# TK35303

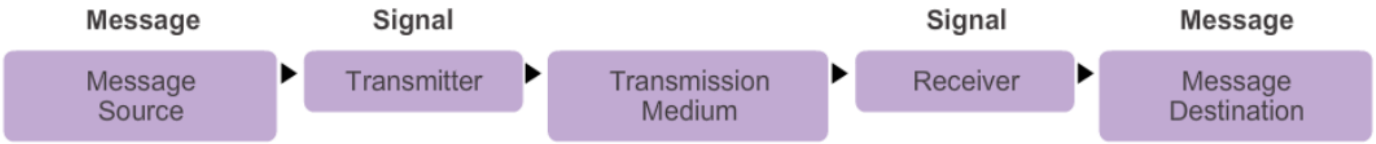
# Computer Networks

## #2 Communication Protocol

Susmini Indriani Lestariningati, M.T

# Rules of Communication

- Human Communication

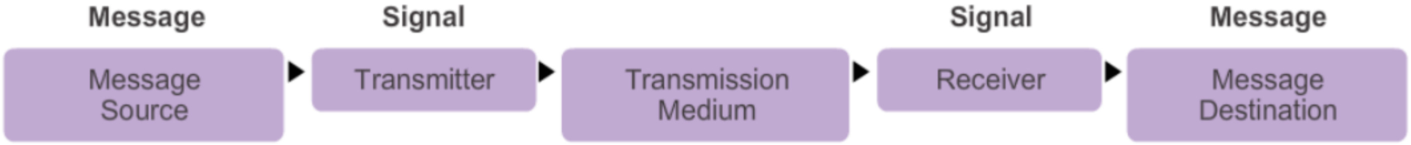


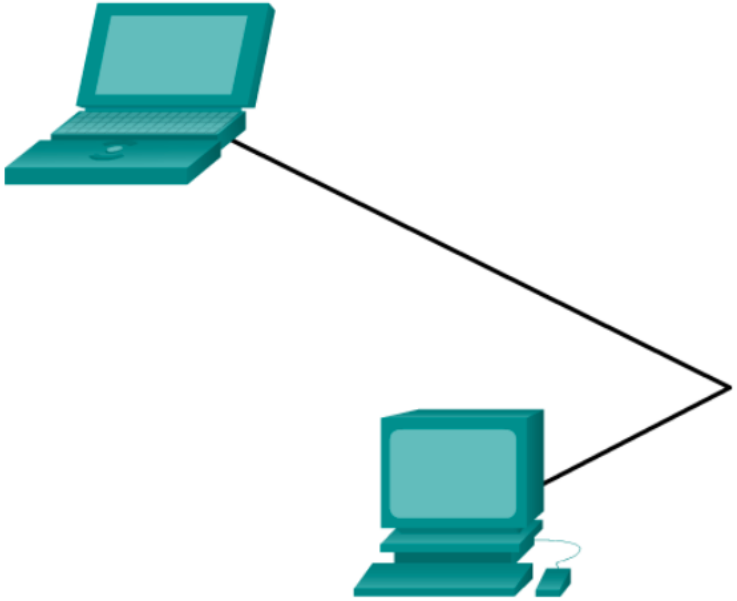
Message | Signal | | Signal | Message

Message Source → Transmitter → Transmission Medium → Receiver → Message Destination

# Rules of Communication

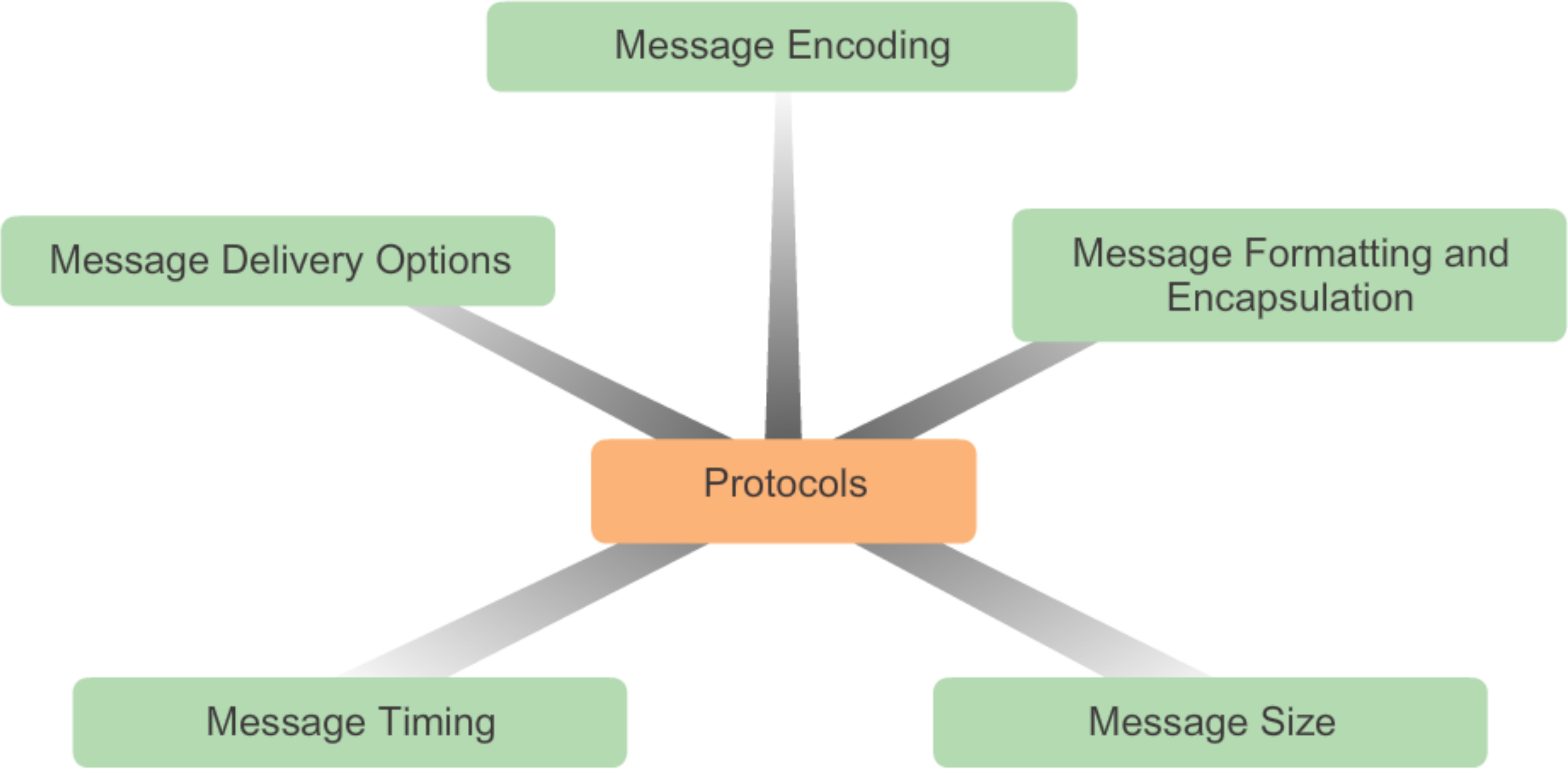
- Computer Communication





# Rules of Communication

- Before communicating with one another, individuals must use established rules or agreements to govern the conversation.
- 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.
- 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**



Message Encoding

Message Delivery Options

Message Formatting and Encapsulation

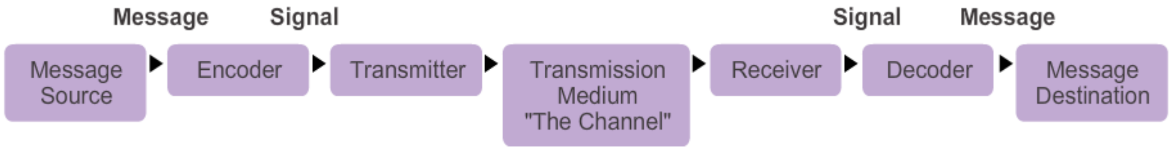
Protocols

Message Timing

Message Size

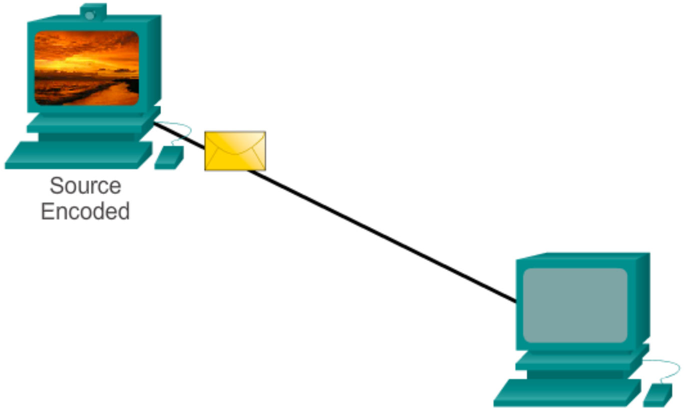
# Message Encoding

- 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.



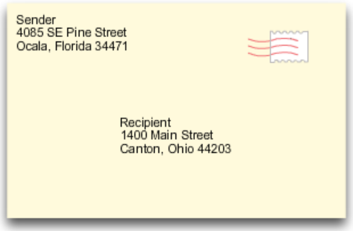
Message Signal Signal Message

Message Source ▶ Encoder ▶ Transmitter ▶ Transmission Medium "The Channel" ▶ Receiver ▶ Decoder ▶ Message Destination



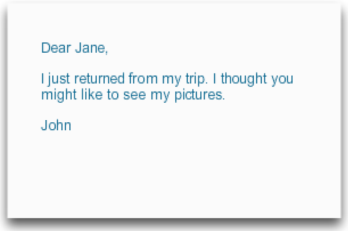
# Message Formatting and Encapsulation

- 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.



Sender
4085 SE Pine Street
Ocala, Florida 34471

Recipient
1400 Main Street
Canton, Ohio 44203



Dear Jane,

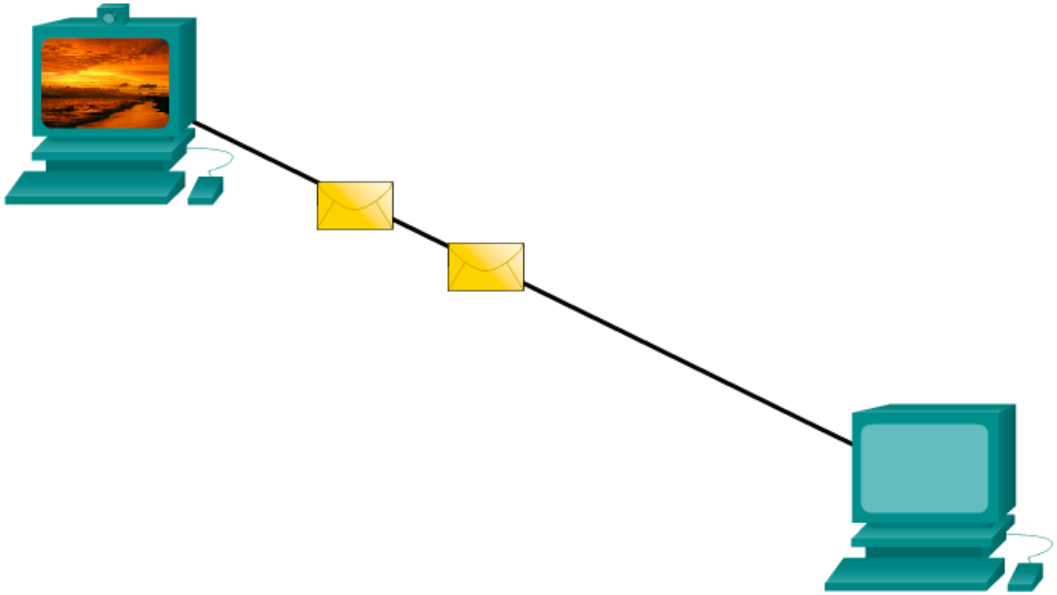
I just returned from my trip. I thought you might like to see my pictures.

John

| 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 | |

# 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, as shown in Figure . 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.



# Message Timing

- **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.

- **Access Method**

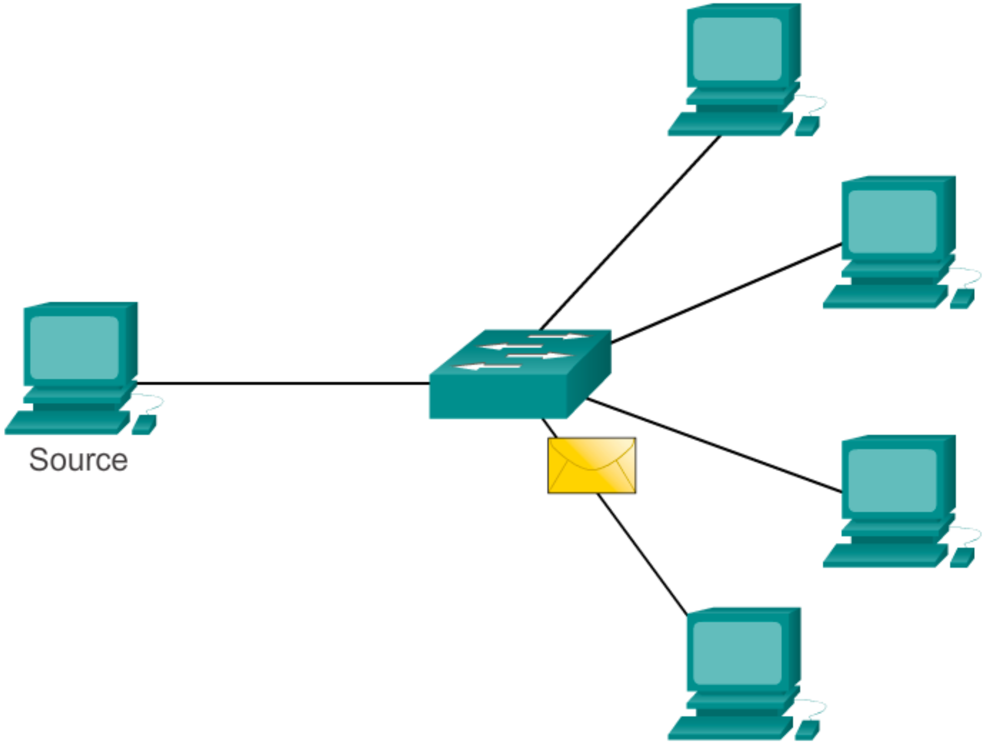
  Access method determines when someone is able to send a message.

- **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.

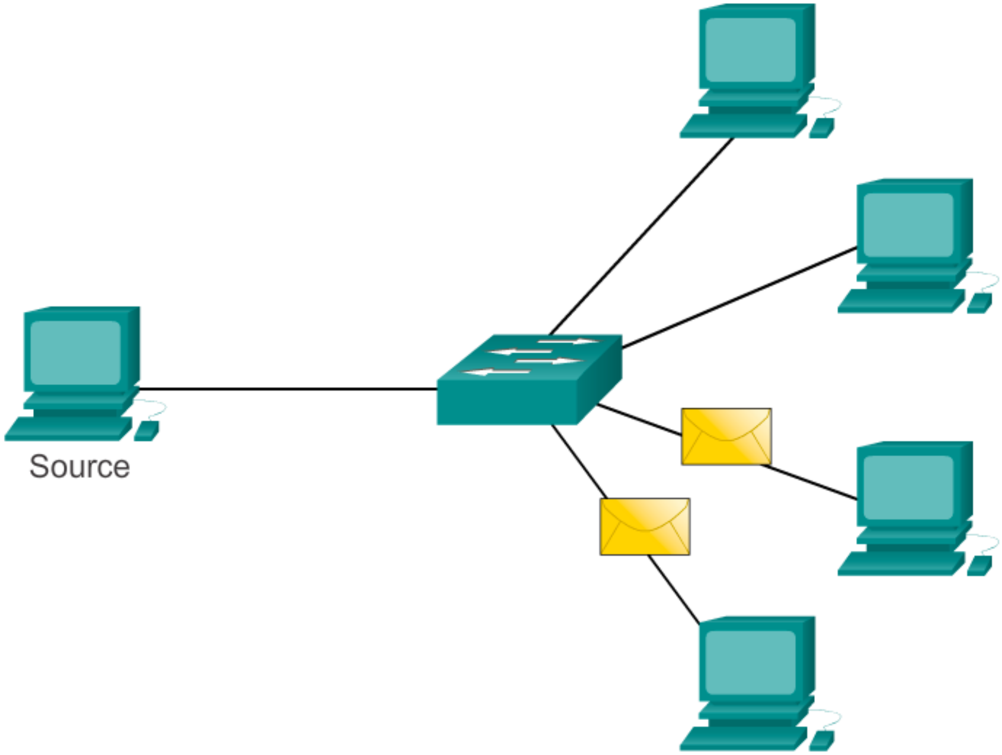
# Message Delivery Option (1)

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



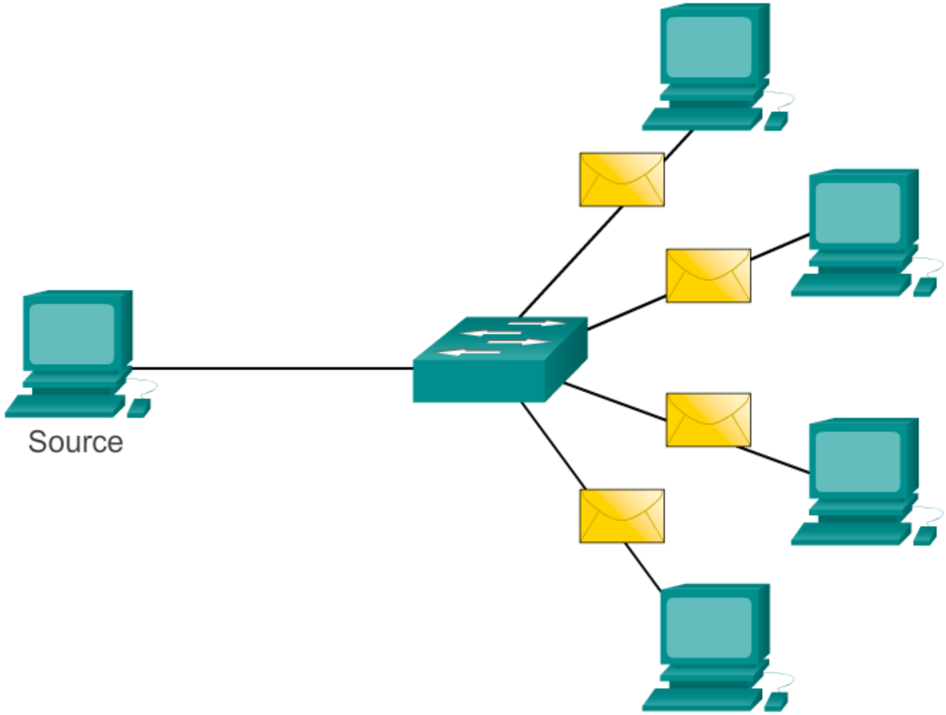
# Message Delivery Option (2)

- 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.



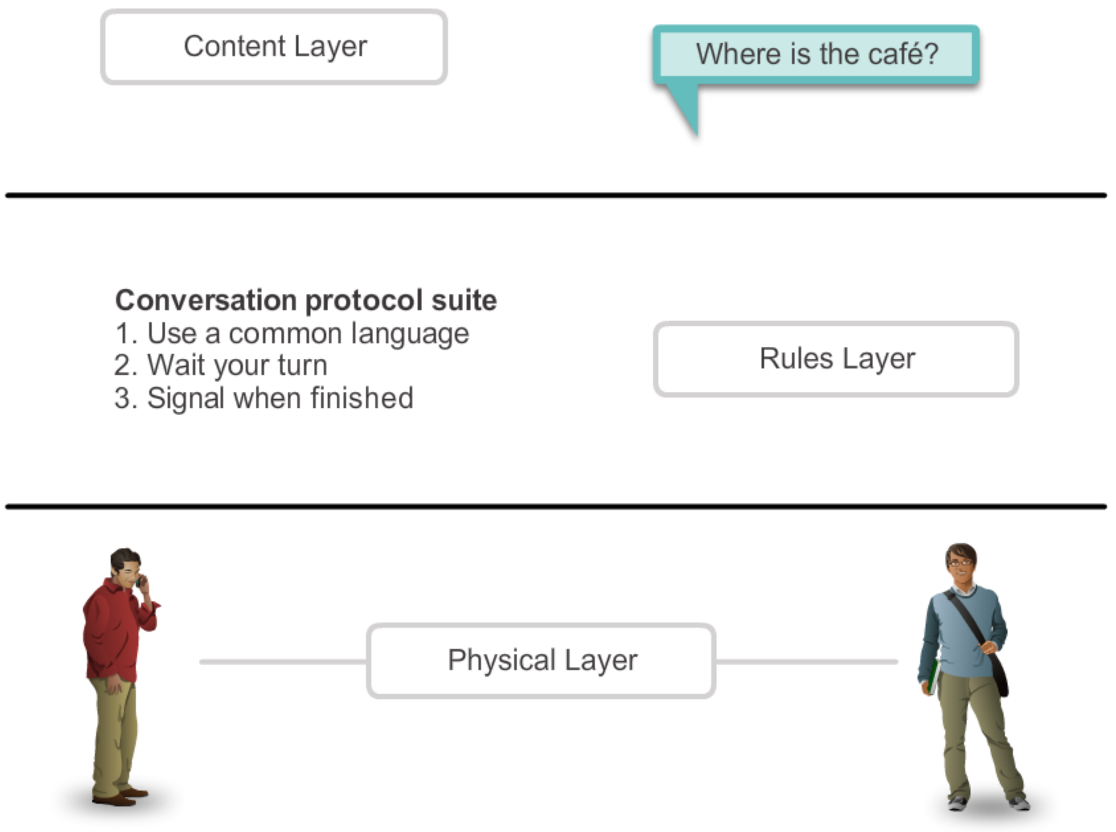
# Message Delivery Option (3)

- 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.



# Network Protocols and Standards

## Protocols: Rules that Govern Communications



Content Layer

Where is the café?

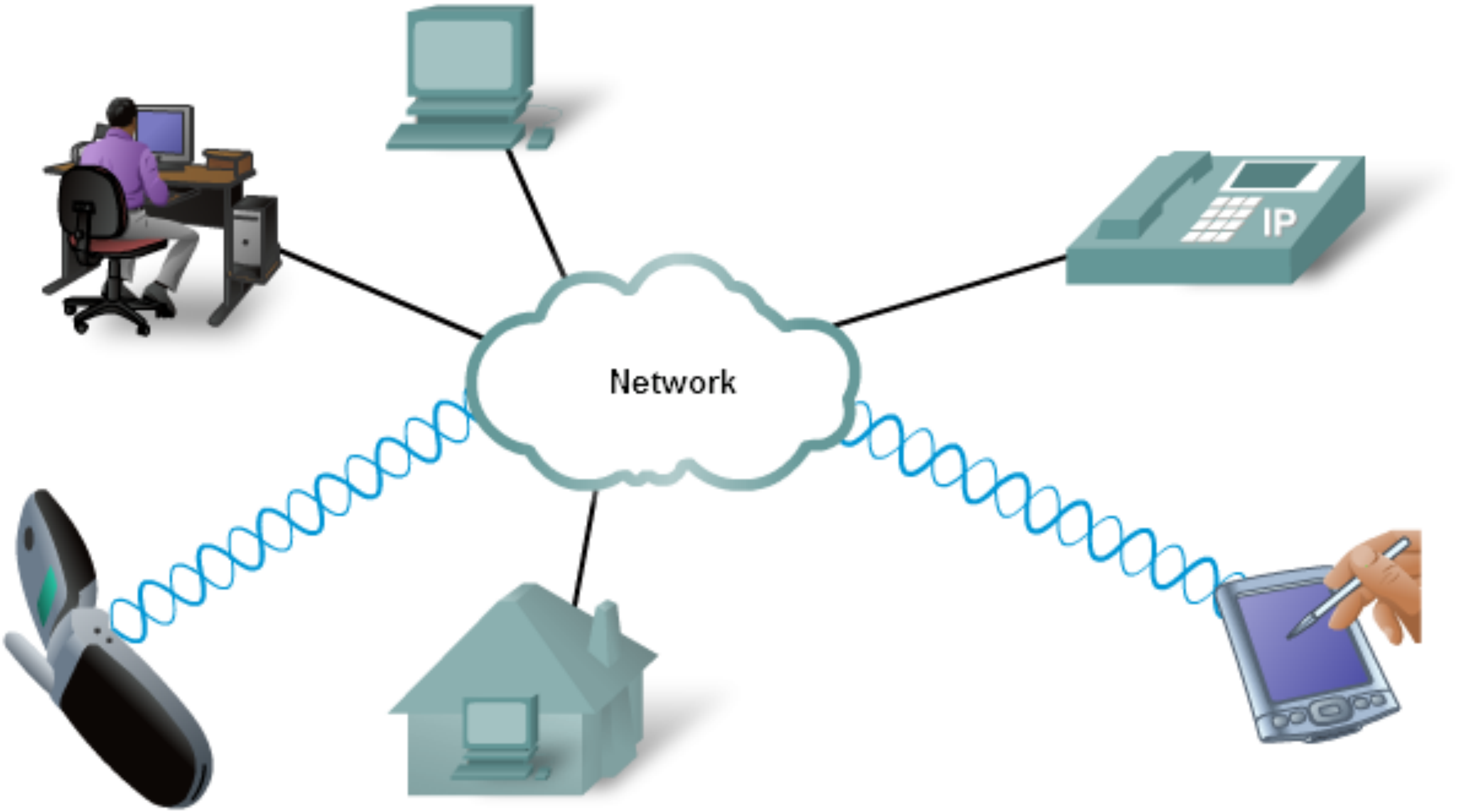
**Conversation protocol suite**
1. Use a common language
2. Wait your turn
3. Signal when finished

Rules Layer

Physical Layer

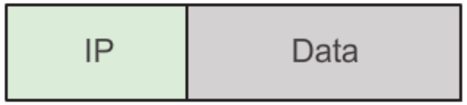
Protocol suites are sets of rules that work together to help solve a problem.

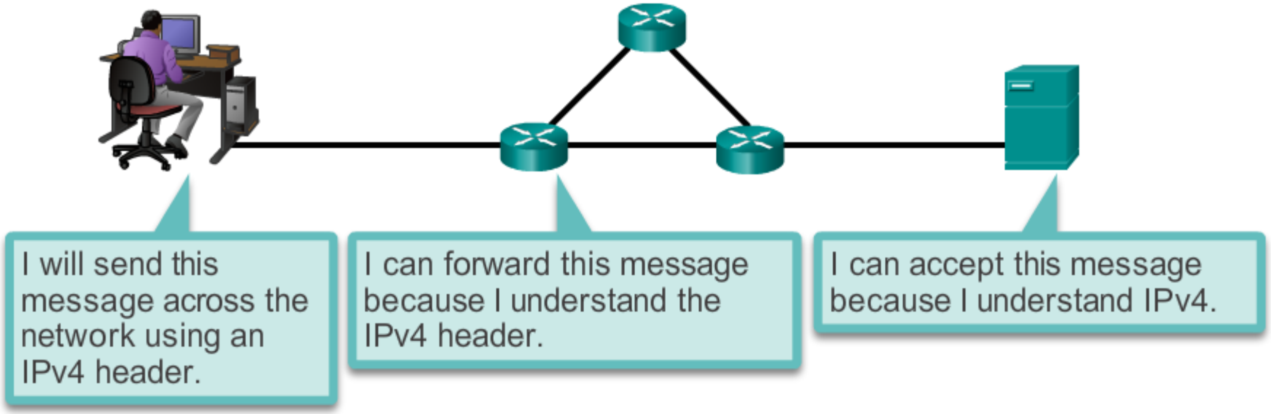
Many diverse types of devices can communicate using the same sets of protocols. This is because protocols specify network functionality, not the underlying technology to support this functionality.



# Protocols

- For devices to successfully communicate, a network protocol suite must describe precise requirements and interactions. Networking protocols define a common format and set of rules for exchanging messages between devices.
- The figures illustrate networking protocols that describe the following processes:
    - How the message is formatted or structured, as shown in Figure



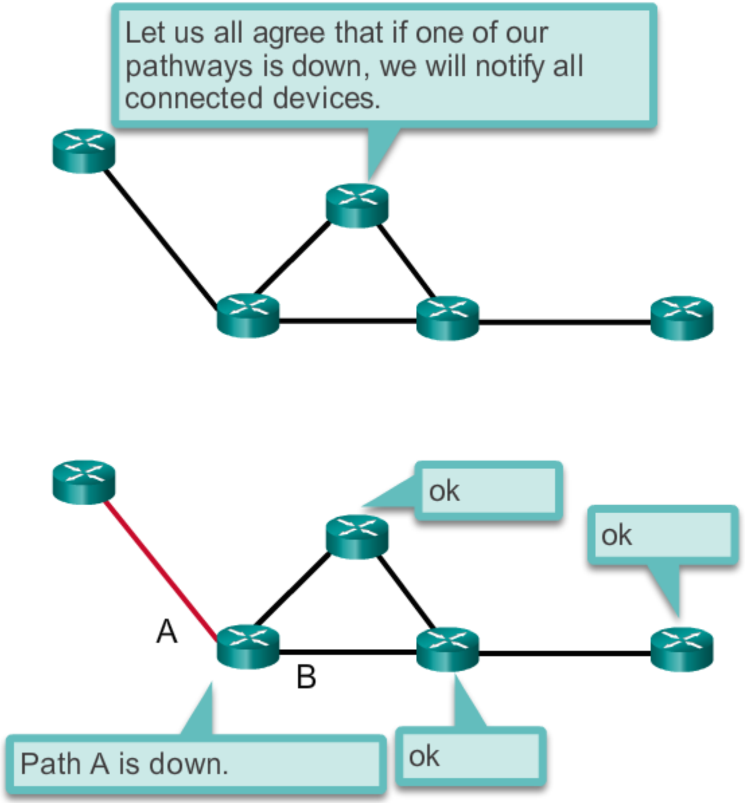


I will send this message across the network using an IPv4 header.

I can forward this message because I understand the IPv4 header.

I can accept this message because I understand IPv4.

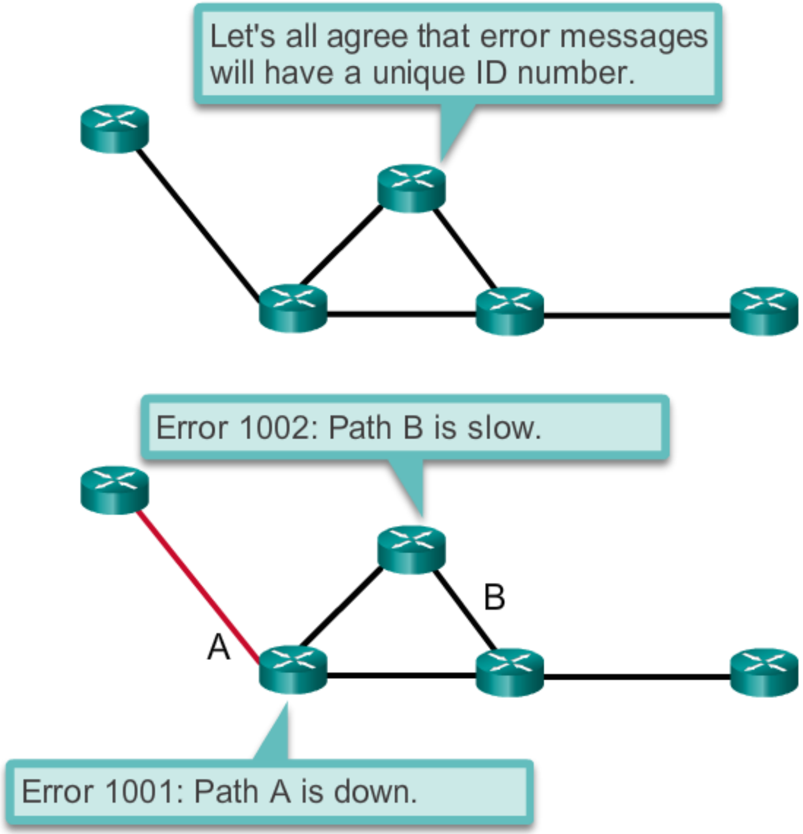
- The process by which networking devices share information about pathways with other networks



Let us all agree that if one of our pathways is down, we will notify all connected devices.

Path A is down.

- How and when error and system messages are passed between devices

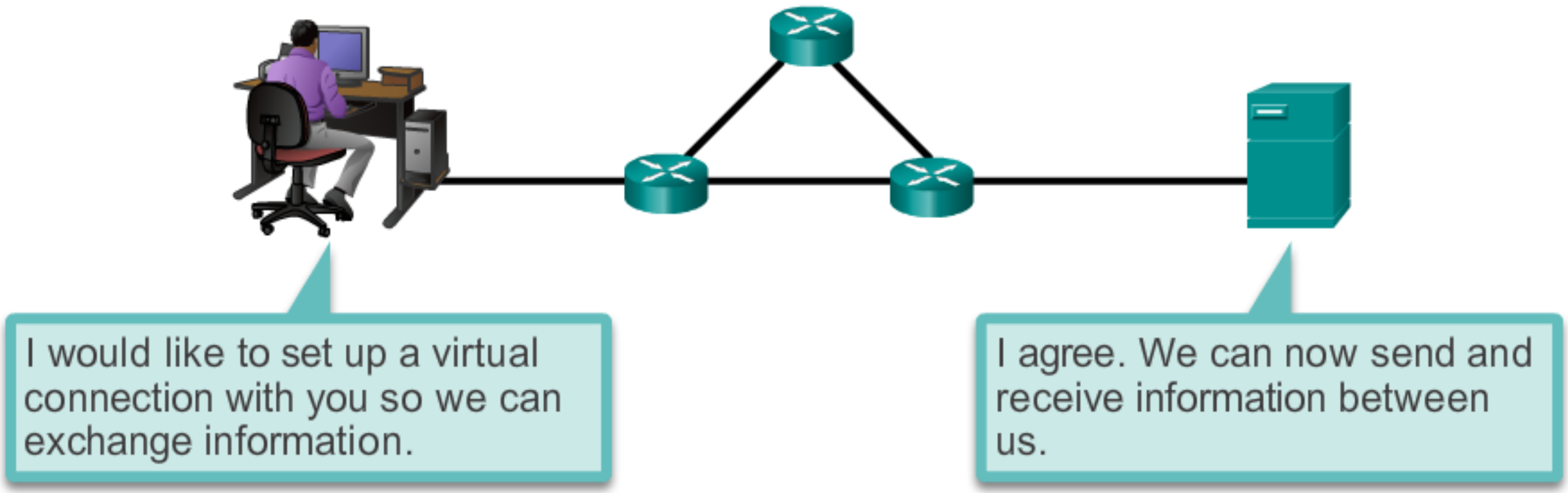


Let's all agree that error messages will have a unique ID number.

Error 1002: Path B is slow.

Error 1001: Path A is down.

- The setup and termination of data transfer sessions


I would like to set up a virtual connection with you so we can exchange information.
I agree. We can now send and receive information between us.

- There are two basic types of networking models:
  - Protocol models
  - Reference models.

# Protocol Model

- A protocol model provides a model that closely matches the structure of a particular protocol suite.
  - The hierarchical set of related protocols in a suite typically represents all the functionality required to interface the human network with the data network.
  - The TCP/IP model is a protocol model because it describes the functions that occur at each layer of protocols within the TCP/IP suite.

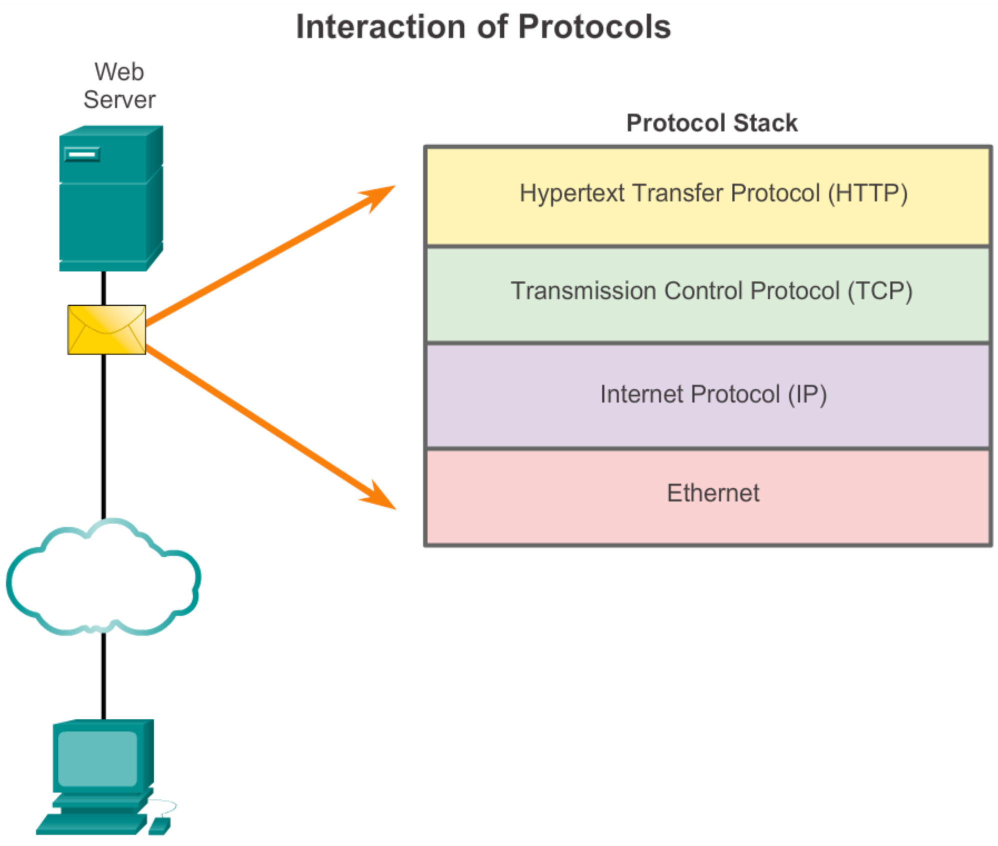
# Reference Model

- A reference model provides a common reference for maintaining consistency within all types of network protocols and services.
- A reference model is not intended to be an implementation specification or to provide a sufficient level of detail to define precisely the services of the network architecture.
- The primary purpose of a reference model is to aid in clearer understanding of the functions and process involved.
- The Open Systems Interconnection (OSI) model is the most widely known internetwork reference model. It is used for data network design, operation specifications, and troubleshooting.

- TCP/IP and OSI models are the primary models used when discussing network functionality, designers of network protocols, services, or devices can create their own models to represent their products.
- Ultimately, designers are required to communicate to the industry by relating their product or service to either the OSI model or the TCP/IP model, or to both.

# Interaction of Protocols

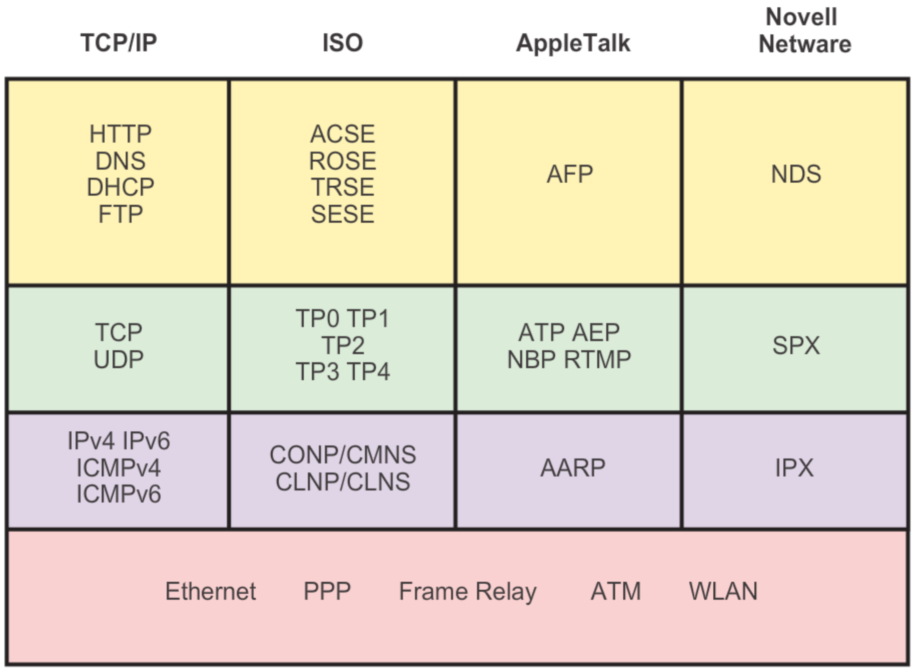
- An example of using the protocol suite in network communications is the interaction between a web server and a web client. This interaction uses a number of protocols and standards in the process of exchanging information between them. The different protocols work together to ensure that the messages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



# Protocol Suites

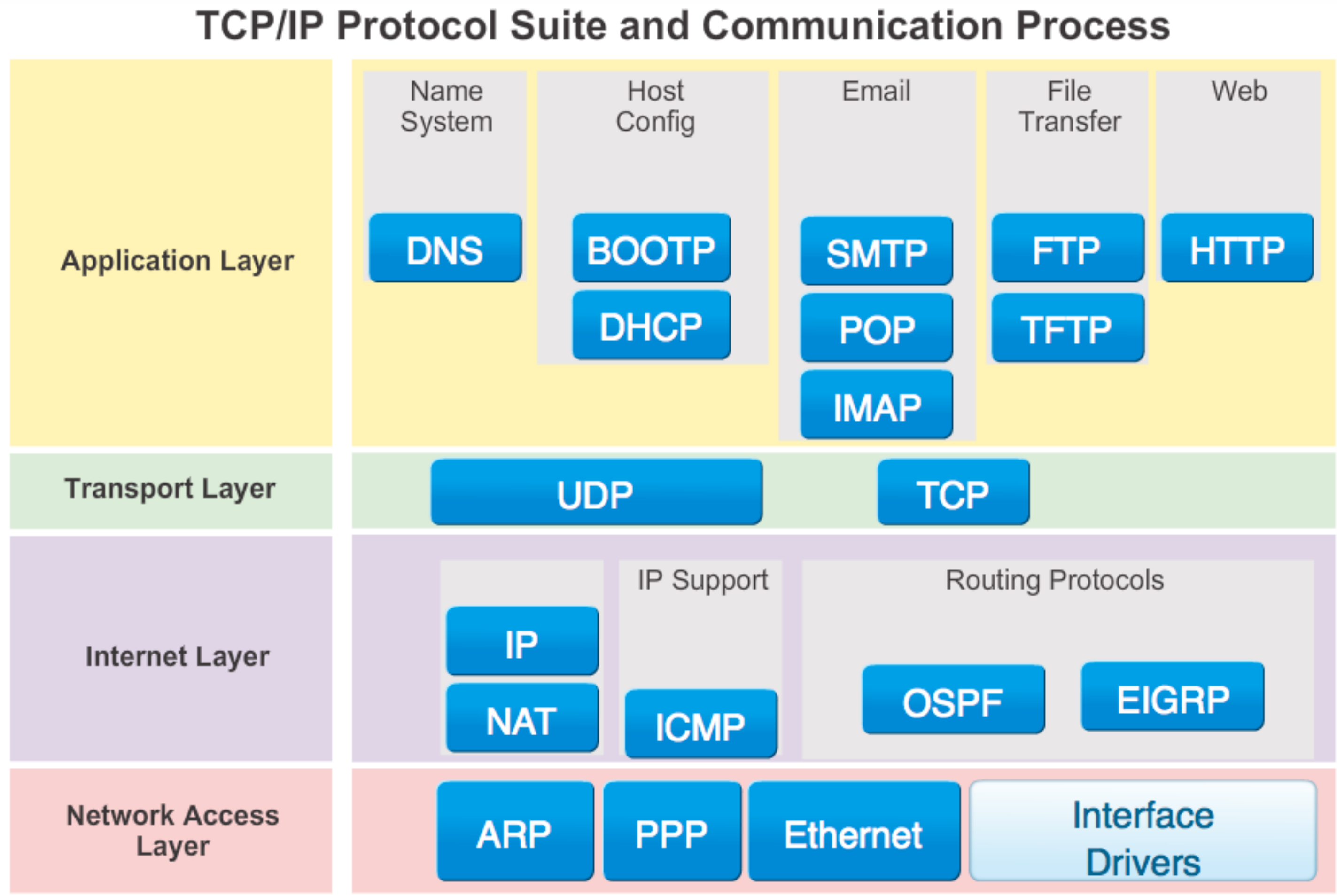
- A protocol suite is a set of protocols that work together to provide comprehensive network communication services. A protocol suite may be specified by a standards organization or developed by a vendor.
- The protocols IP, HTTP, and DHCP are all part of the Internet protocol suite known as Transmission 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.

Protocol Suites and Industry Standards



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

# TCP/IP Protocol Suite and Communication Process



TCP/IP Protocol Suite and Communication Process

Application Layer

Name System: DNS

Host Config: BOOTP, DHCP

Email: SMTP, POP, IMAP

File Transfer: FTP, TFTP

Web: HTTP

Transport Layer

UDP, TCP

Internet Layer

IP, NAT

IP Support: ICMP

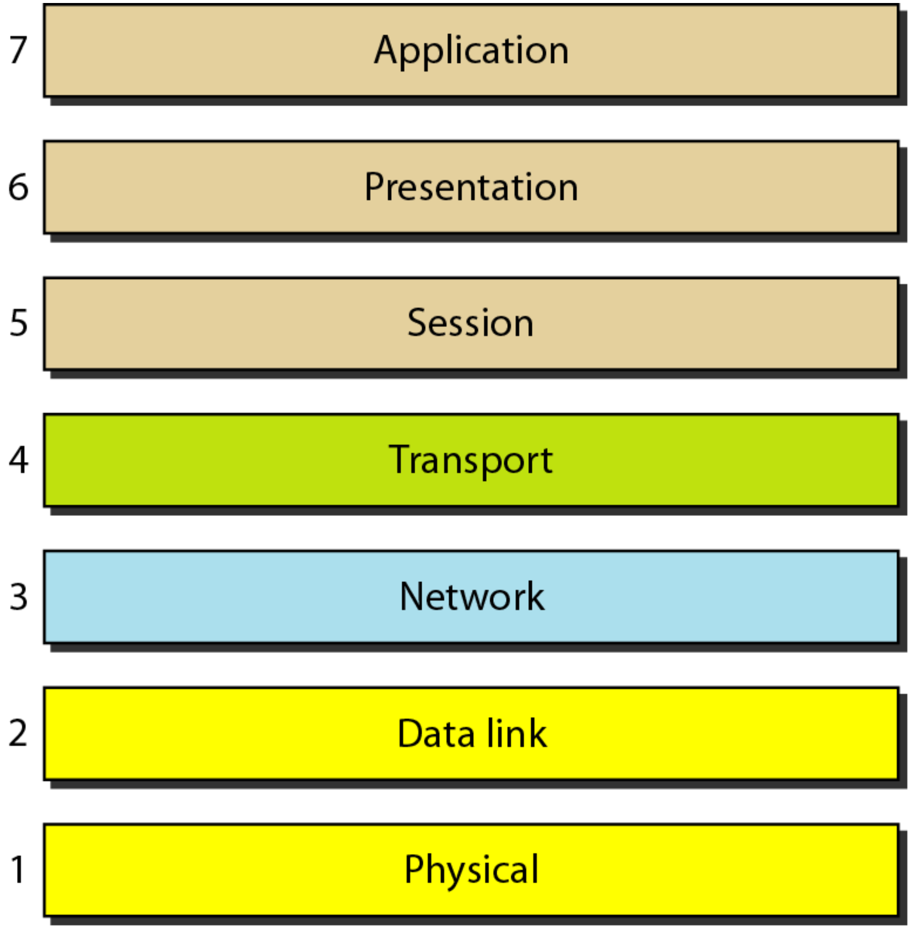
Routing Protocols: OSPF, EIGRP

Network Access Layer

ARP, PPP, Ethernet, Interface Drivers

# Reference Models

- The OSI model is the most widely known internetwork reference model.
- It is used for data network design, operation specifications, and troubleshooting.



7 Application

6 Presentation

5 Session

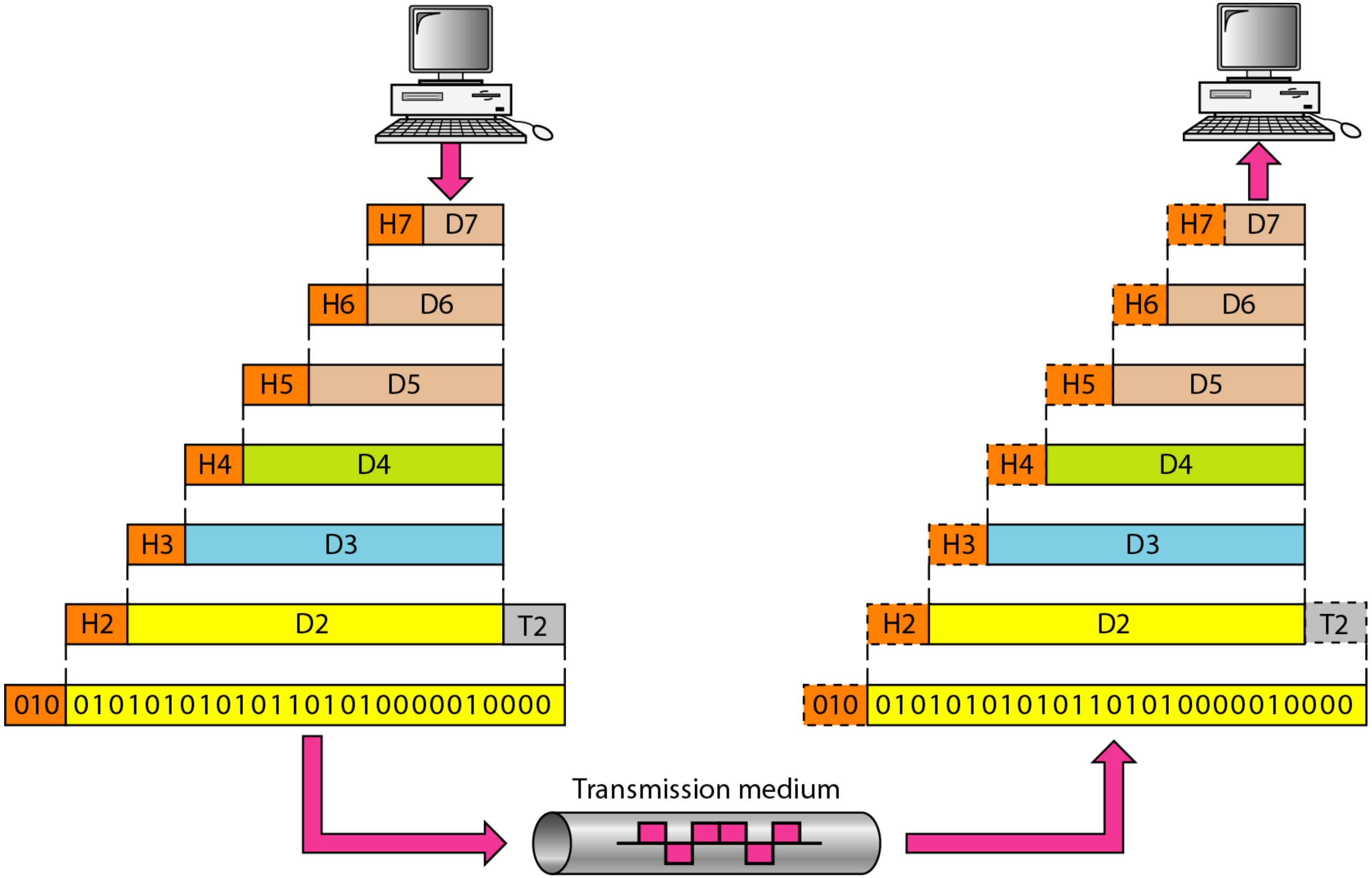
4 Transport

3 Network

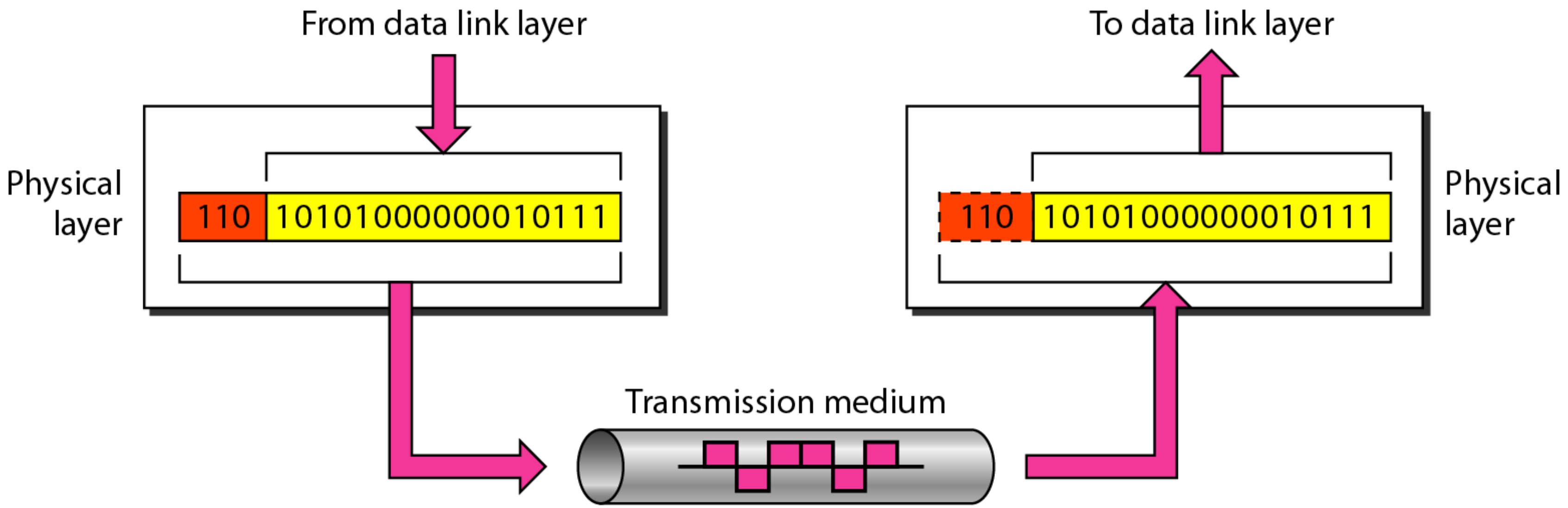
2 Data link

1 Physical

# Exchanging the OSI Model

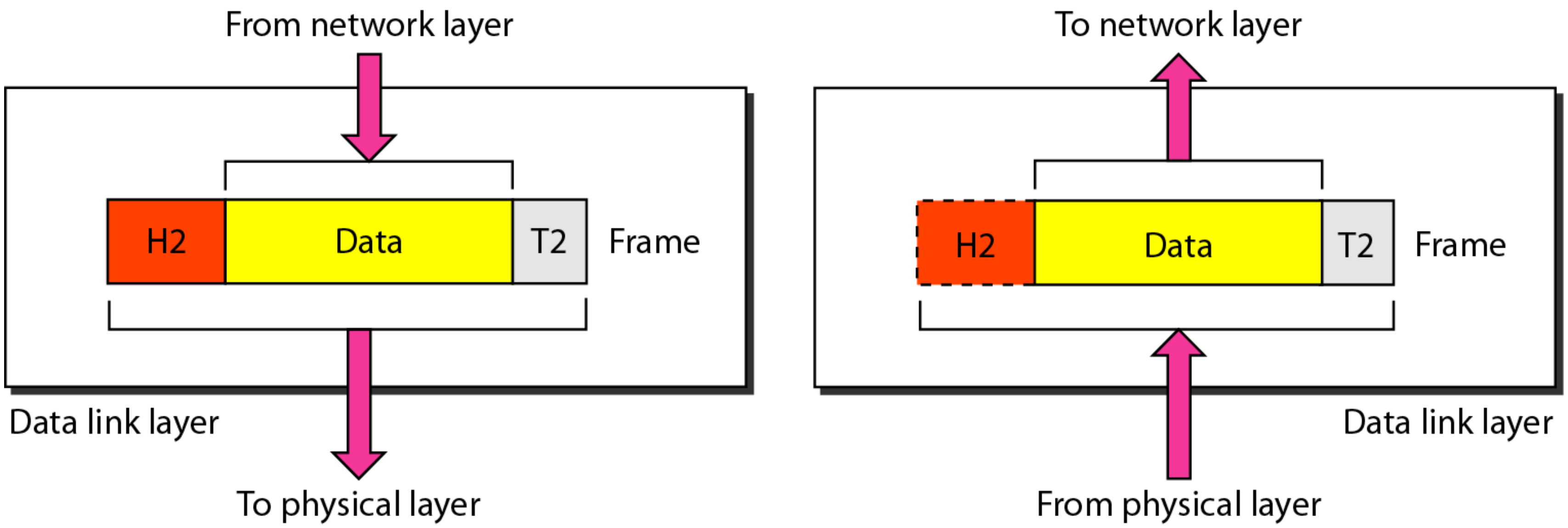


# Physical Layer

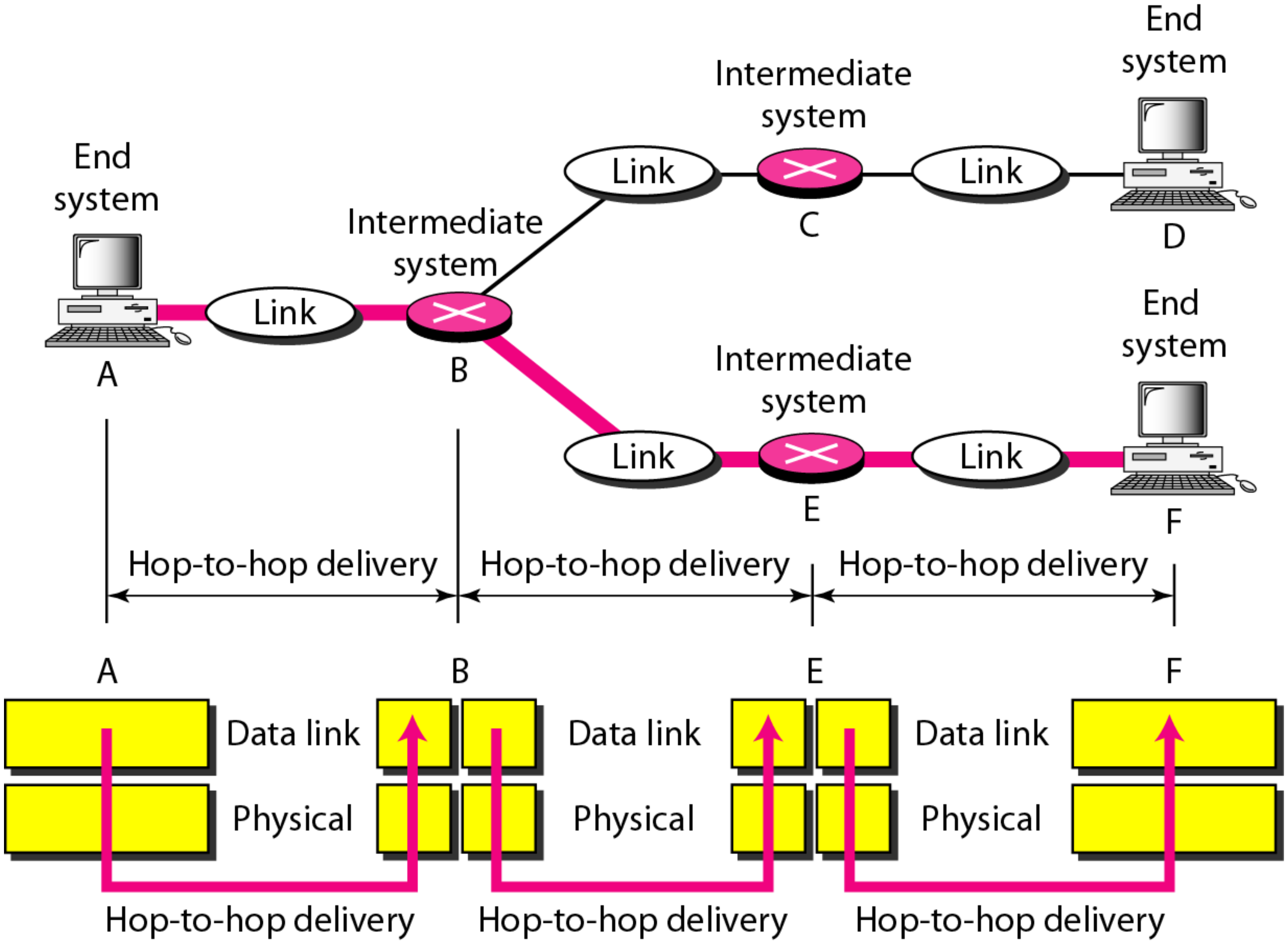


**The physical layer is responsible for movements of individual bits from one hop (node) to the next.**

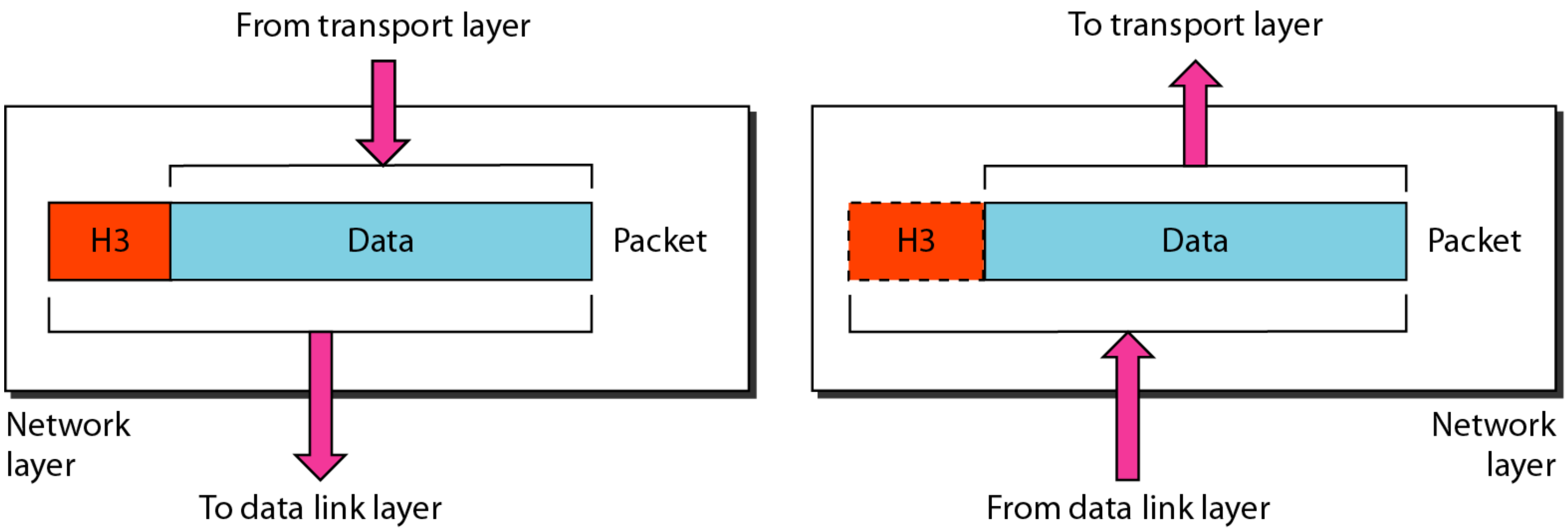
# Data Link Layer



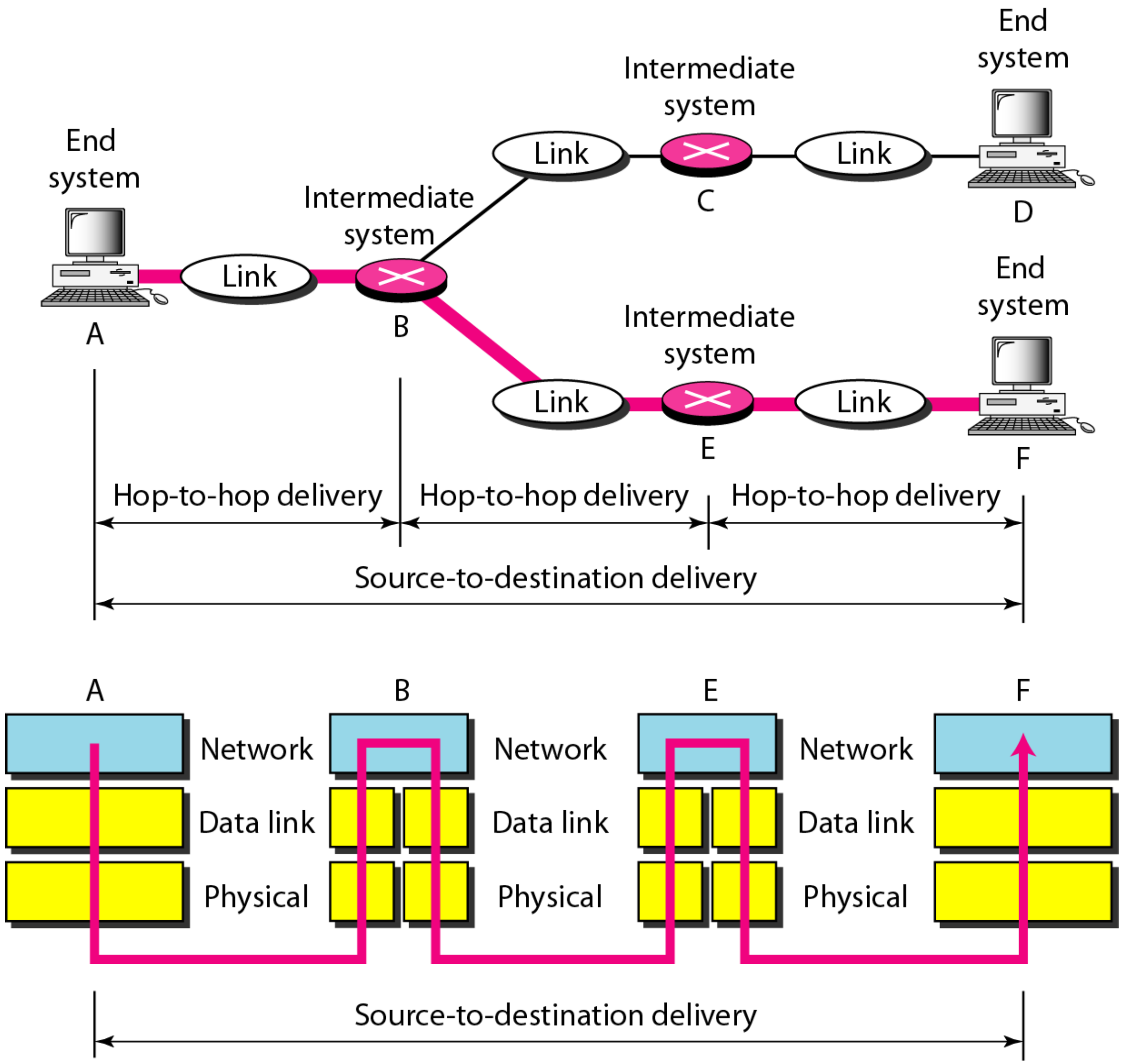
**The data link layer is responsible for moving frames from one hop (node) to the next.**


End system
A
Link
Intermediate system
B
Link
Intermediate system
C
Link
End system
D
Link
Intermediate system
E
Link
End system
F
Hop-to-hop delivery
Hop-to-hop delivery
Hop-to-hop delivery
A
B
E
F
Data link
Physical
Data link
Physical
Data link
Physical
Hop-to-hop delivery
Hop-to-hop delivery
Hop-to-hop delivery

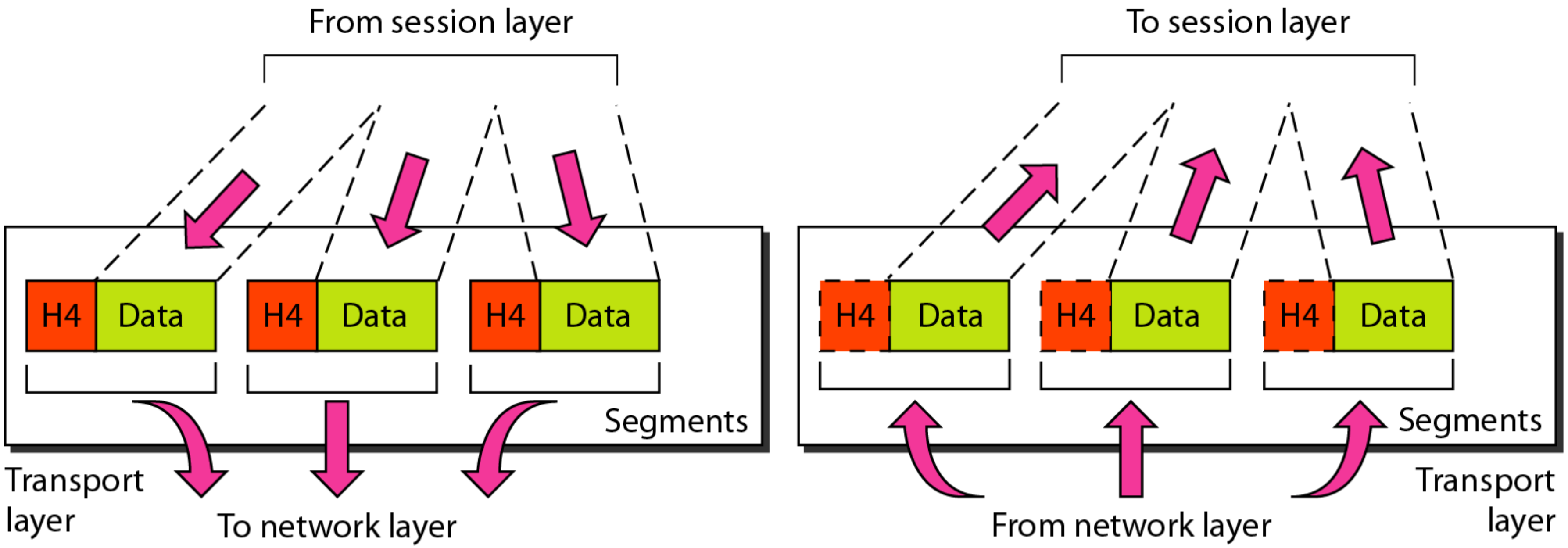
# Network Layer



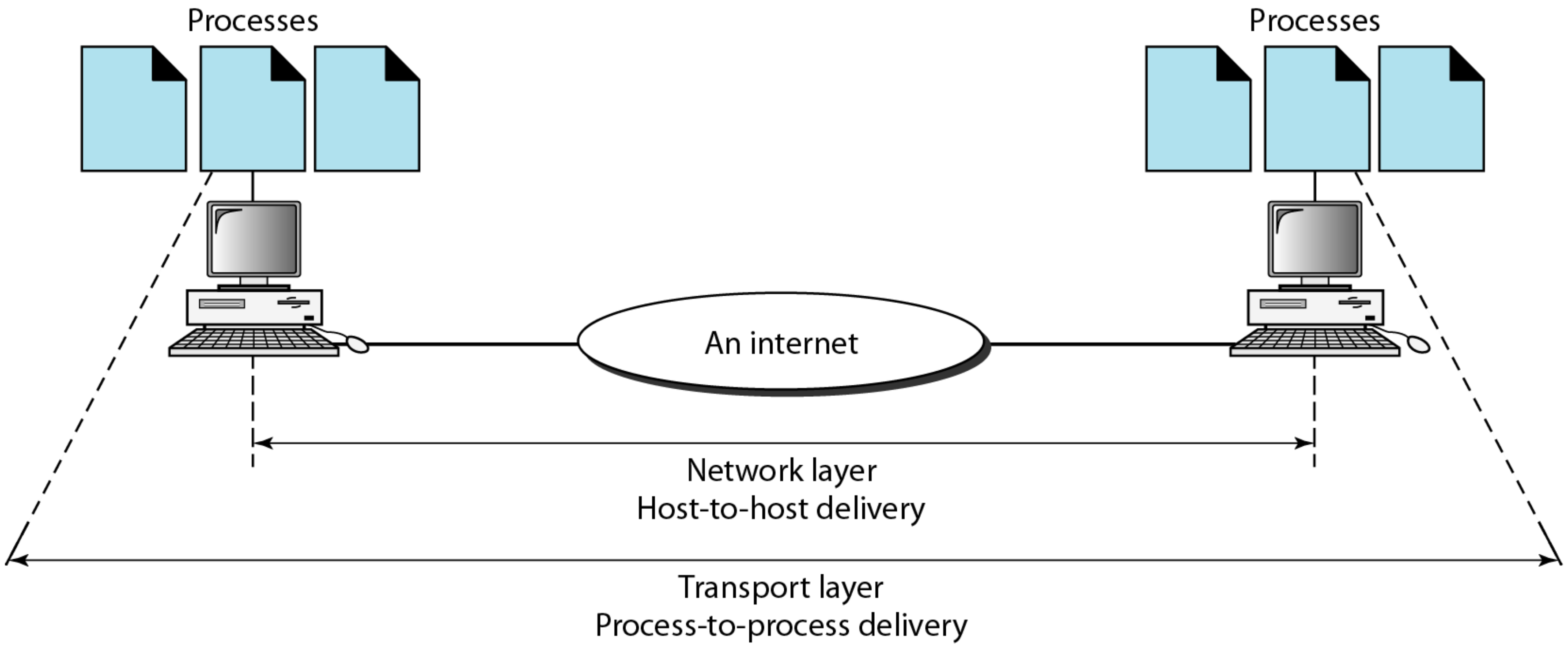
**The network layer is responsible for the delivery of individual packets from the source host to the destination host.**


End system
Intermediate system
Intermediate system
End system
Link
Link
Link
A
B
C
D
Intermediate system
End system
Link
Link
E
F
Hop-to-hop delivery
Hop-to-hop delivery
Hop-to-hop delivery
Source-to-destination delivery
A
B
E
F
Network
Network
Network
Data link
Data link
Data link
Physical
Physical
Physical
Source-to-destination delivery

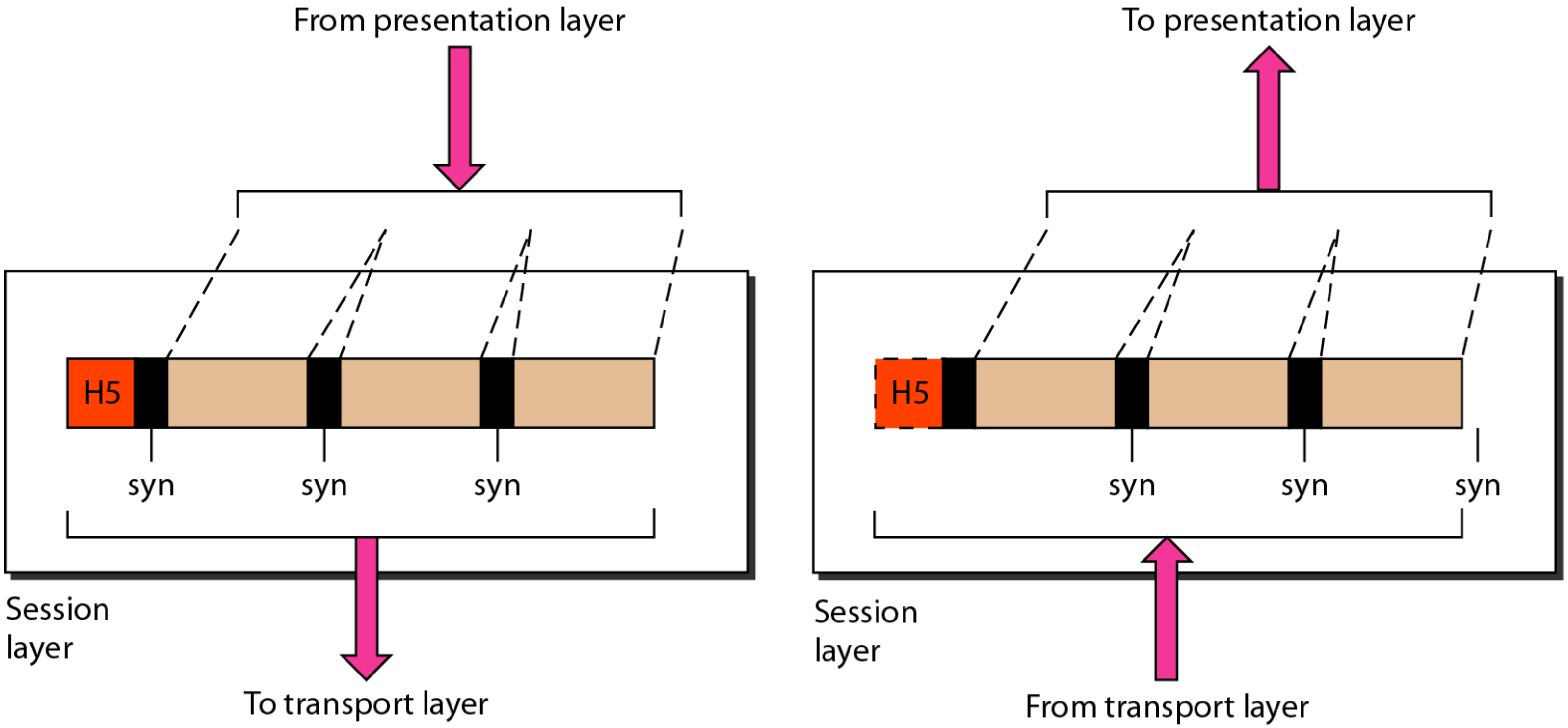
# Transport Layer



**The transport layer is responsible for the delivery of a message from one process to another.**

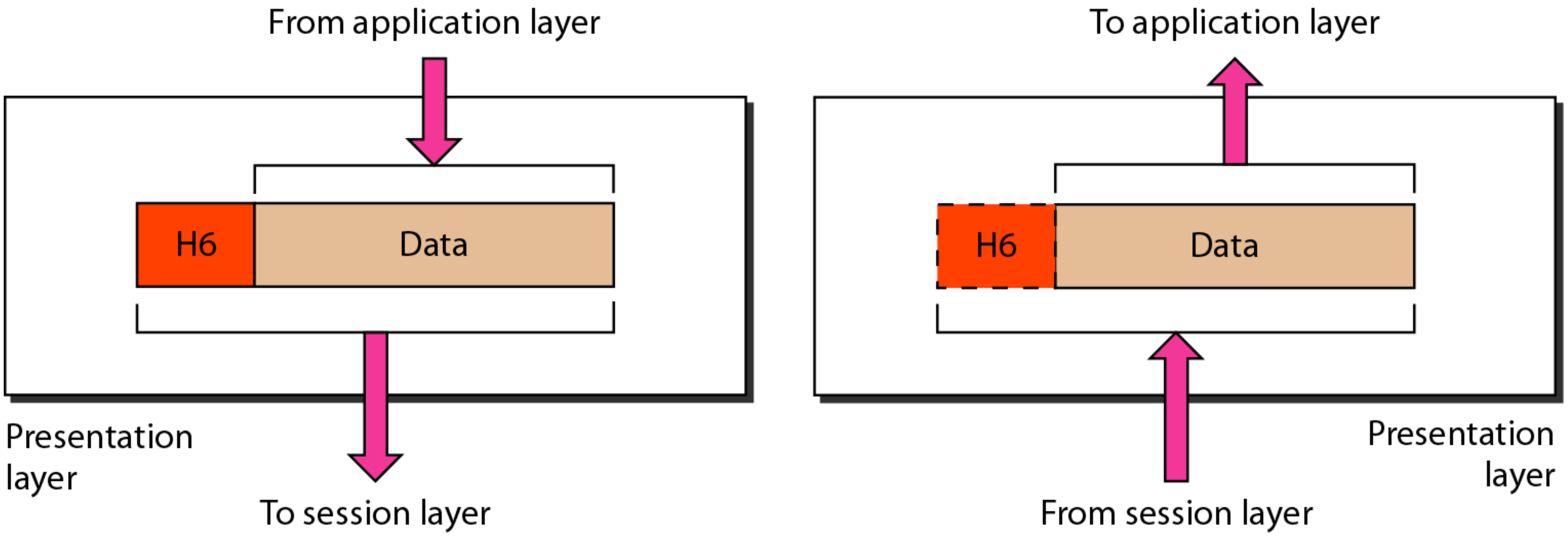

Processes
Processes
An internet
Network layer
Host-to-host delivery
Transport layer
Process-to-process delivery

# Session Layer



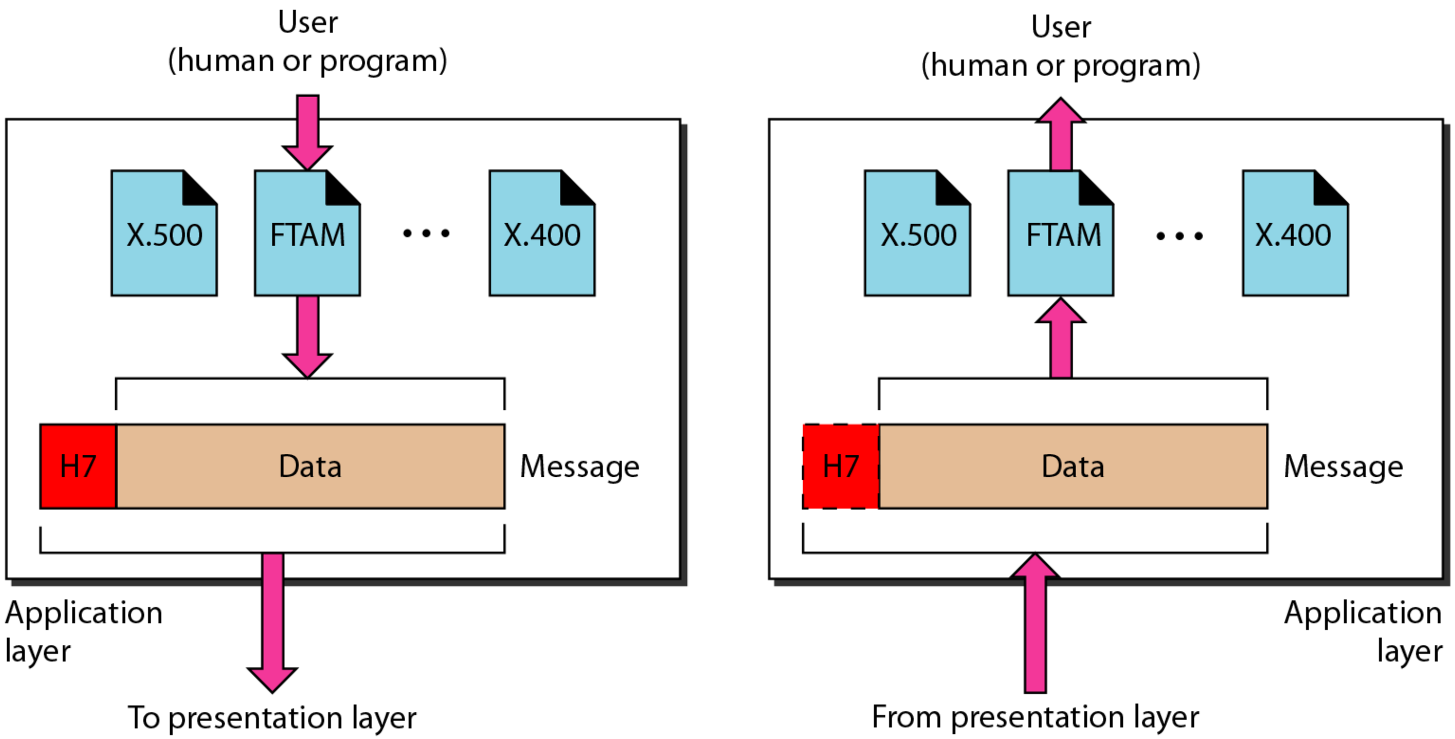
**The session layer is responsible for dialog control and synchronization.**

# Presentation Layer



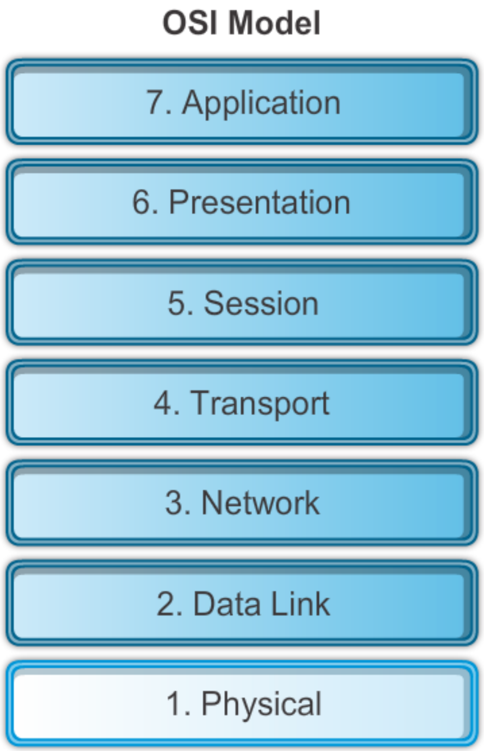
**The presentation layer is responsible for translation, compression, and encryption.**

# Application Layer



**The application layer is responsible for providing services to the user.**

# OSI Reference Model



**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.

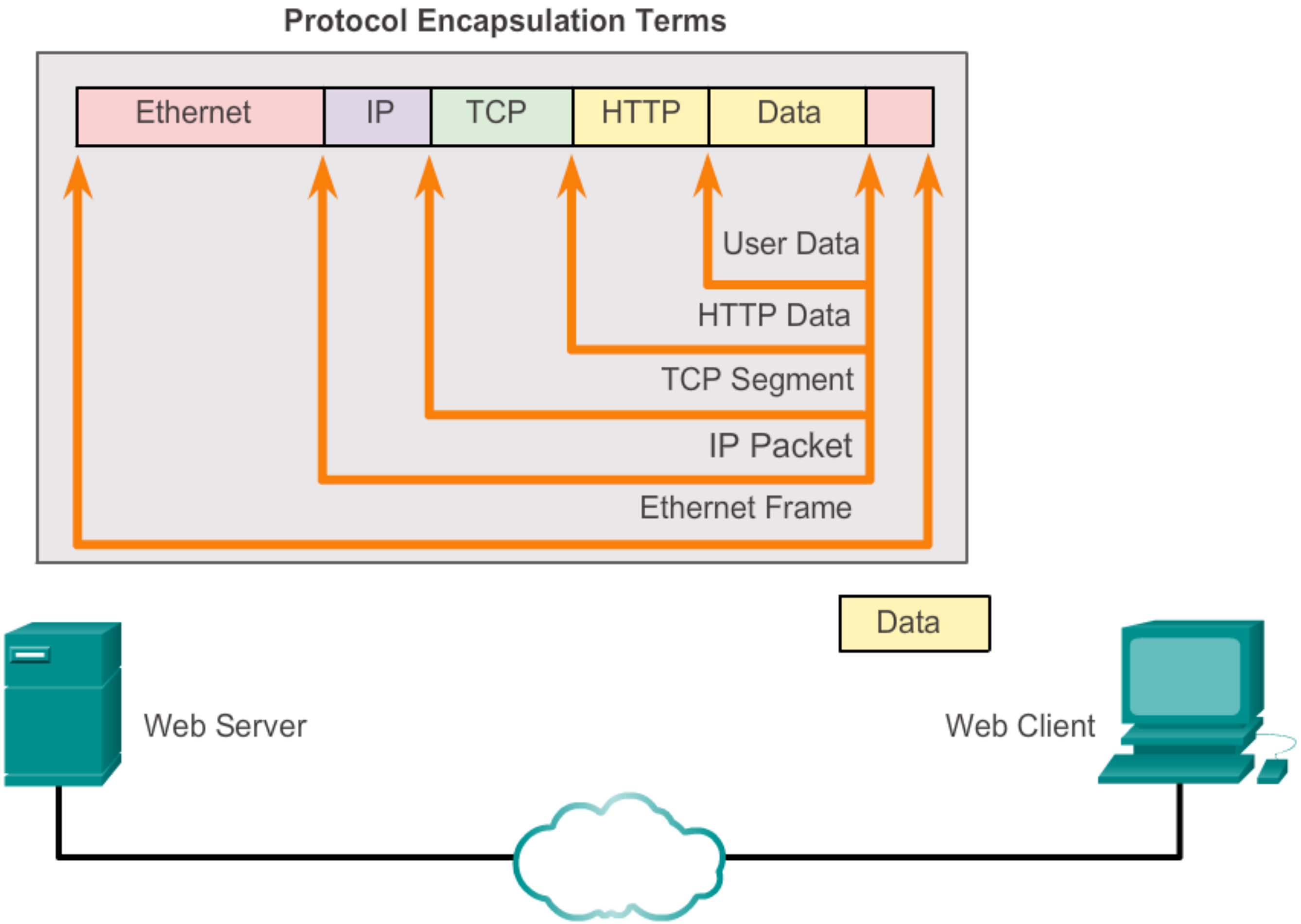
**Application**

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

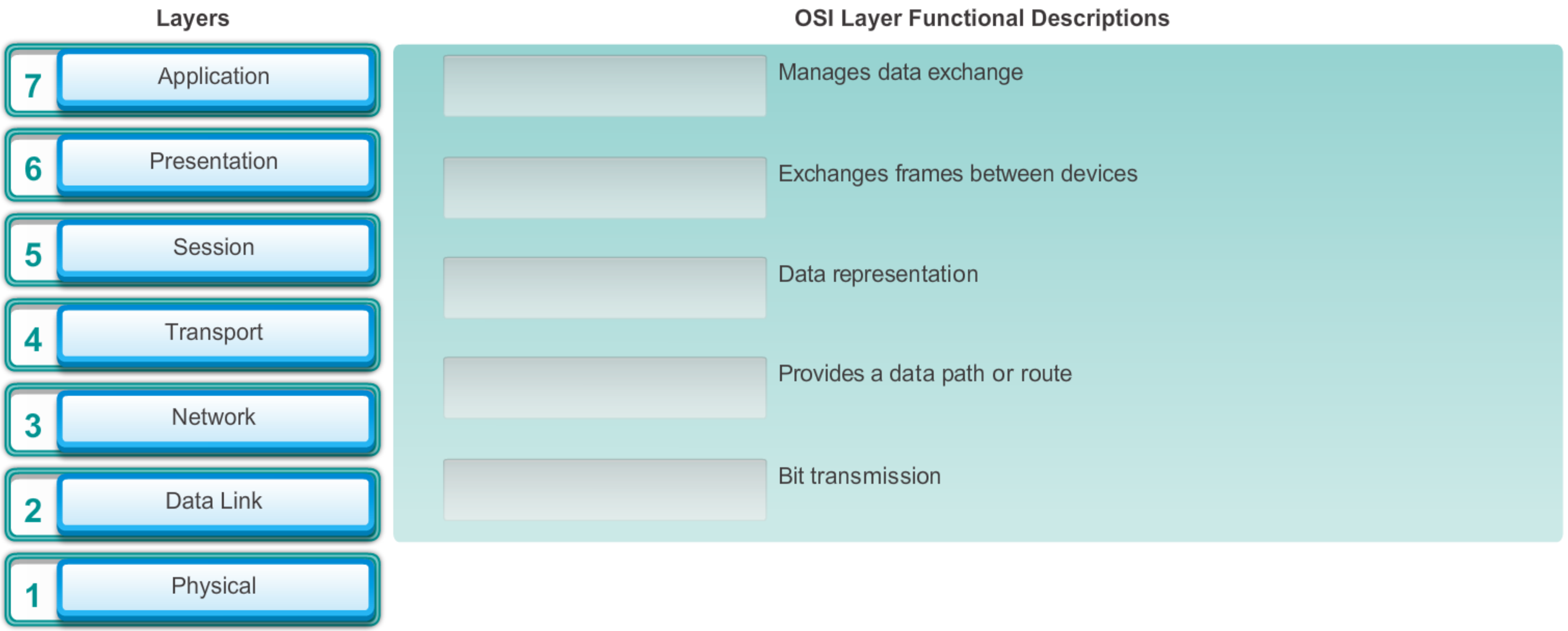
**Presentation**

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

# Protocol Operation of Sending and Receiving a Message



# Activity - Identify Layers and Function



Layers

7 Application

6 Presentation

5 Session

4 Transport

3 Network

2 Data Link

1 Physical

OSI Layer Functional Descriptions

Manages data exchange

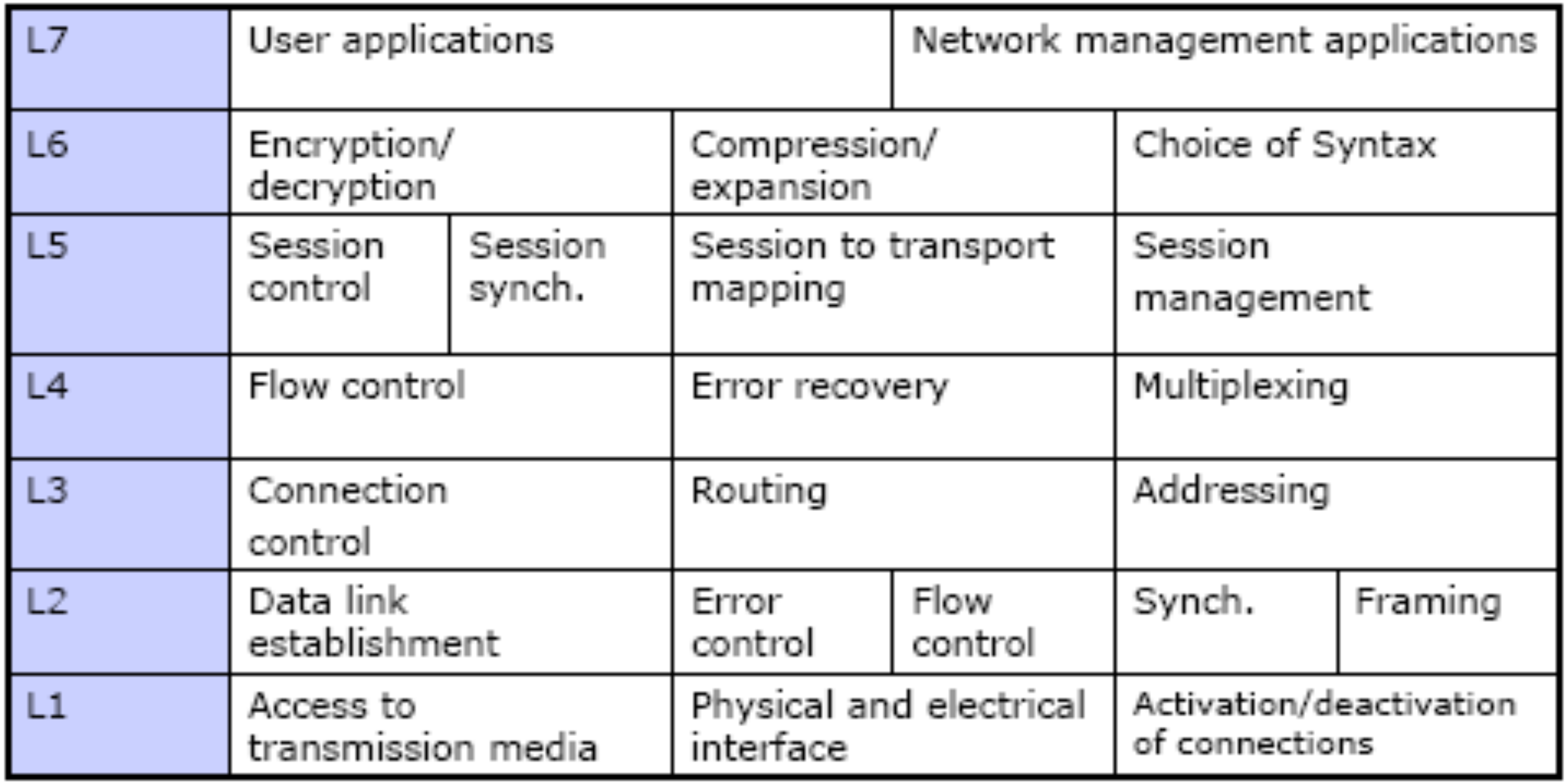
Exchanges frames between devices

Data representation

Provides a data path or route

Bit transmission

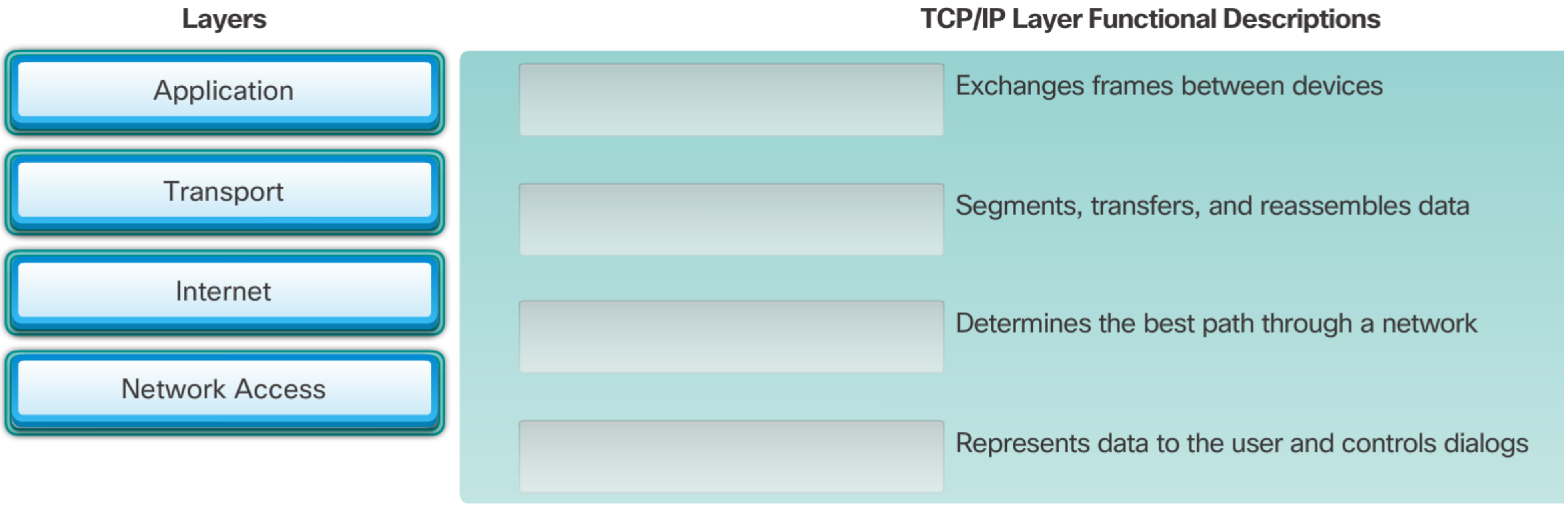
# Summary



| | | | | | | |
|---|---|---|---|---|---|---|
| L7 | User applications | | | Network management applications | | |
| L6 | Encryption/ decryption | | Compression/ expansion | | Choice of Syntax | |
| L5 | Session control | Session synch. | Session to transport mapping | | Session management | |
| L4 | Flow control | | Error recovery | | Multiplexing | |
| L3 | Connection control | | Routing | | Addressing | |
| L2 | Data link establishment | | Error control | Flow control | Synch. | Framing |
| L1 | Access to transmission media | | Physical and electrical interface | | Activation/deactivation of connections | |

Base on Understanding Telecommunications, Ericsson & Telia, Student Litterature, 1998

# Activity - Identify Layers and Function



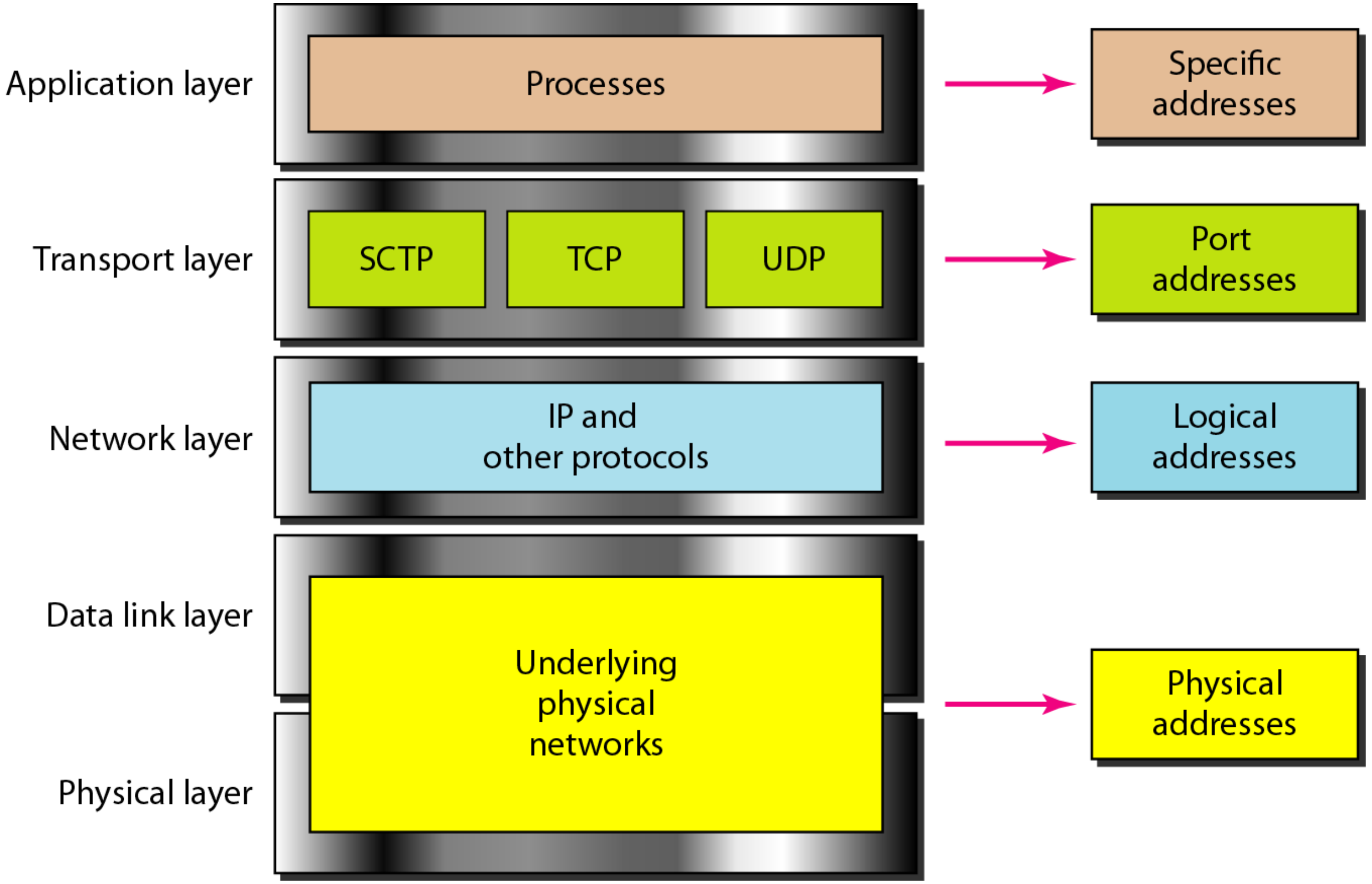
Layers

- Application
- Transport
- Internet
- Network Access

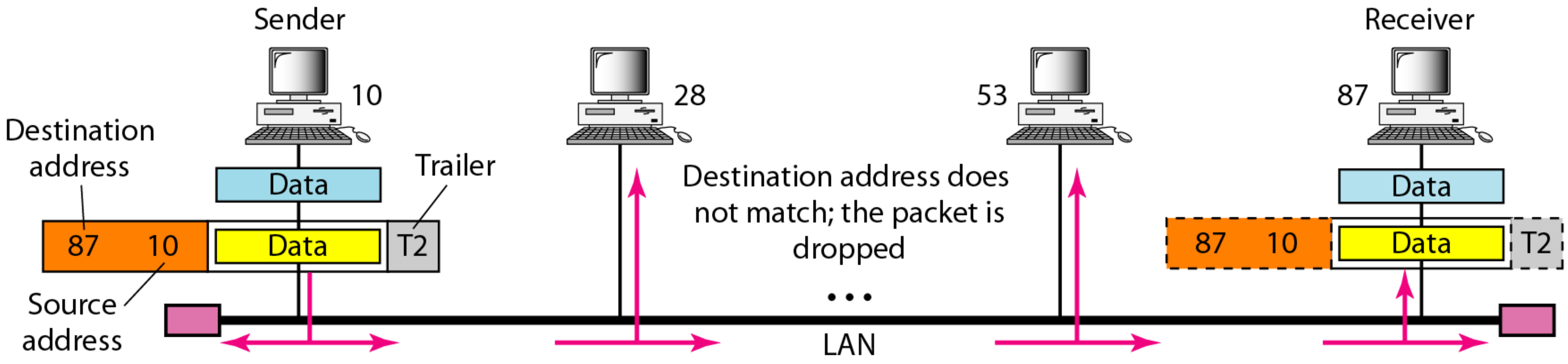
TCP/IP Layer Functional Descriptions

- Exchanges frames between devices
- Segments, transfers, and reassembles data
- Determines the best path through a network
- Represents data to the user and controls dialogs

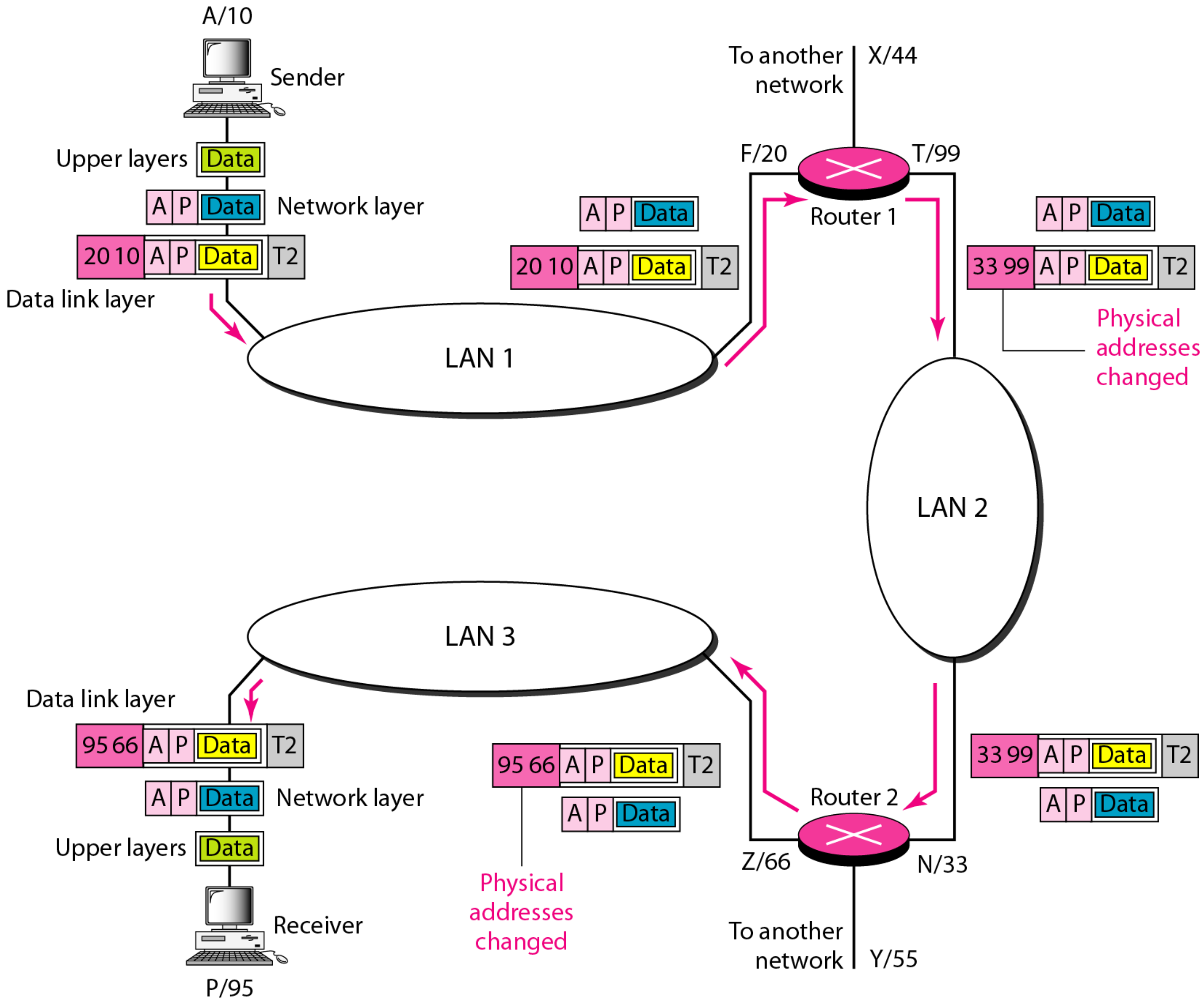
# Relationship of layers and addresses in TCP/IP



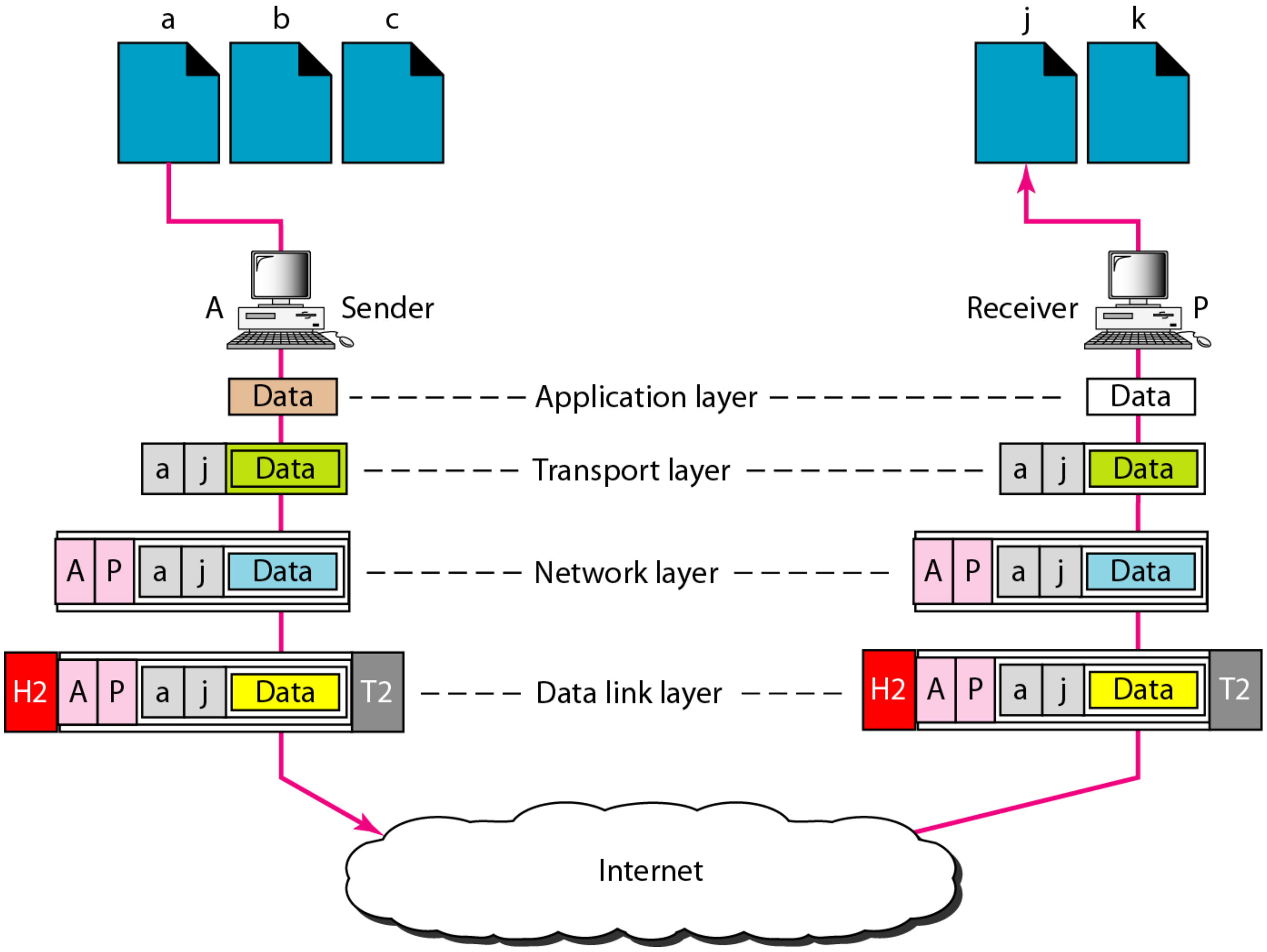
# Physical Addresses



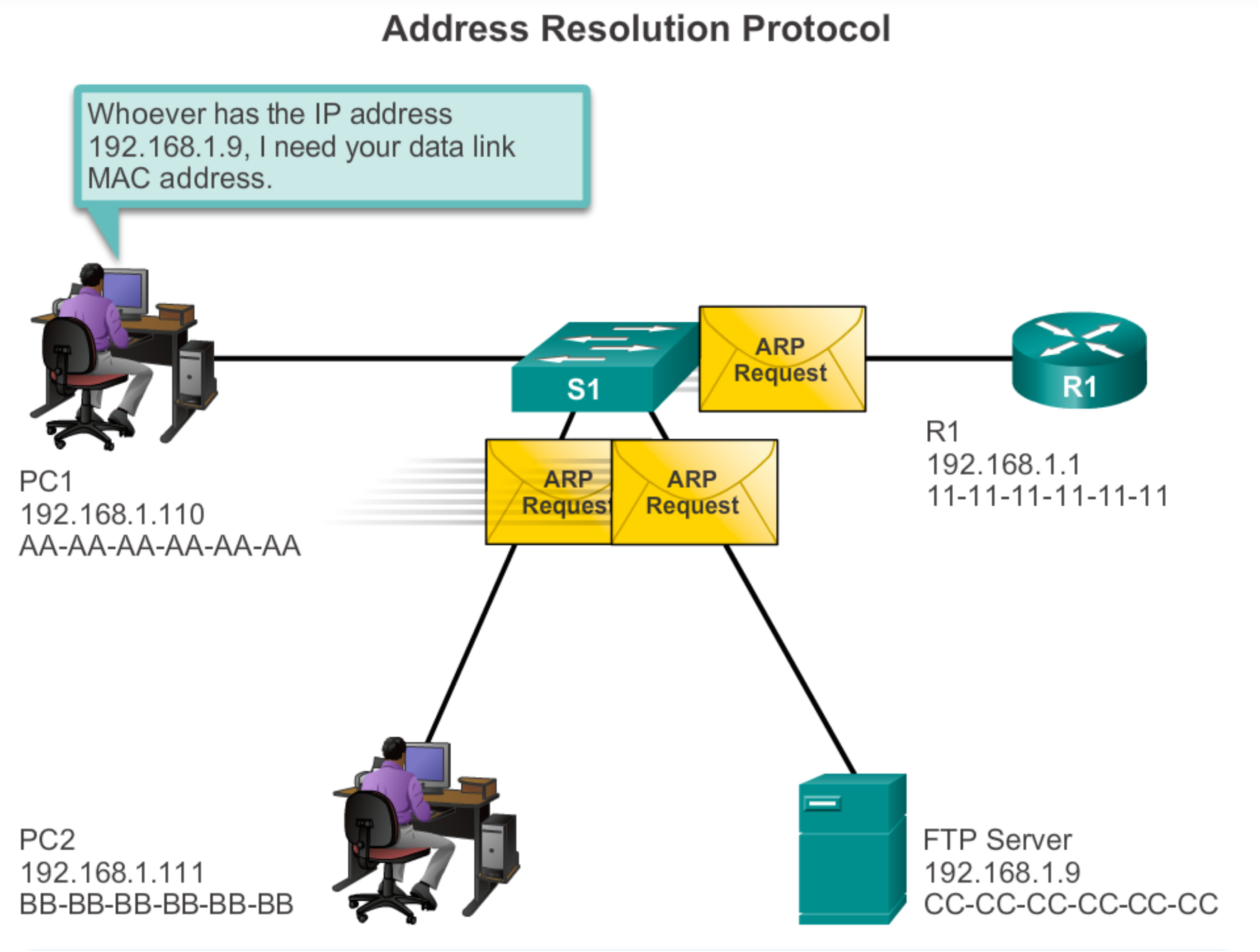
# Logical Addresses



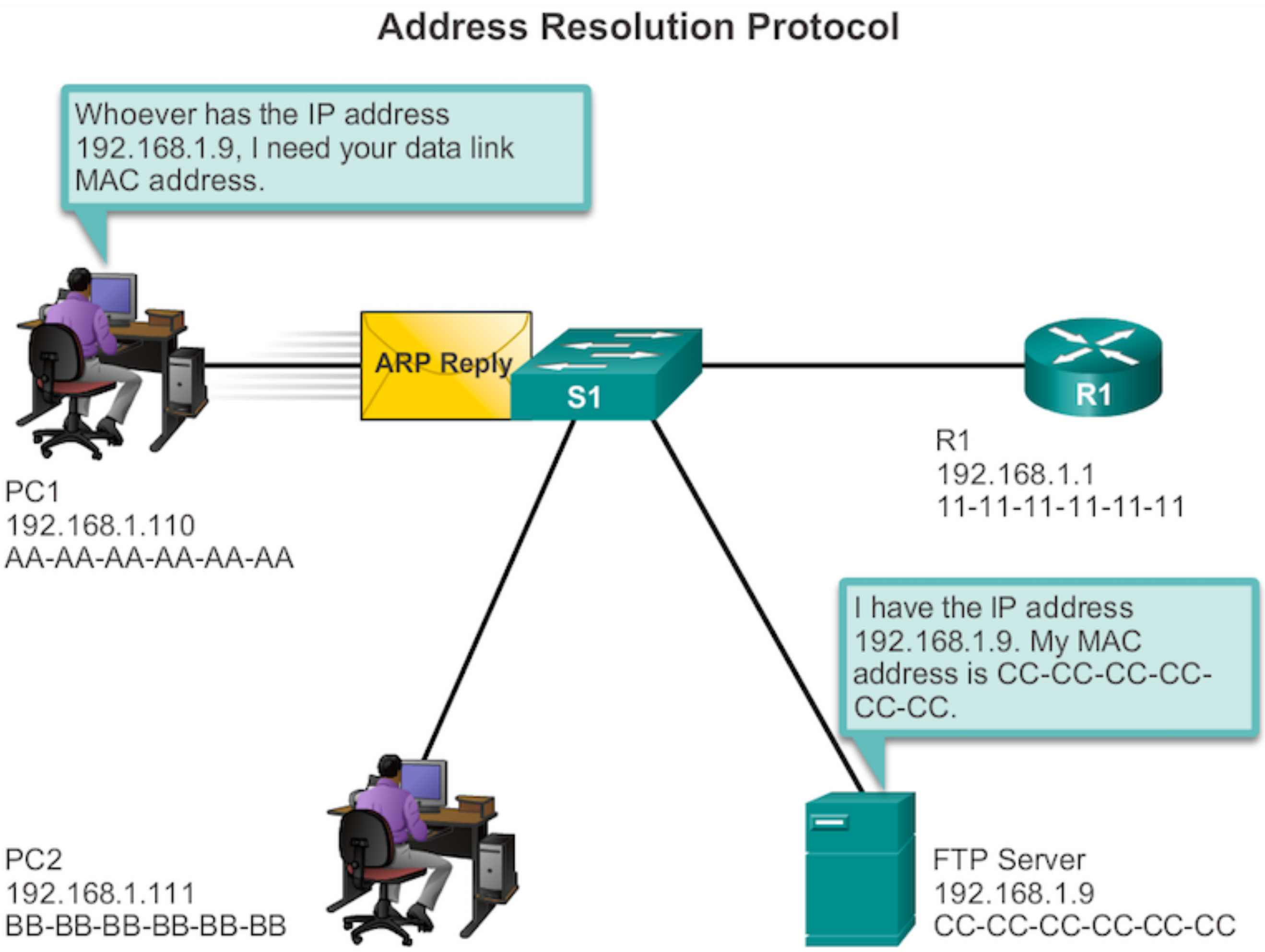
# Port Addresses



# MAC and IP Address (1)



# MAC and IP Address (2)

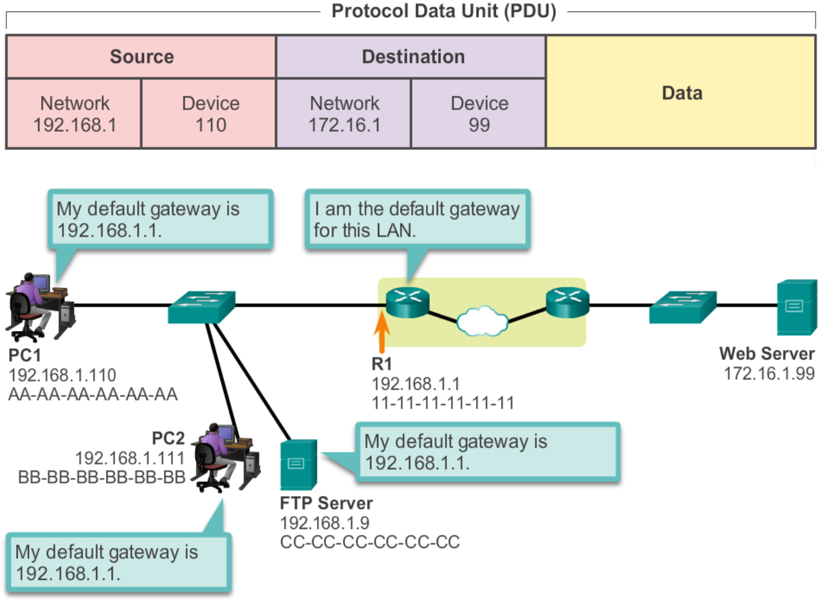

Address Resolution Protocol
Whoever has the IP address 192.168.1.9, I need your data link MAC address.
ARP Reply
S1
R1
R1
192.168.1.1
11-11-11-11-11-11
PC1
192.168.1.110
AA-AA-AA-AA-AA-AA
I have the IP address 192.168.1.9. My MAC address is CC-CC-CC-CC-CC-CC.
PC2
192.168.1.111
BB-BB-BB-BB-BB-BB
FTP Server
192.168.1.9
CC-CC-CC-CC-CC-CC

# Accessing Remote Resources

## Default Gateway

- 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.
- It is important that the address of the default gateway be configured on each host on the local network. 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.

Getting the Pieces to the Correct Network



Protocol Data Unit (PDU)

| Source | | Destination | | Data |
|---|---|---|---|---|
| Network<br>192.168.1 | Device<br>110 | Network<br>172.16.1 | Device<br>99 | |

My default gateway is 192.168.1.1.

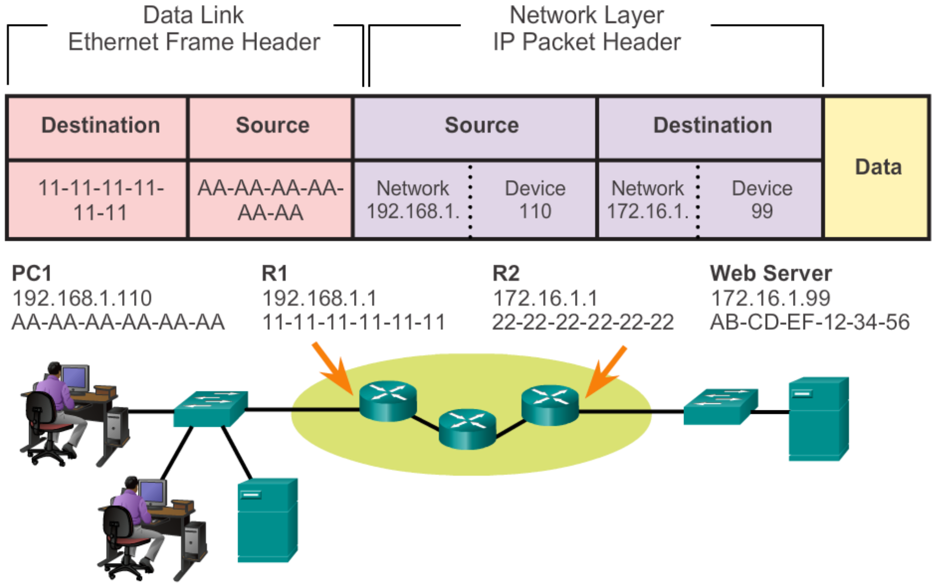
I am the default gateway for this LAN.

My default gateway is 192.168.1.1.

My default gateway is 192.168.1.1.

## Network Addresses

- IP addresses indicate the network and device addresses of the source and destination. When the sender of the packet is on a different network from the receiver, the source and destination IP addresses will represent hosts on different networks. This will be indicated by the network portion of the IP address of the destination host.
    - Source IP address - The IP address of the sending device, the client computer PC1: 192.168.1.110.
    - Destination IP address - The IP address of the receiving device, the server, Web Server: 172.16.1.99.



| Data Link<br>Ethernet Frame Header | | Network Layer<br>IP Packet Header | | | | |
|---|---|---|---|---|---|---|
| Destination | Source | Source | | Destination | | Data |
| 11-11-11-11-11-11 | AA-AA-AA-AA-AA-AA | Network<br>192.168.1. | Device<br>110 | Network<br>172.16.1. | Device<br>99 | |