TestOut

Lesson Plans

CCNA

(Exam 640-802)

Version 6.0

The lessons only experience can teach

Table of Contents

Course Overview

This course prepares students for the Cisco Certified Network Associate (CCNA) certification exam 640-802 by Cisco. It focuses on implementing, managing, protecting, and troubleshooting small to medium size enterprise branch networks.

Module 0 – Introduction

This module introduces the prerequisites to this course and discusses the two paths students can take to obtain CCNA certification. Students will become familiar with how to use the Cisco Simulator as a learning tool to complete the simulations throughout the course.

Module 1 – Networking Concepts

This module discusses the basics of networking, starting with how the OSI Model and TCP/IP protocols relate to data flow in a network. Students will learn the steps to data encapsulation and the fundamentals of Ethernet architecture. They will learn how bridging, switching, and routing function in the network environment.

Module 2 – Cisco Devices

In this module students will learn about accessing, starting up, configuring, and managing Cisco devices. They will learn how to use **show** commands to find information about the status of a Cisco switched network and how to change the device host name and configure descriptions on device interfaces. They will also learn how to apply router security through system passwords and banners and how to use Cisco Discovery Protocol (CDP) to learn and share information about neighboring Cisco devices.

Module 3 – LAN Implementation

This module covers LAN implementation; devices to connect switches and routers to network devices and hosts, configuring switch port parameters, configuring and verifying settings for a TCP/IP network, configuring DHCP and DNS operations on a router, configuring Static and RIP routing, and using LAN segmentation to increase network performance and reduce congestion.

Module 4 – Wireless Networks

In Module 4 students will learn the basics of using radio waves for data transmissions. They will learn wireless standards, infrastructure, security, and how to implement a wireless configuration.

Module 5 – Subnetting

Module 5 teaches the students how to calculate an addressing scheme for a network, configure subnet addresses, masks, and host addresses, and select the appropriate subnet addresses and masks for summarization.

Module 6 – WAN Implementation

Module 6 discusses implementing Wide Area Networks (WANs). Students will become familiar with WAN types, components, transmission carriers, connectors, and how to configure a basic WAN connection. Students will learn how to configure PPP encapsulation on serial links, and the basics of Network Address Translation (NAT). They will also learn how to troubleshoot WANs with the commands used to verify device and network connectivity.

Module 7 – Advanced Switching

In Module 7 students will learn advanced switching concepts that can be implemented depending upon the needs and configuration of the system; Virtual LANs (VLANs), Trunking, VLAN Trunking Protocol (VTP), Spanning Tree, EtherChannel, and Inter-VLAN routing.

Module 8 – Access Lists

This module discusses the basics of access lists and configuring and applying access lists to allow or deny the flow of packets between networks.

Module 9 – IP Routing

In this module students will learn basic routing concepts. They will learn to compare and configure Routing Information Protocol (RIP), Open Shortest Path First (OSPF), and Enhanced IGRP (EIGRP).

Module 10 – Troubleshooting Routing

This section covers troubleshooting of routers. Troubleshooting tips and commands used to verify RIP, OSPF, and EIGRP configurations are presented.

Module 11 – Frame Relay

In Module 11 students will learn the fundamentals of Frame Relay. They will learn how to configure Frame Relay on Cisco routers, configure address mappings, configure subinterfaces, and troubleshoot a Frame Relay configuration.

Module 12 – Advanced TCP/IP Configuration

Module 12 teaches the students how to implement an IPv6 configuration, configure DHCP from the command line, and configure Dynamic and Static NAT.

Module 13 – Network Security

Module 13 discusses a variety of network security threats and solutions. Students will learn how to harden a network to tighten security controls and use switch port security to control communication through a switch port. They will also learn the basics of protecting IP traffic on a TCP/IP network using Virtual Private Network (VPN) security technologies.

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 CCNA certification test.

Section 0.1: Introduction

Preparation

This section introduces the prerequisite knowledge a student should have before attempting this course. They include knowledge of:

- CompTIA's Network+
- Or equivalent networking experience

There are two paths available for obtaining the CCNA certification:

1. Pass Exam 640-802 or
2. Pass Exam 640-822 and Exam 640-816

In this section students will learn how to use the Cisco Simulator. They should be familiar with launching the lab, completing the instructions in the scenario and reviewing the lab report. They will also need to identify the Cisco Device Icons used to represent network devices and connections in this course.

Experiment with the router simulations so you will be able to demonstrate them in class. The first router simulation in the course is in *2.5.3: Find Device Information*.

Time

About 10 minutes

Section 1.1: The OSI Model

Preparation

This section discusses the OSI model and explains how it relates to network communication. Familiarize yourself with the basic operation of the 7 layers of the OSI Model:

- Layer 7 Application
- Layer 6 Presentation
- Layer 5 Session
- Layer 4 Transport
- Layer 3 Network
- Layer 2 Data Link
- Layer 1 Physical

CCNA Objectives

- 103. Use the OSI and TCP/IP models and their associated protocols to explain how data flows in a network
- 105. Describe the purpose and basic operation of the protocols in the OSI and TCP models
- 110. Identify and correct common network problems at layers 1, 2, 3 and 7 using a layered model approach

Lecture Focus Questions:

- What is the OSI model and why is it important in understanding networking?
- How does the third OSI model layer relate to administering routers?
- Which OSI model layer is concerned with MAC addresses?
- What protocols correspond to the Presentation and Session layers?
- What is the difference between the TCP and UDP protocols?
- What is the EIA/TIA 232 protocol concerned with?

Time

About 40 minutes

Section 1.2: TCP/IP

Preparation

This section examines the basic operation of the protocols in the TCP/IP Protocol Suite. The layers of the TCP/IP (also known as Department of Defense (DoD) Model) are compared to the OSI Model Layers. Students will become familiar with description and purpose of several TCP/IP protocols and how IP Addresses allow hosts to participate on IP based networks.

CCNA Objectives

- 103. Use the OSI and TCP/IP models and their associated protocols to explain how data flows in a network
- 104. Describe common networked applications including web applications
- 105. Describe the purpose and basic operation of the protocols in the OSI and TCP models
- 106. Describe the impact of applications (Voice Over IP and Video Over IP) on a network
- 301. Describe the operation and benefits of using private and public IP addressing

Lecture Focus Questions:

- How does the DOD model correspond to the OSI model?
- Which TCP/IP protocols allow for copying and moving files?
- What does the Telnet protocol allow you to do?
- Which protocol includes a set of messages that controls how data moves through a network?
- What is the role of the subnet mask?
- What is the default address class of the IP address 132.11.166.5?
- What three address ranges are used for private IP addresses?
- What is the broadcast address of network 132.11.0.0?

Time

About 25 minutes

Section 1.3: Device Communication

Preparation

This section explains data encapsulation. Students will need to know the five steps to the process of data encapsulation when transmitting a message from one device to another:

1. Data
2. Segment
3. Packet
4. Frame
5. Bits

CCNA Objectives

- 103. Use the OSI and TCP/IP models and their associated protocols to explain how data flows in a network

Lecture Focus Questions:

- Which OSI model layer uses service data units called frames?
- When moving from top to bottom through the OSI model layers, which comes first, packets or segments?
- What gets added to the service data unit at the Network layer? At the Data Link layer?

Time

About 10 minutes

Section 1.4: Ethernet

Preparation

In this section the students will learn the essentials of Ethernet architectural concepts; topology, media access, transmission media, frame type, and physical address. They will compare the characteristics of different Ethernet implementations available and examine the traits of half-duplex and full duplex modes.

CCNA Objectives

- 109. Describe the components required for network and Internet communications
- 201. Select the appropriate media, cables, ports, and connectors to connect switches to other network devices and hosts
- 202. Explain the technology and media access control method for Ethernet networks
- 403. Select the appropriate media, cables, ports, and connectors to connect routers to other network devices and hosts

Lecture Focus Questions:

- What is the purpose of the jam signal and the back off in Ethernet communications?
- What is the maximum cable length allowed for 100BaseTX?
- What is the physical device address used on Ethernet networks?
- Two devices are using full-duplex communications with the 1000BaseT standards. What is the amount of bandwidth available?
- Under what conditions can you disable collision detection on an Ethernet network?

Time

About 25 minutes

Section 1.5: Bridging and Switching

Preparation

This section discusses the basics of how bridges and switches work. A bridge is a data forwarding device that provides data transfer. A switch is a multiport bridge that can perform switching tasks much faster than a bridge. Switches have replaced bridges in most network applications.

Students will learn how bridges and switches use MAC addresses and ports to build a forwarding database. They will also learn the different methods the switch uses to forward packets:

- Store-and-forward
- Cut-through
- Fragment-free

CCNA Objectives

- 101. Describe the purpose and functions of various network devices
- 102. Select the components required to meet a network specification
- 103. Use the OSI and TCP/IP models and their associated protocols to explain how data flows in a network
- 108. Determine the path between two hosts across a network
- 109. Describe the components required for network and Internet communications
- 204. Explain basic switching concepts and the operation of Cisco switches

Lecture Focus Questions:

- What is the difference between a bridge and a switch?
- What is the 80/20 rule of network segmentation with bridges?
- How do bridges and switches learn MAC addresses?
- What is the difference between the store-and-forward and the fragment-free switching methods?
- Which switching method is the fastest?

Time

About 25 minutes

Section 1.6: Routing

Preparation

This section discusses routing. A router is a device that sends packets from one network to another network. Routers use routing tables to maintain information about destination networks. Students will learn what type of information is stored in the routing table and how routers build and maintain the routing database.

CCNA Objectives

- 101. Describe the purpose and functions of various network devices
- 103. Use the OSI and TCP/IP models and their associated protocols to explain how data flows in a network
- 108. Determine the path between two hosts across a network
- 109. Describe the components required for network and Internet communications
- 401. Describe basic routing concepts (including: packet forwarding, router lookup process)

Lecture Focus Questions:

- What type of information is stored in the routing table?
- What is convergence?
- What is the function of a routing protocol?
- A computer needs to send a message to another computer on the same network. What MAC address would go into the destination portion of the frame?
- A computer needs to send a message to another computer on a different network. What MAC address would go into the destination portion of the frame?
- As a packet moves from device to device through an internetwork, do the Network layer addresses change or remain the same?

Time

About 20 minutes

Section 2.1: Connecting Cisco Devices

Preparation

In this section students will become familiar with the following common Cisco devices:

- 3745 Router
- 3640 Router
- Network Module
- 2500 Series Router
- 1841 Router
- 1604 Router
- 2950 Switch
- 2960 Switch
- 3550 Switch

They will also learn how to manage the device by connecting to the router or switch through either a dedicated terminal or PC. Students will learn how to use HyperTerminal to connect to a Cisco device console and to use Telnet to create a virtual terminal connection to a Cisco device.

CCNA Objectives

- 205. Perform and verify initial switch configuration tasks including remote access management
- 405. Access and utilize the router to set basic parameters

Lecture Focus Questions:

- What HyperTerminal settings should you use to connect to the router console for the first time?
- What are the requirements for using a VTY (virtual terminal) connection to a Cisco device?
- What type of cable do you use to connect a PC to a router console port?

Time

About 15 minutes

Section 2.2: System Startup

Preparation

Students will learn the basic startup sequence of Cisco devices.

1. Verify hardware using POST.
2. Load the IOS images (operating system) from flash memory into RAM.
3. Apply the device configuration in the startup-config file to customize the router configuration and save it into NVRAM.

They will learn how to use Setup mode to complete an initial configuration and Express setup to configure a Cisco device using a GUI interface.

CCNA Objectives

- 205. Perform and verify initial switch configuration tasks including remote access management
- 402. Describe the operation of Cisco routers (including: router bootup process, POST, router components)

Lecture Focus Questions:

- If the router can't find an IOS image in flash, where will it look next?
- What happens if the router can't find a configuration file at startup?
- What is the role of the configuration register?
- What configuration register value tells the router to skip the startup-config file?

Time

About 20 minutes

Section 2.3: Command Line Interface (CLI)

Preparation

This section examines the basic command mode prompts and commands of the Command Line Interface (CLI). Students will learn how to use **help** no matter what mode they are in to identify possible commands, keywords, and parameters. They will learn how to use advanced editing features to efficiently enter commands at the console. Students will also learn how to access commands in the history buffer and control response messages that are displayed on the screen.

CCNA Objectives

- 205. Perform and verify initial switch configuration tasks including remote access management
- 405. Access and utilize the router to set basic parameters

Lecture Focus Questions:

- What router mode is indicated by the # prompt?
- How can you get a list of allowed keywords for a command?
- You use help to get a list of keywords for a command. In the list of options you see: A.B.C.D. What should you type to complete the command?
- How can you move the cursor backwards one word?
- How do you turn off console configuration messages?

Time

About 30 minutes

Lab/Activity

- Use Command Help

Section 2.4: Managing System Files

Preparation

In this section students will learn how to manage system files by saving configuration changes, loading an IOS image from an alternate location and upgrading the IOS image.

CCNA Objectives

- 405. Access and utilize the router to set basic parameters
- 409. Manage IOS configuration files (including: save, edit, upgrade, restore)
- 410. Manage Cisco IOS

Lecture Focus Questions:

- Where is the startup-config file stored? Where is the running-config file stored?
- What is stored in ROM?
- What is the generic syntax for loading a configuration file into RAM?
- What does the **boot system** command do?

Time

About 35 minutes

Section 2.5: Using Show Commands

Preparation

This section discusses using common **show** commands to find information about the device configuration. The **show** command is only available in enable and user modes. Students will learn how to save time in verifying information while in config mode by using the **do show** command rather than having to move back into enable or user mode to use the **show** command.

CCNA Objectives

- 215. Interpret the output of various show and debug commands to verify the operational status of a Cisco switched network
- 416. Verify router hardware and software operation using SHOW & DEBUG commands

Time

About 10 minutes

Lab/Activity

- Find Device Information

Section 2.6: Hostname and Descriptions

Preparation

In this section students will learn how to change the device host name and configure descriptions on device interfaces. They will learn the switch and router interface numbering schemes. Students will also learn the abbreviations for the interface types; FastEthernet, Gigabit, Serial, and Ethernet.

CCNA Objectives

- 205. Perform and verify initial switch configuration tasks including remote access management
- 405. Access and utilize the router to set basic parameters
- 406. Connect, configure, and verify operation status of a device interface

Lecture Focus Questions:

- When is the Slot/Sub-slot/Port numbering used?
- How do fixed ports and WIC slots affect the numbering scheme for a device?
- What changes in the prompt after you set a hostname?

Time

About 20 minutes

Lab/Activity

- Configure Hostnames and Descriptions

Section 2.7: System Passwords

Preparation

This section examines how to configure router passwords for enable, console, and VTY. Students will learn how to restrict console and VTY access to a Cisco device and how to recover device passwords.

CCNA Objectives

- 205. Perform and verify initial switch configuration tasks including remote access management
- 405. Access and utilize the router to set basic parameters
- 417. Implement basic router security

Lecture Focus Questions:

- What is the difference between the **enable** and the **enable secret** passwords? Which one is more secure?
- How would you require a password when logging on through the console?
- You have configured the VTY lines on a router with a password but you did not use the **login** command. Will VTY login be allowed? Will a password be required?
- What must you do to disable VTY login?

Time

About 50 minutes

Lab/Activity

- Exploring Enable Passwords
- Set Console and VTY Passwords
- Modify System Passwords

Section 2.8: Banners

Preparation

In this section students will learn how to use banners to display message for users logging into the device. Four types of banners can be displayed at various times during the login or startup sequence.

CCNA Objectives

- 205. Perform and verify initial switch configuration tasks including remote access management
- 405. Access and utilize the router to set basic parameters
- 417. Implement basic router security

Lecture Focus Questions:

- When do each of the banners display?
- What banner do you configure if you use the **banner** command without specifying the banner type?
- What is the role of the delimiting character?
- You type the following command at the router: **banner exec this is it**. What will show following a successful login?

Time

About 15 minutes

Lab/Activity

- Configure Banners
- Modify Banners

Section 2.9: Cisco Discovery Protocol (CDP)

Preparation

This section discusses how Cisco devices use the Cisco Discovery Protocol (CDP) to learn and share information about neighboring Cisco devices. Students will learn how to enable and disable CDP on devices and specific interfaces. They will also learn how to configure CDP timers.

CCNA Objectives

- 205. Perform and verify initial switch configuration tasks including remote access management
- 405. Access and utilize the router to set basic parameters
- 406. Connect, configure, and verify operation status of a device interface

Lecture Focus Questions:

- What are the requirements for using CDP?
- You have not yet configured an IP address on a Cisco router, but the interface is up. Will the router be able to use CDP to discover neighboring device information?
- You want to view information about a router that is two hops away? How can you view this information?
- How do you turn off CDP advertisements for a single interface? How do you disable CDP on a router?

Time

About 40 minutes

Lab/Activity

- Exploring CDP
- Configure CDP
- Modify the CDP Configuration
- Find CDP Information

Section 3.1: Connecting Devices

Preparation

This section examines different types of Ethernet cables used for LAN connections. Students will learn the uses for a straight-through Ethernet cable and a crossover Ethernet cable and the pin positions for each.

CCNA Objectives

- 201. Select the appropriate media, cables, ports, and connectors to connect switches to other network devices and hosts
- 403. Select the appropriate media, cables, ports, and connectors to connect routers to other network devices and hosts

Lecture Focus Questions:

- When would you use a crossover cable when connecting to a Cisco device?
- What type of cable do you use to connect two switches?
- What is the SFP slot on a switch used for?
- How does Auto-MDI/MDIX affect cable selection when connecting devices?

Time

About 15 minutes

Section 3.2: Switch Configuration

Preparation

In this section students will learn how to configure basic switch port parameters specifically for the Catalyst 2960 series switch. They will learn how to recognize the switch's activity by the various colored status lights. Students will become familiar with the switch configuration modes and commands. Also discussed, are the commands to view the interface status.

CCNA Objectives

- 205. Perform and verify initial switch configuration tasks including remote access management
- 207. Identify, prescribe, and resolve common switched network media issues, configuration issues, auto negotiation, and switch hardware failures
- 215. Interpret the output of various show and debug commands to verify the operational status of a Cisco switched network.

Lecture Focus Questions:

- What configuration modes are unique to switches?
- How do you identify ports which are administratively shut down?
- What information does the SYST LED provide?

Time

About 40 minutes

Lab/Activity

- Configure Switch Ports
- Exploring Switch Port Status

Section 3.3: TCP/IP Configuration

Preparation

This section examines the configuration settings for a TCP/IP network and the methods used to assign the settings. Students will learn how to configure workstation TCP/IP settings, configure an IP address and default gateway on a switch, and configure a router interface with an IP address.

CCNA Objectives

- 205. Perform and verify initial switch configuration tasks including remote access management
- 304. Implement static and dynamic addressing services for hosts in a LAN environment
- 405. Connect, configure, and verify operation status of a device interface

Lecture Focus Questions:

- What is the minimum amount of information a workstation needs to communicate on a single subnet? What additional configuration values are required for inter-network communications?
- What address range indicates an APIPA address assignment?
- What are the drawbacks to using manual IP address assignments?
- Why does a switch have an IP address? Which interface is assigned the IP address?

Time

About 40 minutes

Lab/Activity

- Configure Workstation Settings
- Configure Switch IP Settings
- Configure Device IP Settings

Section 3.4: DHCP

Preparation

In this section students will learn how the DHCP protocol is used to obtain parameters that are needed for the clients to operate in a network. They will become familiar with common DHCP parameters that can be configured and will learn how to use the Security Device Manager (SDM) interface to configure the DHCP service on a router.

CCNA Objectives

- 302. Explain the operation and benefits of using DHCP and DNS
- 303. Configure, verify and troubleshoot DHCP and DNS operation on a router

Lecture Focus Questions:

- What is the difference between the ARP and RARP protocols?
- What is the difference between the BootP and DHCP protocols?
- What type of information is delivered by DHCP options?
- How can you make sure a specific host gets the same IP address from the DHCP server each time it boots?
- How does the router determine which interfaces will respond to DHCP requests?
- How can you enable DHCP messages to work across subnets?

Time

About 20 minutes

Section 3.5: DNS

Preparation

This section discusses the basics of the Domain Name System (DNS) database. Students will learn the commands to configure DNS services on a router.

CCNA Objectives

- 302. Explain the operation and benefits of using DHCP and DNS
- 303. Configure, verify and troubleshoot DHCP and DNS operation on a router

Time

About 15 minutes

Section 3.6: Routing

Preparation

This section provides an overview of routing protocols used to automatically share and learn routes. Both default routes and static routes are presented. The steps to configuring a routing protocol are discussed as well as the commands for configuring the Routing Information Protocol (RIP). Student will learn the function of the routing table and how to view the routing table. They will also learn how to configure static routes and RIP routing.

CCNA Objectives

- 401. Describe basic routing concepts (including: packet forwarding, router lookup process)
- 404. Configure, verify, and troubleshoot RIPv2
- 408. Perform and verify routing configuration tasks for a static or default route given specific routing requirements

Lecture Focus Questions:

- What is the difference between a static and a default route?
- In what cases would you use a static route rather than a routing protocol?
- What does a route to network 0.0.0.0 identify?
- What happens to a packet that does not match any of the routes in a routing table?
- What does an asterisk (*) on a route indicate?
- How does a router choose between two routes to the same destination network?

Time

About 60 minutes

Lab/Activity

- Configure Static Routes
- Enable RIP
- Configure RIP Routing
- Find Routing Table Information

Section 3.7: Verifying TCP/IP Configuration

Preparation

In this section students will learn how to verify TCP/IP configurations. They will become familiar with different types of Internet Control Message Protocol (ICMP) messages. Hosts use ICMP to send error messages to other hosts. **Ping, Traceroute,** and **Telnet** can be used to verify connectivity between devices. Students will examine common symptoms and suggested remedies for communication problems.

CCNA Objectives

- 110. Identify and correct common network problems at layers 1, 2, 3 and 7 using a layered model approach
- 206. Verify network status and switch operation using basic utilities (including: ping, traceroute, telnet, SSH, arp, ipconfig), SHOW & DEBUG commands
- 309. Identify and correct common problems associated with IP addressing and host configurations
- 407. Verify device configuration and network connectivity using ping, traceroute, telnet, SSH or other utilities
- 414. Verify network connectivity (including: using ping, traceroute, and telnet or SSH)

Lecture Focus Questions:

- What are the differences and similarities between **ping** and **traceroute**?
- You can ping a device but can't open a Telnet session with that device. What is the problem?
- Which utility can you use to test upper-layer protocols as well as lower-layer connectivity?
- Which utility would you use on a workstation to view the IP address received from the DHCP server?

Time

About 40 minutes

Lab/Activity

- Exploring TCP/IP Communications

Section 3.8: LAN Segmentation

Preparation

This section covers the basics of using LAN segmentation to increase network performance and reduce congestion. Students will become familiar with collision and broadcast domains and that segmentation may increase the number of both domains. Voice over IP (VoIP) provides telephony signals as digital audio encapsulated in a data packet stream over IP.

CCNA Objectives

- 106. Describe the impact of applications (Voice Over IP and Video Over IP) on a network
- 203. Explain network segmentation and basic traffic management concepts

Lecture Focus Questions:

- 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?
- 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?
- What happens to the collision and broadcast domains as you segment the network with routers?
- Which device provides guaranteed bandwidth between devices?
- Which device can you use to filter broadcast traffic?
- What is the relationship between delay and jitter with VoIP?
- What special features might you need on a switch to support VoIP?

Time

About 25 minutes

Section 4.1: Wireless Standards

Preparation

This section discusses using radio waves for data transmission. The students will learn about the four organizations that influence wireless standards and the characteristic descriptions of radio waves. Students will compare the specifications of four wireless standards.

CCNA Objectives

- 501. Describe standards associated with wireless media (including: IEEE WI-FI Alliance, ITU/FCC)

Lecture Focus Questions:

- How are the FCC and ITU-R similar?
- How are FHSS and DSSS different?
- What are the differences between 802.11a and 802.11g specifications?
- What is the difference between channel bonding and dual band?
- When should you implement a dual band access point?
- What improvements are included with 802.11n standards that improve speed and distance?

Time

About 15 minutes

Section 4.2: Wireless Infrastructure

Preparation

This section provides an overview of wireless networking methods; Ad Hoc and Infrastructure. Students will learn the process of Carrier Sense Access/Collision Avoidance (CSMA/CA) to control media access and avoid collision. Half-duplex provides a shared, two-way communication between devices allowing both to take turns sending and receiving.

CCNA Objectives

- 502. Identify and describe the purpose of the components in a small wireless network. (Including: SSID, BSS, ESS)
- 503. Identify the basic parameters to configure on a wireless network to ensure that devices connect to the correct access point

Lecture Focus Questions:

- Under which circumstances might you choose an ad hoc wireless network?
- What is an SSID? How does the BSSID differ from the SSID?
- How many access points are in a BSS and an ESS?
- What media access method do wireless networks use? How does this differ from the media access used on Ethernet?

Time

About 15 minutes

Section 4.3: Wireless Security

Preparation

This section explores security on a wireless network. The students will become familiar with different kinds of wireless security attacks and countermeasures to secure the wireless network against these attacks. They will also learn about wireless standards and practices to put into effect to protect the wireless network.

CCNA Objectives

- 504. Compare and contrast wireless security features and capabilities of WPA security (including: open, WEP, WPA-1/2)

Lecture Focus Questions:

- What is the difference between a rogue access point and a spoofed access point?
- What does open authentication use to authenticate a device?
- How does 802.1x authentication differ from shared key authentication?
- What improvements did WPA make to overcome the weaknesses of WEP?
- You have an older wireless access point that supports WEP. You would like to use WPA instead. What action would you typically take to do this? What would you need to do to use WPA2?
- Which wireless security standards use Temporal Key Integrity Protocol (TKIP) encryption?
- What are three actions you should take to increase the security of a wireless access point?
- How does MAC address filtering improve security of a wireless access point? Why is this action by itself insufficient to prevent unauthorized access?

Time

About 25 minutes

Section 4.4: Wireless Configuration

Preparation

This section discusses implementing a wireless configuration. Students will learn to configure the basic options and security on a wireless access point and configure a wireless client connection.

CCNA Objectives

- 503. Identify the basic parameters to configure on a wireless network to ensure that devices connect to the correct access point
- 505. Identify common issues with implementing wireless networks. (Including: Interface, misconfiguration)

Lecture Focus Questions:

- You have a network with two wireless access points. Should the SSID be the same or different? Should the channel on each be the same or different?
- Where is the best place to locate your wireless access point?
- What type of objects might obstruct radio frequency wireless transmissions?
- How does range and antenna placement affect wireless networks?
- When should you use open authentication on your wireless network?
- What authentication type should you not use when using WEP for encryption?
- What is required in order to implement 802.1x authentication?

Time

About 30 minutes

Lab/Activity

- Configure a Wireless Client

Section 5.1: Subnet Operations

Preparation

In this section students will learn how to perform the following subnet operations:

- Given a subnet mask and an IP address, find the network address.
- Given a network address and a number of desired subnets and hosts, select the subnet mask.
- From a network address and subnet mask, identify valid subnet addresses.
- From a subnet address and mask, identify the range of valid host addresses.

Students will learn how to convert decimal and binary numbers and how to find the exponential values of 2. They will also learn how to identify solutions to common subnetting tasks.

CCNA Objectives

- 305. Calculate and apply an addressing scheme including VLSM IP addressing design to a network

Lecture Focus Questions:

- When should you use the 2^n-2 formula to determine the amount of available subnets?
- What is the magic number and how can it help while subnetting a network?
- What is the difference between a classful and classless subnet mask?

Time

About 70 minutes

Section 5.2: Subnet Design

Preparation

This section discusses the process to subnet design. Students will learn how to select and configure subnet addresses, masks, and host addresses.

CCNA Objectives

- 305. Calculate and apply an addressing scheme including VLSM IP addressing design to a network

Lecture Focus Questions:

- How does authentication differ from authorization?
- What are the differences between administrative, physical, and technical access controls?
- How are corrective and recovery access controls similar?
- How do preventive access controls differ from deterrent access controls?
- How do directory services benefit a computer network?
- What services do most directory services perform?

Time

About 40 minutes

Lab/Activity

- Configure Subnet Masks 1
- Configure Subnet Masks 2

Section 5.3: Route Summarization

Preparation

In this section students will become familiar with route summarization. Students will learn how to select the appropriate subnet addresses and masks for summarization. They will also learn how to identify the summarized route.

CCNA Objectives

- 306. Determine the appropriate classless addressing scheme using VLSM and summarization to satisfy addressing requirements in a LAN/WAN environment

Lecture Focus Questions:

- What are the advantages of route summarization?
- If automatic route summarization is used, how does the router determine which routes to summarize? What route becomes the summarized network?
- Which routing protocol does not support automatic route summarization?
- Why do discontiguous networks pose a problem for route summarization?

Time

About 30 minutes

Lab/Activity

- Exploring Auto-Summarization

Section 6.1: Wide Area Networks

Preparation

In this section the students will learn how Wide Area Networks (WANs) are used to connect sites. WAN types discussed are point-to-point, circuit switching, and packet switching. Students will become familiar with the components of a WAN structure and common WAN transmission carriers.

CCNA Objectives

- 111. Differentiate between LAN/WAN operation and features
- 801. Describe different methods for connecting to a WAN

Lecture Focus Questions:

- How does a packet *switched* WAN service differ from a circuit *switched* WAN service?
- Who is responsible for the local loop, the customer or the service provider?
- What is the significance of the *demarc*?
- What is the difference between the Data Terminal Equipment (DTE) and Data Communication Equipment (DCE)?
- Which WAN services use already-installed telephone lines?
- What media type is used by ATM?

Time

About 15 minutes

Section 6.2: WAN Connections

Preparation

This section discusses the details to consider when selecting WAN connections. Several connector types and ports are presented. The encapsulation method that is selected depends upon the WAN service and connection method. Students will learn the commands to configure the router. They will also practice configuring a serial interface for a basic WAN connection and a serial connection between back-to-back routers.

CCNA Objectives

- 403. Select the appropriate media, cables, ports, and connectors to connect routers to other network devices and hosts
- 406. Connect, configure, and verify operation status of a device interface
- 801. Describe different methods for connecting to a WAN
- 802. Configure and verify a basic WAN serial connection

Lecture Focus Questions:

- Which interface provides clocking in the WAN connection?
- How is a DB-60 connector different from a Smart Serial connector?
- When would you use an RJ-48 connector?
- What is the default encapsulation protocol on Cisco routers?
- When should you use PPP as the encapsulation protocol?

Time

About 40 minutes

Lab/Activity

- Exploring Serial Interface Status
- Configure Back-to-back Routers

Section 6.3: PPP

Preparation

In this section students will learn how to configure PPP encapsulation on serial links, and configure PAP authentication including username and password combinations.

CCNA Objectives

- 801. Describe different methods for connecting to a WAN
- 802. Configure and verify a basic WAN serial connection
- 806. Configure and verify a PPP connection between Cisco routers

Lecture Focus Questions:

- What is the purpose of LCPs in PPP communications?
- Which authentication method is more secure, PAP or CHAP?
- How do you configure the password used with PPP authentication?

Time

About 35 minutes

Lab/Activity

- Configure PPP

Section 6.4: Network Address Translation (NAT)

Preparation

Students will learn the basics of Network Address Translation (NAT). NAT is used to connect a private network to the Internet by translating the public address of the NAT router.

CCNA Objectives

- 706. Explain the basic operation of NAT
- 707. Configure NAT for given network requirements

Lecture Focus Questions:

- What are the IP address ranges for private networks?
- Which network devices are most likely to be assigned a public IP address?
- What benefits come from using NAT?
- What is the difference between an inside global address and an outside global address?
- What is overloading, and why is it important in a NAT configuration?
- How is PAT different than NAT?

Time

About 40 minutes

Section 6.5: WAN Troubleshooting

Preparation

This section explores tips for troubleshooting WAN communications. Students will become familiar with commands used to view the status of the interface. They will practice troubleshooting serial connections.

CCNA Objectives

- 407. Verify device configuration and network connectivity using ping, traceroute, telnet, SSH or other utilities
- 414. Verify network connectivity (including: using ping, traceroute, and telnet or SSH)
- 804. Troubleshoot WAN implementation issues

Lecture Focus Questions:

- What are possible causes of Layer 1 problems on a serial connection?
- Which interface status indicates a Layer 2 connection problem?
- What steps can you take to correct a Layer 2 problem?
- How does having an incorrect interface IP address affect a WAN connection?
- A ping test to a remote router succeeds, but the Telnet connection fails. What can you assume about the router configuration? Can the router route packets?
- You have Layer 2 connectivity to a remote device but full connectivity does not exist. What steps can you take to identify the problem?

Time

About 50 minutes

Lab/Activity

- View Serial Interface Status
- Troubleshoot a Serial Connection 1
- Troubleshoot a Serial Connection 2
- Troubleshoot a Serial Connection 3
- Troubleshoot a Serial Connection 4

Section 7.1: Virtual LANs (VLANs)

Preparation

This section examines using Virtual LANs (VLANs) to configure ports on the switch to provide segmentation, flexibility, and security. Common VLAN configuration commands are discussed and students will learn how to create VLANs and assign switch ports to a VLAN.

CCNA Objectives

- 208. Describe enhanced switching technologies
- 209. Describe how VLANs create logically separate networks and the need for routing between them
- 210. Configure, verify, and troubleshoot VLANs

Lecture Focus Questions:

- What are two advantages to creating VLANs on your network?
- You have two VLANs configured on a single switch. How many broadcast domains are there? How many collision domains are there?
- What happens if two devices on the same switch are assigned to different VLANs?

Time

About 30 minutes

Lab/Activity

- Create VLANs

Section 7.2: Trunking

Preparation

In this section students will learn about trunking, which is used when you connect two switches together. It is used to configure VLANs that span multiple switches. Students will become familiar with commands for configuring and monitoring trunking on a switch. They will configure a switch port as an access port or a trunk port and configure dynamic trunking modes.

CCNA Objectives

- 208. Describe enhanced switching technologies
- 211. Configure, verify, and troubleshoot trunking on Cisco switches

Lecture Focus Questions:

- Why is trunking important to VLAN configuration?
- Which trunking protocols are supported on a Cisco 2960 switch? Which protocol is an industry standard?
- What protocol does a Cisco switch use to automatically detect trunk ports?
- By default, traffic from which VLANs are allowed on trunk ports?
- A trunk port is set to **dynamic desirable**. What configurations on other switches are allowed so the port enters a trunking state?

Time

About 40 minutes

Lab/Activity

- Configure Trunking

Section 7.3: VLAN Trunking Protocol (VTP)

Preparation

This section discusses how the VLAN Trunking Protocol (VTP) is used to manage VLANs in a multi-switch network by maintaining a consistent database of configuration changes and propagating changes to other switches in the network. Switches are placed in one of three configuration modes; server, client, or transparent. In this section students will become familiar with common VTP commands and the function of each. They will learn how to configure the VTP mode on a switch and set VTP domain and password parameters.

CCNA Objectives

- 208. Describe enhanced switching technologies
- 213. Configure, verify, and troubleshoot VTP

Lecture Focus Questions:

- What is the function of the VTP protocol?
- A switch in transparent mode. Will the switch learn VLAN information from other switches? Will the switch propagate information to other switches?
- Where does a switch in client mode save VLAN information?
- When would a switch in client mode update VLAN information on a switch in server mode?
- Why is the default VTP mode of a switch important?
- What conditions must be met before two switches will share VLAN information using VTP?

Time

About 40 minutes

Lab/Activity

- Configure VTP Settings

Section 7.4: Spanning Tree

Preparation

In this section students will learn how Spanning Tree is used to provide a loop-free path through a network. Rapid Spanning Tree will converge much faster than Spanning Tree. Per-VLAN Spanning allows for multiple pathways with control along the VLAN boundaries by configuring which ports will be active for which VLANs and which ports will be blocking.

CCNA Objectives

- 208. Describe enhanced switching technologies
- 214. Configure, verify, and troubleshoot RSTP operation

Lecture Focus Questions:

- What is the purpose of the spanning tree protocol?
- What is the role of designated bridges?
- What are BPDUs and when are they exchanged?
- A switch port is in the blocking state. Will it learn MAC addresses? Will it send and receive frames?
- A switch port is in the learning state. Will it learn MAC addresses? Will it send and receive frames?
- A switch port is identified as a backup port. What state is it in?
- What advantages are added to spanning tree with the edge port type definition? How does this improve performance?
- How does PVST+ differ from Rapid PVST+?

Time

About 70 minutes

Section 7.5: Spanning Tree Configuration

Preparation

This section discusses commands that can be used to configure spanning tree. Students will learn how to configure the spanning tree mode and configure UplinkFast on access ports.

CCNA Objectives

- 208. Describe enhanced switching technologies
- 214. Configure, verify, and troubleshoot RSTP operation

Time

About 35 minutes

Section 7.6: EtherChannel

Preparation

In this section students will learn how EtherChannel uses multiple links to increase bandwidth and provide redundant links. They will learn how to enable EtherChannel by using the **channel-group** command.

CCNA Objectives

- 208. Describe enhanced switching technologies

Lecture Focus Questions:

- What advantages does the EtherChannel feature provide?
- Why must EtherChannel be used to create multiple links between switches that can be used at the same time? How does EtherChannel interact with spanning tree?

Time

About 5 minutes

Section 7.7: Inter-VLAN Routing

Preparation

In this section students will learn the basics of configuring subinterfaces and ISL encapsulation to enable inter-VLAN routing on a router.

CCNA Objectives

- 208. Describe enhanced switching technologies
- 209. Describe how VLANs create logically separate networks and the need for routing between them
- 212. Configure, verify, and troubleshoot interVLAN routing

Lecture Focus Questions:

- What is required before members of two VLANs can communicate with each other?
- Why doesn't trunking enable inter-VLAN communication?
- What method is used to allow a single router to perform inter-VLAN routing using a single physical interface?
- What protocol do you configure on a router to enable inter-VLAN routing?

Time

About 15 minutes

Section 8.1: Access List Concepts

Preparation

This section discusses how routers use access lists to control traffic. Students will learn how to calculate the wildcard mask value to use in an access list statement.

CCNA Objectives

- 701. Describe the purpose and types of ACLs

Lecture Focus Questions:

- You want to create an access list that restricts traffic from host 12.0.15.166. What type of access list can you use?
- You want to create an access list that restricts ICMP traffic. What type of access list would you choose?
- How many access lists can be applied to a single interface?
- What is the last statement in every access list?
- How is a wildcard mask related to the subnet mask?
- What does a 0 in a wildcard mask indicate?

Time

About 25 minutes

Section 8.2: Configuring Access Lists

Preparation

This section provides the details of how to configure access lists. Students will learn how to configure both standard IP and extended IP access lists. They will learn how to construct access list statements, create an access list, and apply it to an interface.

CCNA Objectives

- 702. Configure and apply ACLs based on network filtering requirements
- 703. Configure and apply an ACLs to limit telnet and SSH access to the router
- 704. Verify and monitor ACLs in a network environment
- 705. Troubleshoot ACL issues

Time

About 75 minutes

Lab/Activity

- Restrict Telnet and SSH Access
- Permit Traffic
- Block Source Hosts
- Configure Allowed Networks
- Create Access Lists Statements

Section 8.3: Access List Implementation

Preparation

This section explores using access list implementation to allow or deny the flow of packets between networks. Students will learn how to create an access list according to the customer requirements and apply an existing access list to the appropriate router and interface.

CCNA Objectives

- 702. Configure and apply ACLs based on network filtering requirements
- 703. Configure and apply an ACLs to limit telnet and SSH access to the router
- 704. Verify and monitor ACLs in a network environment
- 705. Troubleshoot ACL issues

Lecture Focus Questions:

- How do you identify where to place an access list (on a specific router, a specific interface, and a specific direction)?
- Why should each access list contain at least one allow statement?

Time

About 15 minutes

Lab/Activity

- Block Invalid Addresses
- Allow Only Specific Services

Section 9.1: Routing Protocols

Preparation

This section discusses how routers use routing protocols to dynamically discover routes, build routing tables, and make decisions about how to send packets through the internetwork. Students will become familiar with both vector routing and link state routing..

CCNA Objectives

- 401. Describe basic routing concepts
- 411. Compare and contrast methods of routing and routing protocols

Lecture Focus Questions:

- What is the difference between a routing protocol and a routed protocol?
- What is the difference between distance vector routing and link state routing?
- What is a flash update?
- What is poison reverse?
- Why don't link state protocols use hold down timers, split horizon, or poison reverse?
- What is in an LSP?
- What is a designated router?

Time

About 30 minutes

Section 9.2: RIP

Preparation

This section provides an overview of using the Routing Information Protocol (RIP) to reduce the amount of administration required for maintaining routes between small to medium sized networks. The steps to configuring a routing protocol are presented as well as the commands for configuring RIP. Students will learn how to enable IP routing and configure RIP networks.

CCNA Objectives

- 404. Configure, verify, and troubleshoot RIPv2

Lecture Focus Questions:

- What are the differences between RIP version 1 and RIP version 2?
- What is the metric used with RIP? What is the maximum metric value?
- Can RIP v2 do load balancing across multiple paths? If so, what are the limitations?
- How does RIP v2 perform auto-summarization?

Time

About 20 minutes

Lab/Activity

- Configure RIP Routing

Section 9.3: OSPF

Preparation

This section explores the popular Open Shortest Path First (OSPF) routing protocol commonly used on larger networks. Students will learn how to configure OSPF routing by using the OSPF commands.

CCNA Objectives

- 412. Configure, verify, and troubleshoot OSPF

Lecture Focus Questions:

- Must the process ID number used on different OSPF routers match?
- What is Area 0 in an OSPF implementation?
- How many areas can a single subnet be in?
- How does the DR and BDR reduce network traffic?
- When is the DR not used?
- How is the DR elected? How can you ensure that a specific device becomes the DR?
- What conditions must be met before two routers running OSPF will share information?

Time

About 60 minutes

Lab/Activity

- Enable OSPF
- Exploring OSPF
- Configure OSPF Routing

Section 9.4: EIGRP

Preparation

This section discusses configuring Enhanced IGRP (EIGRP). Students will learn the commands to configure EIGRP routing and how to use show commands to monitor EIGRP routing.

CCNA Objectives

- 413. Configure, verify, and troubleshoot EIGRP

Lecture Focus Questions:

- What type of routing protocol is EIGRP?
- What is the metric used with EIGRP?
- How does the router calculate the feasible distance?
- What condition must be met for a route to become a feasible successor route?
- What is the difference between a feasible successor and a successor?
- How does EIGRP determine how many paths to keep in its topology database?
- What conditions must be met before two routers running OSPF will share information?

Time

About 30 minutes

Lab/Activity

- Enable EIGRP

Section 9.5: Routing Protocol Comparison

Preparation

In this section students will compare the characteristics of three routing protocols; RIP, OSPF, and EIGRP. Students will also learn that when multiple routes exist to a destination the administrative distance is used to determine which route will be taken.

CCNA Objectives

- 411. Compare and contrast methods of routing and routing protocols

Lecture Focus Questions:

- Which routing protocols support route summarization and variable length subnet masks (VLSM)?
- Which routing protocols are public-standard protocols?
- Which routing protocol uses areas for configuration?
- Which routing protocol uses wildcard masks for configuration?
- If a router learns of a route to network B through both EIGRP and OSPF, which route will it prefer?

Time

About 10 minutes

Section 10.1: Troubleshooting Routing

Preparation

In this section students will learn tips for troubleshooting routing, verifying routing protocol configuration, and handling route summarization issues.

CCNA Objectives

- 415. Troubleshoot routing issues

Lecture Focus Questions:

- The **show ip route** command on a router does not show two directly-connected networks. What conditions might be causing this problem?
- When might static routes configured on a router not show in the routing table?
- What does an asterisks (*) next to a route in the routing table indicate?
- How can you tell how many paths a routing protocol can use for load balancing?
- For the **show ip protocols** command, what does the **Routing for Networks** section indicate?
- Why might subnetted routes be missing from the routing table? Which settings control this behavior?
-

Time

About 15 minutes

Section 10.2: Troubleshooting RIP

Preparation

This section covers troubleshooting RIP. Students will learn how to interpret the output of the **debug ip rip** command to troubleshoot RIP routing. They will also learn how to verify the RIP configuration of a network and correct any problems to restore full connectivity.

CCNA Objectives

- 404. Configure, verify, and troubleshoot RIPv2
- 415. Troubleshoot routing issues

Time

About 35 minutes

Lab/Activity

- Troubleshoot RIP 1
- Troubleshoot RIP 2
- Troubleshoot RIP 3

Section 10.3: Troubleshooting OSPF

Preparation

In this section students will become familiar with troubleshooting OSPF routers. Students will learn how to use **show** commands to verify the OSPF operation. They will also learn how to verify the OSPF configuration of a network and correct any problems to restore full connectivity.

CCNA Objectives

- 412. Configure, verify, and troubleshoot OSPF
- 415. Troubleshoot routing issues

Time

About 30 minutes

Lab/Activity

- Troubleshoot OSPF 1
- Troubleshoot OSPF 2

Section 10.4: Troubleshooting EIGRP

Preparation

This section examines troubleshooting EIGRP. Students will learn show commands to verify the EIGRP operation and how to interpret the output of the **show ip eigrp topology all-links** command. They will also learn how to verify the EIGRP configuration of a network and correct any problems to restore full connectivity.

CCNA Objectives

- 413. Configure, verify, and troubleshoot EIGRP
- 415. Troubleshoot routing issues

Time

About 35 minutes

Lab/Activity

- Troubleshoot EIGRP 1
- Troubleshoot EIGRP 2

Section 11.1: Frame Relay Concepts

Preparation

In this section the students will learn about Frame Relay, one of the most common WAN protocols. Students will learn how Frame Relay networks send data and over what connection lines they operate. Frame relay addressing and configuration methods are also presented. This section contains a multitude of acronyms. Make sure that the students understand the following acronyms, what they stand for, and their function:

- DTE (Data Terminal Equipment) – routers are the DTE component that receives the clocking speed sent from the Frame Relay Cloud.
- DCE (Data Communications Equipment) – generates and sends clock speeds from the Frame Relay providers' switches.
- CIR (Committed Information Rate) – provider guaranteed minimum access rate.
- VC (Virtual Circuit) – connection between your router and the destination.
- PVC (Permanent Virtual Circuit) – most common Virtual Circuit.
- SVC (Switched Virtual Circuit) – not commonly available from providers.
- DLCI (Data Link Connection Identifier) is a number that represents the connection between two frame relay devices.
- LMI (Local Management Interface) - router communicates via Frame Relay to provider's switch
- FECN (Forward Explicit Congestion Notification) notifies forward devices that the rate will slow
- BECN (Backward Explicit Congestion Notification) notifies the backwards device to slow down
- DE (Discard Eligible) packets with the discard eligible bit set are the first to be dropped in case of congestion.

CCNA Objectives

- 801. Describe different methods for connecting to a WAN
- 803. Configure and verify Frame Relay on Cisco routers

Lecture Focus Questions:

- What is the CIR?
- What does *locally significant* mean in relation to the DLCI number?
- What functions are performed by LMI?
- What is the difference between a point-to-point and a multipoint link?
- When are the FECN and BECN bits set? What do each mean?
- How does inverse ARP simplify Frame Relay configuration?
- What is a *subinterface*?

Time

About 30 minutes

Section 11.2: Enabling Frame Relay

Preparation

In this section students will learn the commands to configure Frame Relay on Cisco routers by setting the encapsulation type and letting the router discover the LMI type and DLCI values automatically. They will also learn the commands to configure frame relay to use inverse arp for address discovery and the commands to display DLCI and IP information to verify that Frame Relay is functioning properly.

CCNA Objectives

- 803. Configure and verify Frame Relay on Cisco routers

Time

About 20 minutes

Lab/Activity

- Configure Frame Relay

Section 11.3: Address Mapping

Preparation

In this section students will learn the commands to manually set an LMI type, disable inverse arp, and configure static Frame Relay mappings.

CCNA Objectives

- 803. Configure and verify Frame Relay on Cisco routers

Time

About 10 minutes

Lab/Activity

- Configure Static Mappings

Section 11.4: Subinterfaces

Preparation

Students will learn how subinterfaces are used to overcome the limitations of split horizon when sending updates out the same interface. They will configure both a multipoint subinterface and point-to-point subinterface.

CCNA Objectives

- 803. Configure and verify Frame Relay on Cisco routers

Time

About 25 minutes

Lab/Activity

- Configure Point-to-Point Frame Relay
- Configure Multipoint Frame Relay

Section 11.5: Troubleshooting Frame Relay

Preparation

This section explores the show commands used to troubleshoot a Frame Relay configuration by viewing Frame Relay information on the router.

CCNA Objectives

- 803. Configure and verify Frame Relay on Cisco routers

Lecture Focus Questions:

- Which command would you use to view the DLCI numbers for each interface?
- Why wouldn't you use the DLCI number included in the show interfaces command to identify assigned DLCIs?
- Which commands can you use to view the LMI type used on your router?
- Which Frame Relay encapsulation type should you use when connecting to routers from different vendors?

Time

About 15 minutes

Section 12.1: IPv6 Concepts

Preparation

This section examines the advantages of the new IP addressing version IPv6 which will replace the IPv4. Students will become familiar with the 128-bit addressing scheme for IPv6 address including the 64-bit prefix and 64-bit interface ID. The organization of Global routing information will help to increase the speed of communication. IPv4 supports two address types; unicast and multicast. IPv6 will support both these and an additional address type called anycast.

CCNA Objectives

- 308. Describe IPv6 addresses

Lecture Focus Questions:

- How does IPv6 help route summarization on the Internet?
- How many hexadecimal numbers are in an IPv6 address?
- Which of the following can be left out of an IPv6 address: leading zeros or trailing zeros?
- How many bits do most organizations have for creating subnets with IPv6 addresses?
- How do you transform a MAC address into an IPv6 interface ID?
- What does IPv6 use instead of a broadcast address?
- How can you easily identify IPv6 multicast addresses?
- What does the special address FF02::2 mean? When is address ::1 used?

Time

About 35 minutes

Section 12.2: IPv6 Implementation

Preparation

In this section students will learn the methods used to configure an IPv6 address. Various implementation methods are presented for deploying IPv6. Students will learn how to configure an IP6 address and enable IPv6 support on a Cisco router.

CCNA Objectives

- 307. Describe the technological requirements for running IPv6 in conjunction with IPv4

Lecture Focus Questions:

- How does a host get its IPv6 address when using stateless autoconfiguration?
- What information does the DHCP server provide when using stateless DHCPv6?
- What address does a host use to request an address from a DHCP server?
- What limitations does ISATAP have for IPv6 implementation?
- Which IPv6 tunneling methods work through NAT?
- What is the only method possible to enable an IPv6-only host to communicate with an IPv4-only host?

Time

About 30 minutes

Section 12.3: DHCP and NAT

Preparation

This section discusses the steps used to configure DHCP from the command line. Students will also learn how to configure NAT interfaces, static NAT, and NAT pools.

CCNA Objectives

- 303. Configure, verify and troubleshoot DHCP and DNS operation on a router
- 707. Configure NAT for given network requirements
- 708. Troubleshoot NAT issues

Lecture Focus Questions:

- How does the DHCP service determine on which interfaces to listen for DHCP requests?
- How is an access list used in NAT configuration?
- How do you link a NAT address pool to an access list and an interface?
- What parameter must you use in your NAT configuration if you have more private hosts than public IP addresses?
- Which NAT configuration method do you use to associate a specific outside IP address with an inside host?

Time

About 45 minutes

Lab/Activity

- Configure Overloaded PAT
- Configure Dynamic NAT
- Configure Static NAT

Section 13.1: Network Security

Preparation

This section discusses different types of network security threats and the solutions to implement to protect the network from the various threats. The instructor stresses that the most important thing to do is to first develop a Network Security Policy. This policy is used to create a continual process to secure, monitor, test and manage network resources. He recommends a policy based on the RFC 2106 model.

CCNA Objectives

- 601. Describe today's increasing network security threats and explain the need to implement a comprehensive security policy to mitigate the threats
- 602. Explain general methods to mitigate common security threats to network devices, hosts, and applications
- 603. Describe the functions of common security appliances and applications

Lecture Focus Questions:

- What is *social engineering*? What is the best defense against social engineering?
- How does a worm differ from a boot sector virus? A Trojan horse?
- How are Denial of Service (DoS) attacks a security threat?
- In addition to implementing virus scanning software, what must you do to ensure that you are protected from the latest virus variations?
- Which types of attacks are directed against passwords?
- How does a firewall protect a network?
- What is an IPS and how does it differ from an IDS?
- What are the benefits of using centralized authentication?

Time

About 40 minutes

Section 13.2: Network Hardening

Preparation

This section provides an overview of general actions to harden a network by securing devices and software to reduce the security exposure and tighten security controls. It also provides the details of how to secure a network by configuring a Cisco device to accept SSH remote connections.

CCNA Objectives

- 602. Explain general methods to mitigate common security threats to network devices, hosts, and applications
- 604. Describe security recommended practices including initial steps to secure network devices

Lecture Focus Questions:

- What is the most important method of protecting network devices?
- What measures should you take to increase the security of remote connections to your router?
- What benefits come from disabling the broadcast of CDP information?
- How do banners add to the security of a device?
- Why is SSH more secure than Telnet?

Time

About 25 minutes

Section 13.3: Switch Port Security

Preparation

This section explores using switch port security to control which devices are allowed to communicate through a given switch port. Port Security uses the MAC address to identify allowed and denied devices. MAC addresses are stored in RAM in a table, and are identified with the port and by one of the following MAC address types: SecureConfigured, SecureDynamic, and Secure Sticky. Three types of actions can be configured to occur on the switch when a violation occurs; protect, restrict and shutdown. In this section, students will learn the commands to configure and monitor port security.

CCNA Objectives

- 216. Implement basic switch security
- 604. Describe security recommended practices including initial steps to secure network devices

Lecture Focus Questions:

- How does switch port security increase the security of your network?
- What does the **sticky** keyword do when used with the **switchport port-security** command?
- What can you do to save sticky addresses?
- How does switchport security differ from an access list?
- How does using VoIP effect switchport security settings?
- What is the difference between the **protect** and **restrict** violation actions?
- How does a switch identify which MAC addresses to allow if you do not manually configure the allowed addresses?

Time

About 45 minutes

Section 13.4: Virtual Private Networks (VPNs)

Preparation

In this section students will learn the basics of using a Virtual Private Network (VPN) to protect IP traffic on a TCP/IP network through the use of encryption. Some of the most common VPN security technologies include:

- Internet Protocol Security (IPSec)
- Secure Sockets Layer (SSL)
- Transport Layer Security (TLS)

Students will learn which types of VPN are available to use for a site-to-site solution and which are available to use for a remote access solution.

CCNA Objectives

- 805. Describe VPN technology

Lecture Focus Questions:

- What is the difference between confidentiality and integrity?
- Which VPN technology is commonly used on Web servers?
- What is the main difference between a site-to-site VPN and a remote access VPN?
- Which IPSec protocol provides data confidentiality?
- Which IPSec mode is used for host-to-host communications?
- What are the client requirements for operating in full tunnel mode with the AnyConnect VPN Client? What advantages does full tunnel mode provide over the other modes?
- Which Cisco SSL VPN mode would you choose for a public computer? Why?

Time

About 40 minutes

Practice Exams

Preparation

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 100. Networking Concepts are grouped together and presented in practice exam *100. Networking Concepts, All Questions*. Students will typically take about 60-90 minutes to complete each of the following practice exams.

100. Networking Concepts, All Questions (59 questions)
200. Switching, All Questions (135 questions)
300. IP Addressing, All Questions (73 questions)
400. Routing All Questions (155 questions)
500. Wireless, All Questions (28 questions)
600. Security, All Questions (42 questions)
700. ACLs and NAT, All Questions (48 questions)
800. WANs, All Questions (52 questions)

The *Certification Practice Exam* consists of 60 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 test.