TestOut

Lesson Plans

Network+

(Exam N10-004)

Version 3.0

The lessons only experience can teach

Table of Contents

Course Overview

This course prepares students for CompTIA's Network+ Exam: N10-004. It focuses on configuring, managing and troubleshooting the elements of a basic network infrastructure.

Module 0 – Introduction

This module introduces the course, prerequisites and required skills for the exam. Students will also learn how to use the hardware simulator so they can complete the simulations as they proceed through the course.

Module 1 – Networking Basics

This module lays the foundation of the basics of networking. This includes information on networking terminology, common physical and logical topologies, networking architectures and protocols, network connections, and the Open Systems Interconnection (OSI) model.

Module 2 – Cables and Connectors

This module examines common cables and connectors used in networks. Twisted pair, coaxial and fiber optic cabling are discussed. Students will become familiar with the standards, specifications, and components used for wiring implementation.

Module 3 – Networking Devices

In this module students will learn about using network adapters and devices to connect to a network. They will also learn about internetworking devices (routers, firewalls, and layer3 switches).

Module 4 – Ethernet

This module teaches the students the basics of working with Ethernet architecture, specifications, and details about connecting network devices.

Module 5– Network Implementation

This module discusses aspects of a network implementation. This includes understanding IP addressing, assigning IP addresses, mapping logical host names to IP addresses, routing, and accessing the Internet,. Students will learn why IPv6 is necessary and how multicasting works. They will also learn the basics of using Voice over IP (VoIP).

Module 6 – Wireless Networking

This module examines using a radio frequency wireless network to connect to hosts. Students will learn the basics of networking architecture, infrastructure, and wireless standards (802.11, Infrared, and Bluetooth). They will learn how to implement security on a wireless network, configure a wireless network, and identify factors that can effect a wireless connection.

Module 7 – Wide Area Networks (WANs)

In this module students will learn facts about Wide Area Networks (WAN) technologies, structure, and services. They will learn methods to connect to the Internet through an ISP and how to create a remote access connection.

Module 8 – Network Security

This module teaches the students how to secure the network from various network threats. Students will learn how to use a firewall, a Virtual Private Network (VPN), and switch features to enhance security. They will also learn about the elements that can be used to provide authentication and encryption for the network. An Intrusion Detection System (IDS) and network monitoring tools are used to help prevent attacks.

Module 9 – Network Management

This module examines components of network management. This includes configuration management documentation, SNMP, remote management, network monitoring tools, and elements to optimize the performance of the network.

Module 10 – Troubleshooting

In this module students will learn a systematic methodology for troubleshooting, tools to troubleshoot network connectivity problems, and commands to gather network information and troubleshoot IP configuration problems. They will also learn how to troubleshoot name resolution, switching and routing problems.

Practice Exams

In Practice Exams students will have the opportunity to test themselves and verify that they understand the concepts and are ready to take the certification exam.

Section 0.1: Course Introduction

Summary

This section discusses the Network+ certification. The Network+ certification is a vendor neutral with a broad based knowledge base. The purpose of Network + certification is to validate and demonstrate that the recipient has the required networking skills and experience to manage a basic network infrastructure. The Network+ certification is valuable in the workplace and also may provide college credits at many colleges and universities.

The Network+ certification exam consists of one exam and is considered a stepping stone in your student's career path. Many other vendor-specific certifications require Network+ certification (or its equivalent) as a foundation.

Recommended prerequisites include:

- CompTIA A+ certification or equivalent knowledge and experience
- About 9 months of hands-on experience

Students should have the following skills before studying for the Network+ certification:

- Knowledge of PC hardware installation and configuration
- Knowledge of using and administering a Windows client computer

Time

About 5 minutes

Section 0.2: Using the Hardware Simulator

Summary

This section teaches the students how to use the hardware simulator included in this course. Experiment with the simulations in this section until you are familiar with how the hardware simulator works. You will recognize the simulations in this course by the mouse icon to the left of the entry.

Students will learn how to:

- Read simulated component documentation and view components to make appropriate choices to meet the scenario.
- Add simulated computer components to the work bench.
- Add and remove simulated computer components.
- Change views to view and add simulated components.
- Use the zoom feature to view additional image details.
- Attach simulated cables.
- Use the simulation interface to identify where simulated cables connect to the computer.

Time

About 40 minutes

Lab/Activity

- Put an Item on the Workbench
- Select an Item Based on Its Documentation
- Select Item Categories
- Install and Uninstall Components
- Set Dials and Switches
- Add Cabled Components

Section 1.1: Networking Overview

Summary

This section provides an introduction to networking. Students will become familiar with the following aspects of a network:

- Components of a network
  - Computers
  - Transmission media
  - Network interfaces
  - Protocols
- Money saving capabilities of a network
- Host roles
  - Peer-to-peer
  - Client/server
- Geography and size
  - Local Area Network (LAN)
  - Wide Area Network (WAN)
- Management
  - Network
  - Subnet
  - Internetwork
- Participation
  - Internet
  - Intranet
  - Extranet

Network+ Objectives

- 2.7 Explain common logical network topologies and their characteristics
  - Peer to peer
  - Client/server

Lecture Focus Questions:

- Why are *protocols* important for networking?
- What are the advantages of a client/server network when compared to a peer-to-peer network?
- What is the main characteristic of a *subnet*? How can you tell one subnet from another?
- How does an *intranet* differ from the Internet?
- What is the main purpose of an *extranet*?

Time

About 40 minutes

Number of Exam Questions
2 questions

Section 1.2: Network Topologies

Summary

This section discusses network topologies; how devices are connected and how messages flow from device to device. Two types of network topologies are discussed:

- Physical topologies identify the physical way the network is wired.
- Logical topologies identify the way in which messages are sent.

Network+ Objectives

- 2.3 Identify common physical network topologies
  - Star
  - Mesh
  - Bus
  - Ring
  - Hybrid

Lecture Focus Questions:

- 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 the physical mesh topology normally an impractical solution?
- What are the advantages of a logical star topology over the logical bus topology?
- Why is termination important on a physical bus topology?
- How do hosts on a physical ring topology communicate?

Time

About 25 minutes

Number of Exam Questions

10 questions

Section 1.3: Protocols

Summary

This section explores typical network architectures and the TCP/IP protocol suite. Students will become familiar with the common networking protocols used for:

- Web browsing
- Security protocols
- File transfer
- E-mail
- Network services
- Network management
- Transport protocols
- Control protocols

Network+ Objectives

- 1.1 Explain the function of common networking protocols
  - TCP
  - FTP
  - UDP
  - TCP/IP suite
  - DHCP
  - TFTP
  - DNS
  - HTTP(S)
  - ARP
  - SSH
  - POP3
  - NTP
  - IMAP4
  - Telnet
  - SMTP
  - SNMP2/3
  - ICMP
  - IGMP
  - TLS

Time

Lecture Focus Questions:

- Which architecture type is the most common architecture for a local area network?
- Which architecture types use digital signals over regular telephone lines?

- What is the transmission medium used for wireless networks?
- How does a protocol suite differ from a protocol?
- How does TCP differ from UDP?
- What is the difference between the three e-mail protocols: IMAP4, POP3, and SMTP?
- How does SSH differ from Telnet? How does HTTPS differ from HTTP?

Time

About 35 minutes

Number of Exam Questions

8 questions

Section 1.4: Network Connections

Summary

This section discusses the configuration settings required to connect to a TCP/IP network. Parameters include the:

- IP address
- Subnet mask
- Default gateway
- DNS server
- Host name

Students will learn how to:

- View the status of network connections.
- Configure basic IP configuration values necessary to connect to the Internet.

Network+ Objectives

- 1.3 Identify the following address formats
  - IPv4

Lecture Focus Questions:

- What two pieces of information is contained within an IP address? How does a computer tell the difference between these two parts?
- When assigning IP addresses to hosts, which portions of the configuration must match values used by other hosts in the same subnet?
- A router has two network interfaces, each connected to a different subnet. When configuring the default gateway value on a host, which IP address would you use?
- What capability does the DNS server address provide? What would happen if the computer was not configured to use a DNS server?

Time

About 25 minutes

Lab/Activity

- Configure TCP/IP Settings

Section 1.5: The OSI Model

Summary

In this section students will learn about the Open Systems Interconnection (OSI) model; a theoretical model that defines standards for programmers and network administrators.

Students will become familiar with the:

- Advantages of using the OSI model to discuss networking concepts.
- Limitations of the OSI model.
- Names of the 7 layers of the OSI model.
- Functions performed at each OSI model layer.

Network+ Objectives

- 1.1 Explain the function of common networking protocols
  - TCP
  - UDP
- 4.1 Explain the function of each layer of the OSI model
  - Layer 1 -- physical
  - Layer 2 -- data link
  - Layer 3 -- network
  - Layer 4 -- transport
  - Layer 5 -- session
  - Layer 6 -- presentation
  - Layer 7 -- application

Lecture Focus Questions:

- What is the OSI model and why is it important in 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?
- At which OSI model layer would you find a *frame*?
- What is the difference between connectionless and connection-oriented services?

Time

About 40 minutes

Number of Exam Questions

13 questions

Section 2.1: Twisted Pair

Summary

This section examines the basics of twisted pair cabling. Concepts discussed include the:

- Components of a twisted pair cable.
- Unshielded twisted pair (UTP) cable types (categories).
- Substitution rule for UTP cable.
- Connectors used with twisted pair cables.

Students will learn how to:

- Select and install cables for connecting to a dial-up network.
- Select and install cables for connecting to an Ethernet network.

Network+ Objectives

- 2.1 Categorize standard cable types and their properties
    - Type:
        - CAT3, CAT5, CAT5e, CAT6
        - STP, UTP
        - Plenum vs. Non-plenum
    - Properties:
        - Transmission speeds
        - Noise immunity (security, EMI)
- 2.2 Identify common connector types
    - RJ-11
    - RJ-45

Lecture Focus Questions:

- Why are wires twisted together in twisted pair cables?
- What is the difference between STP and UTP cabling?
- What is the difference between Cat3 and Cat5 cable?
- How can you tell the difference between an RJ-11 and an RJ-45 connector?
- You have an installation that requires Cat5 cable. Which cable ratings could you use for the installation?

Time

About 25 minutes

Lab/Activity

- Connect a Modem
- Connect to an Ethernet Network

Number of Exam Questions

5 questions

Section 2.2: Coaxial

Summary

This section provides the fundamentals of using coaxial cabling. Students will become familiar with the:

- Components of a coaxial cable.
- Advantages and disadvantages of a coaxial cable.
- Common coaxial cable grades.
- Selection of coaxial cables being determined by the resistance (impedance) rating.
- Connector types used with coaxial cable.

Students will learn how to:

- Select and install components to connect to a cable network.

Network+ Objectives

- 2.1 Categorize standard cable types and their properties
  - Type:
    - Coaxial
      - RG-59
      - RG-6
  - Properties:
    - Noise immunity (security, EMI)
- 2.2 Identify common connector types
  - BNC
  - RG-59
  - RG-6

Lecture Focus Questions:

- What is the function of the wire mesh in coaxial cables?
- Which part of the cable is used to carry data?
- Which connector type and cable grade is used to connect a cable modem to the Internet connection?
- Which cable type is more immune to EMI, twisted pair or coaxial?

Time

About 20 minutes

Lab/Activity

- Connect a Cable Modem

Number of Exam Questions
6 questions

Section 2.3: Fiber Optic

Summary

This section discusses facts about fiber optic cabling. Concepts discussed include the:

- Components of a fiber optic cable.
- Advantages and disadvantages of fiber optic cabling.
- Multi-mode and single mode fiber cables.
- Connectors used with fiber optic cables.
- Installation of fiber optic cables and connectors.

Students will learn how to:

- Select and install components to connect to a network that uses fiber-optic.

Network+ Objectives

- 2.1 Categorize standard cable types and their properties
  - Type:
    - Multimode fiber, single-mode fiber
  - Properties:
    - Transmission speeds
    - Distance
    - Noise immunity (security, EMI)
- 2.2 Identify common connector types
  - SC
  - ST
  - LC

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 or other media choices? What are the disadvantages to implementing fiber optic cables?
- What is the difference between single mode and multi-mode cables?
- How can you tell the difference between an ST and an SC connector?
- Which connector types combine two strands of fiber into a single connector?

Time

About 30 minutes

Lab/Activity

- Connect Fiber Optic Cables 1

- Connect Fiber Optic Cables 2

Number of Exam Questions
8 questions

Section 2.4: Wiring Implementation

Summary

This section presents information about implementing the wiring to connect computers in a network. Facts discussed about making and distributing cables for a network include:

- Standards for creating a straight-through cable configuration.
- Standards for creating crossover cable configurations.
- Ethernet pin specifications for Ethernet cables.
- Installation and purchase of Ethernet cables and connectors.
- Components used for wiring distribution for data and telephone wiring.

.Students will learn how to:

- Use the appropriate tools to create Cat5 drop cables.
- Use the appropriate tools to connect cables using punchdown blocks.

Network+ Objectives

- 2.4 Given a scenario, differentiate and implement appropriate wiring standards
  - 568A
  - 568B
  - Straight vs. cross-over
- 2.8 Install components of wiring distribution
  - Vertical and horizontal cross connects
  - Patch panels
  - 66 block
  - MDFs
  - IDFs
  - 25 pair
  - 100 pair
  - 110 block
  - Demarc
  - Demarc extension
- 5.3 Given a scenario, utilize the appropriate hardware tools
  - Cable testers
  - Punch down tool
  - Cable stripper
  - Snips

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 using a punchdown tool, which way should the blade be facing?

Time

About 60 minutes

Number of Exam Questions

15 questions

Section 3.1: Network Adapters

Summary

This section examines using a network adapter (network interface card or NIC) to connect a host to the network medium. Students will become familiar with the function of:

- A transceiver
- A modem
- A media converter
- The MAC address
- The Address Resolution Protocol (ARP)
- The Reverse Address Resolution Protocol (RARP)
- The Cyclic Redundancy Check (CRC)

Students will learn how to:

- Select and install network cards to meet network connection requirements.

Network+ Objectives

- 1.1 Explain the function of common networking protocols
  - ARP
- 1.3 Identify the following address formats
  - MAC addressing
- 3.1 Install, configure and differentiate between common network devices
  - Modem
  - NIC
  - Media converters

Lecture Focus Questions:

- What are two major differences between a modem and an Ethernet NIC?
- How can you identify a network card manufacturer from the MAC address?
- What is the function of a transceiver?
- What is the purpose of the CRC?
- At which OSI layer does a network adapter card operate? At which layer does a media converter work?
- Can a media converter be used to connect network segments using 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?

Time

About 35 minutes

Lab/Activity

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

Number of Exam Questions

10 questions

Section 3.2: Network Devices

Summary

In this section students will explore information about common connection devices used within a LAN. This includes information about a:

- Hub
- Bridge
- Switch
- Wireless Access Point (WAP)

Students will learn how to:

- Select and install appropriate networking hardware.

Network+ Objectives

- 3.1 Install, configure and differentiate between common network devices
  - Hub
  - Repeater
  - Basic switch
  - Bridge
  - Wireless access point

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 to using switches over 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?

Time

About 35 minutes

Lab/Activity

- Select a Networking Device

Number of Exam Questions
9 questions

Section 3.3: Internetwork Devices

Summary

This section discusses common internetworking devices. This includes facts about the function of a:

- Router
- Firewall
- Layer 3 switch

Students will become familiar with the process routers use to route packets from one host to another on a different network. They will also learn about the function of:

- Data Link physical addresses
- Network logical addresses

Students will learn how to:

- Select the appropriate device to connect two networks.

Network+ Objectives

- 1.6 Explain the purpose and properties of routing
  - Next hop
  - Understanding routing tables and how they pertain to path selection
- 3.1 Install, configure and differentiate between common network devices
  - Basic router
  - Basic firewall
- 3.2 Identify the functions of specialized network devices
  - Multilayer switch

Lecture Focus Questions:

- What is the main role of a router?
- How does a router differ from a switch or a hub?
- How are the physical and logical (network) addresses used when routing data through an internetwork? Which addresses stay the same? Which addresses change from hop to hop?
- How does a firewall protect a network?

Time

About 25 minutes

Lab/Activity

- Select a Router

Number of Exam Questions

8 questions

Section 4.1: Ethernet

Summary

This section examines facts about Ethernet architecture. The following details about Ethernet are discussed:

- Topology
- Networking devices
- Transmission media
- Media access Method
- Physical addresses
- Frames

Network+ Objectives

- 2.6 Categorize LAN technology types and properties
    - Properties
        - CSMA/CD
        - Collision

Lecture Focus Questions:

- What logical topologies are supported on an Ethernet network?
- What is the purpose of the *backoff* on Ethernet networks?
- How can you eliminate collisions on an Ethernet network?
- What device do you use to enable full-duplex communications with Ethernet?

Time

About 24 minutes

Number of Exam Questions

3 questions

Section 4.2: Ethernet Specifications

Summary

This section discusses Ethernet specifications of various Ethernet implementations. Students will compare the standards and characteristics of various Ethernet categories:

- Ethernet
- Fast Ethernet
- Gigabit Ethernet
- 10 Gigabit Ethernet

Students will learn to:

- Select and install Ethernet NICs based on speed and transmission medium.
- Install UTP and fiber optic cables.

Network+ Objectives

- 2.6 Categorize LAN technology types and properties
  - Types:
    - Ethernet
    - 10BaseT
    - 100BaseTX
    - 100BaseFX
    - 1000BaseT
    - 1000BaseX
    - 10GBaseSR
    - 10GBaseLR
    - 10GBaseER
    - 10GBaseSW
    - 10GBaseLW
    - 10GBaseEW
    - 10GBaseT
  - Properties
    - Speed
    - Distance

Lecture Focus Questions:

- What is the maximum cable length for most Ethernet standards that use twisted pair cables?
- Which twisted pair cable category should you use on a 1000BaseT network?
- What is the advantage of using single mode cable on a 1000BaseLX network?
- What is the difference between 10GBaseSR and 10GBaseSW?

Time
About 45 minutes

Lab/Activity

- Connect to a 100BaseTX Network
- Select Ethernet Cable
- Connect a Fiber Optic Network

Number of Exam Questions
13 questions

Section 4.3: Connecting Network Devices

Summary

This section examines facts about connecting network devices. Students will become familiar with cable types to use in various connection scenarios:

- Straight-through cable
- Crossover cable
- Rollover cable

They will also learn general rules and details about connecting network devices such as:

- When to select a crossover cable
- When to select a straight-through cable
- Differentiating between a crossover and a straight-through cable.
- Implementing an uplink port
- Implementing hubs and switches with Auto-MDI/MDIX

Students will learn how to:

- Select the correct cable type when connecting devices together.

Network+ Objectives

- 2.1 Categorize standard cable types and their properties
  - Type:
    - Serial
- 2.2 Identify common connector types
  - RS-232
- 2.4 Given a scenario, differentiate and implement appropriate wiring standards
  - 568A
  - 568B
  - Straight vs. cross-over
  - Rollover

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?

Time
About 30 minutes

Lab/Activity

- Connect Network Devices

Number of Exam Questions
8 questions

Section 5.1: IP Addressing

Summary

In this section students will learn facts about IP addressing and subnetting. Details will include:

- Representing IP addresses in a decimal or a binary notation
- Converting binary numbers to decimal numbers
- Using a subnet mask to identify the network portion of the address
- Using default address classes to identify the range of IP addresses
- Implementing IP addresses to hosts
- Implementing IP addresses on the Internet
- Creating subnets to divide a larger network into smaller networks
- Implementing custom subnet masks
- Comparing default and custom subnet mask descriptions
- Implementing classful addresses vs. classless addresses

Network+ Objectives

- 1.3 Identify the following address formats
  - IPv4
- 1.4 Given a scenario, evaluate the proper use of the following addressing technologies and addressing schemes
  - Addressing Technologies
    - Subnetting
    - Classful vs. classless (e.g. CIDR, Supernetting)

Lecture Focus Questions:

- What is an *octet*?
- What is the decimal equivalent for the following binary number: 01100111? What is the binary equivalent of the following decimal number: 211?
- How is the network portion of an IP address identified?
- Which portion of a class C address designates the network address?
- What is the difference between *subnetting* and *supernetting*? Which method uses a subnet mask that is *longer* than the default subnet mask?
- What does the **/14** mean in the following IP address: 199.78.11.12/**14**?

Time

About 60 minutes

Lab/Activity

- Configure IP Addresses

Number of Exam Questions
13 questions

Section 5.2: Address Assignment

Summary

This section discusses assigning IP addresses. The following concepts are covered:

- Dynamic Host Configuration Protocol (DHCP)
- Automatic Private IP Addressing (APIPA)
- Alternate IP configuration
- Static (manual assignment

Students will learn how to:

- Configure a DHCP server to deliver IP configuration information.
- Configure a host to use DHCP for IP configuration.
- Configure an alternate IP configuration.

Network+ Objectives

- 1.1 Explain the function of common networking protocols
  - DHCP
- 1.4 Given a scenario, evaluate the proper use of the following addressing technologies and addressing schemes
  - Addressing Technologies
    - DHCP (static, dynamic, APIPA)
- 3.1 Install, configure and differentiate between common network devices
  - Basic DHCP server

Lecture Focus Questions:

- What type of configuration parameters can be delivered using DHCP?
- How do you know if a host is using an APIPA address?
- Which IP configuration parameters are set when APIPA are used? Which ones are not set?
- What are the advantages of static IP address assignments?
- When might you want to use static IP addressing?
- In which scenarios would an alternate IP configuration simplify IP configuration?

Time

About 40 minutes

Lab/Activity

- Configure a DHCP Client

Number of Exam Questions
5 questions

Section 5.3: Name Resolution

Summary

This section provides information about using name resolution to map logical host names to IP addresses. Concepts covered include:

- Components of a Domain Name System (DNS) hierarchy
- Elements of a fully-qualified domain name (FQDN)
- Steps to finding the IP address from a computer host name

Students will learn facts about the function of:

- Forward lookup
- Reverse lookup
- Authoritative server
- Zone files
    - A records
    - PTR (pointer) records
- Recursion
- Root DNS servers
- HOSTS file

Students will learn how to:

- Configure DNS zones and records to identify individual hosts.
- Configure preferred and alternate DNS server addresses on a Windows host.

Network+ Objectives

- 1.1 Explain the function of common networking protocols
    - DNS
- 3.2 Identify the functions of specialized network devices
    - DNS server

Lecture Focus Questions:

- How are host names organized in DNS?
- What is the difference between a forward lookup and a reverse lookup?
- What is the role of the root servers in DNS?
- What is the difference between a zone and a domain in DNS?
- What is the difference between an A record and a PTR record?

Time
About 30 minutes

Lab/Activity

- Configure DNS Addresses

Number of Exam Questions
2 questions

Section 5.4: Routing

Summary

In this section students will learn the basics of using routers to send packets from one network to another. Routing facts that are discussed include:

- The purpose of a router
- The information stored in a routing table
- Static routing vs. dynamic routing
- Managing routing tables
- Convergence of routing information

Routing protocol characteristics discussed include:

- Scope
- Metric
- Routing update method
- Classful or classless

Specific routing protocols presented include:

- Routing Information Protocol (RIP)
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Open Shortest Path First (OSPF)
- Intermediate System to Intermediate System (IS-IS)
- Border Gateway Protocol (BGP)

Students will learn how to:

- Configure a router with static routes
- Configure a router for dynamic routing.

Network+ Objectives

- 1.5 Identify common IPv4 and IPv6 routing protocols
    - Link state
        - OSPF
        - IS-IS
    - Distance vector
        - RIP
        - RIPv2
        - BGP
    - Hybrid

        - EIGRP
- 1.6 Explain the purpose and properties of routing
    - IGP vs. EGP
    - Static vs. dynamic
    - Next hop
    - Understanding routing tables and how they pertain to path selection
    - Explain convergence (steady state)

Lecture Focus Questions:

- When would you configure both static and dynamic routing on the same router?
- Which type of route is preferred, one with a higher metric or one with a lower metric?
- Why is the hop count sometimes an unreliable metric for choosing the best path to a destination network?
- What is the state of routing tables before convergence is reached? Why might this cause communication problems in a network?
- How does the link state method differ from the distance vector method?
- What is the difference between RIP and RIPv2? Why is this important in today's networks?
- Which routing protocol is typically used within an ISP? Which protocol is used on the Internet?
- Which routing protocol(s) divide an autonomous system into areas?
- How does IS-IS differ from OSPF?

Time

About 70 minutes

Number of Exam Questions

13 questions

Section 5.5: NAT and ICS

Summary

This section covers using Network Address Translation (NAT) and Internet Connection Sharing (ICS) to access the Internet. The following concepts are covered:

- The role of NAT
- The role of Port Address Translation (PAT)
- The role of a NAT router
- Implementations of NAT
    - Dynamic NAT
    - Static NAT (SNAT)
    - Dynamic and Static NAT
- The role of private IPv4 address ranges
- The configuration tasks when using ICS

Students will learn how to:

- Implement network address translation (NAT).
- Configure Internet connection sharing (ICS).

Network+ Objectives

- 1.4 Given a scenario, evaluate the proper use of the following addressing technologies and addressing schemes
    - Addressing Technologies
        - NAT
        - PAT
        - SNAT
        - Public vs. private

Lecture Focus Questions:

- What are two advantages to using NAT?
- What is the difference between static NAT and dynamic NAT?
- What is the relationship between NAT and ICS?
- When you configure ICS, what IP address is assigned to the network interface to the private network?
- What default gateway and DNS server addresses are automatically delivered by the ICS computer to hosts on the private network?

Time

About 35 minutes

Lab/Activity

- Share an Internet Connection

Number of Exam Questions

8 questions

Section 5.6: IP version 6

Summary

This section discusses facts about IP version 6. The following concepts are discussed:

- Address formatting conventions for an IPv6 address
- Components of a 128-bit address
  - Prefix
  - Interface ID
- Features added to IPv6 not available in IPv4
- Recommended strategies for IPv6 to IPv4 compatibility
  - Dual Stack
  - Tunneling
  - Network Address Translation-Protocol Translation (NAT-PT)

Network+ Objectives

- 1.3 Identify the following address formats
  - IPv6

Lecture Focus Questions:

- What is the primary reason for developing IPv6?
- How many hexadecimal numbers are in an IPv6 address? How does this compare to a MAC address?
- What do you add to an IPv6 address when you remove one or more quartets with all 0's?
- What information is included within the IPv6 address *prefix*?
- How many numbers are used for the interface ID? How can the interface ID be related to the MAC address?
- What is the difference between ISATAP and 6-to-4 tunneling?
- What is the difference between tunneling and NAT-PT?

Time

About 20 minutes

Number of Exam Questions

2 questions

Section 5.7: Multicast

Summary

In this section students will learn how creating a multicast group allows messages to be received by all group members. Students will learn about the following addressing schemes:

- Multicasting
- Unicasting
- Broadcasting

Additional concepts discussed are:

- The function of the Internet Group Management Protocol (IGMP)
- The process used when sending a multicast stream
- Details about membership of groups
- Specifics about a multicast IP address
- A router's response to multicast traffic
- A switch's response to multicast traffic

Network+ Objectives

- 1.1 Explain the function of common networking protocols
  - IGMP
- 1.4 Given a scenario, evaluate the proper use of the following addressing technologies and addressing schemes
  - Addressing schemes
    - Unicast
    - Multicast

Lecture Focus Questions:

- How does multicast differ from unicast or 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?

Time

About 15 minutes

Number of Exam Questions

5 questions

Section 5.8: Voice over IP (VoIP)

Summary

This section provides the basics of using Voice over IP (VoIP) to provide telephone calls through a packet switched network such as the Internet. Students will learn:

- How to obtain VoIP services
- How VoIP uses IP datagrams to send voice data over a network
- The advantages of using an IP network for voice transmission
- Possible problems with VoIP
  - Delay (latency)
  - Jitter
  - Packet loss
  - Echo
  - Power loss
- Implementation of Quality of Service (QoS) measures to reduce the negative effects of using an IP network

Network+ Objectives

- 1.1 Explain the function of common networking protocols
  - SIP (VoIP)
  - RTP (VoIP)
- 3.3 Explain the advanced features of a switch
  - PoE

Lecture Focus Questions:

- What are the advantages of using VoIP compared to traditional phones? What are the disadvantages?
- What switch feature is often used when implementing VoIP?
- What is the difference between the SIP and RTP protocols used with VoIP?
- How do delay, jitter, and packet loss affect VoIP calls?
- Why is Quality of Service (QoS) important for VoIP?

Time

About 15 minutes

Number of Exam Questions

3 questions

Section 6.1: Wireless Concepts

Summary

This section discusses wireless architecture and infrastructure. The following areas are discussed about wireless networking architecture:

- Signaling methods
  - Frequency Hopping Spread Spectrum (FHSS)
  - Direct-Sequence Spread Spectrum (DSSS)
- Topology
  - Ad hoc
  - Infrastructure
- Media access
- Devices
  - Wireless NIC
  - Wireless access point (AP)
  - Wireless bridge

The following concepts about wireless infrastructure are presented:

- Components of a wireless network
  - Station (STA)
  - Access Point (AP)
  - Basic Service Set (BSS)
  - Independent Basic Service Set (IBSS)
  - Extended Service Set (ESS)
  - Distribution System (DS)
- Identifiers for wireless networks
  - Service Set Identifier (SSID)
  - Basic Service Set Identifier (BSSID)

Network+ Objectives

- 3.4 Implement a basic wireless network
  - Install access point
    - Configure channels and frequencies

Lecture Focus Questions:

- Under which 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?

Time
About 25 minutes

Number of Exam Questions
1 question

Section 6.2: Wireless Standards

Summary

This section explores 802.11, Infrared, and Bluetooth wireless standards. Details about 802.11 standards include:

- Specifications of common standards:
  - 802.11a
  - 802.11b
  - 802.11g
  - 802.11n
- Technologies to improve the speed or distance of wireless transmissions
  - Multiple Input Multiple Output (MIMO)
  - Channel bonding
  - Frame composition
- Factors that can affect a wireless network implementation
  - Distance
  - Obstructions
  - Interference
  - Antenna strength
  - Backwards compatibility issues
  - Dual band access point
  - Mixed mode to provide communication with legacy clients
  - Mixing clients using different standards
  - Using MIMO and channel bonding to increase speed

Students will learn the following about Infrared (IR) wireless networking:

- Light waves employed by Infrared
- Modes that are used by infrared devices
  - Line of Sign (LoS)
  - Diffuse Mode
- Speed and security of IR

Facts presented about the Bluetooth standard include:

- Bluetooth equipped devices
- Specifications
- Master/slave networking mode
- Encryption

Network+ Objectives

- 1.7 Compare the characteristics of wireless communication standards

- 802.11 a/b/g/n
  - Speeds
  - Distance
  - Channels
  - Frequency

Lecture Focus Questions:

- What are the differences between 802.11a and 802.11g specifications?
- Devices that support the 802.11g standards are typically compatible with which other wireless standard?
- How does MIMO differ from channel bonding?
- Why is channel bonding typically not used with the 2.4 GHz range?
- What happens when an 802.11a device connects to an access point that supports both 802.11n and 802.11a? What happens if the access point uses MIMO and supports dual band?
- What is the difference between diffuse mode and line of sight?
- Which types of devices typically use Bluetooth wireless?

Time

About 50 minutes

Lab/Activity

- Select a Wireless Card
- Create a Wireless Network 1
- Create a Wireless Network 2

Number of Exam Questions

9 questions

Section 6.3: Wireless Security

Summary

This section examines facts about security on wireless networks.

- Authentication methods
  - Open
  - Shared key
  - 802.1x
- Security standards for wireless networking
  - Wired Equivalent Privacy (WEP)
  - Wi-Fi Protect Access (WPA)
  - Wi-Fi Protected Access 2 (WPA2) or 802.11i
- Security best practices to implement
  - Change the administrator account name and password
  - Change SSID from defaults
  - Update the firmware
  - Enable the firewall on the access point
  - Disable DHCP
  - Enable MAC address filtering

Network+ Objectives

- 1.7 Compare the characteristics of wireless communication standards
  - Authentication and encryption
    - WPA
    - WEP
    - TKIP
- 3.4 Implement a basic wireless network
  - Install access point
    - Configure appropriate encryption

Lecture Focus Questions:

- What does open authentication use for authenticating a device? Why is this not a very secure solution?
- What two additional components are required to implement 802.1x authentication?
- What does WEP use for the encryption key? Why does this present a security problem?
- Why should you *not* use shared key authentication with WEP?
- What is the difference between WPA Personal and WPA Enterprise?
- You have an access point that currently supports only WEP. What would you typically need to do to support WPA2?
- What is the encryption method used with WPA? WPA2?

- Which default values should you always change on your wireless network?

Time
About 25 minutes

Number of Exam Questions
9 questions

Section 6.4: Wireless Configuration

Summary

This section provides information about configuring a wireless network. Possible configuration tasks include:

- Setting the SSID
- Configuring the region (AP only)
- Configuring the channel
- Configuring security
- Configuring the beacon

Students will learn how to:

- Select and install wireless networking devices based on speed and network requirements.
- Configure a wireless access point.
- Configure wireless network connections.

Network+ Objectives

- 3.4 Implement a basic wireless network
  - Install client
  - Access point placement
  - Install access point
    - Configure appropriate encryption
    - Configure channels and frequencies
    - Set ESSID and beacon
  - Verify installation

Lecture Focus Questions:

- You are configuring a wireless network with multiple access points. When configuring the channel and the SSID, which value should match on all access points, and which should be different?
- When might you configure an access point to not use encryption?
- You have a device that supports only WEP. What could you possibly do to enable it to use WPA?
- What is the effect of decreasing the beacon interval on wireless traffic? How does increasing the beacon interval affect the ability of clients to connect to the wireless network?

Time

About 25 minutes

Lab/Activity

- Configure a Wireless Profile

Number of Exam Questions

8 questions

Section 6.5: Wireless Considerations

Summary

This section provides an overview of considerations that can effect a wireless connection.

- Incorrect configuration
- Range and obstructions
- Channel interference
- Atmospheric and EMI conditions
- AP placement
- Antennae orientation

Network+ Objectives

- 3.4 Implement a basic wireless network
  - Verify installation
- 4.7 Given a scenario, troubleshoot common connectivity issues and select an appropriate solution
  - Wireless Issues:
    - Interference (bleed, environmental factors)
    - Incorrect encryption
    - Incorrect channel
    - Incorrect frequency
    - ESSID mismatch
    - Standard mismatch (802.11 a/b/g/n)
    - Distance
    - Bounce
    - Incorrect antenna placement

Lecture Focus Questions:

- Where is the best place to locate your wireless access point?
- What type of objects might obstruct radio frequency wireless transmissions?
- How many channels should separate two different wireless networks?
- Which types of wireless networks require line-of-sight connections?
- How do range and antenna placement affect wireless networks?

Time

About 25 minutes

Number of Exam Questions

11 questions

Section 7.1: WAN Concepts

Summary

In this section students will learn concepts about Wide Area Networks (WAN) technologies, structure and services.

- Common WAN carriers
  - POTS
  - T1
  - T3
  - E1
  - E3
  - J1
  - J3
  - OC-1
  - OC-3
  - OC-12
  - OC-24
  - OC-48
  - OC-192
  - OC-256
  - OC-768
- Components of a WAN
  - WAN cloud
  - Central office (CO)
  - Local loop
  - Demarcation point
  - Consumer Premises Equipment (CPE)
  - Channel Service Unite/Data Service Unit (CSU/DSU)
- Methods to transfer data
  - Circuit switching
  - Packet switching
- WAN services
  - Public Switched Telephone Network (PSTN)
  - Integrated Services Digital Network (ISDN)
  - Frame Relay
  - Asynchronous Transfer Mode (ATM)
  - Synchronous Optical Networking (SONET)
  - Multiprotocol Label Switching (MPLS)

Network+ Objectives

- 2.3 Identify common physical network topologies
  - Point to point
  - Point to multipoint

- 2.5 Categorize WAN technology types and properties
  - Type:
    - Frame relay
    - E1/T1
    - ADSL
    - SDSL
    - VDSL
    - E3/T3
    - OC-x
    - ATM
    - SONET
    - MPLS
    - ISDN BRI
    - ISDN PRI
    - POTS
    - PSTN
  - Properties
    - Circuit switch
    - Packet switch
    - Speed
    - Transmission media
    - Distance
- 3.2 Identify the functions of specialized network devices
  - CSU/DSU

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? J1 and J3?
- With WAN technologies, what is a *channel* and how is it important?
- What is the difference between a packet switched network and a circuit switched network?
- What are the two parts of a CSU/DSU and what functions do each perform?
- Which WAN technology uses fixed-length cells?
- Which WAN technology is a transport technology for carrying signals over fiber optic cables?
- Which WAN technology can be implemented over regular telephone lines?
- How does MPLS add labels to packets? What are these labels used for?

Time

About 60 minutes

Number of Exam Questions

12 questions

Section 7.2: Internet Connectivity

Summary

This section discusses connecting to the Internet through an ISP. The following methods are presented:

- Public switched telephone network (PSTN)
- Digital Subscriber Line (DSL)
- Integrated Services Digital Network (ISDN)
- Cable
- Satellite
- Wireless

Students will learn how to:

- Select and install components to connect to the Internet through the PSTN using dial-up and DSL.
- Configure a dial-up connection.

Network+ Objectives

- 2.5 Categorize WAN technology types and properties
  - Type:
    - ADSL
    - SDSL
    - VDSL
    - Cable modem
    - Satellite
    - Wireless
    - ISDN BRI
    - ISDN PRI
    - POTS
    - PSTN
  - Properties
    - Speed
    - Transmission media
    - Distance

Lecture Focus Questions:

- What connection speeds should you expect with a PSTN Internet connection?
- What is *multiplexing*? How does this 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 is the difference between BRI and PRI with ISDN?
- What is the difference between a B channel and a D channel?
- What are the disadvantages of a satellite Internet connection?

Time

About 45 minutes

Lab/Activity

- Connect to the PSTN
- Connect to a DSL Network
- Create a Dial-up Internet Connection

Number of Exam Questions

13 questions

Section 7.3: Remote Access

Summary

This section examines establishing a remote access connection to allow a remote host to access resources on a local network. The following processes are presented:

- Physical connection
- Connection parameters
  - Point-to-Point Protocol (PPP)
  - PPP over Ethernet (PPPoE)
- Authentication
  - Challenge Handshake Authentication Protocol (CHAP)
  - Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)
  - Extensible Authentication Protocol (EAP)
- Authorization
- Accounting

Students will learn how to:

- Create and configure a remote access connection.
- Configure a server for remote access connections.
- Configure a RADIUS solution to provide AAA for remote access.

Network+ Objectives

- 4.7 Given a scenario, troubleshoot common connectivity issues and select an appropriate solution
  - Issues that should be identified but escalated:
    - Proxy arp
- 6.3 Explain the methods of network access security
  - Remote access
    - RAS
    - PPPoE
    - PPP
- 6.4 Explain methods of user authentication
  - AAA
    - RADIUS
    - TACACS+
  - CHAP
  - MS-CHAP
  - EAP

Lecture Focus Questions:

- What functions are performed by PPP for remote access connections?
- How does PPPoE differ from PPP?
- Why is proxy ARP necessary for dialup remote access clients?
- How does EAP differ from CHAP or MS-CHAP?
- What is the difference between *authentication* and *authorization*?
- What is an advantage of using RADIUS or TACACS+ in your remote access solution?
- How does RADIUS differ from TACACS+?

Time

About 60 minutes

Lab/Activity

- Configure a Remote Access Connection

Number of Exam Questions

9 questions

Section 8.1: Network Threats

Summary

In this section students will learn about threats to a network and the countermeasures to reduce the effects of an attack. Threats discussed include:

- Denial of Service (DoS)
- Smurf
- Virus
- Worm
- Man-in-the –middle
- Rogue access point
- Social engineering

Generic countermeasures discussed include implementation of:

- Security policies and procedures
- User training and awareness programs
- Patches and updates
- Strong physical security

Specific countermeasures are presented to prevent:

- Automated attacks
- Malware
- Man-in-the-middle attacks
- Social engineering

Network+ Objectives

- 6.5 Explain issues that affect device security
  - Physical security
- 6.6 Identify common security threats and mitigation techniques
  - Security threats
    - DoS
    - Viruses
    - Worms
    - Attackers
    - Man in the middle
    - Smurf
    - Rogue access points
    - Social engineering (phishing)
  - Mitigation techniques
    - Policies and procedures
    - User training
    - Patches and updates

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*?
- What is *social engineering*? What is the best defense against social engineering?
- What are some examples of physical security measures you can implement to protect your network?
- In addition to implementing virus scanning software, what must you do to ensure that you are protected from the latest virus variations?

Time

About 45 minutes

Number of Exam Questions

13 questions

Section 8.2: Firewalls

Summary

This section discusses using firewalls to allow or block network traffic. The following details about firewalls are discussed:

- Network-based firewall
- Host-based firewall
- Filtering rules
- Firewall types
  - Packet filtering firewall
  - Circuit-level proxy
- Zones used with firewalls
- Demilitarized zone (DMZ) configurations

Students will learn how to:

- Enable ICF for a connection.
- Open and close ports in ICF.

Network+ Objectives

- 1.2 Identify commonly used TCP and UDP default ports
  - TCP ports
    - FTP -- 20, 21
    - SSH -- 22
    - TELNET -- 23
    - SMTP -- 25
    - DNS -- 53
    - HTTP -- 80
    - POP3 -- 110
    - NTP -- 123
    - IMAP4 -- 143
    - HTTPS -- 443
  - UDP ports
    - TFTP -- 69
    - DNS -- 53
    - BOOTPS/DHCP -- 67
    - SNMP -- 161
- 3.1 Install, configure and differentiate between common network devices
  - Basic firewall
- 3.2 Identify the functions of specialized network devices
  - Proxy server
- 4.7 Given a scenario, troubleshoot common connectivity issues and select an appropriate solution

    - Issues that should be identified but escalated:
        - Proxy arp
- 6.1 Explain the function of hardware and software security devices
    - Network based firewall
    - Host based firewall
- 6.2 Explain common features of a firewall
    - Application layer vs. network layer
    - Stateful vs. stateless
    - Scanning services
    - Content filtering
    - Zones
- 6.3 Explain the methods of network access security
    - Filtering:
        - ACL
        - IP filtering

Lecture Focus Questions:

- How does a packet filtering firewall differ from a circuit-level gateway?
- Why is a packet filtering firewall a *stateless* device?
- What types of filter criteria can an application layer firewall use for filtering?
- What type of computers might exist inside of a demilitarized zone (DMZ)?
- Which security device might you choose to restrict access by user account?

Time

About 45 minutes

Lab/Activity

- Configure Windows Firewall

Number of Exam Questions

15 questions

Section 8.3: VPNs

Summary

This section provides details of how a Virtual Private Network (VPN) uses encryption to secure IP traffic over a TCP/IP network. Facts discussed include:

- The role of a tunneling protocol
- The role of tunnel endpoints
- Possible VPN implementations
- Implementation methods
  - Host-to-host VPN
  - Site-to-site VPN
  - Remote access VPN
- A comparison of common tunneling protocols
  - Point-to-Point Tunneling Protocol (PPTP)
  - Layer Two Tunneling Protocol (L2TP)
  - Internet Protocol Security (IPSec)
  - Secure Sockets Layer (SSL)

Students will learn how to:

- Configure the VPN protocol on a remote access server.
- Configure a client VPN connection.

Network+ Objectives

- 2.7 Explain common logical network topologies and their characteristics
  - VPN
- 6.1 Explain the function of hardware and software security devices
  - VPN concentrator
- 6.3 Explain the methods of network access security
  - Tunneling and encryption
    - SSL VPN
    - VPN
    - L2TP
    - PPTP
    - IPSEC

Lecture Focus Questions:

- How does a remote access VPN differ from a host-to-host VPN?
- With a site-to-site VPN, which devices are configured as the VPN tunnel endpoints?
- What does PPTP use for encryption? What does L2TP use?

- What is the difference between AH and ESP used with IPsec?
- Why are SSL VPNs more likely to be implemented when creating VPNs across the Internet through firewalls that you do not control?

Time

About 30 minutes

Lab/Activity

- Configure a VPN Connection

Number of Exam Questions

7 questions

Section 8.4: Switch Security

Summary

This section explores details about using switch features to increase security.

- Types of switch features
  - Virtual LAN (VLAN)
  - MAC filtering/port security
  - Port authentication (802.1x)
- Switch security implementation
  - Administrative benefits
  - Role of routers
  - Traffic priority when using Voice over IP (VoIP)
  - Port authentication

Students will learn how to:

- Create VLANs on a switch.

Network+ Objectives

- 2.7 Explain common logical network topologies and their characteristics
  - VLAN
- 3.3 Explain the advanced features of a switch
  - VLAN
  - Trunking
  - Port authentication
- 6.3 Explain the methods of network access security
  - Filtering:
    - MAC filtering

Lecture Focus Questions:

- How does a switch identify devices that are in different VLANs?
- What is required for devices to communicate between VLANs?
- Which type of switch port is a member of all VLANs identified on the switch?
- How are VLANs associated with frames as they move between switches?
- How is port security different from port filtering?
- What does port filtering use to control access?
- When using 802.1x authentication, a device connected to an unauthenticated port can communicate with which other devices on the LAN?
- Which networking feature commonly uses VLANs?

Time
About 40 minutes

Lab/Activity

- Exploring VLANs

Number of Exam Questions
13 questions

Section 8.5: Authentication

Summary

This section discusses using authentication to prove the identity of a user. Students will become familiar with the following concepts:

- Certificates
- Public Key Infrastructure (PKI)
- Certification Authorities (CAs)
- Trusted CAs and certificates
- Digital signatures
- Authentication protocols
    - Challenge Handshake Authentication Protocol (CHAP)
    - Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)
    - Extensible Authentication Protocol (EAP)
    - Kerberos
    - 802.1x

Students will learn how to:

- Configure remote access authentication protocols.

Network+ Objectives

- 6.4 Explain methods of user authentication
    - PKI
    - Kerberos
    - Network access control
        - 802.1x
    - CHAP
    - MS-CHAP
    - EAP
- 6.5 Explain issues that affect device security
    - Restricting local and remote access

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?
- How does CHAP protect the password (or shared secret) during the authentication process?
- 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?
- What device is required to implement 802.1x authentication?

Time

About 35 minutes

Number of Exam Questions

11 questions

Section 8.6: Secure Protocols

Summary

This section provides information about using secure protocols to provide authentication or encryption. Details discussed include:

- Secure protocols
  - Secure Sockets Layer (SSL)
  - Transport Layer Security (TLS)
  - Secure Shell (SSH)
- Comparison of unsecure and secure protocols

Students will learn how to:

- Require SSL on a Web site.

Network+ Objectives

- 1.1 Explain the function of common networking protocols
  - FTP
  - HTTP(S)
  - SSH
  - Telnet
  - SNMP2/3
  - TLS
- 6.5 Secure methods vs. unsecure methods
  - SSH, HTTPS, SNMPv3, SFTP, SCP
  - TELNET, HTTP, FTP, RSH, RCP, SNMPv1/2

Lecture Focus Questions:

- Which protocol is the secure alternative to Telnet?
- What is the difference between SFTP and FTPS?
- Which protocol is added to HTTP for secure Web browsing?
- What improvements does SNMPv3 provide over earlier SNMP versions?

Time

About 20 minutes

Number of Exam Questions

8 questions

Section 8.7: Detection and Prevention

Summary

This section explores using an intrusion detection system (IDS) to detect and prevent attacks. Typical detection system methods include:

- Response capability
  - Passive IDS
  - Active IDS
- Recognition method
  - Signature recognition
  - Anomaly recognition
- Detection scope
  - Host-based IDS
  - Network-based IDS

Network tools to monitor a network for threats include:

- Packet sniffer
- Port scanner
- Security scanning software
- Up to date patches for operating systems and application
- System logs
- Firewall logs

Network+ Objectives

- 3.2 Identify the functions of specialized network devices
  - IDS/IPS
- 5.2 Explain the purpose of network scanners
  - Packet sniffers
  - Intrusion detection software
  - Intrusion prevention software
  - Port scanners
- 6.1 Explain the function of hardware and software security devices
  - IDS
  - IPS
- 6.2 Explain common features of a firewall
  - Signature identification

Lecture Focus Questions:

- What type of recognition method is used by most virus scanning software?
- How does an IPS differ from an IDS?

- What is the advantage to using a network-based IDS instead of a host-based IDS?
- What should you regularly do when using a signature-based IDS?
- How can packet sniffing and port scanning software be used to improve the security of your network?

Time

About 20 minutes

Number of Exam Questions

12 questions

Section 9.1: Documentation

Summary

This section examines using documentation to track actions that have taken place on a network. Different types of documentation that can be used to manage a network include:

- Policies
- Regulations
- Procedures
- Network diagrams
- Wiring schematics
- Configurations
- Change/job logs
- Baselines

Network+ Objectives

- 4.2 Identify types of configuration management documentation
  - Wiring schematics
  - Physical and logical network diagrams
  - Baselines
  - Policies, procedures and configurations
  - Regulations
- 4.3 Given a scenario, evaluate the network based on configuration management documentation
  - Compare wiring schematics, physical and logical network diagrams, baselines, policies and procedures and configurations to network devices and infrastructure
  - Update wiring schematics, physical and logical network diagrams, configurations and job logs as needed

Lecture Focus Questions:

- What is the difference between a *policy* and a *procedure*?
- How do *regulations* affect network policies?
- Why does keeping good records help in managing your network?
- What type of information is shown on a wiring diagram? How does this differ from a network diagram?
- What should you do after making a change to a network device?

Time

About 20 minutes

Number of Exam Questions
11 questions

Section 9.2: SNMP

Summary

This section provides facts about using Simple Network Management Protocol (SNMP) to manage complex networks. SNMP uses the following components:

- Manager
- Agent
- Management Information BASE (MIB)
- Trap

Network+ Objectives

- 1.1 Explain the function of common networking protocols
  - SNMP2/3

Lecture Focus Questions:

- What is the role of the MIB when using SNMP?
- What is a *trap* and how can you use it in network administration?
- How is the community name used with SNMP?
- Why doesn't the community name provide security for SNMP devices?

Time

About 5 minutes

Number of Exam Questions

2 questions

Section 9.3: Remote Management

Summary

This section discusses solutions for remote management of network devices.

- Terminal emulation
- Remote desktop

Students will learn how to:

- Establish a remote desktop connection to another computer.
- Configure remote desktop connection parameters and device redirection.

Network+ Objectives

- 1.1 Explain the function of common networking protocols
  - SSH
  - Telnet
- 6.3 Remote access
  - RDP
  - VNC
  - ICA

Lecture Focus Questions:

- What is the difference between Telnet and SSH?
- How does remote desktop software differ from terminal emulation software?
- How can you use a remote desktop solution for troubleshooting and technical support within your organization?
- How does a remote desktop protocol minimize the data sent between the client and server devices for a remote connection?
- What is device redirection and how does it add flexibility to remote desktop connections?

Time

About 20 minutes

Lab/Activity

- Allow Remote Desktop Connections

Number of Exam Questions

4 questions

Section 9.4: Monitoring

Summary

This section presents information about the tools used to monitor a network for potential problems.

- Logs
- Load tester
- Throughput tester
- Packet sniffer

Students will learn how to:

- View events recorded in system and application logs.
- Use a packet sniffer to monitor network traffic.

Network+ Objectives

- 4.4 Conduct network monitoring to identify performance and connectivity issues using the following:
  - Network monitoring utilities (e.g. packet sniffers, connectivity software, load testing, throughput testers)
  - System logs, history logs, event logs
- 5.2 Explain the purpose of network scanners
  - Packet sniffers

Lecture Focus Questions:

- Why should you only enable logging for specific events you want to track?
- After configuring system logging, what else must you do to take advantage of the benefits of logging?
- How does a *load tester* differ from a *throughput tester*?
- What must you do to configure a packet sniffer to be able to see all frames on a subnet?

Time

About 35 minutes

Number of Exam Questions

9 questions

Section 9.5: Optimization

Summary

This section examines optimization of the network. Solutions discussed to provide accessibility and improve performance include:

- Ethernet bonding
- Spanning tree
- Load balancing
- Caching engine
- Quality of Service (QoS)
- Traffic shaper
- Multilayer switch/content switch

Students will become familiar with using network segmentation to optimize network performance. Concepts discussed include:

- Collision domain
- Broadcast domain
- Membership
- Guidelines for connection devices

Network+ Objectives

- 1.4 Given a scenario, evaluate the proper use of the following addressing technologies and addressing schemes
  - Addressing schemes
    - Broadcast
- 2.6 Categorize LAN technology types and properties
  - Properties
    - Broadcast
    - Bonding
- 3.2 Identify the functions of specialized network devices
  - Multilayer switch
  - Content switch
  - Load balancer
  - Bandwidth shaper
- 3.3 Explain the advanced features of a switch
  - Spanning tree
- 4.5 Explain different methods and rationales for network performance optimization
  - Methods:
    - QoS
    - Traffic shaping

        - Load balancing
        - High availability
        - Caching engines
        - Fault tolerance
    - Reasons:
        - Latency sensitivity
        - High bandwidth applications
            - VoIP
            - Video applications
        - Uptime
- 4.7 Given a scenario, troubleshoot common connectivity issues and select an appropriate solution
    - Physical issues:
        - Collisions
    - Issues that should be identified but escalated:
        - Broadcast storms

Lecture Focus Questions:

- What 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 your network?
- What is the difference between a *collision domain* and a *broadcast domain*?
- Your network uses only 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?
- Your network uses only 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?

Time

About 50 minutes

Number of Exam Questions

14 questions

Section 10.1: Troubleshooting Overview

Summary

This section provides a troubleshooting overview for the students. They will become familiar with a systematic approach to problem solving. Tools that can be used to perform the following tasks when troubleshooting network problems include:

- View the ARP table
  - arp (Windows)
- View IP configuration information
  - ipconfig (Windows 2000 and higher)
  - ifconfig (Linux)
- View IP and routing statistics
  - netstat (Windows)
- View NetBIOS over TCP/IP information
  - nbstat (Windows)
- Test host-to-host connectivity
  - ping
- Identify the path between two hosts
  - tracert (Windows)
  - traceroute (Linux)
  - mtr (Linux)
- Test host-to-host connectivity using ARP
  - arping (Linux)
- Test name resolution
  - nslookup (Windows and Linux)
  - dig (Linux)
  - host (Linux)
- View and modify the routing table
  - route

Network+ Objectives

- 1.1 Explain the function of common networking protocols
  - ICMP
- 4.6 Given a scenario, implement the following network troubleshooting methodology
  - Information gathering -- identify symptoms and problems
  - Identify the affected areas of the network
  - Determine if anything has changed
  - Establish the most probable cause
  - Determine if escalation is necessary
  - Create an action plan and solution identifying potential effects
  - Implement and test the solution

    - Identify the results and effects of the solution
    - Document the solution and the entire process
- 5.1 Given a scenario, select the appropriate command line interface tool and interpret the output to verify functionality
    - Traceroute
    - Ipconfig
    - Ifconfig
    - Ping
    - Arp ping
    - Arp
    - Nslookup
    - Host
    - Dig
    - Mtr
    - Route
    - Nbtstat
    - Netstat

Lecture Focus Questions:

- Why is it important to follow a troubleshooting methodology?
- When faced with a problem, why shouldn't you start trying fixes immediately?
- What is *escalation* and when should it be performed?
- After the problem is fixed, what else must you do to finish troubleshooting?
- What is the difference between **ping** and **traceroute**?
- What Linux command is similar to **ipconfig**?
- When would you use **nslookup** or **dig**?

Time

About 30 minutes

Number of Exam Questions

12 questions

Section 10.2: Troubleshooting Network Communication

This section discusses using **ping** and **traceroute** to troubleshoot network communication problems. It provides a scenario for the students to learn the steps to trace the source of a connectivity problem.

Students will learn how to:

- Use troubleshooting utilities to isolate, diagnose, and resolve network communication problems.

Network+ Objectives

- 4.6 Given a scenario, implement the following network troubleshooting methodology
  - Information gathering -- identify symptoms and problems
  - Identify the affected areas of the network
- 4.7 Given a scenario, troubleshoot common connectivity issues and select an appropriate solution

Lecture Focus Questions:

- What might it tell you if all hosts in your network had the same problem when communicating with another host in another network?
- What types of problems might you encounter if the default gateway router were down?
- What types of problems might you encounter if a single router in an internetwork were down?
- What additional information does the **traceroute** command give you over the **ping** command?

Time

About 30 minutes

Lab/Activity

- Exploring Network Communications
- Troubleshoot Network Communications

Number of Exam Questions

4 questions

Section 10.3: Troubleshooting Physical Connectivity

Summary

This section examines troubleshooting the physical connectivity of a network. Troubleshooting facts about the following are discussed:

- Identifying the fault domain (location of a physical problem)
- Verifying the physical connectivity using Link Status lights
  - Link light
  - Activity light
  - Collision light
- Identifying faulty wiring
  - Interference
  - Crosstalk
    - Near end crosstalk (NEXT)
    - Far end crosstalk (FEXT)
    - Alien crosstalk
  - Attenuation
  - Open impedance mismatch (echo)
  - Shorts
  - Open circuit
  - Miswired
    - Reverse connection
    - Wiremapping
    - Split pair
- Troubleshooting tools
  - Loopback plug
  - Smart jack
  - Known good spares
  - Cable tester
  - Time Domain Reflector (TDR)
  - Certifier
  - Toner probe
  - Butt set
  - Multimeter
  - Voltage event recorder
  - Temperature monitor

Students will learn how to:

- Select the appropriate tool when troubleshooting physical issues.

Network+ Objectives

- 2.4 Given a scenario, differentiate and implement appropriate wiring standards
  - Loopback
- 2.8 Install components of wiring distribution
  - Smart jack
- 4.7 Given a scenario, troubleshoot common connectivity issues and select an appropriate solution
  - Physical issues:
    - Cross talk
    - Nearing crosstalk
    - Near End crosstalk
    - Attenuation
    - Collisions
    - Shorts
    - Open impedance mismatch (echo)
    - Interference
- 5.3 Given a scenario, utilize the appropriate hardware tools
  - Cable testers
  - Certifiers
  - TDR
  - OTDR
  - Multimeter
  - Toner probe
  - Butt set
  - Voltage event recorder
  - Temperature monitor

Lecture Focus Questions:

- What happens if a host in a star topology goes down? A token ring topology?
- What happens if there is a cable break on a bus topology? 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?
- What is the difference between alien crosstalk and near-end crosstalk?
- Which cable types are immune to the effects of EMI?
- How does distance affect attenuation? How does it affect impedance?
- What is the single best method to reduce the effects of an impedance mismatch?
- How does an *open* circuit differ from a *short*?
- 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?

Time

About 75 minutes

Number of Exam Questions
15 questions

Section 10.4: Troubleshooting IP Configuration

Summary

In this section students will learn commands to troubleshoot IP configuration problems. They will learn how to interpret the output of **ipconfig /all** for the following conditions:

- Static IP configuration
- DHCP configuration
- Rogue DHCP server
- Incorrectly configured DHCP server
- APIPA configuration
- Alternate configuration

Commands that can be used on a Windows system to gather network information include:

- **arp -a**
- **netstat**
- **netstat -a**
- **netstat -r**
- **netstat -s**
- **nbstat -c**

The **netsh** command is used to clear the ARP cache.

Students will learn to:

- Find information about IP configuration settings on Windows and Linux systems.
- Troubleshoot IP configuration problems caused by misconfiguration or DHCP-related issues.

Network+ Objectives

- 4.7 Given a scenario, troubleshoot common connectivity issues and select an appropriate solution
    - Logical issues:
        - Incorrect IP address
        - Wrong gateway
        - Wrong subnet mask
- 5.1 Given a scenario, select the appropriate command line interface tool and interpret the output to verify functionality
    - Ipconfig
    - Ifconfig
    - Arp
    - Nbtstat

- Netstat

Lecture Focus Questions:

- What does the **/all** switch do when used with **ipconfig**?
- How can you tell if a rogue DHCP server is active on your network?
- How do you know if a host is using APIPA?
- What is the difference between the **netstat** and **nbtstat** commands?

Time

About 55 minutes

Lab/Activity

- Find Configuration Information
- Troubleshoot IP Configuration Problems

Number of Exam Questions

14 questions

Section 10.5: Troubleshooting Name Resolution

Summary

This section examines troubleshooting name resolution problems. Students will learn:

- Symptoms
- Tools for troubleshooting DNS name resolution
  - nslookup
  - dig
  - host

Students will learn how to:

- Identify, diagnose, and resolve problems with name resolution.

Network+ Objectives

- 4.7 Given a scenario, troubleshoot common connectivity issues and select an appropriate solution
  - Logical issues:
    - Wrong DNS
- 5.1 Given a scenario, select the appropriate command line interface tool and interpret the output to verify functionality
  - Nslookup
  - Host
  - Dig

Lecture Focus Questions:

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

Time

About 15 minutes

Number of Exam Questions

9 questions

Section 10.6: Troubleshooting Switching

Summary

In this section students will learn how to troubleshoot switches on the network. Several problems and countermeasures to the problems are presented.

- Collisions
- Duplex mismatch
- Slow link speed
- Switching loop
- Broadcast storm
- Incorrect VLAN membership
- Frame errors

Network+ Objectives

- 4.7 Given a scenario, troubleshoot common connectivity issues and select an appropriate solution
    - Physical issues:
        - Collisions
    - Logical issues:
        - Port speed
        - Port duplex mismatch
        - Incorrect VLAN
    - Issues that should be identified but escalated:
        - Switching loop
        - Broadcast storms

Lecture Focus Questions:

- You have a network connected using switches with a single device connected to each switch port. Why should you be surprised to see collisions on this network?
- What is a *duplex mismatch*?
- What conditions lead to a *broadcast storm*?
- How can you prevent switching loops from forming?
- You move a device from one switch port to another, and now it cannot communicate with any other device on the network. The switch link lights are lit. What switch configuration should you check?
- Besides the switch configuration, what should you check if you see excessive frame errors on the switch?

Time

About 20 minutes

Number of Exam Questions
6 questions

Section 10.7: Troubleshooting Routing

Summary

This section discusses facts about troubleshooting routing issues. The following routing problems are discussed:

- Can't access hosts outside the local subnet
- Can't communicate with any host on a specific network
- Can't access the Internet
- Remote clients can't access network resources

Students will learn how to:

- View the routing table on a device.
- Trace the path used between two devices through a network.

Network+ Objectives

- 4.7 Given a scenario, troubleshoot common connectivity issues and select an appropriate solution
    - Logical issues:
        - Wrong gateway
    - Issues that should be identified but escalated:
        - Routing loop
        - Route problems
        - Proxy arp
- 5.1 Given a scenario, select the appropriate command line interface tool and interpret the output to verify functionality
    - Traceroute
    - Ping
    - Mtr
    - Route

Lecture Focus Questions:

- How is it possible for all hosts on a subnet to be configured with the wrong default gateway address?
- What is the format for the default route entry in a routing table? What purpose does the default route serve?
- What are the symptoms of a routing loop? How can you identify a routing loop?
- Why might you escalate routing problems that you observe?
- How can proxy ARP settings appear as routing problems?

Time
About 35 minutes

Lab/Activity

- Find Path Information

Number of Exam Questions
9 questions

Practice Exams

Summary

This section provides information to help prepare students to take the exam and to register for the exam.

Students will also have the opportunity of testing their mastery of the concepts presented in this course to reaffirm that they are ready for the certification exam. For example, all questions that apply to **Objective 1.0: Network Technologies** are grouped together and presented in practice exam ***Domain 1: Network Technologies, All Questions***. Students will typically take about 60-90 minutes to complete each of the following practice exams.

Domain 1: Network Technologies, All Questions (129 questions)
Domain 2: Network Media and Topologies, All Questions (124 questions)
Domain 3: Network Devices, All Questions (58 questions)
Domain 4: Network Management, All Questions (101 questions)
Domain 5: Network Tools, All Questions (54 questions)
Domain 6: Network Security, All Questions (78 questions)

The *Certification Practice Exam* consists of 100 questions that are randomly selected from the above practice exams. Each time the Certification Practice Exam is accessed different questions may be presented. The Certification Practice Exam has a time limit of 90 minutes -- just like the real certification exam. A passing score of 95% should verify that the student has mastered the concepts and is ready to take the real certification exam.