What is packet tracer ?

Packet Tracer is a **network simulation tool** developed by **Cisco** that allows users to create, configure, and simulate complex network topologies. It is widely used for **learning networking concepts**, especially for **CCNA (Cisco Certified Network Associate) training** and other networking certifications.

Hubs were the earliest devices used to interconnect computers in a network. Their simplicity meant that every data packet was broadcast to all devices, leading to collisions and inefficiencies. While they were cost-effective and easy to use, their limitations in performance and security eventually rendered them obsolete in favor of more intelligent devices.
Switches emerged as the natural successor to hubs. By operating at the data link layer and using MAC addresses to direct traffic, switches dramatically improved network performance and security. They effectively create separate collision domains for each port, ensuring that data is only sent to the intended recipient. Modern switches also offer advanced features such as VLANs, QoS, and even Layer 3 routing capabilities in certain cases, making them the backbone of modern LANs.
Routers serve as the gateways between networks. Operating at the network layer, routers use IP addresses and routing protocols to determine the best paths for data to travel across different networks. Their ability to segment broadcast domains, enforce security policies, and dynamically adjust to network changes makes them indispensable for inter-network communication, whether it's connecting a local network to the internet or linking multiple corporate sites together.

What is Host?

All computers that are connected to a network and participate directly in network communication are classified as hosts. Hosts can be called end devices. Some hosts are also called clients. However, the term hosts specifically refers to devices on the network that are assigned a number for communication purposes. This number identifies the host within a particular network. This number is called the Internet Protocol (IP) address. An IP address identifies the host and the network to which the host is attached.

What is p2p network?

Client and server software usually run on separate computers, but it is also possible for one computer to be used for both roles 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 peer-to-peer network.

What are end devices ?

The network devices that people are most familiar with are end devices. To distinguish one end device from another, each end device on a network has an address. When an end

device initiates communication, it uses the address of the destination end device to specify where to deliver the message.

What is NIC?

A **Network Interface Card (NIC)** is a hardware component that allows a computer or other device to connect to a network. It can be built into the motherboard (integrated) or added as a separate expansion card. Here's a breakdown of what a NIC is and how it works:

LANs

A LAN is a network infrastructure that spans a small geographical area. LANs have specific characteristics:

- LANs interconnect end devices in a limited area such as a home, school, office building, or campus.
- A LAN is usually administered by a single organization or individual. Administrative control is enforced at the network level and governs the security and access control policies.
- LANs provide high-speed bandwidth to internal end devices and intermediary devices, as shown in the figure.

WANs

The figure shows a WAN which interconnects two LANs. A WAN is a network infrastructure that spans a wide geographical area. WANs are typically managed by service providers (SPs) or Internet Service Providers (ISPs).

WANs have specific characteristics:

- WANs interconnect LANs over wide geographical areas such as between cities, states, provinces, countries, or continents.
- WANs are usually administered by multiple service providers.
- WANs typically provide slower speed links between LANs.

What is Intranet ?

Intranet is a term often used to refer to a private connection of LANs and WANs that belongs to an organization. An intranet is designed to be accessible only by the organization's members, employees, or others with authorization.

What is DSL?

DSL is a technology used to deliver digital data over the copper wires of the telephone network. Unlike traditional dial-up connections that require the line to be exclusively used for data (preventing simultaneous voice calls), DSL separates the frequency bands used for voice and data. This allows users to make phone calls and access the Internet at the same time.

==========

As networks evolve, we have learned that there are four basic characteristics that network architects must address to meet user expectations:

- Fault Tolerance
- Scalability
- Quality of Service (QoS)
- Security

Fault Tolerance

A fault tolerant network is one that limits the number of affected devices during a failure. It is built to allow 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. Having multiple paths to a destination is known as redundancy.

Implementing a packet-switched network is one way that reliable networks provide redundancy. Packet switching splits traffic into packets that are routed over a shared network. A single message, such as an email or a video stream, is broken into multiple message blocks, called packets. Each packet has the necessary addressing information of the source and destination of the message. The routers within the network switch the packets based on the condition of the network at that moment. This means that all the packets in a single messsage could take very different paths to the same destination. In the figure, the user is unaware and unaffected by the router that is dynamically changing the route when a link fails.

Scalability

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. The figure shows how a new network is easily added to an existing network. These networks are scalable because the designers follow accepted standards and protocols. This lets software and hardware vendors focus on improving products and services without having to design a new set of rules for operating within the network.

Quality of Service (QoS) is an increasing requirement of networks today. New applications available to users over networks, such as voice and live video transmissions, create higher expectations for the quality of the delivered services. Have you ever tried to watch a video with constant breaks and pauses? 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.

Congestion occurs when the demand for bandwidth exceeds the amount available. Network bandwidth is measured in the number of bits that can be transmitted in a single second, or bits per second (bps). When simultaneous communications are attempted across the network, the demand for network bandwidth can exceed its availability, creating network congestion.

When the volume of traffic is greater than what can be transported across the network, devices will hold the packets in memory until resources become available to transmit them. In the figure, one user is requesting a web page, and another is on a phone call. With a QoS policy in place, the router can manage the flow of data and voice traffic, giving priority to voice communications if the network experiences 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.

—----------

As new technologies and end-user devices come to market, businesses and consumers must continue to adjust to this ever-changing environment. There are several networking trends that affect organizations and consumers:

- Bring Your Own Device (BYOD)
- Online collaboration
- Video communications
- Cloud Computing

Network Security

There are several common external threats to networks:

- **Viruses, worms, and Trojan horses** - These contain malicious software or code running on a user device.
- **Spyware and adware** - These are types of software which are installed on a user's device. The software then secretly collects information about the user.
- **Zero-day attacks** - Also called zero-hour attacks, these occur on the first day that a vulnerability becomes known.

- **Threat actor attacks** - A malicious person attacks user devices or network resources.
- **Denial of service attacks** - These attacks slow or crash applications and processes on a network device.
- **Data interception and theft** - This attack captures private information from an organization's network.
- **Identity theft** - This attack steals the login credentials of a user in order to access private data.

These are the basic security components for a home or small office network:

- **Antivirus and antispyware** - These applications help to protect end devices from becoming infected with malicious software.
- **Firewall filtering** - Firewall filtering blocks unauthorized access into and out of the network. This may include a host-based firewall system that prevents unauthorized access to the end device, or a basic filtering service on the home router to prevent unauthorized access from the outside world into the network.

Modes in IOS

- User EXEC Mode - This mode has limited capabilities but is useful for basic operations. It allows only a limited number of basic monitoring commands but does not allow the execution of any commands that might change the configuration of the device. The user EXEC mode is identified by the CLI prompt that ends with the > symbol.
- Privileged EXEC Mode - To execute configuration commands, a network administrator must access privileged EXEC mode. Higher configuration modes, like global configuration mode, can only be reached from privileged EXEC mode. The privileged EXEC mode can be identified by the prompt ending with the # symbol.

2.2.4 Navigate Between IOS Modes

Various commands are used to move in and out of command prompts. To move from user EXEC mode to privileged EXEC mode, use the **enable** command. Use the **disable** privileged EXEC mode command to return to user EXEC mode.

Note: Privileged EXEC mode is sometimes called *enable mode*.

To move in and out of global configuration mode, use the **configure terminal** privileged EXEC mode command. To return to the privileged EXEC mode, enter the **exit** global config mode command.

There are many different subconfiguration modes. For example, to enter line subconfiguration mode, you use the **line** command followed by the management line type and number you wish to access. Use the **exit** command to exit a subconfiguration mode and return to global configuration mode.

? in IOS

n Cisco IOS, the ? (question mark) is used as a context-sensitive help command that provides guidance on available commands and their options. It helps users explore the command-line interface (CLI) and understand the syntax of commands.

Switches Module recap

All end devices and network devices require an operating system (OS). The user can interact with the shell using a command-line interface (CLI) to use a keyboard to run CLI-based network programs, use a keyboard to enter text and text-based commands, and view output on a monitor.

As a security feature, the 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 subconfiguration modes. Each of these modes allows the configuration of a particular part or function of the

IOS device. Two common subconfiguration modes include: Line Configuration Mode and Interface Configuration Mode. To move in and out of global configuration mode, use the **configure terminal** privileged EXEC mode command. To return to the privileged EXEC mode, enter the **exit** global config mode command.

Each IOS command has a specific format or syntax and can only be executed in the appropriate mode. The general syntax for a command is the command followed by any appropriate keywords and arguments. The IOS has two forms of help available: context-sensitive help and command syntax check.

The first configuration command on any device should be to give it a unique device name or hostname. Network devices should always have passwords configured to limit administrative access. Cisco IOS can be configured to use hierarchical mode passwords to allow different access privileges to a network device. Configure and encrypt all passwords. Provide a method for declaring that only authorized personnel should attempt to access the device by adding a banner to the device output.

There are two system files that store the device configuration: startup-config and running-config. Running configuration files can be altered if they have not been saved. Configuration files can also be saved and archived to a text document.

IP addresses enable devices to locate one another and establish end-to-end communication on the internet. Each end device on a network must be configured with an IP address. The structure of an IPv4 address is called dotted decimal notation and is represented by four decimal numbers between 0 and 255.

IPv4 address information can be entered into end devices manually, or automatically using Dynamic Host Configuration Protocol (DHCP). In a network, DHCP enables automatic IPv4 address configuration for every end device that is DHCP-enabled. To access the switch remotely, an IP address and a subnet mask must be configured on the SVI. To configure an SVI on a switch, use the **interface vlan 1** command in global configuration mode.

In the same way that you use commands and utilities to verify a PC host's network configuration, you also use commands to verify the interfaces and address settings of intermediary devices like switches and routers. The **show ip interface brief** command verifies the condition of the switch interfaces. The **ping** command can be used to test connectivity to another device on the network or a website on the internet.

Internet Standards

Various organizations have different responsibilities for promoting and creating standards for the internet and TCP/IP protocol.

- **Internet Society (ISOC)** - Responsible for promoting the open development and evolution of internet use throughout the world.
- **Internet Architecture Board (IAB)** - Responsible for the overall management and development of internet standards.
- **Internet Engineering Task Force (IETF)**- Develops, updates, and maintains internet and TCP/IP technologies. This includes the process and documents for developing new protocols and updating existing protocols, which are known as Request for Comments (RFC) documents.
- **Internet Research Task Force (IRTF)**- Focused on long-term research related to internet and TCP/IP protocols such as Anti-Spam Research Group (ASRG), Crypto Forum Research Group (CFRG), and Peer-to-Peer Research Group (P2PRG).
- **Internet Corporation for Assigned Names and Numbers (ICANN)**- Based in the United States, ICANN coordinates IP address allocation, the

management of domain names, and assignment of other information used in TCP/IP protocols.
- **Internet Assigned Numbers Authority (IANA)**- Responsible for overseeing and managing IP address allocation, domain name management, and protocol identifiers for ICANN.

Protocol Data Units

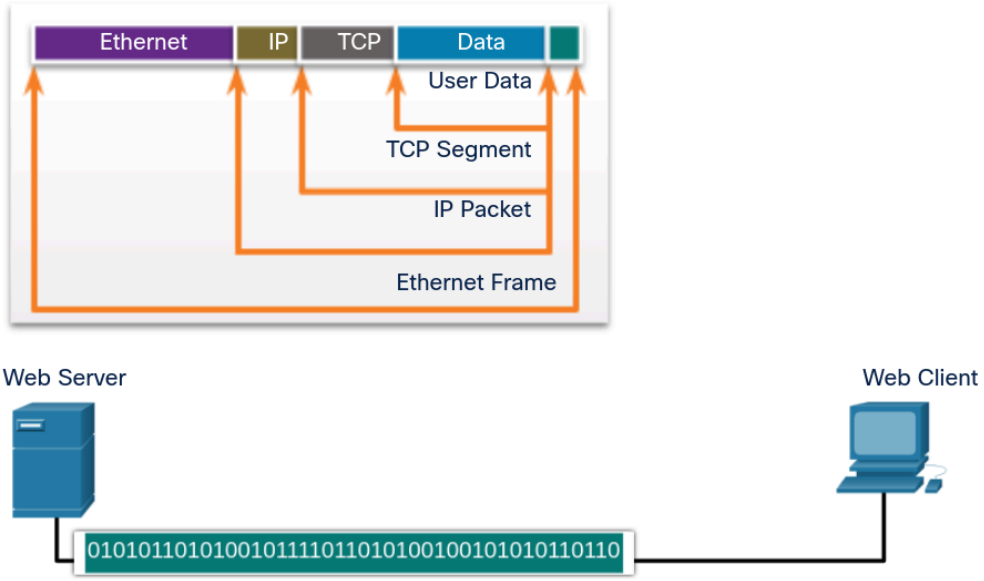
As application data is passed down the protocol stack on its way to be transmitted across the network media, various protocol information is added at each level. This is known as the encapsulation process.

Note: Although the UDP PDU is called datagram, IP packets are sometimes also referred to as IP datagrams.

The form that a piece of data takes at any layer is called a protocol data unit (PDU). During encapsulation, each succeeding layer encapsulates the PDU that it receives from the layer above in accordance with the protocol being used. At each stage of the process, a PDU has a different name to reflect its new functions. Although there is no universal naming convention for PDUs

- Data - The general term for the PDU used at the application layer
- Segment - Transport layer PDU
- Packet - Network layer PDU
- Frame - Data Link layer PDU
- Bits - Physical layer PDU used when physically transmitting data over the medium

Note: If the Transport header is TCP, then it is a segment. If the Transport header is UDP then it is a datagram.



3.6.5 De-encapsulation Example

This process is reversed at the receiving host and is known as de-encapsulation. De-encapsulation is the process used by a receiving device to remove one or more of the protocol headers. The data is de-encapsulated as it moves up the stack toward the end-user application.

Layer 3 logical address

The IP packet contains two IP addresses:

- **Source IP address** - The IP address of the sending device, which is the original source of the packet.
- **Destination IP address** - The IP address of the receiving device, which is the final destination of the packet.

The IP addresses indicate the original source IP address and final destination IP address. This is true whether the source and destination are on the same IP network or different IP networks.

An IP address contains two parts:

- **Network portion (IPv4) or Prefix (IPv6)** - The left-most part of the address that indicates the network in which the IP address is a member. All devices on the same network will have the same network portion of the address.
- **Host portion (IPv4) or Interface ID (IPv6)** - The remaining part of the address that identifies a specific device on the network. This portion is unique for each device or interface on the network.

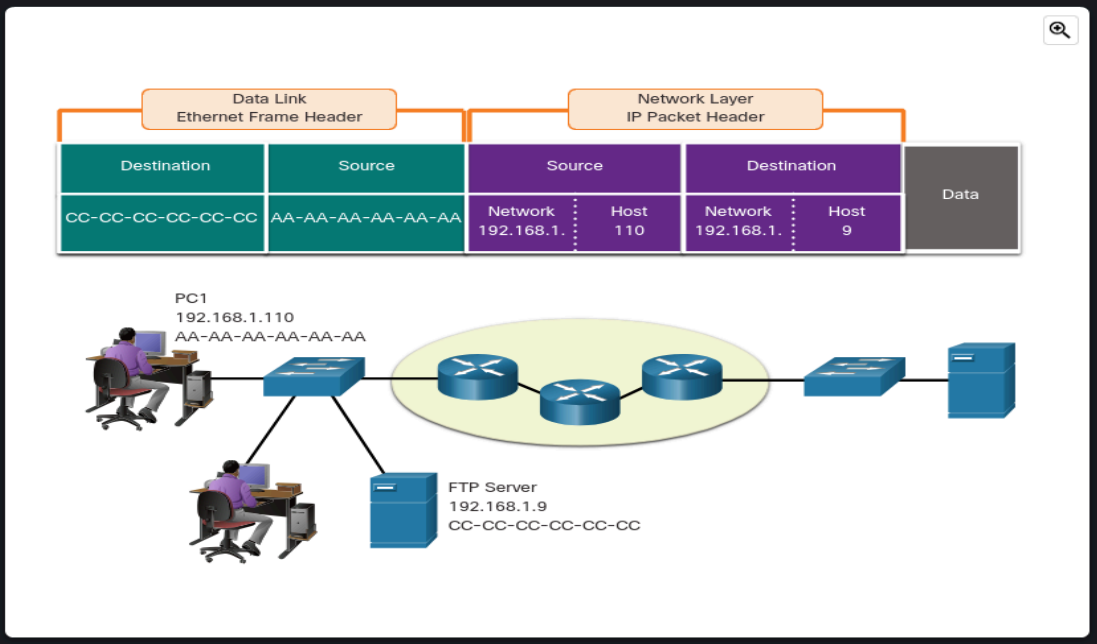
Note: The subnet mask (IPv4) or prefix-length (IPv6) is used to identify the network portion of an IP address from the host portion.

3.7.3 Devices on the Same Network

In this example we have a client computer, PC1, communicating with an FTP server on the same IP network.

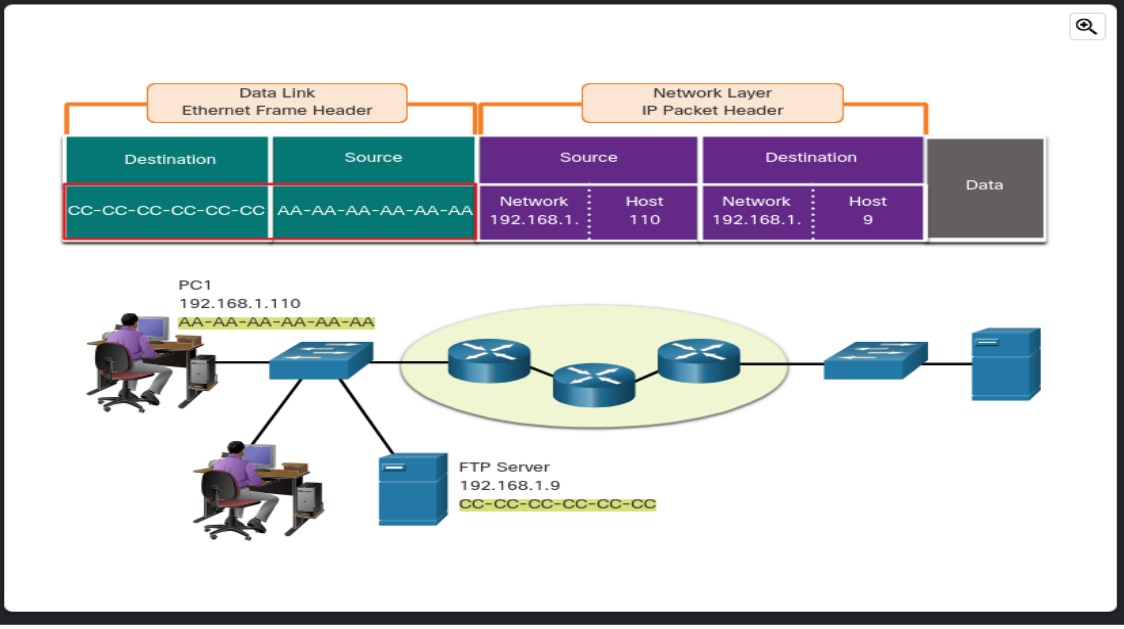
- **Source IPv4 address** - The IPv4 address of the sending device, the client computer PC1: 192.168.1.110.
- **Destination IPv4 address** - The IPv4 address of the receiving device, FTP server: 192.168.1.9.

Notice in the figure that the network portion of the source IPv4 address and the network portion of the destination IPv4 address are the same and therefore; the source and destination are on the same network.



3.7.4 Role of the Data Link Layer Addresses - Same IP Network

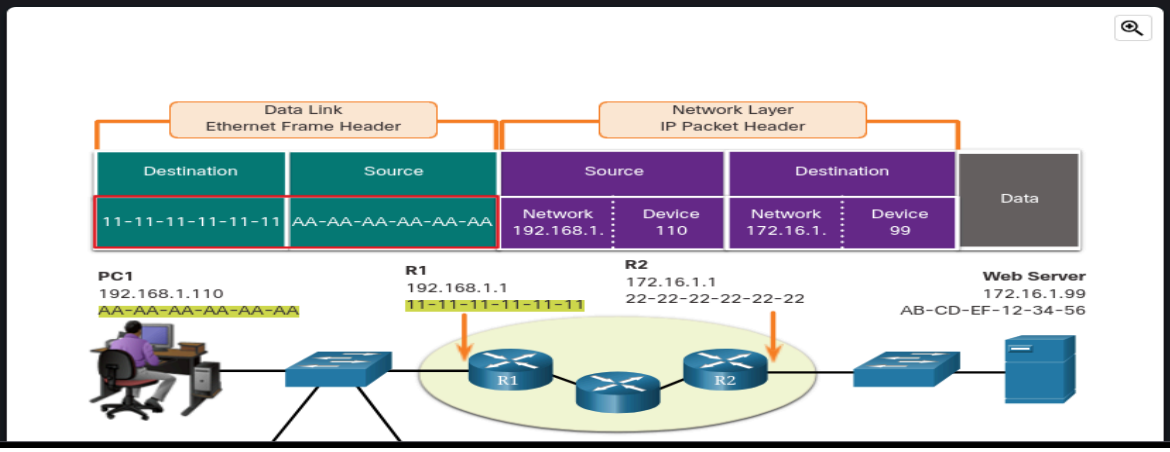
When the sender and receiver of the IP packet are on the same network, the data link frame is sent directly to the receiving device. On an Ethernet network, the data link addresses are known as Ethernet Media Access Control (MAC) addresses, as highlighted in the figure.



3.7.7 Role of the Data Link Layer Addresses - Different IP Networks

When the sender and receiver of the IP packet are on different networks, the Ethernet data link frame cannot be sent directly to the destination host because the host is not directly reachable in the network of the sender. The Ethernet frame must be sent to another device known as the router or default gateway. In our example, the default gateway is R1. R1 has an Ethernet data link address that is on the same network as PC1. This allows PC1 to reach the router directly.

- **Source MAC address** - The Ethernet MAC address of the sending device, PC1. The MAC address of the Ethernet interface of PC1 is AA-AA-AA-AA-AA-AA.
- **Destination MAC address** - When the receiving device, the destination IP address, is on a different network from the sending device, the sending device uses the Ethernet MAC address of the default gateway or router. In this example, the destination MAC address is the MAC address of the R1 Ethernet interface, 11-11-11-11-11-11. This is the interface that is attached to the same network as PC1, as shown in the figure.



Reacap: Protocols and Models

The Rules

All communication methods have three elements in common: message source (sender), message destination (receiver), and channel. Sending a message is governed by rules called *protocols*. Protocols must include: an identified sender and receiver, common language and grammar, speed and timing of delivery, and confirmation or acknowledgment requirements. Common computer protocols include these requirements: message encoding, formatting and encapsulation, size, timing, and delivery options. Encoding is the process of converting information into another acceptable form, for transmission. Decoding reverses this process to interpret the information. Message formats depend on the type of message and the channel that is used to deliver the message. Message timing includes flow control, response timeout, and access method. Message delivery options include unicast, multicast, and broadcast.

Protocols

Protocols are implemented by end-devices and intermediary devices in software, hardware, or both. A message sent over a computer network typically requires the use of several protocols, each one with its own functions and format. Each network protocol has its own function, format, and rules for communications. The Ethernet family of protocols includes IP, TCP, HTTP, and many more. Protocols secure data to provide authentication, data integrity, and data encryption: SSH, SSL, and TLS. Protocols enable routers to exchange route

information, compare path information, and then to select the best path to the destination network: OSPF and BGP. Protocols are used for the automatic detection of devices or services: DHCP and DNS. Computers and network devices use agreed-upon protocols that provide the following functions: addressing, reliability, flow control, sequencing, error-detection, and application interface.

Protocol Suites

A protocol suite is a group of inter-related protocols necessary to perform a communication function. A protocol stack shows how the individual protocols within a suite are implemented. Since the 1970s there have been several different protocol suites, some developed by a standards organization and others developed by various vendors. TCP/IP protocols are available for the application, transport, and internet layers. TCP/IP is the protocol suite used by today's networks and internet. TCP/IP offers two important aspects to vendors and manufacturers: open standard protocol suite, and standards-based protocol suite. The TCP/IP protocol suite communication process enables such processes as a web server encapsulating and sending a web page to a client, as well as the client de-encapsulating the web page for display in a web browser.

Standards Organizations

Open standards encourage interoperability, competition, and innovation. Standards organizations are usually vendor-neutral, non-profit organizations established to develop and promote the concept of open standards. Various organizations have different responsibilities for promoting and creating standards for the internet including: ISOC, IAB, IETF, and IRTF. Standards organizations that develop and support TCP/IP include: ICANN and IANA. Electronic and communications standards organizations include: IEEE, EIA, TIA, and ITU-T.

Reference Models

The two reference models that are used to describe network operations are OSI and TCP/IP. The OSI model has seven layers:

7 - Application

6 - Presentation

5 - Session

4 - Transport

3 - Network

2 - Data Link

1 - Physical

The TCP/IP model has four layers:

4 - Application

3 - Transport

2 - Internet

1 - Network Access

Data Encapsulation

Segmenting messages has two primary benefits:

- By sending smaller individual pieces from source to destination, many different conversations can be interleaved on the network. This is called *multiplexing*.
- Segmentation can increase the efficiency of network communications. If part of the message fails to make it to the destination only the missing parts need to be retransmitted.

TCP is responsible for sequencing the individual segments. The form that a piece of data takes at any layer is called a *protocol data unit (PDU)*. During encapsulation, each succeeding layer encapsulates the PDU that it receives from the layer above in accordance with the protocol being used. When sending messages on a network, the encapsulation process works from top to bottom. This process is reversed at the receiving host and is known as *de-encapsulation*. De-encapsulation is the process used by a receiving device to remove one or more of the protocol headers. The data is de-encapsulated as it moves up the stack toward the end-user application.

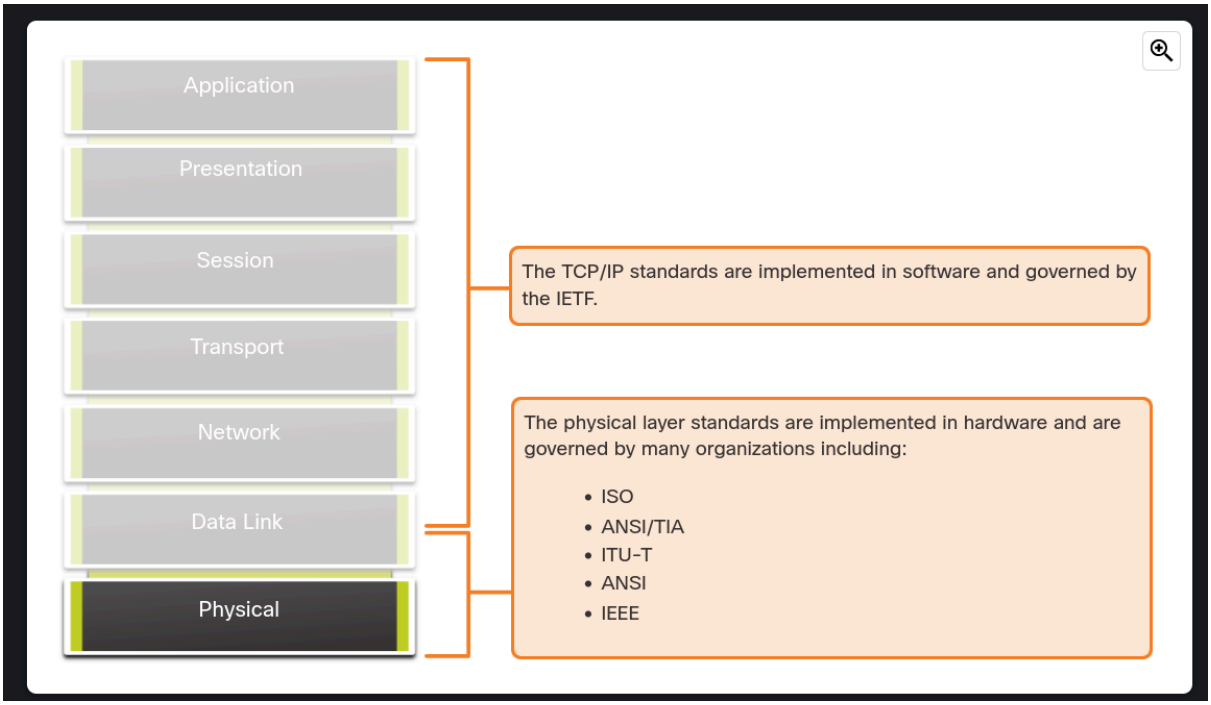
Data Access

The network and data link layers are responsible for delivering the data from the source device to the destination device. Protocols at both layers contain a source and destination address, but their addresses have different purposes:

- **Network layer source and destination addresses** - Responsible for delivering the IP packet from the original source to the final destination, which may be on the same network or a remote network.
- **Data link layer source and destination addresses** - Responsible for delivering the data link frame from one network interface card (NIC) to another NIC on the same network.

The IP addresses indicate the original source IP address and final destination IP address. An IP address contains two parts: the network portion (IPv4) or Prefix (IPv6) and the host portion (IPv4) or Interface ID (IPv6). When the sender and receiver of the IP packet are on the same network, the data link frame is sent directly to the receiving device. On an Ethernet network, the data link addresses are known as Ethernet Media Access Control (MAC) addresses. When the sender of the packet is on a different network from the receiver, the source and destination IP addresses will represent hosts on different networks. The Ethernet frame must be sent to another device known as the router or default gateway.

Physical Layer



Bandwidth

4.2.5 Bandwidth

Different physical media support the transfer of bits at different rates. Data transfer is usually discussed in terms of bandwidth. Bandwidth is the capacity at which a medium can 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 kilobits per second (kbps), megabits per second (Mbps), or gigabits per second (Gbps). Bandwidth is sometimes thought of as the speed that bits travel, however this is not accurate. For example, in both 10Mbps and 100Mbps Ethernet, the bits are sent at the speed of electricity. The difference is the number of bits that are transmitted per second.

A combination of factors determines the practical bandwidth of a network:

- The properties of the physical media
- The technologies chosen for signaling and detecting network signals

Physical media properties, current technologies, and the laws of physics all play a role in determining the available bandwidth.

The table shows the commonly used units of measure for bandwidth.

Unit of Bandwidth	Abbreviation	Equivalence
Bits per second	bps	1 bps = fundamental unit of bandwidth
Kilobits per second	Kbps	1 Kbps = 1,000 bps = 10^3 bps
Megabits per second	Mbps	1 Mbps = 1,000,000 bps = 10^6 bps
Gigabits per second	Gbps	1 Gbps = 1,000,000,000 bps = 10^9 bps
Terabits per second	Tbps	1 Tbps = 1,000,000,000,000 bps = 10^{12} bps

4.4.1 Properties of UTP Cabling

In the previous topic, you learned a bit about unshielded twisted-pair (UTP) copper cabling. Because UTP cabling is the standard for use in LANs, this topic goes into detail about its advantages and limitations, and what can be done to avoid problems.

When used as a networking medium, UTP cabling consists of four pairs of color-coded copper wires that have been twisted together and then encased in a flexible plastic sheath. Its small size can be advantageous during installation.

UTP cable does not use shielding to counter the effects of EMI and RFI. Instead, cable designers have discovered other ways that they can limit the negative effect of crosstalk:

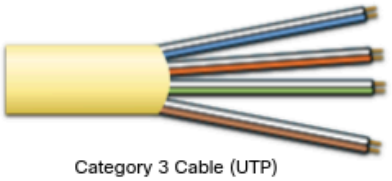
- **Cancellation** - Designers now pair wires in a circuit. When two wires in an electrical circuit are placed close together, their magnetic fields are the exact opposite of each other. Therefore, the two magnetic fields cancel each other and also cancel out any outside EMI and RFI signals.
- **Varying the number of twists per wire pair** - To further enhance the cancellation effect of paired circuit wires, designers vary the number of twists of each wire pair in a cable. UTP cable must follow precise specifications governing how many twists or braids are permitted per meter (3.28 feet) of cable. Notice in the figure that the orange/orange white pair is twisted less than the blue/blue white pair. Each colored pair is twisted a different number of times.

UTP cable relies solely on the cancellation effect produced by the twisted wire pairs to limit signal degradation and effectively provide self-shielding for wire pairs within the network media.

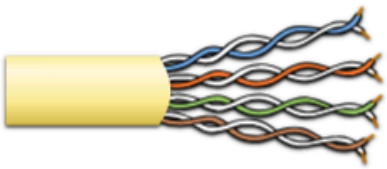
The figure shows three categories of UTP cable:

- Category 3 was originally used for voice communication over voice lines, but later used for data transmission.
- Category 5 and 5e is used for data transmission. Category 5 supports 100Mbps and Category 5e supports 1000 Mbps
- Category 6 has an added separator between each wire pair to support higher speeds. Category 6 supports up to 10 Gbps.
- Category 7 also supports 10 Gbps.
- Category 8 supports 40 Gbps.

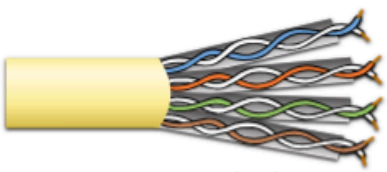
Some manufacturers are making cables exceeding the TIA/EIA Category 6a specifications and refer to these as Category 7.



Category 3 Cable (UTP)

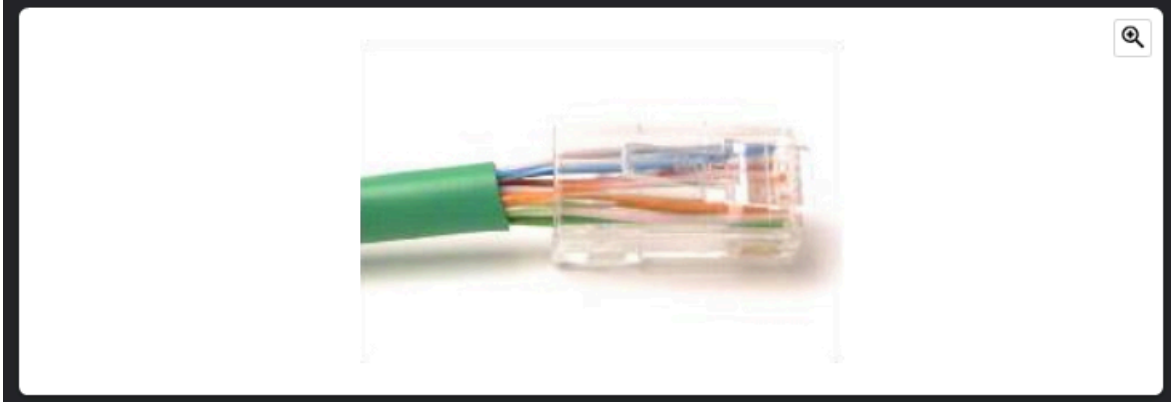


Category 5 and 5e Cable (UTP)



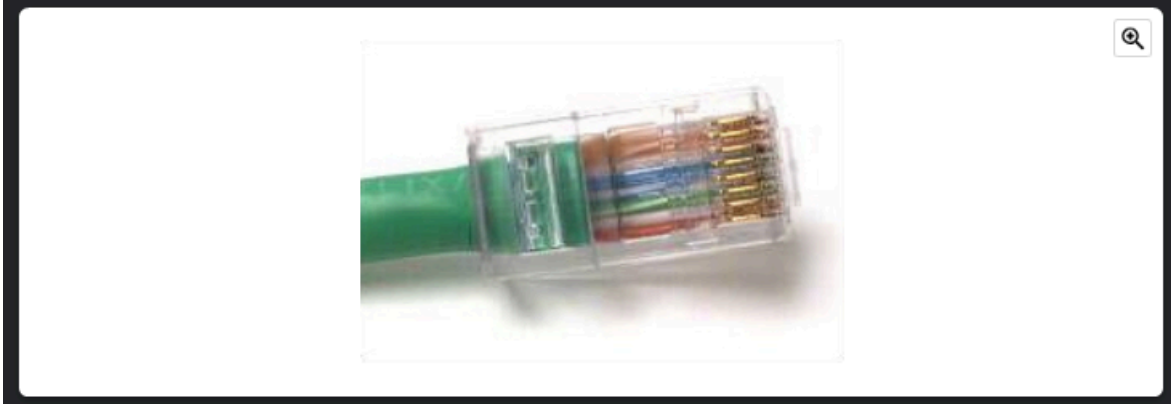
Category 6 Cable (STP)

Poorly Terminated UTP Cable



The next figure shows a properly terminated UTP cable. It is a good connector with wires that are untwisted only to the extent necessary to attach the connector.

Properly Terminated UTP Cable



Note: Improper cable termination can impact transmission performance.

Physical Layer Recap
Purpose of the Physical Layer

Before any network communications can occur, a physical connection to a local network must be established. A physical connection can be a wired connection using a cable or a wireless connection using radio waves. Network Interface Cards (NICs) connect a device to the network. Ethernet NICs are used for a wired connection, whereas WLAN (Wireless Local Area Network) NICs are used for wireless. The OSI physical layer provides the means to transport the bits that make up a data link layer frame across the network media. This layer accepts a complete frame from the data link layer and encodes it as a series of signals that are transmitted onto the local media. The encoded bits that comprise a frame are received by either an end device or an intermediary device.

Physical Layer Characteristics

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. Bandwidth is the capacity at which a medium can carry data. Digital bandwidth measures the amount of data that can flow from one place to another in a given amount of time. Throughput is the measure of the transfer of bits across the media over a given period of time and is usually lower than bandwidth. Latency refers to the amount of time, including delays, for data to travel from one given point to another. Goodput is the measure of usable data transferred over a given period of time. The physical layer produces the representation and groupings of bits for each type of media as follows:

- Copper cable - The signals are patterns of electrical pulses.
- Fiber-optic cable - The signals are patterns of light.
- Wireless - The signals are patterns of microwave transmissions.

Copper Cabling

Networks use copper media because it is inexpensive, easy to install, and has low resistance to electrical current. However, copper media is limited by distance and signal interference. The timing and voltage values of the electrical pulses are also susceptible to interference from two sources: EMI and crosstalk. Three types of copper cabling are: UTP, STP, and coaxial cable (coax). UTP has an outer jacket to protect the copper wires from physical damage, twisted pairs to protect the signal from interference, and color-coded plastic insulation that electrically isolates wires from each other and identifies each pair. The STP cable uses four pairs of wires, each wrapped in a foil shield, which are then wrapped in an overall metallic braid or foil. Coaxial cable, or coax for short, gets its name from the fact that there are two conductors that share the same axis. Coax is used to attach antennas to wireless devices. Cable internet providers use coax inside their customers' premises.

UTP Cabling

UTP cabling consists of four pairs of color-coded copper wires that have been twisted together and then encased in a flexible plastic sheath. UTP cable does not use shielding to counter the effects of EMI and RFI. Instead, cable designers have discovered other ways that they can limit the negative effect of crosstalk: cancellation and varying the number of twists per wire pair. 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). UTP cable is usually terminated with an RJ-45 connector. The main cable types that are obtained by using specific wiring conventions are Ethernet Straight-through and Ethernet Crossover. Cisco has a proprietary UTP cable called a rollover that connects a workstation to a router console port.

Fiber-Optic Cabling

Optical fiber cable transmits data over longer distances and at higher bandwidths than any other networking media. Fiber-optic cable can transmit signals with less attenuation than copper wire and is completely immune to EMI and RFI. Optical fiber is a flexible, but extremely thin, transparent strand of very pure glass, not much bigger than a human hair. Bits are encoded on the fiber as light impulses. Fiber-optic cabling is now being used in four types of industry: enterprise networks, FTTH, long-haul networks, and submarine cable networks. 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. In most enterprise

environments, optical fiber is primarily used as backbone cabling for high-traffic point-to-point connections between data distribution facilities and for the interconnection of buildings in multi-building campuses.

Wireless Media

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.

6.1.1 The Data Link Layer

The data link layer of the OSI model (Layer 2), as shown in the figure, prepares network data for the physical network. The data link layer is responsible for network interface card (NIC) to network interface card communications. The data link layer does the following:

- Enables upper layers to access the media. The upper layer protocol is completely unaware of the type of media that is used to forward the data.
- Accepts data, usually Layer 3 packets (i.e., IPv4 or IPv6), and encapsulates them into Layer 2 frames.
- Controls how data is placed and received on the media.
- Exchanges frames between endpoints over the network media.
- Receives encapsulated data, usually Layer 3 packets, and directs them to the proper upper-layer protocol.
- Performs error detection and rejects any corrupt frame.

6.1.2 IEEE 802 LAN/MAN Data Link Sublayers

IEEE 802 LAN/MAN standards are specific to Ethernet LANs, wireless LANs (WLAN), wireless personal area networks (WPAN) and other types of local and metropolitan area networks. The IEEE 802 LAN/MAN data link layer consists of the following two sublayers:

- **Logical Link Control (LLC)** - 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.
- **Media Access Control (MAC)** - Implements this sublayer (IEEE 802.3, 802.11, or 802.15) in hardware. It is responsible for data encapsulation and media access control. It provides data link layer addressing and it is integrated with various physical layer technologies.

The figure shows the two sublayers (LLC and MAC) of the data link layer.

6.1.3 Providing Access to Media

Each network environment that packets encounter as they travel from a local host to a remote host can have different characteristics. For example, an Ethernet LAN usually consists of many hosts contending for access on the network medium. The MAC sublayer resolves this. With serial links the access method may only consist of a direct connection between only two devices, usually two routers. Therefore, they do not require the techniques employed by the IEEE 802 MAC sublayer.

Router interfaces encapsulate the packet into the appropriate frame. A suitable media access control method is used to access each link. In any given exchange of network layer packets, there may be numerous data link layers and media transitions.

At each hop along the path, a router performs the following Layer 2 functions:

1. Accepts a frame from a medium
2. De-encapsulates the frame
3. Re-encapsulates the packet into a new frame
4. Forwards the new frame appropriate to the medium of that segment of the physical network

6.2.6 Access Control Methods

Ethernet LANs and WLANs are examples of multiaccess networks. A multiaccess network is a network that can have two or more end devices attempting to access the network simultaneously.

Some multiaccess networks require rules to govern how devices share the physical media. There are two basic access control methods for shared media:

- Contention-based access
- Controlled access

Contention-based access

In contention-based multiaccess networks, all nodes are operating in half-duplex, competing for the use of the medium. However, only one device can send at a time. Therefore, there is a process if more than one device transmits at the same time. Examples of contention-based access methods include the following:

- Carrier sense multiple access with collision detection (CSMA/CD) used on legacy bus-topology Ethernet LANs
- Carrier sense multiple access with collision avoidance (CSMA/CA) used on Wireless LANs

6.2.8 Contention-Based Access - CSMA/CA

Another form of CSMA used by IEEE 802.11 WLANs is carrier sense multiple access/collision avoidance (CSMA/CA).

CMSA/CA uses a method similar to CSMA/CD to detect if the media is clear. CMSA/CA uses additional techniques. In wireless environments it may not be possible for a device to detect a collision. CMSA/CA does not detect collisions but attempts to avoid them by waiting before transmitting. Each device that transmits includes the time duration that it needs for the transmission. All other wireless devices receive this information and know how long the medium will be unavailable.

In the figure, if host A is receiving a wireless frame from the access point, hosts B, and C will also see the frame and how long the medium will be unavailable.

6.3.1 The Frame

This topic discusses in detail what happens to the data link frame as it moves through a network. The information appended to a frame is determined by the protocol being used.

The data link layer prepares the encapsulated data (usually an IPv4 or IPv6 packet) for transport across the local media by encapsulating it with a header and a trailer to create a frame.

The data link protocol is responsible for NIC-to-NIC communications within the same network. Although there are many different data link layer protocols that describe data link layer frames, each frame type has three basic parts:

- Header
- Data
- Trailer

Unlike other encapsulation protocols, the data link layer appends information in the form of a trailer at the end of the frame.

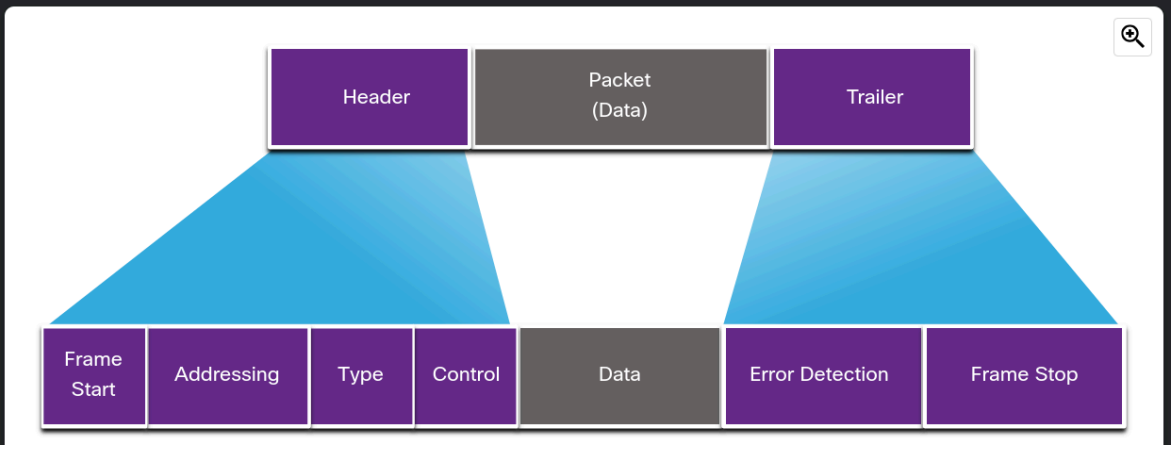
All data link layer protocols encapsulate the data within the data field of the frame. However, the structure of the frame and the fields contained in the header and trailer vary according to the protocol.

There is no one frame structure that meets the needs of all data transportation across all types of media. Depending on the environment, the amount of control information needed in the frame varies to match the access control requirements of the media and logical topology. For example, a WLAN frame must include procedures for collision avoidance and therefore requires additional control information when compared to an Ethernet frame.

6.3.2 Frame Fields

Framing breaks the stream into decipherable groupings, with control information inserted in the header and trailer as values in different fields. This format gives the physical signals a structure that are by recognized by nodes and decoded into packets at the destination.

The generic frame fields are shown in the figure. Not all protocols include all these fields. The standards for a specific data link protocol define the actual frame format.



6.3.3 Layer 2 Addresses

The data link layer provides the addressing used in transporting a frame across a shared local media. Device addresses at this layer are referred to as physical addresses. Data link layer addressing is contained within the frame header and specifies the frame destination node on the local network. It is typically at the beginning of the frame, so the NIC can quickly determine if it matches its own Layer 2 address before accepting the rest of the frame. The frame header may also contain the source address of the frame.

Unlike Layer 3 logical addresses, which are hierarchical, physical addresses do not indicate on what network the device is located. Rather, the physical address is unique to the specific device. A device will still function with the same Layer 2 physical address even if the device moves to another network or subnet. Therefore, Layer 2 addresses are only used to connect devices within the same shared media, on the same IP network.

The figures illustrate the function of the Layer 2 and Layer 3 addresses. As the IP packet travels from host-to-router, router-to-router, and finally router-to-host, at each point along the way the IP packet is encapsulated in a new data link frame. Each data link frame contains the source data link address of the NIC sending the frame, and the destination data link address of the NIC receiving the frame.

Data link layer protocols include:

- **Ethernet**
- **802.11 Wireless**
- **Point-to-Point Protocol (PPP)**
- **High-Level Data Link Control (HDLC)**
- **Frame Relay**

Summary

1. Data Link Layer (Layer 2)

The **data link layer** is responsible for **framing, addressing, and error detection** in local communication between network devices. It has **two sublayers**:

a. Logical Link Control (LLC) Sublayer

- Manages **communication between upper and lower layers**.
- Identifies **network layer protocols (like IPv4, IPv6)** inside the frame.
- Ensures **flow control and error control**.

b. Media Access Control (MAC) Sublayer

- Responsible for **framing and addressing** (uses **MAC addresses**).
- Controls **how devices access the shared network medium**.
- **Implements Ethernet standards** for wired LANs.

Purpose of the Data Link Layer

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. Without the data link layer, network layer protocols such as IP, would have to make provisions for connecting to every type of media that could exist along a delivery path. The IEEE 802 LAN/MAN data link layer consists of the following two sublayers: LLC and MAC. The MAC sublayer provides data encapsulation through frame delimiting, addressing, and error detection. Router interfaces encapsulate the packet into the appropriate frame. A suitable media access control method is used to access each link. Engineering organizations that define open standards and protocols that apply to the network access layer include: IEEE, ITU, ISO, and ANSI.

Topologies

The two types of topologies used in LAN and WAN networks are physical and logical. The data link layer "sees" the logical topology of a network when controlling data access to the media. The logical topology influences the type of network framing and media access control used. Three common types of physical WAN topologies are: point-to-point, hub and spoke, and mesh. Physical point-to-point topologies directly connect two end devices (nodes).

Adding intermediate physical connections may not change the logical topology. In multi-access LANs, nodes are interconnected using star or extended star topologies. In this type of topology, nodes are connected to a central intermediary device. Physical LAN topologies include: star, extended star, bus, and ring. Half-duplex communications exchange data in one direction at a time. Full-duplex sends and receives data simultaneously. Two interconnected interfaces must use the same duplex mode or there will be a duplex mismatch creating inefficiency and latency on the link. Ethernet LANs and WLANs are examples of multi-access networks. A multi-access network is a network that can have multiple nodes accessing the network simultaneously. Some multi-access networks require rules to govern how devices share the physical media. There are two basic access control methods for shared media: contention-based access and controlled access. In contention-based multi-access networks, all nodes are operating in half-duplex. There is a process if more than one device transmits at the same time. Examples of contention-based access methods include: CSMA/CD for bus-topology Ethernet LANs and CSMA/CA for WLANs.

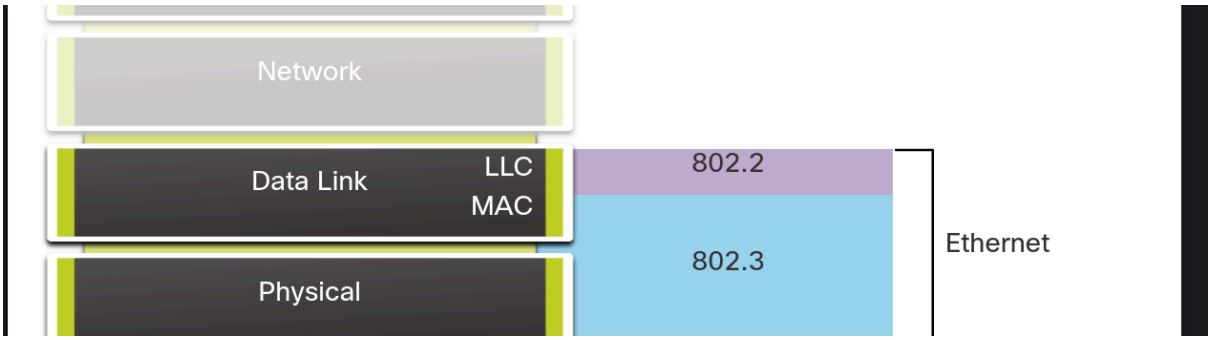
Data Link Frame

The data link layer prepares the encapsulated data (usually an IPv4 or IPv6 packet) for transport across the local media by encapsulating it with a header and a trailer to create a frame. The data link protocol is responsible for NIC-to-NIC communications within the same network. There are many different data link layer protocols that describe data link layer frames, each frame type has three basic parts: header, data, and trailer. Unlike other encapsulation protocols, the data link layer appends information in the trailer. There is no one frame structure that meets the needs of all data transportation across all types of media. Depending on the environment, the amount of control information needed in the frame varies to match the access control requirements of the media and logical topology. Frame fields include: frame start and stop indicator flags, addressing, type, control, data, and error detection. The data link layer provides addressing used to transport a frame across shared local media. Device addresses at this layer are physical addresses. Data link layer addressing is contained within the frame header and specifies the frame destination node on the local network. The data link layer address is only used for local delivery. In a TCP/IP network, all OSI Layer 2 protocols work with IP at OSI Layer 3. However, the Layer 2 protocol used depends on the logical topology and the physical media. Each protocol performs media access control for specified Layer 2 logical topologies. The Layer 2 protocol that is used for a particular network topology is determined by

the technology used to implement that topology. Data link layer protocols include: Ethernet, 802.11 Wireless, PPP, HDLC, and Frame Relay.

What is CSMA/CD?

CSMA/CD (Carrier Sense Multiple Access with Collision Detection) is a network access method used in wired Ethernet networks (IEEE 802.3) to manage how devices share a common communication medium and prevent data collisions.



What is Media Access Control (MAC)?

Media Access Control (MAC) is a sublayer of the Data Link Layer (Layer 2) in the OSI model. It is responsible for controlling how devices access the network medium and send data without collisions.

MAC ensures that multiple devices can share the same network efficiently and without interference.

7.1.3 MAC Sublayer

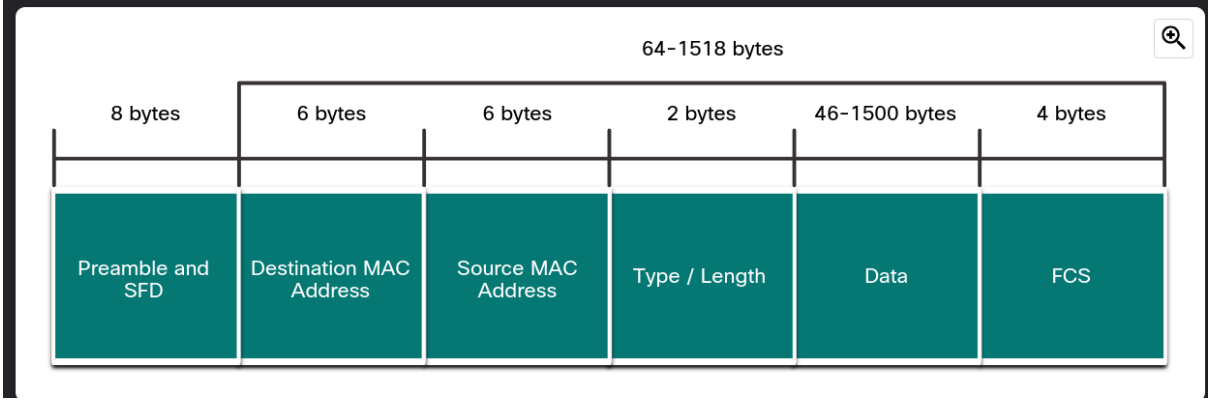
The MAC sublayer is responsible for data encapsulation and accessing the media.

Data Encapsulation

IEEE 802.3 data encapsulation includes the following:

- **Ethernet frame** - This is the internal structure of the Ethernet frame.
- **Ethernet Addressing** - The Ethernet frame includes both a source and destination MAC address to deliver the Ethernet frame from Ethernet NIC to Ethernet NIC on the same LAN.
- **Ethernet Error detection** - The Ethernet frame includes a frame check sequence (FCS) trailer used for error detection.

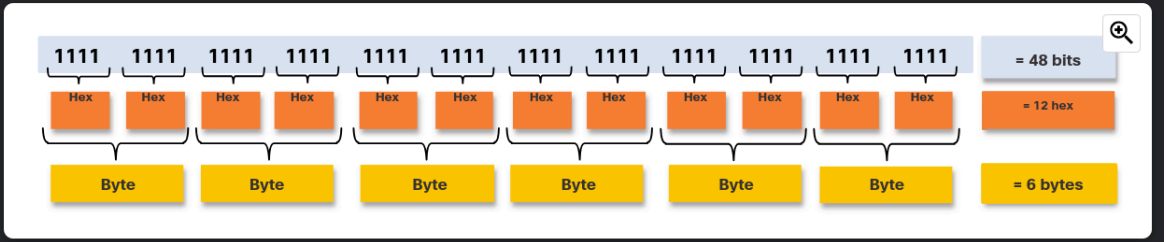
Ethernet Frame Fields



7.2.2 Ethernet MAC Address

In an Ethernet LAN, every network device is connected to the same, shared media. The MAC address is used to identify the physical source and destination devices (NICs) on the local network segment. 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, as shown in the figure. Because a byte equals 8 bits, we can also say that a MAC address is 6 bytes in length.



2. Ensuring Uniqueness: The Role of the IEEE

The **IEEE Registration Authority** ensures uniqueness by requiring vendors to **register and obtain an OUI**.

(A) Organizationally Unique Identifier (OUI) - First 6 Hex Digits

🔹 The **OUI is assigned by IEEE** to each vendor that manufactures Ethernet hardware.
🔹 This OUI is **unique to the vendor** and ensures that no two vendors issue the same range of MAC addresses.

Example of Vendor OUIs:

Vendor	OUI (First 6 Hex Digits)
Apple	**00:17:F2**
Cisco	**00:40:96**
Intel	**00:1A:2B**
Dell	**00:14:22**

3. What if a Vendor Runs Out of Addresses?

If a vendor **exhausts all possible device-specific values** within an OUI (i.e., **16.7 million unique addresses** per OUI), they must:

1. **Request another OUI from IEEE**.
2. **Continue issuing unique MAC addresses using the new OUI.**

Example:

- **Apple's OUI:** `00:17:F2`
- **Apple requests a second OUI:** `B8:27:EB`
- **Devices assigned under the new OUI remain unique.**

3. Why Can't We Always Capture All Messages?

🔒 **Switches Use MAC Address Tables**

Unlike hubs, **switches** use a **MAC address table (CAM table)** to forward frames **only to the intended destination**. This prevents sniffing **unless an attack is performed (e.g., ARP spoofing).**

🔒 **Encrypted Traffic (HTTPS, TLS, VPNs)**

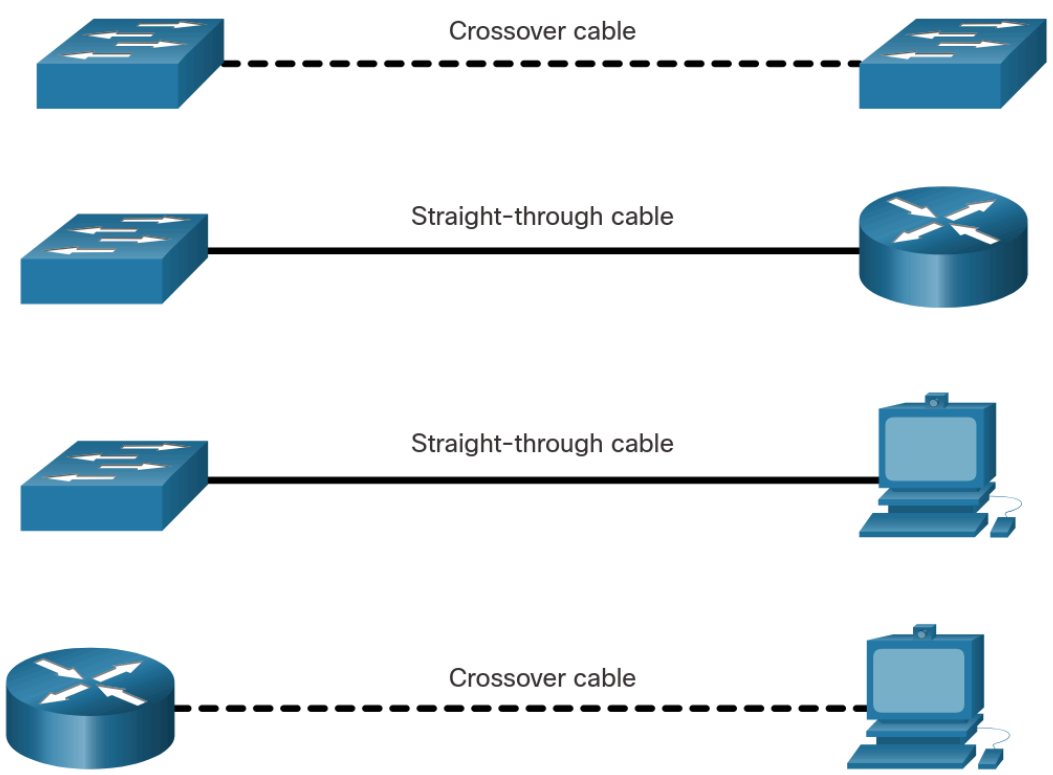
Even if you capture packets, data inside **encrypted packets** (like HTTPS traffic) cannot be easily read.

🔒 **Network Segmentation (VLANs)**

Switches use **VLANs (Virtual LANs)** to **isolate traffic**, preventing devices in different VLANs from seeing each other's packets.

🔒 **Security Mechanisms**

- **Port Security**: Limits the number of MAC addresses per switch port.
- **Dynamic ARP Inspection (DAI)**: Blocks ARP spoofing.
- **MAC Address Filtering**: Prevents unauthorized devices from connecting.



What is Auto-MDIX?

Auto-MDIX is a feature found in modern network switches that automatically detects the type of Ethernet cable (straight-through or crossover) connected to a port and adjusts the interface accordingly. This eliminates the need for manually choosing the correct cable type when connecting network devices.

Ethernet Frame

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. Data encapsulation includes the following: Ethernet frame, Ethernet addressing, and Ethernet error detection. Ethernet LANs use switches that operate in full-duplex. The Ethernet frame fields are: preamble and start frame delimiter, destination MAC address, source MAC address, EtherType, data, and FCS.

Ethernet MAC Address

Binary number system uses the digits 0 and 1. Decimal uses 0 through 9. Hexadecimal uses 0 through 9 and the letters A through F. The MAC address is used to identify the physical source and destination devices (NICs) on the local network segment. 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. An Ethernet MAC address consists of a 6 hexadecimal vendor OUI code followed by a 6 hexadecimal vendor assigned value. 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.

The MAC Address Table

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. 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.

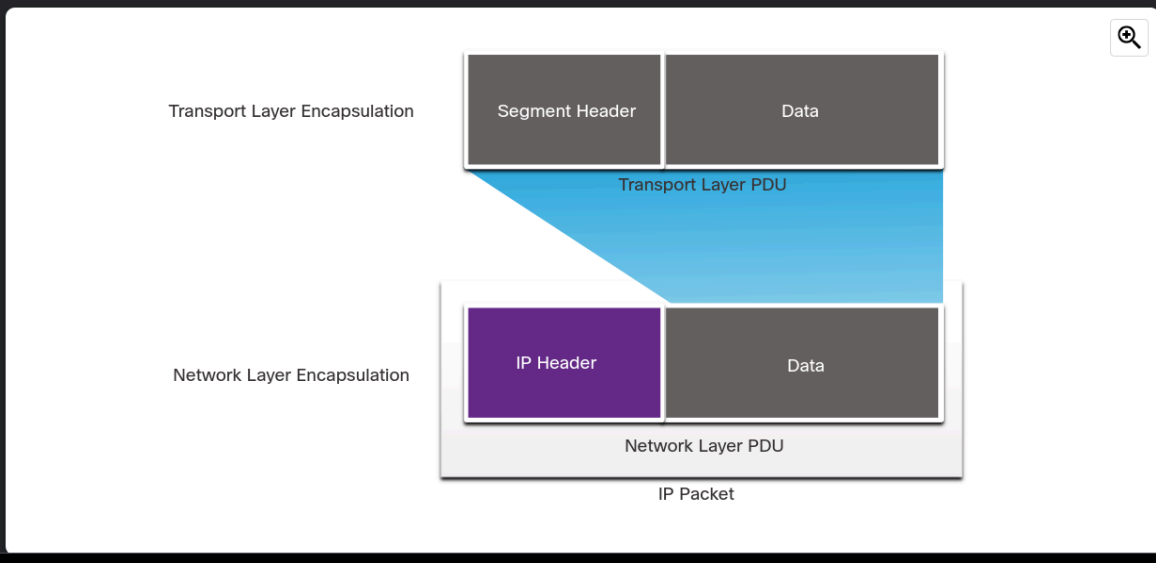
Switch Speeds and Forwarding Methods

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. Autonegotiation is an optional function found on most Ethernet switches and NICs. It enables two devices to automatically negotiate the best speed and duplex capabilities. Full-duplex is chosen if both devices have the capability along with their highest common bandwidth. Most switch devices now support the automatic medium-dependent interface crossover (auto-MDIX) feature. When enabled, the switch automatically detects the type of cable attached to the port and configures the interfaces accordingly.

IP encapsulates the transport layer (the layer just above the network layer) segment or other data by adding an IP header. The IP header is used to deliver the packet to the destination host.

The figure illustrates how the transport layer PDU is encapsulated by the network layer PDU to create an IP packet.



8.1.4 Connectionless

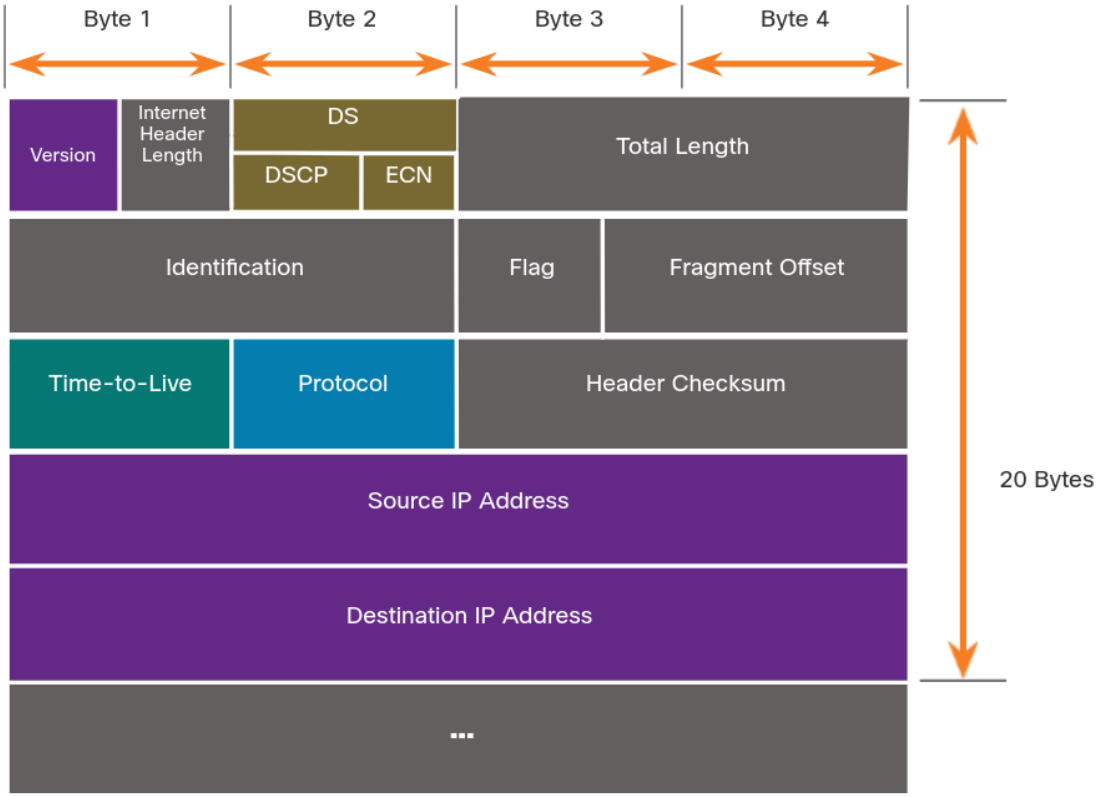
IP is connectionless, meaning that no dedicated end-to-end connection is created by IP before data is sent. Connectionless communication is conceptually similar to sending a letter to someone without notifying the recipient in advance. The figure summarizes this key point.

Connectionless - Analogy

The OSI data link layer is responsible for taking an IP packet and preparing it for transmission over the communications medium. This means that the delivery of IP packets is not limited to any particular medium.

There is, however, one major characteristic of the media that the network layer considers: the maximum size of the PDU that each medium can transport. This characteristic is referred to as the maximum transmission unit (MTU). Part of the control communication between the data link layer and the network layer is the establishment of a maximum size for the packet. The data link layer passes the MTU value up to the network layer. The network layer then determines how large packets can be.

In some cases, an intermediate device, usually a router, must split up an IPv4 packet when forwarding it from one medium to another medium with a smaller MTU. This process is called fragmenting the packet, or fragmentation. Fragmentation causes latency. IPv6 packets cannot be fragmented by the router.



8.3.2 IPv6 Overview

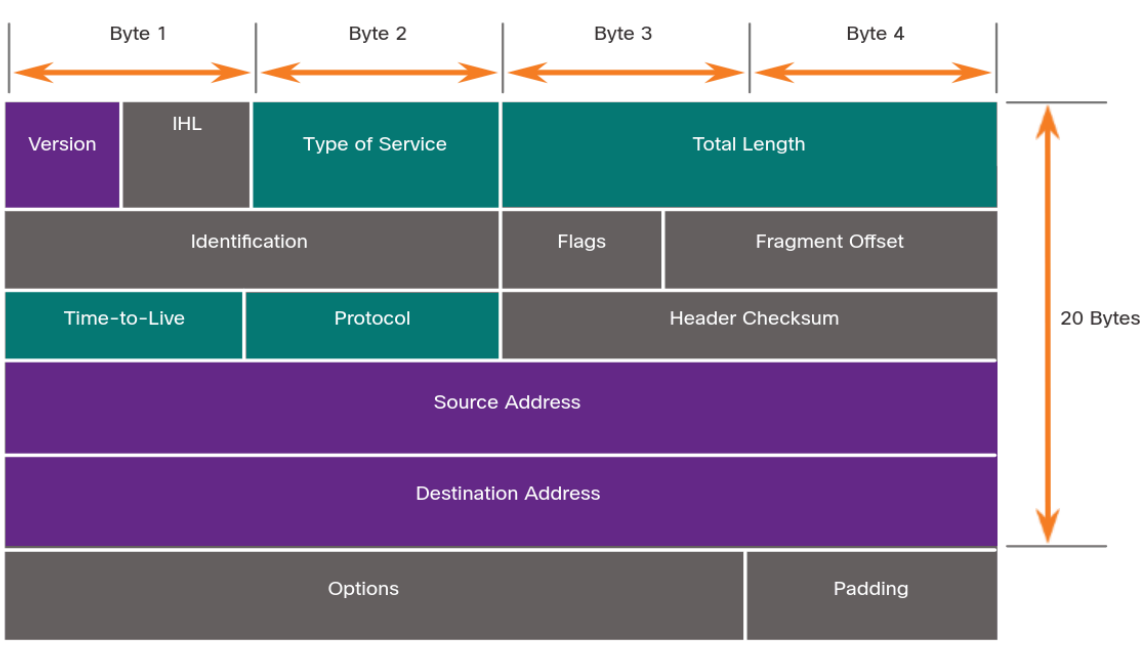
In the early 1990s, the Internet Engineering Task Force (IETF) grew concerned about the issues with IPv4 and began to look for a replacement. This activity led to the development of IP version 6 (IPv6). IPv6 overcomes the limitations of IPv4 and is a powerful enhancement with features that better suit current and foreseeable network demands.

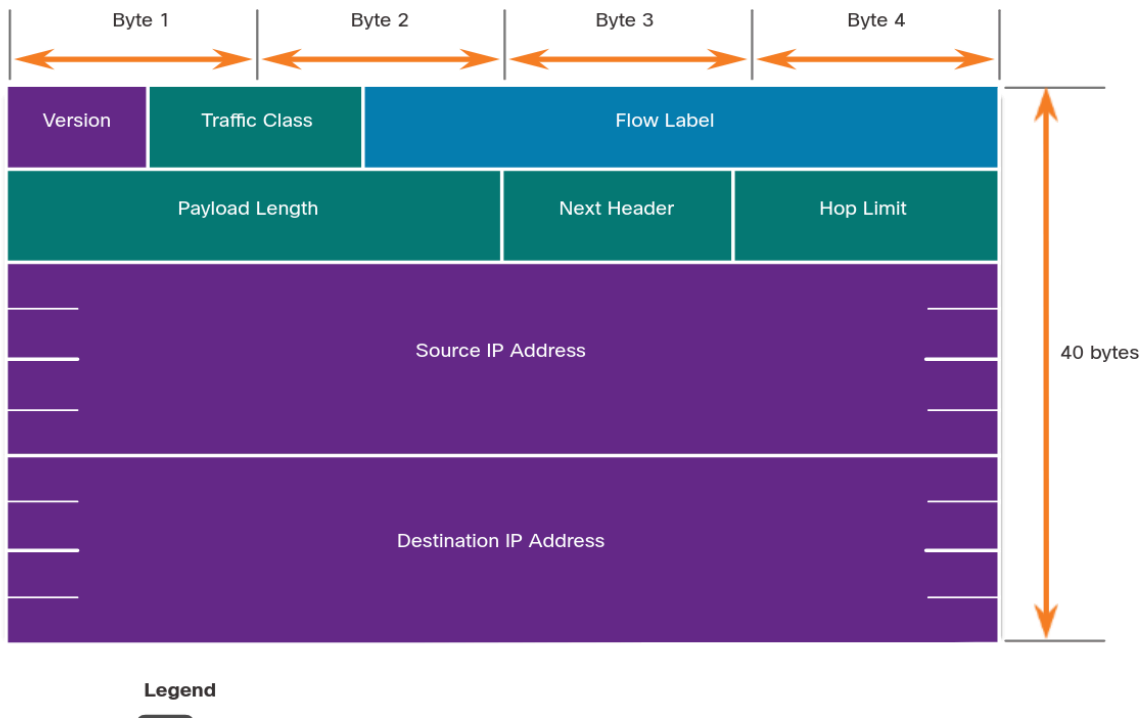
Improvements that IPv6 provides include the following:

- **Increased address space** - IPv6 addresses are based on 128-bit hierarchical addressing as opposed to IPv4 with 32 bits.
- **Improved packet handling** - The IPv6 header has been simplified with fewer fields.
- **Eliminates the need for NAT** - With such a large number of public IPv6 addresses, NAT between a private IPv4 address and a public IPv4 is not needed. This avoids some of the NAT-induced problems experienced by applications that require end-to-end connectivity.

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 figure provides a visual to compare the IPv4 and IPv6 address space.





Legend

What is a Subnet Mask?

A subnet mask is like a helper that tells your computer or router which part of an IP address refers to the network and which part refers to the individual device (host) within that network.

What Does it Do?

- **It helps split an IP address into two parts:**
  1. **The Network part: Which identifies the network you're on (like the neighborhood or building).**
  2. **The Host part: Which identifies a specific device (like a computer or phone in that network).**

Example:

Let’s look at an IP address and its subnet mask.

- **IP Address: `192.168.1.10`**
- **Subnet Mask: `255.255.255.0`**

Step-by-Step Explanation:

1. **IP Address:**
   - **The IP address `192.168.1.10` is made up of 4 numbers (called octets) separated by dots. Each number can range from `0` to `255` (which is 8 bits in binary).**
2. **Subnet Mask:**
   - **The subnet mask `255.255.255.0` is also made up of 4 octets, and it tells us which part of the IP address belongs to the network and which part belongs to the host.**
3. **What the Subnet Mask Means:**
   - **`255` is like saying, "This part of the IP address is used for the network."**

    - `0` is like saying, "This part of the IP address is used for the device (host)."
4. So, with the subnet mask `255.255.255.0`:
    - The first three parts (192.168.1) are used for the network.
    - The last part (10) is used for the device.
5. This means that the network is `192.168.1` and the device within that network is `.10`.

Why is it Important?

- The subnet mask helps your computer know whether another device is on the same network or on a different network.
- It's like your home address: the network part is the city, and the host part is your house number. When you want to send a letter, you need to know which part of the address to use to deliver it to the correct place.

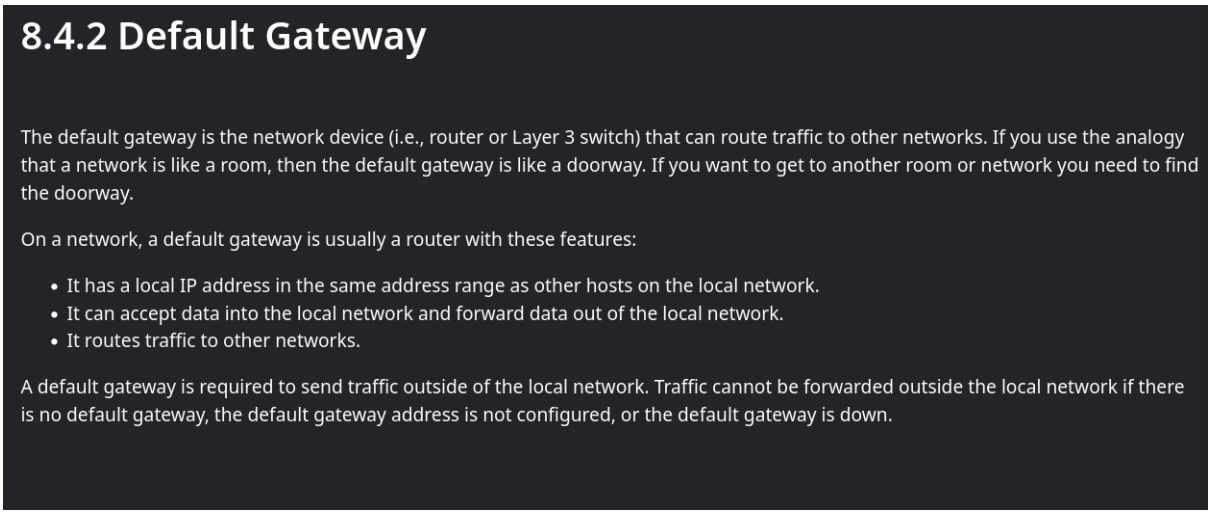
Quick Recap:

- Subnet Mask = It tells your device which part of the IP address is for the network and which part is for the device.
- It helps devices know where to send data—either to the same network or to a different one.

In Simple Terms:

- IP Address = Home address of a device.

- **Subnet Mask = Helps figure out the neighborhood (network) and house (device).**



8.4.2 Default Gateway

The default gateway is the network device (i.e., router or Layer 3 switch) that can route traffic to other networks. If you use the analogy that a network is like a room, then the default gateway is like a doorway. If you want to get to another room or network you need to find the doorway.

On a network, a default gateway is usually a router with these features:

- It has a local IP address in the same address range as other hosts on the local network.
- It can accept data into the local network and forward data out of the local network.
- It routes traffic to other networks.

A default gateway is required to send traffic outside of the local network. Traffic cannot be forwarded outside the local network if there is no default gateway, the default gateway address is not configured, or the default gateway is down.

Network Layer

Network Layer Characteristics

The network layer (OSI Layer 3) provides services to allow end devices to exchange data across networks. IPv4 and IPv6 are the principle network layer communication protocols. The network layer also includes the routing protocol OSPF and messaging protocols such as ICMP. Network layer protocols perform four basic 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. IP encapsulates the transport layer segment by adding an IP header, which is used to deliver the packet to the

destination host. The IP header is examined by Layer 3 devices (i.e., routers) as it travels across a network to its destination. The 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. The IP protocol does not guarantee that all packets that are delivered are, in fact, received. This is the definition of the unreliable, or best effort characteristic. IP operates independently of the media that carry the data at lower layers of the protocol stack.

IPv4 Packet

An IPv4 packet header consists of fields containing information about the packet. These fields contain binary numbers which are examined by the Layer 3 process. The binary values of each field identify various settings of the IP packet. Significant fields in the IPv4 packet header include: version, DS, header checksum, TTL, protocol, and the source and destination IPv4 addresses.

IPv6 Packet

IPv6 is designed to overcome the limitations of IPv4 including: IPv4 address depletion, lack of end-to-end connectivity, and increased network complexity. IPv6 increases the available address space, improves packet handling, and eliminates the

need for NAT. The fields in the IPv6 packet header include: version, traffic class, flow label, payload length, next header, hop limit, and the source and destination IPv6 addresses.

How a Host Routes

A host can send a packet to itself, another local host, and a remote host. In IPv4, the source device uses its own subnet mask along with its own IPv4 address and the destination IPv4 address to determine whether the destination host is on the same network. In IPv6, the local router advertises the local network address (prefix) to all devices on the network, to make this determination. The default gateway is the network device (i.e., router) that can route traffic to other networks. On a network, a default gateway is usually a router that has a local IP address in the same address range as other hosts on the local network, can accept data into the local network and forward data out of the local network, and route traffic to other networks. A host routing table will typically include a default gateway. In IPv4, the host receives the IPv4 address of the default gateway either dynamically via DHCP or it is configured manually. In IPv6, the router advertises the default gateway address, or the host can be

configured manually. On a Windows host, the route print or netstat -r command can be used to display the host routing table.

Introduction to Routing

When a host sends a packet to another host, it consults its routing table to determine where to send the packet. If the destination host is on a remote network, the packet is forwarded to the default gateway which is usually the local router. What happens when a packet arrives on a router interface? The router examines the packet's destination IP address and searches its routing table to determine where to forward the packet. The routing table contains a list of all known network addresses (prefixes) and where to forward the packet. These entries are known as route entries or routes. The router will forward the packet using the best (longest) matching route entry. The routing table of a router stores three types of route entries: directly connected networks, remote networks, and a default route. Routers learn about remote networks manually, or dynamically using a dynamic routing protocol. Static routes are route entries that are manually configured. Static routes include the remote network address and the IP address of the next hop router. OSPF and EIGRP are two dynamic routing protocols. The show ip route privileged EXEC mode command is used to view the IPv4

routing table on a Cisco IOS router. At the beginning of an IPv4 routing table is a code that is used to identify the type of route or how the route was learned. Common route sources (codes) include:

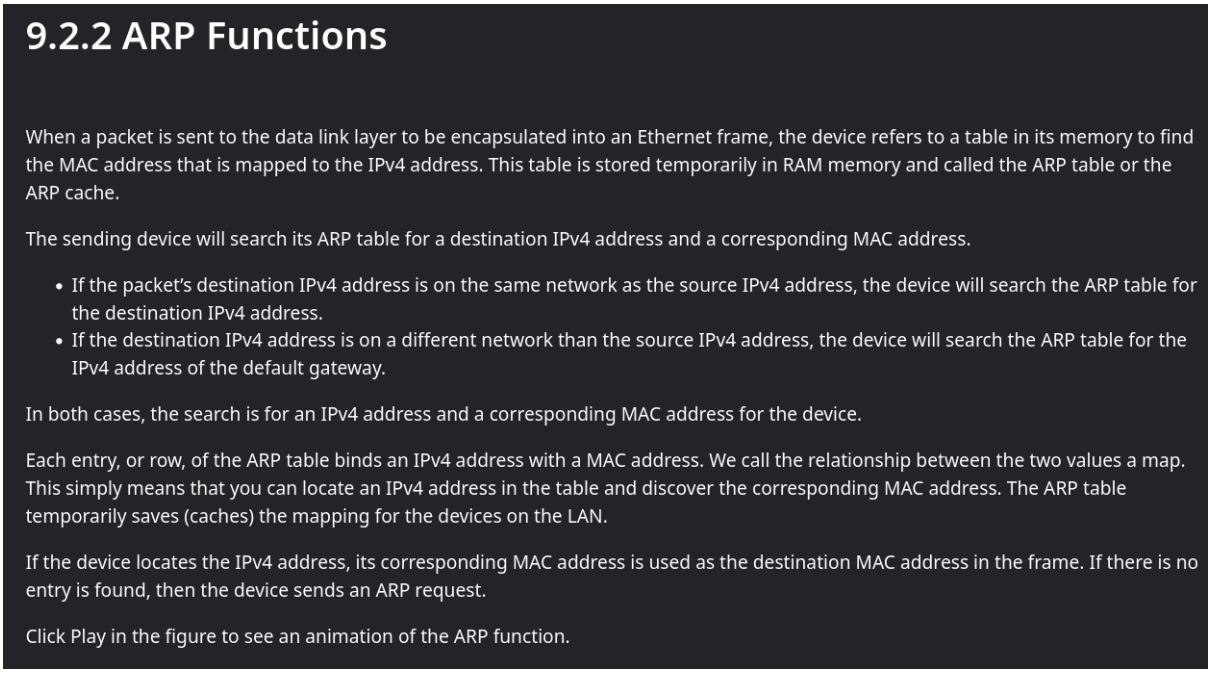
L - Directly connected local interface IP address

C - Directly connected network

S - Static route was manually configured by an administrator

O - Open Shortest Path First (OSPF)

D - Enhanced Interior Gateway Routing Protocol (EIGRP)



AC and IP

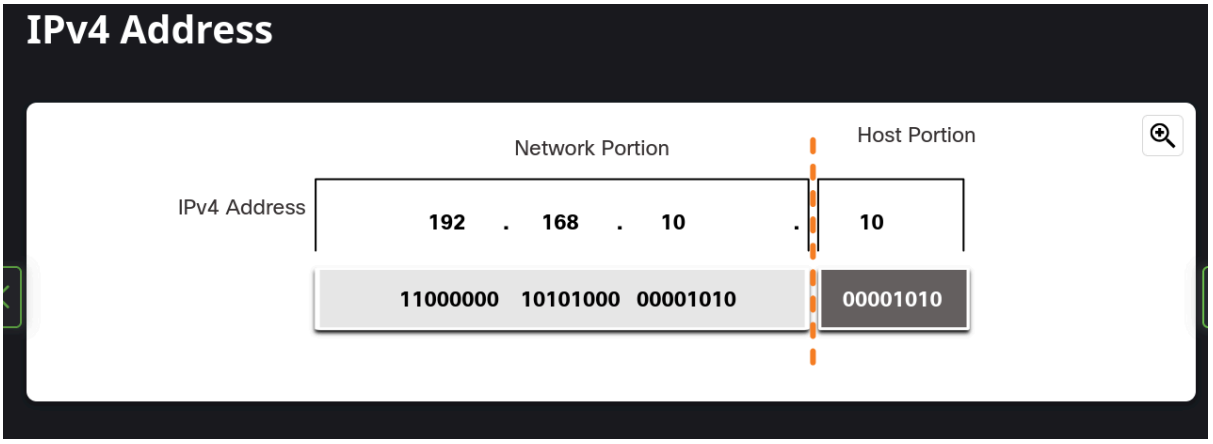
Layer 2 physical addresses (i.e., Ethernet MAC addresses) are used to deliver the data link frame with the encapsulated IP packet from one NIC to

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). Along each link in a path, an IP packet is encapsulated in a frame. The frame is specific to the data link technology associated 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. How are the IP addresses of the IP packets in a data flow associated with the MAC addresses on each link along the path to the destination? For IPv4 packets, this is done through a process called ARP. For IPv6 packets, the process is ICMPv6 ND.

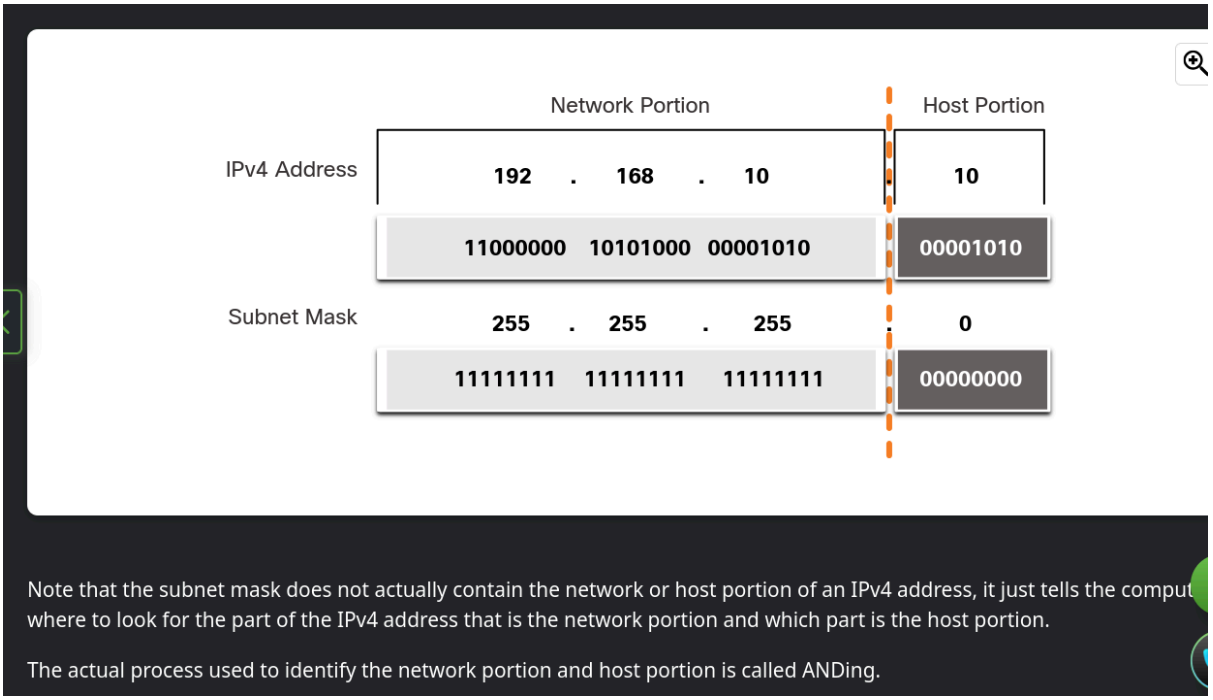
ARP

Every IP device on an Ethernet network has a unique Ethernet MAC address. When a device sends an Ethernet Layer 2 frame, it contains these two addresses: destination MAC address and source MAC address. A 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. The ARP request is encapsulated in an Ethernet frame using this header information: source and destination MAC addresses and type. Only one device on the LAN will have an IPv4 address that matches the target IPv4 address in the ARP request. All other devices will not reply. The ARP reply contains the same header fields as the request. Only the device that originally sent the ARP request will receive the unicast ARP reply. After the ARP reply is received, the device will add the IPv4 address and the corresponding MAC address to its ARP table. When the destination IPv4 address is not on the same network as the source IPv4 address, the source device needs to send the frame to its default gateway. This is the interface of the local router. For each device, an ARP cache timer removes ARP entries that have not been used for a specified period of time. Commands may also be used to manually remove some or all of the entries in the ARP table. As a broadcast frame, an ARP request is received and processed by every device on the local network, which could cause the network to slow down. A threat actor can use ARP spoofing to perform an ARP poisoning attack.



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.



Note that the subnet mask does not actually contain the network or host portion of an IPv4 address, it just tells the comput where to look for the part of the IPv4 address that is the network portion and which part is the host portion.

The actual process used to identify the network portion and host portion is called ANDing.

Expressing network addresses and host addresses with the dotted decimal subnet mask address can become cumbersome. Fortunately, there is 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. Therefore, count the number of bits in the subnet mask and prepend it with a slash.

Refer to the table for examples. The first column lists various subnet masks that can be used with a host address. The second column displays the converted 32-bit binary address. The last column displays the resulting prefix length.

255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.252	11111111.11111111.11111111.11111100	/30

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.

To illustrate how AND is used to discover a network address, consider a host with IPv4 address 192.168.10.10 and subnet mask of 255.255.255.0, as shown in the figure:

- **IPv4 host address (192.168.10.10)** - The IPv4 address of the host in dotted decimal and binary formats.
- **Subnet mask (255.255.255.0)** - The subnet mask of the host in dotted decimal and binary formats.
- **Network address (192.168.10.0)** - The logical AND operation between the IPv4 address and subnet mask results in an IPv4 network address shown in dotted decimal and binary formats.

- All IPv4 host addresses are 32 bits in length
- A portion of the address represents the network that the host belongs to (starts at the left)
- The remaining part is the host portion which identifes the host on the network
- There are two special reserved addresses on every network that can't be assigned to hosts
  - The network address (*lowest*)
  - The broadcast address (*highest*)

A **private IP address** is assigned to devices within a local network (LAN) and is not accessible from the internet. These IPs allow communication between devices inside the same network without exposing them to the public internet.

Private IP Ranges (IPv4)

The following IP ranges are reserved for private networks:

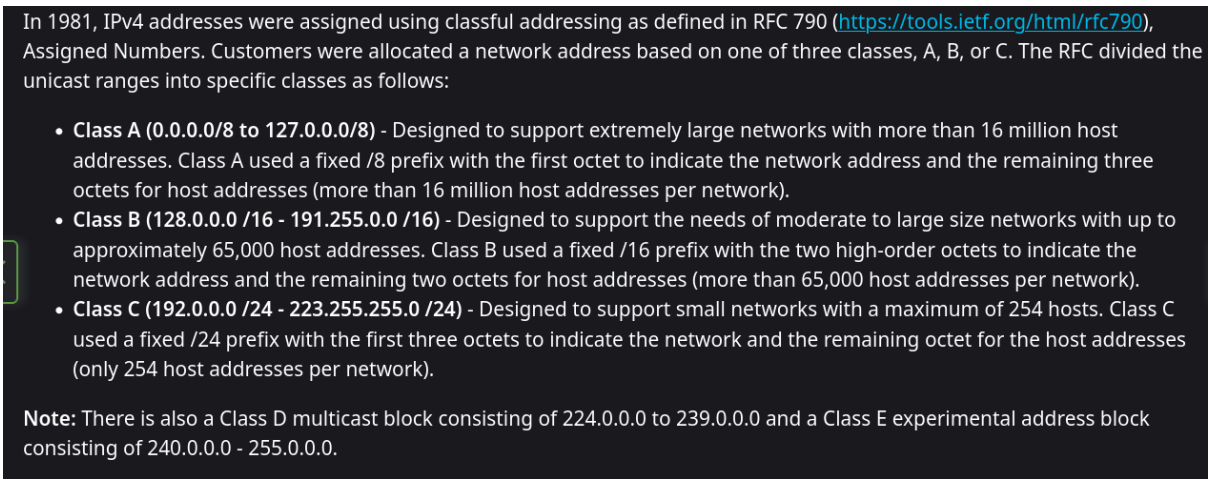
- **10.0.0.0 – 10.255.255.255** (10.0.0.0/8)
- **172.16.0.0 – 172.31.255.255** (172.16.0.0/12)
- **192.168.0.0 – 192.168.255.255** (192.168.0.0/16)

Characteristics of Private IPs:

- Not routable over the internet.
- Used within homes, offices, and internal networks.
- Can be assigned dynamically by **DHCP** or manually.
- Require **Network Address Translation (NAT)** to access the internet.

Loopback addresses

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. For example, it can be used on a host to test if the TCP/IP configuration is operational, as shown in the figure. Notice how the 127.0.0.1 loopback address replies to the ping command. Also note how any address within this block will loop back to the local host, which is shown with the second ping in the figure.


In 1981, IPv4 addresses were assigned using classful addressing as defined in RFC 790 (https://tools.ietf.org/html/rfc790), 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 A used a fixed /8 prefix with the first octet to indicate the network address and the remaining three octets for host addresses (more than 16 million host addresses per network).
- **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 B used a fixed /16 prefix with the two high-order octets to indicate the network address and the remaining two octets for host addresses (more than 65,000 host addresses per network).
- **Class C (192.0.0.0 /24 - 223.255.255.0 /24)** - Designed to support small networks with a maximum of 254 hosts. Class C used a fixed /24 prefix with the first three octets to indicate the network and the remaining octet for the host addresses (only 254 host addresses per network).

Note: 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.

Class A: Large networks (millions of hosts).

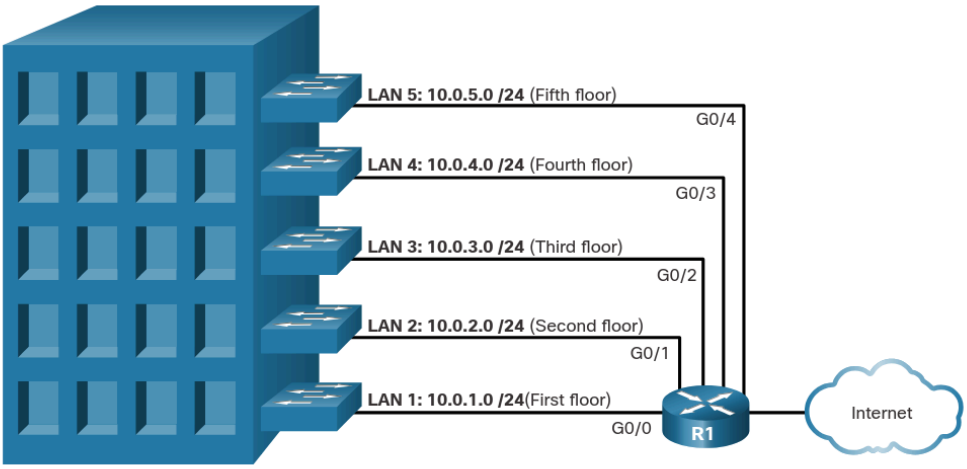
Class B: Medium-sized networks (thousands of hosts).

Class C: Small networks (hundreds of hosts).

Class D & E: Special cases (multicasting, research).

Subnetting reduces overall network traffic and improves network performance. It also enables an administrator to implement security policies such as which subnets are allowed or not allowed to communicate together. Another reason is that it reduces the number of devices affected by abnormal broadcast traffic due to misconfigurations, hardware/software problems, or malicious intent.

Subnetting by Location



For each bit borrowed in the fourth octet, the number of subnetworks available is doubled, while reducing the number of host addresses per subnet:

- **/25 row** - Borrowing 1 bit from the fourth octet creates 2 subnets supporting 126 hosts each.
- **/26 row** - Borrowing 2 bits creates 4 subnets supporting 62 hosts each.
- **/27 row** - Borrowing 3 bits creates 8 subnets supporting 30 hosts each.
- **/28 row** - Borrowing 4 bits creates 16 subnets supporting 14 hosts each.
- **/29 row** - Borrowing 5 bits creates 32 subnets supporting 6 hosts each.
- **/30 row** - Borrowing 6 bits creates 64 subnets supporting 2 hosts each.

Subnet Mask Cheat Sheet

Subnet Mask	CIDR	Network Bits	Host Bits	Max Hosts
255.0.0.0	/8	8	24	16,777,214
255.255.0.0	/16	16	16	65,534
255.255.255.0	/24	24	8	254
255.255.255.192	/26	26	6	62

Here's a **summary and notes** on **subnet masking** for quick reference:

📌 Subnet Masking - Summary & Notes

1. What is a Subnet Mask?

- A **subnet mask** is a **32-bit number** that separates an **IP address** into:
    - **Network portion** (Identifies the network)
    - **Host portion** (Identifies individual devices)

Example:

IP Address: 192.168.1.10 → 11000000.10101000.00000001.00001010

Subnet Mask: 255.255.255.0 → 11111111.11111111.11111111.00000000

-
    - **Network portion:** `192.168.1.0`
    - **Host portion:** `0.0.0.10`

---

2. How to Find the Network and Host Portions

1. Convert **IP Address** and **Subnet Mask** to **Binary**.
2. **Network portion** → Bits where the subnet mask has `1`s.
3. **Host portion** → Bits where the subnet mask has `0`s.
4. **Network Address = IP Address** `AND` **Subnet Mask`
5. **Host Portion = IP Address** `AND` (NOT Subnet Mask)

---

3. Subnet Mask Notation (CIDR)

- CIDR (Classless Inter-Domain Routing) notation represents the number of **network bits**.
- Example: `255.255.255.0` = **/24** (24 bits for network, 8 bits for hosts).

Subnet Mask	CIDR	Network Bits	Host Bits	Max Hosts
255.0.0.0	/8	8	24	16,777,214
255.255.0.0	/16	16	16	65,534
255.255.255.0	/24	24	8	254
255.255.255.192	/26	26	6	62

💡 **Formula for Hosts:**
`2^HostBits - 2` (Subtracting network and broadcast addresses)

---

4. Subnetting Example

Find the network address for 192.168.1.75 with a /26 subnet

Convert to binary:
192.168.1.75 → 11000000.10101000.00000001.01001011

255.255.255.192 → 11111111.11111111.11111111.11000000

1.

Apply AND operation:
Network Address → 192.168.1.64

2.
3. **Subnet range:**
    - First usable IP: `192.168.1.65`
    - Last usable IP: `192.168.1.126`

- Broadcast Address: `192.168.1.127`

---

5. Quick Tricks

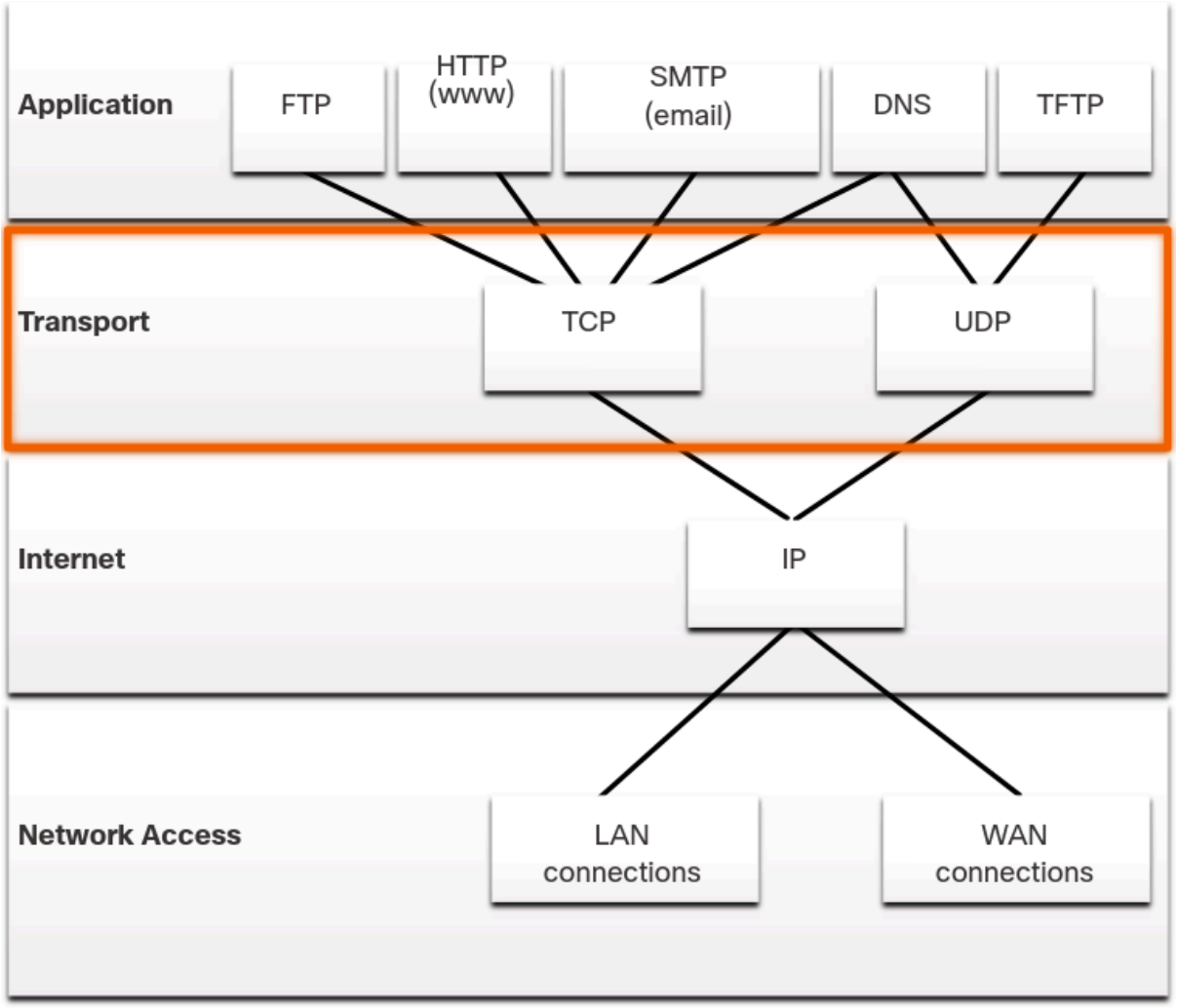
✅ **Network address**: IP `AND` Subnet Mask
✅ **Broadcast address**: Last address in subnet (all `1`s in host bits)
✅ **First usable host**: Network address +1
✅ **Last usable host**: Broadcast address -1
✅ **Total hosts**: `2^host bits - 2`

💡 Key Takeaways

✔ **Subnetting** allows efficient IP allocation.
✔ **CIDR notation** is widely used (`/24`, `/26`, etc.).
✔ Use **bitwise AND** to find the **network address**.
✔ Always reserve **network** and **broadcast** addresses.
✔ More **network bits** → Smaller subnets, Fewer hosts.

Conversation Multiplexing

Conversation multiplexing is a technique used in networking, particularly in the **transport layer**, to enable **multiple communication streams** to occur **concurrently** on the same network. This is crucial for **efficient data transmission**, preventing any single communication (such as streaming video or large file transfer) from **monopolizing the network's bandwidth**. By **interleaving multiple communication streams**, multiplexing ensures that data can be transmitted **simultaneously** across different applications or devices without interference.



Transmission Control Protocol

IP is concerned only with the structure, addressing, and routing of packets, from original sender to final destination. IP is not responsible for guaranteeing delivery or determining whether a connection between the sender and receiver needs to be established.

TCP is considered a reliable, full-featured transport layer protocol, which ensures that all of the data arrives at the destination. TCP includes fields which ensure the delivery of the application data. These fields require additional processing by the sending and receiving hosts.

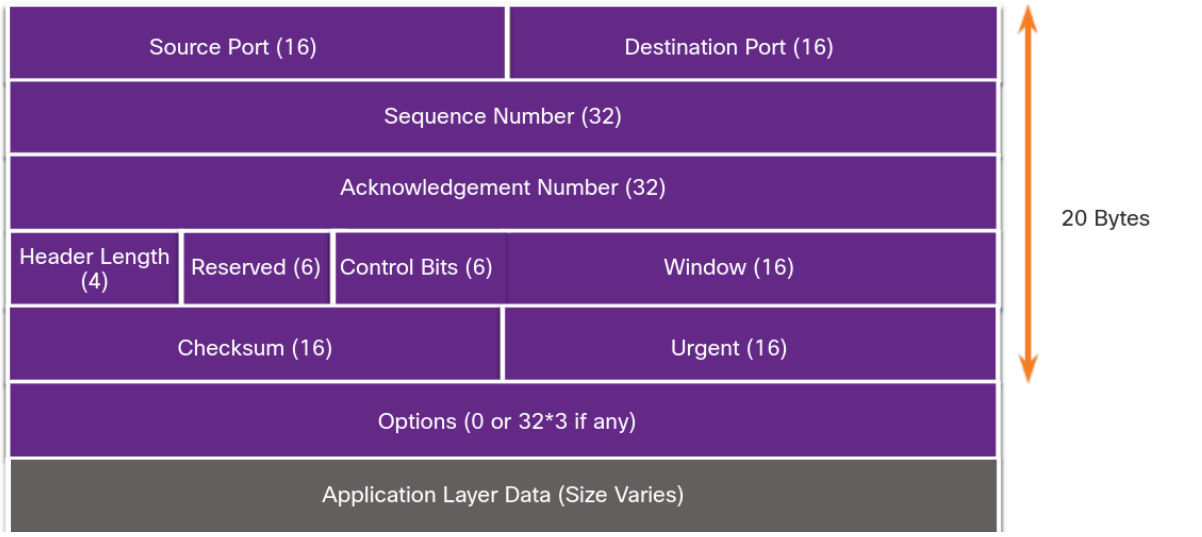
User Datagram Protocol

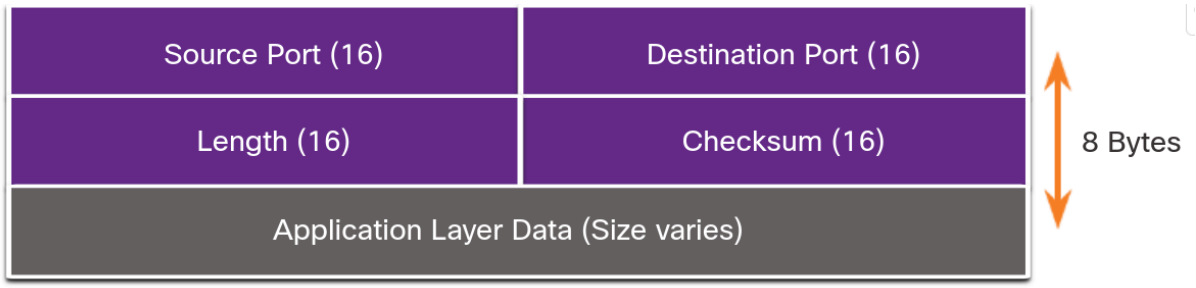
UDP is a simpler transport layer protocol than TCP. It does not provide reliability and flow control, which means it requires fewer header fields. Because the sender and the receiver UDP processes do not have to manage

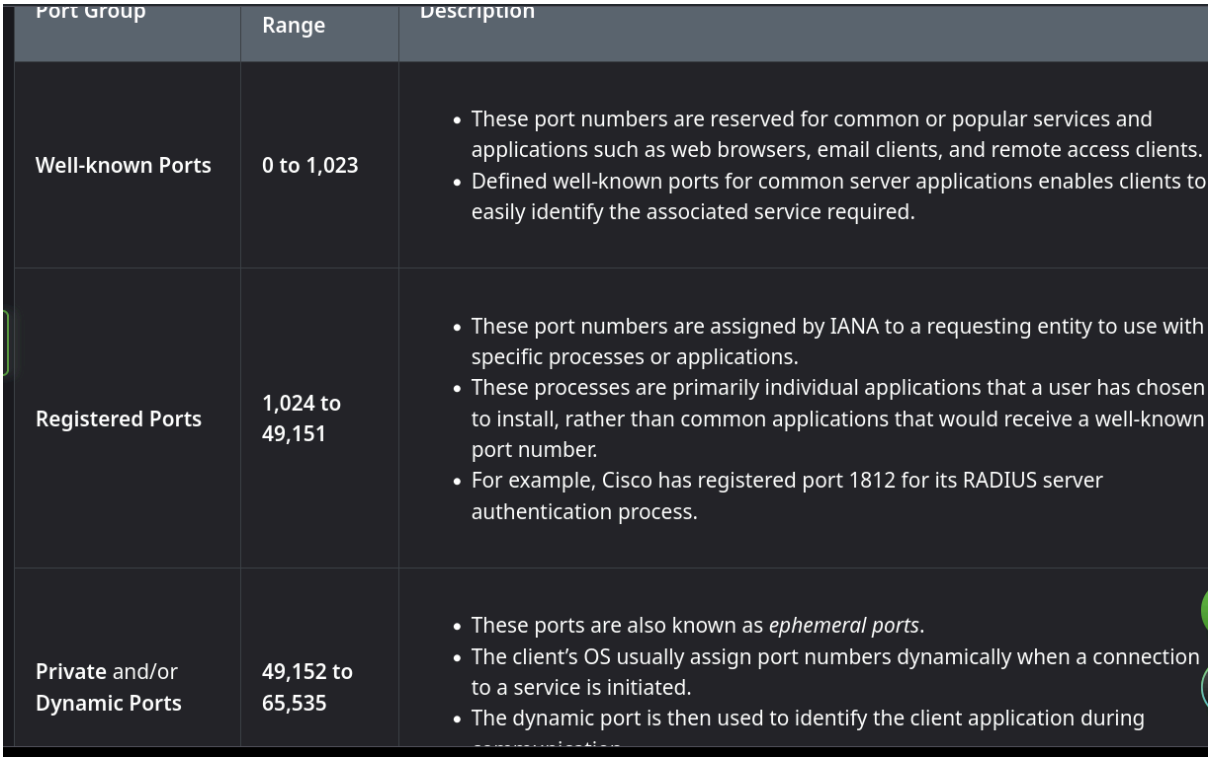
reliability and flow control, this means UDP datagrams can be processed faster than TCP segments. UDP provides the basic functions for delivering datagrams between the appropriate applications, with very little overhead and data checking.

Note: UDP divides data into datagrams that are also referred to as segments.

- **Establishes a Session** - TCP is a connection-oriented protocol that negotiates and establishes a permanent connection (or session) between source and destination devices prior to forwarding any traffic. Through session establishment, the devices negotiate the amount of traffic that can be forwarded at a given time, and the communication data between the two can be closely managed.
- **Ensures Reliable Delivery** - For many reasons, it is possible for a segment to become corrupted or lost completely, as it is transmitted over the network. TCP ensures that each segment that is sent by the source arrives at the destination.
- **Provides Same-Order Delivery** - Because networks may provide multiple routes that can have different transmission rates, data can arrive in the wrong order. By numbering and sequencing the segments, TCP ensures segments are reassembled into the proper order.
- **Supports Flow Control** - Network hosts have limited resources (i.e., memory and processing power). When TCP is aware that these resources are overtaxed, it can request that the sending application reduce the rate of data flow. This is done by TCP regulating the amount of data the source transmits. Flow control can prevent the need for retransmission of the data when the resources of the receiving host are overwhelmed.







Port Group	Range	Description
Well-known Ports	**0 to 1,023**	• These port numbers are reserved for common or popular services and applications such as web browsers, email clients, and remote access clients. • Defined well-known ports for common server applications enables clients to easily identify the associated service required.
Registered Ports	**1,024 to 49,151**	• These port numbers are assigned by IANA to a requesting entity to use with specific processes or applications. • These processes are primarily individual applications that a user has chosen to install, rather than common applications that would receive a well-known port number. • For example, Cisco has registered port 1812 for its RADIUS server authentication process.
Private and/or **Dynamic Ports**	**49,152 to 65,535**	• These ports are also known as *ephemeral ports*. • The client's OS usually assign port numbers dynamically when a connection to a service is initiated. • The dynamic port is then used to identify the client application during

To close a connection, the Finish (FIN) control flag must be set in the segment header. To end each one-way TCP session, a two-way handshake, consisting of a FIN segment and an Acknowledgment (ACK) segment, is used. Therefore, to terminate a single conversation supported by TCP, four exchanges are needed to end both sessions. Either the client or the server can initiate the termination.

TCP Three-way Handshake Analysis

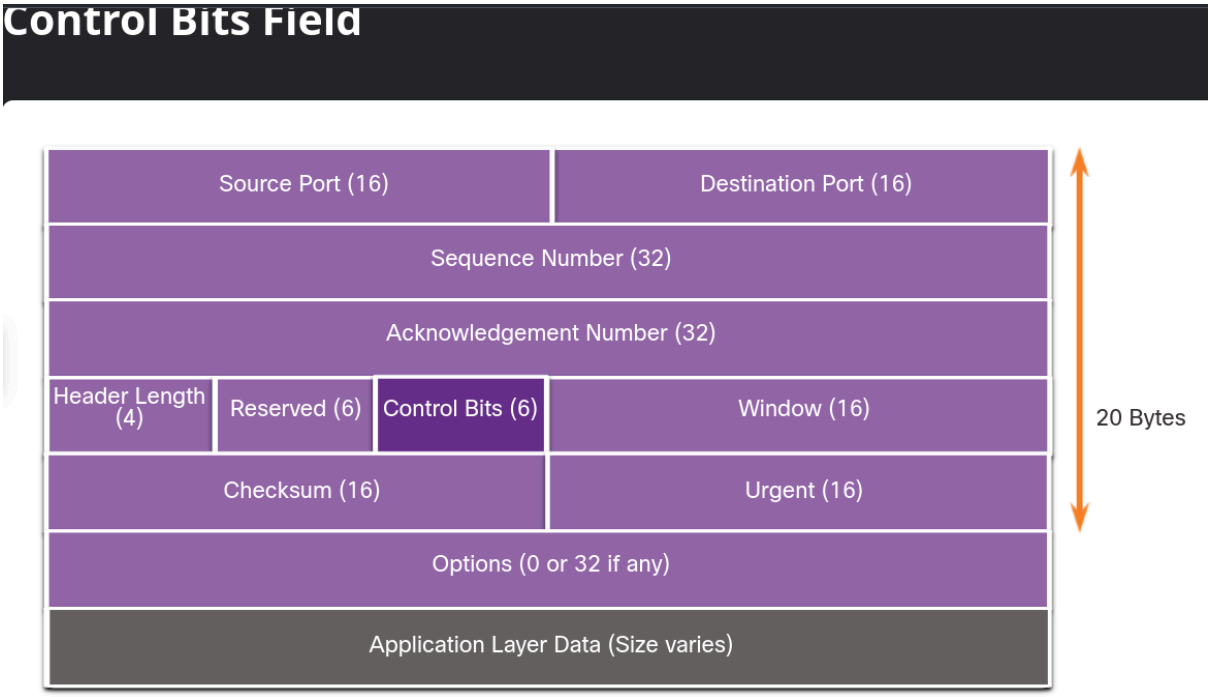
Hosts maintain state, track each data segment within a session, and exchange information about what data is received using the information in the TCP header. TCP is a full-duplex protocol, where each connection represents two one-way communication sessions. To establish the connection, the hosts perform a three-way handshake. As shown in the figure, control bits in the TCP header indicate the progress and status of the connection.

These are the functions of the three-way handshake:

- It establishes that the destination device is present on the network.

- It verifies that the destination device has an active service and is accepting requests on the destination port number that the initiating client intends to use.
- It informs the destination device that the source client intends to establish a communication session on that port number.

After the communication is completed the sessions are closed, and the connection is terminated. The connection and session mechanisms enable TCP reliability function.



Here's a **detailed explanation** of the **TCP handshake and termination process**, covering how connections are established and closed in **Transmission Control Protocol (TCP)**. I'll break it down into different sections, explaining each part thoroughly.

TCP Handshake and Termination – A Detailed Guide

1. Introduction to TCP

Transmission Control Protocol (TCP) is a fundamental protocol in the **Transport Layer** of the OSI model. It ensures reliable, **connection-oriented** communication between devices. TCP is widely used in applications like web browsing, email, and file transfers.

To **establish** a reliable connection, TCP uses a process called the **Three-Way Handshake**, and to **terminate** a connection, it follows the **Four-Step Termination** process.

Before we dive into the details, let's understand why TCP follows this method.

Why Does TCP Use a Handshake and Termination Process?

1. **Reliability:** Ensures all packets are properly acknowledged.
2. **Connection Management:** Establishes and terminates connections gracefully.
3. **Flow Control:** Prevents overwhelming the receiver with too much data at once.
4. **Error Checking:** Ensures the data is intact and reaches the correct destination.

---

2. TCP Three-Way Handshake (Connection Establishment)

Before two devices communicate over TCP, they **establish a connection** using a process called the **Three-Way Handshake**. This ensures both sender and receiver are ready for communication.

Step 1: SYN (Synchronize)

- The client sends a **SYN** (synchronize) packet to the server.
- The **SYN packet** contains:
    - **SYN flag = 1**
    - **Initial Sequence Number (ISN)** (random number chosen by the client)
    - Client indicates the port it wants to use.

📌 **Example:**

Client → Server: SYN, Seq=1000

- The sequence number (e.g., **1000**) is randomly generated by the client.

Step 2: SYN-ACK (Synchronize-Acknowledge)

- The server responds with a **SYN-ACK** packet.
- The **SYN-ACK packet** contains:
    - **SYN flag = 1** (Server also wants to synchronize)
    - **ACK flag = 1** (Acknowledges the client's SYN request)
    - **Server's own Sequence Number (ISN)**
    - **Acknowledgment Number = Client's Sequence Number + 1**

📌 **Example:**

Server → Client: SYN-ACK, Seq=5000, Ack=1001

- The acknowledgment number is **1001** (Client's ISN + 1).
- The server's ISN is a different random number (e.g., **5000**).

Step 3: ACK (Acknowledgment)

- The client sends an **ACK** packet to confirm the connection.
- The **ACK packet** contains:
    - **ACK flag = 1** (Acknowledging server's SYN-ACK)
    - **Acknowledgment Number = Server's Sequence Number + 1**

📌 **Example:**

Client → Server: ACK, Seq=1001, Ack=5001

- The acknowledgment number is **5001** (Server's ISN + 1).

At this point, the **TCP connection is fully established**, and both client and server can **start exchanging data**.

---

3. TCP Connection Termination (Four-Way Handshake)

Once communication is complete, TCP needs to **gracefully close** the connection. This is done using a **Four-Step Termination Process**.

Step 1: FIN (Finish) Request

- The client (or server) initiates the connection termination by sending a **FIN** (Finish) packet.
- The **FIN packet** contains:
    - **FIN flag = 1**
    - **Sequence Number** of the last transmitted data.

📌 **Example:**

Client → Server: FIN, Seq=1050

- This means the client has **no more data to send**.

Step 2: ACK (Acknowledgment of FIN)

- The server acknowledges the FIN packet.
- The **ACK packet** contains:
    - **ACK flag = 1**
    - **Acknowledgment Number = FIN sequence number + 1**

📌 **Example:**

Server → Client: ACK, Seq=5001, Ack=1051

- This means the server **acknowledges** that the client is done sending data.

Step 3: FIN (Server Sends Its Own FIN)

- After acknowledging the client's FIN, the server may still need to send some data.

- Once the server finishes sending data, it sends its own **FIN** packet.

📌 **Example:**

Server → Client: FIN, Seq=5001

- The server **initiates its own termination request**.

Step 4: Final ACK (Acknowledgment of Server's FIN)

- The client sends a final **ACK** packet to acknowledge the server's FIN request.
- The **ACK packet** contains:
  - **ACK flag = 1**
  - **Acknowledgment Number = Server's FIN sequence number + 1**

📌 **Example:**

Client → Server: ACK, Seq=1051, Ack=5002

- After this step, the connection is fully **terminated**.

---

4. TCP States During Handshake and Termination

TCP follows a **state transition model** to track its status during the handshake and termination process.

TCP States in the Handshake Process

1. **CLOSED** → No connection exists.
2. **SYN-SENT** → Client sends SYN request.
3. **SYN-RECEIVED** → Server responds with SYN-ACK.
4. **ESTABLISHED** → Connection is fully established.

TCP States in the Termination Process

1. **FIN-WAIT-1** → Client sends FIN request.
2. **FIN-WAIT-2** → Client waits for server's FIN after ACK.
3. **TIME-WAIT** → Client waits before fully closing (to ensure all packets are received).
4. **CLOSED** → Connection is fully terminated.

---

5. Important Concepts Related to TCP Handshake and Termination

1. Half-Closed Connection

- Sometimes, **one side** may send a **FIN**, but the other still needs to send more data.
- The connection remains **half-open** until both parties send FIN.

2. Time-Wait State

- After sending the final ACK, the client **waits** in the **TIME-WAIT** state before fully closing.
- This prevents old or delayed packets from interfering with a new connection.

3. TCP Reset (RST)

- If an **unexpected termination** occurs, TCP can send an **RST (Reset) packet**.
- This happens if:
    - A connection is **abruptly closed**.
    - A packet is sent to a **non-listening** port.

---

6. Summary of TCP Handshake & Termination

Process	Steps	Description

Connection Establishment (Three-Way Handshake)	SYN → SYN-ACK → ACK	Ensures both client and server are ready to communicate.
Connection Termination (Four-Way Handshake)	FIN → ACK → FIN → ACK	Ensures both client and server gracefully close the connection.
TCP States	LISTEN, SYN-SENT, ESTABLISHED, FIN-WAIT, TIME-WAIT, CLOSED	Tracks the status of a TCP connection.
RST (Reset)	Immediate termination	Used in case of errors or unexpected disconnections.

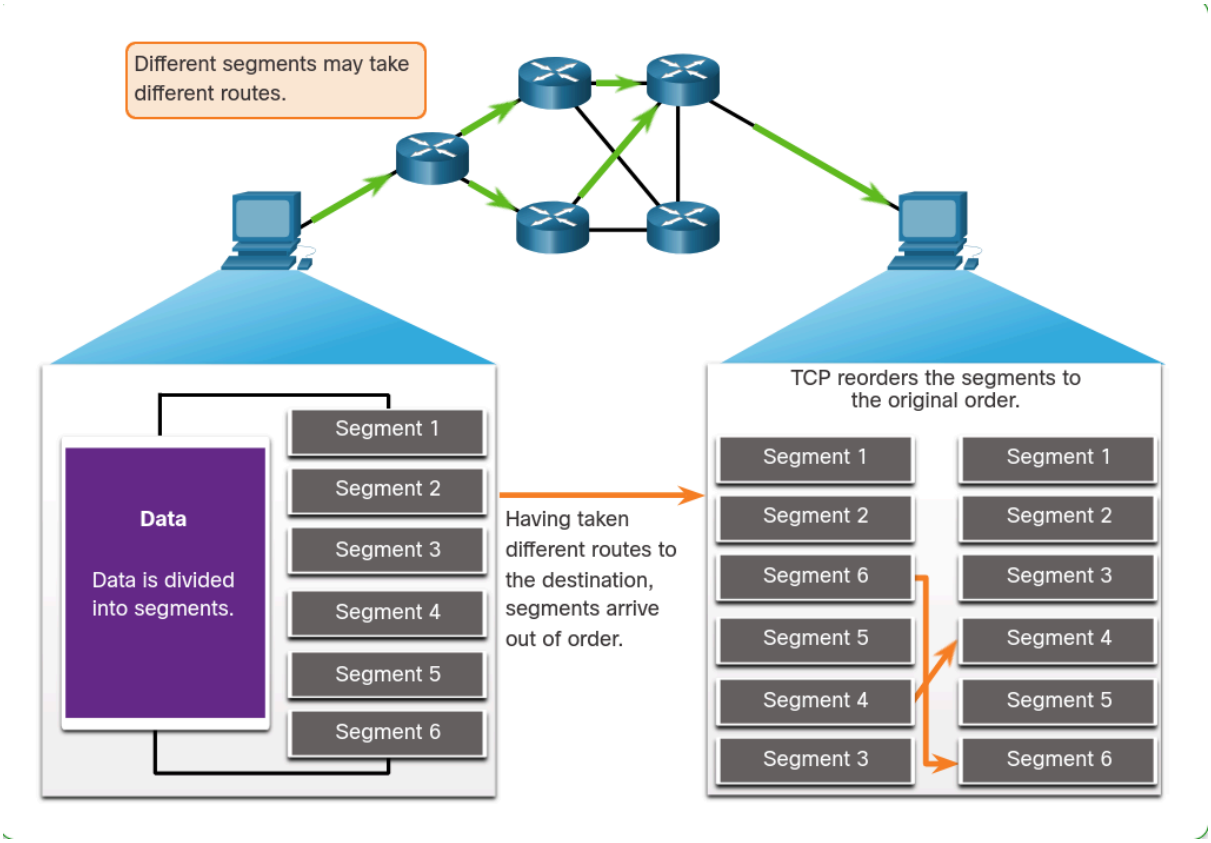
---

7. Conclusion

The **TCP handshake and termination process** are crucial for ensuring **reliable**, **ordered**, and **error-checked** communication between devices. The **Three-Way Handshake** ensures that **both parties agree to communicate**, while the **Four-Way Termination** ensures a **graceful disconnection**.

Understanding these processes is essential for **network engineers, software developers, and security professionals**, as it helps in diagnosing **network issues, optimizing performance**, and preventing **cyberattacks** like **TCP SYN Flood attacks**.

Let me know if you need further clarifications! 🚀



The window size determines the number of bytes that can be sent before expecting an acknowledgment. The acknowledgment number is the number of the next expected byte.

The window size is the number of bytes that the destination device of a TCP session can accept and process at one time. In this example, the PC B initial window size for the TCP session is 10,000 bytes. Starting with the first byte, byte number 1, the last byte PC A can send without receiving an acknowledgment is byte 10,000. This is known as the send window of PC A. The window size is included in every TCP segment so the destination can modify the window size at any time depending on buffer availability.

The initial window size is agreed upon when the TCP session is established during the three-way handshake. The source device must limit the number of bytes sent to the destination device based on the window size of the destination. Only after the source device receives an acknowledgment that the bytes have been received, can it continue sending more data for the session. Typically, the destination will not wait for all the bytes for its window size to be received before replying with an acknowledgment. As the bytes are received and processed, the destination will send acknowledgments to inform the source that it can continue to send additional bytes.

For example, it is typical that PC B would not wait until all 10,000 bytes have been received before sending an acknowledgment. This means PC A can adjust its send window as it receives acknowledgments from PC B. As shown in the figure, when PC A receives an acknowledgment with the acknowledgment number 2,921, which is the next expected byte. The PC A send window will increment 2,920 bytes. This changes the send window from 10,000 bytes to 12,920. PC A can now continue to send up to another 10,000 bytes to PC B as long as it does not send more than its new send window at 12,920.

A destination sending acknowledgments as it processes bytes received, and the continual adjustment of the source send window, is known as sliding windows. In the previous example, the send window of PC A increments or slides over another 2,921 bytes from 10,000 to 12,920.

If the availability of the destination's buffer space decreases, it may reduce its window size to inform the source to reduce the number of bytes it should send without receiving an acknowledgment.

Note: Devices today use the sliding windows protocol. The receiver typically sends an acknowledgment after every two segments it receives. The number of segments received before being acknowledged may vary. The advantage of sliding windows is that it allows the sender to continuously transmit segments, as long as the receiver is acknowledging previous segments. The details of sliding windows are beyond the scope of this course.

TCP Flow Control - Congestion Avoidance

When congestion occurs on a network, it results in packets being discarded by the overloaded router. When packets containing TCP segments do not reach their destination, they are left unacknowledged. By determining the rate at which TCP segments are sent but not acknowledged, the source can assume a certain level of network congestion.

Whenever there is congestion, retransmission of lost TCP segments from the source will occur. If the retransmission is not properly controlled, the additional retransmission of the TCP segments can make the congestion even worse. Not only are new packets with TCP segments introduced into the network, but the feedback effect of the retransmitted TCP segments that were lost will also add to the congestion. To avoid and control congestion, TCP employs several congestion handling mechanisms, timers, and algorithms.

VoIP (Voice over Internet Protocol) is a technology that allows you to make **voice calls over the internet** instead of using traditional phone lines. It converts **your voice into digital signals** and transmits them over a network (like Wi-Fi or mobile data).

How VoIP Works:

1. **Voice to Digital Conversion:** Your voice is turned into **packets of data**.
2. **Transmission Over the Internet:** These packets are sent over the internet **like any other data** (emails, videos, etc.).
3. **Reception and Playback:** The receiver's device converts the data **back into voice** so the other person can hear you.

Examples of VoIP Services:

- **WhatsApp Calls**
- **Skype, Zoom, Google Meet**
- **Discord Voice Chat**
- **Business VoIP solutions like Cisco Webex or RingCentral**

Why Use VoIP?

✅ **Cheaper than traditional calls** (especially international calls).
✅ **Works on multiple devices** (phones, laptops, tablets).
✅ **Extra features** like video calls, conference calling, and call recording.
✅ **No need for physical phone lines**, just a stable internet connection.

Downsides of VoIP:

❌ **Needs a good internet connection** (poor internet = bad call quality).
❌ **Emergency calls (911) may not be as reliable** as traditional landlines.
❌ **Latency or delays** if the network is congested.

Basically, **VoIP is how the world makes phone calls now**, and it's taking over traditional telephone systems. 🚀

What is a Socket ?

What is a Socket?

A **socket** is an **endpoint for communication** between two machines over a **network**. It allows applications to send and receive data over the internet or a local network.

1️⃣ Components of a Socket

A socket is defined by **four main elements**:

📌 **IP Address** → Identifies the device on the network.
📌 **Port Number** → Identifies the application/service on that device.
📌 **Protocol (TCP/UDP)** → Defines how data is sent.
📌 **Transport Layer Connection** → Binds everything together.

What Happens if a Particular Port is Asking for Data?

If a **specific port** is needed to request data (e.g., a client making a request to a server's known service port):

- The client **randomly selects its own source port** to send the request. The source port is not related to the port that is requesting data from the server.
- If the client is waiting for data (e.g., after making a request), the **server sends the response to the client's selected random source port**.

Presentation Layer

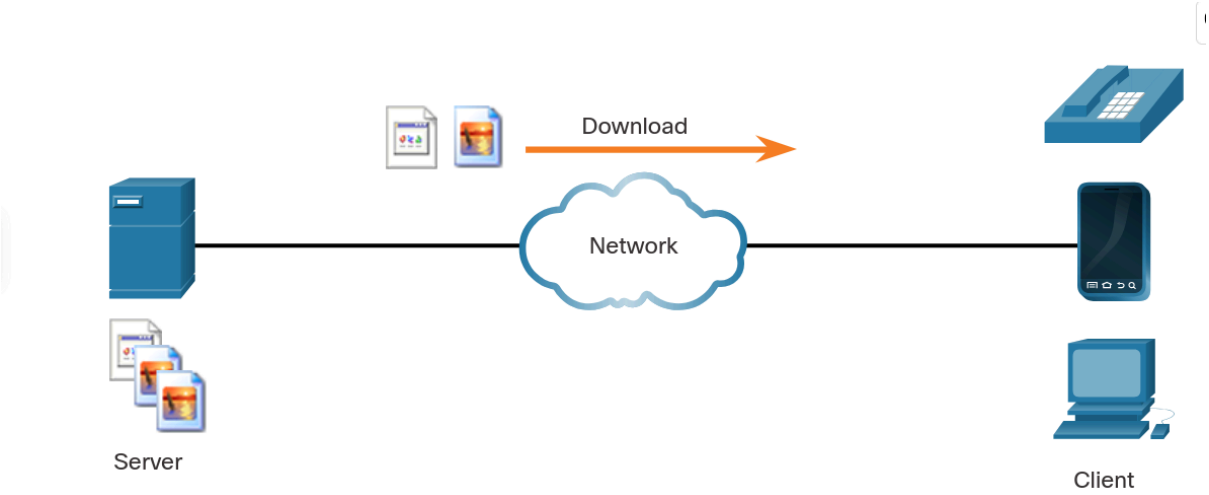
The presentation layer has three primary functions:

- Formatting, or presenting, data at the source device into a compatible format for receipt by the destination device.
- Compressing data in a way that can be decompressed by the destination device.
- Encrypting data for transmission and decrypting data upon receipt.

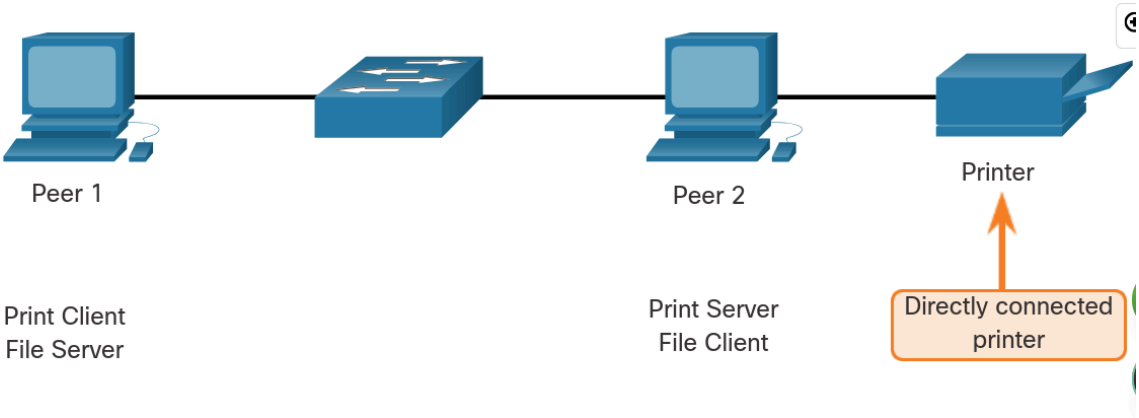
Session Layer

As the name implies, functions at the session layer create and maintain dialogs between source and destination applications. The session layer handles the exchange of information to initiate dialogs, keep them active, and to restart sessions that are disrupted or idle for a long period of time.

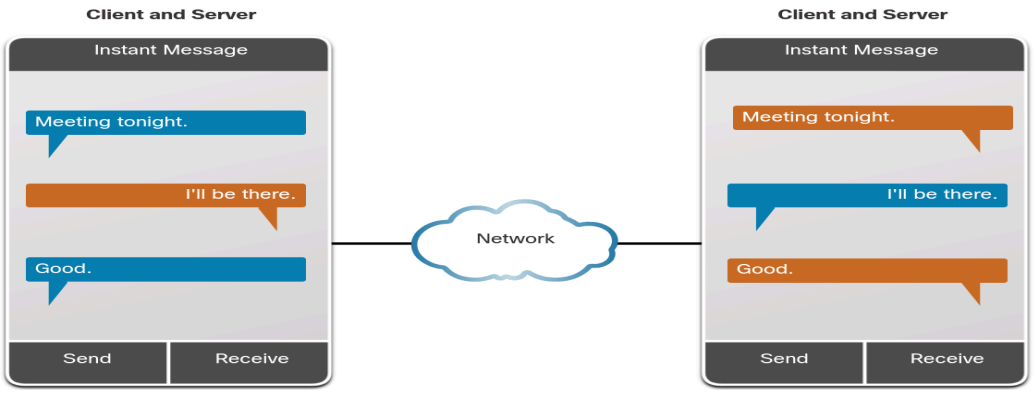
Client-Server Model



P2P Networks



Peer-to-Peer Applications



DNS

- **.com** - a business or industry
- **.org** - a non-profit organization
- **.au** - Australia
- **.co** - Colombia

The **Dynamic Host Configuration Protocol (DHCP)** for IPv4 service automates the assignment of IPv4 addresses, subnet masks, gateways, and other IPv4 networking parameters. This is referred to as dynamic addressing. The alternative to dynamic addressing is static addressing. When using static addressing, the network administrator manually enters IP address information on hosts.

When a host connects to the network, the DHCP server is contacted, and an address is requested. The DHCP server chooses an address from a configured range of addresses called a pool and assigns (leases) it to the host.

On larger networks, or where the user population changes frequently, DHCP is preferred for address assignment. New users may arrive and need connections; others may have new computers that must be connected. Rather than use static addressing for each connection, it is more efficient to have IPv4 addresses assigned automatically using DHCP.

DHCP can allocate IP addresses for a configurable period of time, called a lease period. The lease period is an important DHCP setting, When the lease period expires or the DHCP server gets a DHCPRELEASE message the address is returned to the DHCP pool for reuse. Users can freely move from location to location and easily re-establish network connections through DHCP.

As the figure shows, various types of devices can be DHCP servers. The DHCP server in most medium-to-large networks is usually a local, dedicated PC-based server. With home networks, the DHCP server is usually located on the local router that connects the home network to the ISP.

DHCP Operations

As shown in the figure, when an IPv4, DHCP-configured device boots up or connects to the network, the client broadcasts a DHCP discover

(DHCPDISCOVER) message to identify any available DHCP servers on the network. A DHCP server replies with a DHCP offer (DHCPOFFER) message, which offers a lease to the client. The offer message contains the IPv4 address and subnet mask to be assigned, the IPv4 address of the DNS server, and the IPv4 address of the default gateway. The lease offer also includes the duration of the lease.

The client may receive multiple DHCPOFFER messages if there is more than one DHCP server on the local network. Therefore, it must choose between them, and sends a DHCP request (DHCPREQUEST) message that identifies the explicit server and lease offer that the client is accepting. A client may also choose to request an address that it had previously been allocated by the server.

Assuming that the IPv4 address requested by the client, or offered by the server, is still available, the server returns a DHCP acknowledgment (DHCPACK) message that acknowledges to the client that the lease has been finalized. If the offer is no longer valid, then the selected server responds with a DHCP negative acknowledgment (DHCPNAK) message. If a DHCPNAK message is returned, then the selection process must begin again with a new DHCPDISCOVER message being transmitted. After the client has the lease, it must be renewed prior to the lease expiration through another DHCPREQUEST message.

The DHCP server ensures that all IP addresses are unique (the same IP address cannot be assigned to two different network devices simultaneously). Most ISPs use DHCP to allocate addresses to their customers.

DHCPv6 has a set of messages that is similar to those for DHCPv4. The DHCPv6 messages are SOLICIT, ADVERTISE, INFORMATION REQUEST, and REPLY.

The **Server Message Block (SMB)** protocol is a widely used **client/server file-sharing protocol** that facilitates access to shared resources like files, directories, printers, and serial ports over a network. It follows a **request-response model**, where clients send requests to servers, and the servers respond with the appropriate data or actions. Here's an explanation of the key points you mentioned:

Functions of SMB Messages:

1. **Start, authenticate, and terminate sessions**:

    - **Session management** is one of SMB's core features. A session allows clients to connect to a server, authenticate the user, and establish communication.
    - SMB handles the start of a session (initial connection), authentication (verifying the client and user credentials), and termination (closing the connection and releasing resources).
2. **Control file and printer access**:

    - **File and printer sharing** are central to SMB. When a client connects to a shared file or printer resource on the server, SMB controls access by permitting or denying read/write actions, print requests, or even listing available resources.
    - SMB enables the client to read, write, delete, and modify files on the server, as well as manage printers shared over the network.
3. **Allow an application to send or receive messages to/from another device**:

    - SMB also allows applications to exchange messages with other devices over the network. For example, a client can send a request to a server to perform an action on a shared resource, and the server responds with the result.

SMB in Microsoft Networking:

- **SMB and Microsoft Networking**: SMB has been a cornerstone of **Microsoft networking** for decades. It allows seamless integration of file and printer sharing between computers running Microsoft Windows and other devices, regardless of the underlying hardware.

- **Changes in Windows 2000**:

    - Before **Windows 2000**, Microsoft's implementation of SMB used non-TCP/IP protocols for name resolution and resource sharing. This meant that Microsoft systems didn't directly use the standard Internet protocols like **TCP/IP** for resolving names (hostnames, IP addresses) and establishing network connections.
    - **Windows 2000 and beyond**: Microsoft introduced **DNS (Domain Name System)** naming support in SMB, which allowed SMB to natively work over **TCP/IP** networks. By leveraging DNS, systems

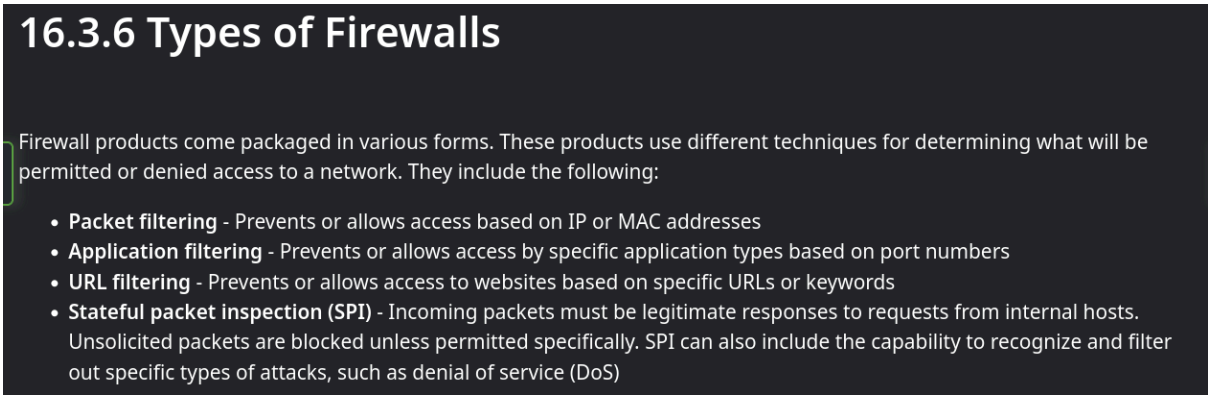
could resolve names and perform resource sharing over the Internet or within large corporate networks, making SMB much more efficient and aligned with standard internet protocols.

Impact of DNS on SMB:

- **DNS Naming**: By using DNS, SMB was able to simplify and improve name resolution. This eliminated the need for older proprietary methods for resolving names, such as **NetBIOS** or **WINS** (Windows Internet Name Service), which were often slower or unreliable.
- **Direct Support for SMB via TCP/IP**: With DNS and TCP/IP integration, SMB resource sharing became more reliable and scalable across networks. SMB could now take advantage of modern network infrastructure without needing specialized services or non-TCP/IP protocols.

Summary:

The introduction of **DNS-based naming** in **Windows 2000** marked a significant shift in how SMB works. It aligned SMB with **TCP/IP** protocols, allowing seamless integration with the Internet and improving the scalability and performance of **file-sharing**, **printer sharing**, and other SMB-based services across modern networks. This change removed the need for older name-resolution systems and provided better support for SMB in global, TCP/IP-based environments.



Security Threats and Vulnerabilities

Attacks on a network can be devastating and can result in a loss of time and money due to damage or theft of important information or assets. Intruders who gain access by modifying software or exploiting software vulnerabilities are threat actors. 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.

Network Attacks

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. The four classes of physical threats are: hardware, environmental, electrical, and maintenance. The three types of reconnaissance attacks are: internet queries, ping sweeps, and port scans. The four types of access attacks are: password (brute-force, Trojan horse, packet sniffers), trust exploitation, port redirection, and man-in-the-middle. The two types of disruption of service attacks are: DoS and DDoS.

Network Attack Mitigation

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. Servers accessible to outside users are usually located on a special network referred to as the DMZ. Firewalls use various techniques for determining what is permitted or denied access to a network including: packet filtering, application filtering, URL filtering and SPI. 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.

Device Security

The security settings are set to the default values when a new OS is installed on a device. This level of security is inadequate. For Cisco routers, the Cisco AutoSecure 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 pass phrase 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.

Devices in a Small Network

Small networks typically have a single WAN connection provided by DSL, cable, or an Ethernet connection. Small networks are managed by a local IT technician or by a contracted professional. 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. In fact, a good network design will implement quality of service (QoS) to classify traffic carefully according to priority.

Small Network Applications and Protocols

There are two forms of software programs or processes that provide access to the network: network applications and application layer services. Some end-user applications implement application layer protocols and are able to communicate directly with the lower layers of the protocol stack. Email clients and web browsers are examples of this type of application. Other programs may need the assistance of application layer services to use network resources like file transfer or network print spooling. These are the programs that interface with the network and prepare the data for transfer. The two most common remote access solutions are Telnet and Secure Shell (SSH). SSH service is a secure alternative to Telnet. Network administrators must also support common network servers and their required related network protocols such as web server, email server, FTP server, DHCP server, and DNS server. Businesses today are increasingly using IP telephony and streaming media to communicate with customers and business partners. These are real-time applications. The network infrastructure must support VoIP, IP telephony, and other real-time applications.

Scale to Larger Networks

To scale a network, several elements are required: network documentation, device inventory, budget, and traffic analysis. Know the type of traffic that is crossing the network as well as the current traffic flow. Capture traffic during peak utilization times to get a good representation of the different traffic types and perform the capture on different network segments and devices as some traffic will be local to a particular segment. Network administrators must know how network use is changing. Usage details of employee computers can be captured in a 'snapshot' with such tools as the Windows Task Manager, Event Viewer, and Data Usage.

Verify Connectivity

The **ping** command is the most effective way to quickly test Layer 3 connectivity between a source and destination IP address. The command also displays various round-trip time statistics. 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. Extended ping is entered in privileged EXEC mode by typing ping without a destination IP address. Traceroute can help locate Layer 3 problem areas in a network. A trace returns a list of hops as a packet is routed through a network. It is used to identify the point along the path where the problem can be found. In Windows, the command is **tracert**. In Cisco IOS the command is **traceroute**. There is also an extended **traceroute** command. It allows the administrator to adjust parameters related to the command operation. The output derived from network commands contributes data to the network baseline. One method for starting a baseline is to copy and paste the results from an executed ping, trace, or other relevant commands into a text file. These text files can be time stamped with the date and saved into an archive for later retrieval and comparison.

Host and IOS Commands

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.

Troubleshooting Methodologies

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.

A problem should be escalated when it requires a the decision of a manager, some specific expertise, or network access level unavailable to the troubleshooting technician. OS processes, protocols, mechanisms and events generate messages to communicate their status. The IOS **debug** command allows the administrator to display these messages in real-time for analysis. To display log messages on a terminal (virtual console), use the **terminal monitor** privileged EXEC command.

Troubleshooting Scenarios

There are two duplex communication modes: half-duplex and full-duplex. If one of the two connected devices is operating in full-duplex and the other is operating in half-duplex, a duplex mismatch occurs. While data communication will occur through a link with a duplex mismatch, link performance will be very poor.

Wrongly assigned IP addresses create a variety of issues, including IP address conflicts and routing problems. Two common causes of incorrect IPv4 assignment are manual assignment mistakes or DHCP-related issues. Most end devices are configured to rely on a DHCP server for automatic IPv4 address assignment. If the device is unable to communicate with the DHCP server, then the server cannot assign an IPv4 address for the specific network and the device will not be able to communicate.

The default gateway for an end device is the closest networking device that can forward traffic to other networks. If a device has an incorrect or nonexistent default gateway address, it will not be able to communicate with devices in remote networks. Because the default gateway is the path to remote networks, its address must belong to the same network as the end device.

DNS failures often lead the user to conclude that the network is down. If a user types in a domain name such as www.cisco.com in a web browser and the DNS server is unreachable, the name will not be translated into an IP address and the website will not display.

11.8.4 VLSM

In all of the previous subnetting examples, the same subnet mask was applied for all the subnets. This means that each subnet has the same number of available host addresses. As illustrated in the left side of the figure, traditional subnetting creates subnets of equal size. Each subnet in a traditional scheme uses the same subnet mask. As shown in the right side of the figure, VLSM allows a network space to be divided into unequal parts. With VLSM, the subnet mask will vary depending on how many bits have been borrowed for a particular subnet, thus the “variable” part of the VLSM.

VLSM is just subnetting a subnet. The same topology used previously is shown in the figure. Again, we will use the 192.168.20.0/24 network and subnet it for seven subnets, one for each of the four LANs, and one for each of the three connections between the routers.