Chapter 3: Network Protocols and Communications

CCNA Routing and Switching

Introduction to Networks v6.0

Cisco | Networking Academy®
Mind Wide Open™

Chapter 3 - Sections & Objectives

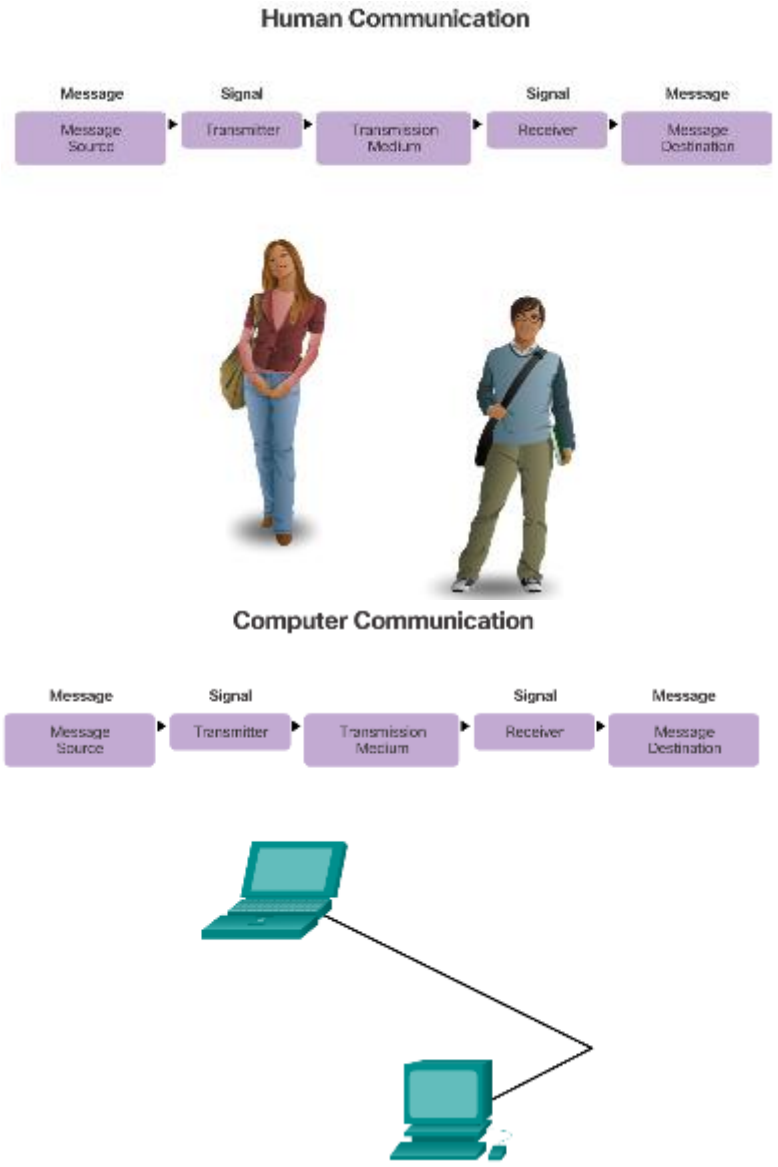
- 3.1 Rules of Communication
  - Describe the types of rules that are necessary to successfully communicate.
- 3.2 Network Protocols and Standards
  - Explain why protocols are necessary in communication.
  - Explain the purpose of adhering to a protocol suite.
  - Explain the role of standards organizations in establishing protocols for network interoperability.
  - Explain how the TCP/IP model and the OSI model are used to facilitate standardization in the communication process.
- 3.3 Data Transfer in the Network
  - Explain how data encapsulation allows data to be transported across the network.
  - Explain how local hosts access local resources on a network.

3.1 Rules of Communication

Cisco | Networking Academy®
Mind Wide Open™

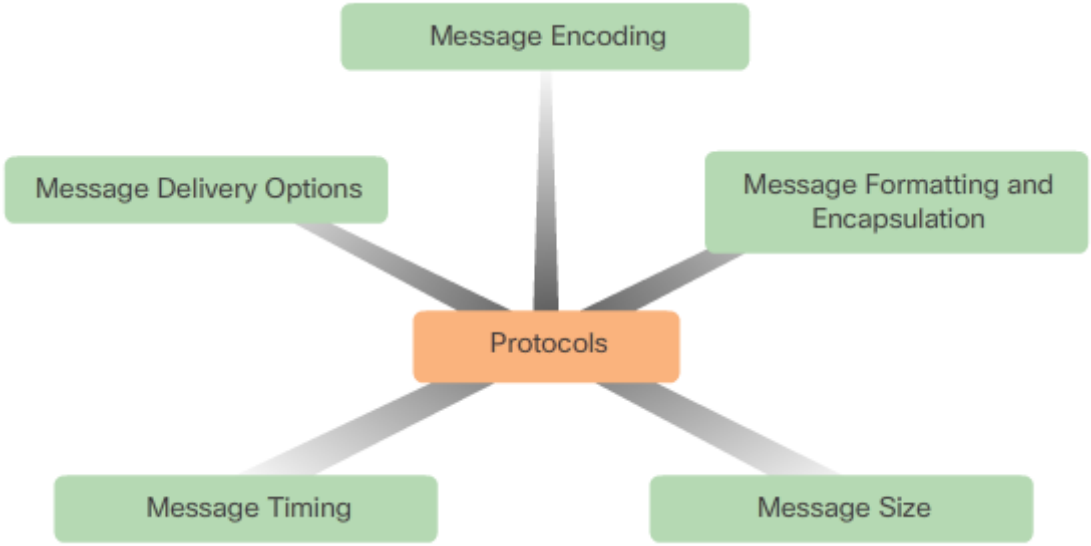
The Rules

- Exchange of Messages
  - People or Machine exchange ideas or messages using many different communication methods.
  - In order for communication to take there should be “rules” identified like what language to use, what medium, speed, size etc. These rules is otherwise known as **protocol**.
- Three elements involved in communication
  - Sender
  - Receiver
  - Medium



The Rules

- Rule Establishment
  - Identified sender and receiver
  - Common language and grammar
  - Speed and timing of delivery
  - Confirmation or acknowledgment requirements
- Message Encoding
  - Process of converting information into another acceptable form
- Message Formatting and Encapsulation
- Message Size
- Message Timing
  - Access method
  - Flow control
  - Response timeout
- Message Delivery Options
  - Unicast
  - Multicast
  - Broadcast



The Rules

- Message Encoding
  - Process of converting information into another acceptable form
  - Example : From ASCII to EBCDIC format

DEC	HEX	EBCDIC	ASCII	BINARY
000	00	NUL	NUL	0000 0000
001	01	SOH	SOH	0000 0001
002	02	STX	STX	0000 0010
003	03	ETX	ETX	0000 0011
004	04	SEL	EOT	0000 0100
005	05	TAB	ENQ	0000 0101
006	06	RNL	ACK	0000 0110
007	07	DEL	BEL	0000 0111
008	08	GE	BS	0000 1000
009	09	SPS	TAB	0000 1001
010	0A	RPT	LF	0000 1010
011	0B	VT	VT	0000 1011
012	0C	FF	FF	0000 1100
013	0D	CR	CR	0000 1101
014	0E	SO	SO	0000 1110
015	0F	SI	SI	0000 1111

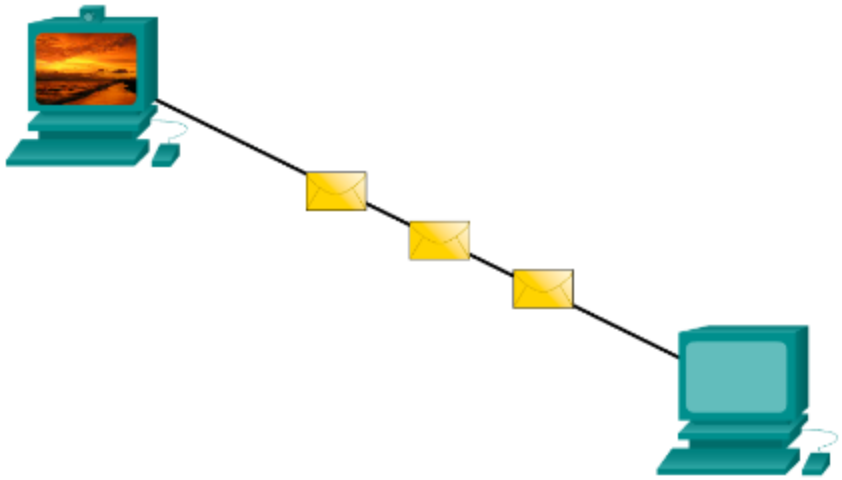
The Rules

- Message Formatting and Encapsulation
  - Each computer message is encapsulated in a specific format, called a frame, before it is sent over the network. A frame acts like an envelope; it provides the address of the destination and the address of the source host.

Destination (physical / hardware address)	Source (physical / hardware address)	Start Flag (start of message indicator)	Recipient (destination identifier)	Sender (source identifier)	Encapsulated Data (bits)	End of Frame (end of message indicator)
Frame Addressing		Encapsulated Message				

The Rules

- Message Size
  - When a long message is sent from one host to another over a network, it is necessary to break the message into smaller pieces. The process of breaking long messages into smaller ones is called **segmentation**.
  - The rules that govern the size of the pieces, or frames, communicated across the network are very strict. They can also be different, depending on the channel used. Frames that are too long or too short are not delivered.

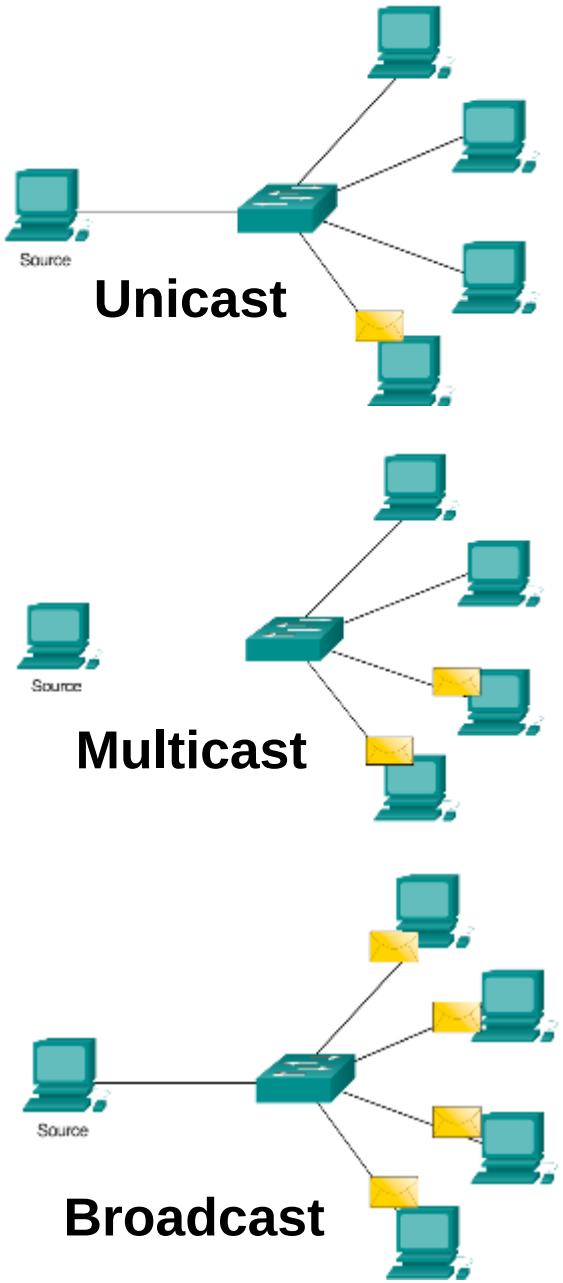


The Rules

- Message Timing
  - **Access method -** determines when someone is able to send a message. If two people talk at the same time, a collision of information occurs and it is necessary for the two to back off and start again.
  - **Flow control -** In network communication, source and destination hosts use flow control methods to negotiate correct timing and speed for successful communication.
  - **Response timeout -** Hosts on the network have rules that specify how long to wait for responses and what action to take if a response timeout occurs.

The Rules

- Message Delivery Options
  - **Unicast** - one-to-one delivery wherein only a single destination for the message.
  - **Multicast** - a one-to-many delivery wherein same message is delivered to a group of host destinations simultaneously.
  - **Broadcast** - a one-to-all message delivery wherein all hosts on the network need to receive the message at the same time.

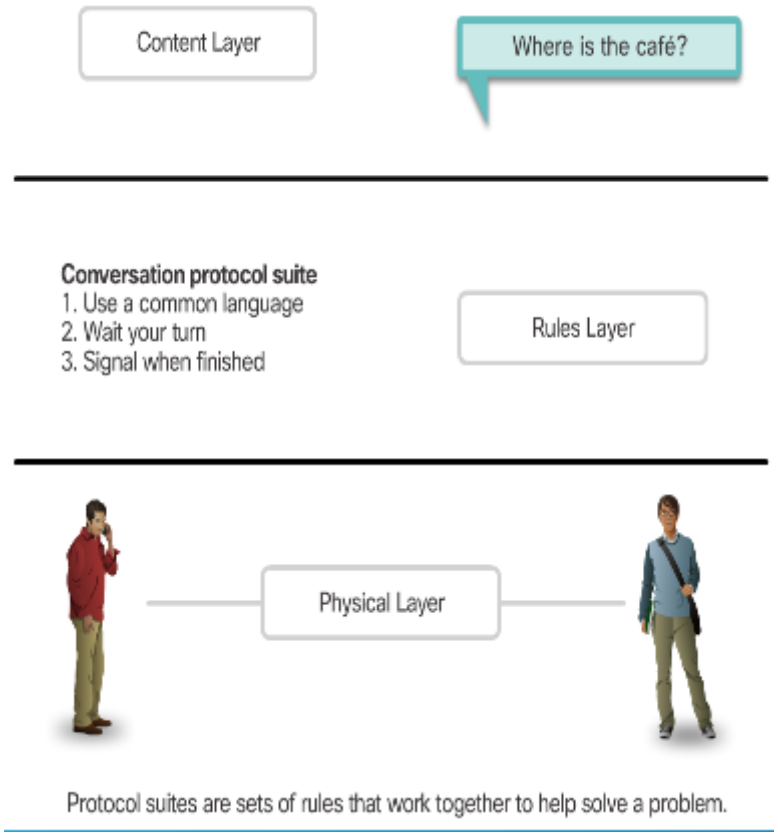


3.2 Network Protocols and Standards

Cisco | Networking Academy®
Mind Wide Open™

Protocols

- Rules that Govern Communications
  - A group of inter-related protocols necessary to perform a communication function is called a **protocol suite**. Protocol suites are implemented by hosts and networking devices in software, hardware or both.
  - One of the best ways to visualize how the protocols within a suite interact is to view the interaction as a **stack**. A protocol stack shows how the individual protocols within a suite are implemented. The protocols are viewed in terms of **layers**, with each higher level service depending on the functionality defined by the protocols shown in the lower levels. The lower layers of the stack are concerned with moving data over the network and providing services to the upper layers, which are focused on the content of the message being sent.

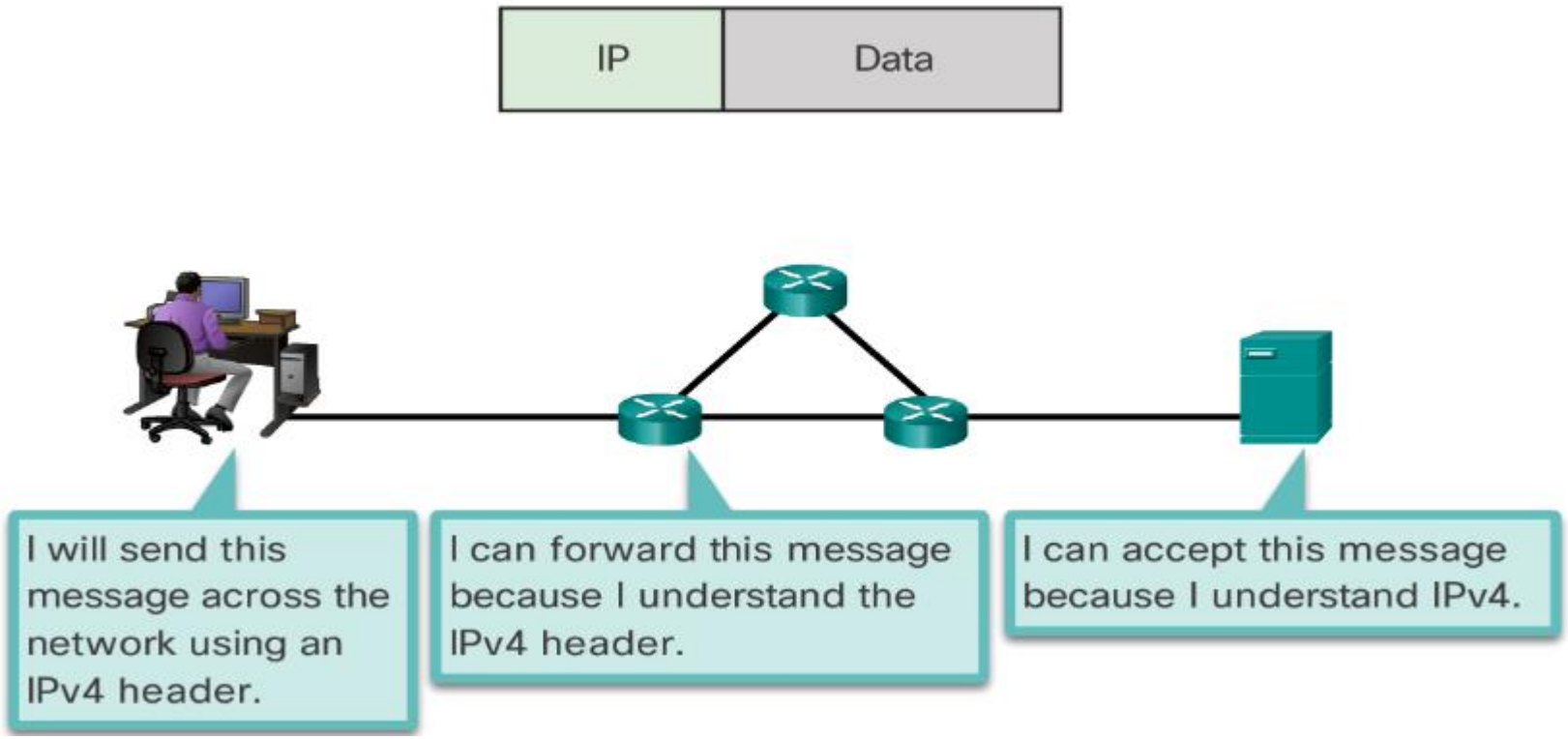


Protocols

- Network Protocols
  - For devices to successfully communicate, a network protocol suite must describe precise requirements and interactions. 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)

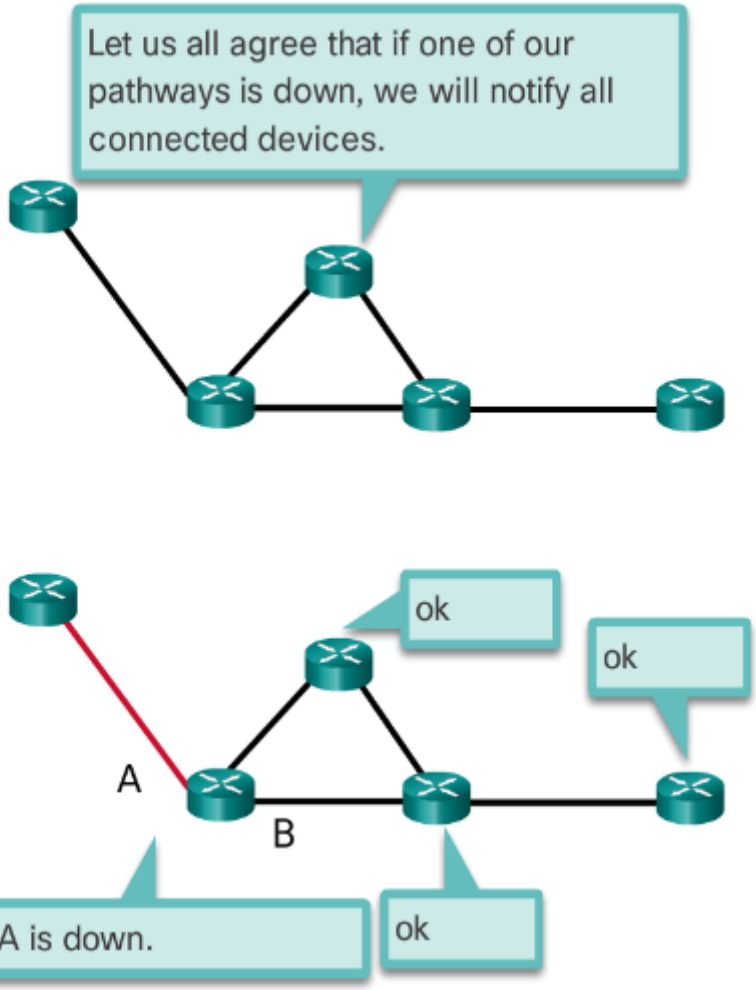
Protocols

- Role of Network Protocols
  - How the message is formatted or structured



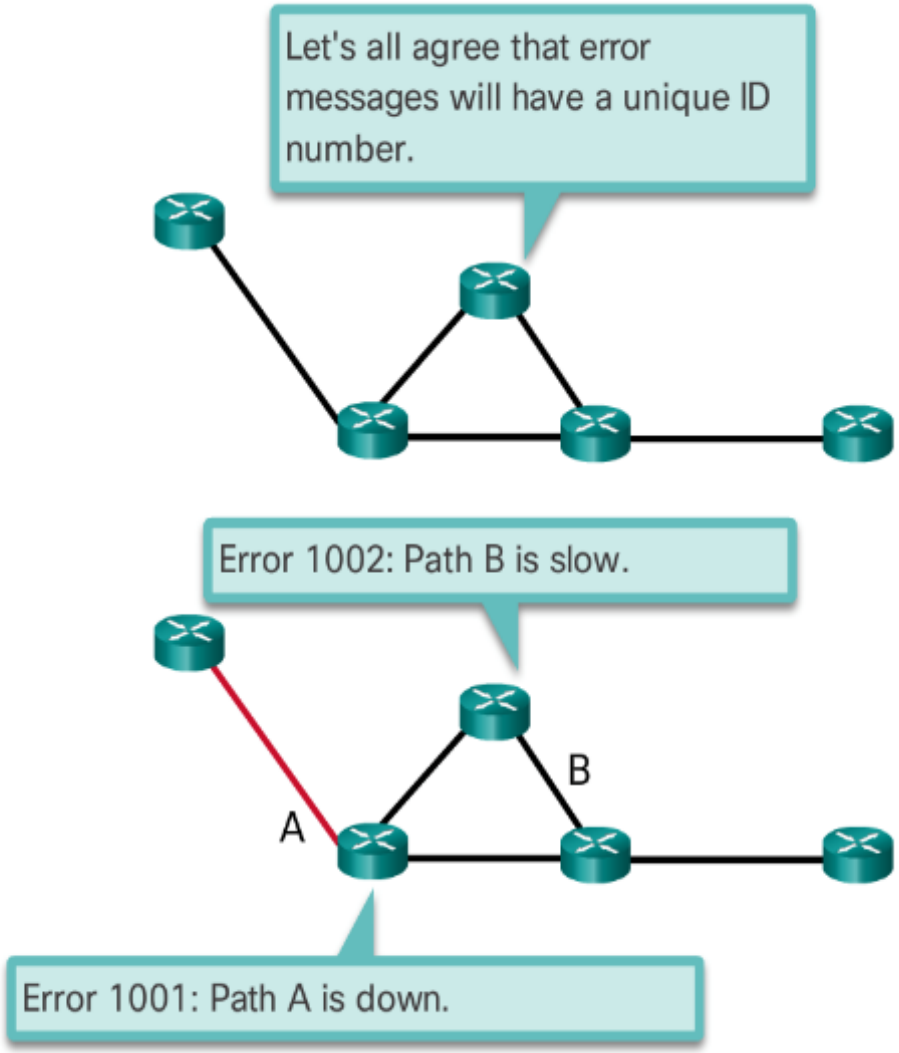
Protocols

- Role of Network Protocols
  - The process by which networking devices share information about pathways with other networks



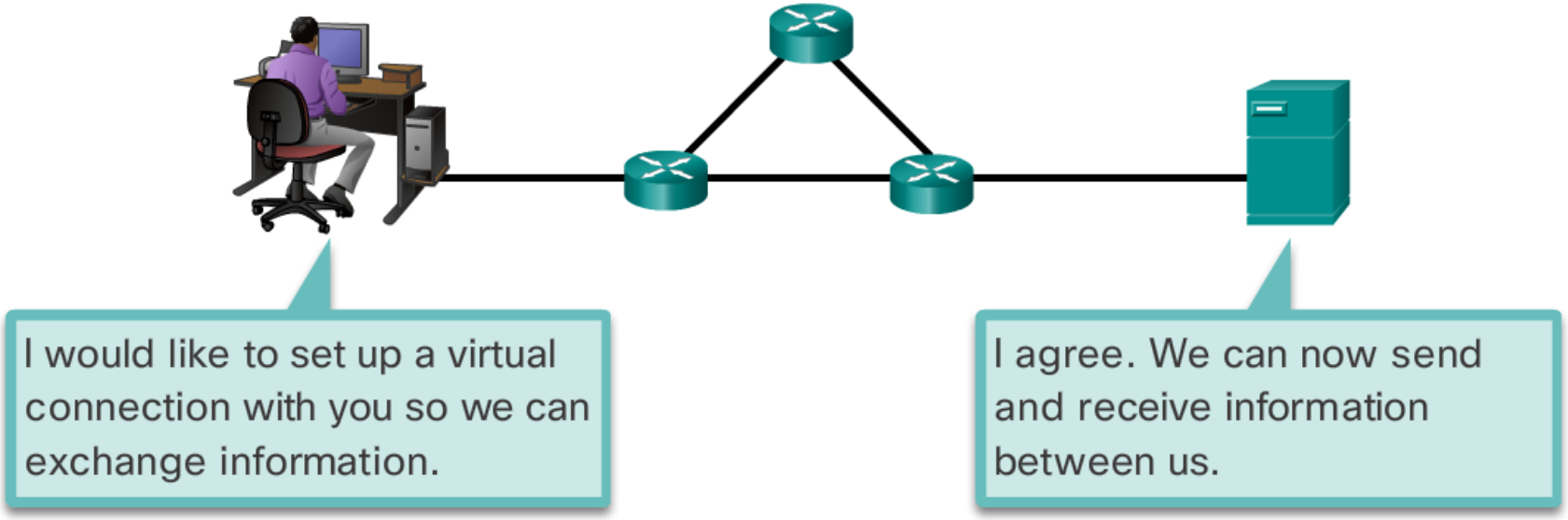
Protocols

- Role of Network Protocols
  - How and when error and system messages are passed between devices



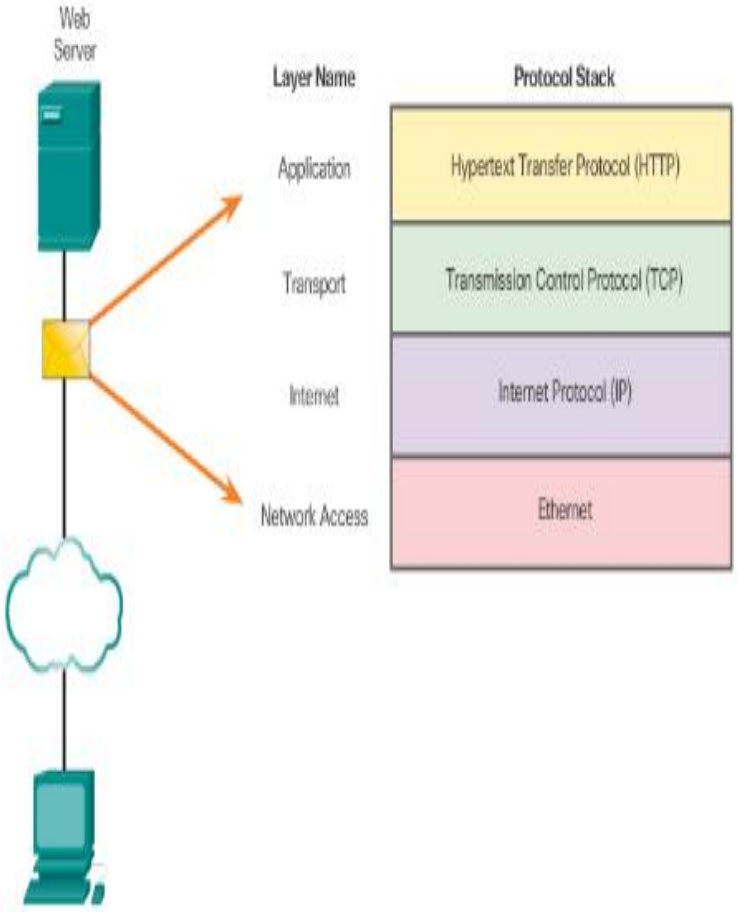
Protocols

- Role of Network Protocols
  - The setup and termination of data transfer sessions



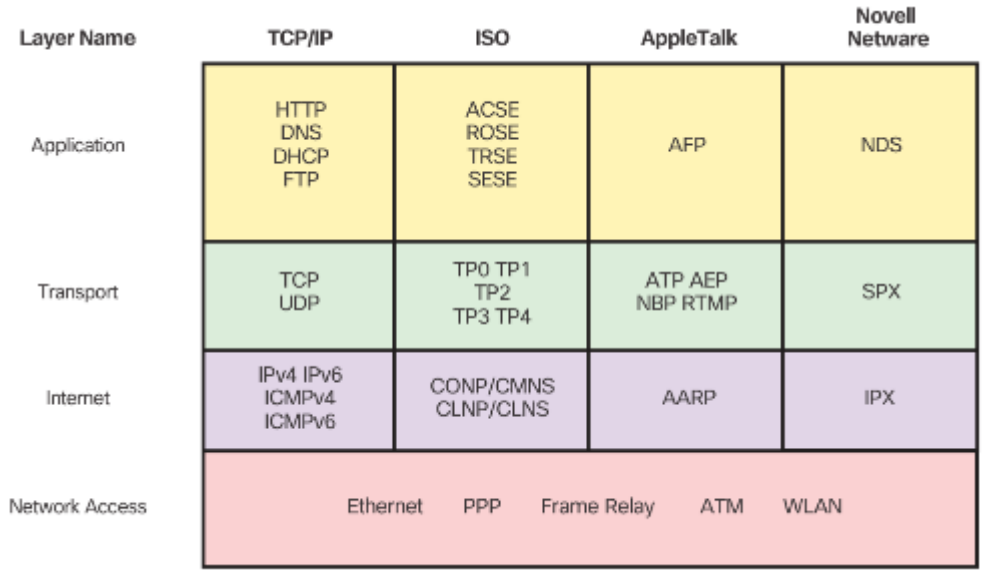
Protocols

- Protocol Interaction
  - Communication between a web server and web client is an example of an interaction between several protocols
- **HTTP** - is an application protocol that governs the way a web server and a web client interact. HTTP defines the content and formatting of the requests and responses that are exchanged between the client and server.
- **TCP** - is the transport protocol that manages the individual conversations. TCP divides the HTTP messages into smaller pieces, called segments. These segments are sent between the web server and client processes running at the destination host. TCP is also responsible for controlling the size and rate at which messages are exchanged between the server and the client.
- **IP** - is responsible for taking the formatted segments from TCP, encapsulating them into packets, assigning them the appropriate addresses, and delivering them to the destination host.
- **Ethernet** - is a network access protocol that describes two primary functions: communication over a data link and the physical transmission of data on the network media. Network access protocols are responsible for taking the packets from IP and formatting them to be transmitted over the media.



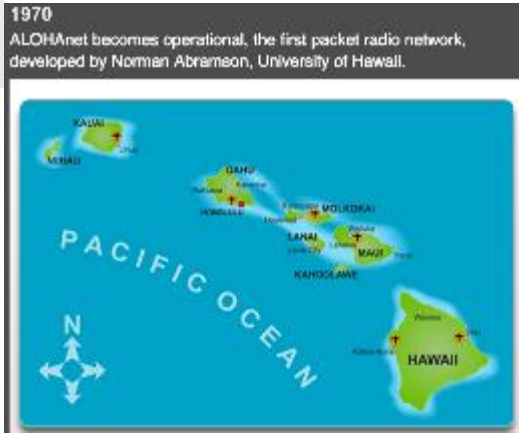
Protocol Suites

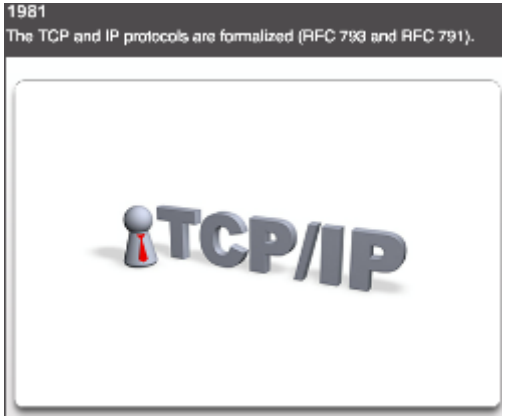
- It is a set of protocols that work together to provide comprehensive network communication services. A protocol suite may be specified by a standards organization or developed by a vendor.
- The **TCP/IP** protocol suite, the de-facto protocol for the Internet is an open standard, meaning these protocols are freely available to the public, and any vendor is able to implement these protocols on their hardware or in their software.



Development of TCP/IP

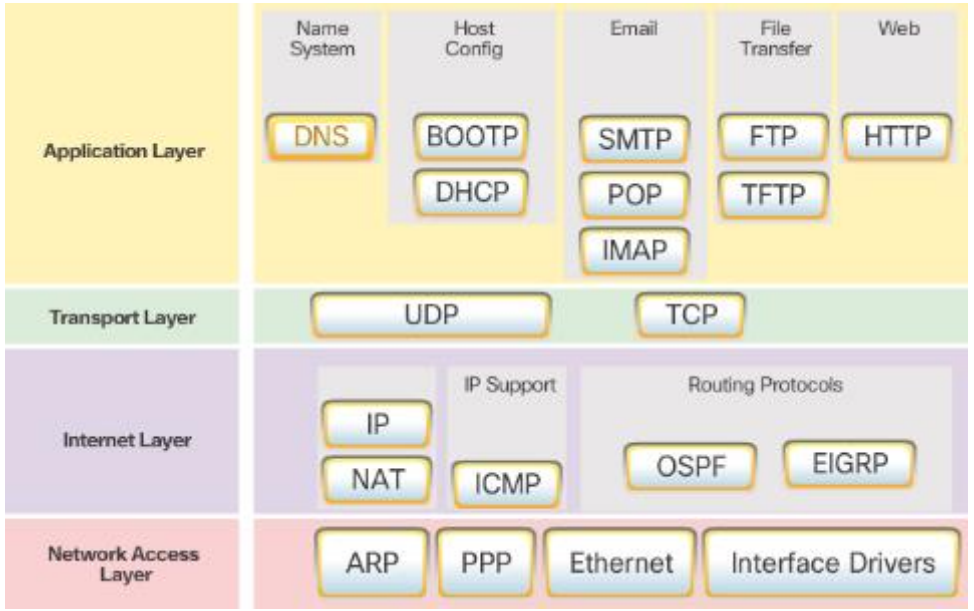
- The first packet switching network and predecessor to today's Internet was the Advanced Research Projects Agency Network (ARPANET), which came to life in 1969 by connecting mainframe computers at four locations. ARPANET was funded by the U.S. Department of Defense for use by universities and research laboratories.





Protocol Suites

- Protocol Suites and Industry Standards
  - TCP/IP is an open standard
  - Can you name other protocol suites?
- TCP/IP Protocol Suites
  - Can you name some of the protocols from the TCP/IP protocol suite.
- TCP/IP Communication Process
  - Can you describe the process?

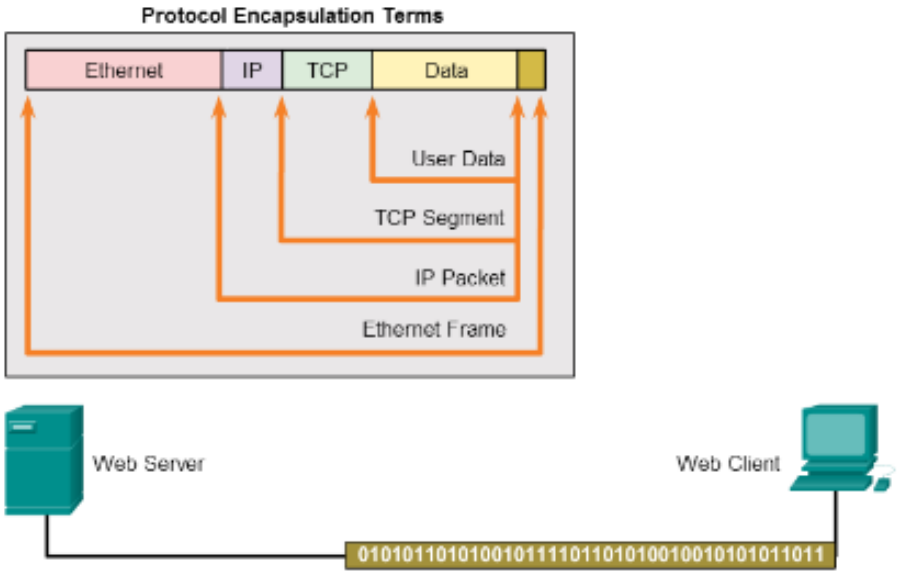


3.3 Data Transfer in the Network

Cisco | Networking Academy®
Mind Wide Open™

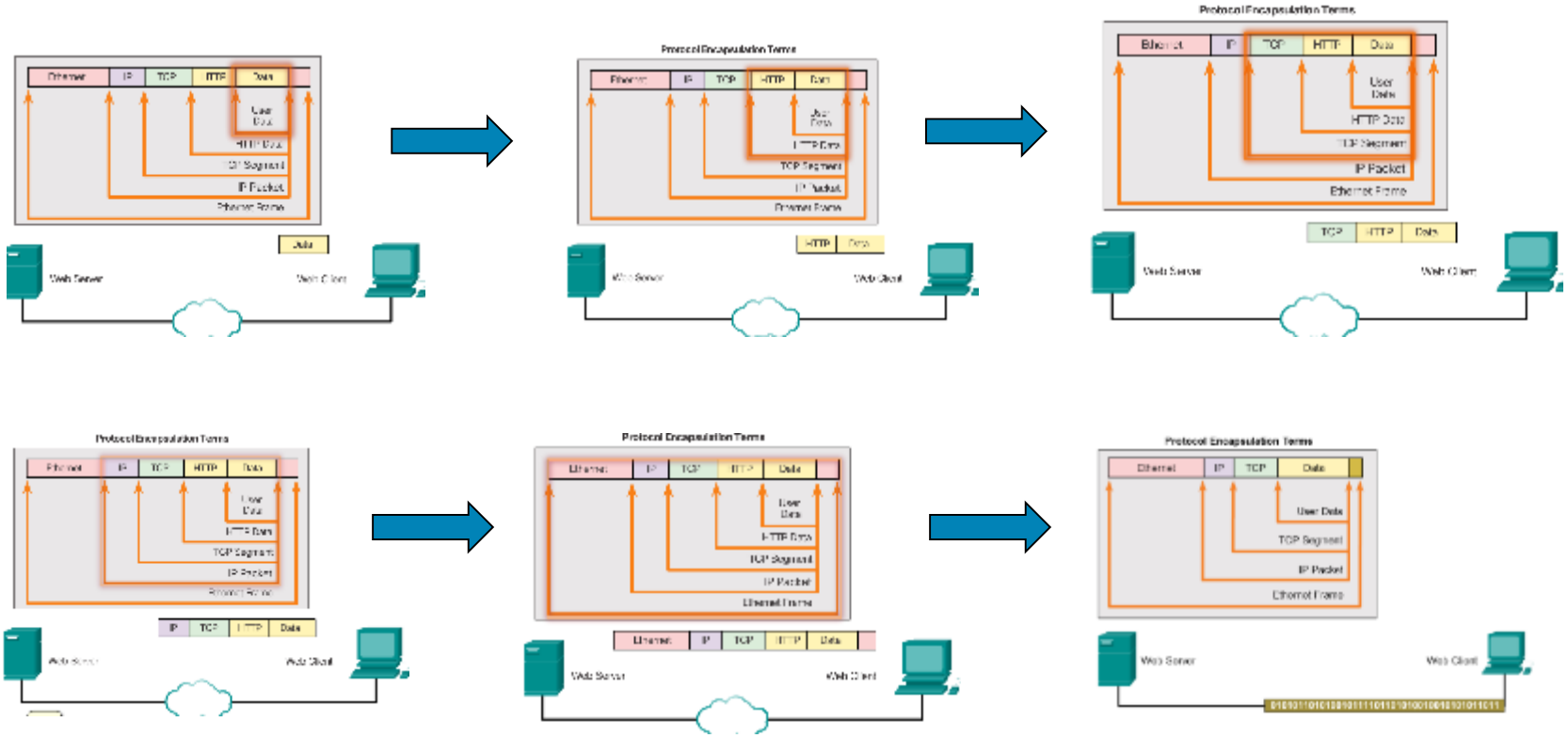
Data Encapsulation

- Encapsulation and de-encapsulation process



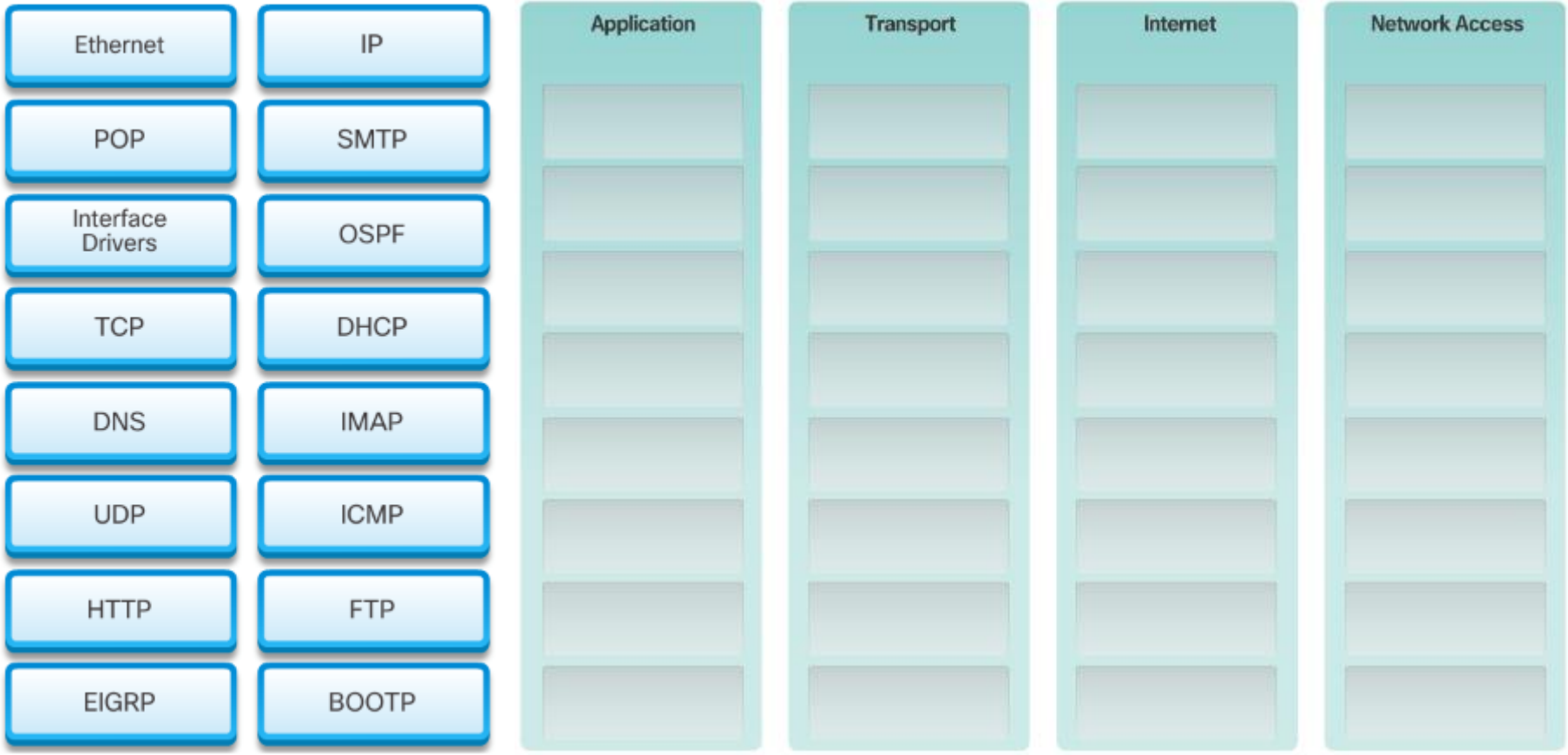
Data Encapsulation

- Encapsulation and de-encapsulation process



Activity

- Mapping the Protocols of TCP/IP Protocol Suite



Standards

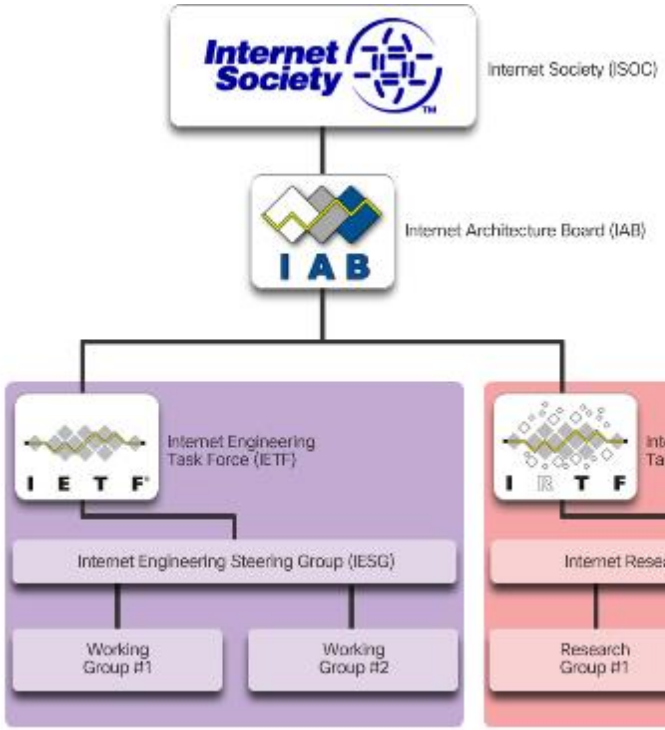
- Open Standards
  - Open standards encourage interoperability, competition, and innovation. They also guarantee that no single company's product can monopolize the market, or have an unfair advantage over its competition.
  - A good example of this is when purchasing a wireless router for the home. There are many different choices available from a variety of vendors, all of which incorporate standard protocols such as IPv4, DHCP, 802.3 (Ethernet), and 802.11 (Wireless LAN). These open standards also allow a client running Apple's OS X operating system to download a web page from a web server running the Linux operating system. This is because both operating systems implement the open standard protocols, such as those in the TCP/IP protocol suite.

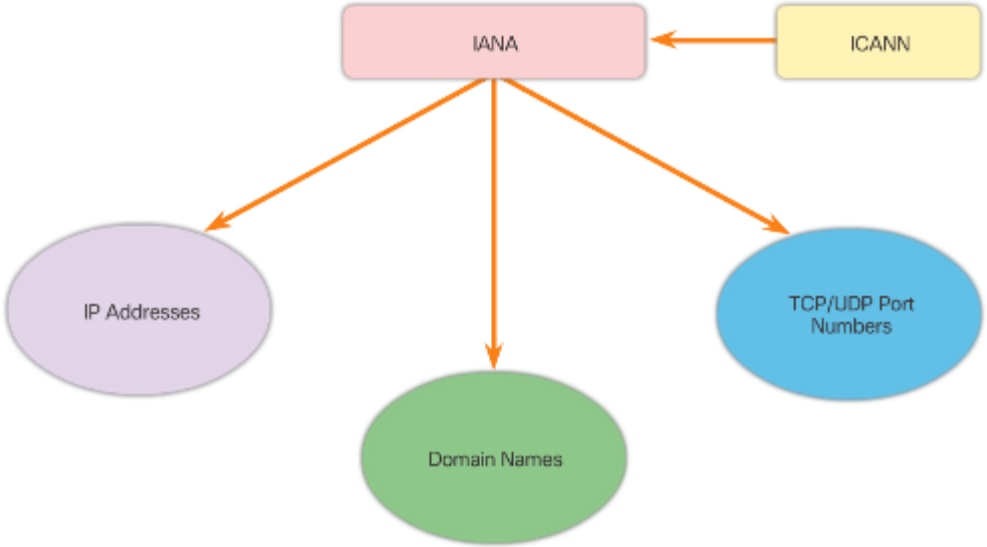
Standards

- Internet Standards
  - **Internet Society (ISOC)** – Responsible for promoting the open development and evolution of Internet use throughout the world.
  - **Internet Architecture Board (IAB)** - Responsible for the overall management and development of Internet standards.
  - **Internet Engineering Task Force (IETF)** - Develops, updates, and maintains Internet and TCP/IP technologies. This includes the process and documents for developing new protocols and updating existing protocols know as Request for Comments (RFC) documents.
  - **Internet Research Task Force (IRTF)** - Focused on long-term research related to Internet and TCP/IP protocols such as Anti-Spam Research Group (ASRG), Crypto Forum Research Group (CFRG), and Peer-to-Peer Research Group (P2PRG).

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

Standards





Standards

- Electronics & Communications Standards
  - **Institute of Electrical and Electronics Engineers (IEEE, pronounced "I-triple-E") –** Organization of electrical engineering and electronics dedicated to advancing technological innovation and creating standards in a wide area of industries including power and energy, healthcare, telecommunications, and networking.
  - **Electronic Industries Alliance (EIA) -** Best known for its standards related to electrical wiring, connectors, and the 19-inch racks used to mount networking equipment.
- Electronics & Communications Standards
  - **Telecommunications Industry Association (TIA) -** Responsible for developing communication standards in a variety of areas including radio equipment, cellular towers, Voice over IP (VoIP) devices, satellite communications, Ethernet cable and more.
  - **International Telecommunications Union-Telecommunication** Standardization Sector (ITU-T) - One of the largest and oldest communication standard organizations. The ITU-T defines standards for video compression, Internet Protocol Television (IPTV), and broadband communications, such as a digital subscriber line (DSL).

Standards – Electronics & Communications

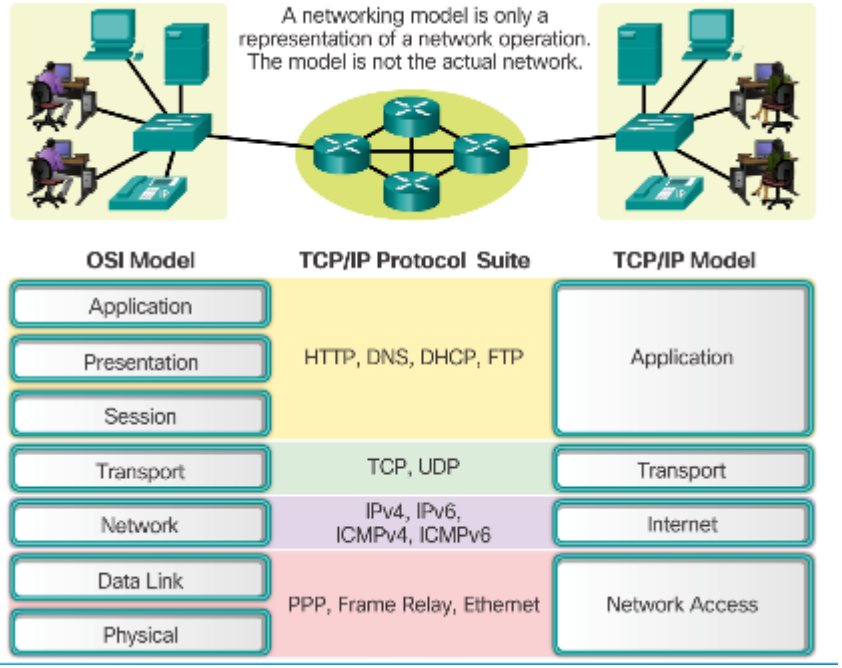
IEEE 802 Working Groups and Study Groups

- 802.1 Higher Layer LAN Protocols Working Group
- 802.3 Ethernet Working Group
- 802.11 Wireless LAN Working Group
- 802.15 Wireless Personal Area Network (WPAN) Working Group
- 802.16 Broadband Wireless Access Working Group
- 802.18 Radio Regulatory TAG
- 802.19 Wireless Coexistence Working Group
- 802.21 Media Independent Handover Services Working Group
- 802.22 Wireless Regional Area Networks
- 802.24 Smart Grid TAG

EIA/TIA Standards

Reference Models

- The Benefits of Using a Layered Model
  - Assisting 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.
  - Fostering competition because products from different vendors can work together.
  - Preventing technology or capability changes in one layer from affecting other layers above and below.
  - Providing a common language to describe networking functions and capabilities.



Reference Models

- The OSI Reference Model
  - he OSI model provides an extensive list of functions and services that can occur at each layer. It also describes the interaction of each layer with the layers directly above and below.

Reference Models

- Physical Layer
  - The physical layer protocols describe the mechanical, electrical, functional, and procedural means to activate, maintain, and de-activate physical connections for bit transmission to and from a network device.
- Data Link Layer
  - The data link layer protocols describe methods for exchanging data frames between devices over a common media.

Reference Models

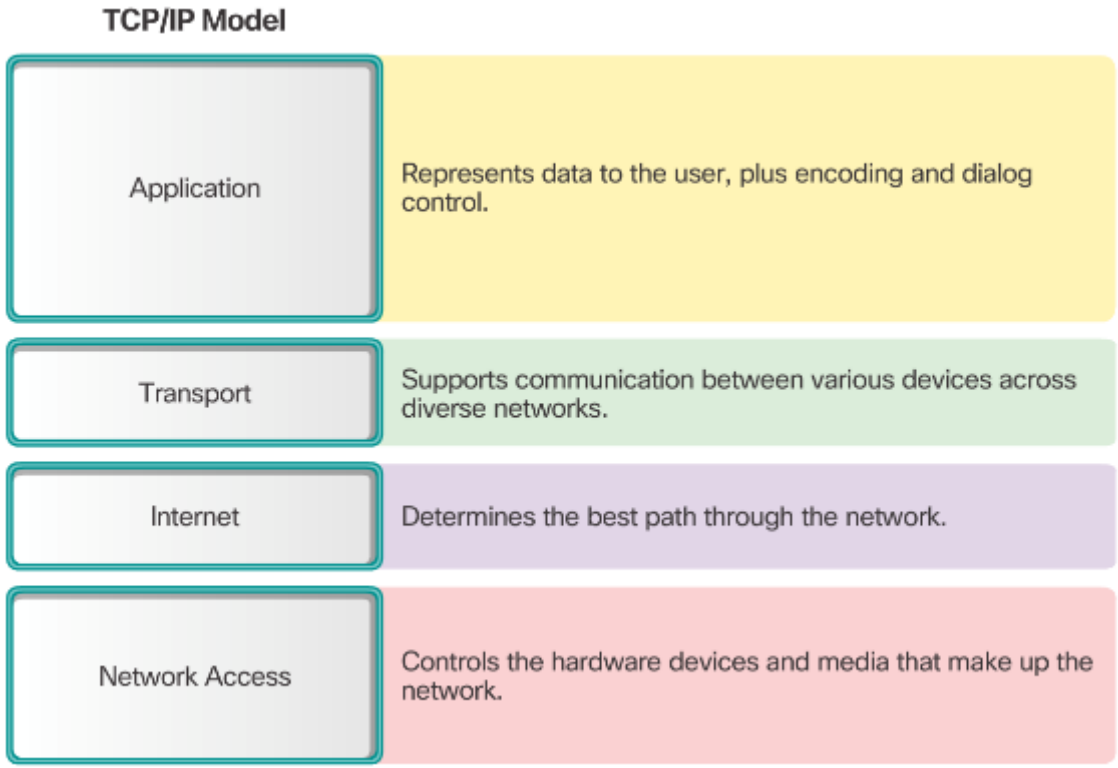
- Network Layer
  - Provides services to exchange the individual pieces of data over the network between identified end devices.
- Transport Layer
  - Defines services to segment, transfer, and reassemble the data for individual communications between the end devices.
- Session Layer
  - Provides services to the presentation layer to organize its dialogue and to manage data exchange.

Reference Models

- Presentation Layer
  - Provides for common representation of the data transferred between application layer services.
- Application Layer
  - Contains protocols used for process-to-process communications.

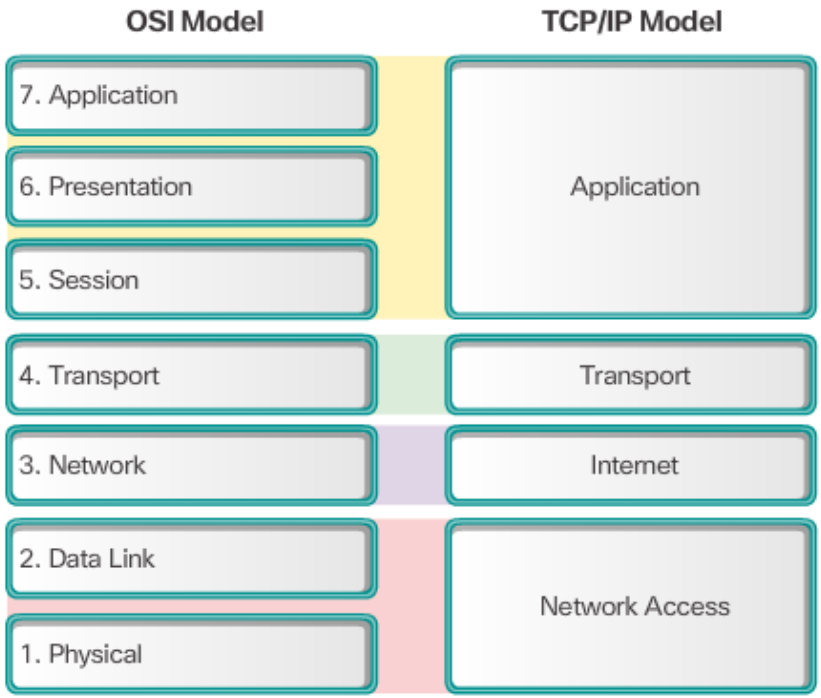
Reference Models

- The TCP/IP Protocol Model
  - The TCP/IP protocol model for internetwork communications was created in the early 1970s and is sometimes referred to as the Internet model. As shown in the figure, it defines four categories of functions that must occur for communications to be successful. The architecture of the TCP/IP protocol suite follows the structure of this model. Because of this, the Internet model is commonly referred to as the TCP/IP model.



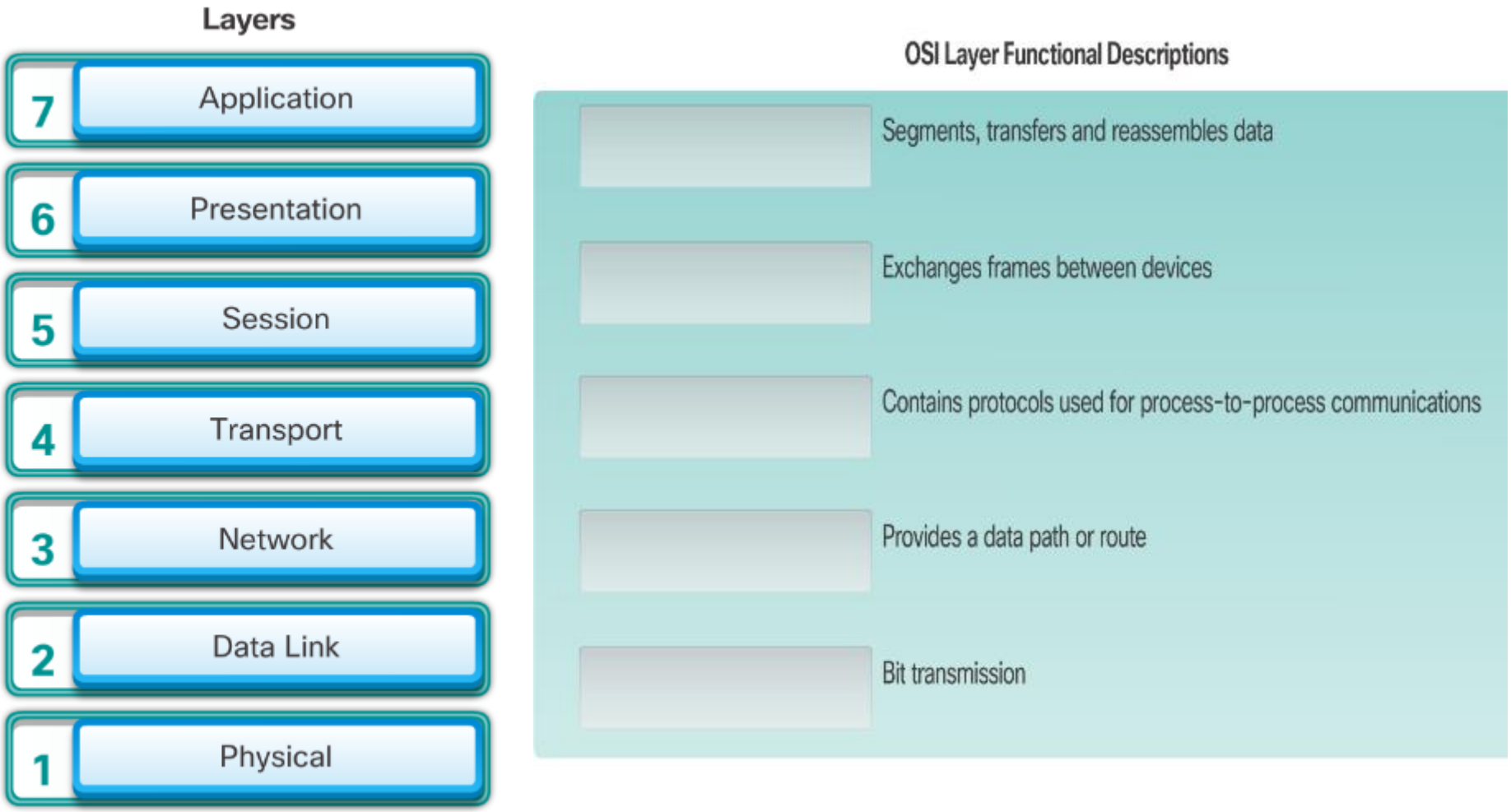
Reference Models

- OSI Model and TCP/IP Model Comparison
  - The TCP/IP protocol model for internetwork communications was created in the early 1970s and is sometimes referred to as the Internet model. As shown in the figure, it defines four categories of functions that must occur for communications to be successful. The architecture of the TCP/IP protocol suite follows the structure of this model. Because of this, the Internet model is commonly referred to as the TCP/IP model.
  - OSI Layers 3 & 4, the network layer, maps directly to the TCP/IP Internet and Transport layers respectively.
  - The TCP/IP application layer includes a number of protocols that provide specific functionality to a variety of end user applications. The OSI model Layers 5, 6, and 7 are used as references for application software developers and vendors to produce products that operate on networks.



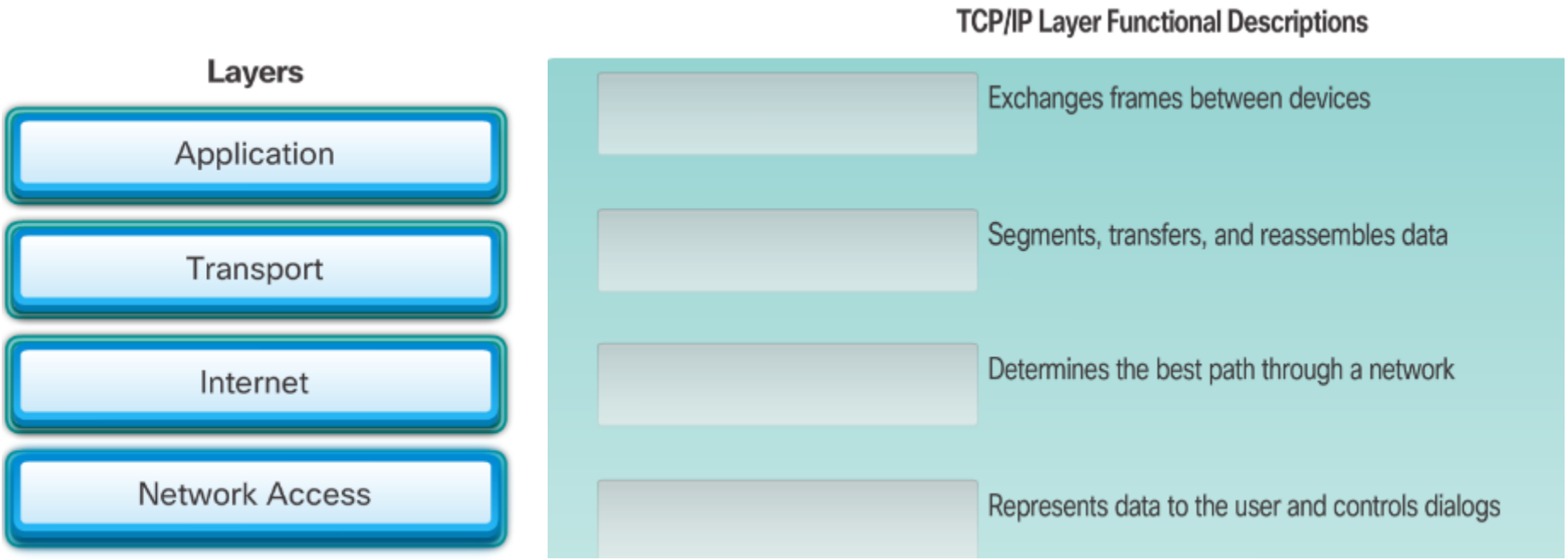
Activity

- OSI Layer Functions



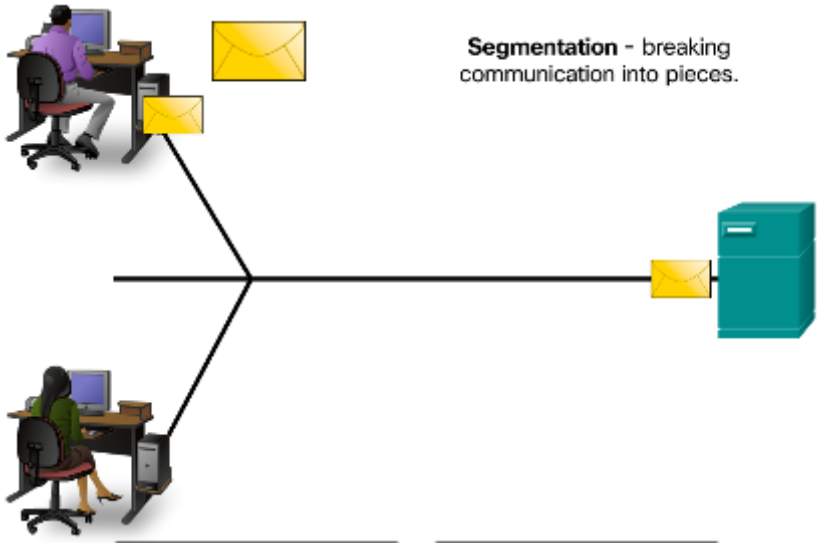
Activity

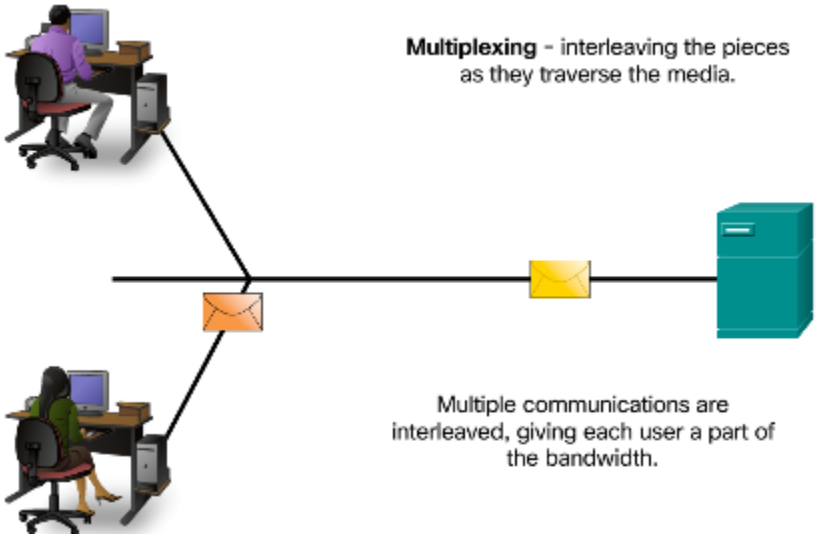
- TCP/IP Layer Functions



Segmentation

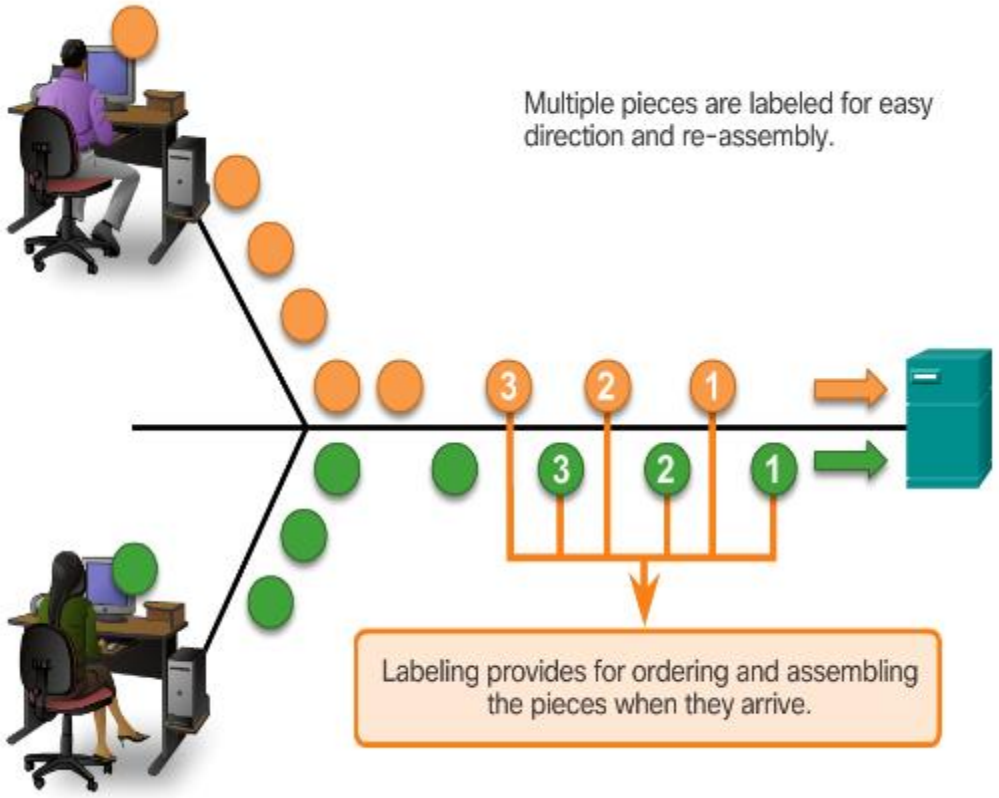
- Message Segmentation
  - Segmentation - Break communication into pieces
  - Multiplexing – interleaving the pieces





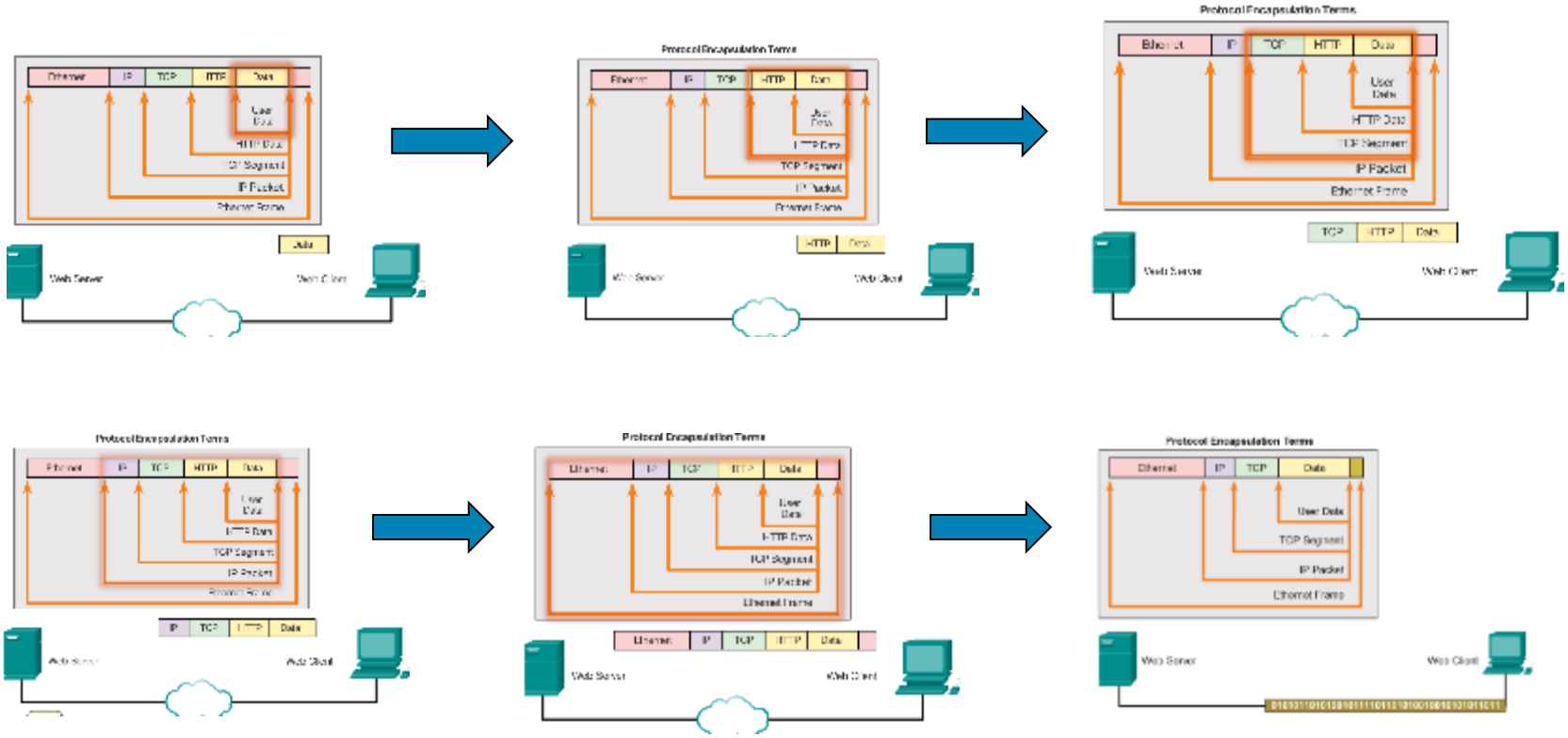
Segmentation

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



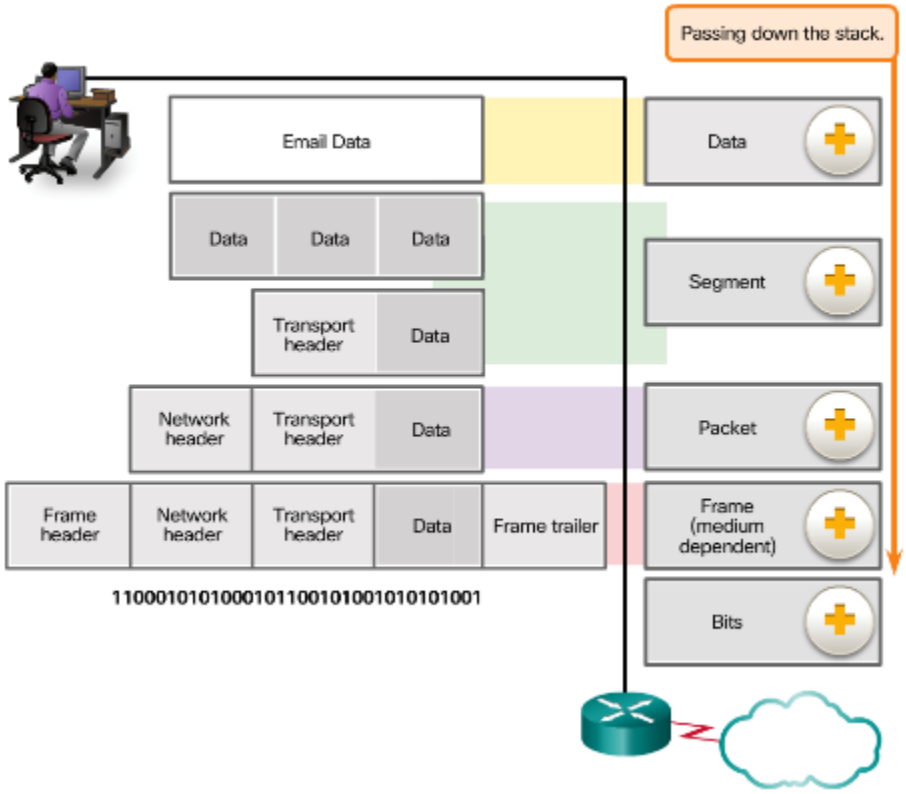
Data Encapsulation

- Encapsulation and de-encapsulation process



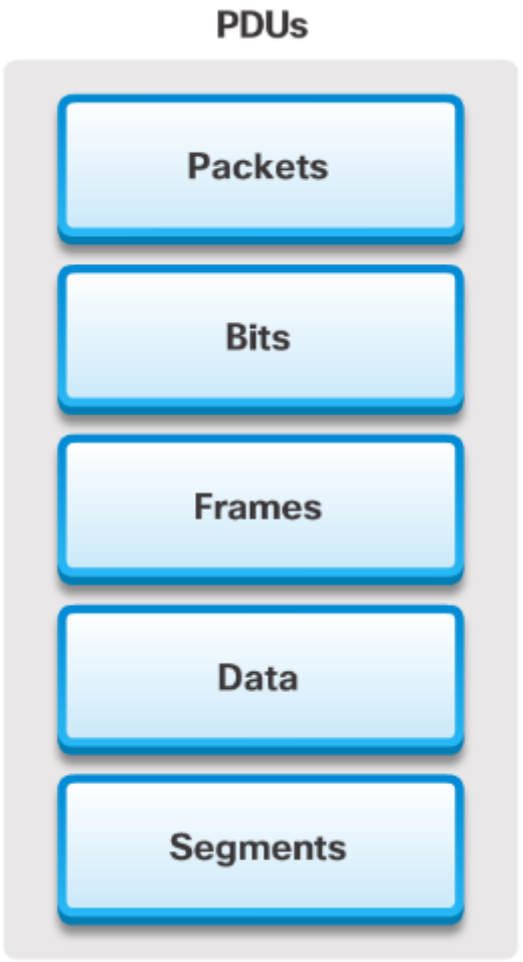
Data Encapsulation

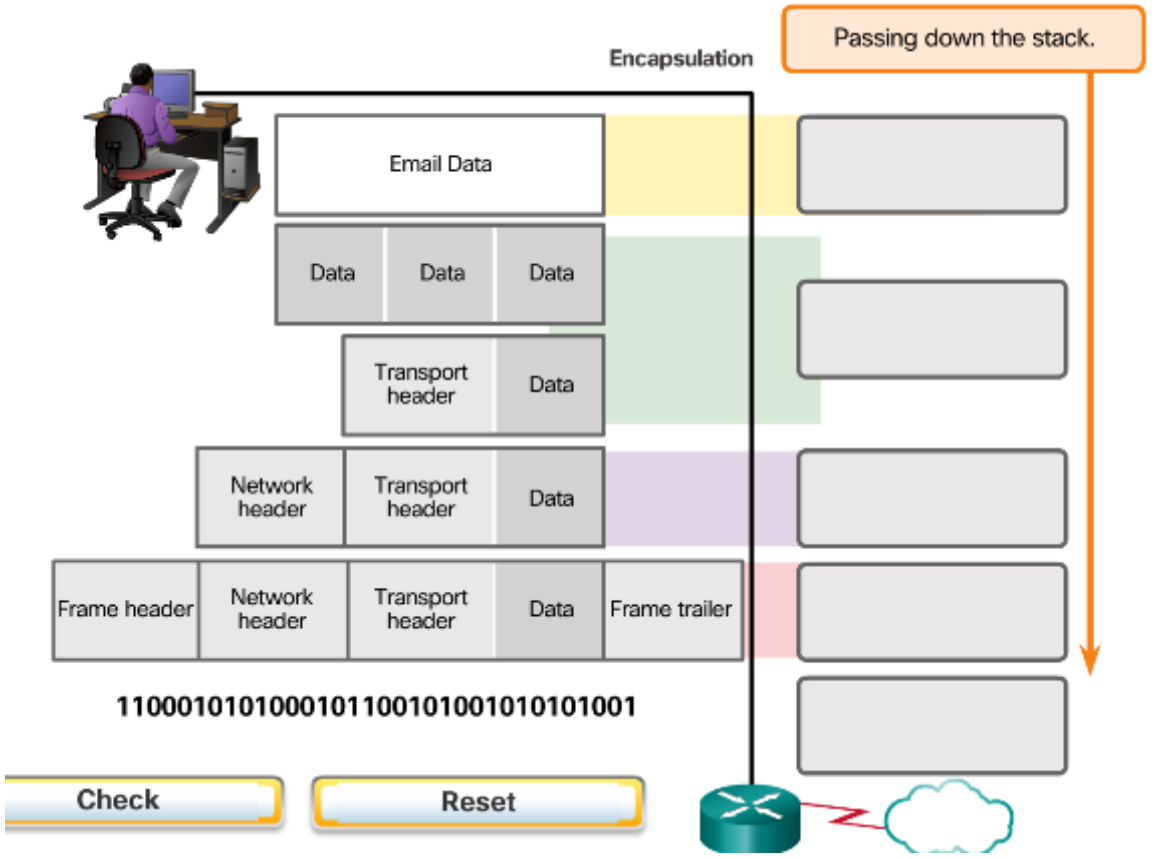
- Protocol Data Units
  - As application data is passed down the protocol stack on its way to be transmitted across the network media, various protocol information is added at each level. This is known as the encapsulation process.
  - The form that a piece of data takes at any layer is called a protocol 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.



Activity

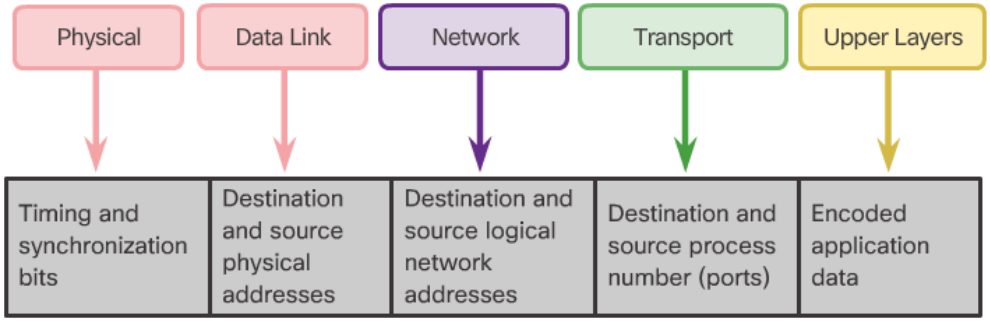
- Encapsulation





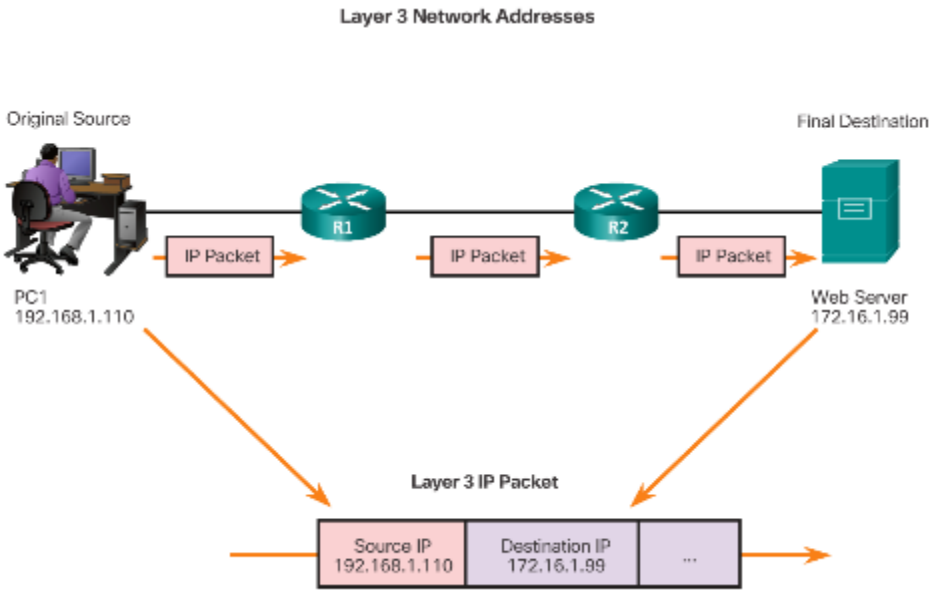
Data Access

- Network Addresses
  - Source IP address
  - Destination IP address
  - Deliver the IP packet from the original source to the final destination, either on the same network or to a remote network.
- Data Link Addresses
  - Source data link address
  - Destination data link address
  - Deliver the data link frame from one network interface card (NIC) to another NIC on the same network
- Devices on the Same Network
- Devices on a Remote Network



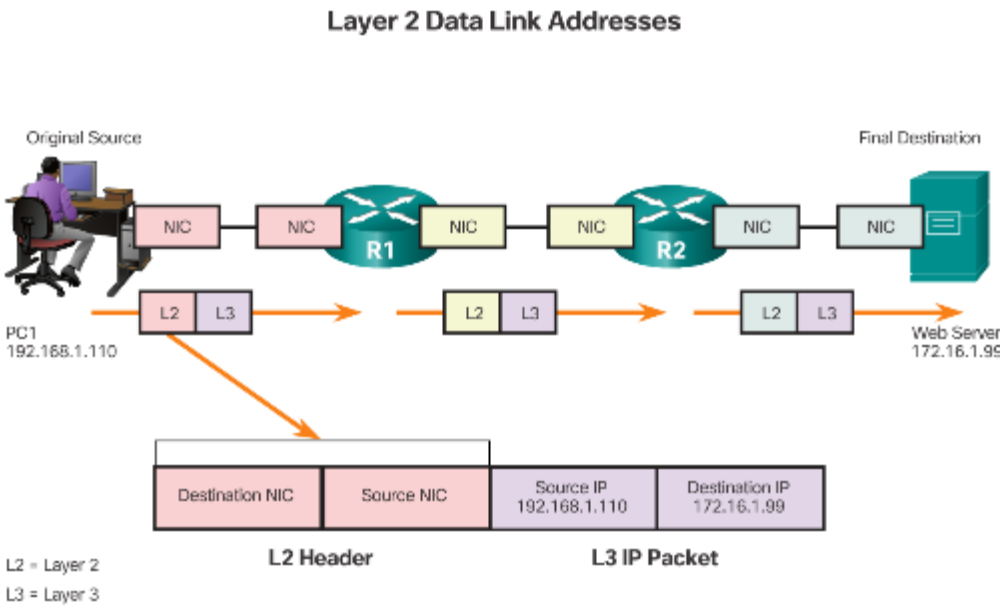
Data Access

- Layer 3 – IP Address
  - An **IP address** is the **network layer**, or **Layer 3**, logical address used to deliver the IP packet from the original source to the final destination
  - The IP packet contains two IP addresses:
    - **Source IP address** - The IP address of the sending device, the original source of the packet.
    - **Destination IP address** - The IP address of the receiving device, the final destination of the packet.



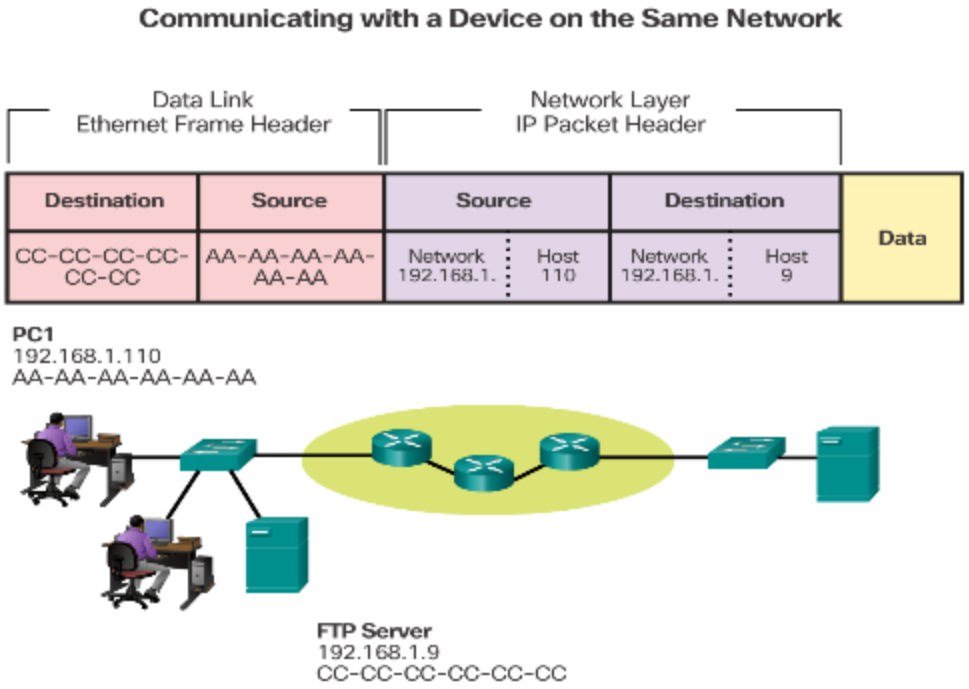
Data Access

- Layer 2 – MAC Address
  - The **Data Link**, or **Layer 2**, **physical address** or **MAC address** has a different role. It is only used to deliver the packet from NIC-to-NIC on the same network.
  - Before an IP packet can be sen over a wired or wireless network, it must be encapsulated in a data link frame so it can be transmitted over the physical medium.
  - As the IP packet travels from host-to-router, router-to-router, and finally router-to-host, at each point along the way the IP packet is encapsulated in a new data link frame.



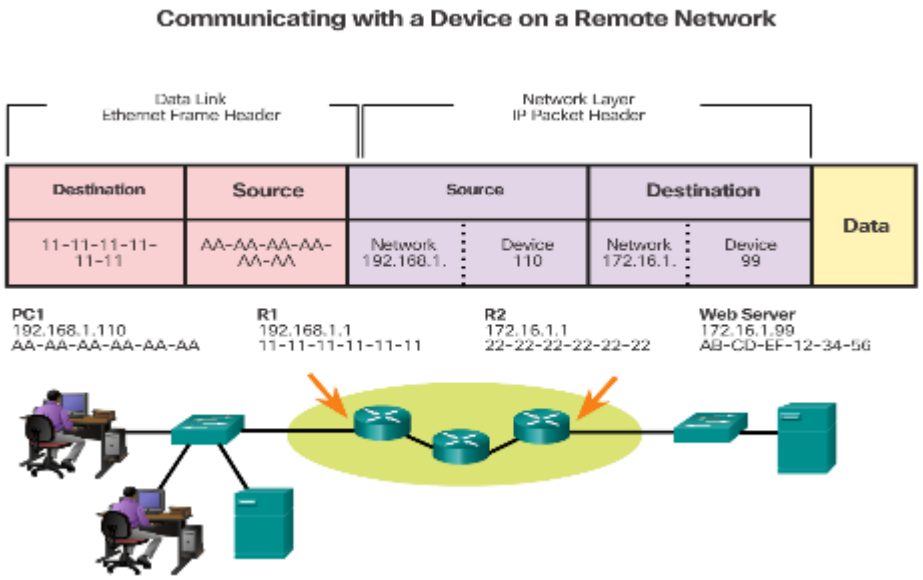
Data Access

- Communication on same network.
  - The **IP Address** of the **Network layer** contains two portion, namely, **Network** and **Host portion**. It could easily be identified through its subnet mask.
  - The **MAC** (Media Access Control) address or Physical address of the **Data Link layer** is a **48-bit Hexadecimal address**.
  - When the sender and receiver of the IP packet are on the same network, the data link frame is sent directly to the receiving device.



Data Access

- Communication on remote network.
  - When the sender of the packet is on a different network from the receiver, the source and destination IP addresses will represent hosts on different networks. This will be indicated by the network portion of the IP address of the destination host.
  - When the sender and receiver of the IP packet are on different networks, the Ethernet data link frame cannot be sent directly to the destination host because the host is not directly reachable in the network of the sender. The Ethernet frame must be sent to another device known as the router or default gateway. In our example, the default gateway is R1. R1 has an Ethernet data link address that is on the same network as PC1.



3.4 Chapter Summary

Cisco | Networking Academy®
Mind Wide Open™

Summary

- Explain how rules are used to facilitate communication.
- Explain the role of protocols and standards organizations in facilitating interoperability in network communications.
- Explain how devices on a LAN access resources in a small to medium-sized business network.