be stored on a browser controlled by a server.
Licensed feature	Features that require licenses to be purchased in order to provide the programs and services. If licenses are not set up correctly, the features will not be available for use on the network.
Incorrect VLAN	A VLAN port not configured correctly. This can result in security and connectivity issues on a network.
Optical link budget	An equation that reports communication signal gains and losses on a network. A low optical link budget indicates signal losses on the network that may affect efficiency.

This section helps you prepare for the following certification exam objectives:

Exam	Objective

CompTIA Network+ N10-008

5.1 Explain the network troubleshooting methodology

- 5.1.1 Identify the problem
  - Gather information
  - Question users
  - Identify symptoms
  - Determine if anything has changed
  - Approach multiple problems individually
- 5.1.2 Establish a theory of probably cause
  - Question the obvious
  - Consider multiple approaches
- 5.1.3 Test the theory to determine the cause
  - Determine the next steps to resolve the problem
  - Reestablish a new theory or escalate
- 5.1.4 Establish a plan of action to resolve the problem and identify potential effects
- 5.1.5 Implement the solution or escalate as necessary
- 5.1.6 Verify full system functionality and, if applicable, implement preventive measure
- 5.1.7 Document findings, actions, outcomes, and lessons learned

5.5 Given a scenario, troubleshoot general networking issues.

- 5.5.2 Common Issues
-
  - Hardware failure
  - Rogue DHCP
  - DHCP scope exhaustion
  - DNS Issues
  - BYOD Challenges
  - Certificate issues
  - NTP Issues
  - Licensed feature issues
  - Incorrect VLAN
  - Low optical link budget
  - Network performance issues
  - Blocked services, ports, or addresses
  - Host-based/network-based firewall settings
  - Switching loops
  - Routing loops

Video/Demo	Time
14.2.1 Troubleshooting Methodology	9:47
14.2.3 Common Network Issues	14:07

Total Video Time **23:54**

Fact Sheets

- 14.2.2 Troubleshooting Methodology Facts
- 14.2.4 Common Network Issues Facts

Number of Exam Questions

10 questions

Total Time

About 44 minutes

14.3: Troubleshooting Utilities

Lecture Focus Questions:

- Which command utilities can help you map a network?
- Which command utilities can help you resolve whether there is a network issue or a DNS issue?
- Which commands utilities can help figure out the layout of switches on a network?

In this section, you will learn to:

- Scan the network
- Troubleshoot with Wireshark
- Use tcpdump
- Scan network with Angry IP Scanner

The key terms for this section include:

Tool	Description
ping	A command that is part of the ICMP protocol. It sends a request in the form of a packet to another network device. The packet requests a reply in return, which is also in packet form.
tracert	A command that measures the distance between two devices by the number of other devices it has to pass through in order to get to its destination.
nslookup and dig	Tools that can look up information such as an IP address from a domain server.
ipconfig (Windows)	A command that gives the user the state of the media device on a network and how it is configured.
ifconfig (Linux)	A command that gives the user the state of the media device on a network and how it is configured.
netstat	A command that displays network connections for Transmission Control Protocol (TCP).
Hostname	A unique name for a computer on a network. A computer is discovered on the network using the hostname.
Address Resolution Protocol (ARP)	A communication protocol used for discovering the MAC address associated with an IP address.
Telnet	A network protocol that allows a remote console to access other devices within a network.
SSH	A network protocol similar to Telnet except that it uses encryption to hide certain information, such as user credentials, on the other end of the transmission.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Network Pro	3.3 Manage device discovery and VLANs • 3.3.2 Scan networks 5.1 Troubleshoot configuration and services • 5.1.4 Troubleshoot with a network protocol analyzer

CompTIA Network+ N10-008	5.3 Given scenario, use the appropriate network software tools and commands.
	• 5.3.1 Software tools
	  ○ WiFi analyzer
	  ○ Protocol analyzer/packet capture
	  ○ Bandwidth speed tester
	  ○ Port scanner
	  ○ iperf
	  ○ NetFlow analyzers
	  ○ Trivial File Transfer Protocol (TFTP) server
	  ○ Terminal emulator
	  ○ IP scanner
	• 5.3.2 Command line
	  ○ ping
	  ○ ipconfig/ifconfig/ip
	  ○ nslookup/dig
	  ○ traceroute/tracert
	  ○ arp
	  ○ netstat
	  ○ hostname
	  ○ route
	  ○ telnet
	  ○ tcpdump
	  ○ nmap

Video/Demo	Time
14.3.1 Command Line Troubleshooting Utilities	12:01
14.3.3 Use TCPDump	5:42
14.3.5 Software Troubleshooting Utilities	8:14
14.3.7 Troubleshoot with Wireshark	7:53
14.3.8 Use Wireshark to Troubleshoot Network Issues	4:24
14.3.11 Scan Network with Angry IP Scanner	4:07

14.3.12 Scan Network with Zenmap	3:24
Total Video Time	**45:45**

Lab/Activity

- 14.3.9 Troubleshoot with Wireshark

Fact Sheets

- 14.3.2 Command Line Troubleshooting Utility Facts
- 14.3.4 TCPDump Facts
- 14.3.6 Software Troubleshooting Utilities Facts
- 14.3.10 Wireshark Facts

Number of Exam Questions

10 questions

Total Time

About 88 minutes

Practice Exams

A.0: TestOut Network Pro - Practice Exams

TestOut Network Pro Certification Practice Exam (20 questions)

B.0: CompTIA Network+ N10-008 Practice Exams

CompTIA Network+ N10-008 Certification Practice Exam (90 questions)

Appendix A: Approximate Time for the Course

The total time for the LabSim for TestOut Network Pro course is approximately **72 hours and 45 minutes**. Time is calculated by adding the approximate time for each section which is calculated using the following elements:

- Video/demo times
- Text Lessons (5 minutes assigned per text lesson)
- Simulations (12 minutes assigned per simulation)
- Questions (1 minute per question)

Additionally, there are approximately another **45 hours and 9 minutes** of Practice Test material at the end of the course.

The breakdown for this course is as follows:

Module Sections	Time	Videos	Labs	Text	Exams
1.0: Introduction					
1.1: Network Pro Introduction	5	5	0	0	0
1.2: Use the Simulator	39	15	24	0	0
Total (hh:mm)	**0:44**	**0:20**	**0:24**	**0:00**	**0:00**
2.0: Networking Basics					
2.1: Networking Overview	51	31	0	10	10
2.2: OSI Model and Data Encapsulation	35	15	0	10	10
2.3: Data Encapsulation	45	20	0	15	10
2.4: Network Protocols	43	23	0	10	10
Total (hh:mm)	**2:54**	**1:29**	**0:00**	**0:45**	**0:40**
3.0: Network Cabling and Hardware Devices					
3.1: Copper Cables and Connectors	61	17	24	10	10
3.2: Fiber Optic Cables and Connectors	38	11	12	5	10
3.3: Wiring Implementation	64	20	24	10	10
3.4: Troubleshoot Network Media	53	28	0	15	10
3.5: Network Adapters	48	9	24	5	10
3.6: Networking Devices	86	25	36	15	10
Total (hh:mm)	**5:50**	**1:50**	**2:00**	**1:00**	**1:00**
4.0: Network Addressing and Services					
4.1: IP Addressing	100	46	24	20	10
4.2: APIPA and Alternate Addressing	35	8	12	5	10
4.3: DHCP	98	35	48	5	10
4.4: DHCP Relay	50	11	24	5	10
4.5: DNS	106	31	60	5	10
4.6: NTP	41	14	12	5	10
4.7: IP Version 6	70	33	12	15	10
4.8: Multicast	24	9	0	5	10

4.9: Troubleshoot IP Configuration Issues		84	21	48	5	10
4.10: Troubleshoot IP Communications		61	29	12	10	10
4.11: Troubleshoot DNS		53	26	12	5	10
	Total (hh:mm)	**12:02**	**4:23**	**4:24**	**1:25**	**1:50**
5.0: Ethernet						
5.1: Ethernet		47	15	12	10	10
5.2: Connect Network Devices		35	8	12	5	10
5.3: Troubleshoot Physical Connectivity		103	11	72	10	10
	Total (hh:mm)	**3:05**	**0:34**	**1:36**	**0:25**	**0:30**
6.0: Firewalls and Intrusion Detection						
6.1: Firewalls		57	25	12	10	10
6.2: Firewall Design and Implementation		94	38	36	10	10
6.3: Screened Subnets (DMZ)		35	8	12	5	10
6.4: Intrusion Detection and Prevention		38	11	12	5	10
	Total (hh:mm)	**3:44**	**1:22**	**1:12**	**0:30**	**0:40**
7.0: Switching and Routing						
7.1: Switching		54	27	12	5	10
7.2: Basic Switch Configuration		92	24	48	10	10
7.3: Switch Ports		114	34	60	10	10
7.4: Switch Security		101	33	48	10	10
7.5: Routing		91	49	12	20	10
7.6: Network Address Translation		47	20	12	5	10
7.7: Switching and Routing Troubleshooting		35	21	0	5	9
	Total (hh:mm)	**8:54**	**3:28**	**3:12**	**1:05**	**1:09**
8.0: Specialized Networks						
8.1: Corporate and Datacenter Networks		70	26	24	10	10
8.2: Voice over IP (VoIP)		64	25	24	5	10
8.3: Virtualization		32	17	0	5	10
8.4: Virtual Networking		36	16	0	10	10
8.5: Cloud Concepts and Connectivity		44	19	0	15	10
8.6: Internet of Things (IoT)		69	30	24	5	10
	Total (hh:mm)	**5:15**	**2:13**	**1:12**	**0:50**	**1:00**
9.0: Wireless Networking						
9.1: Wireless Concepts and Standards		58	33	0	15	10
9.2: Wireless Configuration		74	23	36	5	10
9.3: Wireless Network Design		68	24	24	10	10
9.4: Wireless Network Implementation		42	15	12	5	10
9.5: Wireless Security		125	45	60	10	10
9.6: Wireless Troubleshooting		85	34	36	5	10
	Total (hh:mm)	**7:32**	**2:54**	**2:48**	**0:50**	**1:00**
10.0: Wide Area Networks (WANs)						
10.1: WAN Concepts		27	12	0	5	10
10.2: Internet Connectivity		53	26	12	5	10
10.3: Remote Access		23	8	0	5	10
10.4: Virtual Private Networks		65	21	24	10	10
	Total (hh:mm)	**2:48**	**1:07**	**0:36**	**0:25**	**0:40**
11.0: Network Operations and Management						

11.1: Performance Metrics		21	6	0	5	10
11.2: Network Management with SNMP		31	16	0	5	10
11.3: Log File Management		66	27	24	5	10
11.4: Monitoring		68	48	0	10	10
11.5: Organization Policies		44	19	0	15	10
11.6: Redundancy and High Availability		91	54	12	15	10
11.7: Data Backup and Storage		70	31	24	5	10
11.8: Remote Management		45	18	12	5	10
	Total (hh:mm)	**7:16**	**3:39**	**1:12**	**1:05**	**1:20**
12.0: Network Security						
12.1: Security Concepts		69	44	0	15	10
12.2: Risk Management		53	23	0	20	10
12.3: Physical Security		36	9	12	5	10
12.4: Social Engineering		48	21	12	5	10
12.5: Network Threats and Attacks		81	43	12	15	11
12.6: Spoofing Attacks		107	44	48	5	10
	Total (hh:mm)	**6:34**	**3:04**	**1:24**	**1:05**	**1:01**
13.0: Hardening and Update Management						
13.1: Network Hardening		57	18	24	5	10
13.2: Authentication		52	32	0	10	10
13.3: Hardening Authentication		85	34	36	5	10
13.4: Update Management		44	17	12	5	10
	Total (hh:mm)	**3:58**	**1:41**	**1:12**	**0:25**	**0:40**
14.0: Network Optimization and Troubleshooting						
14.1: Optimization		35	20	0	5	10
14.2: General Network Issues		44	24	0	10	10
14.3: Troubleshooting Utilities		88	46	12	20	10
	Total (hh:mm)	**2:47**	**1:30**	**0:12**	**0:35**	**0:30**
Total Course Time 72:45 (hh:mm)						

Practice Exams

A.0: TestOut Network Pro - Practice Exams	**Number of Questions**	**Time (hh:mm)**
A.2: TestOut Network Pro Domain Review Questions	107	21:24
A.3: TestOut Network Pro Certification Practice Exam	20	1:20
Total	**127**	**22:44**

B.0: CompTIA Network+ N10-008 Practice Exams	**Number of Questions**	**Time (hh:mm)**
B.2: CompTIA Network+ N10-008 Domain Review Questions	100	1:40
B.3: CompTIA Network+ N10-008 Practice Exam Questions (All)	1,155	19:15
B.4: CompTIA Network+ N10-008 Certification Practice Exam	90	1:30
Total	**1,345**	**22:25**

Total Practice Exam Time 45:09 (hh:mm)