Ch 3: Network Protocols and Communications

Computer Networks Course

BY

Dr. Essam Halim Houssein

Cisco | Networking Academy®
Mind Wide Open™

The Rules

A network can be as complex as devices connected across the Internet, or as simple as two computers directly connected to one another with a single cable, and anything in-between. Networks can vary in size, shape, and function. However, simply having the physical connection between end devices is not enough to enable communication. **For communication to occur, devices must know "how" to communicate.**

The protocols put in place must account for the following requirements:

- An identified sender and receiver
- Common language and grammar
- Speed and timing of delivery
- Confirmation or acknowledgement requirements

In addition to identifying the source and destination, computer and network protocols define the details of how a message is transmitted across a network to answer the above requirements. While there are many protocols that must interact, common computer protocols include:

- **Message encoding**
- **Message formatting and encapsulation**
- **Message size**
- **Message timing**
- **Message delivery options**

Encoding is the process of converting information into another, acceptable form, for transmission. **Decoding** reverses this process in order to interpret the information.

Encoding between hosts must be in an appropriate form 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 in order to interpret the message.

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.

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 intended 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				

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 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 size restrictions of frames require the source host to break a long message into individual pieces that meet both the minimum and maximum size requirements. This is known as **segmenting**. Each segment is encapsulated in a separate frame with the address information, and is sent over the network. At the receiving host, the messages are **de-encapsulated** and put back together to be processed and interpreted.

Message Timing

Another factor that affects how well a message is received and understood is timing. People use timing to determine when to speak, how fast or slow to talk, and how long to wait for a response. These are the rules of engagement for message timing.

1. **Access Method**
2. **Flow Control**
3. **Response Timeout**

Access Method

Access method **determines when someone is able to send** a message. These timing rules are based on the environment. For example, you may be able to speak whenever you have something to say. In this environment, a person must wait until no one else is talking before speaking. 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.

it is necessary for computers to define an access method. Hosts on a network need an access method to know when to begin sending messages and how to respond when errors occur.

Flow Control

Timing also affects **how much information can be sent and the speed** that it can be delivered.

In network communication, a sending host can transmit messages at a faster rate than the destination host can receive and process. Source and destination hosts use flow control to negotiate correct timing for successful communication.

Response Timeout

If a person asks a question and does not hear a response within an acceptable amount of time, the person assumes that no answer is coming and reacts accordingly. The person may repeat the question, or may go on with the conversation. Hosts on the network also have rules that **specify how long to wait for responses** and what action to take if a response timeout occurs.

Message Delivery Options

A one-to-one delivery option is referred to as a **unicast**, meaning that there is only a single destination for the message.

When a host needs to send messages using a one-to-many delivery option, it is referred to as a multicast. **Multicasting** is the delivery of the same message to a group simultaneously.

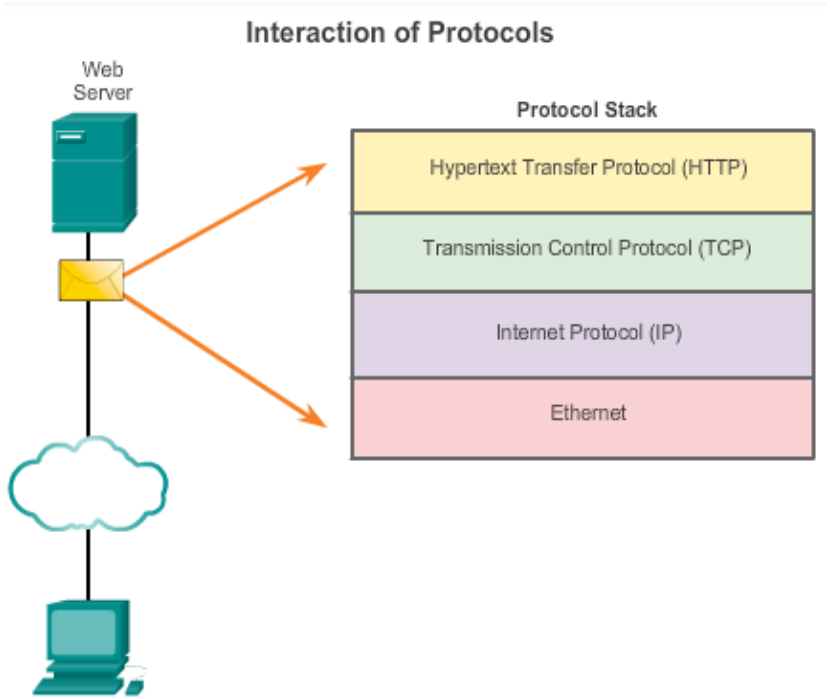
If all hosts on the network need to receive the message at the same time, a **broadcast** is used. Broadcasting represents a one-to-all message delivery option. Additionally, hosts have requirements for acknowledged versus unacknowledged messages.

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.

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 IP, HTTP, and DHCP

An example of using the protocol suite in network communications is the interaction between a web server and a web client. This interaction uses a number of protocols and standards in the process of exchanging information between them. **The different protocols work together to ensure that the messages are received and understood by both parties.**



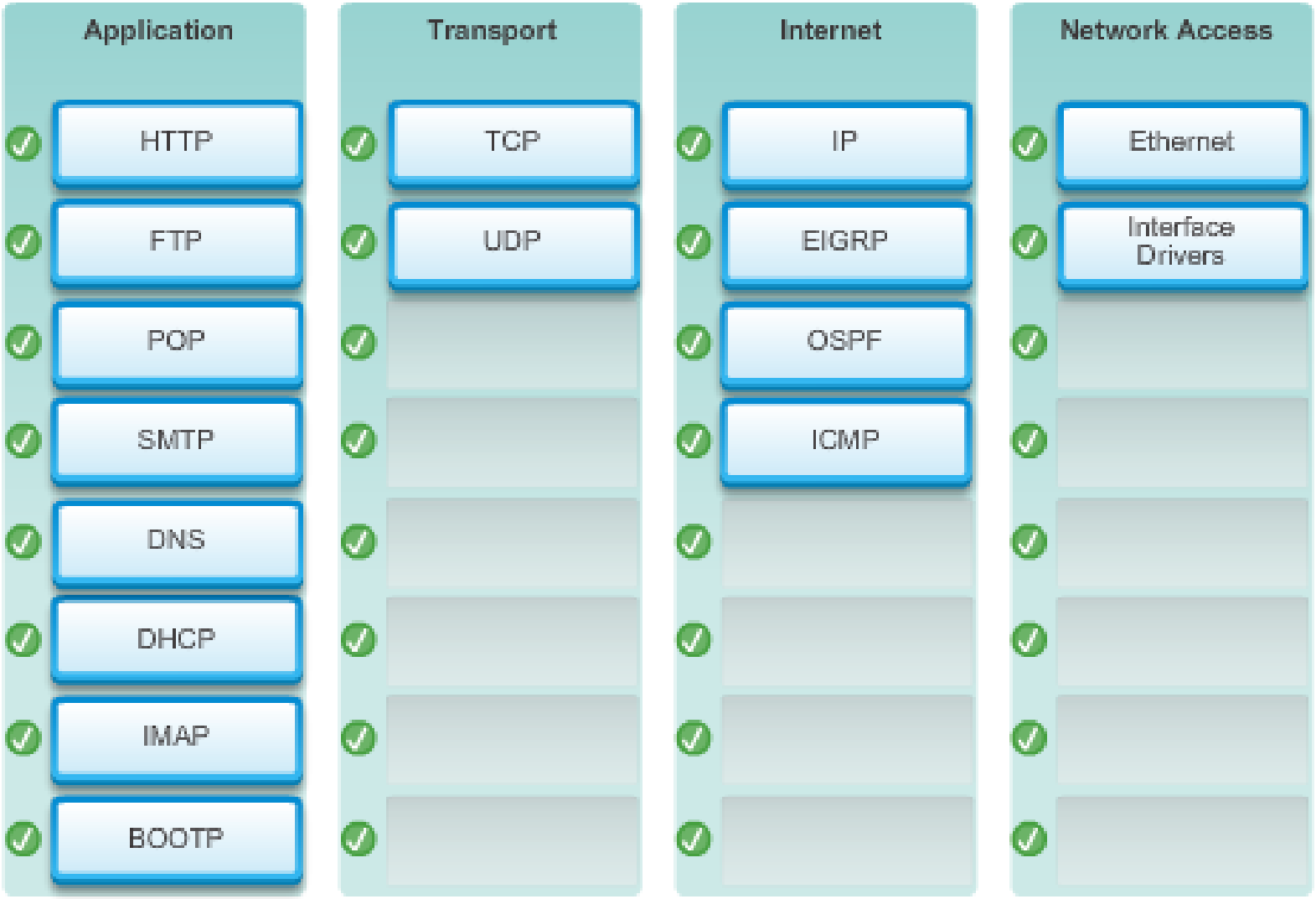
Protocol Suites

A protocol suite 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.

Protocol Suites and Industry Standards

TCP/IP	ISO	AppleTalk	Novell Netware
HTTP DNS DHCP FTP	ACSE ROSE TRSE SESE	AFP	NDS
TCP UDP	TP0 TP1 TP2 TP3 TP4	ATP AEP NBP RTMP	SPX
IPv4 IPv6 ICMPv4 ICMPv6	CONP/CMNS CLNP/CLNS	AARP	IPX
Ethernet PPP Frame Relay ATM WLAN			

Network Protocols and Standards



The Institute of Electrical and Electronics Engineers (IEEE)

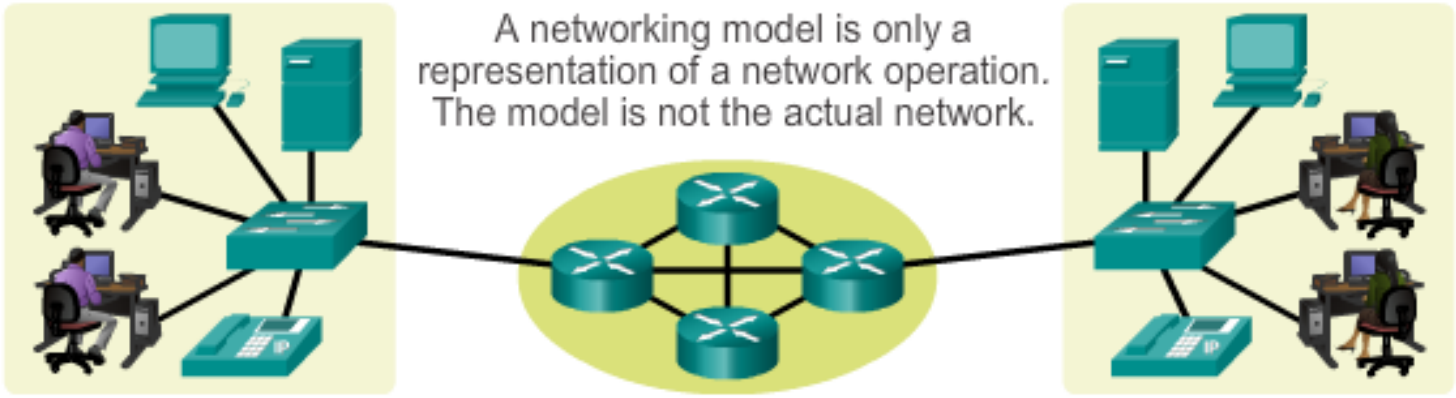
IEEE 802 Working Groups and Study Groups

- 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

The Benefits of Using a Layered Model

1. 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.
2. Fostering competition because products from different vendors can work together.
3. Preventing technology or capability changes in one layer from affecting other layers above and below.
4. Providing a common language to describe networking functions and capabilities.

Open Systems Interconnection



OSI Model	TCP/IP Protocol Suite	TCP/IP Model
Application	HTTP, DNS, DHCP, FTP	Application
Presentation		
Session		
Transport	TCP, UDP	Transport
Network	IPv4, IPv6, ICMPv4, ICMPv6	Internet
Data Link	PPP, Frame Relay, Ethernet	Network Access
Physical		

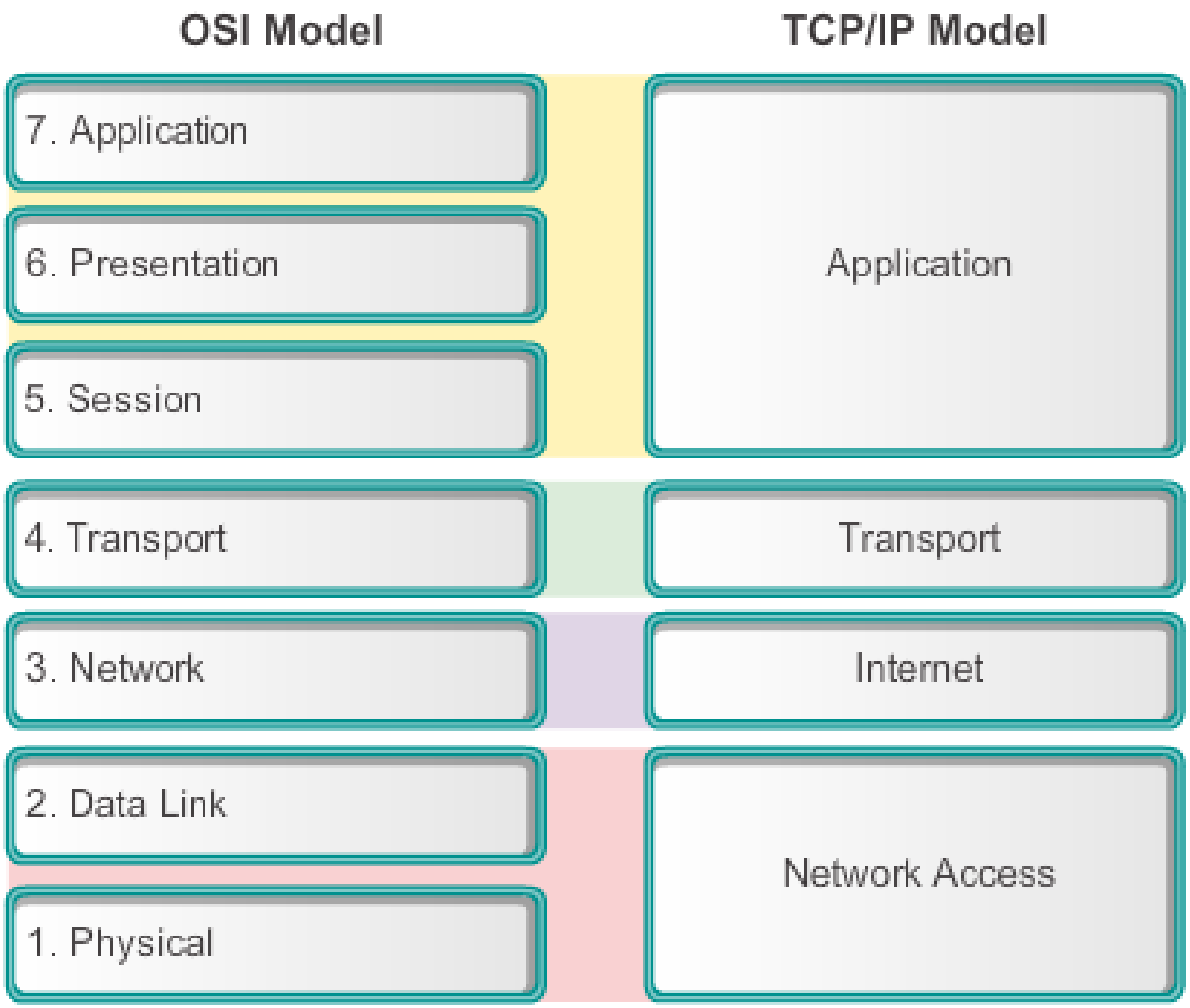
Transmission Control Protocol/IP

7-contains protocols used for process-to-process communications.
6-provides for common representation of the data transferred between application layer services.
5-provides services to the presentation layer to organize its dialogue and to manage data exchange.
4-defines services to segment, transfer, and reassemble the data for individual communications between the end devices.
3-provides services to exchange the individual pieces of data over the network between identified end devices.
2-describe methods for exchanging data frames between devices over a common media.
1-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.

TCP/IP 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.

Comparing the OSI Model and the TCP/IP Model



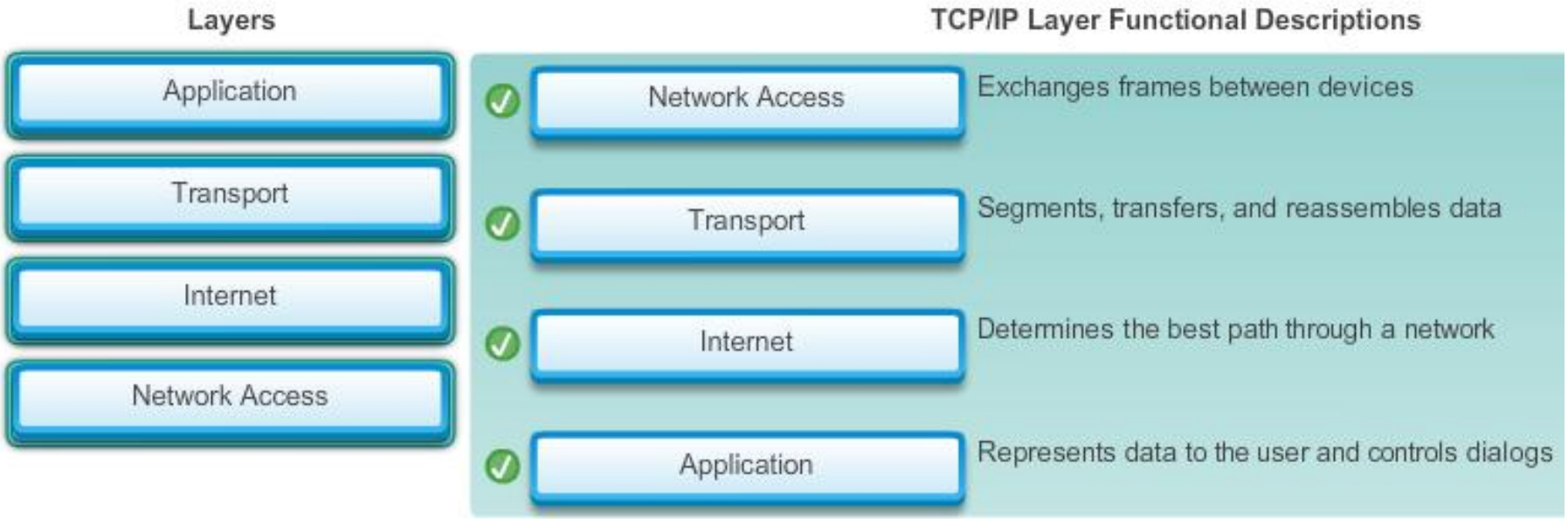
Activity (1)

Layers		OSI Layer Functional Descriptions
7	Application	Segments, transfers and reassembles data
6	Presentation	Exchanges frames between devices
5	Session	Contains protocols used for process-to-process communications
4	Transport	Provides a data path or route
3	Network	Bit transmission
2	Data Link	
1	Physical	

Layers		OSI Layer Functional Descriptions	
7	Application	Transport	Segments, transfers and reassembles data
6	Presentation	Data Link	Exchanges frames between devices
5	Session	Application	Contains protocols used for process-to-process communications
4	Transport	Network	Provides a data path or route
3	Network	Physical	Bit transmission
2	Data Link		
1	Physical		

Activity (2)

Layers	TCP/IP Layer Functional Descriptions
Application	Exchanges frames between devices
Transport	Segments, transfers, and reassembles data
Internet	Determines the best path through a network
Network Access	Represents data to the user and controls dialogs

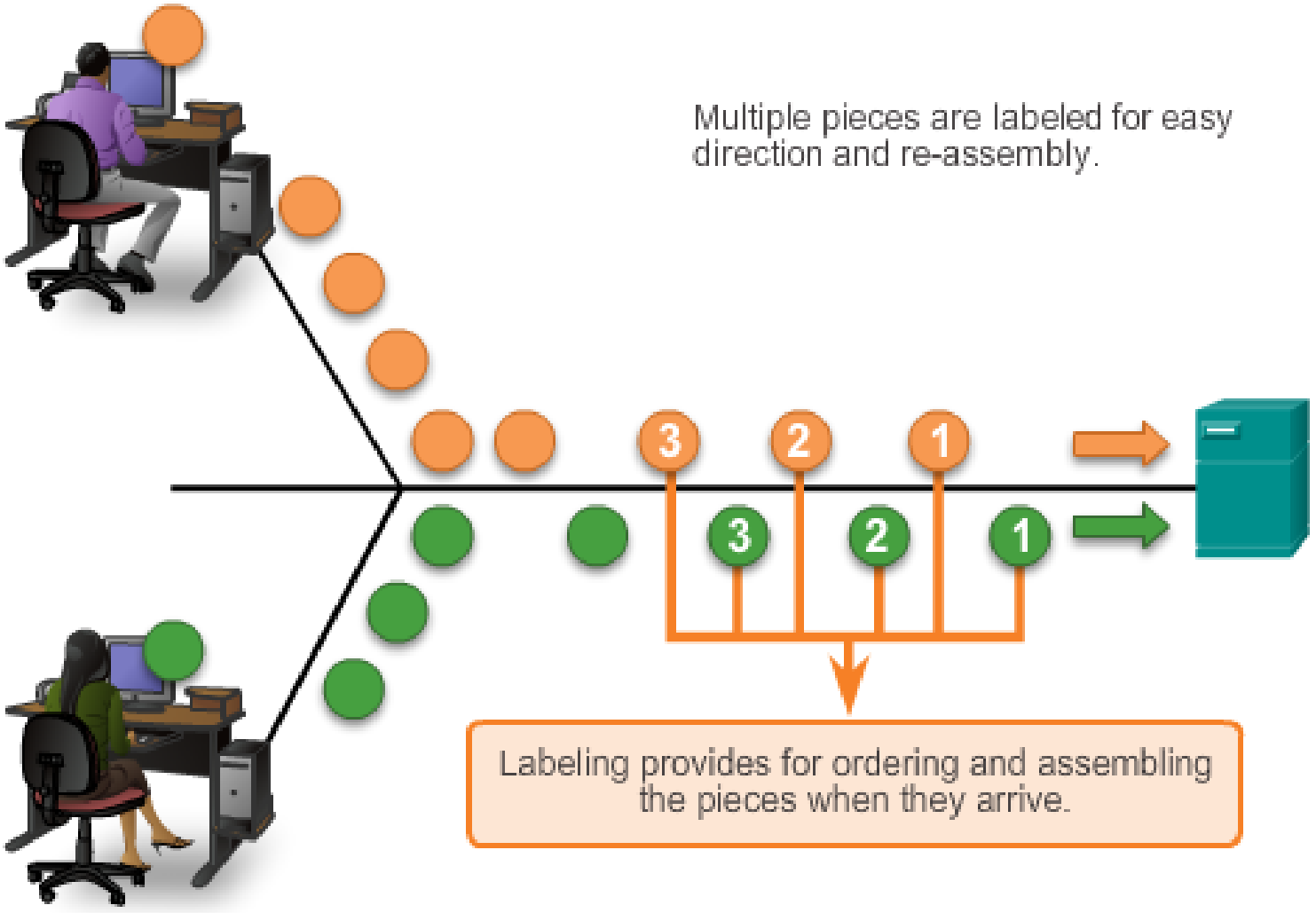


Moving Data in the Network

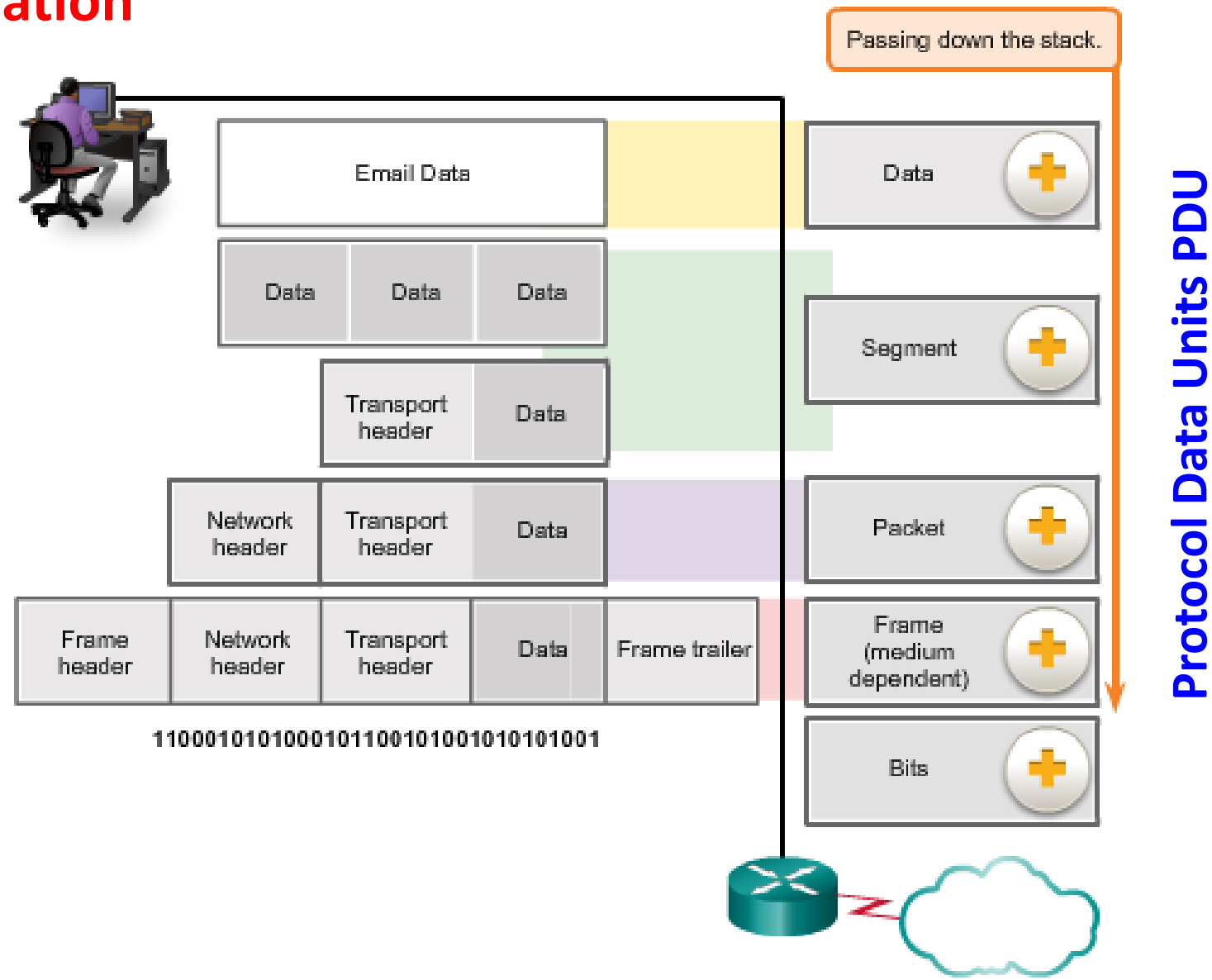
A better approach is to divide the data into smaller, more manageable pieces to send over the network. This division of the data stream into smaller pieces is called **segmentation**.

Multiplexing – interleaving the pieces as they traverse the media.

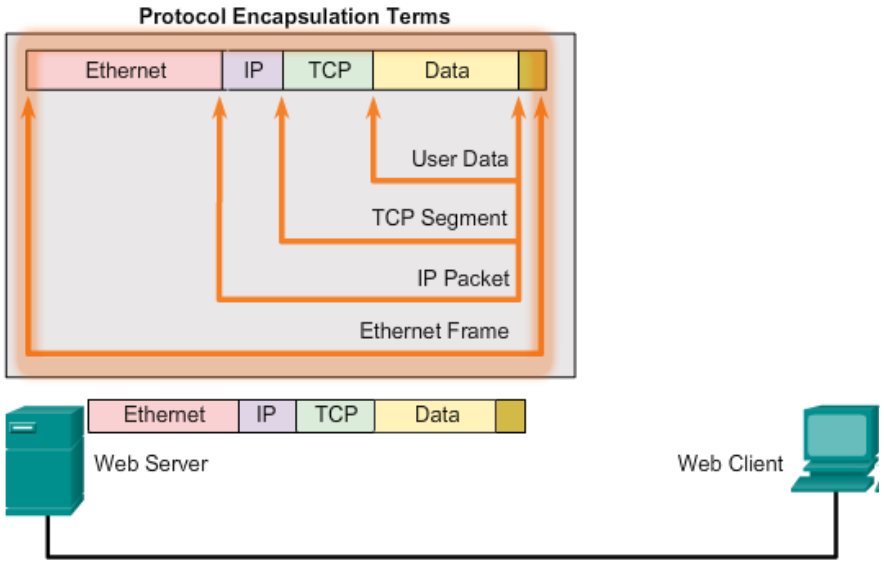
Communicating the Message



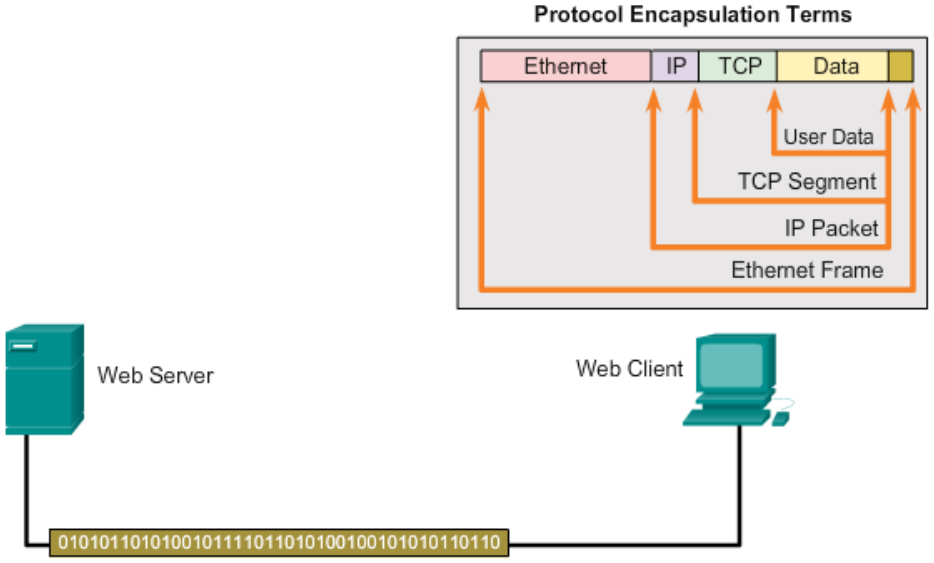
Encapsulation



Protocol Operation of Sending a Message



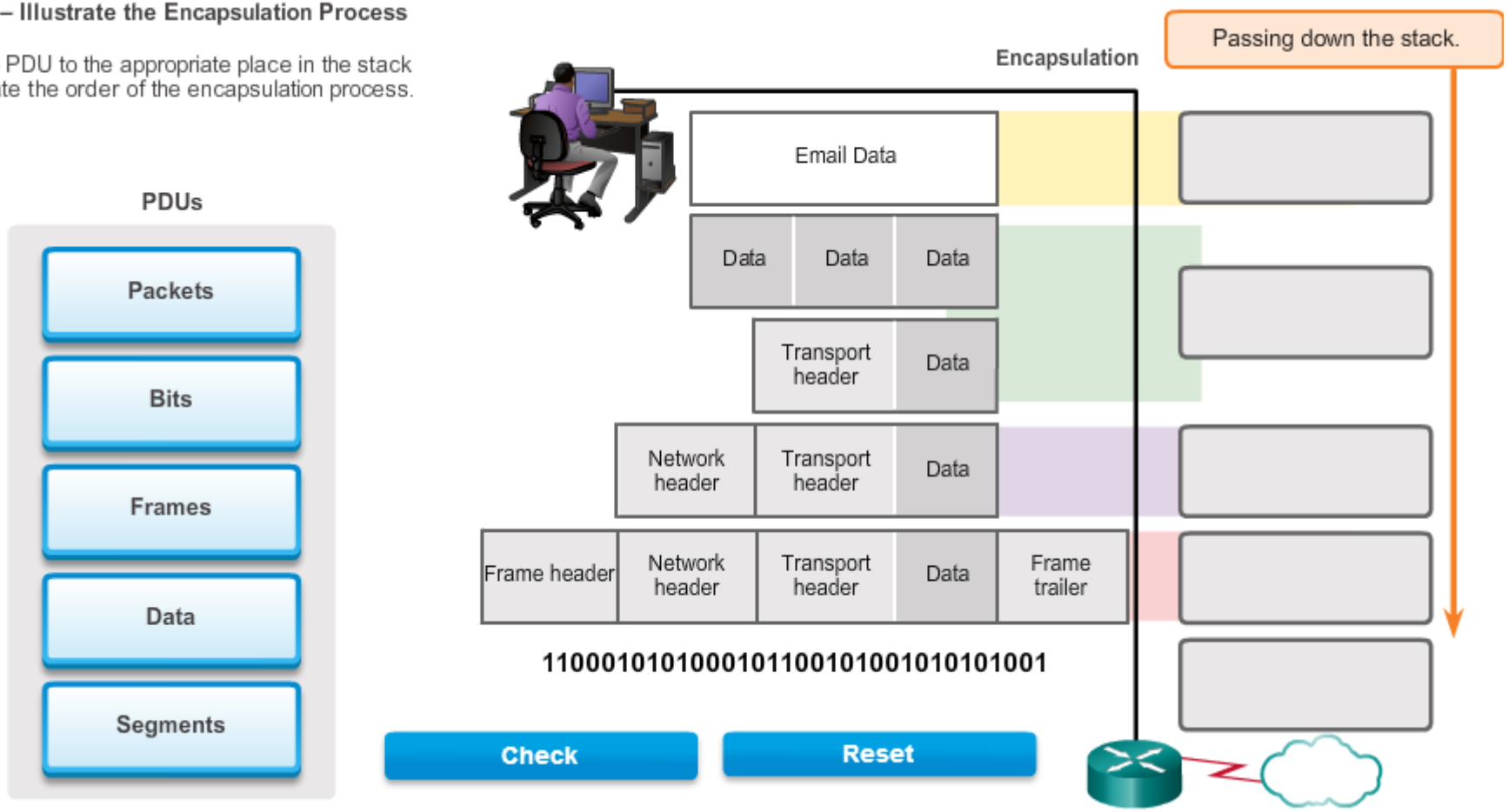
Protocol Operation of Receiving a Message



Activity (3)

Activity – Illustrate the Encapsulation Process

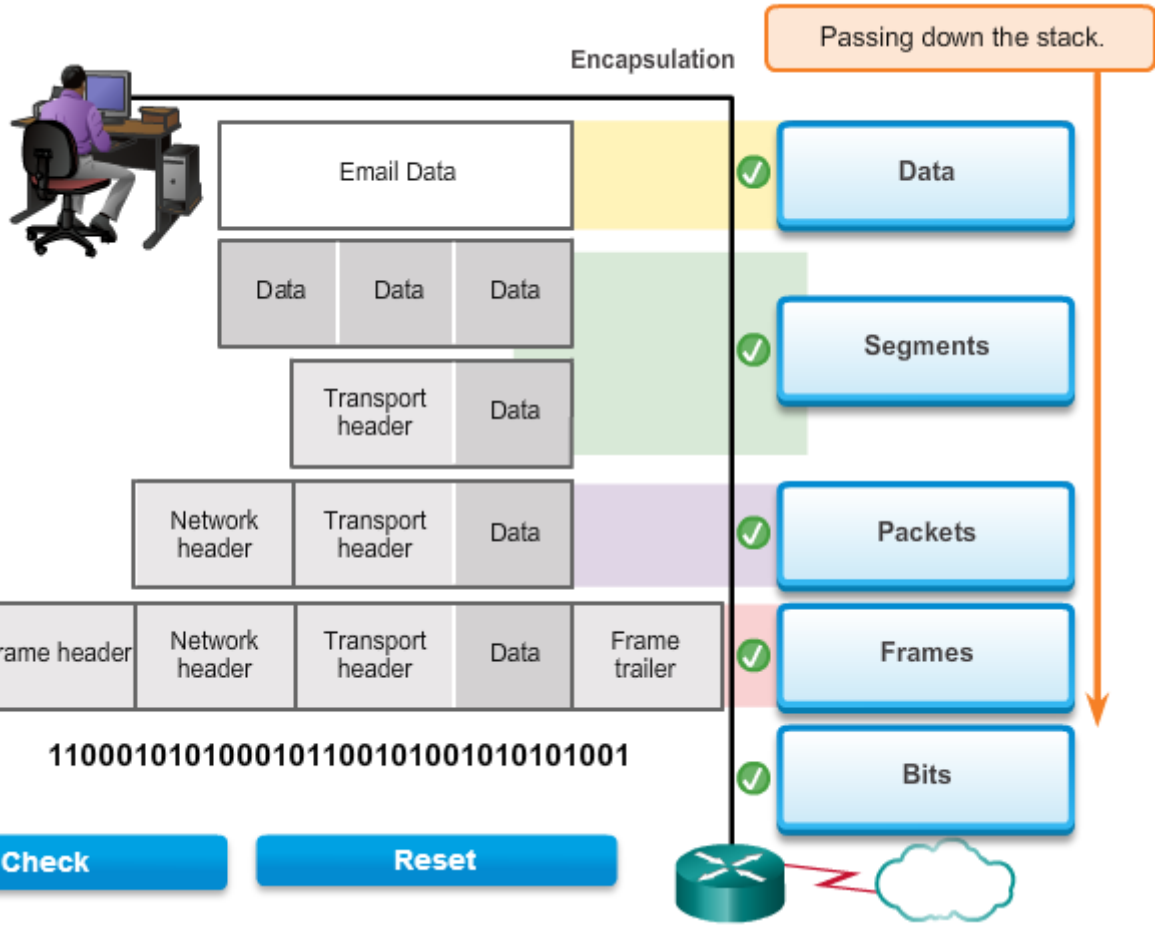
Drag the PDU to the appropriate place in the stack to illustrate the order of the encapsulation process.



Activity – Illustrate the Encapsulation Process

Drag the PDU to the appropriate place in the stack to illustrate the order of the encapsulation process.

PDUs



Network Addresses

The network and data link layers are **responsible** for delivering the data from the source device to the destination device.

Network layer source and destination addresses - Responsible for delivering the **IP packet** from the original source to the final destination, either on the same network or to a remote network.

Data link layer source and destination addresses – Responsible for delivering the data link **frame** from one network interface card (NIC) to another NIC on the same network.

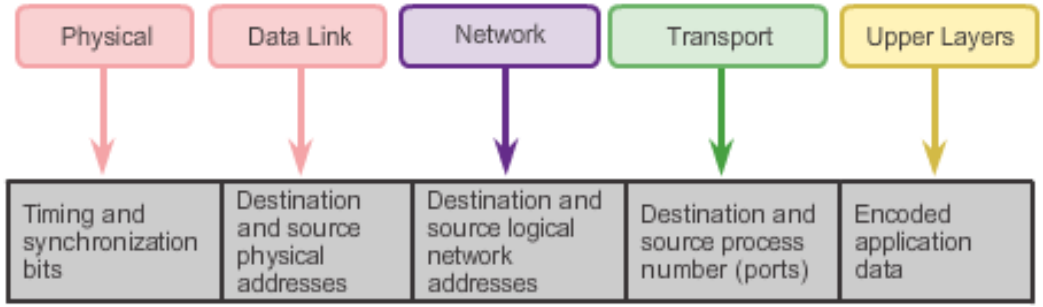
An **IP address** is the network layer, or Layer 3, logical address used to deliver the IP packet from the original source to the final destination.

The IP packet contains two IP addresses:

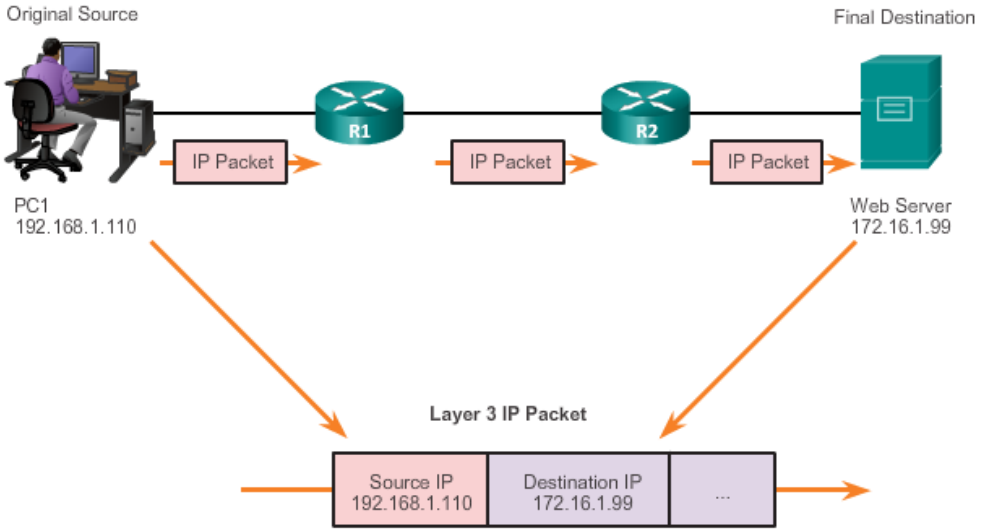
Source IP address - The IP address of the sending device, the original source of the packet.

Destination IP address - The IP address of the receiving device, the final destination of the packet.

Network Addresses and Data Link Addresses



Layer 3 Network Addresses



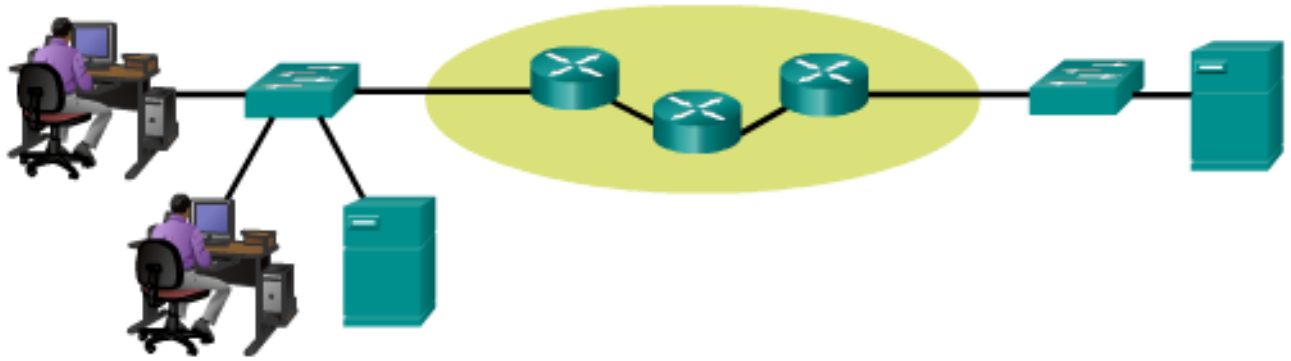
Communicating with a Device on the Same Network

Data Link
Ethernet Frame Header

Network Layer
IP Packet Header

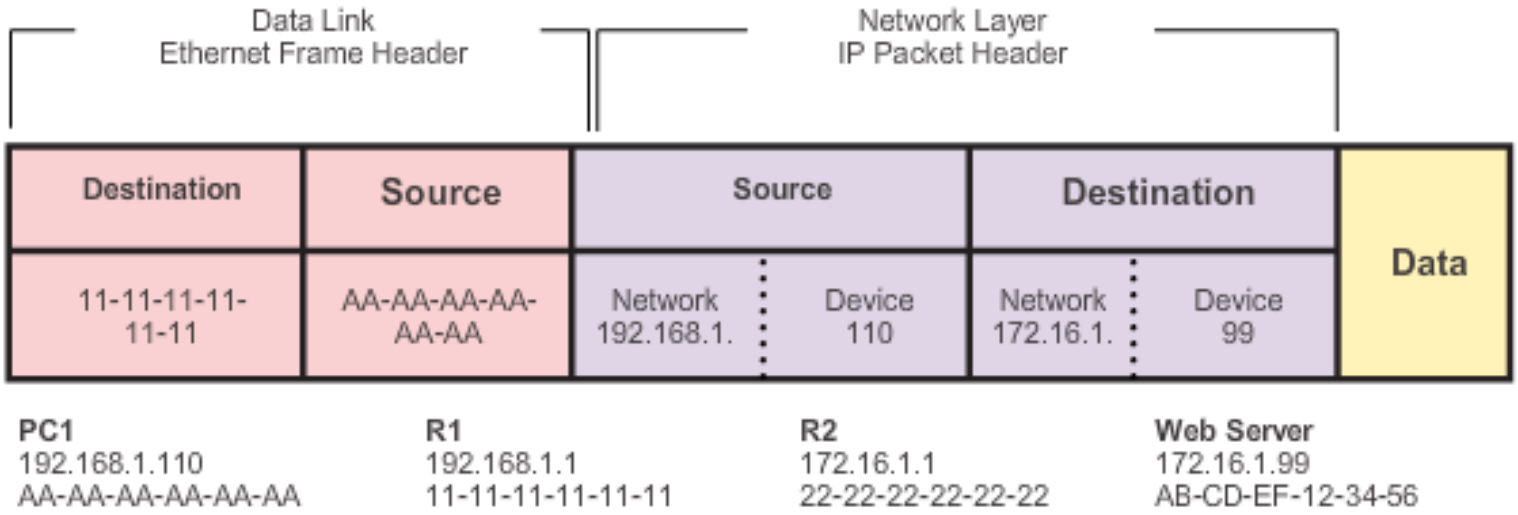
Destination	Source	Source		Destination		Data
CC-CC-CC-CC-CC-CC	AA-AA-AA-AA-AA-AA	Network 192.168.1.	Host 110	Network 192.168.1.	Host 9	

PC1
192.168.1.110
AA-AA-AA-AA-AA-AA



FTP Server
192.168.1.9
CC-CC-CC-CC-CC-CC

Communicating with a Device on a Remote Network



Summary

Data networks are systems of end devices, intermediary devices, and the media connecting them. For communication to occur, these devices must know how to communicate.

These devices must comply with communication rules and protocols. TCP/IP is an example of a protocol suite. Most protocols are created by a standards organization such as the IETF or IEEE. The Institute of Electrical and Electronics Engineers is a professional organization for those in the electrical engineering and electronics fields. ISO, the International Organization for Standardization, is the world's largest developer of international standards for a wide variety of products and services.

The most widely-used networking models are the OSI and TCP/IP models. Associating the protocols that set the rules of data communications with the different layers of these models is useful in determining which devices and services are applied at specific points as data passes across LANs and WANs.

Data that passes down the stack of the OSI model is segmented into pieces and encapsulated with addresses and other labels. The process is reversed as the pieces are de-encapsulated and passed up the destination protocol stack. The OSI model describes the processes of encoding, formatting, segmenting, and encapsulating data for transmission over the network.

The TCP/IP protocol suite is an open standard protocol that has been endorsed by the networking industry and ratified, or approved, by a standards organization. The Internet Protocol Suite is a suite of protocols required for transmitting and receiving information using the Internet.

Protocol Data Units (PDUs) are named according to the protocols of the TCP/IP suite: data, segment, packet, frame, and bits.