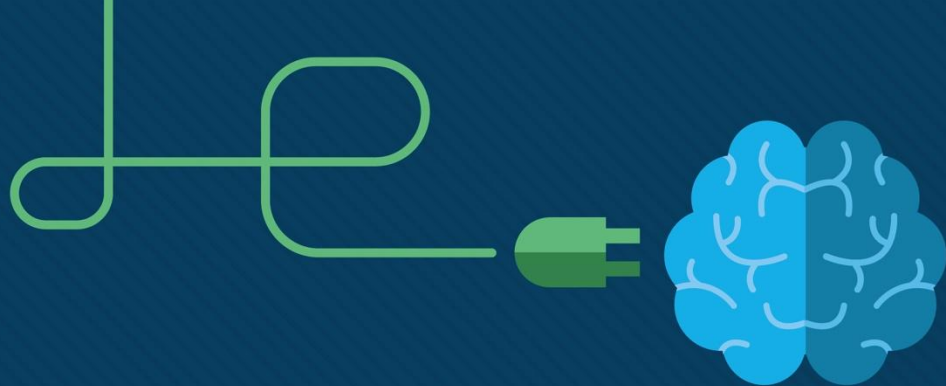


Introduction to Networking  
CT043-3-1 & Version VE1

## Protocols and Models



# Protocols and Models



# Topic and structure of the Lesson

Topic Title	Topic Objective
The Rules	Describe the types of rules that are necessary to successfully communicate.
Protocols	Explain why protocols are necessary in network communication.
Protocol Suites	Explain the purpose of adhering to a protocol suite.
Standards Organizations	Explain the role of standards organizations in establishing protocols for network interoperability.
Reference Models	Explain how the TCP/IP model and the OSI model are used to facilitate standardization in the communication process.
Data Encapsulation	Explain how data encapsulation allows data to be transported across the network.
Data Access	Explain how local hosts access local resources on a network.

# Key Terms You Must Be Able To Use:

If you have mastered this topic, you should be able to use the following terms correctly in your exams:

- Protocols
- Unicast, Multicast and Broadcast
- TCP/IP Protocol Suite
- OSI Layers
- Protocol Data Unit
- Encapsulation and De-encapsulation
- Segments
- Packets
- Frame
- Bits
- Network Address
- Data Link Address

# The Rules

# Rule Establishment

- Individuals must **use established rules or agreements** to govern the conversation.
- The first message is difficult to read because it is not formatted properly. The second shows the message properly formatted

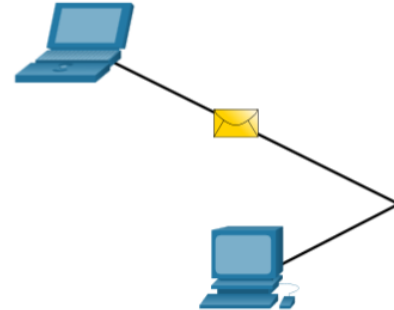
```
humans communication between govern rules. It is verydifficult tounderstand messages that are not
correctly formatted and donot follow the established rules and protocols. A estrutura da
gramatica, da lingua, da pontuacao e do sentence faz a configuracao humana compreensivel por
muitos individuos diferentes.
```

```
Rules govern communication between humans. It is very difficult to understand messages that are
not correctly formatted and do not follow the established rules and protocols. The structure of
the grammar, the language, the punctuation and the sentence make the configuration humanly
understandable for many different individuals.
```

# The Rules

## Communications Protocols

- All communications are governed **by protocols**.
- Protocols are the **rules** that communications will follow.
- These rules will vary depending on the protocol.



# Network Protocol Requirements

**Common computer protocols** must be in agreement and include the following requirements:

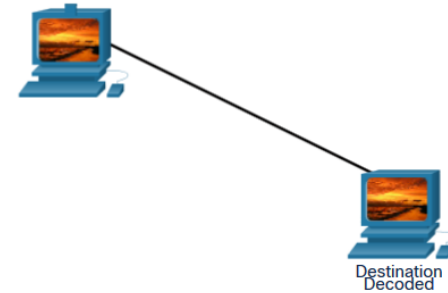
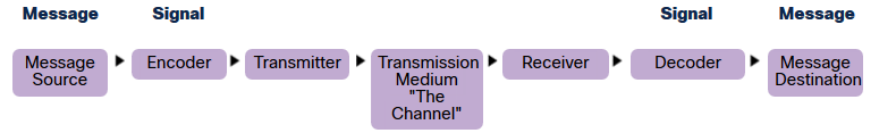
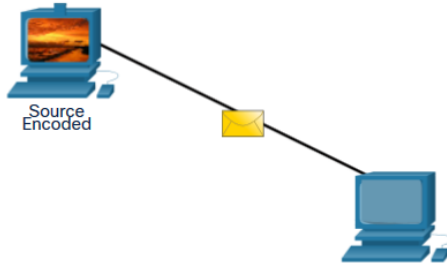
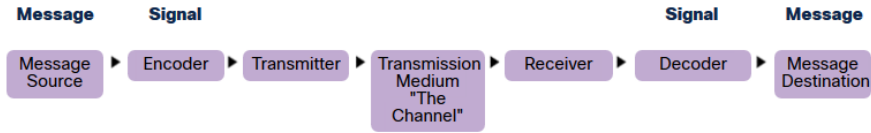
- Message **encoding**
- Message **formatting** and **encapsulation**
- Message **size**
- Message **timing**
- Message **delivery options**



# The Rules

## Message Encoding

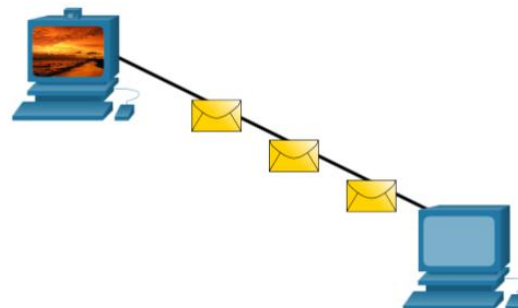
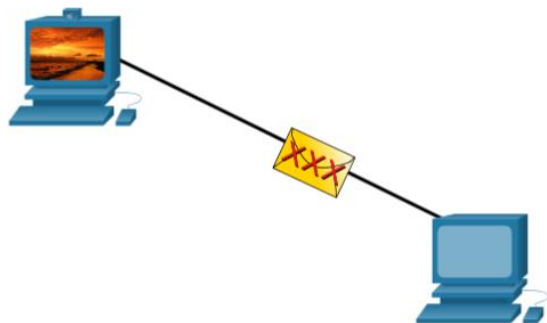
- Encoding is the process of **converting information into another acceptable form** for transmission.
- **Decoding reverses** this process to interpret the information.



# Message Encoding

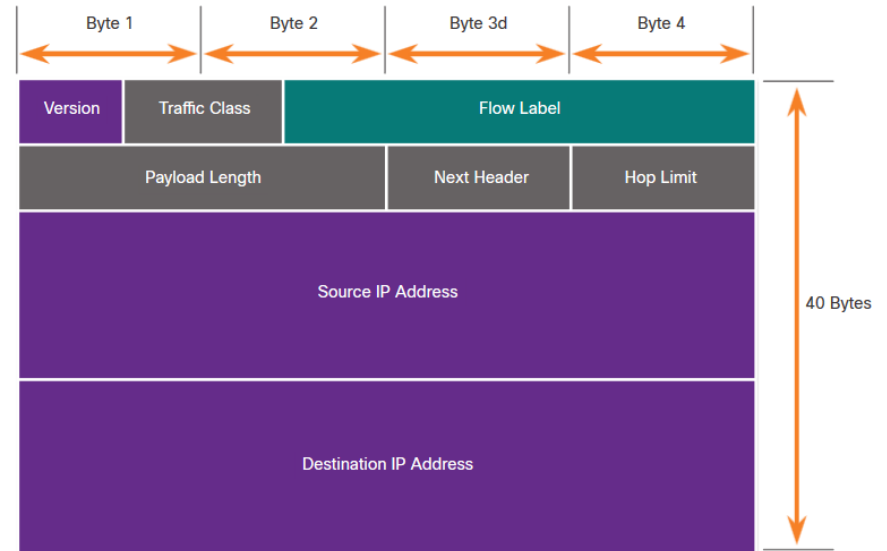
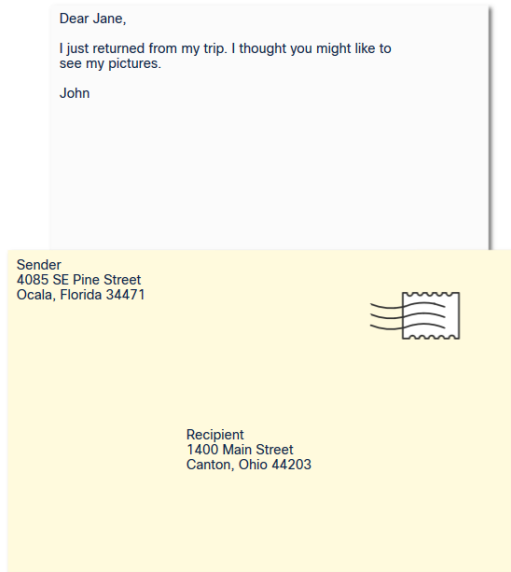
**Encoding** between hosts must be in an appropriate format for the medium.

- Messages sent across the network are **converted to bits**
- The bits are encoded into a pattern of **light, sound, or electrical impulses**.
- The destination host **must decode the** signals to interpret the message.



# Message Formatting and Encapsulation

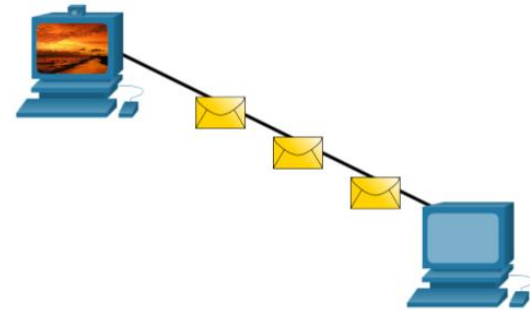
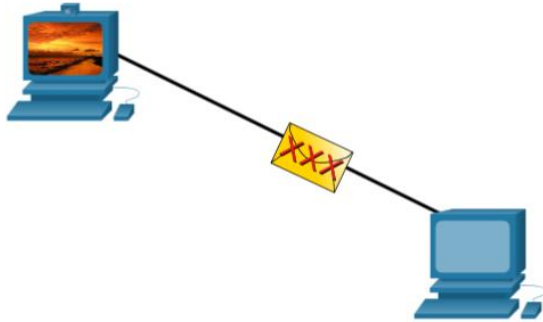
- When a message is sent, it must use a **specific format or structure**.
- Message formats depend on the type of message and the channel that is used to deliver the message.



## 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 (packets).



# Message Timing

Message timing includes the following:

**Flow Control** – Manages the rate of data transmission and defines **how much information can be sent and the speed** at which it can be delivered.

**Response Timeout** – Manages **how long a device waits** when it does **not hear a reply** from the destination.

**Access method** - Determines when someone can send a message.

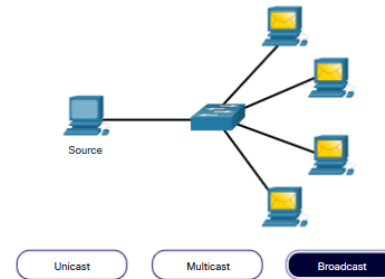
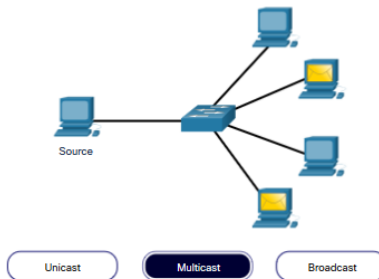
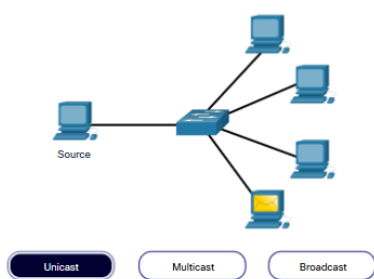
- There may be various rules governing issues like “**collisions**”. This is when **more than one device sends traffic at the same time** and the messages become **corrupt**.
- Some protocols are proactive and attempt to **prevent collisions**; other protocols are reactive and **establish a recovery method** after the collision occurs.

# Message Delivery Options

Message delivery may use one of the following methods:

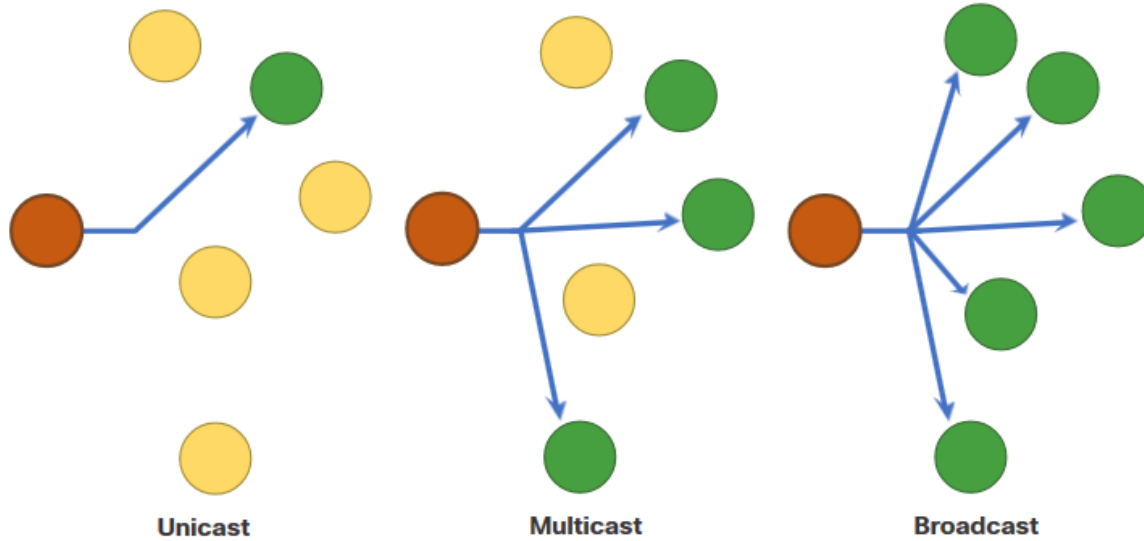
- **Unicast** – one to one communication
- **Multicast** – one to many, typically not all
- **Broadcast** – one to all

**Note:** Broadcasts are used in IPv4 networks, but are not an option for IPv6. Later we will also see “Anycast” as an additional delivery option for IPv6.



# A Note About the Node Icon

- Documents may use the **node icon** , typically a **circle**, to represent all devices.
- The figure illustrates the use of the node icon for delivery options.



# Protocols



# Network Protocol Overview

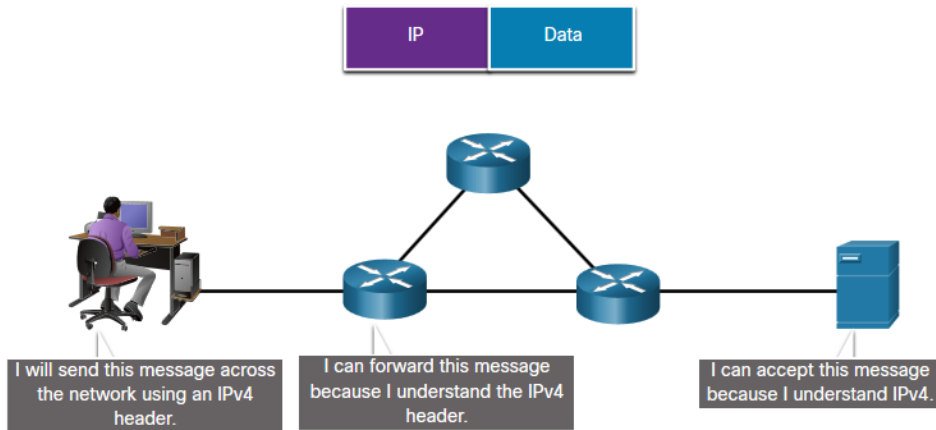
Network protocols define a common **set of rules**.

- Can be **implemented** on devices in:
  - **Software**
  - **Hardware**
  - **Both**
- Protocols have their own:
  - **Function**
  - **Format**

Protocol Type	Description
Network Communications	<b>enable two or more devices</b> to communicate over one or more networks
Network Security	<b>secure data</b> to provide <b>authentication</b> , data <b>integrity</b> , and data <b>encryption</b>
Routing	enable routers to exchange route information, compare path information, and <b>select best path</b>
Service Discovery	used for the <b>automatic detection of devices or services (example HTTPS, DHCP, DNS, etc)</b>

# Network Protocol Functions

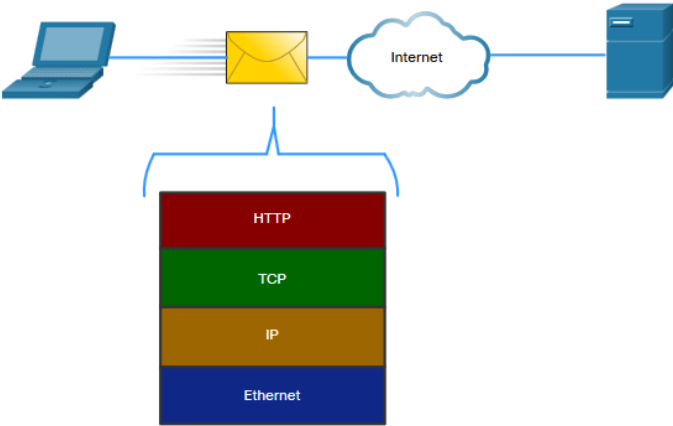
- Devices use **agreed-upon protocols** to communicate .
- Protocols may have one or more functions.



Function	Description
Addressing	<b>Identifies</b> sender and receiver
Reliability	Provides <b>guaranteed delivery</b>
Flow Control	Ensures <b>data flows at an efficient rate</b>
Sequencing	Uniquely <b>labels</b> each transmitted segment of data
Error Detection	Determines if data became <b>corrupted</b> during transmission
Application Interface	<b>Process-to-process</b> communications between network applications

# Protocol Interaction

- When we use network, we require the **use of several protocols**.
- Each protocol has its own function and format.



Protocol	Function
Hypertext Transfer Protocol (HTTP)	<ul style="list-style-type: none"><li>▪ Governs the way a <b>web server</b> and a <b>web client</b> interact</li><li>▪ Defines content and format</li></ul>
Transmission Control Protocol (TCP)	<ul style="list-style-type: none"><li>▪ Manages the <b>individual conversations</b></li><li>▪ Provides <b>guaranteed delivery</b></li><li>▪ Manages <b>flow control</b></li></ul>
Internet Protocol (IP)	Delivers <b>messages globally</b> from the sender to the receiver
Ethernet	Delivers messages from <b>one NIC to another NIC</b> on the same Ethernet Local Area Network (LAN)

# Protocol Suites

# Network Protocol Suites

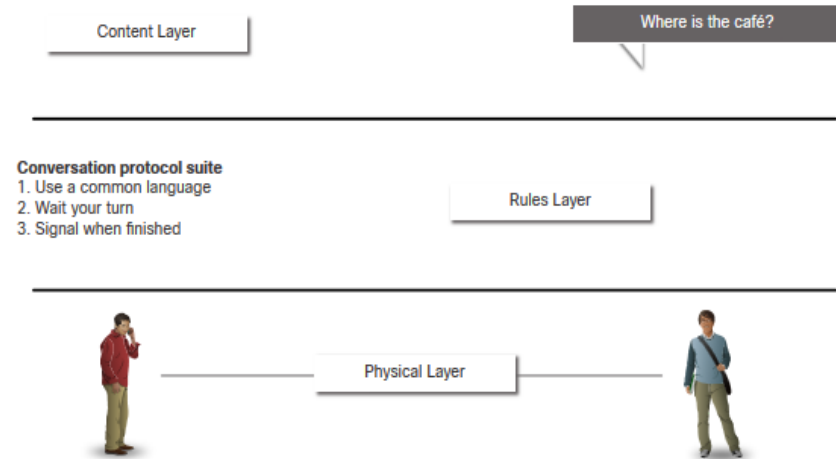
Protocols must be able to work with other protocols.

Protocol suite:

- **A group of inter-related protocols** necessary to perform a communication function
- **Sets of rules that work together** to help solve a problem

The protocols are viewed in **terms of layers**:

- Higher Layers
- Lower Layers- concerned with moving data and provide services to upper layers



Protocol suites are sets of rules that work together to help solve a problem.

# Evolution of Protocol Suites

There are **several protocol suites**.

- **Internet Protocol Suite or TCP/IP**- The most common protocol suite and maintained by the Internet Engineering Task Force (IETF)
- **Open Systems Interconnection (OSI) protocols**- Developed by the International Organization for Standardization (ISO) and the International Telecommunications Union (ITU)
- **AppleTalk**- Proprietary suite release by Apple Inc.
- **Novell NetWare**- Proprietary suite developed by Novell Inc.

TCP/IP 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 ARP WLAN			

# Standards Organizations

# Standards Organizations

## Open Standards



**I E T F<sup>®</sup>**



Open standards encourage:

- **interoperability**
- **competition**
- **innovation**

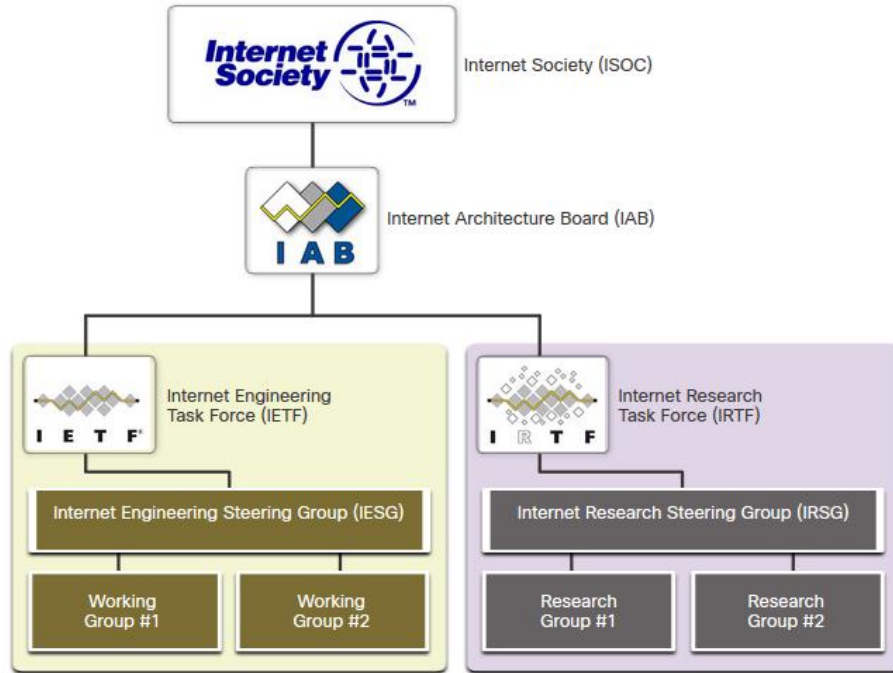
Standards organizations are:

- **vendor-neutral**
- **non-profit organizations**
- established to develop and promote the concept of open standards.



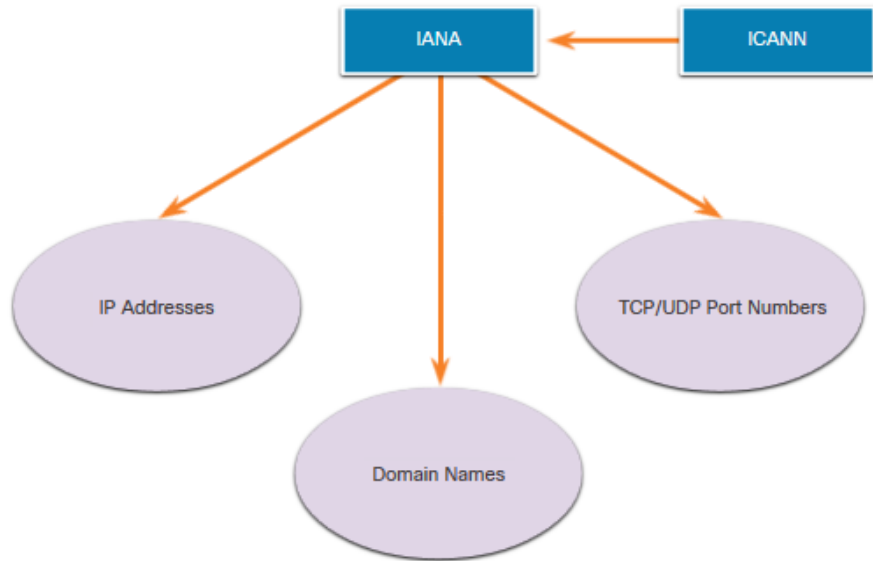
# Standards Organizations

## Internet Standards



- **Internet Society (ISOC)** - Promotes the open development and evolution of internet
- **Internet Architecture Board (IAB)** - Responsible for 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 Standards (Cont.)



Standards organizations involved with the development and support of TCP/IP

- **Internet Corporation for Assigned Names and Numbers (ICANN)** - Coordinates **IP address allocation**, the management of domain names, and assignment of other information
- **Internet Assigned Numbers Authority (IANA)** - Oversees and manages IP address allocation, **domain name** management, and protocol identifiers for ICANN

# Electronic and Communications Standards

- **Institute of Electrical and Electronics Engineers (IEEE)**, pronounced “I-triple-E”) - dedicated to creating standards in power and energy, healthcare, telecommunications, and **networking**
- **Electronic Industries Alliance (EIA)** - develops standards relating to electrical **wiring**, **connectors**, and the 19-inch racks used to mount networking equipment
- **Telecommunications Industry Association (TIA)** - develops communication standards in radio equipment, cellular towers, **Voice over IP** (VoIP) devices, **satellite** communications, and more
- **International Telecommunications Union-Telecommunication Standardization Sector (ITU-T)** - defines standards for **video** compression, **Internet Protocol Television** (IPTV), and broadband communications, such as a digital subscriber line (DSL)

# Reference Models

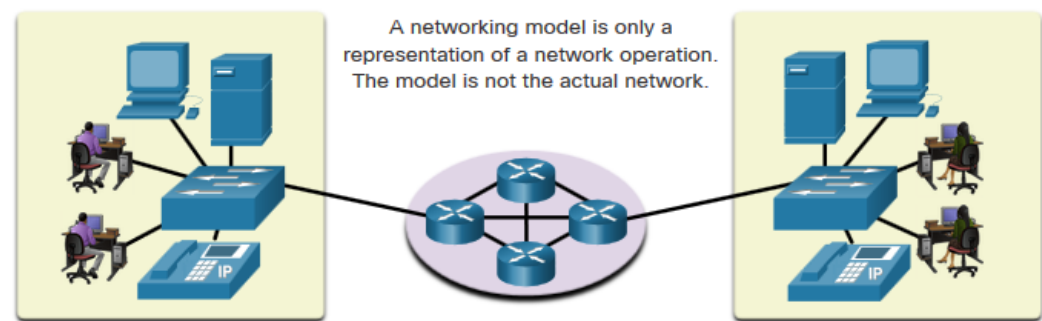
## The Benefits of Using a Layered Model (Cont.)

These are **the benefits of using** a layered model:

- **Assist 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
- **Foster competition** because products from different vendors can work together
- **Prevent technology** or capability changes in one layer from **affecting other layers above and below**
- **Provide a common language** to describe networking functions and capabilities

# Reference Models

## OSI vs TCP/IP Layered Model



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	Ethernet, WLAN, SONET, SDH	Network Access
Physical		

Complex concepts such as how a network operates can be **difficult to explain and understand**. For this reason, a layered model is used.

Two layered models describe network operations:

- **Open System Interconnection (OSI) Reference Model**
- **TCP/IP Reference Model**

# The OSI Reference Model

OSI Model Layer	Description
7 - Application	Contains protocols used for <b>process-to-process communications</b> .
6 - Presentation	Provides for common <b>representation of the data</b> transferred between application layer services.
5 - Session	Provides services to the presentation layer and to <b>manage data exchange</b> .
4 - Transport	Defines services to <b>segment, transfer, and reassemble</b> the data for individual communications.
3 - Network	Provides services to <b>exchange the individual pieces of data over the network</b> .
2 - Data Link	Describes methods for <b>exchanging data frames over a common media</b> .
1 - Physical	Describes the means to activate, maintain, and de-activate <b>physical connections</b> .

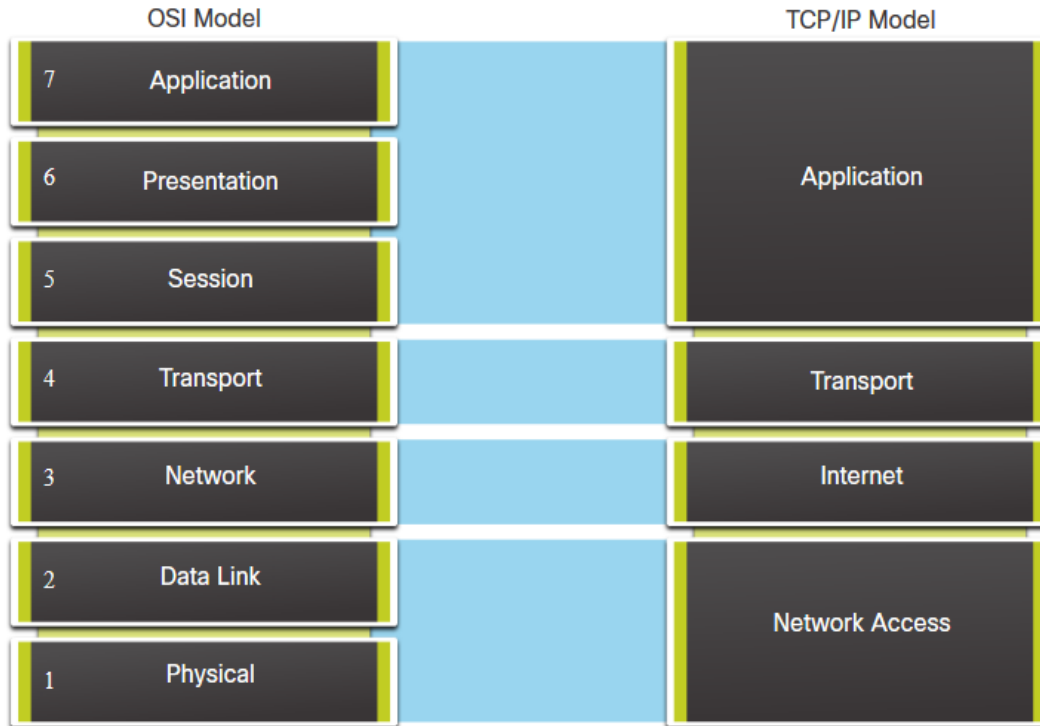
## Reference Models

# The TCP/IP Reference Model

TCP/IP Model Layer	Description
Application	<b>Represents data</b> to the user, plus encoding and dialog control.
Transport	Supports <b>communication between various devices</b> across diverse networks.
Internet	Determines the <b>best path through the network</b> .
Network Access	Controls the <b>hardware devices and media</b> that make up the network.



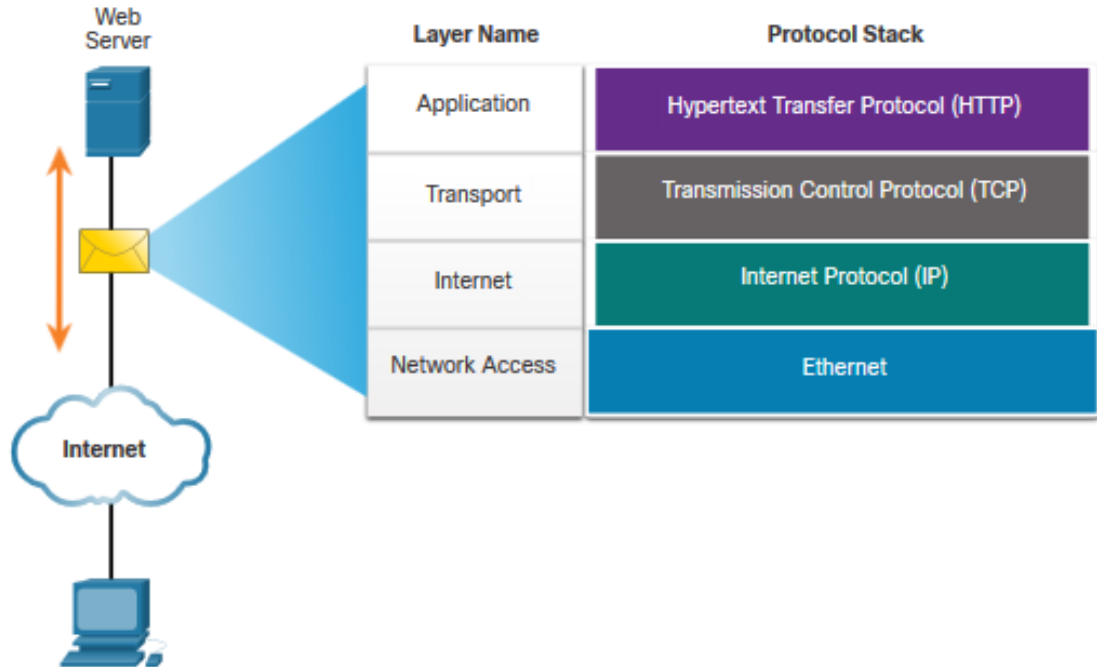
# OSI and TCP/IP Model Comparison



- The OSI model divides the network access layer and the application layer of the TCP/IP model into multiple layers.
- The TCP/IP protocol suite does not specify which protocols to use when transmitting over a physical medium.
- OSI Layers 1 and 2 discuss the necessary procedures to access the media and the physical means to send data over a network.

# TCP/IP Protocol Example

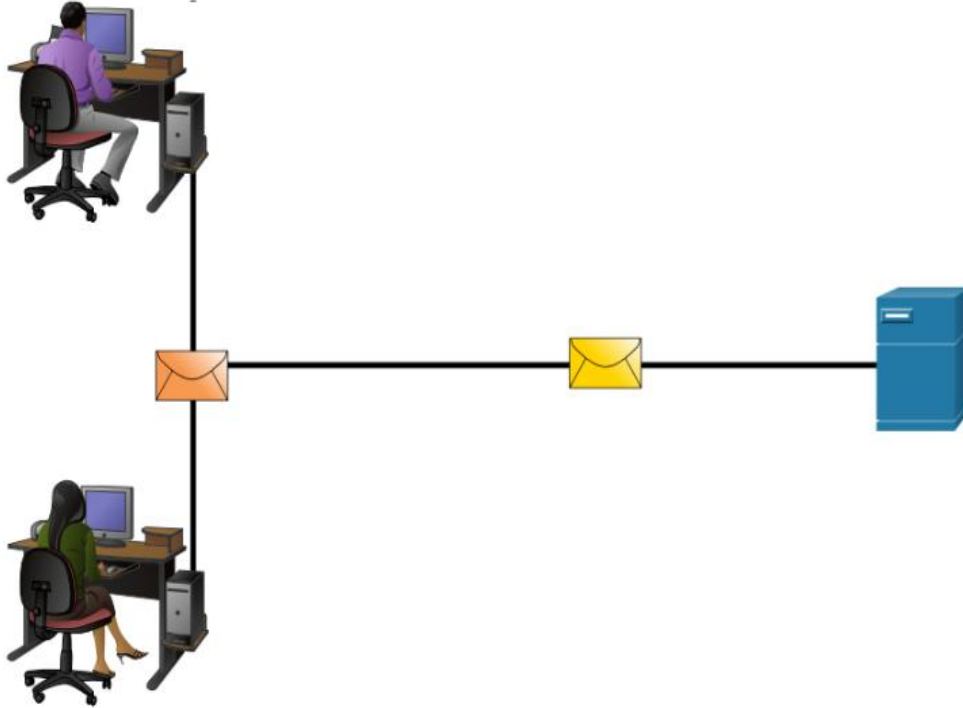
- **TCP/IP protocols** operate at the application, transport, and internet layers.
- The most common network access layer LAN protocols are Ethernet and WLAN (wireless LAN).



# Data Encapsulation

## Data Encapsulation

# Segmenting Messages



Segmenting is the **process of breaking up messages into smaller units.**

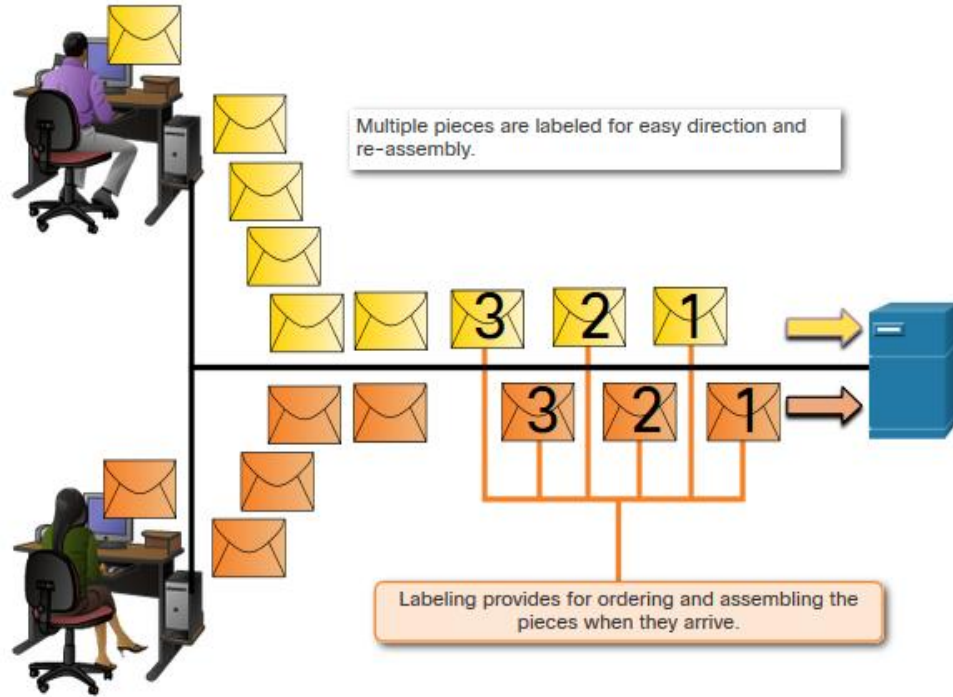
**Multiplexing** is the processes of taking **multiple streams** of segmented data and **interleaving them together.**

Segmenting messages has **two primary benefits:**

- **Increases speed** - Large amounts of data can be sent over the network without **tying up a communications link.**
- **Increases efficiency** - Only segments which **fail** to reach the destination need to be **retransmitted**, not the entire data stream.

# Data Encapsulation

## Sequencing

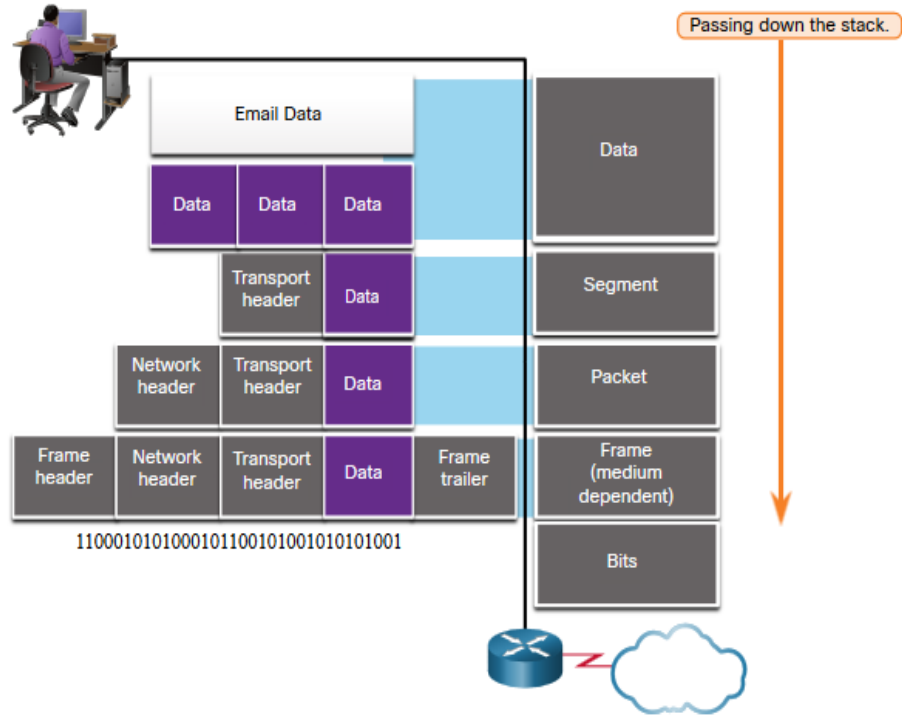


Sequencing messages is the process of **numbering the segments** so that the message may be reassembled at the destination.

**TCP is responsible for sequencing** the individual segments.

# Data Encapsulation

## Protocol Data Units (PDU)



**Encapsulation** is the process where protocols **add their information to the data**.

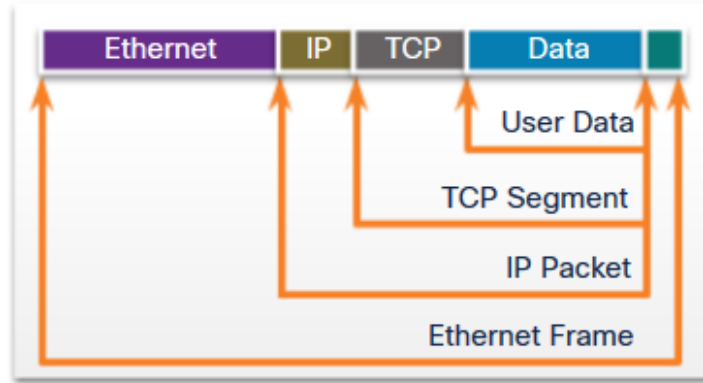
- At each stage of the process, a **PDU has a different name** to reflect its new functions.
- There is no universal naming convention for PDUs, in this course, the PDUs are named according to the protocols of the TCP/IP suite.
- PDUs passing down the stack are as follows:

1. **Data (Data Stream)**
2. **Segment**
3. **Packet**
4. **Frame**
5. **Bits (Bit Stream)**

# Data Encapsulation

## Encapsulation Example

- Encapsulation is a top down process.
- The level above does its process and then **passes it down to the next level** of the model. This process is repeated by each layer until it is sent out as a bit stream.



Web Server



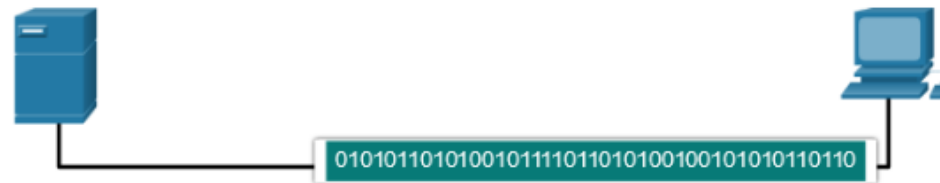
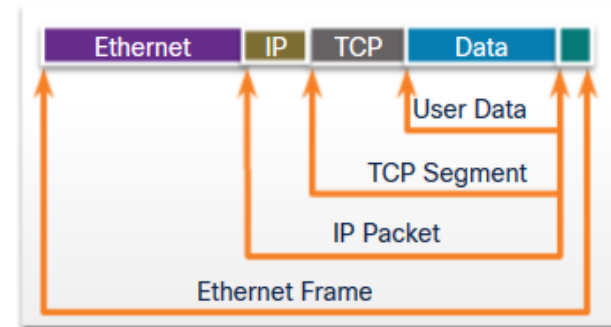
Web Client



# De-encapsulation Example

- Data is de-encapsulated as it **moves up the stack**.
- When a layer completes its process, that layer strips off its header and passes it up to the next level to be processed. This is repeated at each layer until it is a data stream that the application can process.

1. **Received as Bits (Bit Stream)**
2. **Frame**
3. **Packet**
4. **Segment**
5. **Data (Data Stream)**





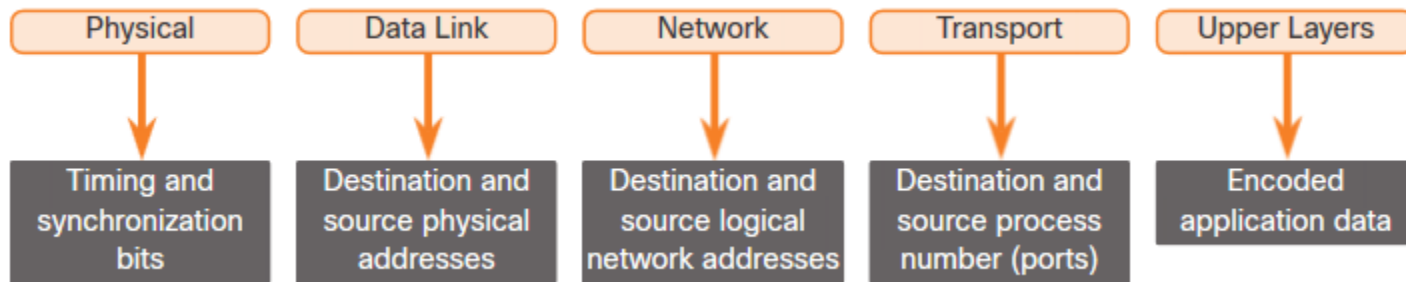
# Data Access

# Addresses

Both the **data link and network layers use addressing** to deliver data from source to destination.

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

**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.



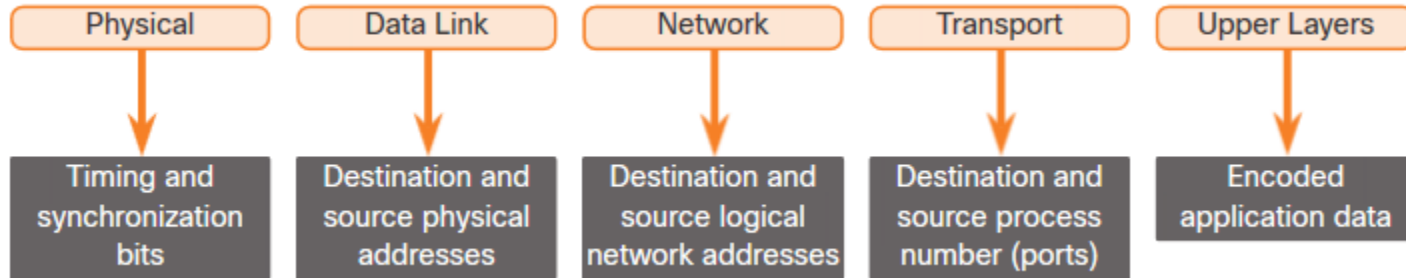
# Data Access Addresses

## Layer 2 Address:

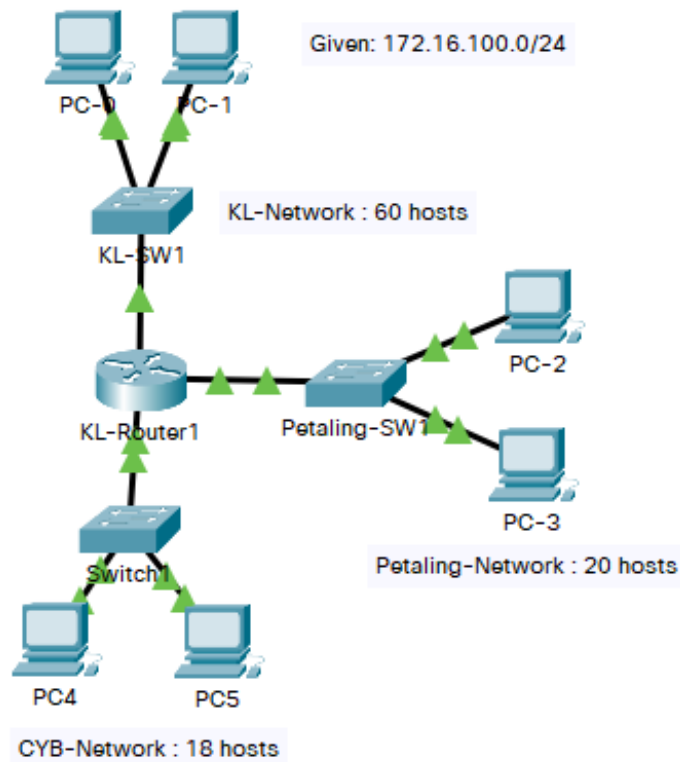
- MAC Address / Physical Address/ Data Link Address

## Layer 3 Address:

- IP Address/ Logical address/ Network Address,

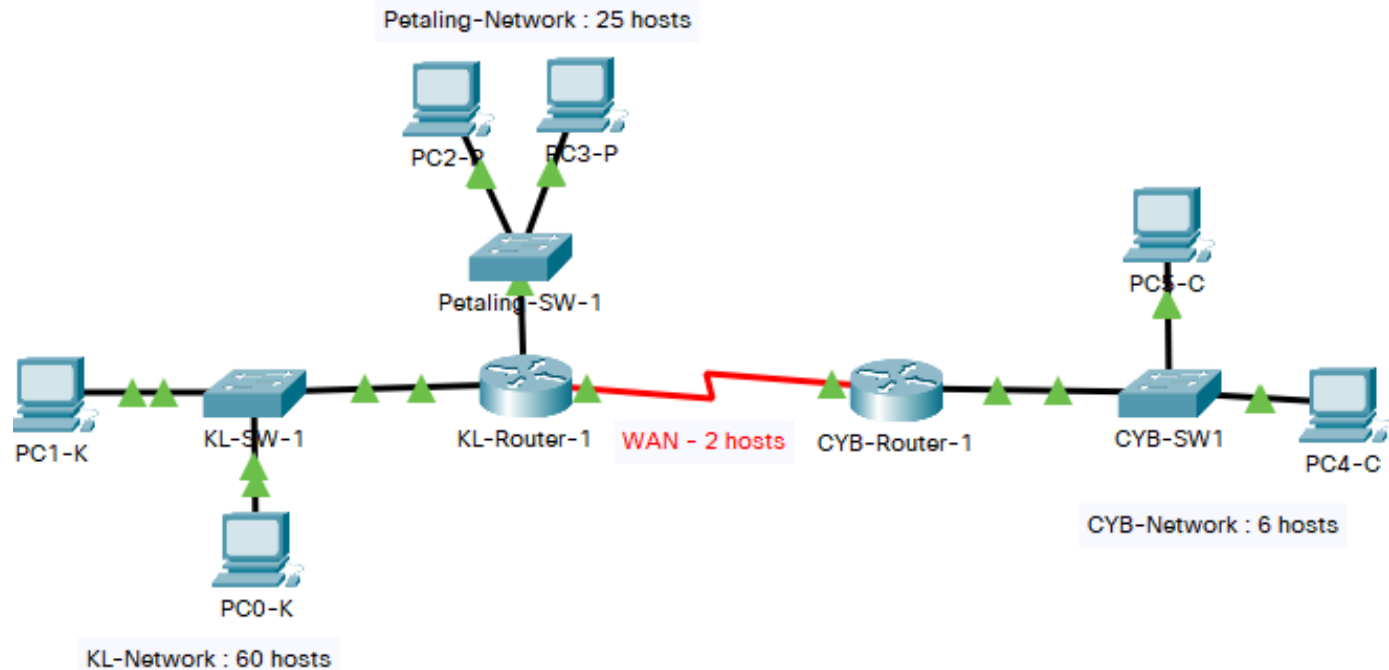


# Layer 2 and Layer 3 Address



# Layer 2 and Layer 3 Address

Given: 192.168.10.0/24

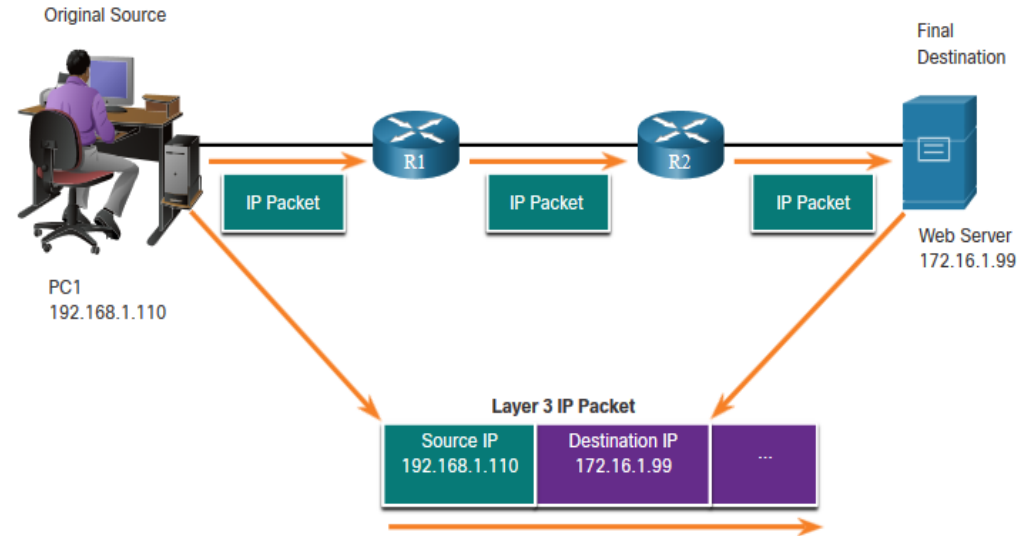


# Layer 3 Logical Address

The IP packet contains two IP addresses:

- **Source IP address** - The IP address of the sending device, original source of the packet.
- **Destination IP address** - The IP address of the receiving device, final destination of the packet.

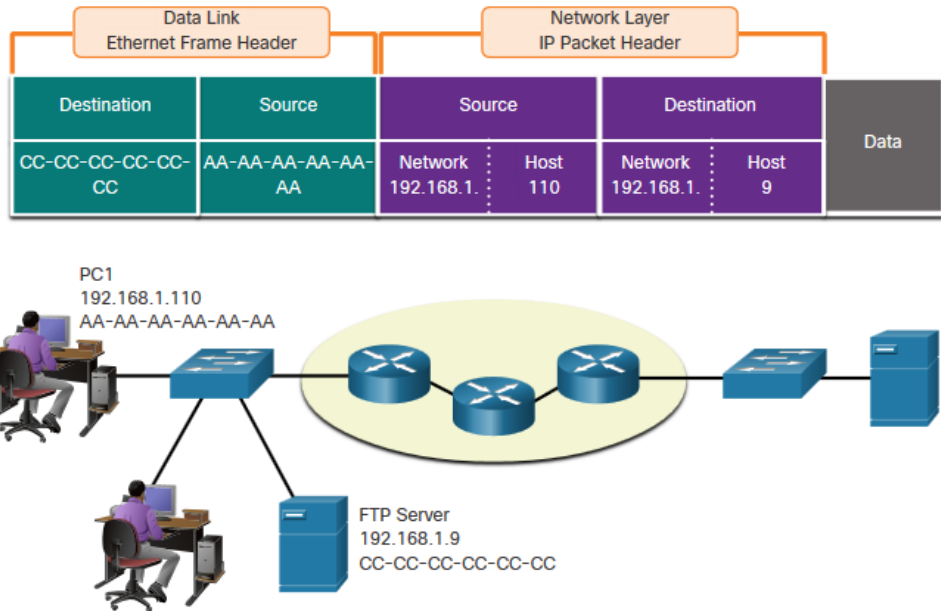
These addresses may be on the same link or remote.



# Devices on the Same Network

When **devices are on the same** network the source and destination will have the same number in network portion of the address.

- PC1 – 192.168.1.110
- FTP Server – 192.168.1.9

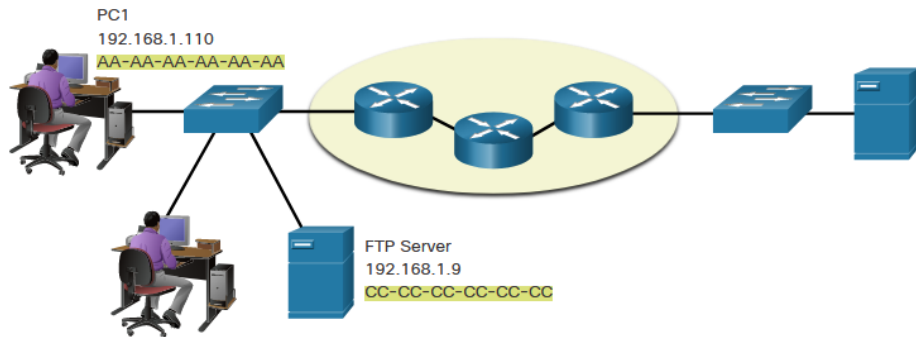
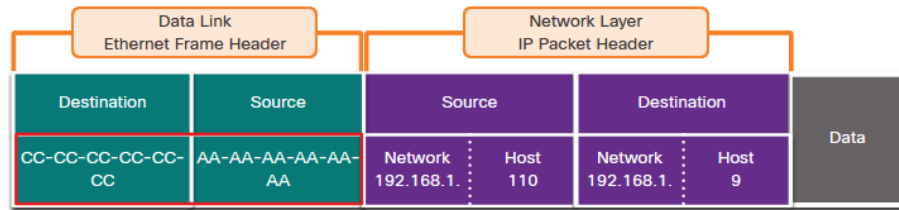


# Role of the Data Link Layer Addresses: Same IP Network

When devices are on the same **Ethernet network** the data link frame will use the actual **MAC address** of the destination NIC.

MAC addresses are physically embedded into the Ethernet NIC and are local addressing.

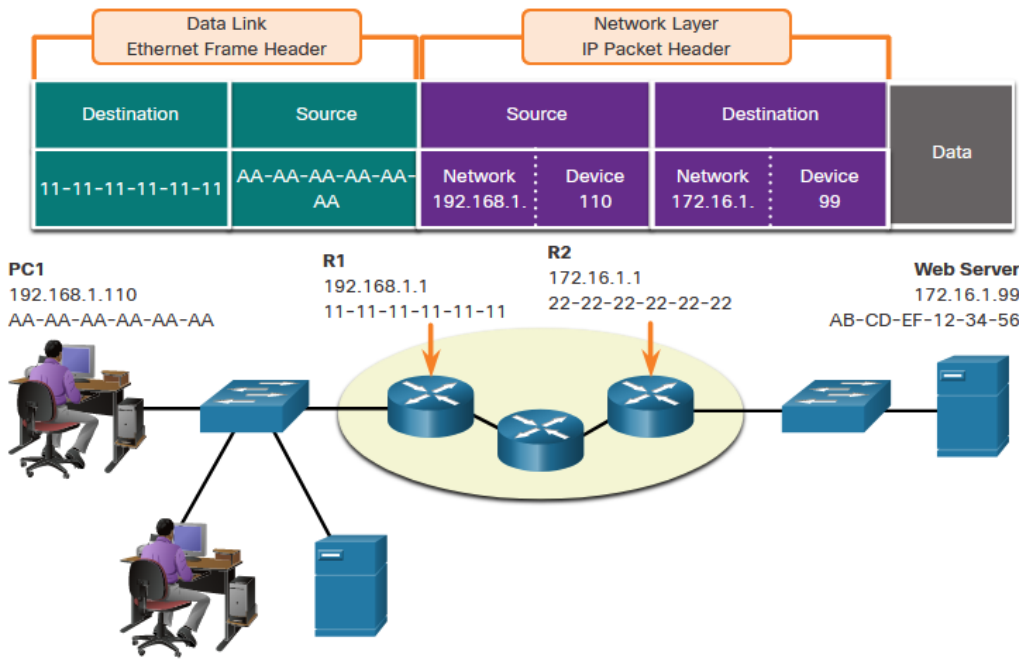
- The **Source MAC** address will be that of the originator on the link.
- The **Destination MAC** address will always be on the same link as the source, even if the ultimate destination is remote.





# Devices on a Remote Network

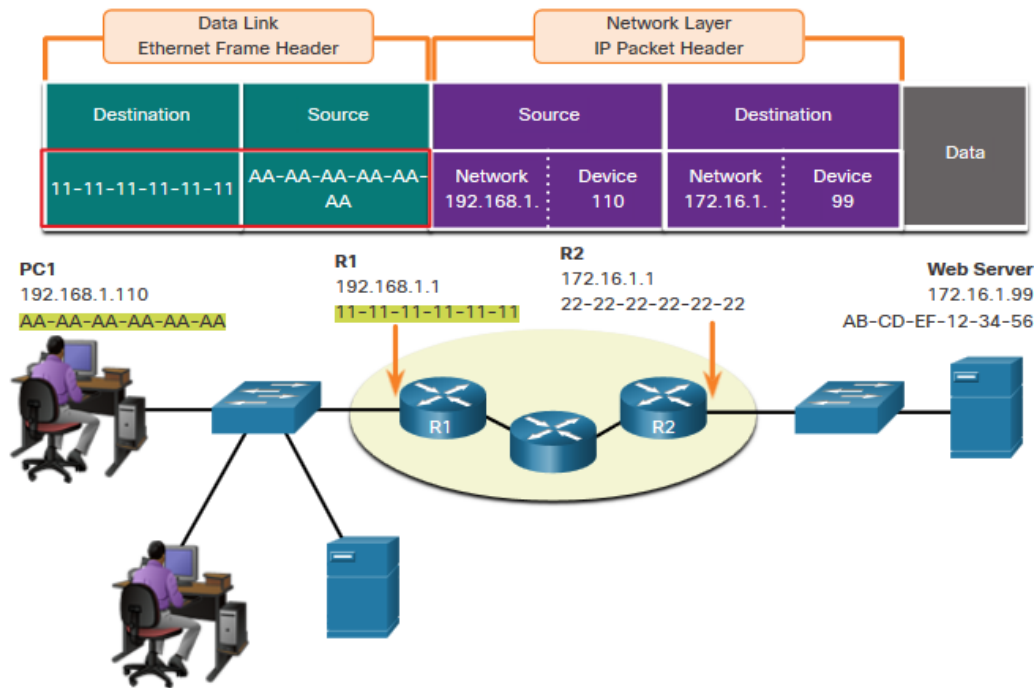
- What happens when the actual (ultimate) destination is not on the same LAN and is remote?
- What happens when PC1 tries to reach the Web Server?
- Does this impact the network and data link layers?



# Role of the Data Link Layer Addresses: Different IP Networks

When the final destination is remote, Layer 3 will provide Layer 2 with the local **default gateway IP address**, also known as the router address.

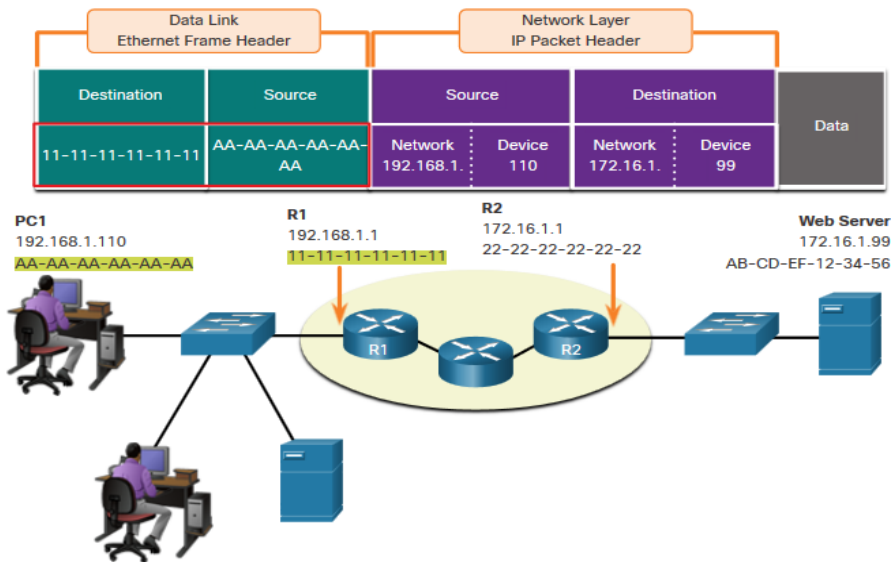
- The **default gateway (DGW)** is the **router interface IP address** that is part of this LAN and will be the “door” or “gateway” to all other remote locations.
- All devices on the LAN must be told about this address or their traffic will be confined to the LAN only.
- Once Layer 2 on PC1 forwards to the default gateway (Router), **the router then can start the routing process** of getting the information to actual destination.



## Role of the Data Link Layer Addresses: Different IP Networks (Cont.)

- The data link addressing is local addressing so it will have a source and destination for each link.
- The MAC addressing for the first segment is :
  - Source – AA-AA-AA-AA-AA-AA (PC1) Sends the frame.
  - Destination – 11-11-11-11-11-11 (R1-Default Gateway MAC) Receives the frame.

**Note:** While the **L2 local addressing will change from link to link or hop to hop**, the L3 addressing remains the same.



- <https://www.youtube.com/watch?v=xaKvGnnuYmk>

# Summary

# Summary of Main Teaching Points

- 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.



# Q & A

# What To Expect Next Week

## In Class

- Application Layer



