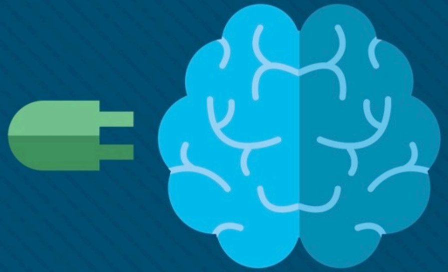
Chapter 3: Network Protocols and Services

Information Security



Dr. Ayman Aljarbouh

3.1 Network Protocols

Module Objectives

Module Title: Network Protocols

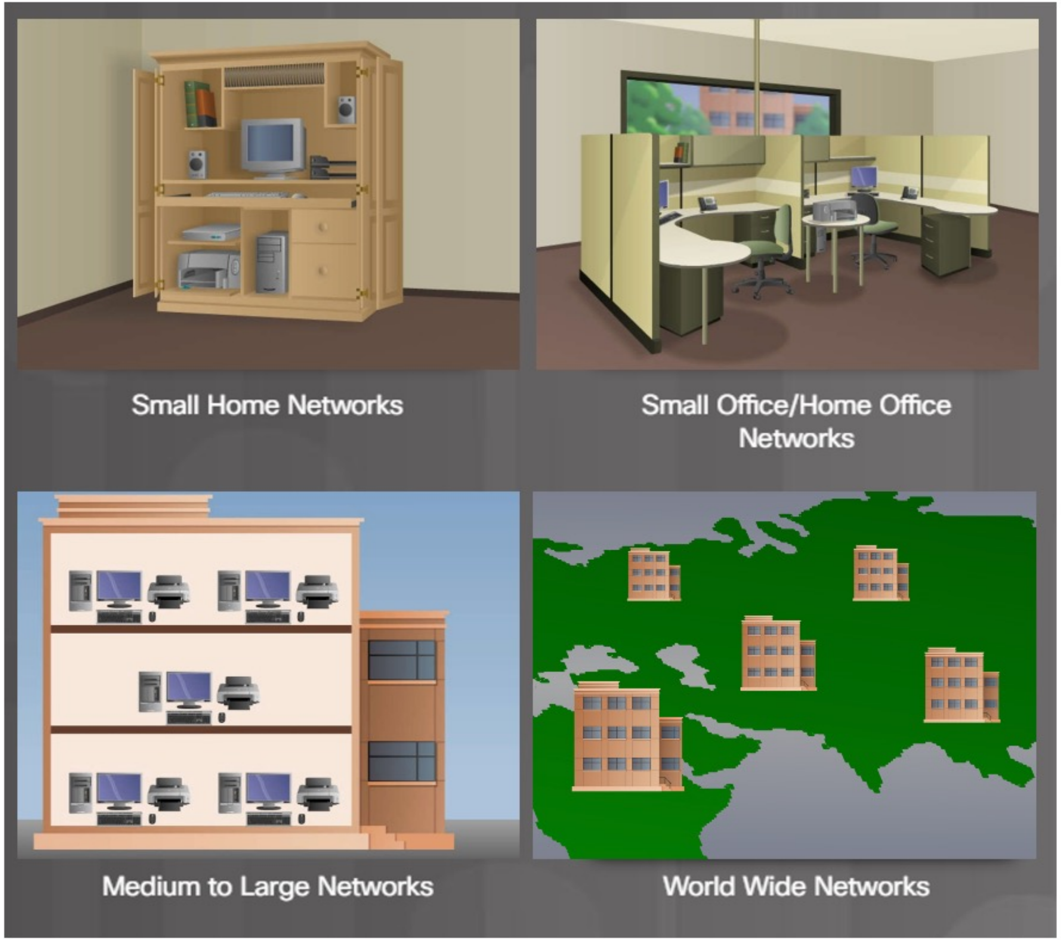
Module Objective: Explain how protocols enable network operations.

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.

Network Communications Process

Views of the Network

- Views of the network
  - Small home network
  - SOHO (Small Office/Home Office)
  - Medium to large networks
  - World-wide networks



Small Home Networks

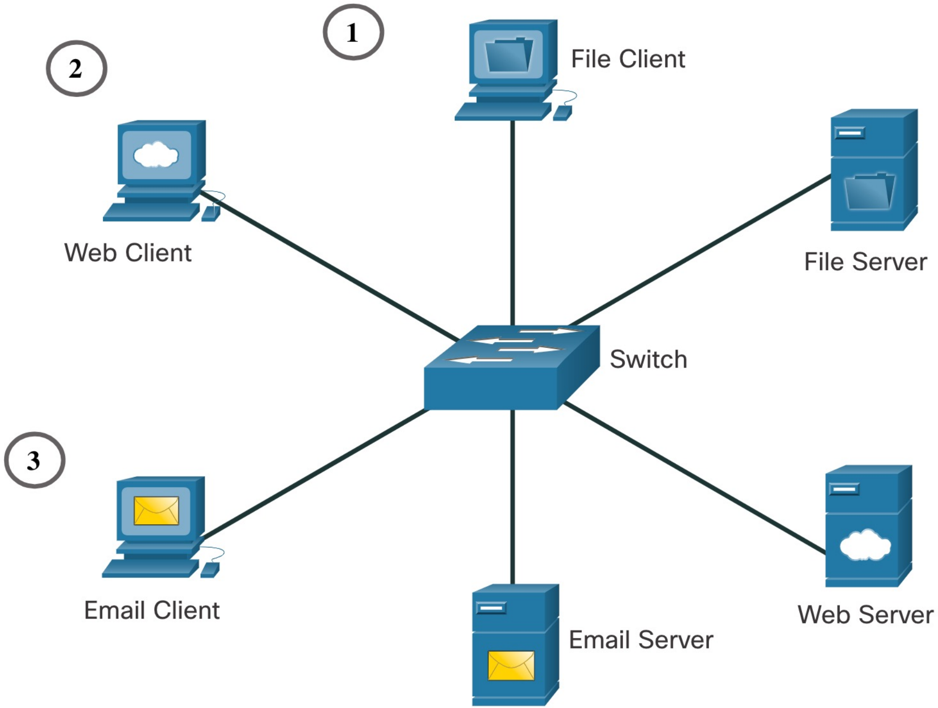
Small Office/Home Office Networks

Medium to Large Networks

World Wide Networks

Client-Server Communications

- File Client and Server communications
  - Server stores corporate and user files.
  - Client devices access these files or services with client software.
- Web Client Server
  - Web Server runs web server software and client uses browser software.
- Email Client-Server communications
  - Email Server runs email server software.



A Typical Session: Student

- A Typical Session: Student
  - Determine the origin of the traffic enter the network.
  - For example, Terry’s data flows with the data of thousands of other users along a fiber-optic network that connects Terry’s ISP with the several other ISPs, including the ISP that is used by the search engine company. Eventually, Terry’s search string enters the search engine company’s website and is processed by its powerful servers. The results are then encoded and addressed to Terry’s school and her device.

A Typical Session: Gamer

- A Typical Session: Gamer
  - Determine the origin of the traffic enter the network.
  - Michelle’s network, like many home networks, connects to an ISP using a router and modem. These devices allow Michelle’s home network to connect to a cable TV network that belongs 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. This fiber-optic network connects many neighborhoods that are served by Michelle’s ISP.

Network Communications Process

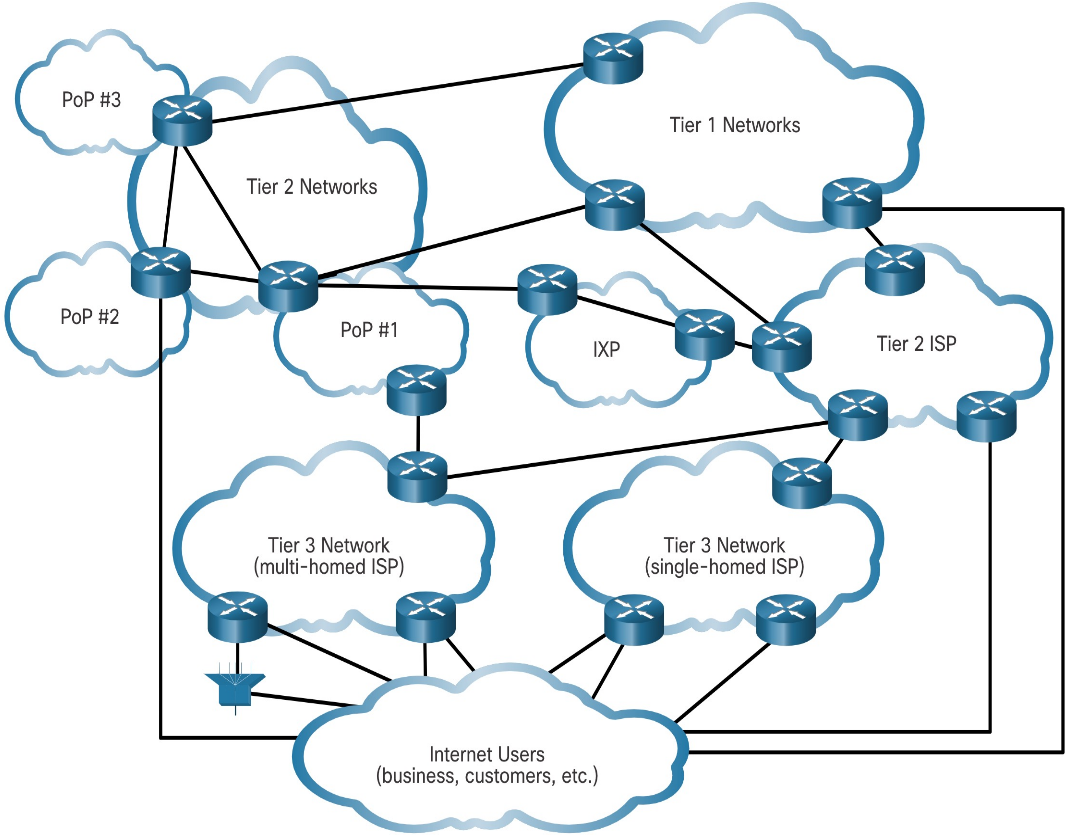
A Typical Session: Surgeon

- A Typical Session: Surgeon
  - Determine the origin of the traffic enter the network
  - Dr. Ismael Awad is an oncologist who performs surgery on cancer patients. He frequently needs to consult with radiologists and other specialists on patient cases. The hospital that Dr. Awad works for subscribes to a special service called a cloud. The cloud allows medical data, including patient x-rays and MRIs to be stored in a central location that is accessed over the Internet.

Network Communications Process

Tracing the Path

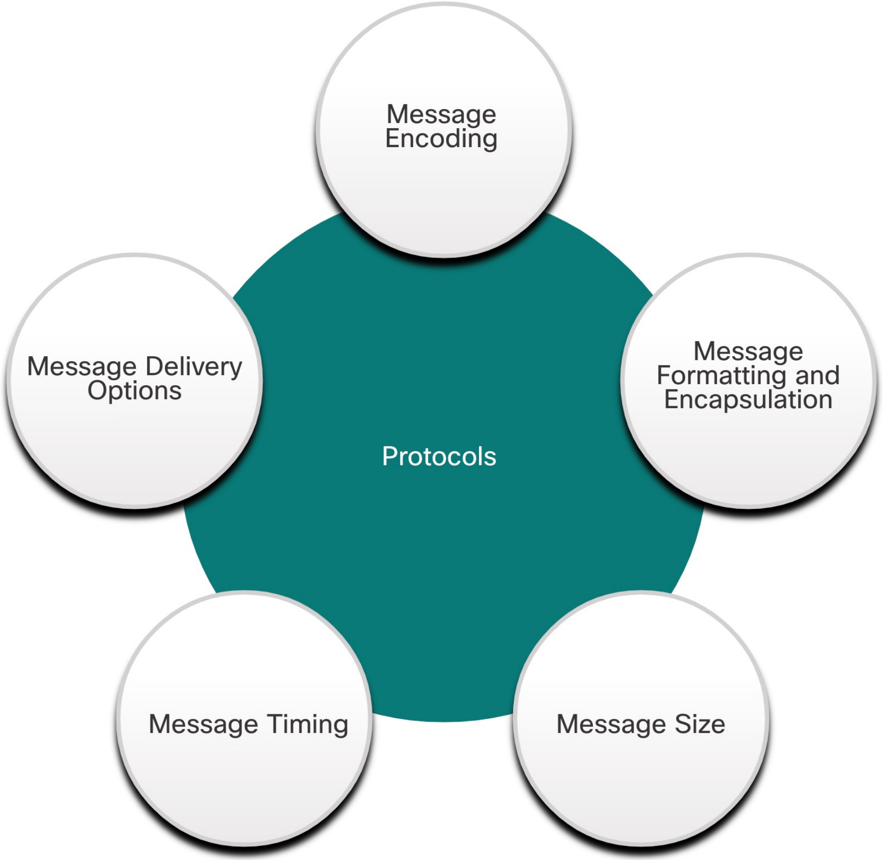
- Cybersecurity analysts must be able to determine the origin of traffic that enters the network, and the destination of traffic that leaves it. Understanding the path that network traffic takes is essential to this.
- Tier 1 Network and Tier 2 networks usually connect through an Internet Exchange Point (IXP).
- Larger networks connect to Tier 2 networks, usually through a Point of Presence (POP).
- Tier 3 ISPs connect homes and businesses to the Internet.



Communications Protocols

What are Protocols?

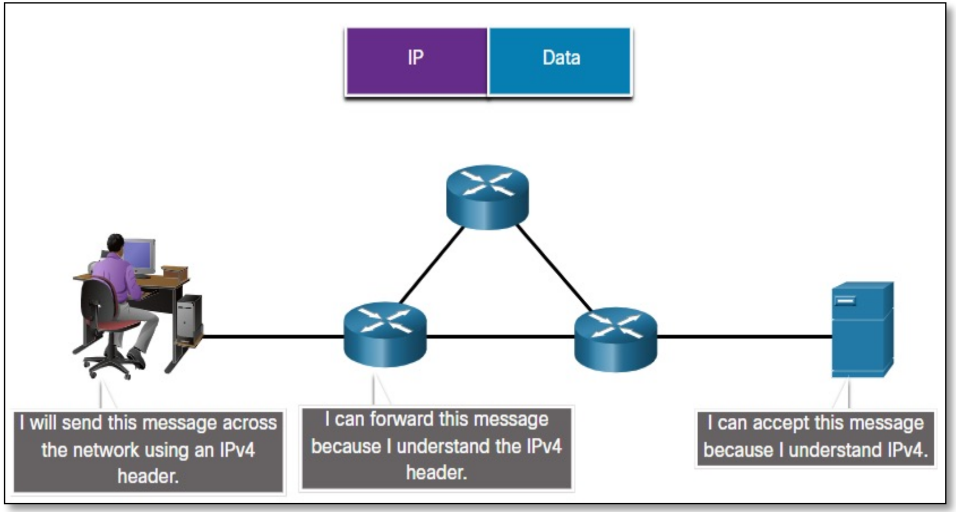
- Protocol – The rules of communications
  - Network protocols provide the means for computers to communicate on networks.
  - Network protocols dictate the message encoding, formatting, encapsulation, size, timing, and delivery options.
  - Some common networking protocols are Hypertext Transfer Protocol (HTTP), Transmission Control Protocol (TCP), and Internet Protocol (IP).



Network Protocol

Message Structure specifies how the message is formatted or structured.

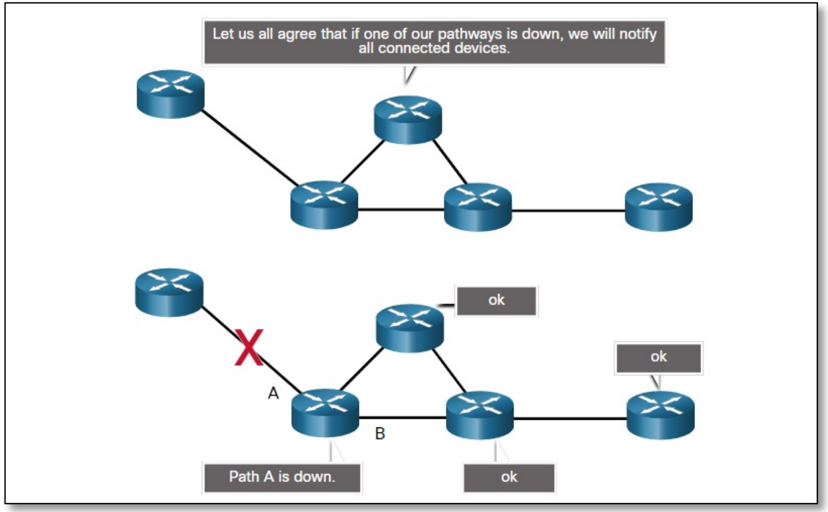
Path Sharing specifies the process by which networking devices share information about pathways with other networks.



I will send this message across the network using an IPv4 header.

I can forward this message because I understand the IPv4 header.

I can accept this message because I understand IPv4.

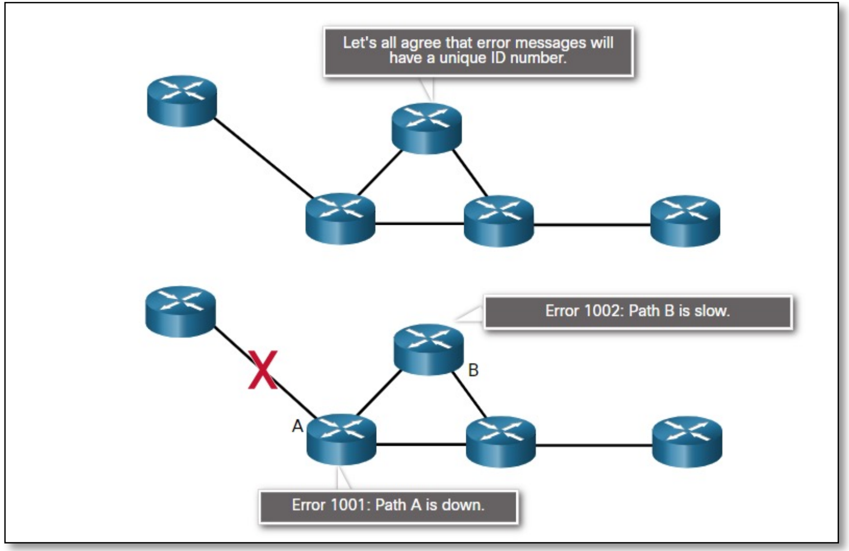

Let us all agree that if one of our pathways is down, we will notify all connected devices.

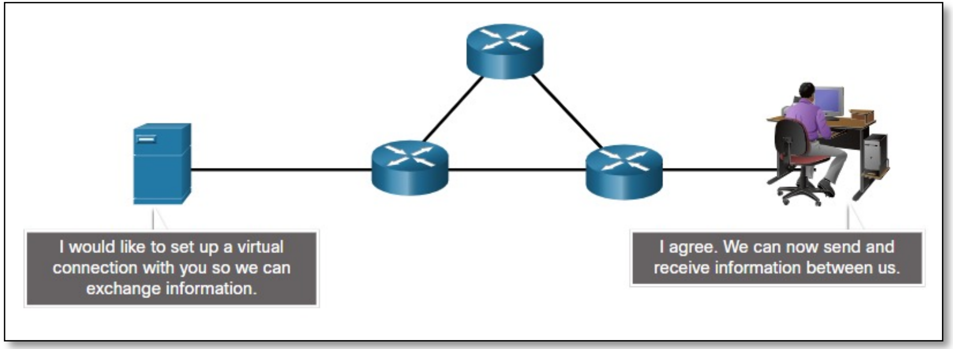
Path A is down.

Network Protocol

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.

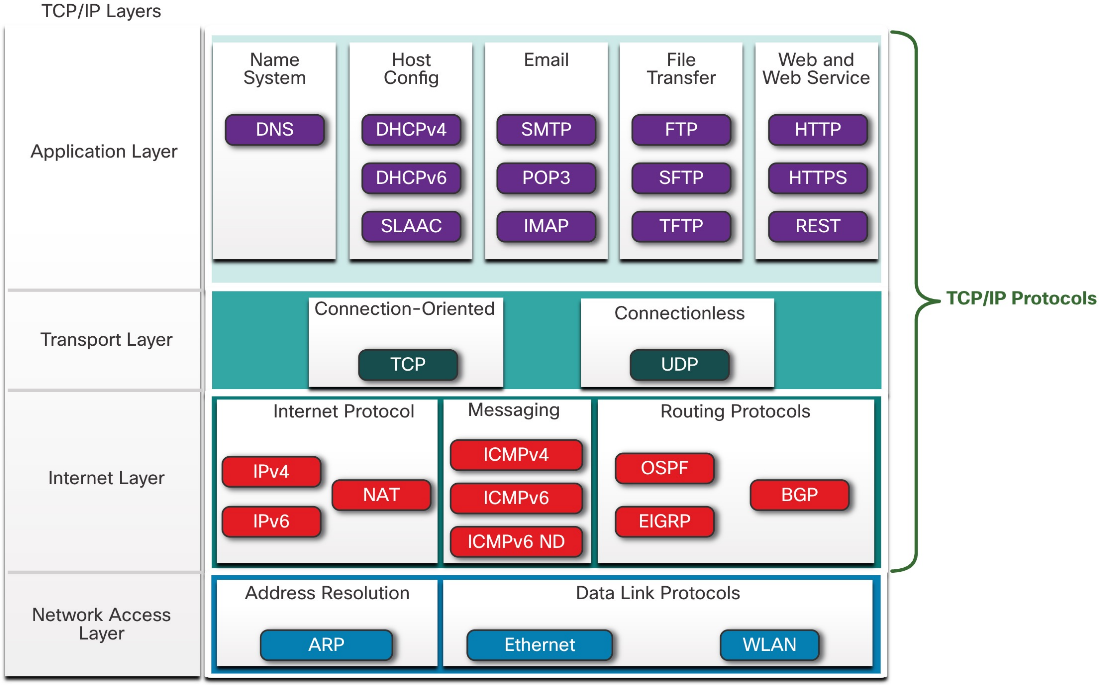

Let's all agree that error messages will have a unique ID number.
Error 1002: Path B is slow.
B
A
Error 1001: Path A is down.


I would like to set up a virtual connection with you so we can exchange information.
I agree. We can now send and receive information between us.

Communications Protocols

The TCP/IP Protocol Suite

- TCP/IP has standardized the way the computers communicate.
- TCP/IP protocols are specific to the application, transport, Internet, and network access layers.
- TCP/IP protocol suite is implemented on both the sending and receiving hosts to provide end-to-end delivery of messages over a network.



TCP/IP Layers

Application Layer

Name System: DNS

Host Config: DHCPv4, DHCPv6, SLAAC

Email: SMTP, POP3, IMAP

File Transfer: FTP, SFTP, TFTP

Web and Web Service: HTTP, HTTPS, REST

Transport Layer

Connection-Oriented: TCP

Connectionless: UDP

Internet Layer

Internet Protocol: IPv4, IPv6, NAT

Messaging: ICMPv4, ICMPv6, ICMPv6 ND

Routing Protocols: OSPF, EIGRP, BGP

Network Access Layer

Address Resolution: ARP

Data Link Protocols: Ethernet, WLAN

TCP/IP Protocols

Communications Protocols

The TCP/IP Protocol Suite (Contd.)

Let's 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.

Communications Protocols

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.

Communications Protocols

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

Communications Protocols

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.

Communications Protocols

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.)

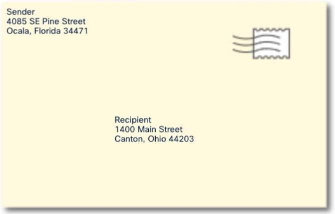
Network Access Layer

- **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.

Communications Protocols

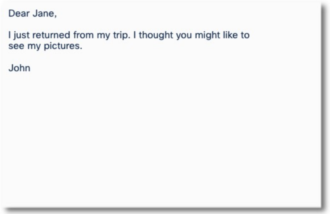
Format, Size, and Timing

- **Format**
  - **Encapsulation** - process of placing one message format inside another message format.
  - **Decapsulation** - the reverse process of encapsulation.
- **Size** – Message is broken up into many frames when sent and reconstructed into the original message when received.
- **Timing** – includes the access method, flow control, and response timeout.



Sender
4085 SE Pine Street
Ocala, Florida 34471

Recipient
1400 Main Street
Canton, Ohio 44203



Dear Jane,

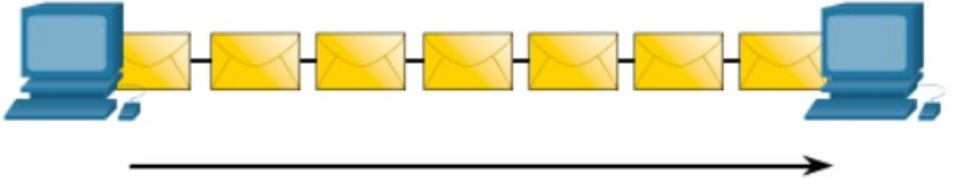
I just returned from my trip. I thought you might like to see my pictures.

John

Recipient (destination) Location address	Sender (source) Location address	Salutation (start of message indicator)	Recipient (destination) identifier	Content of Letter (encapsulated data)	Sender (source) identifier	End of Frame (End of message indicator)
Envelope Addressing		Encapsulated Letter				
1400 Main Street Canton, Ohio 44203	4085 SE Pine Street Ocala, Florida 34471	Dear	Jane	I just returned from my trip. I thought you might like to see my pictures.	John	

Format, Size, and Timing

- **Format**
  - **Encapsulation** - process of placing one message format inside another message format.
  - **Decapsulation** - the reverse process of encapsulation.
- **Size** – Message is broken up into many frames when sent and reconstructed into the original message when received.
- **Timing** – includes the access method, flow control, and response timeout.



The email message and attachment are broken up into many frames and then sent on the network.

Communications Protocols

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.

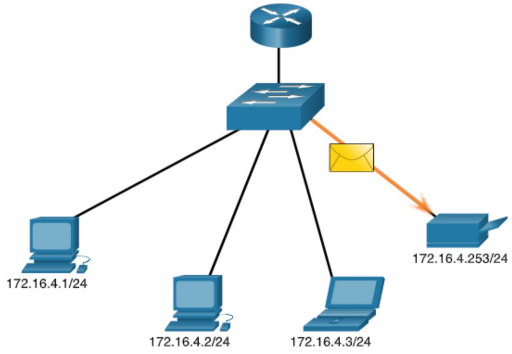
Unicast: A one-to-one delivery option means there is only a single destination for the message.

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.

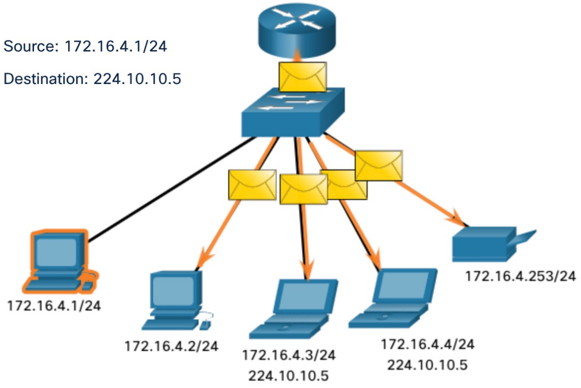
Source: 172.16.4.1/24

Destination: 172.16.4.253/24



Source: 172.16.4.1/24

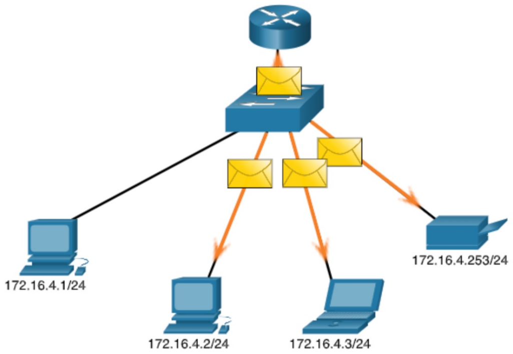
Destination: 224.10.10.5



Limited Broadcast

Source: 172.16.4.1/24

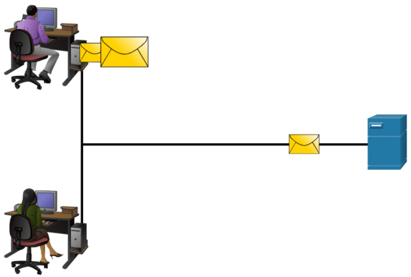
Destination: 255.255.255.255

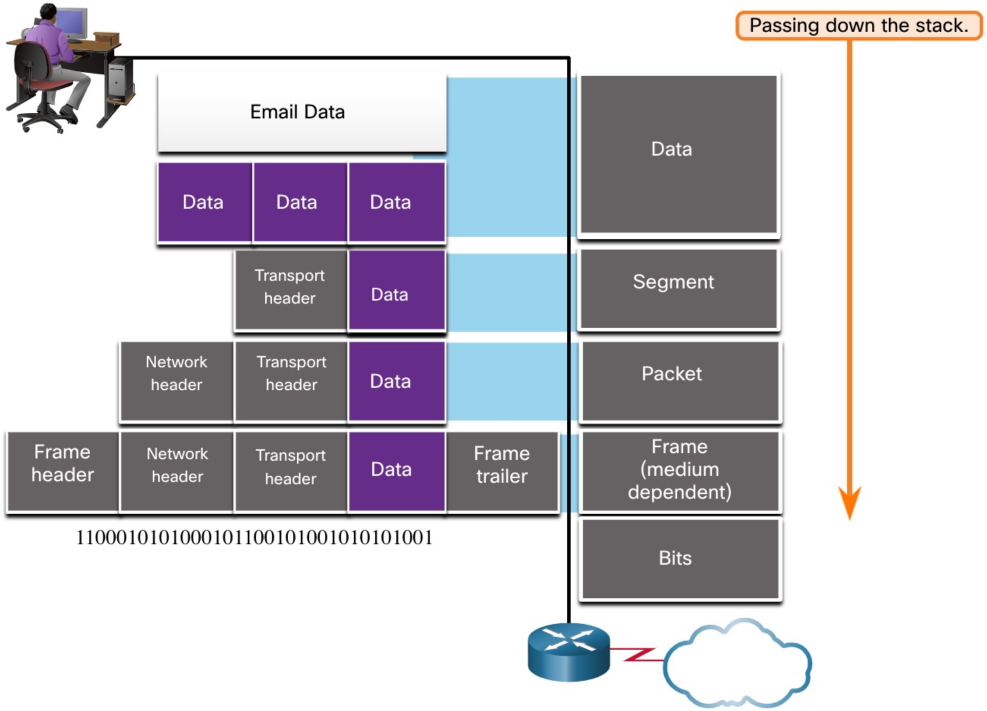


Data Encapsulation

Encapsulation

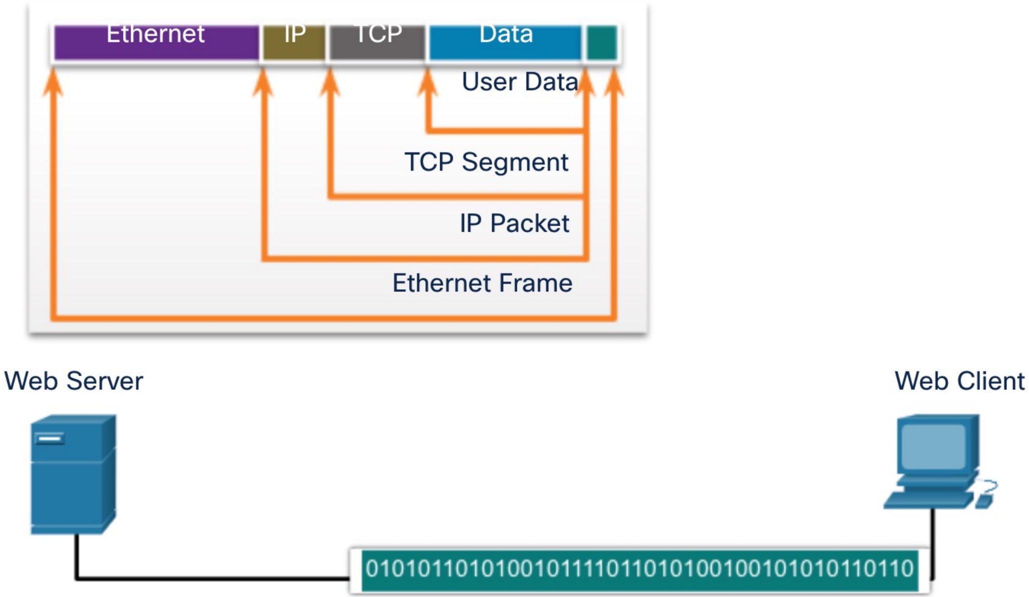
- This division of data into smaller pieces is called segmentation. Segmenting messages has two primary benefits:
  - **Segmentation**
  - **Multiplexing**
- The application data is encapsulated with various protocol information as it is passed down the protocol stack.
- The form that an encapsulated piece of data takes at any layer is called a protocol data unit (PDU).





Encapsulation

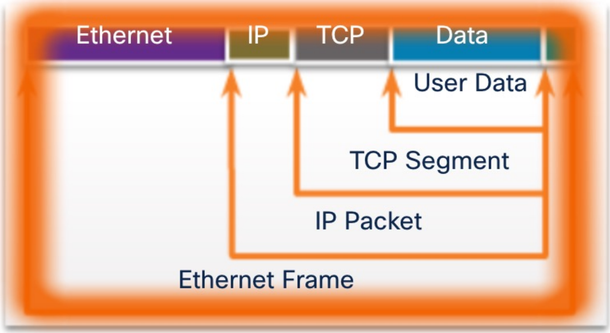
- When messages are being sent on a network, the encapsulation process works from top to bottom.
- At each layer, the upper layer information is considered data within the encapsulated protocol. For example, the TCP segment is considered data within the IP packet.

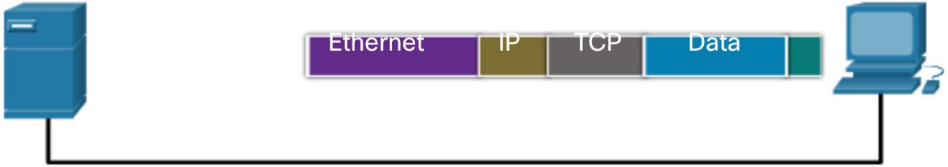


Data Encapsulation

De-encapsulation

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

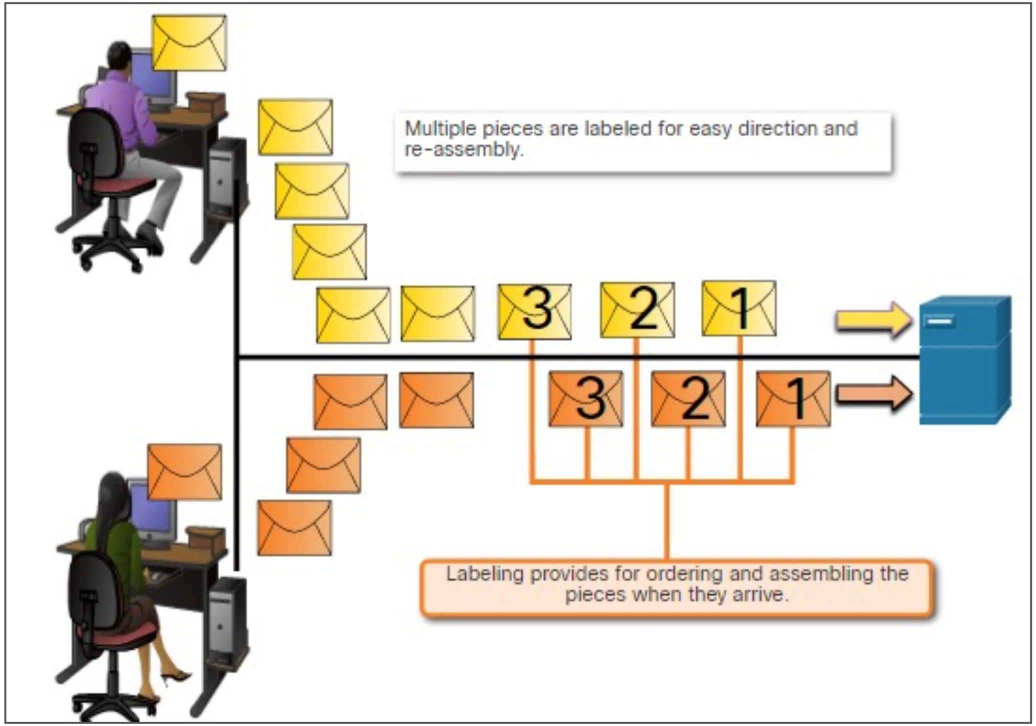




Data Encapsulation

Sequencing

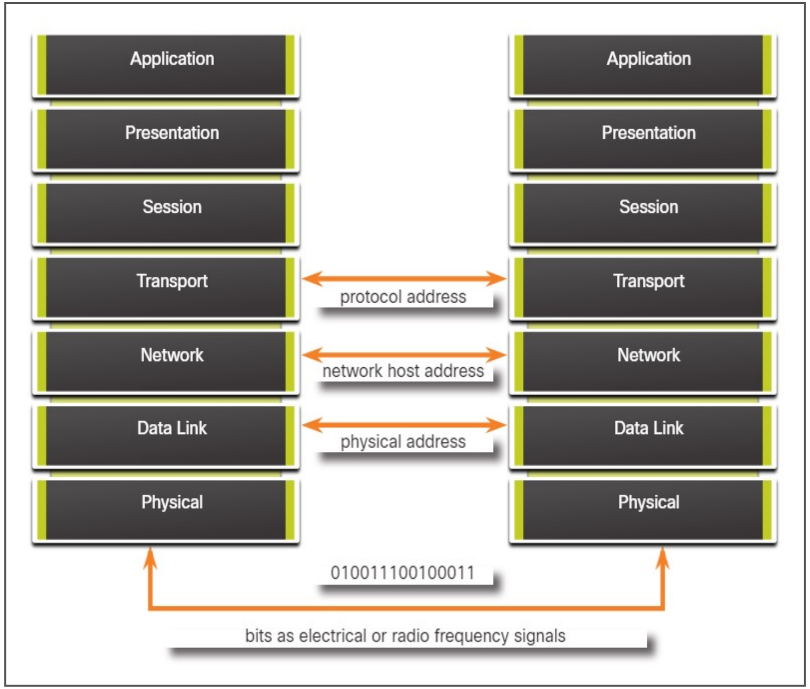
- While transmitting messages using segmentation and multiplexing, there is a possibility of data to reach the destination in a collapsed order.
- Each segment of the message must go through a sequencing process to ensure that it gets to the correct destination and can be reassembled similar to the content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


Multiple pieces are labeled for easy direction and re-assembly.
3
2
1
3
2
1
Labeling provides for ordering and assembling the pieces when they arrive.

Data Encapsulation

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.



New Terms and Commands

- Small office and home office (SOHO)
- Application layer
- Internet Exchange Point (IXP).
- Server Message Block (SMB)
- Domain Name System (DNS)
- Internet service provider (ISP)
- Transmission control protocol (TCP)
- User Datagram Protocol (UDP)
- Open System Interconnection (OSI)

Lab 9 – 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