NETWORK AND DATA COMMUNICATION

Norsulliatie Binti Muhammad
Suhaila Binti Sarif
Siti Fartimah Binti Mohamed Yusop

POLITEKNIK MALAYSIA
METRO TASEK GELUGOR

NETWORK AND DATA COMMUNICATION

Norsulliatie Binti Muhammad
Suhaila Binti Sarif
Siti Fartimah Binti Mohamed Yusop

Network And Data Communication

First Edition 2025

Published by
POLITEKNIK METrO TASEK GELUGOR,
DEPARTMENT OF INFORMATION TECHNOLOGY AND COMMUNICATION,
No 25, Jalan Komersial 2,
Pusat Komersial Tasek Gelugor,
13300 Tasek Gelugor,
PULAU PINANG.

Content & Design by
Norsulliatie binti Muhammad,
Suhaila binti Sarif,
Siti Fartimah Binti Mohamed Yusop

Perpustakaan Negara Malaysia

Abstract

NETWORK AND DATA COMMUNICATION introduces the architecture, structure, functions, components, and models of the Internet and other computer networks. This course also explains the principles and structure of IP addressing and the fundamentals of Ethernet concepts, media, and operations are introduced to provide a foundation for the curriculum. Students will be able to design simple Local Area Networks (LAN), perform basic configurations for routers and switches, troubleshoot connectivity issue and implement IP addressing schemes.

AR USER MANUAL FOR APPLICATION

Below are the steps to download and use the AR application on your Android phone.
The Augmented Reality (AR) application for this book was developed with the aim of diversifying readers' learning experiences in the field of Network and Data Communication, through the use of innovative AR technology. With this application, readers can explore learning methods beyond the classroom, using techniques presented in a more dynamic and interactive 3D environment. Follow the steps below to begin using the AR application effectively.

1 INSTALL THE APPLICATION

Scan the QR code to download and install the application.
You may see a pop-up window asking for permissions required by the application. Review the permissions and click "Accept" to continue with the installation.

2 OPEN THE APPLICATION

Once the application has been downloaded and installed, you will see a pop-up message requesting permission.
Click "Allow" to grant camera access while using the application.
Next, you will see a "Play" button icon as the main page.
Click this button to start the application immediately and proceed to the menu screen.

3

MAIN PAGE
You will be taken to the menu page, where you can choose one of the following options:
Play AR : To use the augmented reality camera and view images in 3D.
Apps Info: To view guides how to use AR Camera.
Couse : Summary of the eBook
Exit : Leave the application

PLAY AR
When you click the "PLAY AR" button, it will open the camera.
You can use the camera to scan AR markers to begin your AR experience.
Try scanning the target image on the next page to experience 3D objects, images, and videos.

Table of Contents

01
EXPLORE THE NETWORK

1.1.1 How does network impact our daily life?

Networks support the way we learn.

Networks support the way we communicate.

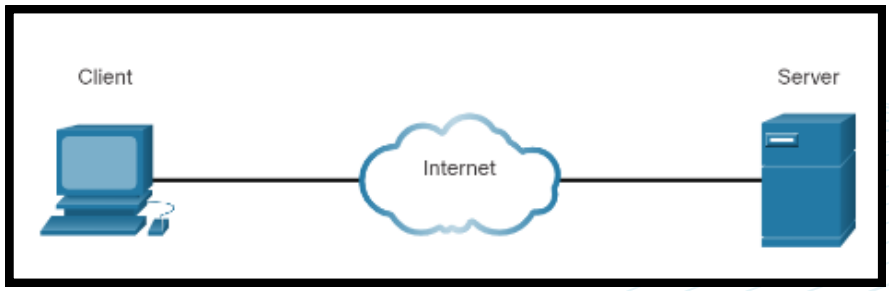
Networks support the way we work.

Networks support the way we play.

1.1.2 Function of host and network devices

a. Host Roles

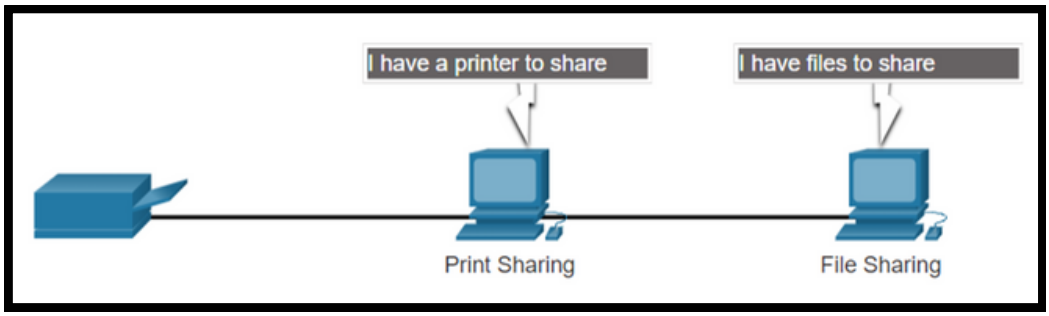
- Hosts are computers connected to a network that participate in communication. They are assigned an IP address which identifies them on the network.
- IP Address (Internet Protocol address): A unique number used to identify a host and its associated network.
- Clients are a type of host that request services or information.
- Servers are computers with specific software that provide services (e.g., web or email) to other devices (clients).
- A server can handle requests from multiple clients at once.
- Clients use special software to request and display information from servers.



1.1.2 Function of host and network devices

b. Peer-to-Peer

- Client and server software typically run on separate computers.
- One computer can perform both roles (client and server) simultaneously.
- In small businesses and homes, computers often act as both servers and clients. This setup is known as a peer-to-peer (P2P) network.
- In the figure, the print sharing PC has a Universal Serial Bus (USB) connection to the printer and a network connection, using a network interface card (NIC), to the file sharing PC.



Advantages	Disadvantages
•Easy to setup •Less complex •Lower cost because network devices are dedicated servers may not be required •Can be use for simple tasks such as transferring files and sharing printers	•No centralized administration •Not as secure •Not scalable •All devices may act as both clients and server which can slow their performance

1.1.2 Function of host and network devices

c. End Devices

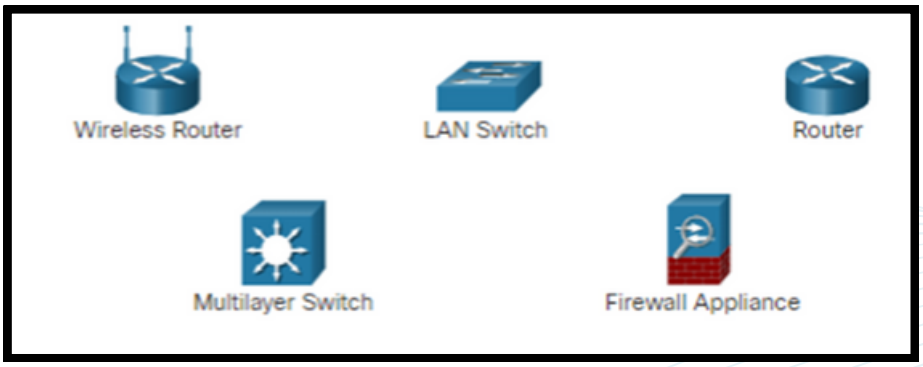
- End devices are the devices at the edge of a network that users interact with directly. They either send, receive, or request data across a network.
- Some examples of end devices are:

1. Computers (work stations, laptops, file servers, web servers)
2. Network printers
3. VoIP phones
4. TelePresence endpoint
5. Security cameras
6. Mobile handheld devices (such as smart phones, tablets, PDAs, and wireless debit / credit card readers and barcode scanners)

1.1.2 Function of host and network devices

d. Intermediary Devices

- An intermediary device interconnects end devices in a network.
- The management of data as it flows through a network is also the role of an intermediary device including:
  1. Regenerate and retransmit data signals.
  2. Maintain information about what pathways exist through the network and internetwork.
  3. Notify other devices of errors and communication failures.
- Examples of intermediary network devices are:
  1. Network Access Devices (switches and wireless access points)
  2. Internetworking Devices (routers)
  3. Security Devices (firewalls)

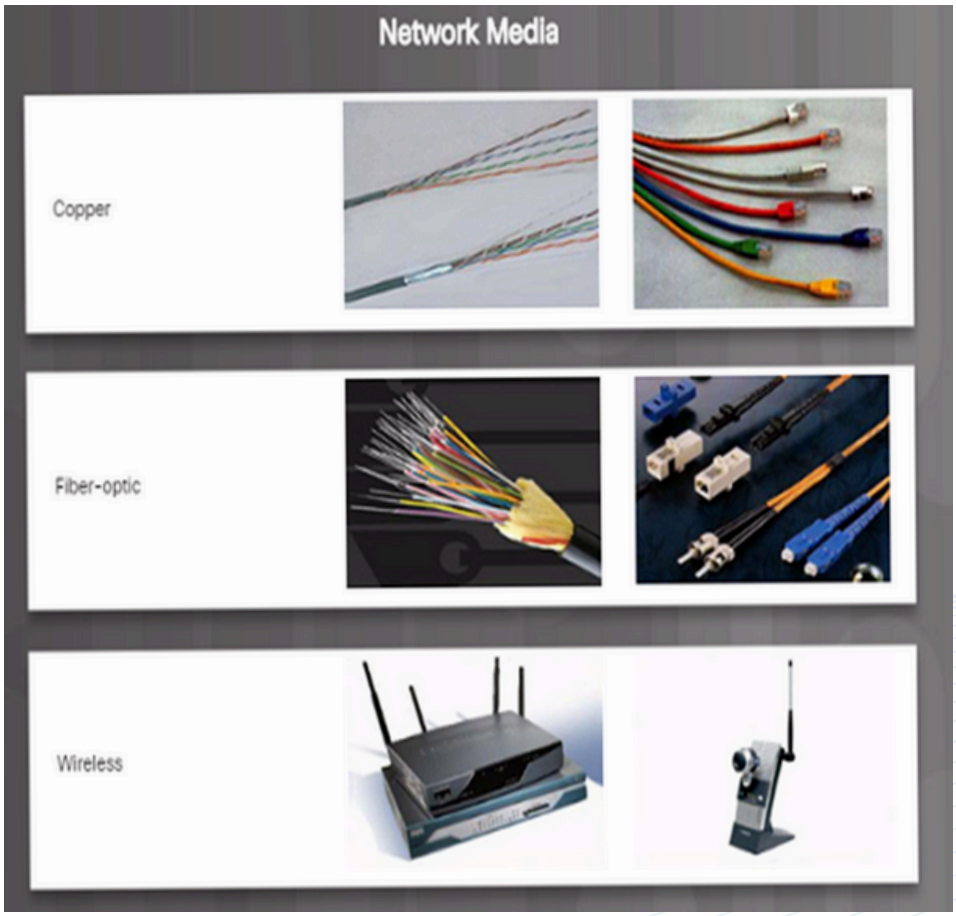


1.1.2 Function of host and network devices

e. Network Media

- Communication across a network is carried through a medium which allows a message to travel from source to destination.

- Networks typically use three types of media:
  1. Metallic wires within cables, such as copper
  2. Glass, such as fiber optic cables
  3. Wireless transmission



1.1.3 Types of networks

Local Area Network (LAN)

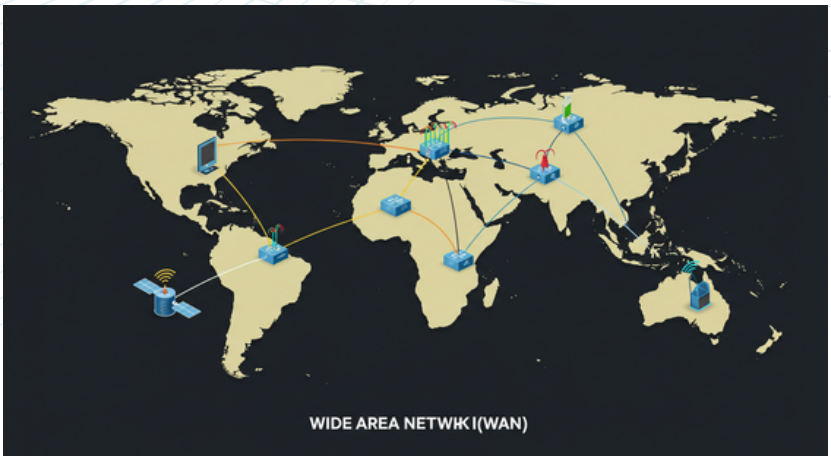
- A Local Area Network (LAN) is a network that connects computers and other devices within a limited area, such as:
    1. A home
    2. An office
    3. A school
    4. A small building or group of nearby buildings

- Key Features of LAN:
    1. Covers a small geographic area
    2. High-speed connections (typically using Ethernet or Wi-Fi)
    3. Privately owned and managed
    4. Allows resource sharing (e.g., printers, files, internet)

- Examples of LAN Use:
    1. Connecting multiple PCs in a computer lab
    2. Sharing a printer among office employees
    3. Connecting a router, smart TV, and laptops at home

1.1.3 Types of networks

Wide Area Network (WAN)



- A Wide Area Network (WAN) is a type of network that spans a large geographic area, often across cities, countries, or even continents. It connects multiple smaller networks like LANs (Local Area Networks).
    1. A home
    2. An office
    3. A school
    4. A small building or group of nearby buildings

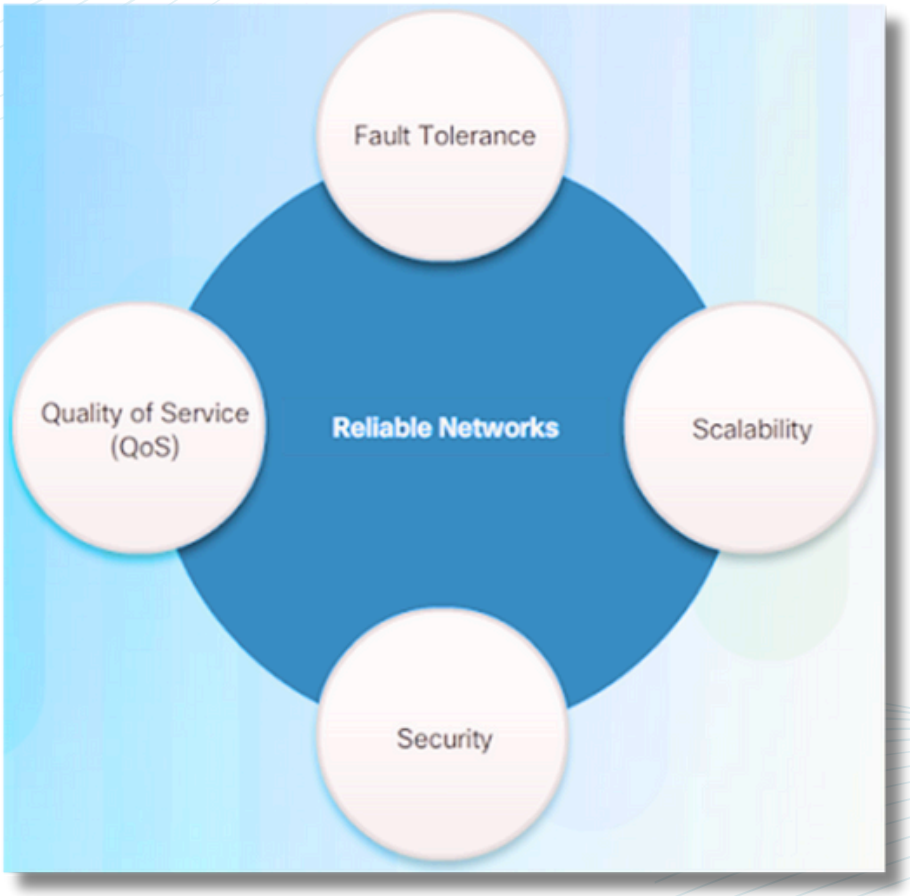
- Key Features of WAN:
    1. Covers large distances
    2. Connects multiple LANs
    3. Uses public or leased communication lines (e.g., telephone lines, satellites, fiber optics)
    4. Often managed by Internet Service Providers (ISPs)
    5. Enables global communication and data transfer

- Examples of WAN Use:
    1. The Internet (largest WAN in the world)
    2. A corporation connecting offices in different cities or countries
    3. Banks linking ATMs across regions

1.1.4 Basic Requirement of a Reliable Network

There are four basic characteristics that the underlying architectures need to address to meet user expectations:

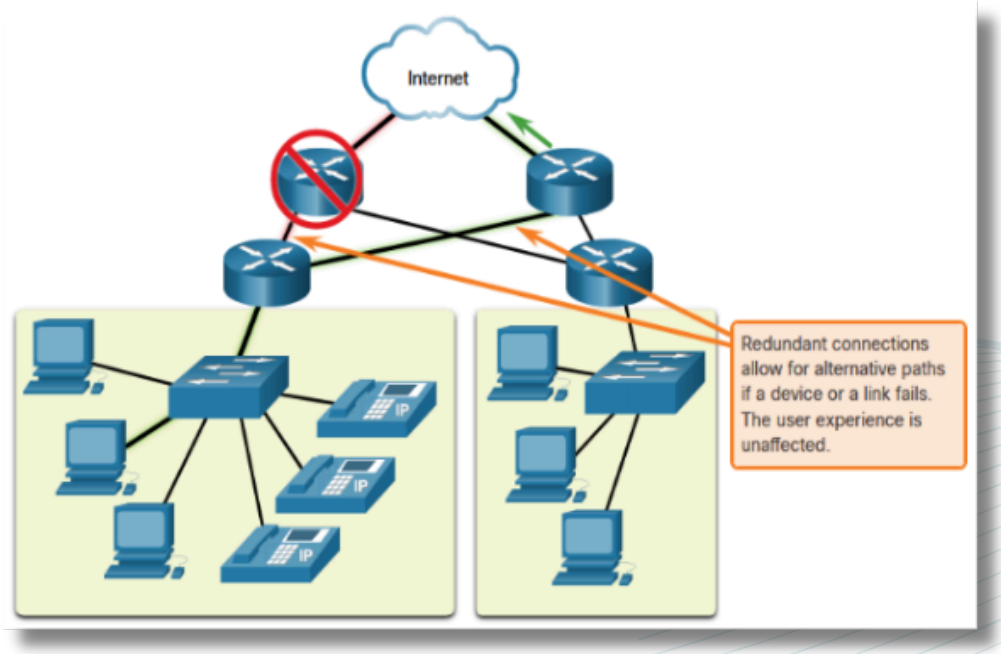
a. Fault Tolerance
b. Scalability
c. Quality of Service (QoS)
d. Security



1.1.4 Basic Requirement of a Reliable Network

a. Fault Tolerance

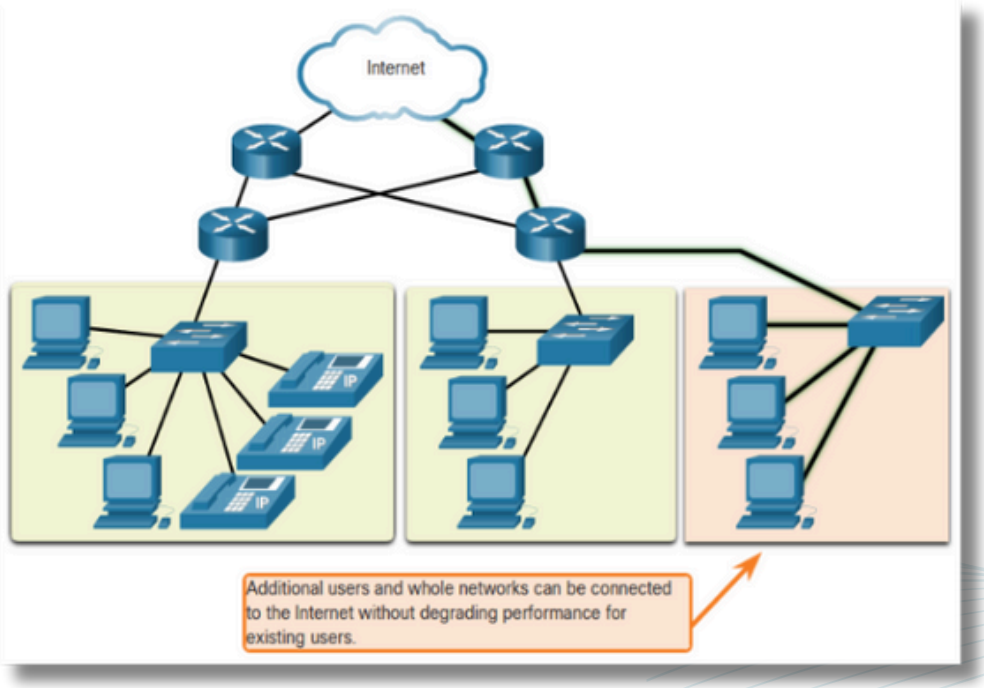
- A fault tolerant network limits the impact of a failure by limiting the number of affected devices. Multiple paths are required for fault tolerance.
- Reliable networks provide redundancy by implementing a packet switched network.
- Packet switching splits traffic into packets that are routed over a network.
- Each packet could theoretically take a different path to the destination.
- This is not possible with circuit-switched networks which establish dedicated circuits.



1.1.4 Basic Requirement of a Reliable Network

b. Scalability

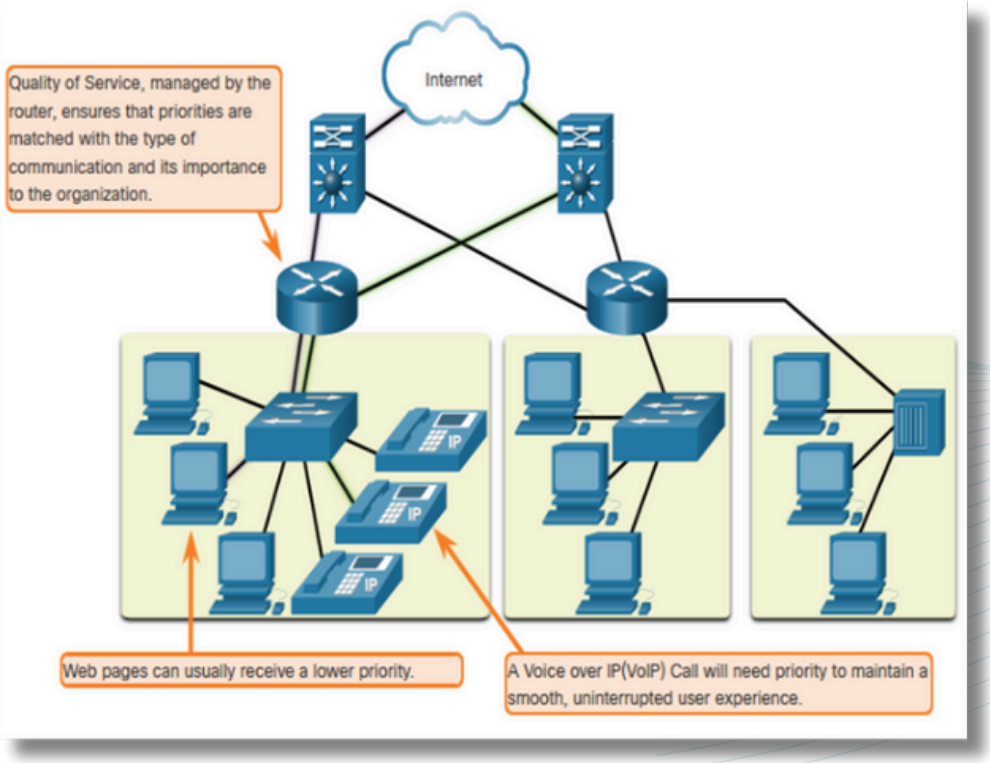
- A scalable network can expand quickly and easily to support new users and applications without impacting the performance of services to existing users.
- Network designers follow accepted standards and protocols in order to make the networks scalable.



1.1.4 Basic Requirement of a Reliable Network

c. Quality of Service (QoS)

- Voice and live video transmissions require higher expectations for those services being delivered.
- Have you ever watched a live video with constant breaks and pauses? This is caused when there is a higher demand for bandwidth than available – and QoS isn't configured.
- Quality of Service (QoS) is the primary mechanism used to ensure reliable delivery of content for all users.
- With a QoS policy in place, the router can more easily manage the flow of data and voice traffic.

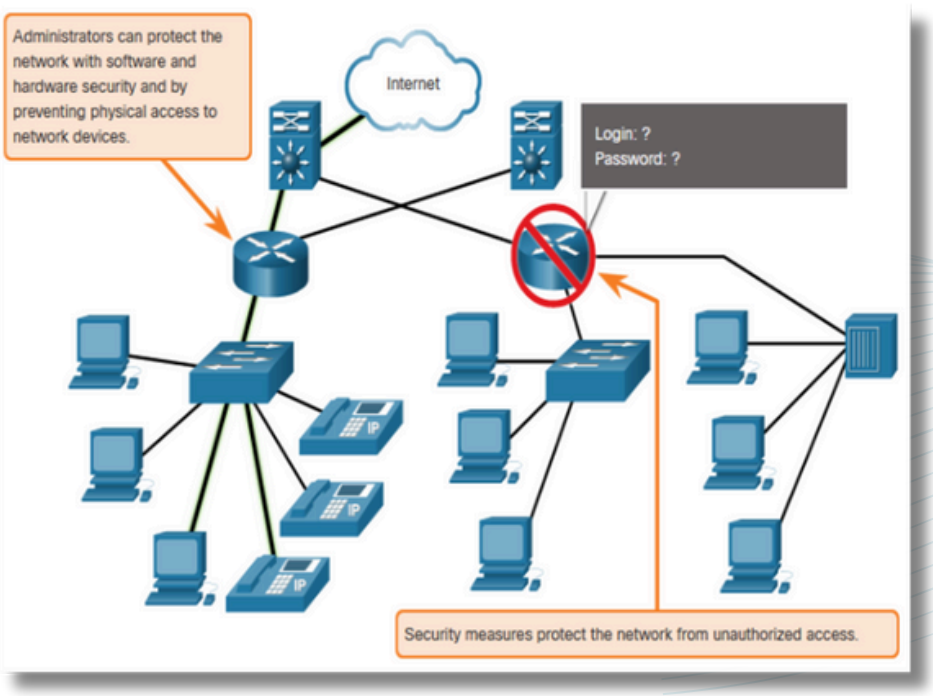


1.1.4 Basic Requirement of a Reliable Network

d. Network Security

- There are two main types of network security that must be addressed:
    1. Network infrastructure security
        - Physical security of network devices
        - Preventing unauthorized access to the devices
    2. Information Security
        - Protection of the information or data transmitted over the network

- Three goals of network security:
    1. Confidentiality – only intended recipients can read the data
    2. Integrity – assurance that the data has not be altered with during transmission
    3. Availability – assurance of timely and reliable access to data for authorized users



1.1.5 The Network Trends

BYOD

- Bring Your Own Device (BYOD) is a major global trend that allows users to use their own devices giving them more opportunities and greater flexibility.

- BYOD allows end users to have the freedom to use personal tools to access information and communicate using their:

  i. Laptops
  ii. Netbooks
  iii. Tablets
  iv. Smartphones
  v. E-readers

1.1.5 The Network Trends

Online Collaboration

- Individuals want to collaborate and work with others over the network on joint projects.
- Collaboration tools like example, Cisco WebEx gives users a way to instantly connect, interact and achieve their objectives.
- Collaboration is a very high priority for businesses and in education.

1.1.5 The Network Trends

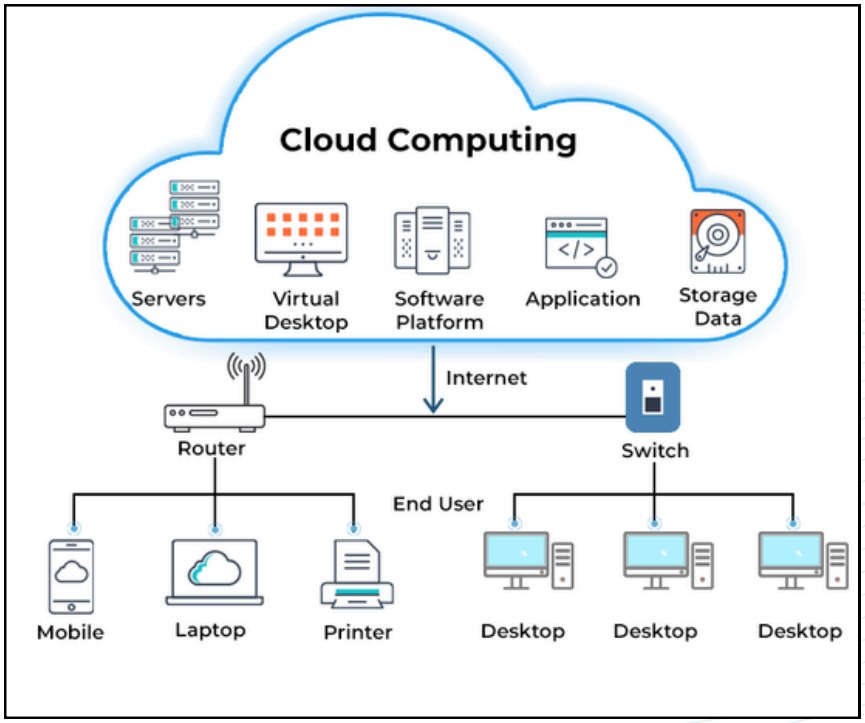
Video Communication

- Cisco TelePresence powers the new way of working where everyone, everywhere, can be more productive through face to face collaboration.
- Around the world each day, we transform organizations by transforming our customer experiences.

1.1.5 The Network Trends

Cloud Computing

- Cloud computing is a global trend that allows us to store personal files or backup our data on servers over the Internet.
- Applications such as word processing and photo editing can also be accessed using the Cloud.
- Cloud computing also allows businesses to extend their capabilities on demand and delivered automatically to any device anywhere in the world.
- Cloud computing is made possible by data centers. Smaller companies that can't afford their own data centers, lease server and storage services from larger data center organizations in the Cloud.

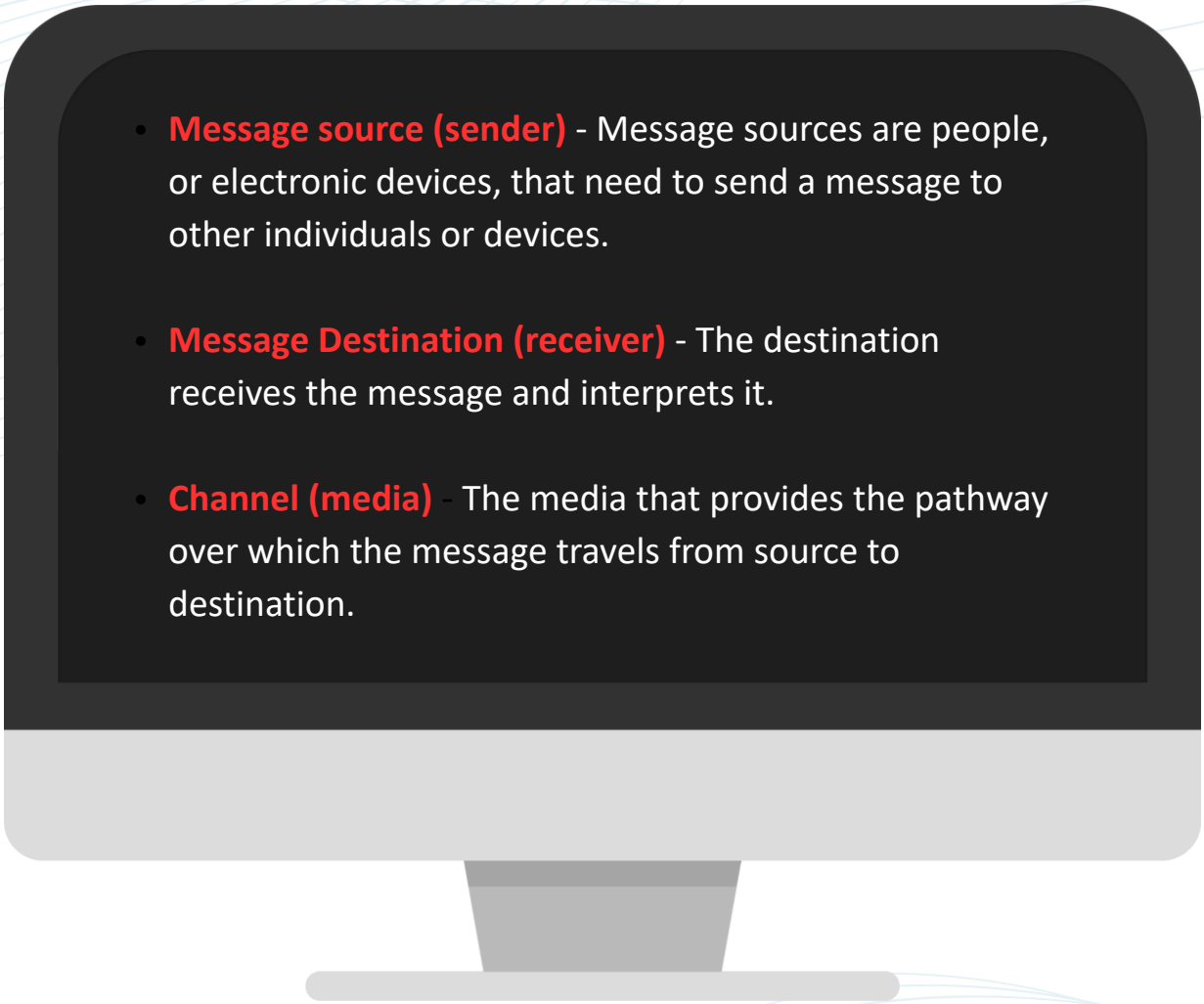


1.1.5 The Network Trends

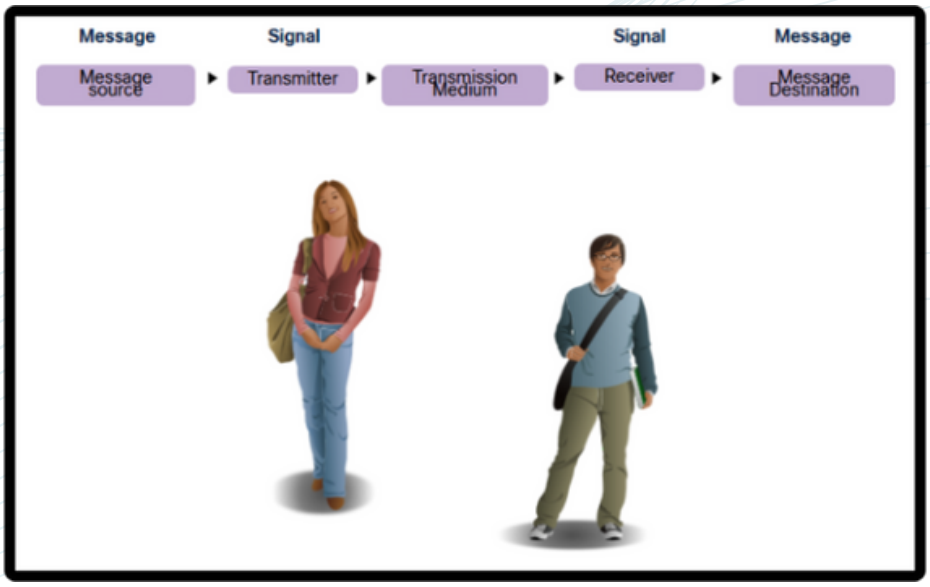
Cloud Computing

Cloud Type	Description
Public clouds	Cloud-based applications and services offered in a public cloud are made available to the general population. Services may be free or are offered on a pay-per-use model, such as paying for online storage. The public cloud uses the internet to provide services.
Private clouds	Cloud-based applications and services offered in a private cloud are intended for a specific organization or entity, such as a government. A private cloud can be set up using the organization's private network, though this can be expensive to build and maintain. A private cloud can also be managed by an outside organization with strict access security.
Hybrid clouds	A hybrid cloud is made up of two or more clouds (example: part private, part public), where each part remains a distinct object, but both are connected using a single architecture. Individuals on a hybrid cloud would be able to have degrees of access to various services based on user access rights.
Community clouds	A community cloud is created for exclusive use by specific entities or organizations. The differences between public clouds and community clouds are the functional needs that have been customized for the community. For example, healthcare organizations must remain compliant with policies and laws (e.g., HIPAA) that require special authentication and confidentiality. Community clouds are used by multiple organizations that have similar needs and concerns. Community clouds are similar to a public cloud environment, but with set levels of security, privacy, and even regulatory compliance of a private cloud.

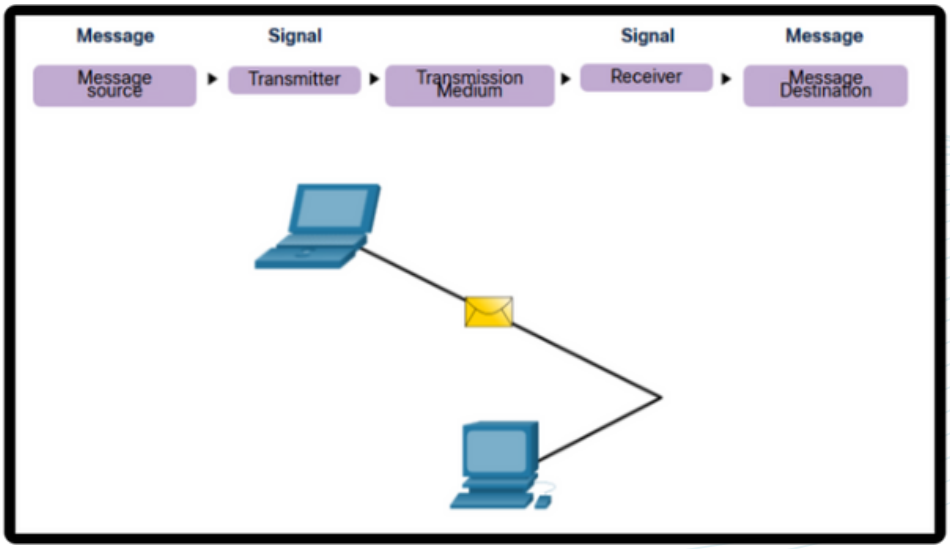
1.2.1 Elements in communications fundamentals



1.2.2 Network Protocol Requirements



- All communications are governed by protocols.
- Protocols are the rules that communications will follow.
- These rules will vary depending on the protocol.



1.2.2 Network Protocol Requirements

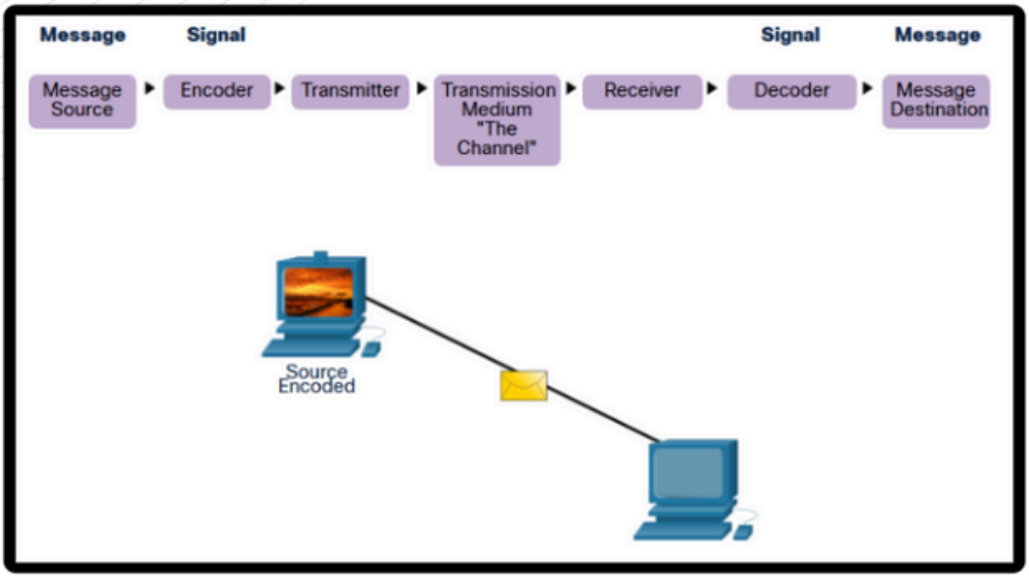
- Common computer protocols must be in agreement and include the following requirements:

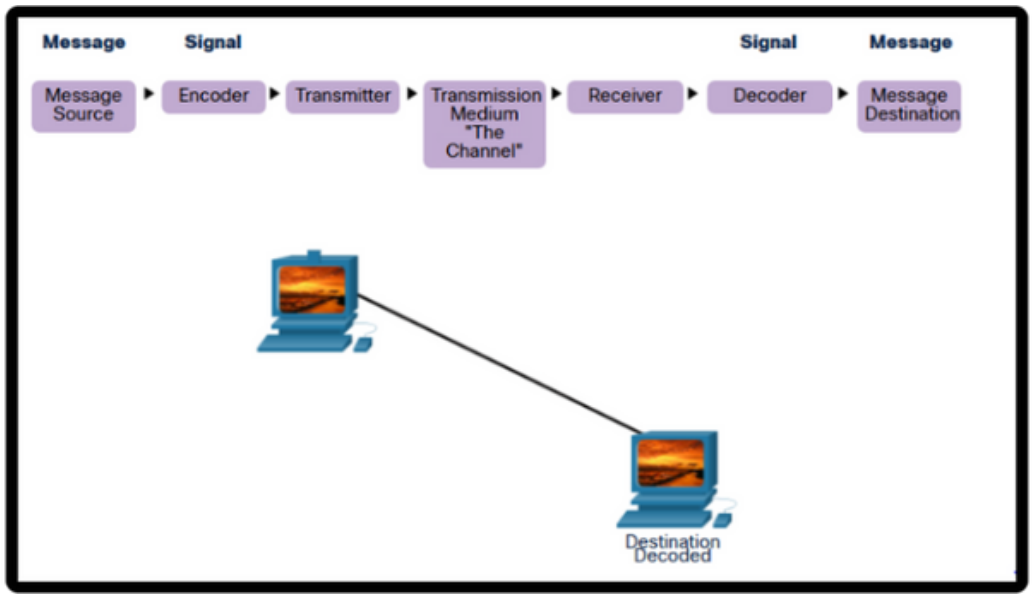
1. **Message encoding**
2. **Message formatting and encapsulation**
3. **Message size**
4. **Message timing**
5. **Message delivery options**

1.2.2 Network Protocol Requirements

1 Message delivery options

- Encoding is the process of converting information into another acceptable form for transmission.
- Decoding reverses this process to interpret the information.

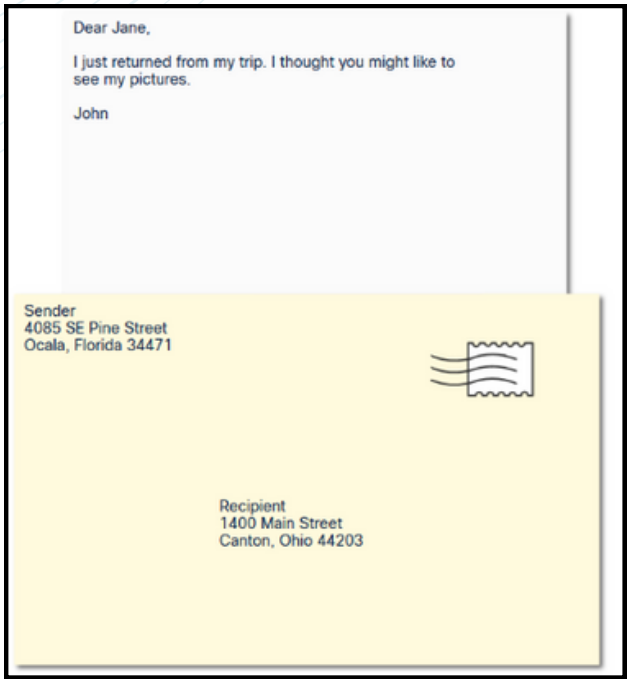


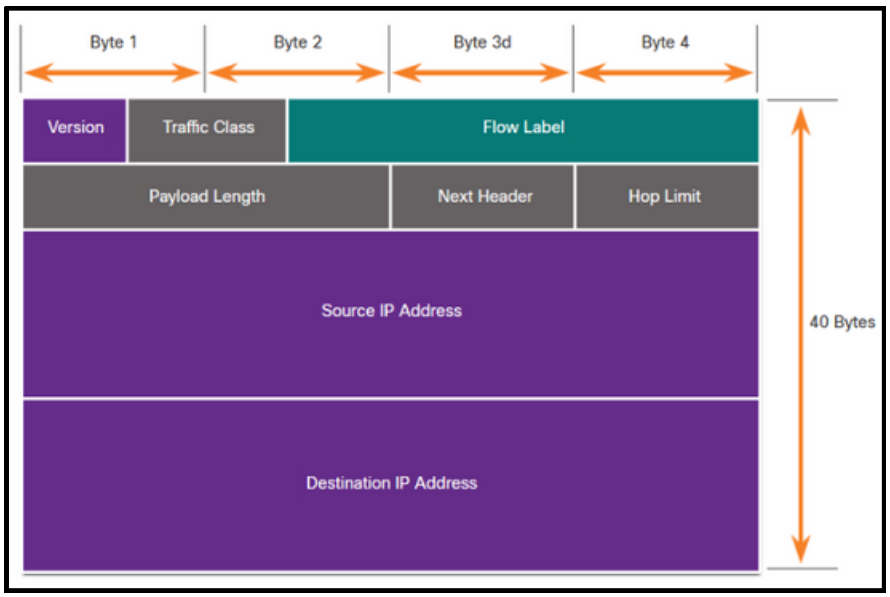


1.2.2 Network Protocol Requirements

2 Message formatting and encapsulation

- When a message is sent, it must use a specific format or structure.
- Message formats depend on the type of message and the channel that is used to deliver the message.

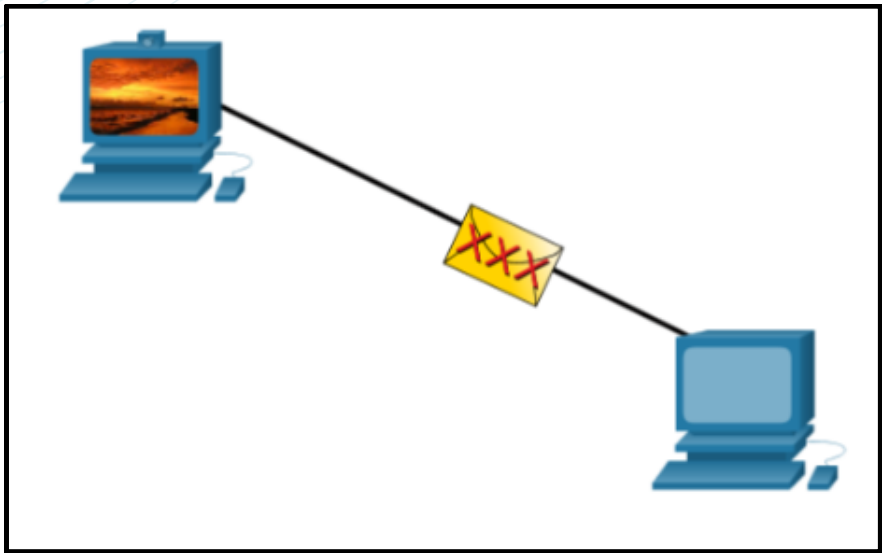


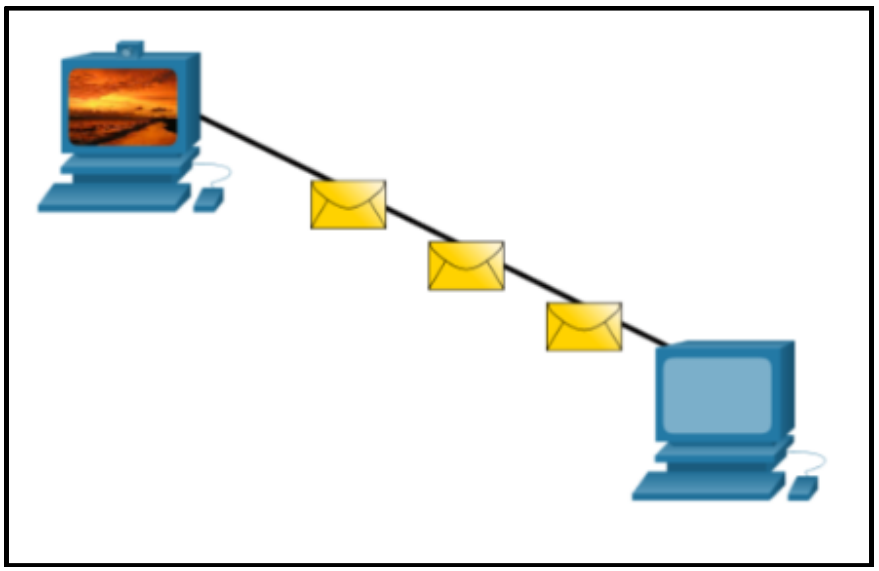


1.2.2 Network Protocol Requirements

3 Message size

- Encoding between hosts must be in an appropriate format for the medium.
  - Messages sent across the network are converted to bits
  - The bits are encoded into a pattern of light, sound, or electrical impulses.
  - The destination host must decode the signals to interpret the message.





1.2.2 Network Protocol Requirements

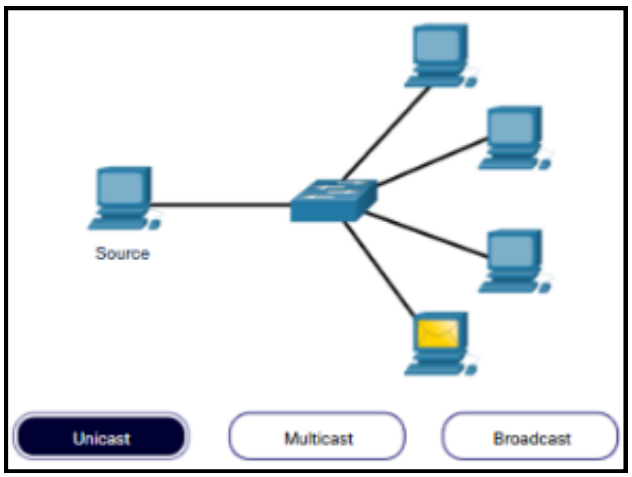
4 Message timing

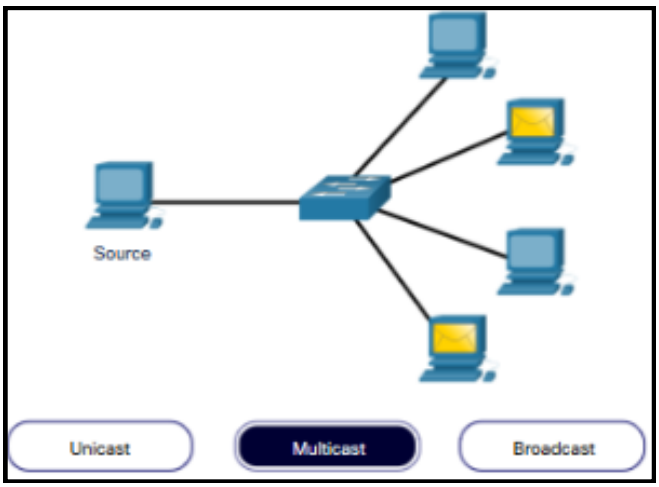
- Message timing includes the following:
  - **Flow Control** – Manages the rate of data transmission and defines how much information can be sent and the speed at which it can be delivered.
  - **Response Timeout** – Manages how long a device waits when it does not hear a reply from the destination.
  - **Access method** - Determines when someone can send a message.
    - There may be various rules governing issues like “collisions”. This is when more than one device sends traffic at the same time and the messages become corrupt.
    - Some protocols are proactive and attempt to prevent collisions; other protocols are reactive and establish a recovery method after the collision occurs.

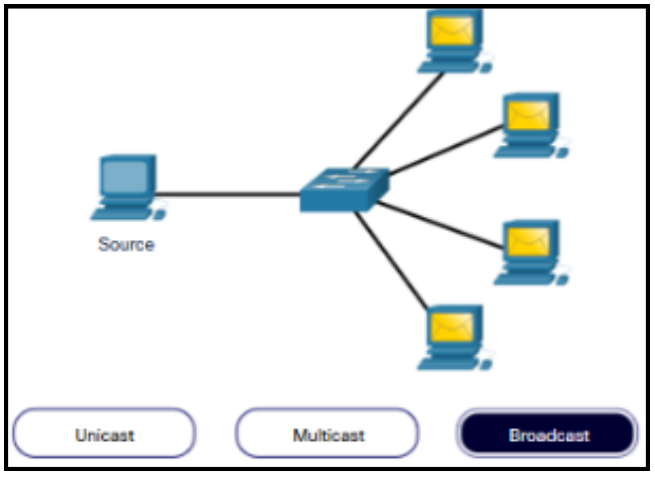
1.2.2 Network Protocol Requirements

5 Message delivery options

- Message delivery may one of the following methods:
  - **Unicast** – one to one communication
  - **Multicast** – one to many, typically not all
  - **Broadcast** – one to all
- Note: Broadcasts are used in IPv4 networks, but are not an option for IPv6. Later we will also see “Anycast” as an additional delivery option for IPv6.



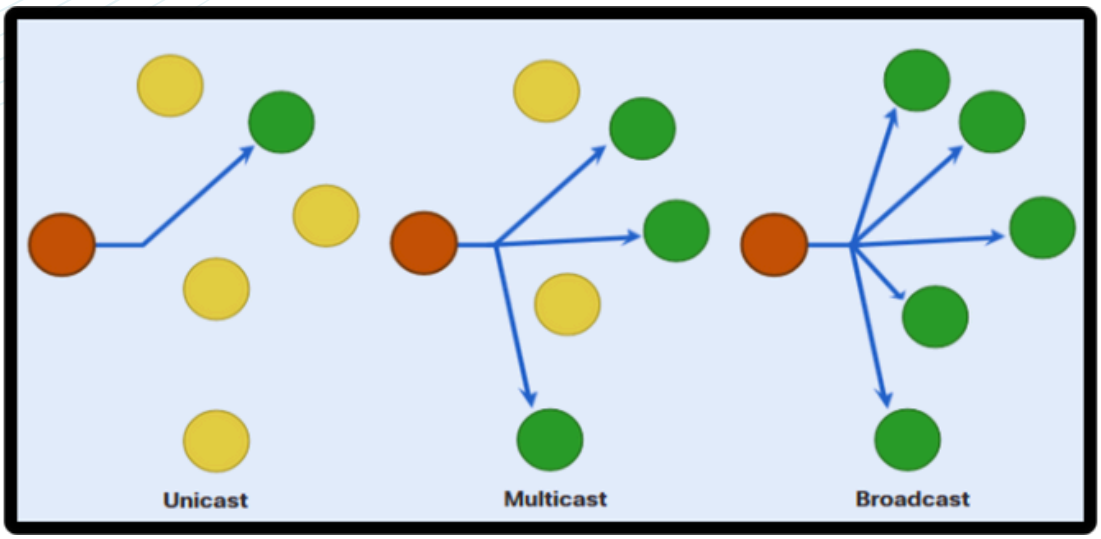




1.2.2 Network Protocol Requirements

5 Message delivery options

- A Note About the Node Icon
  - Documents may use the node icon , typically a circle, to represent all devices.
  - The figure illustrates the use of the node icon for delivery options.



1.2.2 Network Protocol Requirements

Network Protocol Overview

- Network protocols define a common set of rules.

1. Can be implemented on devices in :
   - Software
   - Hardware
   - Both

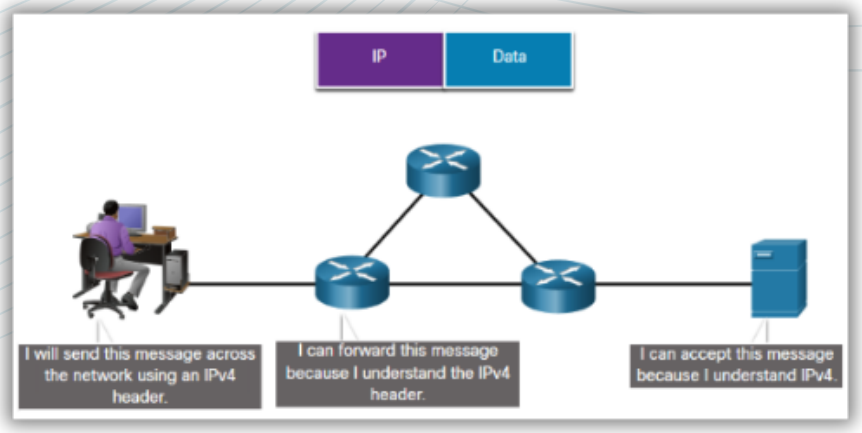
2. Protocols have their own:
   - Function
   - Format
   - Rules

Protocol Type	Description
Network Communications	enable two or more devices to communicate over one or more networks
Network Security	secure data to provide authentication, data integrity, and data encryption
Routing	enable routers to exchange route information, compare path information, and select best path
Service Discovery	used for the automatic detection of devices or services

1.2.2 Network Protocol Requirements

Network Protocol Functions

- Devices use agreed-upon protocols to communicate .
- Protocols may have may have one or functions.

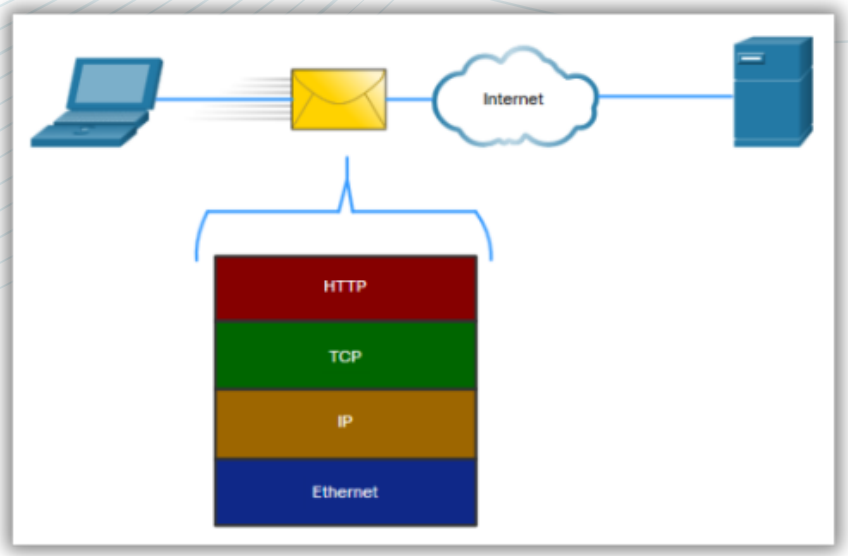


Function	Description
Addressing	Identifies sender and receiver
Reliability	Provides guaranteed delivery
Flow Control	Ensures data flows at an efficient rate
Sequencing	Uniquely labels each transmitted segment of data
Error Detection	Determines if data became corrupted during transmission
Application Interface	Process-to-process communications between network applications

1.2.2 Network Protocol Requirements

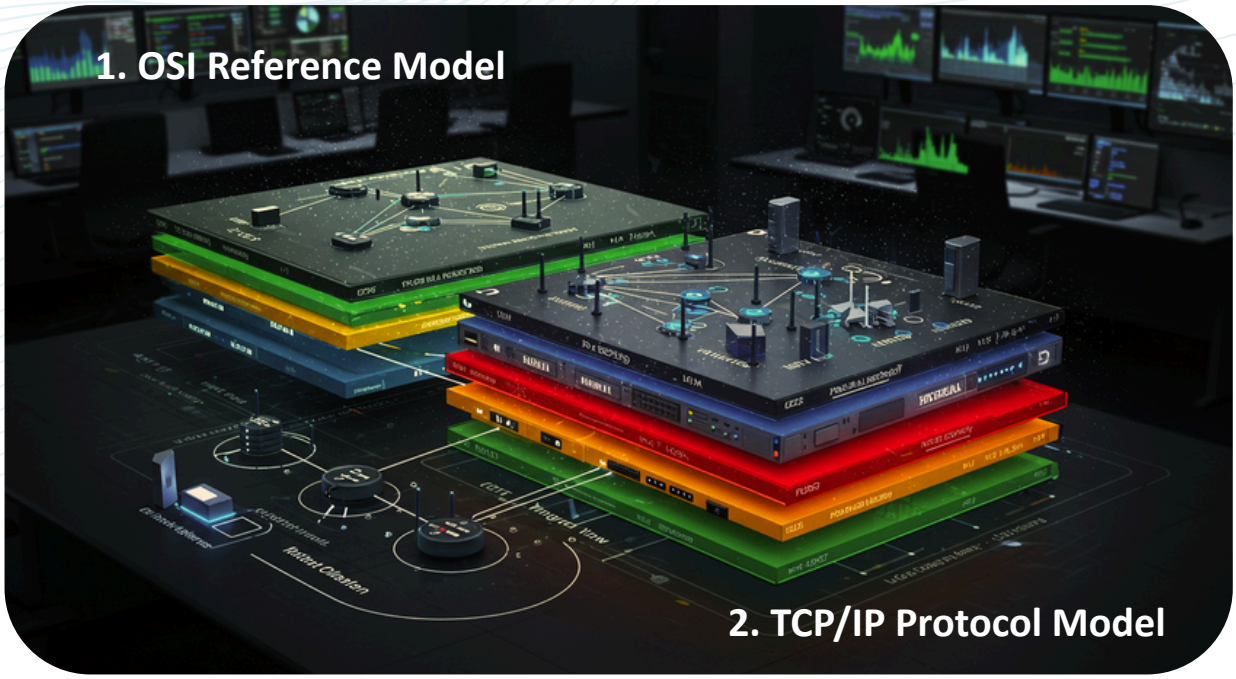
Protocol Interaction

- Networks require the use of several protocols.
- Each protocol has its own function and format.



Protocol	Function
Hypertext Transfer Protocol (HTTP)	▪ Governs the way a web server and a web client interact ▪ Defines content and format
Transmission Control Protocol (TCP)	▪ Manages the individual conversations ▪ Provides guaranteed delivery ▪ Manages flow control
Internet Protocol (IP)	Delivers messages globally from the sender to the receiver
Ethernet	Delivers messages from one NIC to another NIC on the same Ethernet Local Area Network (LAN)

1.2.3 Two layered models in network operations



1.2.3 Two layered models in network operations

1. OSI Reference Model

- The OSI (Open System Interconnection) model is developed by ISO in 1984.
- Why OSI? as a guidelines how network operating systems communicate on a network.
- OSI model was to provide a set of design standards for equipment manufacturers.

A good way to remember the seven layers is :

All

People

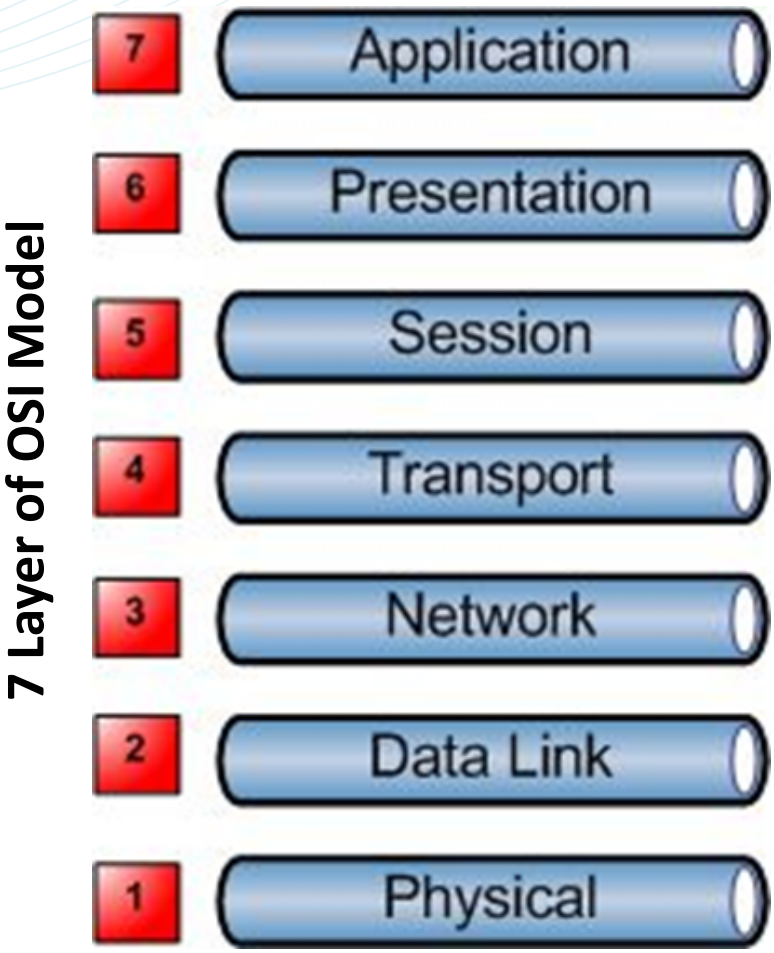
Seem

To

Need

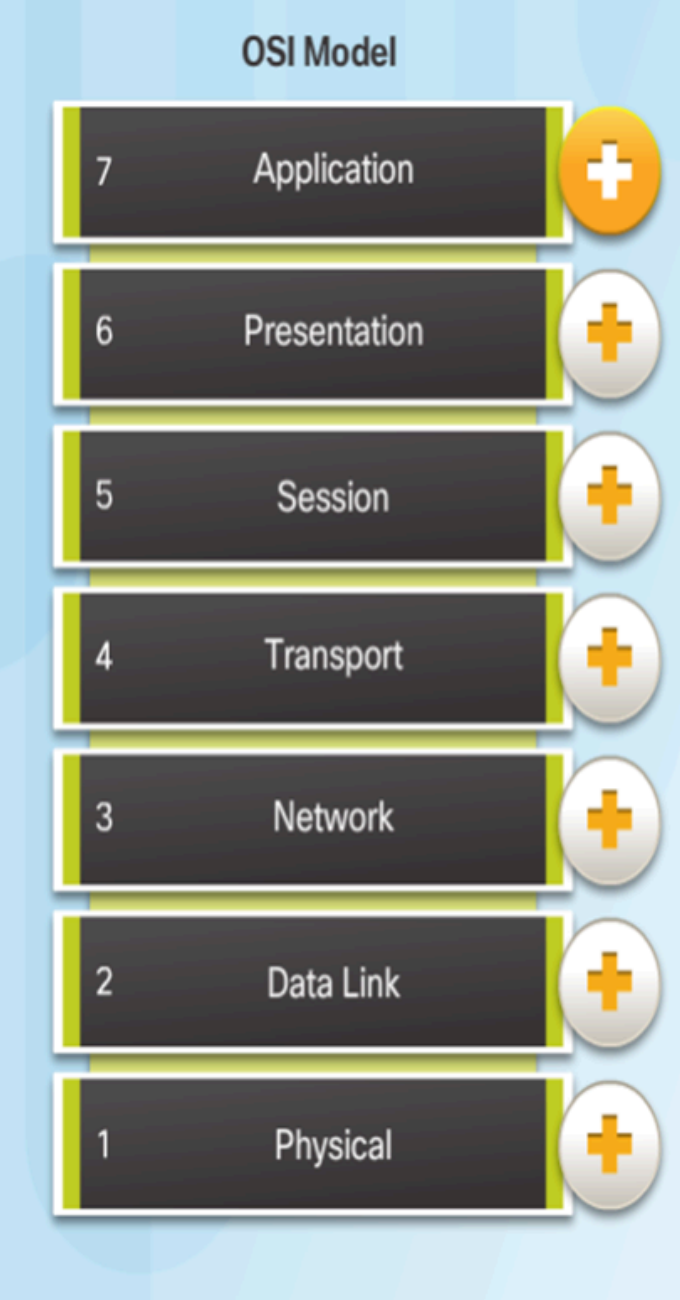
Data

Processing



1.2.3 Two layered models in network operations

1. OSI Reference Model



Application - contains protocols used for process-to-process communications.

Presentation - provides for common representation of the data.

Session - provides services to the presentation layer to organize its dialogue and to manage data exchange.

Transport - defines services to segment, transfer, and reassemble the data.

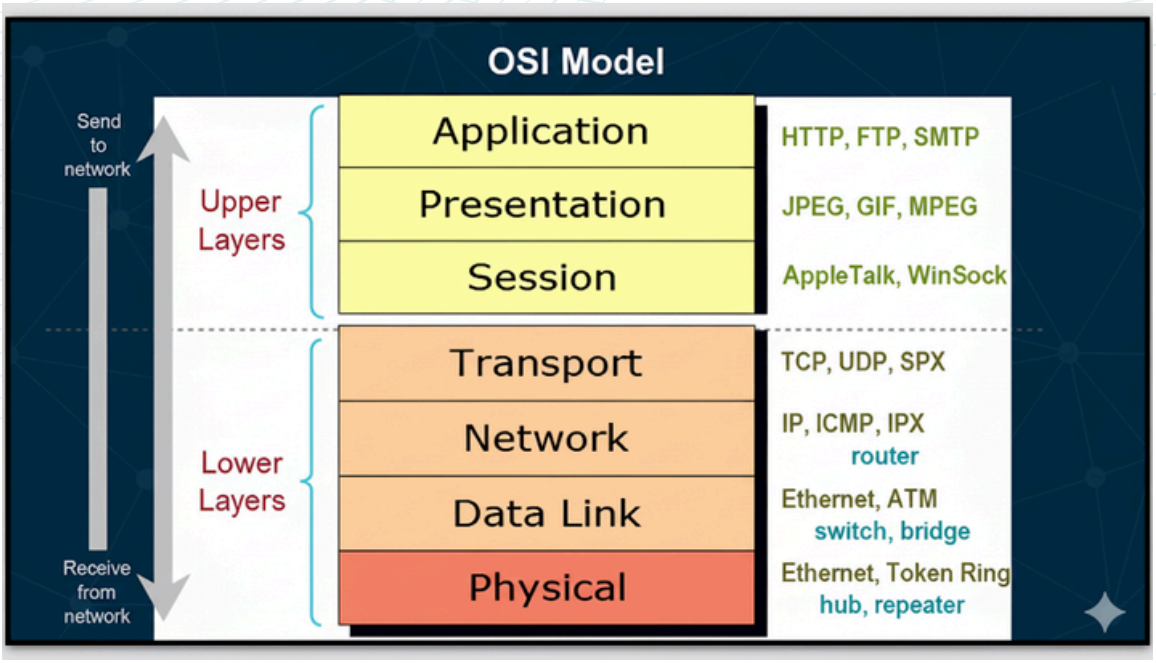
Network - provides services to exchange the individual pieces of data over the network between identified end devices.

Data Link - provides methods for exchanging data frames between devices over a common media.

Physical - describes the mechanical, electrical, functional, and procedural means to transmit bits across physical connections.

1.2.3 Two layered models in network operations

1. OSI Reference Model



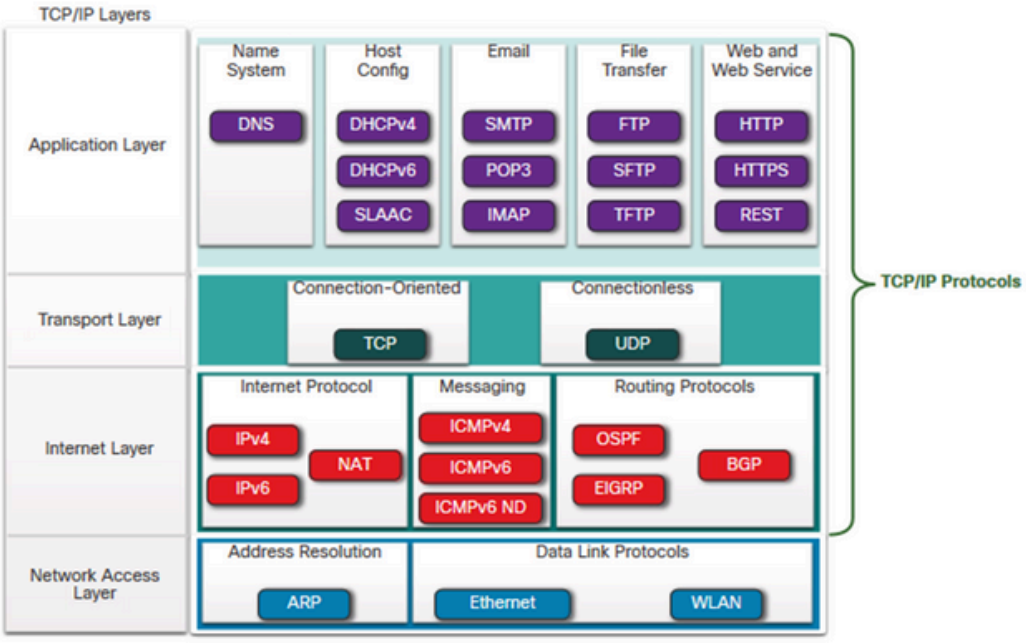
The OSI model defines the communications process into 7 layers, which divides the tasks involved with moving information between networked computers into seven smaller, more manageable task groups.

1.2.3 Two layered models in network operations

2. TCP/IP Protocol Model

- Created in the early 1970s for internetwork communications.
- Open Standard.
- Also called The TCP/IP Model or the Internet Model.
- **Application** - Represents data to the user, plus encoding and dialog control.
- **Transport** - Supports communication between various devices across diverse networks.
- **Internet** – Determines the best path through the network.
- **Network Access** - Controls the hardware devices and media that make up the network.

The TCP/IP Protocol Suites



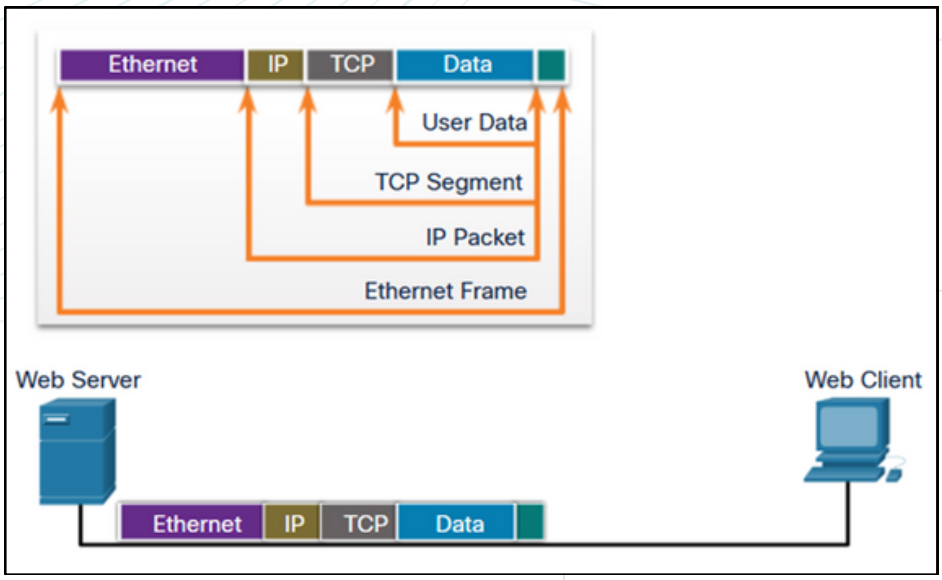
- TCP/IP is the protocol suite used by the internet and includes many protocols.

- TCP/IP is: An open standard protocol suite that is freely available to the public and can be used by any vendor A standards-based protocol suite that is endorsed by the networking industry and approved by a standards organization to ensure interoperability

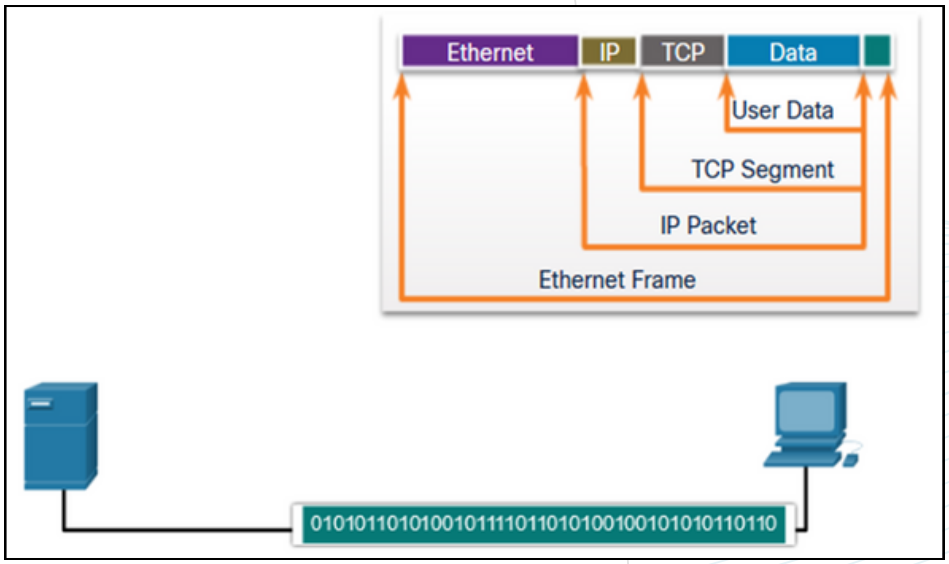
1.2.3 Two layered models in network operations

2. TCP/IP Protocol Model

TCP/IP Communication Process



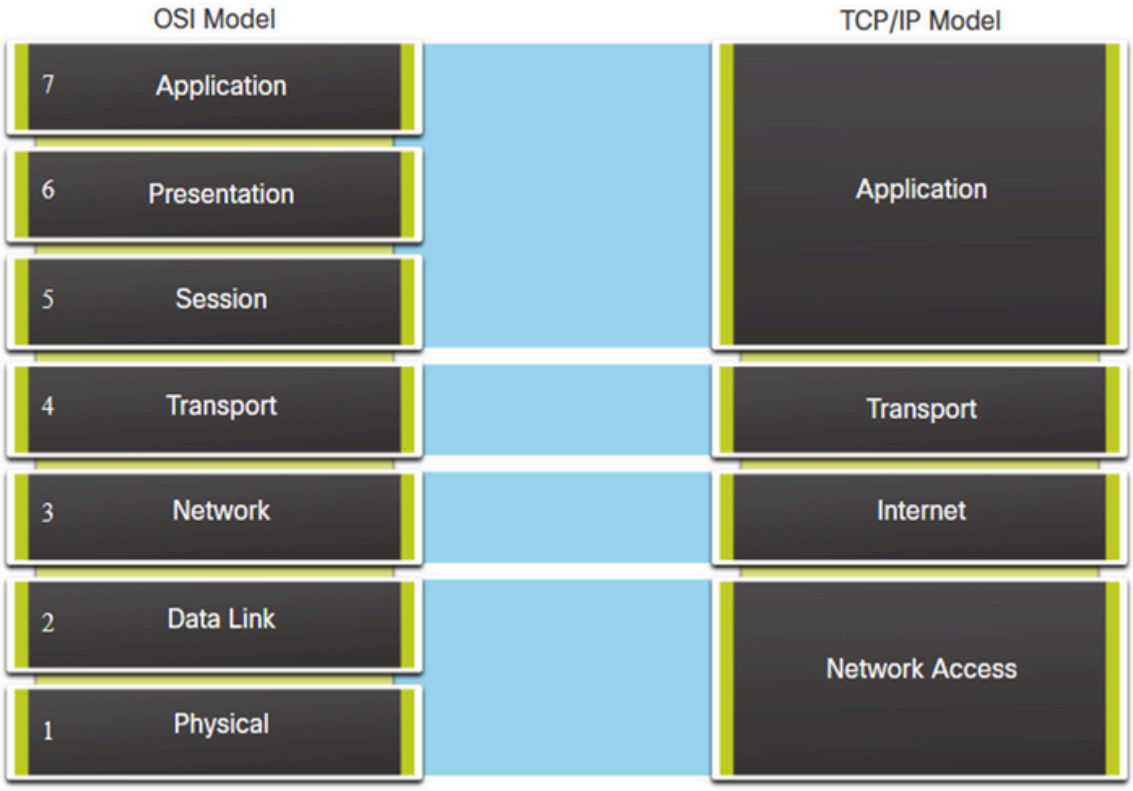
A web server encapsulating and sending a web page to a client.



A client de-encapsulating the web page for the web browser

1.2.3 Two layered models in network operations

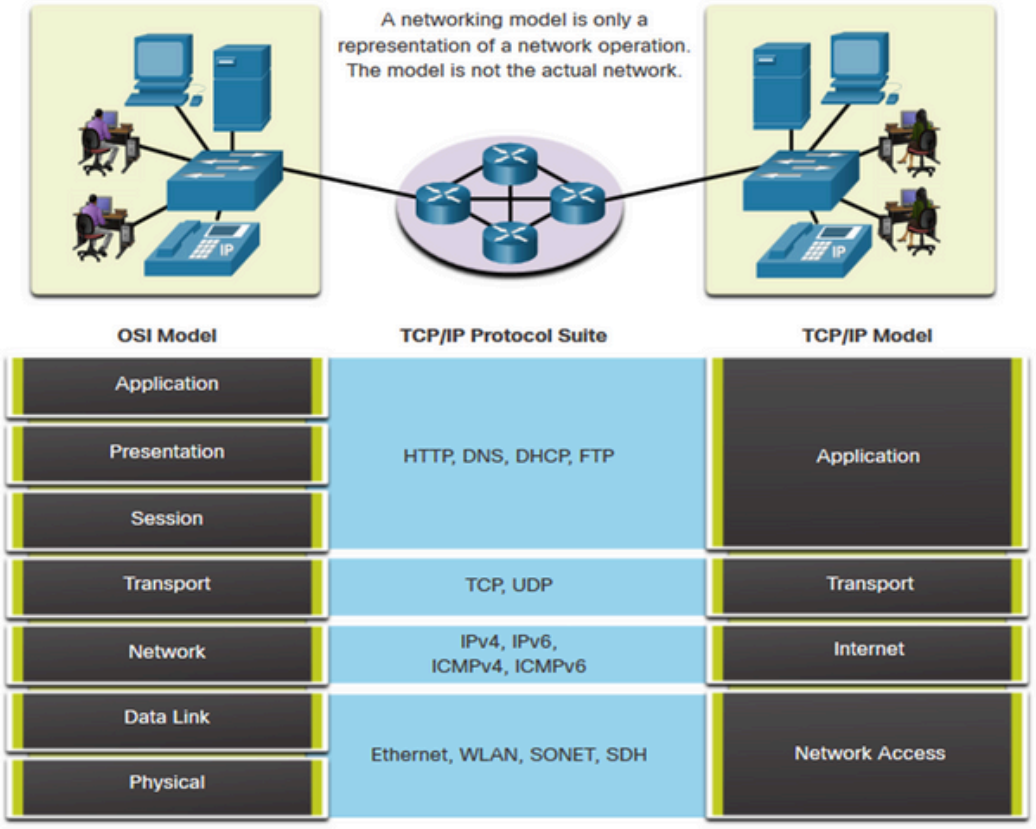
OSI and TCP/IP Model Comparison



- The OSI model divides the network access layer and the application layer of the TCP/IP model into multiple layers.
- The TCP/IP protocol suite does not specify which protocols to use when transmitting over a physical medium.
- OSI Layers 1 and 2 discuss the necessary procedures to access the media and the physical means to send data over a network.

1.2.3 Two layered models in network operations

Benefits of Using Layered Model



These are the benefits of using a layered model:

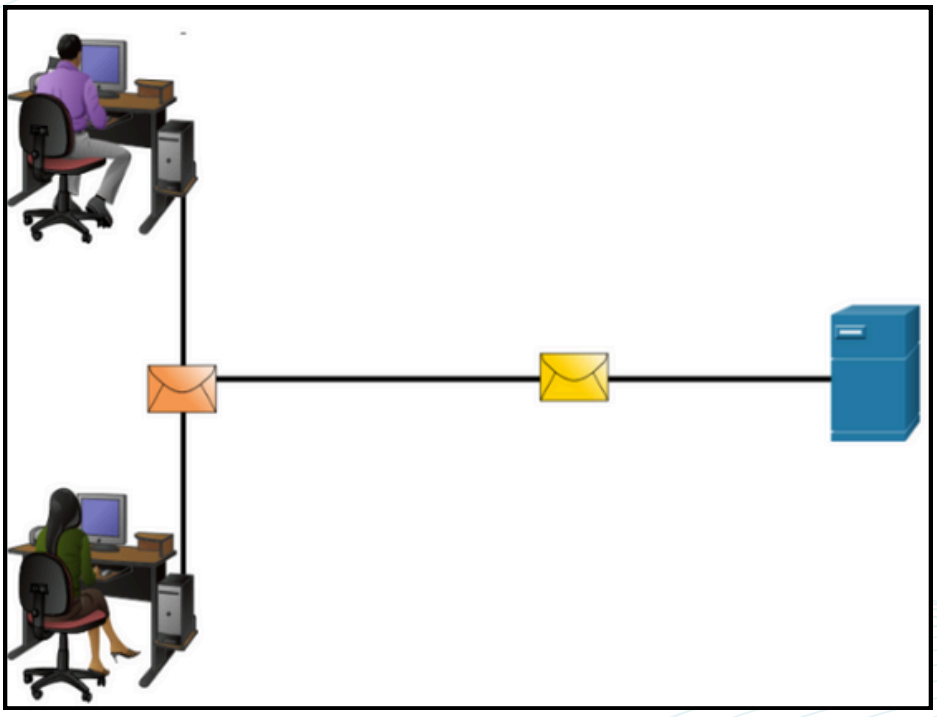
- Assist in protocol design because protocols that operate at a specific layer have defined information that they act upon and a defined interface to the layers above and below
- Foster competition because products from different vendors can work together
- Prevent technology or capability changes in one layer from affecting other layers above and below
- Provide a common language to describe networking functions and capabilities

1.2.4 The encapsulation and de-encapsulation process

Data Encapsulation – Segmenting Messages

Segmenting is the process of breaking up messages into smaller units. Multiplexing is the processes of taking multiple streams of segmented data and interleaving them together. Segmenting messages has two primary benefits:

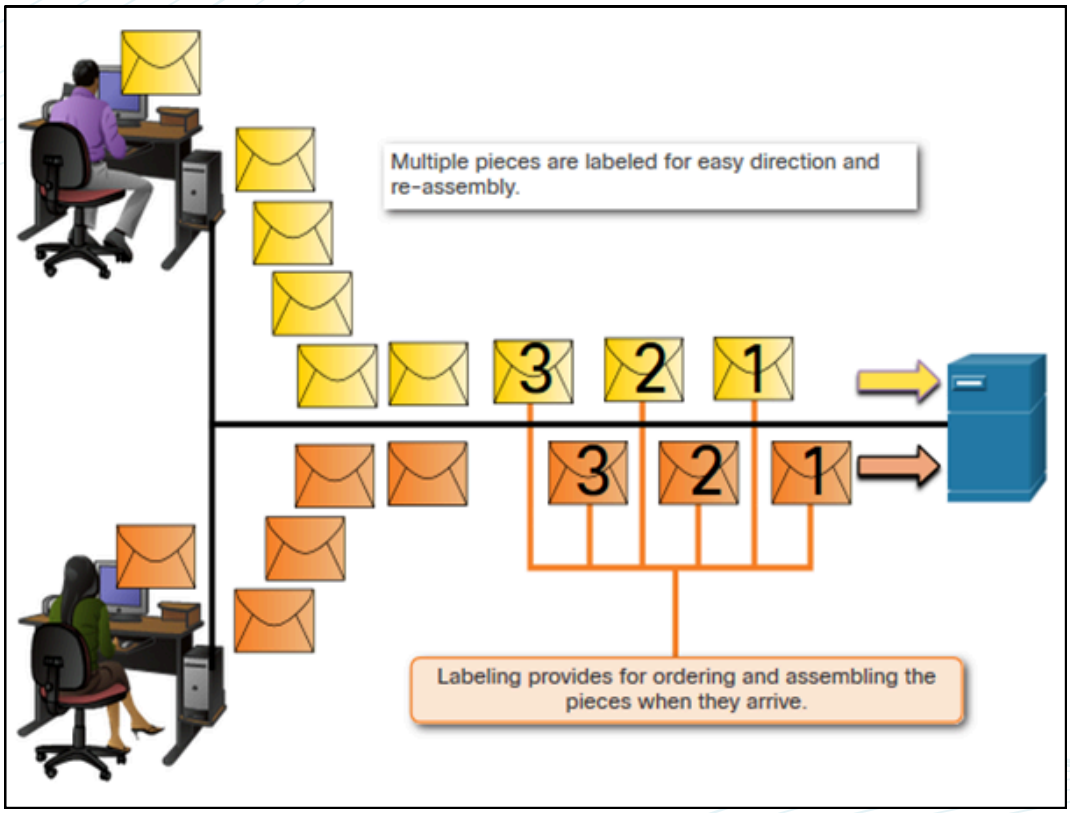
- Increases speed - Large amounts of data can be sent over the network without tying up a communications link.
- Increases efficiency - Only segments which fail to reach the destination need to be retransmitted, not the entire data stream.



1.2.4 The encapsulation and de-encapsulation process

Data Encapsulation – Sequencing

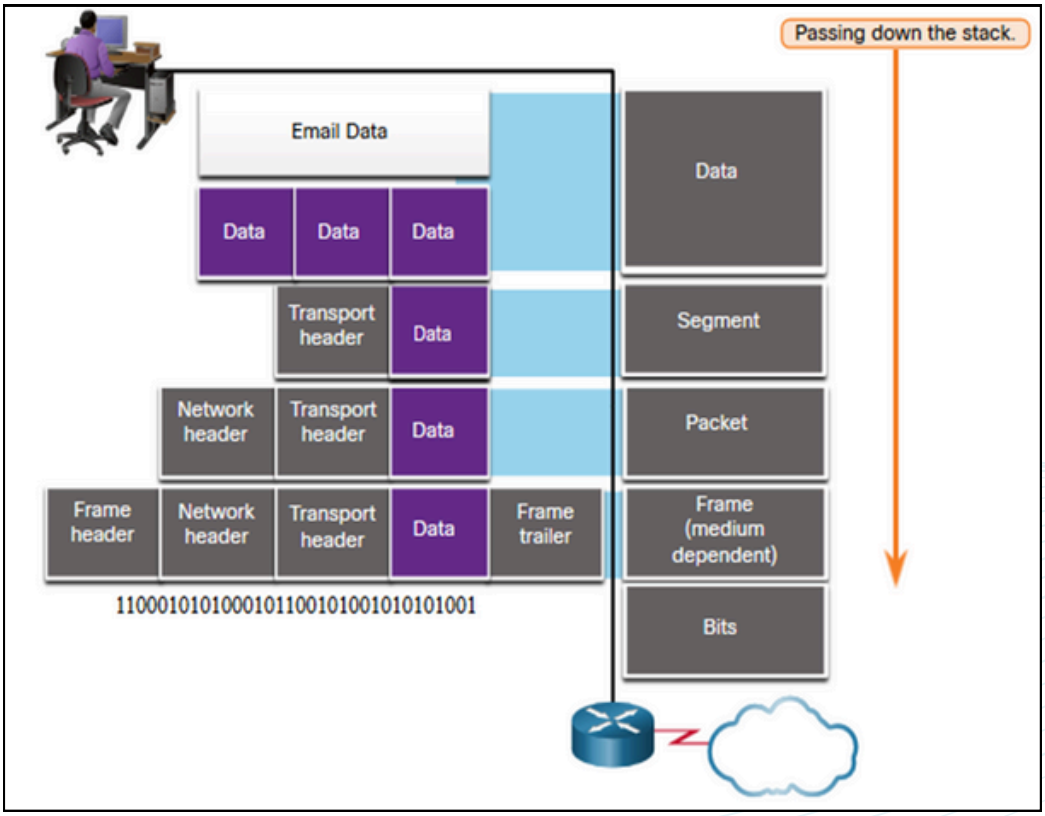
- Sequencing messages is the process of numbering the segments so that the message may be reassembled at the destination.
- TCP is responsible for sequencing the individual segments.



1.2.4 The encapsulation and de-encapsulation process

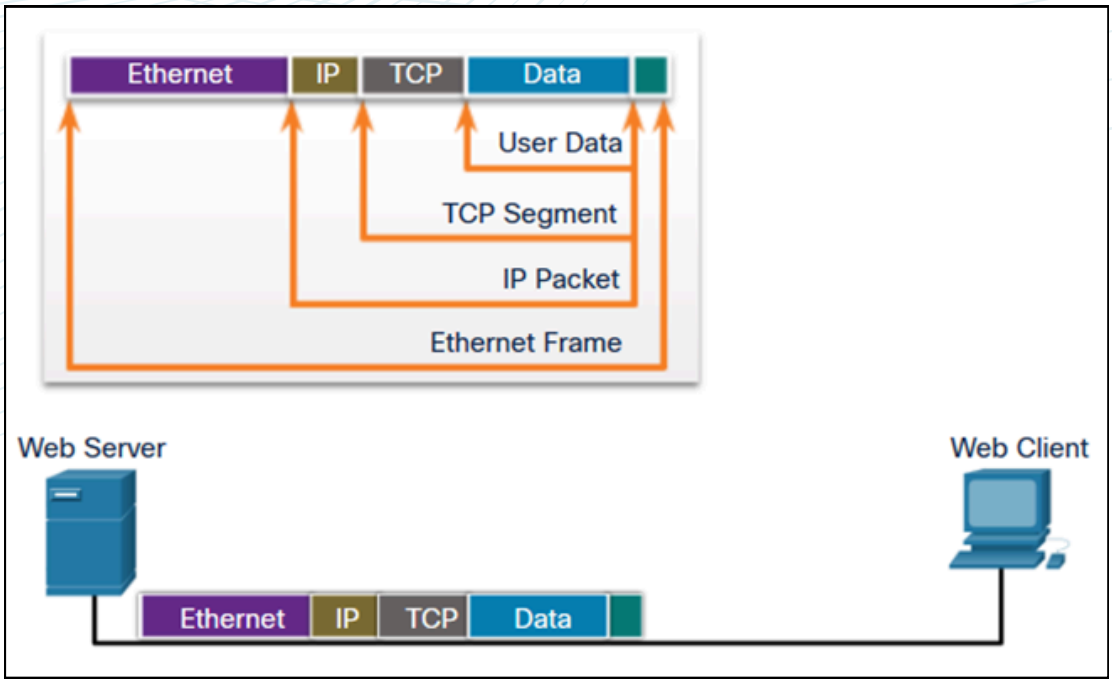
Data Encapsulation – Protocol Data Unit (PDU)

- Encapsulation is the process where protocols add their information to the data.
- At each stage of the process, a PDU has a different name to reflect its new functions.
- There is no universal naming convention for PDUs, in this course, the PDUs are named according to the protocols of the TCP/IP suite.
- PDUs passing down the stack are as follows:
  - Data (Data Stream)
  - Segment
  - Packet
  - Frame
  - Bits (Bit Stream)



1.2.4 The encapsulation and de-encapsulation process

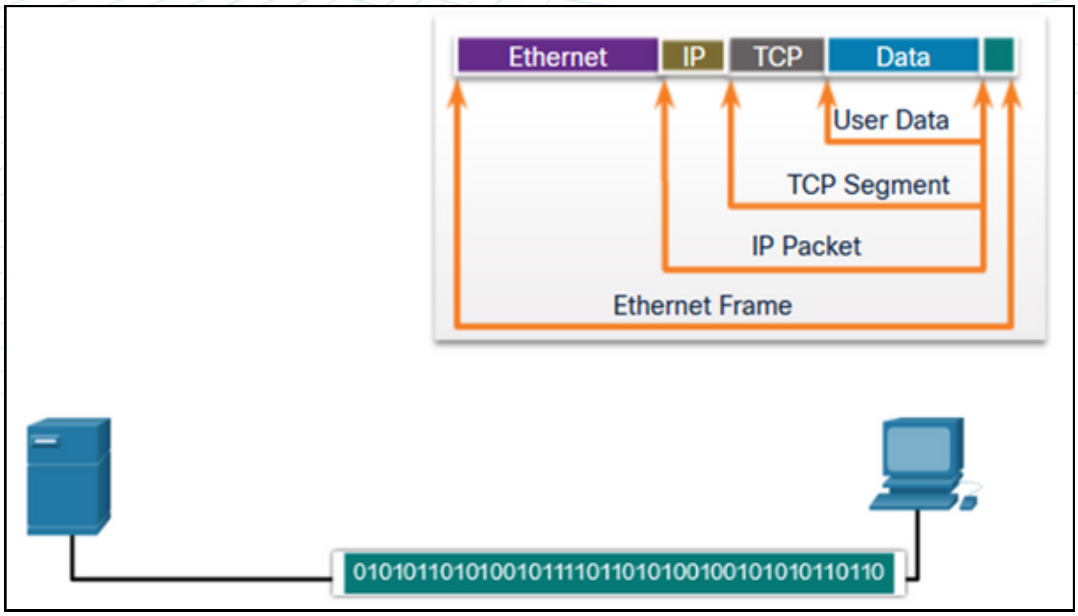
Encapsulation Example



- Encapsulation is a top down process.
- The level above does its process and then passes it down to the next level of the model. This process is repeated by each layer until it is sent out as a bit stream.

1.2.4 The encapsulation and de-encapsulation process

De-Encapsulation Example



- Data is de-encapsulated as it moves up the stack.
- When a layer completes its process, that layer strips off its header and passes it up to the next level to be processed. This is repeated at each layer until it is a data stream that the application can process.
    - 1.Received as Bits (Bit Stream)
    - 2.Frame
    - 3.Packet
    - 4.Segment
    - 5.Data (Data Stream)

02
NETWORK ACCESS

2.1.1 Physical Layer Characteristics

- The Physical Layer is the first layer of the OSI model. It is responsible for transmitting raw bits (0s and 1s) over a physical medium (such as cables, wireless, fiber). It defines the mechanical, electrical, functional, and procedural means to activate and maintain the physical connection between devices. Key functions:
- Convert digital data into signals (electrical, optical, or radio).
- Define physical media (cables, connectors, wireless frequency).
- Specify data rate, voltage levels, and timing.

a. Physical Layer Standards Organizations

Organizations that define and maintain physical layer standards:

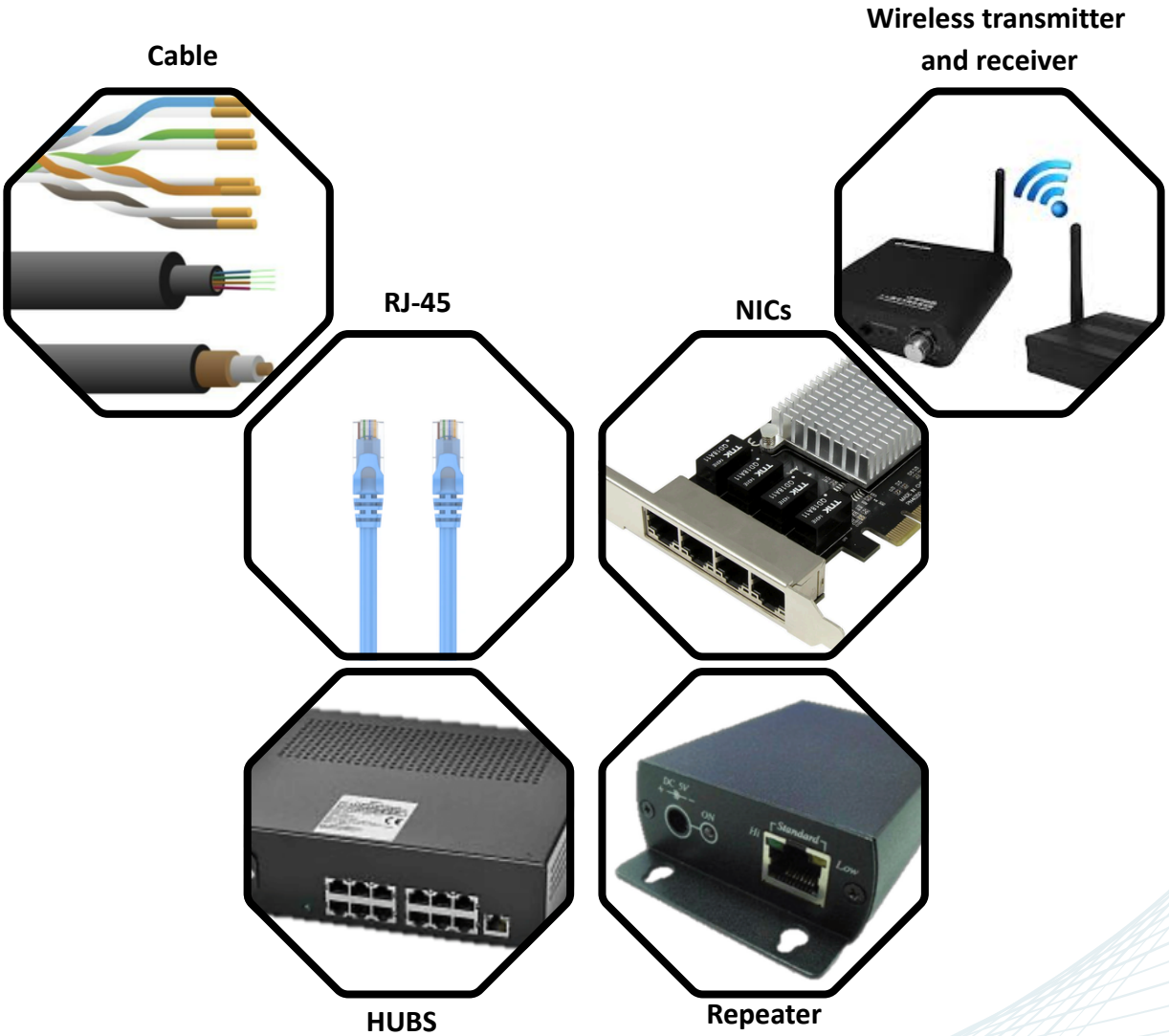
- **IEEE (Institute of Electrical and Electronics Engineers)**
  e.g., IEEE 802.3 for Ethernet, IEEE 802.11 for Wi-Fi.
- **TIA/EIA (Telecommunications Industry Association / Electronic Industries Alliance)**
  Defines cable standards like TIA/EIA-568 (structured cabling).
- **ITU (International Telecommunication Union)**
  Sets global telecommunication standards.
- **ISO (International Organization for Standardization)**
  Developed the OSI model, helps in standardizing data exchange.

2.1.1 Physical Layer Characteristics

b. Physical Components

The physical layer involves hardware elements, such as:

- Cables (UTP, STP, coaxial, fiber optic)
- Connectors (RJ-45, fiber connectors)
- Hubs, Repeaters (amplify signals)
- Network Interface Cards (NICs)
- Wireless transmitters and receivers



2.1.1 Physical Layer Characteristics

c. Encoding

Encoding is the process of converting digital data into signals for transmission.

- **Common Encoding Methods:**
  - NRZ (Non-Return to Zero)
  - Manchester Encoding (used in Ethernet)
  - 4B/5B Encoding
- **Purpose:** To ensure synchronization between sender and receiver and improve error detection.

d. Signalling

Signalling refers to how data is represented on the medium:

- **Analog Signals:** Continuous waveforms
- **Digital Signals**: Discrete 0s and 1s
- **Baseband Transmission:** Uses the entire bandwidth for one signal (Ethernet)
- **Broadband Transmission:** Uses frequency division for multiple signals

e. Bandwidth

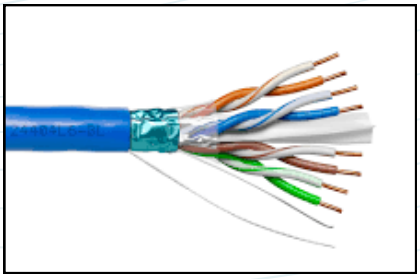
Bandwidth Terminology

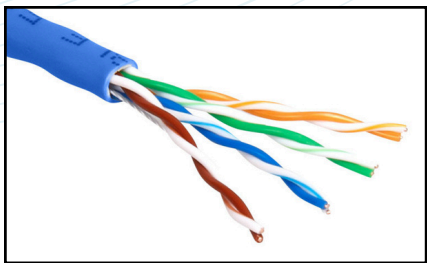
- **Bandwidth:** The maximum rate of data transfer over a network path, measured in bits per second (bps).
- **Throughput:** Actual data transfer rate achieved.
- **Goodput:** Useful data delivered excluding overhead.
- **Latency:** Time taken for data to travel from source to destination.
- **Data Rate:** Number of bits transmitted per second.

2.2.1 The Characteristics of Network Cabling

a. STP (Shielded Twisted Pair) Cable

- Contains twisted wire pairs with shielding (foil or braided).
- Reduces electromagnetic interference (EMI) and crosstalk.
- More expensive and harder to install than UTP.
- Used in environments with high interference (e.g., factories).



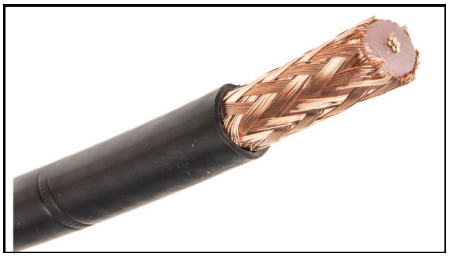


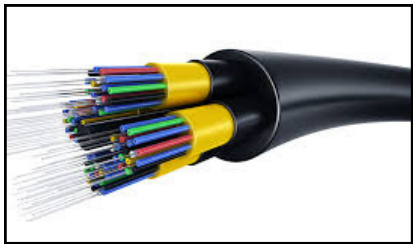
b. UTP (Unshielded Twisted Pair) Cable

- Most commonly used for LANs (Ethernet).
- Consists of 4 pairs of twisted wires without extra shielding.
- Easy to install, lightweight, and cost-effective.
- Susceptible to EMI compared to STP.

c. Coaxial Cable

- Core conductor surrounded by insulation, metallic shield, and outer jacket.
- Used in cable TV, older Ethernet (10Base2, 10Base5).
- Good resistance to EMI, better than UTP.
- Bulkier and less flexible than UTP.

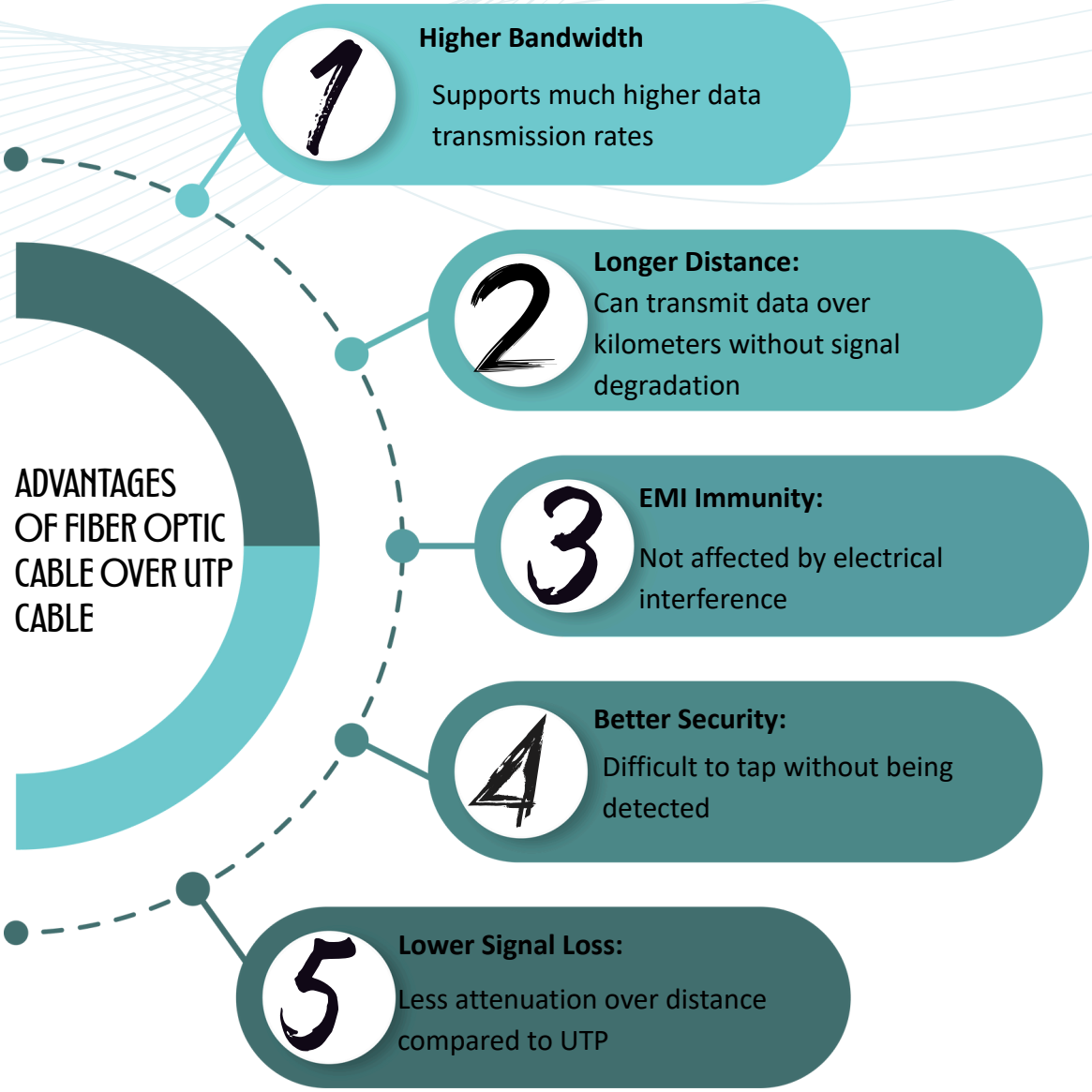




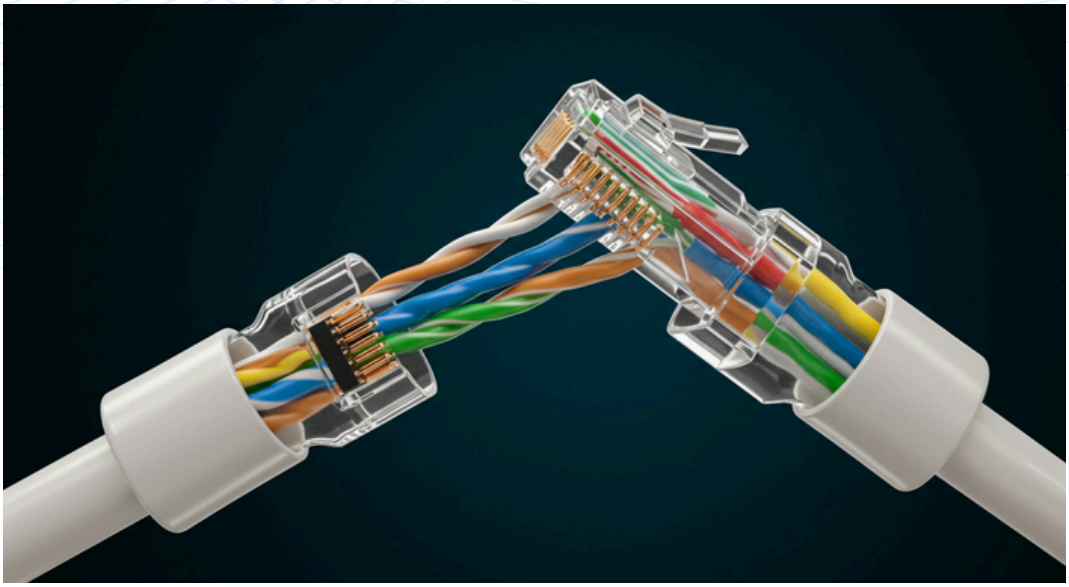
d. Fiber Optic Cable

- Uses light signals through glass or plastic fibers.
- Immune to EMI, supports long distances and very high data rates.
- Expensive and fragile; requires special tools for installation.
- Types: Single-mode (long distance), Multimode (shorter distance).

2.2.2 The Advantages of Fiber Optic Cable over UTP Cable

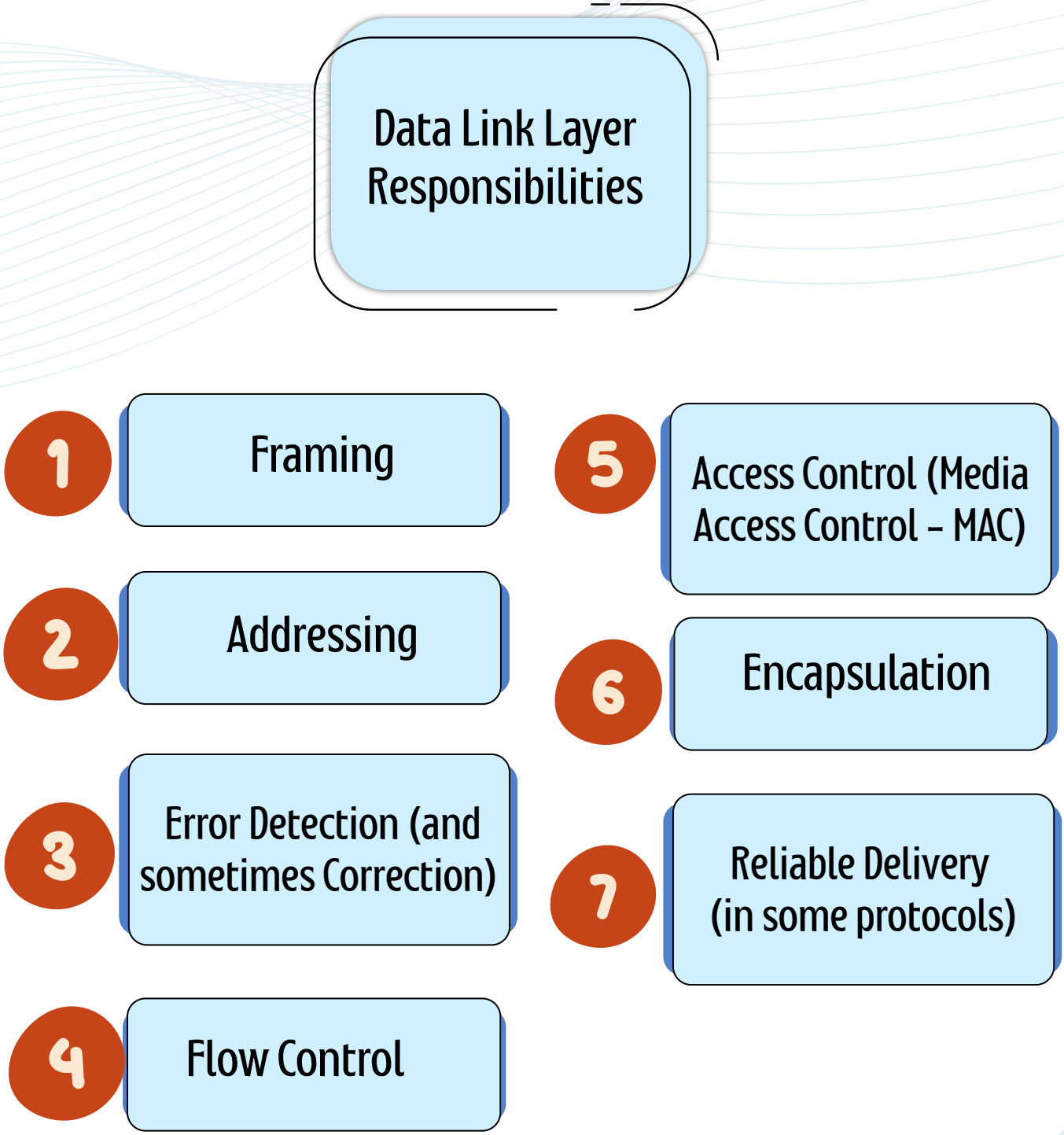


2.2.3 Build a UTP Cable used in Ethernet Network



Video : How to build a UTP Cable

2.3.1 The Data Link Layer Responsibilities



2.3.1 The Data Link Layer Responsibilities

1. Framing

- Divides the stream of bits received from the network layer into frames (structured packets with headers and trailers).
- Adds headers (such as source and destination MAC addresses) and trailers (error-checking information like CRC).
- Helps the receiver to identify frame boundaries.

2. Addressing

- Uses physical (MAC) addresses to identify devices on the same network segment.
- Ensures data is delivered to the correct device on a local network**.**

3. Error Detection (and sometimes Correction)

- Uses Cyclic Redundancy Check (CRC) or checksums in the trailer to detect transmission errors.
- Requests retransmission if errors are found (depending on protocol, e.g., LLC).

4. Flow Control

- Prevents a fast sender from overwhelming a slower receiver by controlling data flow.
- Uses methods like acknowledgments and pause frames.

5. Access Control (Media Access Control - MAC)

- Determines which device can use the network channel when multiple devices are connected (e.g., Ethernet).
- Implements protocols like CSMA/CD (Ethernet) or CSMA/CA (Wi-Fi).

6. Encapsulation

- Encapsulates network layer packets (IP packets) into frames before transmission.
- Adds the MAC header and trailer to create a complete data link layer frame.

7. Reliable Delivery (in some protocols)

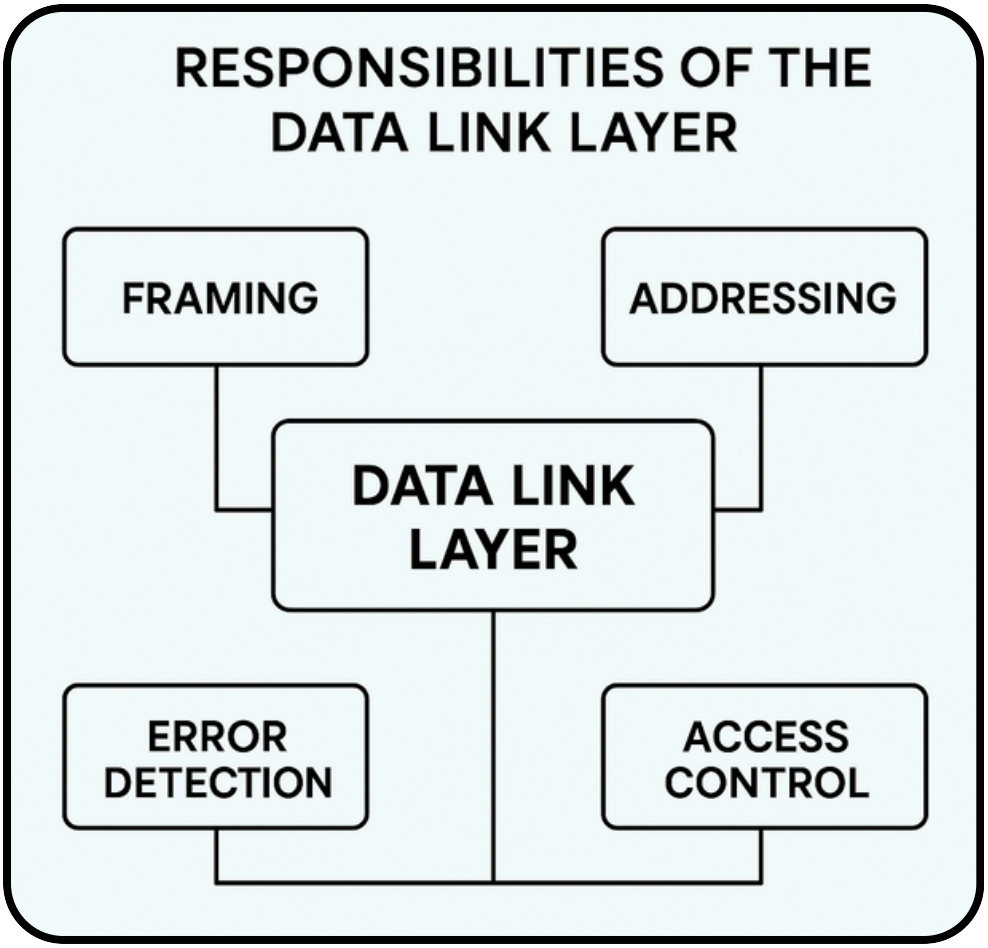
- Provides acknowledgment and retransmission mechanisms (e.g., in Point-to-Point Protocol - PPP).
- Ensures frames arrive in the correct order.

2.3.1 The Data Link Layer Responsibilities

Sub-layers of Data Link Layer

The data link layer is divided into two sub-layers:

- **Logical Link Control (LLC) -** Handles error checking, flow control, and multiplexing.
- **Media Access Control (MAC) -** Manages access to the physical medium and defines hardware addressing (MAC addresses).



2.3.2 The Data Link Layer Standard Organizations

The Data Link Layer standards are developed and maintained by several well-known organizations to ensure interoperability and compatibility across devices and networks.
Key Standard Organizations:

1. Institute of Electrical and Electronics Engineers (IEEE)

- Responsible for defining LAN and MAN standards.
- The IEEE 802 committee defines various data link layer protocols:
  - IEEE 802.3 – Ethernet (wired LANs)
  - IEEE 802.11 – Wi-Fi (wireless LANs)
  - IEEE 802.5 – Token Ring
  - IEEE 802.15 – Wireless Personal Area Networks (WPANs, e.g., Bluetooth)

2. International Organization for Standardization (ISO)

- Defines High-Level Data Link Control (HDLC) and other data communication standards.
- HDLC is widely used for point-to-point and multipoint connections.

3. International Telecommunication Union (ITU-T)

- Develops standards for telecommunications, including the data link protocols such as:
  - LAPB (Link Access Procedure, Balanced)
  - LAPD (Link Access Procedure for D-channel)

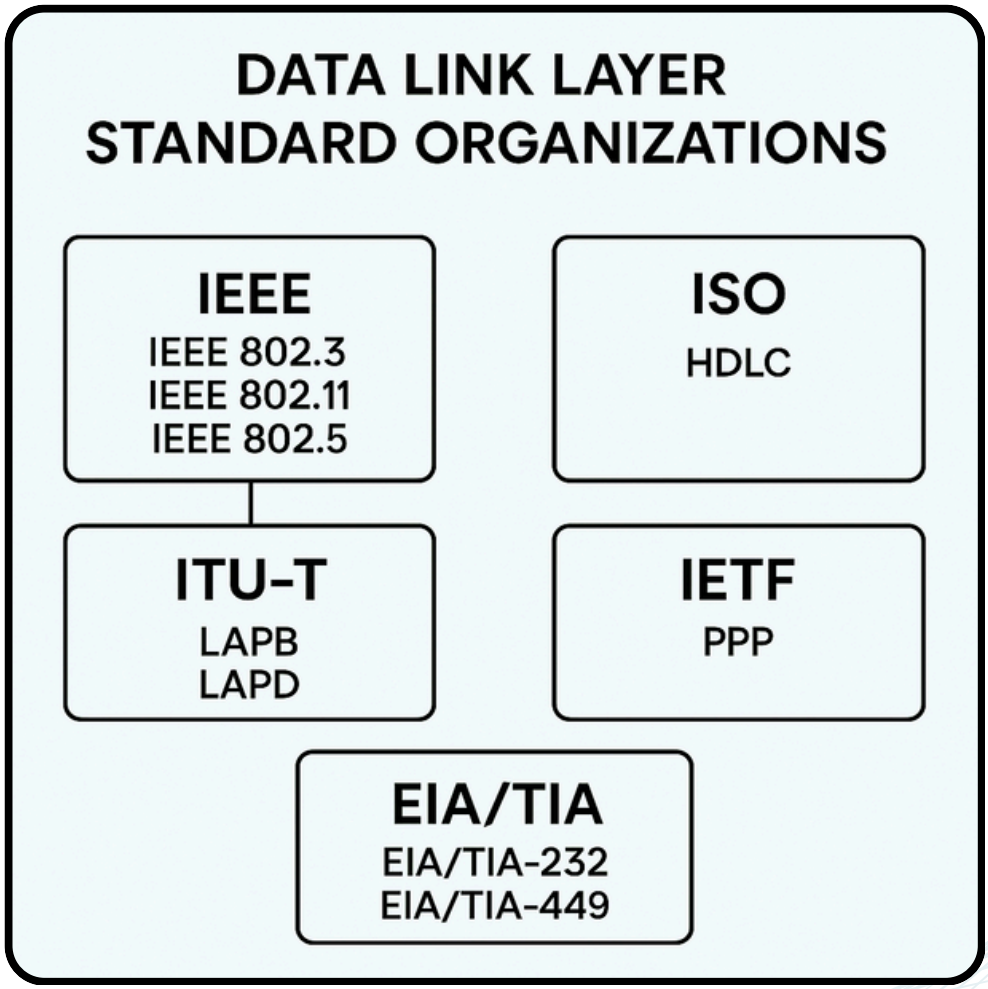
2.3.2 The Data Link Layer Standard Organizations

4. Internet Engineering Task Force (IETF)

- Defines protocols used in networking, including those operating at the data link layer (e.g., PPP – Point-to-Point Protocol).

5. Electronic Industries Alliance (EIA) & Telecommunications Industry Association (TIA)

- Define physical and data link layer standards for serial communication (e.g., EIA/TIA-232, EIA/TIA-449).



2.3.2 The Data Link Layer Standard Organizations

A network topology describes how devices are arranged and how data flows within a network. Topologies are classified into physical and logical types, which serve different purposes.

Physical Topology

Definition: Refers to the actual physical layout of devices, cables, and network components.

Focus: How the devices (computers, switches, routers) are physically connected.

Examples:

- Bus Topology – All devices connected to a single backbone cable.
- Star Topology – All devices connected to a central hub or switch.
- Ring Topology – Devices connected in a circular path.
- Mesh Topology – Each device is connected to every other device.

Key Characteristics:

- Affects the installation cost and troubleshooting.
- Involves physical hardware like cables and connectors.

Logical Topology

Definition: Refers to the way data flows across the network, regardless of the physical design.

Focus: Path taken by data packets and how devices communicate.

Examples:

- Logical Bus – Data is transmitted to all devices, but only the intended recipient accepts it (e.g., Ethernet).
- Logical Ring – Data travels in a circular pattern, even if the physical layout is a star (e.g., FDDI or Token Ring).

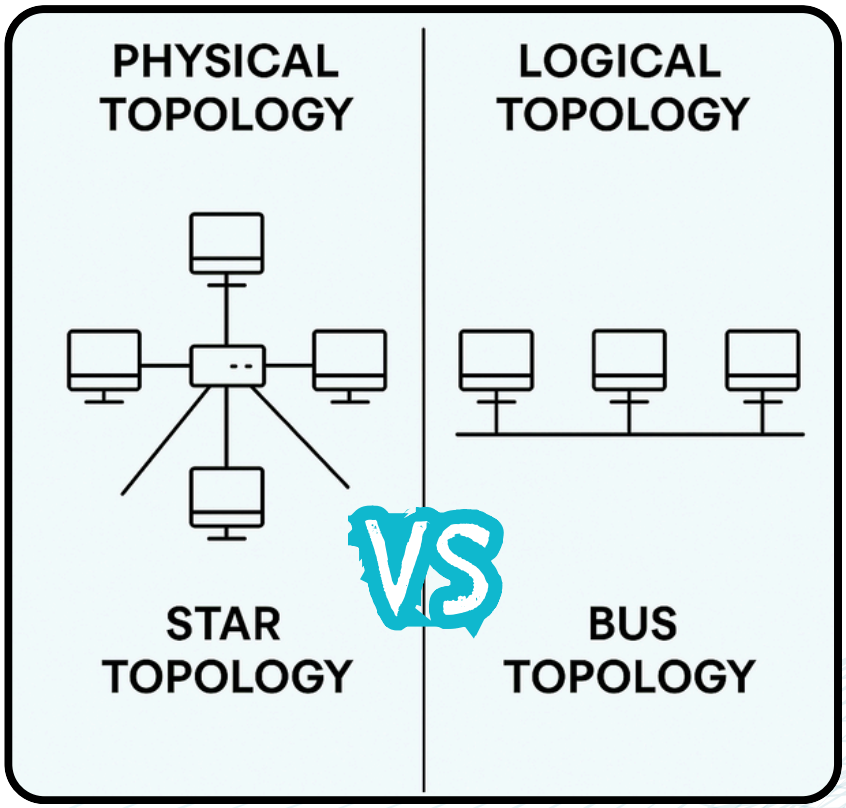
Key Characteristics:

- Determined by network protocols (e.g., Ethernet, Token Ring).
- Does not depend on the physical cabling layout.

2.3.3 Differentiate Physical and Logical Topologies

Comparison Table

Aspect	Physical Topology	Logical Topology
Definition	Physical layout of devices & cables	Data flow pattern across the network
Focus	Hardware arrangement	Transmission of data
Determined by	Network hardware setup	Network protocols
Examples	Bus, Star, Ring, Mesh	Logical Bus, Logical Ring
Changes	Requires rearranging cables	Can change by reconfiguring software



2.3.4 Differentiate LAN and WAN topologies

LAN (Local Area Network) and WAN (Wide Area Network) topologies describe the structure of networks but differ in scope, size, and technologies used

LAN

Definition: A LAN topology refers to how devices are physically and logically arranged within a local network, typically covering a small area (e.g., home, office, campus).

Common LAN Topologies:

- **Bus Topology** – All devices share a single backbone cable.
- **Star Topology** – Devices connect to a central hub/switch.
- **Ring Topology** – Devices form a circular data path.
- **Mesh Topology** – Devices are interconnected for redundancy.

Characteristics:

- High speed (up to Gbps or more).
- Lower cost and easier to maintain compared to WAN.
- Controlled by a single organization.

VS

WAN

Definition: A WAN topology shows how multiple LANs or networks are connected across large geographic areas (e.g., cities, countries, or globally).

Common LAN Topologies:

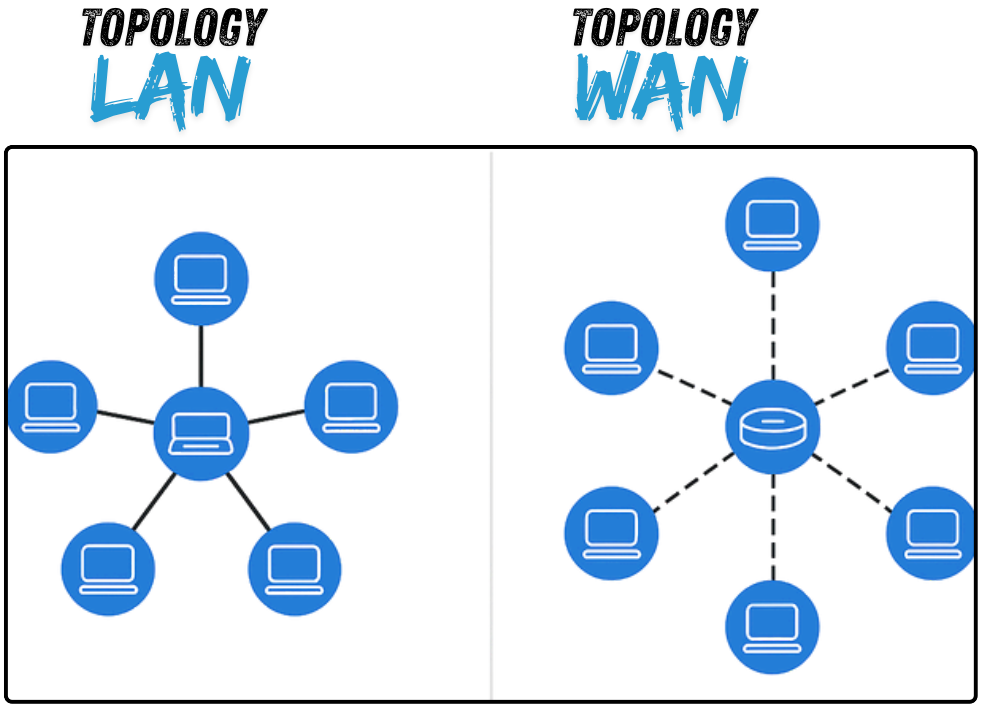
- **Point-to-Point** – A direct link between two sites.
- **Hub-and-Spoke** – Central site connects to multiple branch sites.
- **Full Mesh** – Every site connects to all others.
- **Partial Mesh** – Some sites are directly connected, others via hubs.

Characteristics:

- Lower speed compared to LAN due to long distances.
- Higher cost due to leased lines or carrier infrastructure.
- Uses technologies like MPLS, Frame Relay, or the internet.

2.3.4 Differentiate LAN and WAN topologies

Aspect	LAN Topology	WAN Topology
Coverage Area	Small area (office, campus)	Large area (city, country, global)
Speed	High (100 Mbps – 10 Gbps)	Lower (typically Mbps)
Cost	Lower setup cost	Higher cost (leased lines, ISP)
Management	Single organization controls it	Managed by multiple organizations/ISPs
Examples	Bus, Star, Ring, Mesh	Point-to-Point, Hub-and-Spoke, Full Mesh



LAN AND WAN TOPOLOGY

2.3.5 Half and Full Duplex Communication

In data communication, duplex refers to the direction of data flow between two devices. There are two main modes: Half Duplex and Full Duplex.

Half Duplex

Definition: Data flows in both directions, but only one direction at a time.

Key Points:

- Devices take turns to send or receive data.
- When one device is transmitting, the other must wait.
- Similar to a walkie-talkie system.

Advantages:

- Cost-effective and simpler to implement.
- Reduces interference since only one side transmits at a time.

Disadvantages:

- Slower compared to full duplex due to alternating transmission.

Examples:

- Walkie-talkies
- Older Ethernet (using hubs)
- CB (Citizen Band) radios

Full Duplex

Definition: Data flows in both directions simultaneously.

Key Points:

- Both devices can send and receive data at the same time.
- Similar to a telephone conversation.

Advantages:

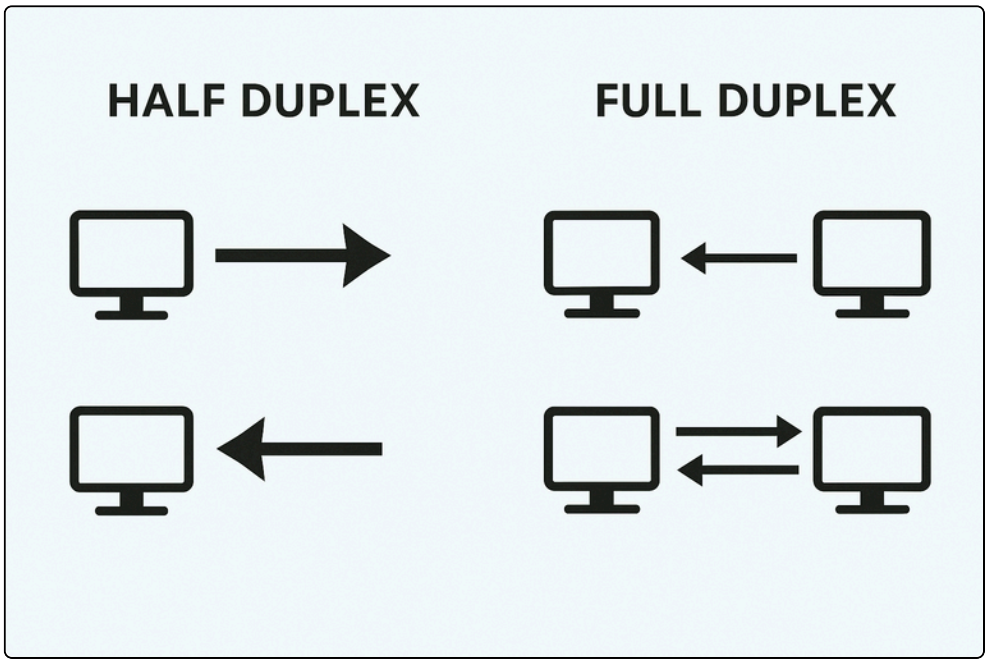
- Faster and more efficient.
- No waiting for turns to transmit.
- Disadvantages:
- More expensive and complex hardware.
- Requires mechanisms to handle simultaneous signals.

Examples:

- Modern Ethernet (with switches)
- Telephones and mobile networks
- Video conferencing

2.3.5 Half and Full Duplex Communication

Aspect	Half Duplex	Full Duplex
Direction	Both ways, but one at a time	Both ways simultaneously
Speed	Slower	Faster
Examples	Walkie-talkie, older Ethernet	Telephones, modern Ethernet
Cost	Cheaper	More expensive hardware



2.4.1 The Roles of the MAC Address and The IP Address

MAC ADD

Definition: A unique hardware address assigned to every network interface card (NIC) by the manufacturer.

Role:

- Functions at the Data Link Layer (Layer 2) of the OSI model.
- Ensures data is delivered to the correct physical device within a local network (LAN).
- Acts like a “house number” on a street (fixed and unique).

Format:

- Usually 48 bits, written in hexadecimal (e.g., 00:1A:2B:3C:4D:5E).

Scope:

- Works only within the same local network segment.

IP ADD

Definition: A logical address assigned to devices in a network to enable identification and communication across networks.

Role:

- Functions at the Network Layer (Layer 3) of the OSI model.
- Ensures data is delivered to the correct network and host.
- Acts like a “postal address” (can change based on network location).

Format:

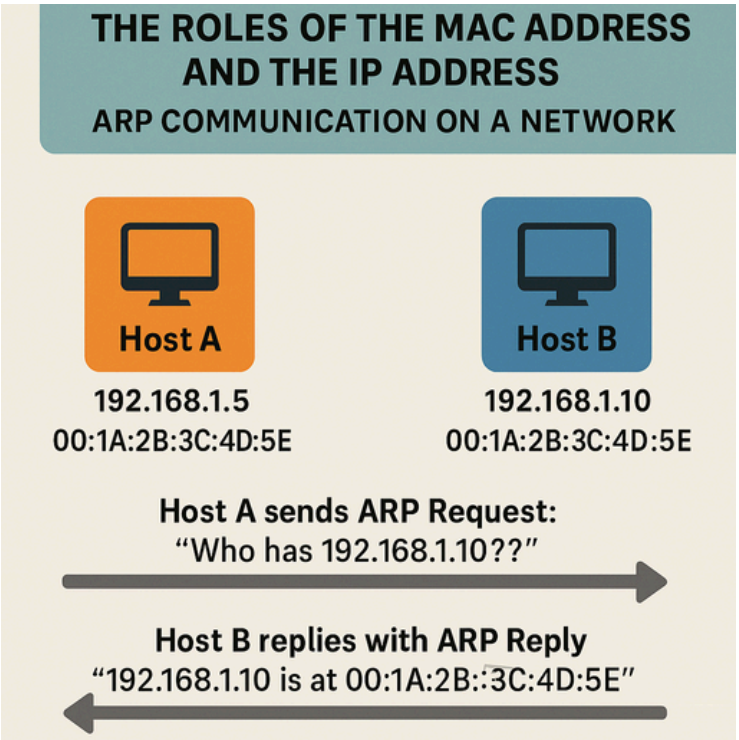
- IPv4 (32 bits, e.g., 192.168.1.10) or IPv6 (128 bits, e.g., 2001:0db8::1).

Scope:

- Used for end-to-end delivery across different networks (LAN/WAN).

2.4.1 The Roles of the MAC Address and The IP Address

Aspect	MAC Address	IP Address
Type	Physical (hardware) address	Logical (software) address
Layer	Data Link Layer (Layer 2)	Network Layer (Layer 3)
Uniqueness	Unique, fixed by manufacturer	Can be changed (static or dynamic)
Scope	Works within a local network (LAN)	Works across networks (LAN/WAN)



2.4.2 The Purpose of ARP

The main purpose of ARP is to map an IP address to a MAC address within a local area network (LAN). This allows devices to communicate on a network when they know the IP address of the destination but need its MAC address to send data at the data link layer (Layer 2 of the OSI model)

Devices communicate using IP addresses at Layer 3 (Network Layer),but data is physically delivered using MAC addresses at Layer 2 (Data Link Layer).
Therefore, there must be a way to translate IP → MAC within the LAN.

ARP in Action

- Host wants to send data to an IP (e.g., 192.168.1.10).
- It checks its ARP cache (a table of known IP-to-MAC mappings).
- If the MAC address is unknown, it sends an ARP Request (broadcast).
- The device with that IP replies with an ARP Reply containing its MAC address.
- The sender stores the result and uses the MAC address to send the data.

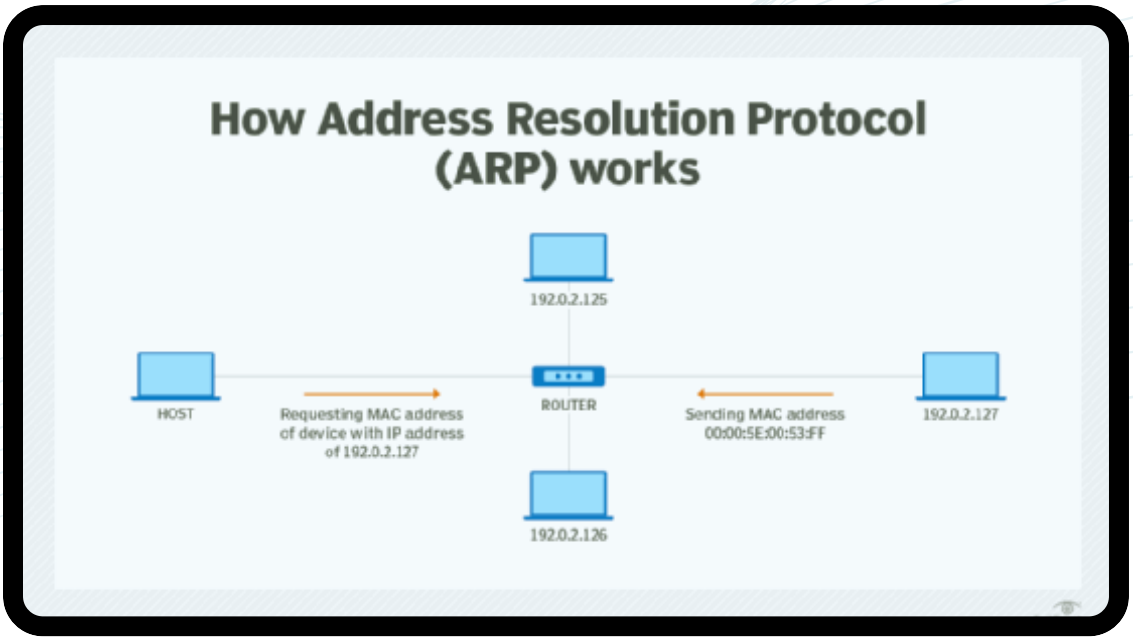
ARP Limitations

Susceptible to spoofing/attacks (e.g., ARP poisoning).
Only works within the same local network segment.

Type	Description
ARP Request	Broadcast query asking “Who has IP X?”
ARP Reply	Unicast response with “IP X is at MAC Y”
Gratuitous ARP	A device announces its own IP-MAC mapping without being asked.
Proxy ARP	A router replies on behalf of another device, useful in certain network configurations.

ARP is essential for enabling communication within a local network by resolving IP addresses to physical MAC addresses.

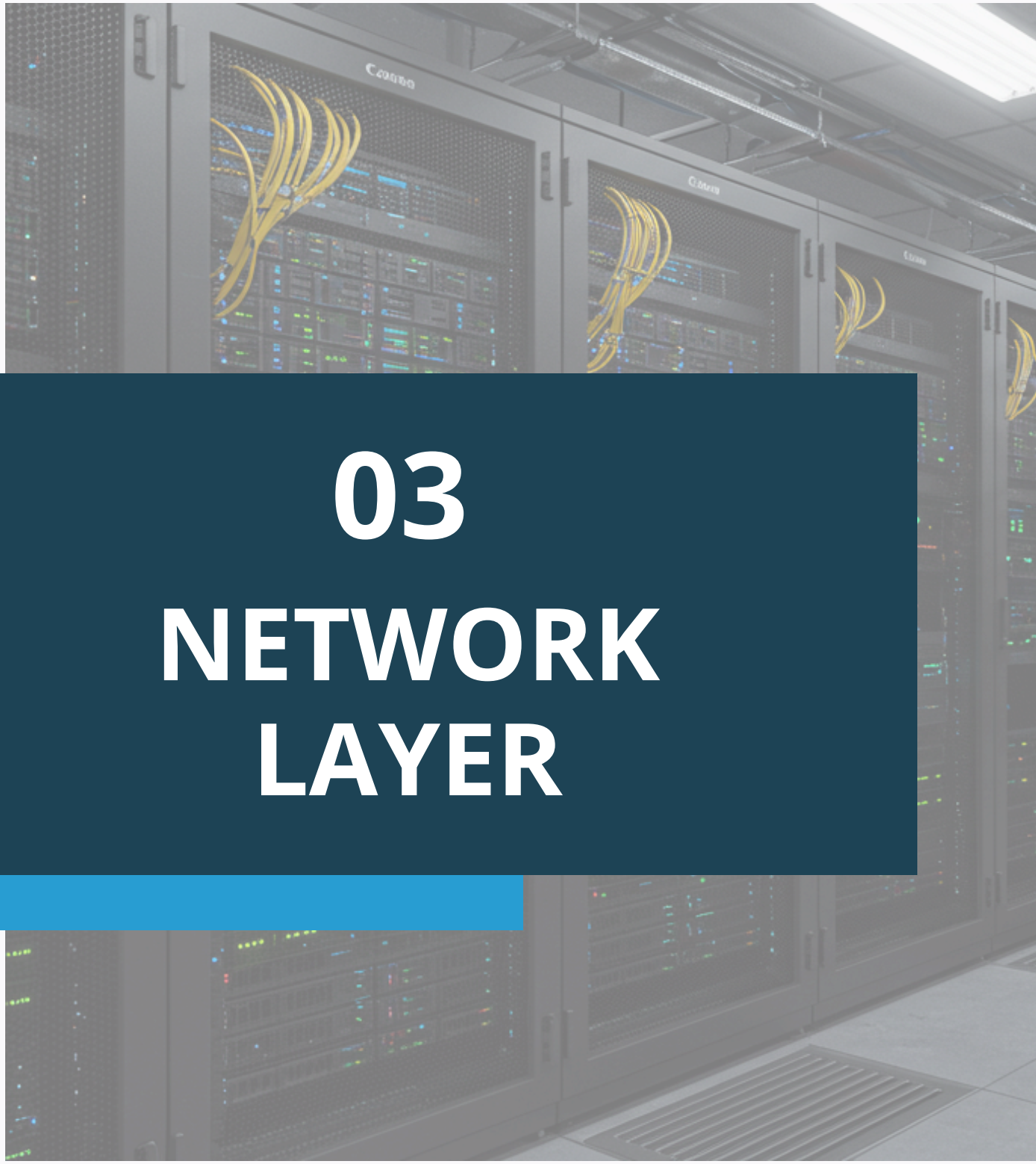
2.4.2 The Purpose of ARP



> ***IP Address:*** *Logical identifier for routing across networks.*

> ***MAC Address:*** *Physical identifier for delivery within a local network*

> ***ARP:*** *The protocol that connects them by mapping IP to MAC.*



03
NETWORK LAYER

3.1.1 The Characteristics of IP Protocol

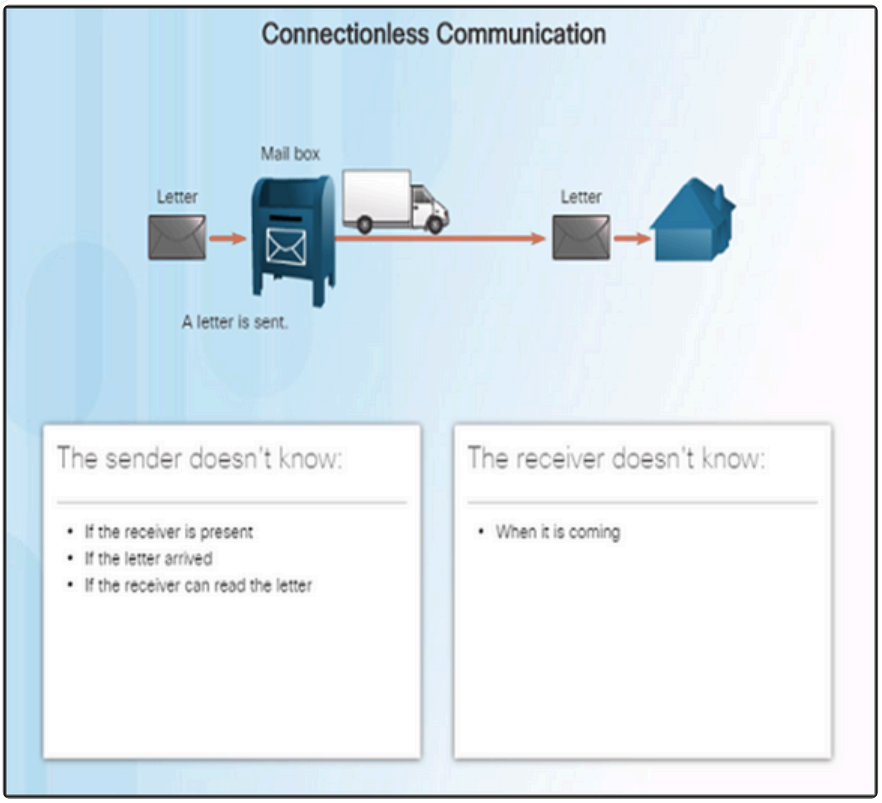
- Connectionless - There is no connection with the destination established before sending data packets.
- Best Effort - IP is inherently unreliable because packet delivery is not guaranteed.
- Media Independent - Operation is independent of the medium (i.e., copper, fiber-optic, or wireless) carrying the data.

Explanation: Internet Protocol (IP) is a network layer protocol that does not require initial exchange of control information to establish an end-to-end connection before packets are forwarded.
Thus, IP is connectionless and does not provide reliable end-to-end delivery by itself. IP is media independent. User data segmentation is a service provided at the transport layer.

3.1.1 The Characteristics of IP Protocol

Connectionless

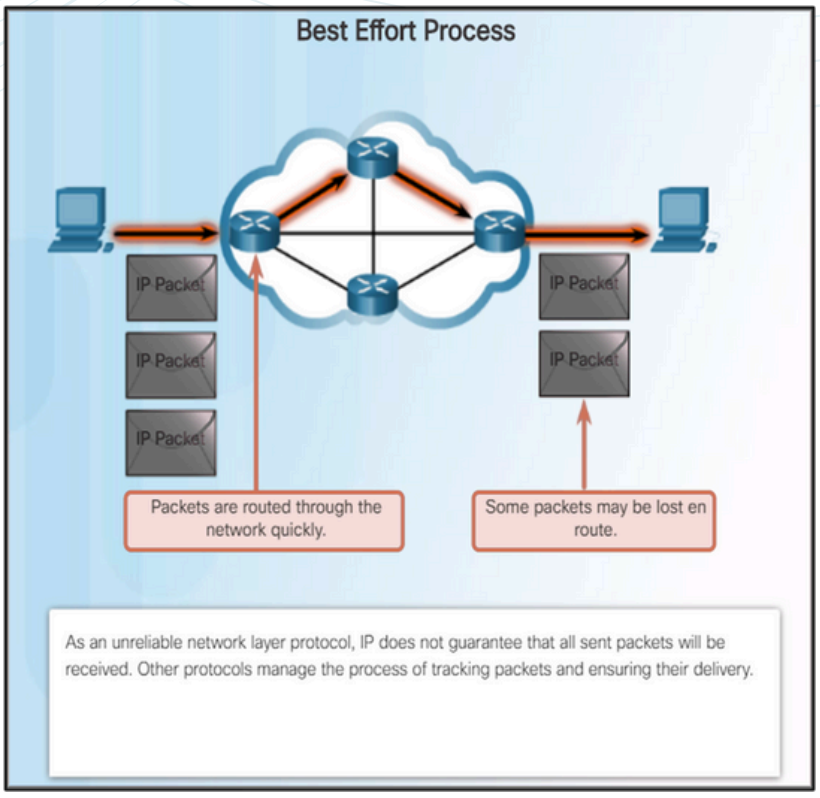
- No dedicated end-to-end connection is created before data is sent.
- Very similar process as sending someone a letter through snail mail.
- Senders do not know whether or not the destination is present, reachable, or functional before sending packets.
- This feature contributes to the low overhead of IP.



3.1.1 The Characteristics of IP Protocol

Best Effort Delivery

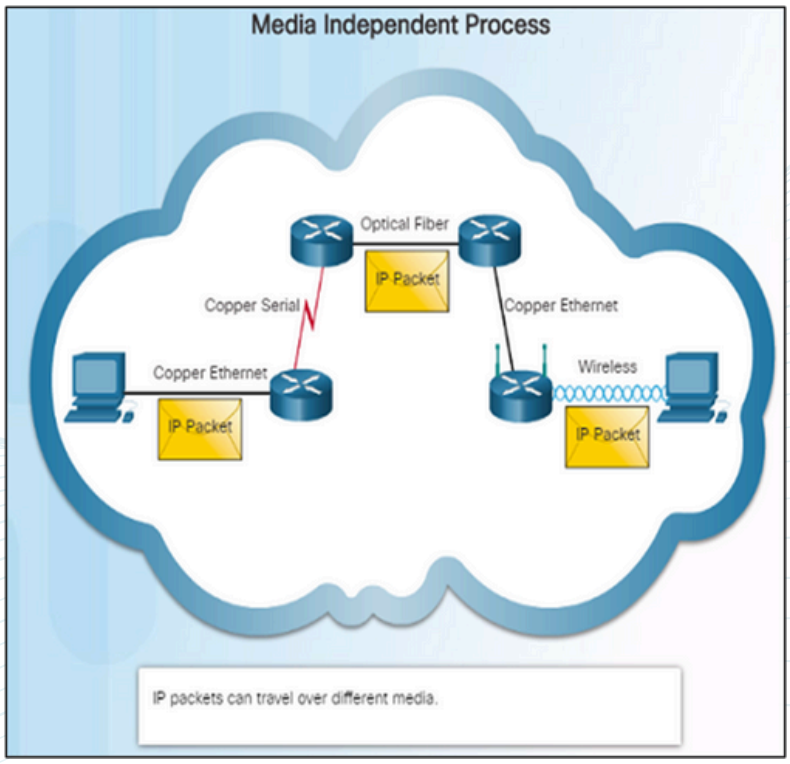
- IP is considered “unreliable” because it does not guarantee that all packets that are sent will be received.
- Unreliable means that IP does not have the capability to manage and recover from undelivered, corrupt, or out of sequence packets.
- If packets are missing or not in the correct order at the destination, upper layer protocols/services must resolve these issues



3.1.1 The Characteristics of IP Protocol

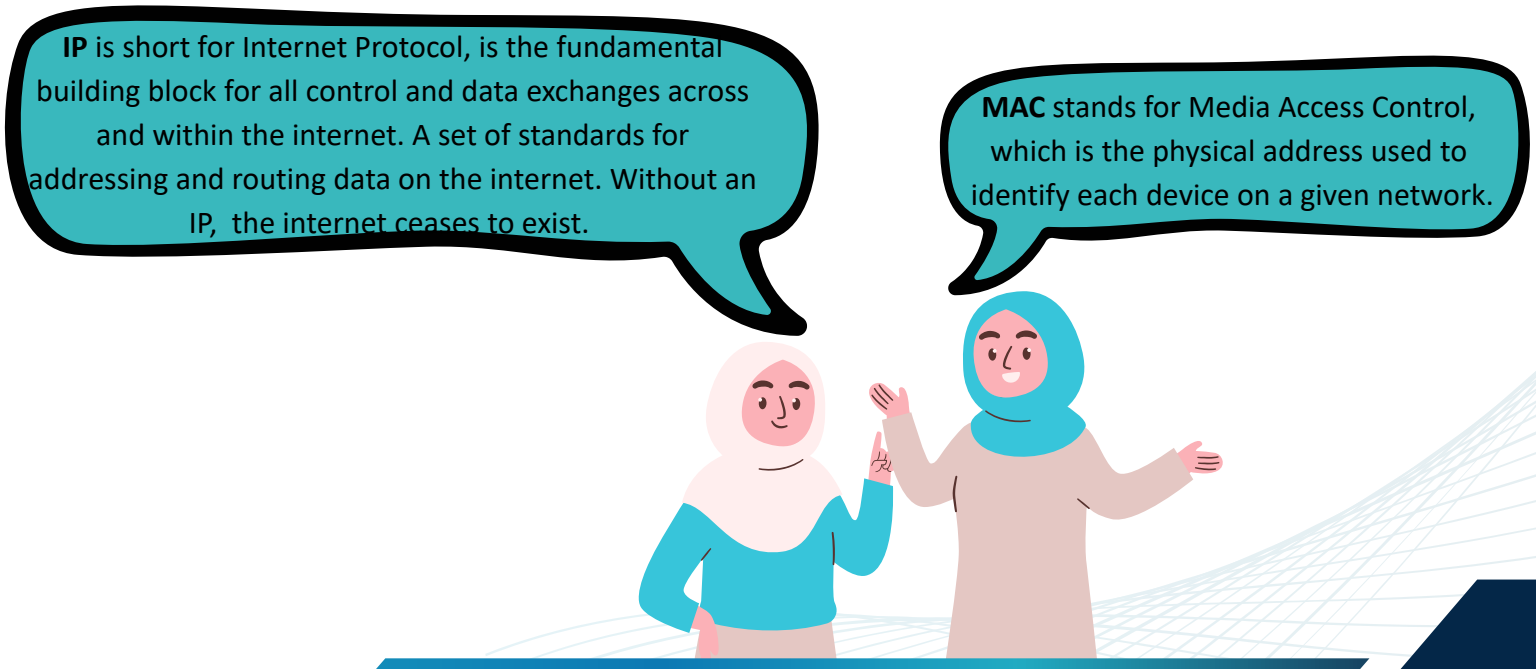
Media Independent

- IP operates independently from the media that carries the data at lower layers of the protocol stack – it does not care if the media is copper cables, fiber optics or wireless.
- The OSI data link layer is responsible for taking the IP packet and preparing it for transmission over the communications medium.
- The network layer does have a maximum size of the PDU that can be transported – referred to as MTU (maximum transmission unit).
- The data link layer tells the network layer the MTU.



3.1.2 Compare the roles of the MAC address and the IP address

Feature	MAC Address	IP Address
Type	Physical (hardware) address	Logical (software) address
OSI Layer	Layer 2 (Data Link)	Layer 3 (Network)
Uniqueness	Globally unique per NIC	Unique within a network
Format	Hexadecimal (48-bit)	IPv4 (32-bit) / IPv6 (128-bit)
Permanence	Permanent (hardcoded)	Dynamic or static
Scope	Local Network only	Local & Global (Internet)



3.1.3 The Purpose of ARP

Introduction of ARP (Address Resolution Protocol)

When a device sends an Ethernet frame, it contains these two addresses:

- Destination MAC address
- Source MAC address

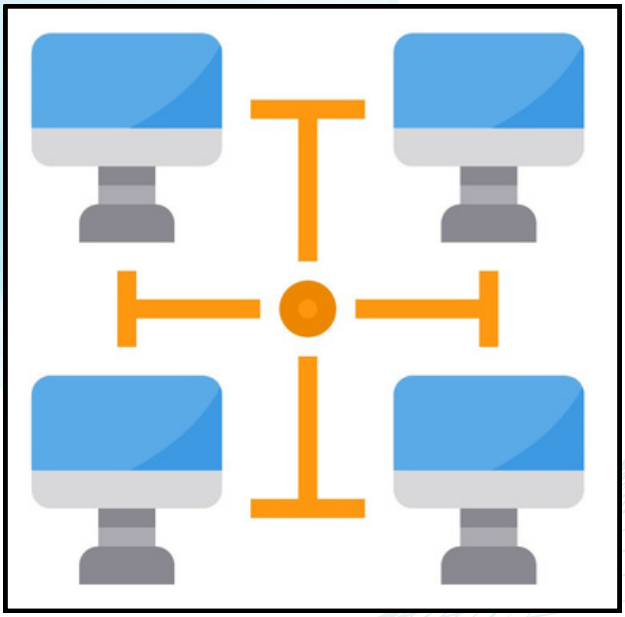
To determine the destination MAC address, the device uses ARP.
ARP provides two basic functions:

- Resolving IPv4 addresses to MAC addresses
- Maintaining a table of mappings

*** MAC address = Physical Address ***

The Purpose of ARP

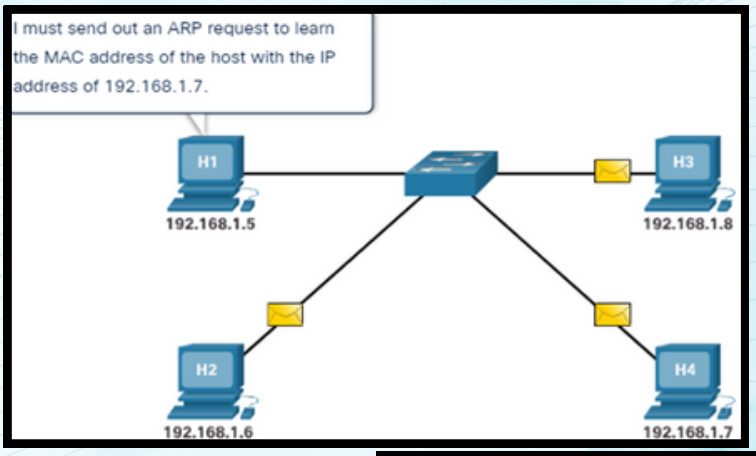
- In the OSI Model and encapsulation / decapsulation when two computers on the LAN want to communicate with each other, the following will happen:
- An IP packet is created with a source and destination IP address carrying the data from an application.
- The IP packet will be encapsulated in an Ethernet frame with a source and destination MAC address.



The sending computer will of course know its source MAC address and also it know the destination MAC address with ARP helps.

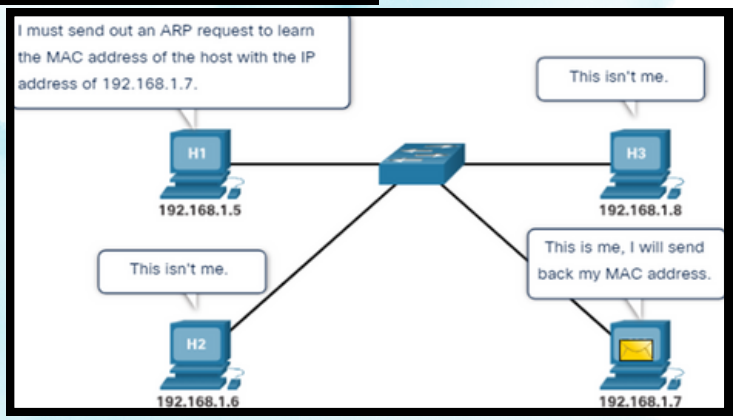
3.1.3 The Purpose of ARP

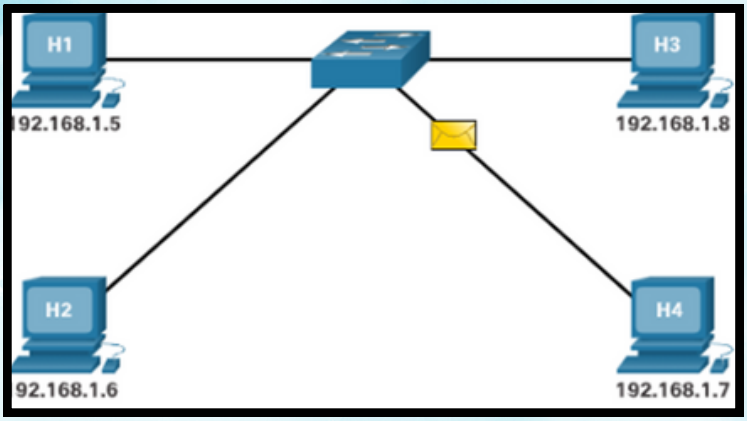
The illustration of ARP function



1

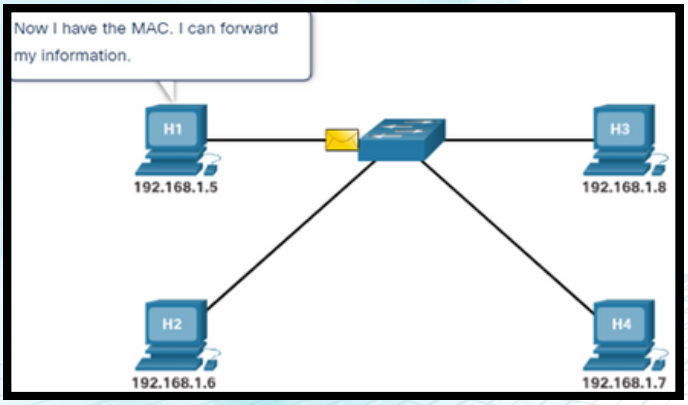
2





3

4



3.1.4 The Structure of an IPv4 address including the network portion, the host portion, and the subnet mask.

IP ADDRESS

- 32 binary bits (*bit 1 and bit 0*)
- Divided into 4 octets
- 1 octet = 8 bits
- Dotted decimal format

00000000.00000000.00000000.00000000

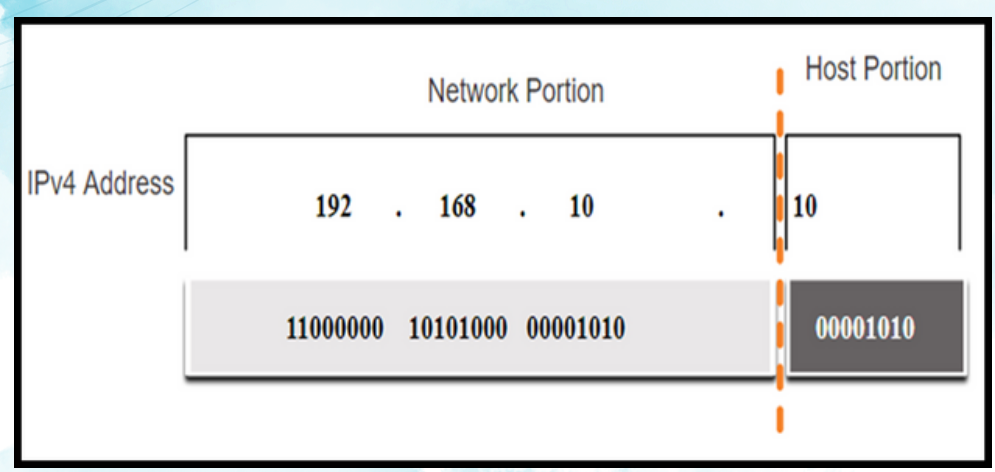
IP ADDRESS CLASSESS

CLASS	FIRST OCTET RANGE	FULL RANGE
A	1 – 127	1.0.0.0 – 127.255.255.255
B	128 – 191	128.0.0.0 – 191.255.255.255
C	192 – 223	192.0.0.0 – 223.255.255.255
D	224 – 239	224.0.0.0 – 239.255.255.255
E	240 – 255	240.0.0.0 – 255.255.255.255

3.1.4 The Structure of an IPv4 address including the network portion, the host portion, and the subnet mask.

NETWORK AND HOST PORTION

- An ipv4 address is a 32-bit hierarchical address that is made up of a network portion and a host portion.
- When determining the network portion versus the host portion, you must look at the 32-bit stream.
- A subnet mask is used to determine the network and host portions.



THE SUBNET MASK

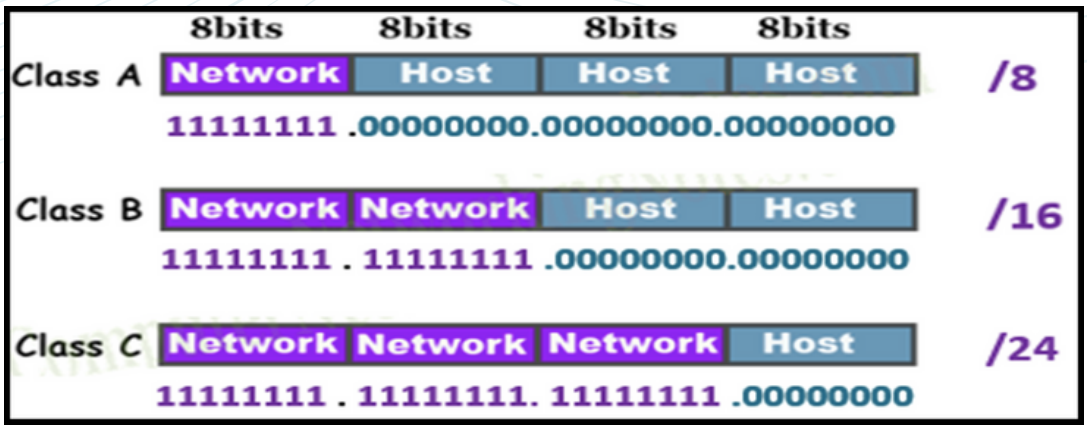
- To identify host and network portions
- To determine the host is belong to which network
- Classless Inter-Domain Routing (CIDR)

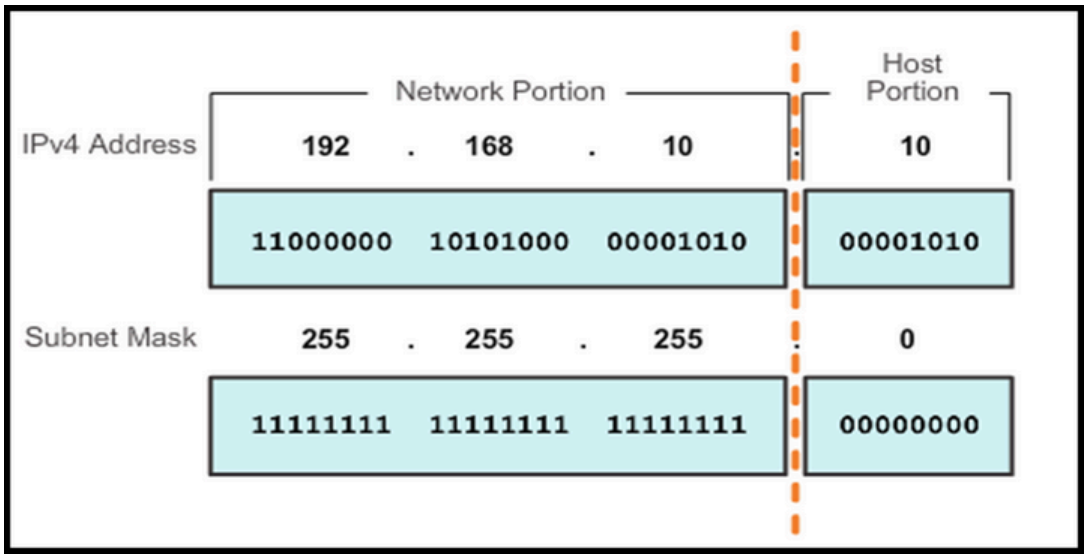
CLASS	DEFAULT SUBNET MASK	PREFIX / CIDR
A	255.0.0.0	/ 8
B	255.255.0.0	/ 16
C	255.255.255.0	/ 24

3.1.4 The Structure of an IPv4 address including the network portion, the host portion, and the subnet mask.

IP ADDRESS HAS TWO PORTIONS

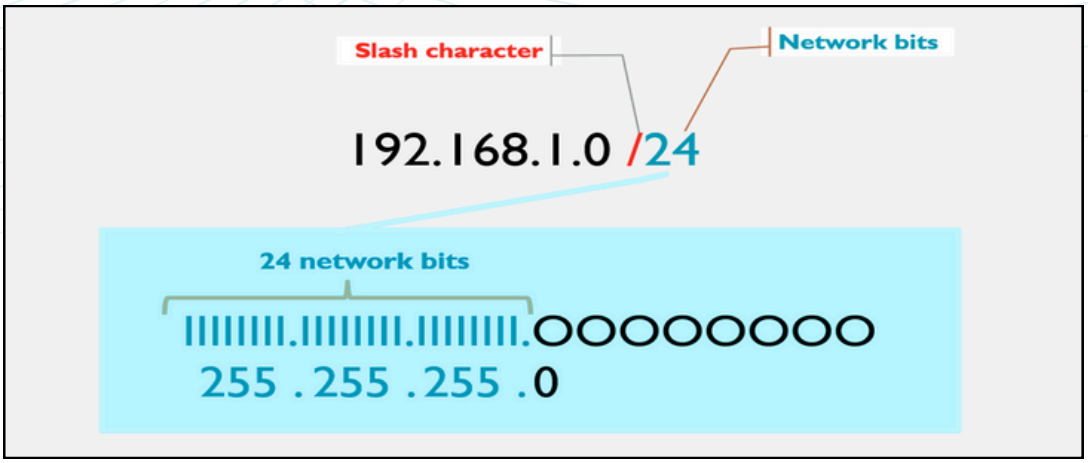
- **Network**
- **Host**

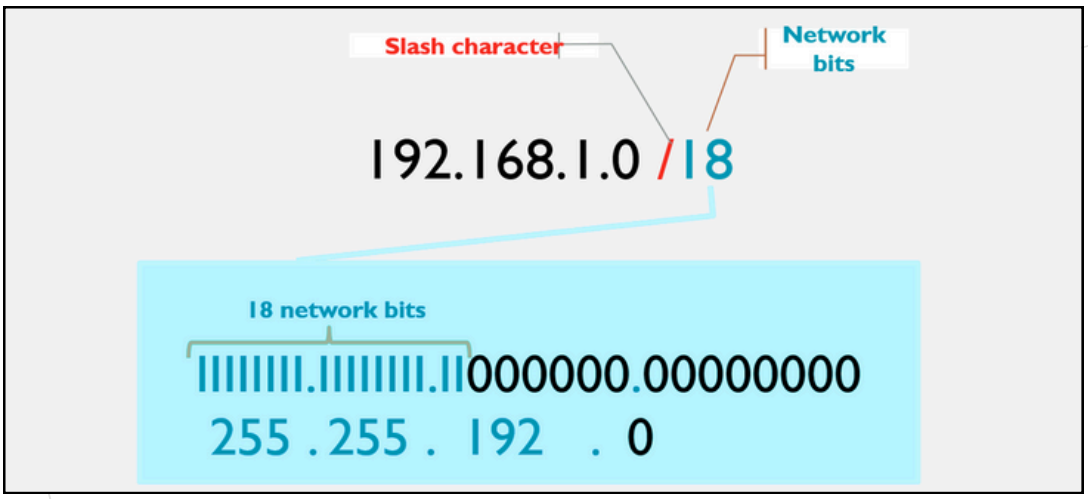




3.1.4 The Structure of an IPv4 address including the network portion, the host portion, and the subnet mask.

WRITE AN IP AND A NETWORK BITS



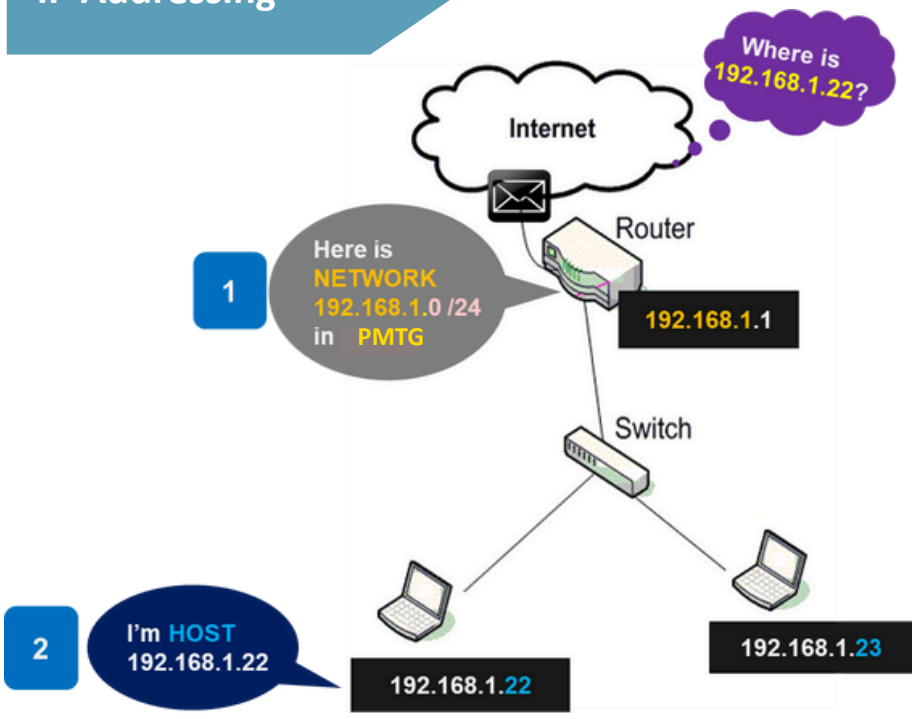


3.1.4 The Structure of an IPv4 address including the network portion, the host portion, and the subnet mask.

SUBNET VALUE

Subnet Value	Bit Value							
	128	64	32	16	8	4	2	1
255	1	1	1	1	1	1	1	1
254	1	1	1	1	1	1	1	0
252	1	1	1	1	1	1	0	0
248	1	1	1	1	1	0	0	0
240	1	1	1	1	0	0	0	0
224	1	1	1	0	0	0	0	0
192	1	1	0	0	0	0	0	0
128	1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0

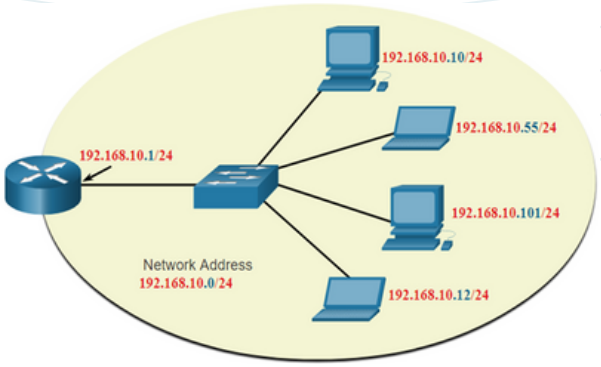
IP Addressing



3.1.4 The Structure of an IPv4 address including the network portion, the host portion, and the subnet mask.

Within each network are three types of IP addresses:

- Network address
- Host addresses
- Broadcast address



	Network Portion	Host Portion	Host Bits
Subnet mask 255.255.255.0 or /24	255 255 255 11111111 11111111 11111111	0 00000000	
Network address 192.168.10.0 or /24	192 168 10 11000000 10100000 00001010	0 00000000	All 0s
First address 192.168.10.1 or /24	192 168 10 11000000 10100000 00001010	1 00000001	All 0s and a 1
Last address 192.168.10.254 or /24	192 168 10 11000000 10100000 00001010	254 11111110	All 1s and a 0
Broadcast address 192.168.10.255 or /24	192 168 10 11000000 10100000 00001010	255 11111111	All 1s

3.1.5 Compare the characteristics and uses of the unicast, broadcast and multicast IPv4 addresses

UNICAST

Characteristics:

- One-to-One Communication: Unicast addresses are used for one-to-one communication between a single sender and a single receiver.
- Unique Identification: Each unicast address identifies a unique device on a network.
- Standard Address Range: Unicast addresses span the entire range of IPv4 addresses from 0.0.0.0 to 255.255.255.255, but certain ranges are reserved for special purposes (e.g., private networks)

Uses:

- Direct Communication: Ideal for direct communication between devices, such as a client requesting data from a server.
- Routing: Routers use unicast addresses to forward packets to specific destinations

BROADCAST

Characteristics:

- One-to-All Communication: Broadcast addresses are used for one-to-all communication within a network segment. All devices on the local network receive the broadcast packet.
- Limited Scope: Broadcast communication is confined to the local subnet or broadcast domain.
- Address Format: The broadcast address for a given subnet is the highest address in that subnet range. For example, in a subnet with 192.168.1.0/24, the broadcast address is 192.168.1.255.

Uses:

- Network Discovery: Commonly used for network discovery and service announcements (e.g., ARP requests).
- Configuration: Devices use broadcasts to locate and configure services or to distribute configuration data.

3.1.5 Compare the characteristics and uses of the unicast, broadcast and multicast IPv4 addresses

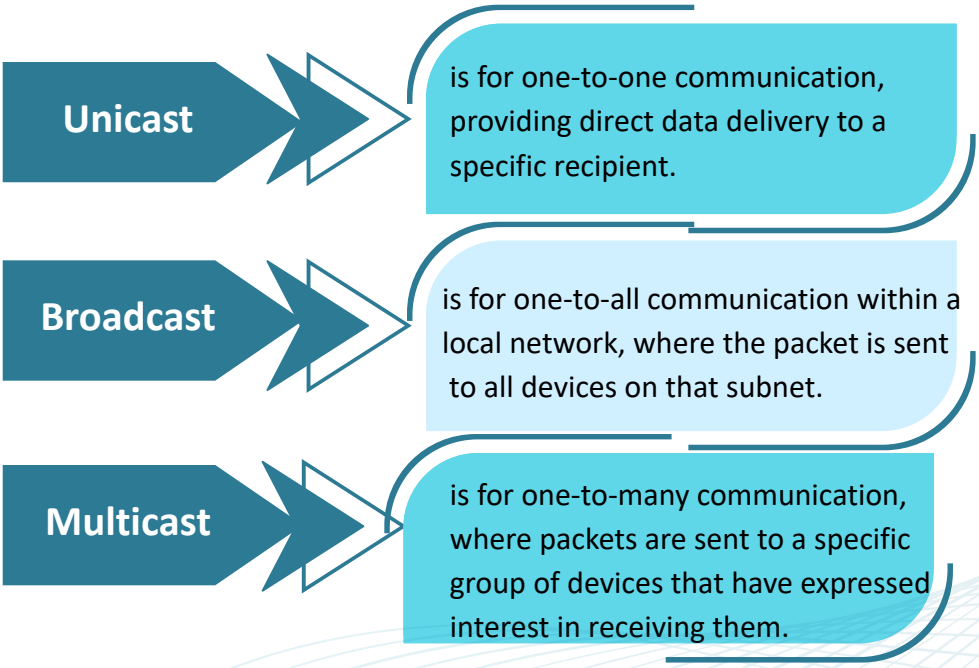
MULTICAST

Characteristics:

- One-to-Many Communication: Multicast addresses are used for one-to-many communication, where packets are sent to multiple, but not all, devices in a group.
- Special Address Range: Multicast addresses range from 224.0.0.0 to 239.255.255.255.
- Group Management: Devices must join a multicast group to receive multicast packets. Multicast routers use protocols like IGMP (Internet Group Management Protocol) to manage group memberships.

Uses:

- Streaming Media: Efficient for streaming applications where multiple receivers need the same data, such as video conferencing or live broadcasts.
- Efficient Data Distribution: Ideal for applications that need to send the same data to multiple recipients without sending duplicate packets.



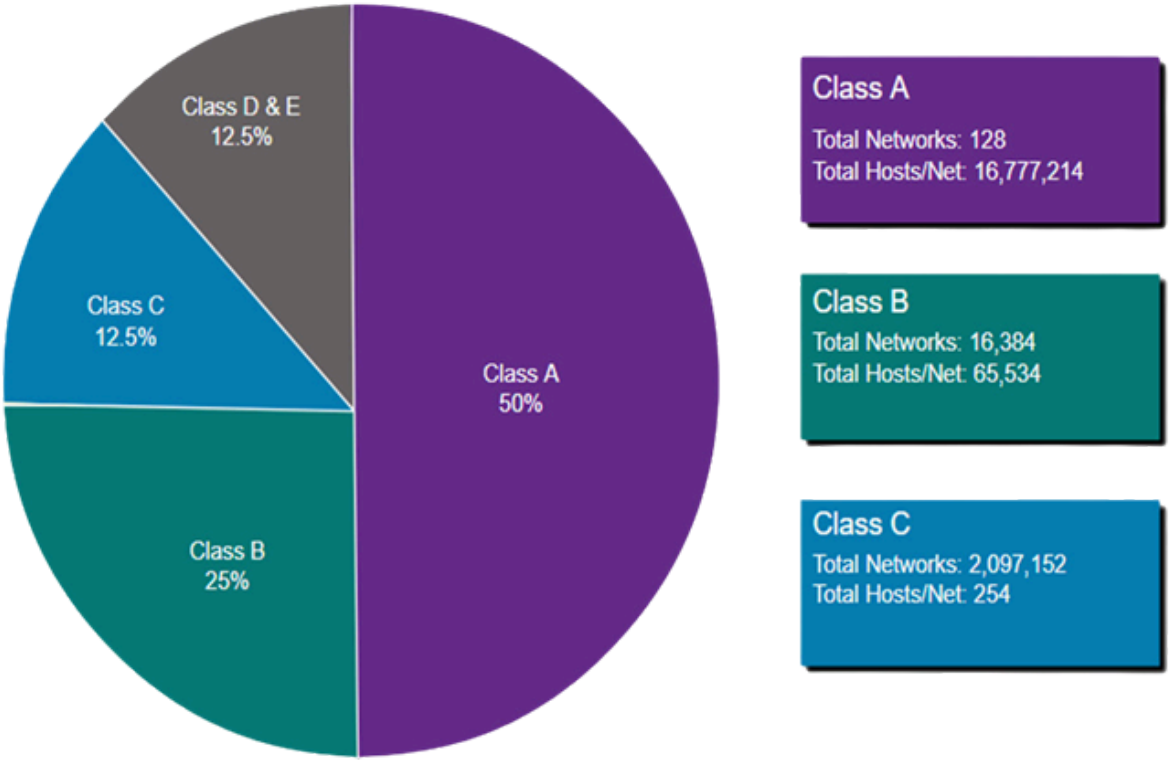
3.1.6 Public, private, and reserved IPv4 addresses.

PUBLIC

As defined in in RFC 1918, public IPv4 addresses are globally routed between internet service provider (ISP) routers.

RFC 790 (1981) allocated IPv4 addresses in classes:

- Class A (0.0.0.0/8 to 127.0.0.0/8)
- Class B (128.0.0.0 /16 – 191.255.0.0 /16)
- Class C (192.0.0.0 /24 – 223.255.255.0 /24)
- Class D (224.0.0.0 to 239.0.0.0)
- Class E (240.0.0.0 – 255.0.0.0)



3.1.6 Public, private, and reserved IPv4 addresses.

PRIVATE

Private IP addresses are a subset of IP addresses designated for use within private networks. These addresses are not routable on the public Internet, meaning they cannot be used to communicate directly with devices outside the local network. Instead, they are intended for internal use, enabling devices within the same network to communicate.

Class	Private Address Range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255

RESERVED

Definition: Reserved IPv4 addresses are set aside for special uses or future needs. They are not intended for general public use or may have specific roles within networking.

Usage: They include addresses reserved for private networks, multicast, documentation, and other purposes.

Examples:

- 0.0.0.0: Used to refer to the current network or as a default route.
- 127.0.0.0 to 127.255.255.255: Reserved for loopback testing (e.g., 127.0.0.1 is commonly used as "localhost").
- 169.254.0.0 to 169.254.255.255: Used for Automatic Private IP Addressing (APIPA) when a device cannot obtain an IP address from a DHCP server.
- 224.0.0.0 to 239.255.255.255: Reserved for multicast.

3.1.7 Convert between binary and decimal numbering systems

Converting between binary and decimal numbering systems involves understanding the relationship between the two systems. Here's a straightforward guide to converting between binary and decimal:

Binary to Decimal Conversion

Binary numbers are base-2, meaning each digit represents a power of 2. To convert a binary number to decimal:

1.Write Down the Binary Number: Identify each bit (0 or 1) in the binary number.

2.Assign Powers of 2: Start from the rightmost bit, which represents 202^020, and assign increasing powers of 2 to each bit as you move left.

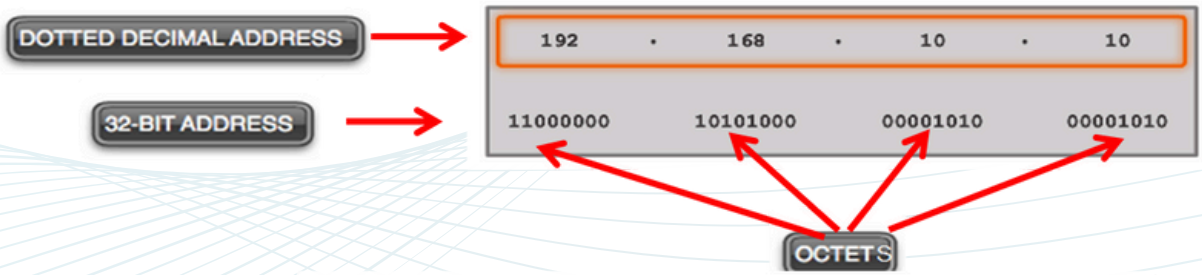
3.Multiply and Sum: Multiply each bit by its corresponding power of 2 and sum the results.

Binary Numbering System

1 octet = 8 bits
Bit 1 (value)
Bit 0 (null)

128	64	32	16	8	4	2	1
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0

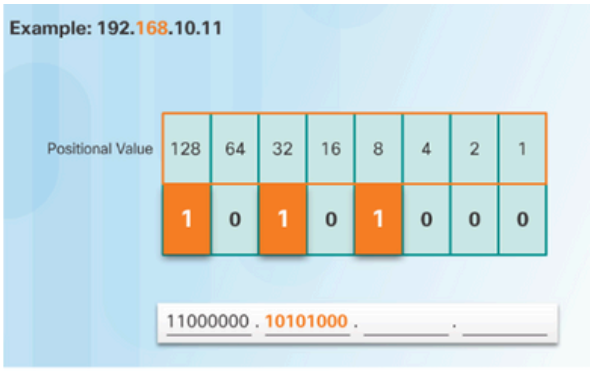
3.1.7 Convert between binary and decimal numbering systems

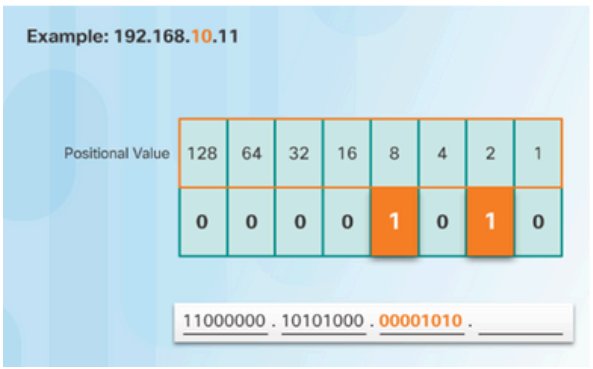


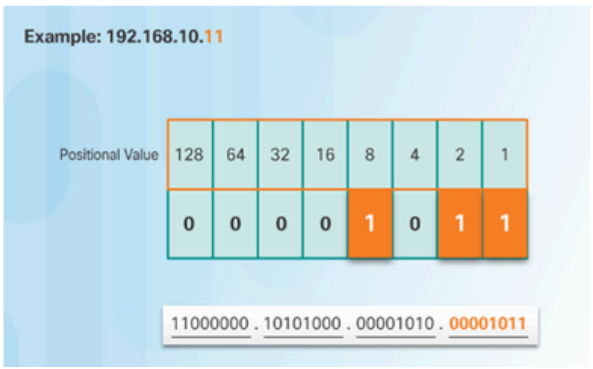
Radix	2	2	2	2	2	2	2	2
Exponent	7	6	5	4	3	2	1	0
Octet Bit Values	128	64	32	16	8	4	2	1
Binary Address	1	1	0	0	0	0	0	0
Binary Bit Values	128	64	0	0	0	0	0	0

Add the binary bit values. 128 + 64 = 192

Decimal to Binary Conversion

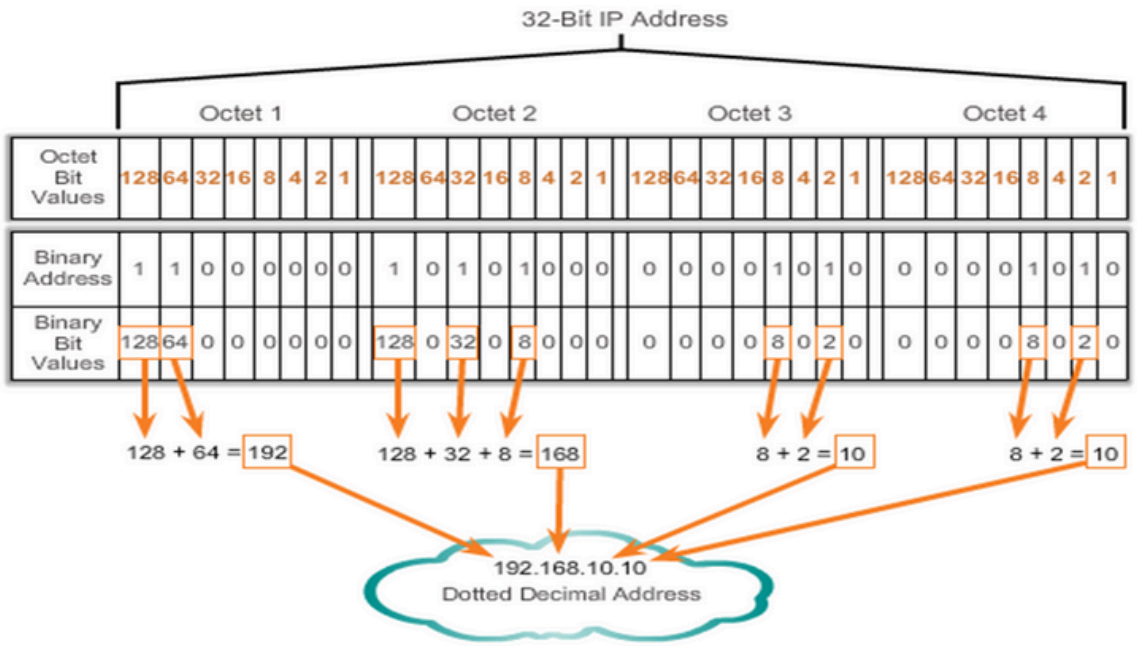


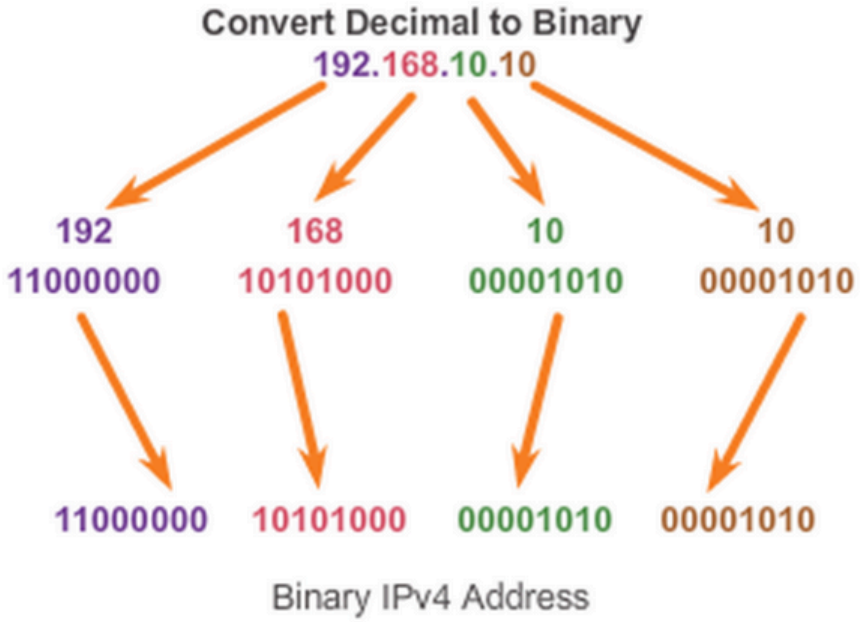




3.1.7 Convert between binary and decimal numbering systems

32 Bit IP Address





3.1.7 Convert between binary and decimal numbering systems

Quick Conversion Table

0	'0000
1	'0001
2	'0010
3	'0011
4	'0100
5	'0101
6	'0110
7	'0111
8	1000
9	1001
10	1001
11	1001
12	1001
13	1001
14	1001
15	1001

3.1.8 Subnetting segments a network to enable better communication

SUBNETTING

Subnetting is the process of dividing a larger network (IP address space) into smaller, more manageable **subnetworks (subnets)**.
This **segmentation** improves communication and efficiency in several ways:

1. **Efficient IP Address Utilization –** Prevents wastage of IP addresses by allocating only the needed addresses per subnet.
2. **Improved Network Performance –** Reduces network congestion by limiting broadcast traffic to within each subnet.
3. **Better Security & Control –** Allows administrators to isolate departments or functions (e.g., finance, HR, students) into different subnets.
4. **Simplified Management –** Makes troubleshooting and monitoring easier since the network is logically segmented.
5. **Scalability –** New subnets can be added without redesigning the whole network.

Subnets are used for a variety of reasons including by:

- Location
- Group of function
- Device type

3.1.9 Calculate IPv4 subnets

Network, Host and Broadcast Addresses

NETWORK ADDRESS:

- FIRST address
- INVALID address
- ALL HOST BIT = 0

HOST ADDRESS:

- WITHIN First & Last address
- VALID address
- HOST BIT = 1 & 0

BROADCAST ADDRESS:

- LAST address
- INVALID address
- ALL HOST BIT = 1

3.1.9 Calculate IPv4 subnets

Default Subnet mask for IP by CLASS

●CLASS A
a)10.0.0.0, 255.0.0.0
b)95.16.1.100, 255.0.0.0

●CLASS B
a)130.13.0.0, 255.255.0.0
b)172.220.66.3, 255.255.0.0

●CLASS C
a)200.200.200.0, 255.255.255.0
b)192.182.172.162, 255.255.255.0

CIDR (Classless Inter Domain Routing)

IP backbone routers have one routing table entry for each network address:

With subnetting, a backbone router only needs to know one entry for each Class A, B, or C networks

This is acceptable for Class A and Class B networks

- **2^7 = 128 Class A networks**
- **2^14 = 16,384 Class B networks**
- **But this is not acceptable for Class C networks 2^21 = 2,097,152 Class C networks**

In 1993, the size of the routing tables started to outgrow the capacity of routers

Consequence: The Class-based assignment of IP addresses had to be abandoned

3.1.9 Calculate IPv4 subnets

CIDR (Classless Inter Domain Routing)

- **Goals:**
  - Restructure IP address assignments to increase efficiency
  - Hierarchical routing aggregation to minimize route table entries

- **CIDR abandons the notion of classes:**
  - **Key Concept:** The length of the network id (prefix) in the IP addresses is kept arbitrary

- **Consequence:**
  - Routers advertise the IP address and the length of the prefix

- CIDR notation of a network address:
  192.0.2.0/18
  "18" says that the first **18 bits** are the **network part of the address (**and **14 bits are available for specific host addresses)**

- **The network part is called the prefix**

- **Assume** that a site requires a **network address with 1000 addresses**

- With **CIDR,** the **network is assigned a continuous block** of 1024 addresses with a 22-bit long prefix

Subnet Mask	32-bit Address	Prefix Length
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000	/26
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

3.1.9 Calculate IPv4 subnets

Number of Host

- Host per subnet
- Size of network

= 2^(host bit)- 2

STEP for doing subnetting

- Check the Number of Hosts (Match with a Power of Two)
- Find The New Subnet
- Turn Host Bits into Subnet Bits
- Calculate The Full Subnet Mask (FSM) — New Subnet Mask (NSM)
- Add IPs Using the Block Size (Increment)

3.1.8 Calculate IPv4 subnets

CIDR Block Prefix	# of Host Addresses
/27	32 hosts
/26	64 hosts
/25	128 hosts
/24	256 hosts
/23	512 hosts
/22	1,024 hosts
/21	2,048 hosts
/20	4,096 hosts
/19	8,192 hosts
/18	16,384 hosts
/17	32,768 hosts
/16	65,536 hosts
/15	131,072 hosts
/14	262,144 hosts
/13	524,288 hosts

3.2.1 Explain how to access a Cisco IOS device for configuration purposes

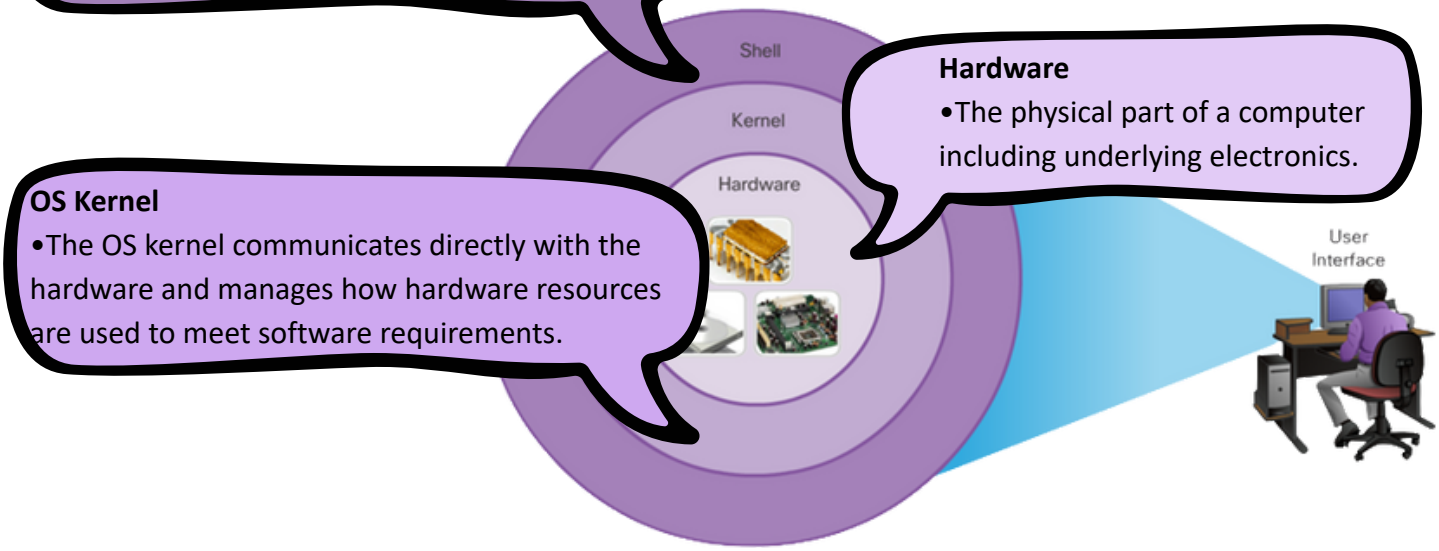
Cisco IOS Operating System

- **All electronic devices require an operating system.**
  - Windows, Mac, and Linux for PCs and laptops
  - Apple iOS and Android for smart phones and tablets
  - oCisco IOS for network devices (e.g., switches, routers, wireless AP, firewall, etc)**.**

OS Shell
•The OS shell is either a command-line interface (CLI) or a graphical user interface (GUI) and enables a user to interface with applications.

Hardware
•The physical part of a computer including underlying electronics.

OS Kernel
•The OS kernel communicates directly with the hardware and manages how hardware resources are used to meet software requirements.



Cisco devices use the Cisco (Internetwork Operating System (IOS).
Although used by Apple, iOS is a registered trademark of Cisco in the U.S. and other countries and is used by Apple under license

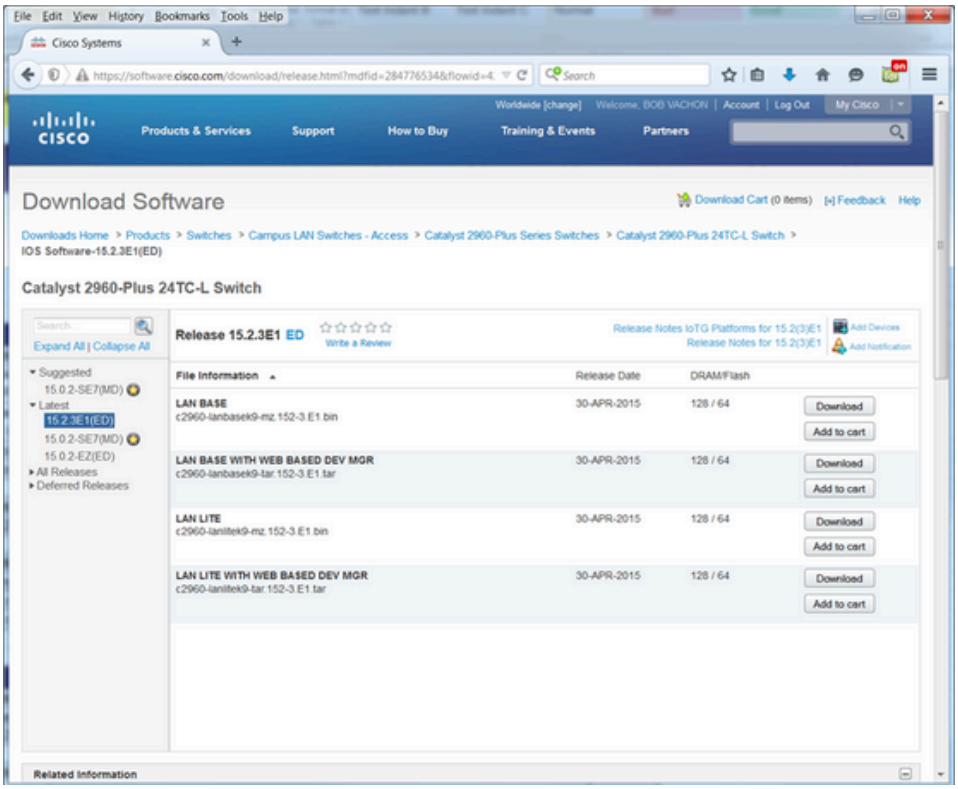
3.2.1 Explain how to access a Cisco IOS device for configuration purposes

Cisco IOS Purpose of OS

- **Using a GUI enables a user to:**
  - Use a mouse to make selections and run programs
  - Enter text and text-based commands

- **Using a CLI on a Cisco IOS switch or router enables a network technician to:**
  - Use a keyboard to run CLI-based network programs
  - Use a keyboard to enter text and text-based commands

- **There are many distinct variations of Cisco IOS:**
  - IOS for switches, routers, and other Cisco networking devices
  - IOS numbered versions for a given Cisco networking devices



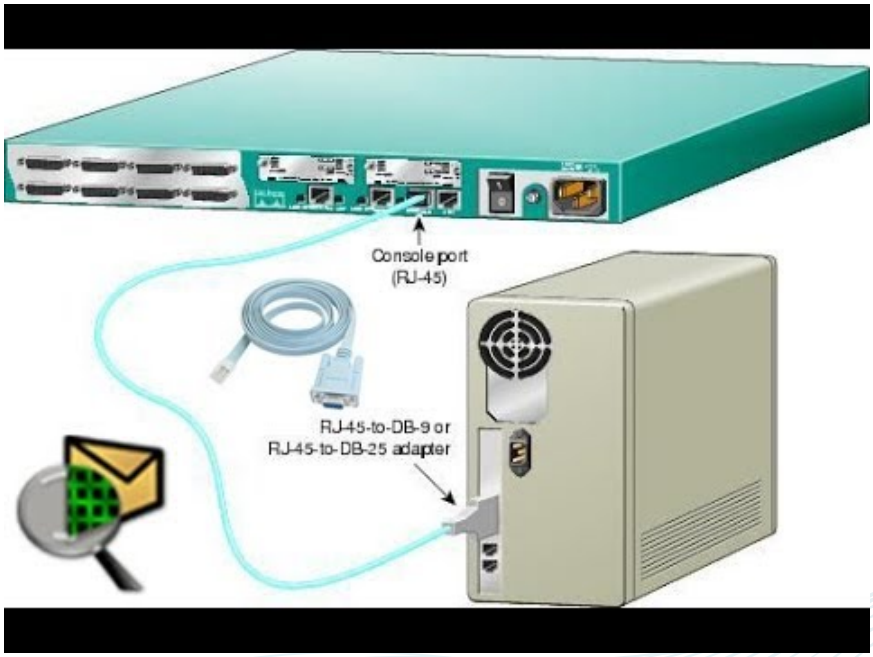
- All devices come with a default IOS and feature set. It is possible to upgrade the IOS version or feature set.
- An IOS can be downloaded from cisco.com. However, a Cisco Connection Online (CCO) account is required.
- Note: The focus of this course will be on Cisco IOS Release 15.x

3.2.1 Explain how to access a Cisco IOS device for configuration purposes

Cisco IOS Access Method

- **The three most common ways to access the IOS are:**
    - **Console port –** Out-of-band serial port used primarily for management purposes such as the initial configuration of the router.
    - **Secure Shell (SSH) -** Inband method for remotely and securely establishing a CLI session over a network. User authentication, passwords, and commands sent over the network are encrypted. As a best practice, use SSH instead of Telnet whenever possible.
    - **Telnet –** Inband interfaces remotely establishing a CLI session through a virtual interface, over a network. User authentication, passwords, and commands are sent over the network in plaintext.
- **Note:** The AUX port is an on older method of establishing a CLI session remotely via a telephone dialup connection using a modem.

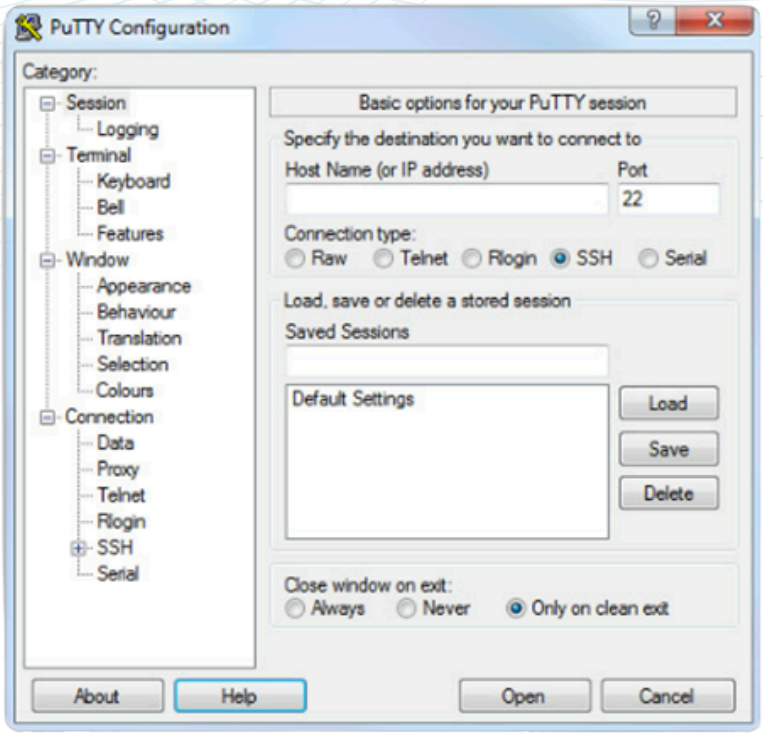
Access Method: Console port



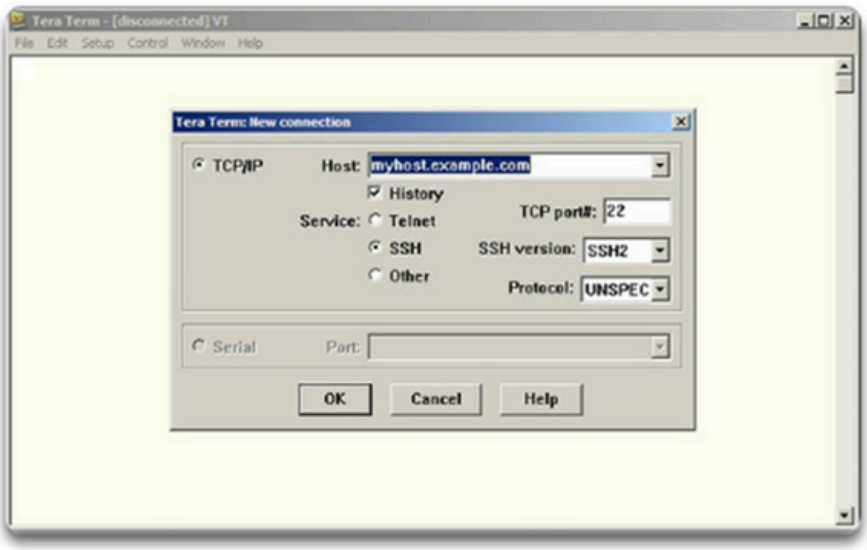
3.2.1 Explain how to access a Cisco IOS device for configuration purposes

Cisco IOS Access Method

Terminal Emulation Program



PUTTY



TERA TERM

Regardless of access method, a terminal emulation program will be required. Popular terminal emulation programs include **PuTTY, Tera Term, SecureCRT,** and **OS X Terminal.**

3.2.2 to navigate Cisco IOS to configure network devices

IOS Navigation

Primary Command Modes

User EXEC Mode:

- Allows access to only a limited number of basic monitoring commands
- Identified by the CLI prompt that ends with the > symbol

```
Router>

Switch>
```

Privileged EXEC Mode:

- Allows access to all commands and features
- Identified by the CLI prompt that ends with the # symbol

```
Router#

Switch#
```

3.2.2 to navigate Cisco IOS to configure network devices

IOS Navigation

Configuration Mode and Subconfiguration Modes

Global Configuration Mode:

- Used to access configuration options on the device

```
Switch(config)#
```

Line Configuration Mode:

- Used to configure console, SSH, Telnet or AUX access

```
Switch(config-line)#
```

Interface Configuration Mode:

- Used to configure a switch port or router interface

```
Switch(config-if)#
```

3.2.2 to navigate Cisco IOS to configure network devices

IOS Navigation

Navigation Between IOS Modes

Privileged EXEC Mode:

- To move from user EXEC mode to privilege EXEC mode, use the enabled command.

```
Switch> enable
Switch#
```

Global Configuration Mode:

- To move in and out of global configuration mode, use the configure terminal command. To return to privilege EXEC mode, use the exit command.

```
Switch(config)#
Switch(config)#exit
Switch#
```

Line Configuration Mode:

- To move in and out of line configuration mode, use the **line** command followed by the management line type. To return to global configuration mode, use the **exit** command.

```
Switch(config)#line console 0
Switch(config-line)#exit
Switch(config)#
```

3.2.2 to navigate Cisco IOS to configure network devices

IOS Navigation

Navigation Between IOS Modes

Subconfiguration Modes:

To move out of any subconfiguration mode to get back to global configuration mode, use the exit command. To return to privilege EXEC mode, use the end command or key combination Ctrl +Z.

```
Switch(config)#line console 0
Switch(config-line)#end
Switch#
```

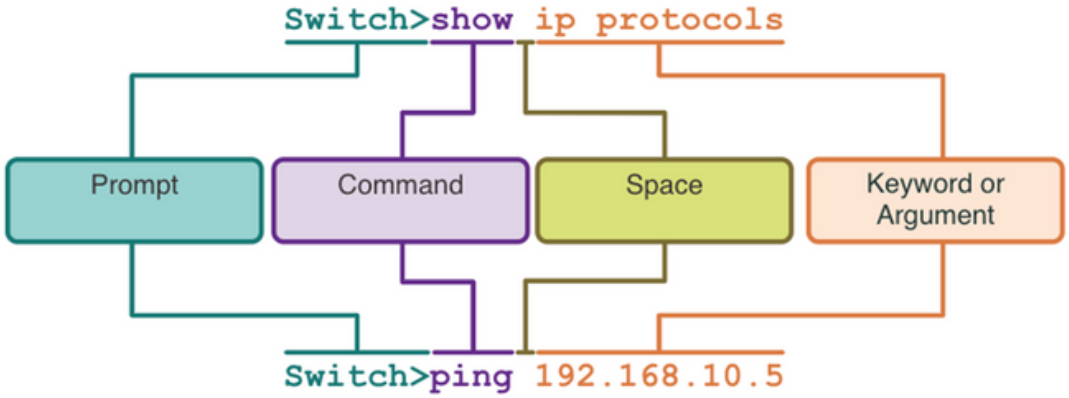
To move directly from one subconfiguration mode to another, type in the desired subconfiguration mode command. In the example, the command prompt changes from (config-line)# to (config-if)#.

```
Switch(config-line)#interface FastEthernet 0/1
Switch(config-if)#
```

3.2.3 The Command Structure of Cisco IOS software

The Command Structure

Basic IOS Command Structure



- **Keyword –** This is a specific parameter defined in the operating system (in the figure, ip protocols).
- **Argument -** This is not predefined; it is a value or variable defined by the user (in the figure, 192.168.10.5).

IOS Command Syntax Check

A command might require one or more arguments. To determine the keywords and arguments required for a command, refer to the command syntax.

- Boldface text indicates commands and keywords that are entered as shown.
- Italic text indicates an argument for which the user provides the value.

Convention	Description
boldface	Boldface text indicates commands and keywords that you enter literally as shown.
italics	Italic text indicates arguments for which you supply values.
[x]	Square brackets indicate an optional element (keyword or argument).
{x}	Braces indicate a required element (keyword or argument).
[x {y | z }]	Braces and vertical lines within square brackets indicate a required choice within an optional element. Spaces are used to clearly delineate parts of the command.

3.2.3 The Command Structure of Cisco IOS software

The Command Structure

IOS Command Syntax Check

The command syntax provides the pattern, or format, that must be used when entering a command.

The command is ping and the user-defined argument is the ip-address of the destination device. For example, ping 10.10.10.5.

```
ping ip-address
```

The command is traceroute and the user-defined argument is the ip-address of the destination device. For example, traceroute 192.168.254.254

```
traceroute ip-address
```

If a command is complex with multiple arguments, you may see it represented like this:

```
Switch(config-if)# switchport port-security aging { static | time time | type {absolute | inactivity}}
```

3.2.3 The Command Structure of Cisco IOS software

The Command Structure

IOS Help Features

The IOS has **two forms** of help available: context-sensitive help and command syntax check.

Context-sensitive help enables you to quickly find answers to these questions:

- Which commands are available in each command mode?
- Which commands start with specific characters or group of characters?
- Which arguments and keywords are available to particular commands?

```
Router#ping ?
  WORD  Ping destination address or hostname
  ip    IP echo
  ipv6  IPv6 echo
```

Command syntax check verifies that a valid command was entered by the user. If the interpreter cannot understand the command being entered, it will provide feedback describing what is wrong with the command.

```
Switch#interface fastEthernet 0/1
                ^
% Invalid input detected at '^' marker.
```

Hot Keys and Shortcuts

Keystroke	Description
Tab	Completes a partial command name entry.
Backspace	Erases the character to the left of the cursor.
Left Arrow or **Ctrl+B**	Moves the cursor one character to the left.
Right Arrow or **Ctrl+F**	Moves the cursor one character to the right.
Up Arrow or **Ctrl+P**	Recalls the commands in the history buffer, beginning with the most recent commands.

3.2.3 The Command Structure of Cisco IOS software

The Command Structure

Hot Keys and Shortcuts

- When a command output produces more text than can be displayed in a terminal window, the IOS will display a "--More--" prompt. The table below describes the keystrokes that can be used when this prompt is displayed.

Keystroke	Description
Enter Key	Displays the next line.
Space Bar	Displays the next screen.
Any other key	Ends the display string, returning to privileged EXEC mode.

The table below lists commands that can be used to exit out of an operation.

Keystroke	Description
Ctrl-C	When in any configuration mode, ends the configuration mode and returns to privileged EXEC mode.
Ctrl-Z	When in any configuration mode, ends the configuration mode and returns to privileged EXEC mode.
Ctrl-Shift-6	All-purpose break sequence used to abort DNS lookups, traceroutes, pings, etc.

3.3.1 Design a simple Local Area Network (LAN)

Devices in a Small Network

Small Network Topologies

- The majority of businesses are small most of the business networks are also small.
- A small network design is usually simple.
- Small networks typically have a single WAN connection provided by DSL, cable, or an Ethernet connection.
- Large networks require an IT department to maintain, secure, and troubleshoot network devices and to protect organizational data. Small networks are managed by a local IT technician or by a contracted professional.

Device Selection for a Small Network

Like large networks, small networks require planning and design to meet user requirements. Planning ensures that all requirements, cost factors, and deployment options are given due consideration. One of the first design considerations is the type of intermediary devices to use to support the network.

Factors that must be considered when selecting network devices include:

- cost
- speed and types of ports/interfaces
- expandability
- operating system features and services

Packet Tracer – Navigate the IOS

In this Packet Tracer, you will do the following:

- Establish Basic Connections, Access the CLI, and Explore Help
- Explore EXEC Modes
- Set the Clock

3.3.2 Configure initial settings on an IOS Cisco devices

Basic Device Configuration

no ip domain-lookup

When type a word (non-command),

- Start to find the corresponding IP address
- Takes time

```
Translating "ct"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address
ccnatutorials>
```

To avoid it:

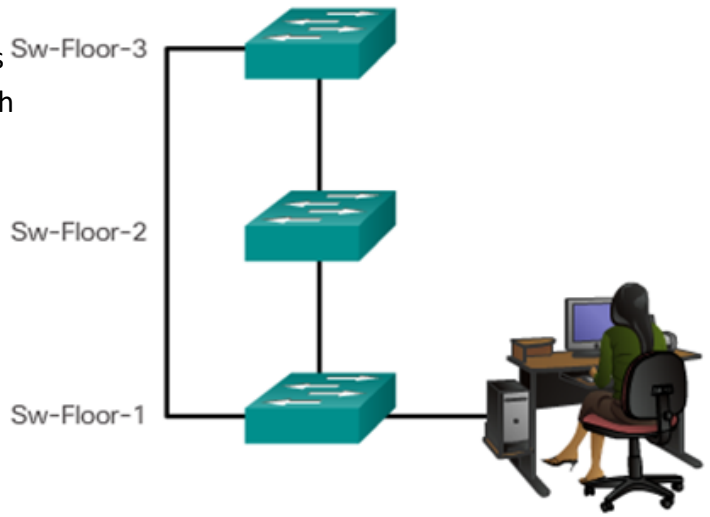
```
R1(config)# no ip domain-lookup
```

Device Names

- The first configuration command on any device should be to give it a unique hostname.
- By default, all devices are assigned a factory default name. For example, a Cisco IOS switch is "Switch."

```
Switch# configure terminal
Switch(config)# hostname Sw-Floor-1
Sw-Floor-1(config)#
```

- **Guideline for naming devices:**
  - Start with a letter
  - Contain no spaces
  - End with a letter or digit
  - Use only letters, digits, and dashes
  - Be less than 64 characters in length



Note: To return the switch to the default prompt, use the no hostname global config command.

3.3.2 Configure initial settings on an IOS Cisco devices

Basic Device Configuration

Password Guidelines

- The use of weak or easily guessed passwords are a security concern.
- All networking devices should limit administrative access by securing privileged EXEC, user EXEC, and remote Telnet access with passwords. In addition, all passwords should be encrypted and legal notifications provided.
- Use passwords that are more than eight characters in length.
- Use a combination of upper and lowercase letters, numbers, special characters, and/or numeric sequences.
- Avoid using the same password for all devices.
- Do not use common words because they are easily guessed.

Note: Most of the labs in this course use simple passwords such as cisco or class. These passwords are considered weak and easily guessable and should be avoided in production environments.

3.3.2 Configure initial settings on an IOS Cisco devices

Basic Device Configuration

Configure Passwords

Securing user EXEC mode access:

- First enter line console configuration mode using the line console 0 command in global configuration mode.
- Next, specify the user EXEC mode password using the password password command.
- Finally, enable user EXEC access using the login command

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line console 0
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# end
Sw-Floor-1#
```

Securing privileged EXEC mode access:

- First enter global configuration mode.
- Next, use the enable secret password command.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# enable secret class
Sw-Floor-1(config)# exit
Sw-Floor-1#
```

Securing VTY line access:

- First enter line VTY configuration mode using the line vty 0 15 command in global configuration mode.
- Next, specify the VTY password using the password password command.
- Finally, enable VTY access using the login command.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line vty 0 15
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# end
Sw-Floor-1#
```

Note: VTY lines enable remote access using Telnet or SSH to the device. Many Cisco switches support up to 16 VTY lines that are numbered 0 to 15.

3.3.2 Configure initial settings on an IOS Cisco devices

Basic Device Configuration

Encrypt Passwords

- The startup-config and running-config files display most passwords in plaintext.
- To encrypt all plaintext passwords, use the service password-encryption global config command.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# service password-encryption
Sw-Floor-1(config)# exit
Sw-Floor-1#
```

Use the show running-config command to verify that the passwords on the device are now encrypted.

```
Sw-Floor-1# show running-config
!

!
line con 0
password 7 094F471A1A0A
login
!
Line vty 0 4
Password 7 03095A0F034F38435B49150A1819
Login
!
!
end
```

3.3.2 Configure initial settings on an IOS Cisco devices

Basic Device Configuration

Banner Messages

- A banner message is important to warn unauthorized personnel from attempting to access the device.
- To create a banner message of the day on a network device, use the banner motd # the message of the day # global config command.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# banner motd #Authorized Access Only!#
```

The banner will be displayed on attempts to access the device.

```
Press RETURN to get started.



Authorized Access Only!

User Access Verification

Password:
```

Note: The "#" in the command syntax is called the delimiting character. It is entered before and after the message.

3.3.3 Configure two active interfaces on a Cisco IOS router

Basic Router Configuration Steps

•Configure the device name.

```
Router(config)# hostname hostname
```

•Secure privileged EXEC mode.

```
Router(config)# enable secret password
```

•Secure user EXEC mode.

```
Router(config)# line console 0
Router(config-line)# password password
Router(config-line)# login
```

•Secure remote Telnet / SSH access.

```
Router(config)# line vty 0 4
Router(config-line)# password password
Router(config-line)# login
Router(config-line)# transport input {ssh | telnet}
```

•Encrypt all plaintext passwords.

```
Router(config)# service password encryption
```

•Provide legal notification and save the configuration.

```
Router(config)# banner motd # message #
Router(config)# end
Router# copy running-config startup-config
```

3.3.3 Configure two active interfaces on a Cisco IOS router

Basic Router Configuration EXAMPLE

- Commands for basic router configuration on R1.
- Configuration is saved to NVRAM.

```
R1(config)# hostname R1
R1(config)# enable secret class
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# transport input ssh telnet
R1(config-line)# exit
R1(config)# service password encryption
R1(config)# banner motd #
Enter TEXT message. End with a new line and the #
**********************************************
WARNING: Unauthorized access is prohibited!
**********************************************
R1(config)# exit
R1# copy running-config startup-config
```

Configure Router Interfaces

Configuring a router interface includes issuing the following commands:

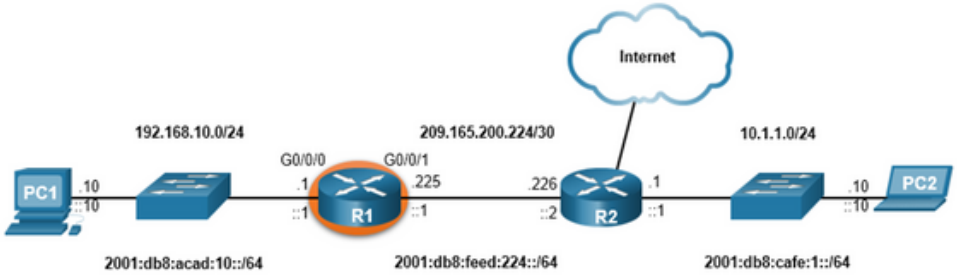
```
Router(config)# interface type-and-number
Router(config-if)# description description-text
Router(config-if)# ip address ipv4-address subnet-mask
Router(config-if)# ipv6 address ipv6-address/prefix-length
Router(config-if)# no shutdown
```

- It is a good practice to use the description command to add information about the network connected to the interface.
- The no shutdown command activates the interface.

3.3.3 Configure two active interfaces on a Cisco IOS router

Configure Router Interfaces EXAMPLE

The commands to configure interface G0/0/0 on R1 are shown here:




```
R1(config)# interface gigabitEthernet 0/0/0
R1(config-if)# description Link to LAN
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:10::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)#
*Aug  1 01:43:53.435: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to down
*Aug  1 01:43:56.447: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to up
*Aug  1 01:43:57.447: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0,
changed state to up
```

The commands to configure interface G0/0/1 on R1 are shown here:

```
R1(config)# interface gigabitEthernet 0/0/1
R1(config-if)# description Link to R2
R1(config-if)# ip address 209.165.200.225 255.255.255.252
R1(config-if)# ipv6 address 2001:db8:feed:224::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)#
*Aug  1 01:46:29.170: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, changed state to down
*Aug  1 01:46:32.171: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, changed state to up
*Aug  1 01:46:33.171: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1,
changed state to up
```

Verify Interface Configuration

To verify interface configuration use the show ip interface brief and show ipv6 interface brief commands shown here:

```
R1#  show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   192.168.10.1    YES manual up                    up
GigabitEthernet0/0/1   209.165.200.225 YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
```

```
R1#  show ipv6 interface brief
GigabitEthernet0/0/0       [up/up]
    FE80::201:C9FF:FE89:4501
    2001:DB8:ACAD:10::1
GigabitEthernet0/0/1       [up/up]
    FE80::201:C9FF:FE89:4502
    2001:DB8:FEED:224::1
Vlan1                      [administratively down/down]
    unassigned
R1#
```

3.3.3 Configure two active interfaces on a Cisco IOS router

Configure Verification Commands

The table summarizes show commands used to verify interface configuration.

Commands	Description
show ip interface brief **show ipv6 interface brief**	Displays all interfaces, their IP addresses, and their current status.
show ip route **show ipv6 route**	Displays the contents of the IP routing tables stored in RAM.
show interfaces	Displays statistics for all interfaces on the device. Only displays the IPv4 addressing information.
show ip interfaces	Displays the IPv4 statistics for all interfaces on a router.
show ipv6 interfaces	Displays the IPv6 statistics for all interfaces on a router.

View status of all interfaces with the **show ip interface brief** and s**how ipv6 interface brief** commands, shown here:

```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   192.168.10.1    YES manual up                    up
GigabitEthernet0/0/1   209.165.200.225 YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
R1#
```

```
R1# show ipv6 interface brief
GigabitEthernet0/0/0       [up/up]
    FE80::201:C9FF:FE89:4501
    2001:DB8:ACAD:10::1
GigabitEthernet0/0/1       [up/up]
    FE80::201:C9FF:FE89:4502
    2001:DB8:FEED:224::1
Vlan1                      [administratively down/down]
    unassigned
R1#
```

3.3.3 Configure two active interfaces on a Cisco IOS router

Configure Verification Commands

Display the contents of the IP routing tables with the **show ip route** and s**how ipv6 route** commands as shown here:

```
R1# show ip route
< output omitted>
Gateway of last resort is not set
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0/0
L        192.168.10.1/32 is directly connected, GigabitEthernet0/0/0
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.224/30 is directly connected, GigabitEthernet0/0/1
L        209.165.200.225/32 is directly connected, GigabitEthernet0/0/1
R1#
```

```
R1# show ipv6 route
<output omitted>
C   2001:DB8:ACAD:10::/64 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   2001:DB8:ACAD:10::1/128 [0/0]
     via GigabitEthernet0/0/0, receive
C   2001:DB8:FEED:224::/64 [0/0]
     via GigabitEthernet0/0/1, directly connected
L   2001:DB8:FEED:224::1/128 [0/0]
     via GigabitEthernet0/0/1, receive
L   FF00::/8 [0/0]
     via Null0, receive
R1#
```

Display statistics for all interfaces with the **show interfaces** command, as shown here:

```
R1# show interfaces gig0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Hardware is ISR4321-2x1GE, address is a0e0.af0d.e140 (bia  a0e0.af0d.e140)
  Description: Link to LAN
  Internet address is 192.168.10.1/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full Duplex, 100Mbps, link type is auto, media type is RJ45
  output flow-control is off, input flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output 00:00:35, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output      drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1180 packets input, 109486 bytes, 0 no buffer
     Received 84 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles

<output omitted>

R1#
```

3.3.3 Configure two active interfaces on a Cisco IOS router

Configure Verification Commands

Display IPv4 statistics for router interfaces with the **show ip interface** command, as shown here:

```
R1# show ip interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing Common access list is not set
  Outgoing access list is not set
  Inbound Common access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP Flow switching is disabled

<output omitted>

R1#
```

3.3.3 Configure two active interfaces on a Cisco IOS router

Configure Verification Commands

Display IPv6 statistics for router interfaces with the **show ipv6 interface** command shown here:

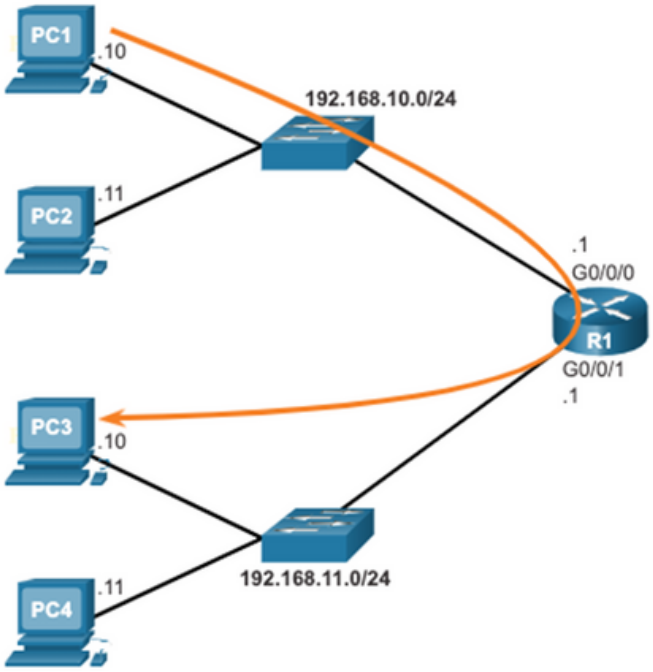
```
R1# show ipv6 interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is
FE80::868A:8DFF:FE44:49B0
  No Virtual link-local address(es):
  Description: Link to LAN
  Global unicast address(es):
    2001:DB8:ACAD:10::1, subnet is 2001:DB8:ACAD:10::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF00:1
    FF02::1:FF44:49B0
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND NS retransmit interval is 1000 milliseconds

R1#
```

3.3.4 Configure devices to use the default gateway

Configure the Default Gateway

Default Gateway on a Host

- The default gateway is used when a host sends a packet to a device on another network.
- The default gateway address is generally the router interface address attached to the local network of the host.
- To reach PC3, PC1 addresses a packet with the IPv4 address of PC3, but forwards the packet to its default gateway, the G0/0/0 interface of R1.



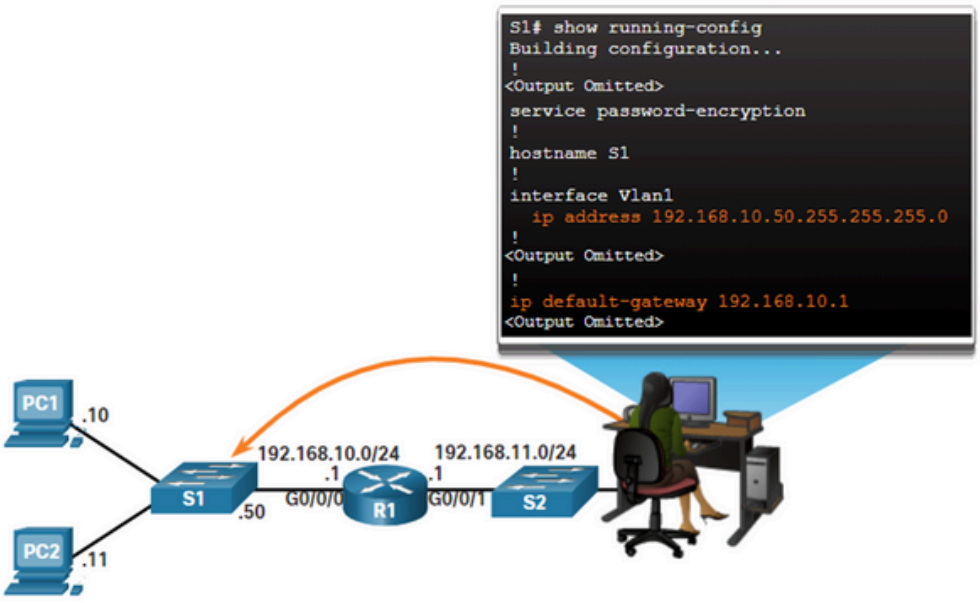
Note: The IP address of the host and the router interface must be in the same network.

3.3.4 Configure devices to use the default gateway

Configure the Default Gateway

Default Gateway on a Switch

- A switch must have a default gateway address configured to remotely manage the switch from another network.
- To configure an IPv4 default gateway on a switch, use the **ip default-gateway ip-address** global configuration command.



Note: The IP address of the host and the router interface must be in the same network.

3.3.4 Configure devices to use the default gateway

Configure the Default Gateway

Ping – Test Connectivity

- The **ping** command is an IPv4 and IPv6 testing utility that uses ICMP echo request and echo reply messages to test connectivity between hosts and provides a summary that includes the success rate and average round-trip time to the destination.
- If a reply is not received within the timeout, ping provides a message indicating that a response was not received.
- It is common for the first ping to timeout if address resolution (ARP or ND) needs to be performed before sending the ICMP Echo Request.

```
S1#ping 192.168.20.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms
```

```
R1#ping 2001:db8:acad:1::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:acad:1::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

- The PING command displays whether the destination responded and how long it took to receive a reply
- If there is an error in the delivery to the destination, the PING command displays an error message
- PING operates by sending an ICMP (Internet Control Message Protocol) echo request to a network address at periodic intervals waiting for an echo ICMP response
- How to PING:
  - ping x.x.x.x (IP address)
  - ping site.com (web address)

3.3.4 Configure devices to use the default gateway

Configure the Default Gateway

Ping – Test Connectivity

```
C:\Users\Alateeq>ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprecated
                   and has no effect on the type of service field in the IP Head
er).
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
    -S srcaddr     Source address to use.
    -4             Force using IPv4.
    -6             Force using IPv6.
```

```
Command Prompt

C:\Users\user>ping 10.10.100.1

Pinging 10.10.100.1 with 32 bytes of data:
Reply from 10.10.100.1: bytes=32 time<1ms TTL=128
Reply from 10.10.100.1: bytes=32 time<1ms TTL=128
Reply from 10.10.100.1: bytes=32 time<1ms TTL=128
Reply from 10.10.100.1: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.100.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\user>_
```

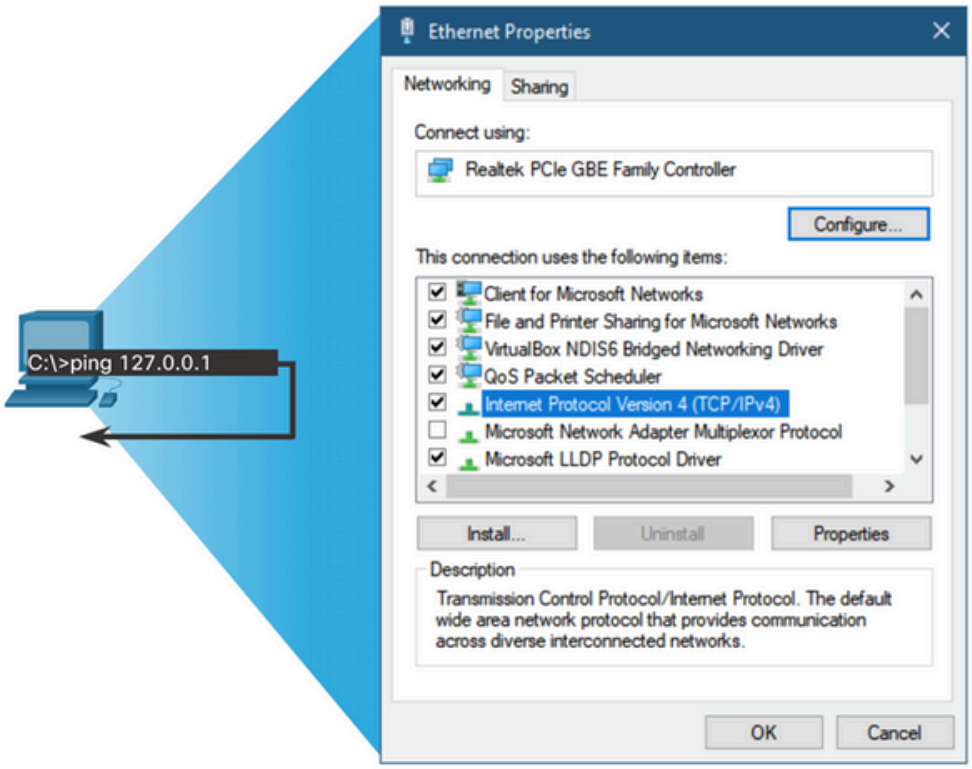
```
Pinging 192.168.0.99 with 32 bytes of data:
Reply from 192.168.0.176: Destination host unreachable.
Reply from 192.168.0.176: Destination host unreachable.
Reply from 192.168.0.176: Destination host unreachable.
Reply from 192.168.0.176: Destination host unreachable.

Ping statistics for 192.168.0.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

3.3.4 Configure devices to use the default gateway

Configure the Default Gateway

Ping the Loopback

- Ping can be used to test the internal configuration of IPv4 or IPv6 on the local host. To do this, ping the local loopback address of 127.0.0.1 for IPv4 (::1 for IPv6).
- A response from 127.0.0.1 for IPv4, or ::1 for IPv6, indicates that IP is properly installed on the host.
- An error message indicates that TCP/IP is not operational on the host.



3.3.4 Configure devices to use the default gateway

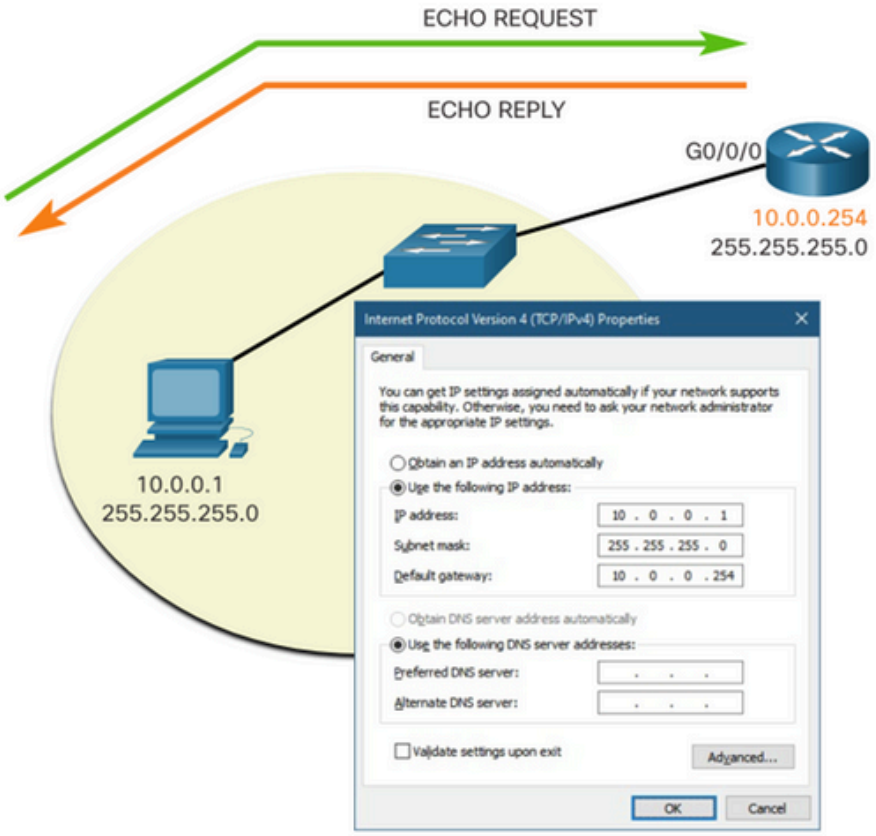
Configure the Default Gateway

Ping a Remote Host

- The ping command can be used to test the ability of a host to communicate on the local network.
- The default gateway address is most often used because the router is normally always operational.

- A successful ping to the default gateway indicates that the host and the router interface serving as the default gateway are both operational on the local network.

- If the default gateway address does not respond, a ping can be sent to the IP address of another host on the local network that is known to be operational.



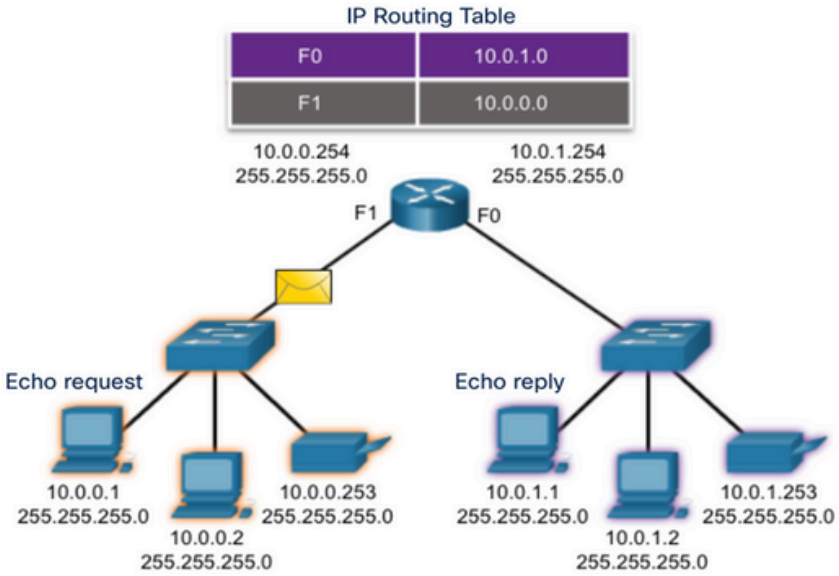
3.3.4 Configure devices to use the default gateway

Configure the Default Gateway

Ping a Remote Host

Ping can also be used to test the ability of a local host to communicate across an internetwork.

A local host can ping a host on a remote network. A successful ping across the internetwork confirms communication on the local network.



Note: Many network administrators limit or prohibit the entry of ICMP messages therefore, the lack of a ping response could be due to security restrictions.

3.3.5 IOS commands to save the running configuration

Save Configurations

There are two system files that store the device configuration:

- startup-config - This is the saved configuration file that is stored in NVRAM. It contains all the commands that will be used by the device upon startup or reboot. Flash does not lose its contents when the device is powered off.
- running-config - This is stored in Random Access Memory (RAM). It reflects the current configuration. Modifying a running configuration affects the operation of a Cisco device immediately. RAM is volatile memory. It loses all of its content when the device is powered off or restarted.
- To save changes made to the running configuration to the startup configuration file, use the copy running-config startup-config privileged EXEC mode command.

```
Router#show startup-config
Using 624 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
```

```
Router#show running-config
Building configuration...

Current configuration : 624 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
```

3.3.5 IOS commands to save the running configuration

Save Configurations

If changes made to the running config do not have the desired effect and the running-config has not yet been saved, you can restore the device to its previous configuration. To do this you can:

- Remove the changed commands individually.
- Reload the device using the reload command in privilege EXEC mode. Note: This will cause the device to briefly go offline, leading to network downtime.

```
Router# reload
Proceed with reload? [confirm]
Initializing Hardware ...
```

If the undesired changes were saved to the startup-config, it may be necessary to clear all the configurations using the erase startup-config command in privilege EXEC mode.

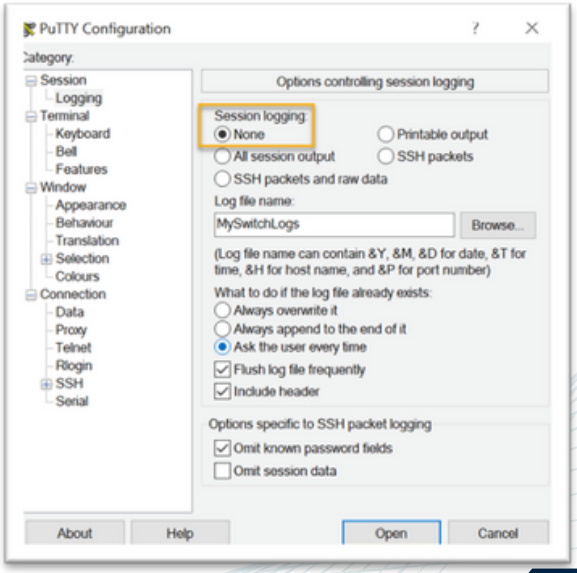
- After erasing the startup-config, reload the device to clear the running-config file from RAM.

```
Router# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#
```

Capture Configuration to a Text File

Configuration files can also be saved and archived to a text document.

- **Step 1.** Open terminal emulation software, such as PuTTY or Tera Term, that is already connected to a switch.
- **Step 2.** Enable logging in to the terminal software and assign a name and file location to save the log file. The figure displays that All session output will be captured to the file specified (i.e., MySwitchLogs).
- **Step 3.** Execute the show running-config or show startup-config command at the privileged EXEC prompt. Text displayed in the terminal window will be placed into the chosen file.
- **Step 4.** Disable logging in the terminal software. The figure shows how to disable logging by choosing the None session logging option



3.3.6 Troubleshoot Default gateway issue

Packet Tracer – Troubleshoot Default Gateway Issues

In this Packet Tracer, you will do the following:

- Verify the network documentation and use tests to isolate problems.
- Determine an appropriate solution for a given problem.
- Implement the solution.
- Test to verify the problem is resolved.
- Document the solution.

Quick Quiz

1. _____ is a Layer 2 address that allows NICs to communicate with each other.

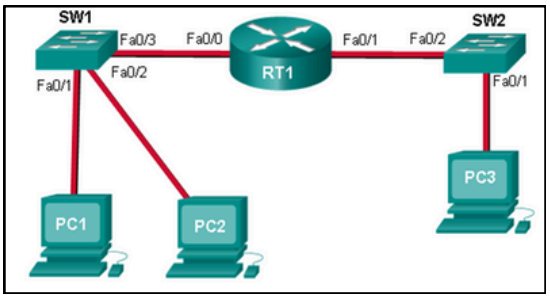
2. _____ is a Layer 3 address that identifies both the network and specific host on that network.

3. ARP also known as? _____

4. ARP table is stored in _____ .

5. _____ the process that is used to find a Layer 2 address when a Layer 3 address is known.

6. The ARP table in a switch maps which two types of addresses together?
   A. Layer 3 address to a Layer 2 address
   B. Layer 3 address to a Layer 4 address
   C. Layer 4 address to a Layer 2 address
   D. Layer 2 address to a Layer 4 address

7. 

PC1 issues an ARP request because it needs to send a packet to PC2. In this scenario, what will happen next?

A. PC2 will send an ARP reply with its MAC address.
B. RT1 will send an ARP reply with its Fa0/0 MAC address.
C. RT1 will send an ARP reply with the PC2 MAC address.
D. SW1 will send an ARP reply with the PC2 MAC address.
E. SW1 will send an ARP reply with its Fa0/1 MAC address.

04

WIRELESS TECHNOLOGIES

4.1.1 Explain the benefits of WLAN

Introduction to Wireless

- A Wireless LAN (WLAN) is a type of wireless network that is commonly used in homes, offices, and campus environments.
- WLANs make mobility possible within the home and business environments.
- Wireless infrastructures adapt to rapidly changing needs and technologies.

Benefits of Wireless

- Mobility
- Convenience
- Productivity
- Deployment
- Expandability
- Cost
- Flexibility
- Reliability

Limitation of Wireless

These are some of the limitations of wireless:

- Coverage area - Wireless data communication technologies work well in open environments. However, certain construction materials used in buildings and structures, and the local terrain, will limit the effective coverage.
- Interference - Wireless is susceptible to interference and can be disrupted by such common devices as household cordless phones, some types of fluorescent lights, microwave ovens, and other wireless communications.
- Security - Wireless communication coverage requires no access to a physical strand of media. Therefore, devices and users, not authorized for access to the network, can gain access to the transmission. Network security is a major component of wireless network administration.
- Shared medium - WLANs operate in half-duplex, which means only one device can send or receive at a time. The wireless medium is shared amongst all wireless users. Many users accessing the WLAN simultaneously results in reduced bandwidth for each user.
- High power consumption
- Degradation in performance
- Speed

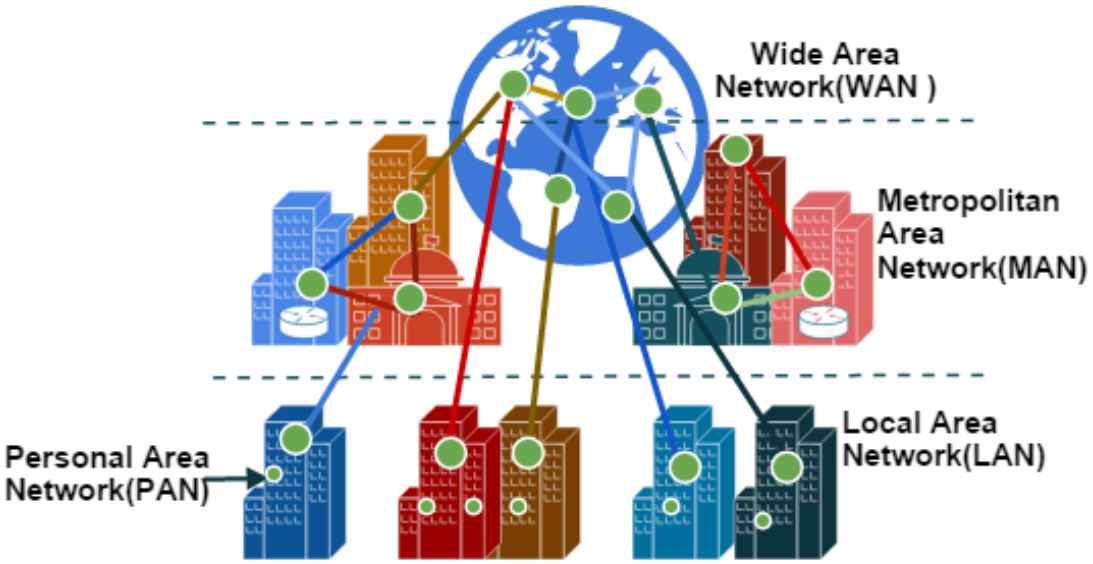
4.1.2 Identify Types of Wireless Networks:

- **Wireless Personal-Area Network (WPAN)**
  - Low power and short-range (20-30ft or 6-9 meters). Based on IEEE 802.15 standard and 2.4 GHz frequency. Bluetooth and Zigbee are WPAN examples.

- **Wireless LAN (WLAN)**
  - Medium sized networks up to about 300 feet. Based on IEEE 802.11 standard and 2.4 or 5.0 GHz frequency.

- **Wireless MAN (WMAN)**
  - Large geographic area such as city or district. Uses specific licensed frequencies.

- **Wireless WAN (WWAN)**
  - Extensive geographic area for national or global communication. Uses specific licensed frequencies.



4.1.3 Identify Wireless Technologies:

a. **Bluetooth**

IEEE WPAN standard used for device pairing at up to 30ft (9m) distance.

- Bluetooth Low Energy (BLE) – Supports mesh topology to large scale network devices.
- Bluetooth Basic Rate/Enhanced Rate (BR/EDR) – Supports point-to-point topologies and is optimized for audio streaming.

b. WiMAX (Worldwide Interoperability for Microwave Access)

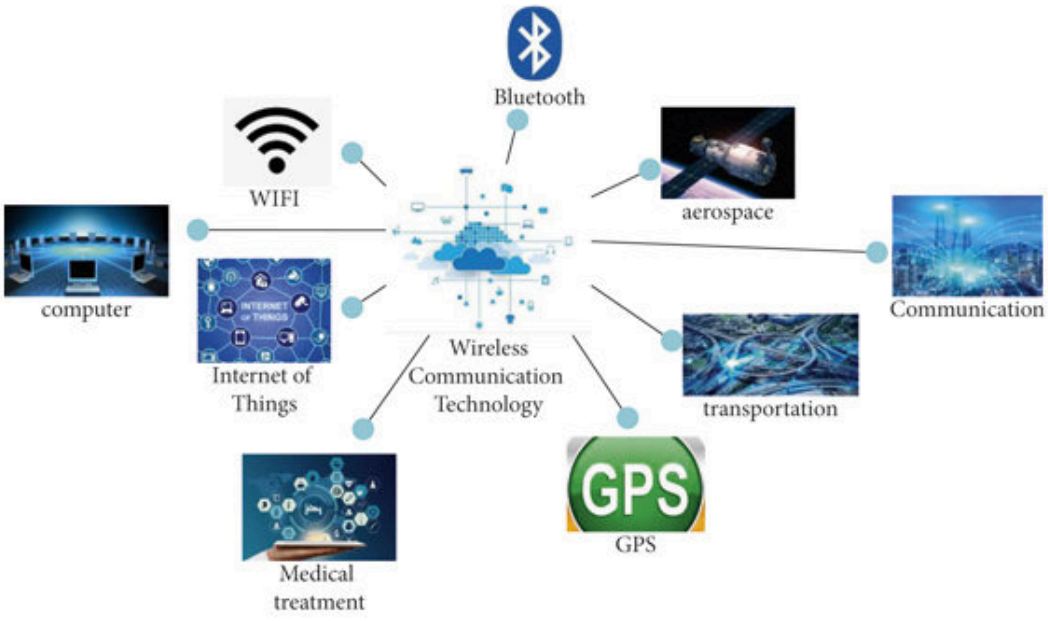
- Alternative broadband wired internet connections. IEEE 802.16 WLAN standard for up 30 miles (50 km).

c. Cellular Broadband

- Carry both voice and data. Used by phones, automobiles, tablets, and laptops.
- Global System of Mobile (GSM) – Internationally recognized
- Code Division Multiple Access (CDMA) – Primarily used on the US.

d. **Satellite Broadband**

- Uses directional satellite dish aligned with satellite in geostationary orbit. Needs clear line of site. Typically used in rural locations where cable and DSL are unavailable.



4.1.4 Identify 802.11 Standards (a, b, g, n, ac, ax)

802.11 Standards

802.11 WLAN standards define how radio frequencies are used for wireless links.

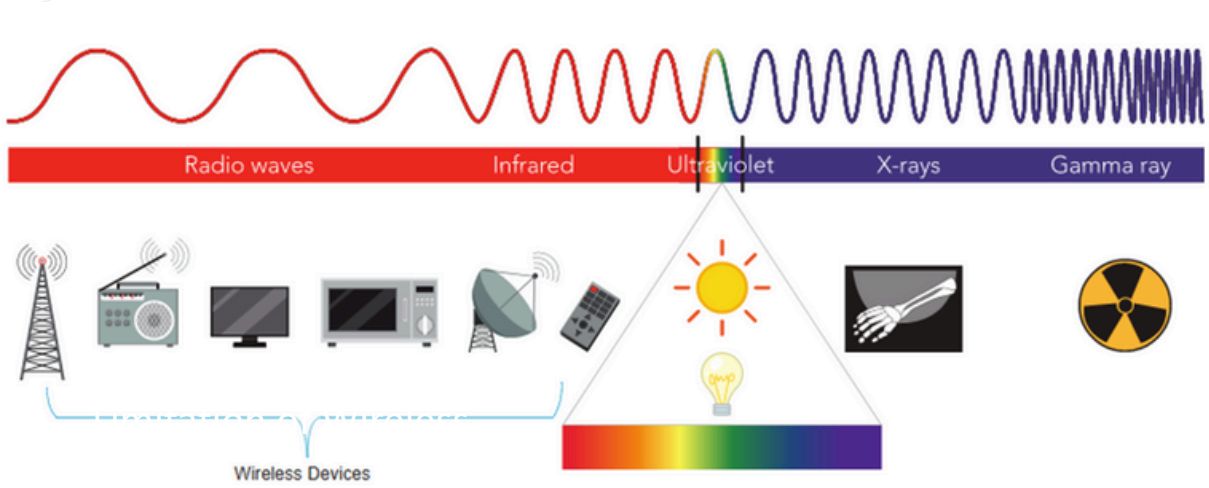
IEEE Standard	Radio Frequency	Description
802.11	2.4 GHz	Data rates up to 2 Mb/s
802.11a	5 GHz	Data rates up to 54 Mb/s Not interoperable with 802.11b or 802.11g
802.11b	2.4 GHz	Data rates up to 11 Mb/s Longer range than 802.11a and better able to penetrate building structures
802.11g	2.4 GHz	Data rates up to 54 Mb/s Backward compatible with 802.11b
802.11n	2.4 and 5 GHz	Data rates 150 – 600 Mb/s Require multiple antennas with MIMO technology
802.11ac	5 GHz	Data rates 450 Mb/s – 1.3 Gb/s Supports up to eight antennas
802.11ax	2.4 and 5 GHz	High-Efficiency Wireless (HEW) Capable of using 1 GHz and 7 GHz frequencies

4.1.4 Identify 802.11 Standards (a, b, g, n, ac, ax)

Radio Frequencies

All wireless devices operate in the range of the electromagnetic spectrum. WLAN networks operate in the 2.4 and 5 GHz frequency bands.

- ○2.4 GHz (UHF) – 802.11b/g/n/ax
- ○5 GHz (SHF) – 802.11a/n/ac/ax



4.1.4 Identify 802.11 Standards (a, b, g, n, ac, ax)

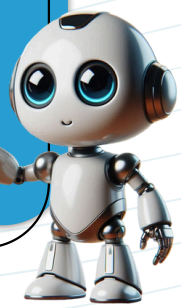
Wireless Standards Organizations

Standards ensure interoperability between devices that are made by different manufacturers. Internationally, the three organizations influencing WLAN standards:

- International Telecommunication Union (ITU) – Regulates the allocation of radio spectrum and satellite orbits.
- Institute of Electrical and Electronics Engineers (IEEE) – Specifies how a radio frequency is modulated to carry information. Maintains the standards for local and metropolitan area networks (MAN) with the IEEE 802 LAN/MAN family of standards.
- Wi-Fi Alliance – Promotes the growth and acceptance of WLANs. It is an association of vendors whose objective is to improve the interoperability of products that are based on the 802.11 standard

4.1.5 Identify WLAN Components:

a. Wireless NICs
b. USB Wireless Adapter
c. Wireless Router
d. Wireless Access Points
e. Wireless Antennas



a. Wireless NICs

- To communicate wirelessly, laptops, tablets, smart phones, and even the latest automobiles include integrated wireless NICs that incorporate a radio transmitter/receiver.

- If a device does not have an integrated wireless NIC, then a USB wireless adapter can be used.

4.1.5 Identify WLAN Components:

a. Wireless NICs
b. USB Wireless Adapter
c. Wireless Router
d. Wireless Access Points
e. Wireless Antennas

b. USB Wireless Adapter

- ○A USB wireless adapter is essentially a wireless network card that is used to access a network through a USB port on your computer. Wireless adapters allow your computer to connect to a wireless network for internet in the absence of an internal network card.

4.1.5 Identify WLAN Components:

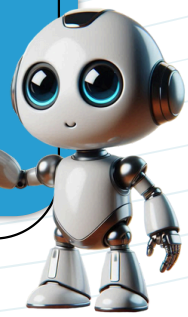
a. Wireless NICs
b. USB Wireless Adapter
c. Wireless Router
d. Wireless Access Points
e. Wireless Antennas

c. Wireless Home Router

- A home user typically interconnects wireless devices using a small, wireless router.
- Wireless routers serve as the following:
  - Access point – To provide wires access
  - Switch – To interconnect wired devices
  - Router - To provide a default gateway to other networks and the Internet

4.1.5 Identify WLAN Components:

a. Wireless NICs
b. USB Wireless Adapter
c. Wireless Router
d. Wireless Access Points
e. Wireless Antennas



d. Wireless Access Points

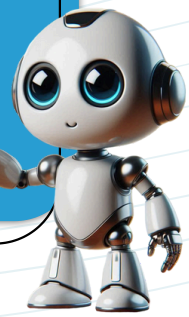
- Wireless clients use their wireless NIC to discover nearby access points (APs).
- Clients then attempt to associate and authenticate with an AP.
- After being authenticated, wireless users have access to network resources.

Cisco Meraki MR33

Meraki Go

4.1.5 Identify WLAN Components:

a. Wireless NICs
b. USB Wireless Adapter
c. Wireless Router
d. Wireless Access Points
e. Wireless Antennas

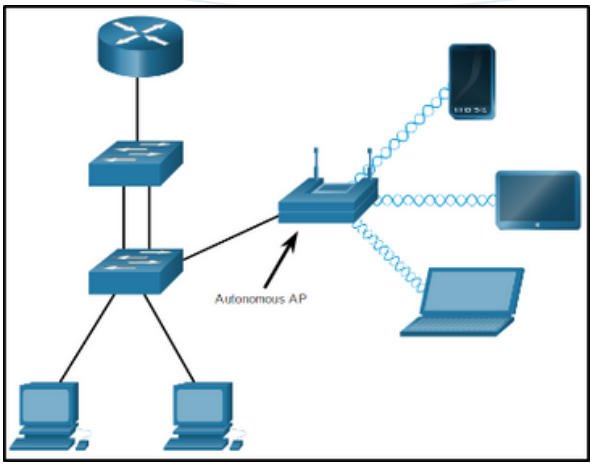


d. Wireless Access Points

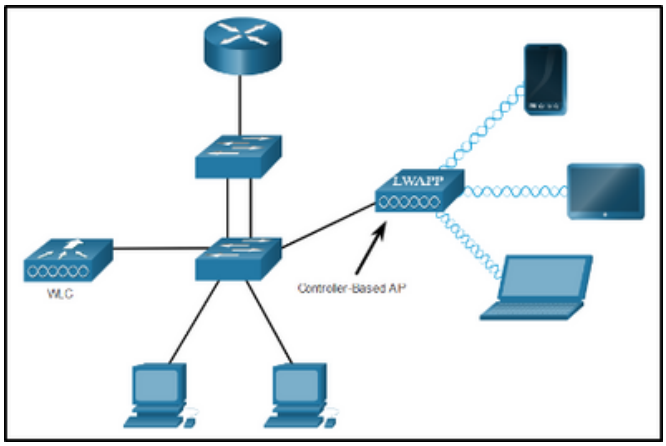
APs Categories

- APs can be categorized as either autonomous APs or controller-based APs.

■ Autonomous APs – Standalone devices configured through a command line interface or GUI. Each autonomous AP acts independently of the others and is configured and managed manually by an administrator.

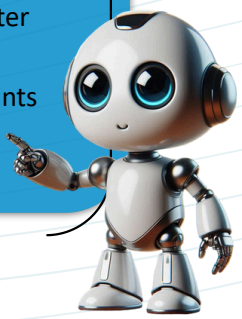


■ **Controller-based APs** – Also known as lightweight APs (LAPs). Use Lightweight Access Point Protocol (LWAPP) to communicate with a LWAN controller (WLC). Each LAP is automatically configured and managed by the WLC.



4.1.5 Identify WLAN Components:

a. Wireless NICs
b. USB Wireless Adapter
c. Wireless Router
d. Wireless Access Points
e. Wireless Antennas

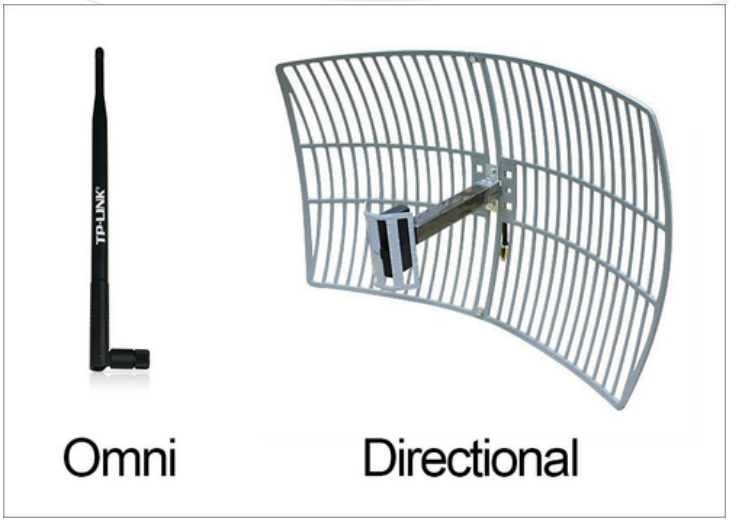


e. Wireless Antennas

● Types of external antennas:

■ **Omnidirectional** – Provide 360-degree coverage. Ideal in houses and office areas.

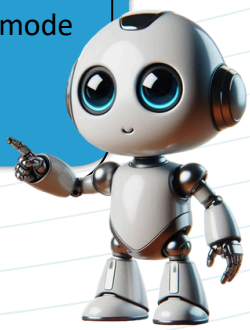
■ **Directional** – Focus the radio signal in a specific direction. Examples are the Yagi and parabolic dish.



■ **Multiple Input Multiple Output (MIMO)** – Uses multiple antennas (Up to eight) to increase bandwidth.

4.1.6 Identify 802.11 Wireless Topology Modes.

a. Ad hoc Mode
b. Infrastructure mode
c. Tethering

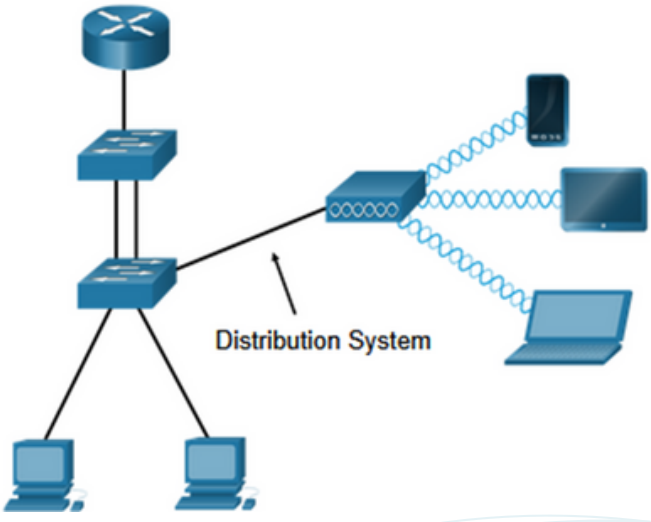


(a) Ad hoc mode

- This is when two devices connect wirelessly in a peer-to-peer (P2P) manner without using APs or wireless routers.
- Examples include wireless clients connecting directly to each other using Bluetooth or Wi-Fi Direct.

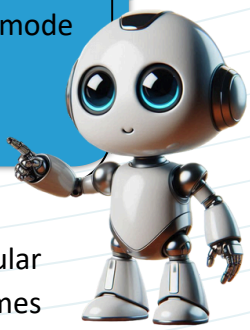
(b) Infrastructure mode

- This is when wireless clients interconnect via a wireless router or AP, such as in WLANs. APs connect to the network infrastructure using the wired distribution system, such as Ethernet.



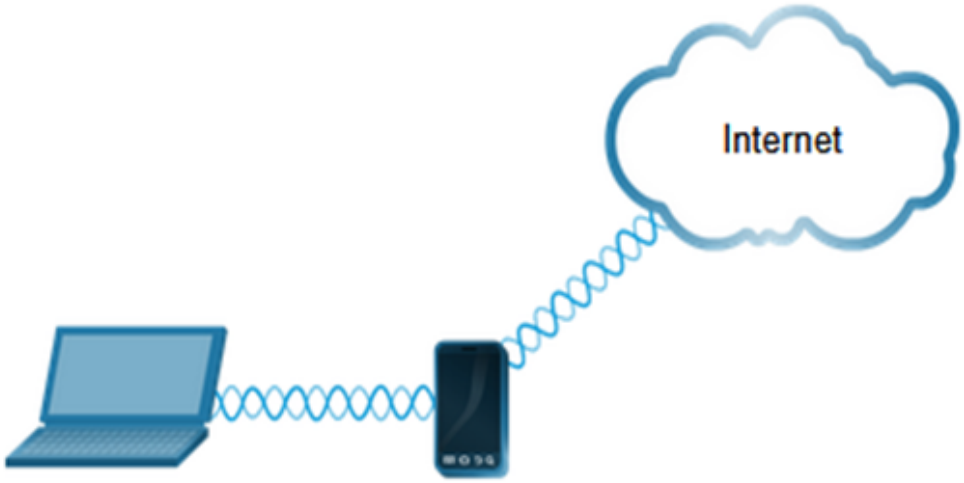
4.1.6 Identify 802.11 Wireless Topology Modes.

a. Ad hoc Mode
b. Infrastructure mode
c. Tethering



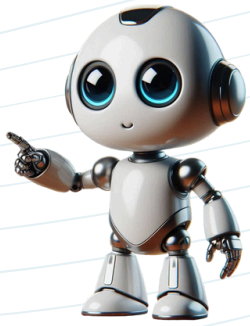
(c) Tethering

- A variation of the ad hoc topology is when a smart phone or tablet with cellular data access is enabled to create a personal hotspot. This feature is sometimes referred to as tethering.
- A hotspot is usually a temporary quick solution that enables a smart phone to provide the wireless services of a Wi-Fi router.
- Other devices can associate and authenticate with the smart phone to use the internet connection.

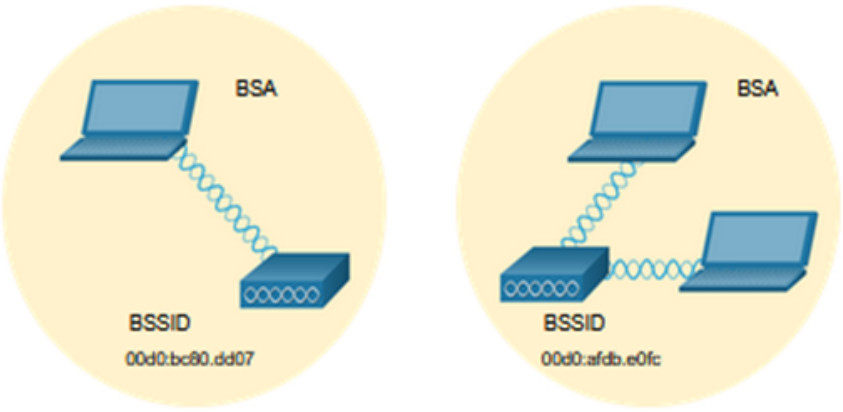


4.1.7 Explain Basic Service Set (BSS) and an Extended Service Set (ESS)

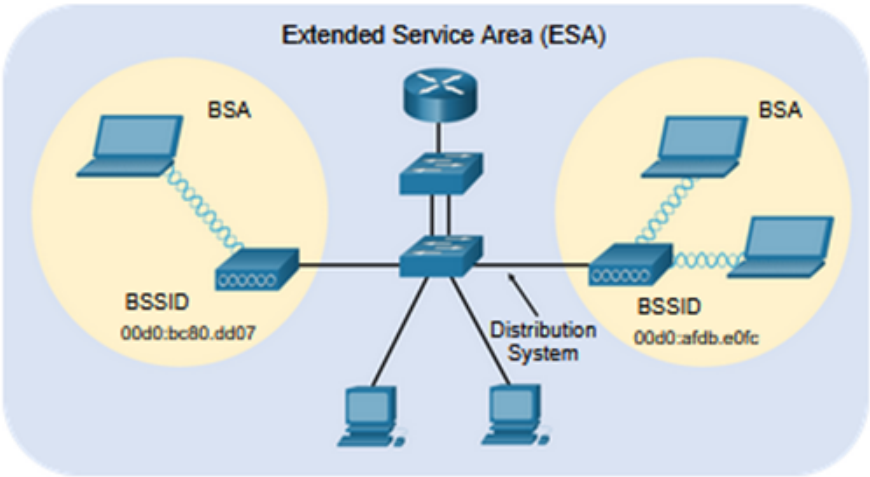
WLANs Operation
BSS and ESS



- Infrastructure mode defines two topology blocks:
  1. Basic Service Set (BSS)
     - Uses single AP to interconnect all associated wireless clients.
     - Clients in different BSSs cannot communicate.

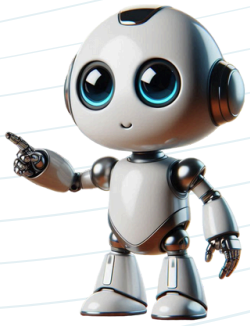


2. Extended Service Set (ESS)
   - A union of two or more BSSs interconnected by a wired distribution system.
   - Clients in each BSS can communication through the ESS.



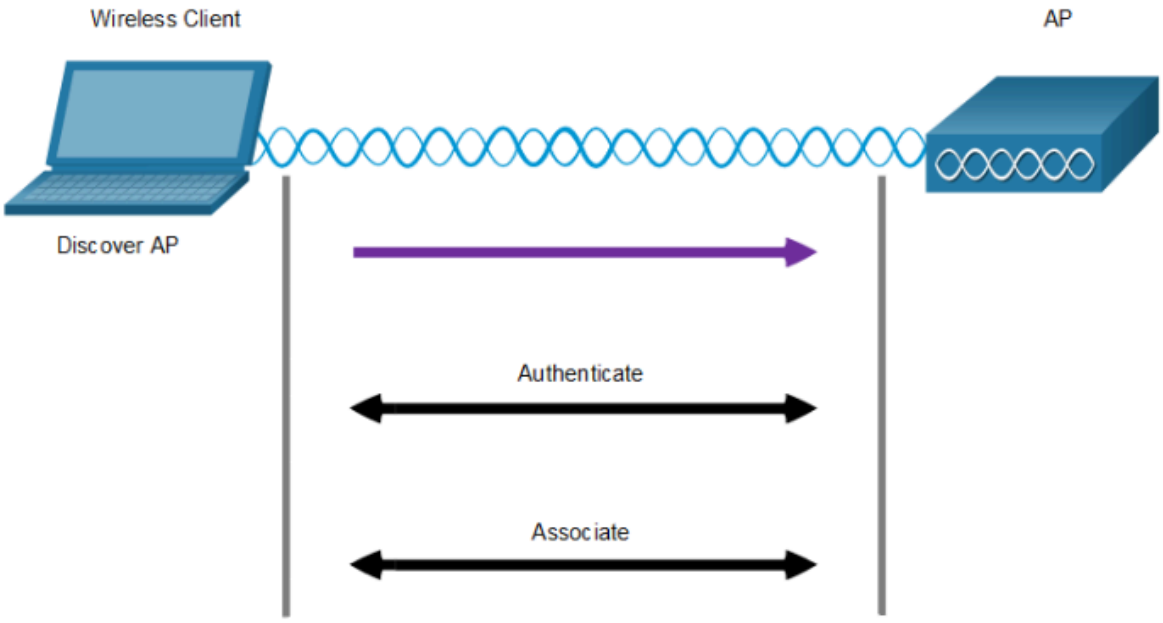
4.1.7 Explain Basic Service Set (BSS) and an Extended Service Set (ESS)

WLANs Operation
Wireless Client and AP Association



- For wireless devices to communicate over a network, they must first associate with an AP or wireless router.

- Wireless devices complete the following three stage process:
  - Discover a wireless AP
  - Authenticate with the AP
  - Associate with the AP



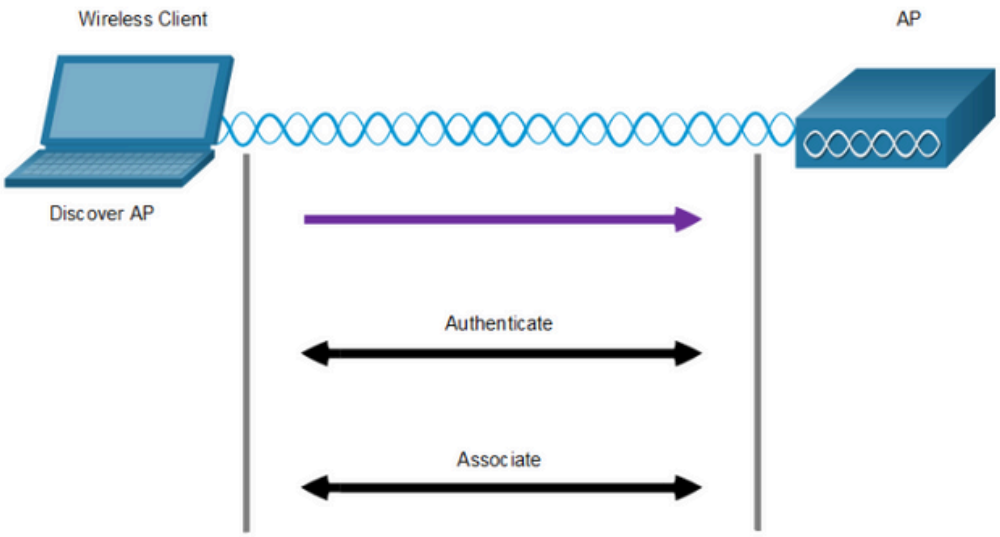
4.1.7 Explain Basic Service Set (BSS) and an Extended Service Set (ESS)

WLANs Operation
Wireless Client and AP Association

- For wireless devices to communicate over a network, they must first associate with an AP or wireless router.

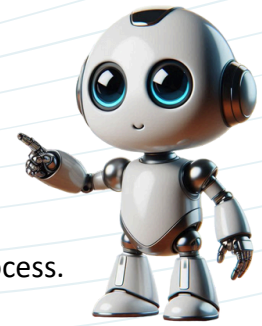
- Wireless devices complete the following three stage process:
  - Discover a wireless AP
  - Authenticate with the AP
  - Associate with the AP

- To achieve successful association, a wireless client and an AP must agree on specific parameters:
  - SSID – The client needs to know the name of the network to connect.
  - Password – This is required for the client to authenticate to the AP.oNetwork mode – The 802.11 standard in use.
  - Security mode – The security parameter settings, i.e. WEP, WPA, or WPA2.
  - Channel settings – The frequency bands in use.



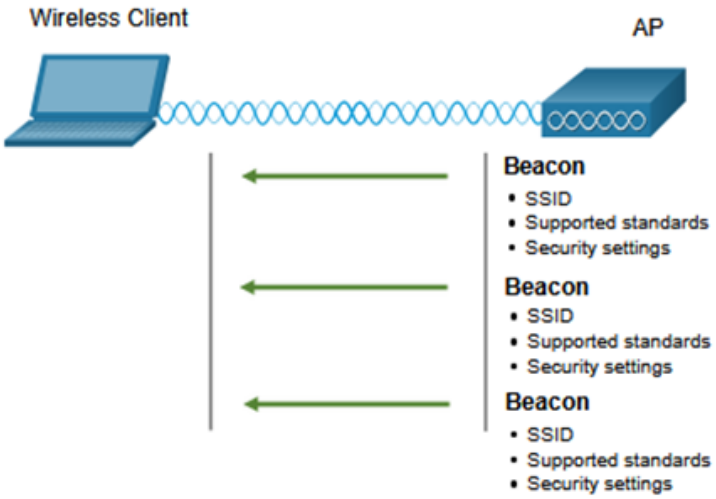
4.1.7 Explain Basic Service Set (BSS) and an Extended Service Set (ESS)

WLANs Operation
Passive and Active Discover Modes

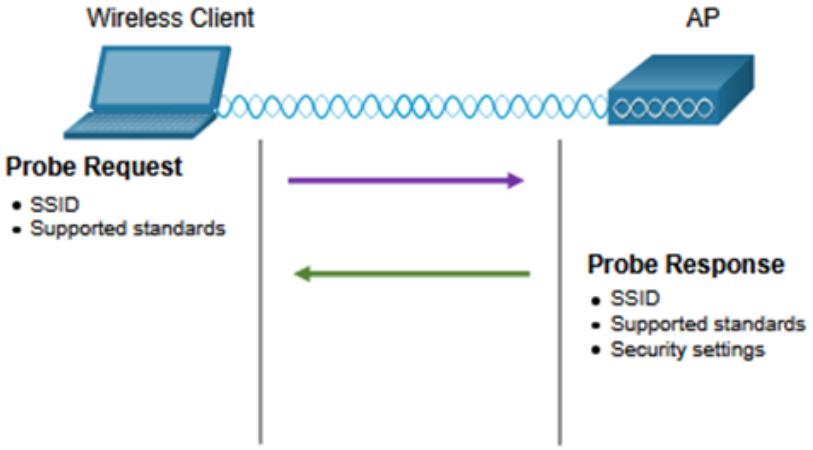


Wireless clients connect to the AP using a passive or active scanning (probing) process.

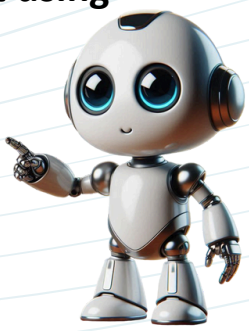
•**Passive mode** – AP openly advertises its service by periodically sending broadcast beacon frames containing the SSID, supported standards, and security settings.



•**Active mode** – Wireless clients must know the name of the SSID. The wireless client initiates the process by broadcasting a probe request frame on multiple channels.



4.2.1 Configure Service Set Identifier (SSID) on an Access Point using the GUI interface



Channel Management
Frequency Channel Saturation

If the demand for a specific wireless channel is too high, the channel may become oversaturated, degrading the quality of the communication.

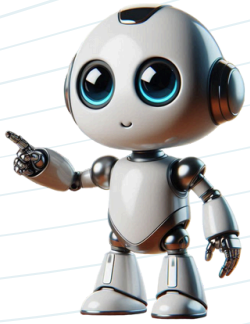
Channel saturation can be mitigated using techniques that use the channels more efficiently.

- Direct-Sequence Spread Spectrum (DSSS) - A modulation technique designed to spread a signal over a larger frequency band. Used by 802.11b devices to avoid interference from other devices using the same 2.4 GHz frequency.

- Frequency-Hopping Spread Spectrum (FHSS) - Transmits radio signals by rapidly switching a carrier signal among many frequency channels. Sender and receiver must be synchronized to “know” which channel to jump to. Used by the original 802.11 standard.

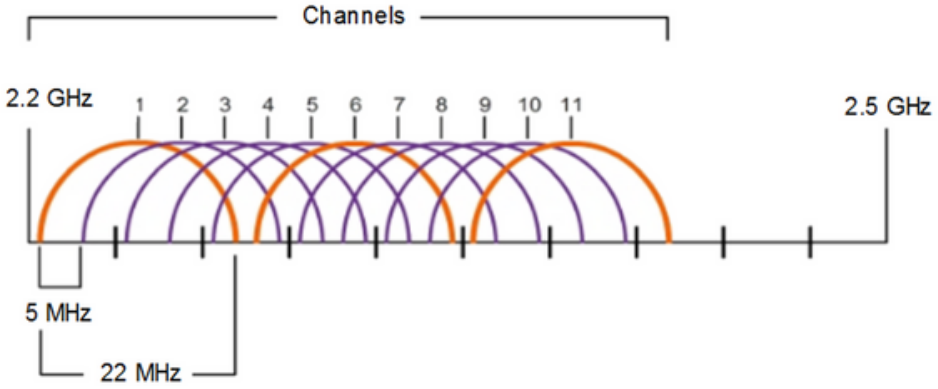
- Orthogonal Frequency-Division Multiplexing (OFDM) - A subset of frequency division multiplexing in which a single channel uses multiple sub-channels on adjacent frequencies. OFDM is used by a number of communication systems including 802.11a/g/n/ac.

4.2.1 Configure Service Set Identifier (SSID) on an Access Point using the GUI interface

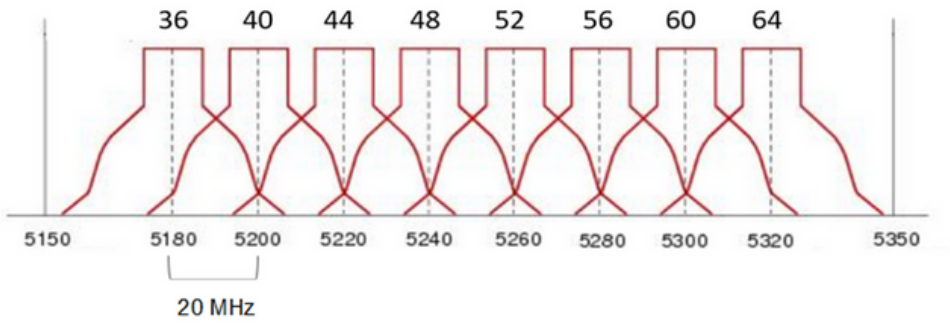


Channel Management
Channel Selection

- The 2.4 GHz band is subdivided into multiple channels each allotted 22 MHz bandwidth and separated from the next channel by 5 MHz.
- A best practice for 802.11b/g/n WLANs requiring multiple APs is to use non-overlapping channels such as 1, 6, and 11.



- For the 5GHz standards 802.11a/n/ac, there are 24 channels. Each channel is separated from the next channel by 20 MHz.
- Non-overlapping channels are 36, 48, and 60.



4.2.2 Configure basic wireless and security setting on an Access Point using the GUI interface

Secure WLANs
SSID Cloaking and MAC Address Filtering

To address the threats of keeping wireless intruders out and protecting data, two early security features were used and are still available on most routers and APs:

1. **SSID Cloaking**

- APs and some wireless routers allow the SSID beacon frame to be disabled. Wireless clients must be manually configured with the SSID to connect to the network.

2. MAC Address Filtering

- An administrator can manually permit or deny clients wireless access based on their physical MAC hardware address. In the figure, the router is configured to permit two MAC addresses. Devices with different MAC addresses will not be able to join the 2.4GHz WLAN.

.

4.2.2 Configure basic wireless and security setting on an Access Point using the GUI interface

Secure WLANs
802.11 Original Authentication Methods

The best way to secure a wireless network is to use authentication and encryption systems. Two types of authentication were introduced with the original 802.11 standard:

1. **Open system authentication**
   - No password required. Typically used to provide free internet access in public areas like cafes, airports, and hotels.

Client is responsible for providing security such as through a VPN.

2. **Shared key authentication**
   - Provides mechanisms, such as WEP, WPA, WPA2, and WPA3 to authenticate and encrypt data between a wireless client and AP. However, the password must be pre-shared between both parties to connect.

4.2.2 Configure basic wireless and security setting on an Access Point using the GUI interface

Secure WLANs
Shared Key Authentication Methods

There are currently four shared key authentication techniques available, as shown in the table.

Authentication Method	Description
Wired Equivalent Privacy (WEP)	The original 802.11 specification designed to secure the data using the Rivest Cipher 4 (RC4) encryption method with a static key. WEP is no longer recommended and should never be used.
Wi-Fi Protected Access (WPA)	A Wi-Fi Alliance standard that uses WEP but secures the data with the much stronger Temporal Key Integrity Protocol (TKIP) encryption algorithm. TKIP changes the key for each packet, making it much more difficult to hack.
WPA2	It uses the Advanced Encryption Standard (AES) for encryption. AES is currently considered the strongest encryption protocol.
WPA3	This is the next generation of Wi-Fi security. All WPA3-enabled devices use the latest security methods, disallow outdated legacy protocols, and require the use of Protected Management Frames (PMF).

4.2.2 Configure basic wireless and security setting on an Access Point using the GUI interface

Secure WLANs
Authenticating a Home User

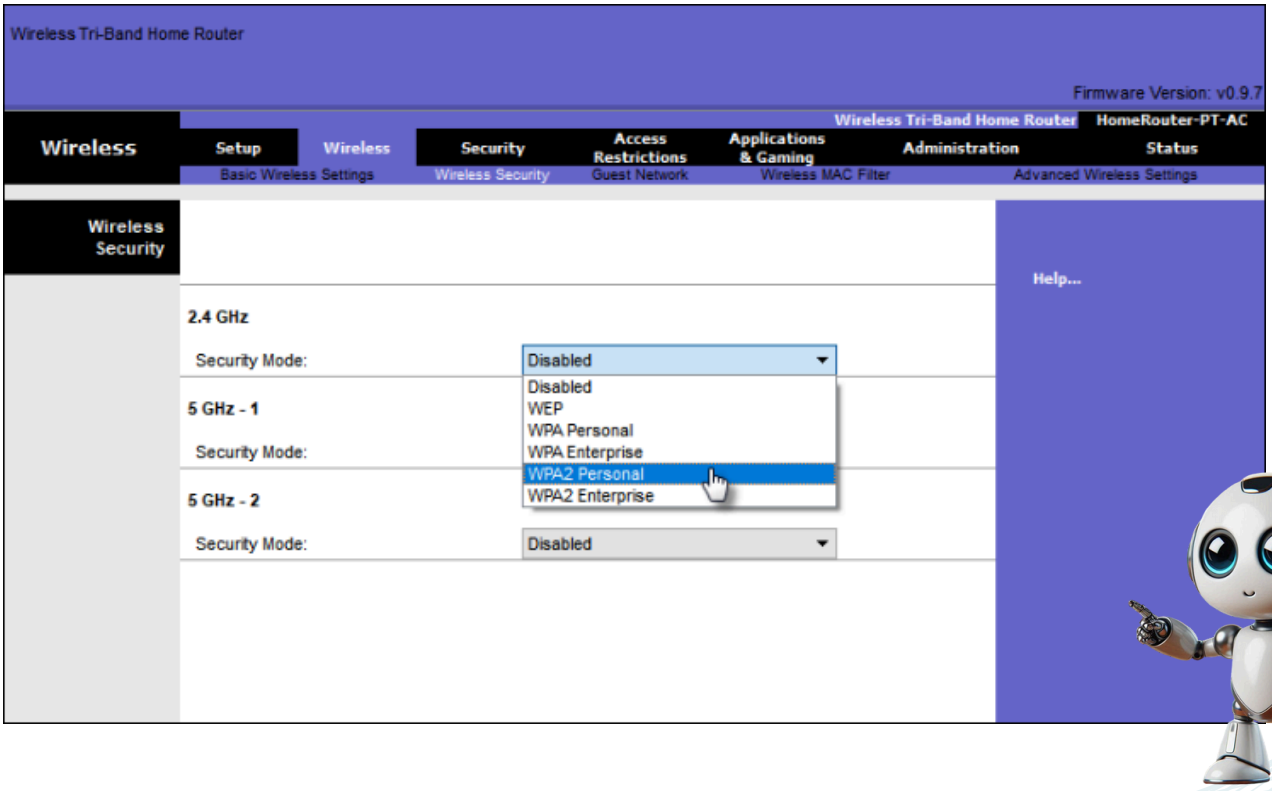
Home routers typically have two choices for authentication: WPA and WPA2, with WPA 2 having two authentication methods.

Personal

– Intended for home or small office networks, users authenticate using a pre-shared key (PSK). Wireless clients authenticate with the wireless router using a pre-shared password. No special authentication server is required.

Enterprise

– Intended for enterprise networks. Requires a Remote Authentication Dial-In User Service (RADIUS) authentication server. The device must be authenticated by the RADIUS server and then users must authenticate using 802.1X standard, which uses the Extensible Authentication Protocol (EAP) for authentication.



4.2.2 Configure basic wireless and security setting on an Access Point using the GUI interface

Secure WLANs Encryption Methods

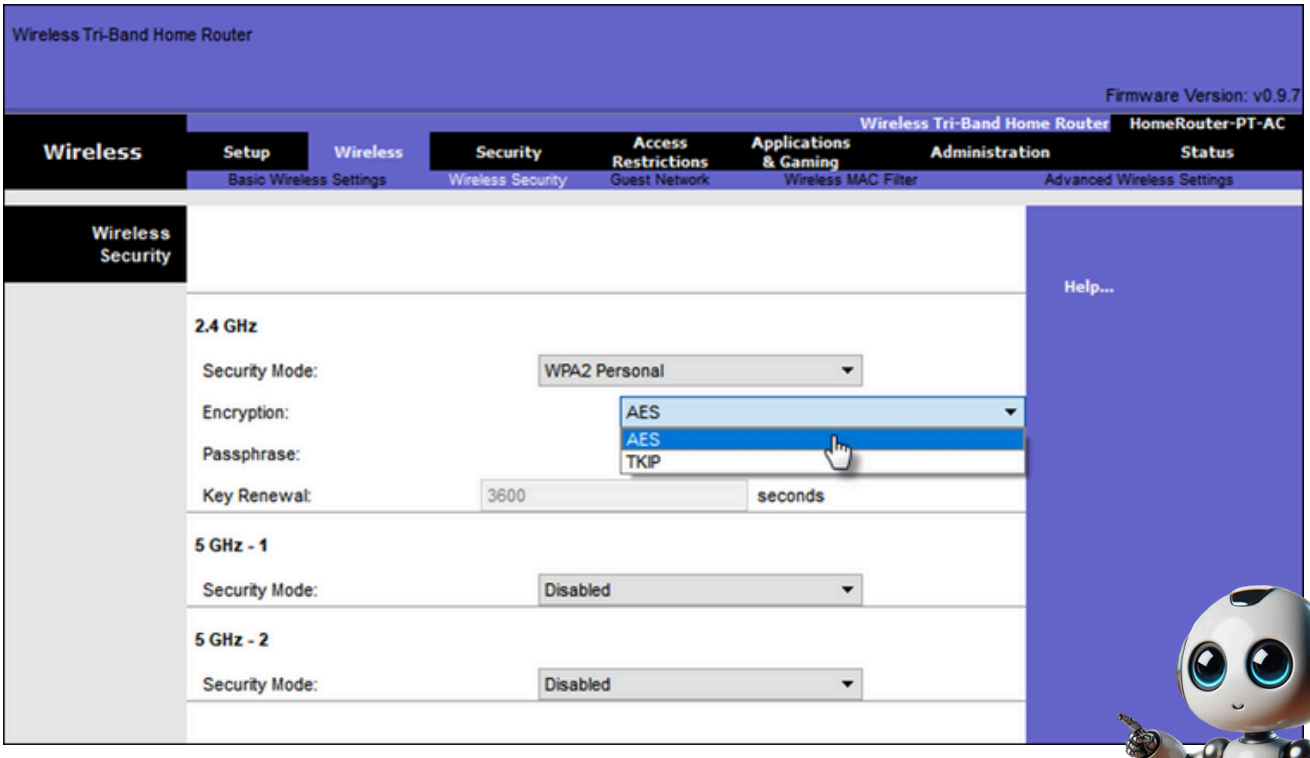
WPA and WPA2 include two encryption protocols:

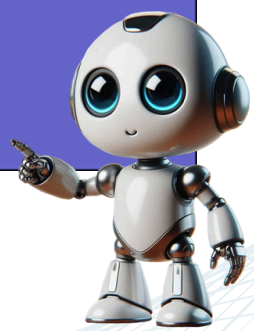
Temporal Key Integrity Protocol (TKIP)

– Used by WPA and provides support for legacy WLAN equipment. Makes use of WEP but encrypts the Layer 2 payload using TKIP.

Advanced Encryption Standard (AES)

– Used by WPA2 and uses the Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP) that allows destination hosts to recognize if the encrypted and non-encrypted bits have been altered.





4.2.2 Configure basic wireless and security setting on an Access Point using the GUI interface

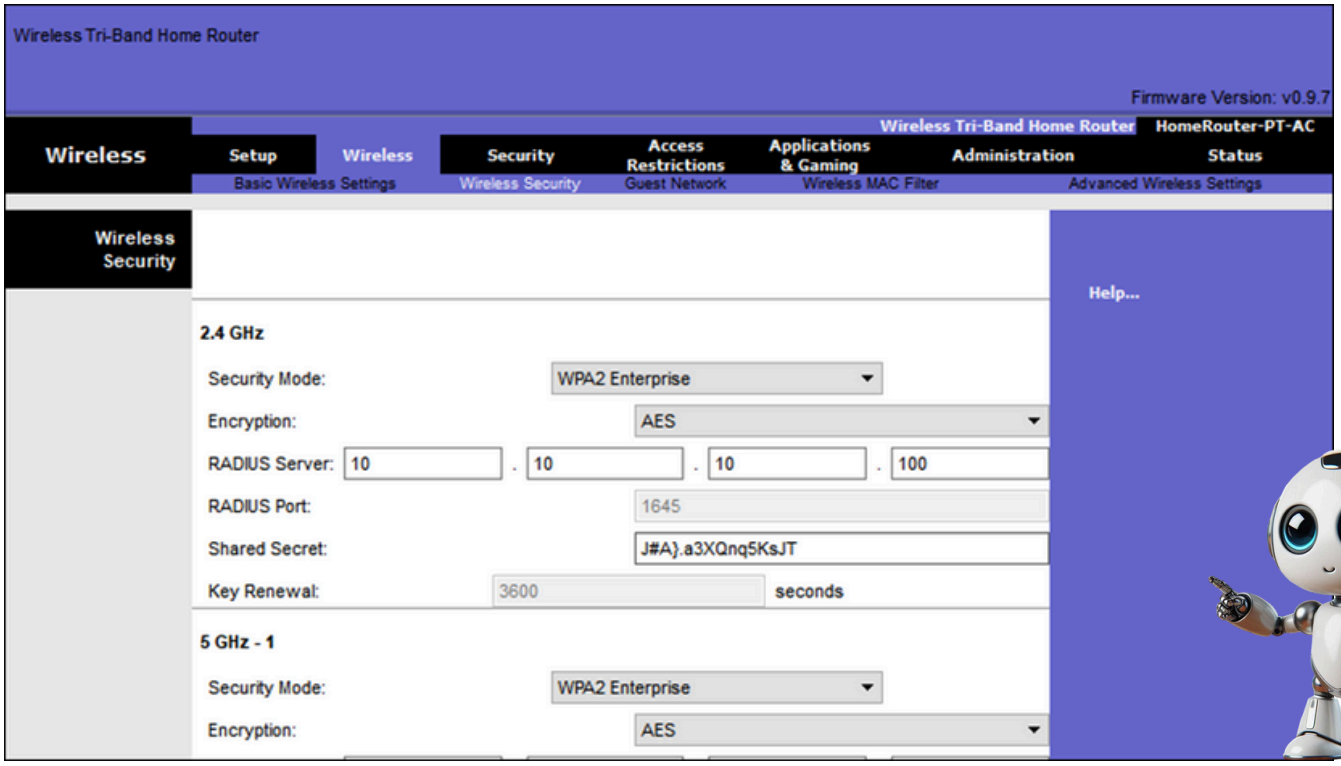
Secure WLANs
Authentication in the Enterprise

Enterprise security mode choice requires an Authentication, Authorization, and Accounting (AAA) RADIUS server. There pieces of information are required:

•RADIUS server IP address
– IP address of the server.

•UDP port numbers
–UDP ports 1812 for RADIUS Authentication, and 1813 for RADIUS Accounting, but can also operate using UDP ports 1645 and 1646.

•Shared key
– Used to authenticate the AP with the RADIUS server.



Note: User authentication and authorization is handled by the 802.1X standard, which provides a centralized, server-based authentication of end users.

4.2.2 Configure basic wireless and security setting on an Access Point using the GUI interface

Secure WLANs
WPA 3

Because WPA2 is no longer considered secure, WPA3 is recommended when available. WPA3 Includes four features:

- **WPA3 – Personal :**

Thwarts brute force attacks by using Simultaneous Authentication of Equals (SAE).

- **WPA3– Enterprise :**

Uses 802.1X/EAP authentication. However, it requires the use of a 192-bit cryptographic suite and eliminates the mixing of security protocols for previous 802.11 standards.

- **Open Networks :**

Does not use any authentication. However, uses Opportunistic Wireless Encryption (OWE) to encrypt all wireless traffic.

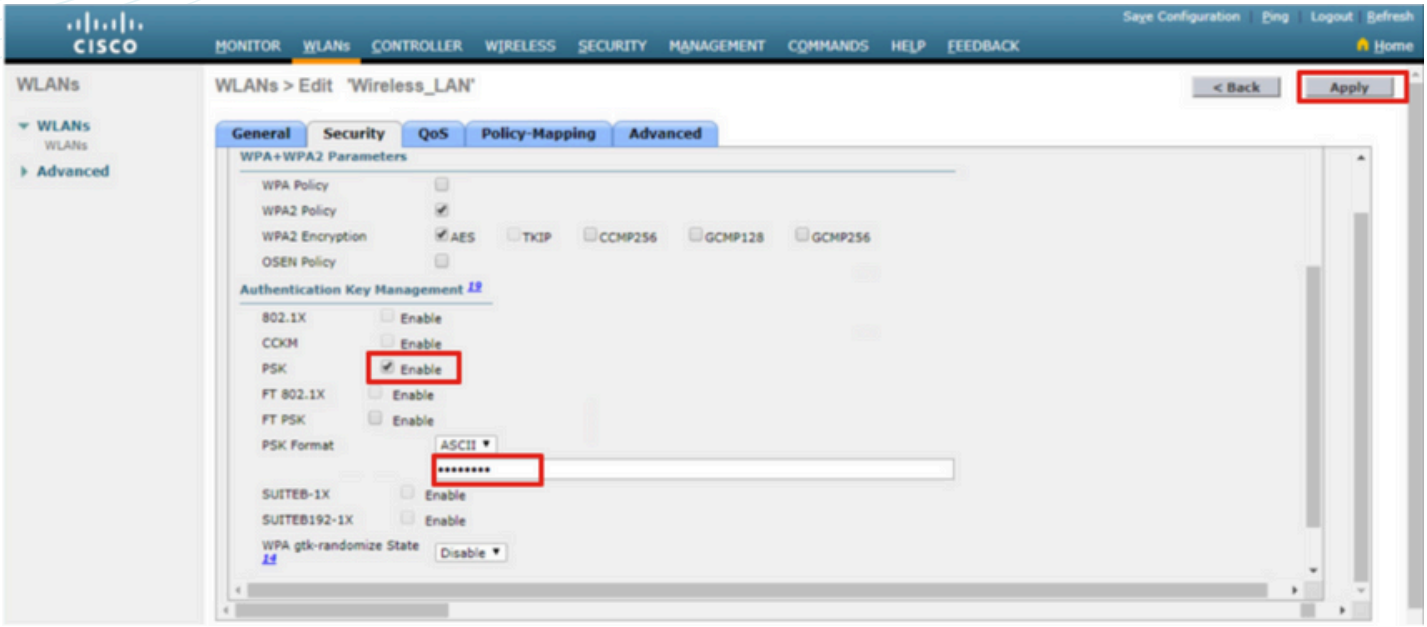
- **IoT Onboarding :**

Uses Device Provisioning Protocol (DPP) to quickly onboard IoT devices.

4.2.2 Configure basic wireless and security setting on an Access Point using the GUI interface

Configure a Basic WLAN
Configure a WLAN

Secure the WLAN:
The Security tab is used to access all the available options for securing the LAN.



05

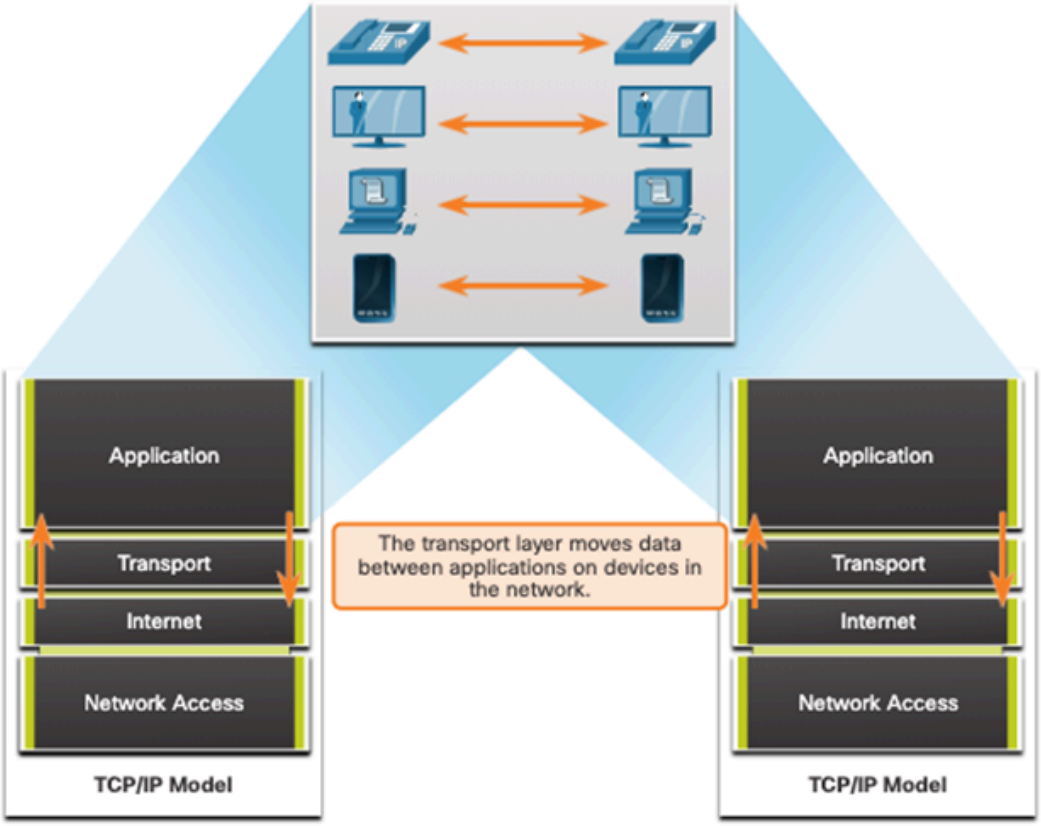
TRANSPORT AND APPLICATION LAYER

5.1.1 Explain transport layer responsibilities and protocols

Transportation of Data
Role of the Transport Layer

The transport layer is:

- Responsible for logical communications between applications running on different hosts.
- The link between the application layer and the lower layers that are responsible for network transmission

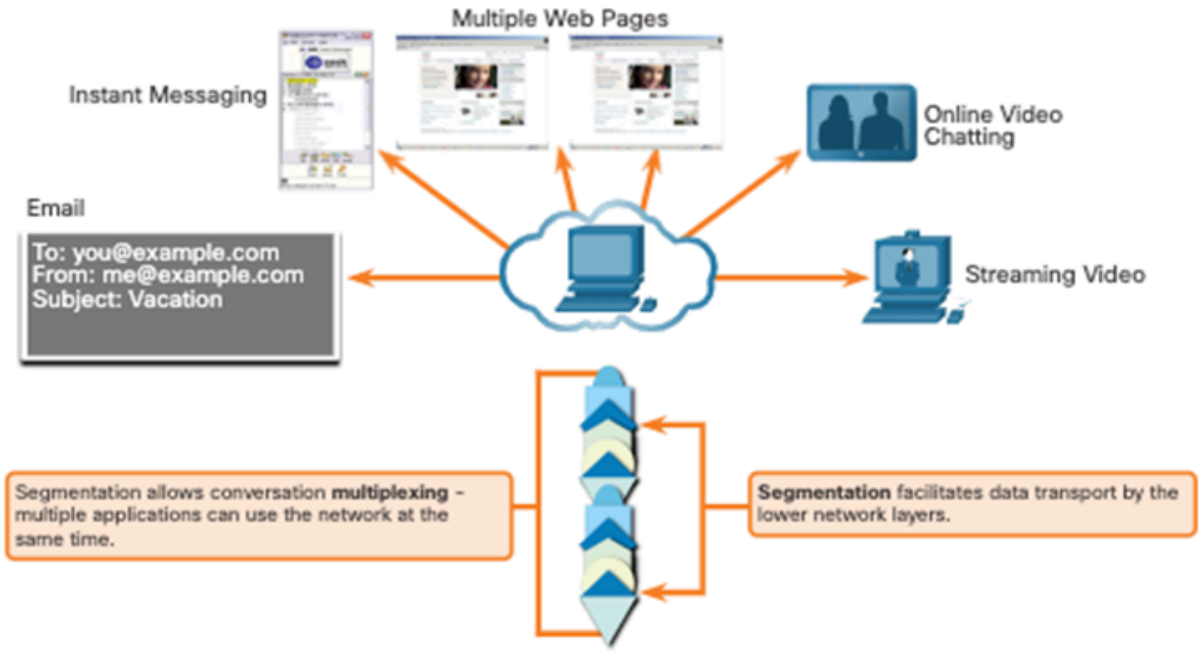


5.1.1 Explain transport layer responsibilities and protocols

Transportation of Data
Transport Layer Responsibilities

The transport layer has the following responsibilities:

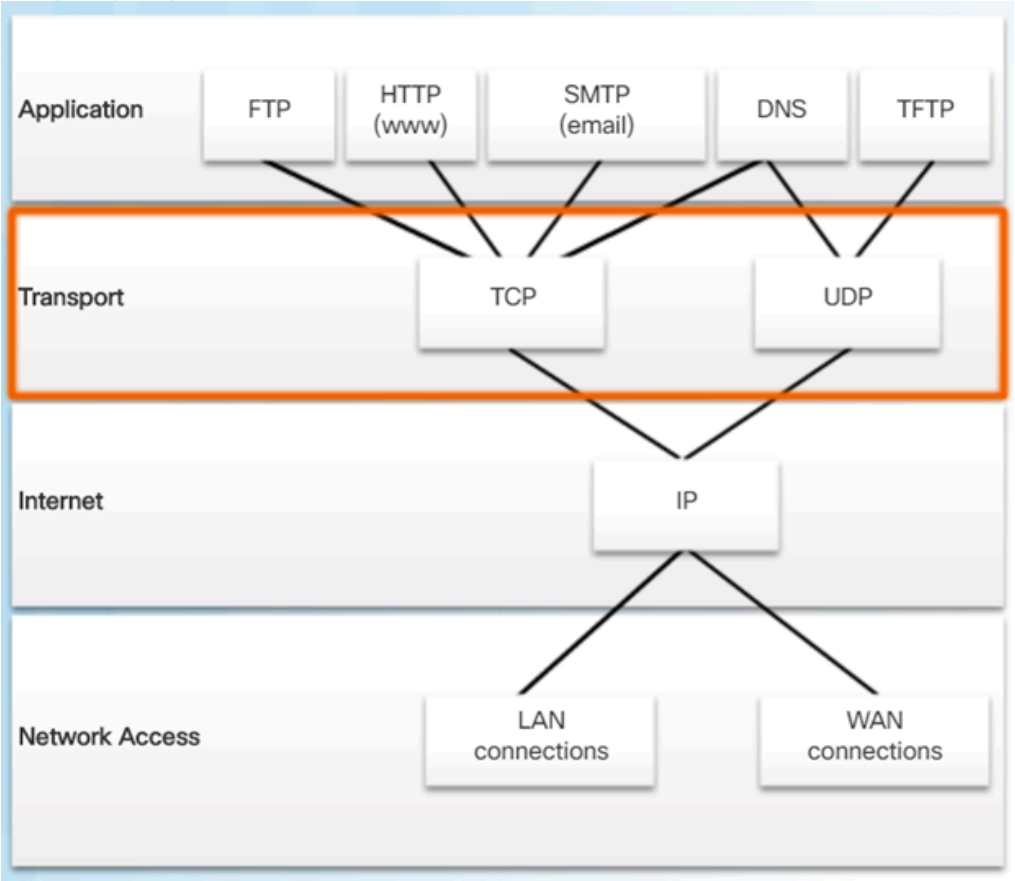
- Tracking individual conversations
- Segmenting data and reassembling segments
- Adds header information
- Identify, separate, and manage multiple conversations
- Uses segmentation and multiplexing to enable different communication conversations to be interleaved on the same network



5.1.2 Differentiate the characteristic of TCP and UDP protocols

Transportation of Data
Transport Layer Protocols

- IP does not specify how the delivery or transportation of the packets takes place.
- Transport layer protocols specify how to transfer messages between hosts, and are responsible for managing reliability requirements of a conversation.
- The transport layer includes the TCP and UDP protocols.

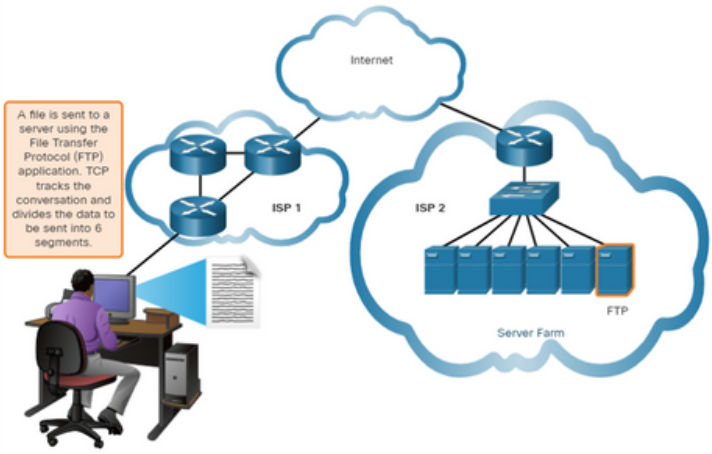


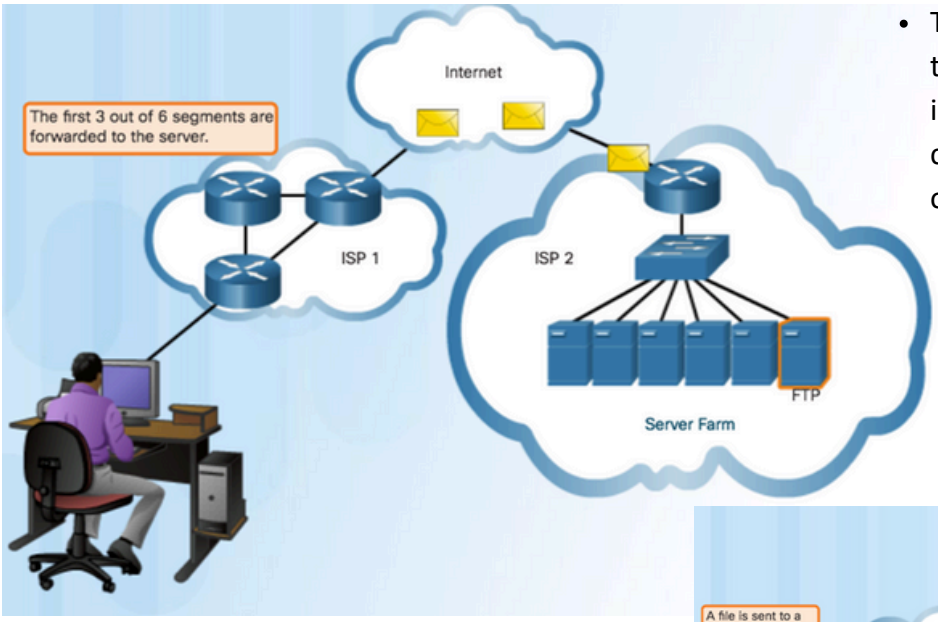
5.1.2 Differentiate the characteristic of TCP and UDP protocols

Transportation of Data
Transmission Control Protocol

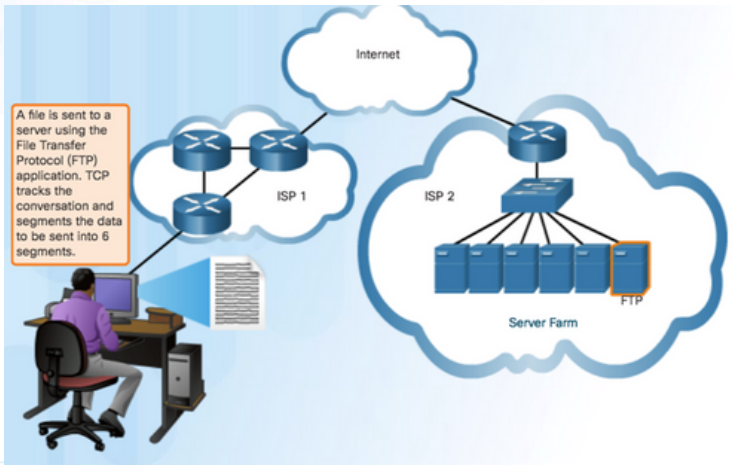
TCP provides reliability and flow control. TCP basic operations:

- Number and track data segments transmitted to a specific host from a specific application
- Acknowledge received data
- Retransmit any unacknowledged data after a certain amount of time
- Sequence data that might arrive in wrong order
- Send data at an efficient rate that is acceptable by the receiver





- TCP transport is similar to sending tracked packages. If a shipping order is broken up into several packages, a customer can check online to see the order of the delivery.

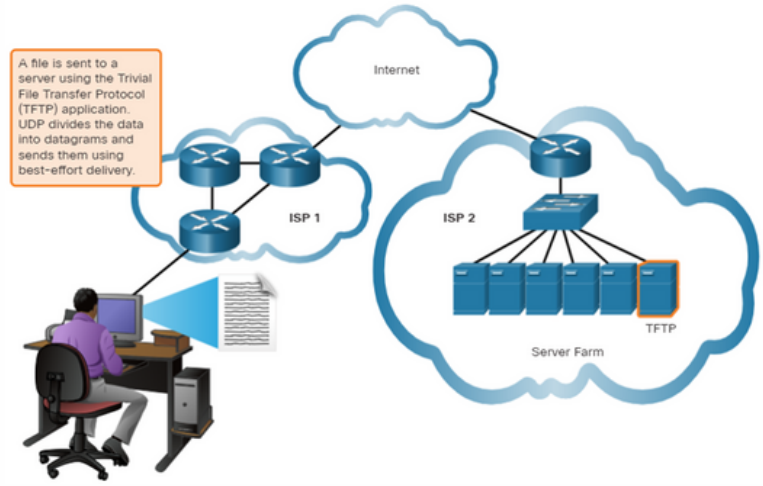


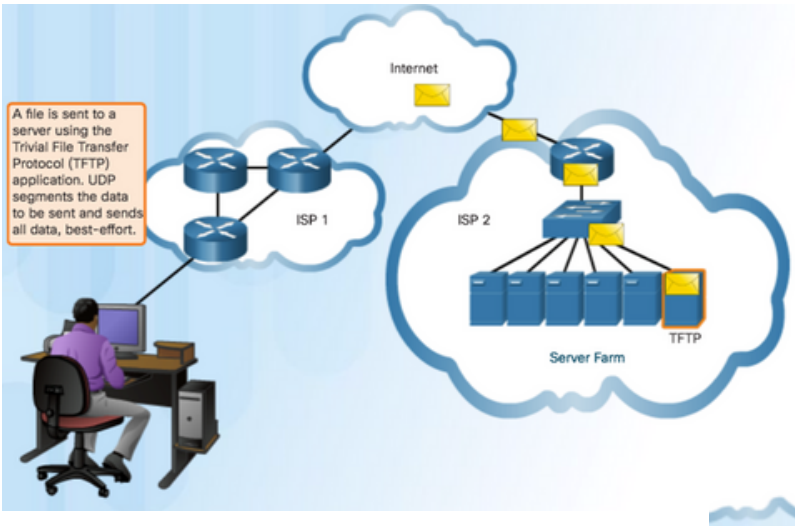
5.1.2 Differentiate the characteristic of TCP and UDP protocols

Transportation of Data
User Datagram Protocol (UDP)

UDP provides the basic functions for delivering datagrams between the appropriate applications, with very little overhead and data checking.

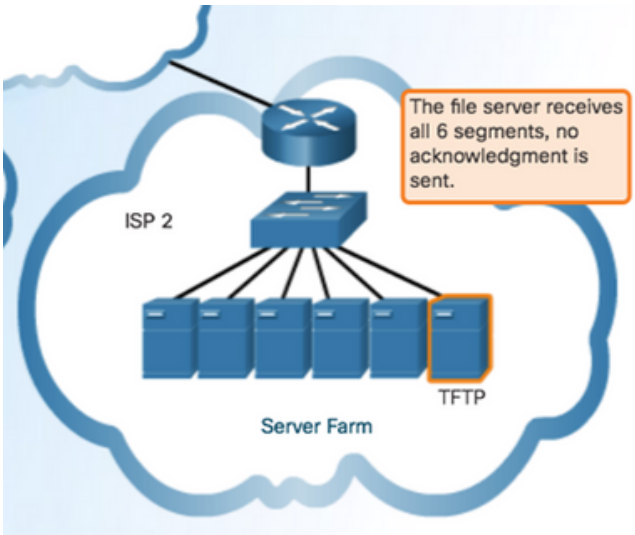
- UDP is a connectionless protocol.
- UDP is known as a best-effort delivery protocol because there is no acknowledgment that the data is received at the destination.





Use UDP for less overhead and to reduce possible delays.

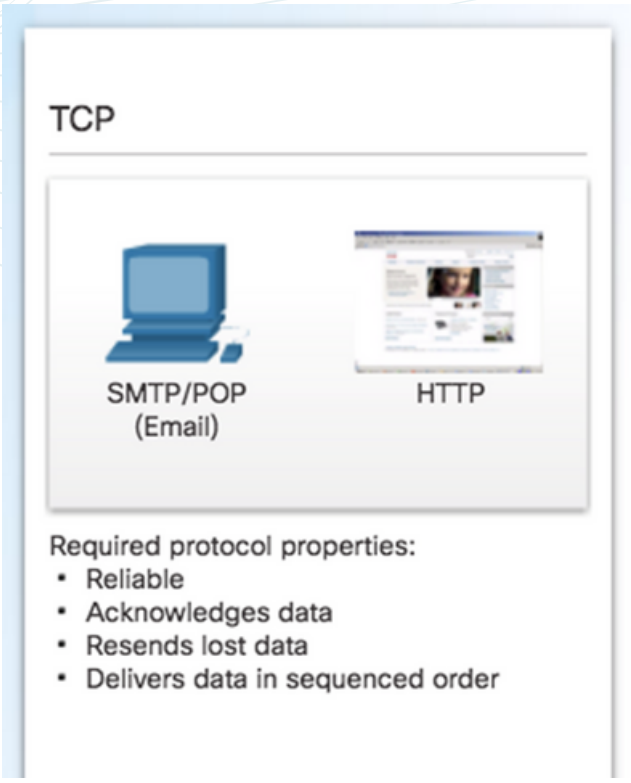
- Best-effort delivery (unreliable)
- No acknowledgment
- Similar to a non-registered

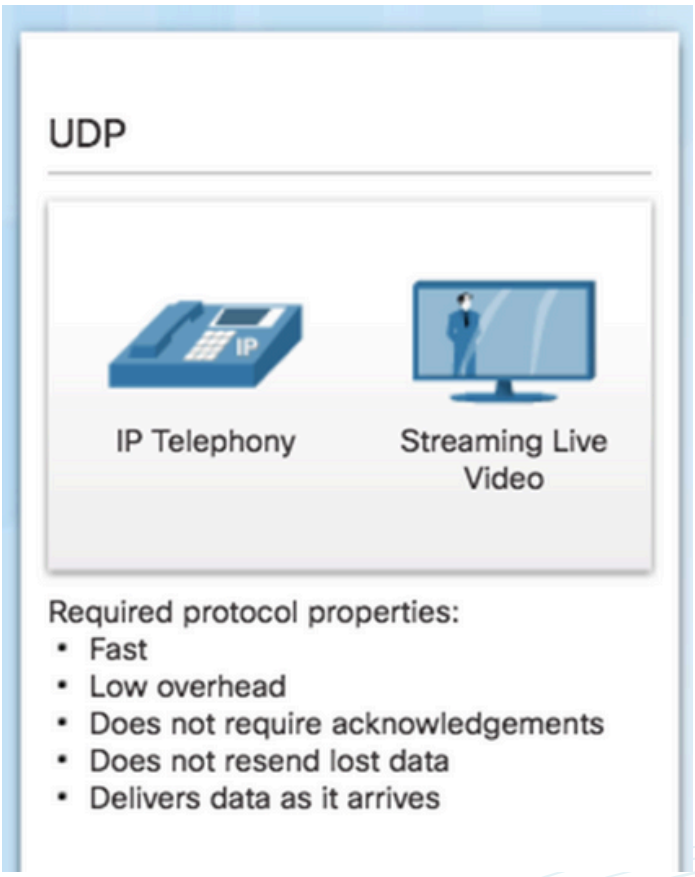


5.1.3 Identify TCP and UDP application

Tansportation of Data
The Right Transport Layer Protocol for the Right Application

- If it is important that all the data arrives and that it can be processed in its proper sequence, TCP is used as the transport protocol.
- **TCP** - databases, web browsers, and email clients require that all data that is sent arrives at the destination in its original condition.





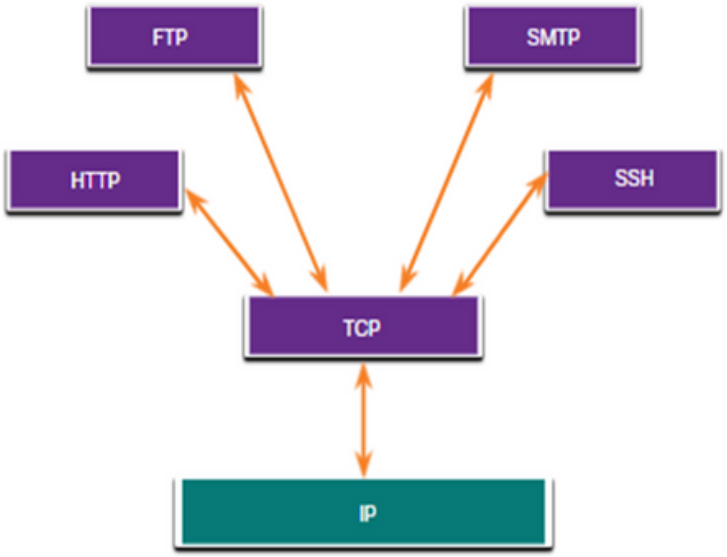
- **UDP** is also used by request-and-reply applications where the data is minimal, and retransmission can be done quickly.
- **UDP** - if one or two segments of a live video stream fail to arrive, if disruption in the stream, may not be noticeable to the user.

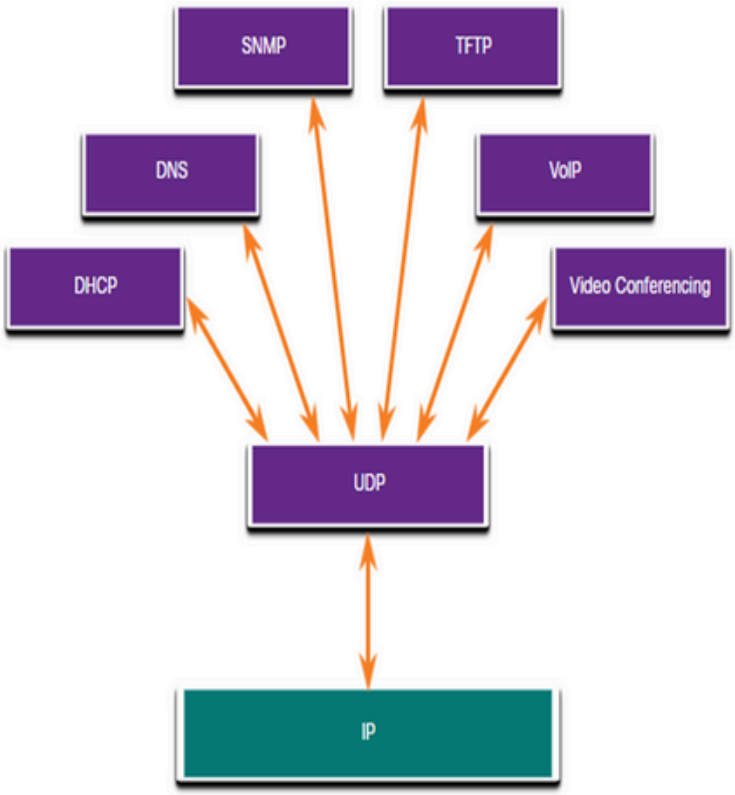
5.1.3 Identify TCP and UDP application

Tansportation of Data
The Right Transport Layer Protocol for the Right Application

Applications that use TCP

- TCP handles all tasks associated with dividing the data stream into segments, providing reliability, controlling data flow, and reordering segments.





Applications that use UDP

- Live video and multimedia applications - These applications can tolerate some data loss but require little or no delay. Examples include VoIP and live streaming video.
- Simple request and reply applications - Applications with simple transactions where a host sends a request and may or may not receive a reply. Examples include DNS and DHCP.
- Applications that handle reliability themselves - Unidirectional communications where flow control, error detection, acknowledgments, and error recovery is not required, or can be handled by the application. Examples include SNMP and TFTP.

5.1.4 Explain port number groups

TCP Overview: TCP Features

- **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.

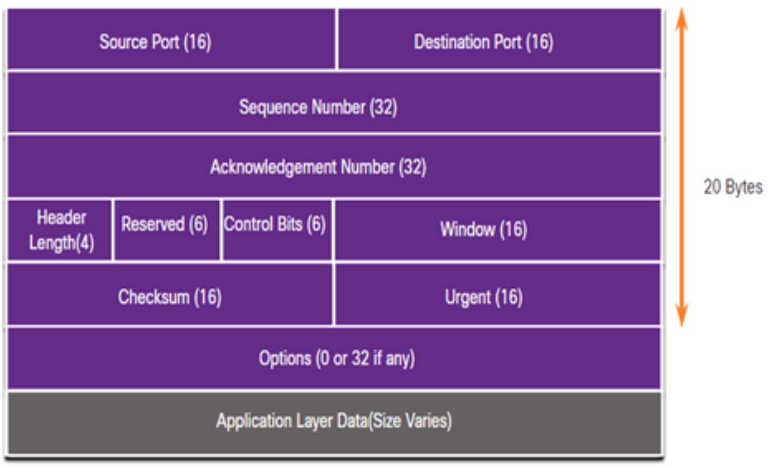
- **Ensures Reliable Delivery**
  - For many reasons, it is possible for a segment to become corrupted or lost completely, as it is transmitted over the network. TCP ensures that each segment that is sent by the source arrives at the destination.

- **Provides Same**
  - Order Delivery - Because networks may provide multiple routes that can have different transmission rates, data can arrive in the wrong order.

- **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.

TCP Overview: TCP Header

- TCP is a stateful protocol which means it keeps track of the state of the communication session.
- TCP records which information it has sent, and which information has been acknowledged.



5.1.4 Explain port number groups

TCP Overview: UDP Header

TCP Header Field	Description
Source Port	A 16-bit field used to identify the source application by port number.
Destination Port	A 16-bit field used to identify the destination application by port number.
Sequence Number	A 32-bit field used for data reassembly purposes.
Acknowledgment Number	A 32-bit field used to indicate that data has been received and the next byte expected from the source.
Header Length	A 4-bit field known as "data offset" that indicates the length of the TCP segment header.
Reserved	A 6-bit field that is reserved for future use.
Control bits	A 6-bit field used that includes bit codes, or flags, which indicate the purpose and function of the TCP segment.
Window size	A 16-bit field used to indicate the number of bytes that can be accepted at one time.
Checksum	A 16-bit field used for error checking of the segment header and data.
Urgent	A 16-bit field used to indicate if the contained data is urgent.

TCP Overview: UDP Features

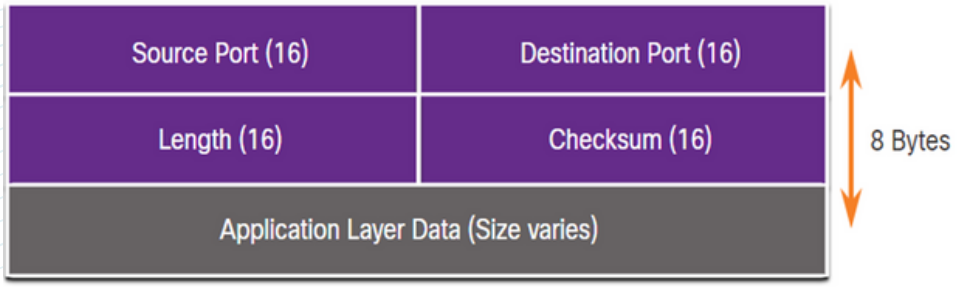
UDP features include the following:

- Data is reconstructed in the order that it is received.
- Any segments that are lost are not resent.
- There is no session establishment.
- The sending is not informed about resource availability.

5.1.4 Explain port number groups

TCP Overview: UDP Header

The UDP header is far simpler than the TCP header because it only has four fields and requires 8 bytes (i.e. 64 bits).



TCP Overview: UDP Header Fields

The table identifies and describes the four fields in a UDP header

UDP Header Field	Description
Source Port	A 16-bit field used to identify the source application by port number.
Destination Port	A 16-bit field used to identify the destination application by port number.
Length	A 16-bit field that indicates the length of the UDP datagram header.
Checksum	A 16-bit field used for error checking of the datagram header and data.

5.1.4 Explain port number groups

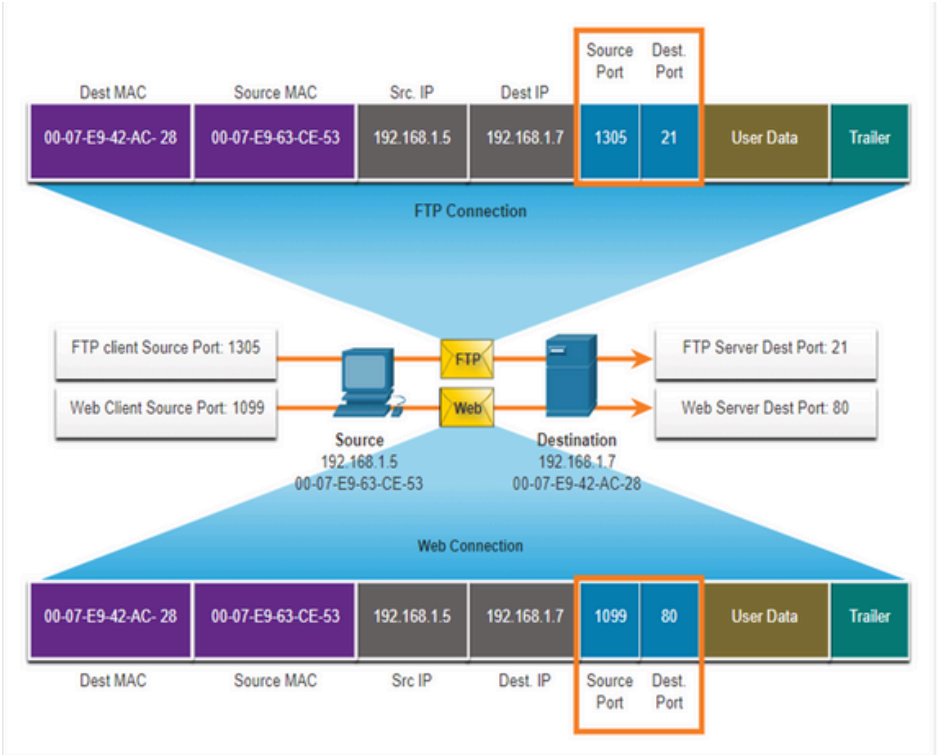
Port Numbers : Multiple Separate Communications

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

The source port number is associated with the originating application on the local host whereas the destination port number is associated with the destination application on the remote host.

Port numbers : Socket Pairs

- Source and destination port placed in segment
- Segments encapsulated in IP packet
- IP and port number = socket
- Example: 192.168.1.7:80
- Sockets enable multiple processes to be distinguished
- Source port acts as a return address

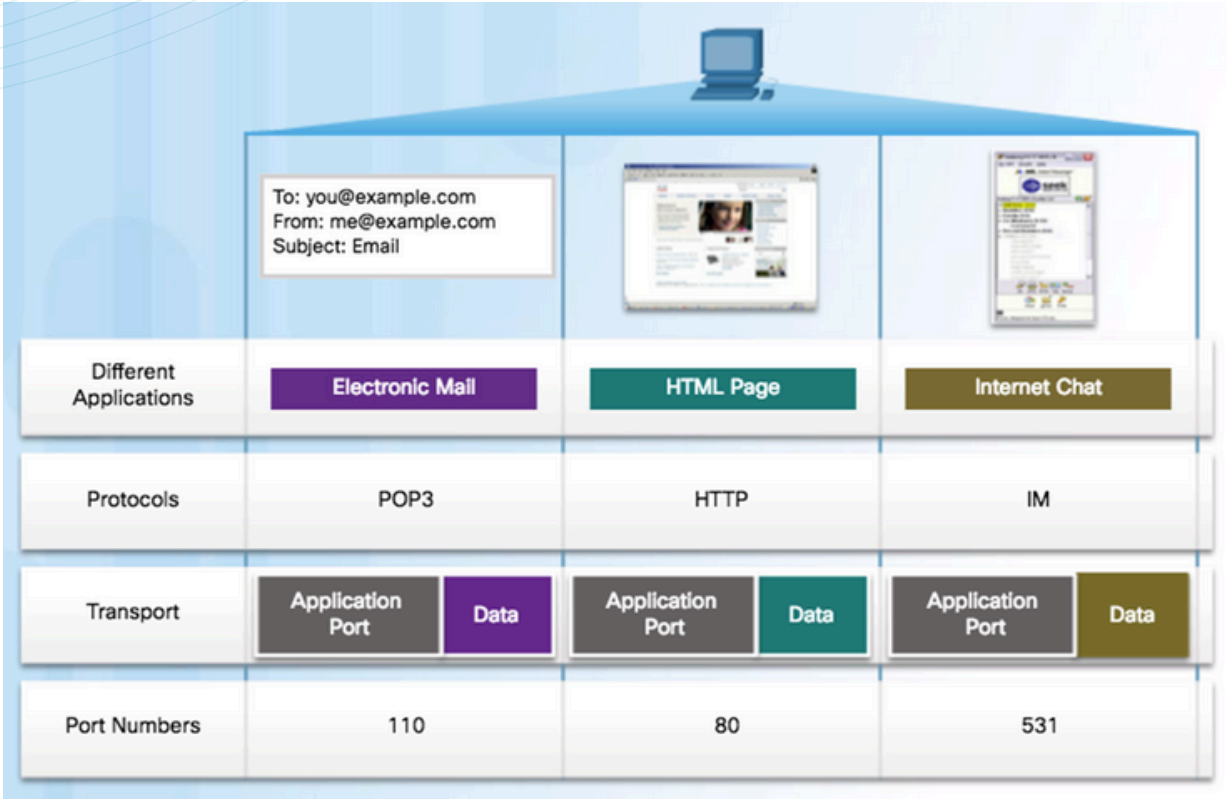


5.1.4 Explain port number groups

Port Numbers : Port Numbers

- Source Port
  - Originating application port that is dynamically generated by sending device
  - Example: Each separate HTTP conversation is tracked based on the source ports.

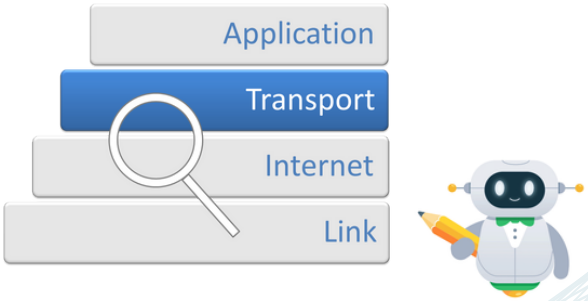
- Destination Port
  - Tell the destination what service is being requested
  - Example: Port 80 web services are being requested



5.1.4 Explain port number groups

Port Numbers : Port Number Groups

Port Group	Number 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 communication.



5.1.4 Explain port number groups

Port Numbers : Port Number Groups

Port Number	Protocol	Application
20	TCP	File Transfer Protocol (FTP) - Data
21	TCP	File Transfer Protocol (FTP) - Control
22	TCP	Secure Shell (SSH)
23	TCP	Telnet
25	TCP	Simple Mail Transfer Protocol (SMTP)
53	UDP, TCP	Domain Name Service (DNS)
67	UDP	Dynamic Host Configuration Protocol (DHCP) - Server
68	UDP	Dynamic Host Configuration Protocol - Client
69	UDP	Trivial File Transfer Protocol (TFTP)
80	TCP	Hypertext Transfer Protocol (HTTP)
110	TCP	Post Office Protocol version 3 (POP3)
143	TCP	Internet Message Access Protocol (IMAP)
161	UDP	Simple Network Management Protocol (SNMP)
443	TCP	Hypertext Transfer Protocol Secure (HTTPS)

5.1.4 Explain port number groups

Port Numbers :The netstat Command

Unexplained TCP connections can pose a major security threat. Netstat is an important tool to verify connections.

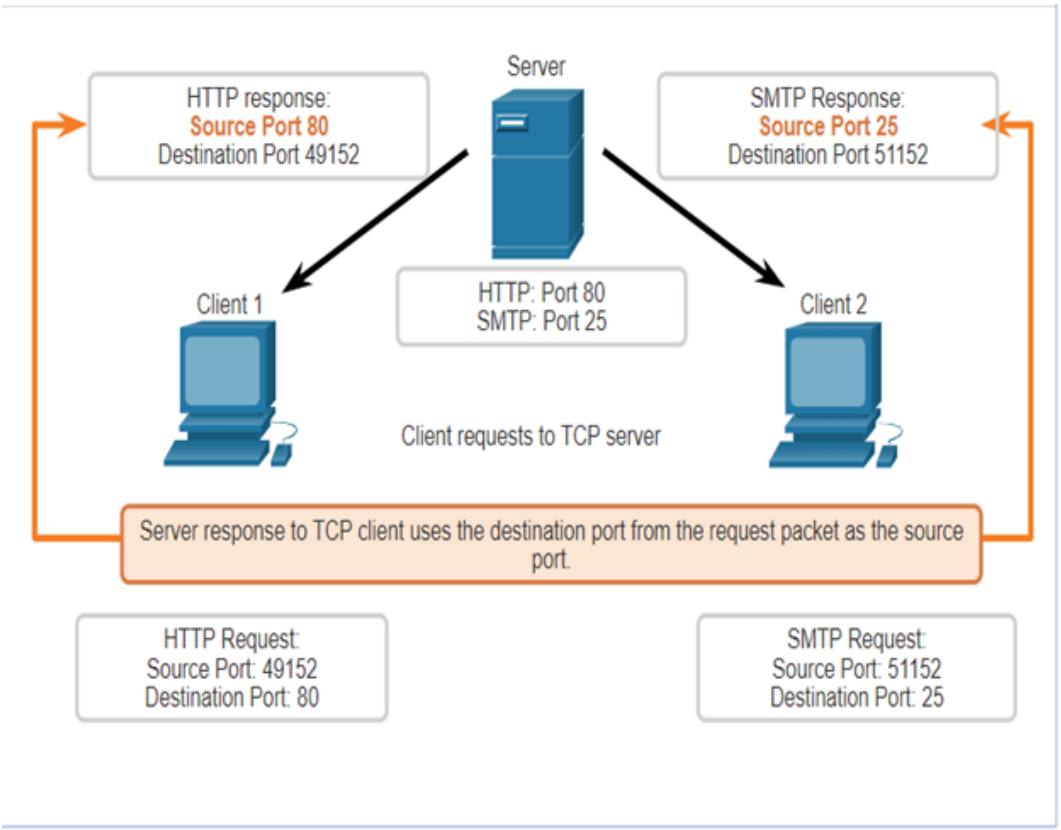
```
C:\> netstat
Active Connections
Proto Local Address                          Foreign Address
                          State
TCP    192.168.1.124:3126             192.168.0.2:netbios-ssn
         ESTABLISHED
TCP    192.168.1.124:3158             207.138.126.152:http
                  ESTABLISHED
TCP    192.168.1.124:3159             207.138.126.169:http
                  ESTABLISHED
TCP    192.168.1.124:3160             207.138.126.169:http
                  ESTABLISHED
TCP    192.168.1.124:3161             sc.msn.com:http
                  ESTABLISHED
TCP    192.168.1.124:3166             www.cisco.com:http
                  ESTABLISHED
```

5.1.5 Explain TCP Three-way Handshake

TCP Communication Process: TCP Server Processes

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

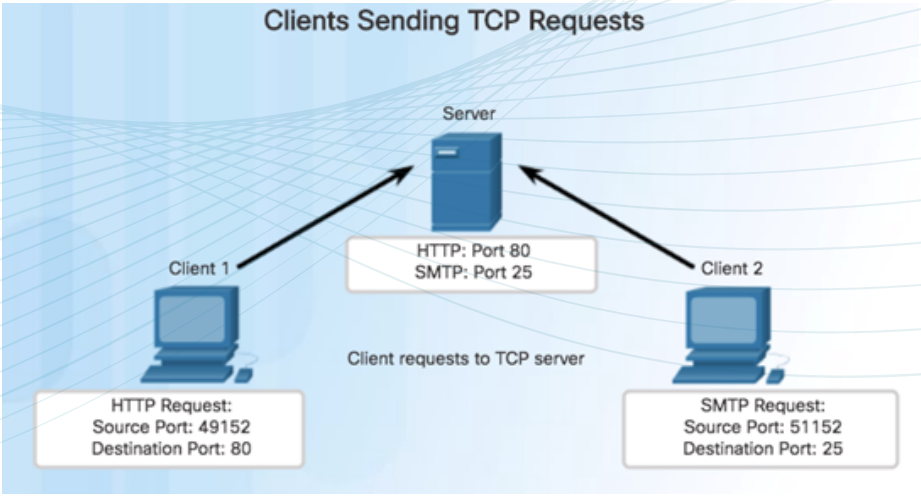
- An individual server cannot have two services assigned to the same port number within the same transport layer services.
- An active server application assigned to a specific port is considered open, which means that the transport layer accepts, and processes segments addressed to that port.
- Any incoming client request addressed to the correct socket is accepted, and the data is passed to the server application.



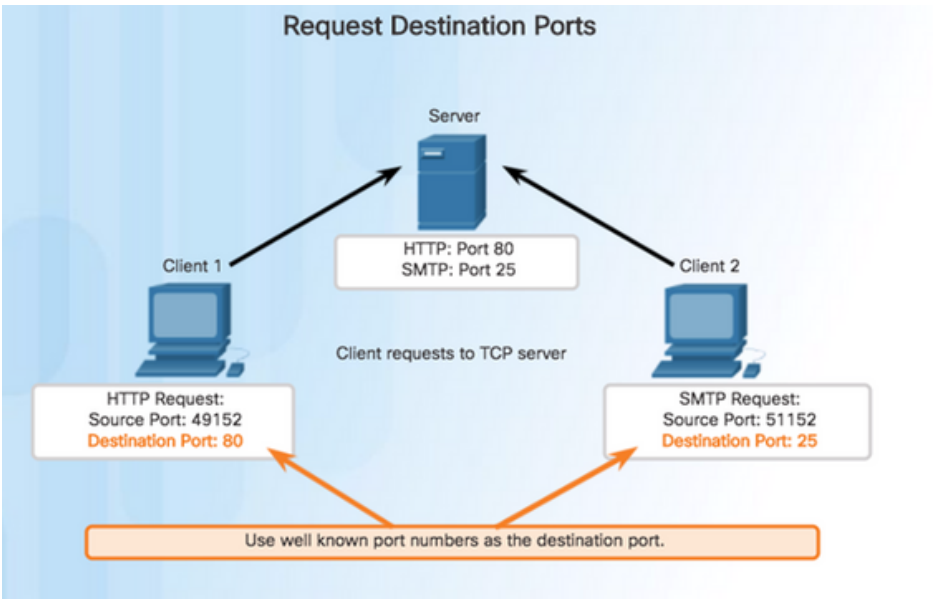
5.1.5 Explain TCP Three-way Handshake

TCP Communication Process: TCP Server Processes

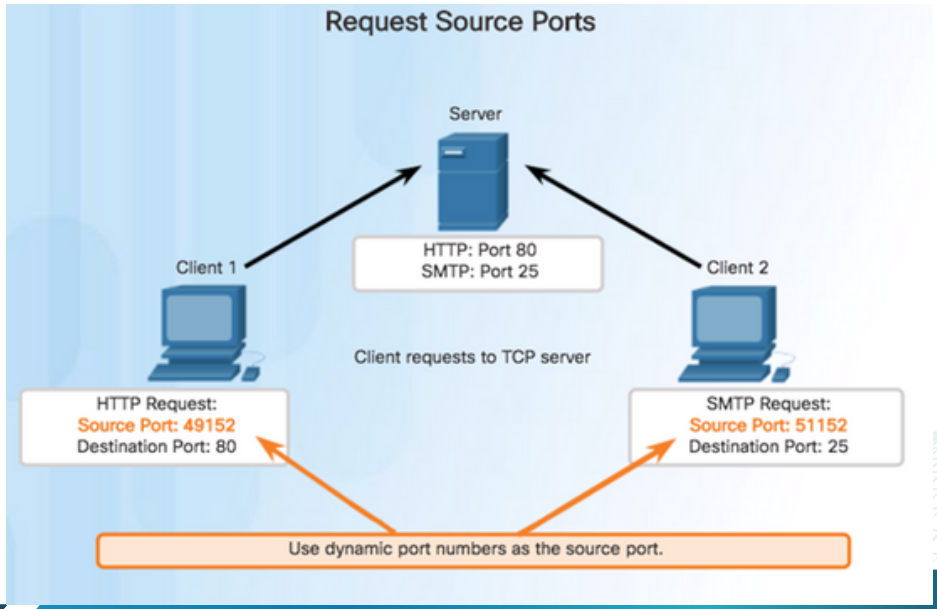
1



2



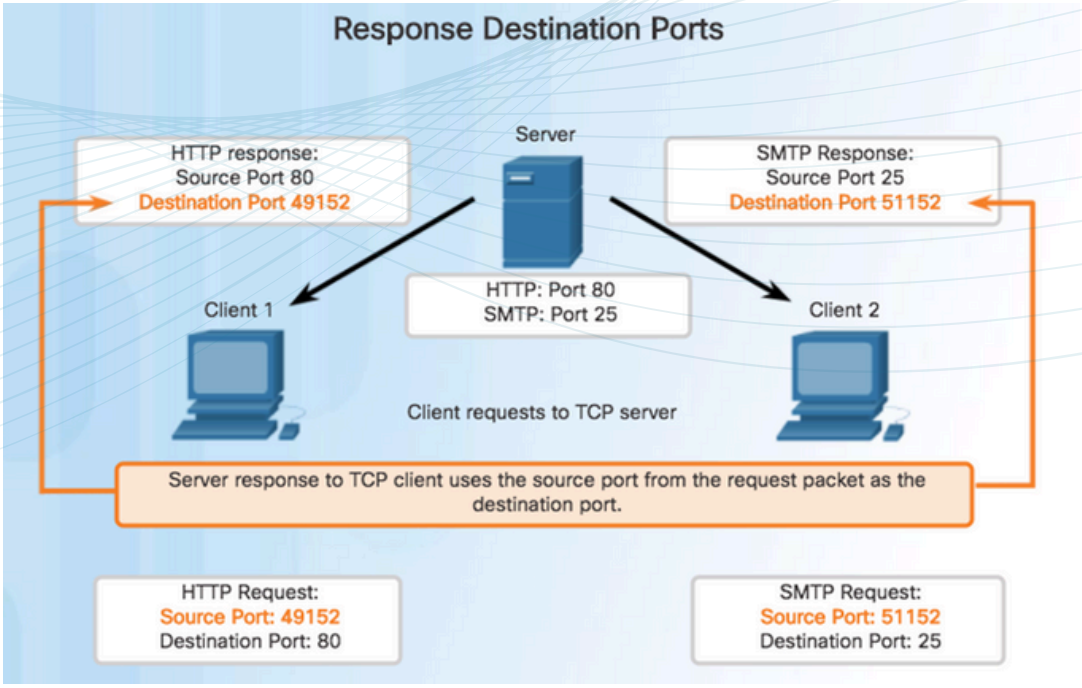
3



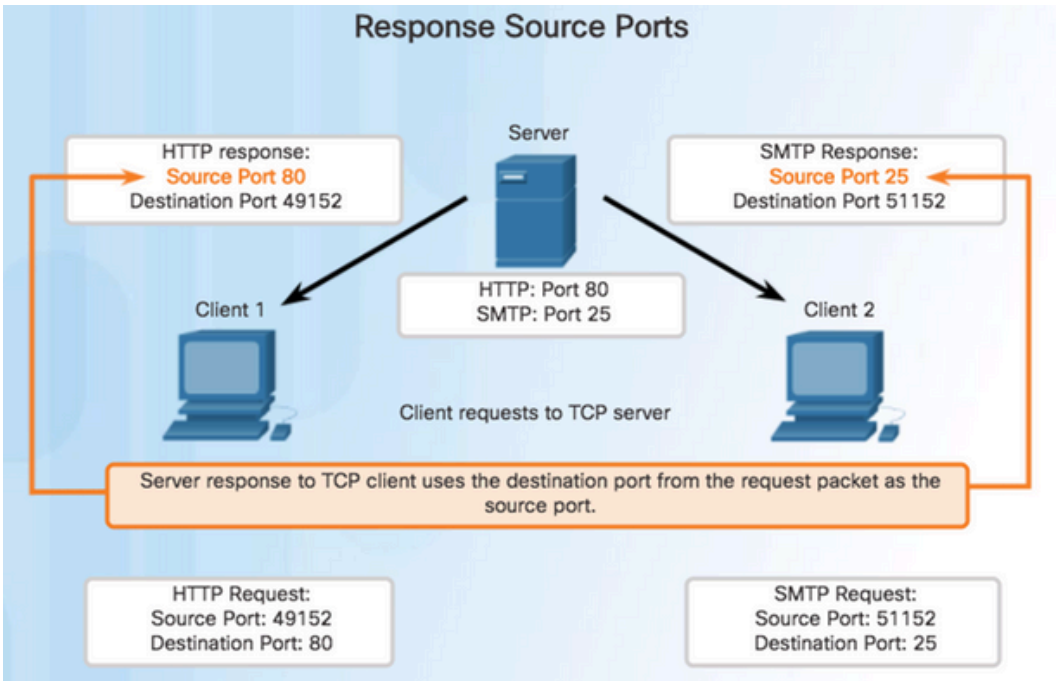
5.1.5 Explain TCP Three-way Handshake

TCP Communication Process: TCP Server Processes

4



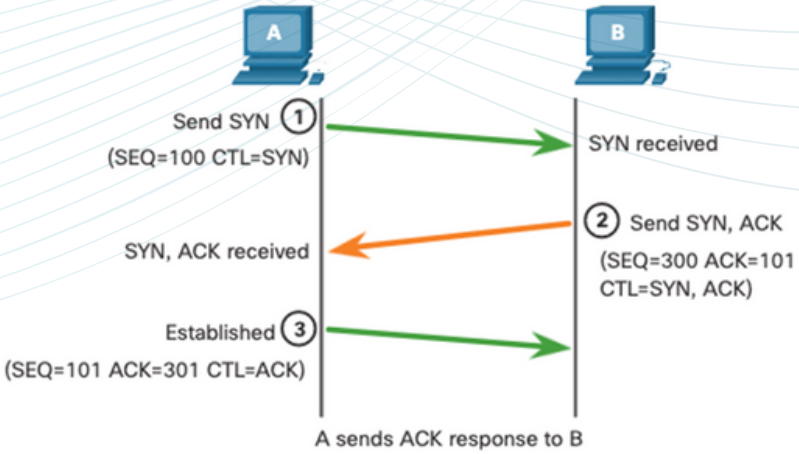
5



5.1.5 Explain TCP Three-way Handshake

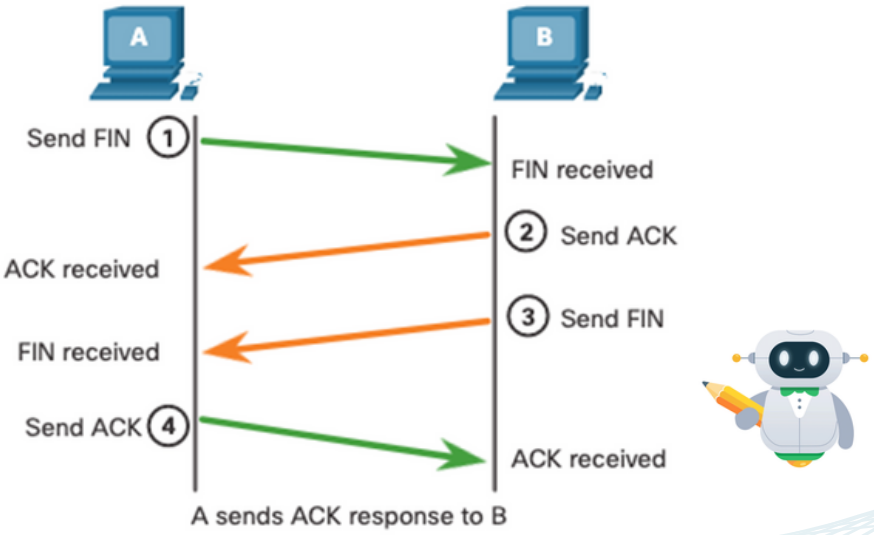
TCP Communication Process: TCP Connection Establishment

Step 1: The initiating client requests a client-to-server communication session with the server.
Step 2: The server acknowledges the client-to-server communication session and requests a server-to-client communication session.
Step 3: The initiating client acknowledges the server-to-client communication session.



TCP Communication Process: Session Termination

Step 1: When the client has no more data to send in the stream, it sends a segment with the FIN flag set.
Step 2: The server sends an ACK to acknowledge the receipt of the FIN to terminate the session from client to server**.**
Step 3: The server sends a FIN to the client to terminate the server-to-client session.
Step 4: The client responds with an ACK to acknowledge the FIN from the server.



5.1.5 Explain TCP Three-way Handshake

TCP Communication Process: TCP Three-Way Handshake Analysis

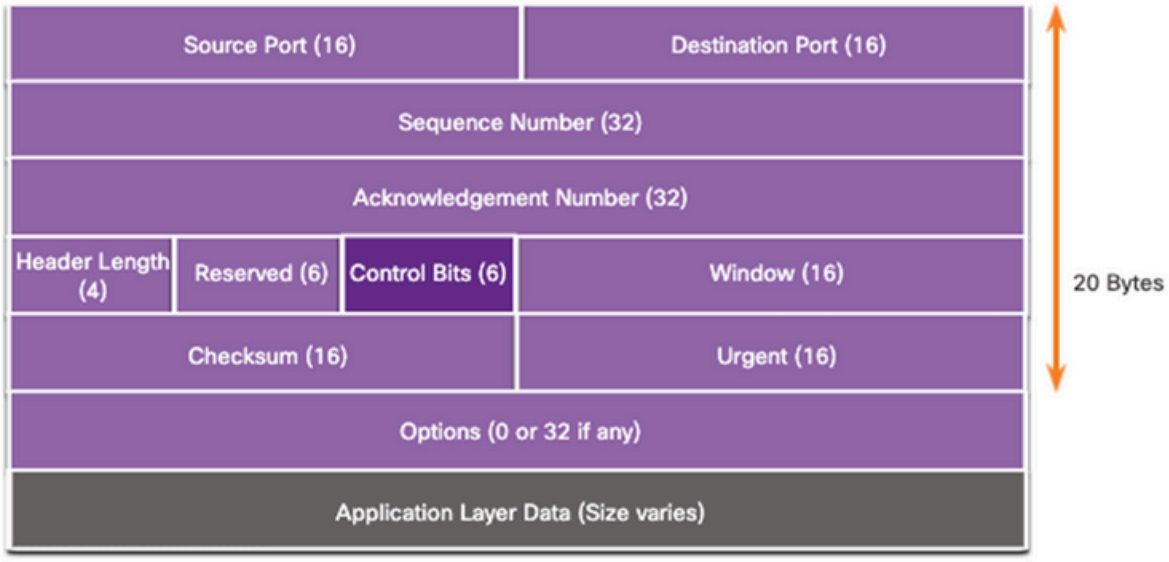
Functions of the Three-Way Handshake:

- 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.

The six control bit flags are as follows:

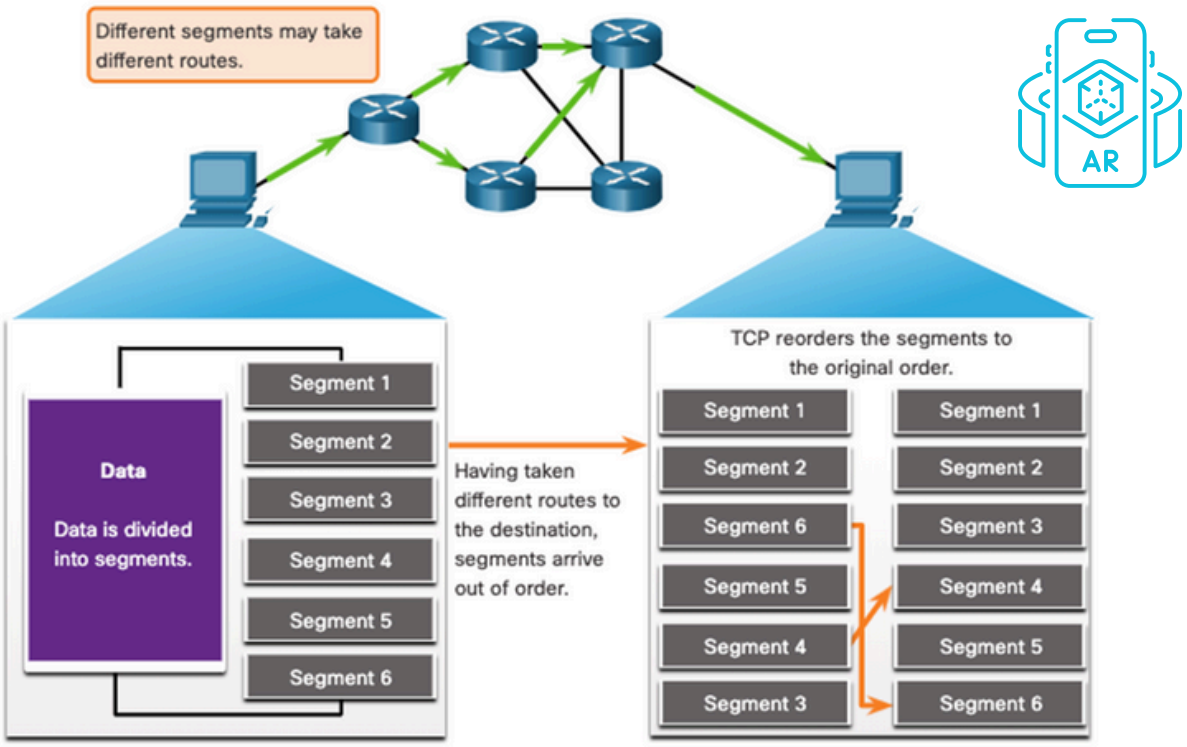
- URG - Urgent pointer field significant
- ACK - Acknowledgment flag used in connection establishment and session termination
- PSH - Push function
- RST - Reset the connection when an error or timeout occurs
- SYN - Synchronize sequence numbers used in connection establishment
- FIN - No more data from sender and used in session termination



5.1.5 Explain TCP Three-way Handshake

Reliability and Flow Control :
TCP Reliability- Guaranteed and Ordered Delivery

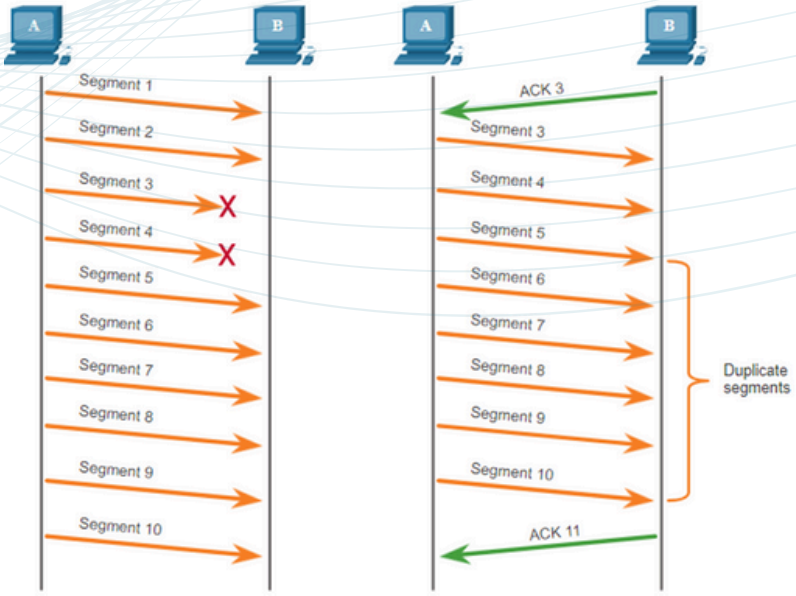
- TCP can also help maintain the flow of packets so that devices do not become overloaded.
- There may be times when TCP segments do not arrive at their destination or arrive out of order.
- All the data must be received and the data in these segments must be reassembled into the original order.
- Sequence numbers are assigned in the header of each packet to achieve this goal.

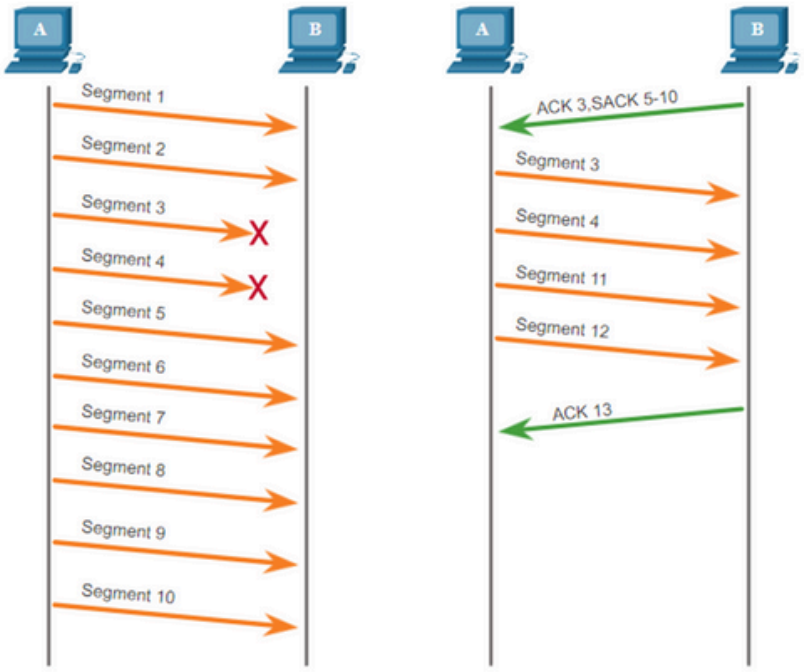


5.1.5 Explain TCP Three-way Handshake

Reliability and Flow Control :
TCP Reliability- Data Loss and Retransmission

- No matter how well designed a network is, data loss occasionally occurs.
- TCP provides methods of managing these segment losses. Among these is a mechanism to retransmit segments for unacknowledged data.



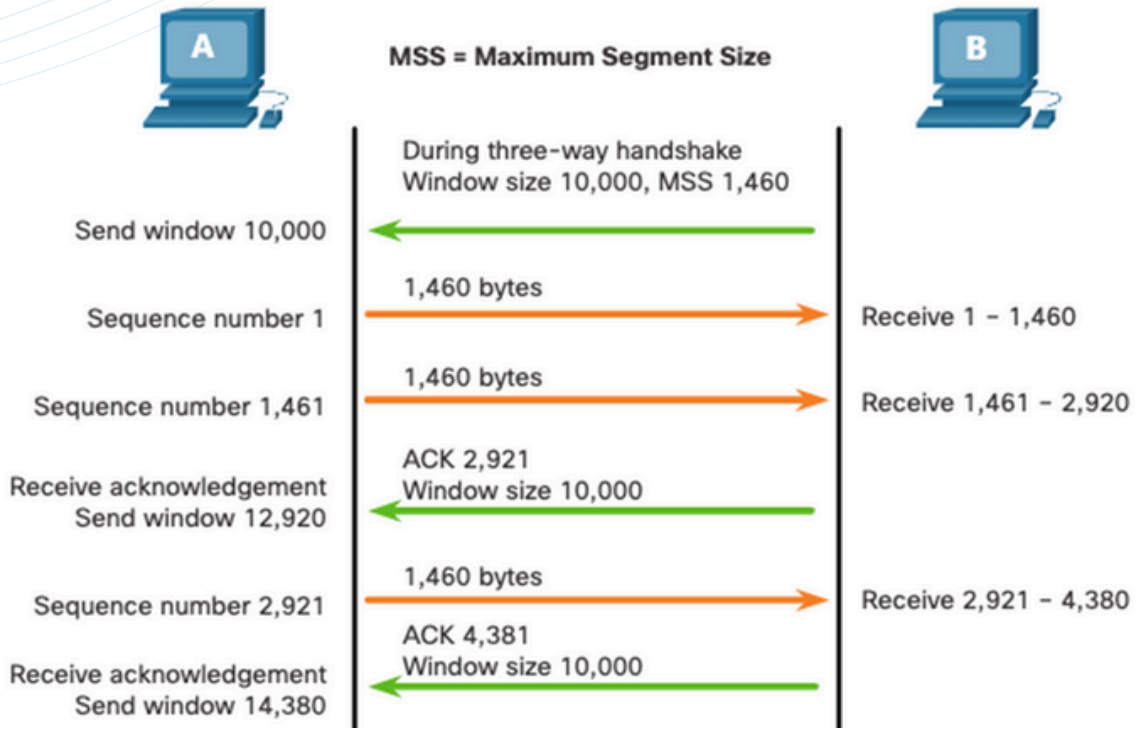


- Host operating systems today typically employ an optional TCP feature called selective acknowledgment (SACK), negotiated during the three-way handshake.
- If both hosts support SACK, the receiver can explicitly acknowledge which segments (bytes) were received including any discontinuous segments.

5.1.5 Explain TCP Three-way Handshake

Reliability and Flow Control :
TCP Flow Control – Window Size and Acknowledgments

- TCP also provides mechanisms for flow control as follows:
- Flow control is the amount of data that the destination can receive and process reliably.
- Flow control helps maintain the reliability of TCP transmission by adjusting the rate of data flow between source and destination for a given session.

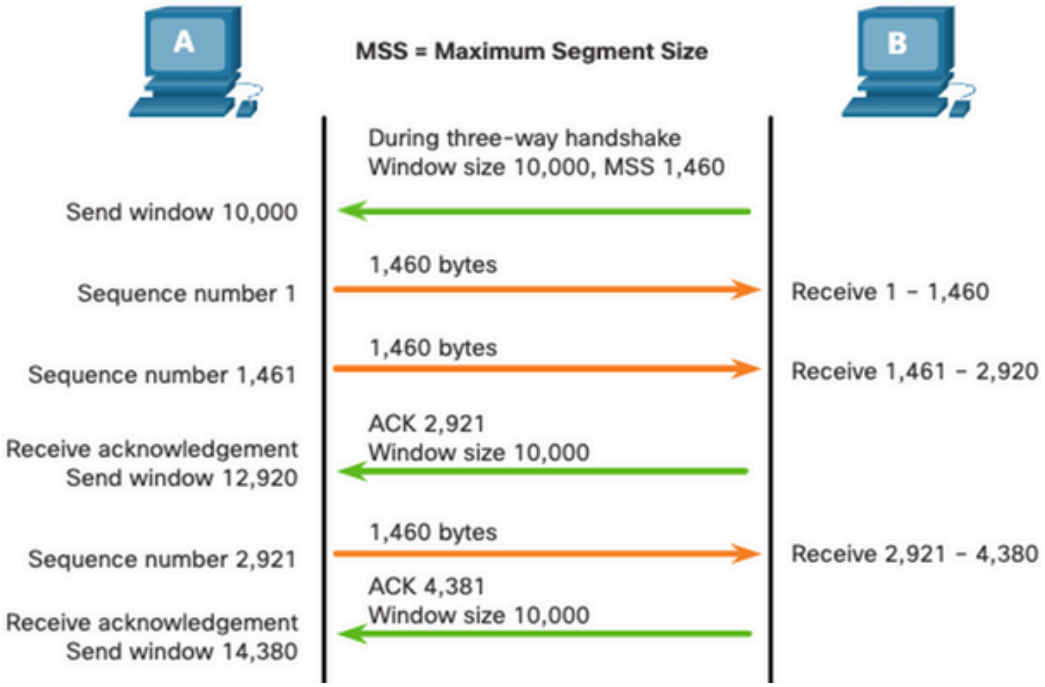


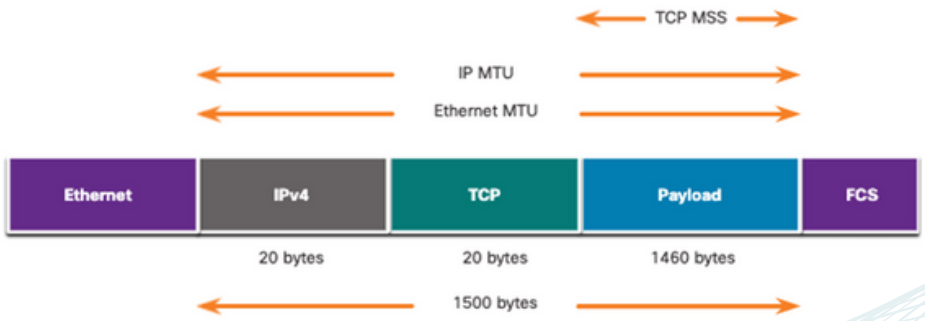
5.1.5 Explain TCP Three-way Handshake

Reliability and Flow Control :
TCP Flow Control –Maximum Segment Size

Maximum Segment Size (MSS) is the maximum amount of data that the destination device can receive:

- A common MSS is 1,460 bytes when using IPv4.
- A host determines the value of its MSS field by subtracting the IP and TCP headers from the Ethernet maximum transmission unit (MTU), which is 1500 bytes be default.
- 1500 minus 40 (20 bytes for the IPv4 header and 20 bytes for the TCP header) leaves 1460 bytes.

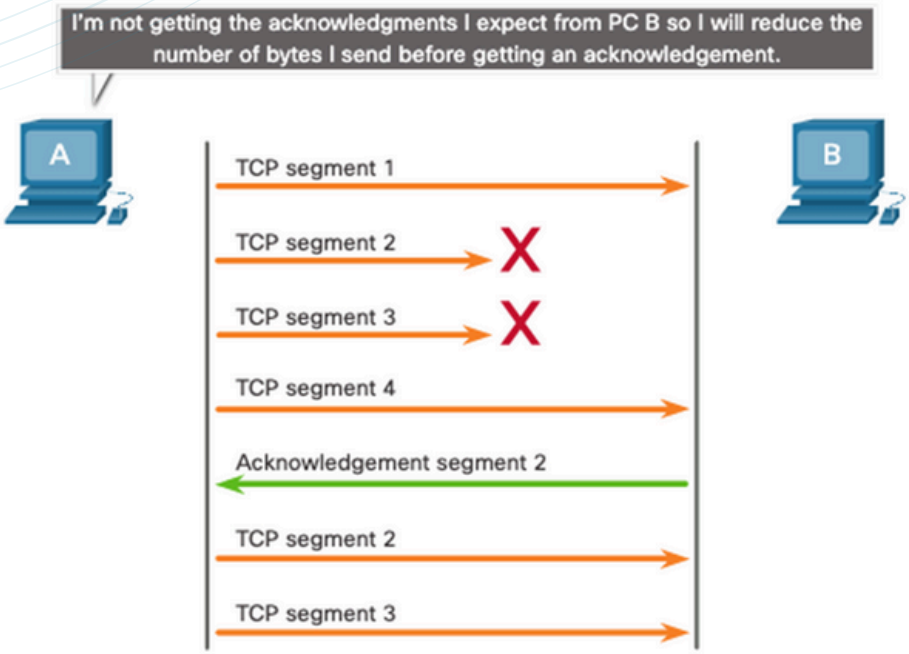




5.1.5 Explain TCP Three-way Handshake

Reliability and Flow Control :
TCP Flow Control –Congestion Avoidance

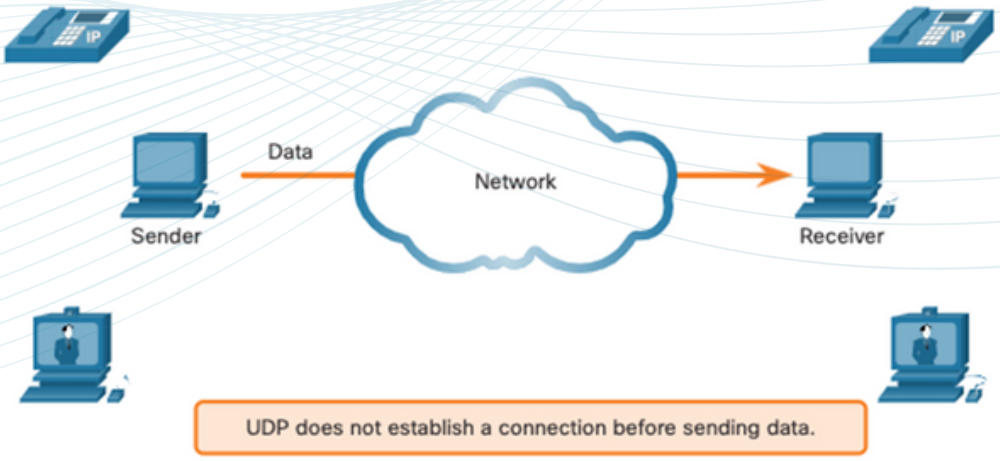
- When congestion occurs on a network, it results in packets being discarded by the overloaded router.
- To avoid and control congestion, TCP employs several congestion handling mechanisms, timers, and algorithms.



5.1.5 Explain TCP Three-way Handshake

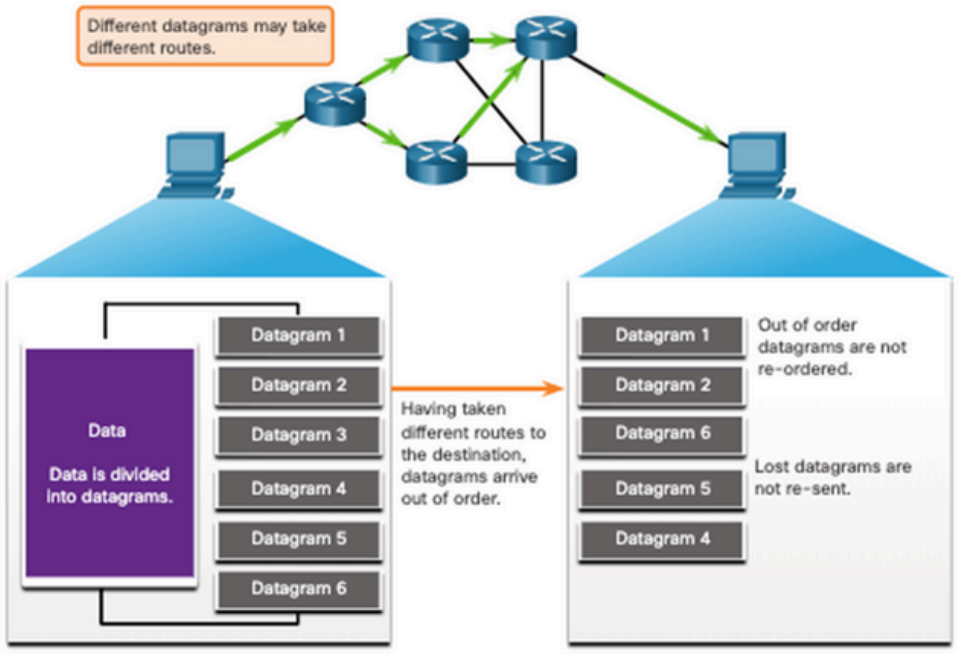
UDP Communication: UDP Low Overhead versus Reliability

- UDP does not establish a connection. UDP provides low overhead data transport because it has a small datagram header and no network management traffic.



UDP Communication: UDP Datagram Reassembly

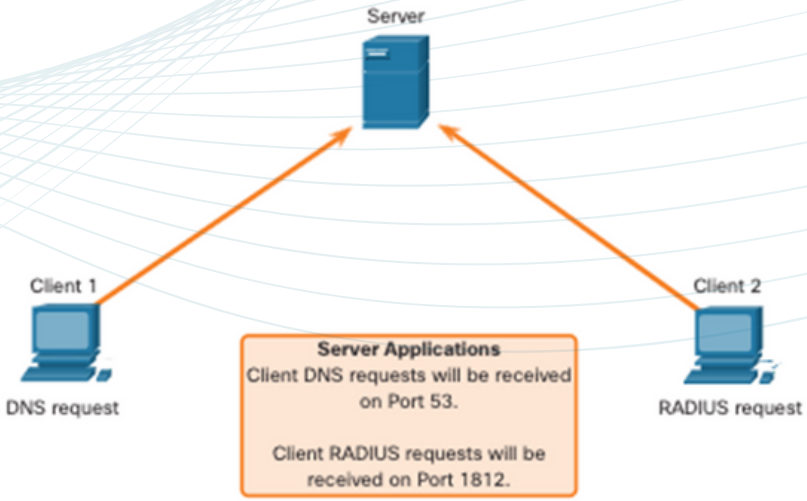
- UDP does not track sequence numbers the way TCP does.
- UDP has no way to reorder the datagrams into their transmission order.
- UDP simply reassembles the data in the order that it was received and forwards it to the application.



5.1.5 Explain TCP Three-way Handshake

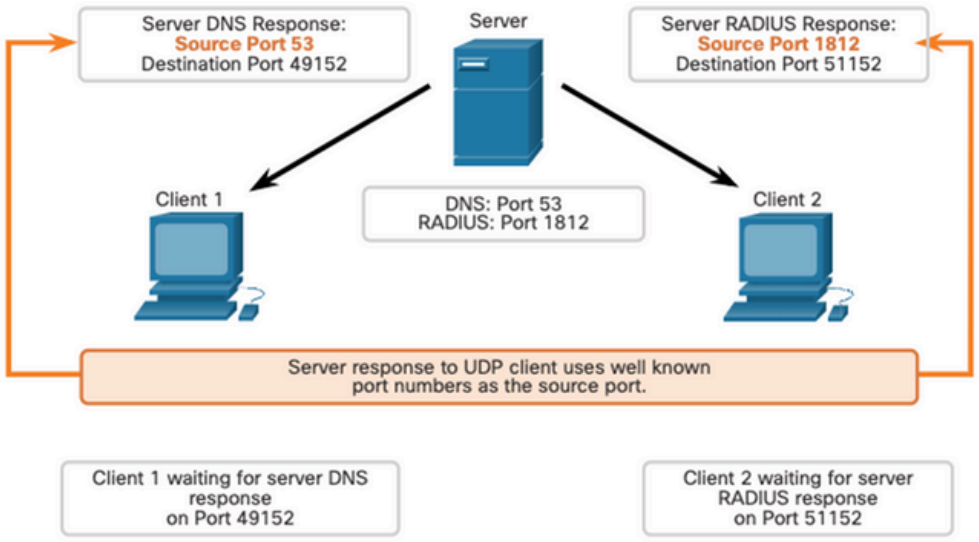
UDP Communication: UDP Server Processes and Requests

- UDP-based server applications are assigned well-known or registered port numbers.
- UDP receives a datagram destined for one of these ports, it forwards the application data to the appropriate application based on its port number.



UDP Communication: UDP Client Processes

- The UDP client process dynamically selects a port number from the range of port numbers and uses this as the source port for the conversation.
- The destination port is usually the well-known or registered port number assigned to the server process.
- After a client has selected the source and destination ports, the same pair of ports are used in the header of all datagrams in the transaction.

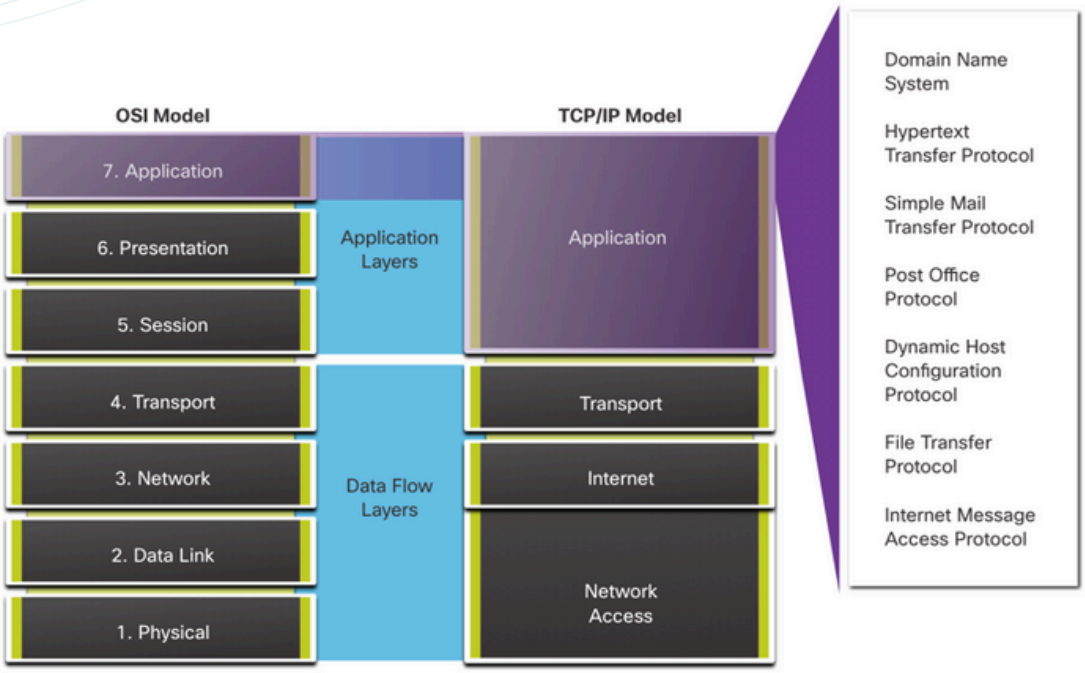


5.2 Explain Application layer protocols

5.2.1 Explain how the functions of the application layer, session layer, and presentation layer work together to provide network services to end user applications

Application, Presentation, and Session : Application Layer

- The upper three layers of the OSI model (application, presentation, and session) define functions of the TCP/IP application layer.
- The application layer provides the interface between the applications used to communicate, and the underlying network over which messages are transmitted.
- Some of the most widely known application layer protocols include HTTP, FTP, TFTP, IMAP and DNS.



5.2 Explain Application layer protocols

5.2.1 Explain how the functions of the application layer, session layer, and presentation layer work together to provide network services to end user applications

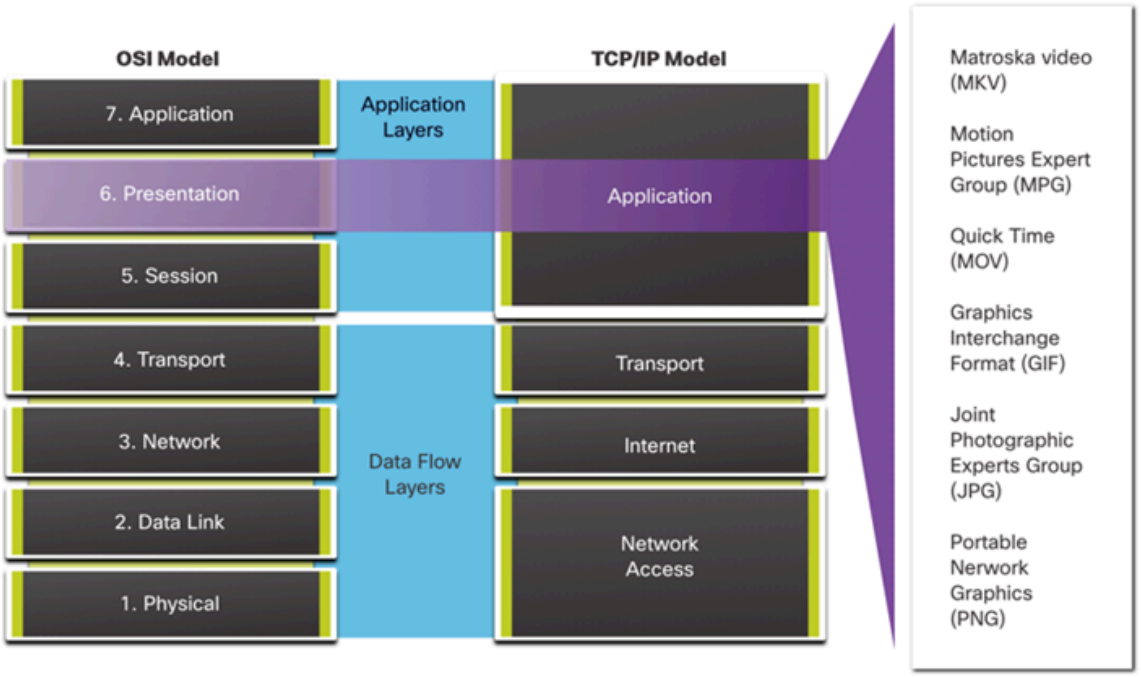
Application, Presentation, and Session : Presentation and Session Layer

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

The session layer functions:

- It creates and maintains dialogs between source and destination applications.
- It 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.



5.2 Explain Application layer protocols

5.2.1 Explain how the functions of the application layer, session layer, and presentation layer work together to provide network services to end user applications

Application, Presentation, and Session :
TCP/IP Application Layer Protocols

- The TCP/IP application protocols specify the format and control information necessary for many common internet communication functions.
- Application layer protocols are used by both the source and destination devices during a communication session.
- For the communications to be successful, the application layer protocols that are implemented on the source and destination host must be compatible.

Name System
DNS - Domain Name System (or Service)
- TCP, UDP client 53
- Translates domain names, such as cisco.com, into IP addresses.

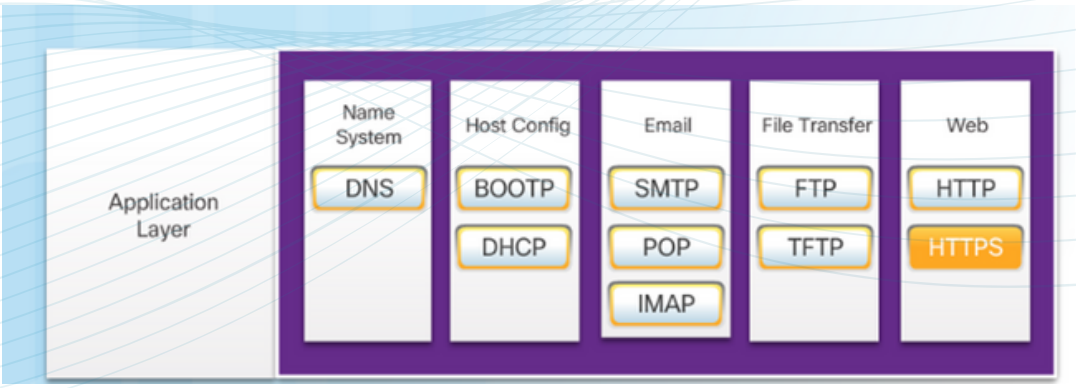
Host Config
DHCP - Dynamic Host Configuration Protocol
- UDP client 68, server 67
- Dynamically assigns IP addresses to be re-used when no longer needed

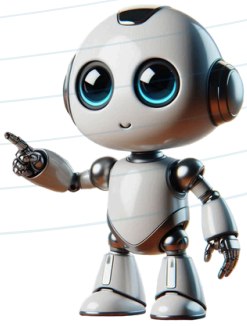
Web
HTTP - Hypertext Transfer Protocol
- TCP 80, 8080
- A set of rules for exchanging text, graphic images, sound, video, and other multimedia files on the World Wide Web

5.2 Explain Application layer protocols

5.2.1 Explain how the functions of the application layer, session layer, and presentation layer work together to provide network services to end user applications

Application, Presentation, and Session :
TCP/IP Application Layer Protocols





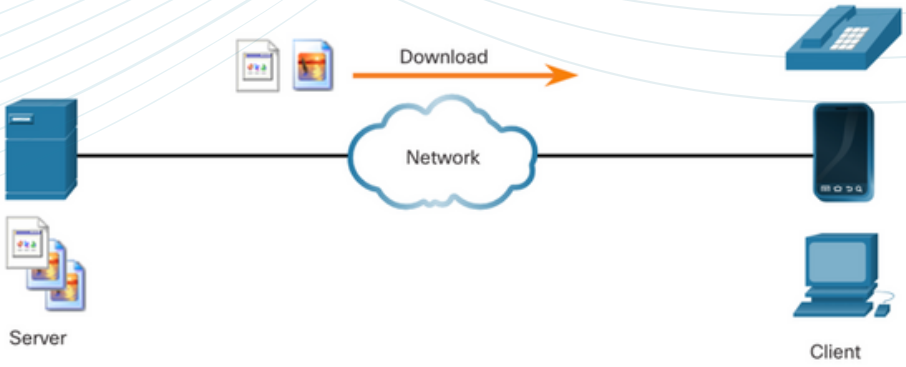
- Domain Name Server (DNS) TCP,UDP 53 - Translates domain names, such as cisco.com, into IP addresses.
- (BOOTP) – Bootstrap Protocol - BOOTP is being superseded by DHCP.
- Dynamic Host Configuration Protocol (DHCP) UDP client 68, server 67 – Dynamically assigns IP addresses to client stations at start-up.
- Simple Mail Transport Protocol (SMTP) TCP 25 - Enables clients to send email to a mail server.
- Post Office Protocol (POP) TCP 110 - Enables clients to retrieve email from a mail server.
- Internet Message Access Protocol (IMAP) TCP 143 - Enables clients to retrieve email from a mail server, maintains email on server.
- File Transfer Protocol (FTP) TCP 20 and 21 - Reliable, connection-oriented, and acknowledged file delivery protocol.
- Trivial File Transfer Protocol (TFTP) UDP 69 – simple connectionless file transfer protocol.
- Hypertext Transfer Protocol (HTTP) TCP 80, 8080 - Set of rules for exchanging text, graphic images, etc. on the World Wide Web.
- Hypertext Transfer Protocol Secure (HTTPS) TCP, UDP 443 – Uses encryption and authentication to secure communication

5.2 Explain Application layer protocols

5.2.1 Explain how the functions of the application layer, session layer, and presentation layer work together to provide network services to end user applications

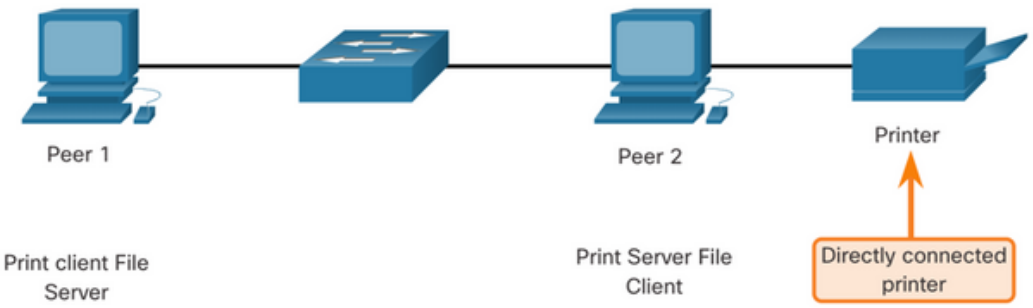
Peer-to-Peer : Client-Server Model

- Client and server processes are considered to be in the application layer.
- In the client/server model, the device requesting the information is called a client and the device responding to the request is called a server.
- Application layer protocols describe the format of the requests and responses between clients and servers.



Peer-to-Peer : Peer-to-Peer Networks

- In a peer-to-peer (P2P) network, two or more computers are connected via a network and can share resources (such as printers and files) without having a dedicated server.
- Every connected end device (known as a peer) can function as both a server and a client.
- One computer might assume the role of server for one transaction while simultaneously serving as a client for another. The roles of client and server are set on a per request basis.

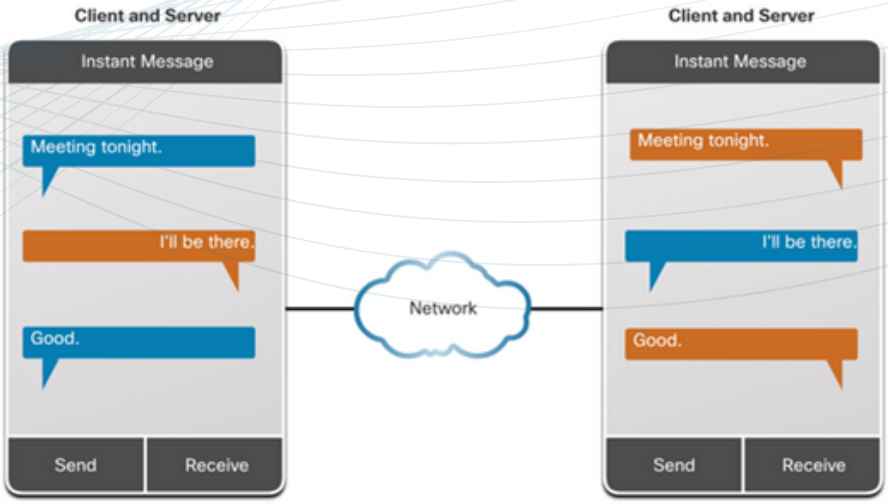


5.2 Explain Application layer protocols

5.2.1 Explain how the functions of the application layer, session layer, and presentation layer work together to provide network services to end user applications

Peer-to-Peer : Peer-to-Peer Applications

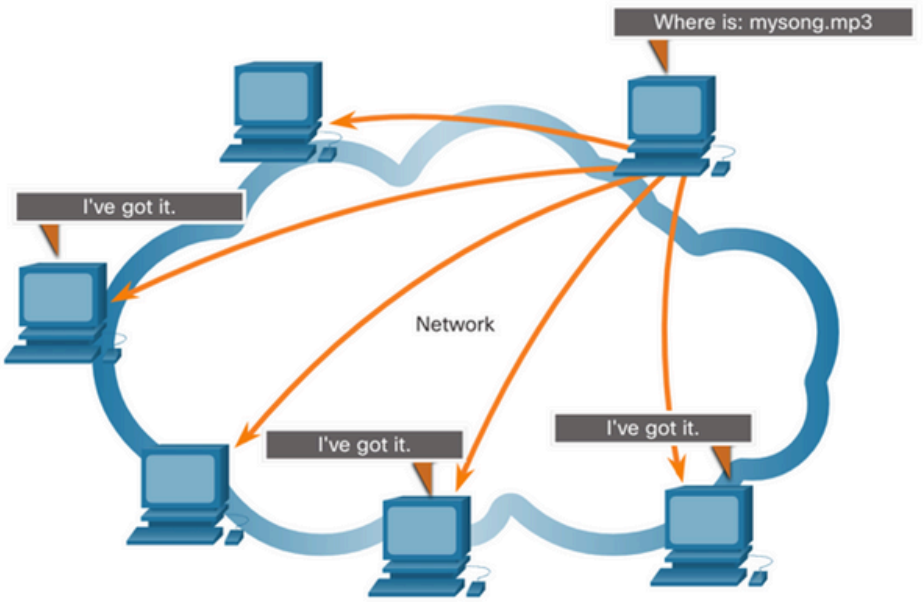
- A P2P application allows a device to act as both a client and a server within the same communication.
- Some P2P applications use a hybrid system where each peer accesses an index server to get the location of a resource stored on another peer.



Peer-to-Peer : Common P2P Applications

- With P2P applications, each computer in the network that is running the application can act as a client or a server for the other computers in the network that are also running the application.

- Common P2P networks include the following:
  - BitTorrent
  - Direct Connect
  - eDonkey
  - Freenet



5.2.2 Explain how web and email protocols operate

Web and Email Protocols :
Hypertext Transfer Protocol and Hypertext Markup Language

- When a web address or Uniform Resource Locator (URL) is typed into a web browser, the web browser establishes a connection to the web service. The web service is running on the server that is using the HTTP protocol.
- To better understand how the web browser and web server interact, examine how a web page is opened in a browser.

Step 1 :

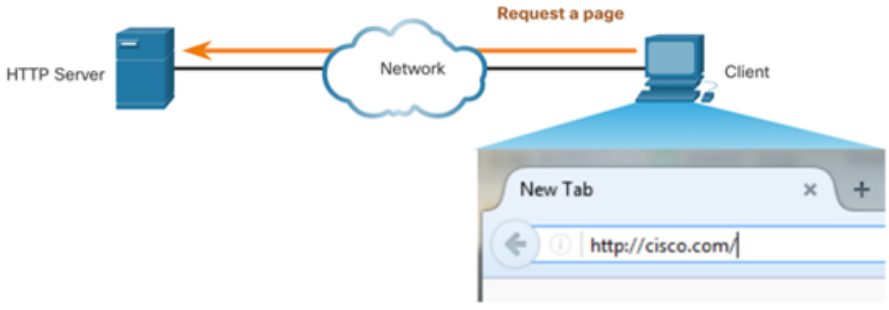
The browser interprets the three parts of the URL:

- http (the protocol or scheme)
- www.cisco.com (the server name)
- index.html (the specific filename requested)

Step 2:

The browser then checks with a name server to convert www.cisco.com into a numeric IP address, which it uses to connect to the server.

The client initiates an HTTP request to a server by sending a GET request to the server and asks for the index.html file.

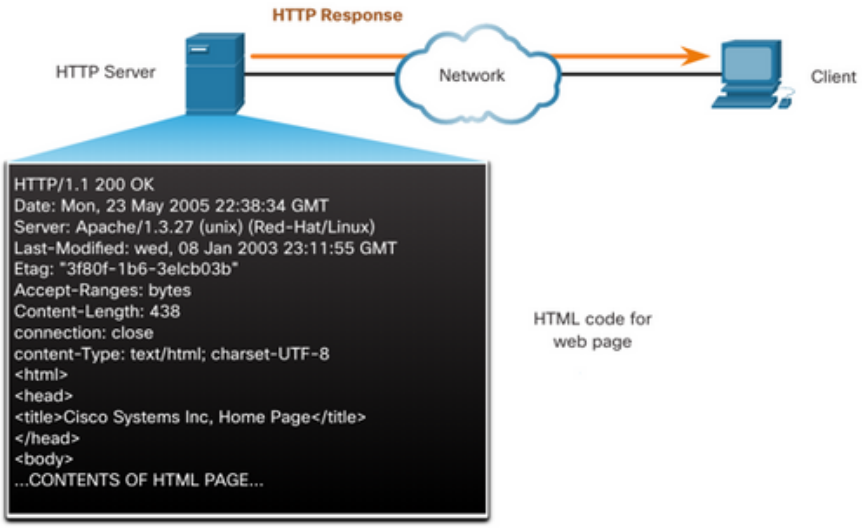


5.2.2 Explain how web and email protocols operate

Web and Email Protocols :
Hypertext Transfer Protocol and Hypertext Markup Language

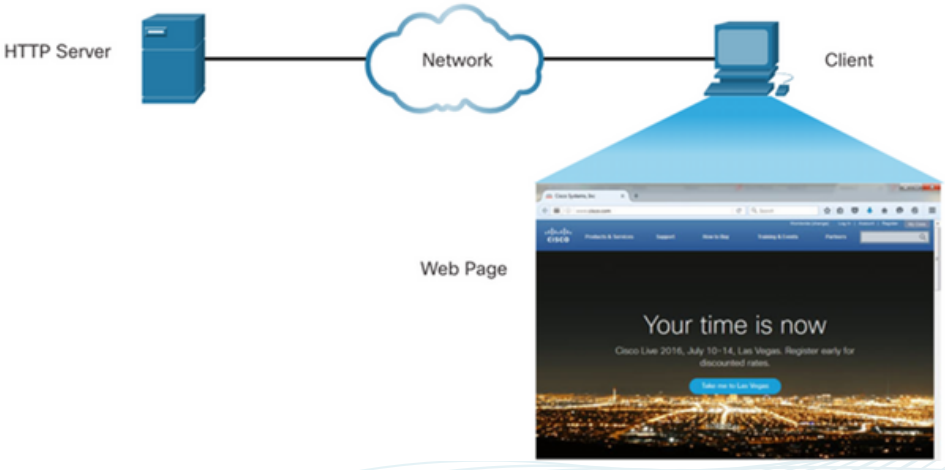
Step 3:

In response to the request, the server sends the HTML code for this web page to the browser.



Step 4:

The browser deciphers the HTML code and formats the page for the browser window.



5.2.2 Explain how web and email protocols operate

Web and Email Protocols : HTTP and HTTPS

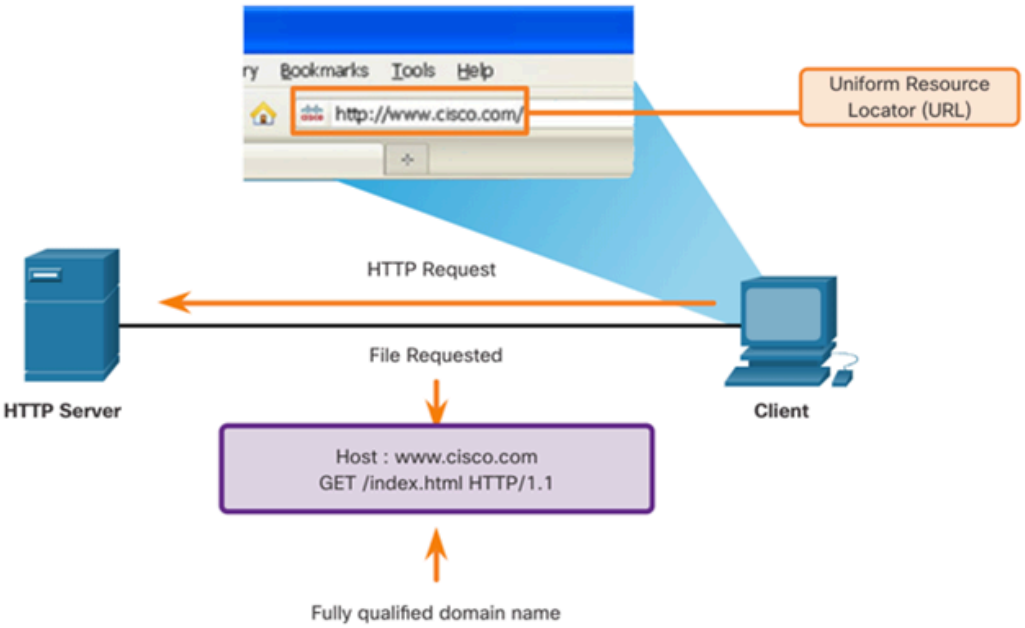
- HTTP is a request/response protocol that specifies the message types used for that communication.

- The three common message types are GET, POST, and PUT:

GET - This is a client request for data. A client (web browser) sends the GET message to the web server to request HTML pages.

POST - This uploads data files to the web server, such as form data.

PUT - This uploads resources or content to the web server, such as an image.



Note: HTTP is not a secure protocol. For secure communications sent across the internet, HTTPS should be used.

5.2.2 Explain how web and email protocols operate

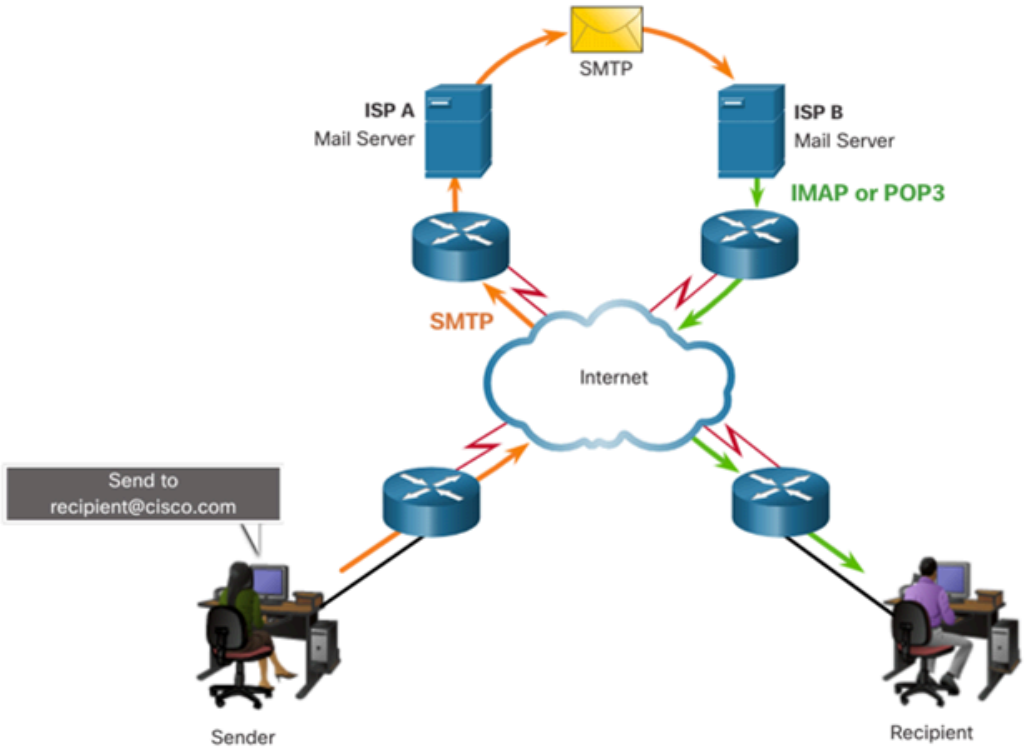
Web and Email Protocols : Email Protocols

- Email is a store-and-forward method of sending, storing, and retrieving electronic messages across a network. Email messages are stored in databases on mail servers. Email clients communicate with mail servers to send and receive email.

- The email protocols used for operation are:

  i) **Simple Mail Transfer Protocol (SMTP**) – used to send mail.

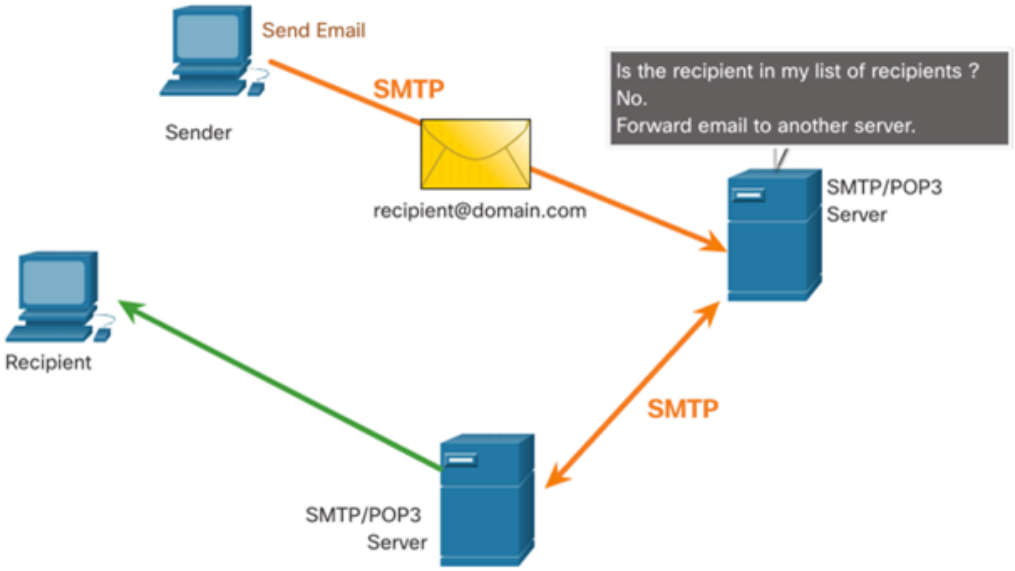
  ii) **Post Office Protocol (POP) & IMAP** – used for clients to receive mail.



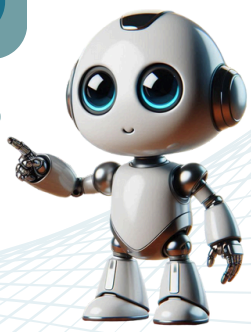
5.2.2 Explain how web and email protocols operate

Web and Email Protocols : SMTP, POP and IMAP

- When a client sends email, the client SMTP process connects with a server SMTP process on well-known port 25.
- After the connection is made, the client attempts to send the email to the server across the connection.
- When the server receives the message, it either places the message in a local account, if the recipient is local, or forwards the message to another mail server for delivery.
- The destination email server may not be online or may be busy. If so, SMTP spools messages to be sent at a later time.



Note: SMTP message formats require a message header (recipient email address & sender email address) and a message body.

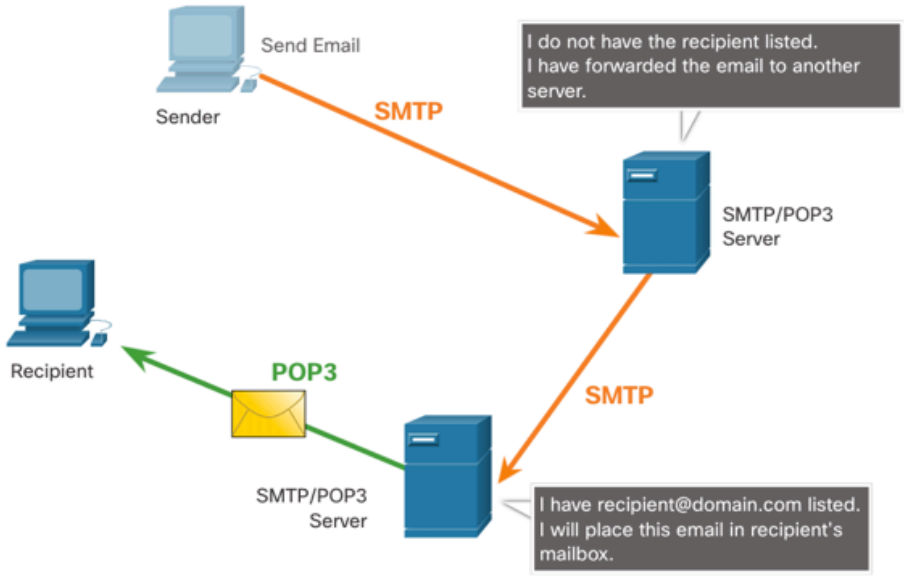


5.2.2 Explain how web and email protocols operate

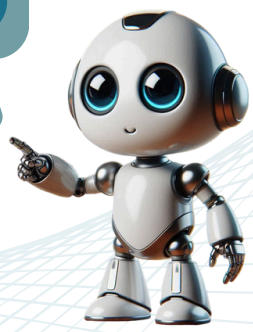
Web and Email Protocols : SMTP, POP and IMAP

POP is used by an application to retrieve mail from a mail server. When mail is downloaded from the server to the client using POP the messages are then deleted on the server.

- The server starts the POP service by passively listening on TCP port 110 for client connection requests.
- When a client wants to make use of the service, it sends a request to establish a TCP connection with the server.
- When the connection is established, the POP server sends a greeting.
- The client and POP server then exchange commands and responses until the connection is closed or aborted.



Note: Since POP does not store messages, it is not recommended for small businesses that need a centralized backup solution.



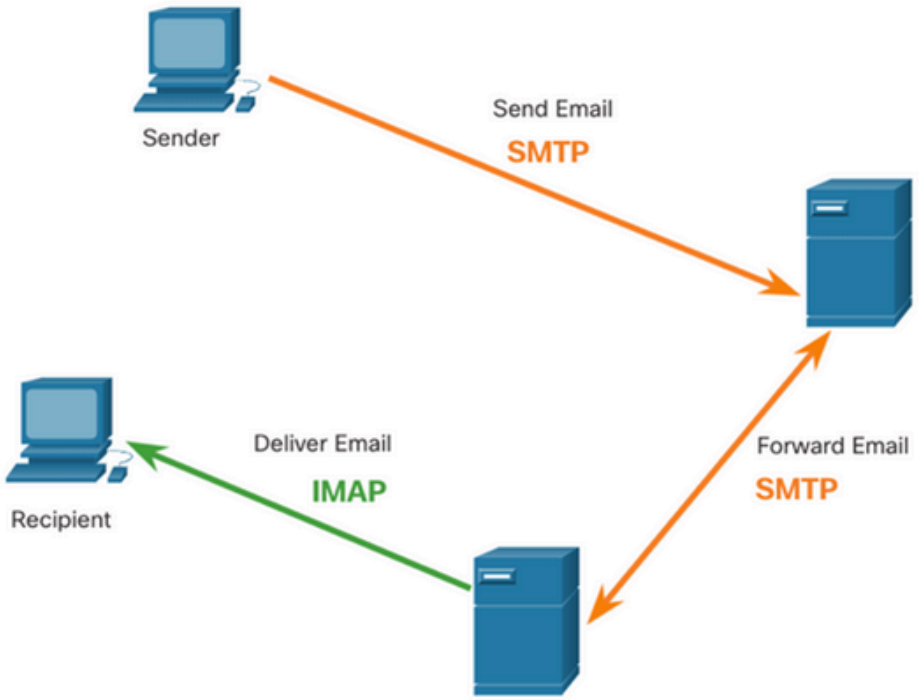
5.2.2 Explain how web and email protocols operate

Web and Email Protocols : SMTP, POP and IMAP

IMAP is another protocol that describes a method to retrieve email messages.

- Unlike POP, when a user connects to an IMAP server, copies of the messages are downloaded to the client application. The original messages are kept on the server until manually deleted.

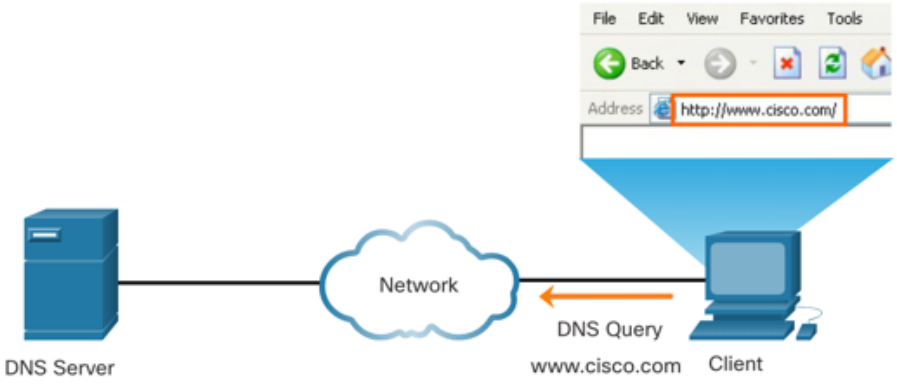
- When a user decides to delete a message, the server synchronizes that action and deletes the message from the server.



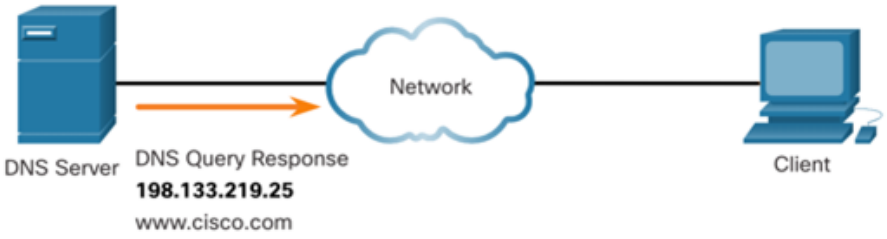
5.2.3 Explain how DNS and DHCP operate

IP Addressing Services : Domain Name Service

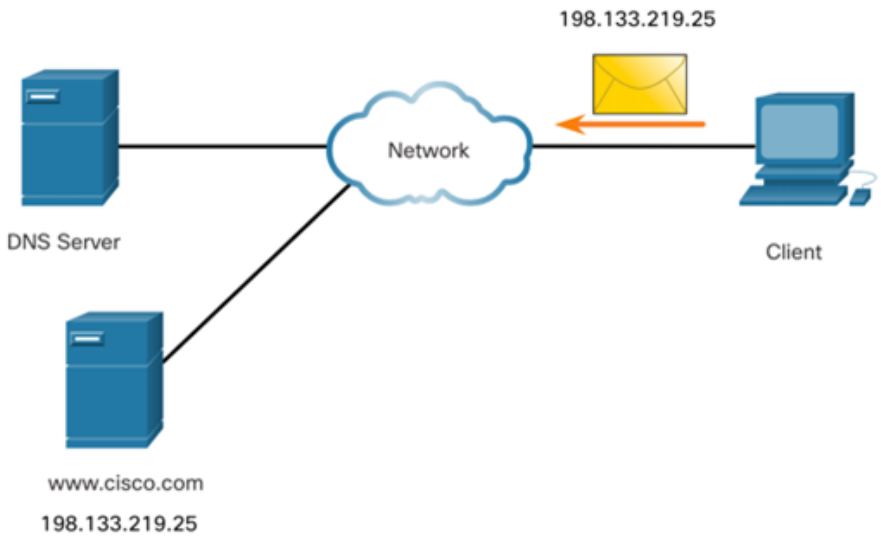
- Domain names were created to convert the numeric IP addresses into a simple, recognizable name.



- Fully-qualified domain names (FQDNs), such as http://www.cisco.com, are much easier for people to remember than 198.133.219.25.



- The DNS protocol defines an automated service that matches resource names with the required numeric network address. It includes the format for queries, responses, and data.

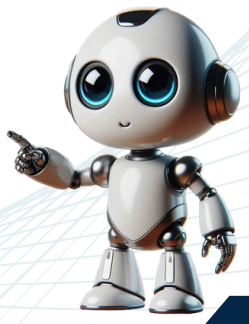


5.2.3 Explain how DNS and DHCP operate

IP Addressing Services : DNS Message Format

- The DNS server stores different types of resource records that are used to resolve names. These records contain the name, address, and type of record.
- Some of these record types are as follows:
- A - An end device IPv4 address
- NS - An authoritative name server
- AAAA - An end device IPv6 address (pronounced quad-A)
- MX - A mail exchange record
- When a client makes a query, the server DNS process first looks at its own records to resolve the name. If it is unable to resolve the name by using its stored records, it contacts other servers to resolve the name.
- After a match is found and returned to the original requesting server, the server temporarily stores the numbered address in the event that the same name is requested again.
- DNS uses the same message format between servers, consisting of a question, answer, authority, and additional information for all types of client queries and server responses, error messages, and transfer of resource record information.

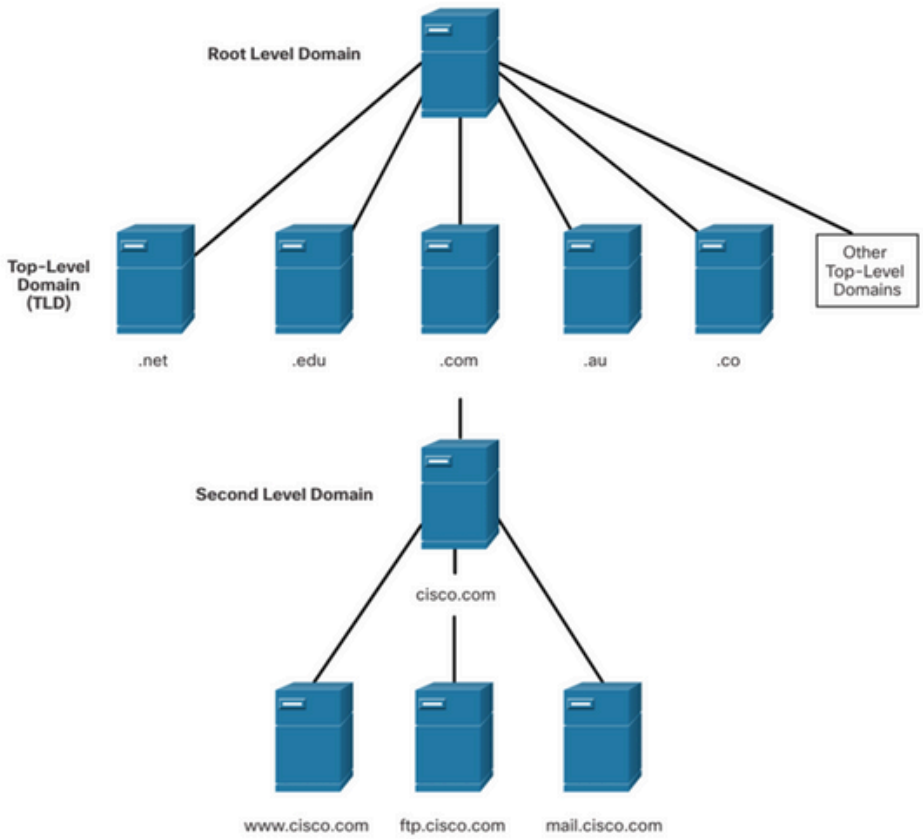
DNS message section	Description
Question	The question for the name server
Answer	Resource Records answering the question
Authority	Resource Records pointing toward an authority
Additional	Resource Records holding additional information

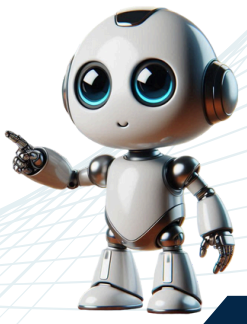


5.2.3 Explain how DNS and DHCP operate

IP Addressing Services : DNS Hierarchy

- DNS uses a hierarchical system to create a database to provide name resolution.
- Each DNS server maintains a specific database file and is only responsible for managing name-to-IP mappings for that small portion of the entire DNS structure.
- When a DNS server receives a request for a name translation that is not within its DNS zone, the DNS server forwards the request to another DNS server within the proper zone for translation.
- Examples of top-level domains:
  .com - a business or industry
  .**org** - a non-profit organization
  .au - Australia



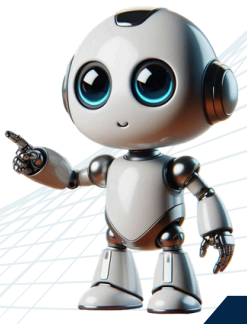


5.2.3 Explain how DNS and DHCP operate

IP Addressing Services : The nslookup Command

- Nslookup is a computer operating system utility that allows a user to manually query the DNS servers configured on the device to resolve a given host name.
- This utility can also be used to troubleshoot name resolution issues and to verify the current status of the name servers.
- When the nslookup command is issued, the default DNS server configured for your host is displayed.
- The name of a host or domain can be entered at the nslookup prompt.

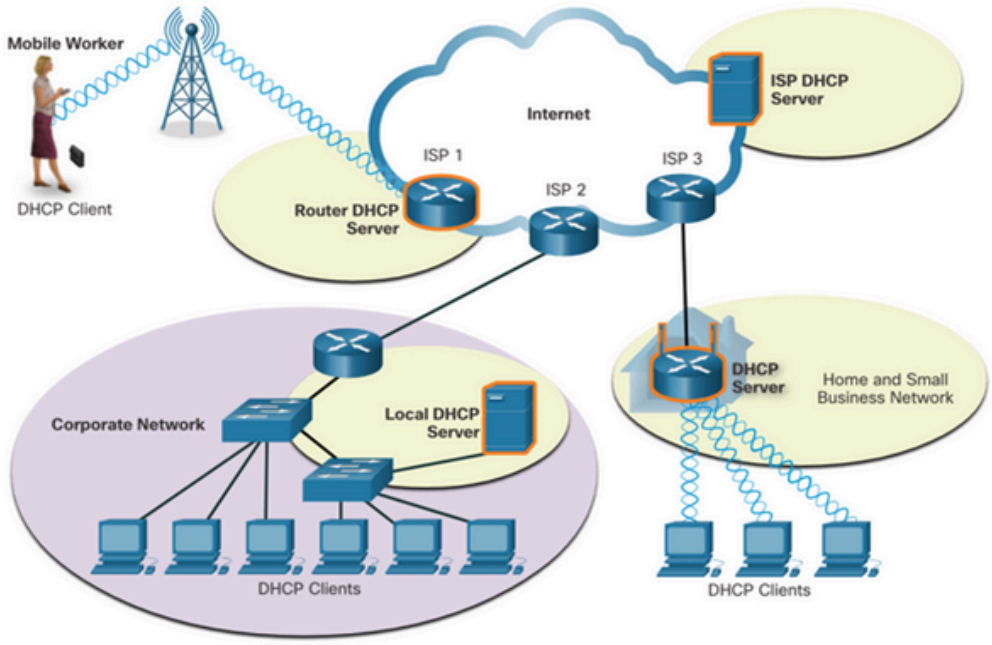
```
C:\Users> nslookup
Default Server:  dns-sj.cisco.com
Address:  171.70.168.183
> www.cisco.com
Server:  dns-sj.cisco.com
Address:  171.70.168.183
Name:    origin-www.cisco.com
Addresses:  2001:420:1101:1::a
          173.37.145.84
Aliases:  www.cisco.com
> cisco.netacad.net
Server:  dns-sj.cisco.com
Address:  171.70.168.183
Name:    cisco.netacad.net
Address:  72.163.6.223
>
```



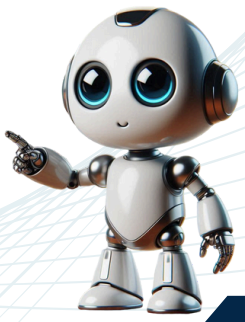
5.2.3 Explain how DNS and DHCP operate

IP Addressing Services : Dynamic Host Configuration Protocol

- The Dynamic Host Configuration Protocol (DHCP) for IPv4 service automates the assignment of IPv4 addresses, subnet masks, gateways, and other IPv4 networking parameters.
- DHCP is considered dynamic addressing compared to static addressing. Static addressing is manually entering IP address information.
- 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.
- Many networks use both DHCP and static addressing. DHCP is used for general purpose hosts, such as end user devices. Static addressing is used for network devices, such as gateway routers, switches, servers, and printers.



Note: DHCP for IPv6 (DHCPv6) provides similar services for IPv6 clients. However, DHCPv6 does not provide a default gateway address. This can only be obtained dynamically from the Router Advertisement message of the router.

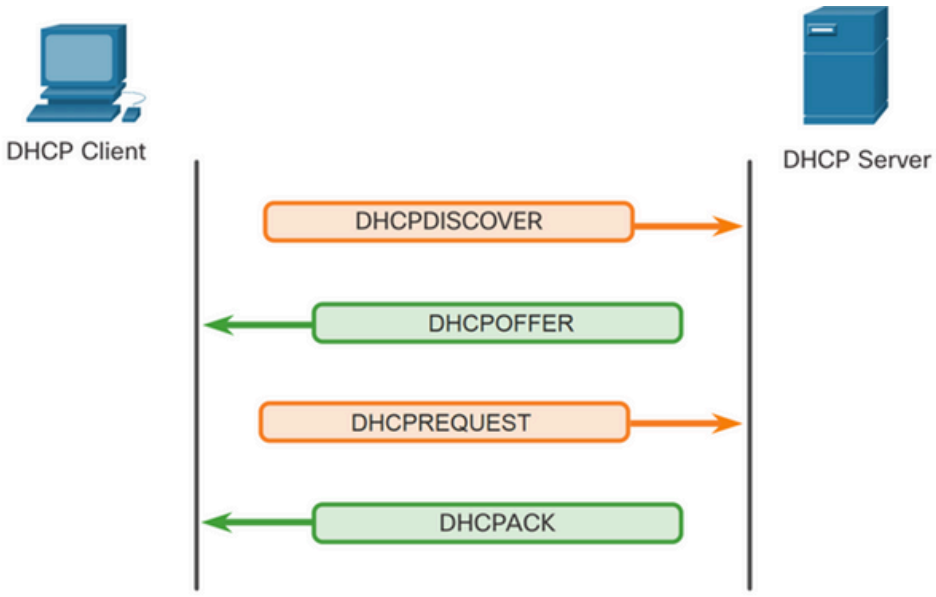


5.2.3 Explain how DNS and DHCP operate

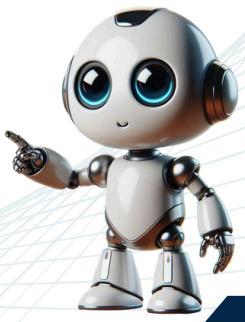
IP Addressing Services : DHCP Operation

The DHCP Process:

- 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. (If a client receives more than one offer due to multiple DHCP servers on the network, it must choose one.)
- The client sends a DHCP request (DHCPREQUEST) message that identifies the explicit server and lease offer that the client is accepting.
- The server then 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 and the process must begin with a new DHCPDISCOVER message.



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



5.2.3 Explain how DNS and DHCP operate

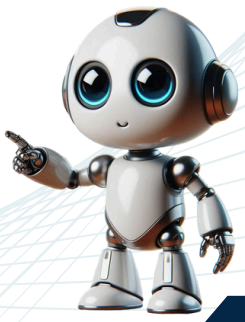
File Sharing Services : File Transfer Protocol

FTP was developed to allow for data transfers between a client and a server. An FTP client is an application which runs on a computer that is being used to push and pull data from an FTP

1. The client establishes the first connection to the server for control traffic using TCP port 21. The traffic consists of client commands and server replies.

2. The client establishes the second connection to the server for the actual data transfer using TCP port 20. This connection is created every time there is data to be transferred.

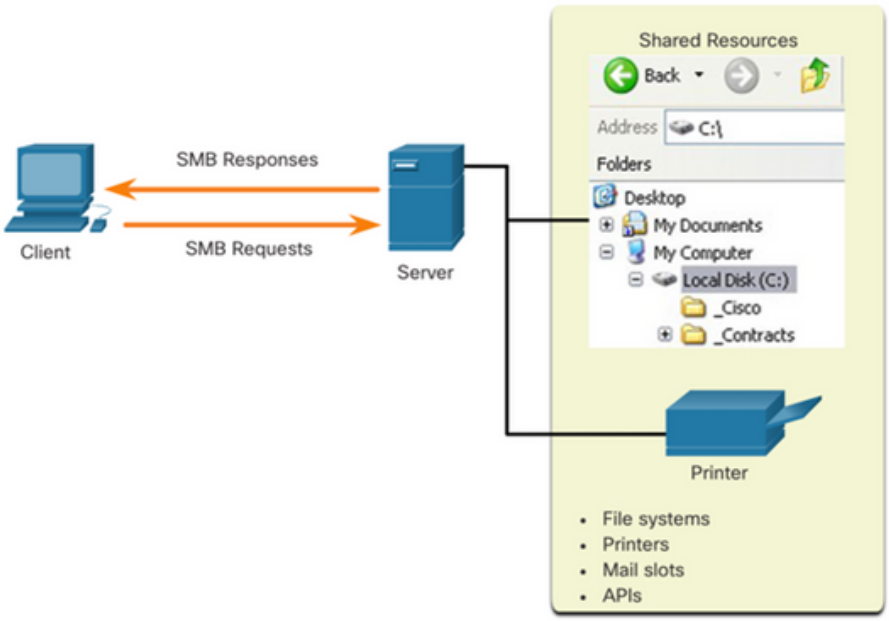
3. The data transfer can happen in either direction. The client can download (pull) data from the server, or the client can upload (push) data to the server.

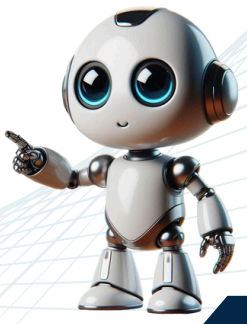


5.2.3 Explain how DNS and DHCP operate

File Sharing Services : Server Message Block

- The Server Message Block (SMB) is a client/server, request-response file sharing protocol. Servers can make their own resources available to clients on the network.
- Three functions of SMB messages:
- Start, authenticate, and terminate sessions
- Control file and printer access
- Allow an application to send or receive messages to or from another device
- Unlike the file sharing supported by FTP, clients establish a long-term connection to servers. After the connection is established, the user of the client can access the resources on the server as though the resource is local to the client host.





Quick Quiz

1. How does a WLAN allow devices to connect to a network?
   A. By using fiber-optic cables
   B. By connecting through radio waves
   C. By using infrared beams only
   D. By connecting through telephone lines

2. Which of the following is a main benefit of WLANs?
   A. Reduced mobility
   B. Requires more cabling
   C. Provides flexible and wireless access
   D. Slower network speeds only

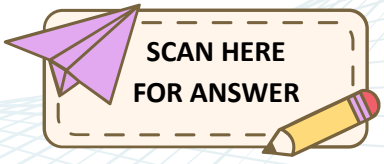
3. Which wireless network type provides national or global coverage using cellular towers?
   A. WPAN
   B. WLAN
   C. WMAN
   D. WWAN

4. Which technology offers long-range wireless Internet similar to DSL or cable?
   A. Bluetooth
   B. WiMAX
   C. Cellular Broadband
   D. Satellite Broadband

5. 802.11 standard operates in the 5 GHz frequency band is _____

6. 802.11 standard also known as Wi-Fi 6 is _____

7. _____ is a client/server, request-response file sharing protocol



06
REFERENCES

REFERENCES

1. Forouzan, A., B. (2022). Data Communications and Networking with TCP/IP Protocol Suite, 6th Edition . Mcgrawhill. (ISBN 978-0078022098)

2. James, F., K. & Keith, R. (2022). Computer Networking: a Top-Down Approach 8th Edition . Pearson. (ISBN 978-0136681557)

3. (2020). Introduction to Networks Companion Guide (CCNAv7), By Cisco Networking Academy, Part of the Companion Guide series.

4. https://www.cisco.com/site/us/en/learn/training-certifications/training/netacad/index.html

5. https://itexamanswers.net/ccna-1-v7-exam-answers-introduction-to-networks-v7-0-itn.html

POLITEKNIK MALAYSIA
METrO TASEK GELUGOR

DEPARTMENT OF INFORMATION TECHNOLOGY AND COMMUNICATION
Politeknik METrO Tasek Gelugor,
No 25, Jalan Komersial 2,
Pusat Komersial Tasek Gelugor,
13300 Tasek Gelugor,
PULAU PINANG.

e ISBN 978-967-2744-27-6

9 789672 744276