



# Chapter 3: Network Protocols and Communication

CCNA Routing and Switching

Introduction to Networks v6.0



# Chapter 3 - Sections & Objectives

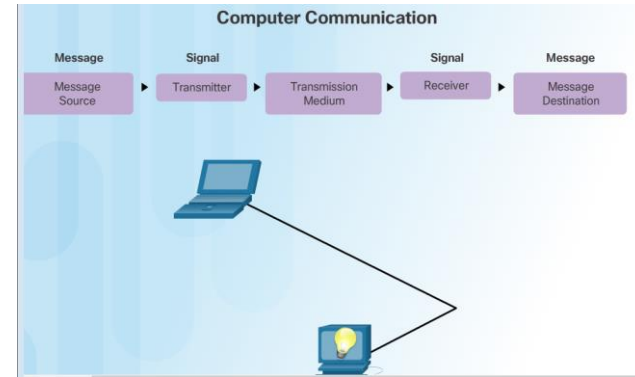
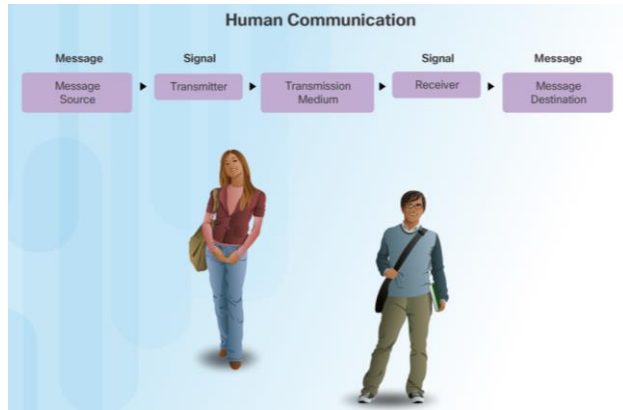
- 3.1 Rules of Communication
  - Explain how rules facilitate communication.
  - Describe the types of rules that are necessary to successfully communicate.
- 3.2 Network Protocols and Standards
  - Explain the role of protocols and standards organizations in facilitating interoperability in network communications.
  - Explain why protocols are necessary in network 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 devices on a LAN access resources in a small to medium-sized business 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

# The Rules

## Communication Fundamentals

- All communication methods have three elements in common:
  - Source or sender
  - Destination or receiver
  - Channel or media
- Rules or protocols govern all methods of communication.



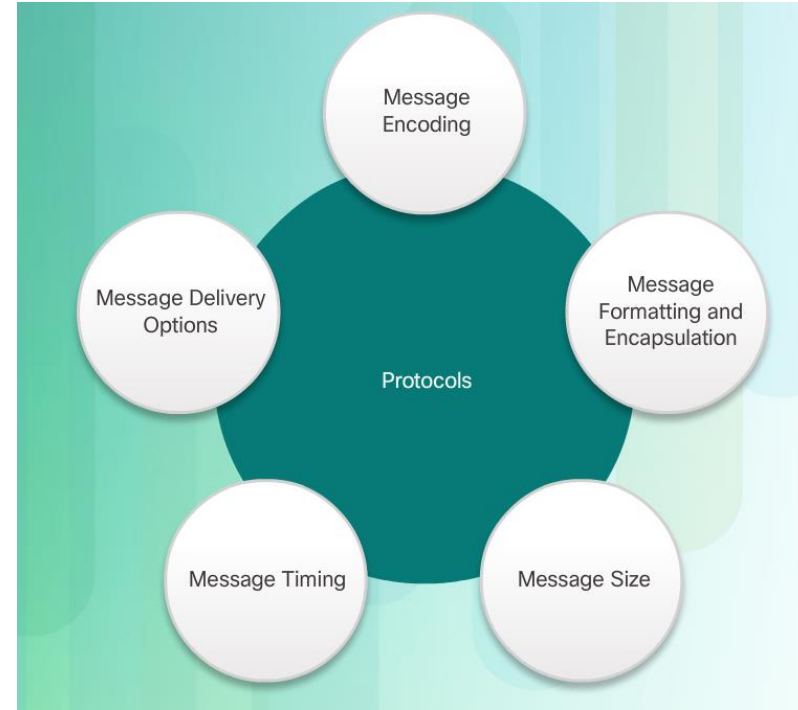
# Rule Establishment

- **Protocols** are necessary for effective communication and include:

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

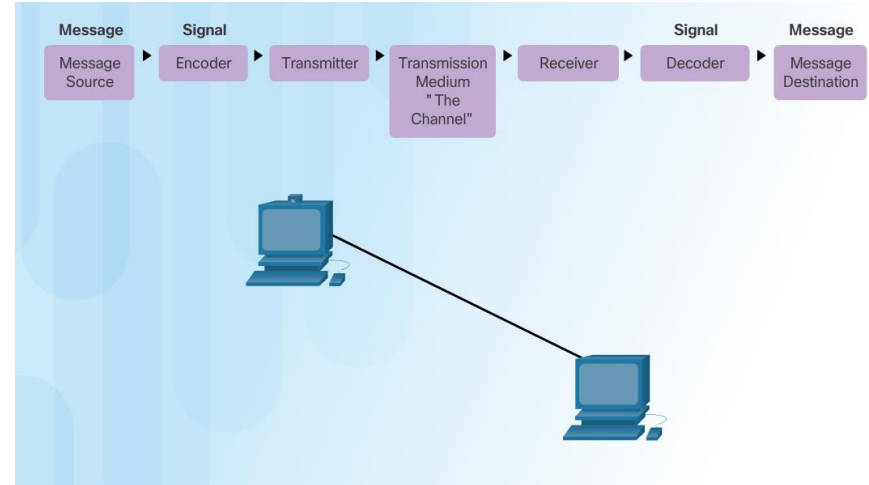
- **Protocols** used in network communications also define:

- Message **encoding**
- Message **delivery options**
- Message **Formatting** and **Encapsulation**
- Message **Timing**
- Message **Size**



# Message Encoding

- Encoding between hosts must be in **appropriate format** for the medium.
- Messages 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
- The destination host **receives** and **decodes** the signals in order to interpret the message.



# Message Formatting and Encapsulation

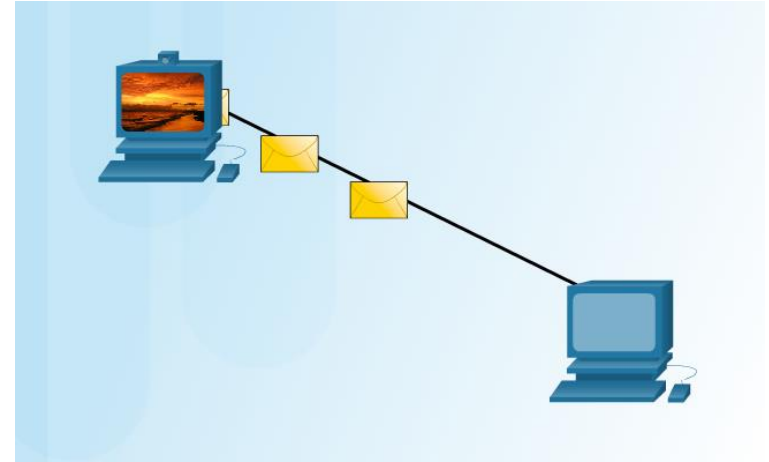
- There is an agreed format for letters and addressing letters which is required for proper delivery.
- Putting the letter into the addressed envelope is called **encapsulation**.
- Each computer message is encapsulated in a specific format, called a **frame**, before it is sent over the network.
- A frame acts like an envelope providing destination address and source address.



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				

# Message Size

- Humans break long messages into smaller parts or sentences.
- Long messages must also be broken into smaller pieces to travel across a network.
  - **Each piece is sent in a separate frame.**
  - Each frame has its own addressing information.
  - A receiving host will reconstruct multiple frames into the original message.





# Message Timing

### ▪ Access Method

- Hosts on a network need to know **when to begin sending** messages and how to respond when collisions occur.

### ▪ Flow Control

- Source and destination hosts use flow control to **negotiate correct timing** to avoid overwhelming the destination and ensure information is received.

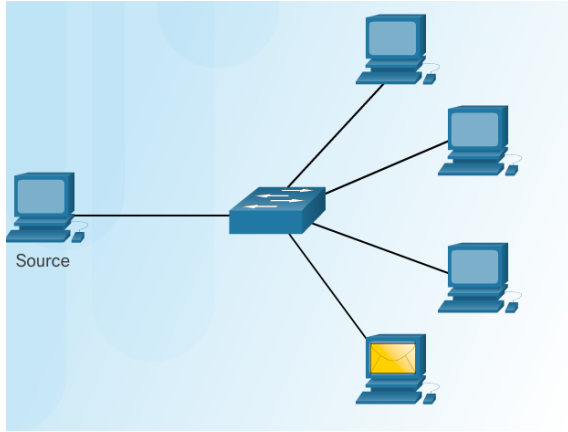
### ▪ Response Timeout

- Hosts on the network have rules that specify **how long to wait for responses** and what action to take if a response timeout occurs.

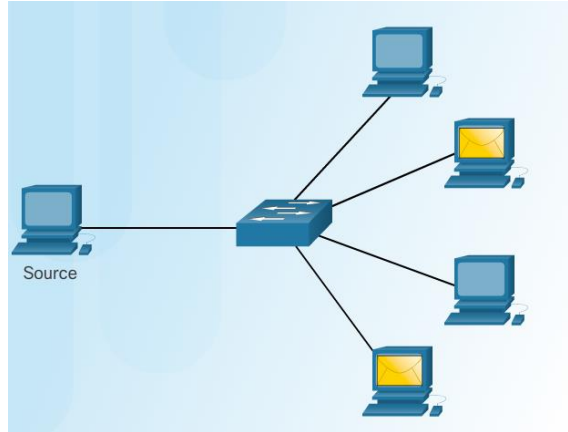


# Message Delivery Options

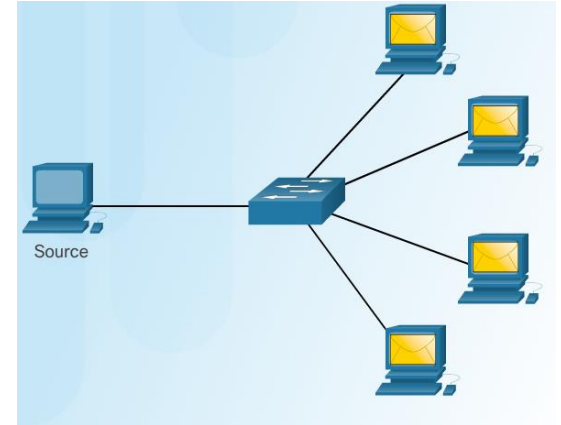
## Unicast Message



## Multicast Message



## Broadcast Message



One-to-one delivery

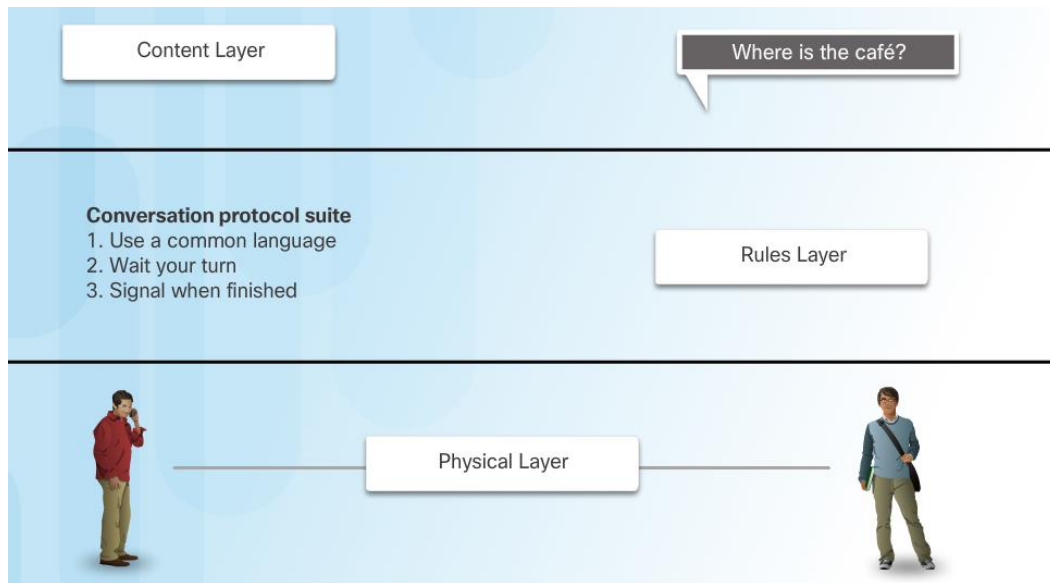
One-to-many delivery

One-to-all delivery

## 3.2 Network Protocols and Standards

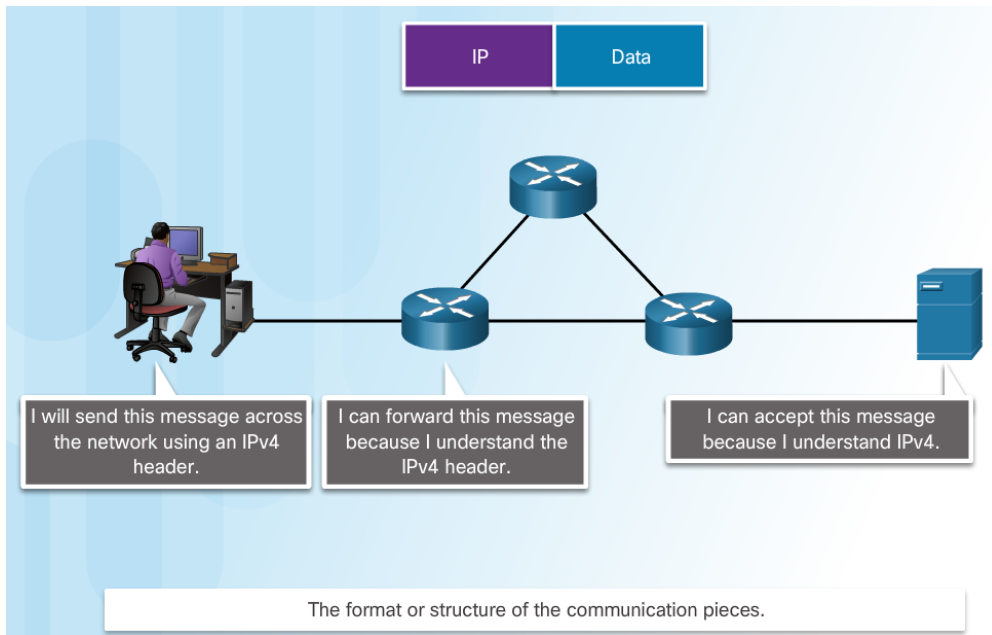
# Rules that Govern Communications

- **Protocol** suites are **implemented** by hosts and networking devices in **software, hardware** or **both**.
- 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.



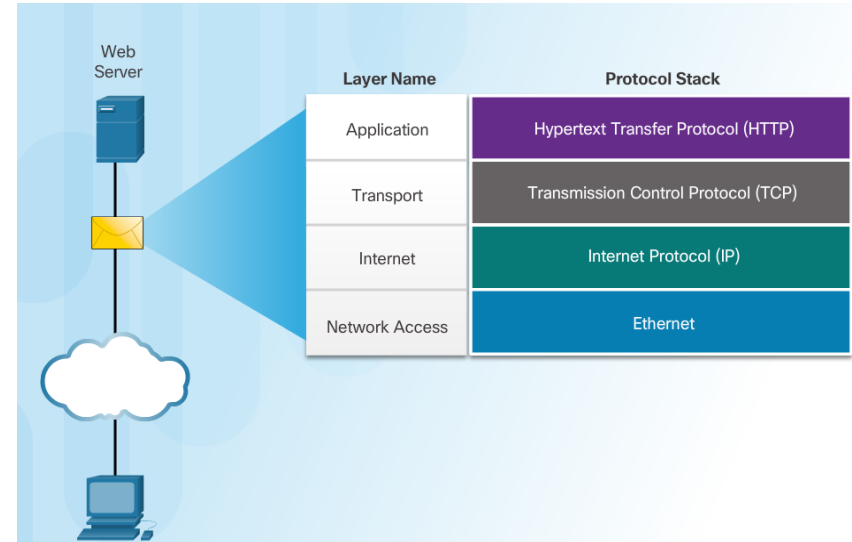
# Network Protocols

- 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).



# Protocol Interaction

- Communication between a web server and web client is an example of an interaction between several protocols:
  - **HTTP** - an application protocol that governs the way a web server and a web client interact.
  - **TCP** - transport protocol that manages the individual conversations.
  - **IP** – encapsulates the TCP segments into packets, assigns addresses, and delivers to the destination host.
  - **Ethernet** - allows communication over a data link and the physical transmission of data on the network media.



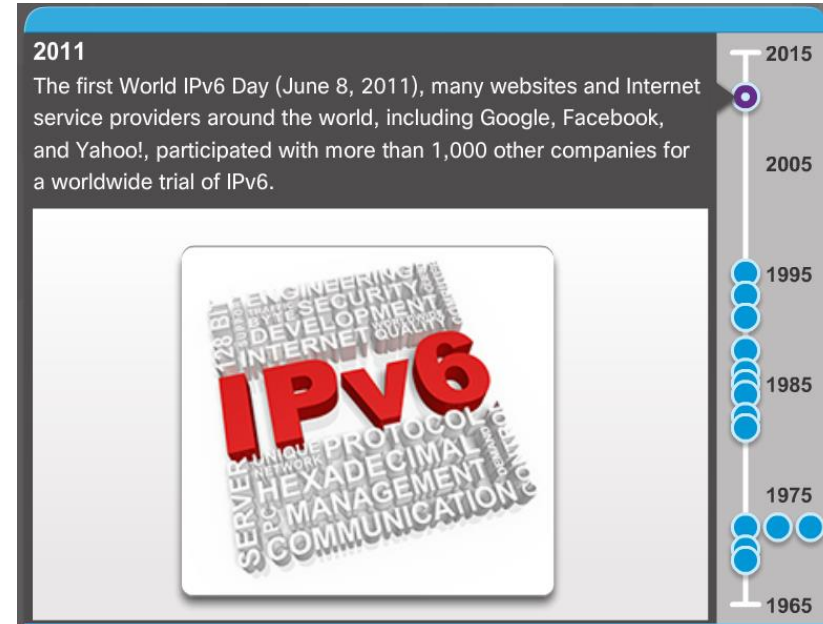
## Protocol Suites and Industry Standards

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

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

# Development of TCP/IP

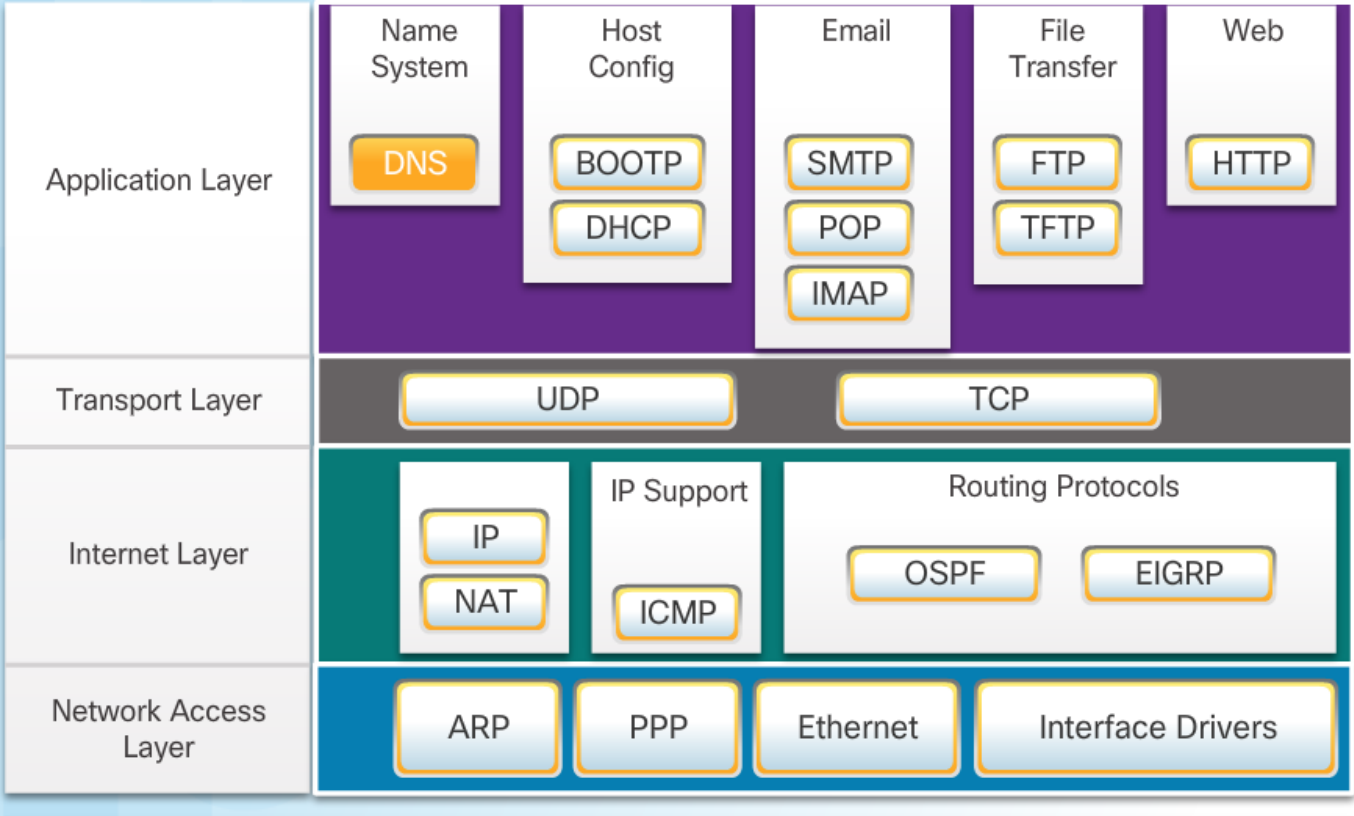
- Advanced Research Projects Agency Network (ARPANET) was the predecessor to today's Internet.
- ARPANET was funded by the U.S. Department of Defense for use by universities and research laboratories.





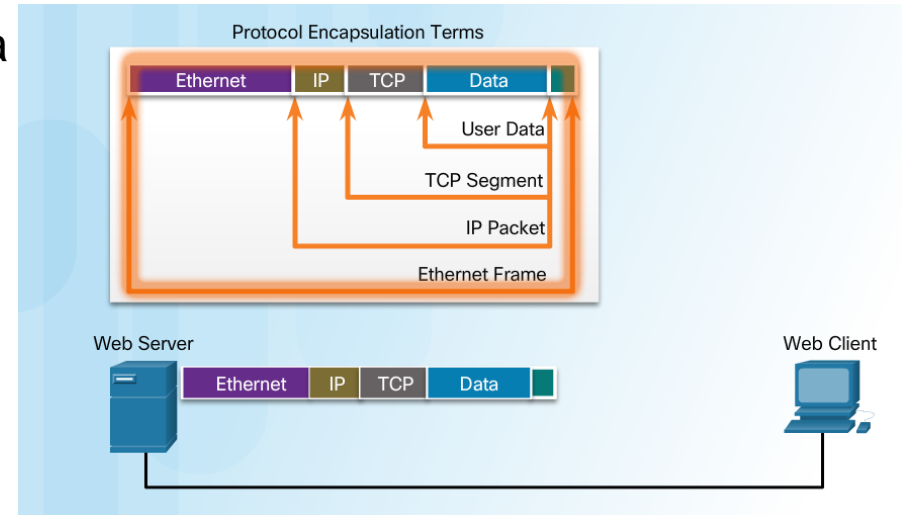
Protocol Suites

# TCP/IP Protocol Suite



# TCP/IP Communication Process

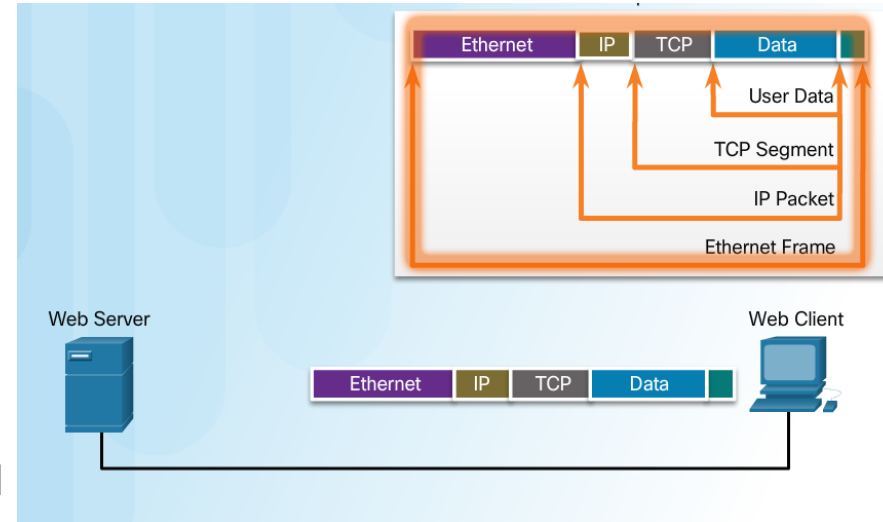
- When sending data from a web server to a client the encapsulation procedure would be as follows:
  - The webserver prepares the Hypertext Markup Language (HTML) page. The HTTP **application layer protocol sends the data to the transport layer**.
  - The transport layer breaks the data into **segments** and identifies each.
  - Next the IP source and destination addresses are added, creating an **IP Packet**.
  - The Ethernet information is then added creating the **Ethernet Frame**, or **data link frame**.



- This frame is **delivered to the nearest router** along the path towards the web client. Each router adds new data link information before forwarding the packet.

# TCP/IP Communication Process (Cont.)

- When receiving the data link frames from the web server, the client **processes** and removes each protocol header **in the opposite order** it was added:
  - First the Ethernet header is removed
  - Then the IP header
  - Then the Transport layer header
  - Finally the HTTP information is processed and sent to the client's web browser



# Standards Organizations

## Open Standards

- Open standards encourage interoperability, competition, and innovation.
- Standards organizations are usually **vendor-neutral**, **non-profit** organizations established to develop and promote the concept of open standards.

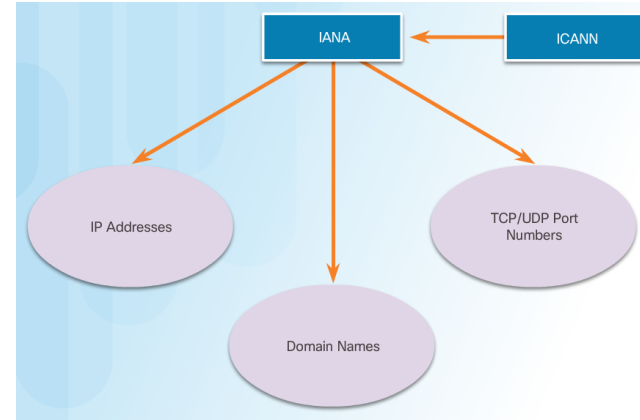


## Standards Organizations

# Internet Standards

- **Internet Society (ISOC)** –promotes open development and evolution of Internet use globally.
- **Internet Architecture Board (IAB)** - management and development of Internet standards.
- **Internet Engineering Task Force (IETF)** - develops, updates, and maintains Internet and TCP/IP technologies.
- **Internet Research Task Force (IRTF)** - focused on long-term research related to Internet and TCP/IP protocols.

- **Internet Corporation for Assigned Names and Numbers (ICANN)** - coordinates IP address allocation and management of domain names.
- **Internet Assigned Numbers Authority (IANA)** - manages IP address allocation, domain name management, and protocol identifiers for ICANN.



# Electronics and Communications Standard Organizations

- **Institute of Electrical and Electronics Engineers (IEEE)** - dedicated to advancing technological innovation and creating standards in a wide area of industries including networking.
- **Electronic Industries Alliance (EIA)** - standards related to electrical wiring, connectors, and network racks.
- **Telecommunications Industry Association (TIA)** standards for radio equipment, cellular towers, Voice over IP (VoIP) devices, and satellite communications.
- **International Telecommunications Union-Telecommunication Standardization Sector (ITU-T)** standards for video compression, Internet Protocol Television (IPTV), and broadband communications.



# Lab-Researching Networking Standards



Cisco Networking Academy®

Mind Wide Open™

## Lab - Researching Networking Standards

### Objectives

**Part 1: Research Networking Standards Organizations**

**Part 2: Reflect on Internet and Computer Networking Experiences**

### Background / Scenario

Using web search engines like Google, research the non-profit organizations that are responsible for establishing international standards for the Internet and the development of Internet technologies.

### Required Resources

Device with Internet access

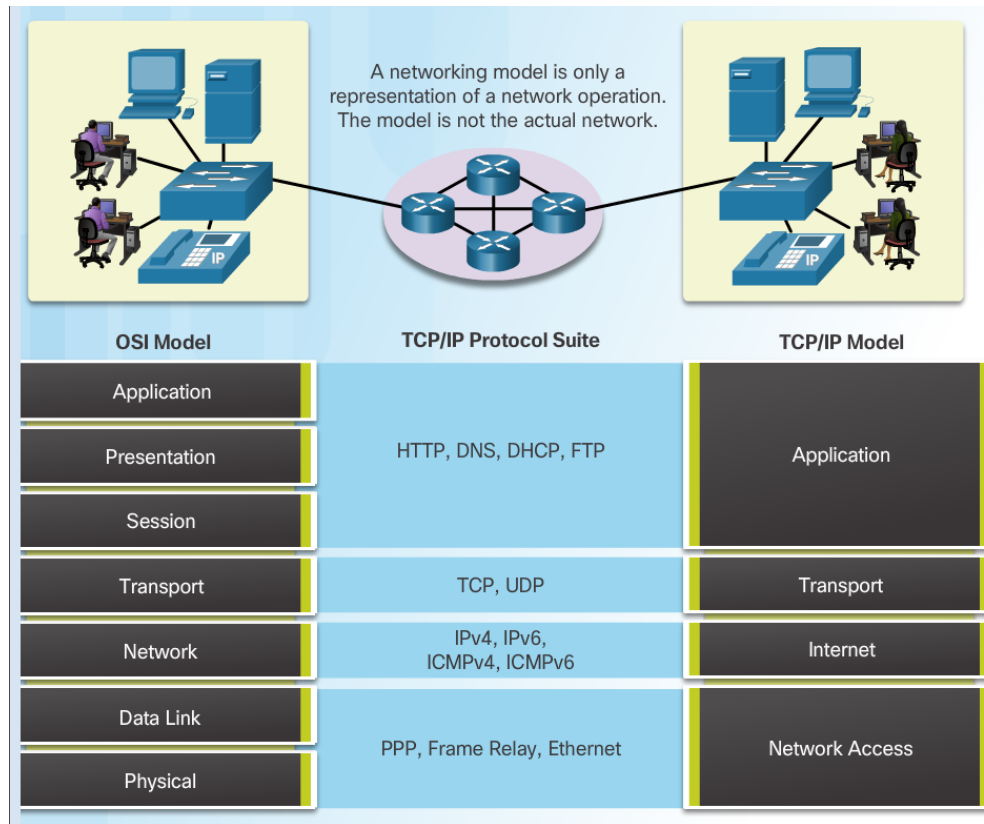
### Part 1: Research Networking Standards Organizations

In Part 1, you will identify some of the major standards organizations and important characteristics, such as the number of years in existence, the size of their membership, the important historical figures, some of the responsibilities and duties, organizational oversight role, and the location of the organization's headquarters.

Use a web browser or websites for various organizations to research information about the following organizations and the people who have been instrumental in maintaining them.

# The Benefits of Using a Layered Model

- The benefits of using a layered model include:
  - **Assisting in protocol design** since protocols at each layer have defined functions.
  - **Fostering competition** because products from different vendors can work together.
  - **Preventing technology changes** in one layer from affecting other layers.
  - **Providing a common language** to describe networking functions and capabilities.





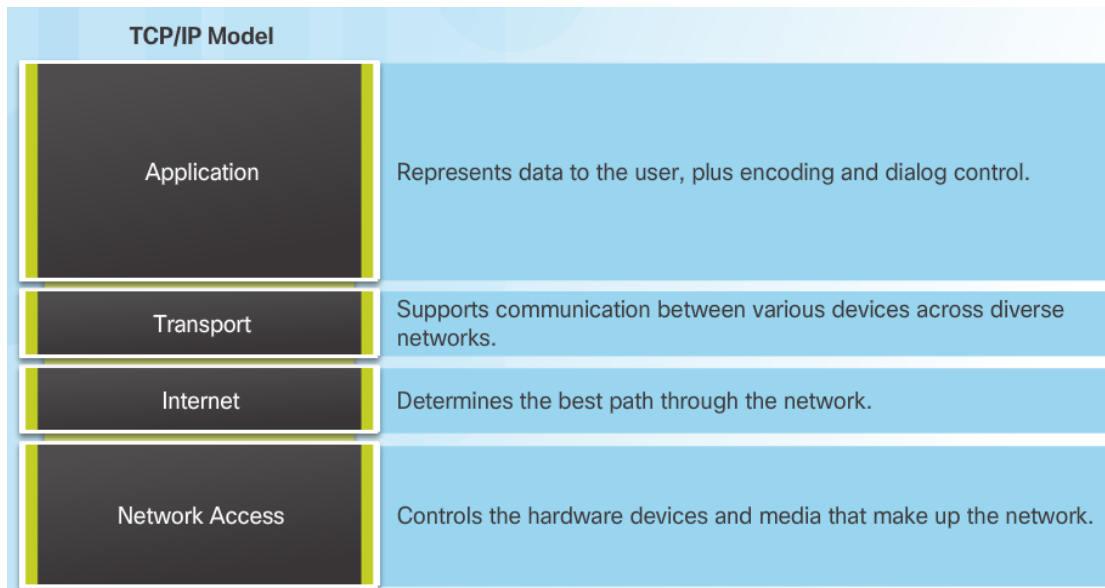
# The OSI Reference Model



- Application - contains protocols used for process-to-process communications.
- Presentation - provides for common representation of the data.
- Session - provides services to the presentation layer to organize its dialogue and to manage data exchange.
- Transport - defines services to segment, transfer, and reassemble the data.
- Network - provides services to exchange the individual pieces of data over the network between identified end devices.
- Data Link - provides methods for exchanging data frames between devices over a common media.
- Physical - describes the mechanical, electrical, functional, and procedural means to transmit bits across physical connections.

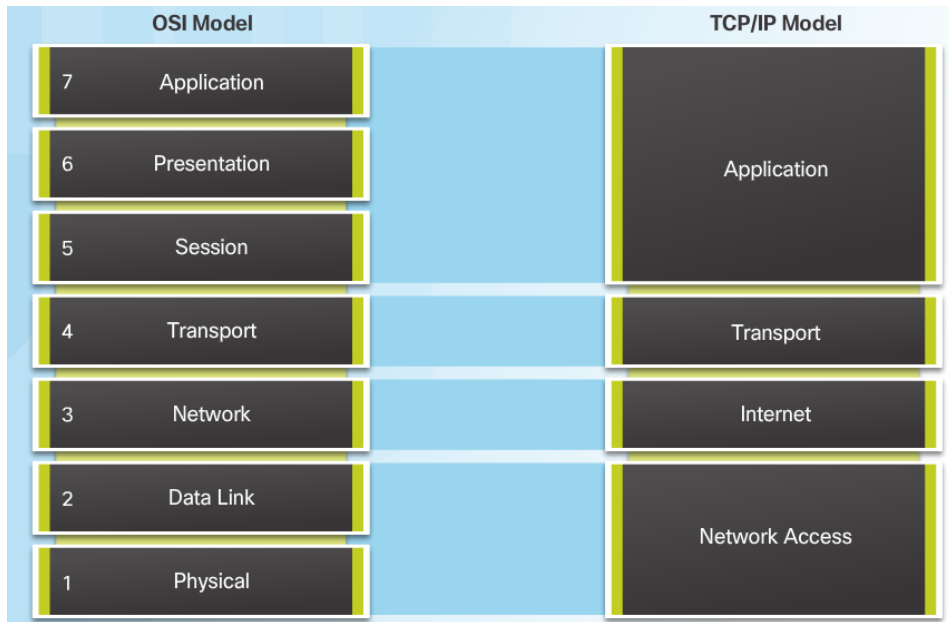
# The TCP/IP Protocol Model

- The TCP/IP Protocol Model
  - Created in the early 1970s for internetwork communications.
  - Open Standard.
  - Also called The TCP/IP Model or the Internet Model.




# OSI Model and TCP/IP Model Comparison

- In the OSI model, the network access layer and the application layer of the TCP/IP model are further divided to describe discrete functions that must occur at these layers.



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



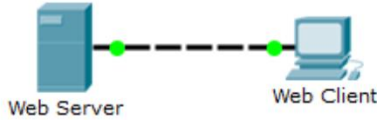
Cisco Networking Academy®

Mind Wide Open™

---

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

**Topology**



Web Server      Web Client

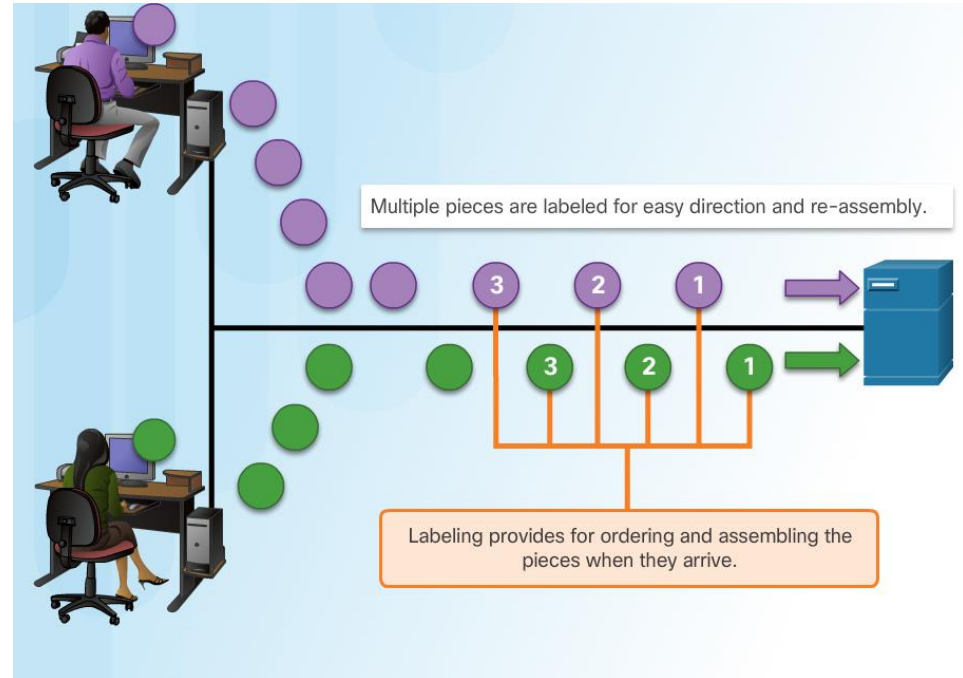
**Objectives**

- Part 1: Examine HTTP Web Traffic
- Part 2: Display Elements of the TCP/IP Protocol Suite

## 3.3 Data Transfer in the Network

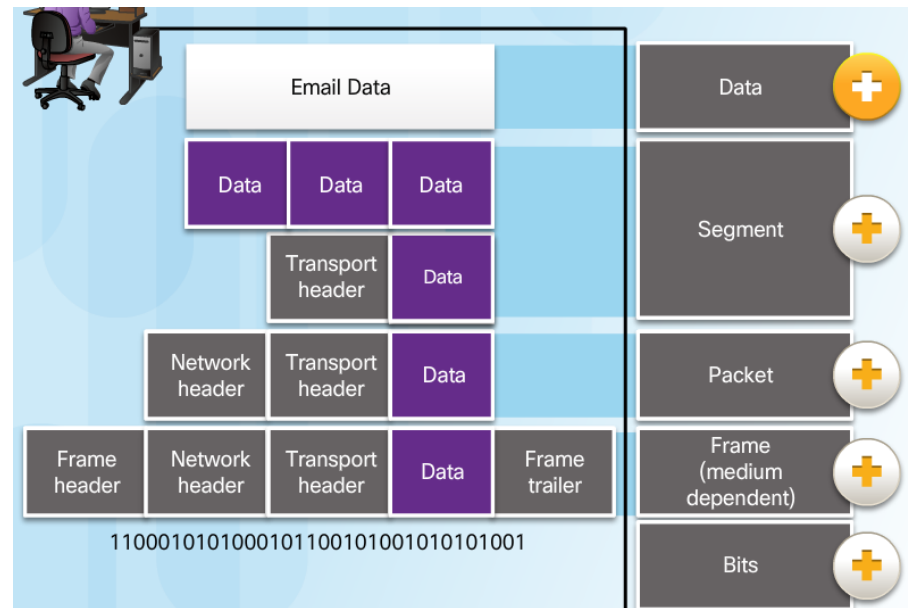
# Message Segmentation

- Large streams of data are divided into smaller, more manageable pieces to send over the network.
- By sending smaller pieces, many different conversations can be interleaved on the network, called **multiplexing**.
- Each piece must be **labeled**.
- If part of the message fails to make it to the destination, only the missing pieces need to be retransmitted.



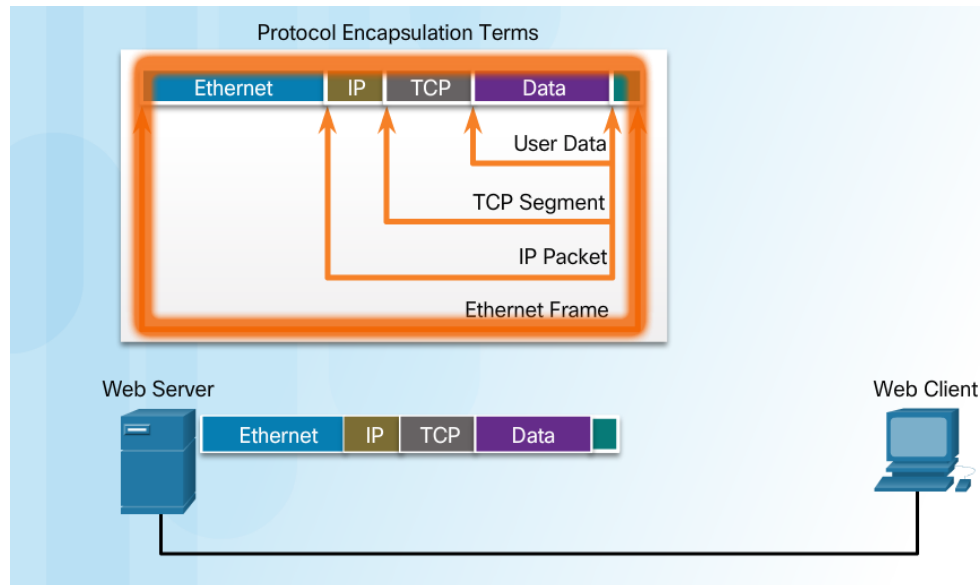
# Protocol Data Units

- As application data is passed down the protocol stack, information is added at each level. This is known as the **encapsulation** process.
- The form that the data takes at each layer is known as a **Protocol Data Unit (PDU)**.
  - Data** - application layer PDU
  - Segment** – Transport layer PDU
  - Packet** – Network layer PDU
  - Frame** – Data Link Layer PDU
  - Bits** – Physical Layer PDU



# Encapsulation Example

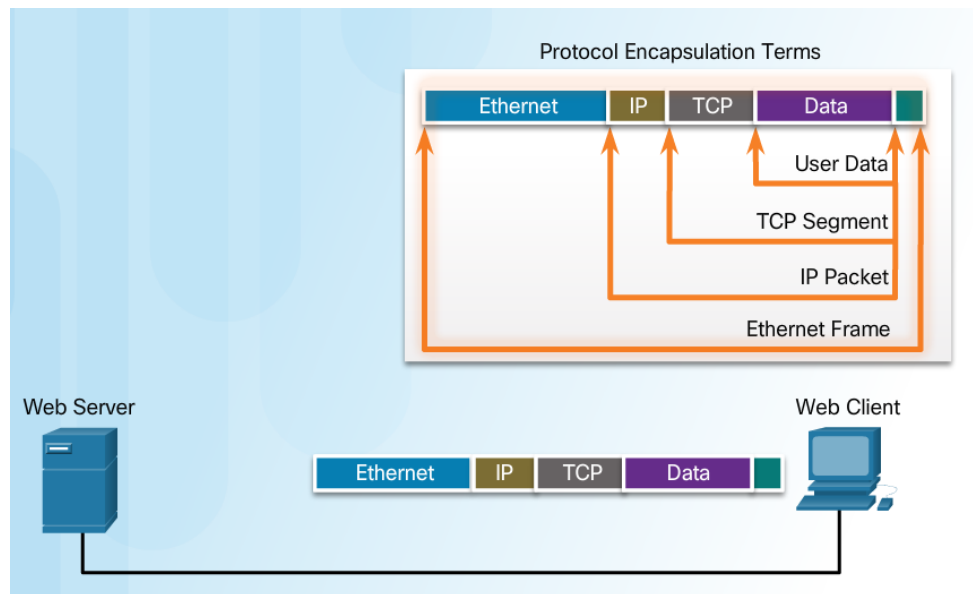
- The encapsulation process works **from top to bottom**:
  - Data is divided into segments.
  - The TCP segment is encapsulated in the IP Packet.
  - The IP packet is encapsulated in the Ethernet Frame.





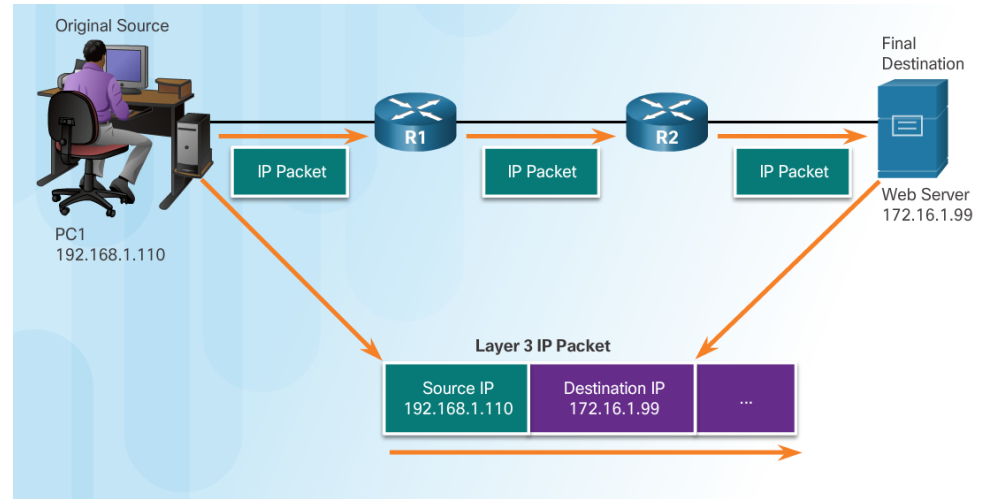
# De-encapsulation

- The de-encapsulation process works **from bottom to top**.
- 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.



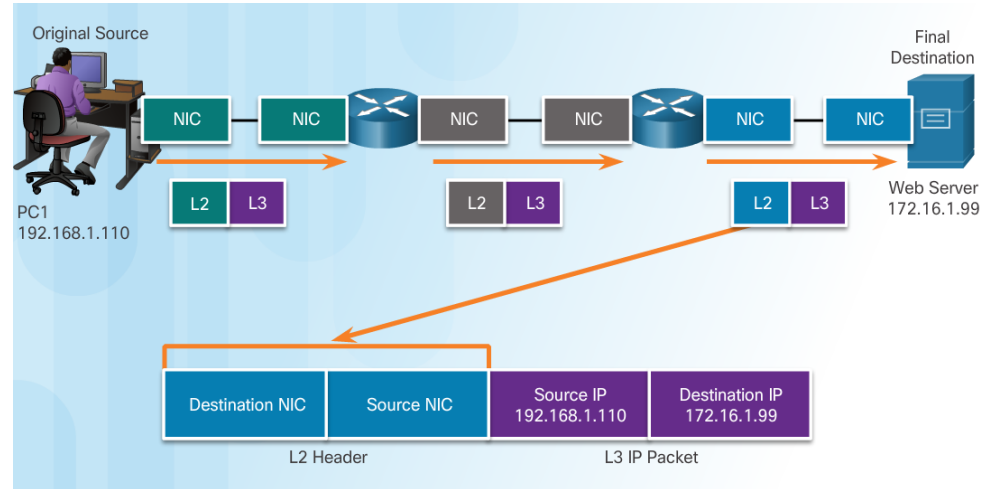
# Network Addresses

- Network layer source and destination addresses - Responsible for delivering the IP packet from the **original source to the final destination**.
  - **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.



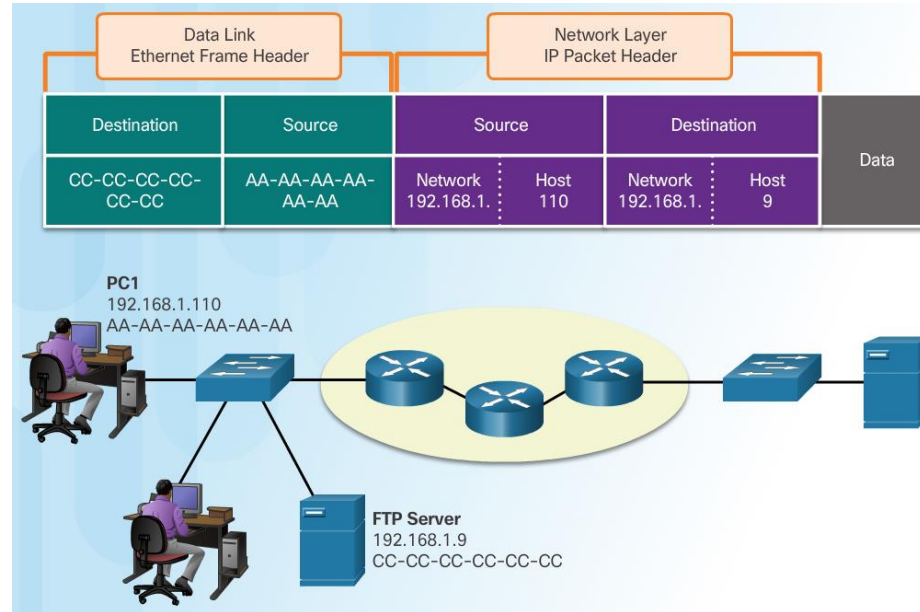
# Data Link Addresses

- The purpose of the data link address is to deliver the data link frame from one network interface to another network interface **on the same network**.
- As the IP packet travels from source to destination it is encapsulated in a new data link frame when it is forwarded by each router.



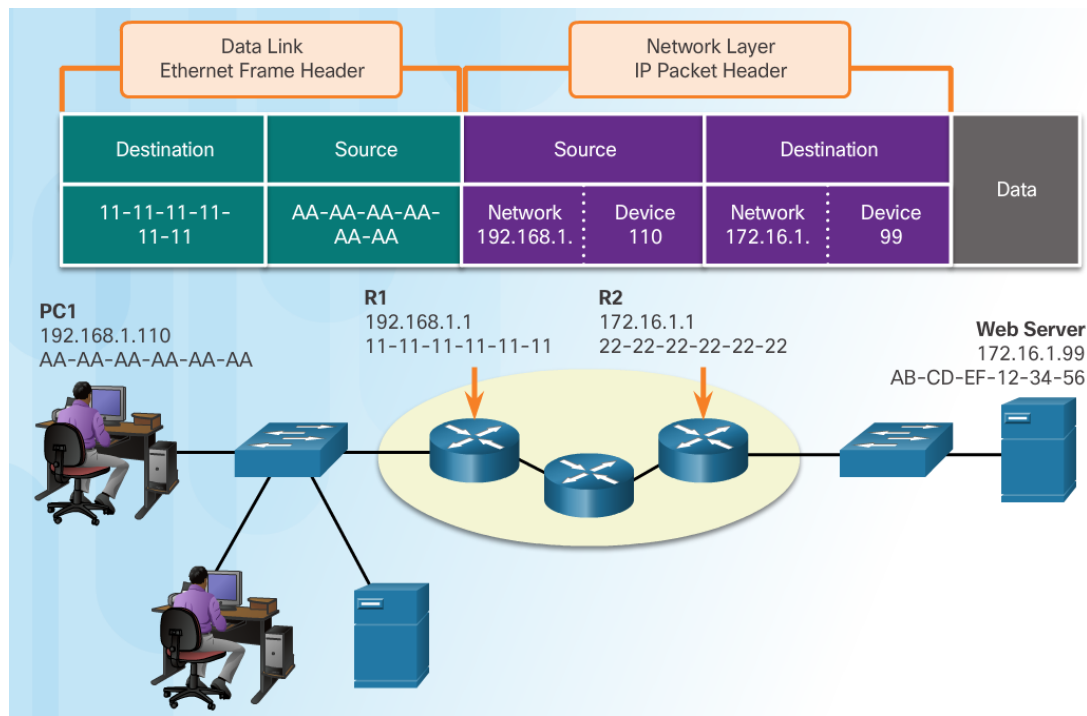
# Devices on the Same Network

- The network layer addresses, or IP addresses, indicate the original source and final destination.
  - Network portion – The left-most part of the address indicates which network the IP address is a member of.
  - Host portion – The remaining part of the address identifies a specific device on the network.
- The data link frame which uses MAC addressing, is sent directly to the receiving device.
  - Source MAC address - address of sending device.
  - Destination MAC address – address of receiving device.



# Devices on a Remote Network

- Sending to a remote network - the source and destination IP addresses represent **hosts on different networks**.
- The data link frame cannot be sent directly to the remote destination host. Therefore the frame is sent to the default gateway (nearest router interface).
- The router removes the received Layer 2 information and adds new data link information before forwarding out the exit interface.



# 3.4 Chapter Summary

# Lab-Installing Wireshark



## Lab – Installing Wireshark

### Objectives

Download and Install Wireshark

### Background / Scenario

Wireshark is a software protocol analyzer, or "packet sniffer" application, used for network troubleshooting, analysis, software and protocol development, and education. As data streams travel back and forth over the network, the sniffer "captures" each protocol data unit (PDU) and can decode and analyze its content according to the appropriate RFC or other specifications.

Wireshark is a useful tool for anyone working with networks and can be used with most labs in the CCNA courses for data analysis and troubleshooting. This lab provides instructions for downloading and installing Wireshark.

### Required Resources

- 1 PC (Windows 7 or 8 with Internet access)

### Download and Install Wireshark


Wireshark has become the industry standard packet-sniffer program used by network engineers. This open source software is available for many different operating systems, including Windows, Mac, and Linux. In this lab, you will download and install the Wireshark software program on your PC.

**Note:** Before downloading Wireshark, check with your instructor about your academy's software download policy.

#### Step 1: Download Wireshark.

- Wireshark can be downloaded from [www.wireshark.org](http://www.wireshark.org).
- Click **Download Wireshark**.

# Lab - Using Wireshark To View Network Traffic

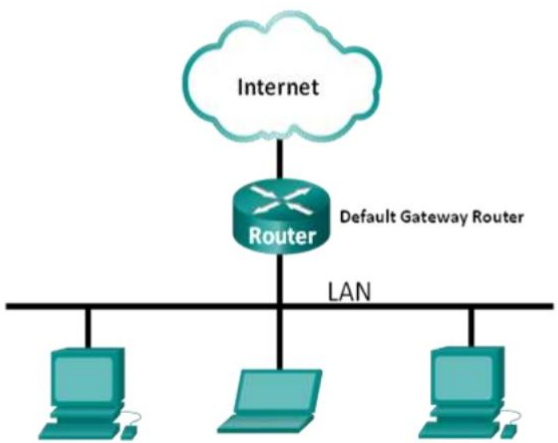
 Cisco Networking Academy<sup>®</sup>

Mind Wide Open<sup>™</sup>

---

## Lab - Using Wireshark to View Network Traffic

Topology



The diagram illustrates a network topology. At the top, a cloud labeled "Internet" is connected to a central router labeled "Router" and "Default Gateway Router". The router is connected to a horizontal line representing a "LAN". Below the LAN line, there are three devices: a desktop PC on the left, a laptop in the center, and another desktop PC on the right.

Objectives

- Part 1: Capture and Analyze Local ICMP Data in Wireshark
- Part 2: Capture and Analyze Remote ICMP Data in Wireshark



## Chapter 3: Network Protocols and Communications

- Explain how rules 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.

