[CCST ROADMAP FROM SKILLS FOR ALL 2](#_Toc14372)

[NETWORKING BASICS 2](#_Toc11030)

[Section 1 (Internet, Data, Signals) 2](#_Toc32367)

[Section 2 (Network Infrastructure) 4](#_Toc15684)

[Section 3 5](#_Toc24026)

[SECTION 4 7](#_Toc3526)

[Section 5 9](#_Toc3621)

[Section 6 11](#_Toc19732)

[Section 7 12](#_Toc16082)

[Section 8 13](#_Toc20963)

[Section 9 14](#_Toc17407)

[Section 13 (ARP) 21](#_Toc32562)

[Section 14 23](#_Toc7863)

[Section 15 26](#_Toc31675)

[Section 16 28](#_Toc25893)

[Section 17 (Troubleshooting Commands) 30](#_Toc19957)

[Networking Devices and Initial Configuration 32](#_Toc28946)

[Section 1 32](#_Toc18689)

# CCST ROADMAP FROM SKILLS FOR ALL

## NETWORKING BASICS

### Section 1 (Internet, Data, Signals)

**The internet** is not owned by any individual or group. The internet is a worldwide collection of interconnected networks (internetwork or internet for short), cooperating with each other to exchange information using common standards. Through telephone wires, fiber-optic cables, wireless transmissions, and satellite links, internet users can exchange information in a variety of forms.

Small home networks connect a few computers to each other and to the internet. The SOHO network allows computers in a home office or a remote office to connect to a corporate network, or access centralized, shared resources. Medium to large networks, such as those used by corporations and schools, can have many locations with hundreds or thousands of interconnected hosts. ***The internet is a network of networks that connects hundreds of millions of computers world-wide.***

There are devices all around that you may interact with on a daily basis that are also connected to the internet. These include mobile devices such as smartphones, tablets, smartwatches, and smart glasses. Things in your home can be connected to the internet such as a security system, appliances, your smart TV, and your gaming console. Outside your home there are smart cars, RFID tags, sensors and actuators, and even medical devices which can be connected.

**The following categories are used to classify types of personal data:**

***Volunteered data*** - This is created and explicitly shared by individuals, such as social network profiles. This type of data might include video files, pictures, text, or audio files.

***Observed data*** - This is captured by recording the actions of individuals, such as location data when using cell phones.

***Inferred data*** - This is data such as a credit score, which is based on analysis of volunteered or observed data.

The term bit is an abbreviation of “binary digit” and represents the smallest piece of data. Each bit can only have one of two possible values, 0 or 1.

There are three common **methods of signal transmission** used in networks:

***Electrical signals*** - Transmission is achieved by representing data as electrical pulses on copper wire.

***Optical signals*** - Transmission is achieved by converting the electrical signals into light pulses.

***Wireless signals*** - Transmission is achieved by using infrared, microwave, or radio waves through the air.

***Bandwidth*** is the capacity of a medium to carry data. Digital bandwidth measures the amount of data that can flow from one place to another in a given amount of time. Bandwidth is typically measured in the number of bits that (theoretically) can be sent across the media in a second. Common bandwidth measurements are as follows:

Thousands of bits per second (Kbps)

Millions of bits per second (Mbps)

Billions of bits per second (Gbps)

Throughput does not usually match the specified bandwidth. Many factors influence throughput including:

The amount of data being sent and received over the connection

The latency created by the number of network devices encountered between source and destination

***Latency*** refers to the amount of time, including delays, for data to travel from one given point to another.

### Section 2 (Network Infrastructure)

Computers connected to a network that participate directly in network communication are classified as **hosts**. Hosts can send and receive messages on the network. In modern networks, computer hosts can act as a client, a server, or both. ***The software installed on the computer determines which role the computer plays.***

Client and server software usually run on separate computers, but it is also possible for one computer to run both client and server software at the same time. In small businesses and homes, *many computers function as the servers and clients on the network.* This type of network is called a **P2P** network. In larger businesses, *because of the potential for high amounts of network traffic*, it is often necessary to have dedicated servers to support the number of service requests. P2P networks are easy to set up, less complex, lower in cost, and can be used for simple tasks such as transferring files and sharing printers. However, there is no centralized administration. They have less security, are not scalable, and can perform slower.

The network infrastructure is the platform that supports the network. It provides the stable and reliable channel over which our communications can occur. The network infrastructure contains three categories of ***hardware components***: end devices, intermediate devices, and network media. Hardware is often *the visible components of the network platform such as a laptop, PC, switch, router, wireless access point, or the cabling used to connect the devices*. Components that are not visible include *wireless media.*

***End devices****,* or hosts, form the interface between users and the underlying communication network. An end device (or host) is either the source or destination of a message.

Some examples of end devices include:

Computers (workstations, laptops, file servers, web servers),network printers

***Intermediary Devices***

Wireless Router,LAN Switch,Router,Multilayer Switch,Firewall Appliance

***Network Media***

Wireless Media,LAN Media,WAN Media

An **ISP** provides the link between the home network and the internet. An ISP can be the ***local cable provider, a landline telephone service provider, the cellular network*** that provides your smartphone service, or an independent provider who leases bandwidth on the physical network infrastructure of another company. Each ISP connects to other ISPs to form a network of links that interconnect users all over the world. ISPs are connected in a hierarchical manner that ensures that internet traffic generally takes the shortest path from the source to the destination.

The interconnection of ISPs that forms the backbone of the internet is a complex web of fiber-optic cables with expensive networking switches and routers that direct the flow of information between source and destination hosts.

For a home user, connecting to the ISP is a fairly uncomplicated process. This is the most common connection option. It consists of using a wireless integrated router to connect to the ISP. The router includes a switch to connect wired hosts and a wireless AP to connect wireless hosts. The router also provides client IP addressing information and security for inside hosts. The two most common methods are cable and DSL. Other options include cellular, satellite, and dial-up telephone.

### Section 3

Mobile phones use radio waves to transmit voice signals to antennas mounted on towers located in specific geographic areas. When a telephone call is made, the voice signal is relayed from one tower to another tower until it is delivered to its destination. This type of network is used when you make a phone call to another mobile phone or to a wired telephone. It is also used to send text messages directly from the phone. The most common type of cellular telephone network is called a GSM network. The abbreviations 3G, 4G, 4G-LTE, and 5G are used to describe enhanced cell phone networks that are optimized for the fast transmission of data. Currently, 4G still dominates as the current mobile network used by most phones.

In addition to the GSM and 4G/5G transmitters and receivers, smartphones make connections in a variety of ways.

***Wi-Fi*** transmitters and receivers located within the smartphone enable the phone to connect to local networks and the internet. Wi-Fi networks are usually privately owned but often provide guest or public access hotspots. A hotspot is an area where Wi-Fi signals are available.

***Bluetooth*** is wireless technology that allows devices to communicate over short distances. Multiple devices can be connected at the same time with Bluetooth.

***NFC*** is a wireless communication technology that enables data to be exchanged by devices that are in very close proximity to each other, usually less than a few centimeters.

Almost all mobile devices are capable of connecting to Wi-Fi networks. These precautions should be taken to protect Wi-Fi communications on mobile devices:

Never send login or password information using unencrypted text (plaintext).

Use a VPN connection when possible if you are sending sensitive data.

Enable security on home networks.

Use WPA2 or higher encryption for security.

Bluetooth technology provides a simple way for mobile devices to connect to each other and to wireless accessories. Bluetooth is wireless, automatic, and uses very little power, which helps conserve battery life. Some examples of devices that use Bluetooth include hands-free headsets, keyboards, a mouse, stereo controls, car speakerphones, and mobile speakers.

Bluetooth pairing occurs when two Bluetooth devices establish a connection to share resources.

### Section 4

Most home networks consist of at least two separate networks. The public network coming in from the service provider. The router is connected to the internet. Most likely, the home router is equipped with both wired and wireless capabilities. A home network is a small LAN with devices that usually connect to an integrated router and to each other in order to exchange information.

Small business and home routers typically have two primary types of ports: ethernet ports and internet ports. In addition to the wired ports, many home routers include a radio antenna and a built-in wireless access point.

Wireless technologies use electromagnetic waves to carry information between devices. The electromagnetic spectrum includes such things as radio and television broadcast bands, visible light, x-rays, and gamma-rays. Some types of electromagnetic waves are not suitable for carrying data. Other parts of the spectrum are regulated by governments and licensed to various organizations for specific applications.

Certain unlicensed sections of the spectrum are incorporated into consumer products, including the ***Wi-Fi routers*** found in most homes. The wireless technologies most frequently used in home networks are ***in the unlicensed 2.4 GHz and 5 GHz frequency ranges.*** ***Bluetooth*** is a technology that makes use of the ***2.4 GHz band***. Other technologies that use the 2.4 GHz and 5 GHz bands are the modern wireless LAN technologies that conform to the various IEEE 802.11 standards. Unlike Bluetooth technology, 802.11 devices transmit at a much higher power level giving them a great range and improved throughput.

Although many home network devices support wireless communications, there are still a few applications where devices benefit from a wired switch connection. The most commonly implemented wired protocol is the ***Ethernet protocol.*** Directly connected devices use an Ethernet patch cable, usually *unshielded twisted pair*(UTP). **Category 5e** is the most common wiring used in a LAN. The cable is made up of 4 pairs of wires that are twisted to reduce *electrical interference*. For those homes that do not have UTP wiring, there are other technologies, such as powerline, that can distribute wired connectivity throughout the premises.

The IEEE 802.11 standard governs the WLAN environment. Wireless standards for LANs use the 2.4 GHz and 5 GHz frequency bands. Collectively these technologies are referred to as Wi-Fi. The ***Wi-Fi Alliance*** is responsible for testing wireless LAN devices from different manufacturers.

Wireless routers using the 802.11 standards have multiple settings that have to be configured. These settings include the following:

***Network mode*** - Determines the type of technology that must be supported. For example, 802.11b, 802.11g, 802.11n or Mixed Mode.

***Network Name*** (SSID) - Used to identify the WLAN. All devices that wish to participate in the WLAN must have the same SSID.

***Standard Channel***- Specifies the channel over which communication will occur. By default, this is set to Auto to allow the access point (AP) to determine the optimum channel to use.

***SSID Broadcast***- Determines if the SSID will be broadcast to all devices within range. By default, set to Enabled.

The 802.11 protocol can provide increased throughput based on the wireless network environment. If all wireless devices connect with the same 802.11 standard, maximum speeds can be obtained for that standard. If the access point is configured to accept only one 802.11 standard, devices that do not use that standard cannot connect to the access point. A mixed mode wireless network environment can include devices that use any of the existing Wi-Fi standards.

When building a wireless network, it is important that the wireless components connect to the appropriate WLAN. This is done using the SSID. The SSID is used to tell wireless devices, called STAs, which WLAN they belong to and with which other devices they can communicate. The SSID broadcast allows other devices and wireless clients to automatically discover the name of the wireless network. When the SSID broadcast is disabled, you must manually enter the SSID on wireless devices.

### Section 5

Protocols are the rules that govern communications. Protocols include HTTP, TCP, IP, and Ethernet. ,these include message format, message size, timing, encoding, encapsulation, and message patterns.

* ****Message format**** - When a message is sent, it must use a specific format or structure.
* ****Message size**** - The rules that govern the size of the pieces communicated across the network are very strict. They can also be different, depending on the channel used.
* ****Timing**** - Timing determines the speed at which the bits are transmitted across the network. It also affects when an individual host can send data and the total amount of data that can be sent in any one transmission.
* ****Encoding**** - Messages sent across the network are first converted into bits by the sending host. Each bit is encoded into a pattern of sounds, light waves, or electrical impulses depending on the network media over which the bits are transmitted.
* ****Encapsulation**** - Each message transmitted on a network must include a header that contains addressing information that identifies the source and destination hosts. Encapsulation is the process of adding this information to the pieces of data that make up the message.
* ****Message pattern**** - Some messages require an acknowledgment before the next message can be sent. This type of request/response pattern is a common aspect of many networking protocols. However, there are other types of messages that may be simply streamed across the network, without concern as to whether they reach their destination

When a new standard is proposed, each stage of the development and approval process is recorded in a numbered ***RFC document*** so that the evolution of the standard is tracked. RFCs for internet standards are published and managed by the ***IETF***.

The interaction between the different protocols on a device can be illustrated as a protocol stack. A stack illustrates the protocols as a layered hierarchy, with each higher-level protocol depending on the services of the protocols shown in the lower levels

The suite of TCP/IP protocols that are used for internet communications follows the structure of this model:

* ****Application**** - Represents data to the user, plus encoding and dialog control
* ****Transport**** -Supports communication between various devices across diverse networks
* ****Internet**** - Determines the best path through the network
* ****Network Access**** - The hardware devices and media that make up the network.

A reference model describes the functions that must be completed at a particular layer but does not specify exactly how a function should be accomplished.

**OSI model**

* ****7 – Application**** - The application layer contains protocols used for process-to-process communications.
* ****6 – Presentation**** - The presentation layer provides for common representation of the data transferred between application layer services.
* ****5 – Session**** - The session layer provides services to the presentation layer to organize its dialogue and to manage data exchange.
* ****4 – Transport**** - The transport layer defines services to segment, transfer, and reassemble the data for individual communications between the end devices.
* ****3 – Network**** - The network layer provides services to exchange the individual pieces of data over the network between identified end devices.
* ****2 - Data Link**** - The data link layer protocols describe methods for exchanging data frames between devices over a common media
* ****1 – Physical**** - The physical layer protocols describe the mechanical, electrical, functional, and procedural means to activate, maintain, and de-activate physical connections for a bit transmission to and from a network device.

The OSI data link and physical layers together are equivalent to the TCP/IP network access layer. The OSI transport layer is functionally equivalent to the TCP/IP transport layer, and the OSI network layer is equivalent to the TCP/IP internet layer. The OSI application, presentation, and session layers are functionally equivalent to the application layer within the TCP/IP model.

### Section 6

Network Media Types  
Communication transmits across a network on media. The media provides the channel over which the message travels from source to destination.

Modern networks primarily use three types of media to interconnect devices are:

Metal wires within cables - Data is encoded into electrical impulses.

Glass or plastic fibers within cables (fiber-optic cable) - Data is encoded into pulses of light.

Wireless transmission - Data is encoded via modulation of specific frequencies of electromagnetic waves.

The four main criteria for choosing media are the following:

* What is the maximum distance that the media can successfully carry a signal?
* What is the environment in which the media will be installed?
* What is the amount if data and at what speed must is be transmitted?
* What is the cost of the media installation?

The three most common network cables are twisted-pair, coaxial cable, and fiber-optic cable. Ethernet technology generally uses twisted-pair cables to interconnect devices. Coaxial cable is the kind of copper cable used by cable TV companies. It is also used for connecting the various components which make up satellite communication systems.

Fiber-optic cable can be either glass or plastic with a diameter about the same as a human hair and it can carry digital information at very high speeds over long distances. Because light is used instead of electricity, electrical interference does not affect the signal.

### Section 7

The process of placing one message format inside another message format is called encapsulation. De-encapsulation occurs when the process is reversed by the recipient and the letter is removed from the envelope.

The Ethernet protocol standards define many aspects of network communication including frame format, frame size, timing, and encoding. The format for Ethernet frames specifies the location of the destination and source MAC addresses, and additional information including preamble for sequencing and timing, start of frame delimiter, length and type of frame, and frame check sequence to detect transmission errors.

Ethernet hubs contain multiple ports that are used to connect hosts to the network. Only one message can be sent through an Ethernet hub at a time. Two or more messages sent at the same time will cause a collision. Because excessive retransmissions can clog up the network and slow down network traffic, hubs are now considered obsolete and have been replaced by Ethernet switches

An Ethernet switch is a device that is used at Layer 2. When a host sends a message to another host connected to the same switched network, the switch accepts and decodes the frames to read the MAC address portion of the message. A table on the switch, called a MAC address table, contains a list of all the active ports and the host MAC addresses that are attached to them. When a message is sent between hosts, the switch checks to see if the destination MAC address is in the table. If it is, the switch builds a temporary connection, called a circuit, between the source and destination ports. Ethernet switches also allow for sending and receiving frames over the same Ethernet cable simultaneously. This improves the performance of the network by eliminating collisions.

A switch builds the MAC address table by examining the source MAC address of each frame that is sent between hosts. When a new host sends a message or responds to a flooded message, the switch immediately learns its MAC address and the port to which it is connected. The table is dynamically updated each time a new source MAC address is read by the switch.

### Section 8

The IPv4 address is a logical network address that identifies a particular host. The logical ***32-bit IPv4*** address is hierarchical and is made up of two parts, the ***network***, and the ***host.*** As an example, there is a host with an IPv4 address 192.168.5.11 with a subnet mask of 255.255.255.0. The first three octets, (192.168.5), identify the network portion of the address, and the last octet, (11) identifies the host. This is known as ***hierarchical addressing*** because the network portion indicates the network on which each unique host address is located.

Routers only need to know how to reach each network, rather than needing to know the location of each individual host. With IPv4 addressing, multiple logical networks can exist on one physical network if the network portion of the logical network host addresses is different.

### Section 9

**Unicast transmission** refers to one device sending a message to one other device in one-to-one communications. A unicast packet has a destination IP address that is a unicast address which goes to a single recipient. A source IP address can only be a unicast address because the packet can only originate from a single source. This is regardless of whether the destination IP address is a unicast, broadcast or multicast. IPv4 unicast host addresses are in the address range of **1.1.1.1 to 223.255.255.255.**

**Broadcast transmission** refers to a device sending a message to all the devices on a network in ***one-to-all communications***. A broadcast packet has a destination IP address with all ones (1s) in the host portion, or 32 one (1) bits. A broadcast packet must be processed by all devices in the same ***broadcast domain***. A broadcast may be directed or limited. A ***directed broadcast*** is sent to all hosts on a specific network. A limited broadcast is sent to 255.255.255.255. By default, ***routers do not forward broadcasts.*** Limited broadcast addresses are never forwarded across routers, while directed broadcast addresses can be

**Multicast transmission** reduces traffic by allowing a host to send a single packet to a selected set of hosts that subscribe to a ***multicast group***. A multicast packet is a packet with a destination IP address that is a multicast address. IPv4 has reserved the **224.0.0.0 to 239.255.255.255** addresses as a multicast range. Each multicast group is represented by a single IPv4 multicast destination address. When an IPv4 host subscribes to a multicast group, the host processes packets addressed to this multicast address, and packets addressed to its uniquely allocated unicast address.

Public IPv4 addresses are addresses which are globally routed between ISP routers. However, not all available IPv4 addresses can be used on the internet. There are blocks of addresses called ***private addresses*** that are used by most organizations to assign IPv4 addresses to ***internal hosts***. Most internal networks, from large enterprises to home networks, use private IPv4 addresses for addressing all internal devices (intranet) including hosts and routers. However, private addresses are not globally routable. Before the ISP can forward this packet, it must translate the source IPv4 address, which is a private address, to a public IPv4 address using NAT.

**Loopback addresses** (127.0.0.0 /8 or 127.0.0.1 to 127.255.255.254) are more commonly identified as only 127.0.0.1, these are special addresses used by a host to direct traffic to itself.

**Link-local addresses** (169.254.0.0 /16 or 169.254.0.1 to 169.254.255.254) are more commonly known as the ***Automatic Private IP Addressing*** (APIPA) addresses or self-assigned addresses. They are used by a Windows DHCP client to self-configure in the event that there are no DHCP servers available.

In 1981, IPv4 addresses were assigned using classful addressing as defined in RFC 790 ([https://tools.ietf.org/html/rfc790](https://datatracker.ietf.org/doc/html/rfc790" \t "https://www.netacad.com/content/nb/1.0/index.html?xAPILaunchKey=13bb1664-71e6-4dbe-85b7-bfec0e961473&xAPILaunchService=https://www.netacad.com/adl/content/&lang=en-US&moduleNumber=9" \l "/courses/content/m9/id/_blank)), Assigned Numbers. Customers were allocated a network address based on one of three classes, A, B, or C. The RFC divided the unicast ranges into specific classes as follows:

* ****Class A (0.0.0.0/8 to 127.0.0.0/8)**** - Designed to support extremely large networks with more than 16 million host addresses.
* ****Class B (128.0.0.0 /16 - 191.255.0.0 /16)**** - Designed to support the needs of moderate to large size networks with up to approximately 65,000 host addresses.
* ****Class C (192.0.0.0 /24 - 223.255.255.0 /24)**** - Designed to support small networks with a maximum of 254 hosts.

There is also a Class D multicast block consisting of 224.0.0.0 to 239.0.0.0 and a Class E experimental address block consisting of 240.0.0.0 - 255.0.0.0.

Public IPv4 addresses are addresses which are globally routed over the internet. Public IPv4 addresses must be unique***. Both IPv4 and IPv6 addresses are managed by the IANA.*** The IANA manages and allocates blocks of IP addresses to the RIRs. ***RIRs are responsible for allocating IP addresses to ISPs who provide IPv4 address blocks to organizations and smaller ISPs.*** Organizations can also get their addresses directly from an RIR.

Private IP Addresses

10.0.0.0 to 10.255.255.255 (10.0.0.0/8)

172.16.0.0 to 172.31.255.255 (172.16.0.0/12)

192.168.0.0 to 192.168.255.255 (192.168.0.0/16)

In an Ethernet LAN, devices use broadcasts and  ***Address Resolution Protocol (ARP)*** to locate other devices. ARP sends Layer 2 broadcasts to a known IPv4 address on the local network to discover the associated MAC address. Devices on Ethernet LANs also locate other devices using services. A host typically acquires its IPv4 address configuration using DHCP which sends broadcasts on the local network to locate a DHCP server. Switches propagate broadcasts out all interfaces except the interface on which it was received.

A large broadcast domain is a network that connects many hosts. A problem with a large broadcast domain is that these hosts can generate excessive broadcasts and negatively affect the network. The solution is to reduce the size of the network to create smaller broadcast domains in a process called subnetting. These smaller network spaces are called subnets. The basis of subnetting is to use host bits to create additional subnets. Subnetting reduces overall network traffic and improves network performance. It helps administrators to implement security policies such as which subnets are allowed or not allowed to communicate together. It reduces the number of devices affected by abnormal broadcast traffic due to misconfigurations, hardware/software problems, or malicious intent.

**Section 10**

The ***depletion of IPv4 address space*** has been the motivating factor for moving to **IPv6.** IPv6 has a larger ***128-bit address space,*** providing 340 undecillion possible addresses. When the IETF began its development of a successor to IPv4, it used this opportunity to fix the limitations of IPv4 and include enhancements. One example is ICMPv6, which includes address resolution and address autoconfiguration not found in ICMPv4.

Both IPv4 and IPv6 coexist and the transition to only IPv6 will take several years. 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***. Dual stack devices run both IPv4 and IPv6 protocol stacks simultaneously. Tunneling is a method of transporting an IPv6 packet over an IPv4 network. The IPv6 packet is encapsulated inside an IPv4 packet, similar to other types of data. NAT64 allows IPv6-enabled devices to communicate with IPv4-enabled devices using a translation technique similar to NAT for IPv4. An IPv6 packet is translated to an IPv4 packet and an IPv4 packet is translated to an IPv6 packet.

IPv6 addresses are 128 bits in length and written as a string of hexadecimal values. Every ***four bits*** is represented by ***a single hexadecimal digit;*** for a total of 32 hexadecimal values. IPv6 addresses are not case-sensitive and can be written in either lowercase or uppercase. In IPv6, a hextet that refers to a segment of 16 bits, or four hexadecimal values. Each “x” is a single hextet, which is 16 bits or four hexadecimal digits. Preferred format means that you write IPv6 address using all ***32 hexadecimal digits***. Here is one example - fe80:0000:0000:0000:0123:4567:89ab:cdef.

There are two rules that help to reduce the number of digits needed to represent an IPv6 address.

**Rule 1 –**Omit Leading Zeros. You can only omit leading zeros, not trailing zeros.

* 01ab can be represented as 1ab
* 09f0 can be represented as 9f0
* 0a00 can be represented as a00
* 00ab can be represented as ab

**Rule 2**– Double Colon. A double colon (::) can replace any single, contiguous string of one or more 16-bit hextets consisting of all zeros. For example, 2001:db8:cafe:1:0:0:0:1 (leading 0s omitted) could be represented as 2001:db8:cafe:1::1. The double colon (::) is used in place of the three all-0 hextets (0:0:0). The double colon (::) can only be used once within an address, otherwise there would be more than one possible resulting address. If an address has more than one contiguous string of all-0 hextets, best practice is to use the double colon (::) on the longest string. If the strings are equal, the first string should use the double colon (::).

Section 11

With a **static assignment**, the network administrator must ***manually configure the network information for a host***. At a minimum, this includes the host IPv4 address, subnet mask, and default gateway. Static assignment of addressing information can provide increased control of network resources, but it can be time consuming to enter the information on each host. When using static IPv4 addressing, it is important to maintain an accurate list of which IPv4 addresses are assigned to which devices.

IPv4 addresses can be ***assigned automatically*** using a protocol known as **DHCP**. DHCP is generally the preferred method of assigning IPv4 addresses to hosts on large networks because it reduces the burden on network support staff and virtually eliminates entry errors. Another benefit of DHCP is that an address is not permanently assigned to a host but is only leased for a period of time. If the host is powered down or taken off the network, the address is returned to the pool for reuse.

As you enter area with a wireless hotspot, your laptop DHCP client contacts the local DHCP server via a wireless connection. The DHCP server assigns an IPv4 address to your laptop. With home networks, the DHCP server may be located at the ISP and a host on the home network receives its IPv4 configuration directly from the ISP. Many home networks and small businesses use a wireless router and modem. In this case, the wireless router is both a DHCP client and a server.

The DHCP server is configured with a range, or pool, of IPv4 addresses that can be assigned to DHCP clients. A client that needs an IPv4 address will send a ***DHCP Discover message*** which is a broadcast with a destination IPv4 address of ***255.255.255.255 (32 ones)*** and a destination MAC address of ***FF-FF-FF-FF-FF-FF (48 ones)***. All hosts on the network will receive this broadcast ***DHCP frame***, but only a DHCP server will reply. The server will respond with a ***DHCP Offer***, suggesting an IPv4 address for the client. The host then sends a ***DHCP Request*** asking to use the suggested IPv4 address. The server responds with a ***DHCP Acknowledgment.***

For most home and small business networks, a wireless router provides DHCP services to the local network clients. To configure a home wireless router, access its graphical web interface by opening the browser and entering the router default IPv4 address. The IPv4 address of 192.168.0.1 and subnet mask of 255.255.255.0 are the defaults for the internal router interface. This is the default gateway for all hosts on the local network and also the internal DHCP server IPv4 address. Most home wireless routers have DHCP Server enabled by default.

**Section 12**

Every host on a network must use the ***router as a gateway to other networks***. Therefore, each host must know the IPv4 address of the router interface connected to the network where the host is attached. This address is known as the default gateway address. It can be either statically configured on the host or received dynamically by DHCP.

The wireless router acts as a DHCP server for all local hosts attached to it, either by Ethernet cable or wirelessly. These local hosts are referred to as being located on an internal, or inside, network. When a wireless router is connected to the ISP, it acts like a DHCP client to receive the correct external network IPv4 address for the internet interface. ISPs usually provide an internet-routable address, which enables hosts connected to the wireless router to have access to the internet. The wireless router serves as the boundary between the local internal network and the external internet.

The wireless router receives a public address from the ISP, which allows it to send and receive packets on the internet. It, in turn, provides private addresses to local network clients.

The process ***used to convert private addresses to internet-routable addresses*** is called **NAT**. With NAT, a private (local) source IPv4 address is translated to a public (global) address. The process is reversed for incoming packets. The wireless router is able to translate many internal IPv4 addresses to the same public address, by using NAT.

Only packets destined for other networks need to be translated. These packets must pass through the gateway, where the wireless router replaces the private IPv4 address of the source host with its own public IPv4 address.

### Section 13 (ARP)

Sometimes a host must send a message, but it only knows the IP address of the destination device. The host needs to know the MAC address of that device. The MAC address can be discovered using ***address resolution***. There are two primary addresses assigned to a device on an Ethernet LAN:

***Physical address*** (the MAC address) – Used for NIC-to-NIC communications on the same Ethernet network.-Network Interface Card (NIC)

***Logical address*** (the IP address) – Used to send the packet from the source device to the destination device. The destination IP address may be on the same IP network as the source, or it may be on a remote network.

***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). Routers examine the destination IPv4 address to determine the best path to forward the IPv4 packet. When the router receives the Ethernet frame, it de-encapsulates the Layer 2 information. Using the destination IPv4 address, it determines the next-hop device, and then encapsulates the IPv4 packet in a new data link frame for the outgoing interface. Along each link in a path, an IP packet is encapsulated in a frame. The frame is specific to the data link technology that is associated with that link, such as Ethernet. If the next-hop device is the final destination, the destination MAC address will be that of the device Ethernet NIC.

A message can only contain one destination MAC address. Address resolution lets a host send a broadcast message to a unique MAC address that is recognized by all hosts. The ***broadcast MAC address is a 48-bit address made up of all ones.*** MAC addresses are usually represented in hexadecimal notation. The broadcast MAC address in hexadecimal notation is FFFF.FFFF.FFFF. Each F in the hexadecimal notation represents four ones in the binary address.

When a host sends a broadcast message, switches forward the message to every connected host within the same local network. For this reason, a local area network***, a network with one or more Ethernet switches, is also referred to as a broadcast domain.***

If too many hosts are connected to the same broadcast domain, broadcast traffic can become excessive. The number of hosts and the amount of network traffic that can be supported on the local network is limited by the capabilities of the switches used to connect them. To improve performance, you may need to divide one local network into multiple networks, or broadcast domains. ***Routers are used to divide the network into multiple broadcast domains.***

On a local Ethernet network, a NIC only accepts a frame if the destination address is either the broadcast MAC address, or else corresponds to the MAC address of the NIC. Most network applications rely on the logical destination IP address to identify the location of the servers and clients. How does the sending host determine what destination MAC address to place within the frame? The sending host can ***ARP to discover the MAC address of any host on the same local network. (in cmd use arp –a to get mac data)***

ARP uses a three-step process to discover and store the MAC address of a host on the local network when only the IPv4 address of the host is known:

The sending host creates and sends a frame addressed to ***a broadcast MAC address.*** Contained in the frame is a message with the IPv4 address of the intended destination host.

Each host on the network receives the broadcast frame and compares the IPv4 address inside the message with its configured IPv4 address. The host with the matching IPv4 address sends its MAC address back to the original sending host.

The sending host receives the message and stores the MAC address and IPv4 address information in a table called an ARP table.

IPv6 uses a similar method known as ***Neighbor Discovery.***

### Section 14

As networks grow, it is often necessary to divide one access layer network into multiple access layer networks. There are many ways to divide networks based on different criteria:

* ****Broadcast containment**** - Routers in the distribution layer can limit broadcasts to the local network where they need to be heard.
* ****Security requirements**** - Routers in the distribution layer can separate and protect certain groups of computers where confidential information resides.
* ****Physical locations**** - Routers in the distribution layer can be used to interconnect local networks at various locations of an organization that are geographically separated.
* ****Logical grouping**** - Routers in the distribution layer can be used to logically group users, such as departments within a company, who have common needs or for access to resources.

***The distribution layer*** connects these independent local networks and controls the traffic flowing between them. It is responsible for ensuring that traffic between hosts on the local network stays local.

A router is a networking device that connects multiple Layer 3, IP networks. At the distribution layer of the network, routers direct traffic and perform other functions critical to efficient network operation. Routers, like switches, are able to decode and read the messages that are sent to them. Unlike switches, which make their forwarding decision based on the Layer 2 MAC address, routers make their forwarding decision based on the Layer 3 IP address.

***Anytime the network portion of the IP addresses of the source and destination hosts do not match, a router must be used to forward the message***.

Each port, or interface, on a router connects to a different local network. Every router contains a table of all locally connected networks and the interfaces that connect to them.

When a router receives a frame, it decodes the frame to get to the packet containing the destination IP address. It matches the network portion of the destination IP address to the networks that are listed in the routing table. If the destination network address is in the table, the router encapsulates the packet in a new frame in order to send it out. It forwards the new frame out of the interface associated with the path, to the destination network. The process of forwarding the packets toward their destination network is called routing.

A router forwards a packet to one of two places: a directly connected network containing the actual destination host, or to another router on the path to reach the destination host. When a router encapsulates the frame to forward it out a routed interface, it must include a destination MAC address. If the router must forward the packet to another router through a routed interface, it will use the MAC address of the connected router. Routers obtain these MAC addresses from ARP tables.

A host is given the IPv4 address of the router through the default gateway address configured in its TCP/IP settings. The default gateway address is the address of the router interface connected to the same local network as the source host. All hosts on the local network use the default gateway address to send messages to the router.

Routing tables contain the addresses of networks, and the best path to reach those networks. Entries can be made to the routing table in two ways: dynamically updated by information received from other routers in the network, or manually entered by a network administrator.

***LAN refers to a local network,*** or a group of interconnected local networks that are ***under the same administrative control***. All the local networks within a LAN are under one administrative control. Other common characteristics of LANs are that they t***ypically use Ethernet or wireless protocols***, and they ***support high data rates.***

Within a LAN, it is possible to place all hosts on a single local network or divide them up between multiple networks connected by a distribution layer device.

Placing all hosts on a single local network allows them to be seen by all other hosts. This is because there is one broadcast domain and hosts use ARP to find each other.

Placing additional hosts on a remote network will decrease the impact of traffic demands. However, hosts on one network will not be able to communicate with hosts on the other network without the use of routing. Routers increase the complexity of the network configuration and can introduce latency, or time delay, on packets sent from one local network to the other.

Nb:

Access layer

The entry point for users to access the network, providing access, authentication, security policies, and local traffic processing. The access layer is also known as the desktop layer.

Distribution layer

Located between the access and core layers, the distribution layer connects access layer subnets and manages traffic. It also implements network foundation technologies like routing, quality of service, and security.

Core layer

The backbone of the network, responsible for high-speed data transmission and traffic exchange. The core layer connects the different aggregation layers and provides high network availability and redundancy.

### Section 15

UDP is a 'best effort' delivery system that does not require acknowledgment of receipt. UDP is preferable with applications such as streaming audio and VoIP. Acknowledgments would slow down delivery and retransmissions are undesirable. Packets take a path from the source to a destination. A few packets may be lost but it is usually not noticeable.

TCP packets take a path from the source to the destination. However, each of the packets has a sequence number. TCP breaks up a message into small pieces known as segments. The segments are numbered in sequence and passed to the IP process for assembly into packets. TCP keeps track of the number of segments that have been sent to a specific host from a specific application. If the sender does not receive an acknowledgment within a certain period of time, it assumes that the segments were lost and retransmits them. Only the portion of the message that is lost is resent, not the entire message.

When a message is delivered using either TCP or UDP, the protocols and services requested are identified by a port number. ***A port is a numeric*** ***identifier within each segment that is used to keep track of specific conversations between a client and serve***r. Every message that a host sends contains both a source and destination port.

When a message is received by a server, it is necessary for the server to be able to determine which service is being requested by the client. Clients are preconfigured to use a destination port that is registered on the internet for each service.

Ports are assigned and managed by an organization known as the **ICANN.** Ports are broken into three categories and range in number from **1 to 65,535:**

* **Well-Known Ports -**Destination ports that are associated with common network applications are identified as well-known ports. These ports are in the range of ***1 to 1023.***
* **Registered Ports -**Ports ***1024 through 49151*** can be used as either source or destination ports. These can be used by organizations to register specific applications such as IM applications.
* **Private Ports -** Ports ***49152 through 65535*** are often used as source ports. These ports can be used by any application.

The source port number is dynamically generated by the sending device to identify a conversation between two devices. This process allows multiple conversations to occur simultaneously. It is common for a device to send multiple HTTP service requests to a web server at the same time. Each separate HTTP conversation is tracked based on the source ports.

The client places a destination port number in the segment to tell the destination server what service is being requested. A server can offer more than one service simultaneously, such as web services on port 80 at the same time that it offers FTP connection establishment on port 21.

Unexplained TCP connections can pose a major security threat. They can indicate that something or someone is connected to the local host. Sometimes it is necessary to know which active TCP connections are open and running on a networked host. ***Netstat*** is an important network utility that can be used to verify those connections. ***The command netstat is used to list the protocols in use, the local address and port numbers, the foreign address and port numbers, and the connection state***.

### Section 16

The term server refers to a host running a software application that provides information or services to other hosts that are connected to the network, such as a web server.

The key characteristic of client/server systems is that the client sends a request to a server, and the server responds by carrying out a function, such as sending the requested document back to the client.

 URI is a string of characters that identifies a specific network resource. The parts of a URI are protocol/scheme, hostname, path and file name, and fragment. A URI has two specializations:

* ****URN**** - This identifies only the namespace of the resource without reference to the protocol.
* ****URL**** - This defines the network location of a specific resource on the network. HTTP or HTTPS URLs are typically used with web browsers. Other protocols such as FTP, SFTP, SSH, and others can be used as a URL.

Common Network services include: DNS, SSH, SMTP, POP, IMAP, DHCP, HTTP, and FTP.

The DNS provides a way for hosts to request the IP address of a specific server. When the DNS server receives the request from a host, it checks its table to determine the IP address associated with that web server. If the local DNS server does not have an entry for the requested name, it queries another DNS server within the domain. When the DNS server learns the IP address, that information is sent back to the host.

***FTP*** provides an easy method to transfer files from one computer to another. A host running FTP client software can access an FTP server to perform various file management functions including file uploads and downloads.To begin an FTP session, control connection requests are sent to the server using destination TCP **port 21**. When the session is opened, the server uses TCP **port 20** to transfer the data files.

***Telnet*** provides a standard method of emulating text-based terminal devices over the data network. Both the protocol itself and the client software that implements the protocol are commonly referred to as Telnet. Telnet servers listen for client requests on **TCP port 23**

Telnet is not considered to be a secure protocol. Although the Telnet protocol can require a user to login, it does not support transporting encrypted data. All data exchanged during Telnet sessions is transported as plaintext across the network. This means that the data can be easily intercepted and understood.

SSH provides the structure for secure remote login and other secure network services. It also provides stronger authentication than Telnet and supports transporting session data using encryption. Network professionals should always use SSH in place of Telnet, whenever possible.

Each mail server receives and stores mail for users who have mailboxes configured on the mail server. Each user with a mailbox must then use an email client to access the mail server and read these messages. Many internet messaging systems use a web-based client to access email including Microsoft 365, Yahoo, and Gmail. Application protocols used in processing email include SMTP, POP3, and IMAP4.

***SMTP*** is used by an email client to send messages to its local email server. The local server then decides if the message is destined for a local mailbox or if the message is addressed to a mailbox on another server. If the server must send the message to a different server, SMTP is used between those two servers. SMTP requests are sent to ***port 25***.

A server that supports POP clients receives and stores messages addressed to its users. When the client connects to the email server, the messages are downloaded to the client. By default, messages are not kept on the server after they have been accessed by the client. Clients contact POP3 servers on ***port 110.***

A server that supports IMAP clients also receives and stores messages addressed to its users. However, unlike POP, IMAP keeps the messages in the mailboxes on the server, unless they are deleted by the user. The most current version of IMAP is IMAP4 which listens for client requests on ***port 143.***

Text messages may be called instant messages, direct messages, private messages, and chat messages. Text messaging enables users to chat over the internet in real-time. Text messaging services on a computer are usually accessed through a web-based client that is integrated into a social media or information sharing site. These clients usually only connect to other users of the same site.

An internet telephony client uses peer-to-peer technology similar to that used by instant messaging. IP telephony uses ***VoIP***, which converts analog voice signals into digital data. The voice data is encapsulated into IP packets which carry the phone call through the network.

### Section 17 (Troubleshooting Commands)

A number of software utility programs are available that can help identify network problems. Most of these utilities are provided by the operating system as CLI commands.

Some of the available utilities include:

ipconfig - Displays IP configuration information.

ping - Tests connections to other IP hosts.

netstat - Displays network connections.

tracert - Displays the route taken to the destination.

nslookup - Directly queries the name server for information on a destination domain.

The ipconfig command is used to display the current IP configuration information for a host. Issuing this command from the command prompt will display the basic configuration information including IP address, subnet mask, and default gateway.

The command ipconfig /all displays additional information including the MAC address, IP addresses of the default gateway, and the DNS servers. It also indicates if DHCP is enabled, the DHCP server address, and lease information.

If IP addressing information is assigned dynamically, the command ipconfig /release will release the current DHCP bindings. ipconfig /renew will request fresh configuration information from the DHCP server. A host may contain faulty or outdated IP configuration information and a simple renewal of this information is all that is required to regain connectivity.

Probably the most commonly used network utility is ping. Most IP enabled devices support some form of the ping command in order to test whether or not network devices are reachable through the IP network. When a ping is sent to an IP address, a packet known as an echo request is sent across the network to the IP address specified. If the destination host receives the echo request, it responds with a packet known as an echo reply. If the source receives the echo reply, connectivity is verified by the reply from the specific IP address.

Networking Devices and Initial Configuration

### Section 1

There are four basic characteristics that network architects must address to meet user expectations: ***Fault Tolerance, scalability, QoS, and security***.

A **fault tolerant** network limits the number of affected devices during a failure. It allows quick recovery when such a failure occurs. ***These networks depend on multiple paths between the source and destination of a message. If one path fails, the messages are instantly sent over a different link.***

A **scalable network** expands quickly to support new users and applications. It does this without degrading the performance of services that are being accessed by existing users. ***Networks can be scalable because the designers follow accepted standards and protocols.***

**QoS** is an increasing requirement of networks today. As data, voice, and video content continue to converge onto the same network, QoS becomes a primary mechanism for managing congestion and ensuring reliable delivery of content to all users. Network bandwidth is measured in bps. When simultaneous communications are attempted across the network, the demand for network bandwidth can exceed its availability, creating network congestion. The focus of QoS is to prioritize time-sensitive traffic. The type of traffic, not the content of the traffic, is what is important.

Network administrators must address two types of network **security concerns**: ***network infrastructure security and information security***. Network administrators must also protect the information contained within the packets being transmitted over the network, and the information stored on network attached devices. There are three primary requirements to achieve the goals of network security: ***Confidentiality, Integrity, and Availability.***

IP addresses contain two parts. One part identifies the network portion. The network portion of the IP address will be the same for all hosts connected to the same local network. The second part of the IP address identifies the individual host on that network. Both the physical MAC and logical IP addresses are required for a computer to communicate on a hierarchical network.

The Network and Sharing Center on a PC shows your basic network information and set up connections, including your active networks and whether you are connected wired or wirelessly to the internet and within your LAN.

***The access layer*** provides a connection point for end user devices to the network and allows multiple hosts to connect to other hosts through a network device, usually a switch or a wireless access point. Typically, all devices within a single access layer will have the same network portion of the IP address. The distribution layer provides a connection point for separate networks and controls the flow of information between the networks. ***Distribution layer devices*** control the type and amount of traffic that flows from the access layer to the core layer.

***The core layer*** is a high-speed backbone layer with redundant connections. It is responsible for transporting large amounts of data between multiple end networks. The main goal of the core layer is to transport data quickly.

### Section 2 (Cloud and Virtualization)

In general, when talking about the cloud, we are talking about ***data centers, cloud computing, and virtualization.*** Data centers are usually large facilities which provide massive amounts of power, cooling, and bandwidth. Only very large companies can afford their own data centers. Most smaller organizations lease the services from a cloud provider.  
***Cloud services*** include the following:

* SaaS – Software as a service
* PaaS – Platform as a service
* IaaS – Infrastructure as a service

There are four primary ***cloud models***

* Public clouds - Cloud-based applications and services offered in a public cloud are made available to the general population.
* Private clouds - Cloud-based applications and services offered in a private cloud are intended for a specific organization or entity, such as the government.
* Hybrid clouds - A hybrid cloud is made up of two or more clouds, where each part remains a separate object, but both are connected using a single architecture.
* Community clouds - A community cloud is created for exclusive use by a specific community. The differences between public clouds and community clouds are the functional needs that have been customized for the community.

Virtualization is the foundation of cloud computing. Without it, cloud computing, as it is most-widely implemented, would not be possible. Virtualization means creating a virtual rather than physical version of something, such as a computer. An example would be running a "Linux computer" on your Windows PC.

One major advantage of virtualization is overall reduced cost:

* Less equipment is required - Virtualization enables server consolidation, which requires fewer physical devices and lowers maintenance costs.
* Less energy is consumed - Consolidating servers lowers the monthly power and cooling costs.
* Less space is required - Server consolidation reduces the amount of required floor space.

These are additional benefits of virtualization:

* Easier prototyping - Self-contained labs, operating on isolated networks, can be rapidly created for testing and prototyping network deployments.
* Faster server provisioning - Creating a virtual server is far faster than provisioning a physical server.
* Increased server uptime - Most server virtualization platforms now offer advanced redundant fault tolerance features.
* Improved disaster recovery - Most enterprise server virtualization platforms have software that can help test and automate failover before a disaster happens.
* Legacy support - Virtualization can extend the life of OSs and applications providing more time for organizations to migrate to newer solutions.

***The hypervisor is a program, firmware, or hardware that adds an abstraction layer on top of the physical hardware. The abstraction layer is used to create virtual machines which have access to all the hardware of the physical machine such as CPUs, memory, disk controllers, and NICs***. Each of these virtual machines runs a complete and separate operating system.

Type 1 hypervisors are also called the “bare metal” approach because the hypervisor is installed directly on the hardware. Type 1 hypervisors are usually used on enterprise servers and data center networking devices.

A Type 2 hypervisor is software that creates and runs VM instances. The computer, on which a hypervisor is supporting one or more VMs, is a host machine. Type 2 hypervisors are also called hosted hypervisors. This is because the hypervisor is installed on top of the existing OS, such as macOS, Windows, or Linux. Then, one or more additional OS instances are installed on top of the hypervisor. A big advantage of Type 2 hypervisors is that management console software is not required.

Cloud computing involves computers, software, servers, network devices, and other services physically held at a remote location,Cloud computing allows people to save, manage, and access data on computer resources located on a remote network. Virtualization is used by the cloud computing vendors so they can provide multiple servers, networks, applications, operating systems, etc. to clients without having to buy the equipment for each one.

### Section 3 (Number Systems)

Binary is a numbering system that consists of the digits 0 and 1 called bits. In contrast, the decimal numbering system consists of 10 digits consisting of the digits 0 – 9. Hosts, servers, and network devices use binary addressing. Specifically, they use binary IPv4 addresses. For ease of use by people, IPv4 addresses are commonly expressed in dotted decimal notation.

This decimal system uses the powers of ten, or base 10. For example, the number 2,146 has a 2 in the thousands place, or two thousand. 2,146 has a 1 in the hundreds place, or one hundred. It has a 4 in the tens place, or forty. It has a 6 in the ones place, or six.

The binary system is a base 2 number system. Each place value can have a 0 or a 1. A useful tool is the binary positional value table. It is common to use a table with eight placeholders. 8 bits equal a byte.

The hexadecimal numbering system is used in networking to represent IP Version 6 addresses and Ethernet MAC addresses. This base sixteen number system uses the digits 0 to 9 and the letters A to F. Binary and hexadecimal work well together because it is easier to express a value as a single hexadecimal digit than as four binary bits.

IPv6 addresses are 128 bits in length and every 4 bits is represented by a single hexadecimal digit; for a total of 32 hexadecimal values. IPv6 addresses are not case-sensitive and can be written in either lowercase or uppercase.

### Section 4 (Ethernet Switching)

*Ethernet protocols* ***define how data is formatted and how it is transmitted over the wired network.*** Ethernet was created in ***1973 by Dr. Robert Metcalf of Xerox Corporation***,There is no official local area networking standard protocol, but over time, Ethernet, has become more common than the others. The Ethernet standards specify protocols that operate at ***Layer 1 and Layer 2 of the OSI model.*** Ethernet has become a de facto standard, which means that it is the technology used by almost all wired local area networks.

**IEEE** maintains the networking standards, including Ethernet and wireless standards. Each technology standard is assigned a number that refers to the committee that is responsible for approving and maintaining the standard. The ***802.3*** Ethernet standard has improved over time.(others were IEEE 802.4 = ARCnet and IEEE 802.5 = Token RIng)

Ethernet switches can send a frame out all ports (excluding the port it was received from). Each host that receives this frame examines the destination MAC address and compares it to their MAC address. It is the Ethernet NIC card that examines and compares the MAC address. If it does not match the host MAC address, the rest of the frame is ignored. When it is a match, that host receives the rest of the frame and the message it contains.

IEEE 802 LAN/MAN protocols, including Ethernet, use the following two separate sublayers of the data link layer to operate. They are the ***Logical Link Control (LLC)*** and the ***Media Access Control (MAC***)

Ethernet is defined by data link layer 802.2 and 802.3 protocols. Ethernet supports data bandwidths from 10 Mbps up to 100 Gps. EEE 802 LAN/MAN protocols, including Ethernet, use two separate sublayers of the data link layer to operate: LLC and MAC.

LLC Sublayer - This IEEE 802.2 sublayer communicates between the networking software at the upper layers and the device hardware at the lower layers. It places information in the frame that identifies which network layer protocol is being used for the frame. This information allows multiple Layer 3 protocols, such as IPv4 and IPv6, to use the same network interface and media.

MAC Sublayer - This sublayer (IEEE 802.3, 802.11, or 802.15 for example) is implemented in hardware and is responsible for data encapsulation and media access control. It provides data link layer addressing and is integrated with various physical layer technologies. Data encapsulation includes the ***Ethernet frame, Ethernet Addressing, and Ethernet error detection.***

The two Ethernet sublayers are LLC and MAC. LLC manages communications with the upper layers. MAC is the lower sublayer and is responsible for encapsulating the data and getting it onto the network media. In order to get the data onto the media, a specific process must be used. Ethernet uses the ***CSMA/CD*** process.

Ethernet LANs of today use switches that operate in full-duplex. Full-duplex communications with Ethernet switches do not require access control through CSMA/CD. The ***minimum Ethernet frame size is 64 bytes*** and the expected ***maximum is 1518 bytes***. The fields are ***Preamble and Start Frame Delimiter, Destination MAC address, Source MAC address, Type / Length, Data(data field contains the Layer 3 PDU, or an IP packet. This field has the minimum length of 46 bytes and maximum length of 1500 bytes. ), and FCS.*** This includes all bytes from the destination MAC address field through the FCS field. A ***runt frame*** is an Ethernet frame that is ***shorter than the minimum length*** of 64 bytes. Runt frames are automatically ***discarded*** by receiving stations

A unicast MAC address is the unique address that is used when a frame is sent from a single transmitting device to a single destination device.

The process that a source host uses to determine the destination MAC address associated with an IPv4 address is known as Address Resolution Protocol **(ARP)**. The process that a source host uses to determine the destination MAC address associated with an IPv6 address is known as Neighbor Discovery (**ND**).

An Ethernet broadcast frame is received and processed by every device on the Ethernet LAN, It has a destination MAC address of FF-FF-FF-FF-FF-FF in hexadecimal, DHCP for IPv4 is an example of a protocol that uses Ethernet and IPv4 broadcast addresses.ARP Requests do not use IPv4, but the ARP message is sent as an Ethernet broadcast.

**Nb:**If the encapsulated data is an IPv4 broadcast packet, this means the packet contains a destination IPv4 address that has all ones (1s) in the host portion

An Ethernet multicast frame is received and processed by a group of devices on the Ethernet LAN that belong to the same multicast group.

* There is a destination MAC address of ***01-00-5E-xx-xx-xx*** when the encapsulated data is an IPv4 multicast packet and a destination MAC address of ***33-33-xx-xx-xx-xx*** when the encapsulated data is an IPv6 multicast packet.
* There are other reserved multicast destination MAC addresses for when the encapsulated data is not IP, such as Spanning Tree Protocol (***STP***) and Link Layer Discovery Protocol (***LLDP***).
* It is flooded out all Ethernet switch ports except the incoming port, unless the switch is configured for multicast snooping.
* It is not forwarded by a router, unless the router is configured to route multicast packets.

The range of IPv4 multicast addresses is 224.0.0.0 to 239.255.255.255. The range of IPv6 multicast addresses begins with ff00::/8. Because multicast addresses

##### Switch Fundamentals;

A Layer 2 Ethernet switch uses Layer 2 MAC addresses to make forwarding decisions. An Ethernet switch examines its MAC address table to make a forwarding decision for each frame, MAC address table is sometimes referred to as a content addressable memory (CAM) table.

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. If the destination MAC address is a unicast address, the switch will look for a match between the destination MAC address of the frame and an entry in its MAC address table. If the destination MAC address is in the table, it will forward the frame out the specified port. If the destination MAC address is not in the table, the switch will forward the frame out all ports except the incoming port. This is called an ***unknown unicast.***

As a switch receives frames from different devices, it is able to populate its MAC address table by examining the source MAC address of every frame. When the MAC address table of the switch contains the destination MAC address, it is able to filter the frame and forward out a single port. A switch can have multiple MAC addresses associated with a single port. This is common when the switch is connected to another switch. The switch will have a separate MAC address table entry for each frame received with a different source MAC address. When a device has an IP address that is on a remote network, the Ethernet frame cannot be sent directly to the destination device. Instead, the Ethernet frame is sent to the MAC address of the ***default gateway,*** the router.

### Section 5 (The Network Layer)

The network layer, or OSI Layer 3, provides services to allow end devices to exchange data across networks. IPv4 and IPv6 are the principal network layer communication protocols. Other network layer protocols include routing protocols such as ***OSPF*** and messaging protocols such as ***ICMP.***

Network layer protocols perform four operations: ***addressing end devices, encapsulation, routing, and de-encapsulation.*** IPv4 and IPv6 specify the packet structure and processing used to carry the data from one host to another host. Operating without regard to the data carried in each packet allows the network layer to carry packets for multiple types of communications between multiple hosts.

IP encapsulates the transport layer segment or other data(PDU- protocol data unit) by adding an IP header. The IP header is used to deliver the packet to the destination host. The IP header is examined by routers and Layer 3 switches as it travels across a network to its destination. IP addressing information remains the same from the time the packet leaves the source host until it arrives at the destination host, except when translated by the device performing NAT for IPv4.

The basic ***characteristics of IP*** are that it is: ***connectionless, best effort, and media independent.*** IP is connectionless, meaning that no dedicated end-to-end connection is created by IP before data is sent. IP does not require additional fields in the header to maintain an established connection. This reduces the overhead of IP. Senders are unaware whether destination devices are present and functional when sending packets, nor are they aware if the destination receives the packet, or if the destination device is able to access and read the packet. IP operates independently of the media that carry the data at lower layers of the protocol stack. IP packets can be communicated as electronic signals over copper cable, as optical signals over fiber, or wirelessly as radio signals. ***One characteristic of the media that the network layer considers is the maximum size of the PDU that each medium can transport, or the MTU.***

#### IPv4 Packet header (20 bytes)

The IPv4 packet header is used to ensure that a packet is delivered to its next stop on the way to its destination end device. An IPv4 packet header consists of fields containing binary numbers which are examined by the Layer 3 process. Significant fields in the IPv4 header include:

***Version;***  4-bit binary value set to 0100 that identifies this as an IPv4 packet.

***DS,*** an 8-bit field used to determine the priority of each packet, the six most significant bits of the ***DiffServ*** field are the differentiated services code point (DSCP) bits and the last two bits are the explicit congestion notification (ECN) bits.

***TTL,***TTL contains an 8-bit binary value that is used to limit the lifetime of a packet. If the TTL field decrements to zero, the router discards the packet and sends an Internet Control Message Protocol (ICMP) Time Exceeded message to the source IP address.

***protocol,*** 8-bit field used to identify the next level protocol. Common values data payloads include ICMP (1), TCP (6), and UDP (17).

***header checksum,*** This is used to detect corruption in the IPv4 header.

***source IPv4 address, and destination IPv4 address;***  a 32-bit binary value that represents the source and destination IPv4 address The IHL, Total Length, and Header Checksum fields are used to identify and validate the packet. The IPv4 packet uses Identification, Flags, and Fragment Offset fields to keep track of the fragments. A router may have to fragment an IPv4 packet when forwarding it from one medium to another with a smaller MTU.

#### IPv6 Packet header

The IPv6 header is a fixed length of ***40 octets*** and contains ***8 header fields***.

IPv4 has limitations, including: IPv4 address depletion, lack of end-to-end connectivity, and increased network complexity. IPv6 overcomes the limitations of IPv4. Improvements that IPv6 provides include the following: increased address space, improved packet handling, and it eliminates the need for NAT.

The 32-bit IPv4 address space provides approximately 4,294,967,296 unique addresses. IPv6 address space provides 340,282,366,920,938,463,463,374,607,431,768,211,456, or 340 undecillion addresses. This is roughly equivalent to every grain of sand on Earth.

The IPv6 simplified header fields include***:***

***version,***  a 4-bit binary value set to 0110

***traffic class,*** 8-bit field is equivalent to the IPv4 Differentiated Services (DS) field.

***flow label, t***his 20-bit field suggests that all packets with the same flow label receive the same type of handling by routers.

***payload length,*** This 16-bit field indicates the length of the data portion or payload of the IPv6 packet. This does not include the length of the IPv6 header, which is a fixed 40-byte header.

***next header,*** this 8-bit field is equivalent to the IPv4 Protocol field. It indicates the data payload type that the packet is carrying, enabling the network layer to pass the data to the appropriate upper-layer protocol

***hop limit,*** This 8-bit field replaces the IPv4 TTL field. This value is decremented by a value of 1 by each router that forwards the packet. When the counter reaches 0, the packet is discarded, and an ICMPv6 Time Exceeded message is forwarded to the sending host,. This indicates that the packet did not reach its destination because the hop limit was exceeded. Unlike IPv4, IPv6 does not include an IPv6 Header Checksum, because this function is performed at both the lower and upper layers. This means the checksum does not need to be recalculated by each router when it decrements the Hop Limit field, which also improves network performance

***source IP address, and destination IP address***.

An IPv6 packet may also contain EH, which provide optional network layer information. Extension headers are optional and are placed between the IPv6 header and the payload. EHs are used for fragmentation, security, to support mobility and more. Unlike IPv4, routers do not fragment routed IPv6 packets.

### Section 6 ( Network and Host Portions)

IPv4 Address Structure  
An IPv4 address is a 32-bit hierarchical address that is made up of a network portion and a host portion. When determining the network portion versus the host portion, you must look at the 32-bit stream. The bits within the network portion of the address must be identical for all devices that reside in the same network. The bits within the host portion of the address must be unique to identify a specific host within a network. If two hosts have the same bit-pattern in the specified network portion of the 32-bit stream, those two hosts will reside in the same network.

The IPv4 subnet mask is used to differentiate the network portion from the host portion of an IPv4 address. When an IPv4 address is assigned to a device, the subnet mask is used to determine the network address of the device. The network address represents all the devices on the same network.

An alternative method of identifying a subnet mask, a method called the prefix length. The prefix length is the number of bits set to 1 in the subnet mask. It is written in “slash notation”, which is noted by a forward slash (/) followed by the number of bits set to 1. For example, 192.168.10.10 255.255.255.0 would be written as 192.168.10.10/24.

The AND operation is used in determining the network address. Logical AND is the comparison of two bits. Note how only a 1 AND 1 produces a 1. Any other combination results in a 0.

1 AND 1 = 1

0 AND 1 = 0

1 AND 0 = 0

0 AND 0 = 0

To identify the network address of an IPv4 host, the IPv4 address is logically ANDed, bit by bit, with the subnet mask. ANDing between the address and the subnet mask yields the network address.

Other Layer 3 protocols:

***ICMP  Internet Control Message Protocol***

***OSPF Open Short Path First***

Mac vendors look up: [https://www.wireshark.org/tools/oui-lookup.html](https://www.wireshark.org/tools/oui-lookup.html" \t "https://www.netacad.com/content/ndic/1.0/courses/content/m4/en-US/assets/_blank).

MAC addresses are 48 bit **(6 bytes)** long and are written in hexadecimal notation. MAC addresses are made up of two parts, the first **3 bytes,** represents the vendor who manufactured the network interface, and is called the OUI (***Organizationally Unique Identifier***). Each vendor who wants to make and sell Ethernet network interfaces must register with the **IEEE** in order to be assigned an OUI. The remaining is the ***Unique Identifier for the Interface***

The **arp**command , Enter **arp /?**at the command prompt and press enter. The **arp**command options enable you to view, add and remove ARP table entries if necessary.

Your computer always checks its local cache before requesting information from other devices on the network. The ARP cache retains dynamically learned address bindings for a short period of time. When traffic is exchanged often between source and destination, the ARP cache prevents the host from needlessly broadcasting ARP requests.

RFID tags