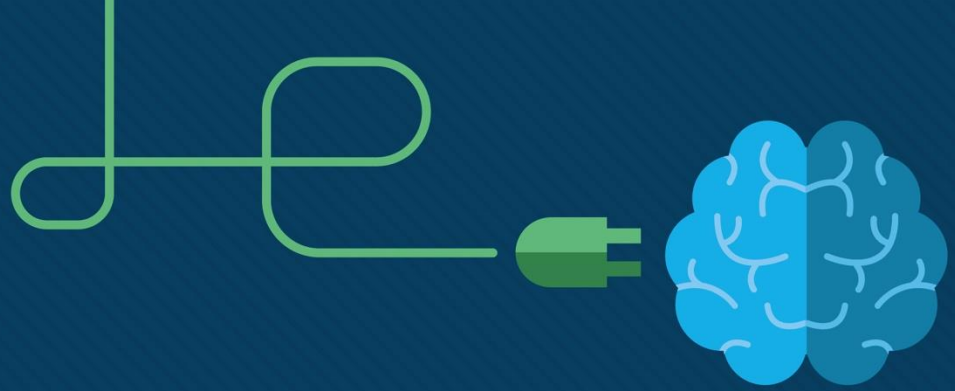
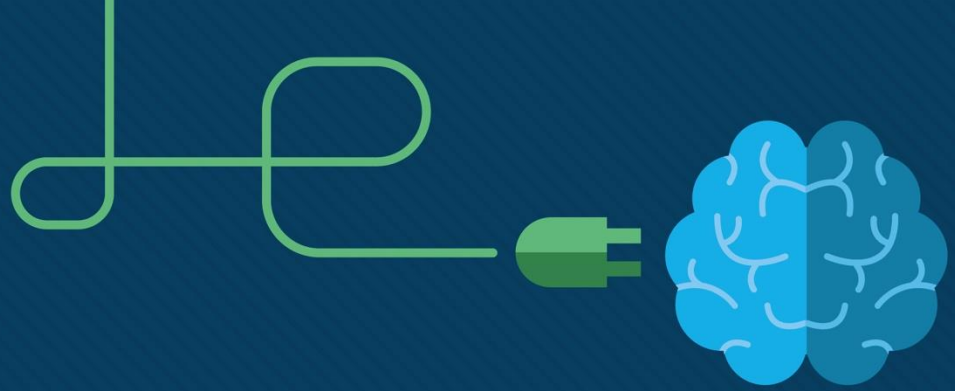


Module 5:Network Protocols

Instructor Materials

CyberOps Associates v1.0



Module 5:Network Protocols

CyberOps Associates v1.0

Module Objectives

Module Title: Network Protocols

Module Objective: Explain how protocols enable network operations.

Topic Title	Topic Objective
Network Communications Process	Explain the basic operation of data networked communications.
Communications Protocols	Explain how protocols enable network operations.
Data Encapsulation	Explain how data encapsulation allows data to be transported across the network.

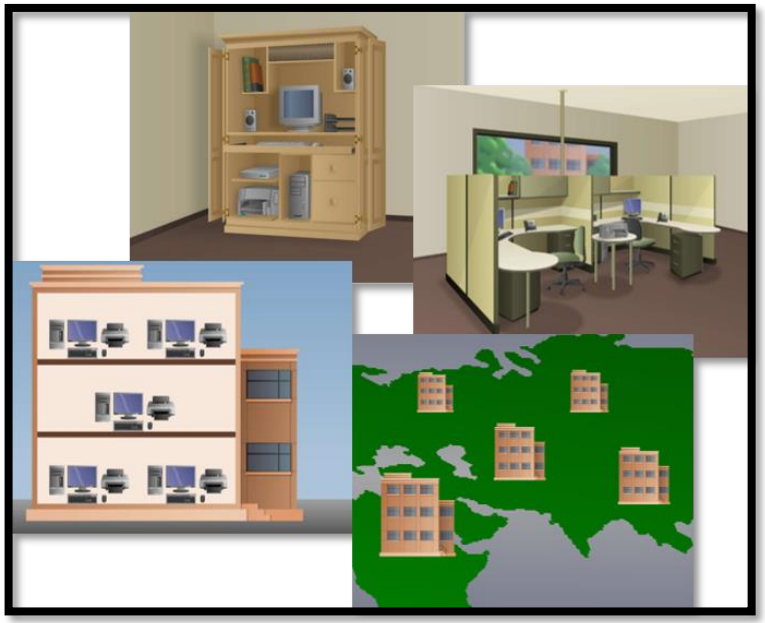
5.1 Network Communications Process

Networks of Many Sizes

- Networks vary in size. They range from simple networks consisting of two computers, to networks connecting millions of devices.
- Businesses and large organizations use networks to provide consolidation, storage, and access to information on network servers. Networks provide email, instant messaging, and collaboration among employees. Many organizations use their network's connection to the internet to provide products and services to customers.
- **Peer-to-peer network:** In small businesses and homes, many computers function as both the servers and clients on the network. This type of network is called a peer-to-peer network.

Networks of Many Sizes (Contd.)

- **Small Home networks:** Small home networks connect a few computers to each other and to the internet.
- **Small Office and Home Office (SOHO) networks:** The SOHO network allows a home office or a remote office to connect to a corporate network, or access centralized, shared resources.
- **Medium to Large networks**: These are used by corporations and schools and can have many locations with hundreds or thousands of interconnected hosts.
- **World Wide networks**: The internet is a network of networks that connects hundreds of millions of computers world-wide.

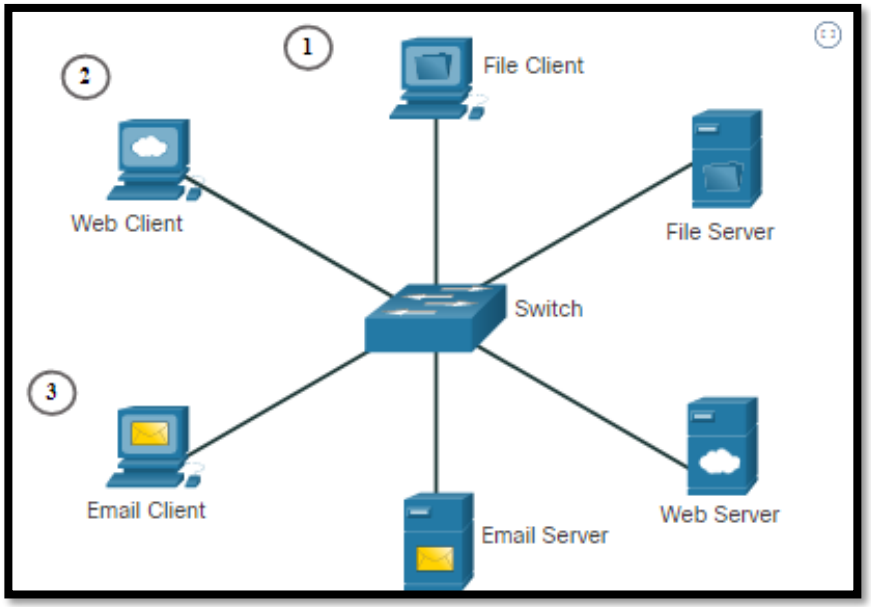


Client-Server Communications

- All computers that are connected to a network and that participate directly in network communication are classified as hosts. Hosts are also called end devices, endpoints, or nodes.
- Servers are simply computers with specialized software that enables servers to provide information to other end devices on the network.
- A server can be single-purpose, providing only one service, such as web pages or it can be multipurpose, providing a variety of services such as web pages, email, and file transfers.
- Client computers have software installed that enables them to request and display the information obtained from the server. A single computer can run multiple types of client software.

Client-Server Communications (Contd.)

- The File Server stores corporate and user files in a central location. The client devices access these files with client software such as Windows Explorer.
- The Web Server runs web server software and clients use their browser software, such as Windows Internet Explorer, to access web pages on the server.
- The Email Server runs email server software and clients use their mail client software, such as Microsoft Outlook, to access email on the server.



Typical Sessions

A typical network user normally uses some type of computing device to establish many connections with network servers. Those servers could be located in the same room or around the world.
Let us see some examples.

At School

- Students are encouraged to use devices such as laptops and tablets to access learning resources.
- Terry, connects to the school's wi-fi network and searches for the required resources using a search engine.
- Her search is submitted wirelessly from her device to the school's network. The search data is addressed so that it can find its way back to Terry.
- The search string of binary data is encoded into radio waves and is converted into electrical signals that travel on the school's wired network to reach the school's Internet Service Provider's (ISP) network.
- A combination of technologies take Terry's search to the search engine website, where the request is processed by the Search Engine's servers.
- The results are then encoded and addressed to her school and eventually to Terry's device.

Typical Sessions (Contd.)

While Gaming

- Michelle uses a gaming console to play games against other players. Her network connects to an ISP using a router and a cable modem that allow her home network to connect to a cable TV network belonging to Michelle's ISP.
- The cable wires for Michelle's neighborhood all connect to a central point on a telephone pole and then connect to a fiber-optic network that connects many neighborhoods served by Michelle's ISP.
- When Michelle connects her gaming console to a company that hosts a popular online game, her actions in her game become data that is sent to the gamer network. Information that identifies Michelle, the game she is playing, and Michelle's network location are added to the game data. The pieces of data that represent Michelle's game play are sent at high speed to the game provider's network.
- The results are returned to Michelle in the form of graphics and sounds.

Typical Sessions (Contd.)

In Medical Consultations

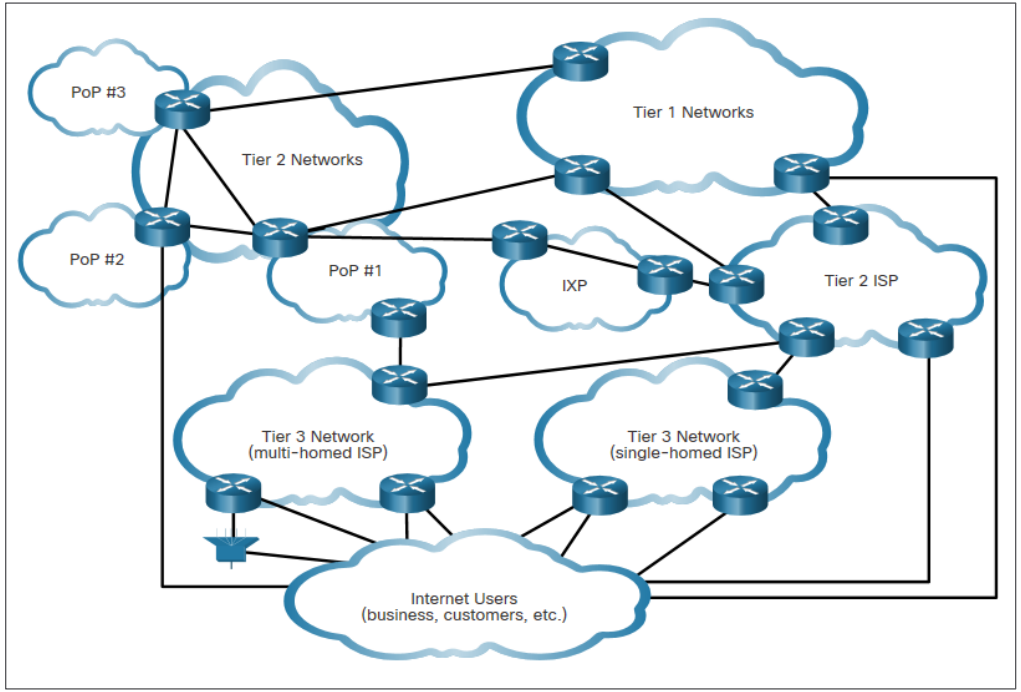
- Dr. Ismael Awad frequently needs to consult with other specialists on patient cases. His hospital has taken subscription to a special service called Cloud that allows medical data including patient x-rays to be stored at a central location that accessible over the internet.
- When a patient has an X-ray taken, the image is digitized as data. The hospital uses network services that encrypt the image data and patient information. This encrypted data cannot be intercepted and read as it travels across the internet to the cloud service provider's data centers. The data is addressed so that it can be routed to the cloud provider's data center to reach the correct services that provide storage and retrieval of high-resolution digital images.
- All of this interaction is digital and takes place using networked services that are provided by the medical cloud service.

Tracing the Path

- Cybersecurity analysts need to have a deep understanding of how networks operate. They must be able to determine the origin of traffic and its destination.
- Traffic from a computer to an internet server can take many paths.

Tracing the Path (Contd.)

- A combination of copper and fiber-optic cables that go over land and under the ocean carry data traffic. These connections connect telecommunications facilities and ISPs distributed throughout the world.
- Global Tier 1 and Tier 2 ISPs connect portions of the internet together, usually through an Internet Exchange Point (IXP).
- Larger networks connect to Tier 2 networks through a Point of Presence (PoP), which is usually a location in the building where physical connections to the ISP are made. The Tier 3 ISPs connect homes and businesses to the internet.



Lab - Tracing a Route

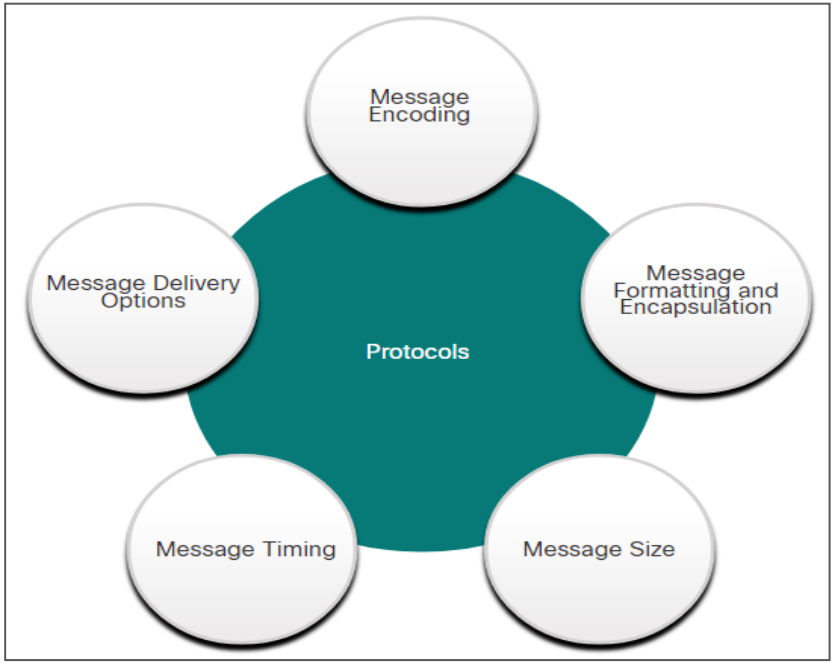
In this lab, you will use two route tracing utilities to examine the internet pathway to destination networks. The objective will be to:

- Verify connectivity to a website
- Use the traceroute utility on the Linux command line
- Use a web-based traceroute tool

5.2 Communications Protocols

What are Protocols?

- Simply having a connection between end devices is not enough to enable communication. For communication to occur, devices must know “how” to communicate.
- Communication is governed by rules called protocols.
- These protocols are specific to the type of communication method occurring.
- Network protocols specify many features of network communication.



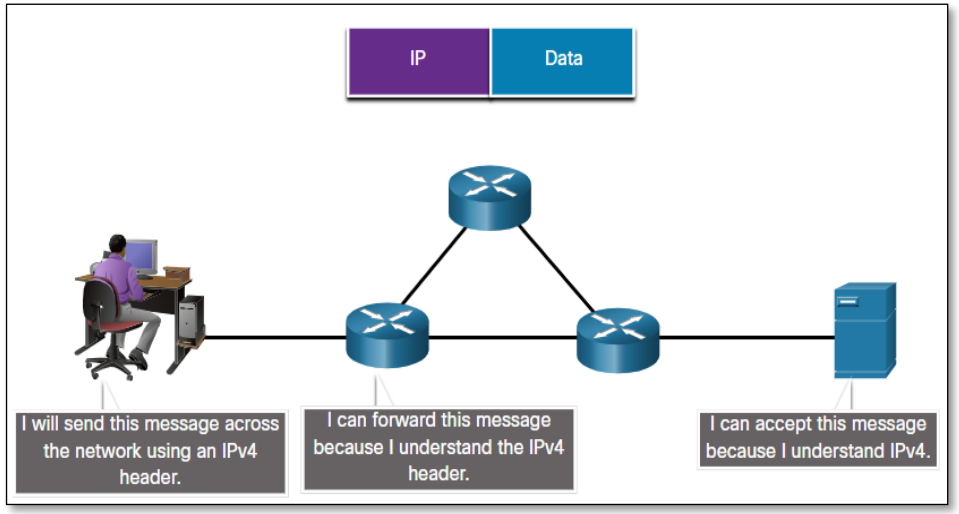
Network Protocols

- Network protocols provide the means for computers to communicate on networks.
- Network protocols dictate the message encoding, formatting, encapsulation, size, timing, and delivery options.
- Networking protocols define a common format and set of rules for exchanging messages between devices.
- Some common networking protocols are Hypertext Transfer Protocol (HTTP), Transmission Control Protocol (TCP), and Internet Protocol (IP).

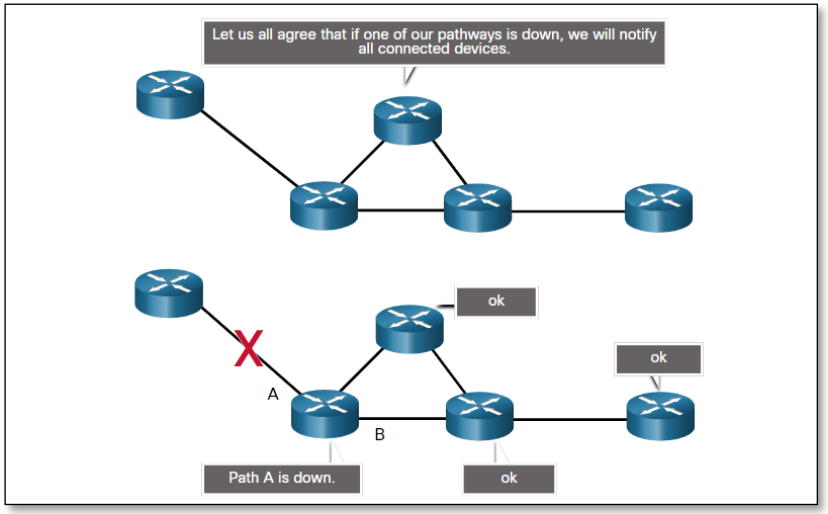
Note: *IP in this course refers to both the IPv4 and IPv6 protocols. IPv6 is the most recent version of IP and will eventually replace the more common IPv4.*

Network Protocols (Contd.)

Message Structure specifies how the message is formatted or structured.

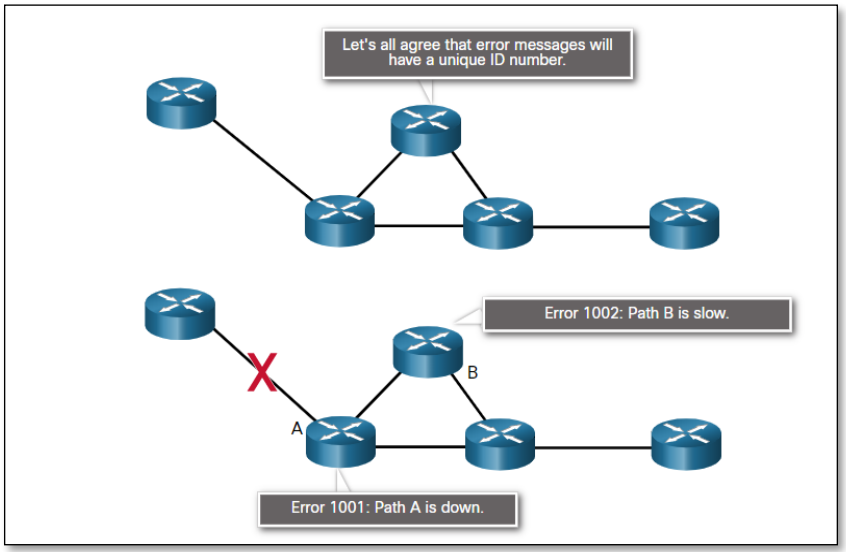


Path Sharing specifies the process by which networking devices share information about pathways with other networks.

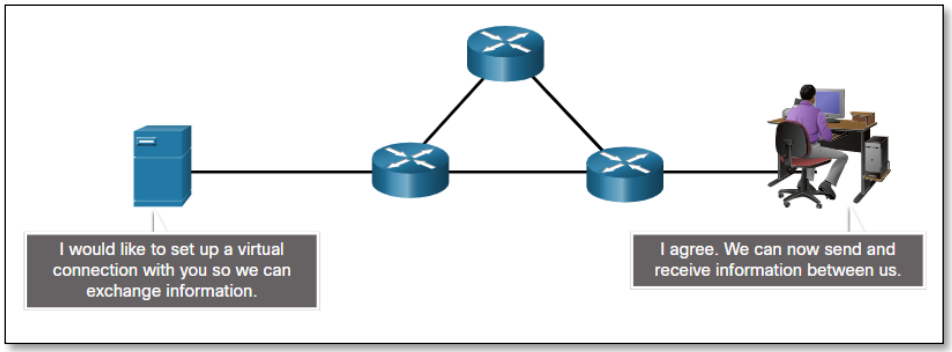


Network Protocols (Contd.)

Information Sharing specifies how and when error and system messages are passed between devices.

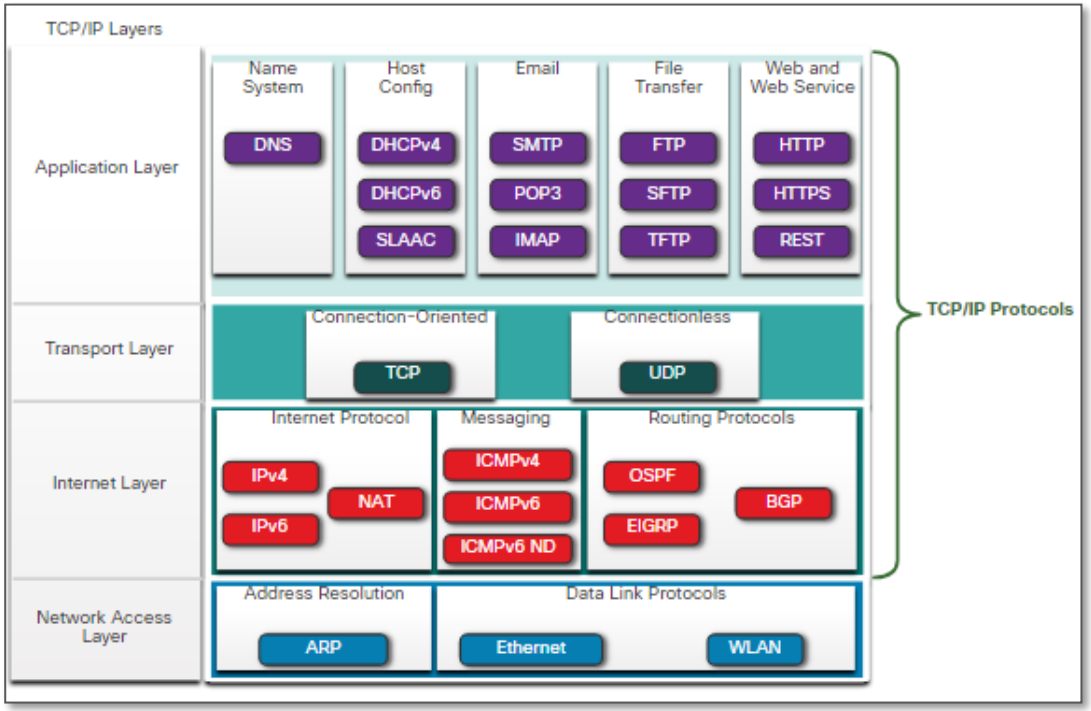


Session Management manages the setup and termination of data transfer sessions.



The TCP/IP Protocol Suite

- TCP/IP is the protocol suite used by the internet and the networks of today.
- TCP/IP has two important aspects for vendors and manufacturers:
  - **Open standard protocol suite** - This means it is freely available to the public and can be used by any vendor on their hardware or in their software.
  - **Standards-based protocol suite** - This means it has been endorsed by the networking industry and approved by a standards organization.



The TCP/IP Protocol Suite (Contd.)

Lets have a look at the brief description of protocols at each layer.

Application Layer

- **Name System - DNS** (Domain Name System): Translates domain names into IP addresses.

Host Config

Protocol	Description
DHCPv4 (Dynamic Host Configuration Protocol for IPv4)	Dynamically assigns IPv4 addressing information to DHCPv4 clients at start-up and allows the addresses to be re-used when no longer needed.
DHCPv6 (Dynamic Host Configuration Protocol for IPv6)	It is similar to DHCPv4. Dynamically assigns IPv6 addressing information to DHCPv6 clients at start-up.
SLAAC (Stateless Address Autoconfiguration)	A method that allows a device to obtain its IPv6 addressing information without using a DHCPv6 server.

The TCP/IP Protocol Suite (Contd.)

Email

Protocol	Description
SMTP (Simple Mail Transfer Protocol)	Enables clients to send email to a mail server and enables servers to send email to other servers.
POP3 (Post Office Protocol version 3)	Enables clients to retrieve email from a mail server and download the email to the client's local mail application.
IMAP (Internet Message Access Protocol)	Enables clients to access email stored on a mail server as well as maintaining email on the server.

File Transfer

Protocol	Description
FTP (File Transfer Protocol)	Sets the rules that enable a user on one host to access and transfer files to and from another host over a network.
SFTP (SSH File Transfer Protocol)	Used to establish a secure file transfer session in which the file transfer is encrypted.
TFTP (Trivial File Transfer Protocol)	A simple and connectionless protocol with best-effort, unrecognized file delivery.

The TCP/IP Protocol Suite (Contd.)

Web and Web Service

Protocol	Description
HTTP (Hypertext Transfer Protocol)	A set of rules for exchanging text, graphic images, sound, video, and other multimedia files on the World Wide Web.
HTTPS (HTTP Secure)	A secure form of HTTP that encrypts the data that is exchanged over the World Wide Web.
REST (Representational State Transfer)	A web service that uses application programming interfaces (APIs) and HTTP requests to create web applications

The TCP/IP Protocol Suite (Contd.)

Transport Layer

- **Connection-Oriented - TCP** (Transmission Control Protocol): Enables reliable communication between processes running on separate hosts and provides reliable transmissions that confirm successful delivery.
- **Connectionless - UDP** (User Datagram Protocol): Enables a process running on one host to send packets to a process running on another host.

The TCP/IP Protocol Suite (Contd.)

Internet Layer

Internet Protocol

Protocol	Description
IPv4 (Internet Protocol version 4)	Receives message segments from the transport layer, packages messages into packets, and addresses packets for end-to-end delivery over a network. IPv4 uses a 32-bit address.
IPv6 (IP version 6)	Similar to IPv4 but uses a 128-bit address.
NAT (Network Address Translation)	Translates IPv4 addresses from a private network into globally unique public IPv4 addresses.

The TCP/IP Protocol Suite (Contd.)

Messaging

Protocol	Description
ICMPv4 (Internet Control Message Protocol for IPv4)	Provides feedback from a destination host to a source host about errors in packet delivery.
ICMPv6 (ICMP for IPv6)	Similar functionality to ICMPv4 but is used for IPv6 packets.
ICMPv6 ND (ICMPv6 Neighbor Discovery)	Includes four protocol messages that are used for address resolution and duplicate address detection.

Routing Protocols

Protocol	Description
OSPF (Open Shortest Path First)	Link-state routing protocol that uses a hierarchical design based on areas. OSPF is an open standard interior routing protocol.
EIGRP (Enhanced Interior Gateway Routing Protocol)	A Cisco proprietary routing protocol that uses a composite metric based on bandwidth, delay, load and reliability.
BGP (Border Gateway Protocol)	An open standard exterior gateway routing protocol used between Internet Service Providers (ISPs).

The TCP/IP Protocol Suite (Contd.)

Network Access Layer

- **Address Resolution - ARP** (Address Resolution Protocol): Provides dynamic address mapping between an IPv4 address and a hardware address.
- **Data Link Protocols -**
  - **Ethernet**: Defines the rules for wiring and signaling standards of the network access layer.
  - **WLAN** (Wireless Local Area Network): Defines the rules for wireless signaling across the 2.4 GHz and 5 GHz radio frequencies.

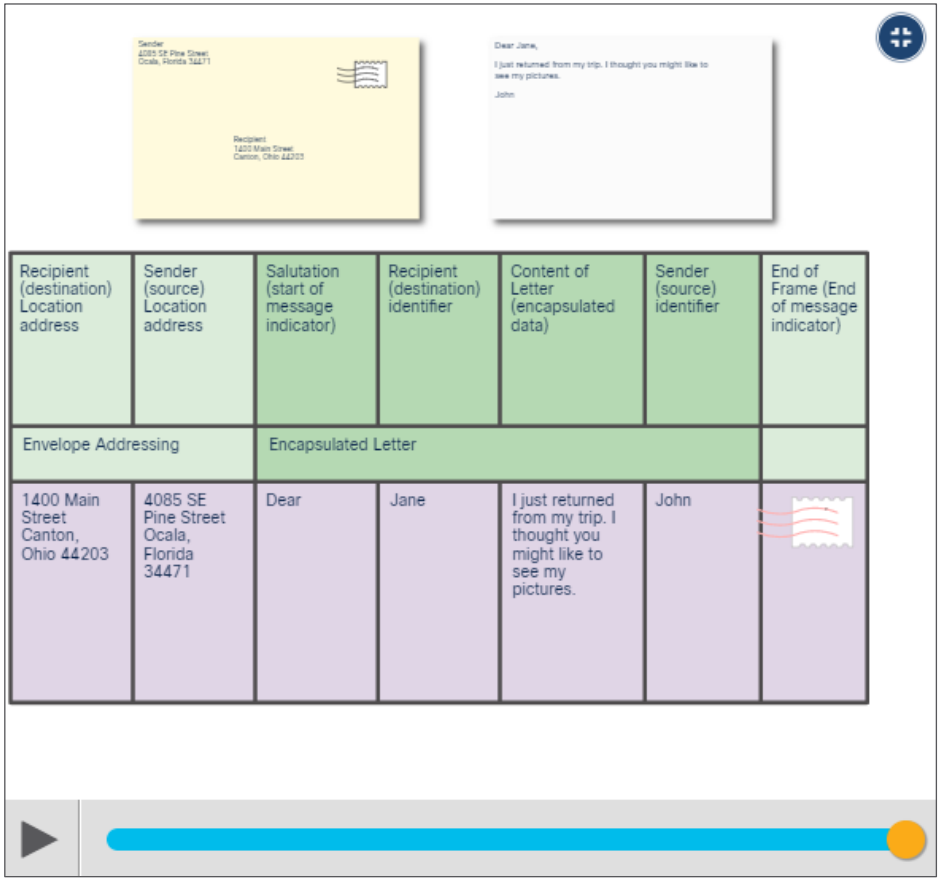
Message Formatting and Encapsulation

- When a message is sent from source to destination, 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.

Message Formatting and Encapsulation (Contd.)

Analogy:

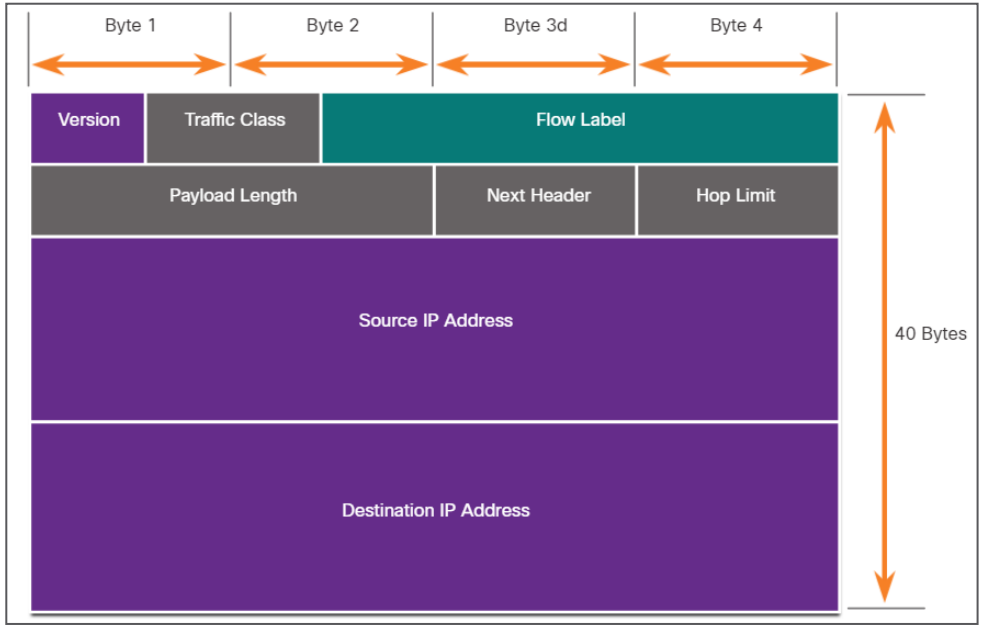
- When sending a letter, correct format is required. An envelope has the address of the sender and receiver, each located at the proper place on the envelope.
- The process of placing one message format (the letter) inside another message format (the envelope) is called encapsulation.
- De-encapsulation occurs when the process is reversed by the recipient and the letter is removed from the envelope.



Message Formatting and Encapsulation (Contd.)

Network:

- Similar to sending a letter, a message that is sent over a computer network follows specific format rules for it to be delivered and processed.
- Internet Protocol (IP) is a protocol with a similar function to the envelope example.
- IP is responsible for sending a message from the message source to destination over one or more networks.

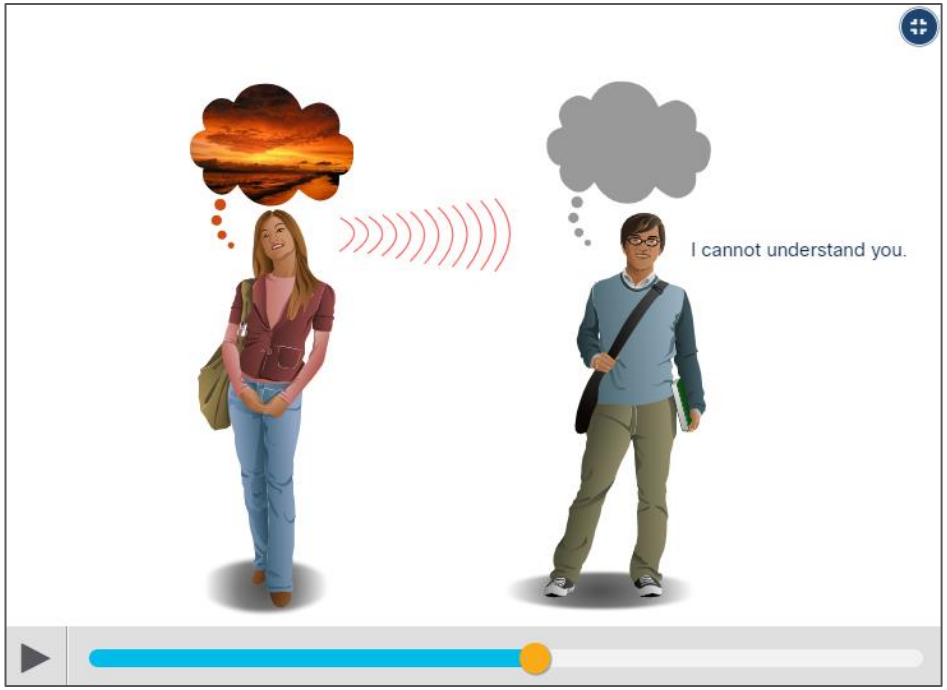


Message Size

Another rule of communication is message size.

Analogy:

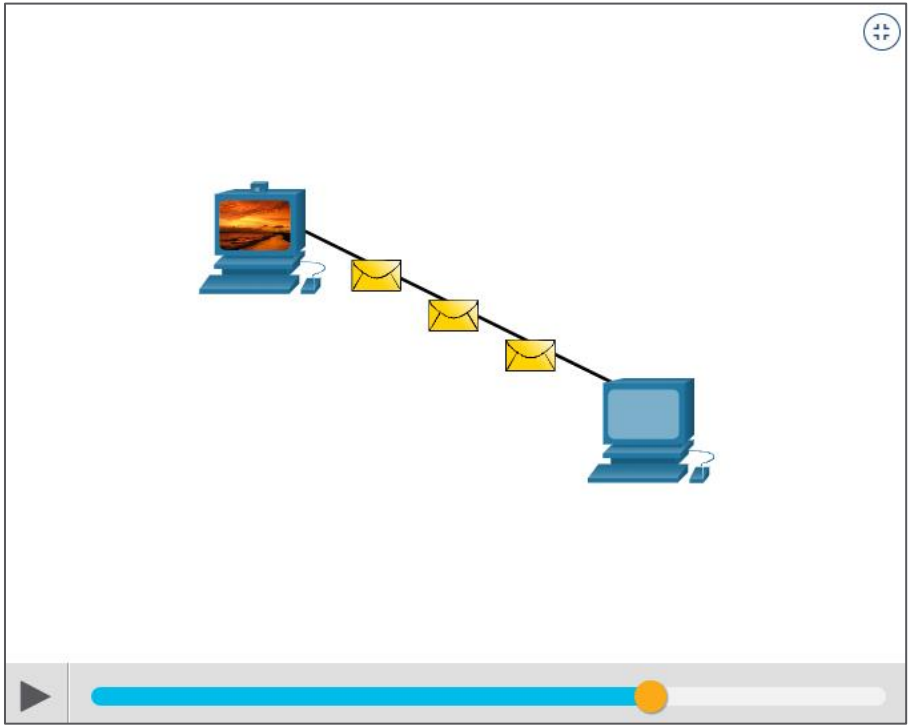
- When people communicate with each other, the messages that they send are usually broken into smaller parts or sentences.
- These sentences are limited in size to what the receiving person can process at one time. It also makes it easier for the receiver to read and comprehend.



Message Size (Contd.)

Network:

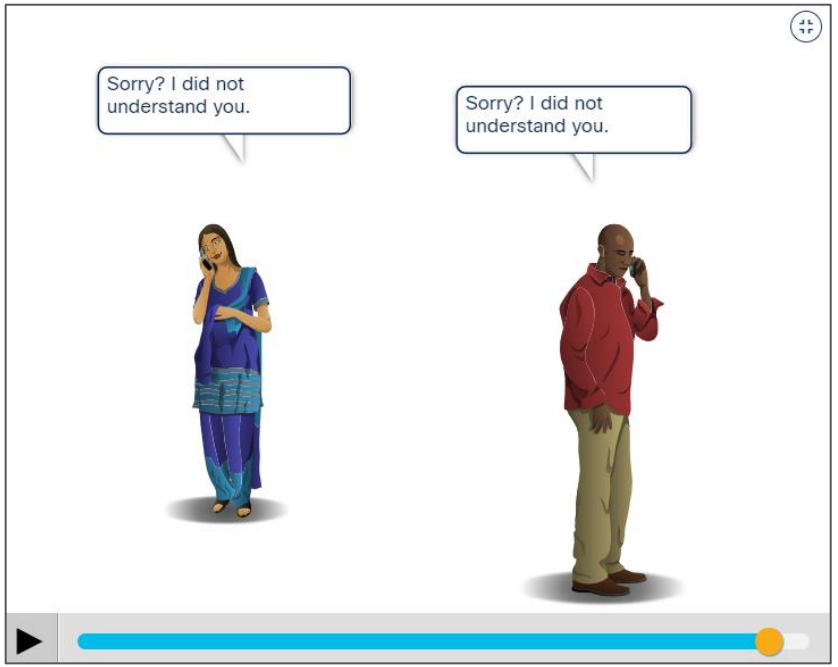
- Encoding between hosts must be in an appropriate format for the medium.
- Messages sent across the network are first converted into bits by the sending host
- Each bit is encoded into a pattern of sounds, light waves, or electrical impulses depending on the network media over which the bits are transmitted.
- The destination host receives and decodes the signals to interpret the message.



Message Timing

Message timing includes the following:

- **Flow Control -** Flow control defines how much information can be sent and the speed at which it can be delivered.
- **Response Timeout -** Hosts on the network use network protocols that specify how long to wait for responses and what action to take if a response timeout occurs.
- **Access method -** This determines when someone can send a message. When a device wants to transmit on a wireless LAN, it is necessary for the WLAN NIC to determine whether the wireless medium is available.



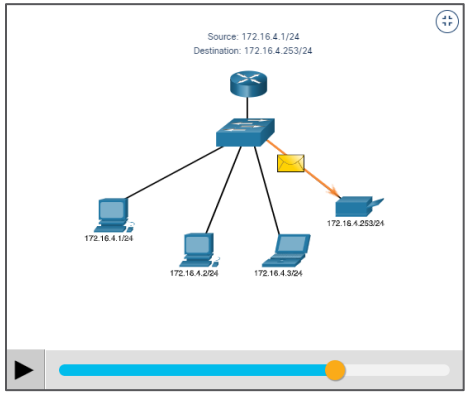
Unicast, Multicast, and Broadcast

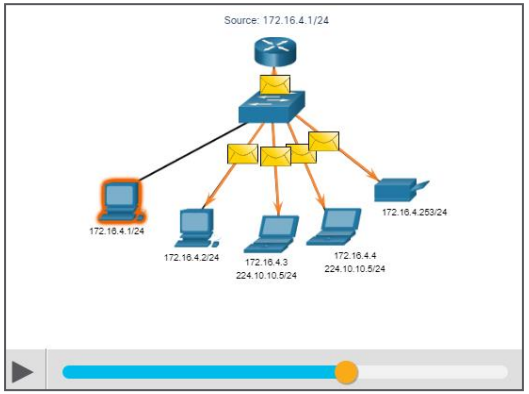
A message can be delivered in different ways. Hosts on a network various delivery options to communicate. The different methods of communication are called as unicast, multicast, and broadcast.

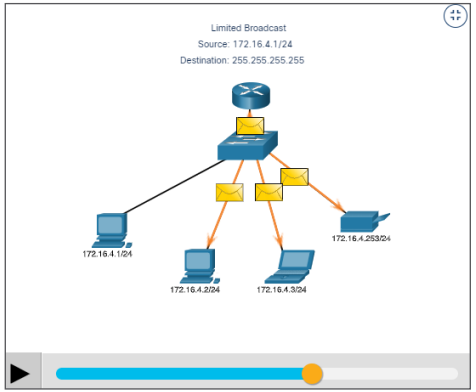
Unicast: A one-to-one delivery option means there is only a single destination for the message.

Multicast: When a host needs to send messages using a one-to many delivery option.

Broadcast: If all hosts on the network need to receive the message at the same time, a broadcast may be used. Broadcasting represents a one-to-all message delivery option.







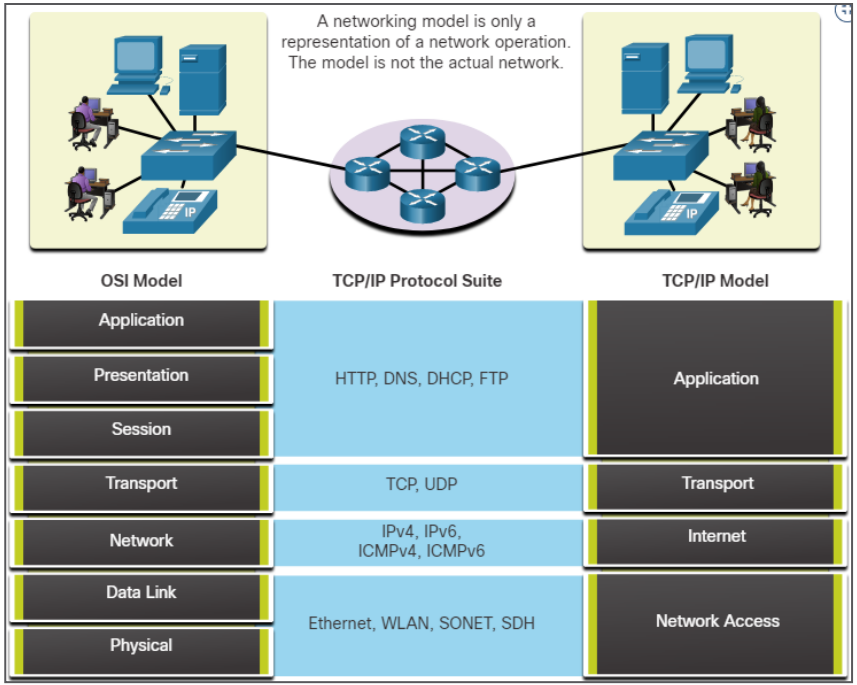
The Benefits of Using a Layered Model

A layered model is used to modularize the operations of a network into manageable layers. These are the benefits of using a layered model:

- Assisting in protocol design
- Fostering competition
- Preventing technology or capability changes
- Providing a common language

Two layered models that are used to describe network operations are:

- Open System Interconnection (OSI) Reference Model
- TCP/IP Reference Model



The OSI Reference Model

- The OSI reference model provides list of functions and services that can occur at each layer.
- This type of model provides consistency within all types of network protocols and services by describing what must be done at a particular layer, but not prescribing how it should be accomplished.
- It also describes the interaction of each layer with the layers directly above and below.
- Note that while the TCP/IP model layers are referred only by name but the seven OSI model layers are more often referred by number rather than by name.

The OSI Reference Model (Contd.)

OSI Model Layer	Description
7 - Application	Contains protocols used for process-to-process communications
6 - Presentation	Provides representation of the data transferred between application layer services
5 - Session	Provides services to the presentation layer to organize its dialogue and to manage data exchange
4 - Transport	Defines services to segment, transfer, and reassemble the data for individual communications between the end devices
3 - Network	Provides services to exchange the individual pieces of data over the network
2 - Data Link	Describe methods for exchanging data frames between devices over a common media
1 - Physical	Describe the mechanical, electrical, functional, and procedural means to activate, maintain, and de-activate physical connections for a bit transmission between devices

The TCP/IP Protocol Model

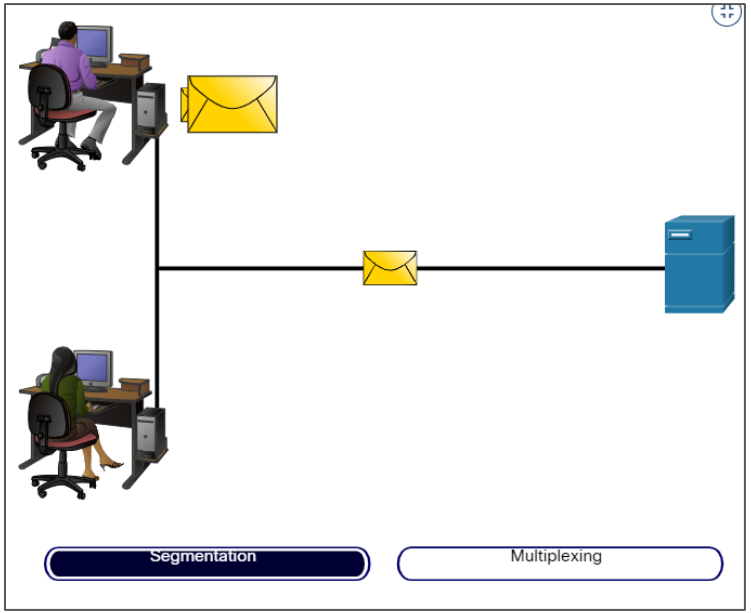
- The TCP/IP protocol model is also referred to as the internet model.
- It describes the functions that occur at each layer of protocols within the TCP/IP suite. TCP/IP is also used as a reference model.

TCP/IP Model Layer	Description
4 - Application	Represents data to the user, plus encoding and dialog control
3 - Transport	Supports communication between various devices across diverse networks
2 - Internet	Determines the best path through the network
1 - Network Access	Controls the hardware devices and media that make up the network

5.3 Data Encapsulation

Segmenting Messages

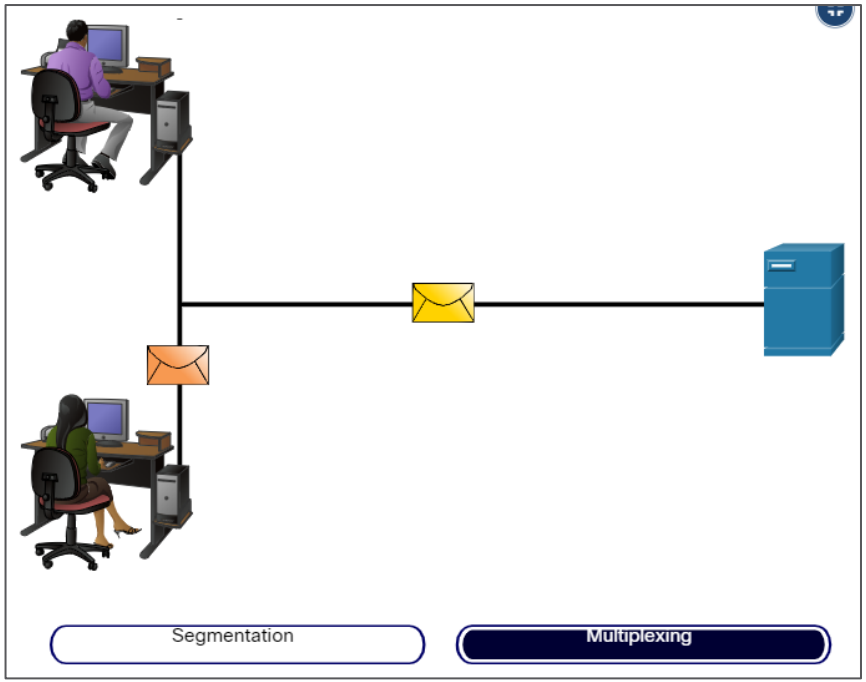
- If large streams of data is sent across a network, it would result in delays. If any link in the interconnected network failed during the transmission, it will result in lost of complete message.
- Segmentation is the process of dividing a stream of data into smaller units for transmissions over the network.
- Segmentation is necessary as networks use the TCP/IP protocol to send data in individual IP packets. Each packet is sent separately and the packets containing segments for the same destination can be sent over different paths.



Segmenting Messages (Contd.)

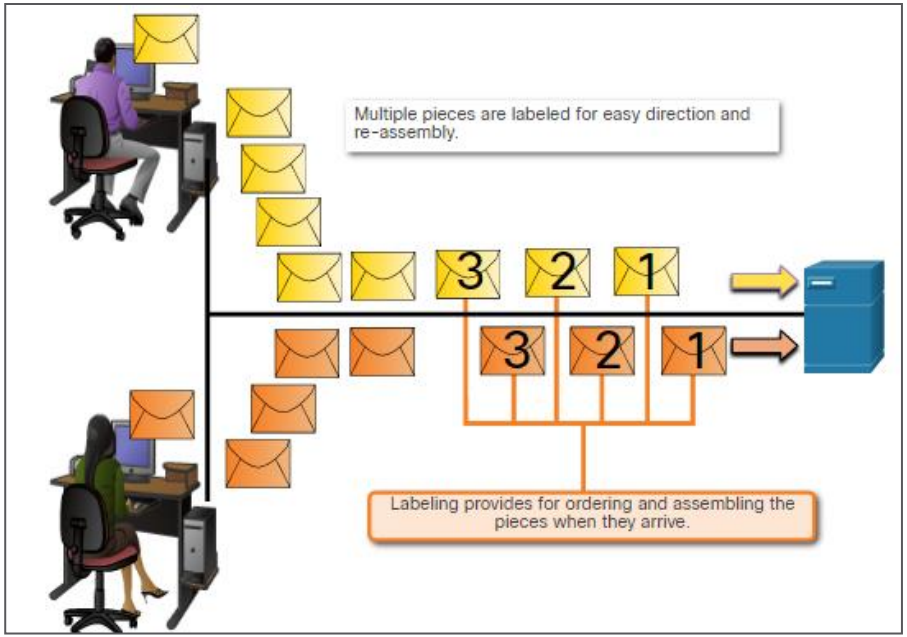
Benefits of segmenting messages:

- **Increases speed** - As a large data stream is segmented into packets, more data can be sent over the network without tying up a communications link. This allows many different conversations to be interleaved on the network called multiplexing.
- **Increases efficiency** - If a single segment fails to reach its destination, only that segment needs to be retransmitted instead of resending the entire data stream.



Sequencing

- While transmitting messages using segmentation and multiplexing, there is a possibility of data to reach the destination in a collapsed order.
- Each segment of the message must go through a sequencing process to ensure that it gets to the correct destination and can be reassembled similar to the content of the original message.
- TCP is responsible for sequencing the individual segments



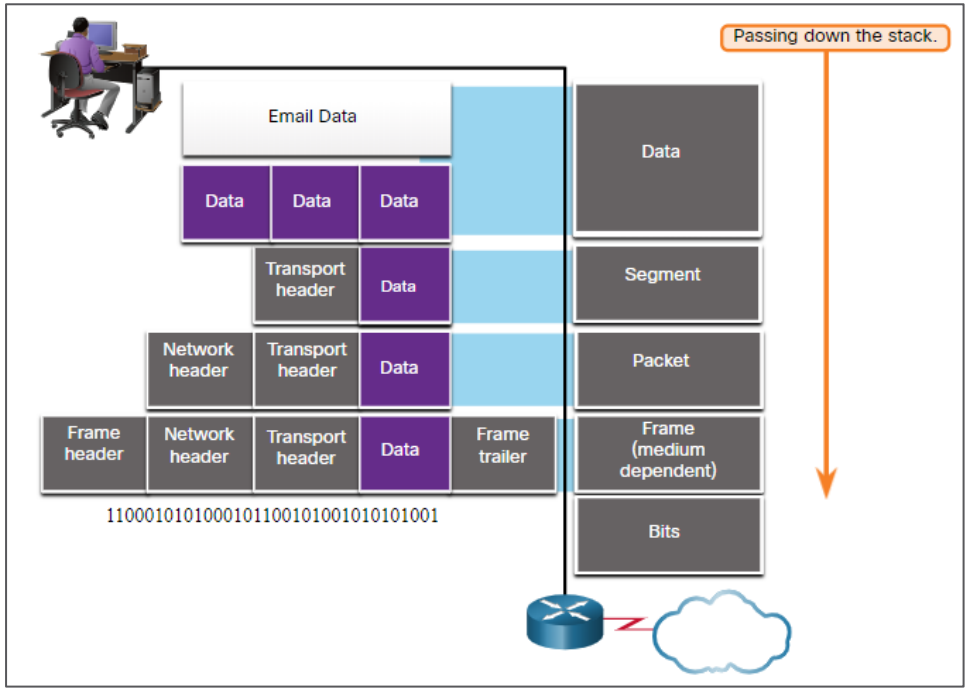
Protocol Data Units

- As application data is passed down the protocol stack on its way to be transmitted across the network media, various protocol information is added at each level. This is known as the encapsulation process.
- The form that a piece of data takes at any layer is called a Protocol Data Unit (PDU).
- During encapsulation, each succeeding layer encapsulates the PDU that it receives from the layer above in accordance with the protocol being used.
- At each stage of the process, a PDU has a different name to reflect its new functions.

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

Protocol Data Units (Contd.)

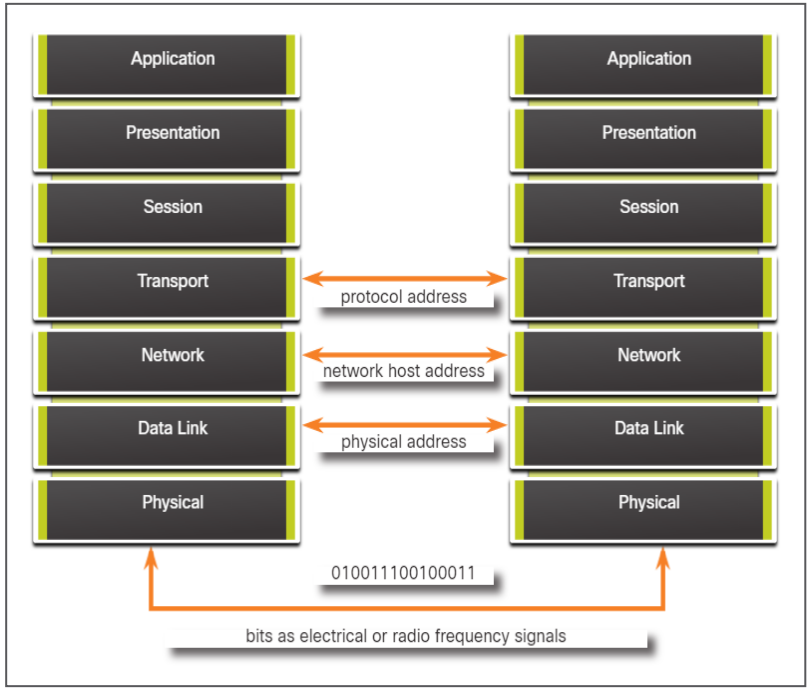
- The PDUs for each form of data are:
  - Data - The general term for the PDU used at the application layer
  - Segment - Transport layer PDU
  - Packet - Network layer PDU
  - Frame - Data Link layer PDU
  - Bits - Physical layer PDU used when physically transmitting data over the medium



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

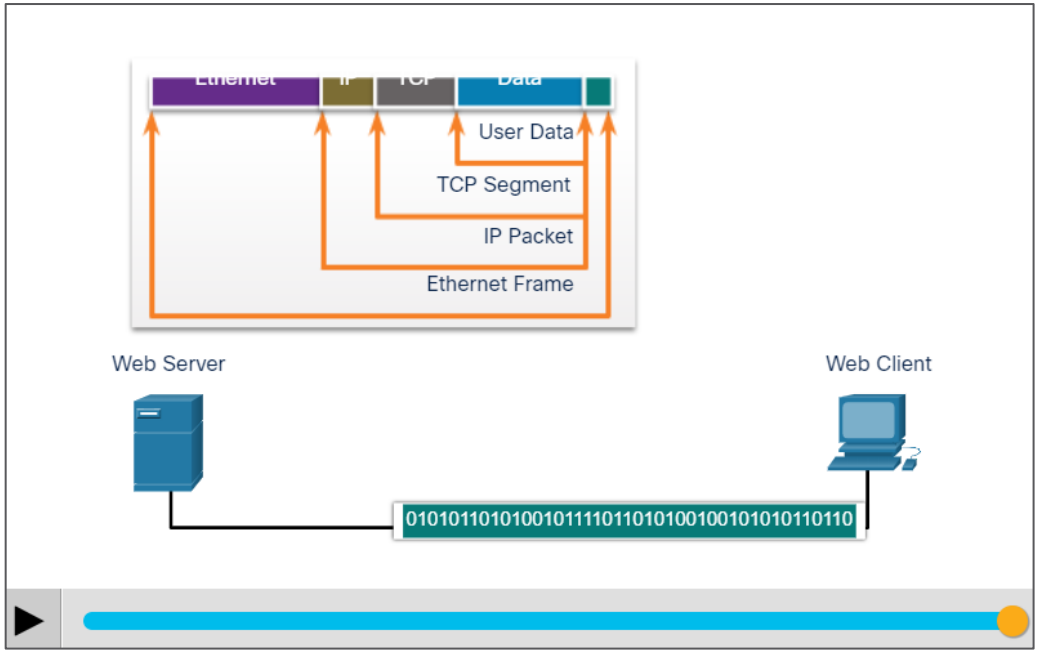
Three Addresses

- Network protocols require addresses to be used for network communication.
- The OSI transport, network, and data link layers use addressing in some form.
- The transport layer uses protocol addresses in the form of port numbers to identify network applications.
- The network layer specifies addresses that identify the networks that clients and servers are attached to.
- Data link layer specifies the devices on the local LAN that should handle data frames.
- All three addresses are required for client-server communication.



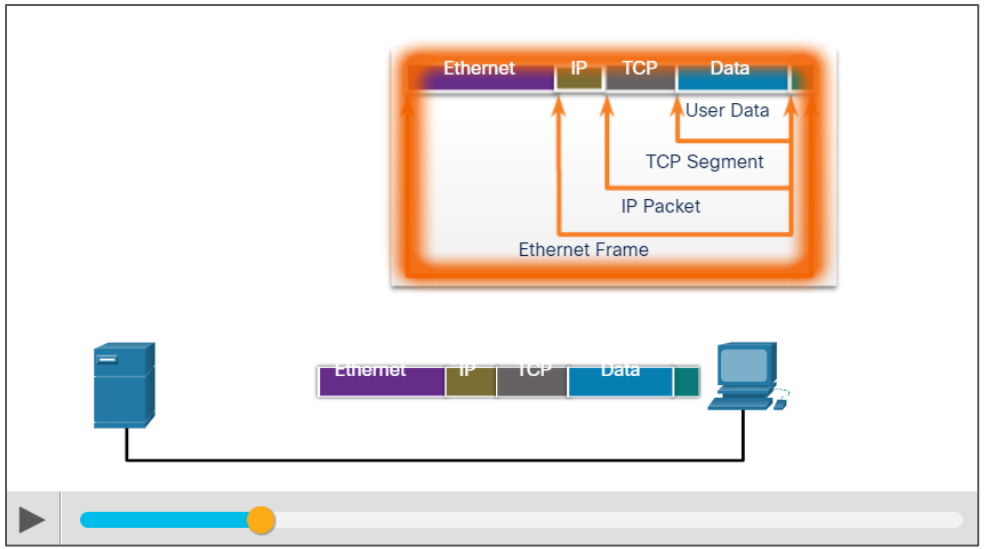
Encapsulation Example

- When messages are being sent on a network, the encapsulation process works from top to bottom.
- At each layer, the upper layer information is considered data within the encapsulated protocol. For example, the TCP segment is considered data within the IP packet.



De-encapsulation Example

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



Lab - Introduction to Wireshark

Wireshark is a software protocol analyzer, or "packet sniffer" application, used for network troubleshooting, analysis, software and protocol development, and education.

In this lab, you will use Wireshark to capture and analyze network traffic.

5.4 Network Protocols Summary

What Did I Learn in this Module?

- Networks come in all sizes and can be found in homes, businesses, and other organizations. The internet is the largest network in existence.
- Servers are hosts that use specialized software to enable them to respond to requests for different types of data from clients.
- Clients are hosts that use software applications such as web browsers, email clients, or file transfer applications to request data from servers.
- Larger businesses may connect to Tier 2 ISPs through a Point of Presence (POP).
- Tier 3 ISPs connect homes and businesses to the internet
- Network protocols specify many features of network communication such as message encoding, message formatting and encapsulation, and delivery options.
- Protocols specify how messages are structured and the way that networking devices share information about pathways to other networks.

What Did I Learn in this Module? (Contd.)

- Common protocols at the application layer of the suite are DNS, DHCP, POP3, and HTTPS.
- The OSI model has seven layers. The TCP/IP model has four layers.
- Data is broken into a series of smaller pieces and sent over the network. This is called segmentation.
- Increased speed is gained because many data conversations can happen at the same time on the network. This is called multiplexing.
- As data is passed down the protocol stack to be sent, different information is added by each layer. This process is called encapsulation.
- The form that data takes at different layer is called a protocol data unit (PDU)
- De-encapsulation is the process used by a receiving device to remove one or more of the protocol headers.


CISCO