



Cisco Networking Academy

CCNA R&S: Introduction to Networks

Chapter 3:

Network Protocols and Communications

Upon completion of this chapter you will be able to:

- 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.
- Explain why RFCs became the process for establishing standards.
- Describe the RFC process.
- Explain how data encapsulation allows data to be transported across the network.
- Explain how local hosts access local resources on a network.
- Explain how local hosts access remote resources on a network.

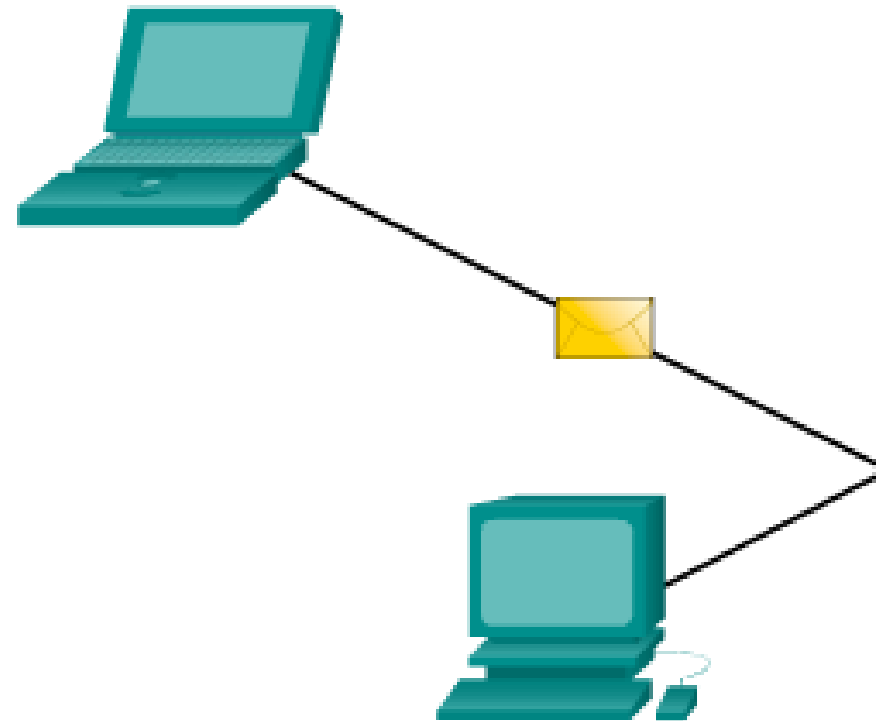
3.0.1.2 Class Activity - Designing a Communications System



Network Protocols and Standards make network communication easier.

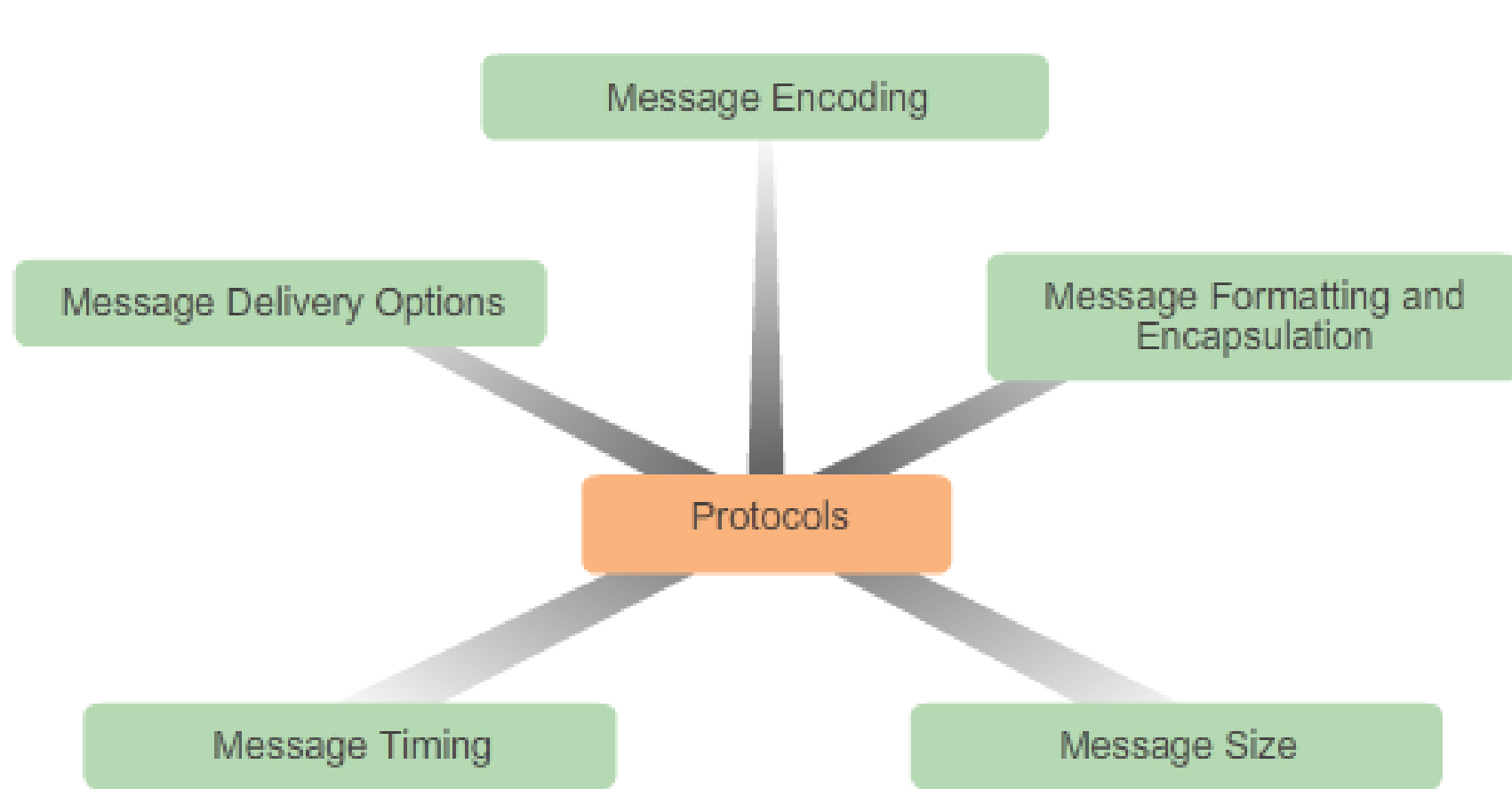
3.1.1.1 What is Communication?

Computer Communication



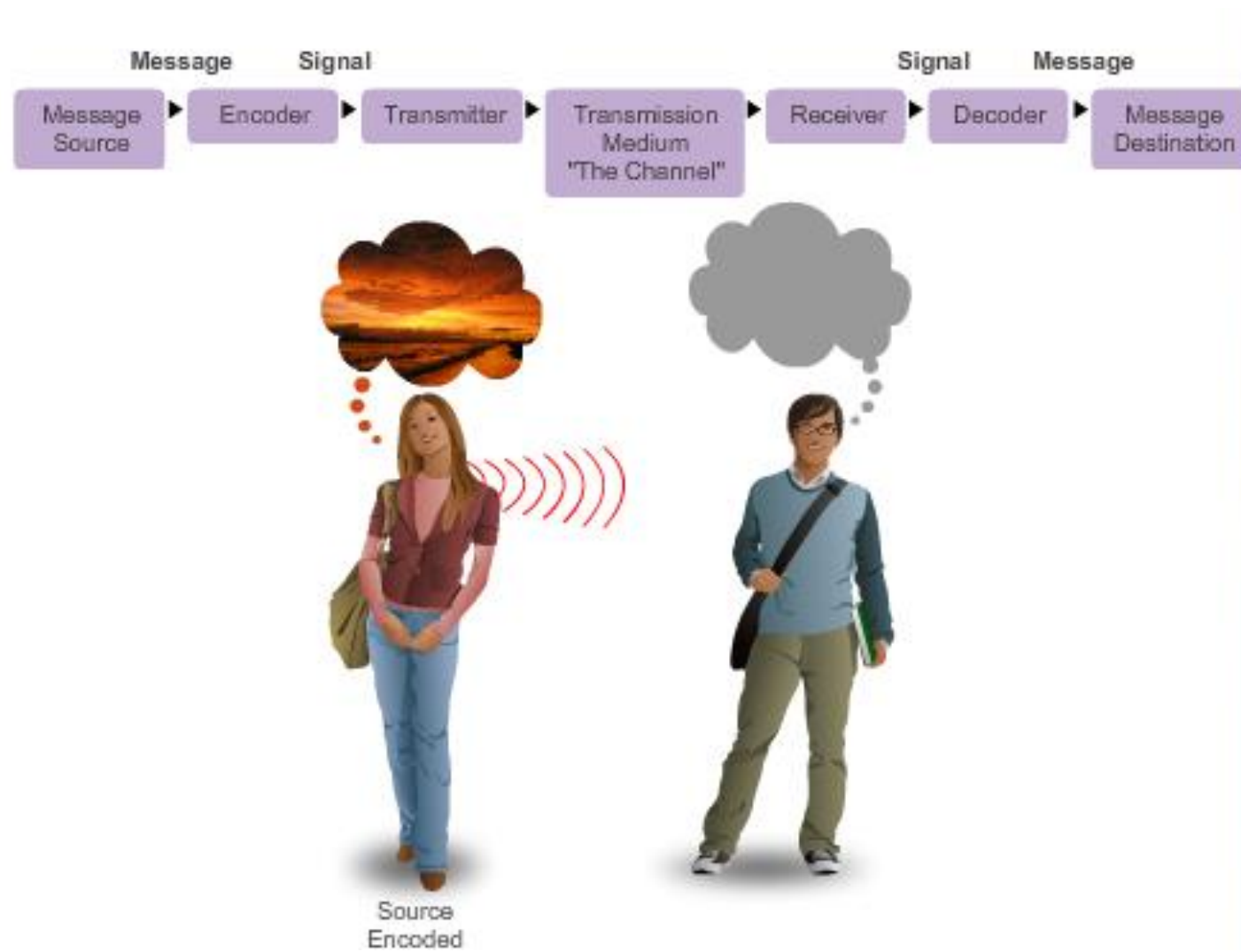
Rules or
Protocols

3.1.1.2 Establishing the Rules



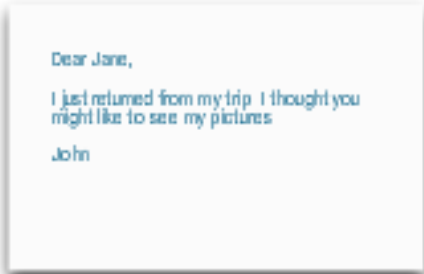
The protocols used are specific to the characteristics of the communication method, including the characteristics of the source, destination and channel. These rules, or protocols, must be followed in order for the message to be successfully delivered and understood


3.1.1.3 Message Encoding



Message Encoding
One of the first steps to sending a message is encoding it. Encoding is the process of converting information into another, acceptable form, for transmission. Decoding reverses this process in order to interpret the information

3.1.1.4 Message Formatting and Encapsulation



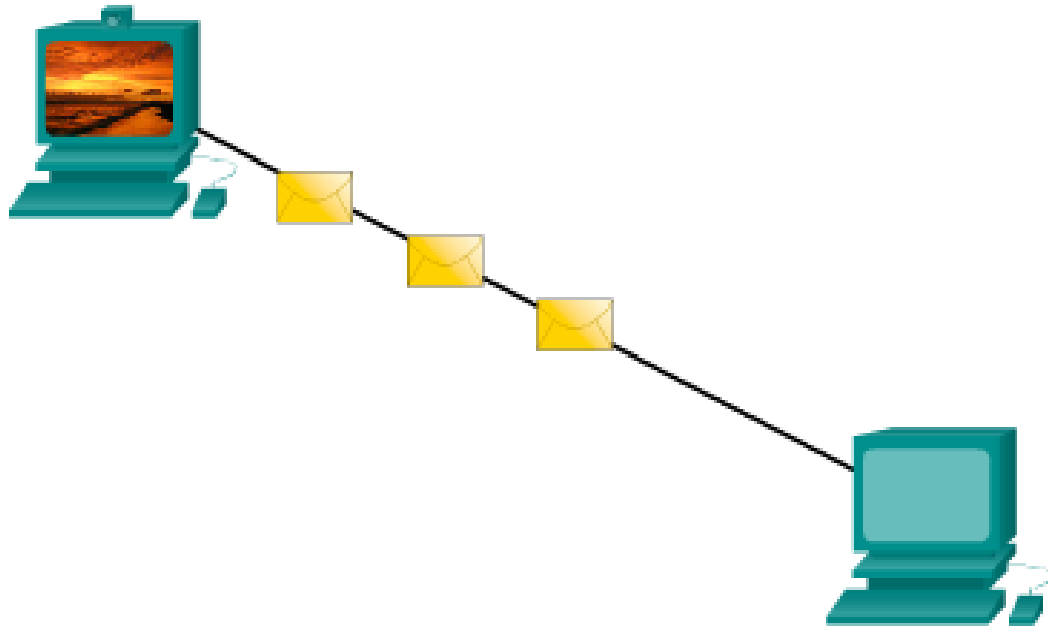
Recipient (destination) Location address	Sender (source) Location address	Salutation (start of message indicator)	Recipient (destination) identifier	Content of Letter (encapsulated data)	Sender (source) identifier	End of Frame (End of message indicator)
Envelope Addressing		Encapsulated Letter				
1400 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	

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 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.

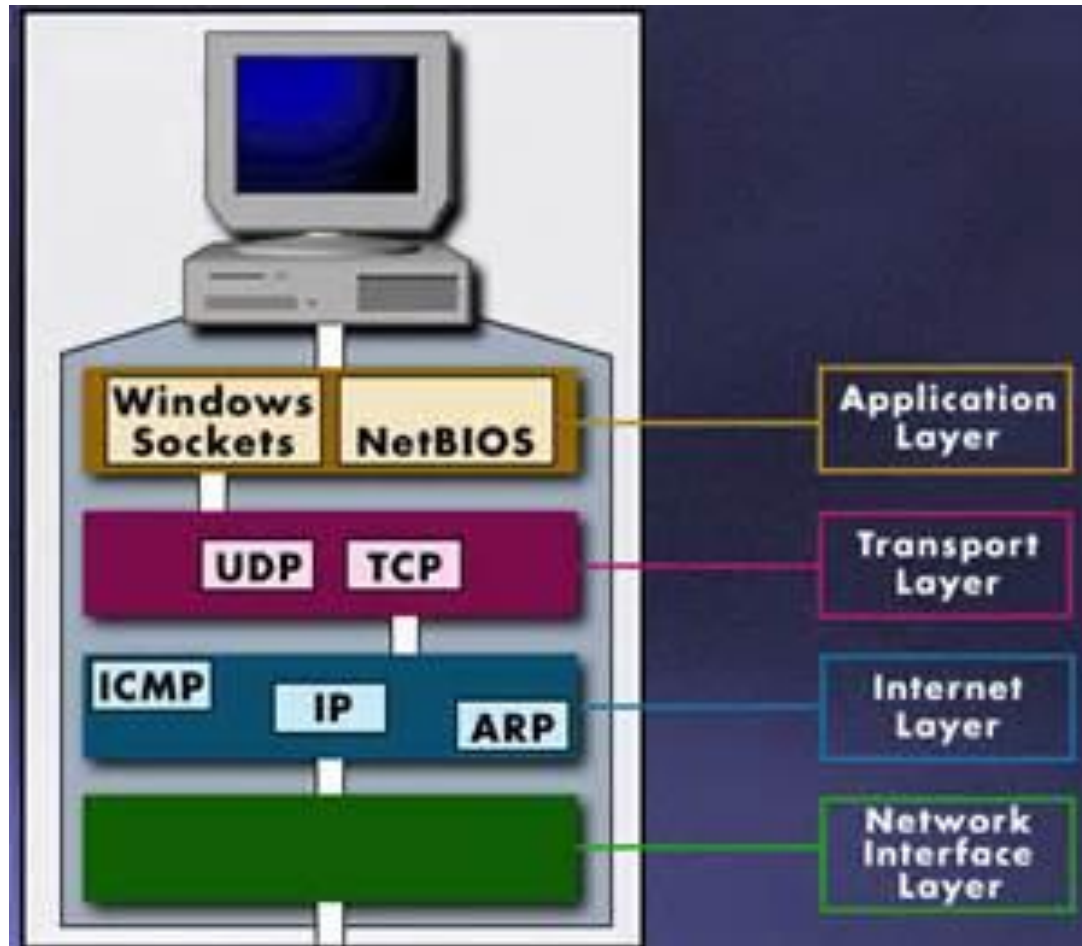
3.1.1.5 Message Size

Computer Communication



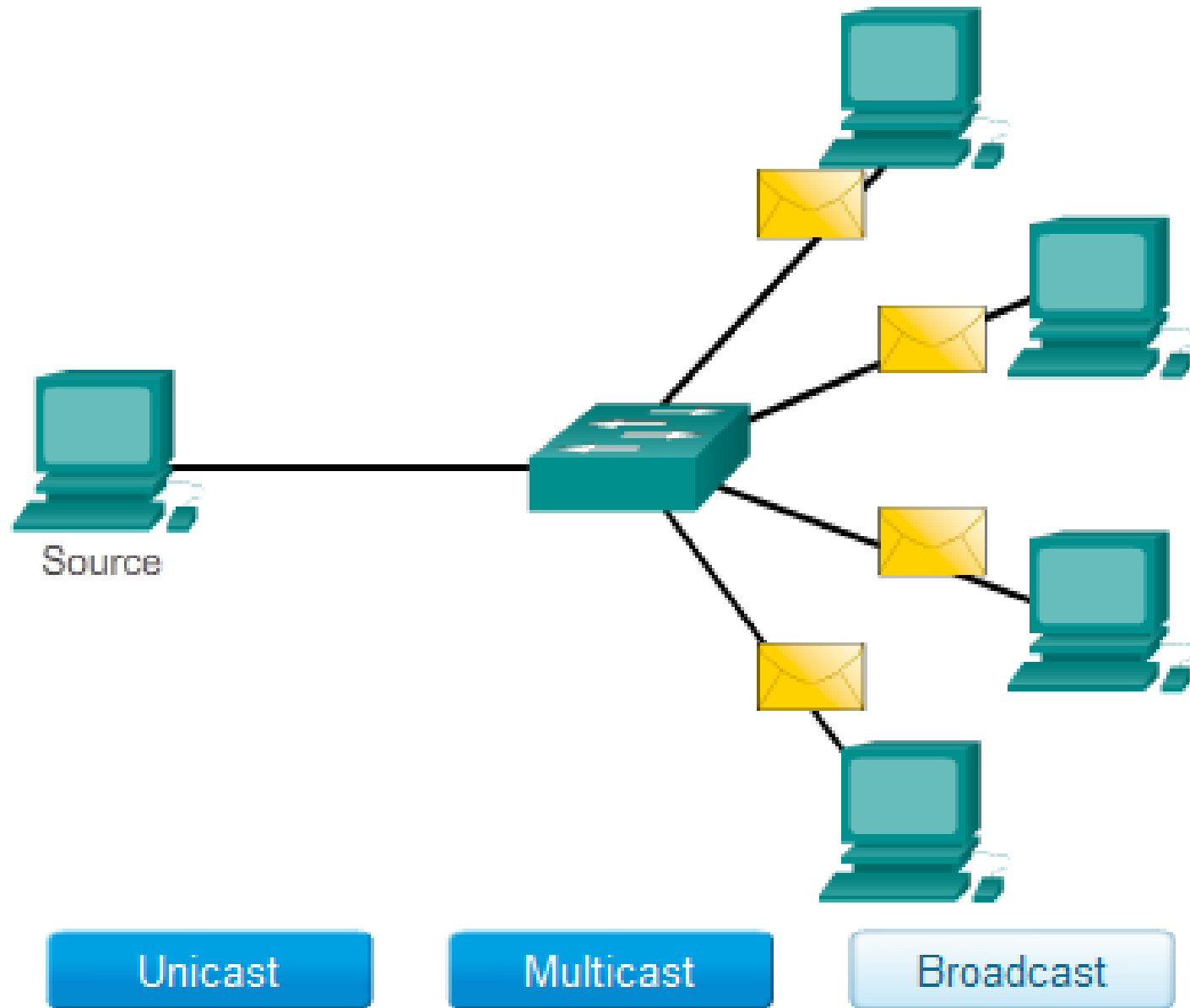
- When a long message is sent from one host to another over a network, it is necessary to break the message into smaller pieces.
- The rules that govern the size of the pieces, or frames, communicated across the network are very strict.
- They can also be different, depending on the channel used. Frames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

TCP/IP



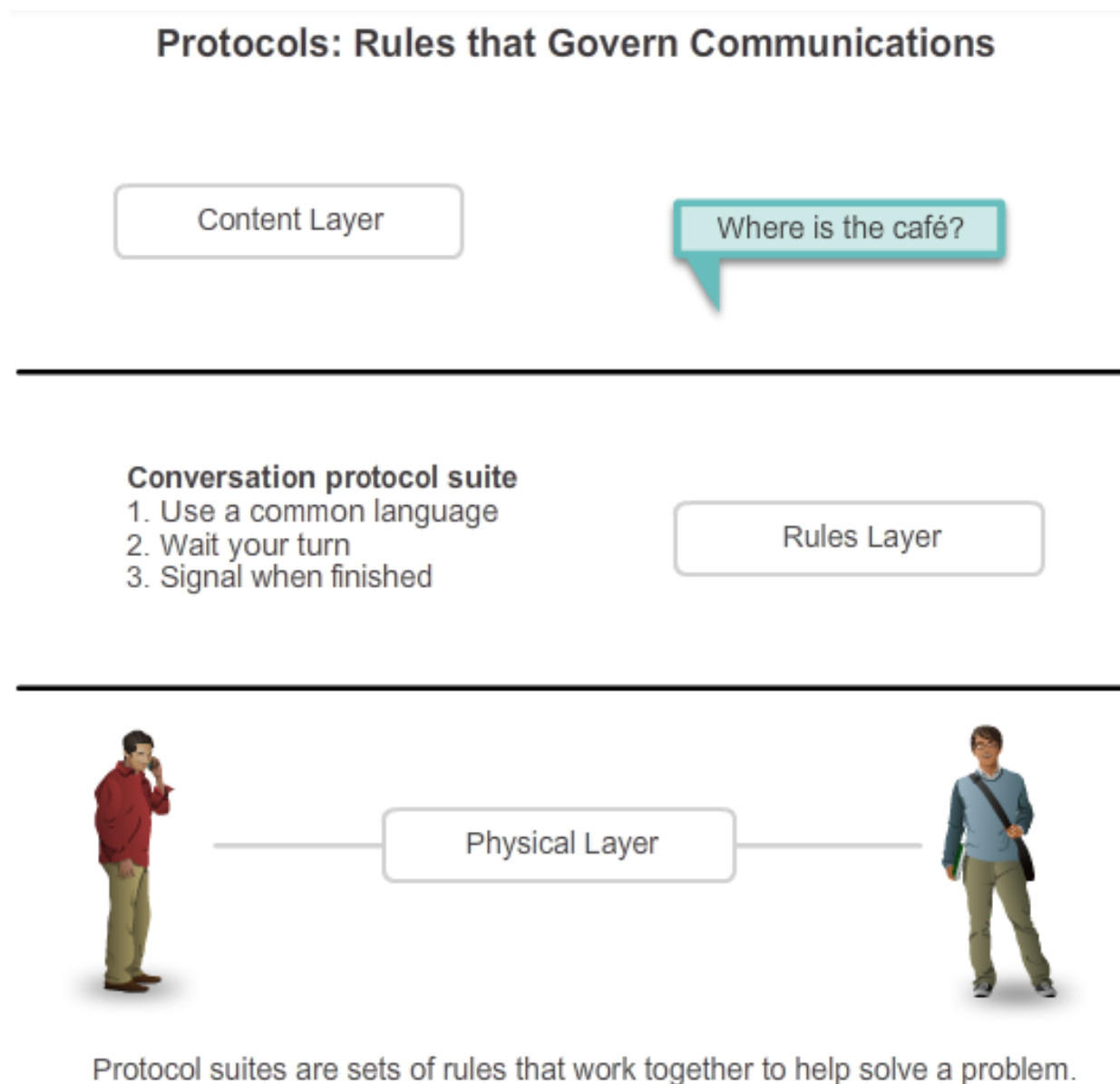
- Hosts on a network need an access method to know when to begin sending messages and how to respond when errors occur.
- Source and destination hosts use flow control to negotiate correct timing for successful communication.
- Hosts on the network also have rules that specify how long to wait for responses and what action to take if a response timeout occurs.

3.1.1.7 Message Delivery Options



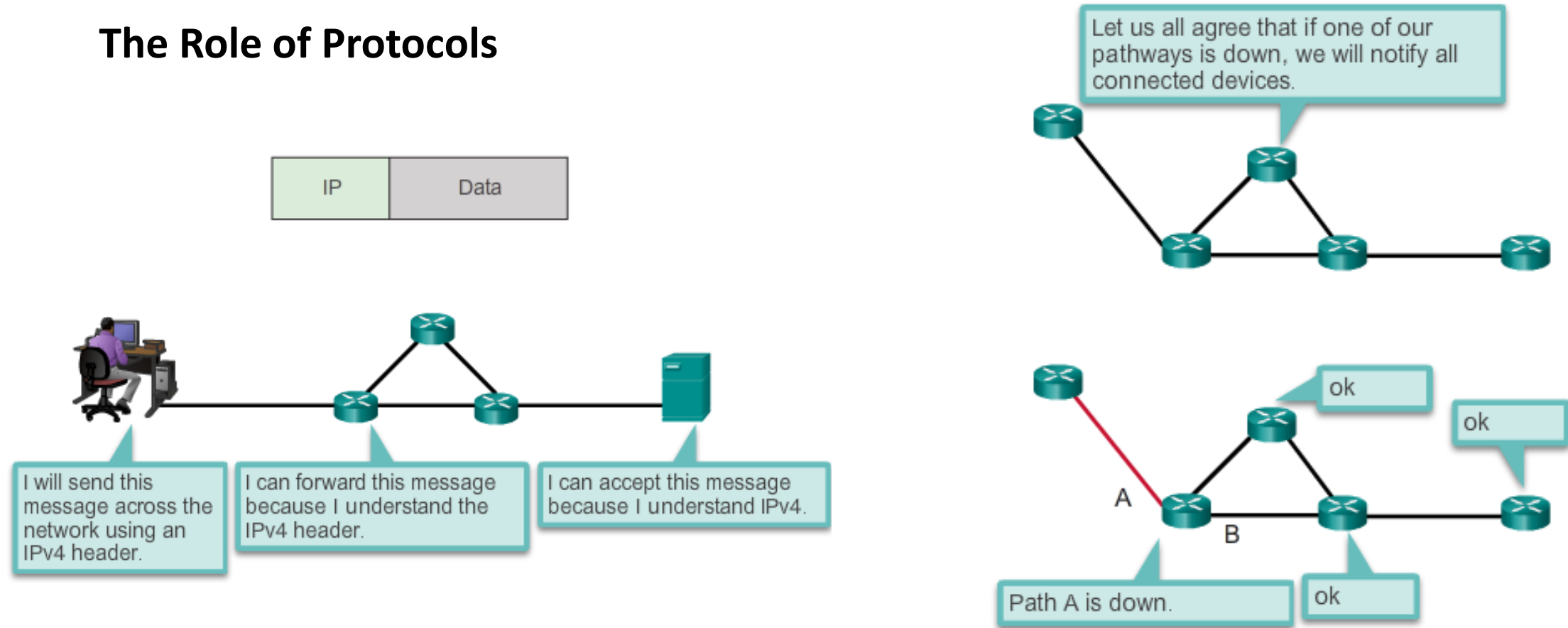
- A one-to-one delivery option is referred to as a **unicast**, meaning that there is only a single destination for the message.
- When a host needs to send messages using a one-to-many delivery option, it is referred to as a **multicast**. Multicasting is the delivery of the same message to a group of host destinations simultaneously.
- If all hosts on the network need to receive the message at the same time, a **broadcast** is used.

3.2.1.1 Protocols: Rules that Govern Communications



- Various network and computer protocols must be able to interact and work together for network communication to be successful.
- 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.

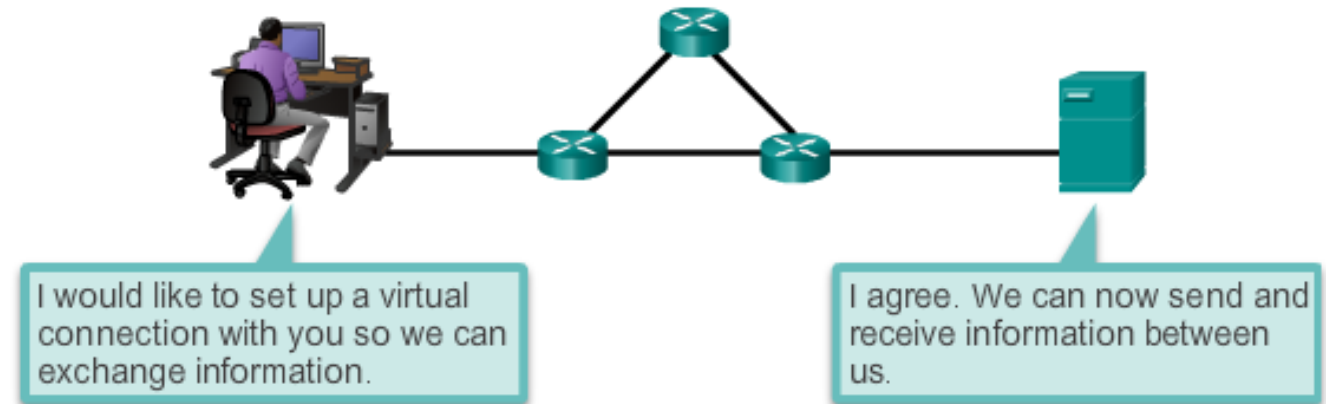
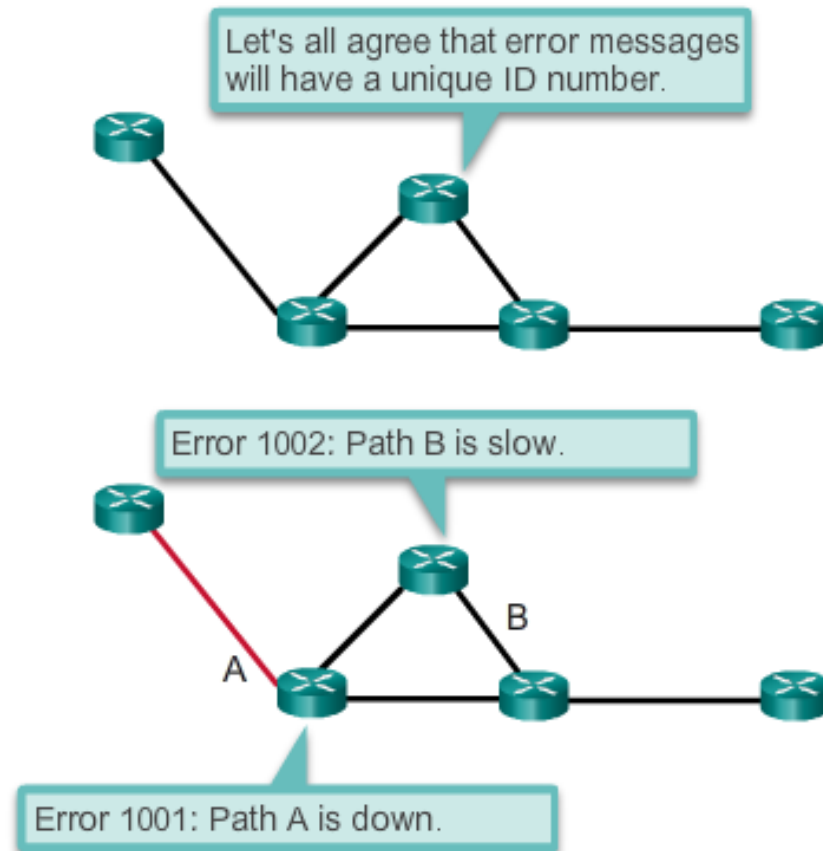
The Role of Protocols



The figures illustrate networking protocols that describe the following processes:

- How the message is formatted or structured, as shown in Figure 1
- The process by which networking devices share information about pathways with other networks, as shown in Figure 2

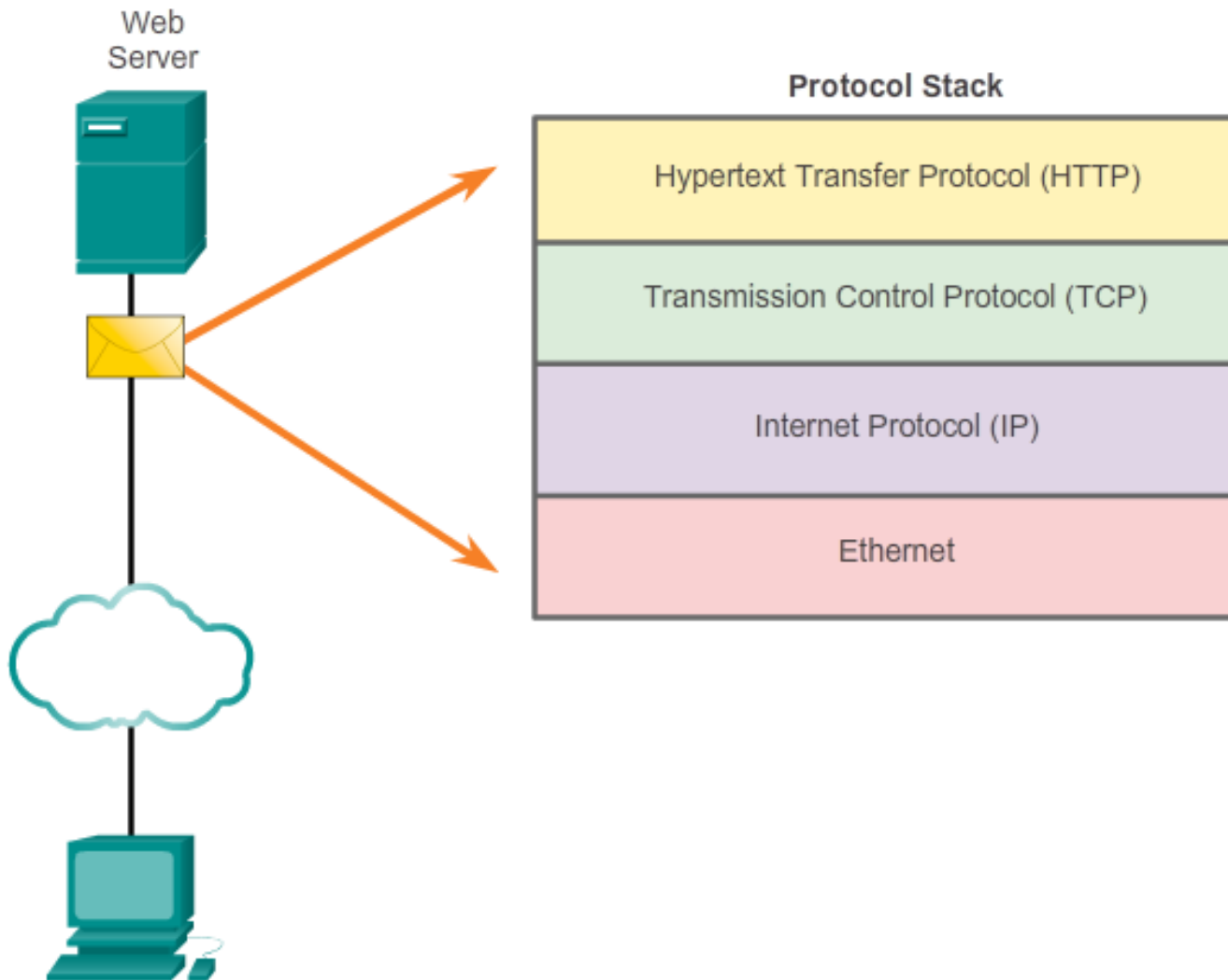
3.2.1.2 Network Protocols



- How and when error and system messages are passed between devices, as shown in Figure 3
- The setup and termination of data transfer sessions, as shown in Figure 4

3.2.1.3 Interaction of Protocols

Interaction of Protocols



- HTTP defines the content and formatting of the requests and responses between the client and server
- TCP divides the HTTP messages into smaller pieces, called segments. Segments are sent between the web server and client processes running at the destination host.
- IP is responsible for formatting segments into packets
- Network access protocols describe two primary functions, communication over a data link and the physical transmission of data on the network media

3.2.2.1 Protocol Suites and Industry Standards

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			

- The protocols IP, HTTP, and DHCP are all part of the Internet protocol suite known as Transmission Control Protocol/IP (TCP/IP).
- The TCP/IP protocol suite 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.

3.2.2.2 Creation of the Internet and Development of TCP/IP

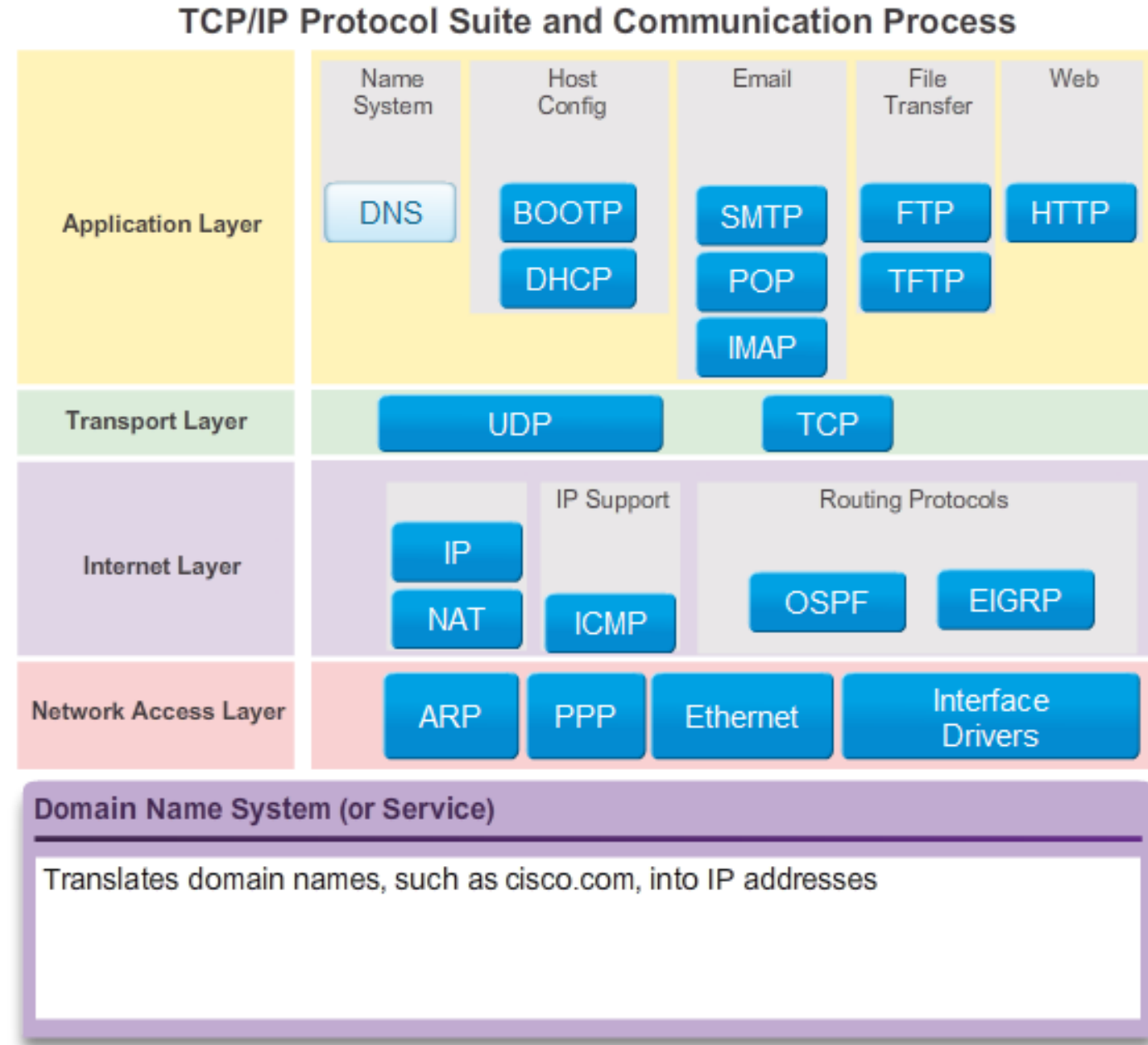


- The IP suite is a suite of protocols required for transmitting and receiving information using the Internet.
- It is commonly known as TCP/IP because the first two networking protocols defined for this standard were TCP and IP.
- The open standards-based TCP/IP has replaced other vendor proprietary protocol suites, such as Apple's AppleTalk and Novell's Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX).

3.2.2.3 TCP/IP Protocol Suite and Communication Process

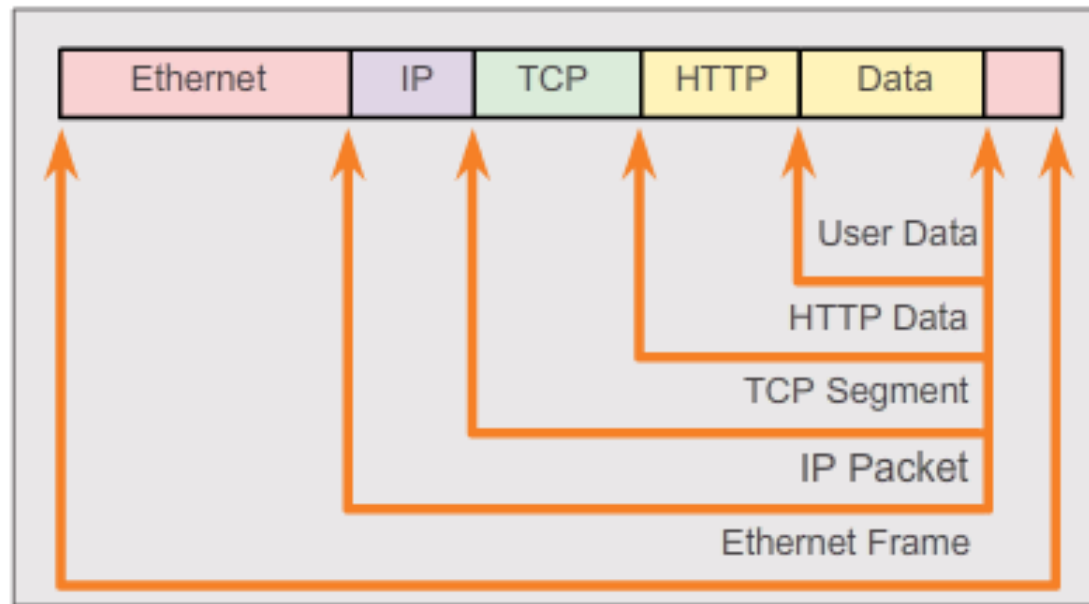
Four layers of the TCP/IP model

1. Application
2. Transport
3. Internet
4. Network Access

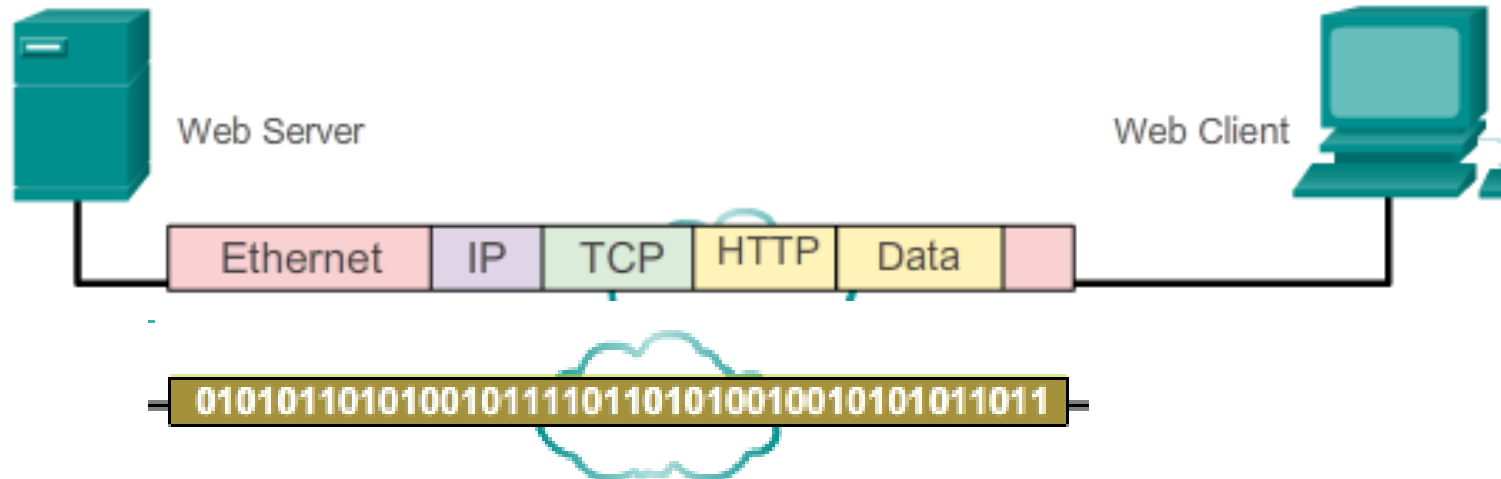


3.2.2.3 TCP/IP Protocol Suite and Communication Process

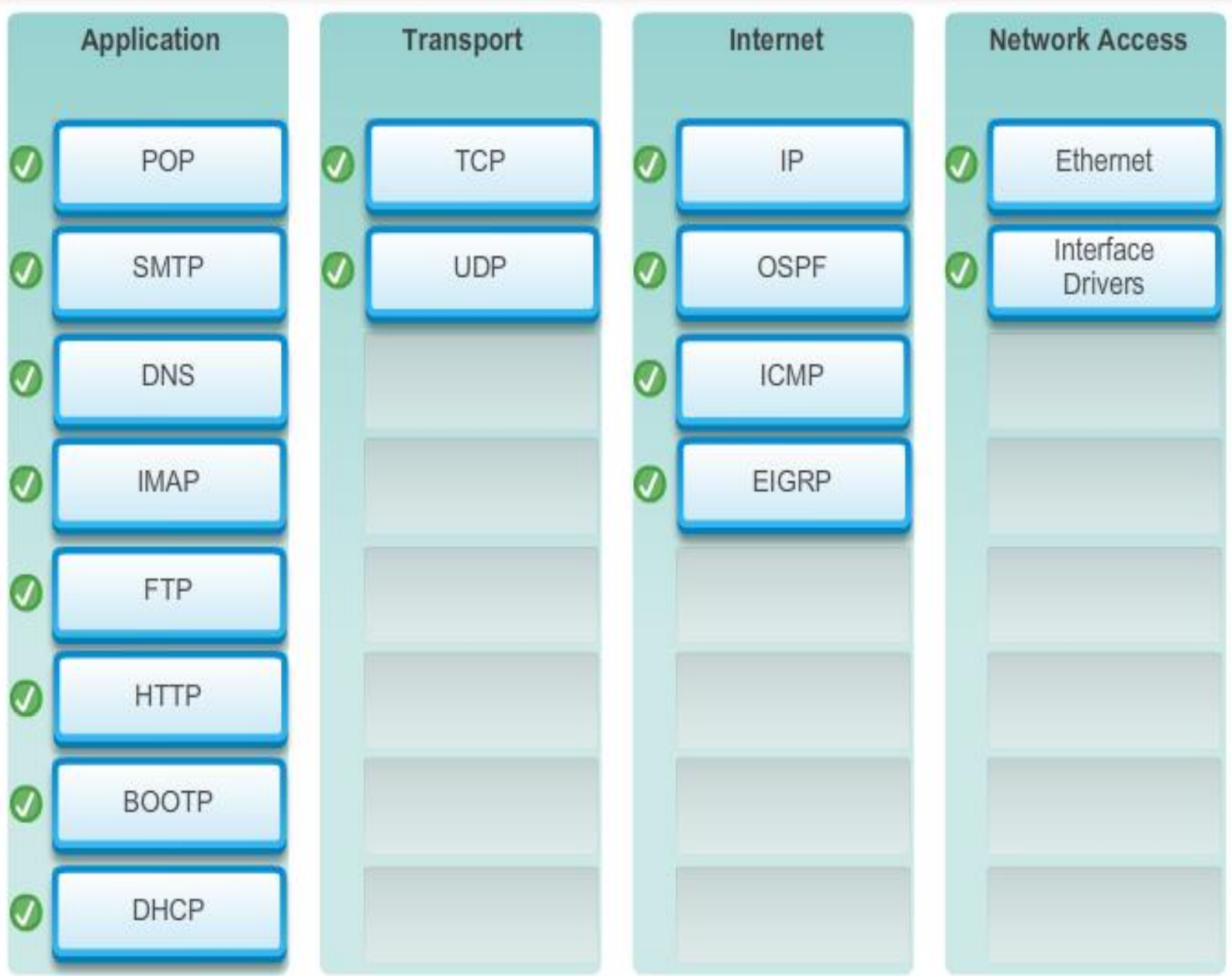
Protocol Encapsulation Terms



Protocol Operation of
Sending and Receiving
a Message



3.2.2.4 Activity – Mapping the Protocols of the TCP/IP Suite



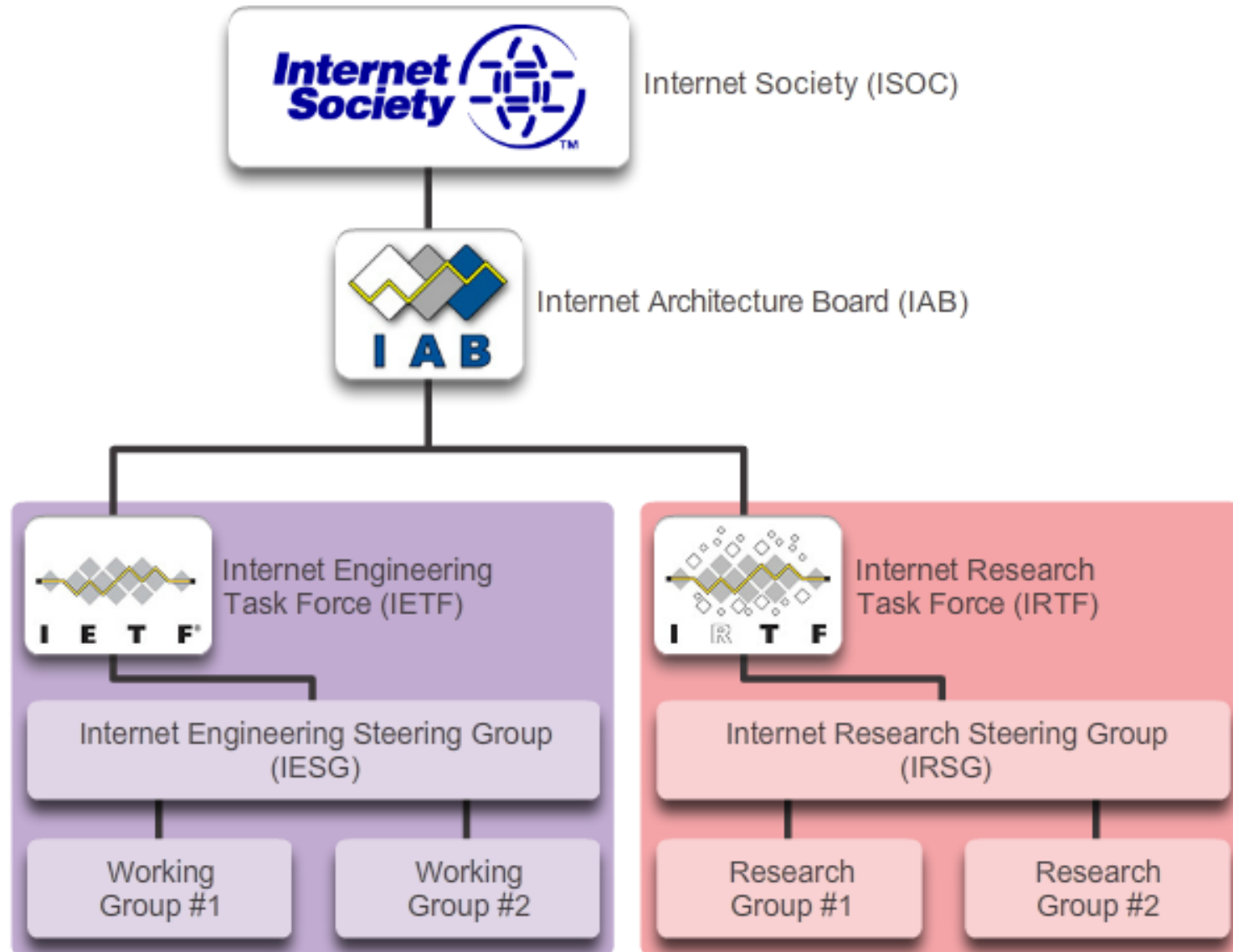
3.2.3.1 Open Standards



Standards organizations are important in maintaining an open Internet with freely accessible specifications and protocols that can be implemented by any vendor. A standards organization may draft a set of rules entirely on its own or in other cases may select a proprietary protocol as the basis for the standard. If a proprietary protocol is used, it usually involves the vendor who created the protocol.

3.2.3.2 ISOC, IAB, and IETF

ISOC, IAB, IETF, and IRTF



ISOC facilitates the open development of standards and protocols for the technical infrastructure of the Internet, including the oversight of the Internet Architecture Board (IAB).

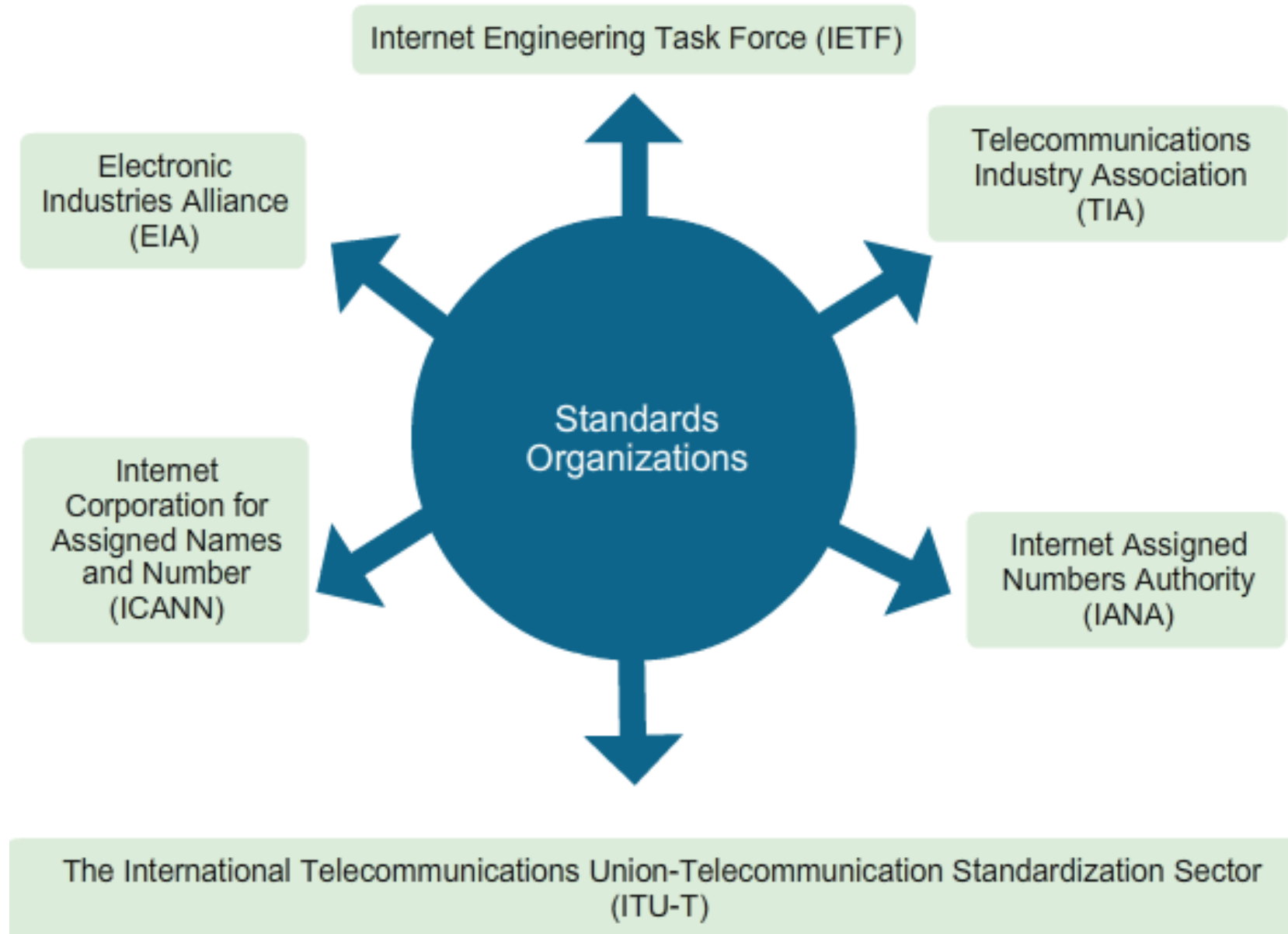
IEEE 802 Working Groups and Study Groups

- 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



- ISO, the International Organization for Standardization, is the world's largest developer of international standards for a wide variety of products and services.
- ISO is not an acronym for the organization's name; rather the ISO term is based on the Greek word "isos", meaning equal.
- The International Organization for Standardization chose the ISO term to affirm its position as being equal to all countries.

3.2.3.5 Other Standards Organizations



3.2.3.6 Lab - Researching Networking Standards



Researching Networking Standards



In this lab, you will complete the following objectives:

- Part 1: Research Networking Standards Organizations
- Part 2: Reflect on Internet and Computer Networking Experiences

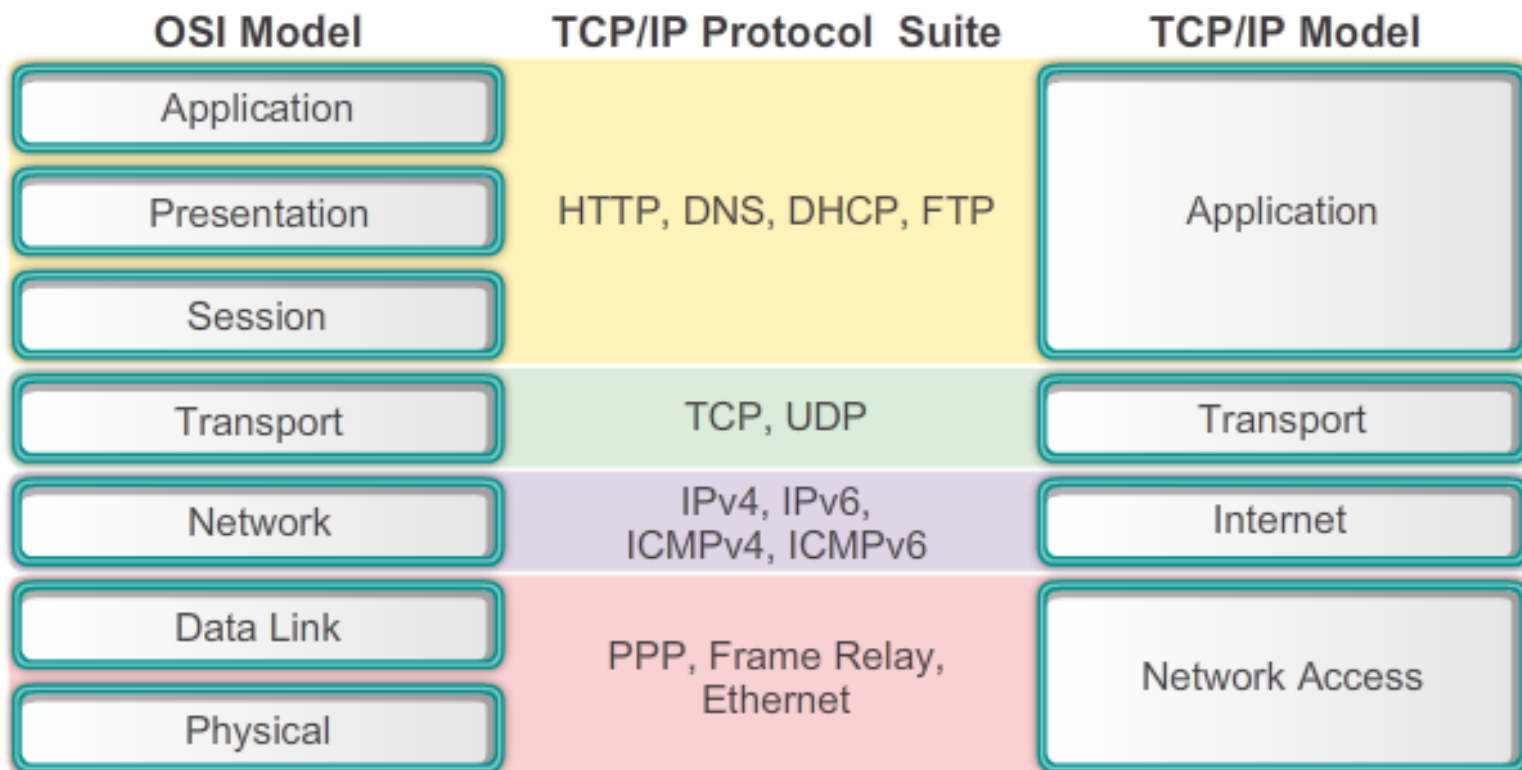
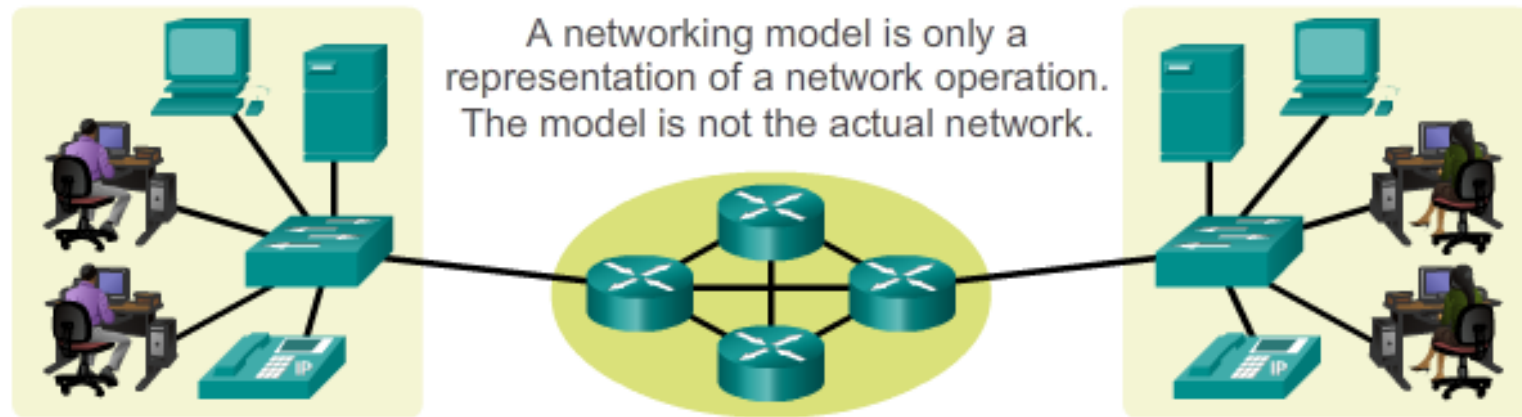
3.2.3.7 Activity - Standards Body Scavenger Hunt

	IANA	ICANN	IEEE	IETF	ITU	TIA
1. Manages the DNS Root Zone standards and the .int registry.	✓					
2. Creates standards for worldwide cabling infrastructure.						✓
3. Defines policies describing how "names and numbers" of the Internet operate.		✓				
4. Official standards products are RFC documents, published free of charge.				✓		
5. Standards are developed using a six stage lifecycle diagram.			✓			
6. Uses communications standards to predict famines and global climate changes.					✓	
7. Supports "bridge the digital divide" initiatives.					✓	
8. Creates standards for wired & wireless technologies.			✓			

	IANA	ICANN	IEEE	IETF	ITU	TIA
9. Serves as the central repository for protocol name and number registries.	✓					
10. Offers online tools and resources for standards and developers.			✓			
11. Provides wireless standards for IPTV.					✓	
12. Coordinates unique international Internet addresses for site names & IP addresses.		✓				
13. Standardizes the IP to Applications protocol layers.				✓		
14. Supports navigation and online maps via radio/satellite transmissions.					✓	
15. Provides a space where Internet protocols are set and maintained.				✓		
16. Manages the DNS, IP addresses, and protocol identifier assignments.		✓				

17. "Makes the Internet work better," using an engineering approach.				✓		
18. Develops standards/protocols affecting cloud computing.						✓
19. Develops standards for homeland security/emergency response teams.						✓

3.2.4.1 The Benefits of Using a Layered Model



- Assists in protocol design
- Fosters competition because products from different vendors can work together.
- Prevents technology or capability changes in one layer from affecting other layers above and below.
- Provides a common language to describe networking functions and capabilities.

3.2.4.2 The OSI Reference Model

Application

The application layer provides the means for end-to-end connectivity between individuals in the human network using data networks.

Presentation

The presentation layer provides for common representation of the data transferred between application layer services.

Session

The session layer provides services to the presentation layer to organize its dialogue and to manage data exchange.

Transport

The transport layer defines services to segment, transfer, and reassemble the data for individual communications between the end devices.

Network

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

Data Link

The data link layer protocols describe methods for exchanging data frames between devices over a common media.

Physical

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.

3.2.4.3 The TCP/IP Protocol Model

TCP/IP Model

Application

Represents data to the user, plus encoding and dialog control.

Transport

Supports communication between diverse devices across diverse networks.

Internet

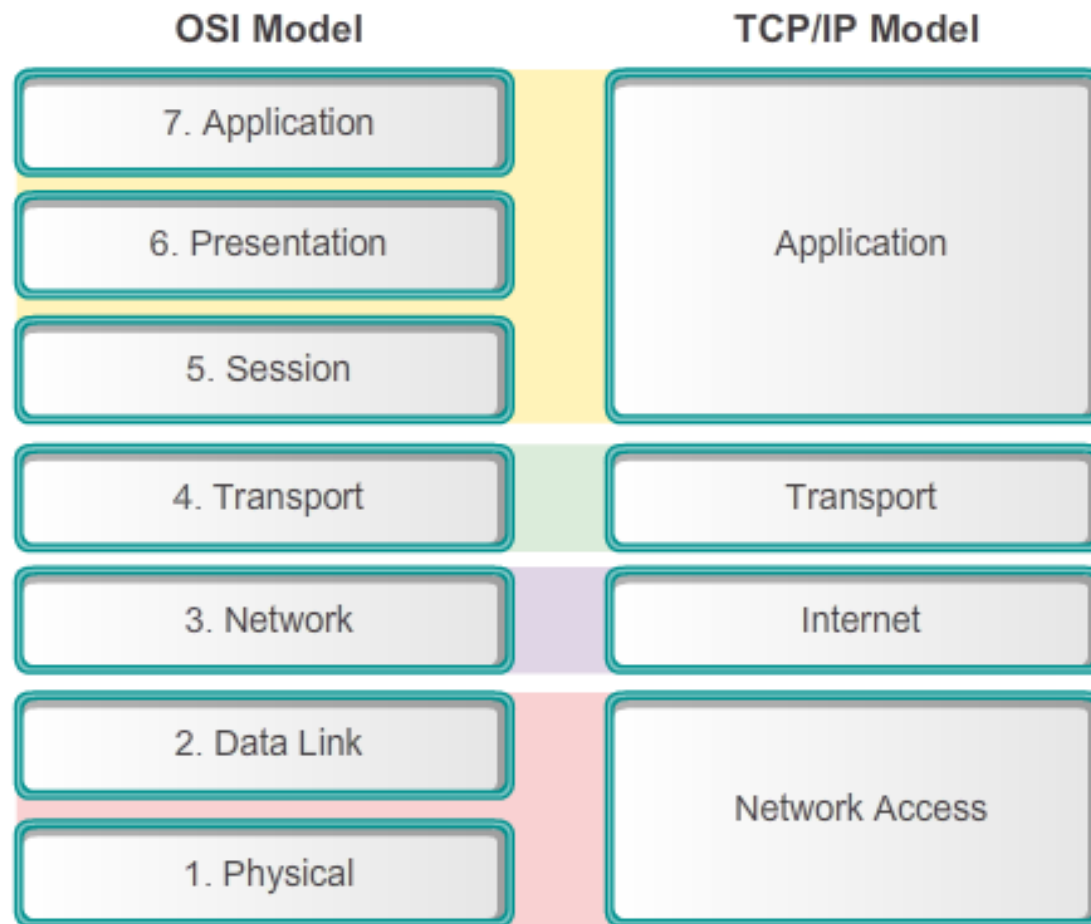
Determines the best path through the network.

Network Access

Controls the hardware devices and media that make up the network.

3.2.4.4 Comparing the OSI Model with the TCP/IP Model

Comparing the OSI Model and the TCP/IP Model



The key similarities are in the transport and network layers; however, the two models differ in how they relate to the layers above and below each layer.

3.2.4.5 Activity – Identify Layers and Functions

Activity – Part 1: OSI Layer Functions

Drag the OSI layer to its functional description.

Layers	OSI Layer Functional Descriptions
7 Application	<div></div> Manages data exchange
6 Presentation	<div></div> Exchanges frames between devices
5 Session	<div></div> Data representation
4 Transport	<div></div> Provides a data path or route
3 Network	<div></div> Bit transmission
2 Data Link	
1 Physical	

3.2.4.6 Packet Tracer - Investigating the TCP/IP and OSI Models in Action



Investigating the TCP/IP and OSI Models in Action



This simulation activity is intended to provide a foundation for understanding the TCP/IP protocol suite and the relationship to the OSI model. Simulation mode allows you to view the data contents being sent across the network at each layer.

3.2.4.7 Lab - Researching RFCs

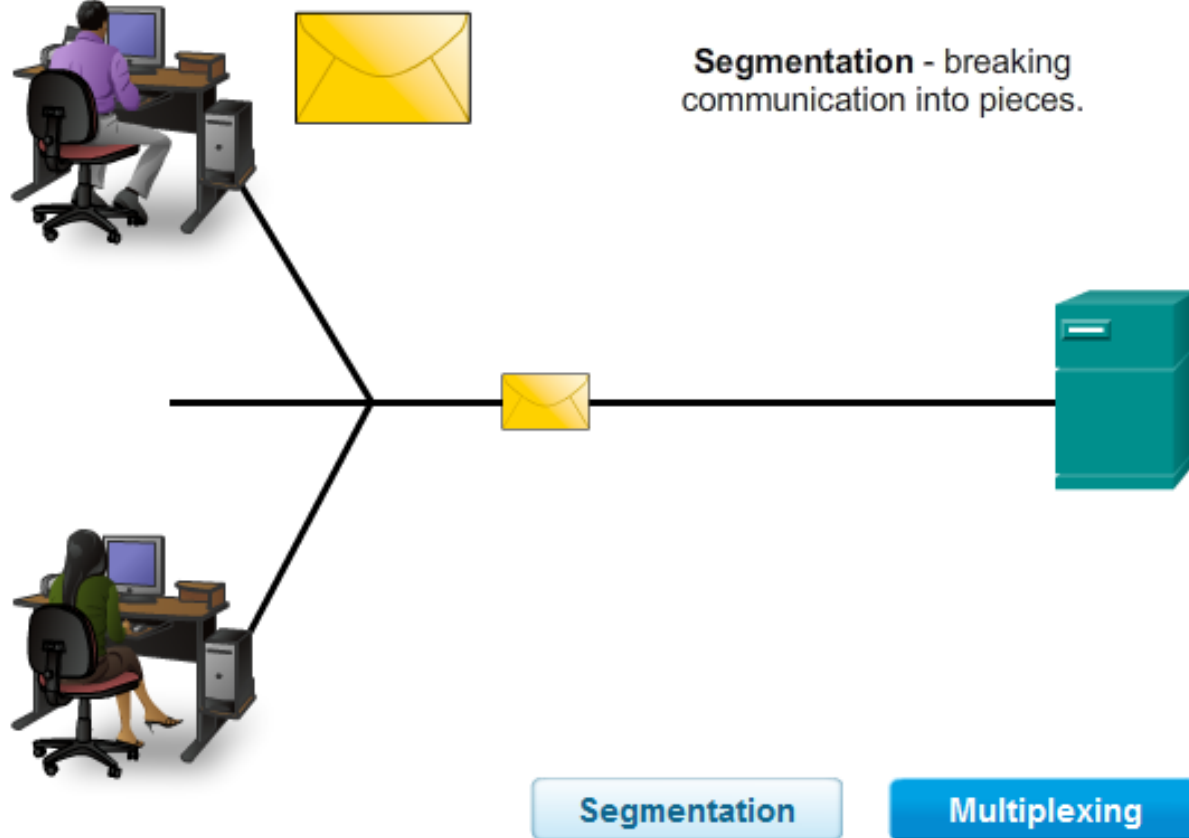


Researching RFCs

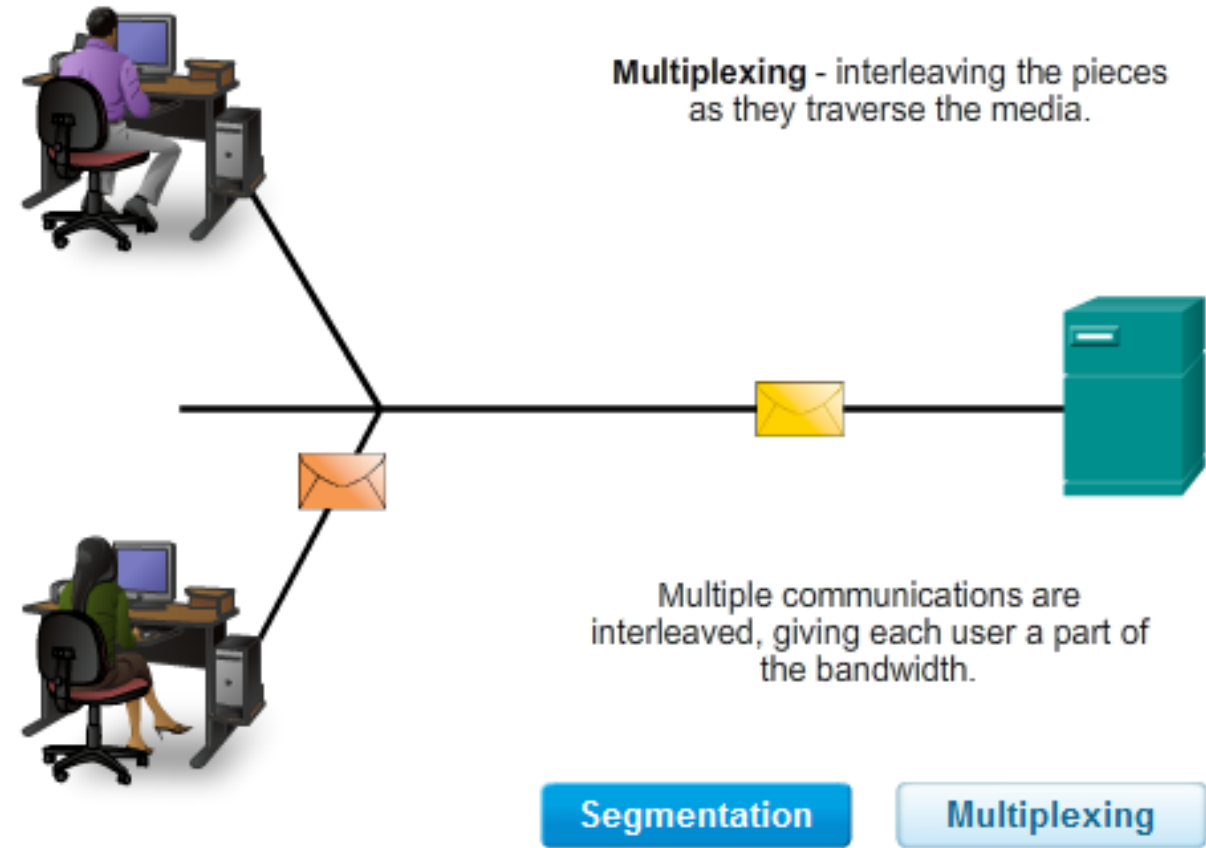


3.3.1.1 Communicating the Messages

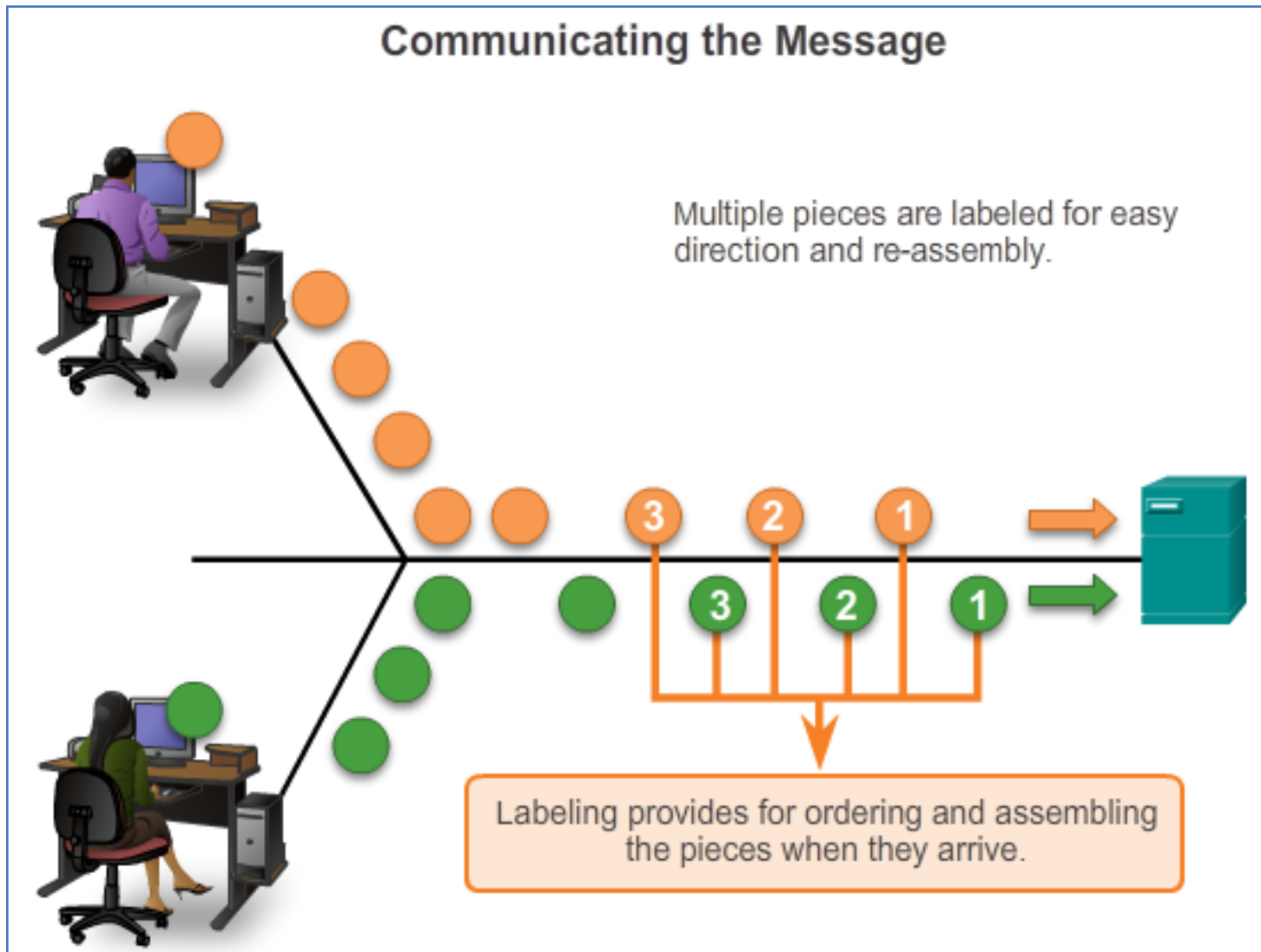
Communicating the Message



Communicating the Message



3.3.1.1 Communicating the Messages

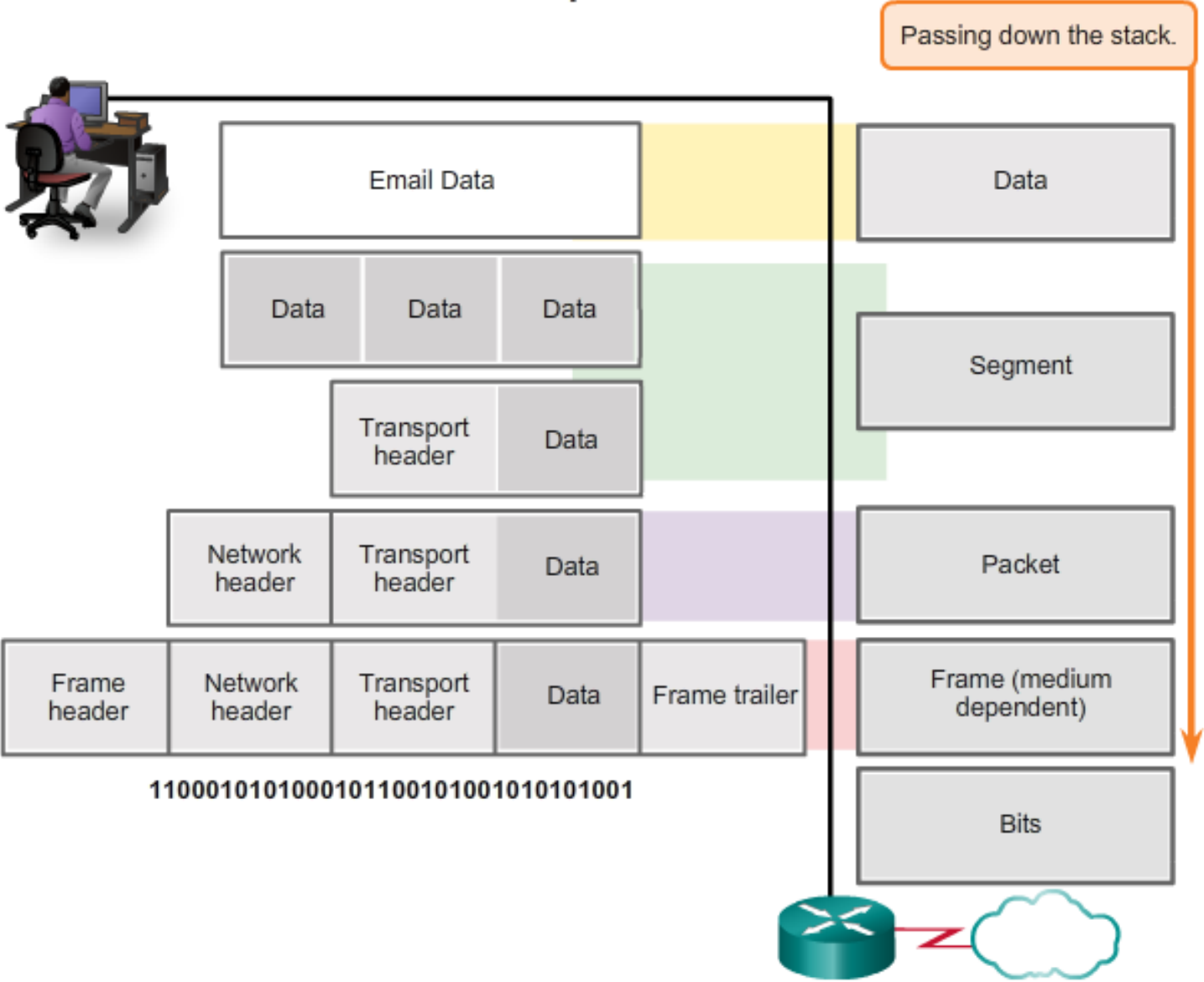


The division of the data stream into smaller pieces is called segmentation. Two primary benefits:

- By sending smaller individual pieces from source to destination, many different conversations can be interleaved on the network.
- Segmentation can increase the reliability of network communications. The separate pieces of each message need not travel the same pathway across the network from source to destination.

3.3.1.2 Protocol Data Units (PDUs)

Encapsulation



Down

Santa

Pushed

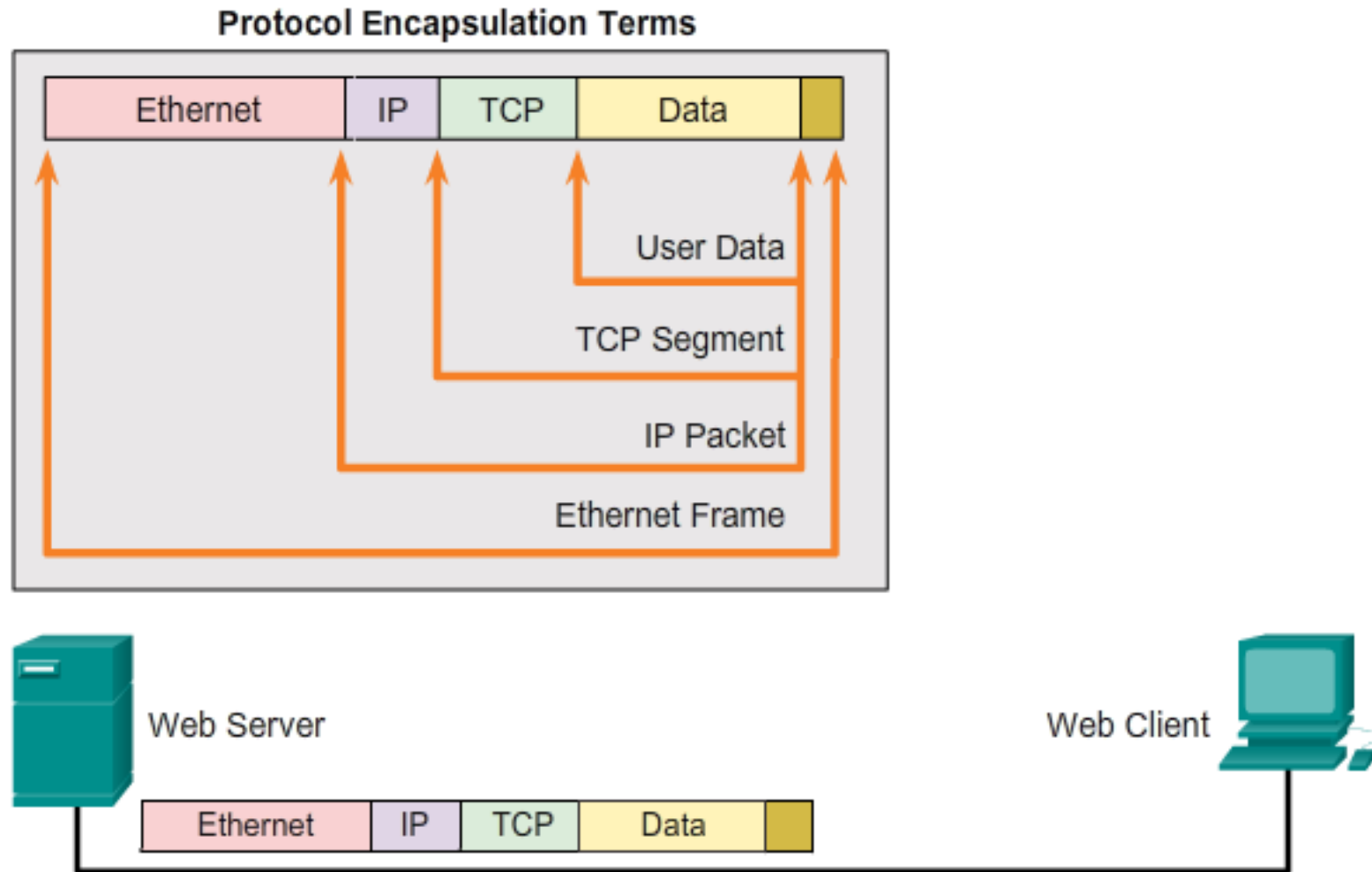
Frank

Big



3.3.1.3 Encapsulation

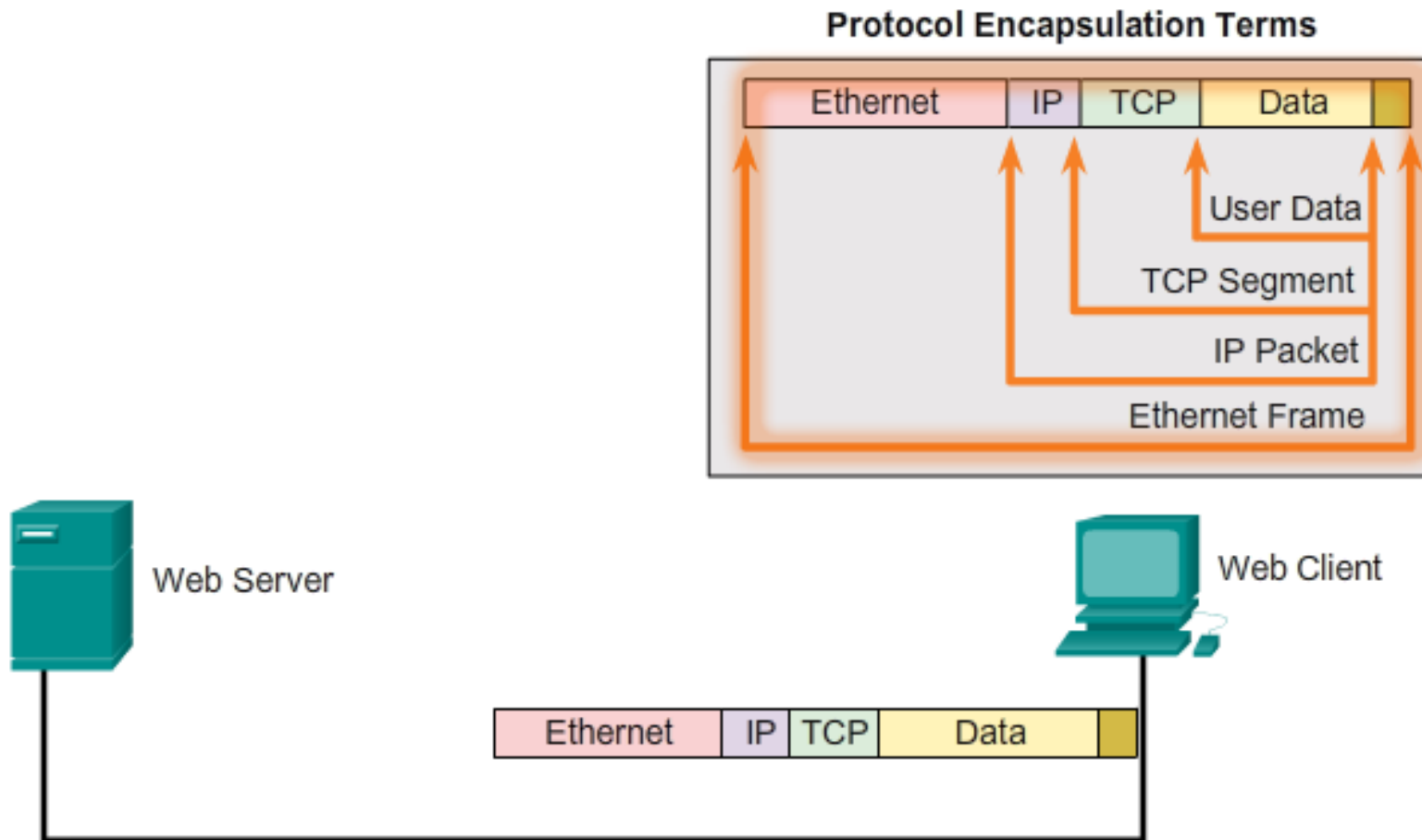
Protocol Operation of Sending a Message



Data encapsulation is the process that adds additional protocol header information to the data before transmission. In most forms of data communications, the original data is encapsulated or wrapped in several protocols before being transmitted.

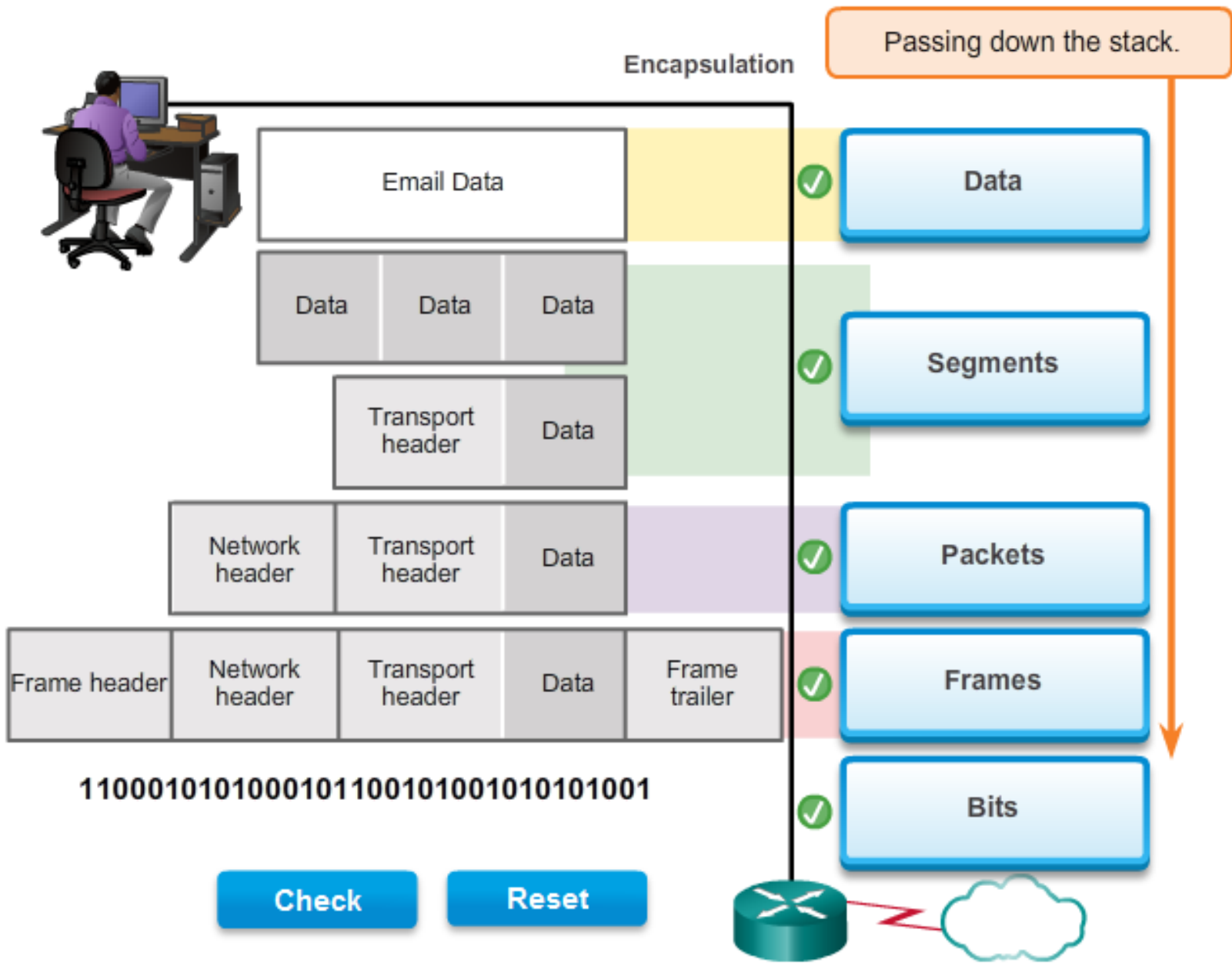
3.3.1.4 De-encapsulation

Protocol Operation of Receiving a Message

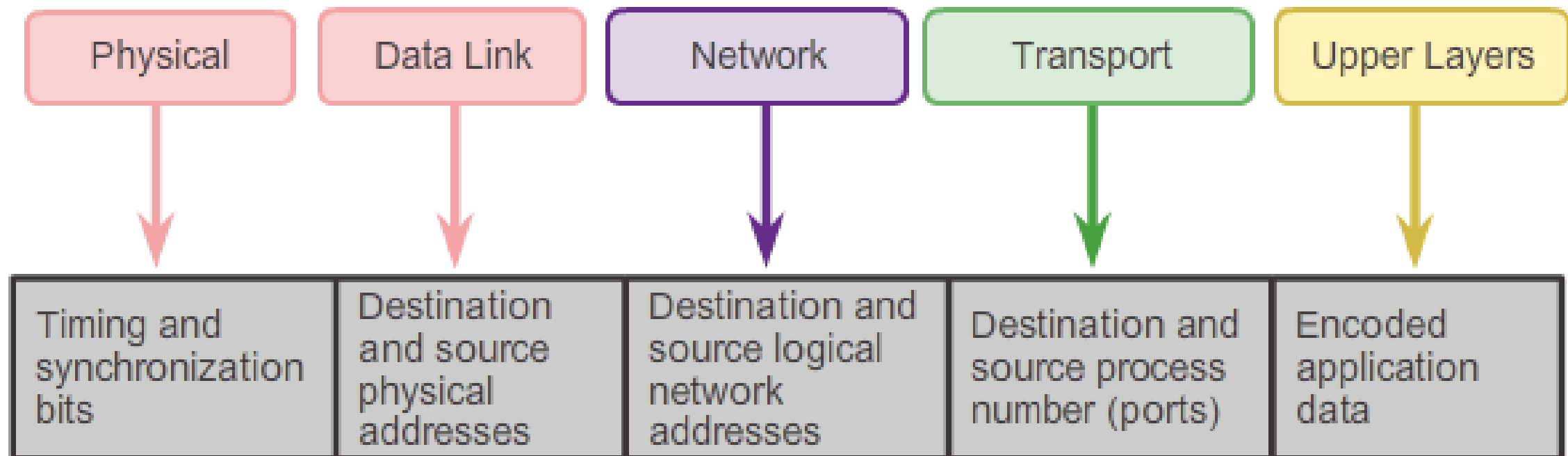


De-encapsulation is the process used by a receiving device to remove one or more of the protocol headers. The data is de-encapsulated as it moves up the stack toward the end-user application. Click the Play button in the figure to see the de-encapsulation process.

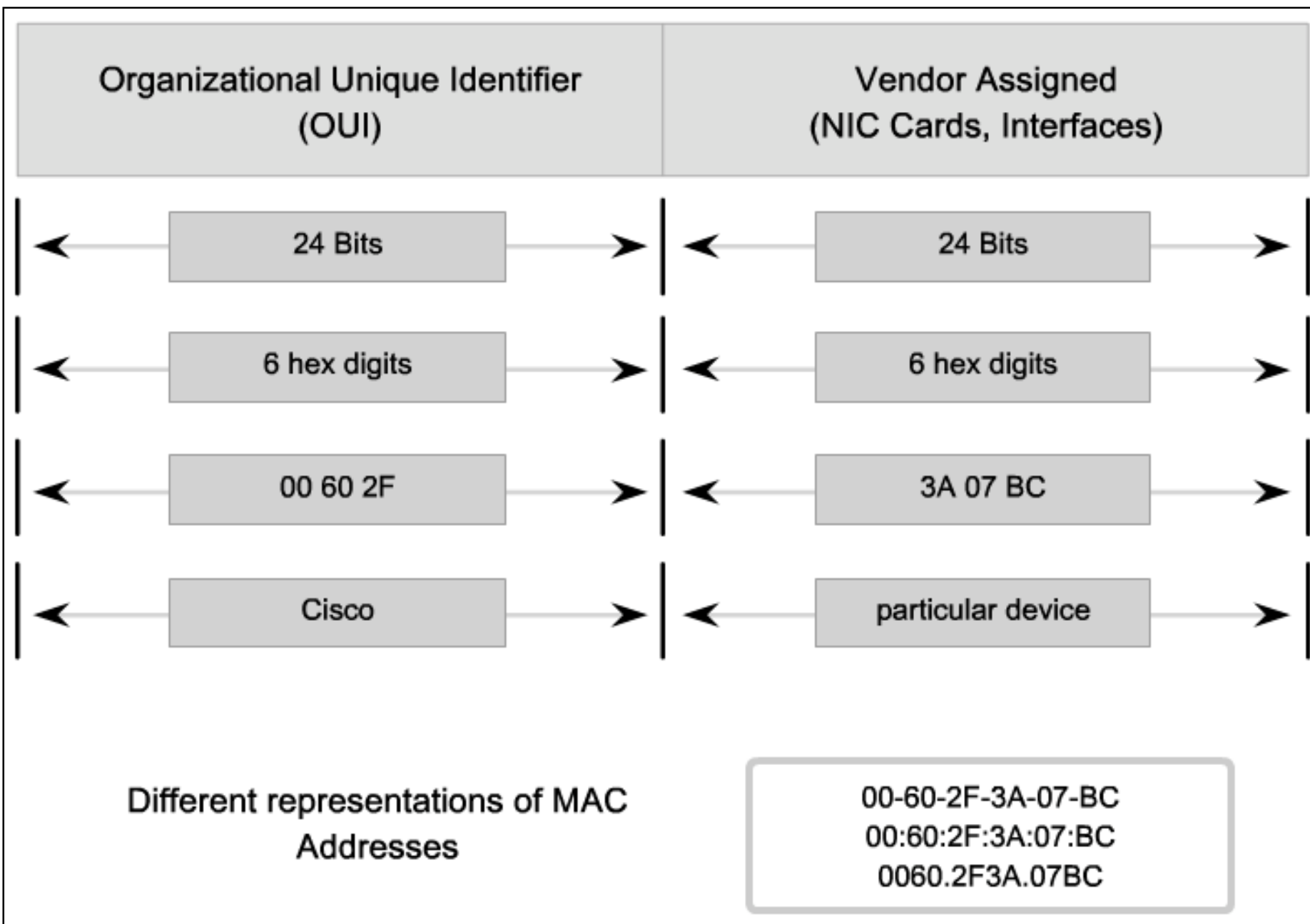
3.3.1.5 Activity – Identify the PDU Layer



Network Addresses and Data Link Addresses

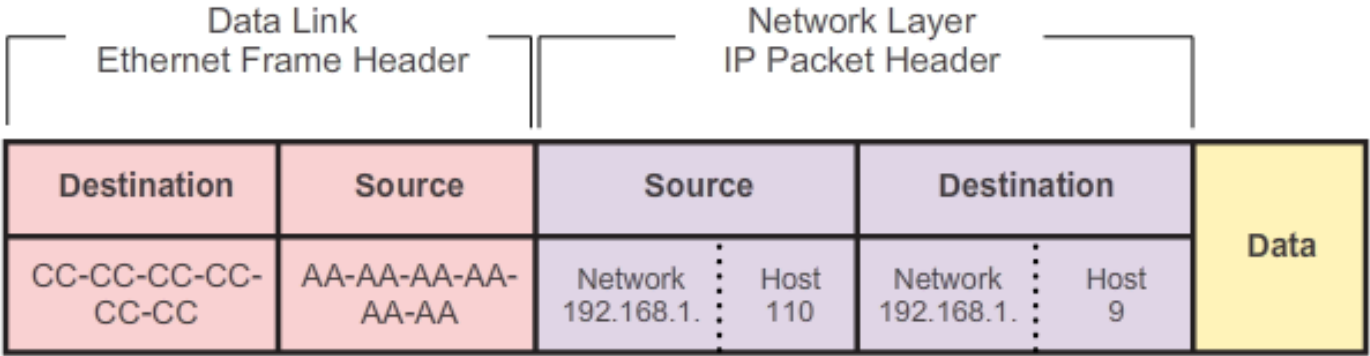


THE MAC ADDRESS

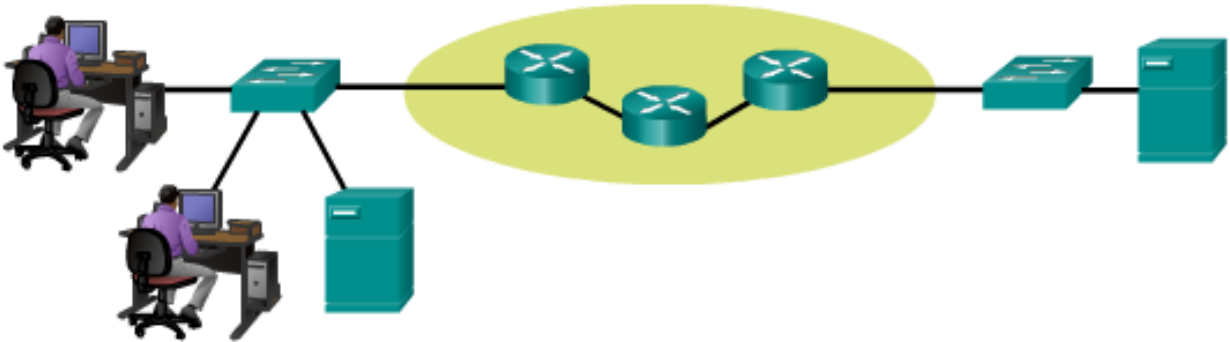


3.3.2.2 Communicating with a Device on the Same Network

Communicating with a Device on the Same Network



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



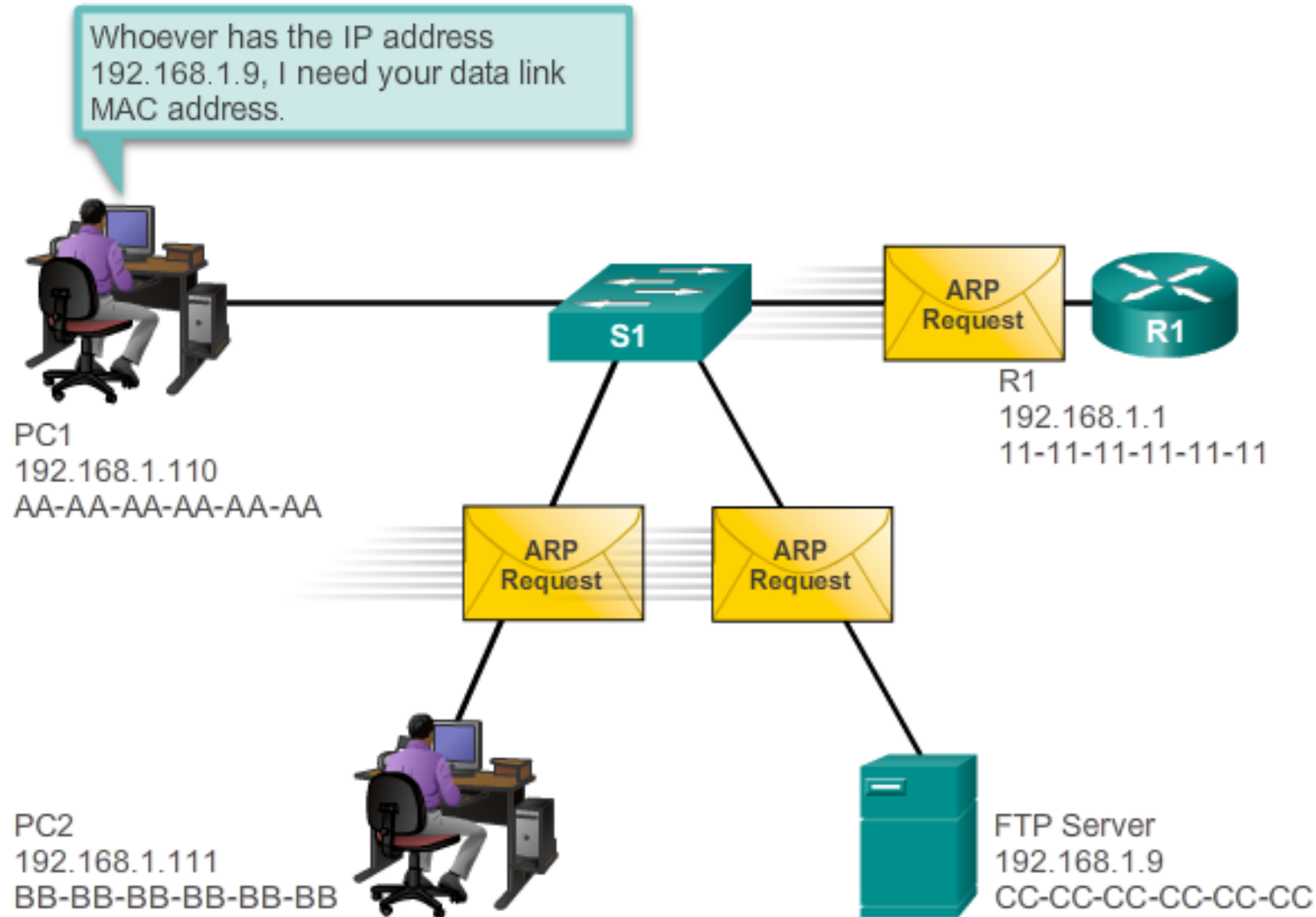
FTP Server
192.168.1.9
CC-CC-CC-CC-CC-CC

The network layer addresses, or IP addresses, indicate the network and host address of the source and destination. The network portion of the address will be the same; only the host or device portion of the address will be different.

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. On an Ethernet network, the data link addresses are known as Ethernet MAC addresses.

3.3.2.3 MAC and IP Addresses

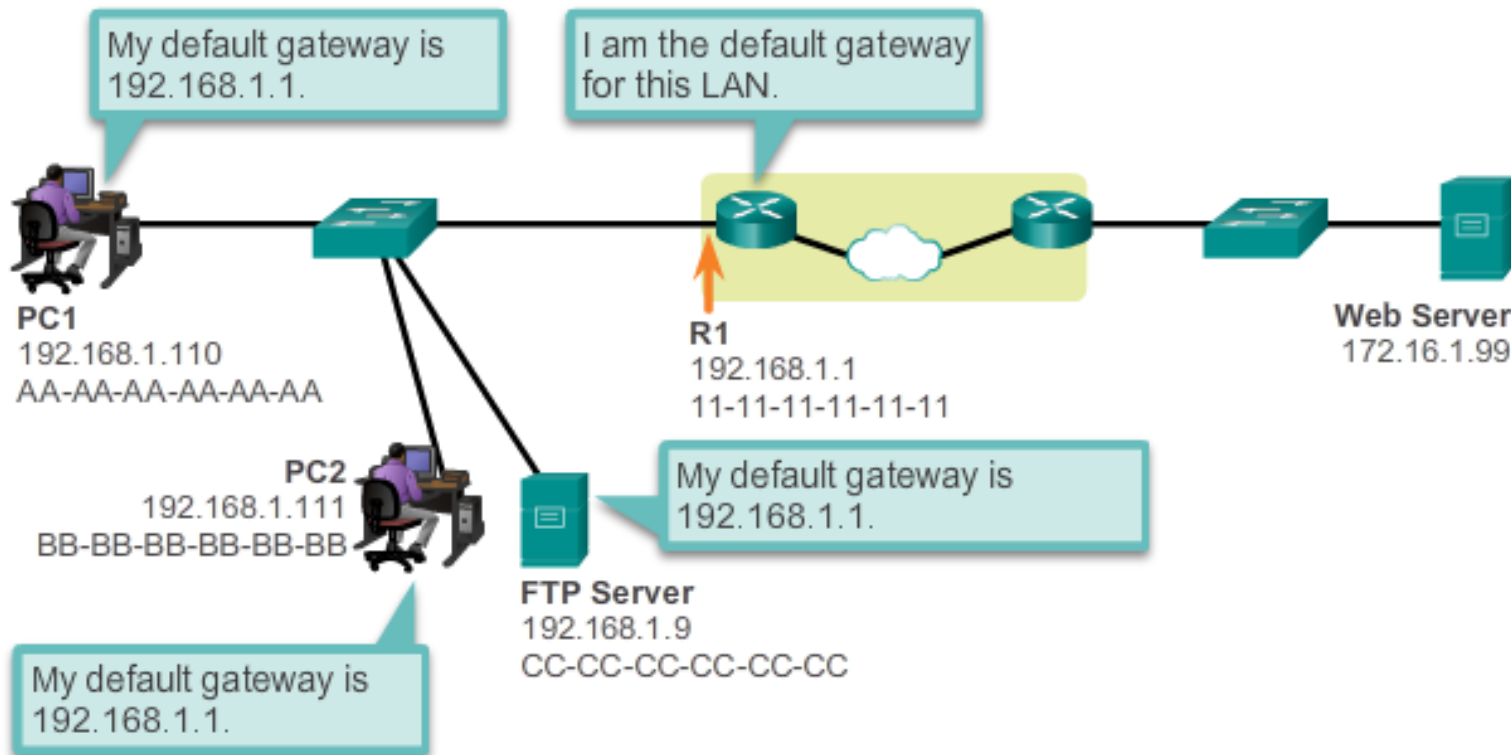
Address Resolution Protocol



3.3.3.1 Default Gateway

Getting the Pieces to the Correct Network

Protocol Data Unit (PDU)				
Source		Destination		Data
Network 192.168.1	Device 110	Network 172.16.1	Device 99	

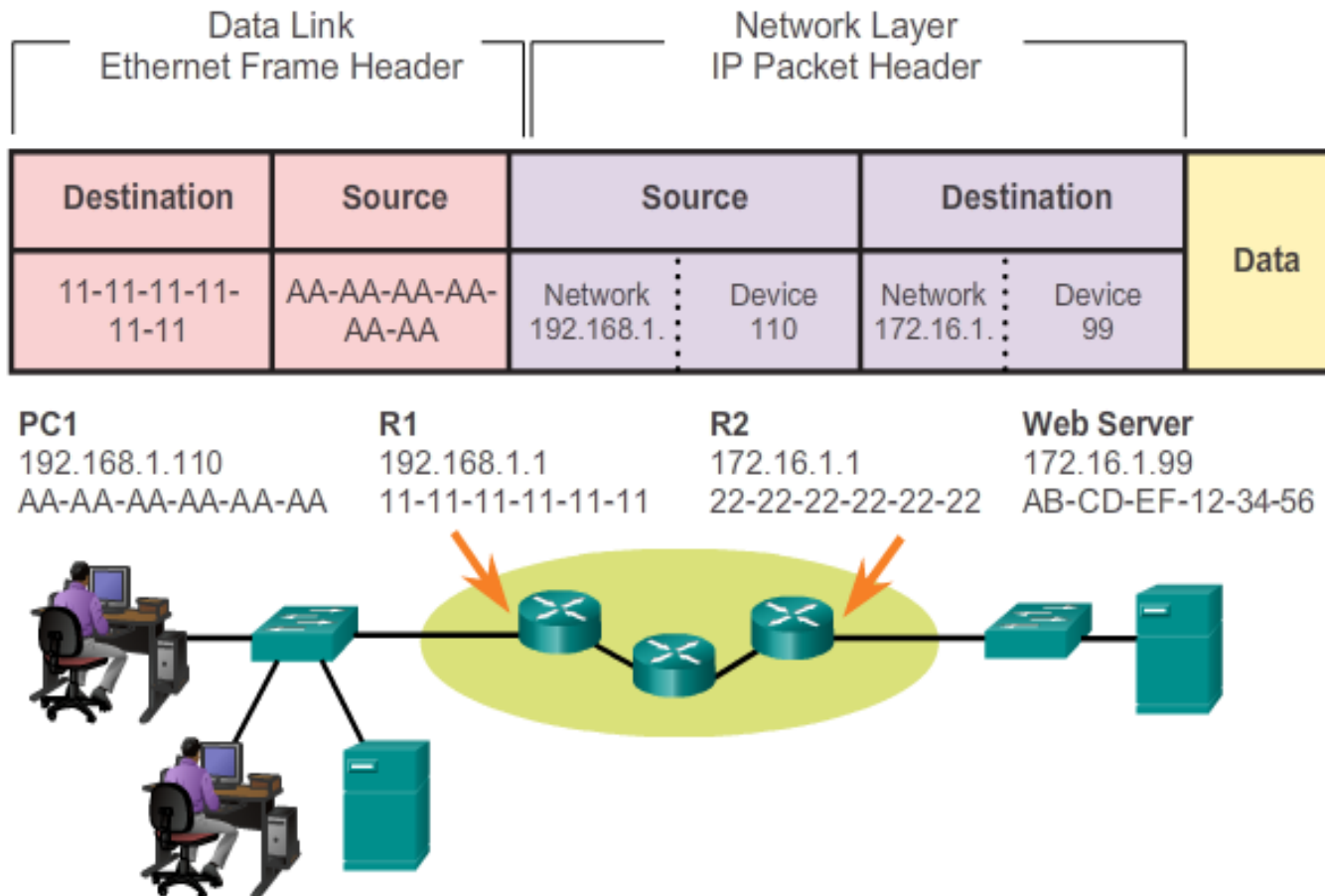


When a host needs to send a message to a remote network, it must use the router, also known as the default gateway. The default gateway is the IP address of an interface on a router on the same network as the sending host.

If no default gateway address is configured in the host TCP/IP settings, or if the wrong default gateway is specified, messages addressed to hosts on remote networks cannot be delivered.

3.3.3.2 Communicating with a Device on a Remote Network

Communicating with a Device on a Remote Network



- Each device knows the IP address of the router through the default gateway address configured in its TCP/IP settings.
- The default gateway address is the address of the router interface connected to the same local
- After the host knows the default gateway IP address, it can use ARP to determine the MAC address of that default gateway.
- The MAC address of the default gateway is then placed in the frame.

3.3.3.3 Packet Tracer - Explore a Network



Explore a Network



This simulation activity is intended to help you understand the flow of traffic and the contents of data packets as they traverse a complex network. Communications will be examined at three different locations simulating typical business and home networks.

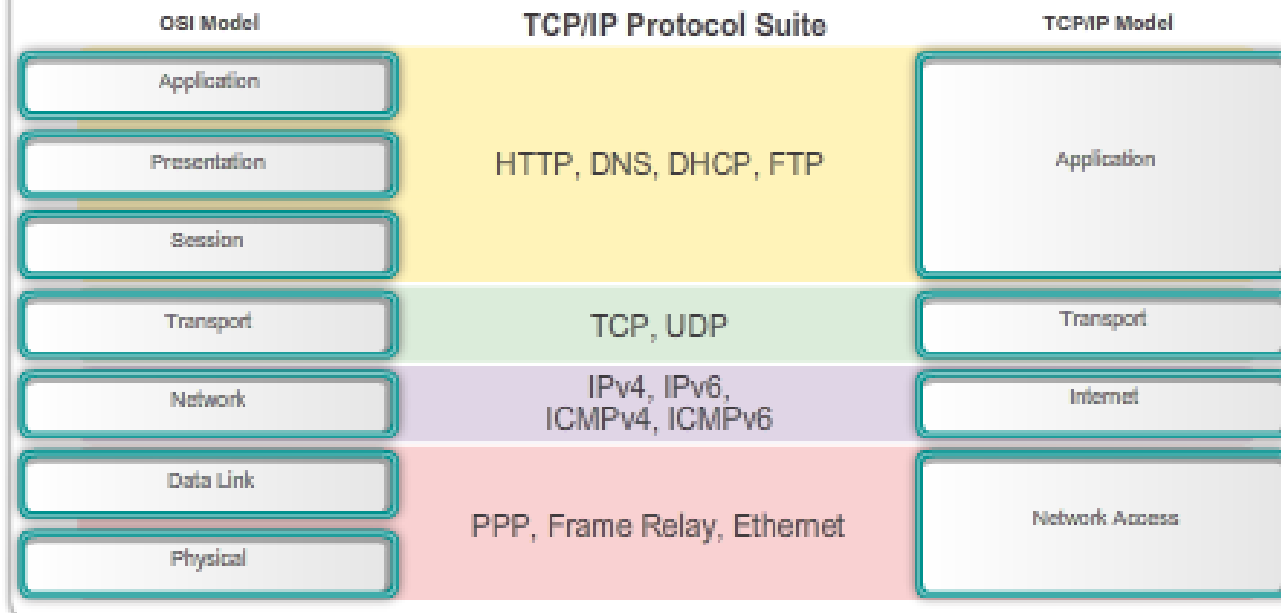
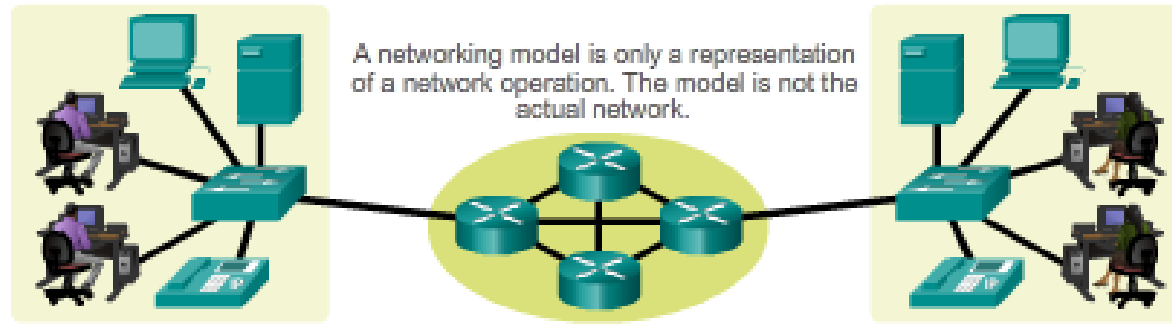
3.3.3.4 Lab - Using Wireshark to View Network Traffic



Using Wireshark to View Network Traffic



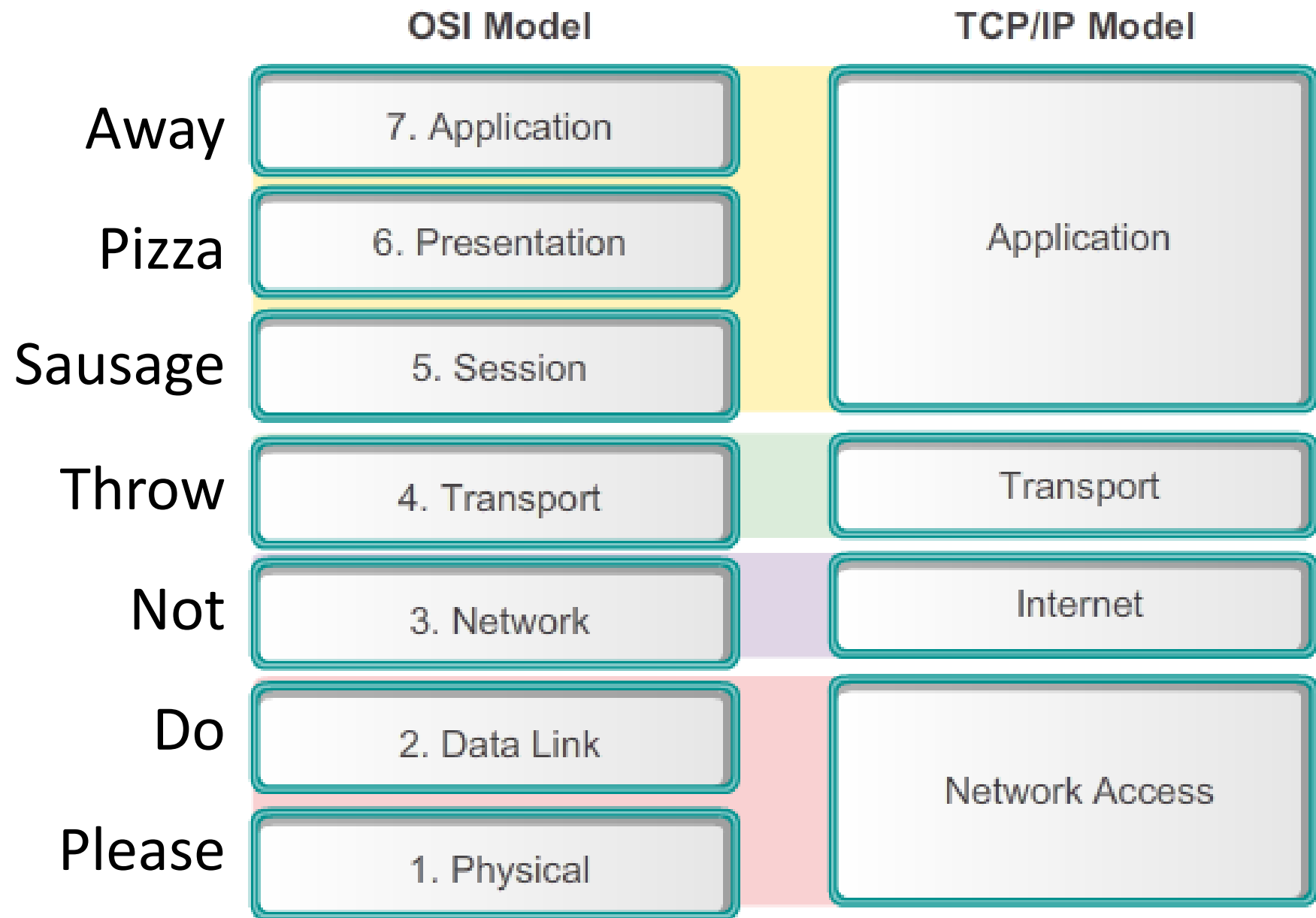
3.4.1.1 Class Activity - Guaranteed to Work!



Assuming you resolved the beginning of this chapter's modeling activity, how would you compare the following steps taken to design a communications system to the networking models used for communications?

Using network protocols and standards facilitates quality data delivery in a timely manner.

3.4.1.2 Summary



Thanks
for your
attention!

