الاسم:احمد محمد الطواب محمد

Level:4

Ccna1 traning Report

Dr:ehab Elshimy

Chapter 1

Networking Today

chapter Objective: Explain the advances in modern technologies.

Topics Objective

1-Networks Affect our Lives: Explain how networks affect our daily lives.

2- Network Components :Explain how host and network devices are used.

3- Network Representations and Topologies :Explain network representations and how they are used in network topologies.

4- Common Types of Networks: Compare the characteristics of common types of networks.

5-Internet Connections: Explain how LANs and WANs interconnect to the internet.

6-Reliable Networks :Describe the four basic requirements of a reliable network.

7- Network Trends: Explain how trends such as BYOD, online collaboration, video, and cloud computing are changing the way we interact.

8-Network Security: Identify some basic security threats and solution for all networks.

9-The IT Professional: Explain employment opportunities in the networking field.

What did I learn in this chapter?

•Through the use of networks, we are connected like never before.

•All computers that are connected to a network and participate directly in network communication are classified as hosts.

•Diagrams of networks often use symbols to represent the different devices and connections that make up a network .

•A diagram provides an easy way to understand how devices connect in a large network.

•The two types of network infrastructures are Local Area Networks (LANs), and Wide Area Networks (WANs).

•SOHO internet connections include cable, DSL, Cellular, Satellite, and Dial-up telephone .

•Business internet connections include Dedicated Leased Line, Metro Ethernet, Business DSL, and Satellite.

•Network architecture refers to the technologies that support the infrastructure and the programmed services and rules, or protocols, that move data across the network.

•There are four basic characteristics of network architecture: Fault Tolerance, Scalability , Quality of Service (QoS), and Security.

•Recent networking trends that affect organizations and consumers: Bring Your Own Device

(BYOD), online collaboration, video communications, and cloud computing.

•There are several common external and internal threats to networks.

•Larger networks and corporate networks use antivirus, antispyware, and firewall filtering, but they also have other security requirements: Dedicated firewall systems, Access control lists (ACL), Intrusion prevention systems (IPS), and Virtual private networks (VPN)

•The Cisco Certified Network Associate (CCNA) certification demonstrates your knowledge of foundational technologies.

Chapter 2

Basic Switch and End Device Configuration

chapter Objective: Implement initial settings including passwords, IP addressing, and default gateway parameters on a network switch and end devices.

Topics Objective

1-Cisco IOS Access :Explain how to access a Cisco IOS device for configuration purposes.

2-IOS Navigation: Explain how to navigate Cisco IOS to configure network devices.

3-The Command Structure :Describe the command structure of Cisco IOS software.

4-Basic Device Configuration: Configure a Cisco IOS device using CLI.

5-Save Configurations: Use IOS commands to save the running configuration.

6-Ports and Addresses :Explain how devices communicate across network media.

7-Configure IP Addressing :Configure a host device with an IP address.

8-Verify Connectivity :Verify connectivity between two end devices.

What did I learn in this chapter?

•All end devices and network devices require an operating system (OS).

•Cisco IOS software separates management access into the following two command modes: User EXEC Mode and Privileged EXEC Mode.

•Global configuration mode is accessed before other specific configuration modes. From global config mode, the user can enter different sub configuration modes.

•Each IOS command has a specific format or syntax and can only be executed in the appropriate mode.

•Basic device configurations- hostname, password, encrypt passwords and banner .

•There are two system files that store the device configuration: startupconfig and running-config.

•IP addresses enable devices to locate one another and establish endto-end communication on the internet. Each end device on a network

must be configured with an IP address.

Chapter 3

Protocols and Models

Chapter Objective: Explain how network protocols enable devices to access local and remote network resources.

Topics Objective

1-The Rules: Describe the types of rules that are necessary to successfully communicate.

2-Protocols: Explain why protocols are necessary in network communication.

3-Protocol Suites :Explain the purpose of adhering to a protocol suite.

4-Standards Organizations :Explain the role of standards organizations in establishing protocols for network interoperability.

5-Reference Models :Explain how the TCP/IP model and the OSI model are used to facilitate standardization in the communication process.

6-Data Encapsulation: Explain how data encapsulation allows data to be transported across the network.

7-Data Access :Explain how local hosts access local resources on a network.

What did I learn in this chapter?

The Rules

•Protocols must have a sender and a receiver.

•Common computer protocols include these requirements: message encoding, formatting

and encapsulation, size, timing, and delivery options.

Protocols

•To send a message across the network requires the use of several protocols.

•Each network protocol has its own function, format, and rules for communications.

Protocol Suites

•A protocol suite is a group of inter-related protocols.

•TCP/IP protocol suite are the protocols used today.

Standards Organizations

• Open standards encourage interoperability, competition, and innovation.

Reference Models

•The two models used in networking are the TCP/IP and the OSI model.

•The TCP/IP model has 4 layers and the OSI model has 7 layers.

Data Encapsulation

•The form that a piece of data takes at any layer is called a protocol data unit (PDU).

•There are five different PDUs used in the data encapsulation process: data, segment, packet，frame, and bits

Data Access

•The Network and Data Link layers are going to provide addressing to move data through the network.

•Layer 3 will provide IP addressing and layer 2 will provide MAC addressing.

•The way these layers handle addressing will depend on whether the source and the destination are on the same network or if the destination is on a different network from the source.

Chapter 4

physical Layer

chapter Objective: Explain how physical layer protocols, services, and network media support communications across data networks.

Topics Objective

1-Purpose of the Physical Layer :Describe the purpose and functions of the physical layer in the network.

2-Physical Layer Characteristics :Describe characteristics of the physical layer.

3-Copper Cabling: Identify the basic characteristics of copper cabling.

4-UTP Cabling :Explain how UTP cable is used in Ethernet networks.

5-Fiber-Optic Cabling :Describe fiber optic cabling and its main advantages over other media.

6-Wireless Media: Connect devices using wired and wireless media.

What did I learn in this chapter?

•Before any network communications can occur, a physical connection to a local network，either wired or wireless, must be established.

•The physical layer consists of electronic circuitry, media, and connectors developed by engineers.

•The physical layer standards address three functional areas: physical components，encoding, and signaling.

•Three types of copper cabling are: UTP, STP, and coaxial cable (coax).

•UTP cabling conforms to the standards established jointly by the TIA/EIA. The electrical characteristics of copper cabling are defined by the Institute of Electrical and Electronics Engineers (IEEE).

•The main cable types that are obtained by using specific wiring conventions are Ethernet Straight-through and Ethernet Crossover.

•Optical fiber cable transmits data over longer distances and at higher bandwidths than any other networking media.

•There are four types of fiber-optic connectors: ST, SC, LC, and duplex multimode LC.

•Fiber-optic patch cords include SC-SC multimode, LC-LC single-mode, ST-LC multimode , and SC-ST single-mode.

•Wireless media carry electromagnetic signals that represent the binary digits of data communications using radio or microwave frequencies. Wireless does have some limitations , including coverage area, interference, security, and the problems that occur with any shared medium.

•Wireless standards include the following: Wi-Fi (IEEE 802.11), Bluetooth (IEEE 802.15) , WiMAX (IEEE 802.16), and Zigbee (IEEE 802.15.4).

• Wireless LAN (WLAN) requires a wireless AP and wireless NIC adapters.

Chapter 5

Number Systems

chapter Objective: Calculate numbers between decimal, binary, and hexadecimal systems.

Topic Objective

1-Binary Number System: Calculate numbers between decimal and binary systems.

2-Hexadecimal Number System :Calculate numbers between decimal and hexadecimal systems**.**

What did I learn in this chapter?

•Binary is a base two numbering system that consists of the numbers 0 and 1, called bits.

•Decimal is a base ten numbering system that consists of the numbers 0 through 9.

•Binary is what hosts, servers, and networking equipment uses to identify each other.

•Hexadecimal is a base sixteen numbering system that consists of the numbers 0 through 9 and the letters A to F.

•Hexadecimal is used to represent IPv6 addresses and MAC addresses.

•IPv6 addresses are 128 bits long, and every 4 bits is represented by a hexadecimal digit for a total of 32 hexadecimal digits.

•To convert hexadecimal to decimal, you must first convert the hexadecimal to binary, then convert the binary to decimal.

•To convert decimal to hexadecimal, you must first convert the decimal to binary and then the binary to hexadecimal.

Chapter 6

Data Link Layer

chapter Objective: Explain how media access control in the data link layer supports communication across networks.

Topic Objective

1- Purpose of the Data Link Layer :Describe the purpose and function of the data link layer in preparing communication for transmission on specific media.

2-Topologies: Compare the characteristics of media access control methods on WAN and LAN topologies.

3-Data Link Frame: Describe the characteristics and functions of the data link frame.

What did I learn in this chapter?

•The data link layer of the OSI model (Layer 2) prepares network data for the physical network .

•The data link layer is responsible for network interface card (NIC) to network interface card communications.

•The IEEE 802 LAN/MAN data link layer consists of the following two sublayers: LLC and MAC.

•The two types of topologies used in LAN and WAN networks are physical and logical.

•Three common types of physical WAN topologies are: point-to-point, hub and spoke, and mesh.

•Half-duplex communications exchange data in one direction at a time. Full-duplex sends and receives data simultaneously.

•In contention-based multi-access networks, all nodes are operating in half-duplex.

•Examples of contention-based access methods include: CSMA/CD for bus-topology Ethernet LANs and CSMA/CA for WLANs.

•The data link frame has three basic parts: header, data, and trailer.

•Frame fields include: frame start and stop indicator flags, addressing, type, control, data, and error detection.

•Data link addresses are also known as physical addresses.

• Data link addresses are only used for link local delivery of frames.

Chapter 7

Ethernet Switching

Chapter Objective: Explain how Ethernet works in a switched network.

Topic Objective

1-Ethernet Frame: Explain how the Ethernet sublayers are related to the frame fields.

2-Ethernet MAC Address: Describe the Ethernet MAC address.

3-The MAC Address Table :Explain how a switch builds its MAC address table and forwards frames.

4-Switch Speeds and Forwarding Methods: Describe switch forwarding methods and port settings available on Layer 2 switch ports.

What did I learn in this chapter?

•Ethernet operates in the data link layer and the physical layer. Ethernet standards define both the Layer 2 protocols and the Layer 1 technologies .

•Ethernet uses the LLC and MAC sublayers of the data link layer to operate .

•The Ethernet frame fields are: preamble and start frame delimiter, destination MAC address , source MAC address, EtherType, data, and FCS.

•MAC addressing provides a method for device identification at the data link layer of the OSI model .

•An Ethernet MAC address is a 48-bit address expressed using 12 hexadecimal digits, or 6 bytes .

•When a device is forwarding a message to an Ethernet network, the Ethernet header includes the source and destination MAC addresses. In Ethernet, different MAC addresses are used for Layer 2 unicast, broadcast, and multicast communications.

•A Layer 2 Ethernet switch makes its forwarding decisions based solely on the Layer 2 Ethernet MAC addresses .

•The switch dynamically builds the MAC address table by examining the source MAC address of the frames received on a port .

•The switch forwards frames by searching for a match between the destination MAC address in the frame and an entry in the MAC address table .

•Switches use one of the following forwarding methods for switching data between network ports: store-and-forward switching or cut-through switching. Two variants of cut-through switching are fast-forward and fragment-free .

•Two methods of memory buffering are port-based memory and shared memory .

• There are two types of duplex settings used for communications on an Ethernet network: full-duplex and half-duplex.

Chapter 8

Network Layer

Topic Objective

1- Network Layer Characteristics: Explain how the network layer uses IP protocols for reliable communications.

2-IPv4 Packet :Explain the role of the major header fields in the IPv4 packet.

3-IPv6 Packet :Explain the role of the major header fields in the IPv6 packet.

4-How a Host Routes :Explain how network devices use routing tables to direct packets to a destination network.

5-Router Routing Tables :Explain the function of fields in the routing table of a router.

What did I learn in this chapter?

•IP is connectionless, best effort, and media independent.

•IP does not guarantee packet delivery.

•IPv4 packet header consists of fields containing information about the packet.

•IPv6 overcomes IPv4 lack of end-to-end connectivity and increased network complexity.

•A device will determine if a destination is itself, another local host, and a remote host.

•A default gateway is router that is part of the LAN and will be used as a door to other networks.

•The routing table contains a list of all known network addresses (prefixes) and where to forward the packet.

•The router uses longest subnet mask or prefix match.

•The routing table has three types of route entries: directly connected networks, remote networks, and a default route.

Chapter 9

Address Resolution

Chapter Objective: Explain how ARP and ND enable communication on a network.

Topic Objective

1-MAC and IP: Compare the roles of the MAC address and the IP address.

2-ARP: Describe the purpose of ARP.

3-Neighbor Discovery :Describe the operation of IPv6 neighbor discovery.

What did I learn in this chapter?

•Layer 2 physical addresses (i.e., Ethernet MAC addresses) are used to deliver the data link frame with the encapsulated IP packet from one NIC to another NIC on the same network.

•If the destination IP address is on the same network, the destination MAC address will be that of the destination device .

•When the destination IP address (IPv4 or IPv6) is on a remote network, the destination MAC address will be the address of the host default gateway (i.e., the router interface).

•An IPv4 device uses ARP to determine the destination MAC address of a local device when it knows its IPv4 address.

•ARP provides two basic functions: resolving IPv4 addresses to MAC addresses and maintaining a table of IPv4 to MAC address mappings.

•After the ARP reply is received, the device will add the IPv4 address and the corresponding MAC address to its ARP table.

•For each device, an ARP cache timer removes ARP entries that have not been used for a specified period of time.

•IPv6 does not use ARP, it uses the ND protocol to resolve MAC addresses .

•An IPv6 device uses ICMPv6 Neighbor Discovery to determine the destination MAC address of a local device when it knows its IPv6 address.

Chapter 10

Basic Router Configuration

Chapter Objective: Implement initial settings on a router and end devices.

Topic Objective

1-Configure Initial Router Settings :Configure initial settings on an IOS Cisco router.

2-Configure Interfaces :Configure two active interfaces on a Cisco IOS router.

3-Configure the Default Gateway :Configure devices to use the default gateway.

What did I learn in this chapter?

•The tasks that should be completed when configuring initial settings on a router.

•Configure the device name.

•Secure privileged EXEC mode.

•Secure user EXEC mode.

•Secure remote Telnet / SSH access.

•Secure all passwords in the config file.

•Provide legal notification.

•Save the configuration.

•For routers to be reachable, the router interfaces must be configured.

•Using the no shutdown command activates the interface. The interface must also be connected to another device, such as a switch or a router, for the physical layer to be active. There are several commands that can be used to verify interface configuration including the show ip interface brief and show ipv6 interface brief, the show ip route and show ipv6 route, as well as show interfaces, show ip interface and show ipv6 interface.

Chapter 11

IPv4 Addressing

Chapter Objective: Calculate an IPv4 subnetting scheme to efficiently segment your network.

Topic Objective

1-IPv4 Address Structure: Describe the structure of an IPv4 address including the network portion, the host portion, and the subnet mask.

2-IPv4 Unicast, Broadcast, and Multicast :Compare the characteristics and uses of the unicast, broadcast and multicast IPv4 addresses.

3-Types of IPv4 Addresses :Explain public, private, and reserved IPv4 addresses.

4-Network Segmentation :Explain how subnetting segments a network to enable better communication.

5-Subnet an IPv4 Network :Calculate IPv4 subnets for a /24 prefix.

What did I learn in this chapter?

•The IP addressing structure consists of a 32-bit hierarchical network address that identifies a network and a host portion. Network devices use a process called ANDing using the IP address and associated subnet mask to identify the network and host portions.

•Destination IPv4 packets can be unicast, broadcast, and multicast.

•There are globally routable IP addresses as assigned by the IANA and there are three ranges

of private IP network addresses that cannot be routed globally but can be used on all internal private networks.

•Reduce large broadcast domains using subnets to create smaller broadcast domains, reduce overall network traffic, and improve network performance.

•Create IPv4 subnets using one or more of the host bits as network bits. However, networks are most easily subnetted at the octet boundary of /8, /16, and /24.

•Larger networks can be subnetted at the /8 or /16 boundaries.

• Use VLSM to reduce the number of unused host addresses per subnet.

•VLSM allows a network space to be divided into unequal parts. Always begin by satisfying the host requirements of the largest subnet. Continue subnetting until the host requirements of the smallest subnet are satisfied .

•When designing a network addressing scheme, consider internal, DMZ, and external requirements. Use a consistent internal IP addressing scheme with a set pattern of how addresses are allocated to each type of device.

Chapter 12

IPv6 Addressing

Chapter Objective: Implement an IPv6 Addressing scheme.

Topic Objective

1-IPv4 Issues: Explain the need for IPv6 addressing.

2-IPv6 Address Representation :Explain how IPv6 addresses are represented.

3-IPv6 Address Types :Compare types of IPv6 network addresses.

4-GUA and LLA Static Configuration :Explain how to Configure static global unicast and link-local IPv6 network addresses.

5-Dynamic Addressing for IPv6 GUAs :Explain how to configure global unicast addresses dynamically.

6-Dynamic Addressing for IPv6 LLAs: Configure link-local addresses dynamically.

7-IPv6 Multicast Addresses :Identify IPv6 addresses.

8-Subnet an IPv6 Network: Implement a subnetted IPv6 addressing scheme.

What did I learn in this chapter?

•IPv4 has a theoretical maximum of 4.3 billion addresses.

•The IETF has created various protocols and tools to help network administrators migrate their networks to IPv6. The migration techniques can be divided into three categories: dual stack ,

tunneling, and translation.

•IPv6 addresses are 128 bits in length and written as a string of hexadecimal values.

•The preferred format for writing an IPv6 address is x:x:x:x:x:x:x:x, with each “x” consisting of four hexadecimal values．

•There are three types of IPv6 addresses: unicast, multicast, and anycast.

•An IPv6 unicast address uniquely identifies an interface on an IPv6-enabled device．

•IPv6 global unicast addresses (GUAs) are globally unique and routable on the IPv6 internet．

•An IPv6 link-local address (LLA) enables a device to communicate with other IPv6-enabled devices on the same link and only on that link (subnet).

•The command to configure an IPv6 GUA on an interface is ipv6 address ipv6-address/prefix□length．

•A device obtains a GUA dynamically through ICMPv6 messages. IPv6 routers periodically send out ICMPv6 RA messages, every 200 seconds, to all IPv6-enabled devices on the network.

•RA messages have three methods: SLAAC, SLAAC with a stateless DHCPv6 server, and stateful DHCPv6 (no SLAAC)．

•The interface ID can be created using the EUI-64 process or a randomly generated 64-bit number．

•The EUIs process uses the 48-bit Ethernet MAC address of the client and inserts another 16 bits in the middle of MAC address to create a 64-bit interface ID.

•Depending upon the operating system, a device may use a randomly generated interface ID.

•All IPv6 devices must have an IPv6 LLA. An LLA can be configured manually or created dynamically．

•Cisco routers automatically create an IPv6 LLA whenever a GUA is assigned to the interface．

•There are two types of IPv6 multicast addresses: well-known multicast addresses and solicited node multicast addresses．

•Two commonIPv6 assigned multicast groups are: ff02::1 All-nodes multicast group and ff02::2 All□routers multicast group.

•A solicited-node multicast address is similar to the all-nodes multicast address. The advantage of a solicited-node multicast address is that it is mapped to a special Ethernet multicast address.

•IPv6 was designed with subnetting in mind. A separate subnet ID field in the IPv6 GUA is used to create subnets.

Chapter 13

ICMP

Chapter Objective: Use various tools to test network connectivity.

Topic Objective

1- ICMP Messages: Explain how ICMP is used to test network connectivity.

2-Ping and Traceroute Testing :Use ping and traceroute utilities to test network connectivity.

What did I learn in this chapter?

•The purpose of ICMP messages is to provide feedback about issues related to the processing of IP packets under certain conditions.

•The ICMP messages common to both ICMPv4 and ICMPv6 are: Host reachability , Destination or Service Unreachable, and Time exceeded.

•The messages between an IPv6 router and an IPv6 device including dynamic address allocation include RS and RA. The messages between IPv6 devices include the redirect (similar to IPv4), NS and NA.

•Ping (used by IPv4 and IPv6) uses ICMP echo request and echo reply messages to test connectivity between hosts

•Ping can be used to test the internal configuration of IPv4 or IPv6 on the local host.

• Traceroute (tracert) generates a list of hops that were successfully reached along the path.

Chapter 14

Transport Layer

Chapter Objective: Compare the operations of transport layer protocols in supporting end-to-end communication.

Topic Objective

1- Transportation of Data :Explain the purpose of the transport layer in managing the transportation of data in end-to-end communication.

2-TCP Overview: Explain characteristics of TCP.

3-UDP Overview: Explain characteristics of UDP.

4-Port Numbers: Explain how TCP and UDP use port numbers.

5-TCP Communication Process :Explain how TCP session establishment and termination processes facilitate reliable communication.

6-Reliability and Flow Control :Explain how TCP protocol data units are transmitted and acknowledged to guarantee delivery.

7-UDP Communication :Compare the operations of transport layer protocols in supporting end-to-end communication.

What did I learn in this chapter?

•The transport layer is the link between the application layer and the lower layers that are responsible for network transmission.

•The transport layer includes TCP and UDP.

•TCP establishes sessions, ensures reliability, provides same-order delivery, and supports flow control.

•UDP is a simple protocol that provides the basic transport layer functions.

•UDP reconstructs data in the order it is received, lost segments are not resent, no session establishment, and UPD does not inform the sender of resource availability.

•The TCP and UDP transport layer protocols use port numbers to manage multiple simultaneous conversations .

•Each application process running on a server is configured to use a port number.

•The port number is either automatically assigned or configured manually by a system administrator.

•For the original message to be understood by the recipient, all the data must be received and the data in these segments must be reassembled into the original order.

•Sequence numbers are assigned in the header of each packet.

•Flow control helps maintain the reliability of TCP transmission by adjusting the rate of data flow between source and destination.

•A source might be transmitting 1,460 bytes of data within each TCP segment. This is the typical MSS that a destination device can receive.

•The process of the destination sending acknowledgments as it processes bytes received and the continual adjustment of the source's send window is known as sliding windows.

• To avoid and control congestion, TCP employs several congestion handling mechanisms.

Chapter 15

Application Layer

Chapter Objective: Explain the operation of application layer protocols in providing support to end-user applications.

Topic Objective

1-Application, Presentation, and Session: Explain how the functions of the application layer, presentation layer, and session layer work together to provide network services to end user applications.

2-Peer-to-Peer: Explain how end user applications operate in a peer-to-peer network.

3-Web and Email Protocols :Explain how web and email protocols operate.

4-IP Addressing Services :Explain how DNS and DHCP operate.

5-File Sharing Services :Explain how file transfer protocols operate.

What did I learn in this chapter?

•Application layer protocols are used to exchange data between programs running on the source and destination hosts. The presentation layer has three primary functions: formatting, or presenting data, compressing data, and encrypting data for transmission and decrypting data upon receipt. The session layer creates and maintains dialogs between source and destination applications.

•In the client/server model, the device requesting the information is called a client and the device responding to the request is called a server.

•In a P2P network, two or more computers are connected via a network and can share resources without having a dedicated server.

•The three common HTTP message types are GET, POST, and PUT.

•Email supports three separate protocols for operation: SMTP, POP, and IMAP.

•DNS protocol matches resource names with the required numeric network address.

•DHCP for IPv4 service automates the assignment of IPv4 addresses, subnet masks, gateways, and other IPv4 networking parameters. The DHCPv6 messages are SOLICIT, ADVERTISE, INFORMATION REQUEST, and REPLY.

•An FTP client is an application which runs on a computer that is being used to push and pull data from an FTP server.

•Three functions of SMB messages: start, authenticate, and terminate sessions, control file and printer access, and allow an application to send or receive messages to or from another device.

Chapter 16

Network Security Fundamentals

Chapter Objective: Configure switches and routers with device hardening features to enhance security.

Topic Objective

1- Security Threats and Vulnerabilities: Explain why basic security measure are necessary on network devices.

2-Network Attacks :Identify security vulnerabilities.

3-Network Attack Mitigation: Identify general mitigation techniques.

4-Device Security :Configure network devices with device hardening features to mitigate security threats.

What Did I Learn In This Chapter?

•After the threat actor gains access to the network, four types of threats may arise: information theft, data loss and manipulation, identity theft, and disruption of service．

•There are three primary vulnerabilities or weaknesses: technological, configuration, and security policy．

•The four classes of physical threats are: hardware, environmental, electrical, and maintenance.

•Malware is short for malicious software. It is code or software specifically designed to damage, disrupt, steal, or inflict “bad” or illegitimate action on data, hosts, or networks．Viruses, worms, and Trojan horses are types of malware．

•Network attacks can be classified into three major categories: reconnaissance, access, and denial of service．

•To mitigate network attacks, you must first secure devices including routers, switches，servers, and hosts. Most organizations employ a defense-in-depth approach to security. This requires a combination of networking devices and services working together．

•Several security devices and services are implemented to protect an organization’s users and assets against TCP/IP threats: VPN, ASA firewall, IPS, ESA/WSA, and AAA server.

•Infrastructure devices should have backups of configuration files and IOS images on an FTP or similar file server. If the computer or a router hardware fails, the data or configuration can be restored using the backup copy．

•The most effective way to mitigate a worm attack is to download security updates from the operating system vendor and patch all vulnerable systems. To manage critical security patches, to make sure all end systems automatically download updates．

•AAA is a way to control who is permitted to access a network (authenticate), what they can do while they are there (authorize), and what actions they perform while accessing the network (accounting)．

•Network firewalls reside between two or more networks, control the traffic between them, and help prevent unauthorized access．

•Securing endpoint devices is critical to network security. A company must have well□documented policies in place, which may include the use of antivirus software and host intrusion prevention. More comprehensive endpoint security solutions rely on network access control.

•For Cisco routers, the Cisco Auto Secure feature can be used to assist securing the system．For most OSs default usernames and passwords should be changed immediately, access to

system resources should be restricted to only the individuals that are authorized to use those resources, and any unnecessary services and applications should be turned off and uninstalled when possible .

•To protect network devices, it is important to use strong passwords. A passphrase is often easier to remember than a simple password. It is also longer and harder to guess .

•For routers and switches, encrypt all plaintext passwords, setting a minimum acceptable password length, deter brute-force password guessing attacks, and disable an inactive privileged EXEC mode access after a specified amount of time.

• Configure appropriate devices to support SSH, and disable unused services.

Chapter 17

Build a Small Network

Chapter Objective: Implement a network design for a small network to include a router, a switch, and end devices.

Topic Objective

1- Devices in a Small Network :Identify the devices used in a small network.

2-Small Network Applications and Protocols :Identify the protocols and applications used in a small network.

3-Scale to Larger Networks: Explain how a small network serves as the basis of larger networks.

4-Verify Connectivity :Use the output of the ping and tracert commands to verify connectivity and establish relative network performance.

5-Host and IOS Commands: Use host and IOS commands to acquire information about the devices in a network.

6-Troubleshooting Methodologies :Describe common network troubleshooting methodologies.

7-Troubleshooting Scenarios: Troubleshoot issues with devices in the network.

What Did I Learn In This Chapter?

•Factors to consider when selecting network devices for a small network are cost, speed and types of ports/interfaces, expandability, and OS features and services .

•When implementing a network, create an IP addressing scheme and use it on end devices , servers and peripherals, and intermediary devices .

•Redundancy can be accomplished by installing duplicate equipment, but it can also be accomplished by supplying duplicate network links for critical areas .

•The routers and switches in a small network should be configured to support real-time traffic , such as voice and video, in an appropriate manner relative to other data traffic .

•There are two forms of software programs or processes that provide access to the network :

network applications and application layer services.

•To scale a network, several elements are required: network documentation, device inventory，budget, and traffic analysis．

•The ping command is the most effective way to quickly test Layer 3 connectivity between a source and destination IP address．

•The Cisco IOS offers an "extended" mode of the ping command which lets the user create special types of pings by adjusting parameters related to the command operation.

•A trace returns a list of hops as a packet is routed through a network．

•There is also an extended traceroute command. It allows the administrator to adjust parameters related to the command operation．

•Network administrators view the IP addressing information (address, mask, router, and DNS) on a Windows host by issuing the ipconfig command. Other necessary commands are ipconfig /all, ipconfig /release and ipconfig /renew, and ipconfig /displaydns．

•Verifying IP settings by using the GUI on a Linux machine will differ depending on the Linux distribution (distro) and desktop interface. Necessary commands are ifconfig, and ip address．

•In the GUI of a Mac host, open Network Preferences > Advanced to get the IP addressing information. Other IP addressing commands for Mac are ifconfig, and networksetup-listallnetworkservices and networksetup -getinfo <network service .<

•The arp command is executed from the Windows, Linux, or Mac command prompt. The command lists all devices currently in the ARP cache of the host, which includes the IPv4 address, physical address, and the type of addressing (static/dynamic), for each device．

• The arp -a command displays the known IP address and MAC address binding.

•Common show commands are show running-config, show interfaces, show ip address, show arp，show ip route, show protocols, and show version. The show cdp neighbor command provides the following information about each CDP neighbor device: identifiers, address list, port identifier, capabilities list, and platform．

•The show cdp neighbors detail command will help determine if one of the CDP neighbors has an IP configuration error．

•The show ip interface brief command output displays all interfaces on the router, the IP address assigned to each interface, if any, and the operational status of the interface.

•The six basic steps to troubleshooting Step 1. Identify the problem Step 2. Establish a theory of probably causes. Step 3. Test the theory to determine the cause. Step 4. Establish a plan of action and implement the solution. Step 5. Verify the solution and implement preventive measures. Step 6. Document findings，actions, and outcomes.