

# Introduction to Computer Networks

**Slide Source: Cisco Networking**

# Networking Today

- Network has no boundary and supports the way we:
  - Learn
  - Communicate
  - Work
  - Play



# Providing Resources in a Network

## ■ Networks of Many Sizes

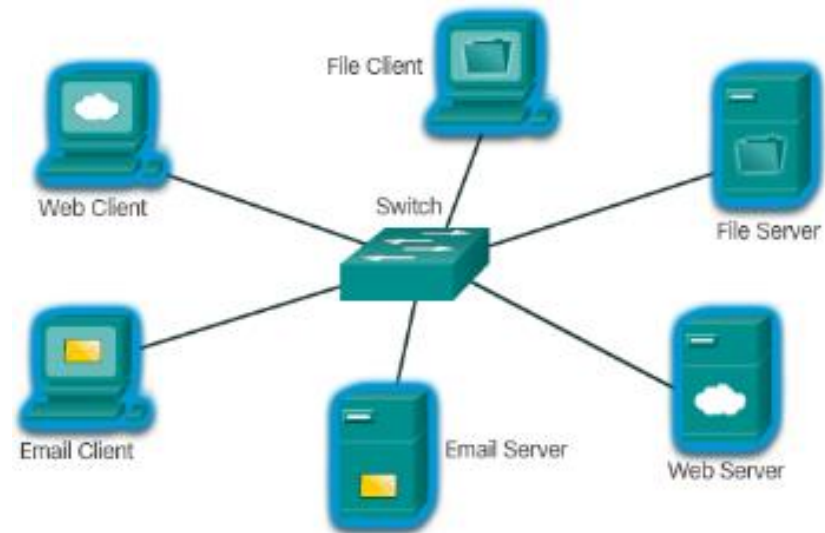
- Small Home / Office Networks
- Medium to Large Networks
- World Wide Network

## ■ Clients and Servers

- Clients request and display information
- Servers provide information to other devices on the network

## ■ Peer-to-Peer

- Computers can be both server and client at the same time.
- What are the advantages?
- What are the disadvantages?



# Network Components

## ■ End Devices

- Either the source or destination of a message
- Name some end devices

## ■ Intermediary Network Devices

- Connect multiple individual networks to form an internetwork
- Connect the individual end devices to the network
- Ensure data flows across the network
- Provide connectivity

## ■ Network Media

- Provide the pathway for data transmission
- Interconnect devices
- Name the three types of media

Copper



Fiber Optic



Wireless



# Network Components

- Network Representations
  - What do the symbols represent?
- Topology Diagrams
  - Physical
  - Logical



# LANs and WANs

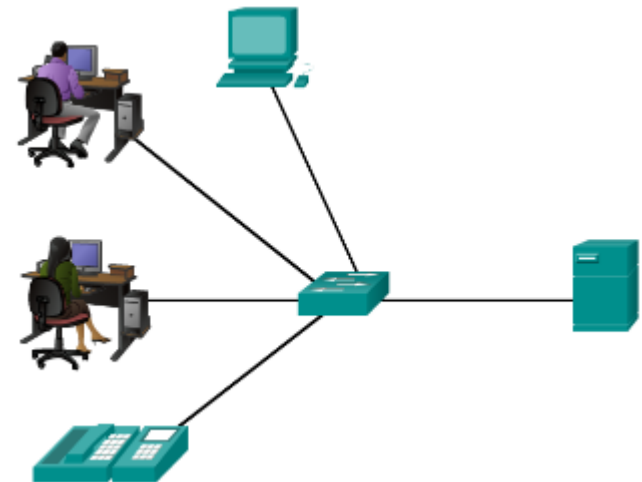
## ■ Local Area Networks

- Spans across small geographical area
- Interconnects end devices
- Administrated by a single organization
- Provide high speed bandwidth to internal devices

## ■ WAN Area Networks

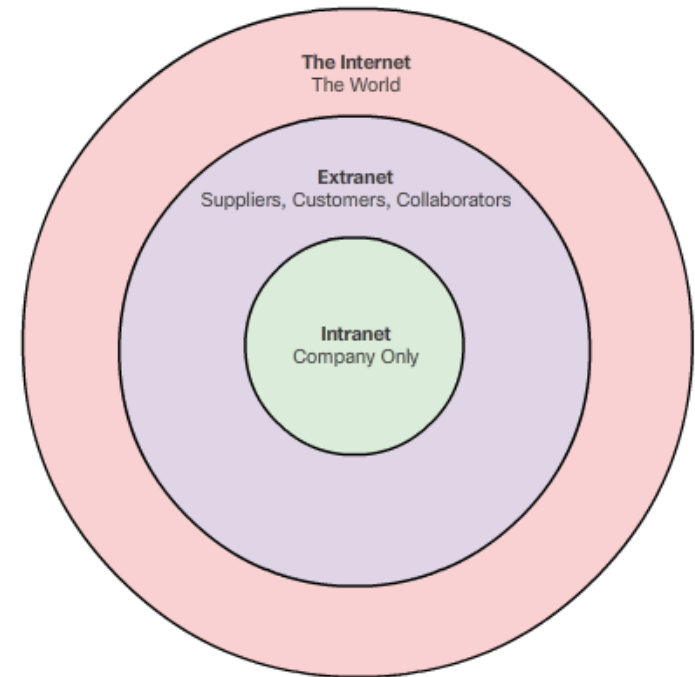
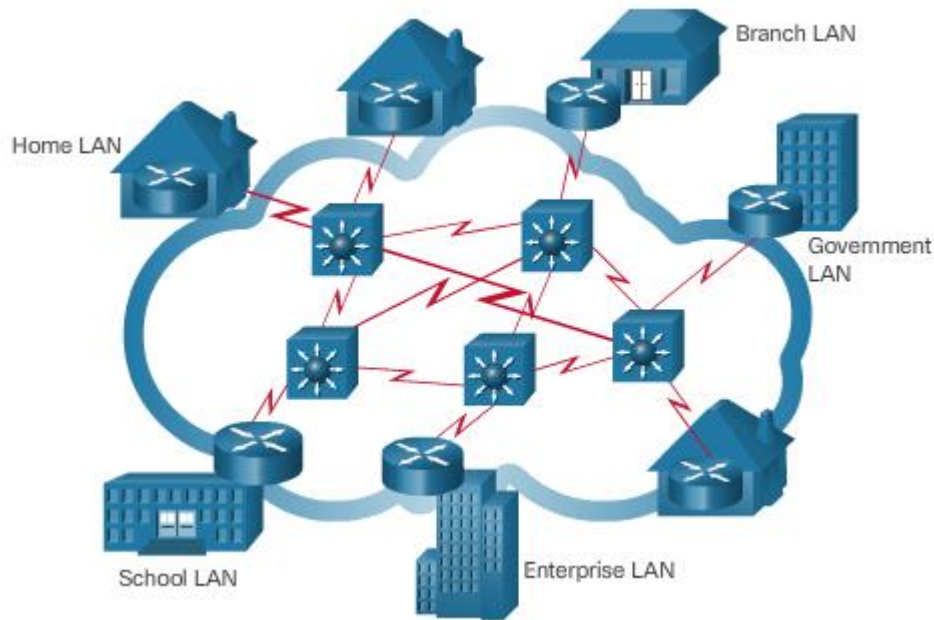
- Interconnects LAN
- Administrated by multiple service providers
- Provide slower speed links between LANS

## ■ Can you name more network types?



# The Internet, Intranets, and Extranets

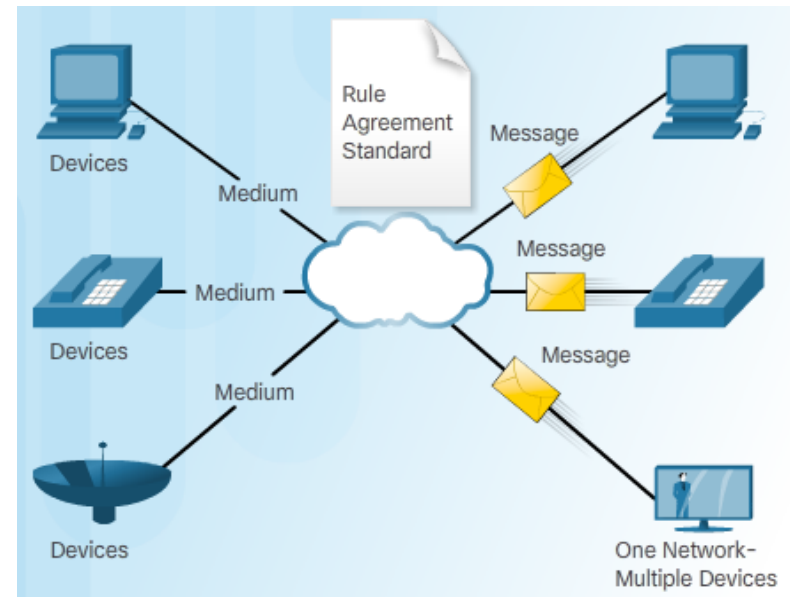
- The Internet
  - Worldwide collection of interconnected networks
  - Not owned by any individual or group
- Intranets and Extranets



## The Network as a Platform

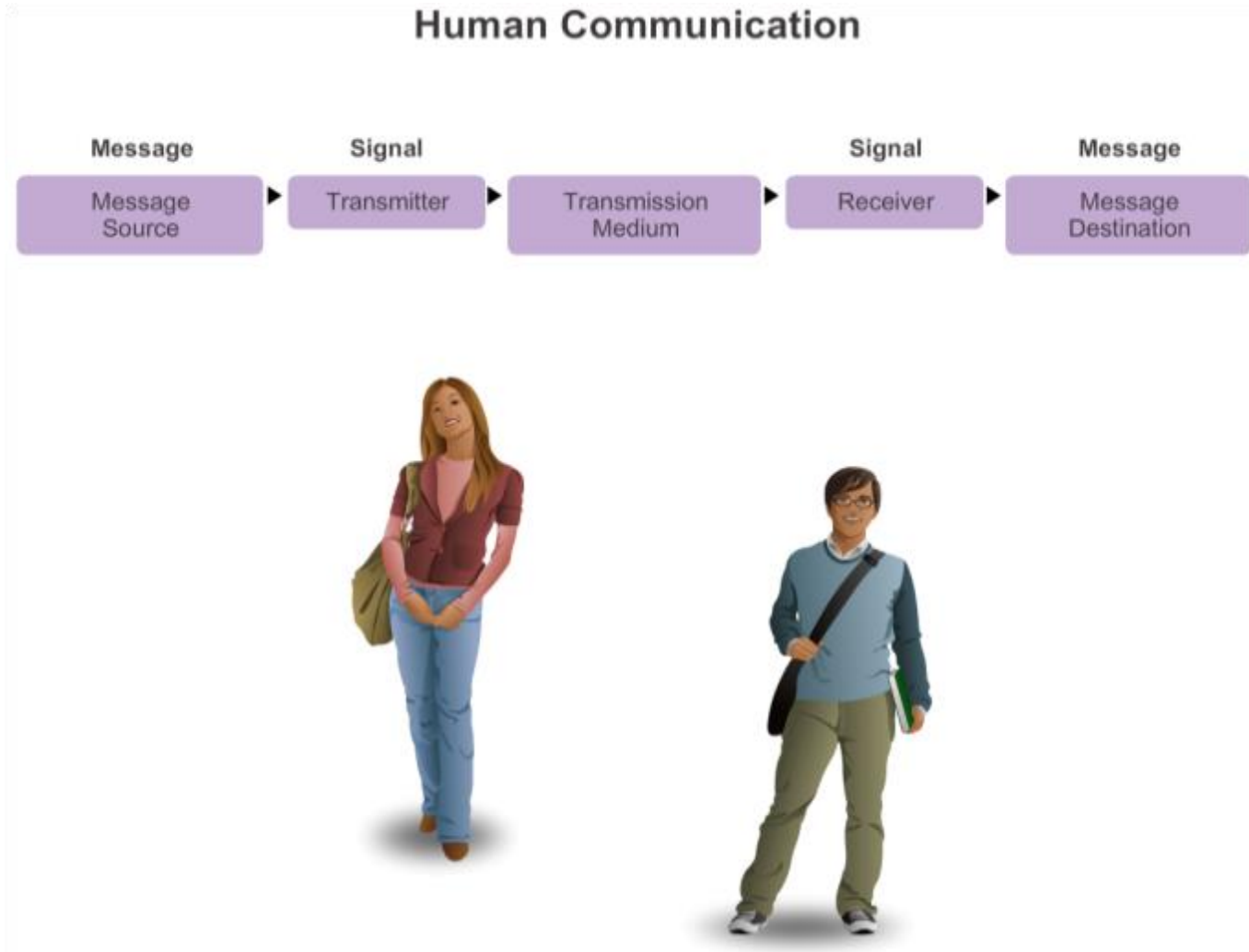
# Converged Networks

- Traditional Separate Networks
  - Each network with its own rules and
- (The Converging Network
  - Capable of delivering data, voice, and video over the same network infrastructure





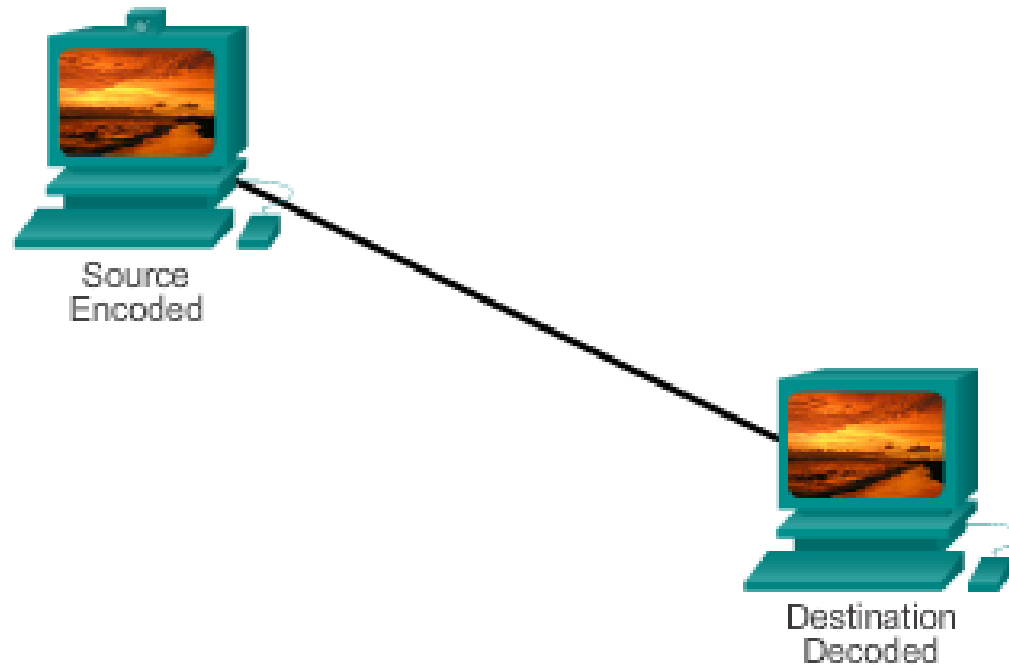
# What is Communication?



# Establishing the Rules

- An identified sender and receiver
- Agreed upon method of communicating (face-to-face, telephone, letter, photograph)
- Common language and grammar
- Speed and timing of delivery
- Confirmation or acknowledgment requirements

# Message Encoding



# Message Formatting and Encapsulation

Example: Personal letter contains the following elements:

- Identifier of the recipient's location
- Identifier of the sender's location
- Salutation or greeting
- Recipient identifier
- The message content
- Source identifier
- End of message indicator



# Message Size

An overview of the segmenting process:

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

# Message Timing

- Access Method
- Flow Control
- Response Timeout

# Network Protocols

- How the message is formatted or structured
- The process by which networking devices share information about pathways with other networks
- How and when error and system messages are passed between devices
- The setup and termination of data transfer sessions

# Interaction of Protocols

FO - 80

- Application Protocol – Hypertext Transfer Protocol (HTTP)
- Transport Protocol – Transmission Control Protocol (TCP)
- Internet Protocol – Internet Protocol (IP)
- Network Access Protocols – Data link & physical layers



# Protocol Suites and Industry Standards

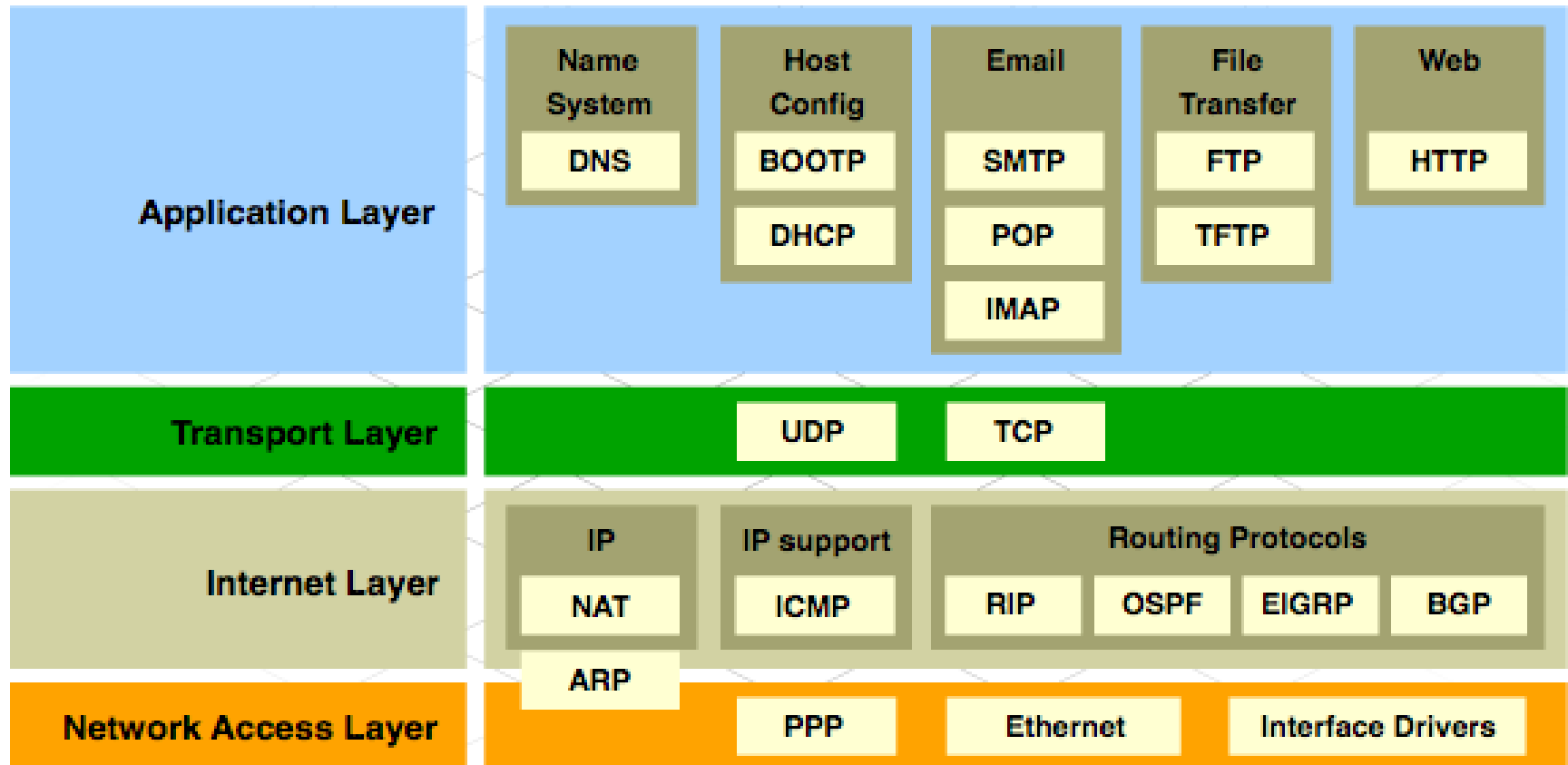
## Protocol Suites and Industry Standards

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			

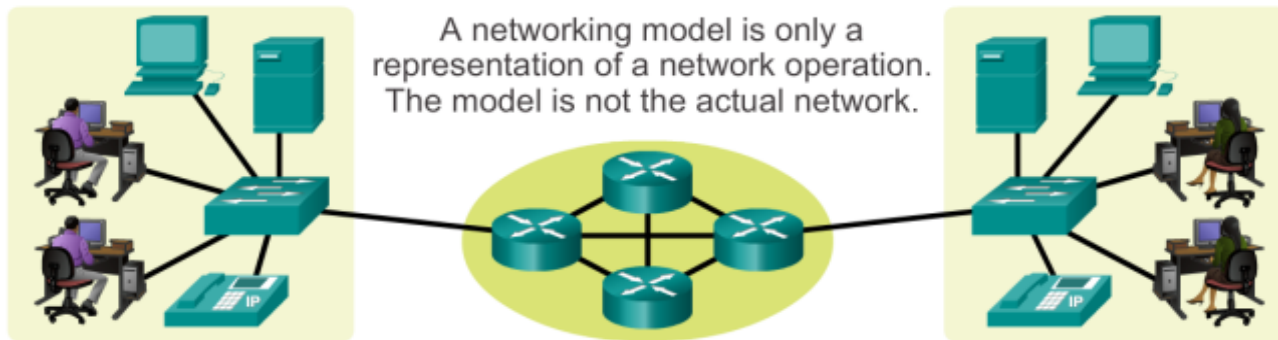
# Creation of Internet, Development of TCP/IP

- The first packet switching network and predecessor to today's Internet was the Advanced Research Projects Agency Network (ARPANET), which came to life in 1969 by connecting mainframe computers at four locations.
- ARPANET was funded by the U.S. Department of Defense for use by universities and research laboratories. Bolt, Beranek and Newman (BBN) was the contractor that did much of the initial development of the ARPANET, including creating the first router known as an Interface Message Processor (IMP).
- In 1973, Robert Kahn and Vinton Cerf began work on TCP to develop the next generation of the ARPANET. TCP was designed to replace ARPANET's current Network Control Program (NCP).
- In 1978, TCP was divided into two protocols: TCP and IP. Later, other protocols were added to the TCP/IP suite of protocols including Telnet, FTP, DNS, and many others.

# TCP/IP Protocol Suite and Communication



# Benefits of Using a 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	PPP, Frame Relay, Ethernet	Network Access
Physical		

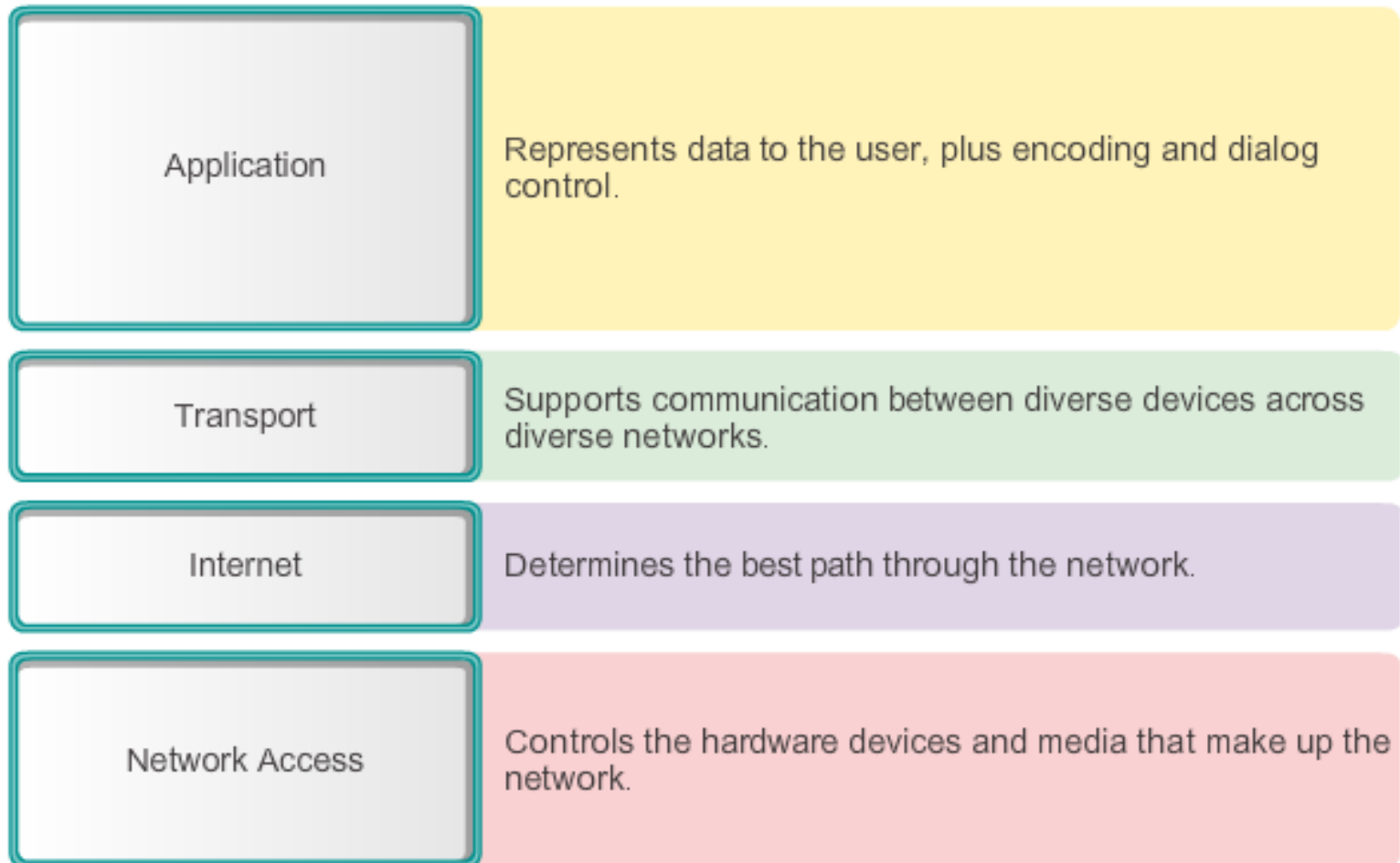
# The OSI Reference Model

## OSI Model

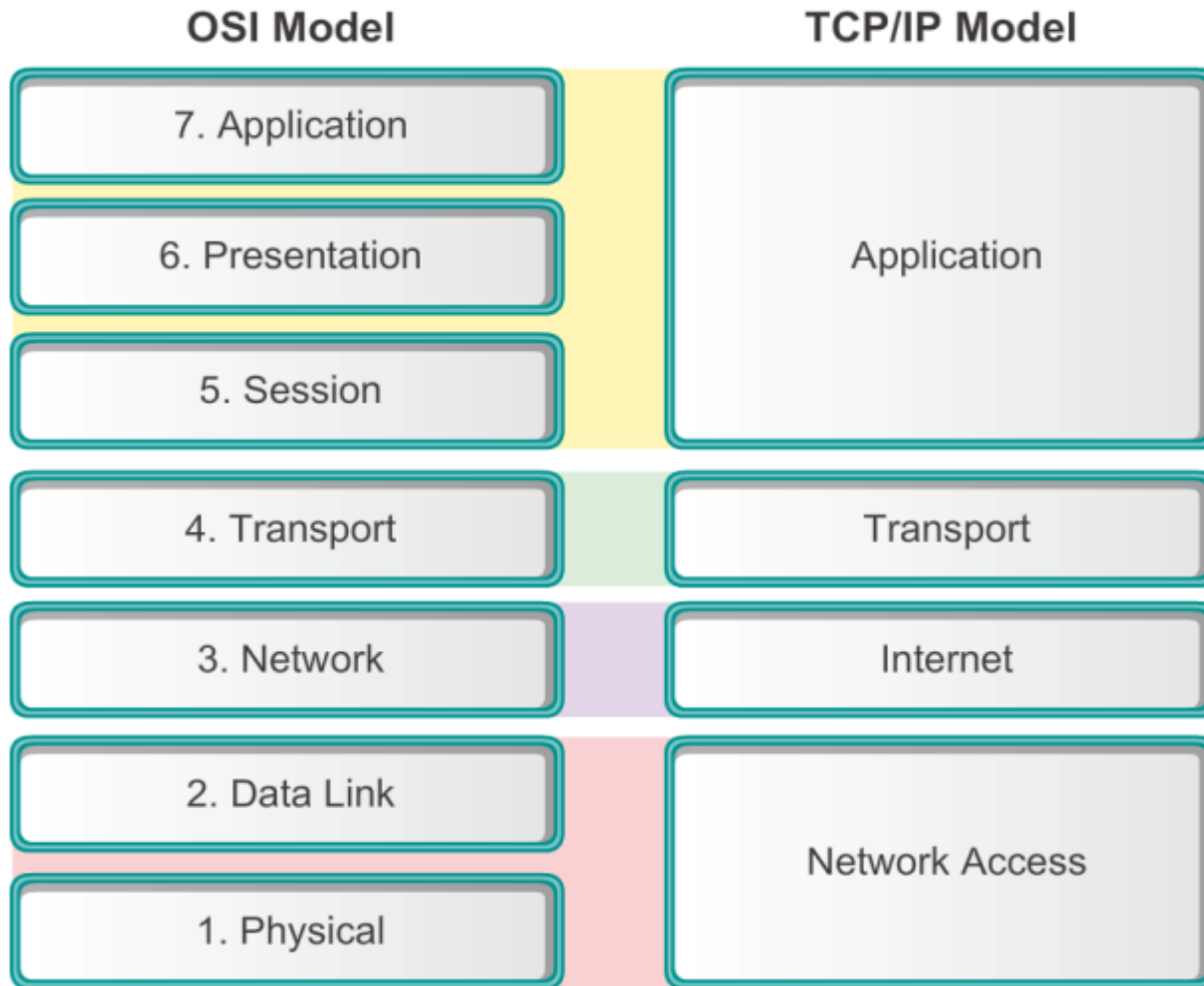


# The TCP/IP Reference Model

## TCP/IP Model

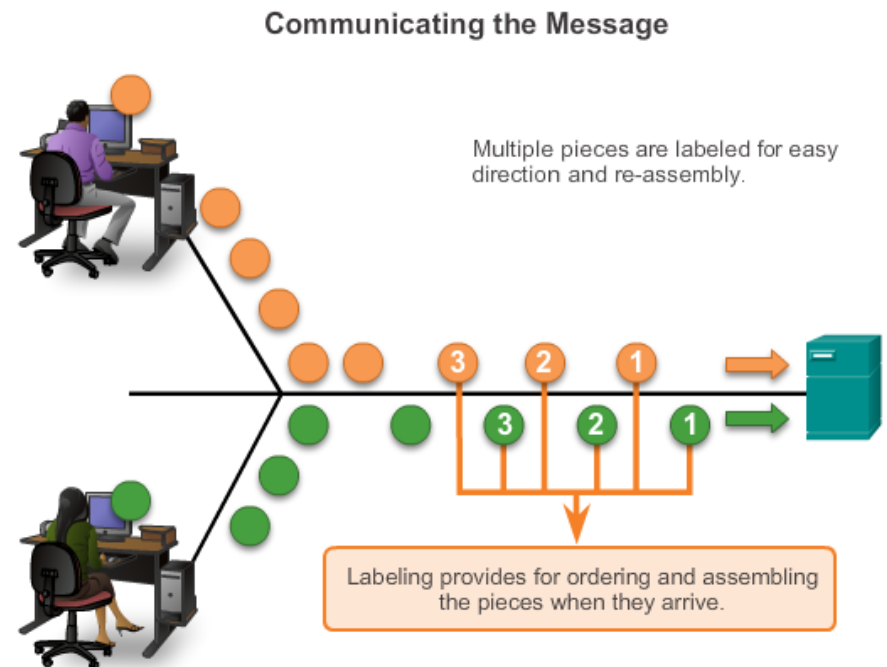


# Comparing the OSI and TCP/IP Models



# Communicating the Messages

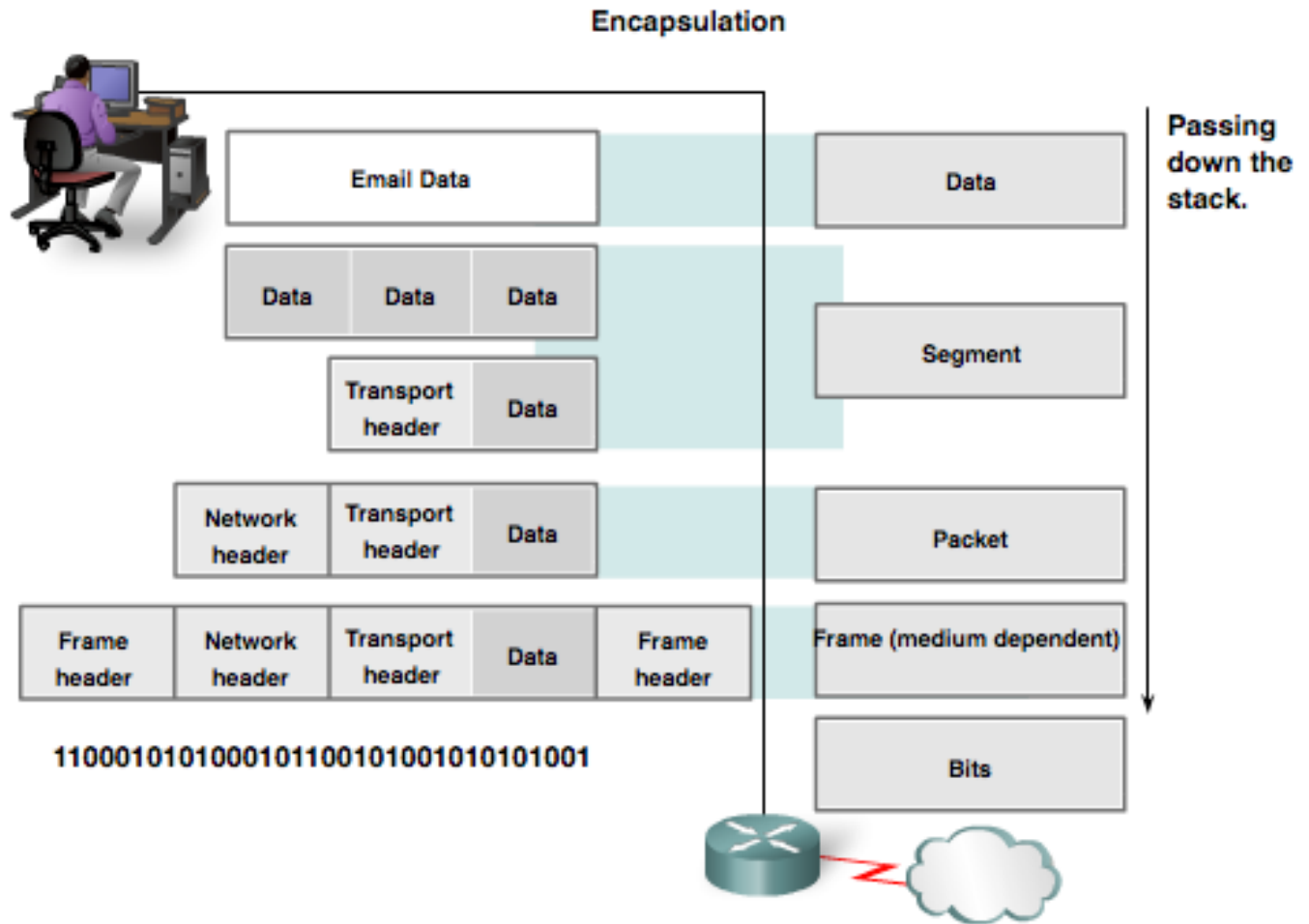
- Segmenting message benefits
  - Different conversations can be interleaved
  - Increased reliability of network communications
- Segmenting message disadvantage
  - Increased level of complexity





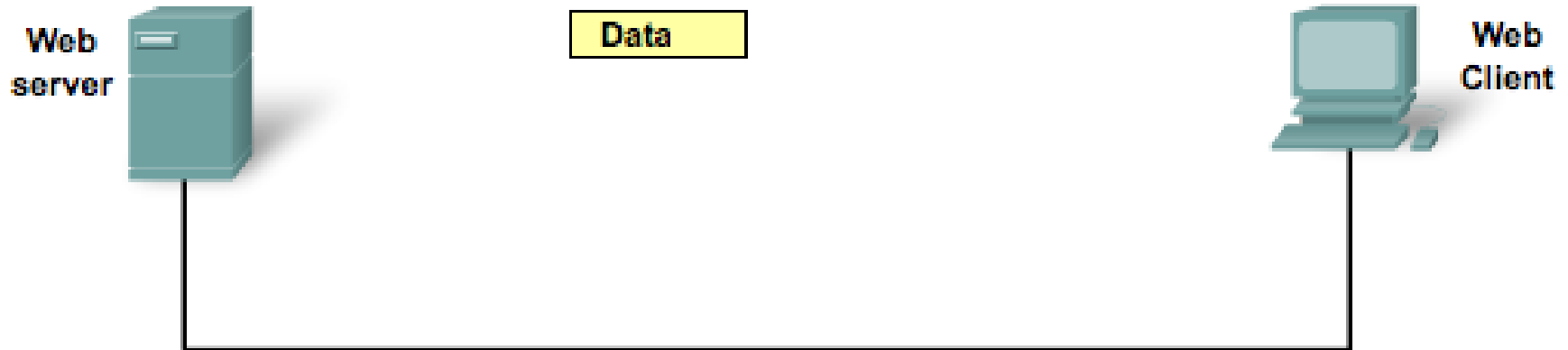
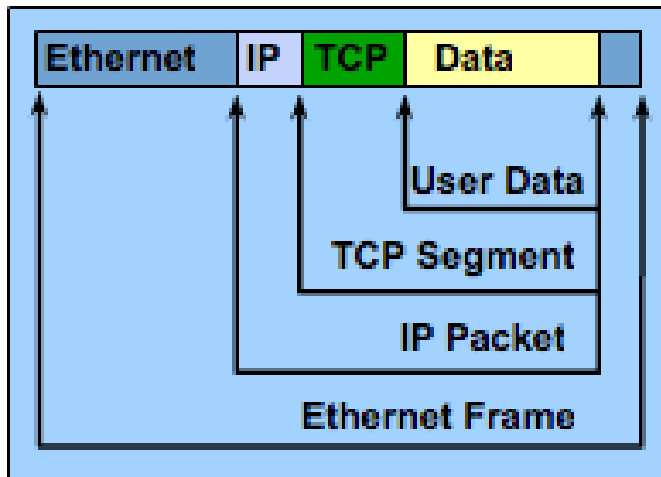
# Protocol Data Units (PDUs)

- Data
- Segment
- Packet
- Frame
- Bits

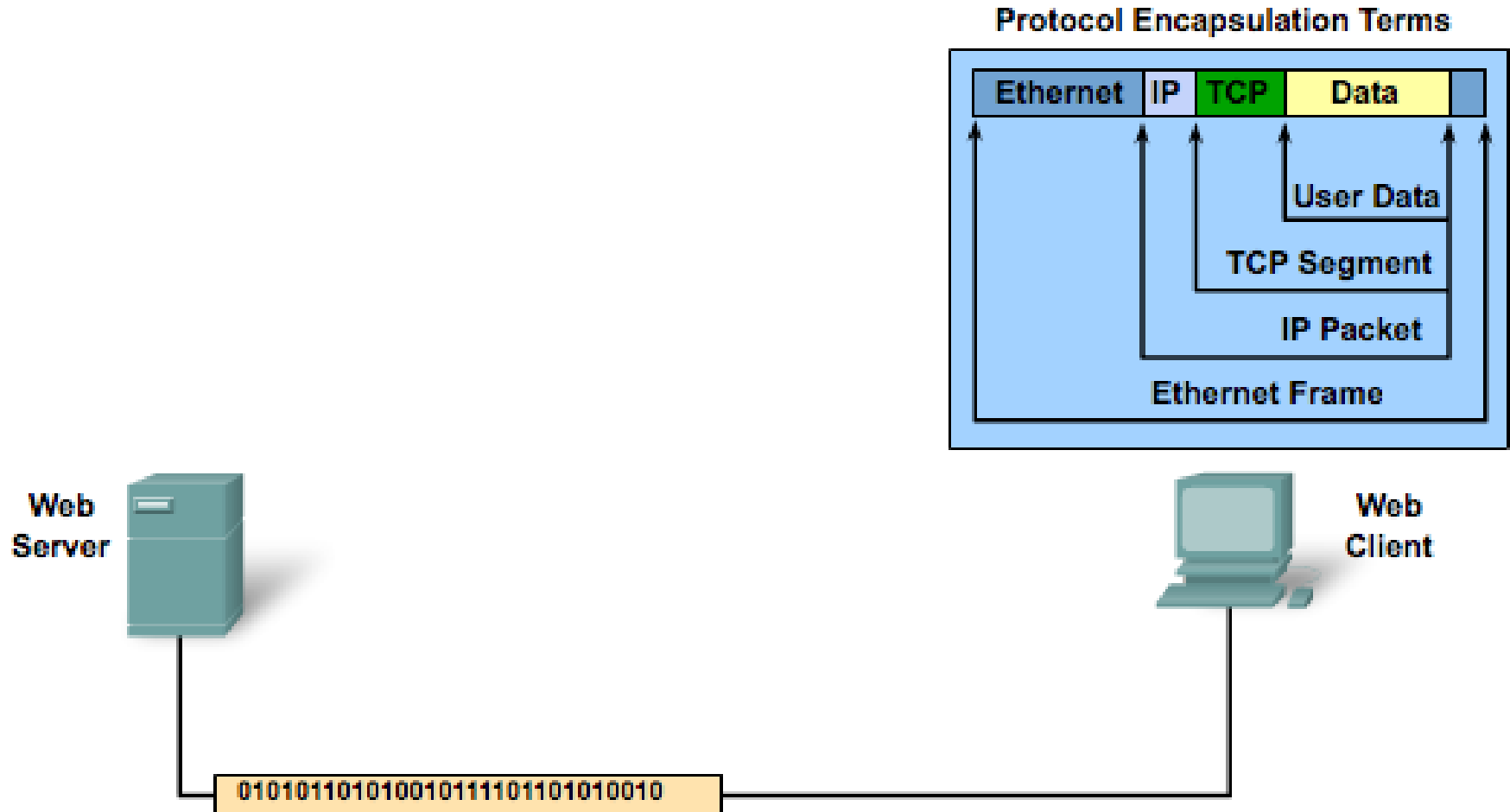


# Protocol Encapsulation

Protocol Encapsulation Terms

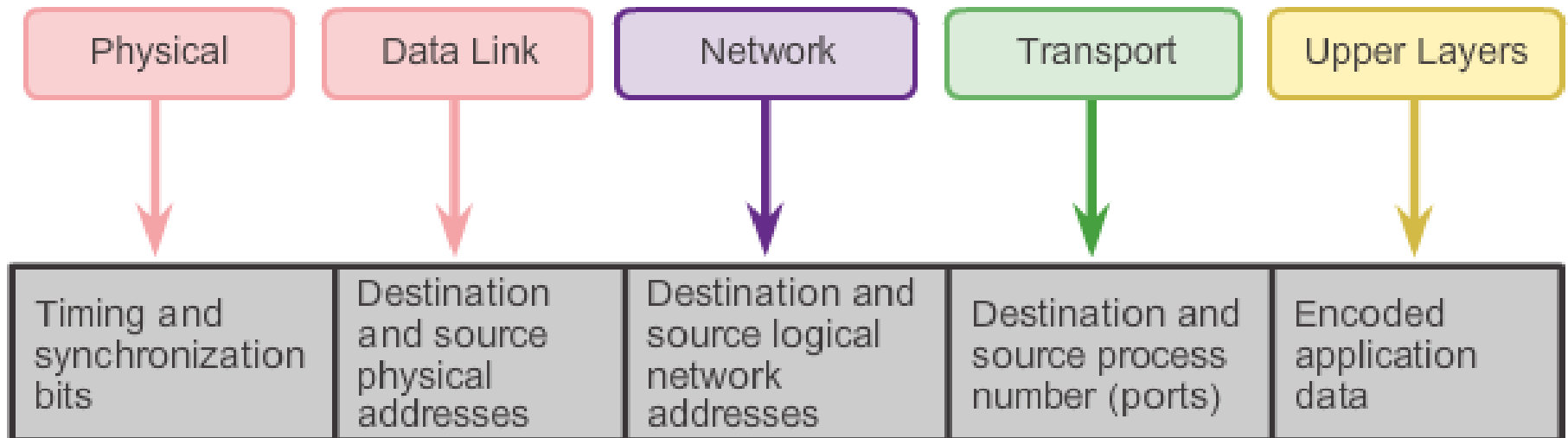


# Protocol De-encapsulation

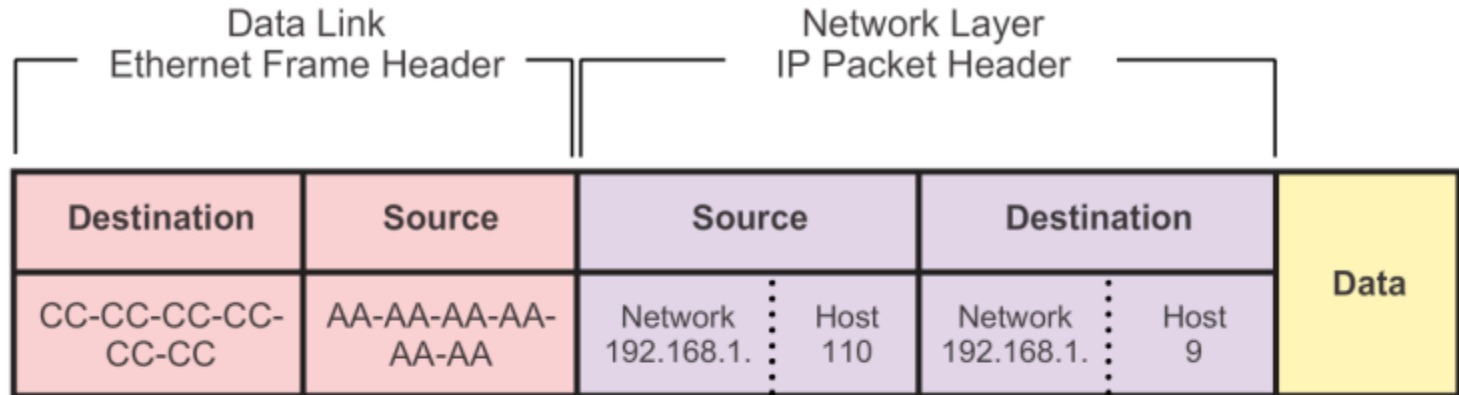


# Accessing Local Resources

## Network Addresses and Data Link Addresses



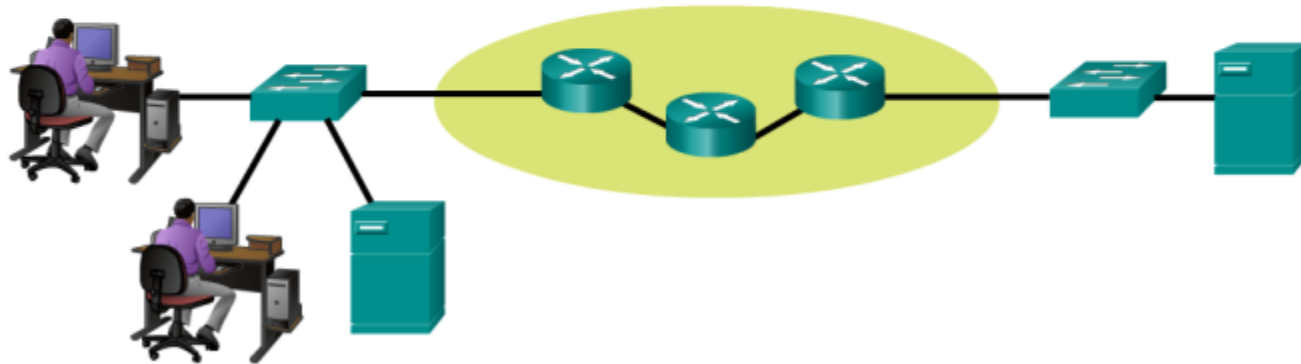
# Communicating with Device / Same Network



**PC1**

192.168.1.110

AA-AA-AA-AA-AA-AA

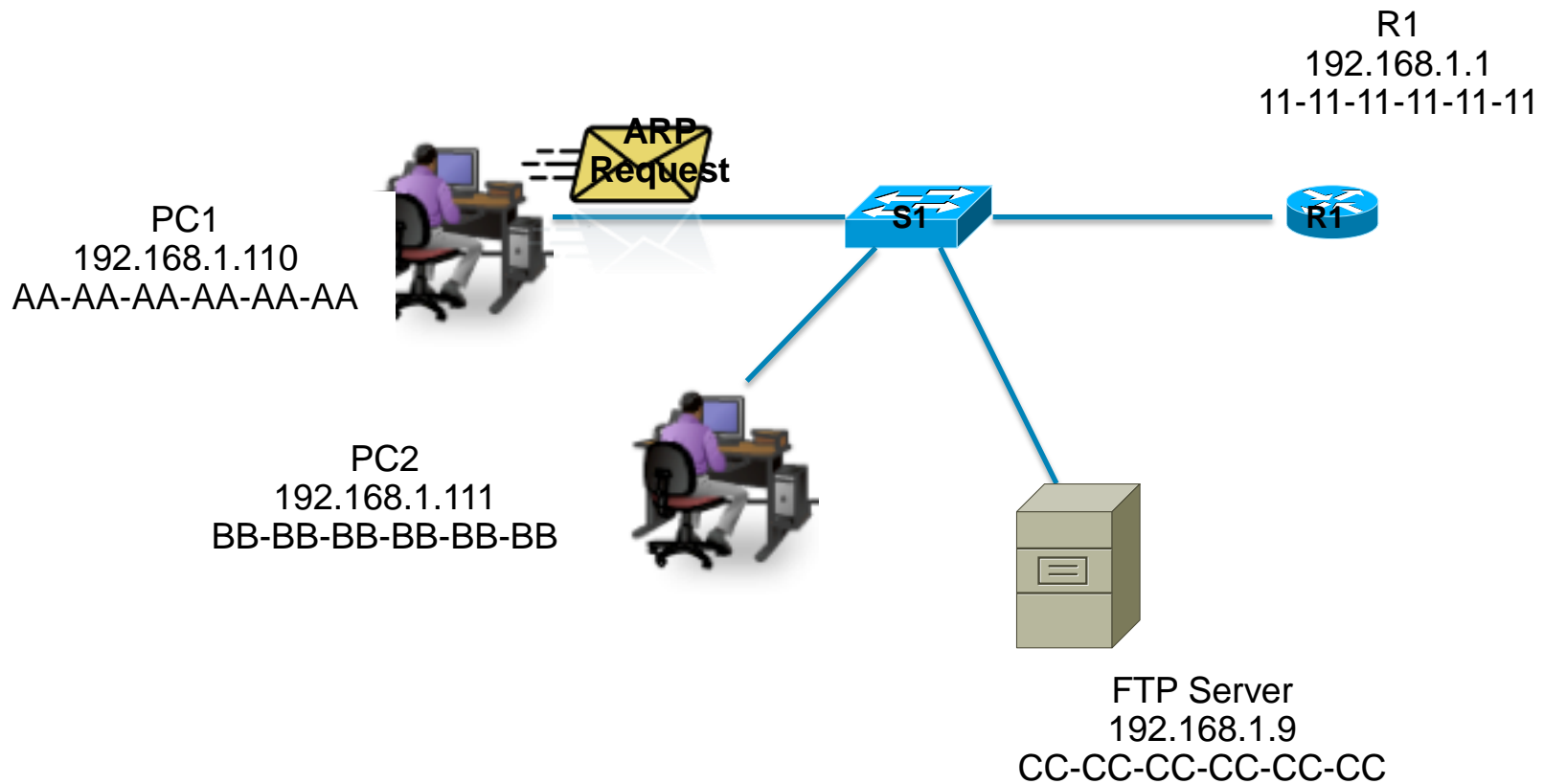


**FTP Server**

192.168.1.9

CC-CC-CC-CC-CC-CC

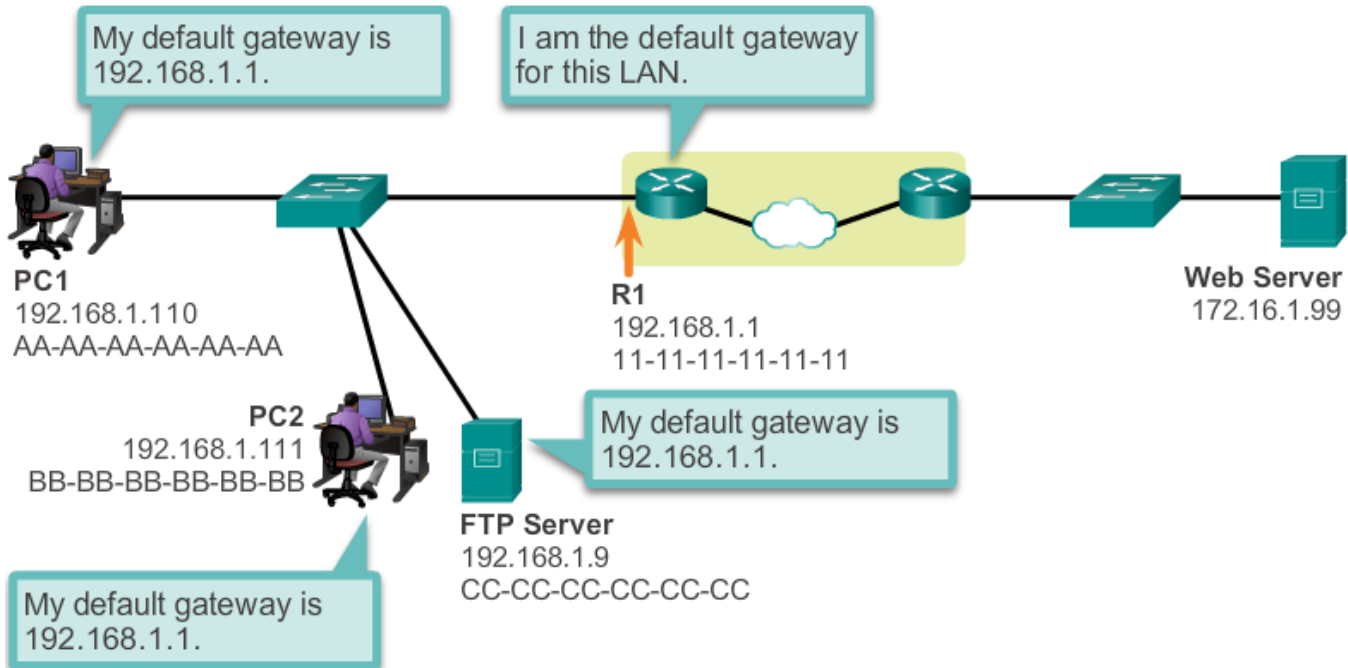
# MAC and IP Addresses



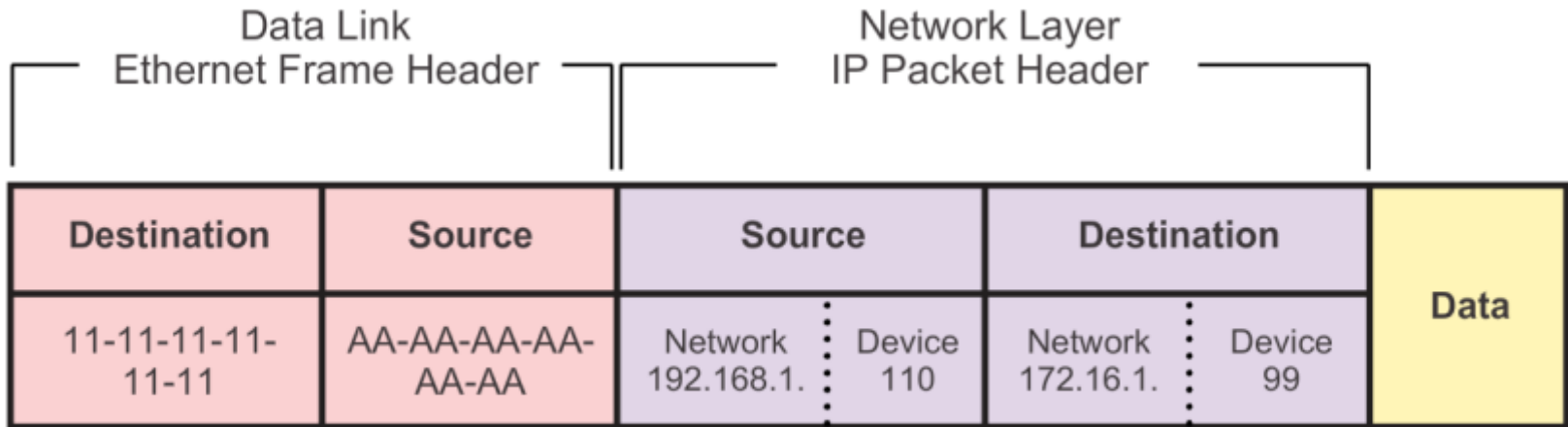
# Default Gateway

## 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	



# Communicating Device / Remote Network

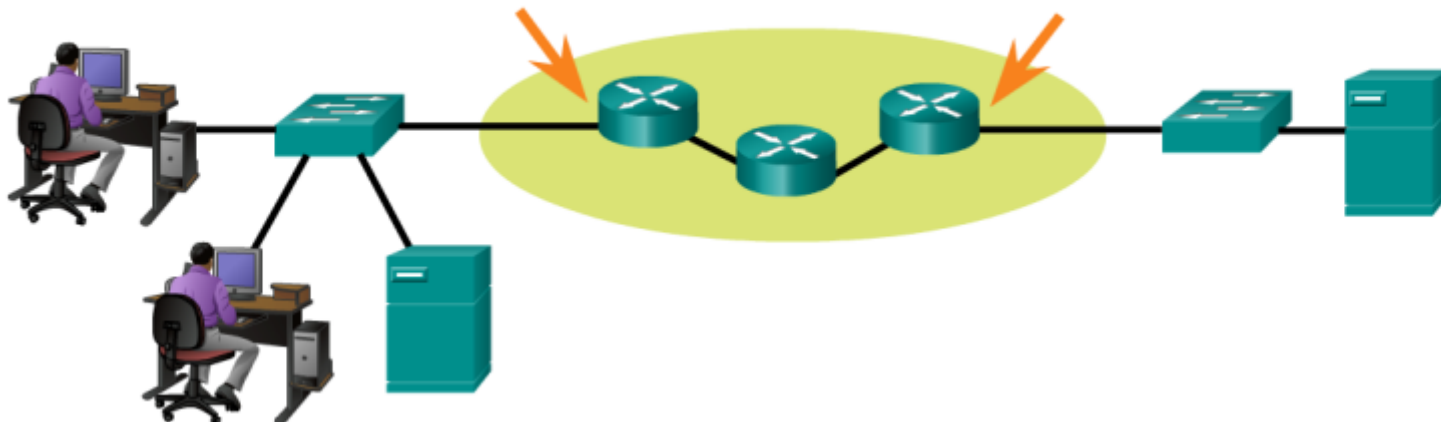


**PC1**  
192.168.1.110  
AA-AA-AA-AA-AA-AA

**R1**  
192.168.1.1  
11-11-11-11-11-11

**R2**  
172.16.1.99  
22-22-22-22-22-22

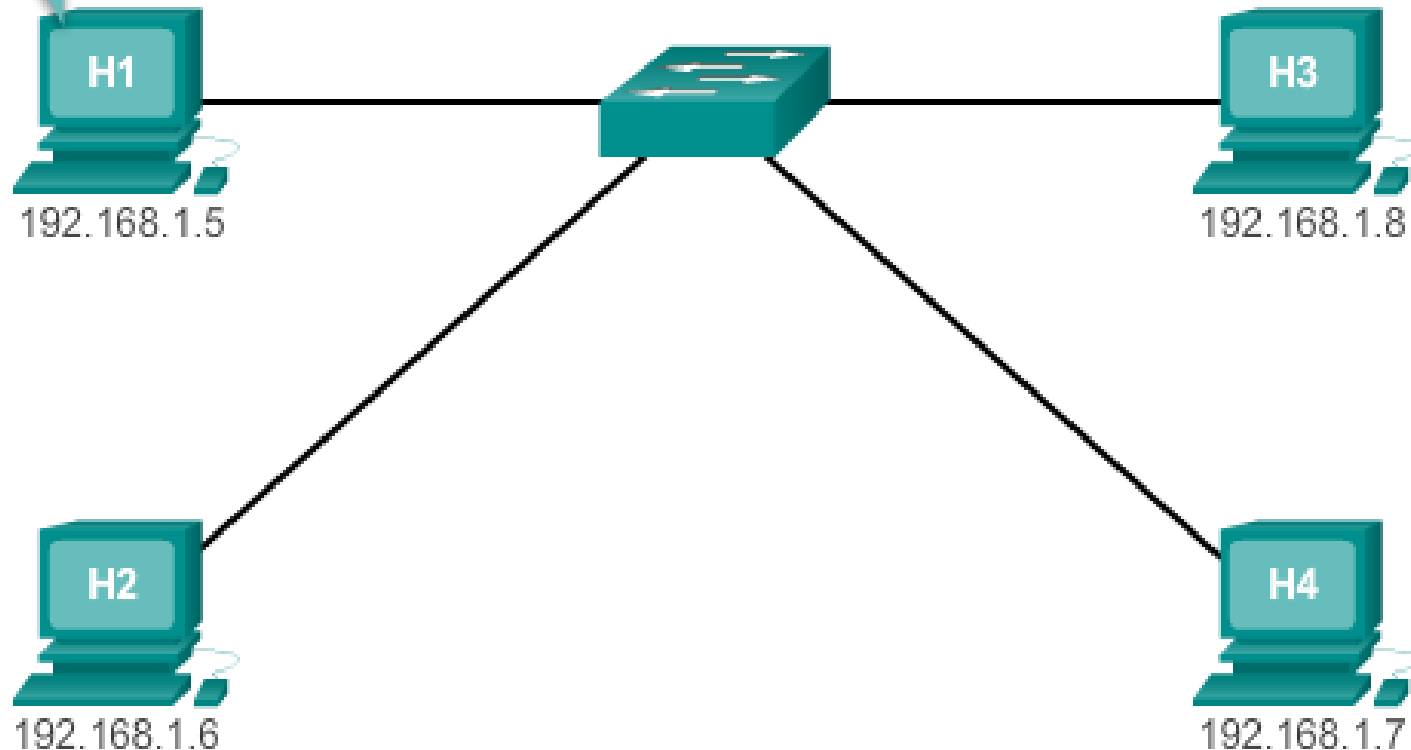
**Web Server**  
172.16.1.99  
AB-CD-EF-12-34-56





# Introduction to ARP

I need to send information to 192.168.1.7, but I only have the IP address. I don't know the MAC address of the device that has that IP.



# ARP Functions/Operation

## ARP Table

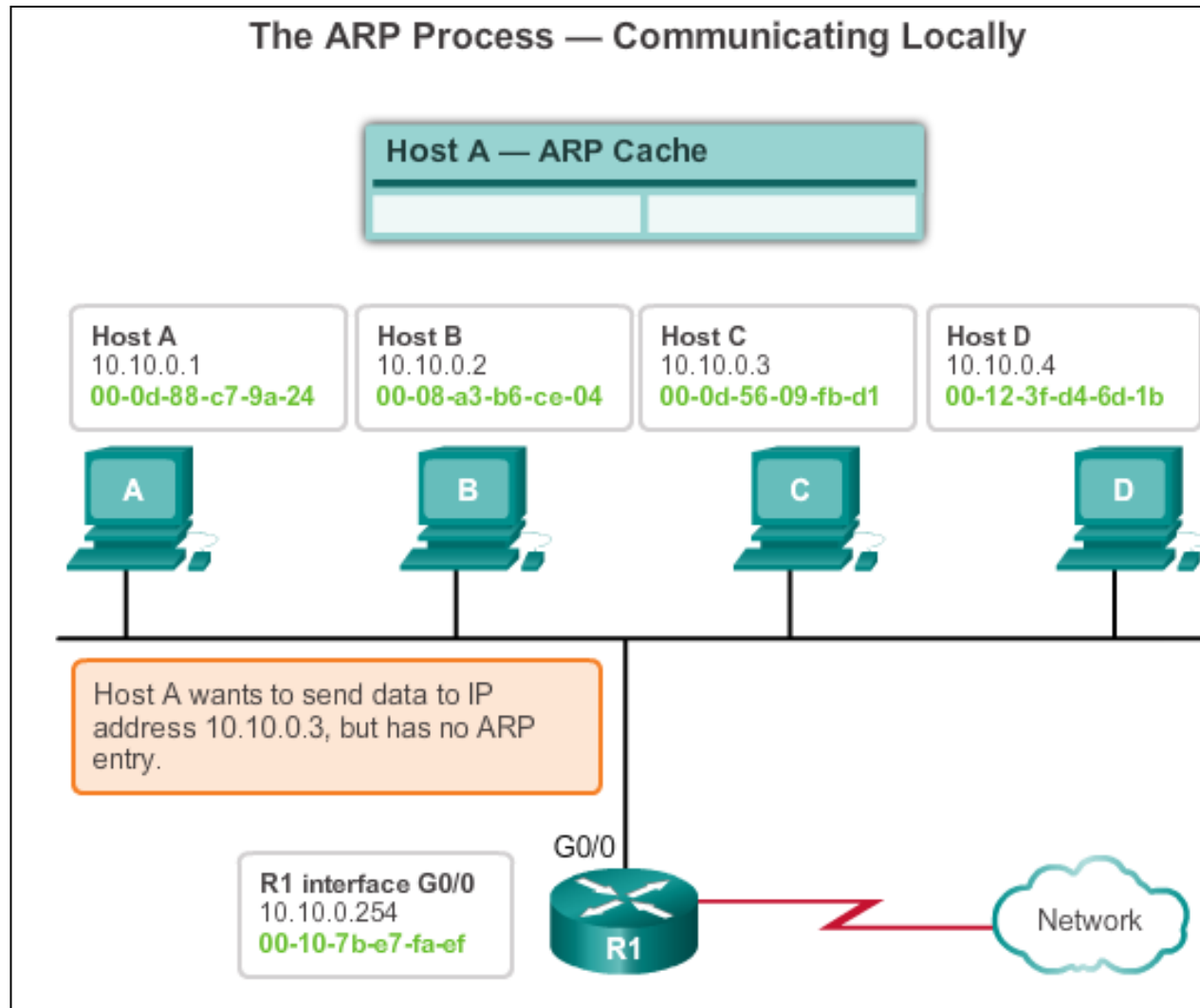
- Used to find the data link layer address that is mapped to the destination IPv4 address.
- As a node receives frames from the media, it records the source IP and MAC address as a mapping in the ARP table.

## ARP Request

- Layer 2 broadcast to all devices on the Ethernet LAN.
- The node that matches the IP address in the broadcast will reply.
- If no device responds to the ARP request, the packet is dropped because a frame cannot be created.

**Note:** Static map entries can be entered in an ARP table, but this is rarely done.

# ARP Operation

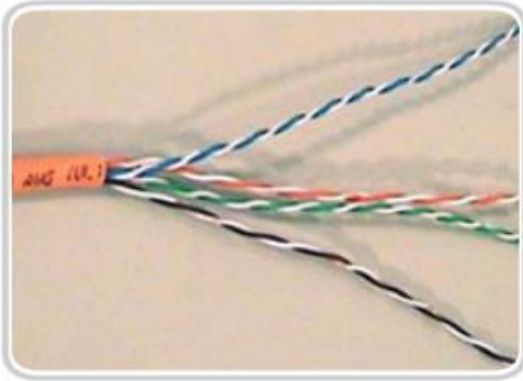


# Physical Layer Fundamental Principles

Media	Physical Components	Frame Encoding Technique	Signalling Method
<b>Copper Cable</b>	<ul style="list-style-type: none"><li>• UTP</li><li>• Coaxial</li><li>• Connectors</li><li>• NICs</li><li>• Ports</li><li>• Interfaces</li></ul>	<ul style="list-style-type: none"><li>• Manchester Encoding</li><li>• Non-Return to Zero (NRZ) techniques</li><li>• 4B/5B codes are used with Multi-Level Transition Level 3 (MLT-3) signaling</li><li>• 8B/10B</li><li>• PAM5</li></ul>	<ul style="list-style-type: none"><li>• Changes in the electromagnetic field</li><li>• Intensity of the electromagnetic field</li><li>• Phase of the electromagnetic wave</li></ul>
<b>Fiber Optic Cable</b>	<ul style="list-style-type: none"><li>• Single-mode Fiber</li><li>• Multimode Fiber</li><li>• Connectors</li><li>• NICs</li><li>• Interfaces</li><li>• Lasers and LEDs</li><li>• Photoreceptors</li></ul>	<ul style="list-style-type: none"><li>• Pulses of light</li><li>• Wavelength multiplexing using different colors</li></ul>	<ul style="list-style-type: none"><li>• A pulse equals 1.</li><li>• No pulse is 0.</li></ul>
<b>Wireless Media</b>	<ul style="list-style-type: none"><li>• Access Points</li><li>• NICs</li><li>• Radio</li><li>• Antennae</li></ul>	<ul style="list-style-type: none"><li>• DSSS (direct-sequence spread-spectrum)</li><li>• OFDM (orthogonal frequency division multiplexing)</li></ul>	<ul style="list-style-type: none"><li>• Radio waves</li></ul>

## Copper Cabling

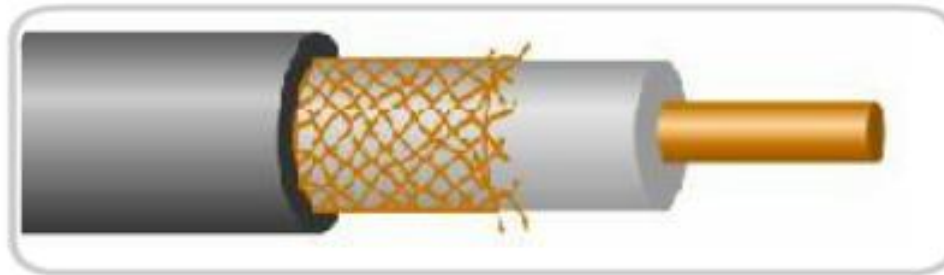
# Copper Media



Unshielded Twisted  
Pair (UTP) Cable



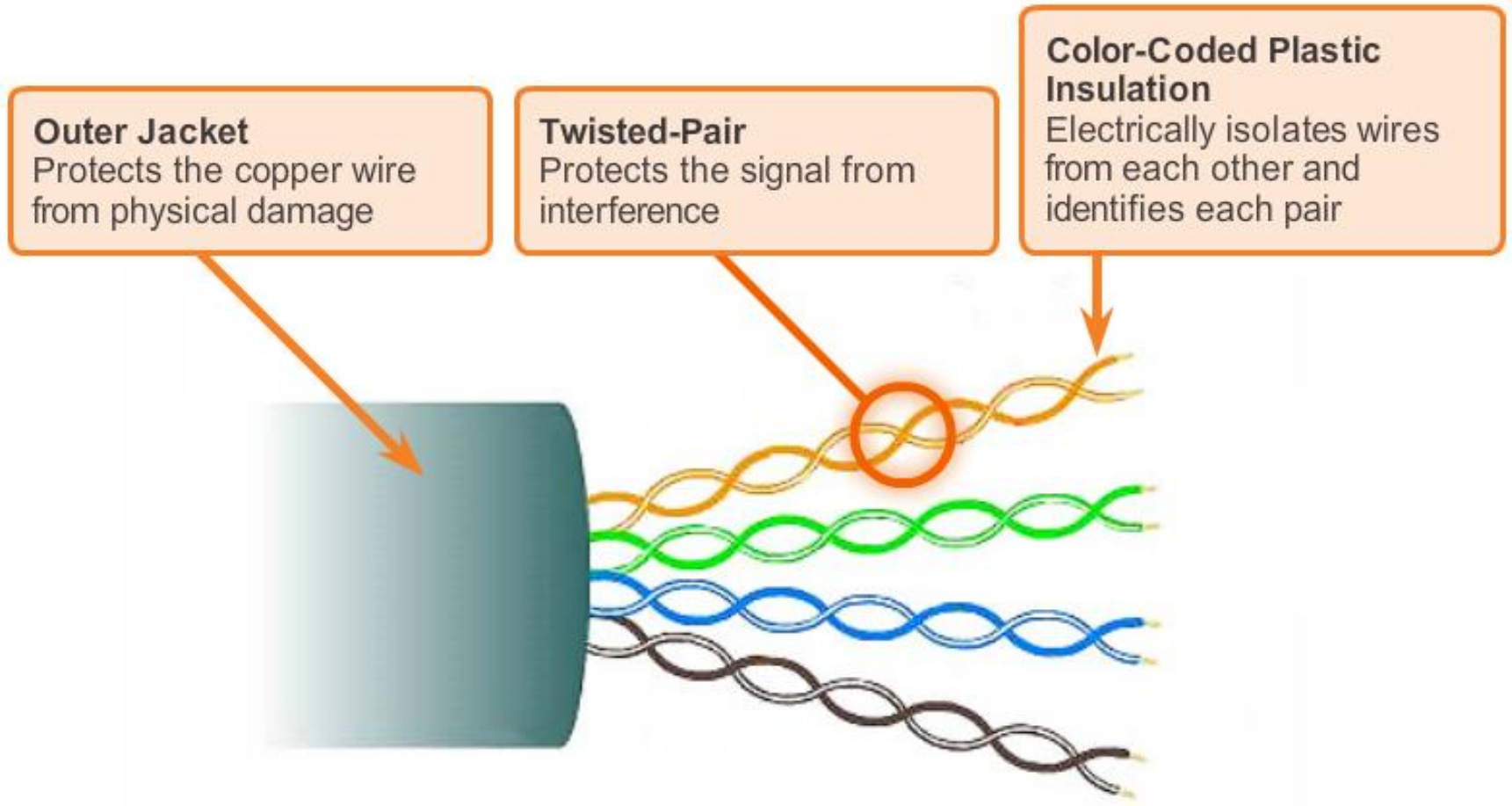
Shielded Twisted  
Pair (STP) Cable



Coaxial Cable

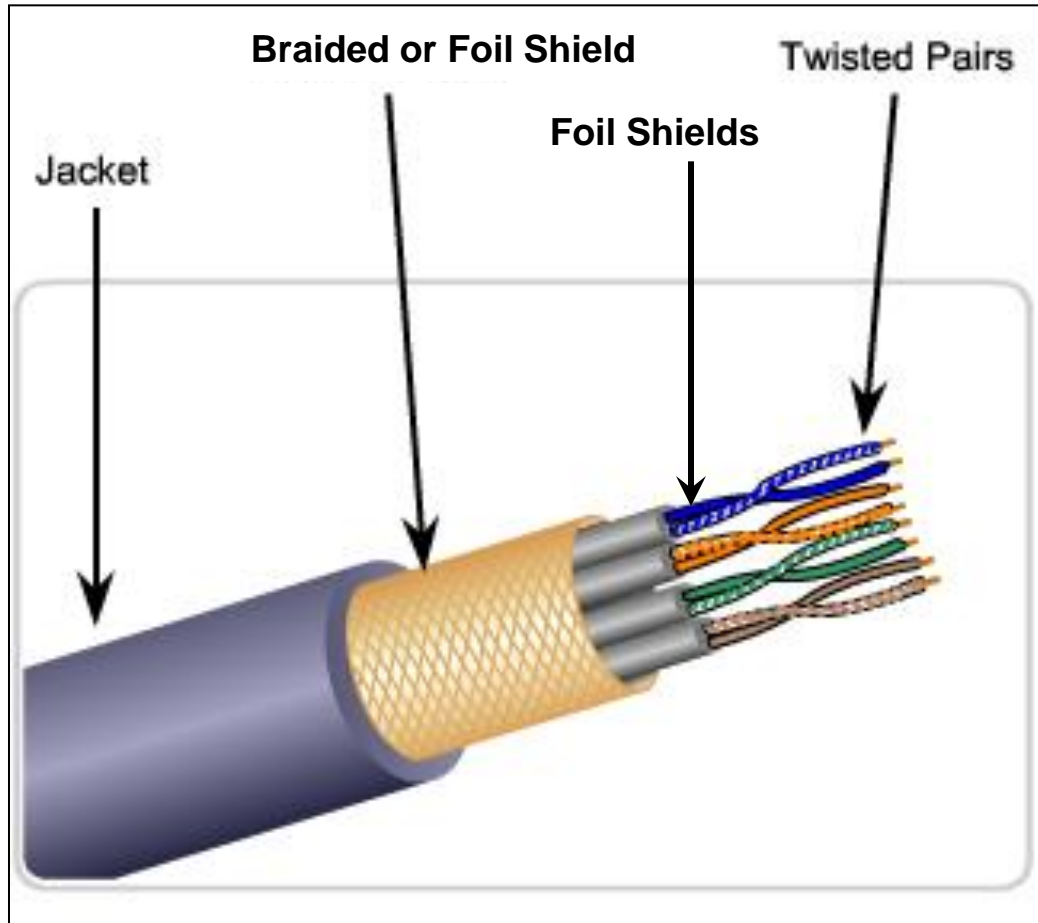
## Copper Cabling

# UTP Cable



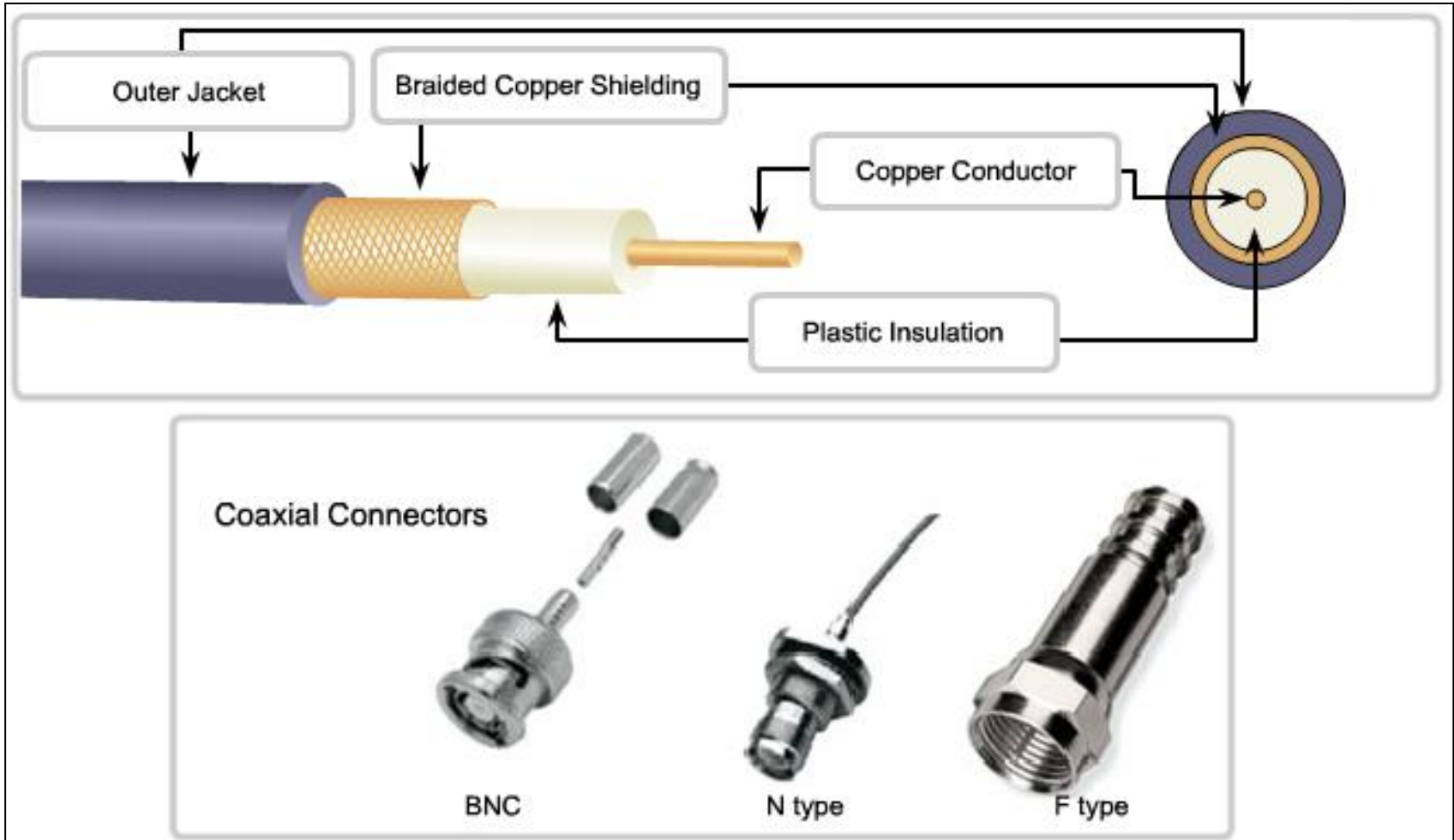
# Copper Cabling

## STP Cable



## Copper Cabling

# Coaxial Cable

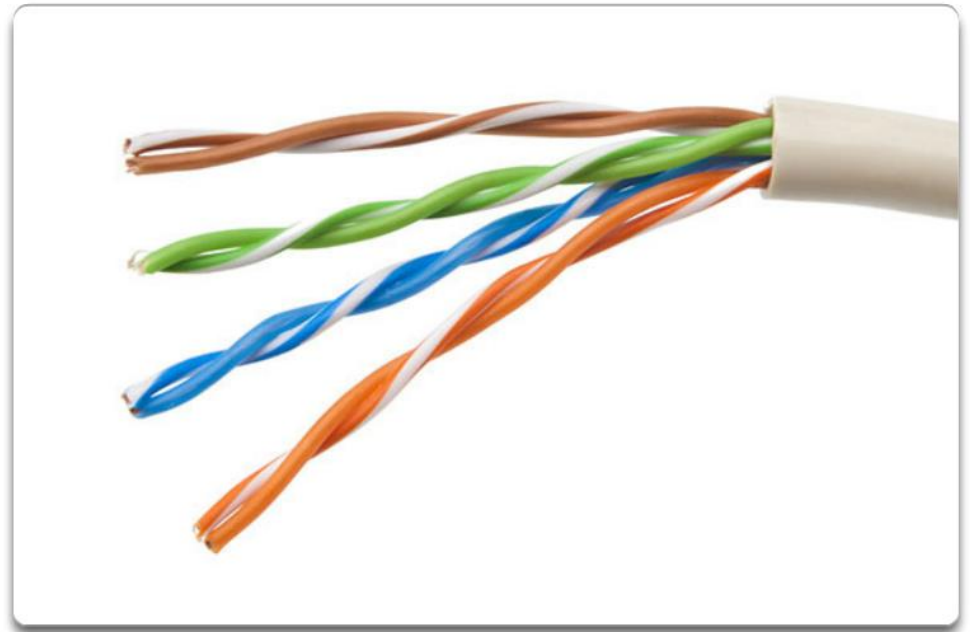




# UTP Cabling

UTP cable does not use shielding to counter the effects of EMI and RFI. Instead, cable designers have discovered that they can limit the negative effect of crosstalk by:

- Cancellation
- Varying the number of twists per wire pair



## UTP Cabling

# UTP Connectors

RJ-45 UTP Plugs

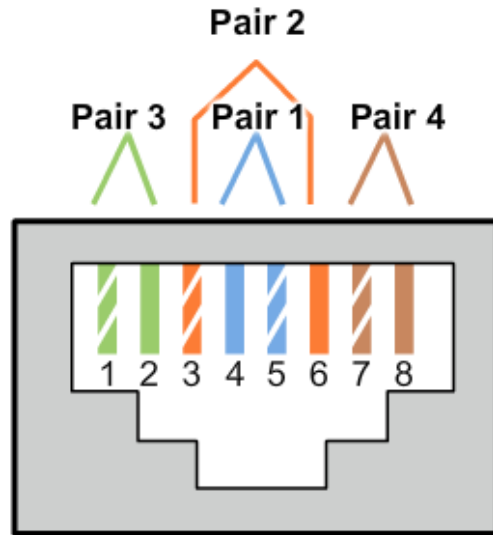


RJ-45 UTP Socket

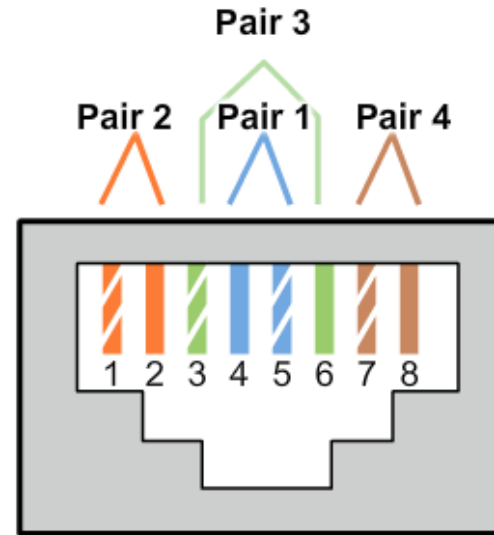


## UTP Cabling

# Types of UTP Cable



**T568A**



**T568B**

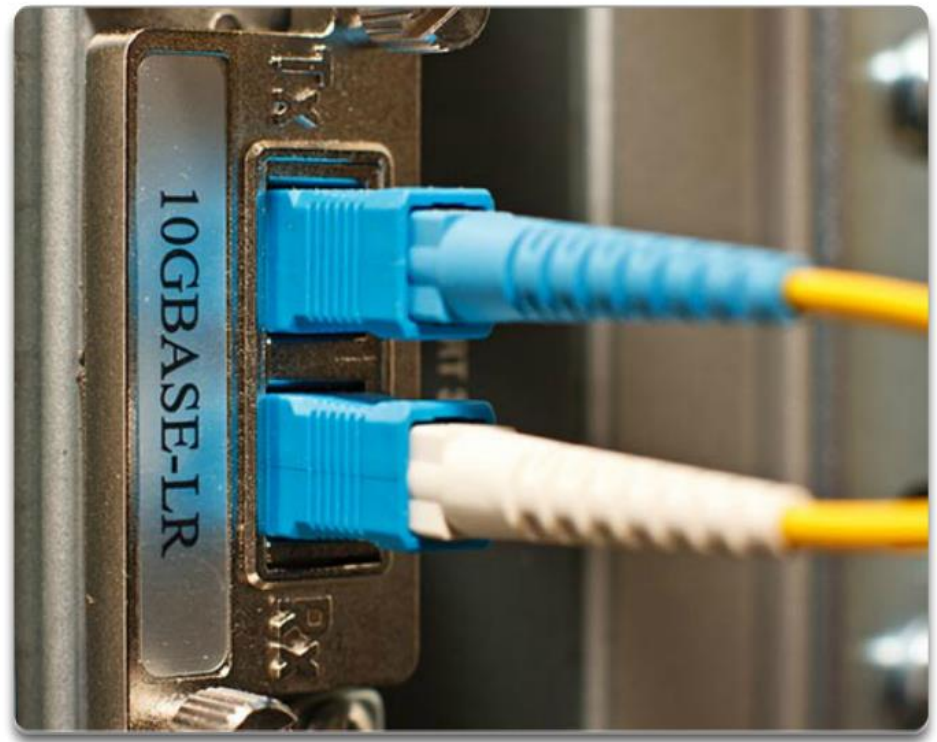
Cable Type	Standard	Application
Ethernet Straight-through	Both ends T568A or both ends T568B	Connects a network host to a network device such as a switch or hub.
Ethernet Crossover	One end T568A, other end T568B	<ul style="list-style-type: none"><li>Connects two network hosts</li><li>Connects two network intermediary devices (switch to switch, or router to router)</li></ul>
Rollover	Cisco proprietary	Connects a workstation serial port to a router console port, using an adapter.

## Fiber Optic Cabling

# Properties of Fiber Optic Cabling

Fiber-optic cabling is now being used in four types of industry:

- Enterprise Networks
- Fiber-to-the-home (FTTH) and Access Networks
- Long-Haul Networks
- Submarine Networks



## Fiber Optic Cabling

# Network Fiber Connectors



ST Connectors



SC Connectors






LC Connector



Duplex Multimode LC Connectors

# Types of Wireless Media

 The Wi-Fi logo, featuring the letters 'Wi' and 'Fi' in a stylized, rounded font. Above the 'i' in 'Wi' and the 'i' in 'Fi' are three curved lines representing radio waves, all in a light blue color.	<ul style="list-style-type: none"><li>• IEEE 802.11 standards</li><li>• Commonly referred to as Wi-Fi.</li><li>• Uses CSMA/CA</li><li>• Variations include:<ul style="list-style-type: none"><li>• 802.11a: 54 Mbps, 5 GHz</li><li>• 802.11b: 11 Mbps, 2.4 GHz</li><li>• 802.11g: 54 Mbps, 2.4 GHz</li><li>• 802.11n: 600 Mbps, 2.4 and 5 GHz</li><li>• 802.11ac: 1 Gbps, 5 GHz</li><li>• 802.11ad: 7 Gbps, 2.4 GHz, 5 GHz, and 60 GHz</li></ul></li></ul>
 The Bluetooth logo, consisting of a blue circular icon with a white stylized 'B' inside, followed by the word 'Bluetooth' in a bold, black, sans-serif font with a registered trademark symbol.	<ul style="list-style-type: none"><li>• IEEE 802.15 standard</li><li>• Supports speeds up to 3 Mb/s</li><li>• Provides device pairing over distances from 1 to 100 meters.</li></ul>
 The WiMAX logo, featuring the letters 'Wi' and 'MAX' in a stylized, rounded font. Above the 'i' in 'Wi' are three curved lines representing radio waves, all in a light blue color.	<ul style="list-style-type: none"><li>• IEEE 802.16 standard</li><li>• Provides speeds up to 1 Gbps</li><li>• Uses a point-to-multipoint topology to provide wireless broadband access.</li></ul>



# Introduction to the Ethernet Frame

## IEEE 802.3

7	1	6	6	2	46 to 1500	4
Preamble	Start of Frame Delimiter	Destination Address	Source Address	Length	802.2 Header and Data	Frame Check Sequence

**Preamble and Start Frame Delimiter Fields –**  
Used for synchronization between the sending and receiving devices.

**Length/Type Field –**  
Defines the exact length of the frame's data field; describes which protocol is implemented.

**Data and Pad Fields –**  
Contains the encapsulated data from a higher layer, an IPv4 packet.

# Introduction to the Ethernet Frame (cont.)

## IEEE 802.3

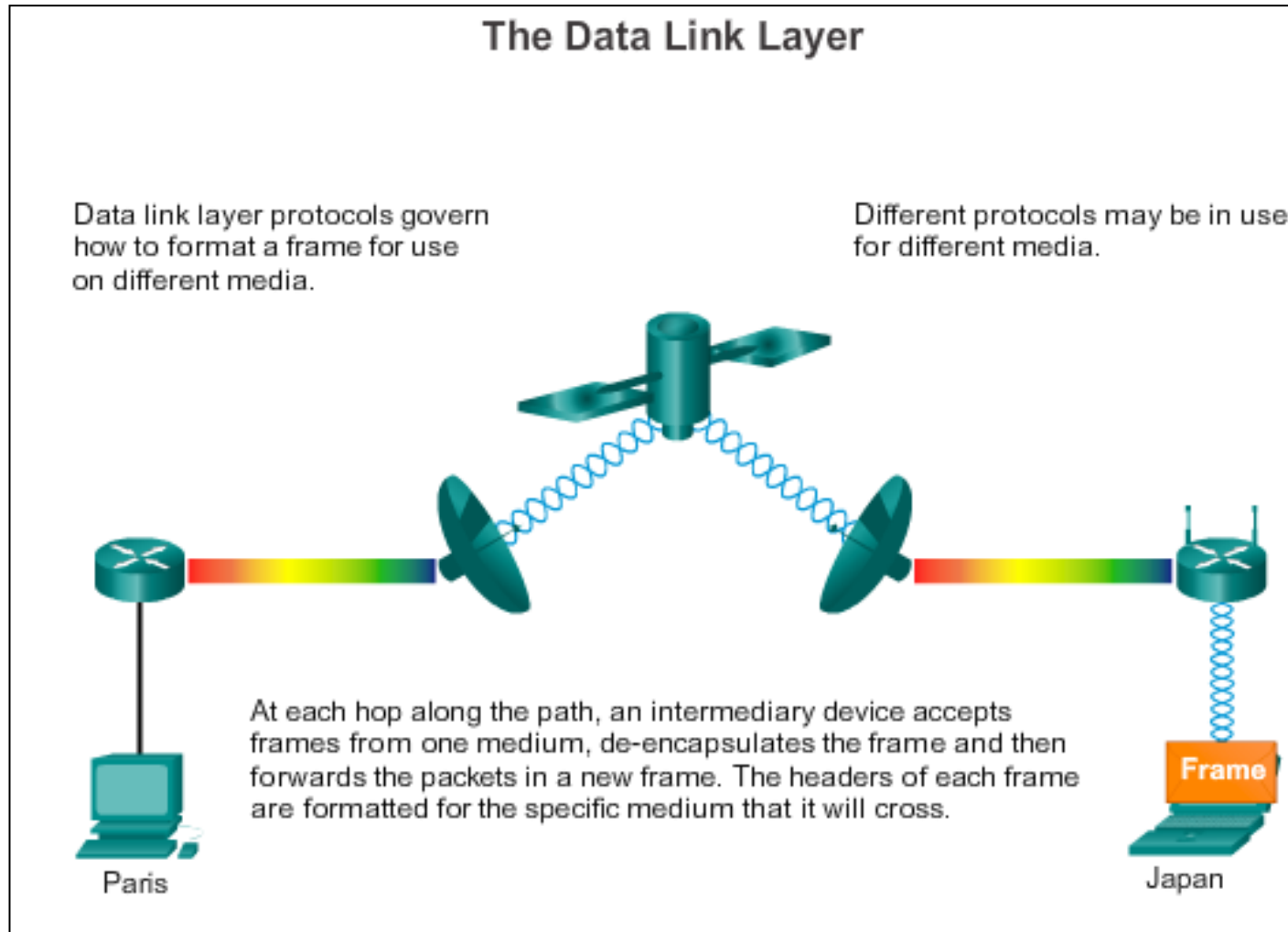
7	1	6	6	2	46 to 1500	4
Preamble	Start of Frame Delimiter	Destination Address	Source Address	Length	802.2 Header and Data	Frame Check Sequence

### Frame Check Sequence Field

Used to detect errors in a frame with cyclic redundancy check (4 bytes); if calculations match at source and receiver, no error occurred.

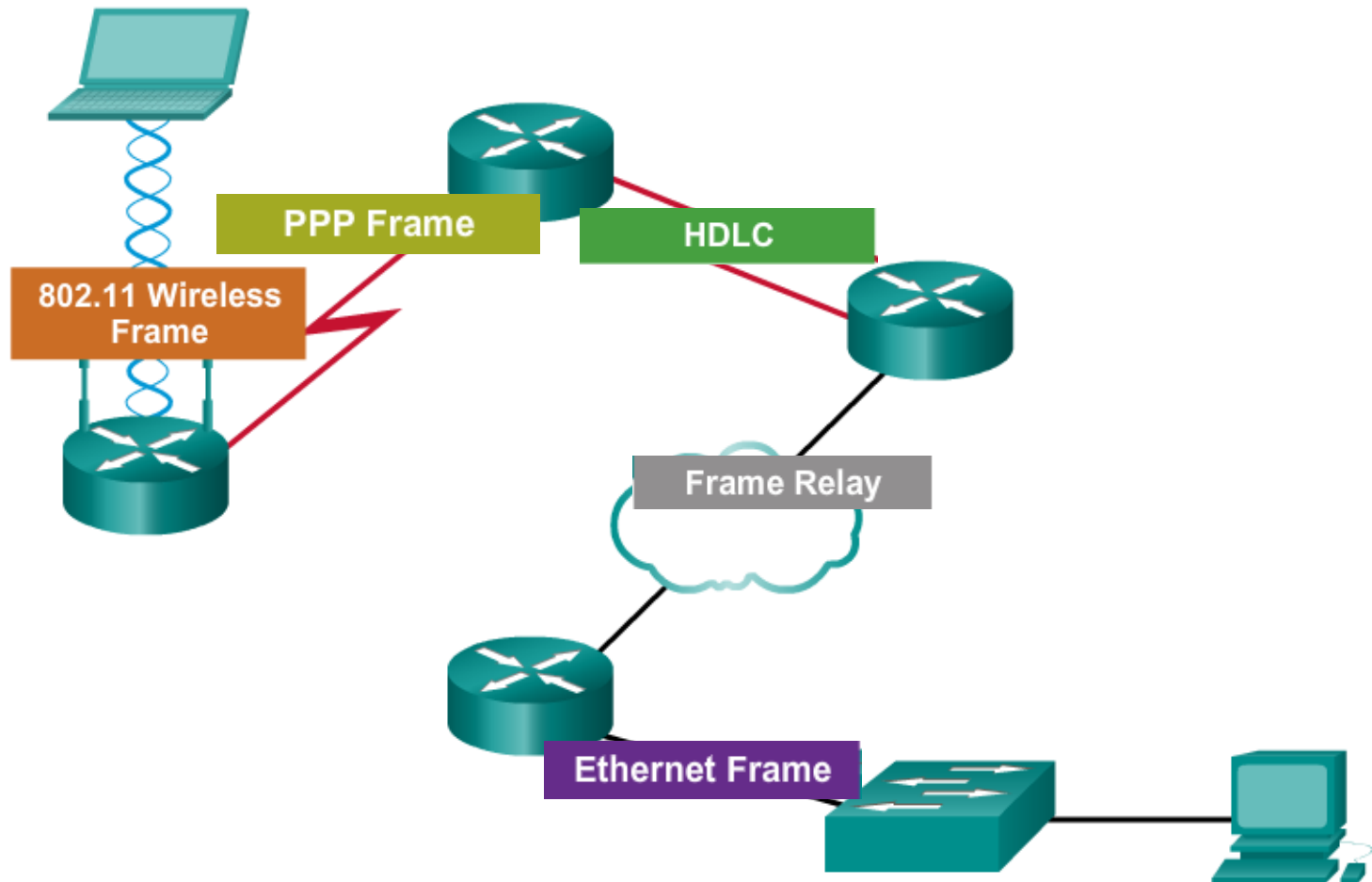


# End-to-End Connectivity, MAC, and IP (cont.)



# LAN and WAN Frames

## Examples of Layer 2 Protocols



# The Network Layer

Start

The network layer, or OSI Layer 3, provides services to allow end devices to exchange data across the network. To accomplish this end-to-end transport, the network layer uses four basic processes:

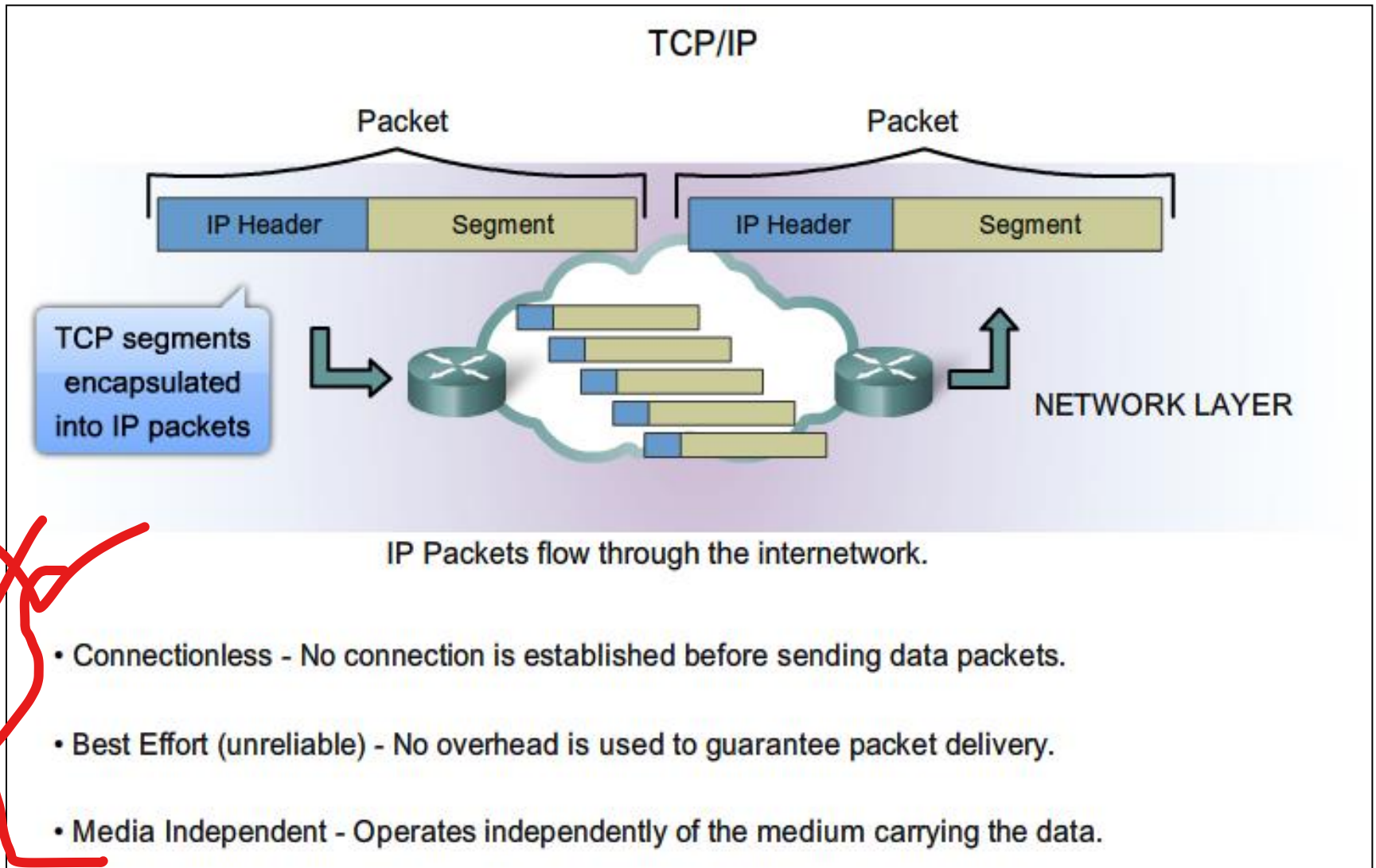
- Addressing end devices
- Encapsulation
- Routing
- De-encapsulating

# Network Layer Protocols

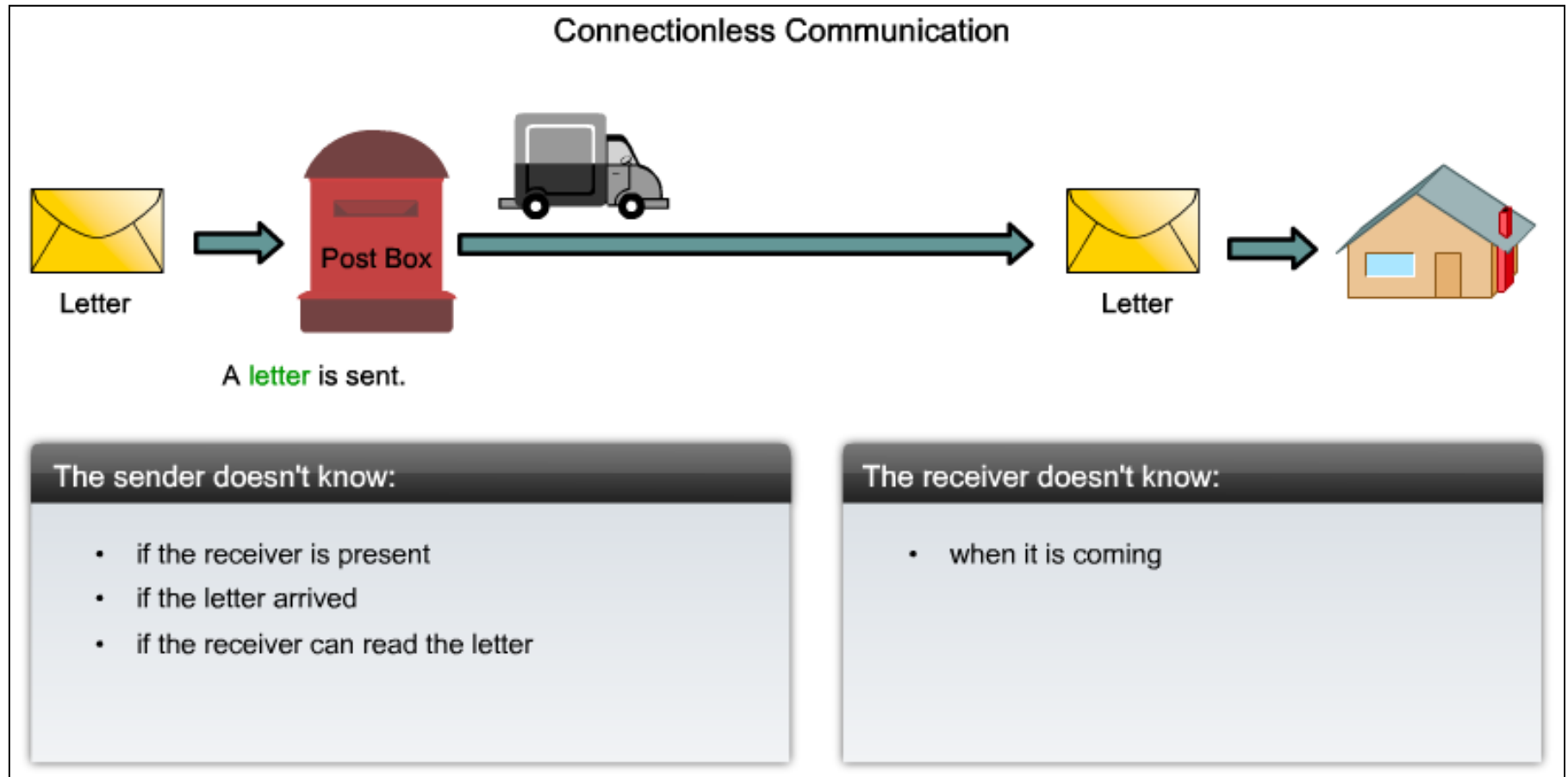
**Common network layer protocols include:**

- IP version 4 (IPv4)
- IP version 6 (IPv6)

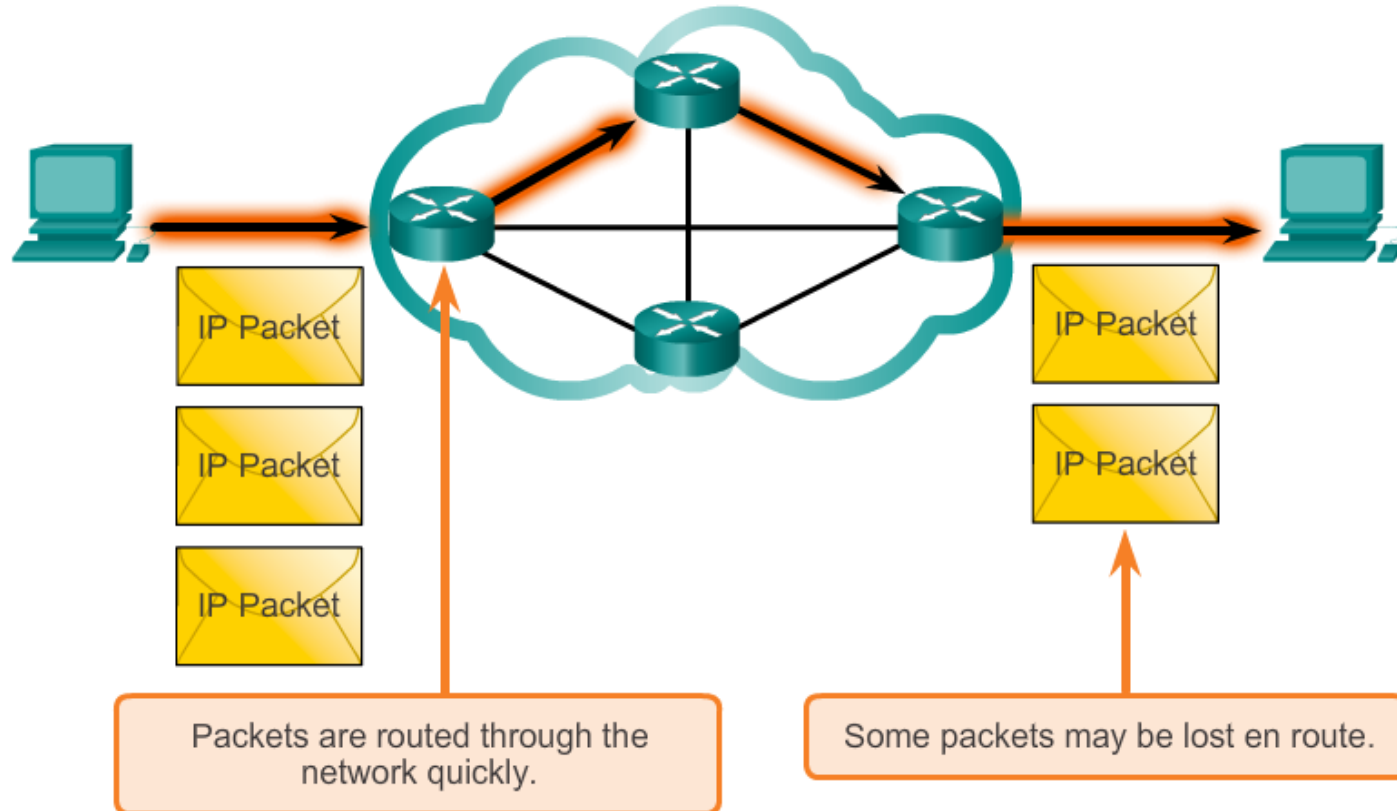
# IP Components



# IP - Connectionless

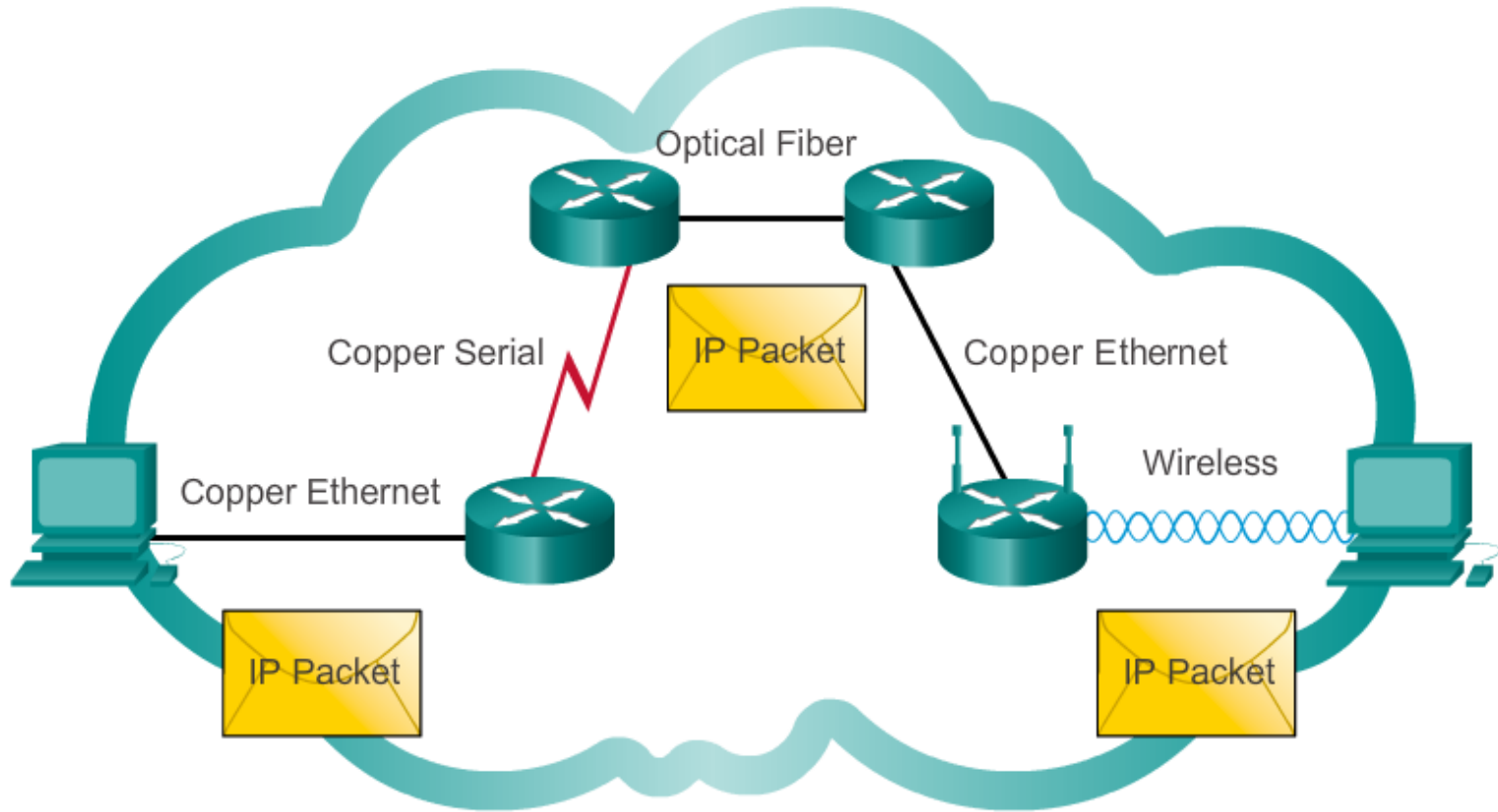


# Best Effort Delivery



As an unreliable network layer protocol, IP does not guarantee that all sent packets will be received. Other protocols manage the process of tracking packets and ensuring their delivery.

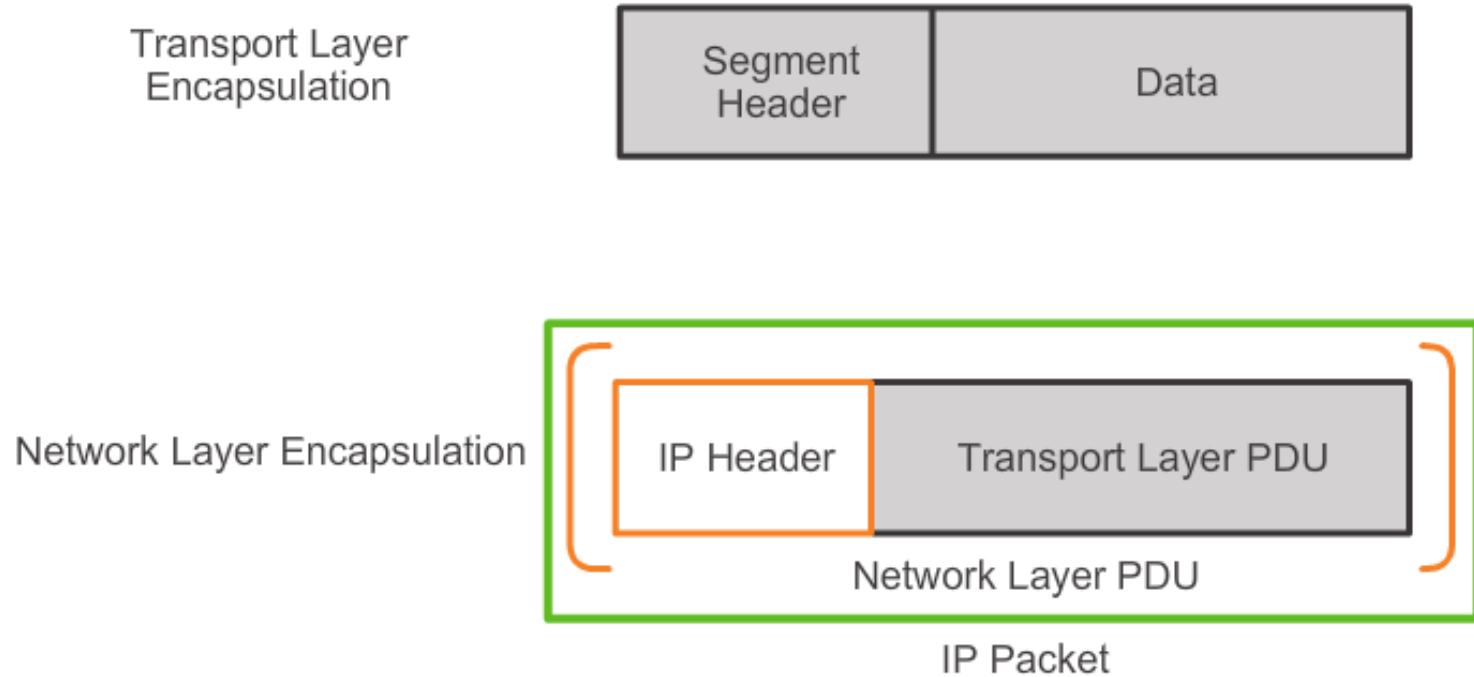
# IP – Media Independent



IP packets can travel over different media.



## IPv4 Packet Encapsulating IP

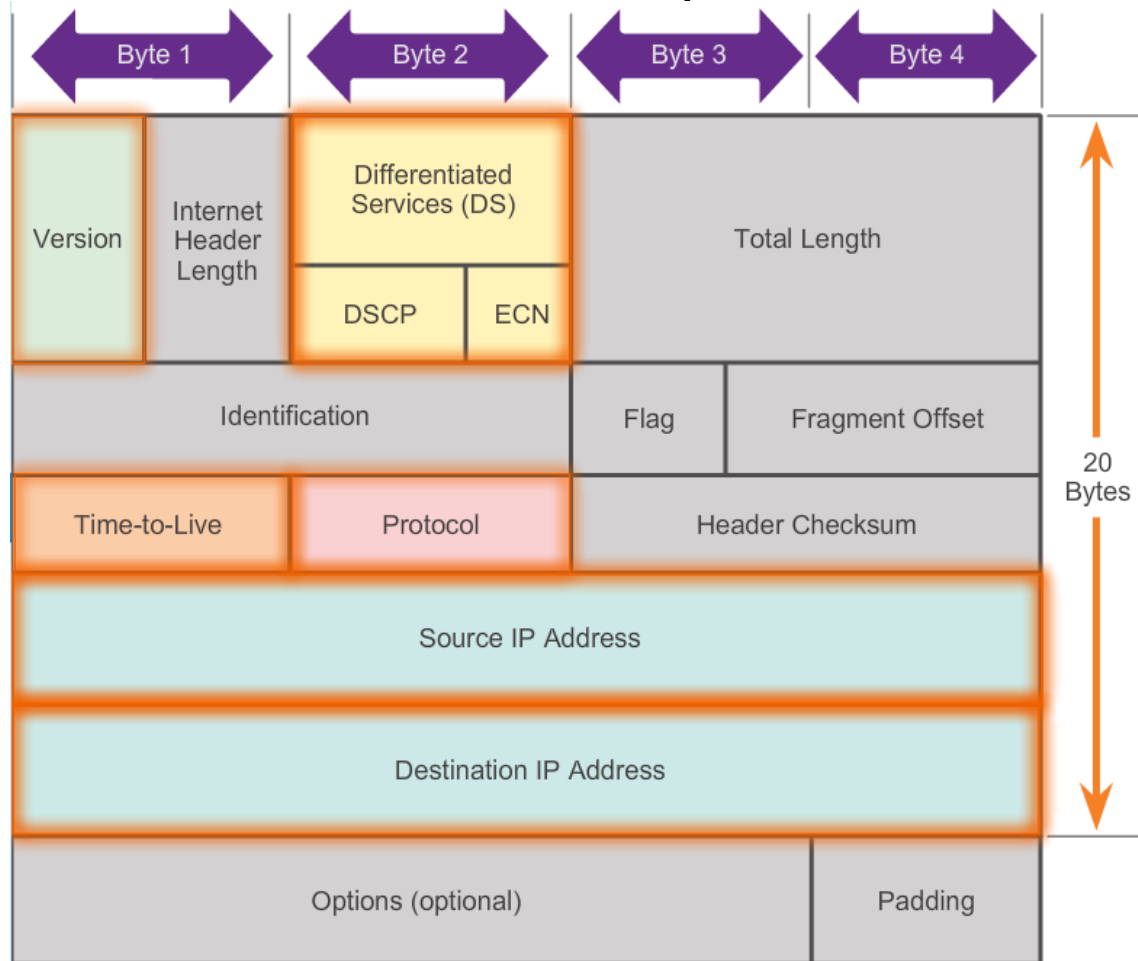


The network layer adds a header so packets can be routed through complex networks and reach their destination. In TCP/IP based networks, the network layer PDU is the IP packet.

## IPv4 Packet

# IPv4 Packet Header

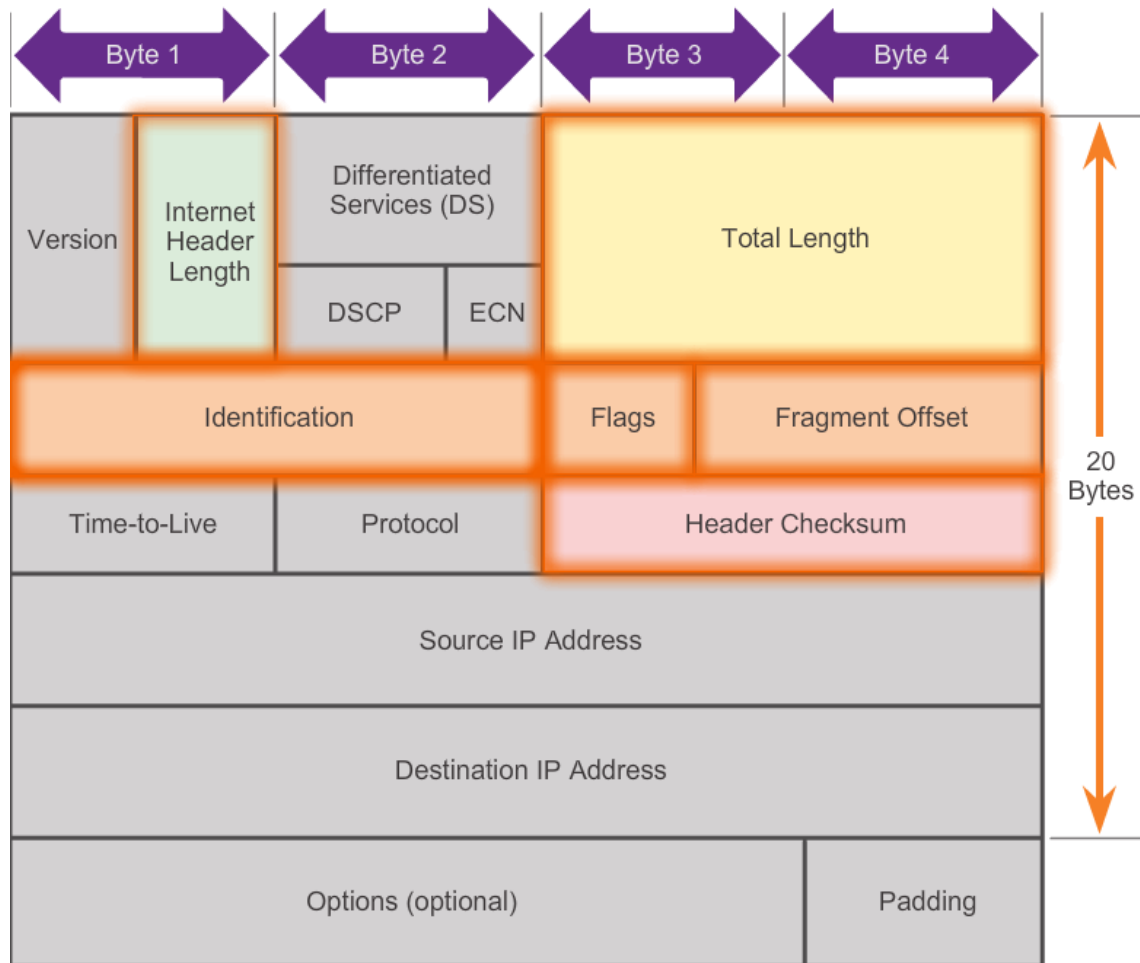
### Contents of the IPv4 packet header



## IPv4 Packet

# IPv4 Header Fields

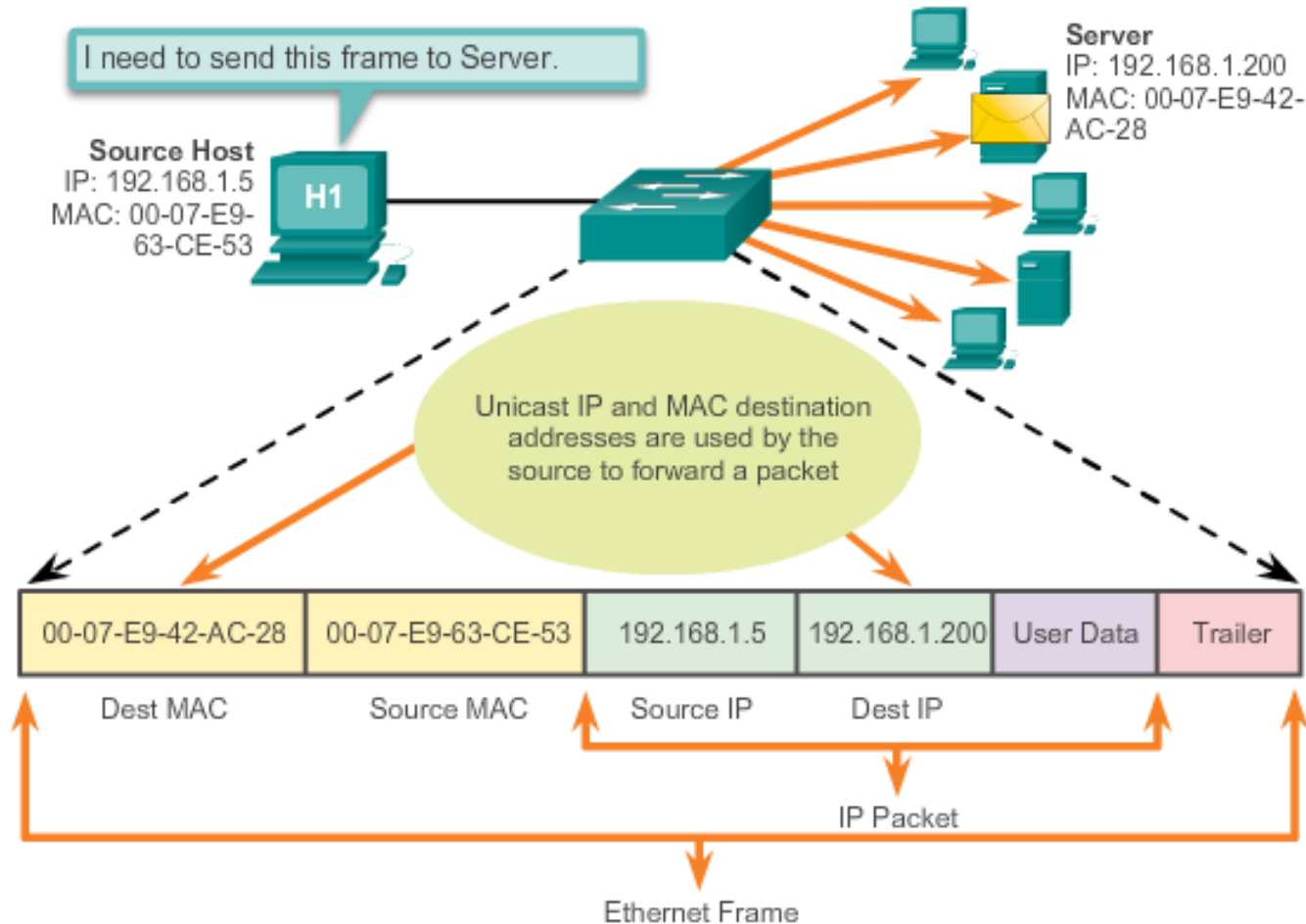
### Contents of the IPv4 header fields



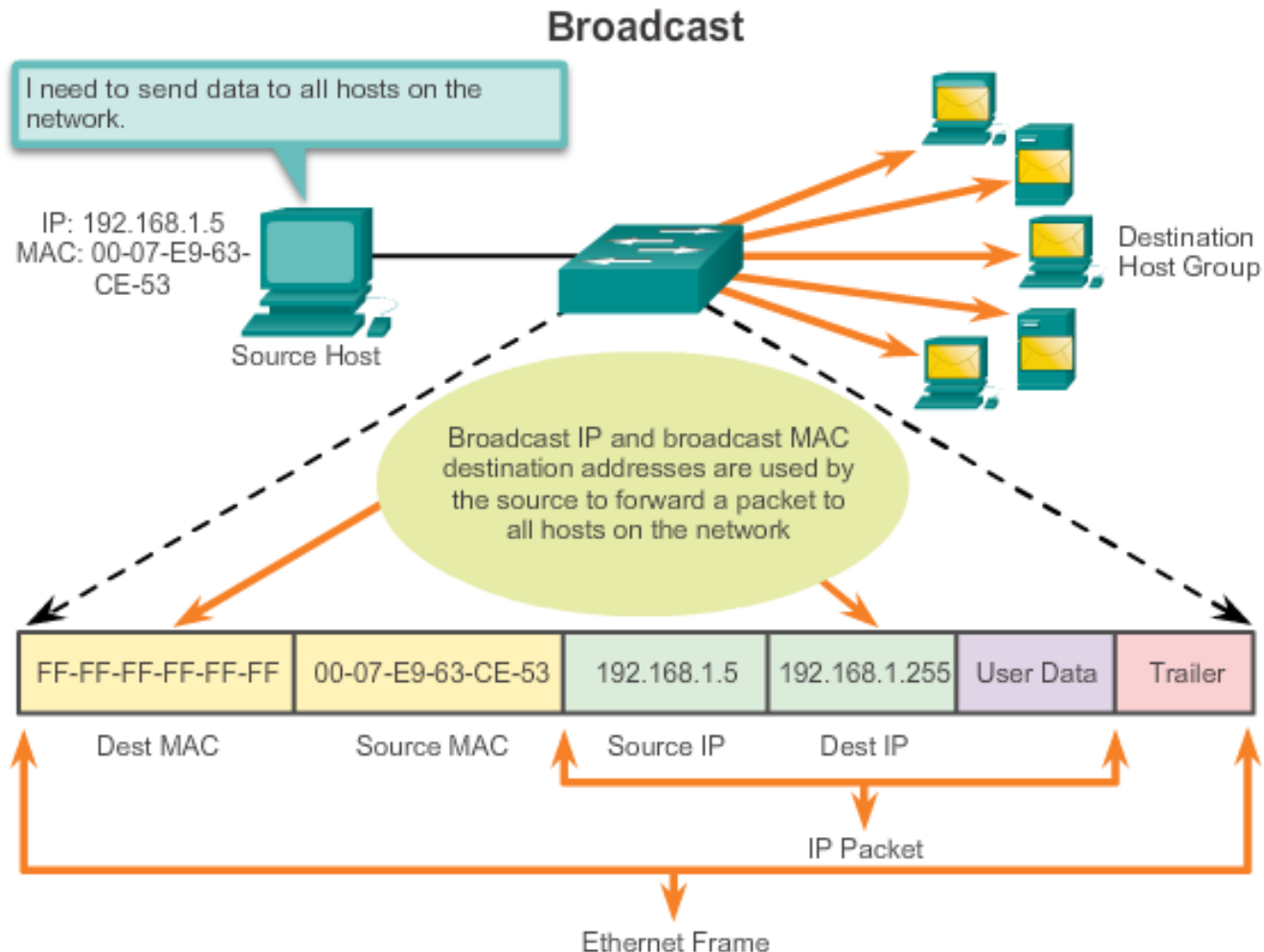
# Unicast Address

from  
(Not Covered)

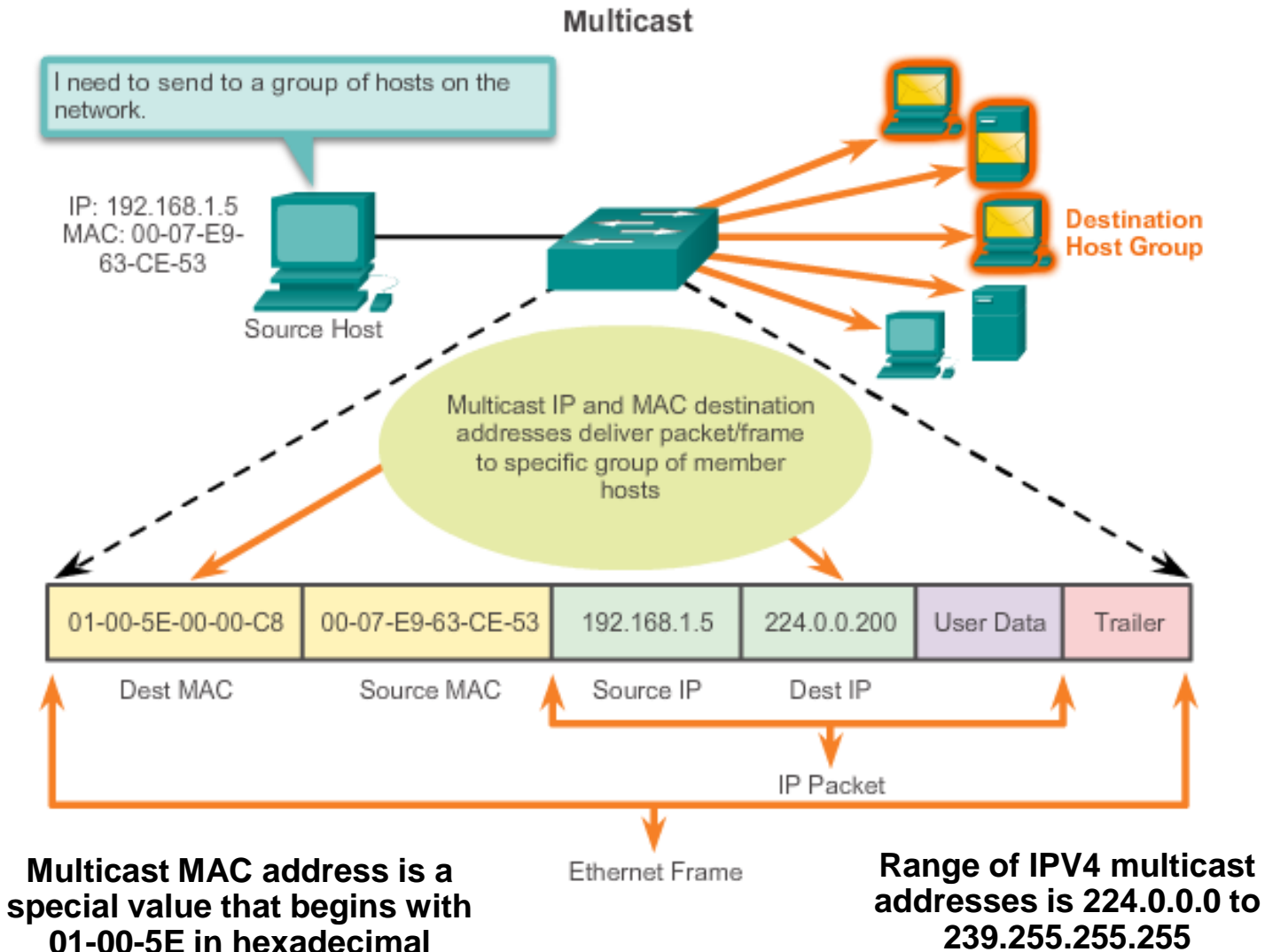
## Unicast



# Broadcast MAC Address



# Multicast Address



# Sample IPv4 Headers in Packet Tracer

Microsoft: \Device\NPF\_{7BB3C130-30C5-4419-B79E-C0868085ABED} [Wireshark 1.8.2 (SVN Rev 44520 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
16	3.64050300	192.168.1.109	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128
17	3.64506800	192.168.1.1	192.168.1.109	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=64
18	3.68215500	192.168.1.109	38.112.107.53	TCP	54	55502 > https [ACK] Seq=1 Ack=134 Win=16661 Len=0
19	4.19945400	fe80::15ff:98d8:d28ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
20	4.60748800	fe80::15ff:98d8:d28ff02::c	fe80::b1ee:c4ae:a11	SSDP	453	HTTP/1.1 200 OK
21	4.64229900	192.168.1.109	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=128
22	4.64509200	192.168.1.1	192.168.1.109	ICMP	74	Echo (ping) reply id=0x0001, seq=6/1536, ttl=64
23	4.73605200	192.168.1.109	255.255.255.255	DB-LSP-	154	Droobox LAN svnc Discoverv Protocol

Frame 16: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0

Ethernet II, Src: IntelCor\_45:5d:c4 (24:77:03:45:5d:c4), Dst: Cisco-Li\_a0:d1:be (00:18:39:a0:d1:be)

Internet Protocol Version 4, Src: 192.168.1.109 (192.168.1.109), Dst: 192.168.1.1 (192.168.1.1)

Version: 4  
Header length: 20 bytes  
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))  
Total Length: 60  
Identification: 0x3704 (14084)  
Flags: 0x00  
Fragment offset: 0  
Time to live: 128  
Protocol: ICMP (1)  
Header checksum: 0x7ffe [correct]  
Source: 192.168.1.109 (192.168.1.109)  
Destination: 192.168.1.1 (192.168.1.1)  
[Source GeoIP: Unknown]  
[Destination GeoIP: Unknown]

Internet Control Message Protocol

0000 00 18 39 a0 d1 be 24 77 03 45 5d c4 08 00 45 00 ..9...\$w .E]...E.  
0010 00 3c 37 04 00 00 80 01 7f fe c0 a8 01 6d c0 a8 .<7.....m..  
0020 01 01 08 00 4d 56 00 01 00 05 61 62 63 64 65 66 ...MV.. ..abcdef  
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv  
0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi

Internet Protocol Version 4 (ip), 20 bytes Packets: 35 Displayed: 35 Marked: 0 Dropped: 0 Profile: Default

# Limitations of IPv4

- IP Address depletion
- Internet routing table expansion
- Lack of end-to-end connectivity





# IPv6

- Increased address space
- Improved packet handling
- Eliminates the need for NAT
- Integrated security
- 4 billion IPv4 addresses  
4,000,000,000
- 340 undecillion IPv6 addresses  
340,000,000,000,000,000,000,000,000,000,000,000,000,000,000

# Encapsulating IPv6

## IPv4 and IPv6 Headers





IPv4 Header

Version	IHL	Type of Service	Total Length	
Identification			Flags	Fragment Offset
Time to Live	Protocol		Header Checksum	
Source Address				
Destination Address				
Options			Padding	

IPv6 Header

Version	Traffic Class	Flow Label	
Payload Length		Next Header	Hop Limit
Source Address			
Destination Address			

### Legend

-  - Field names kept from IPv4 to IPv6
-  - Fields not kept in IPv6
-  - Name & position changed in IPv6
-  - New field in IPv6

# IPv6 Packet Header

