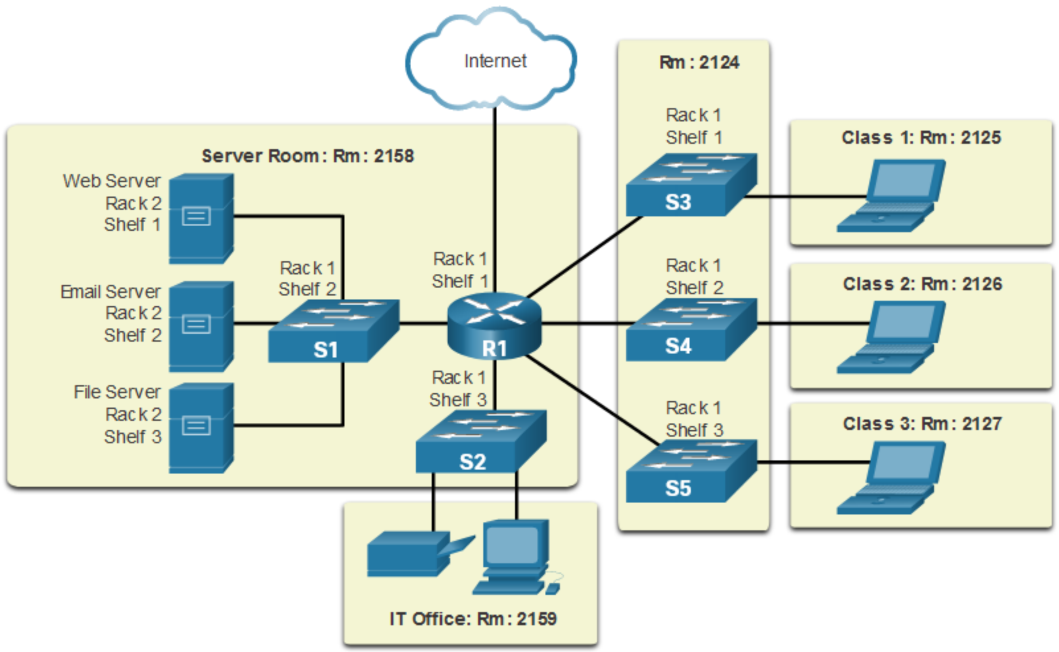
This is still a work in progress I will Update it each week

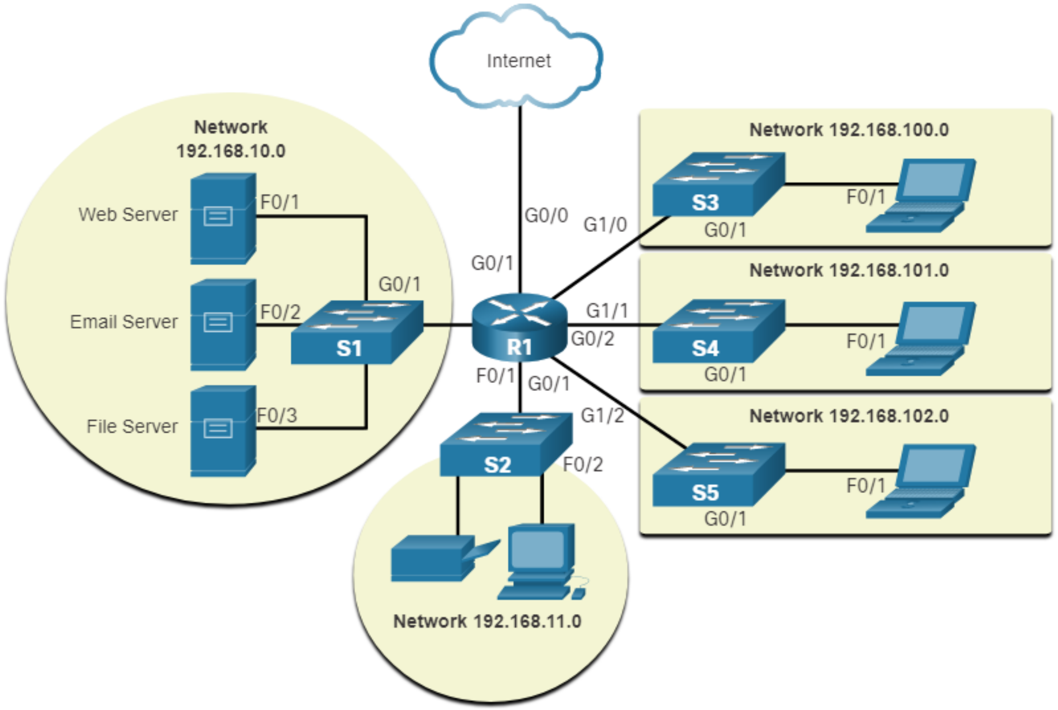
Chapter 1: Network Types, Topologies, and Characteristics

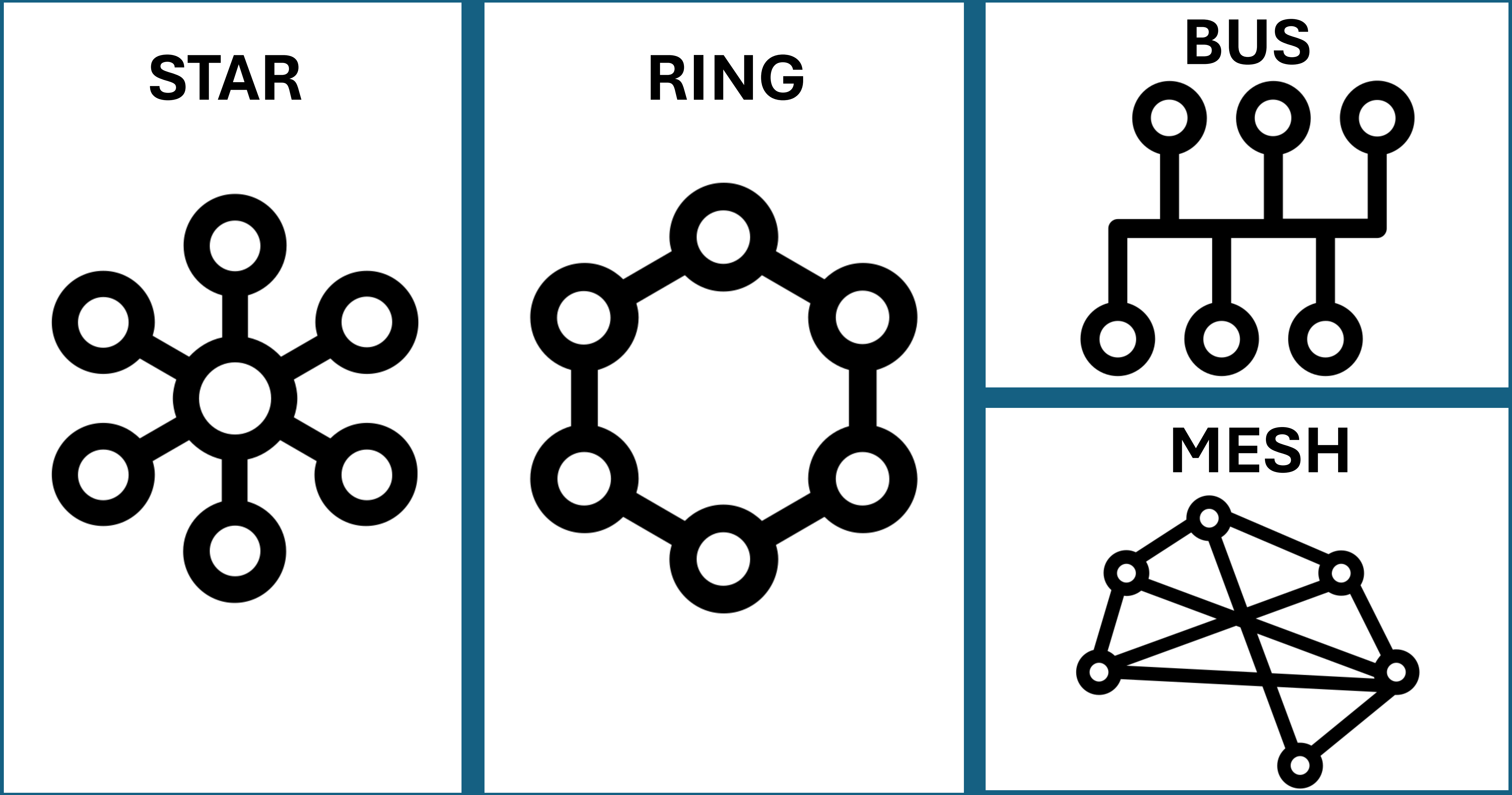
Network topologies

Physical topology diagrams illustrate the physical location of intermediary devices and cable installation.

Logical topology diagrams illustrate devices, ports, and the addressing scheme of the network.

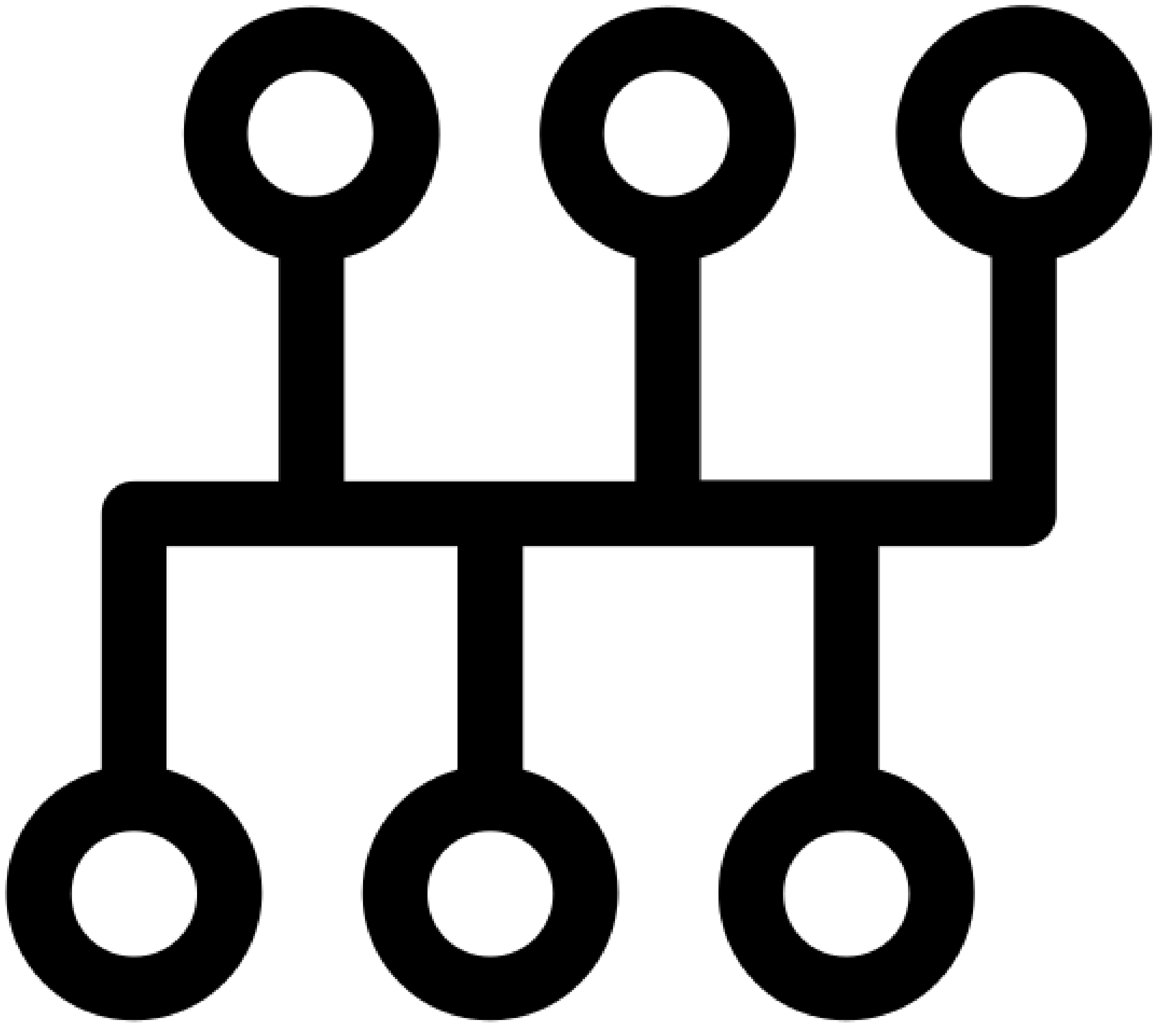





STAR
RING
BUS
MESH

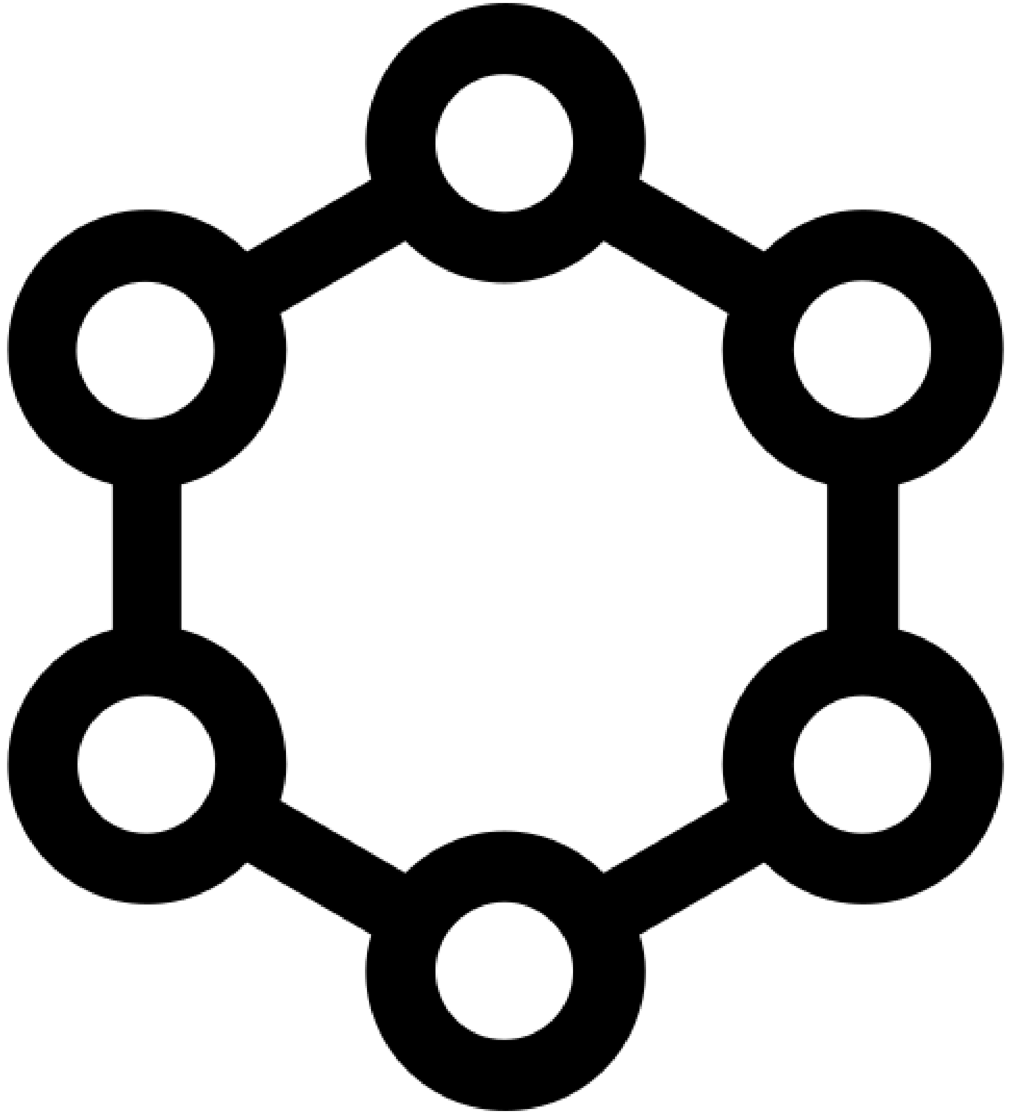
A ***bus topology*** is a physical topology where network nodes are connected to a single cable or bus.

bus topology



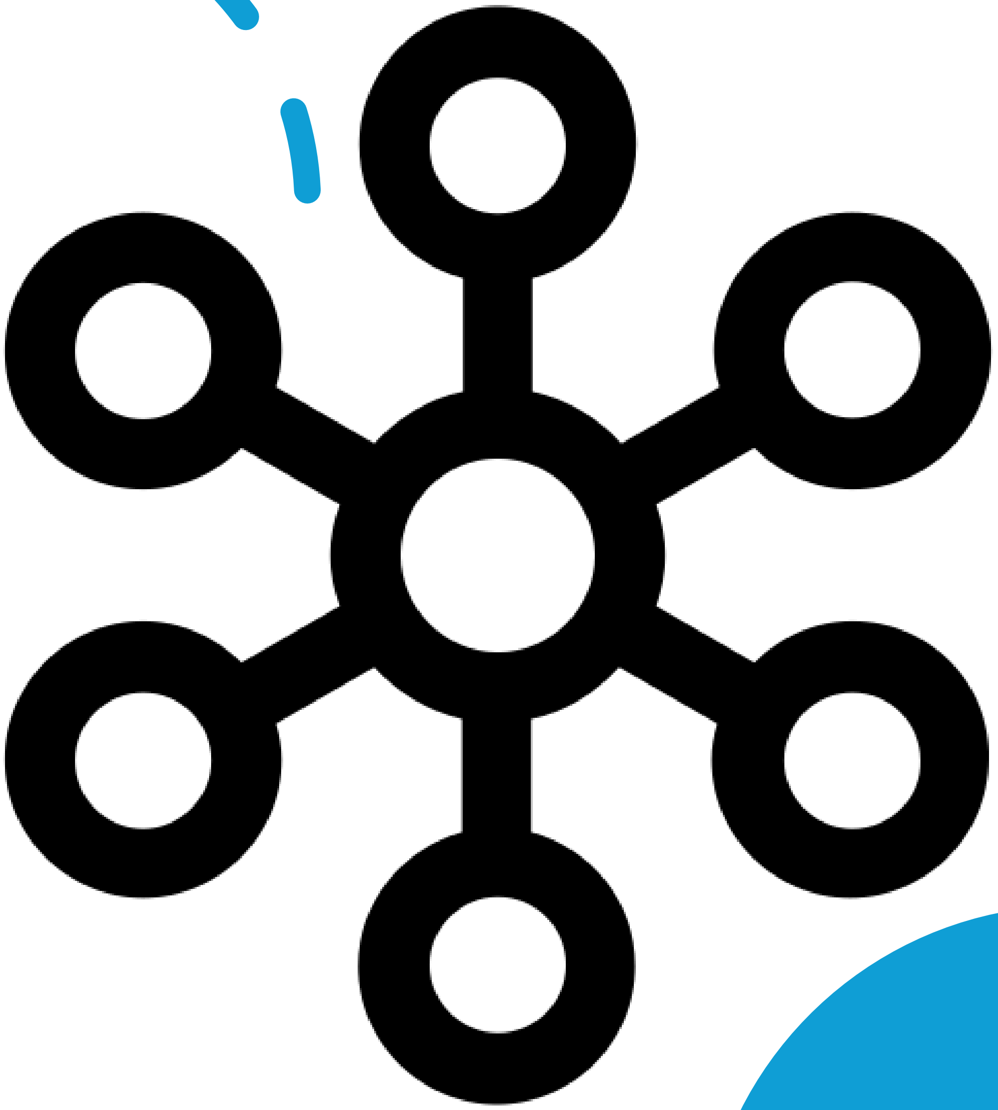
ring topology

- A ***ring topology*** is a physical topology where each node is connected to exactly two other nodes, resembling a ring.



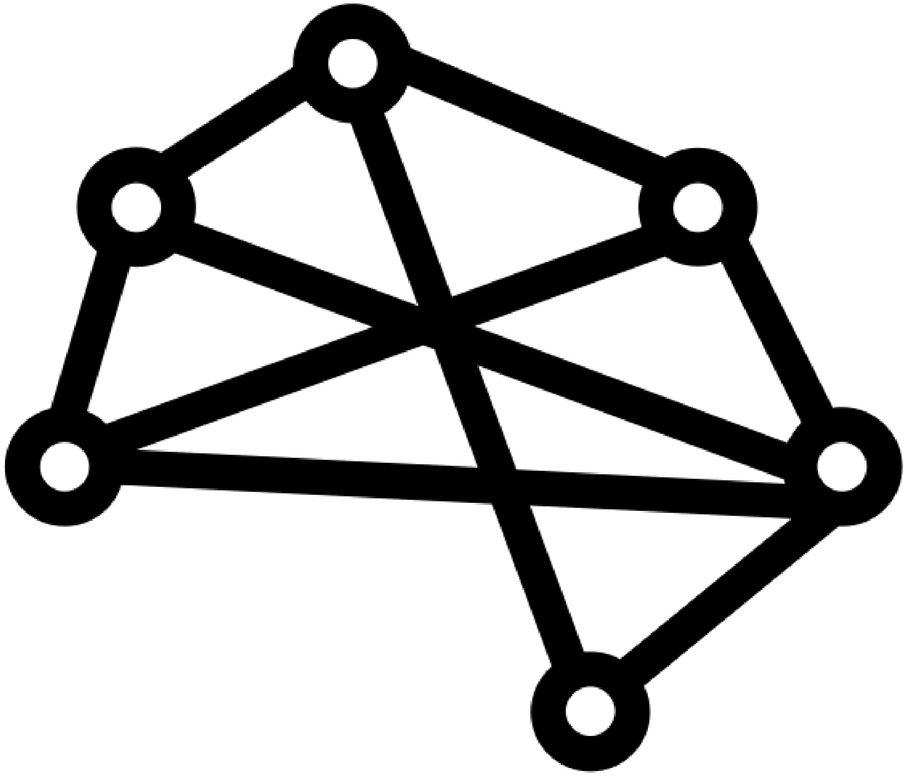
star topology

- A ***star topology*** is a physical topology where each node is connected to a central node, resembling a star or a hub with spokes.



mesh topology

- A ***mesh topology*** is a physical topology where each node is connected to every other node in a network.

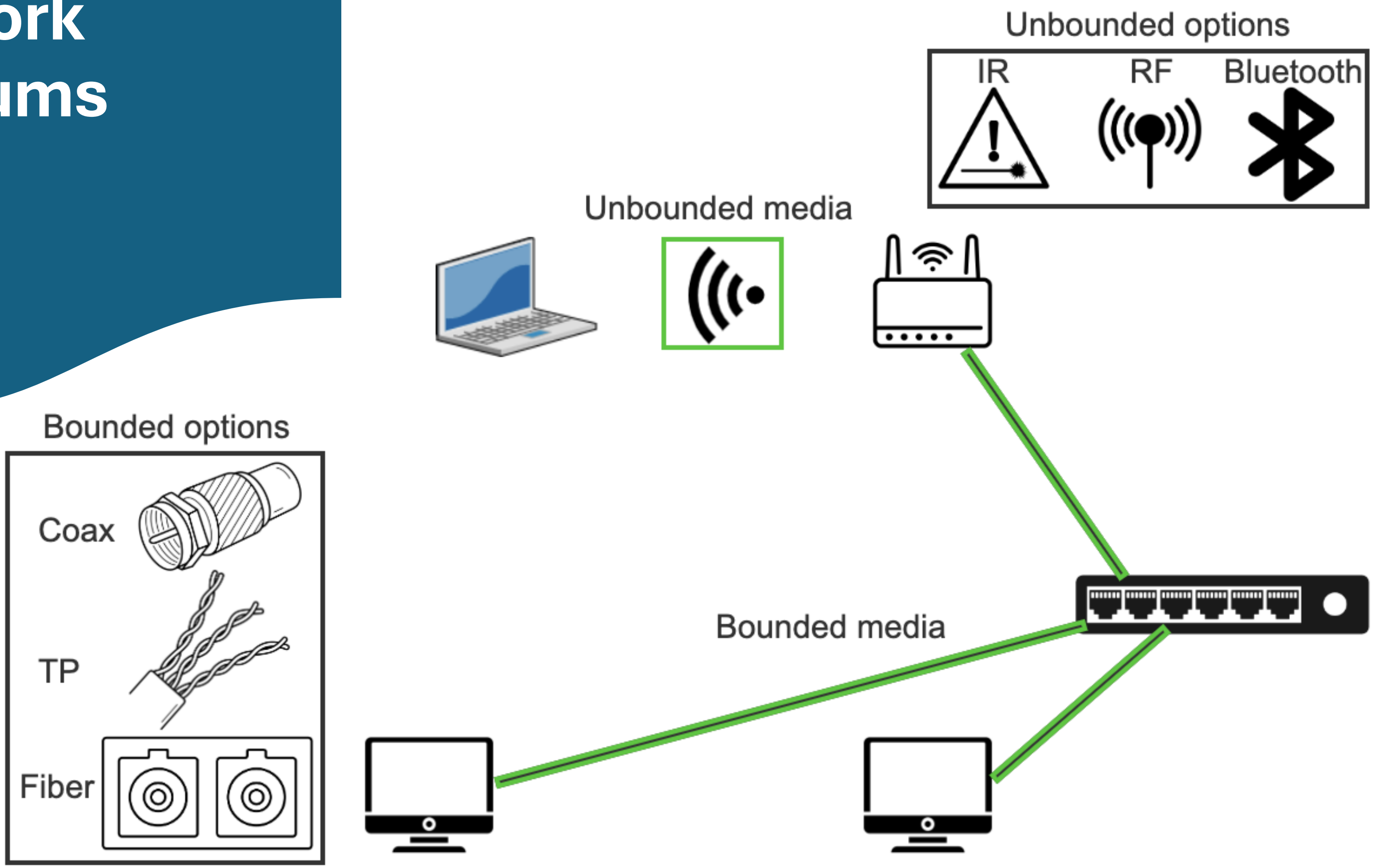


A ***hybrid topology*** is a physical topology where at least two different physical topologies are combined.

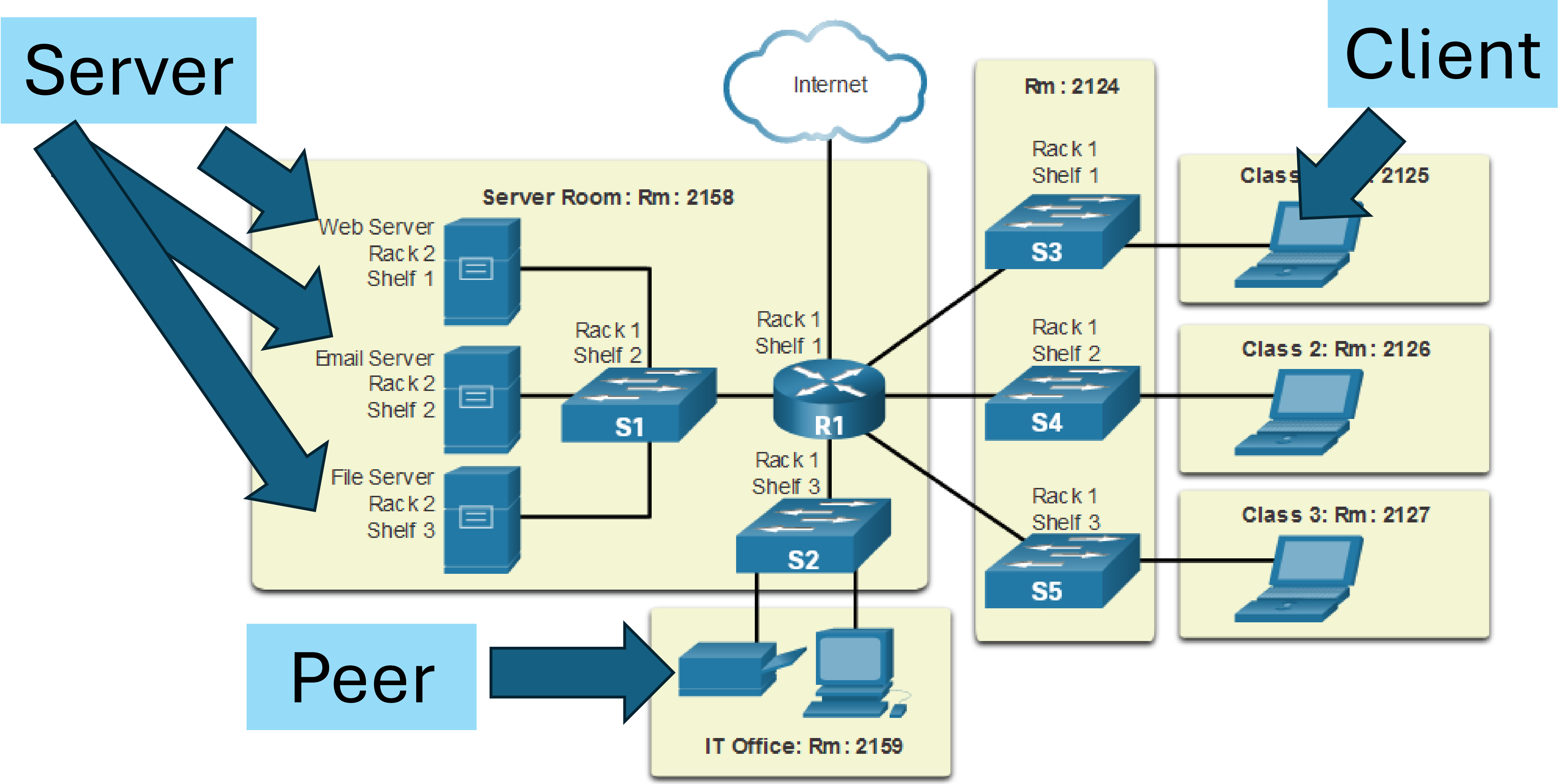
DO MANY WORDS!!!!

- A circuit-switched network uses preconfigured links from source to destination. A circuit-switched network's physical and logical topologies reflect each other.
- A PSN breaks down data into smaller packets for faster transmission. A PSN's logical topology can vary from transmission to transmission.
- A network's control plane relies on various communication standards, or protocols, to determine how data is transmitted.
- A network's data plane carries the data from source to destination. The data plane relies on information provided by the control plane, such as routes and addresses.
- A network's management plane manages and monitors the nodes used in the control and data planes. The management plane oversees the control plane.

Network mediums

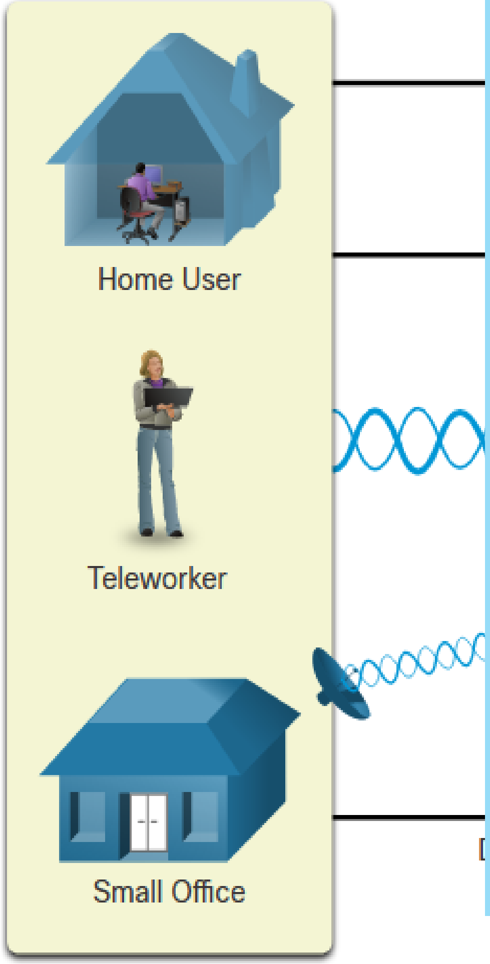


Clients, Server, and Peers



PAN	PERSONAL AREA
LAN	Local Area Network
CAN	Campus Area Network
MAN	Metropolotain Area Network
WAN	Wide Area Network

Service provider links



DEMARCATION POINT

is the location where a service provider's equipment connects to a customer's on-premise equipment.

Connection	Description
	gh bandwidth, always , internet offered by ble television service oviders.
	gh bandwidth, always , internet connection at runs over a telephone e.
	es a cell phone network connect to the internet.
	ajor benefit to rural eas without Internet rvice Providers.
telephone	inexpensive, low bandwidth option using a modem.

Chapter 1: Network Types, Topologies, and Characteristics

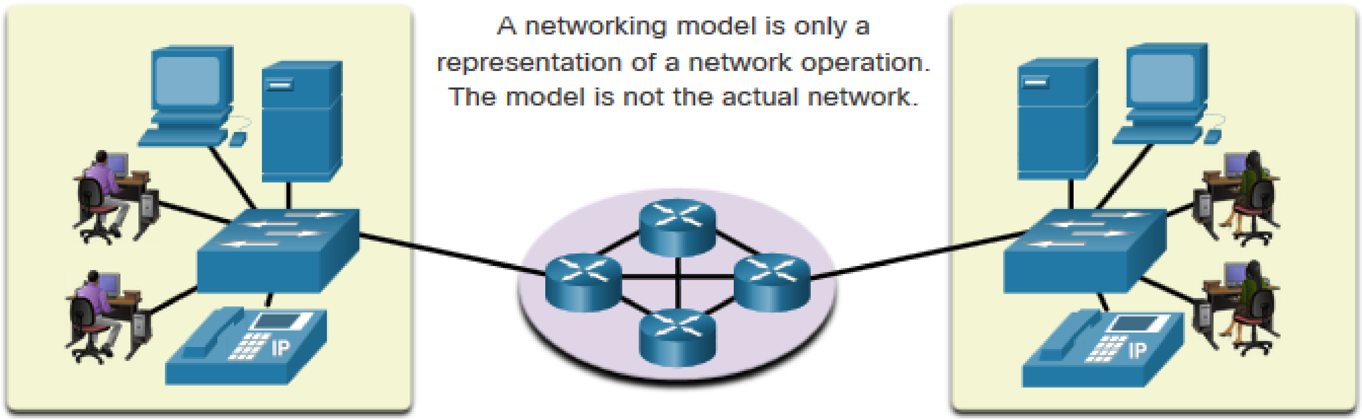
Chapter 2: Conceptual Models and Network Devices

2.1 Conceptual Models

Conceptual model structure

- ***Open Systems Interconnection (OSI) model*** is a seven-layer network conceptual model created by the International Organization for Standardization (ISO).
- ***Department of Defense (DoD) model*** is a four-layer network conceptual model implemented as the internet protocols suite. The DoD model is commonly known as the ***TCP/IP model***.

Reference Models
The 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	Ethernet, WLAN, SONET, SDH	Network Access
Physical		

Reference Models
The OSI Reference Model

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

Reference Models
The TCP/IP Reference Model

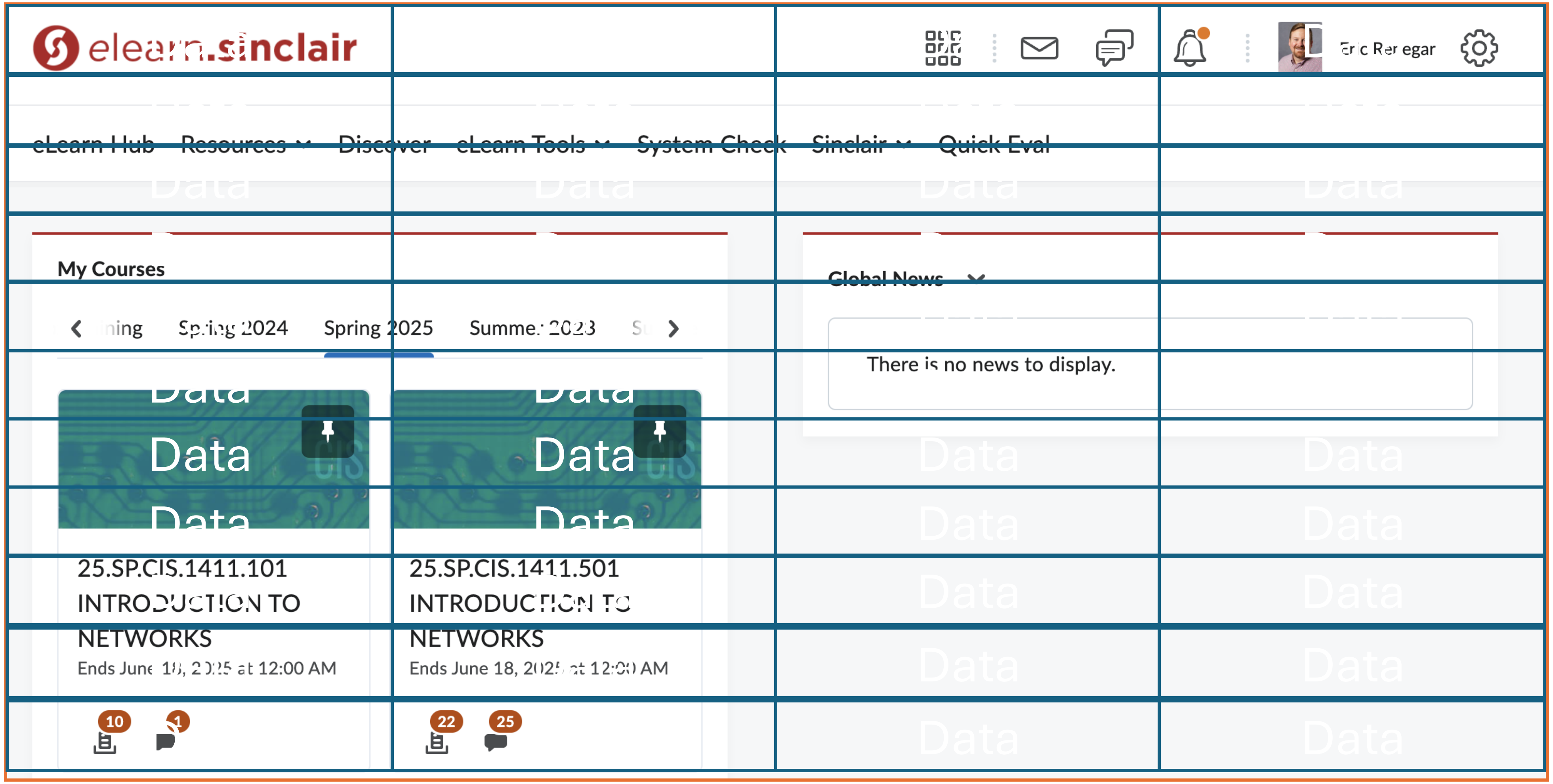
TCP/IP Model Layer	Description
Application	Represents data to the user, plus encoding and dialog control.
Transport	Supports communication between various devices across diverse networks.
Internet	Determines the best path through the network.
Network Access	Controls the hardware devices and media that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

How do we get information from a server

Protocol Suites
TCP/IP Communication Process

Protocol Suites

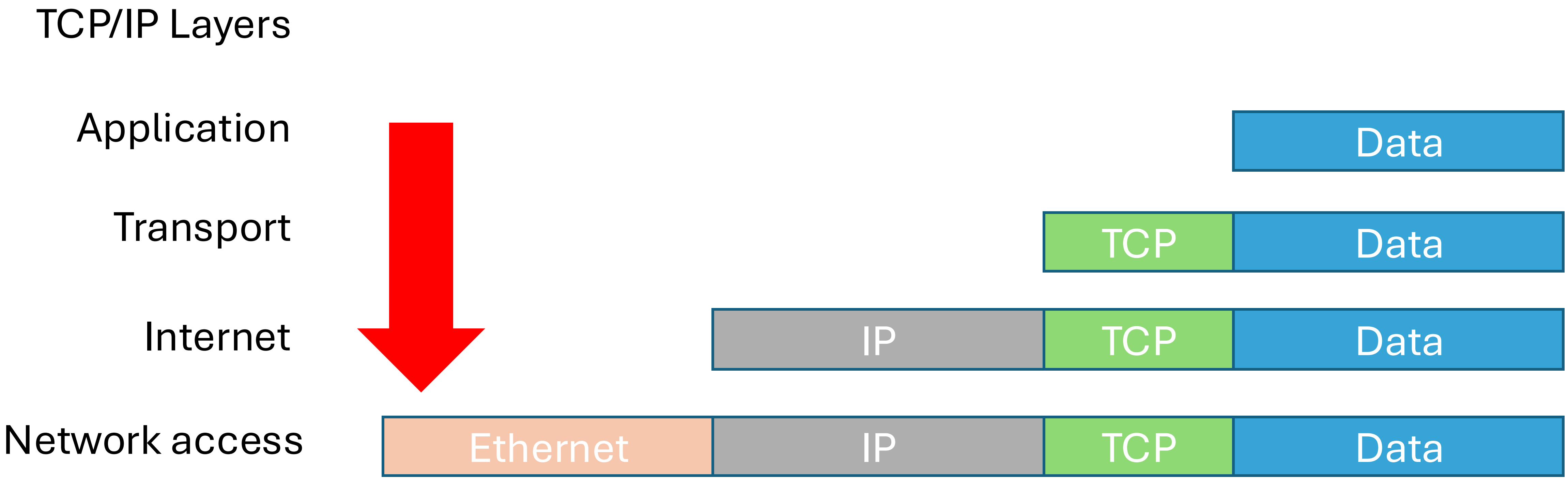
TCP/IP Communication Process



TCP/IP Communication Process

Data	Data	Data	Data
Data	Data	Data	Data
Data	Data	Data	Data
Data	Data	Data	Data
Data	Data	Data	Data
Data	Data	Data	Data
Data	Data	Data	Data
Data	Data	Data	Data
Data	Data	Data	Data
Data	Data	Data	Data
Data	Data	Data	Data

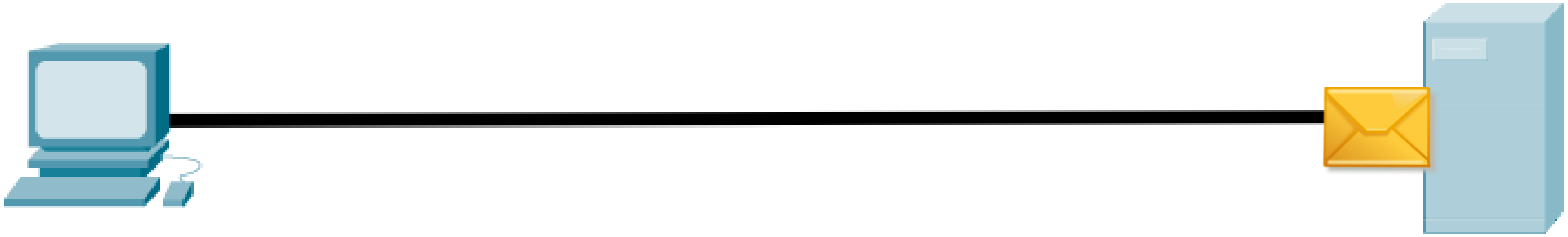
Encapsulation Process



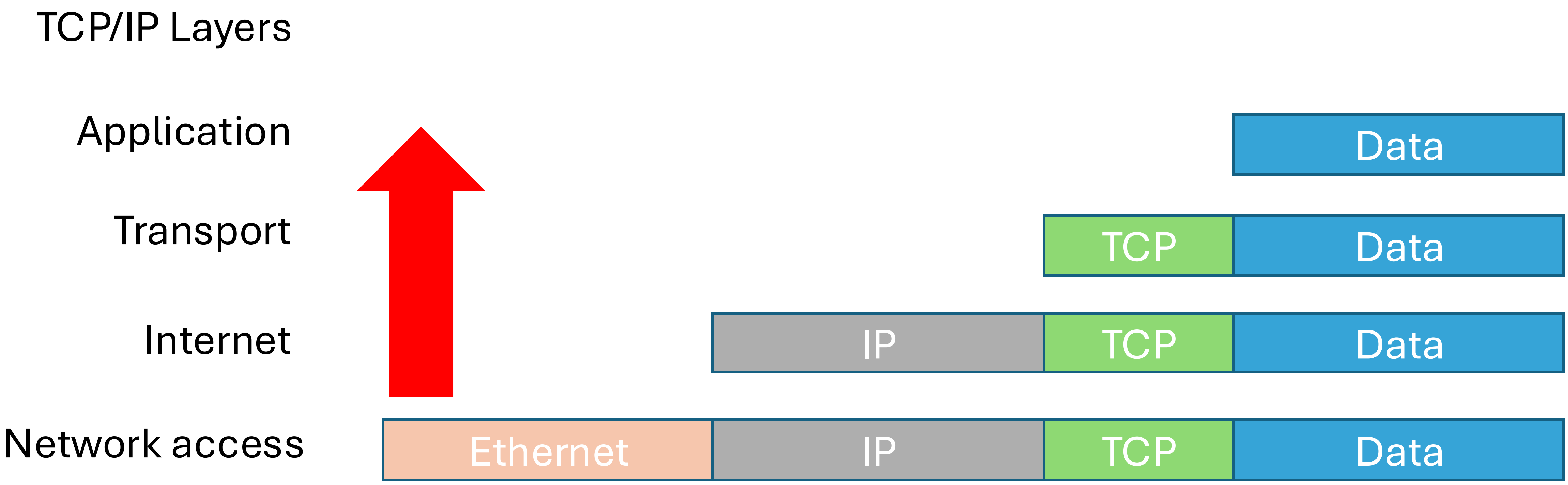
TCP/IP Communication Process

- A client de-encapsulating the web page for the web browser

- A web server encapsulating and sending a web page to a client.



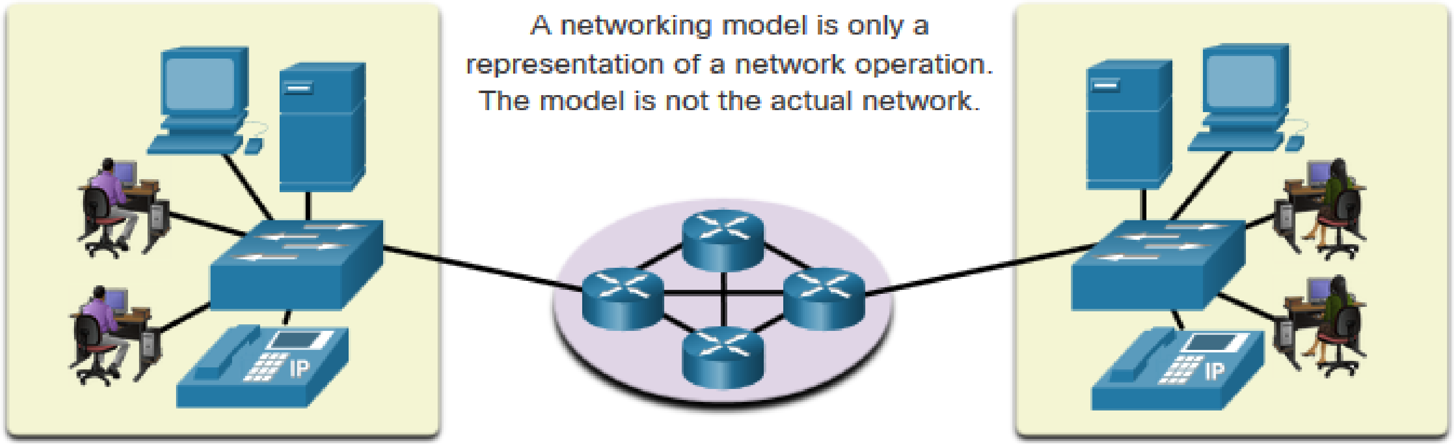
Deencapsulation Process



2.2 OSI Model Layer

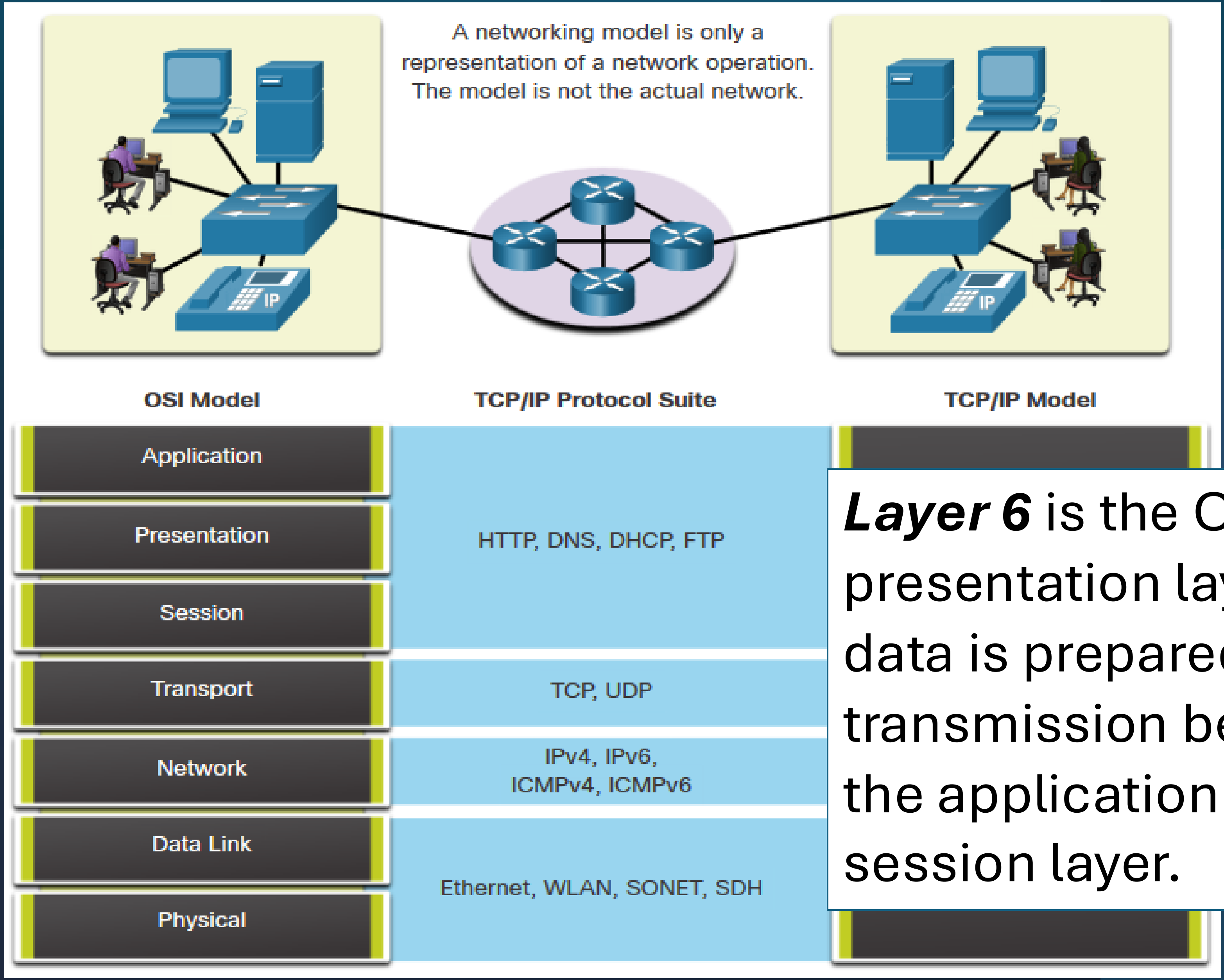
Reference Models
The OSI Reference Model

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

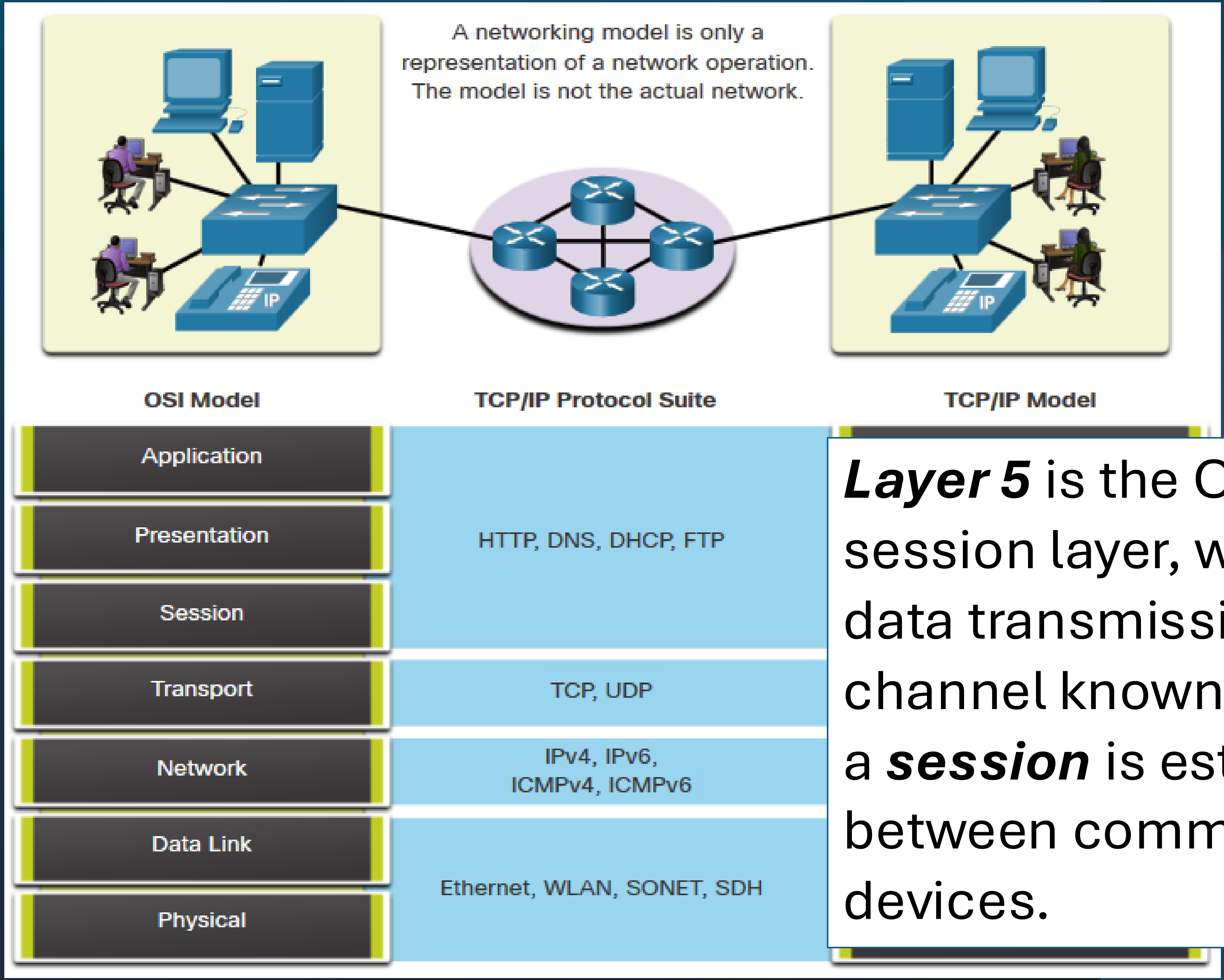


OSI Model	TCP/IP Protocol Suite
Application	HTTP, DNS, DHCP, FTP
Presentation	
Session	
Transport	TCP, UDP
Network	IPv4, IPv6, ICMPv4, ICMPv6
Data Link	Ethernet, WLAN, SONET, SDH
Physical	

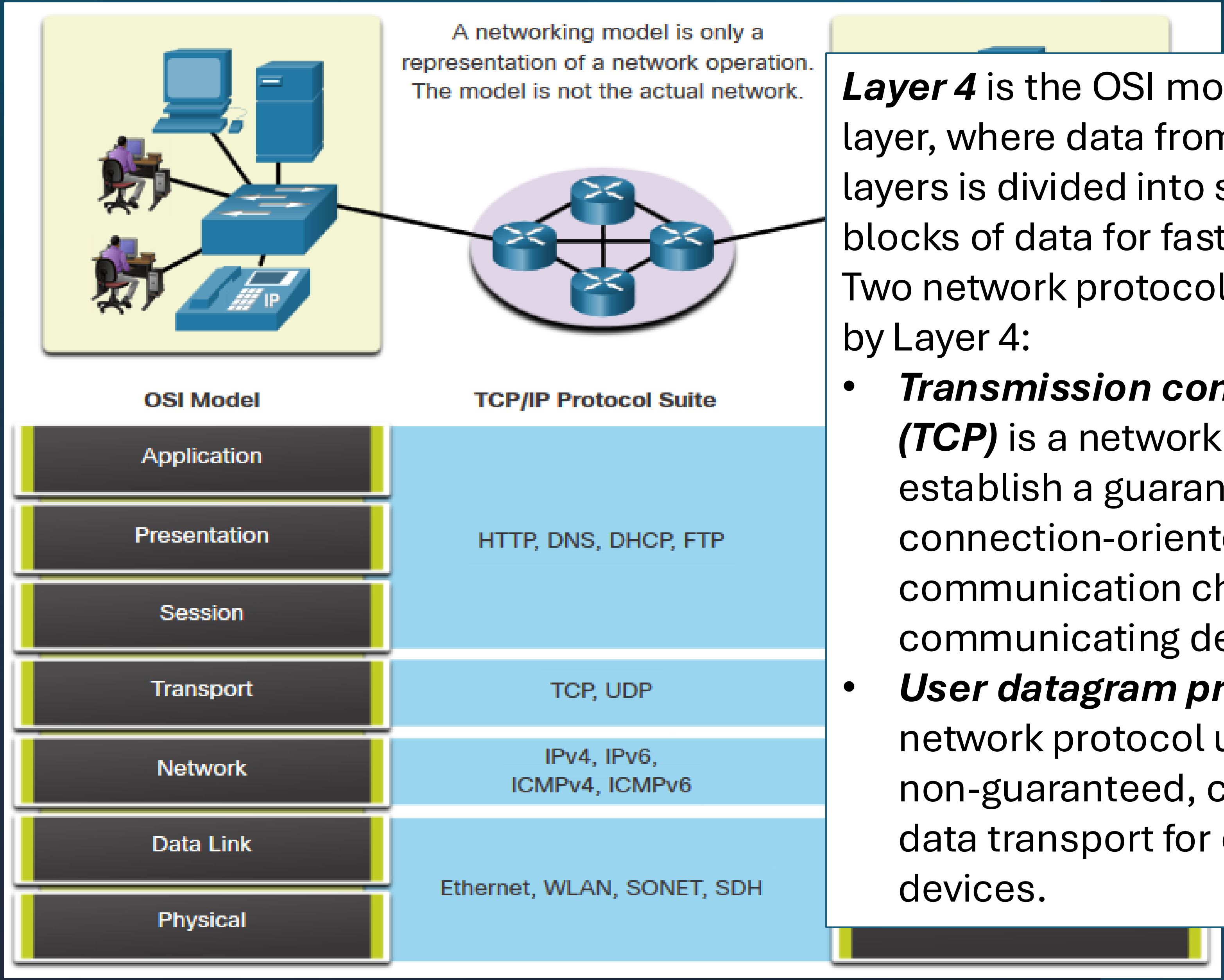
Layer 7 is the OSI model application layer, where a network protocol interacts with a network-aware application.



Layer 6 is the OSI model presentation layer, where data is prepared for transmission between the application layer and session layer.

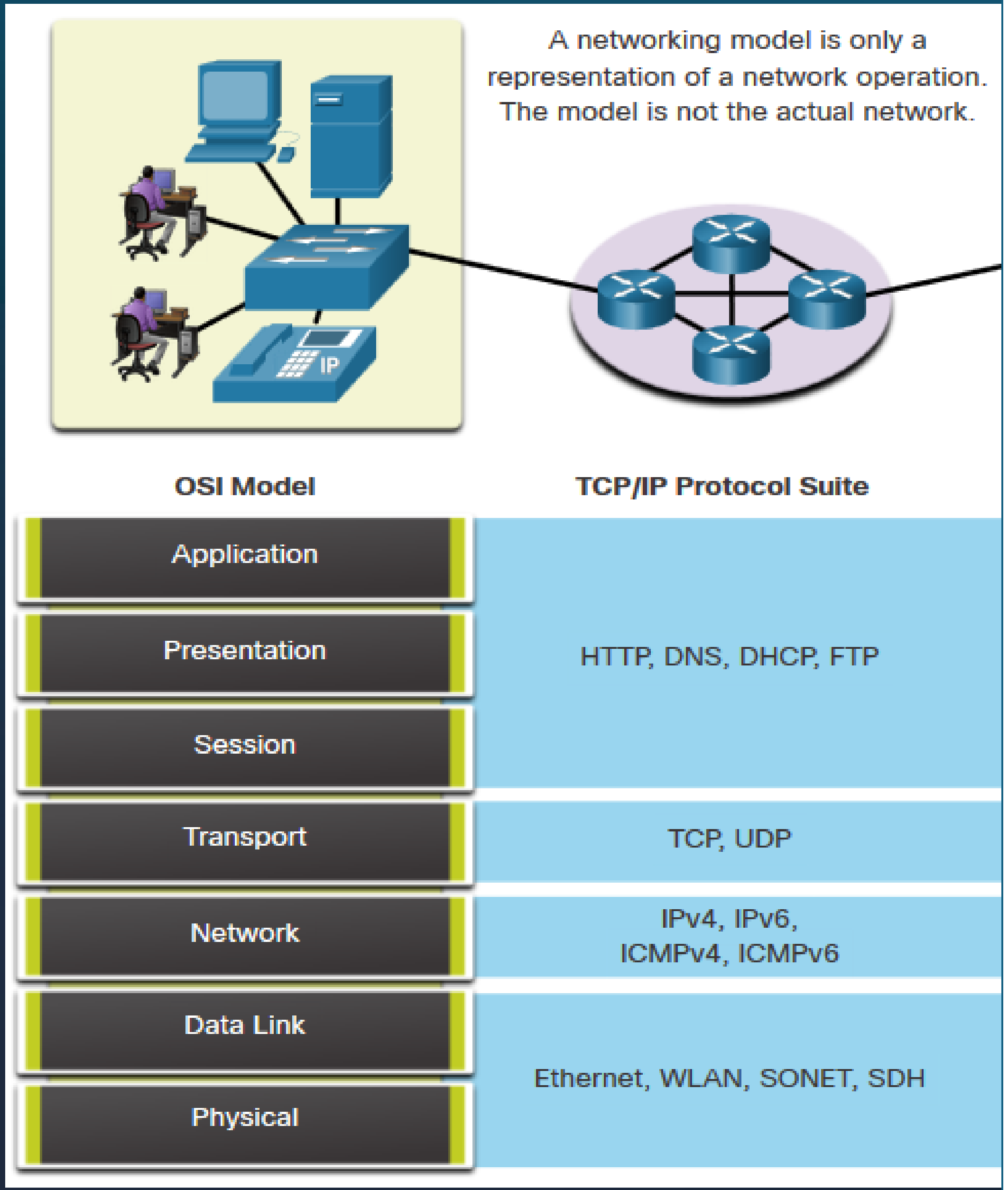


Layer 5 is the OSI model session layer, where a data transmission channel known as a ***session*** is established between communicating devices.



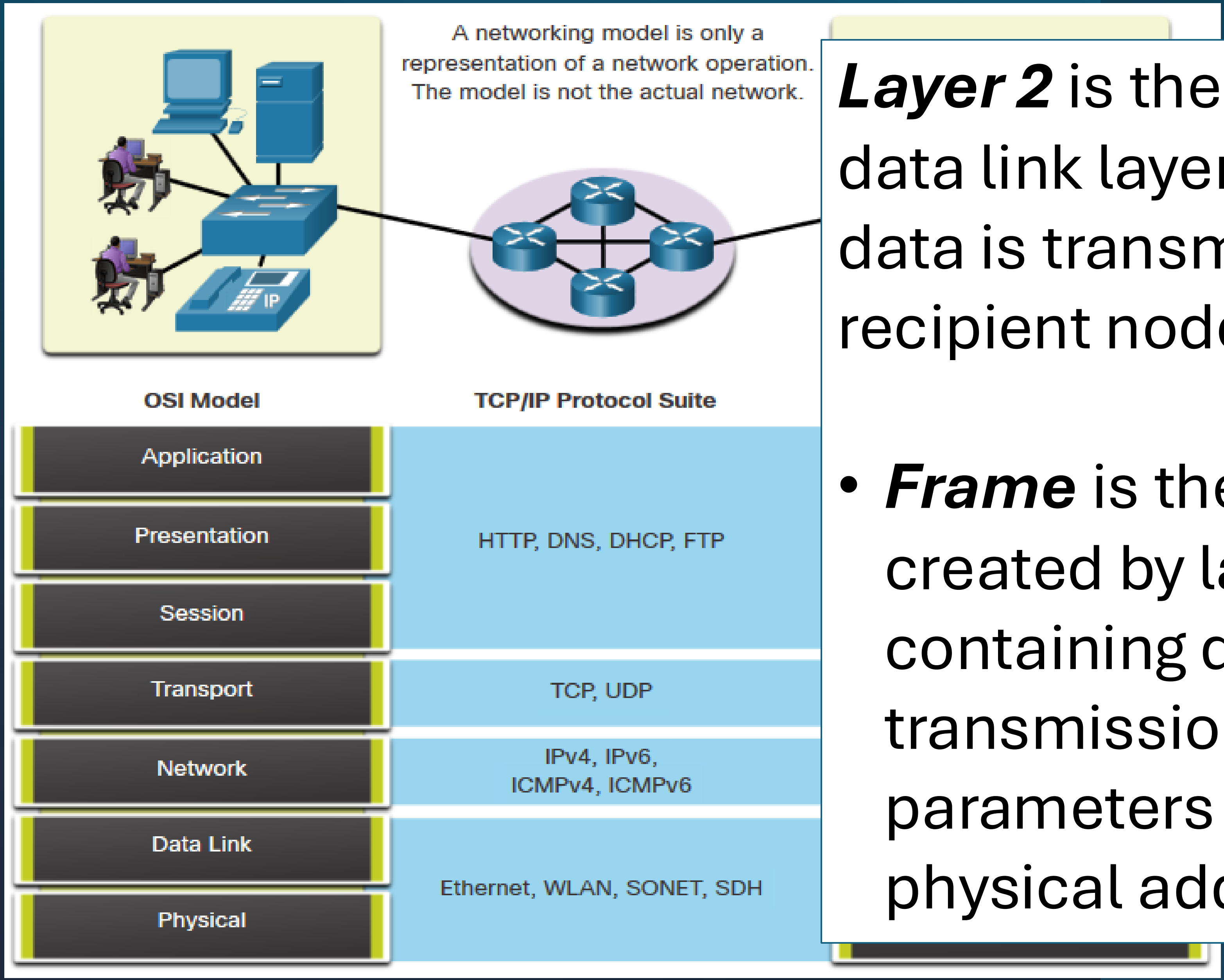
Layer 4 is the OSI model transport layer, where data from the upper-level layers is divided into smaller-sized blocks of data for faster transmission. Two network protocols are referenced by Layer 4:

- ***Transmission control protocol (TCP)*** is a network protocol used to establish a guaranteed, connection-oriented communication channel between communicating devices.
- ***User datagram protocol (UDP)*** is a network protocol used to provide non-guaranteed, connectionless data transport for communicating devices.



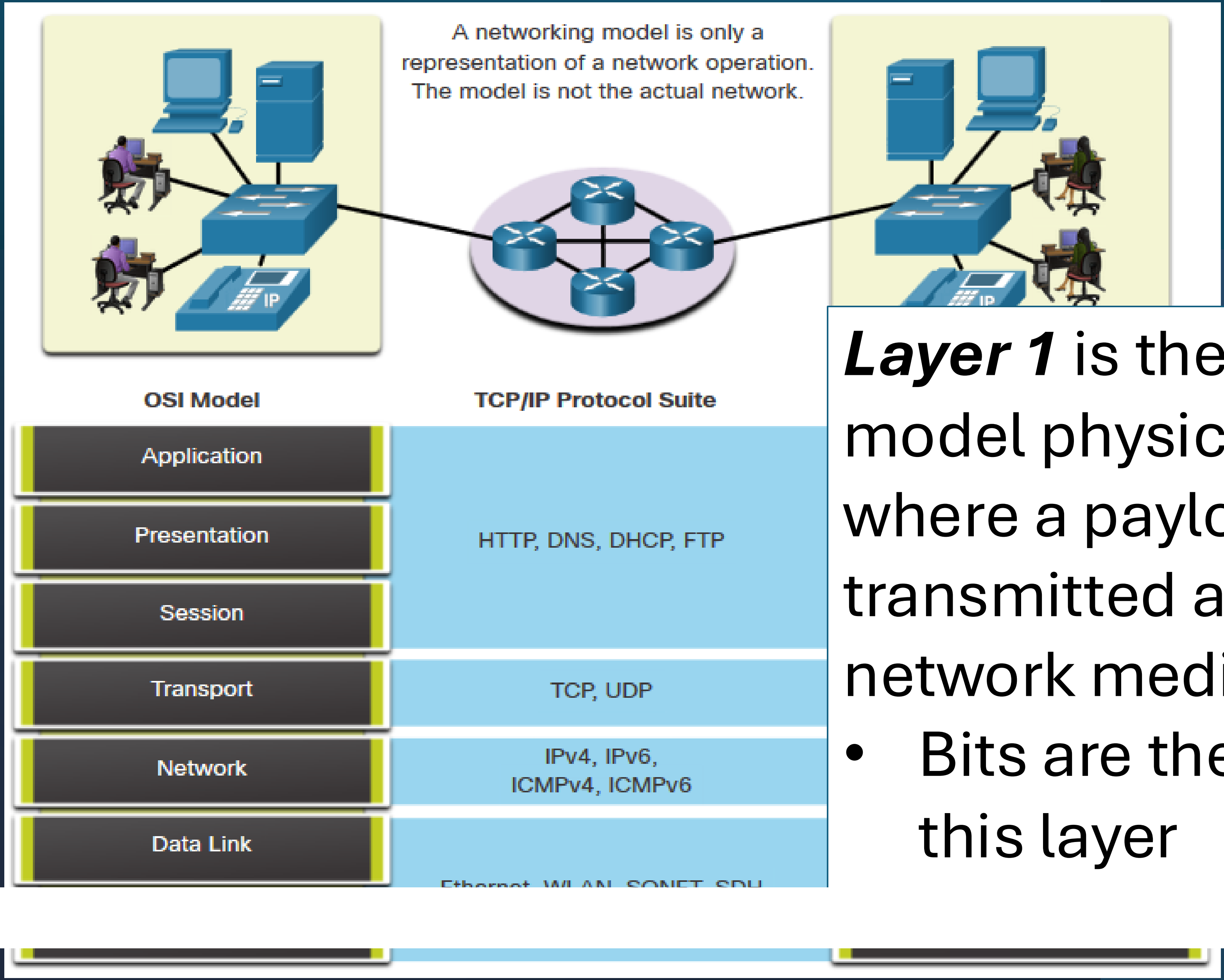
Layer 3 is the OSI model network layer, where data receives logical address information needed to reach the recipient's network.

- ***Internet protocol (IP)*** is the network protocol used to address data sent over the internet or another network.
- ***Packet*** is thePDU created by IP, and includes an IP header consisting of logical address information.



Layer 2 is the OSI model data link layer, where data is transmitted to the recipient node.

- ***Frame*** is the PDU created by layer 2 containing data transmission parameters and physical address.

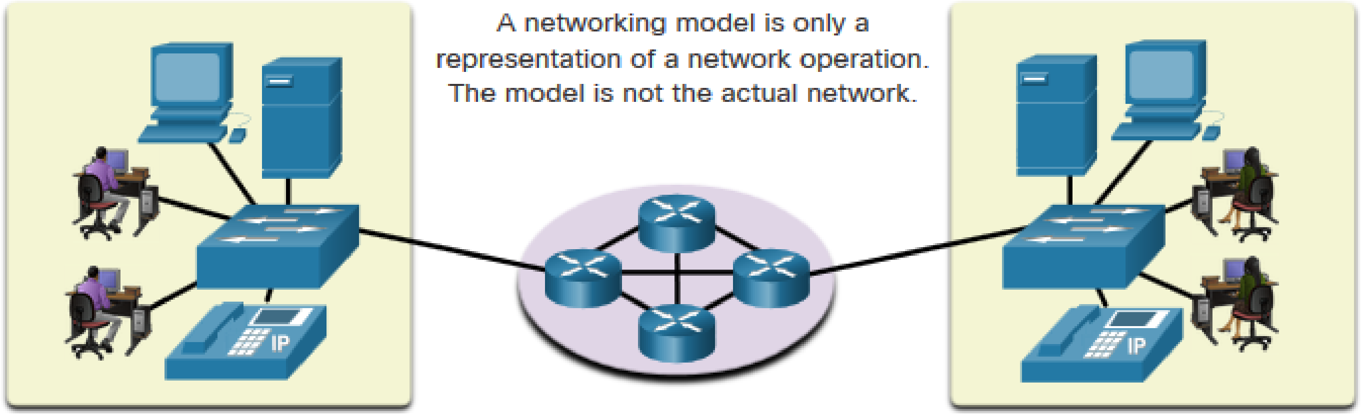


Layer 1 is the OSI model physical layer, where a payload is transmitted across a network medium.

- Bits are the PDU for this layer

2.3 TCP/IP Model

A networking model is only a representation of a network operation. The model is not the actual network.



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		

2.5 Network Devices

2.4 Networking devices

Layer 1: Devices
- Hub (legacy)
- Access Point
- Repeater
- Media Converter

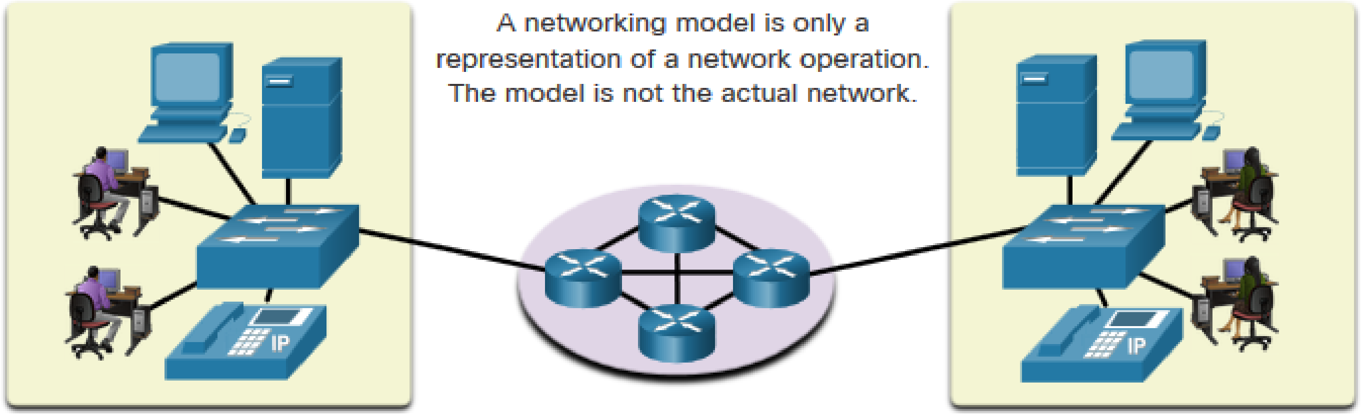
Layer 2: Devices
- Switch
- Access Point (Book)
- Bridge (legacy)

Layer 3: Devices
- Routers
- Layer 3 Switches

Layer 4: Devices
- Firewalls
- Intrusion Detection
- Instruction Prevention

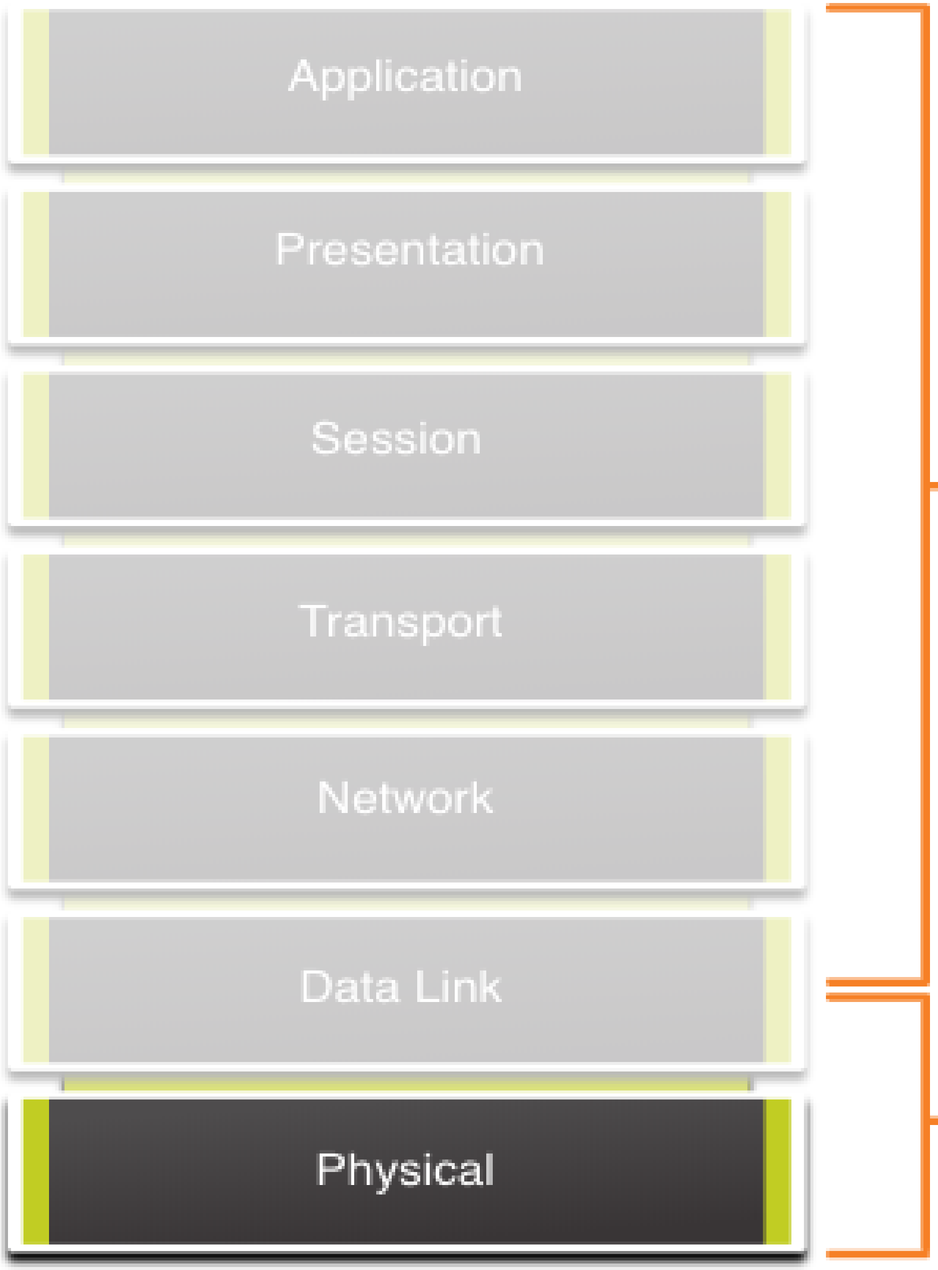
Chapter 2: Conceptual Models and Network Devices

Chapter 3: Bounded Media Standards and Applications



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		

Physical Layer Standards



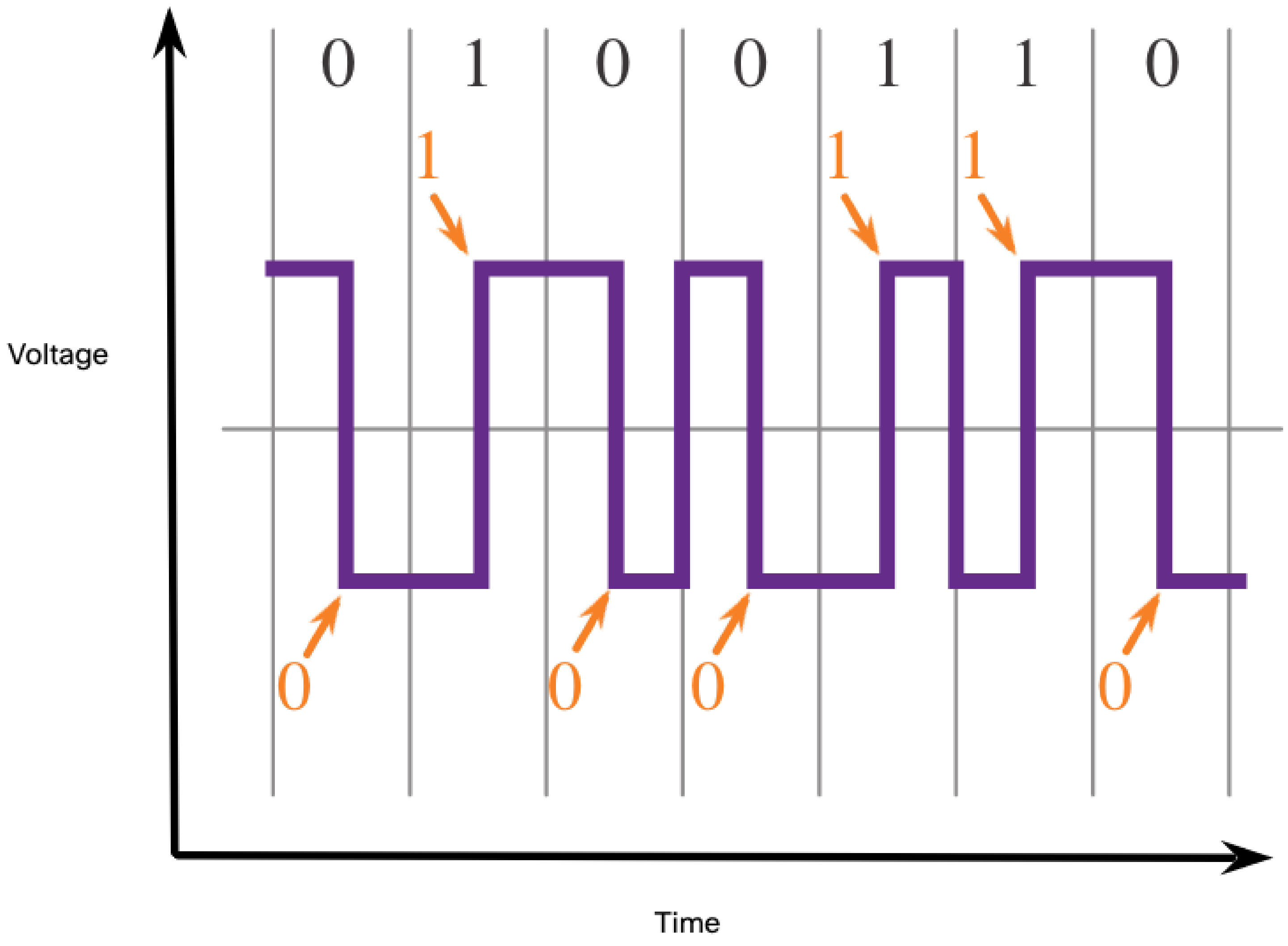
The TCP/IP standards are implemented in software and governed by the IETF.

The physical layer standards are implemented in hardware and are governed by many organizations including:

- ISO
- EIA/TIA
- ITU-T
- ANSI
- IEEE

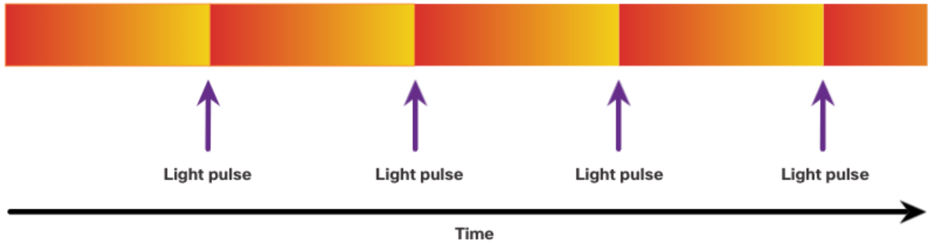
Encoding

- Encoding converts the stream of bits into a format recognizable by the next device in the network path.
- This 'coding' provides predictable patterns that can be recognized by the next device.
- Examples of encoding methods include Manchester (shown in the figure), 4B/5B, and 8B/10B.

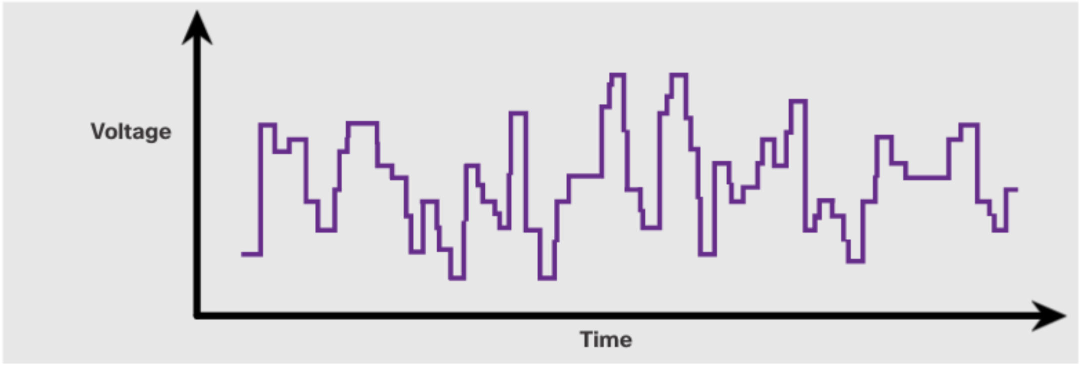


Signaling

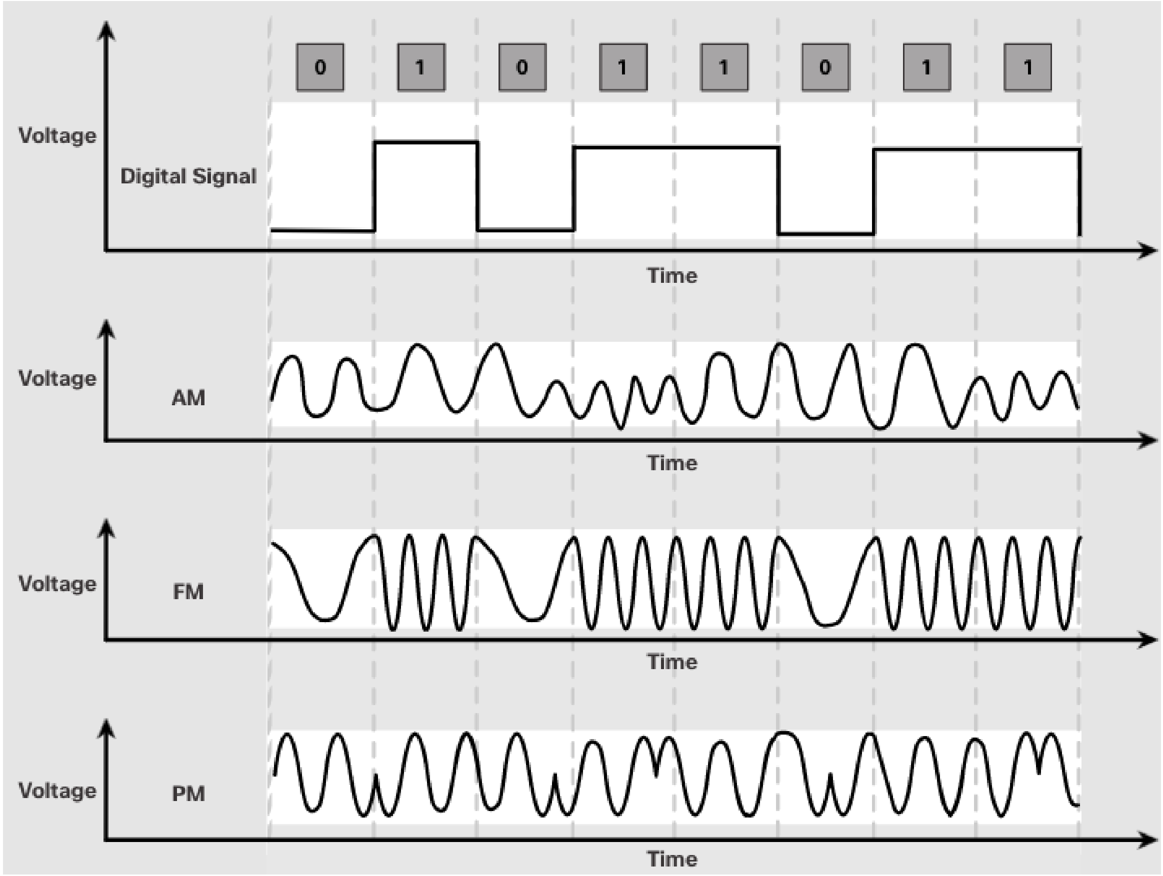
- The signaling method is how the bit values, "1" and "0" are represented on the physical medium.
- The method of signaling will vary based on the type of medium being used.

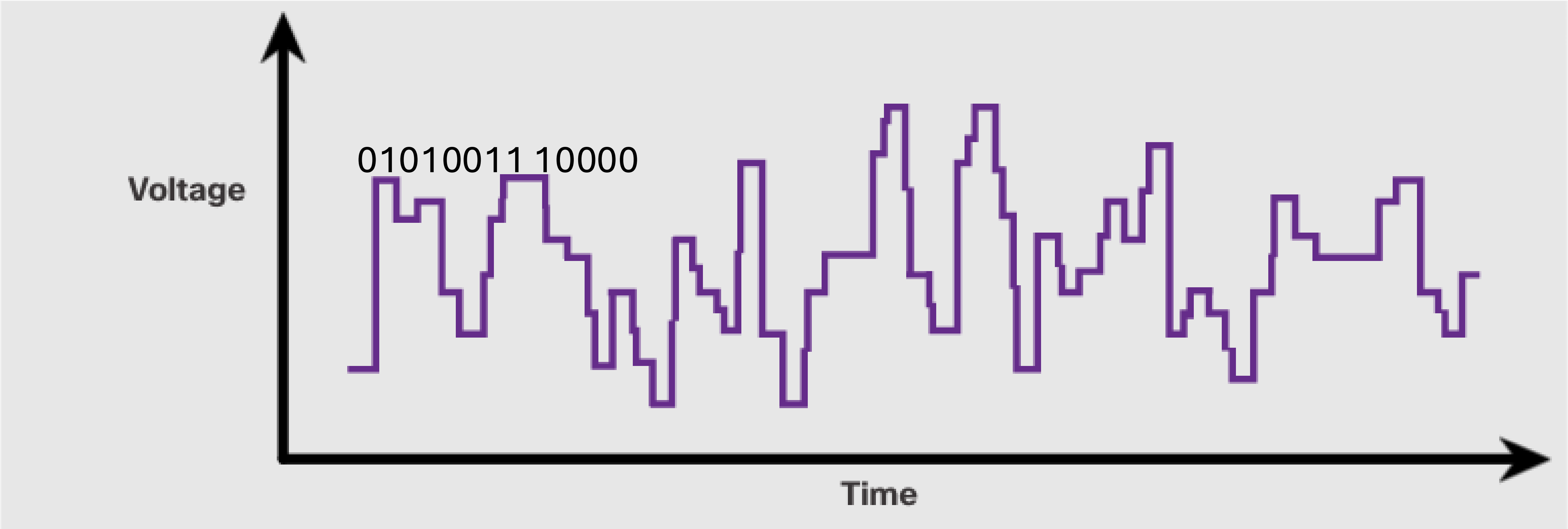


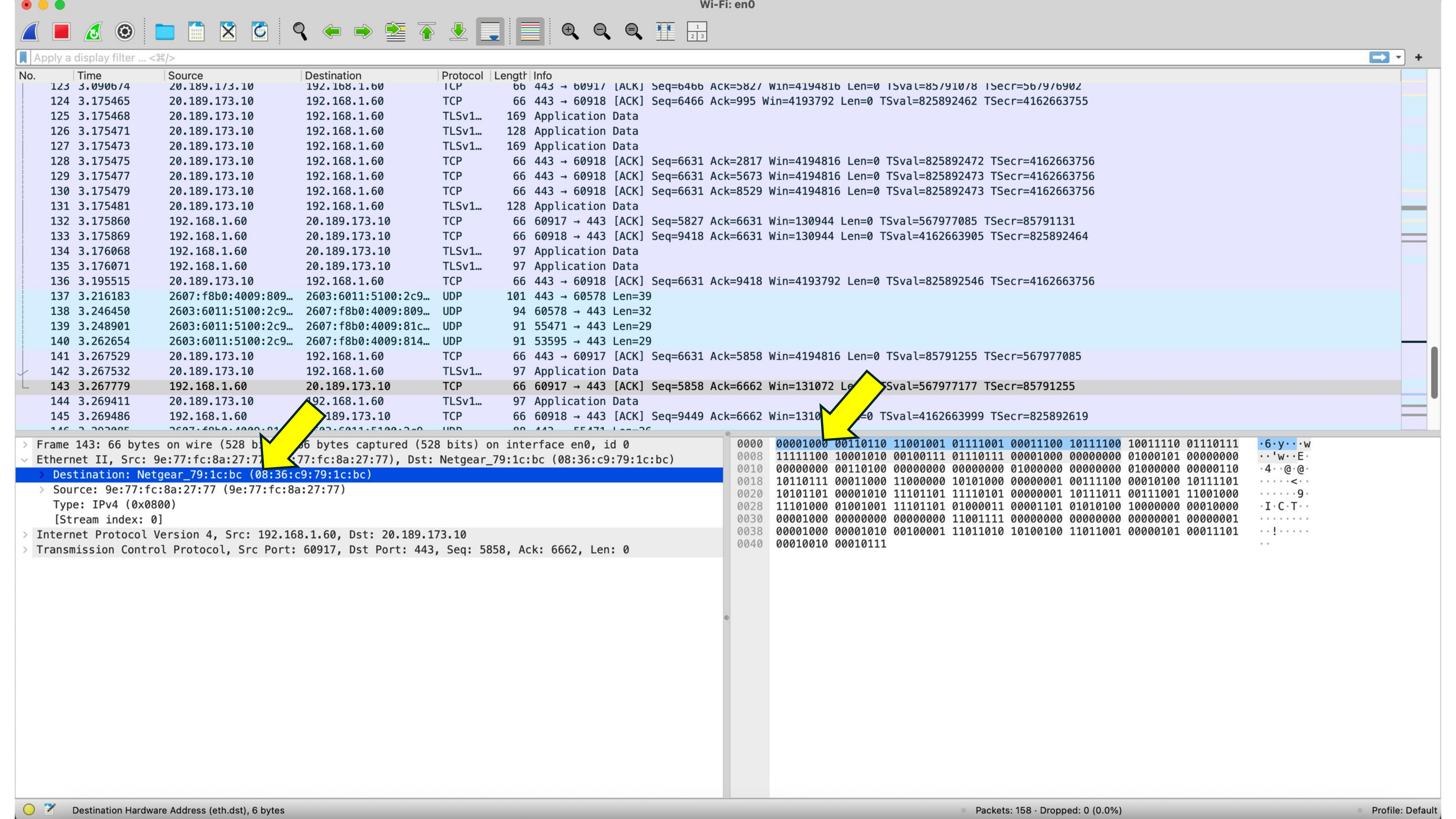
Light Pulses Over Fiber-Optic Cable

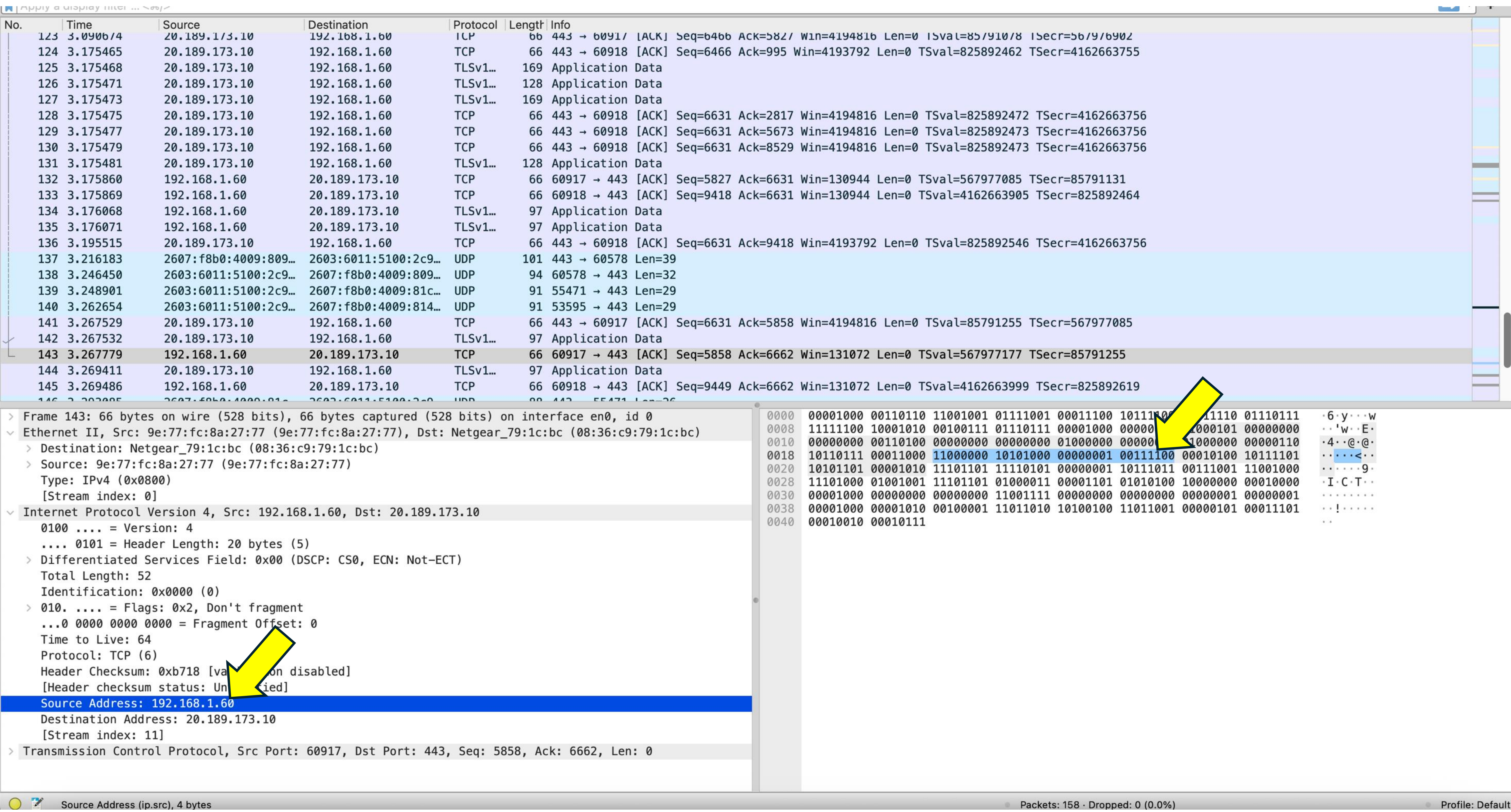


Electrical Signals Over Copper Cable

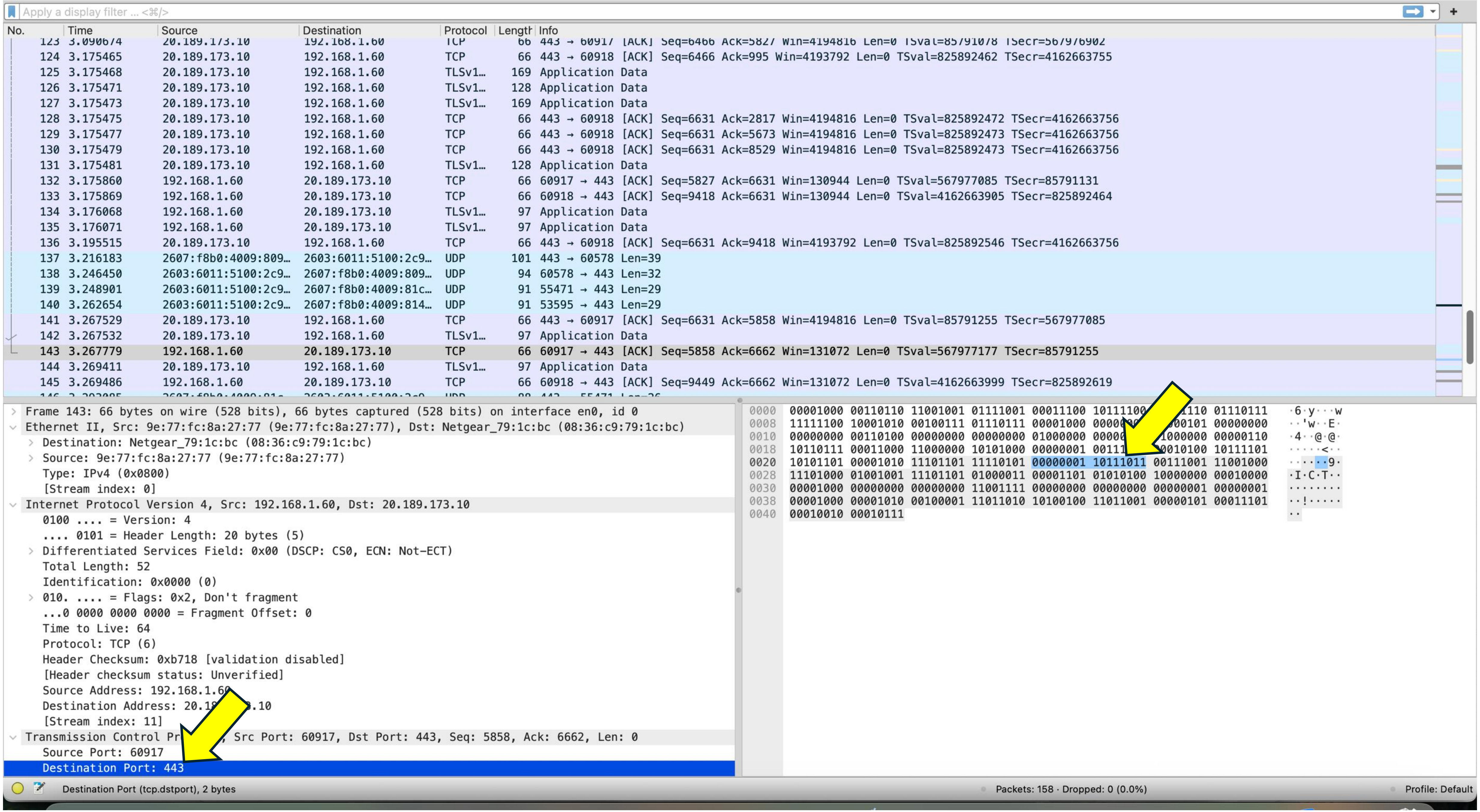



Voltage
01010011 10000
Time


Wi-Fi: en0
Apply a display filter … <⌘/>
No. Time Source Destination Protocol Length Info
123 3.090674 20.189.173.10 192.168.1.60 TCP 66 443 → 60917 [ACK] Seq=6466 Ack=5827 Win=4194816 Len=0 TSval=85791078 TSecr=567976902
124 3.175465 20.189.173.10 192.168.1.60 TCP 66 443 → 60918 [ACK] Seq=6466 Ack=995 Win=4193792 Len=0 TSval=825892462 TSecr=4162663755
125 3.175468 20.189.173.10 192.168.1.60 TLSv1… 169 Application Data
126 3.175471 20.189.173.10 192.168.1.60 TLSv1… 128 Application Data
127 3.175473 20.189.173.10 192.168.1.60 TLSv1… 169 Application Data
128 3.175475 20.189.173.10 192.168.1.60 TCP 66 443 → 60918 [ACK] Seq=6631 Ack=2817 Win=4194816 Len=0 TSval=825892472 TSecr=4162663756
129 3.175477 20.189.173.10 192.168.1.60 TCP 66 443 → 60918 [ACK] Seq=6631 Ack=5673 Win=4194816 Len=0 TSval=825892473 TSecr=4162663756
130 3.175479 20.189.173.10 192.168.1.60 TCP 66 443 → 60918 [ACK] Seq=6631 Ack=8529 Win=4194816 Len=0 TSval=825892473 TSecr=4162663756
131 3.175481 20.189.173.10 192.168.1.60 TLSv1… 128 Application Data
132 3.175860 192.168.1.60 20.189.173.10 TCP 66 60917 → 443 [ACK] Seq=5827 Ack=6631 Win=130944 Len=0 TSval=567977085 TSecr=85791131
133 3.175869 192.168.1.60 20.189.173.10 TCP 66 60918 → 443 [ACK] Seq=9418 Ack=6631 Win=130944 Len=0 TSval=4162663905 TSecr=825892464
134 3.176068 192.168.1.60 20.189.173.10 TLSv1… 97 Application Data
135 3.176071 192.168.1.60 20.189.173.10 TLSv1… 97 Application Data
136 3.195515 20.189.173.10 192.168.1.60 TCP 66 443 → 60918 [ACK] Seq=6631 Ack=9418 Win=4193792 Len=0 TSval=825892546 TSecr=4162663756
137 3.216183 2607:f8b0:4009:809… 2603:6011:5100:2c9… UDP 101 443 → 60578 Len=39
138 3.246450 2603:6011:5100:2c9… 2607:f8b0:4009:809… UDP 94 60578 → 443 Len=32
139 3.248901 2603:6011:5100:2c9… 2607:f8b0:4009:81c… UDP 91 55471 → 443 Len=29
140 3.262654 2603:6011:5100:2c9… 2607:f8b0:4009:814… UDP 91 53595 → 443 Len=29
141 3.267529 20.189.173.10 192.168.1.60 TCP 66 443 → 60917 [ACK] Seq=6631 Ack=5858 Win=4194816 Len=0 TSval=85791255 TSecr=567977085
142 3.267532 20.189.173.10 192.168.1.60 TLSv1… 97 Application Data
143 3.267779 192.168.1.60 20.189.173.10 TCP 66 60917 → 443 [ACK] Seq=5858 Ack=6662 Win=131072 Le Sval=567977177 TSecr=85791255
144 3.269411 20.189.173.10 92.168.1.60 TLSv1… 97 Application Data
145 3.269486 192.168.1.60 189.173.10 TCP 66 60918 → 443 [ACK] Seq=9449 Ack=6662 Win=1310 0 TSval=4162663999 TSecr=825892619
Frame 143: 66 bytes on wire (528 b 6 bytes captured (528 bits) on interface en0, id 0
Ethernet II, Src: 9e:77:fc:8a:27:77 77:fc:8a:27:77), Dst: Netgear_79:1c:bc (08:36:c9:79:1c:bc)
Destination: Netgear_79:1c:bc (08:36:c9:79:1c:bc)
Source: 9e:77:fc:8a:27:77 (9e:77:fc:8a:27:77)
Type: IPv4 (0x0800)
[Stream index: 0]
Internet Protocol Version 4, Src: 192.168.1.60, Dst: 20.189.173.10
Transmission Control Protocol, Src Port: 60917, Dst Port: 443, Seq: 5858, Ack: 6662, Len: 0
0000 00001000 00110110 11001001 01111001 00011100 10111100 10011110 01110111 ·6·y···w
0008 11111100 10001010 00100111 01110111 00001000 00000000 01000101 00000000 ··'w··E·
0010 00000000 00110100 00000000 00000000 01000000 00000000 01000000 00000110 ·4··@·@·
0018 10110111 00011000 11000000 10101000 00000001 00111100 00010100 10111101 ·····<··
0020 10101101 00001010 11101101 11110101 00000001 10111011 00111001 11001000 ······9·
0028 11101000 01001001 11101101 01000011 00001101 01010100 10000000 00010000 ·I·C·T··
0030 00001000 00000000 00000000 11001111 00000000 00000000 00000001 00000001 ········
0038 00001000 00001010 00100001 11011010 10100100 11011001 00000101 00011101 ··!·····
0040 00010010 00010111 ··
Destination Hardware Address (eth.dst), 6 bytes
Packets: 158 · Dropped: 0 (0.0%)
Profile: Default



No. Time Source Destination Protocol Length Info
124 3.175465 20.189.173.10 192.168.1.60 TCP 66 443 → 60918 [ACK] Seq=6466 Ack=995 Win=4193792 Len=0 TSval=825892462 TSecr=4162663755
125 3.175468 20.189.173.10 192.168.1.60 TLSv1… 169 Application Data
126 3.175471 20.189.173.10 192.168.1.60 TLSv1… 128 Application Data
127 3.175473 20.189.173.10 192.168.1.60 TLSv1… 169 Application Data
128 3.175475 20.189.173.10 192.168.1.60 TCP 66 443 → 60918 [ACK] Seq=6631 Ack=2817 Win=4194816 Len=0 TSval=825892472 TSecr=4162663756
129 3.175477 20.189.173.10 192.168.1.60 TCP 66 443 → 60918 [ACK] Seq=6631 Ack=5673 Win=4194816 Len=0 TSval=825892473 TSecr=4162663756
130 3.175479 20.189.173.10 192.168.1.60 TCP 66 443 → 60918 [ACK] Seq=6631 Ack=8529 Win=4194816 Len=0 TSval=825892473 TSecr=4162663756
131 3.175481 20.189.173.10 192.168.1.60 TLSv1… 128 Application Data
132 3.175860 192.168.1.60 20.189.173.10 TCP 66 60917 → 443 [ACK] Seq=5827 Ack=6631 Win=130944 Len=0 TSval=567977085 TSecr=85791131
133 3.175869 192.168.1.60 20.189.173.10 TCP 66 60918 → 443 [ACK] Seq=9418 Ack=6631 Win=130944 Len=0 TSval=4162663905 TSecr=825892464
134 3.176068 192.168.1.60 20.189.173.10 TLSv1… 97 Application Data
135 3.176071 192.168.1.60 20.189.173.10 TLSv1… 97 Application Data
136 3.195515 20.189.173.10 192.168.1.60 TCP 66 443 → 60918 [ACK] Seq=6631 Ack=9418 Win=4193792 Len=0 TSval=825892546 TSecr=4162663756
137 3.216183 2607:f8b0:4009:809… 2603:6011:5100:2c9… UDP 101 443 → 60578 Len=39
138 3.246450 2603:6011:5100:2c9… 2607:f8b0:4009:809… UDP 94 60578 → 443 Len=32
139 3.248901 2603:6011:5100:2c9… 2607:f8b0:4009:81c… UDP 91 55471 → 443 Len=29
140 3.262654 2603:6011:5100:2c9… 2607:f8b0:4009:814… UDP 91 53595 → 443 Len=29
141 3.267529 20.189.173.10 192.168.1.60 TCP 66 443 → 60917 [ACK] Seq=6631 Ack=5858 Win=4194816 Len=0 TSval=85791255 TSecr=567977085
142 3.267532 20.189.173.10 192.168.1.60 TLSv1… 97 Application Data
143 3.267779 192.168.1.60 20.189.173.10 TCP 66 60917 → 443 [ACK] Seq=5858 Ack=6662 Win=131072 Len=0 TSval=567977177 TSecr=85791255
144 3.269411 20.189.173.10 192.168.1.60 TLSv1… 97 Application Data
145 3.269486 192.168.1.60 20.189.173.10 TCP 66 60918 → 443 [ACK] Seq=9449 Ack=6662 Win=131072 Len=0 TSval=4162663999 TSecr=825892619
Frame 143: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface en0, id 0
Ethernet II, Src: 9e:77:fc:8a:27:77 (9e:77:fc:8a:27:77), Dst: Netgear_79:1c:bc (08:36:c9:79:1c:bc)
Destination: Netgear_79:1c:bc (08:36:c9:79:1c:bc)
Source: 9e:77:fc:8a:27:77 (9e:77:fc:8a:27:77)
Type: IPv4 (0x0800)
[Stream index: 0]
Internet Protocol Version 4, Src: 192.168.1.60, Dst: 20.189.173.10
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 52
Identification: 0x0000 (0)
010. .... = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0xb718 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.60
Destination Address: 20.189.173.10
[Stream index: 11]
Transmission Control Protocol, Src Port: 60917, Dst Port: 443, Seq: 5858, Ack: 6662, Len: 0
0018 10110111 00011000 11000000 10101000 00000001 00111100 00010100 10111101
0020 10101101 00001010 11101101 11110101 00000001 10111011 00111001 11001000
0028 11101000 01001001 11101101 01000011 00001101 01010100 10000000 00010000
0030 00001000 00000000 00000000 11001111 00000000 00000000 00000001 00000001
0038 00001000 00001010 00100001 11011010 10100100 11011001 00000101 00111101
0040 00010010 00010111
Source Address (ip.src), 4 bytes
Packets: 158 · Dropped: 0 (0.0%)
Profile: Default



Apply a display filter … <⌘/>
No. Time Source Destination Protocol Length Info
123 3.090674 20.189.173.10 192.168.1.60 TCP 66 443 → 60917 [ACK] Seq=6466 Ack=5827 Win=4194816 Len=0 TSval=85791078 TSecr=567976902
124 3.175465 20.189.173.10 192.168.1.60 TCP 66 443 → 60918 [ACK] Seq=6466 Ack=995 Win=4193792 Len=0 TSval=825892462 TSecr=4162663755
125 3.175468 20.189.173.10 192.168.1.60 TLSv1… 169 Application Data
126 3.175471 20.189.173.10 192.168.1.60 TLSv1… 128 Application Data
127 3.175473 20.189.173.10 192.168.1.60 TLSv1… 169 Application Data
128 3.175475 20.189.173.10 192.168.1.60 TCP 66 443 → 60918 [ACK] Seq=6631 Ack=2817 Win=4194816 Len=0 TSval=825892472 TSecr=4162663756
129 3.175477 20.189.173.10 192.168.1.60 TCP 66 443 → 60918 [ACK] Seq=6631 Ack=5673 Win=4194816 Len=0 TSval=825892473 TSecr=4162663756
130 3.175479 20.189.173.10 192.168.1.60 TCP 66 443 → 60918 [ACK] Seq=6631 Ack=8529 Win=4194816 Len=0 TSval=825892473 TSecr=4162663756
131 3.175481 20.189.173.10 192.168.1.60 TLSv1… 128 Application Data
132 3.175860 192.168.1.60 20.189.173.10 TCP 66 60917 → 443 [ACK] Seq=5827 Ack=6631 Win=130944 Len=0 TSval=567977085 TSecr=85791131
133 3.175869 192.168.1.60 20.189.173.10 TCP 66 60918 → 443 [ACK] Seq=9418 Ack=6631 Win=130944 Len=0 TSval=4162663905 TSecr=825892464
134 3.176068 192.168.1.60 20.189.173.10 TLSv1… 97 Application Data
135 3.176071 192.168.1.60 20.189.173.10 TLSv1… 97 Application Data
136 3.195515 20.189.173.10 192.168.1.60 TCP 66 443 → 60918 [ACK] Seq=6631 Ack=9418 Win=4193792 Len=0 TSval=825892546 TSecr=4162663756
137 3.216183 2607:f8b0:4009:809… 2603:6011:5100:2c9… UDP 101 443 → 60578 Len=39
138 3.246450 2603:6011:5100:2c9… 2607:f8b0:4009:809… UDP 94 60578 → 443 Len=32
139 3.248901 2603:6011:5100:2c9… 2607:f8b0:4009:81c… UDP 91 55471 → 443 Len=29
140 3.262654 2603:6011:5100:2c9… 2607:f8b0:4009:814… UDP 91 53595 → 443 Len=29
141 3.267529 20.189.173.10 192.168.1.60 TCP 66 443 → 60917 [ACK] Seq=6631 Ack=5858 Win=4194816 Len=0 TSval=85791255 TSecr=567977085
142 3.267532 20.189.173.10 192.168.1.60 TLSv1… 97 Application Data
143 3.267779 192.168.1.60 20.189.173.10 TCP 66 60917 → 443 [ACK] Seq=5858 Ack=6662 Win=131072 Len=0 TSval=567977177 TSecr=85791255
144 3.269411 20.189.173.10 192.168.1.60 TLSv1… 97 Application Data
145 3.269486 192.168.1.60 20.189.173.10 TCP 66 60918 → 443 [ACK] Seq=9449 Ack=6662 Win=131072 Len=0 TSval=4162663999 TSecr=825892619
Frame 143: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface en0, id 0
Ethernet II, Src: 9e:77:fc:8a:27:77 (9e:77:fc:8a:27:77), Dst: Netgear_79:1c:bc (08:36:c9:79:1c:bc)
Destination: Netgear_79:1c:bc (08:36:c9:79:1c:bc)
Source: 9e:77:fc:8a:27:77 (9e:77:fc:8a:27:77)
Type: IPv4 (0x0800)
[Stream index: 0]
Internet Protocol Version 4, Src: 192.168.1.60, Dst: 20.189.173.10
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 52
Identification: 0x0000 (0)
010. .... = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0xb718 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.60
Destination Address: 20.189.173.10
[Stream index: 11]
Transmission Control Protocol, Src Port: 60917, Dst Port: 443, Seq: 5858, Ack: 6662, Len: 0
Source Port: 60917
Destination Port: 443
0000 00001000 00110110 11001001 01111001 00011100 10111100 … 01110111 ·6·y···w
0008 11111100 10001010 00100111 01110111 00001000 … 00000000 ··'w··E·
0010 00000000 00110100 00000000 00000000 01000000 … 00000110 ·4··@·@·
0018 10110111 00011000 11000000 10101000 00000001 … 10111101 ·····<··
0020 10101101 00001010 11101101 11110101 00000001 10111011 00111001 11001000 ·······9·
0028 11101000 01001001 11101101 01000011 00001101 01010100 10000000 00010000 ·I·C·T··
0030 00001000 00000000 00000000 11001111 00000000 00000000 00000001 00000001 ········
0038 00001000 00001010 00100001 11011010 10100100 11011001 00000101 00011101 ··!·····
0040 00010010 00010111 ··
Destination Port (tcp.dstport), 2 bytes
Packets: 158 · Dropped: 0 (0.0%)
Profile: Default

3.1 Bounded Media

Physical Media Characteristics

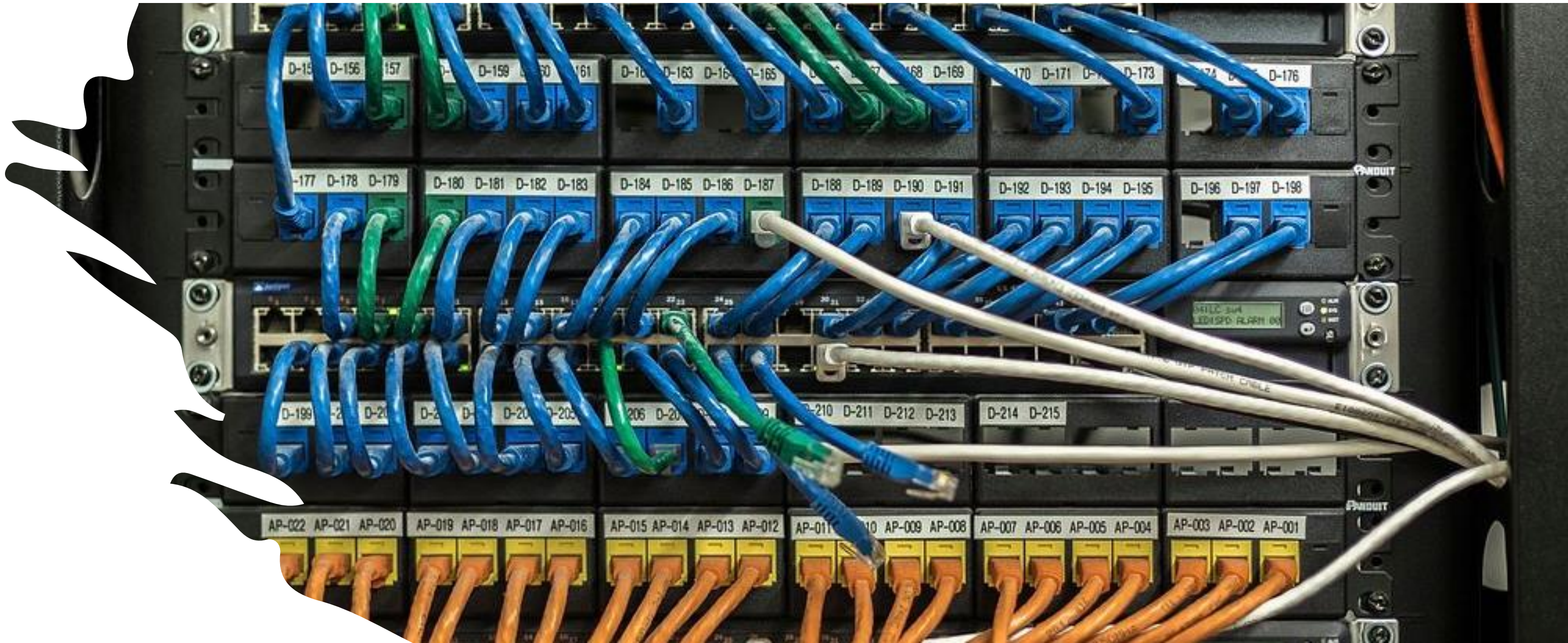
Cost

Speed

Distance

Speed is determined by measuring bandwidth and throughput

- ***Bandwidth*** is the maximum amount of data a connection can transmit in a given amount of time.
- ***Throughput*** is the actual amount of data a connection can transmit in a given amount of time.



Physical Layer Characteristics

Bandwidth

- Bandwidth is the capacity at which a medium can carry data.
- Digital bandwidth measures the amount of data that can flow from one place to another in a given amount of time; how many bits can be transmitted in a second.
- Physical media properties, current technologies, and the laws of physics play a role in determining available bandwidth.

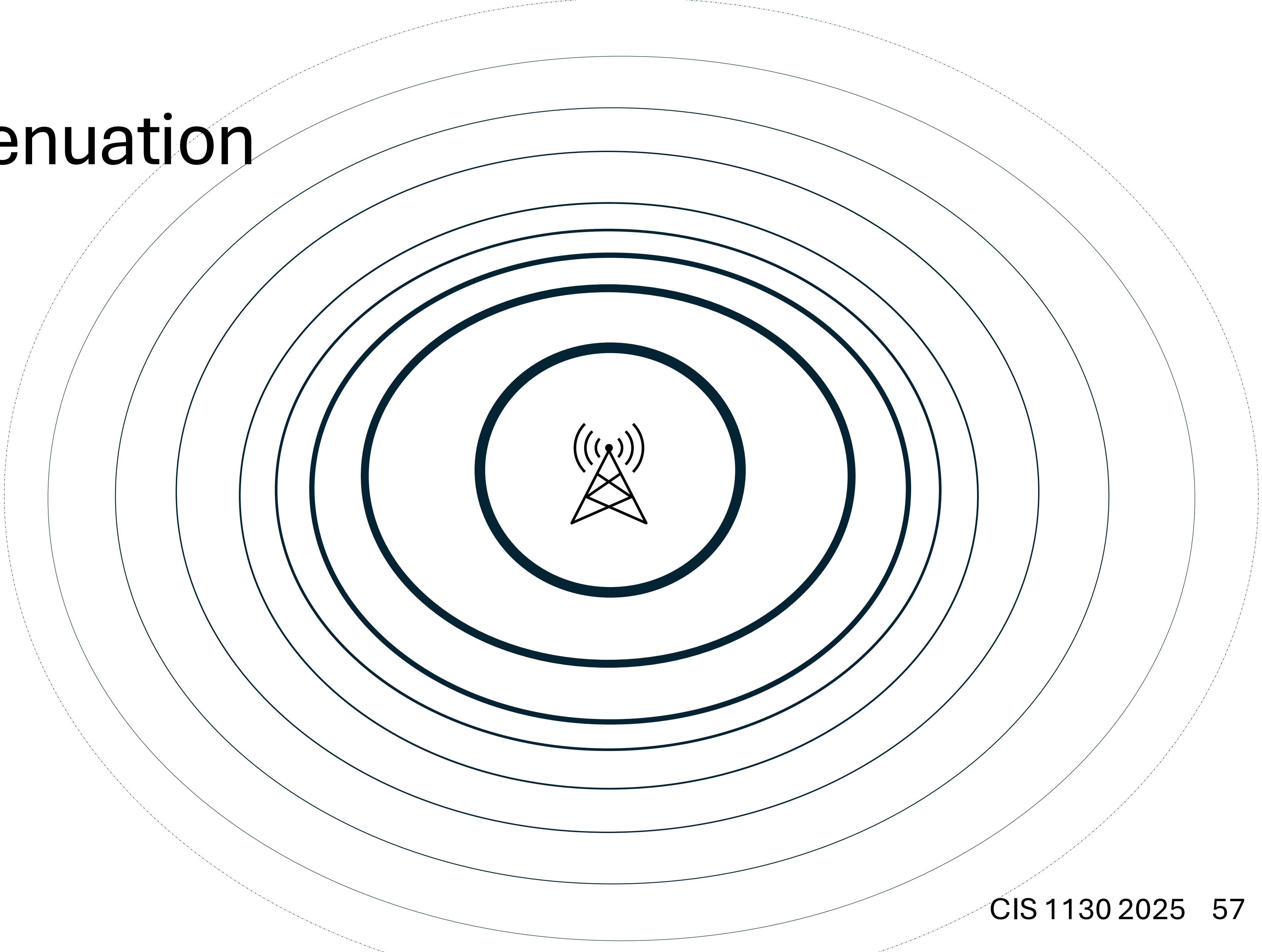
Unit of Bandwidth	Abbreviation	Equivalence
Bits per second	bps	1 bps = fundamental unit of bandwidth
Kilobits per second	Kbps	1 Kbps = 1,000 bps = 10^3 bps
Megabits per second	Mbps	1 Mbps = 1,000,000 bps = 10^6 bps
Gigabits per second	Gbps	1 Gbps – 1,000,000,000 bps = 10^9 bps
Terabits per second	Tbps	1 Tbps = 1,000,000,000,000 bps = 10^{12} bps

Speed and Throughput demo

Attenuation

Transmission's loss of strength over distance

Attenuation



3.2 Coaxial and twinaxial media

Accessories › Networking Products › Modems

Coax

- ***Data over cable service interface specification (DOCSIS)***
- **BroadBand**

Click to see full view

ARRIS (SB8200) - Cable Modem - Fast DOCSIS 3.1 32x8
Gigabit Cable Modem , Approved for Comcast Xfinity, C
Charter Spectrum, & more | 1 Gbps Max Internet Speed
OFDM Channels - (No Built-in Wifi)

Visit the ARRIS Store

4.2 ★★★★☆ 19,981 ratings

#1 Best Seller in Computer Networking Modems

3K+ bought in past month

$169.00

FREE Returns

Get $80 off instantly: Pay $89.00 upon approval for the Amazon Store Card.

Available at a lower price from other sellers that may not offer free Prime shipping.

Style: **SB8200 Gigabit Modem**

DOCSIS 3.1 - G18	DOCSIS 3.1 - G20	DOCSIS 3.1 - G54	SB8200 Gigabit...
$179.00	$234.00 ~~$249.00~~	$478.93 ~~$599.00~~	$169.00

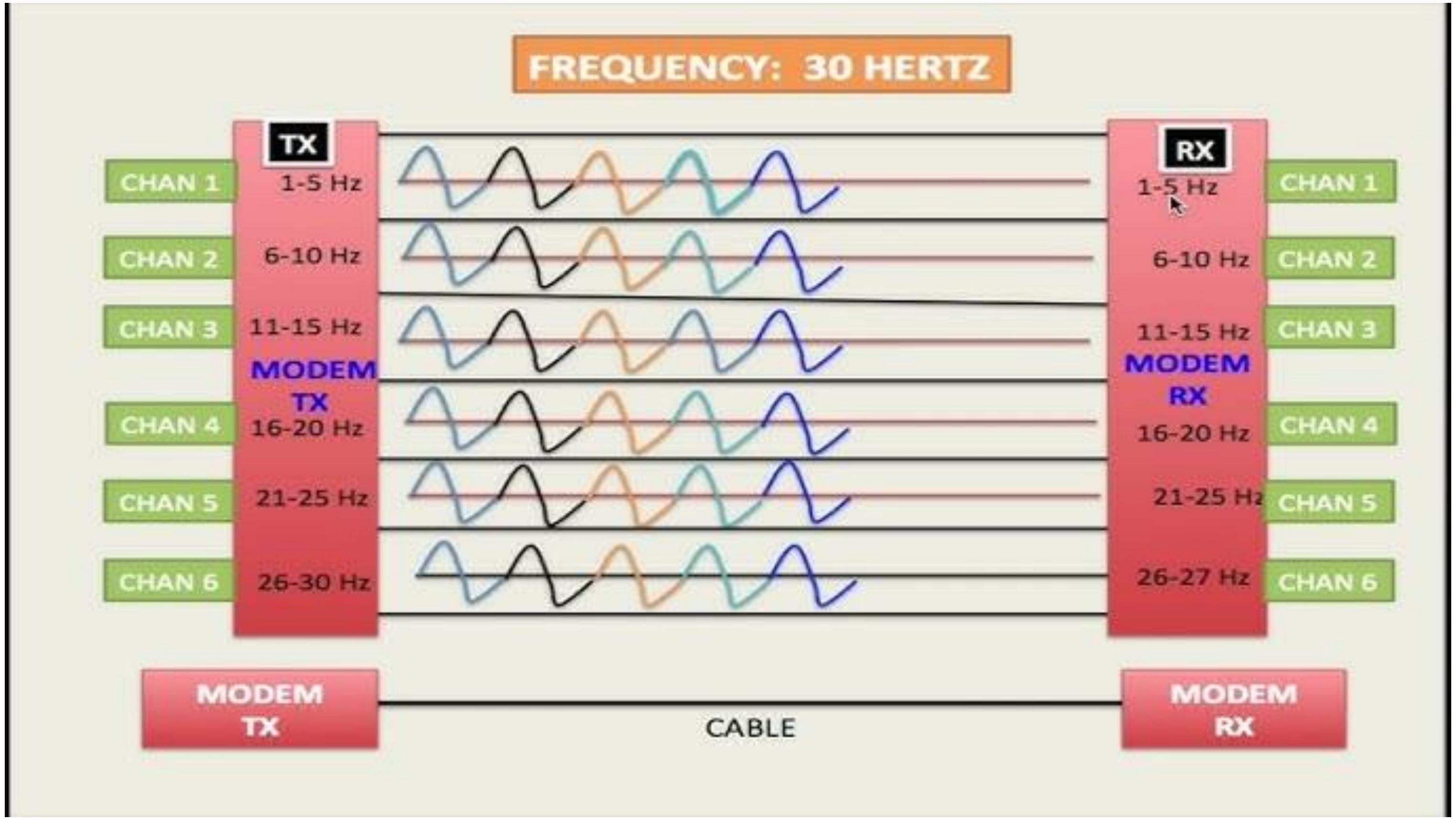
Brand	ARRIS
Internet service provider	Cox, Spectrum, Xfinity
Connectivity Technology	Ethernet
Compatible Devices	Router
Product Dimensions	5.13"L x 1.75"W x 5.25"H

About this item

- A Trusted Name in Home Connectivity: Better connectivity, better speed. The ARRIS SURFbo
SB8200 DOCSIS 3.1 Cable Modem is designed to bring you superior connectivity, increase y
network capability and provide faster streaming and downloading throughout your home. F
trusted brand with over 260 million modems sold and growing. .Telephone Port : None. HD

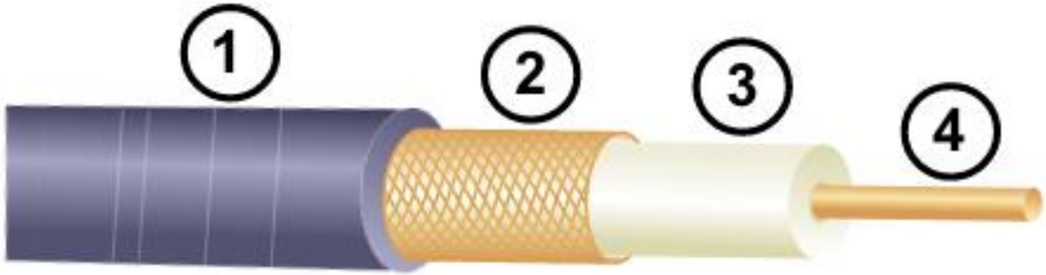
Broadband

It uses more than one frequency



Coaxial Cable

- Consists of the following:
  - Outer cable jacket to prevent minor physical damage
  - A woven copper braid, or metallic foil, acts as the second wire in the circuit and as a shield for the inner conductor.
  - A layer of flexible plastic insulation
  - A copper conductor is used to transmit the electronic signals.



Twinax

- Direct Access Cable
- Shrot range
- High speed
- 10 Gbps, 40 Gbps, and 100 Gbps.

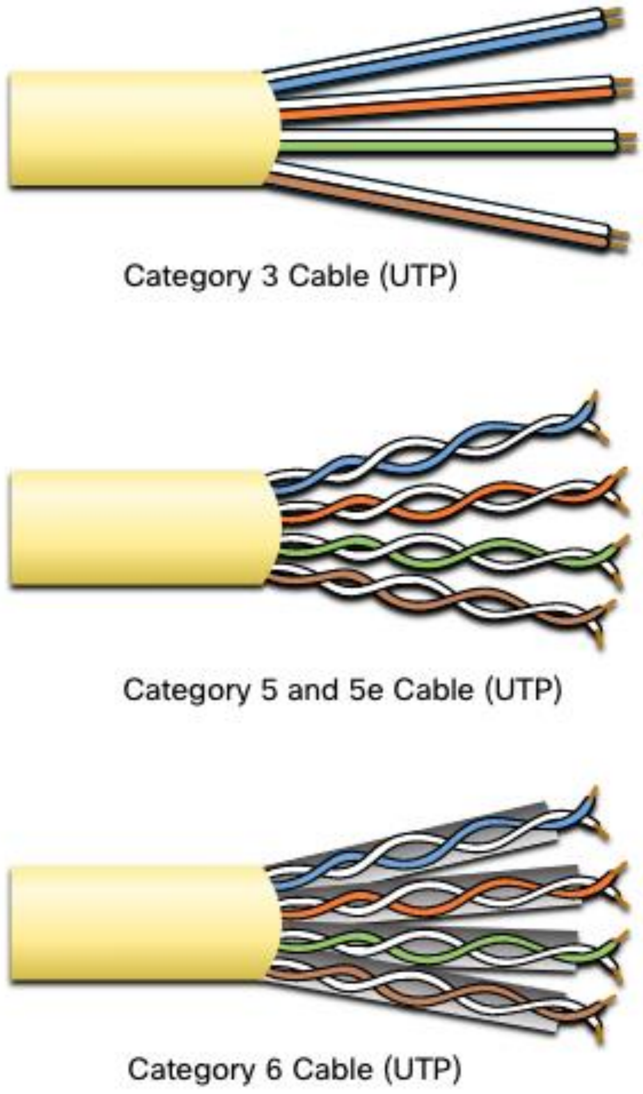
Small Formfactor Pluggable (SFP)

3.3 Twisted Pair Media

Unshielded Twisted Pair

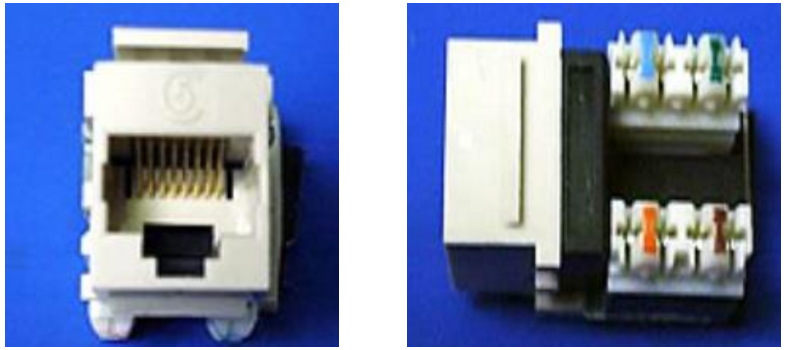
Standards for UTP are established by the TIA/EIA. TIA/EIA-568 standardizes elements like:

- Cable Types
- Cable Lengths
- Connectors
- Cable Termination
- Testing Methods



UTP Cabling Standards and Connectors

RJ-45 Connector

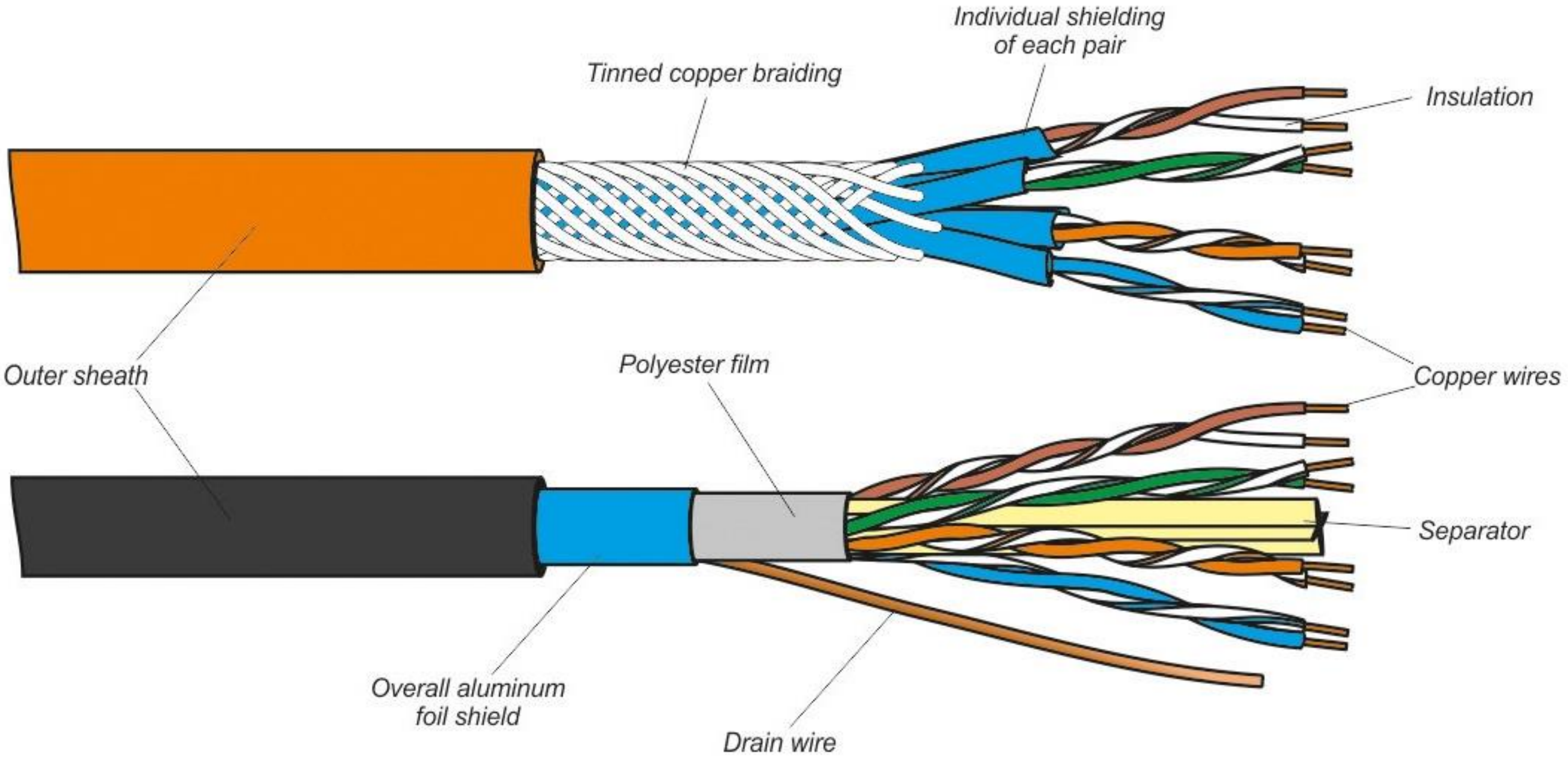


RJ-45 Socket

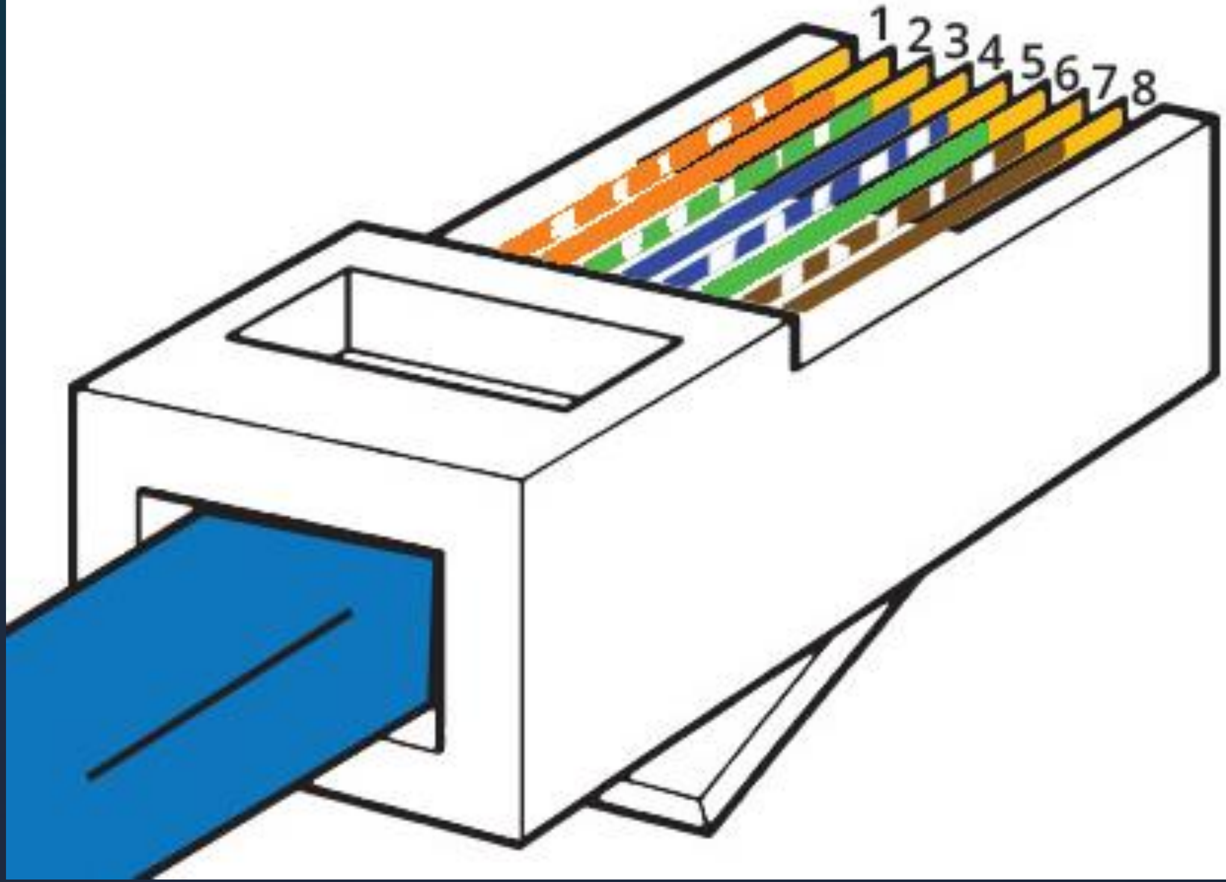
Poorly terminated UTP cable

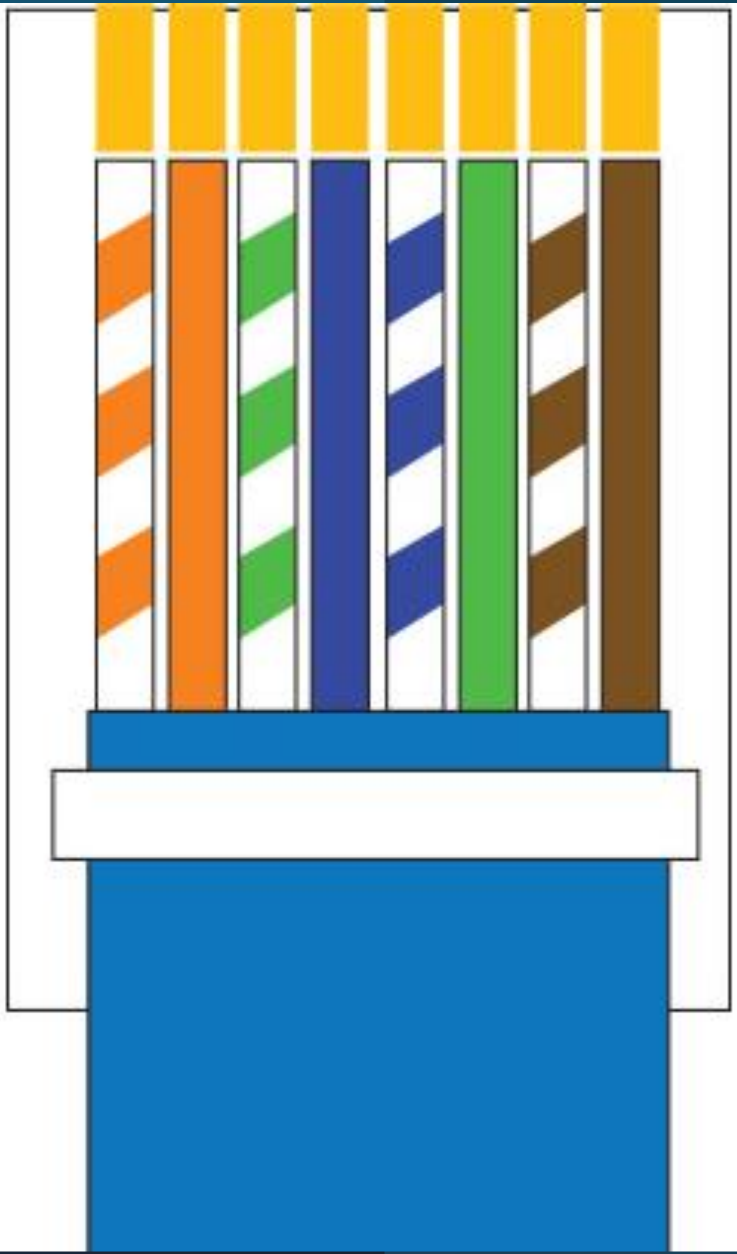
Properly terminated UTP cable

Shielded Twisted Pair

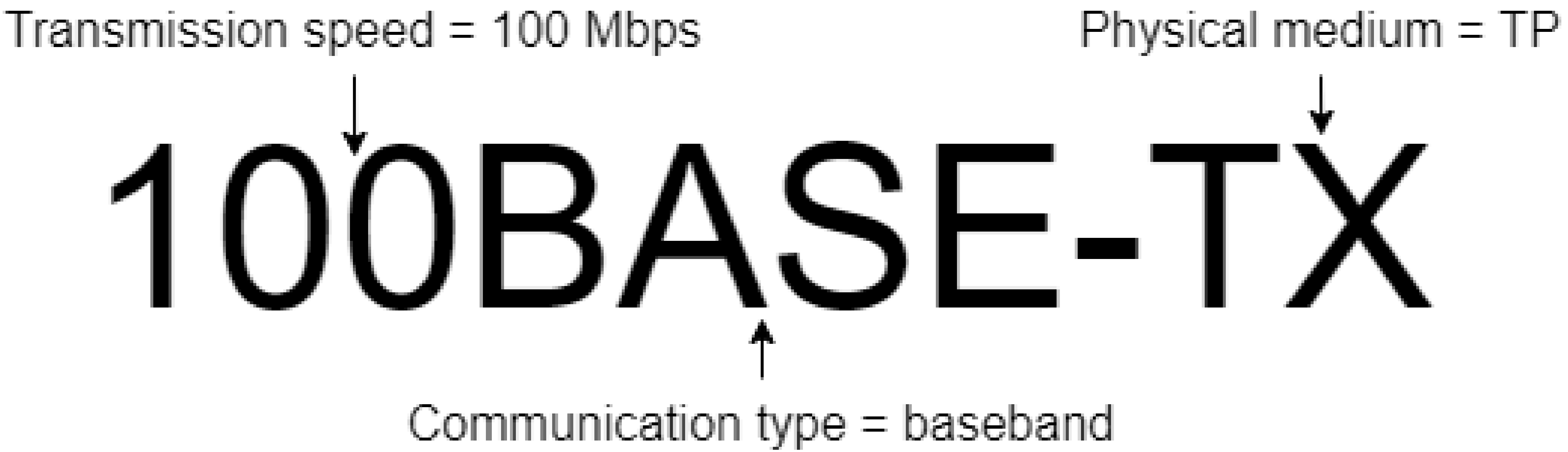


T-568B





Cabling Naming Convention



Decoding the naming Convention

Transmission Speed
10 – 10 Mbps
100 – 100Mbps
1000 – 1Gbps
10000 – 10 Gbps
40,000,0000 – 40Gbps

+

Baseband
Broadband

+

TX – Twisted Pair (Cat 5/5e/6, etc.)
T – Twisted Pair (general)
FX – Fiber Optic, Multimode (100 Mbps, ~2 km)
SX – Short-Range Multimode Fiber (~550 m)
LX – Long-Range **Single-Mode** Fiber (~10 km)
SR – Short-Range Multimode Fiber (10G, ~300–400 m)
LR – Long-Range Single-Mode Fiber
(10 km typical for 10GBASE-LR)

10BASE-T

Transmission Speed
10 – 10 Mbps
100 – 100Mbps
1000 – 1Gbps
10000 – 10 Gbps
40,000,0000 – 40Gbps

\+

Baseband
Broadband

\+

TX – Twisted Pair (Cat 5/5e/6, etc.)
T – Twisted Pair (general)
FX – Fiber Optic, Multimode (100 Mbps, ~2 km)
SX – Short-Range Multimode Fiber (~550 m)
LX – Long-Range **Single-Mode** Fiber (~10 km)
SR – Short-Range Multimode Fiber (10G, ~300–400 m)
LR – Long-Range Single-Mode Fiber
(10 km typical for 10GBASE-LR)

- 10 Mbps
- Baseband
- Twisted Pair

100BASE-FX

Transmission Speed
10 – 10 Mbps
100 – 100Mbps
1000 – 1Gbps
10000 – 10 Gbps
40,000,0000 – 40Gbps

➕

Baseband
Broadband

➕

TX – Twisted Pair (Cat 5/5e/6, etc.)
T – Twisted Pair (general)
FX – Fiber Optic, Multimode (100 Mbps, ~2 km)
SX – Short-Range Multimode Fiber (~550 m)
LX – Long-Range **Single-Mode** Fiber (~10 km)
SR – Short-Range Multimode Fiber (10G, ~300–400 m)
LR – Long-Range Single-Mode Fiber
(10 km typical for 10GBASE-LR)

- 100 Mbps
- Baseband
- Multimode Fiber

40BASE-T

Transmission Speed
10 – 10 Mbps
100 – 100Mbps
1000 – 1Gbps
10000 – 10 Gbps
40,000,0000 – 40Gbps

Baseband
Broadband

TX – Twisted Pair (Cat 5/5e/6, etc.)
T – Twisted Pair (general)
FX – Fiber Optic, Multimode (100 Mbps, ~2 km)
SX – Short-Range Multimode Fiber (~550 m)
LX – Long-Range **Single-Mode** Fiber (~10 km)
SR – Short-Range Multimode Fiber (10G, ~300–400 m)
LR – Long-Range Single-Mode Fiber
(10 km typical for 10GBASE-LR)

- 40 Mbps
- Baseband
- Twisted Pair

10BASE-LR

Transmission Speed
10 – 10 Mbps
100 – 100Mbps
1000 – 1Gbps
10000 – 10 Gbps
40,000,0000 – 40Gbps

+

Baseband
Broadband

+

TX – Twisted Pair (Cat 5/5e/6, etc.)
T – Twisted Pair (general)
FX – Fiber Optic, Multimode (100 Mbps, ~2 km)
SX – Short-Range Multimode Fiber (~550 m)
LX – Long-Range **Single-Mode** Fiber (~10 km)
SR – Short-Range Multimode Fiber (10G, ~300–400 m)
LR – Long-Range Single-Mode Fiber
(10 km typical for 10GBASE-LR)

- 10 Mbps
- Baseband
- Long-Range Single mode Fiber

100BASE-TX

Transmission Speed
10 – 10 Mbps
100 – 100Mbps
1000 – 1Gbps
10000 – 10 Gbps
40,000,0000 – 40Gbps

+

Baseband
Broadband

+

TX – Twisted Pair (Cat 5/5e/6, etc.)
T – Twisted Pair (general)
FX – Fiber Optic, Multimode (100 Mbps, ~2 km)
SX – Short-Range Multimode Fiber (~550 m)
LX – Long-Range **Single-Mode** Fiber (~10 km)
SR – Short-Range Multimode Fiber (10G, ~300–400 m)
LR – Long-Range Single-Mode Fiber
(10 km typical for 10GBASE-LR)

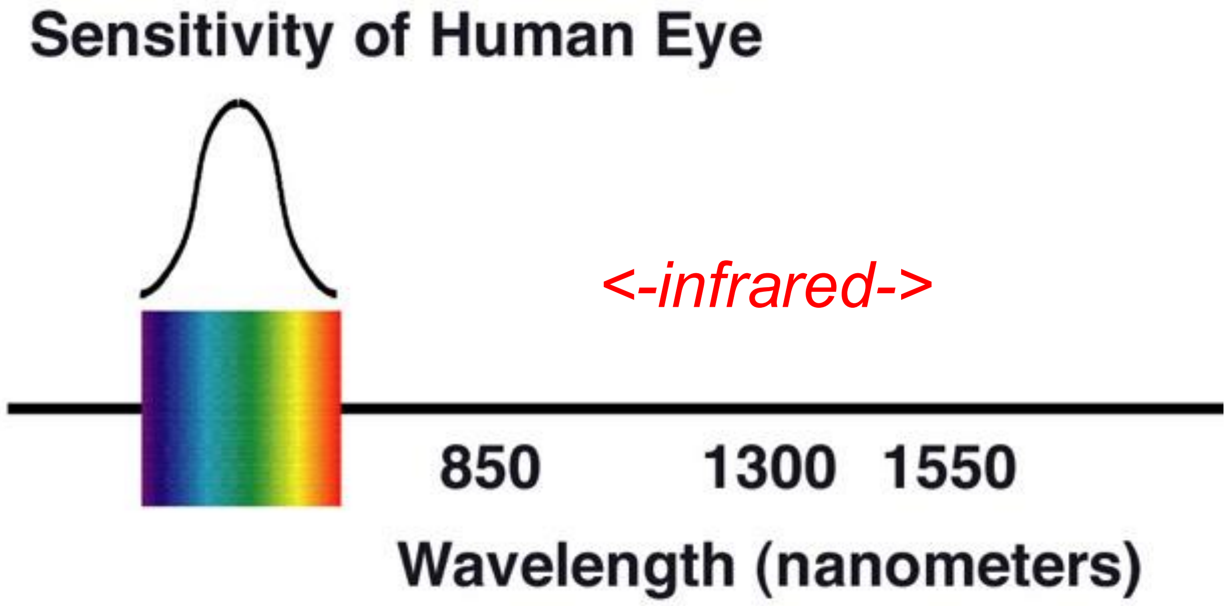
- 100 Mbps
- Baseband
- Twisted Pair

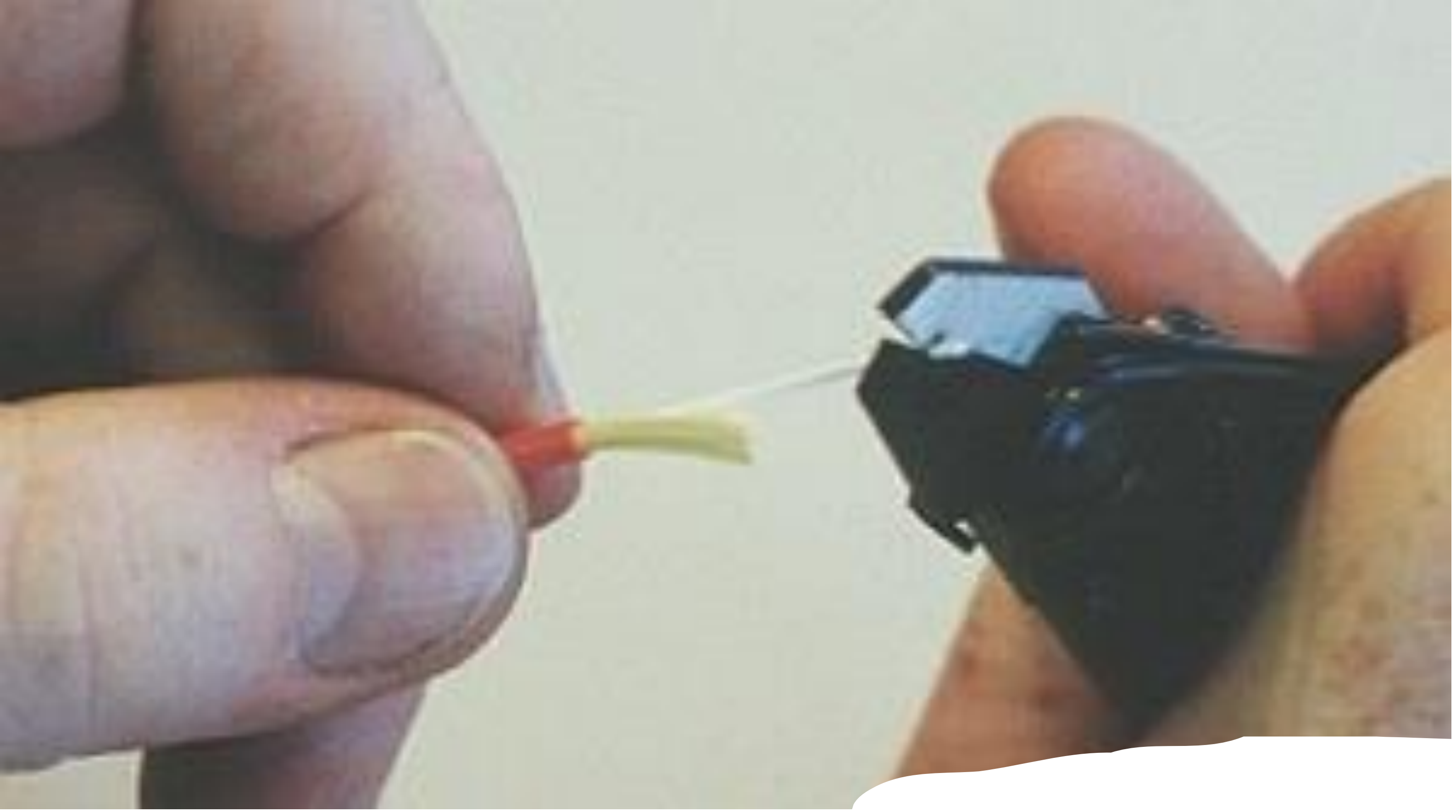
Fiber Optic Media

Safety

- Read and follow rules in lab manual
- Wear safety glasses
- Don't look at fibers
- Dispose of fiber scraps carefully
- Work on dark surface to help spot fiber scraps
- Be careful with chemicals
- No eating or drinking in labs

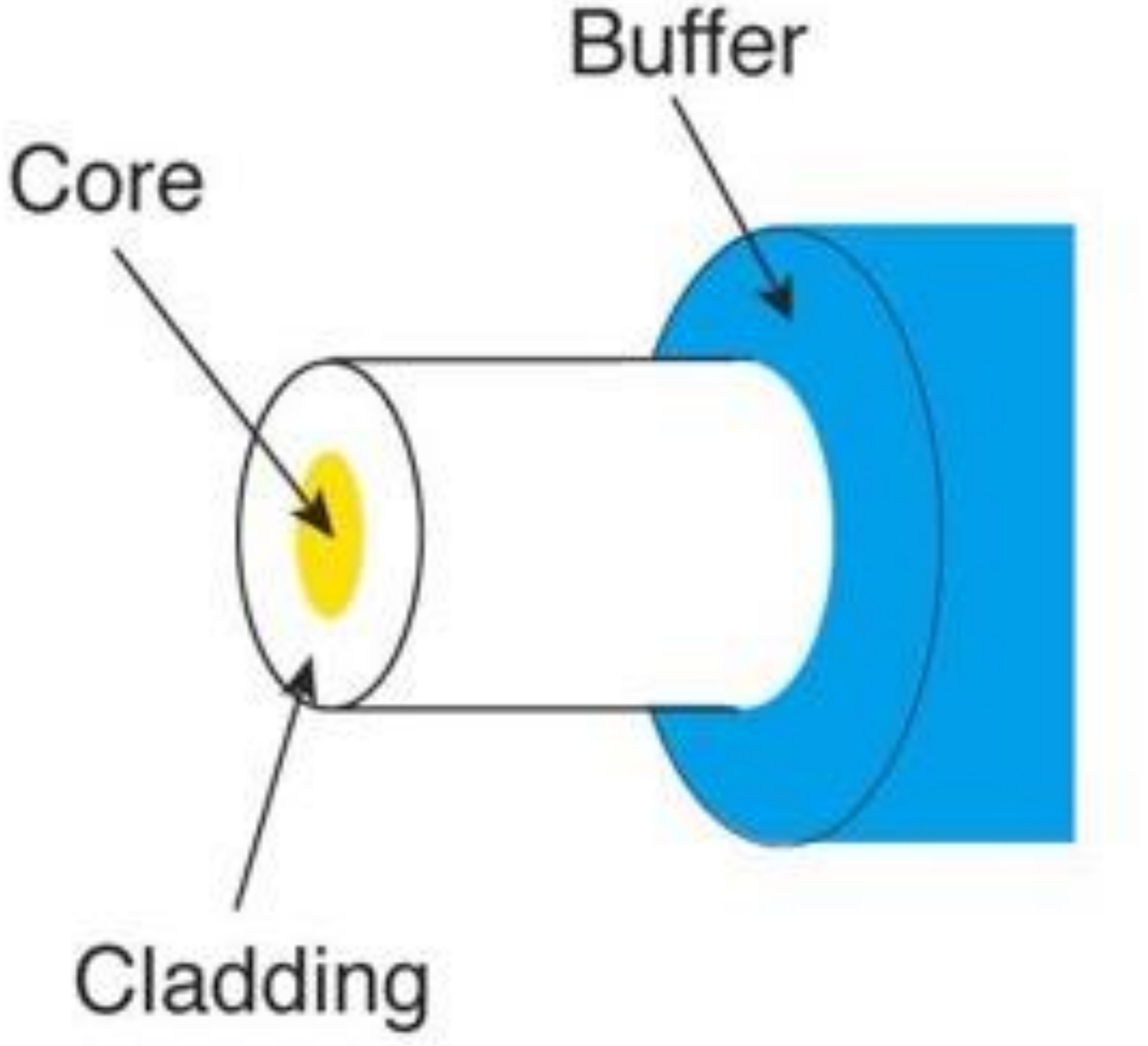
Most light is Infrared





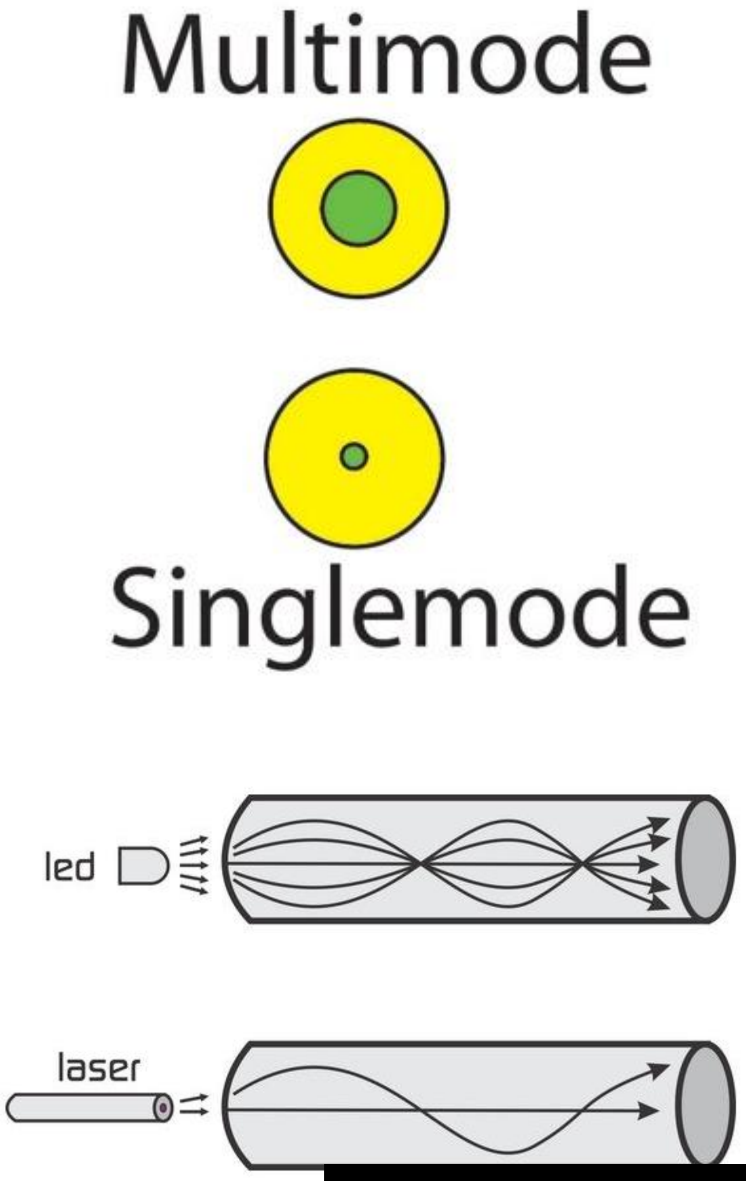
Fiber Scraps (Most Dangerous)

Anatomy of fiber optic cable



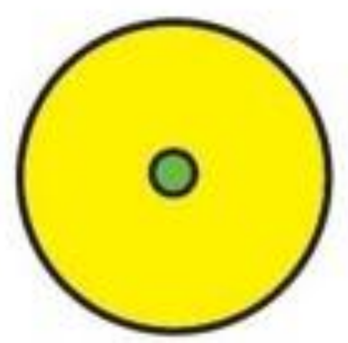
Two types of fiber cable

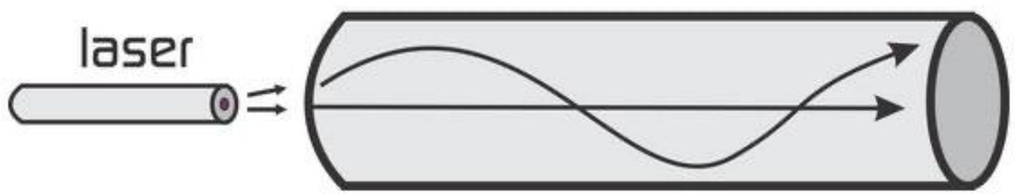
- Multimode (MM) fiber – large core fiber used for slower premises (indoor) networks
- Singlemode (SM) fiber – small core fiber used for everything else – higher bandwidth and lower attenuation



Singlemode

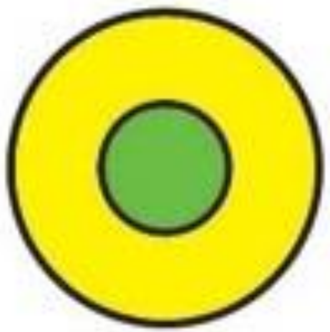
- Singlemode (SM) fiber – small core fiber used for everything else – higher bandwidth and lower attenuation
- Core size is 8 Microns in diameter

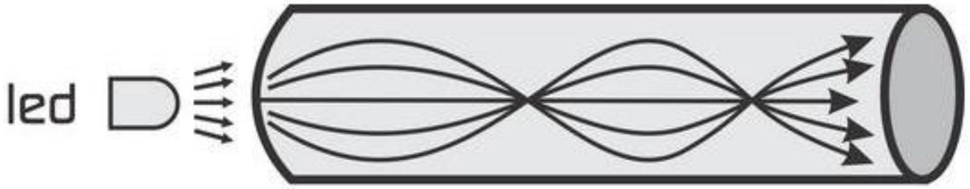




Mulitmode

- Multimode (MM) fiber – large core fiber used for slower premises (indoor) networks
- Fiber cores are 50- 62.6 microns
- Different Rays or Modes of light are transmitted in multimode fiber



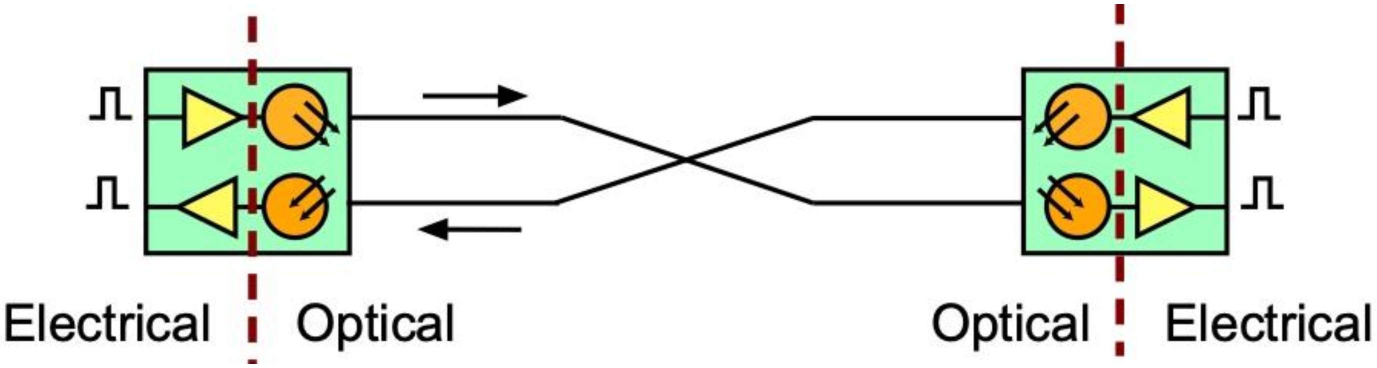


Convert Electrical To Optical

Transceivers

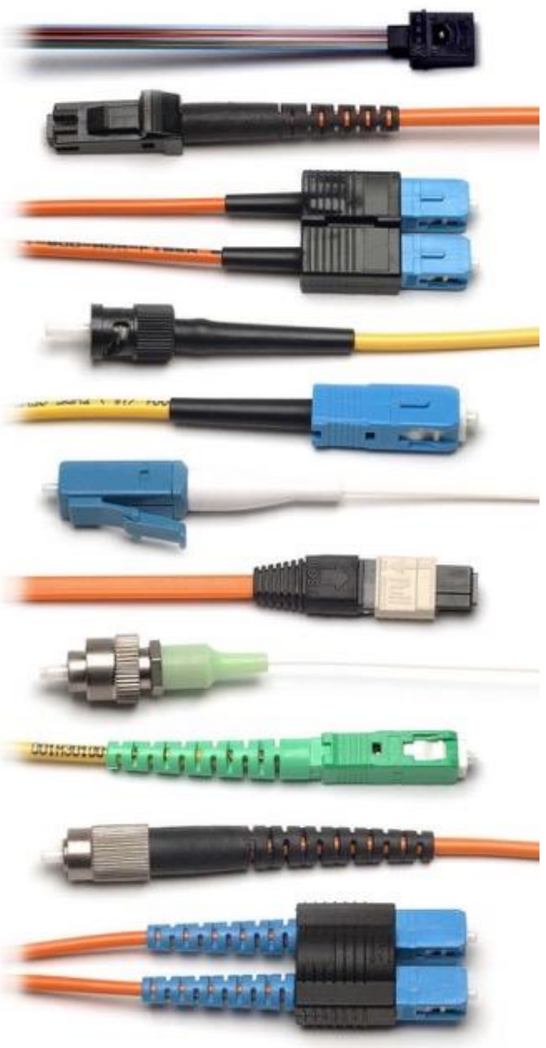
Media

Converters



Fiber Optic Connectors & Splices

- Connectors and splices must have:
  - Low loss
  - Low reflectance
  - Mechanical strength
  - Reliability
  - Ease of use in the field



Connector Identifier

ST

LC

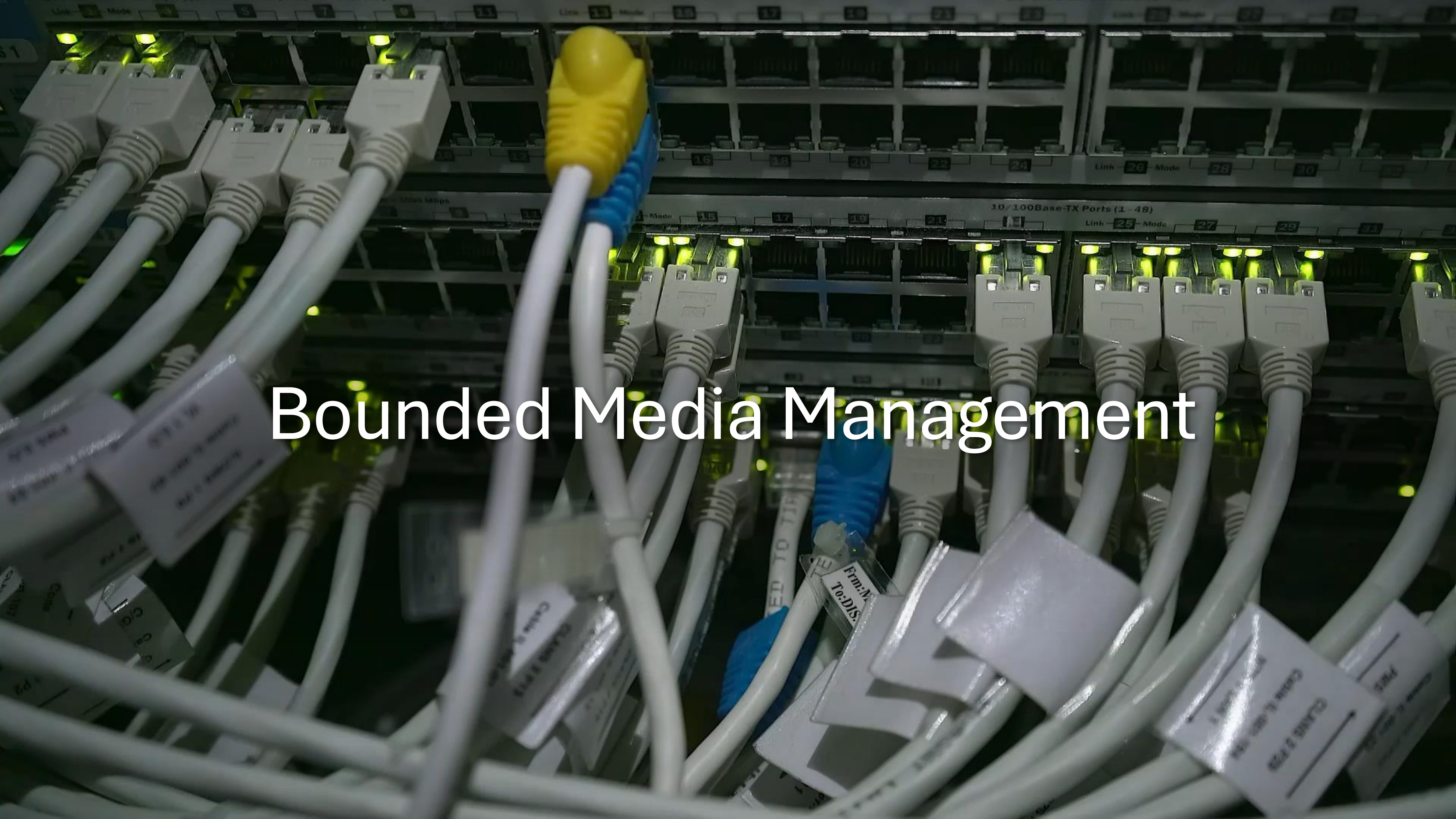
SC

MPO

Do You Have To Field Terminate At All?

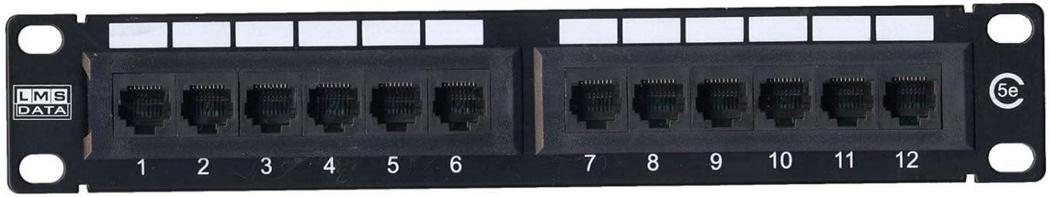
- Design a prefabricated cabling system that you just install, plug in and test
- May be cost effective in new construction
- Premises components shown

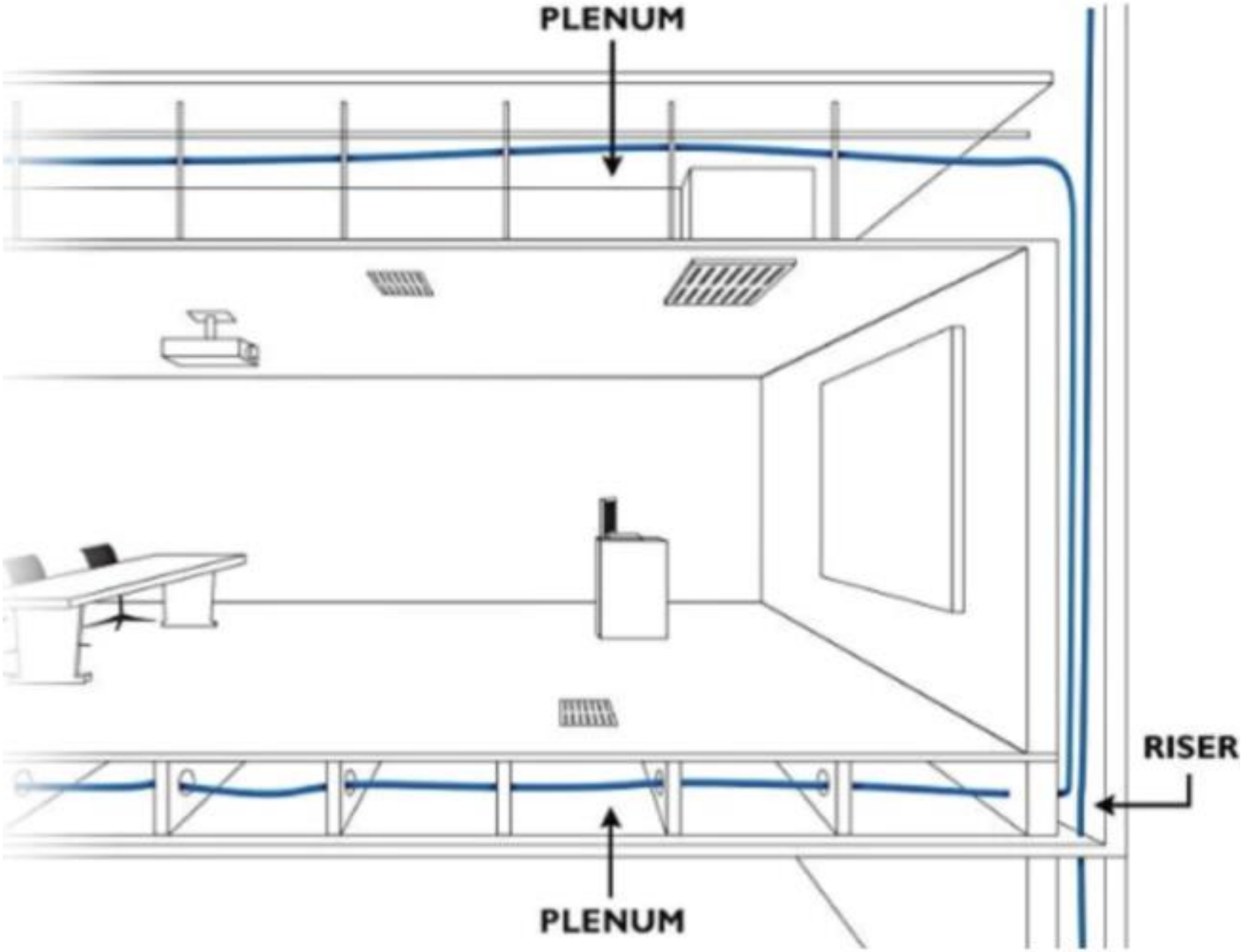
Bounded Media Management



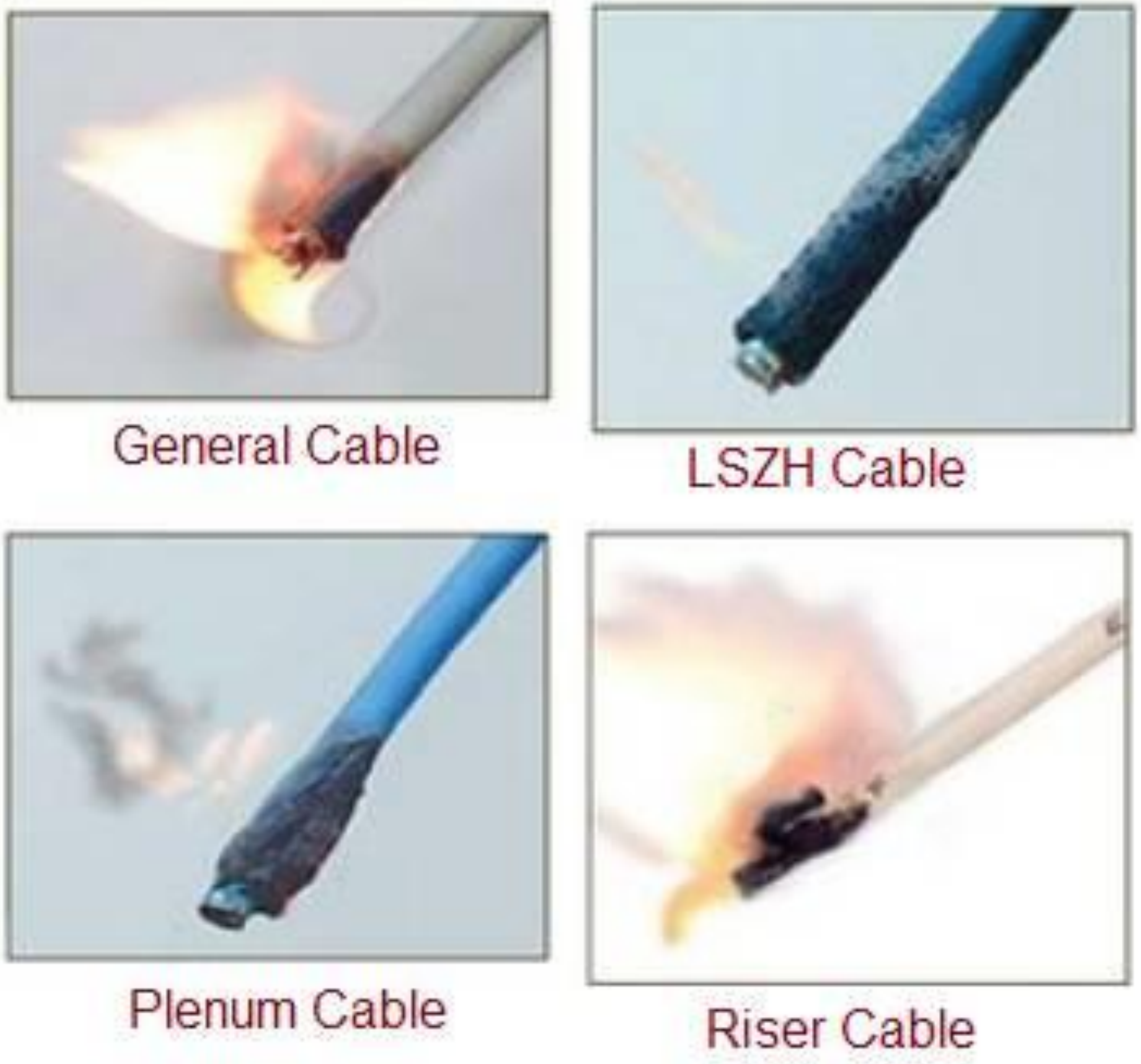
Patch Panels

- Numerous Ports
- Usually in the networking or distribution closet
- Uses a punchdown





structured cabling pathways


General Cable
LSZH Cable
Plenum Cable
Riser Cable

Reading OSP Cable Jackets

- Here is an excellent example of why you need to learn to “read” cables. There is a
- lot of useful information there and some is critical for proper installation of the cable.

Network Cable Making

Station #1

Mapping Network Drops

Station #2

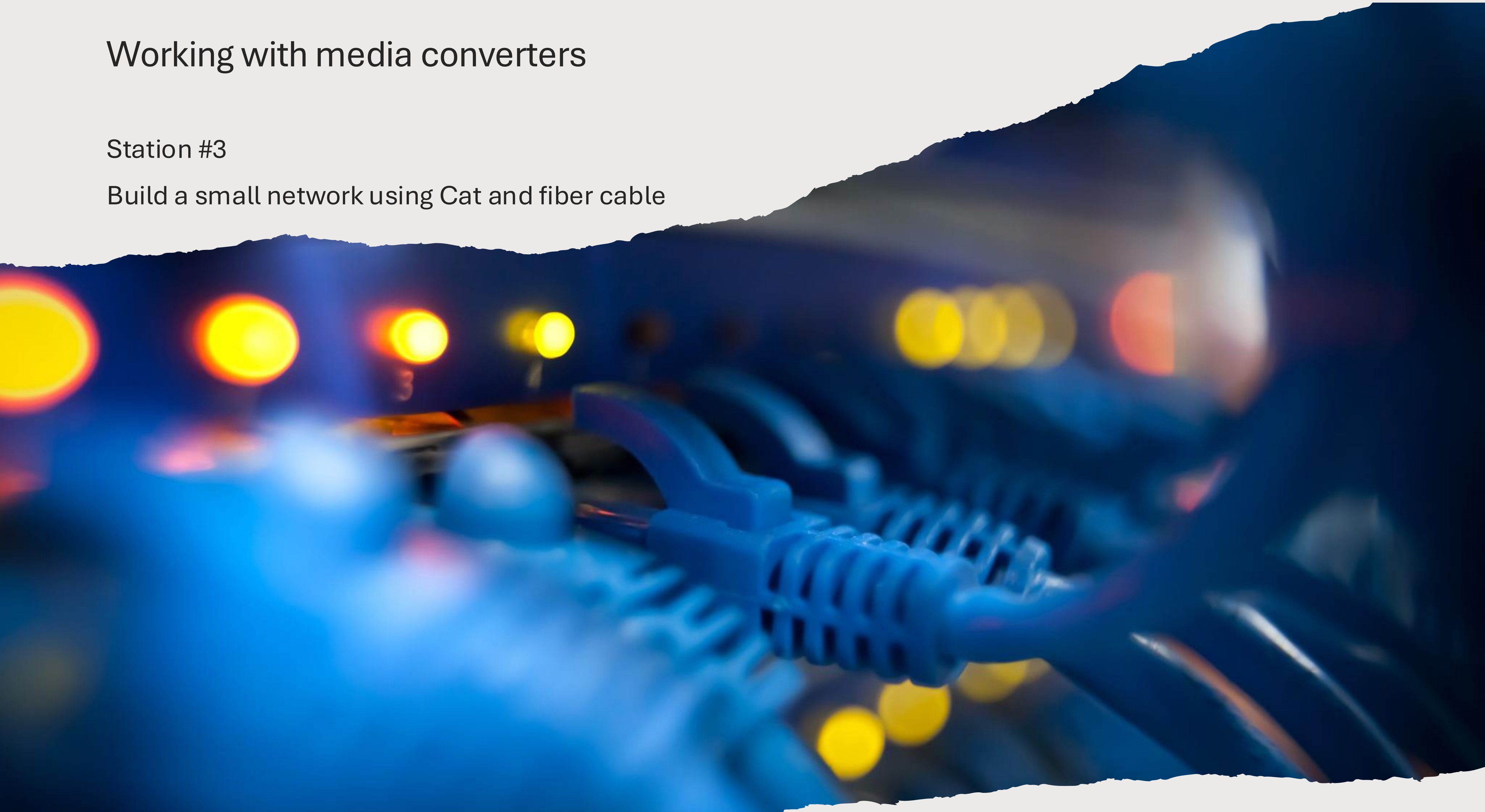
Using a fluke cable tester

Map cables in classroom to patch pannel

Working with media converters

Station #3

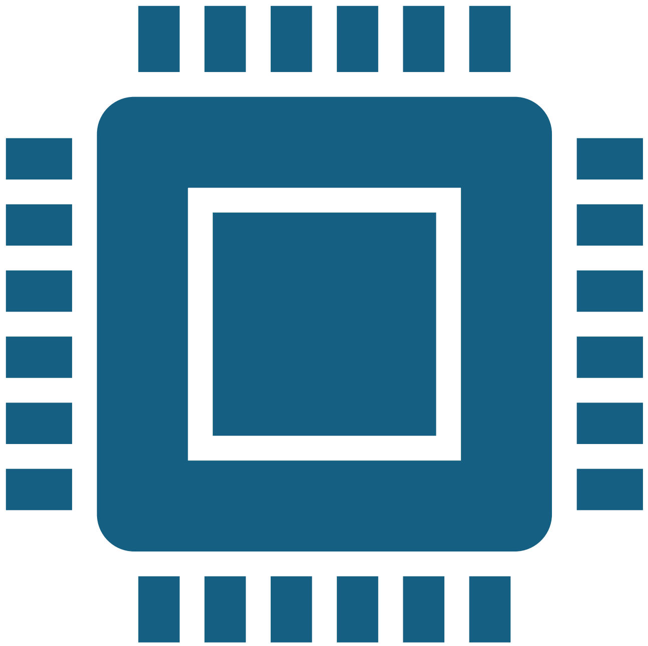
Build a small network using Cat and fiber cable



Station #4

Using a punch down to create patch panels

Making Patch Panels



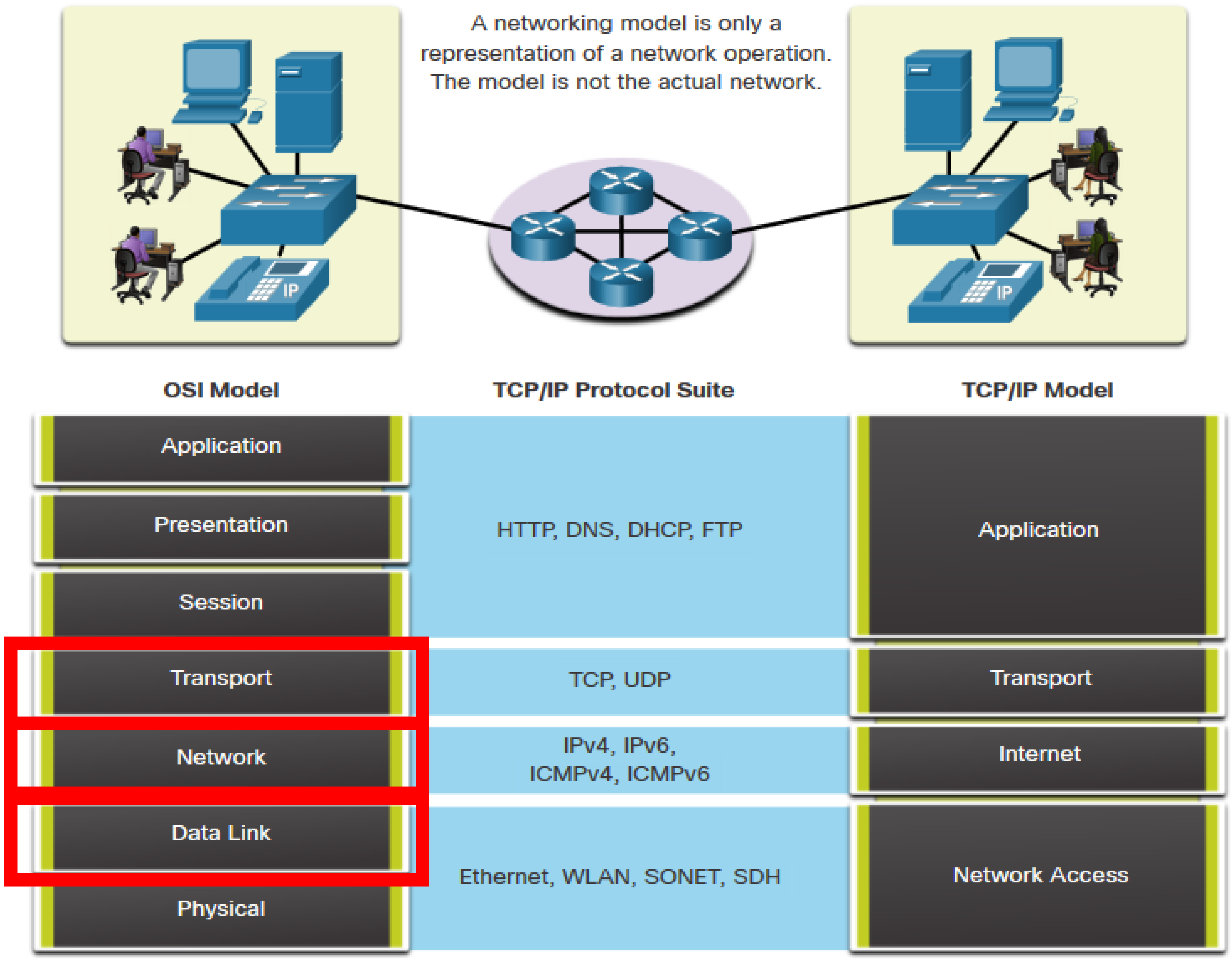
Chapter 3: Bounded Media Standards and Applications

Chapter 4: Address Types

Take out a paper and write down the 7-layer OSI model

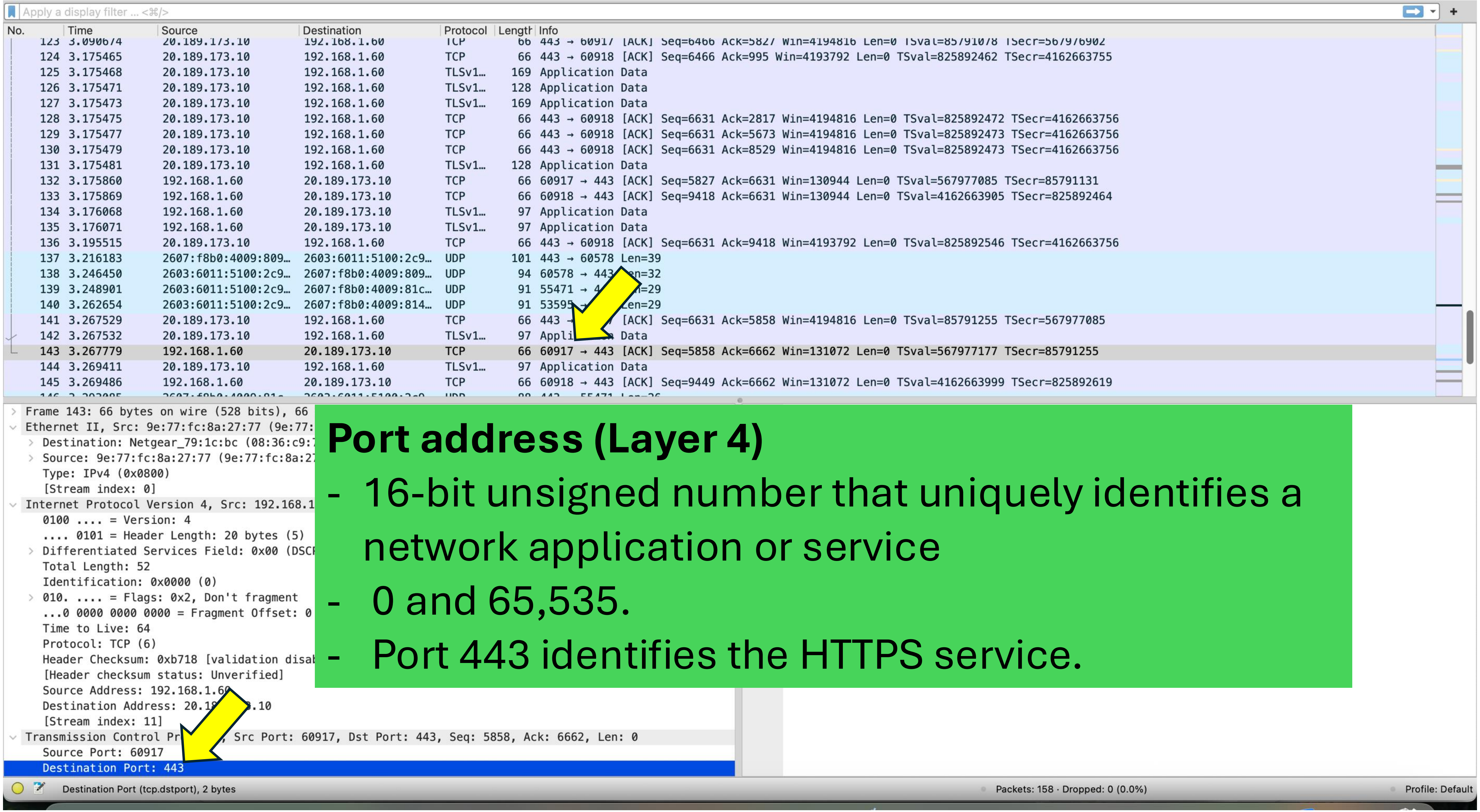
		PDU
Layer 7	Application	DATA
Layer 6	Presentation	
Layer 5	Session	
Layer 4	Transport	Segment
Layer 3	Network	Packet
Layer 2	Data link	Frame
Layer 1	Physical	BITS

4.1 Types of network addresses


A networking model is only a representation of a network operation. The model is not the actual network.
IP
IP
OSI Model
TCP/IP Protocol Suite
TCP/IP Model
Application
Presentation
Session
Transport
Network
Data Link
Physical
HTTP, DNS, DHCP, FTP
TCP, UDP
IPv4, IPv6, ICMPv4, ICMPv6
Ethernet, WLAN, SONET, SDH
Application
Transport
Internet
Network Access

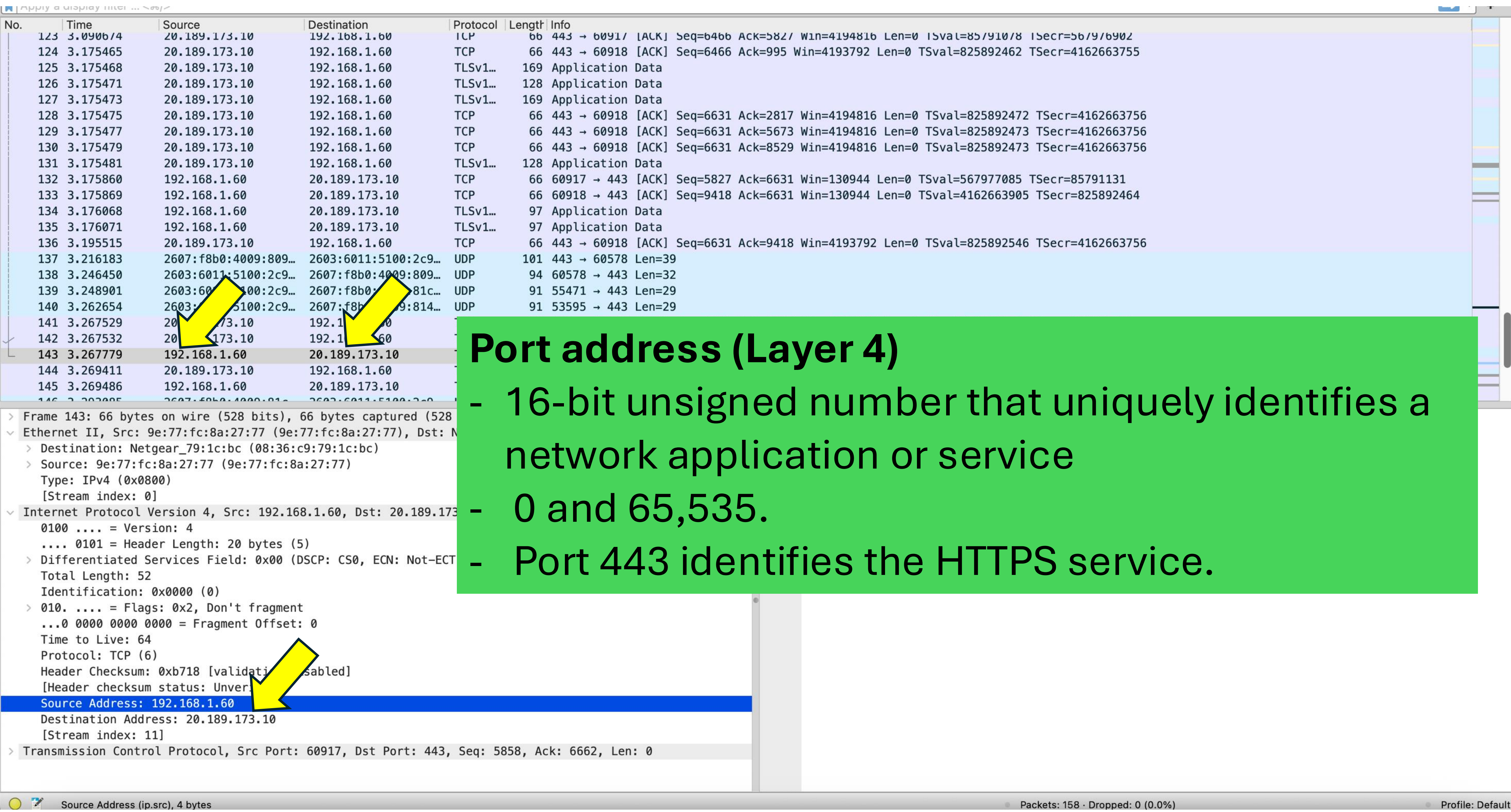
Encapsulation Process

TCP/IP Layers				
Application				Data
Transport			TCP	Data
Internet		IP	TCP	Data
Network access	Ethernet	IP	TCP	Data



Port address (Layer 4)

- 16-bit unsigned number that uniquely identifies a network application or service
- 0 and 65,535.
- Port 443 identifies the HTTPS service.

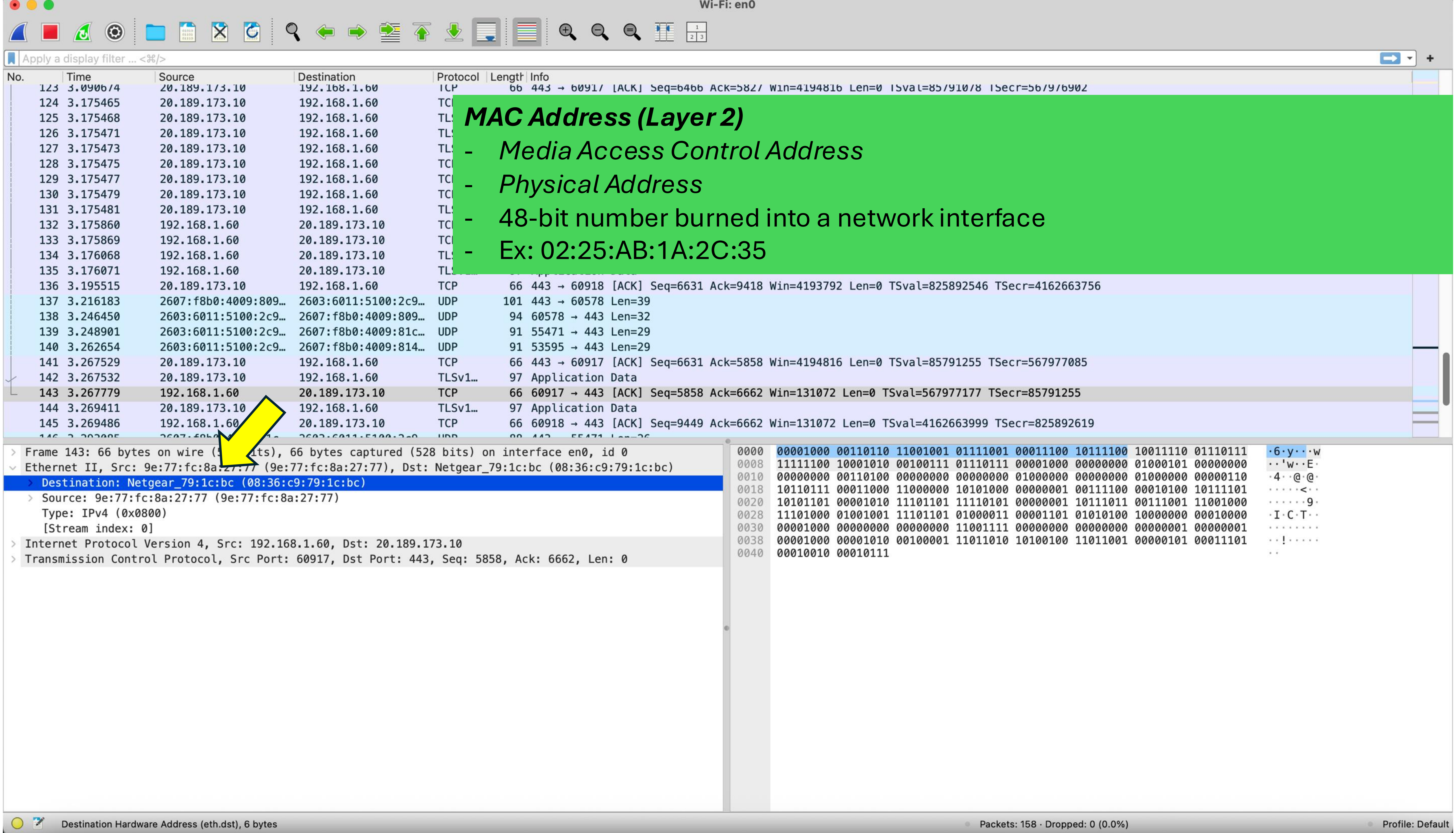


Port address (Layer 4)

- 16-bit unsigned number that uniquely identifies a network application or service
- 0 and 65,535.
- Port 443 identifies the HTTPS service.

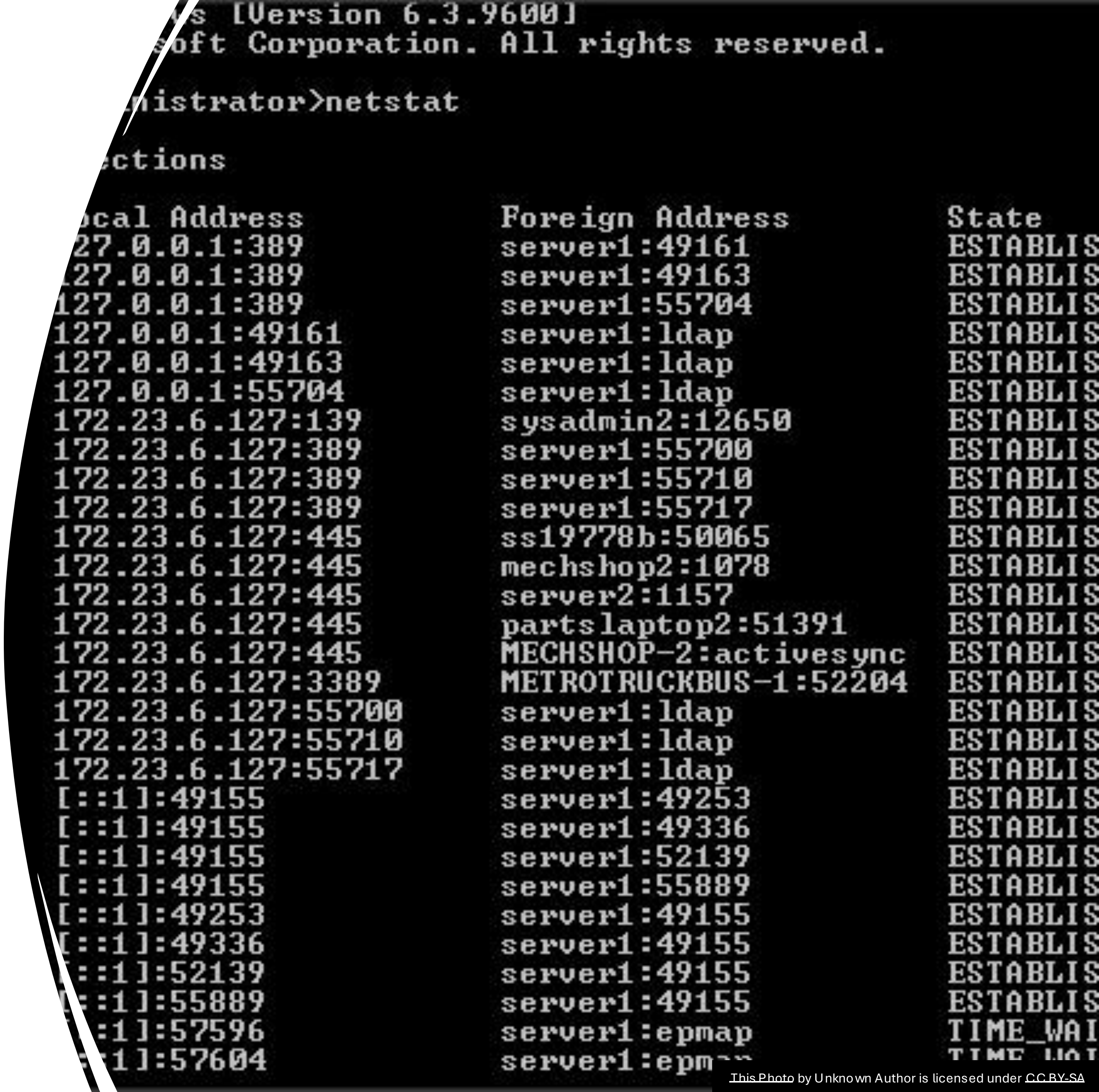
MAC Address (Layer 2)

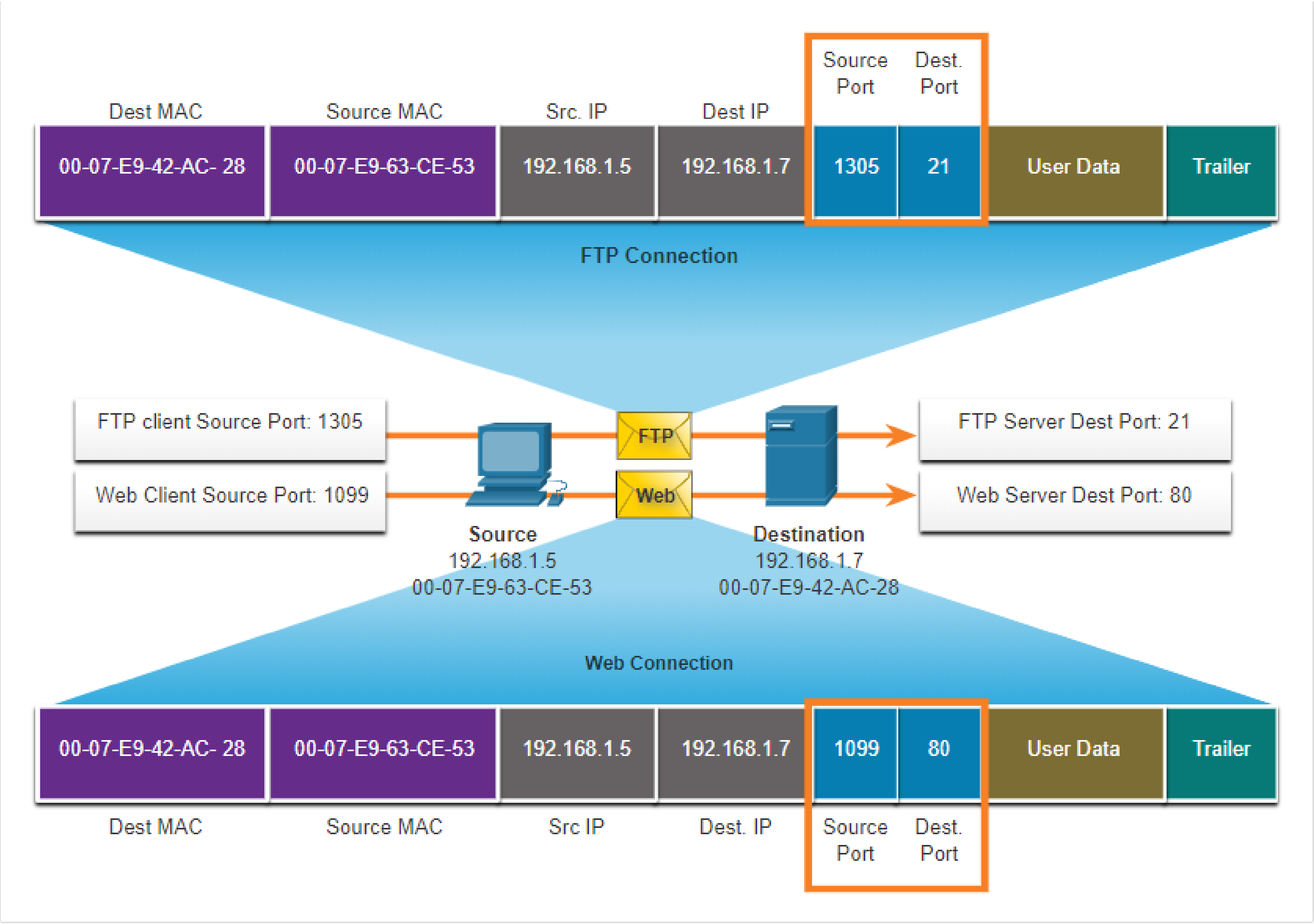
- *Media Access Control Address*
- *Physical Address*
- 48-bit number burned into a network interface
- Ex: 02:25:AB:1A:2C:35



Port Address

- Network connections use **port addresses** to identify services
- IP address → device location; Port address → service/process
- Devices handle multiple services at once (e.g., email, FTP, web)
- Common ports: **20/21 = FTP**, **443 = HTTPS**
- Hackers exploit open ports → close unused ports for security





Source Port
Dest. Port
Dest MAC
Source MAC
Src. IP
Dest IP
00-07-E9-42-AC- 28
00-07-E9-63-CE-53
192.168.1.5
192.168.1.7
1305
21
User Data
Trailer
FTP Connection
FTP client Source Port: 1305
Web Client Source Port: 1099
FTP
Web
FTP Server Dest Port: 21
Web Server Dest Port: 80
Source
192.168.1.5
00-07-E9-63-CE-53
Destination
192.168.1.7
00-07-E9-42-AC-28
Web Connection
00-07-E9-42-AC- 28
00-07-E9-63-CE-53
192.168.1.5
192.168.1.7
1099
80
User Data
Trailer
Dest MAC
Source MAC
Src IP
Dest. IP
Source Port
Dest. Port

iana

Internet Assigned Numbers Authority

Service Name and Transport Protocol Port Number Registry

Last Updated

2025-08-26

Expert(s)

TCP/UDP: Joe Touch; Eliot Lear, Kumiko Ono, Wes Eddy, Brian Trammell,
Jana Iyengar, and Michael Scharf
SCTP: Michael Tuexen
DCCP: Eddie Kohler and Yoshifumi Nishida

Reference

[RFC6335]

Note

```
Service names and port numbers are used to distinguish between different
services that run over transport protocols such as TCP, UDP, DCCP, and
SCTP.

Service names are assigned on a first-come, first-served process, as
documented in [RFC6335].

Port numbers are assigned in various ways, based on three ranges: System
Ports (0-1023), User Ports (1024-49151), and the Dynamic and/or Private
Ports (49152-65535); the different uses of these ranges are described in
[RFC6335]. According to Section 8.1.2 of [RFC6335], System Ports are
assigned by the "IETF Review" or "IESG Approval" procedures described in
[RFC8126]. User Ports are assigned by IANA using the "IETF Review" process,
the "IESG Approval" process, or the "Expert Review" process, as per
[RFC6335]. Dynamic Ports are not assigned.

The registration procedures for service names and port numbers are
described in [RFC6335].

Assigned ports both System and User ports SHOULD NOT be used without
or prior to IANA registration.

************************************************************************
* PLEASE NOTE THE FOLLOWING:                                           *
*                                                                      *
* ASSIGNMENT OF A PORT NUMBER DOES NOT IN ANY WAY IMPLY AN             *
* ENDORSEMENT OF AN APPLICATION OR PRODUCT, AND THE FACT THAT NETWORK  *
* TRAFFIC IS FLOWING TO OR FROM A REGISTERED PORT DOES NOT MEAN THAT   *
* IT IS "GOOD" TRAFFIC, NOR THAT IT NECESSARILY CORRESPONDS TO THE     *
* ASSIGNED SERVICE. FIREWALL AND SYSTEM ADMINISTRATORS SHOULD          *
* CHOOSE HOW TO CONFIGURE THEIR SYSTEMS BASED ON THEIR KNOWLEDGE OF    *
* THE TRAFFIC IN QUESTION, NOT WHETHER THERE IS A PORT NUMBER          *
* REGISTERED OR NOT.                                                   *
************************************************************************
```

Request an Assignment

[https://www.iana.org/protocols/apply]

Available Formats

CSV XML HTML Plain text

Search

1 2 3 4 5 6 ... 145

Port address numbers

Well-known Ports	0 - 1023
Registered Ports	1024 - 49151
Dynamic Ports	49152 - 65565

Common port numbers

Port number	Service	Transport protocol
20, 21	File Transfer Protocol (FTP)	TCP
23	Telnet	TCP
25	SMTP	TCP
53	DNS	UDP/TCP
67, 68	DHCP	UDP
69	TFTP	UDP
80	HyperText Transfer Protocol (HTTP)	TCP
110	POP3	TCP
123	Network Time Protocol (NTP)	UDP
143	IMAP	TCP
443	HTTPS (Secure Socket Layer/Transport Layer Security)	TCP
445	SMB	TCP
514	Syslog	UDP
993	IMAPS	TCP
995	POP3 SSL	TCP
1433	SQL Server	TCP
1521	SQLNET	TCP
2095	Webmail	TCP
3306	MySQL	TCP
3389	RDP	TCP
5060, 5061	SIP	UDP/TCP

Fun Port numbers to know

Minecraft

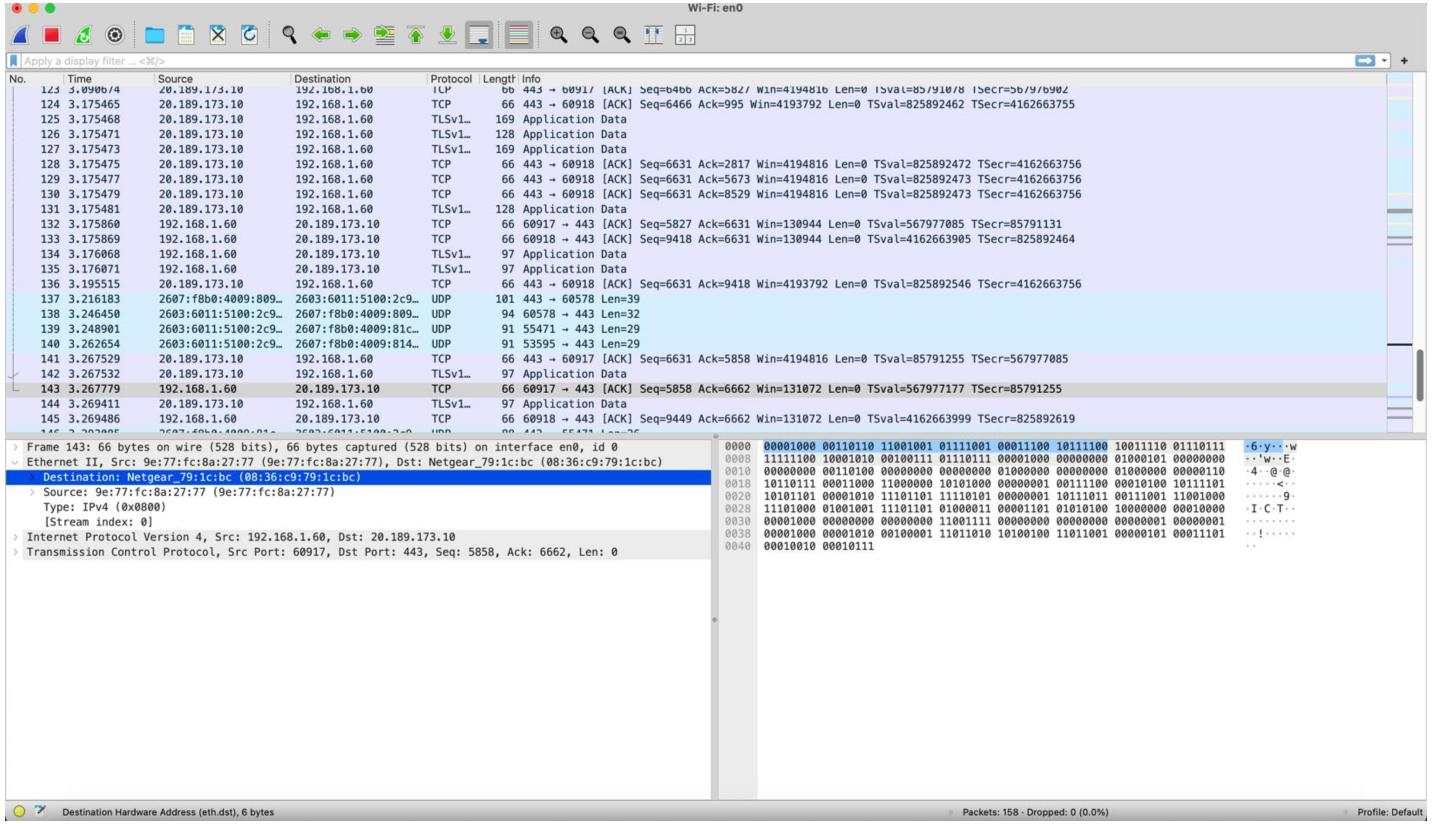
- Java Edition is Port 25565 (TCP/UDP)
- Bedrock Edition Port 19132 UDP and Port 30033 TCP

Call of Duty

PC, Xbox Port 3074
Playstation Port 3478
Xbox Port 88

Fortnite (PC)
Ports: 80 (TCP/UDP), 433 (TCP/UDP), 443 (TCP), 3478 (TCP/UDP), 3479 (TCP/UDP), 5060 (TCP/UDP), 5062 (TCP/UDP), 5222 (TCP), 6250 (TCP/UDP), and 12000-65000 (TCP/UDP).
Action: You need to unblock these ports in your firewall for both the Epic Games Launcher and Fortnite to function properly.
For PlayStation Consoles
PS4: Requires ports 433 (TCP), 1935 (TCP), 3478-3480 (TCP/UDP), and 5222 (TCP).
PS5: Requires ports 433 (TCP), 1935 (TCP), 3478-3480 (TCP), and 5222 (TCP).
For Xbox Consoles
Xbox One: Requires ports 433 (TCP), 3074 (TCP), and 5222 (TCP).
Xbox Series X/S: Requires ports 433 (TCP), 3074 (TCP), and 5222 (TCP).

Wireshark Demo with Port numbers



4.2 MAC address

Windows (command)

1. Open **Command Prompt**.
2. Run: ipconfig /all
3. Find your adapter and read **Physical Address**.

macOS (Terminal)

1. Open **Terminal**.
2. Run (Wi-Fi): `ifconfig en0 | grep ether` or (Ethernet): `ifconfig en1 | grep ether`
3. he `ether` value is the MAC.

Chromebook (Crosh)

- Press **Ctrl+Alt+T** to open crosh.
- Type ifconfig and press Enter.
- Read the ether line for the interface's MAC.

Linux (terminal)

1. Open a terminal.
2. Run either: ip link show **or** ifconfig -a
3. Find your interface; the MAC is listed as link/ether (ip) or ether (ifconfig).

4.2 MAC (Media Access Control Address)

- Unique 48-bit identifier burned into a network interface controller (NIC).
- Assigned by the manufacturer, ensuring each device has a unique address.

a2:ba:78:e2:e2:b4

Organizationally Unique Identifier (OUI)

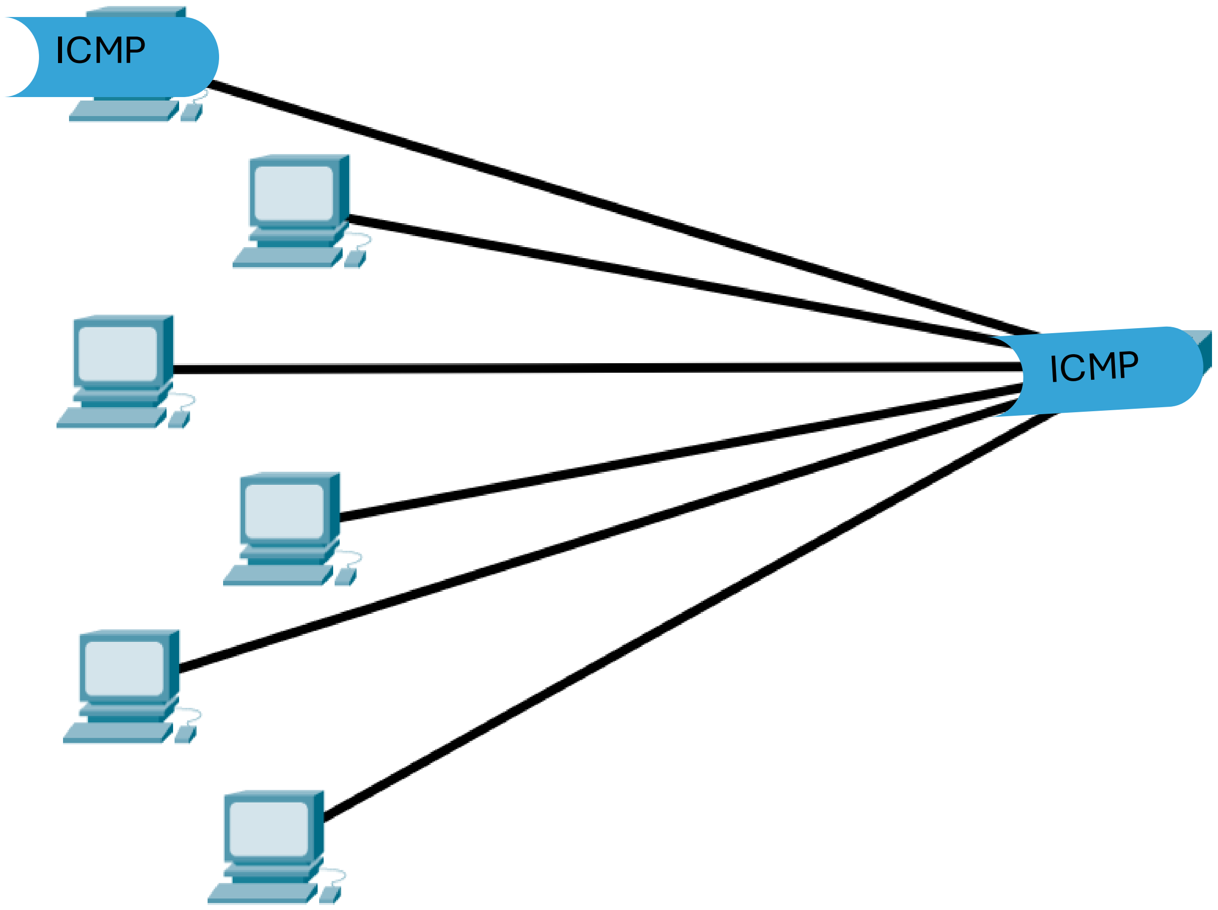
- First 24 bits (first 6 digits).
- Identifies the manufacturer and device model.
- OUIs are purchased from IEEE (creators of the 802 networking standards).

Device ID (Vendor Assigned Identifier)

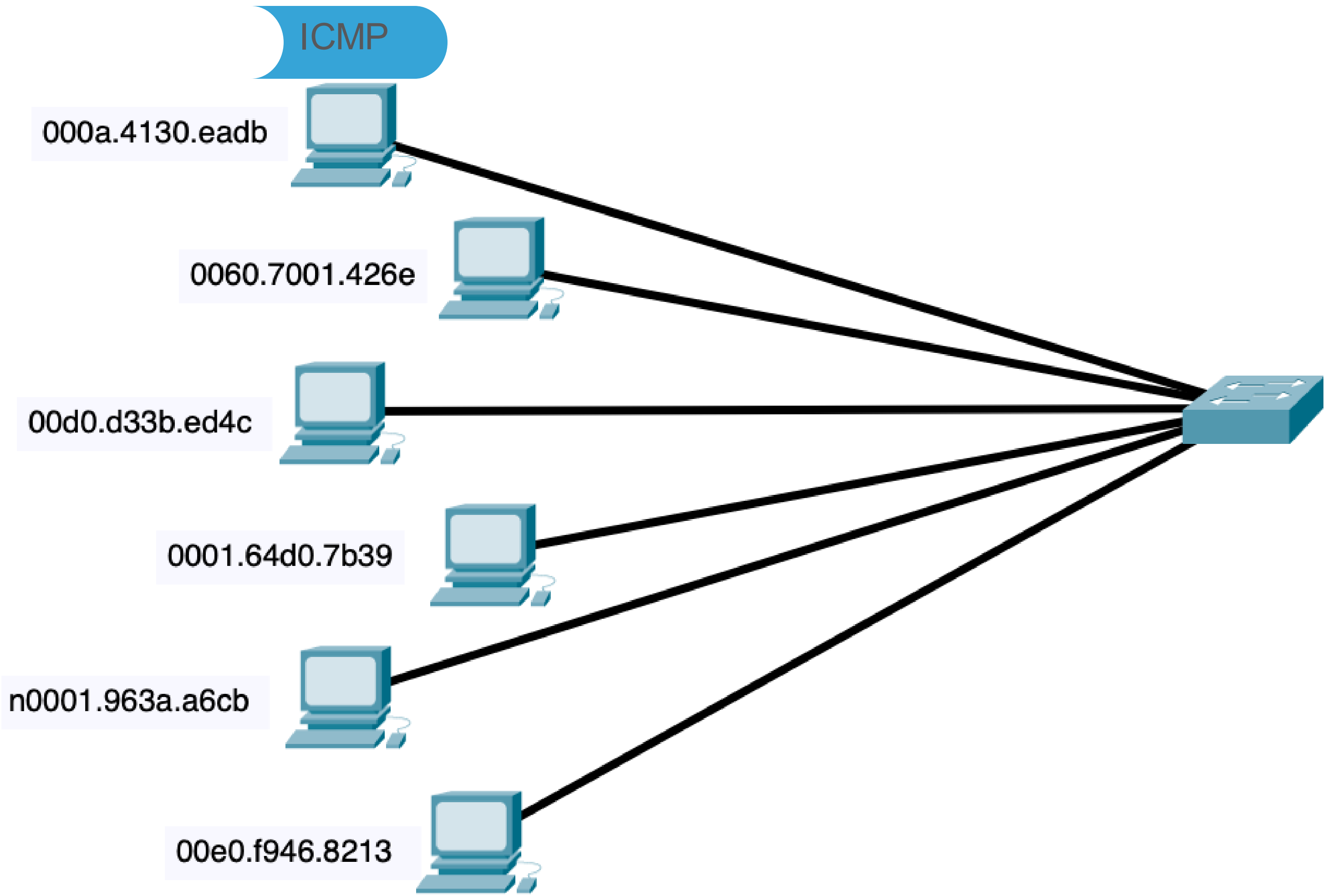
- Last 24 bits (last 6 digits).
- Assigned by the manufacturer, like a serial number.
- Ensures each specific NIC has a unique MAC address.

MAC Address Table

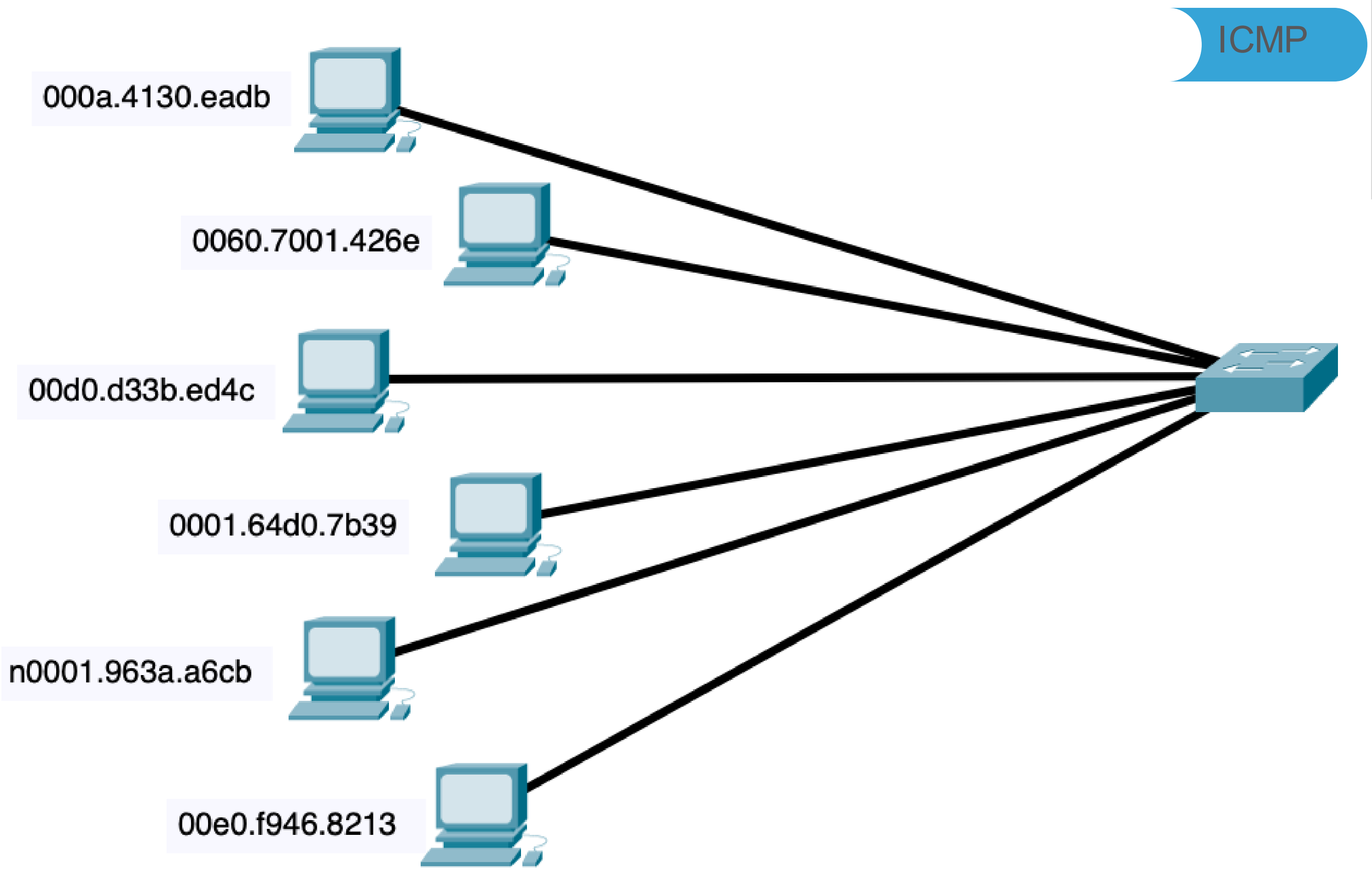
Switch Learning and Forwarding Frames



Layer 2 Destination Mac	Layer 2 Source Mac	Layer 3 Destination IP	Layer 3 Source IP	Layer 4-5-6-7
0001.963a.a6cb	000a.4130.ead	192.168.1.105	192.168.1.101	ICMP



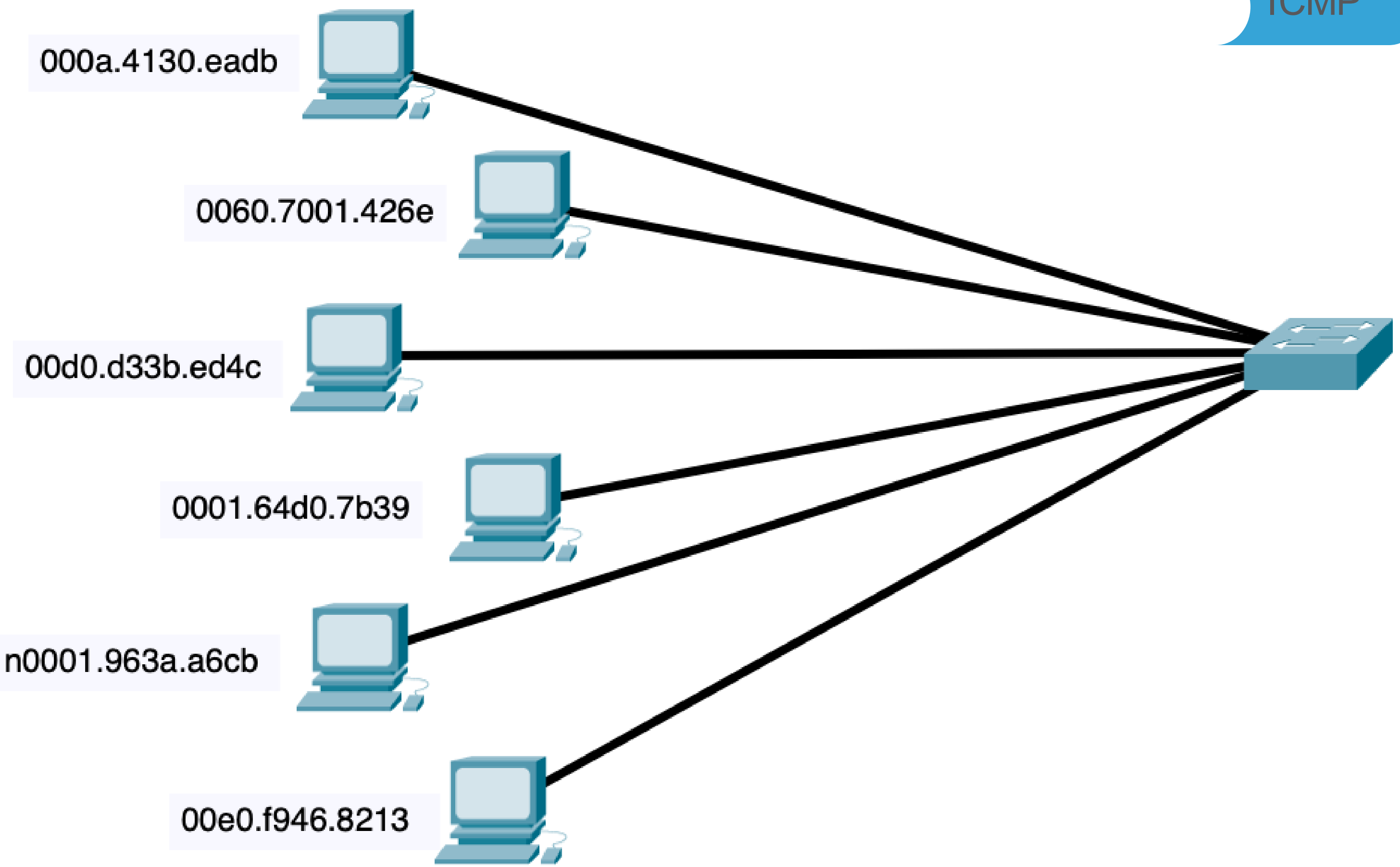
Layer 2 Destination Mac	Layer 2 Source Mac	Layer 3 Destination IP	Layer 3 Source IP	Layer 4-5-6-7
0001.963a.a6cb	000a.4130.eadb	192.168.1.105	192.168.1.101	ICMP



Switch#show mac address-table

Mac Address	Type	Ports
000a.4130.eadb	DYNAMIC	Fa0/1
0060.7001.426e	DYNAMIC	Fa0/2
00d0.d33b.ed4c	DYNAMIC	Fa0/3
0001.64d0.7b39	DYNAMIC	Fa0/4
0001.963a.a6cb	DYNAMIC	Fa0/5
00e0.f946.8213	DYNAMIC	Fa0/6

Layer 2 Destination Mac	Layer 2 Source Mac	Layer 3 Destination IP	Layer 3 Source IP	Layer 4-5-6-7
0001.963a.a6cb	000a.4130.eadb	192.168.1.105	192.168.1.101	ICMP



Switch#show mac address-table

Mac Address	Type	Ports
000a.4130.eadb	DYNAMIC	Fa0/1
0060.7001.426e	DYNAMIC	Fa0/2
00d0.d33b.ed4c	DYNAMIC	Fa0/3
0001.64d0.7b39	DYNAMIC	Fa0/4
0001.963a.a6cb	DYNAMIC	Fa0/5
00e0.f946.8213	DYNAMIC	Fa0/6

Layer 2 Destination Mac 0001.963a.a6cb	Layer 2 Source Mac 000a.4130.eadb	Layer 3 Destination IP 192.168.1.105	Layer 3 Source IP 192.168.1.101	Layer 4-5-6-7 ICMP

Two terms are associated with frames entering or leaving an interface:

- **Ingress** – entering the interface
- **Egress** – exiting the interface

A switch forwards based on the ingress interface and the destination MAC address.

A switch uses its MAC address table to make forwarding decisions.

Note: A switch will never allow traffic to be forwarded out the interface it received the traffic.

Switch#show mac address-table

Mac Address	Type	Ports
000a.4130.eadb	DYNAMIC	Fa0/1
0060.7001.426e	DYNAMIC	Fa0/2
00d0.d33b.ed4c	DYNAMIC	Fa0/3
0001.64d0.7b39	DYNAMIC	Fa0/4
0001.963a.a6cb	DYNAMIC	Fa0/5
00e0.f946.8213	DYNAMIC	Fa0/6

Layer 2 Destination Mac	Layer 2 Source Mac	Layer 3 Destination IP	Layer 3 Source IP	Layer 4-5-6-7
0001.963a.a6cb	000a.4130.eadb	192.168.1.105	192.168.1.101	ICMP

Two terms are associated with frames entering or leaving an interface:

- **Ingress** – entering the interface
- **Egress** – exiting the interface

A switch forwards based on the ingress interface and the destination MAC address.

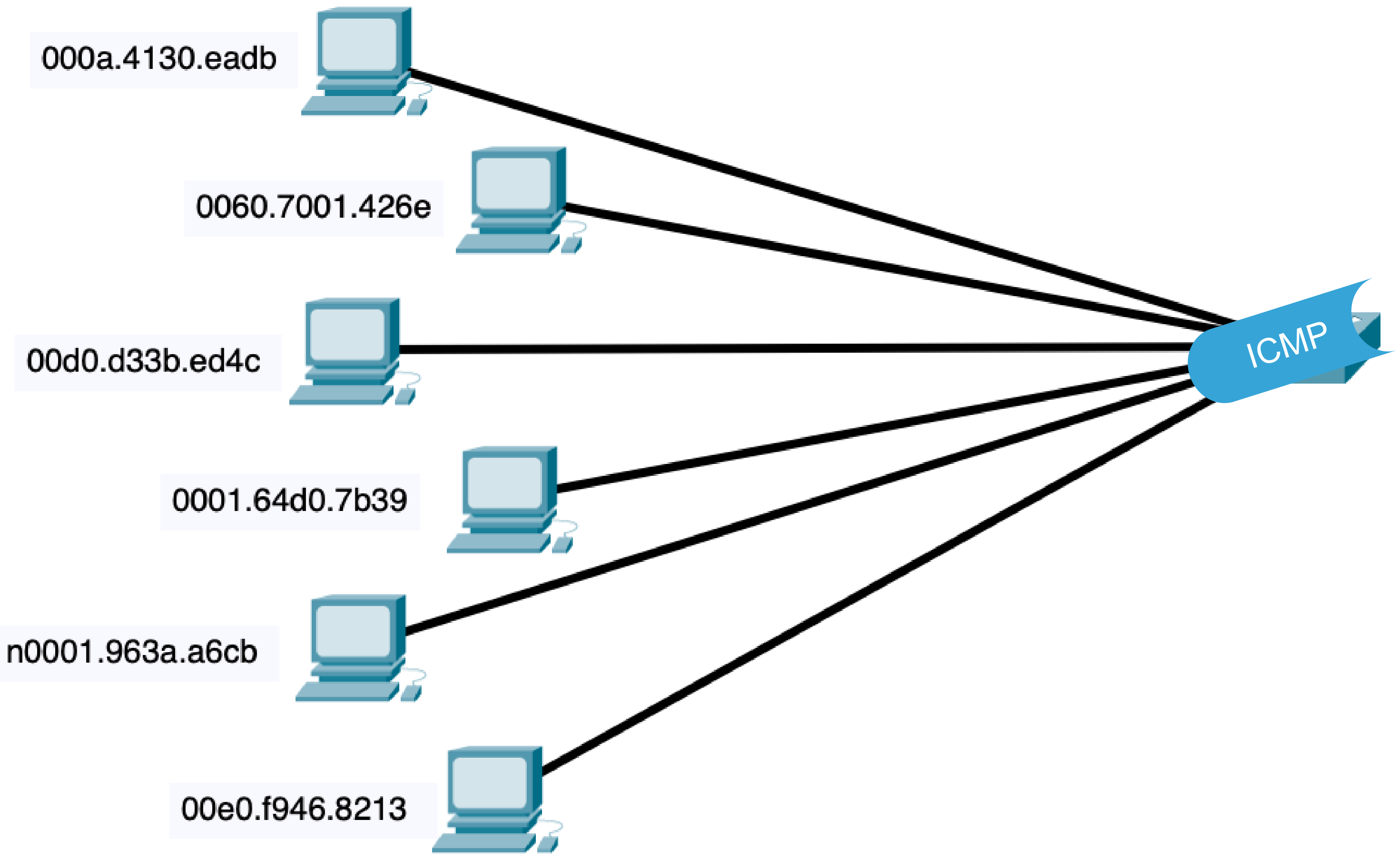
A switch uses its MAC address table to make forwarding decisions.

Note: A switch will never allow traffic to be forwarded out the interface it received the traffic.

Switch#show mac address-table

Mac Address	Type	Ports
000a.4130.eadb	DYNAMIC	Fa0/1
0060.7001.426e	DYNAMIC	Fa0/2
00d0.d33b.ed4c	DYNAMIC	Fa0/3
0001.64d0.7b39	DYNAMIC	Fa0/4
0001.963a.a6cb	DYNAMIC	Fa0/5
00e0.f946.8213	DYNAMIC	Fa0/6

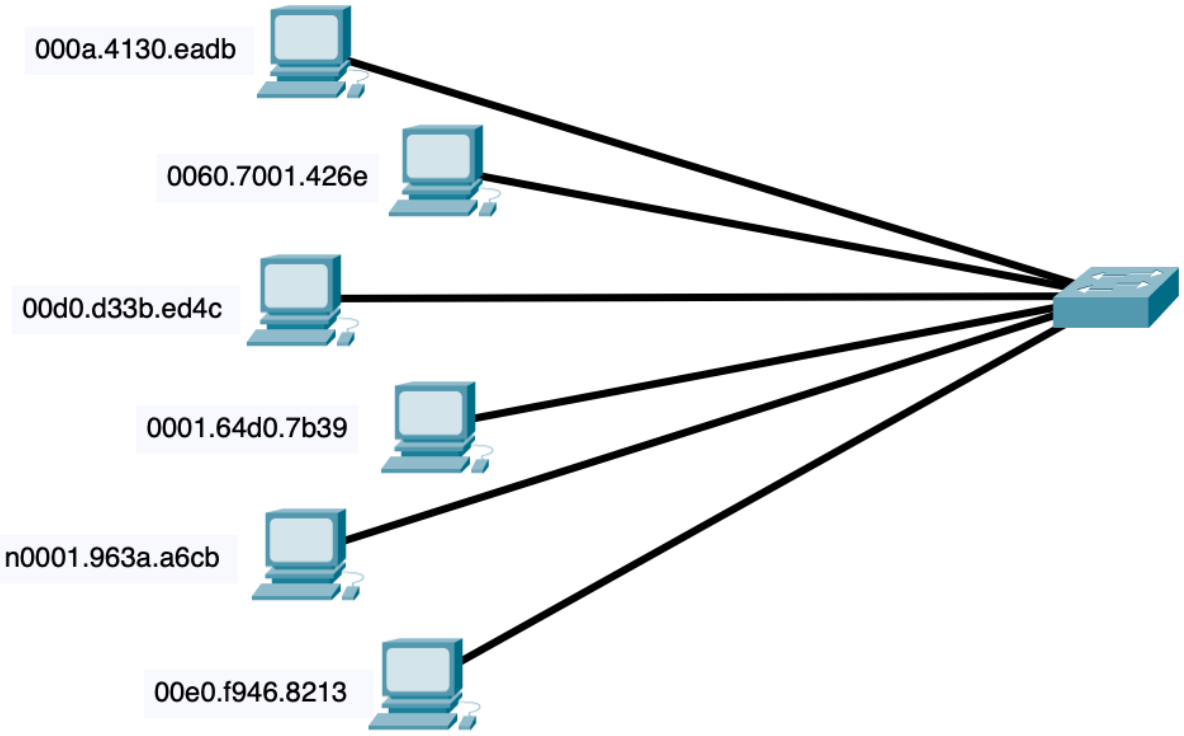
Layer 2 Destination Mac	Layer 2 Source Mac	Layer 3 Destination IP	Layer 3 Source IP	Layer 4-5-6-7
0001.963a.a6cb	000a.4130.eadb	192.168.1.105	192.168.1.101	ICMP



Switch#show mac address-table

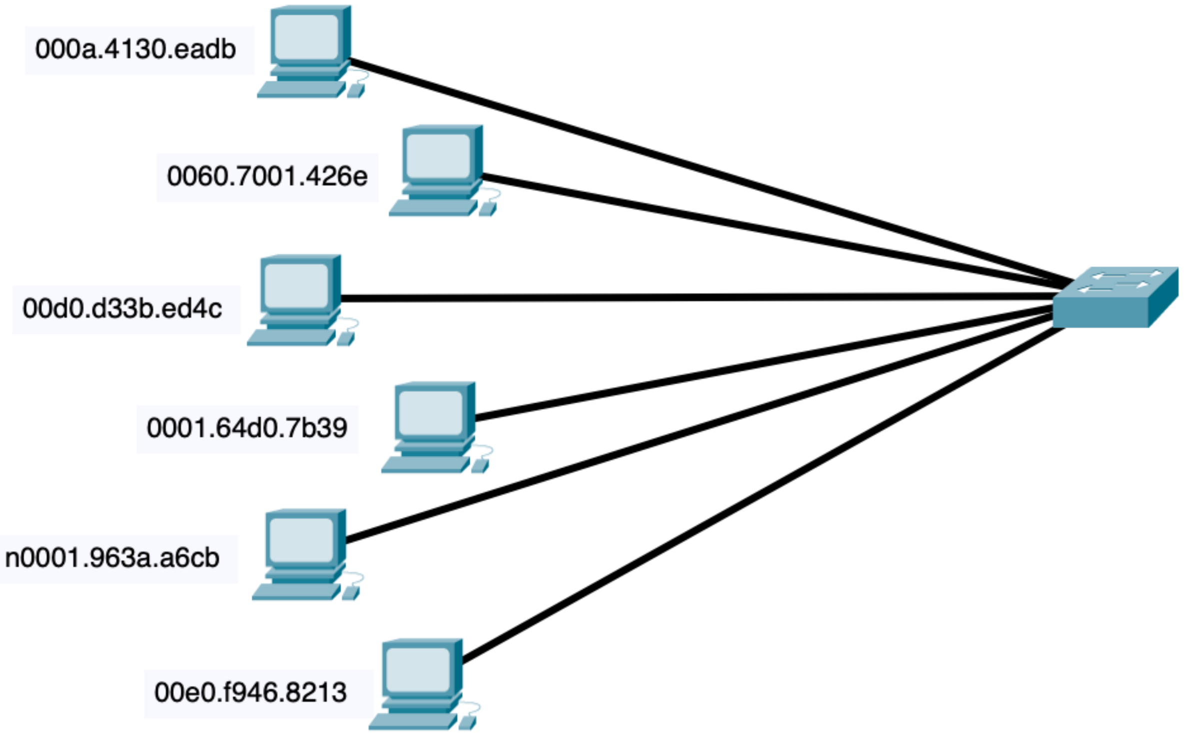
Mac Address	Type	Ports
000a.4130.eadb	DYNAMIC	Fa0/1
0060.7001.426e	DYNAMIC	Fa0/2
00d0.d33b.ed4c	DYNAMIC	Fa0/3
0001.64d0.7b39	DYNAMIC	Fa0/4
0001.963a.a6cb	DYNAMIC	Fa0/5
00e0.f946.8213	DYNAMIC	Fa0/6

Layer 2 Destination Mac	Layer 2 Source Mac	Layer 3 Destination IP	Layer 3 Source IP	Layer 4-5-6-7
0001.963a.a6cb	000a.4130.eadb	192.168.1.105	192.168.1.101	ICMP



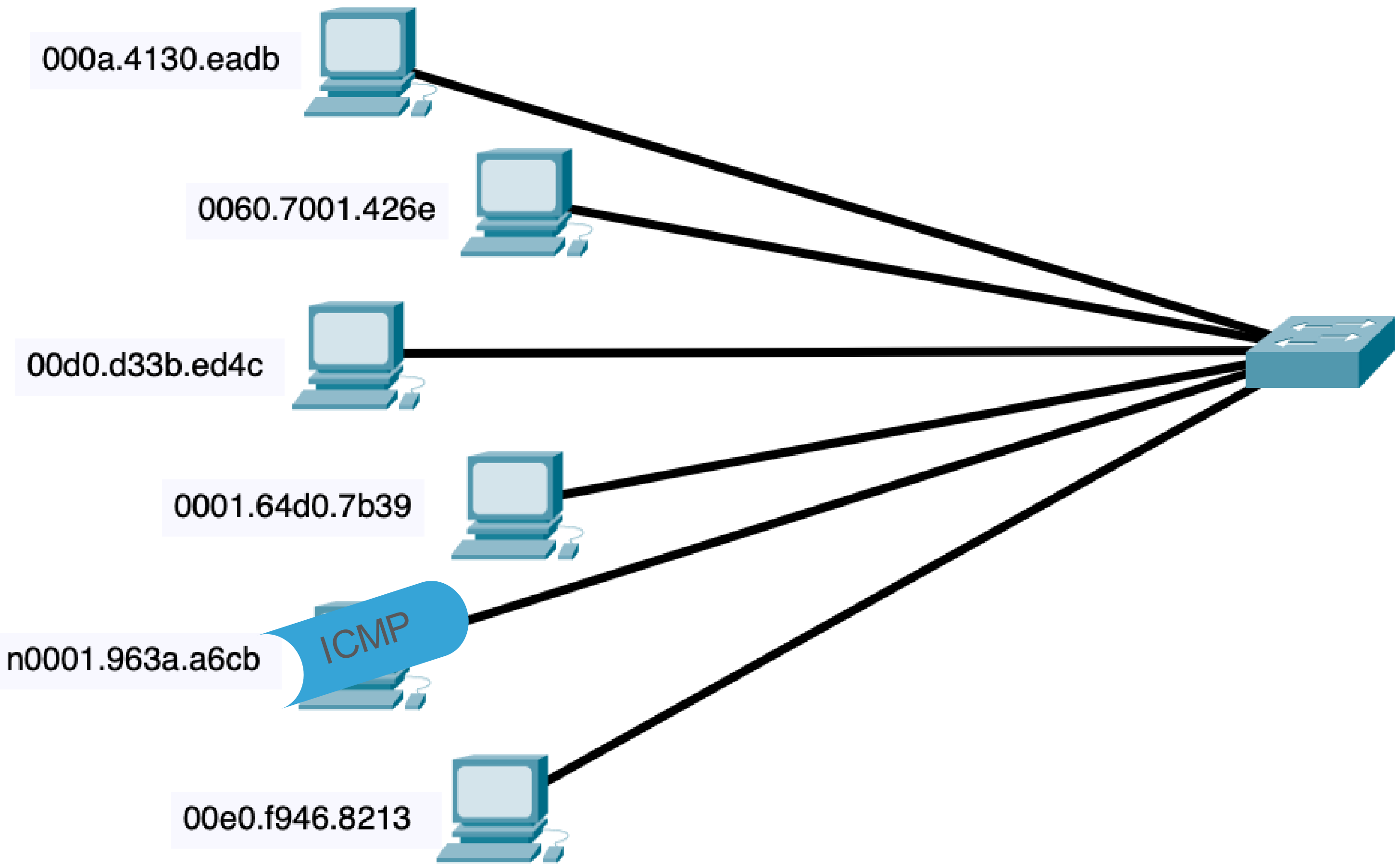
Layer 2 Destination Mac	Layer 2 Source Mac	Layer 3 Destination IP	Layer 3 Source IP	Layer 4-5-6-7
0001.963a.a6cb	0001.963a.a6cb	192.168.1.101	192.168.1.105	ICMP

Layer 2 Destination Mac 0001.963a.a6cb	Layer 2 Source Mac 000a.4130.eadb	Layer 3 Destination IP 192.168.1.105	Layer 3 Source IP 192.168.1.101	Layer 4-5-6-7 ICMP



Layer 2 Destination Mac 000a.4130.eadb	Layer 2 Source Mac 0001.963a.a6cb	Layer 3 Destination IP 192.168.1.101	Layer 3 Source IP 192.168.1.105	Layer 4-5-6-7 ICMP

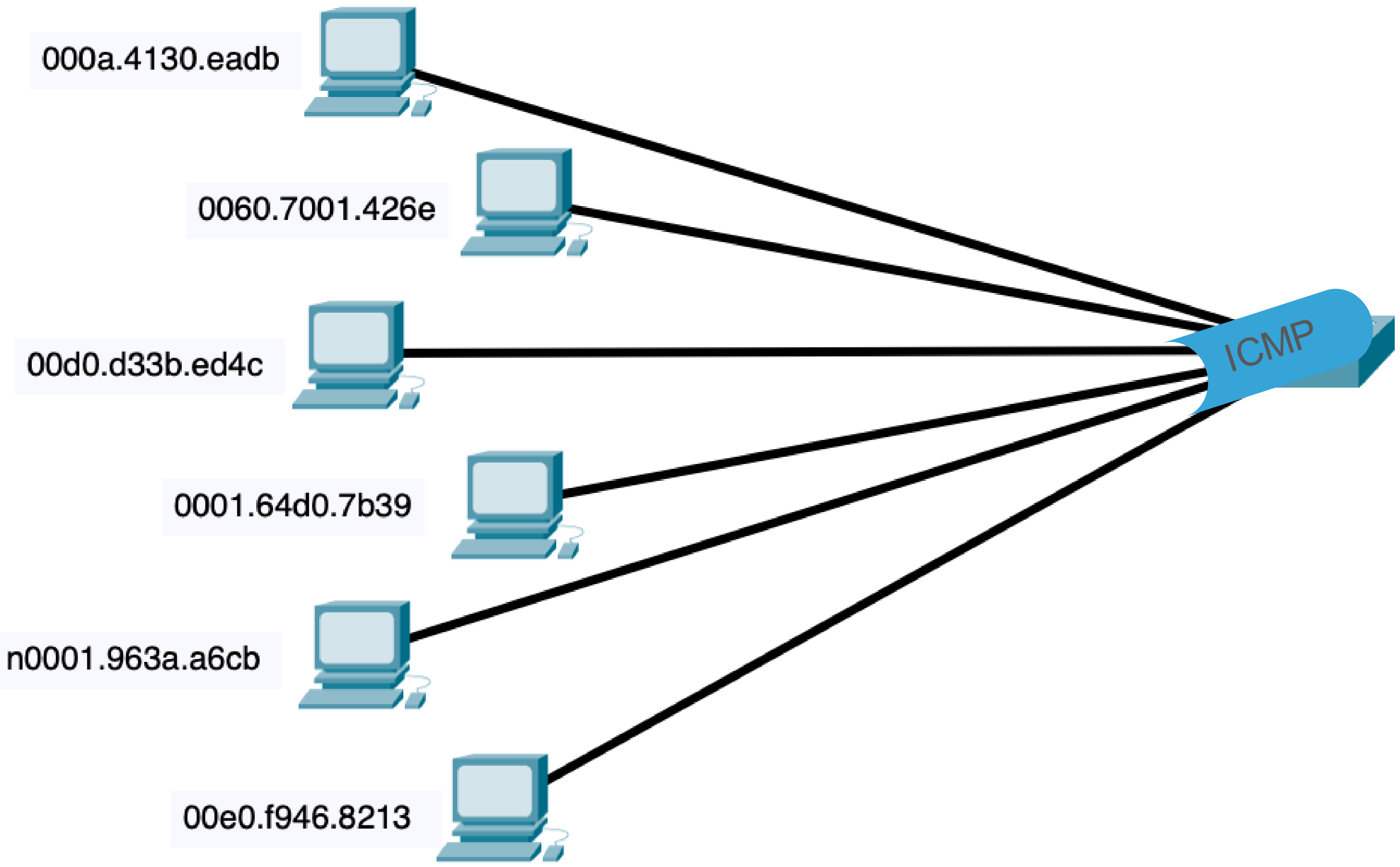
Layer 2 Source Mac	Layer 2 Destination Mac	Layer 3 Source IP	Layer 3 Destination IP	Layer 4-5-6-7
000a.4130.eadb	0001.963a.a6cb	192.168.1.101	192.168.1.105	ICMP



Switch#show mac address-table

Mac Address	Type	Ports
000a.4130.eadb	DYNAMIC	Fa0/1
0060.7001.426e	DYNAMIC	Fa0/2
00d0.d33b.ed4c	DYNAMIC	Fa0/3
0001.64d0.7b39	DYNAMIC	Fa0/4
0001.963a.a6cb	DYNAMIC	Fa0/5
00e0.f946.8213	DYNAMIC	Fa0/6

Layer 2 Source Mac	Layer 2 Destination Mac	Layer 3 Source IP	Layer 3 Destination IP	Layer 4-5-6-7
000a.4130.eadb	0001.963a.a6cb	192.168.1.101	192.168.1.105	ICMP



Switch#show mac address-table

Mac Address	Type	Ports
000a.4130.eadb	DYNAMIC	Fa0/1
0060.7001.426e	DYNAMIC	Fa0/2
00d0.d33b.ed4c	DYNAMIC	Fa0/3
0001.64d0.7b39	DYNAMIC	Fa0/4
0001.963a.a6cb	DYNAMIC	Fa0/5
00e0.f946.8213	DYNAMIC	Fa0/6

4.3 IPv4 Address

IPv4 Address

Unique 32-bit numeric address divided into four 8-bit octets.
A bit is a 1 or a 0

190.158.107.192

8 Bits 8 Bits 8 Bits 8 Bits

10101010.10101010.10101010.10101010

Number System

Decimal	Binary	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
							1

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
						2	1

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
					4	2	1

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
				8	4	2	1

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
			16	8	4	2	1

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
		32	16	8	4	2	1

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
	64	32	16	8	4	2	1

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

Lets convert a binary number to Decimal

10111011

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

10111011

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	0	1	1	1	0	1	1

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	0	1	1	1	0	1	1

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	0	1	1	1	0	1	1

The first bit is on so we need to add 128

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	0	1	1	1	0	1	1

128

Second bit is off so we don't need add anything

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	0	1	1	1	0	1	1

128

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	0	1	1	1	0	1	1

128
32

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	0	1	1	1	0	1	1

128
32

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	0	1	1	1	0	1	1

128
32
16

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	0	1	1	1	0	1	1

128
32
16

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	0	1	1	1	0	1	1

128
32
16
8

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	0	1	1	1	0	1	1

128
32
16
8

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	0	1	1	1	0	1	1

128
32
16
8

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	0	1	1	1	0	1	1

128
32
16
8
2

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	0	1	1	1	0	1	1

128
32
16
8
2

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	0	1	1	1	0	1	1

128
32
16
8
2
1

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	0	1	1	1	0	1	1

$$\begin{array}{r} 128 \\ 32 \\ 16 \\ 8 \\ 2 \\ \underline{1} \\ 187 \end{array}$$

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

These two numbers are the same **10111011** is **187**

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

00110011

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
0	0	1	1	0	0	1	1

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
0	0	1	1	0	0	1	1

32

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
0	0	1	1	0	0	1	1

32
16

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
0	0	1	1	0	0	1	1

32
16
2

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
0	0	1	1	0	0	1	1

32
16
2
1

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
0	0	1	1	0	0	1	1

$$\begin{array}{r} 32 \\ 16 \\ 2 \\ \underline{1} \\ 51 \end{array}$$

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

Lets convert a Decimal number to Binary

242

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

242
-128

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1							

242
-128
114

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1							

242
-128
114

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	1						

242
-128
114
-64

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	1						

242
-128
114
-64
50

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	1	1					

242
-128
114
64
50
-32

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	1	1					

242
-128
114
-64
50
-32

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	1	1					

$$\begin{array}{r} 242 \\ \underline{-128} \\ 114 \\ \underline{-64} \\ 50 \\ \underline{-32} \\ 18 \end{array}$$

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	1	1	1				

242
-128
114
-64
50
-32
18
-16

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	1	1	1				

242
-128
114
-64
50
-32
18
-16
2

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	1	1	1	0			

242
-128
114
-64
50
-32
18
-16
2

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	1	1	1	0	0		

242
-128
114
-64
50
-32
18
-16
2

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	1	1	1	0	0	1	

242
<u>-128</u>
114
<u>-64</u>
50
<u>-32</u>
18
<u>-16</u>
2
<u>-2</u>

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	1	1	1	0	0	1	0

242
<u>-128</u>
114
<u>64</u>
50
<u>32</u>
18
<u>16</u>
2
<u>2</u>
0

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	1	1	1	0	0	1	0

Decimal number 242 is the same as binary
11110010

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

Lets convert a Decimal
number to Binary

250

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	1	1	1	1	0	1	0

Lets convert a Decimal number to Binary

250

128
64
32
16
8
2
___
250

Converting Decimal numbers to Binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

Lets convert a Decimal number to Binary

63

$$
\begin{array}{r}
63 \\
\underline{-32} \\
31 \\
\underline{-16} \\
15 \\
\underline{-8} \\
7 \\
\underline{-6} \\
5 \\
\underline{-4} \\
3 \\
\underline{-2} \\
1 \\
\underline{-1} \\
0
\end{array}
$$

4.3.4 Parts of a subnet mask

1. **Find the IP address, Subnet mask, and Default gateway of the PC you are using. ipconfig**
2. **Convert all the numbers from Decimal to Binary (be carefull and line the numbers up**

IPv4 Address….. : 10.3.68.11

Subnet Mask….. : 255.255.254.0

Default Gateway : 10.3.68.250

4.3.4 Parts of a subnet mask

1. **Find the IP address, Subnet mask, and Default gateway of the PC you are using. ipconfig**
2. **Convert all the numbers from Decimal to Binary (be careful and line the numbers up**

IPv4 Address….. : 10.3.68.11 00001010.00000011.01000100.00001011

Subnet Mask….. : 255.255.254.0 11111111.11111111.11111110.00000000

Default Gateway : 10.3.68.250 00001010.00000011.01000100.11111010

4.3.4 Parts of a subnet mask

1. **Find the IP address, Subnet mask, and Default gateway of the PC you are using. ipconfig**
2. **Convert all the numbers from Decimal to Binary (be careful and line the numbers up**

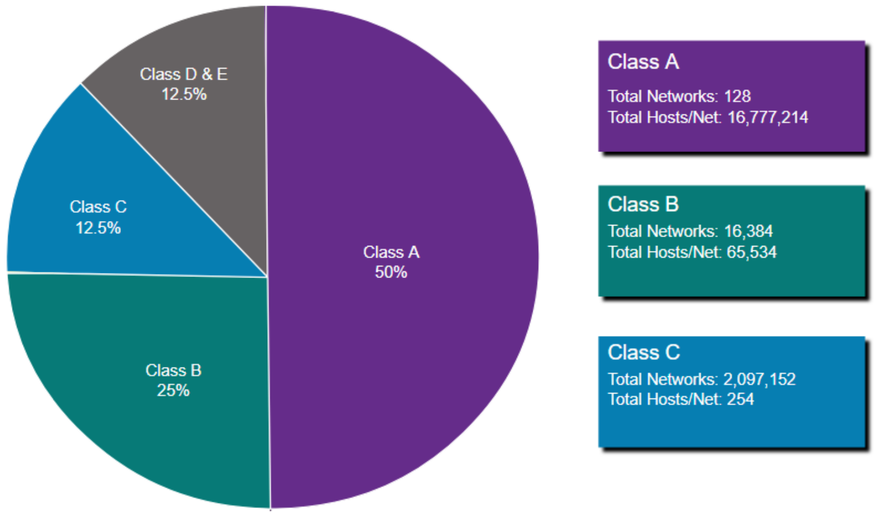
		Network Portion	Host Portion
IPv4 Address….. :	10.3.68.11	00001010.00000011.0100010	0.00001011
Subnet Mask….. :	255.255.254.0	11111111.11111111.1111111	0.00000000
Default Gateway :	10.3.68.250	00001010.00000011.0100010	0.11111010

4.3.6 Legacy Classful Addressing

RFC 790 (1981) allocated IPv4 addresses in classes

- Class A (0.0.0.0/8 to 127.0.0.0/8)
- Class B (128.0.0.0 /16 – 191.255.0.0 /16)
- Class C (192.0.0.0 /24 – 223.255.255.0 /24)
- Class D (224.0.0.0 to 239.0.0.0)
- Class E (240.0.0.0 – 255.0.0.0)

- Classful addressing wasted many IPv4 addresses.



Classful address allocation was replaced with classless addressing which ignores the rules of classes (A, B, C).

4.3.2 Public and Private IPv4 Addresses

- As defined in in RFC 1918, public IPv4 addresses are globally routed between internet service provider (ISP) routers.

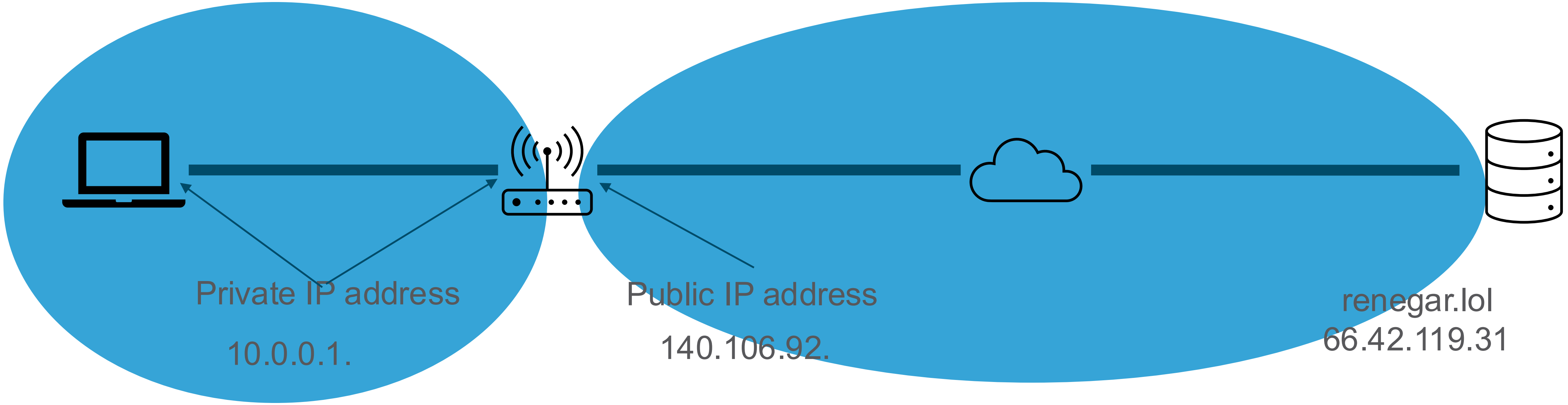
- Private addresses are common blocks of addresses used by most organizations to assign IPv4 addresses to internal hosts.

- Private IPv4 addresses are not unique and can be used internally within any network.

Network Address and Prefix	RFC 1918 Private Address Range
10.0.0.0/8	10.0.0.0 - 10.255.255.255
172.16.0.0/12	172.16.0.0 - 172.31.255.255
192.168.0.0/16	192.168.0.0 - 192.168.255.255

- However, private addresses are not globally routable.

Network Address Translation (NAT)



- Find your Private IP address (ipconfig, ifconfig)
- Go to **renegar.lol/ipaddress** show your public ip address

4.4 IPv6 Address

IPv6 Addressing Formats

- IPv6 addresses are 128 bits in length and written in hexadecimal.
- IPv6 addresses are not case-sensitive and can be written in either lowercase or uppercase.
- The preferred format for writing an IPv6 address is x:x:x:x:x:x:x:x, with each "x" consisting of four hexadecimal values.
- In IPv6, a hextet is the unofficial term used to refer to a segment of 16 bits, or four hexadecimal values.
- Examples of IPv6 addresses in the preferred format:

```
2001:0db8:0000:1111:0000:0000:0000:0200
2001:0db8:0000:00a3:abcd:0000:0000:1234
```

IPv6 Address Representation Rule 1 – Omit Leading Zero

- The first rule to help reduce the notation of IPv6 addresses is to omit any leading 0s (zeros).
- **Examples:**
  - 01ab can be represented as 1ab
  - 09f0 can be represented as 9f0
  - 0a00 can be represented as a00
  - 00ab can be represented as ab

- **Note**: This rule only applies to leading 0s, NOT to trailing 0s, otherwise the address would be ambiguous.

Type	Format
Preferred	2001 : **0**db8 : **000**0 : 1111 : **000**0 : **000**0 : **000**0 : **0**200
No leading zeros	2001 : db8 : 0 : 1111 : 0 : 0 : 0 : 200

IPv6 Address Representation Rule 2 – Double Colon

- A double colon (::) can replace any single, contiguous string of one or more 16-bit hextets consisting of all zeros.
- **Example:**
  - 2001:db8:cafe:1:0:0:0:1 (leading 0s omitted) could be represented as 2001:db8:cafe:1::1

- **Note**: The double colon (::) can only be used once within an address, otherwise there would be more than one possible resulting address.

Type	Format
Preferred	2001 : **0**db8 : **0000** : 1111 : **0000** : **0000** : **0000** : **0**200
Compressed	2001:db8:0:1111::200

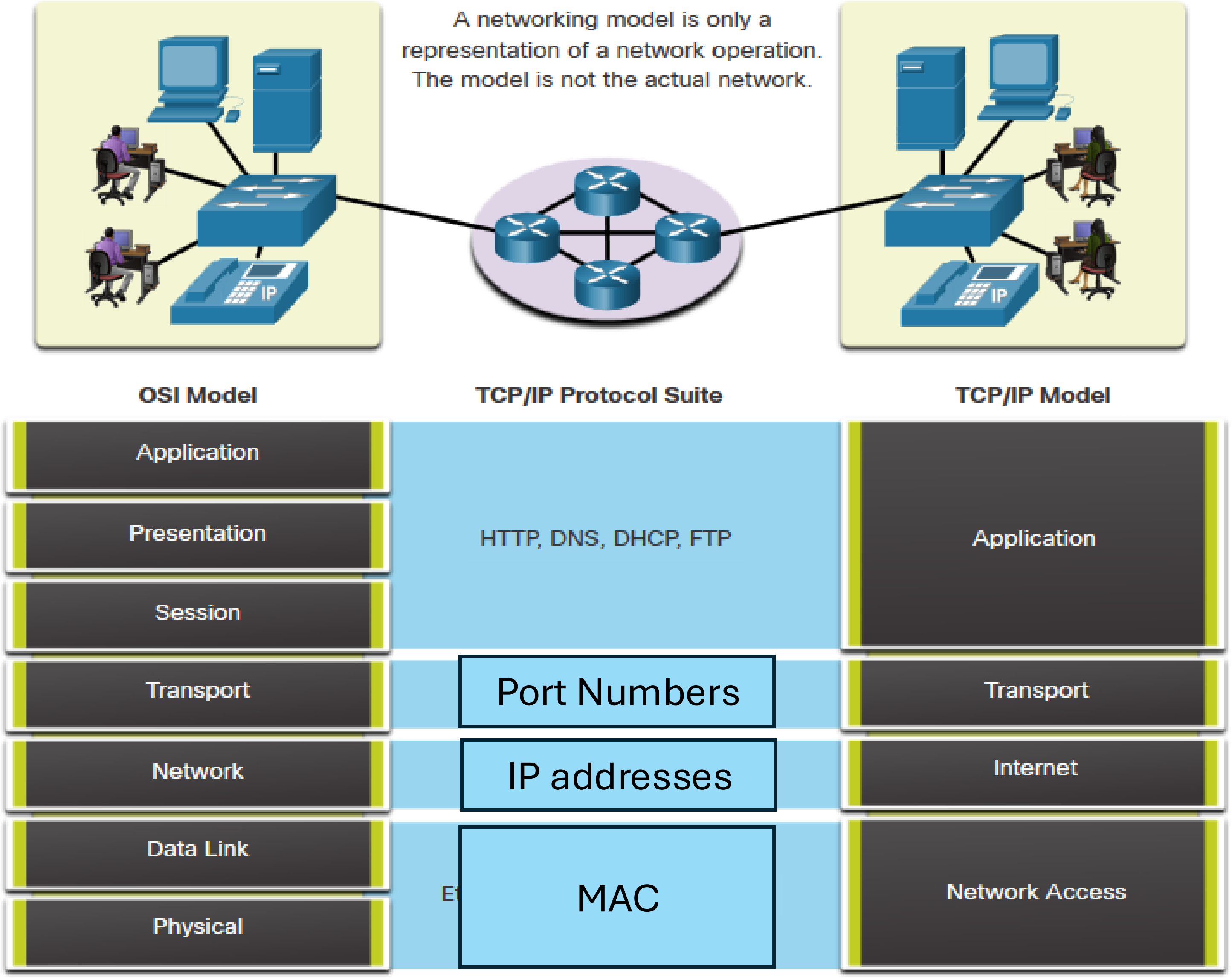
4.4 IPv6 format

- The ***network component*** is an IPv6 address's first 64 bits. A network component is used for routing and consists of two parts:
  - The ***prefix length***, also named ***prefix***, is the first 48 bits of the network component. A prefix describes the public topology.
  - The ***subnet ID*** is the last 16 bits of the network component. A subnet ID describes the private topology. The private topology is also called the site topology.

network component	subnet ID	
2001:0db8:0000:1111	:0000:0000:0000:0200	/64
2001:0db8:0000:00a3	:abcd:0000:0000:1234	/64

Table 4.4.1: IPv4 and IPv6 differences.

Feature	IPv4	IPv6
Subnet mask	Yes	No, uses prefix length
Uses classful addressing	Yes	No
Supports unicast address	Yes	Yes
Supports multicast address	Yes	Yes
Supports anycast address	No	Yes
Supports broadcast address	Yes	No
Address length size	32 bits	128 bits

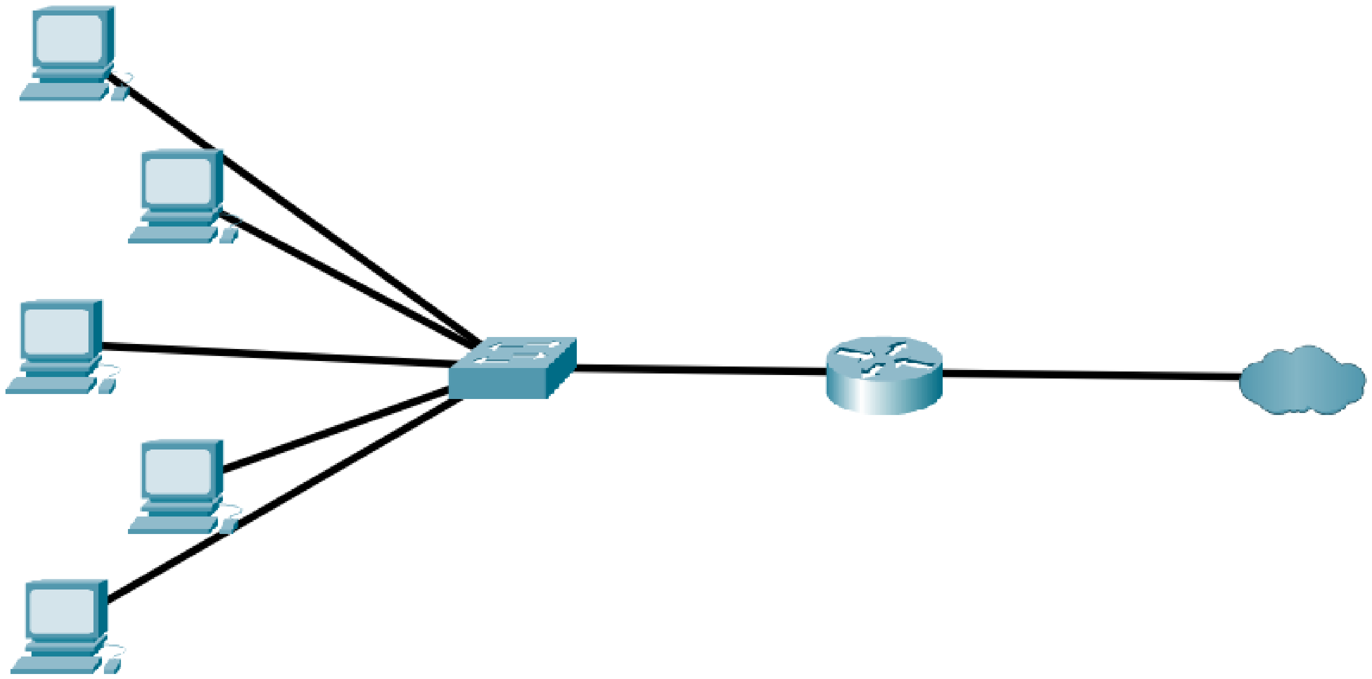

A networking model is only a
representation of a network operation.
The model is not the actual network.
IP
IP
OSI Model
TCP/IP Protocol Suite
TCP/IP Model
Application
Presentation
Session
Transport
Network
Data Link
Physical
HTTP, DNS, DHCP, FTP
Port Numbers
IP addresses
MAC
Application
Transport
Internet
Network Access

Chapter 4: Address Types

Chapter 5: Segmentation

5.1 Network Segmentation

Process of dividing a single network into a physical or logical network subset

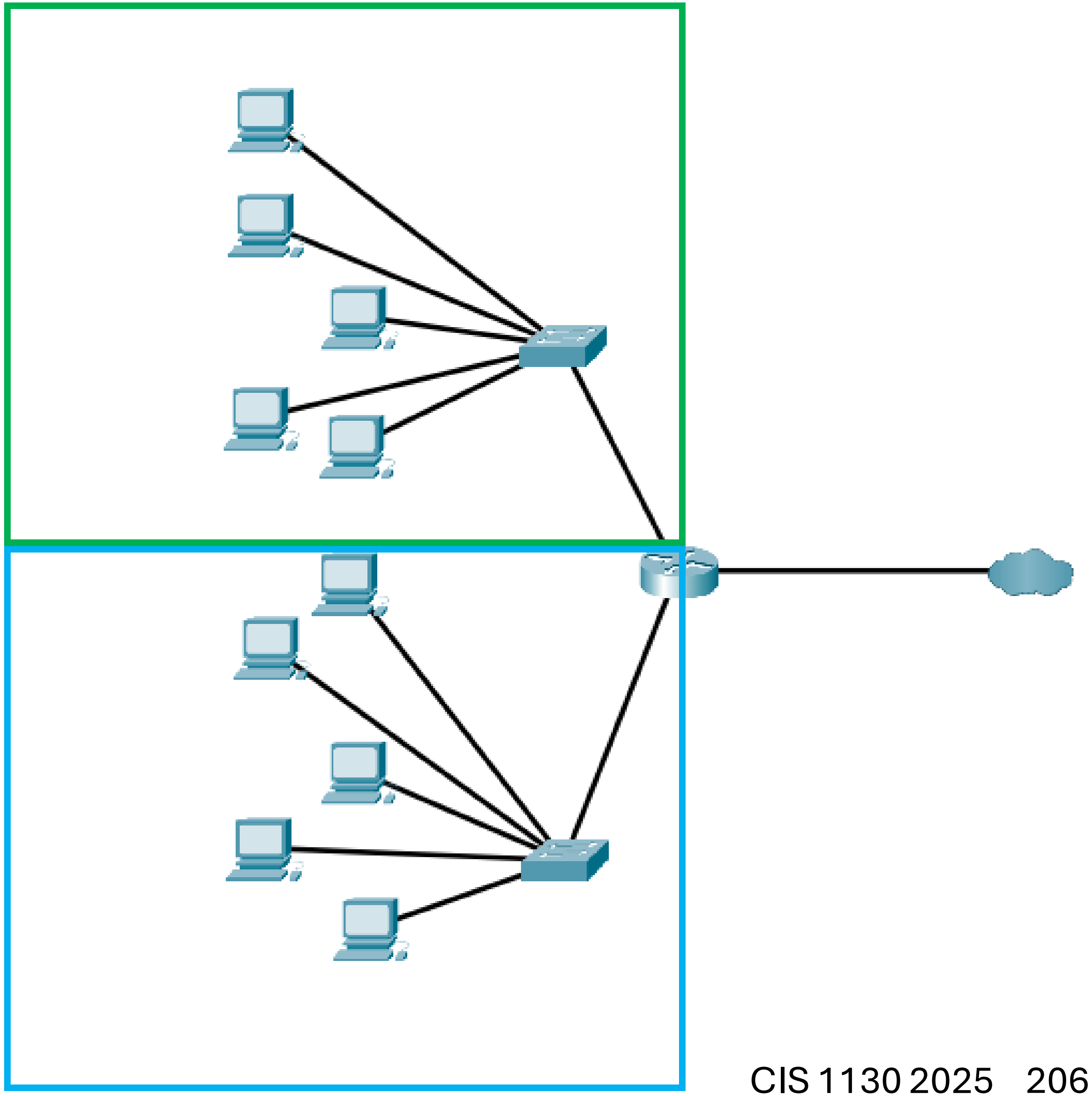


5.1 Network Segmentation

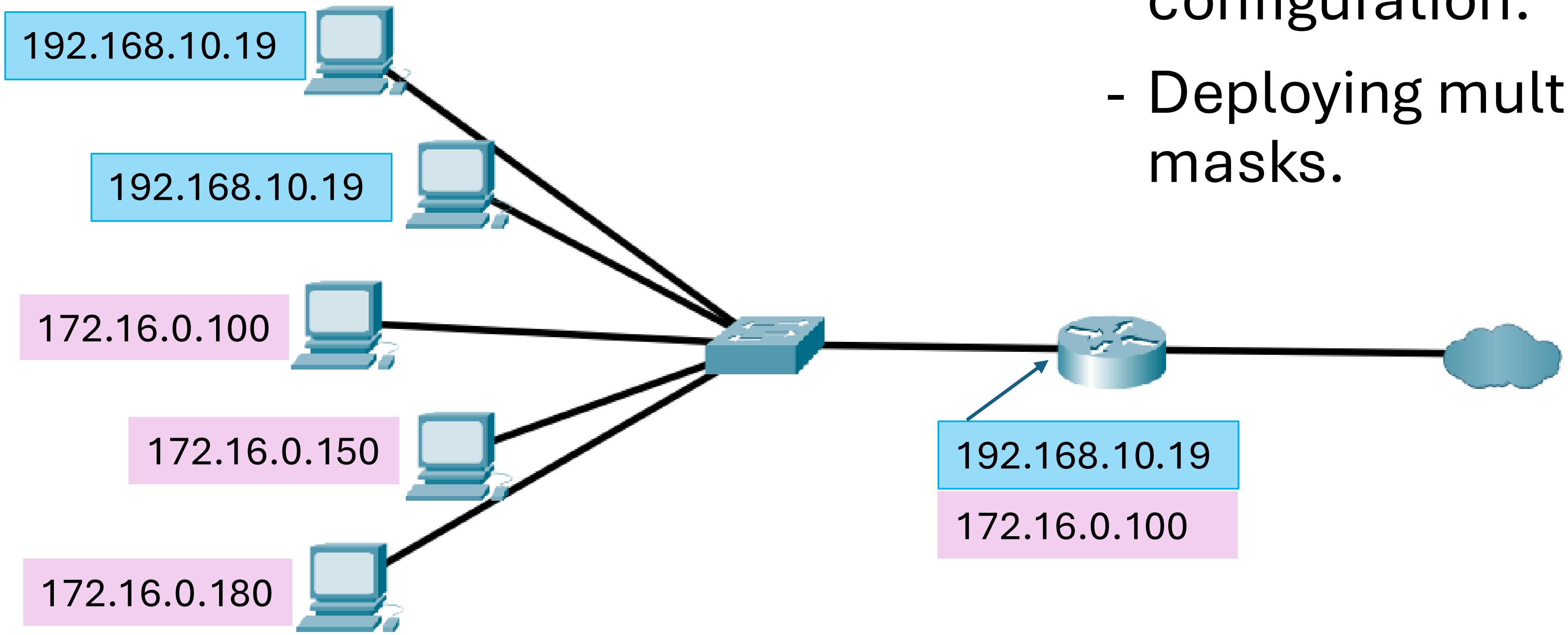
Physical segmentation

- Segments a network with a networking device or hardware.

- Deployment of multiple switches or a firewall.



5.1 Network Segmentation



Logical segmentation

- segments a network with a configuration.
- Deploying multiple subnet masks.

5.2 Binary Decimal Conversion

5.2 Decimal Conversion

1. **Find the IP address, Subnet mask of the PC you are using. ipconfig**
2. **Convert all the numbers from Decimal to Binary (be careful and line the numbers up**

IP Address:	10.3.68.50	00001010.00000011.01000100.00110010
Subnet Mask:	255.255.254.0	11111111.11111111.11111110.00000000

1 and 0 = 0

1 and 1 = 1

0 and 1 = 0

5.2 Decimal Conversion

1. **Find the IP address, Subnet mask of the PC you are using. ipconfig**
2. **Convert all the numbers from Decimal to Binary (be careful and line the numbers up**

IP Address:	10.3.68.50	00001010.00000011.01000100.00110010
Subnet Mask:	255.255.254.0	11111111.11111111.11111110.00000000
		0

1 and 0 = 0

1 and 1 = 1

0 and 1 = 0

5.2 Decimal Conversion

1. **Find the IP address, Subnet mask of the PC you are using. ipconfig**
2. **Convert all the numbers from Decimal to Binary (be careful and line the numbers up**

IP Address:	10.3.68.50	00001010.00000011.01000100.00110010
Subnet Mask:	255.255.254.0	11111111.11111111.11111110.00000000
		00

1 and 0 = 0

1 and 1 = 1

0 and 1 = 0

5.2 Decimal Conversion

1. **Find the IP address, Subnet mask of the PC you are using. ipconfig**
2. **Convert all the numbers from Decimal to Binary (be careful and line the numbers up**

IP Address:	10.3.68.50	00001010.00000011.01000100.00110010
Subnet Mask:	255.255.254.0	11111111.11111111.11111110.00000000
		000

1 and 0 = 0

1 and 1 = 1

0 and 1 = 0

5.2 Decimal Conversion

1. **Find the IP address, Subnet mask of the PC you are using. ipconfig**
2. **Convert all the numbers from Decimal to Binary (be careful and line the numbers up**

IP Address:	10.3.68.50	00001010.00000011.01000100.00110010
Subnet Mask:	255.255.254.0	11111111.11111111.11111110.00000000
		0000

1 and 0 = 0

1 and 1 = 1

0 and 1 = 0

5.2 Decimal Conversion

1. **Find the IP address, Subnet mask of the PC you are using. ipconfig**
2. **Convert all the numbers from Decimal to Binary (be careful and line the numbers up**

IP Address:	10.3.68.50	00001010.00000011.01000100.00110010
Subnet Mask:	255.255.254.0	11111111.11111111.11111110.00000000
		00001

1 and 0 = 0

1 and 1 = 1

0 and 1 = 0

5.2 Decimal Conversion

1. **Find the IP address, Subnet mask of the PC you are using. ipconfig**
2. **Convert all the numbers from Decimal to Binary (be careful and line the numbers up**

IP Address:	10.3.68.50	00001010.00000011.01000100.00110010
Subnet Mask:	255.255.254.0	11111111.11111111.11111110.00000000
		0000010

1 and 0 = 0

1 and 1 = 1

0 and 1 = 0

5.2 Decimal Conversion

1. **Find the IP address, Subnet mask of the PC you are using. ipconfig**
2. **Convert all the numbers from Decimal to Binary (be carefull and line the numbers up**

IP Address:	10.3.68.50	00001010.00000011.01000100.00110010
Subnet Mask:	255.255.254.0	11111111.11111111.11111110.00000000
		0000101

1 and 0 = 0

1 and 1 = 1

0 and 1 = 0

5.2 Decimal Conversion

1. **Find the IP address, Subnet mask of the PC you are using. ipconfig**
2. **Convert all the numbers from Decimal to Binary (be careful and line the numbers up**

IP Address:	10.3.68.50	00001010.00000011.01000100.00110010
Subnet Mask:	255.255.254.0	11111111.11111111.11111110.00000000
		00001010

1 and 0 = 0

1 and 1 = 1

0 and 1 = 0

5.2 Decimal Conversion

1. **Find the IP address, Subnet mask of the PC you are using. ipconfig**
2. **Convert all the numbers from Decimal to Binary (be careful and line the numbers up**

IP Address:	10.3.68.50	00001010.00000011.01000100.00110010
Subnet Mask:	255.255.254.0	11111111.11111111.11111110.00000000
		00001010.00000011.01000100.00000000

1 and 0 = 0

1 and 1 = 1

0 and 1 = 0

5.2 Decimal Conversion

1. **Find the IP address, Subnet mask of the PC you are using. ipconfig**
2. **Convert all the numbers from Decimal to Binary (be careful and line the numbers up**

IP Address:	10.3.68.50	00001010.00000011.01000100.00110010
Subnet Mask:	255.255.254.0	11111111.11111111.11111110.00000000
Network Address:	10.3.68.0	00001010.00000011.01000100.00000000

5.3 Network Address

- IPv4 address **AND** subnet mask = network address (network ID).
- Defines the host range and network segment.
- Network address = first address in a subnet.
- Subnets = smaller logical partitions of a network.

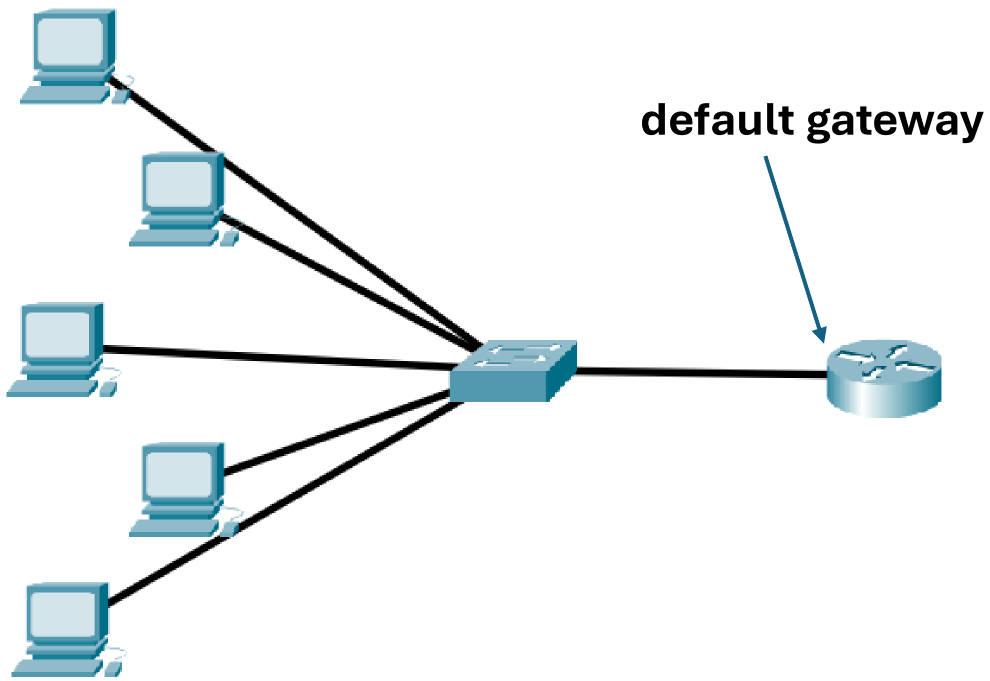
5.3 Network Address and Range

Subnet Mask:	255.255.254.0	11111111.11111111.11111110.00000000
Network Address:	10.3.68.0	00001010.00000011.01000100.00000000
First host Address:	10.3.68.1	00001010.00000011.01000100.00000001
Last host Address:	10.3.69.254	00001010.00000011.01000101.11111110
Broadcast Address:	10.3.69.255	00001010.00000011.01000101.11111111

Network Address:	Network Range:		Broadcast Address:
10.3.68.0	10.3.68.1	10.3.69.254	10.3.69.255

Network & Gateway Addresses

- Devices on different subnets can't talk directly.
- **Router** connects subnets.
- Router's local IP = **gateway (default gateway)** for subnet devices.
- Packet handling:
  - Same subnet → send locally.
  - Different subnet → send to gateway.



5.4 Classless addresses

Classless Addressing (CIDR)

- **Classless Addressing (CIDR)**
- Uses **Variable Length Subnet Mask (VLSM)**.
- Created to reduce IPv4 address shortage.
- Unlike classful (A, B, C), CIDR can allocate on any bit boundary

CIDR Notation

- IP address + “/” + number of network bits.
- Ex: 172.16.10.12/16.
- **Network segment** → routing between networks.
- **Host segment** → address allocation within subnet.

CIDER	Total # of Address	# OF Hosts	Netmask
/30	4	2	255.255.255.252
/29	8	6	255.255.255.248
/28	16	14	255.255.255.240
/27	32	30	255.255.255.224
/26	64	62	255.255.255.192
/25	128	126	255.255.255.128
/24	256	254	255.255.255.0
/23	512	510	255.255.254.0
/22	1024	1022	255.255.252.0
/21	2048	2046	255.255.248.0
/20	4096	4094	255.255.240.0
/19	8192	8190	255.255.224.0
/18	16384	16382	255.255.192.0
/17	32768	32766	255.255.128.0
/16	65536	65534	255.255.0.0

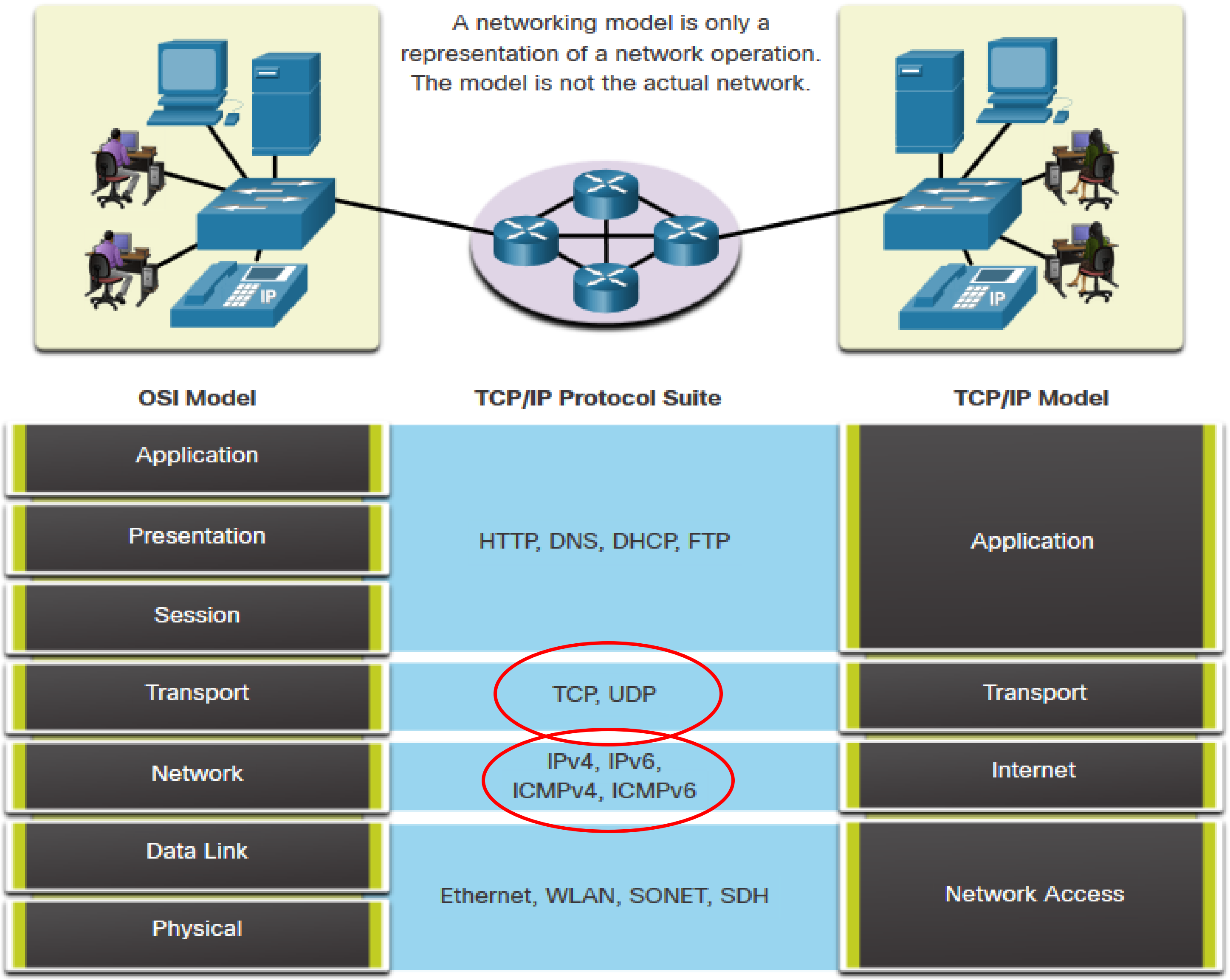
5.5 Subnetting Basics

Chapter 5: Segmentation

Chapter 6: Protocols

Protocol types

- IP
- TCP
- UDP
- TCP/IP



6.1 Protocol types

6.1 Protocol types

Protocol numbers

- Network layer (Layer 3, IP).
- Example: TCP = protocol number 6; UDP = protocol number 17.

Port numbers

- Used within UDP/TCP headers to represent application protocols/services.
- Example: HTTP = TCP port 80; DHCP = UDP ports 67 and 68.

IPv6

- Current internet protocol version.
- Provides addressing for routers to deliver packets to destination devices.

6.1 Protocol types

TCP (Transmission Control Protocol)

- Connection-oriented protocol.
- Ensures reliable transmission of data between devices.

UDP (User Datagram Protocol)

- Connectionless protocol.
- Transmits data between devices without reliability overhead.

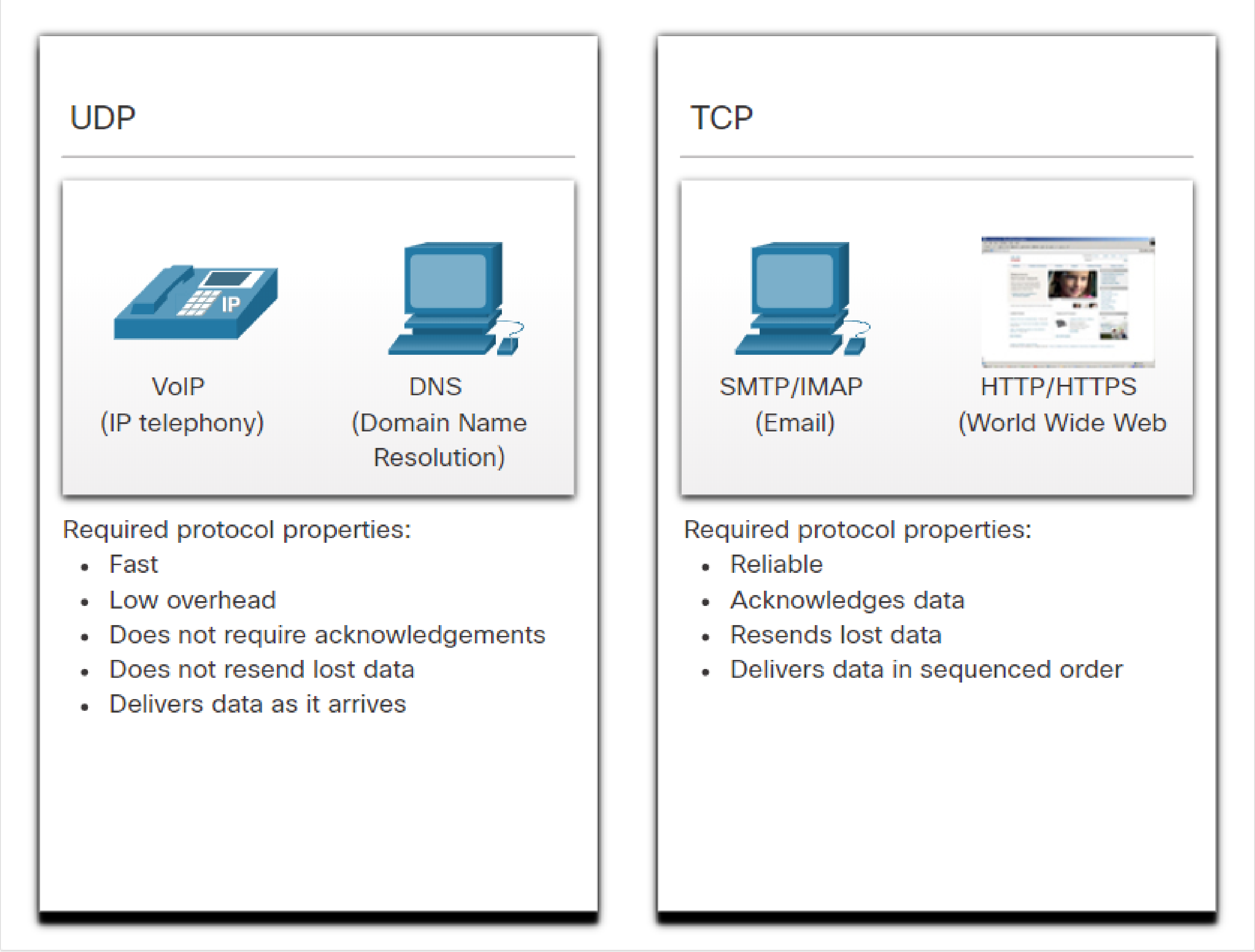
6.1 Protocol types

- **TCP/IP (Transmission Control Protocol/Internet Protocol)**
  - Core communication protocol suite for internet/intranet.
  - TCP: creates reliable connections, assembles messages into packets, reassembles at destination, verifies receipt.
  - IP: defines addressing and routing for packets.
  - Gateways use IP addressing to route data correctly.

Transportation of Data
The Right Transport Layer Protocol for the Right Application

- UDP is also used by request-and-reply applications where the data is minimal, and retransmission can be done quickly.

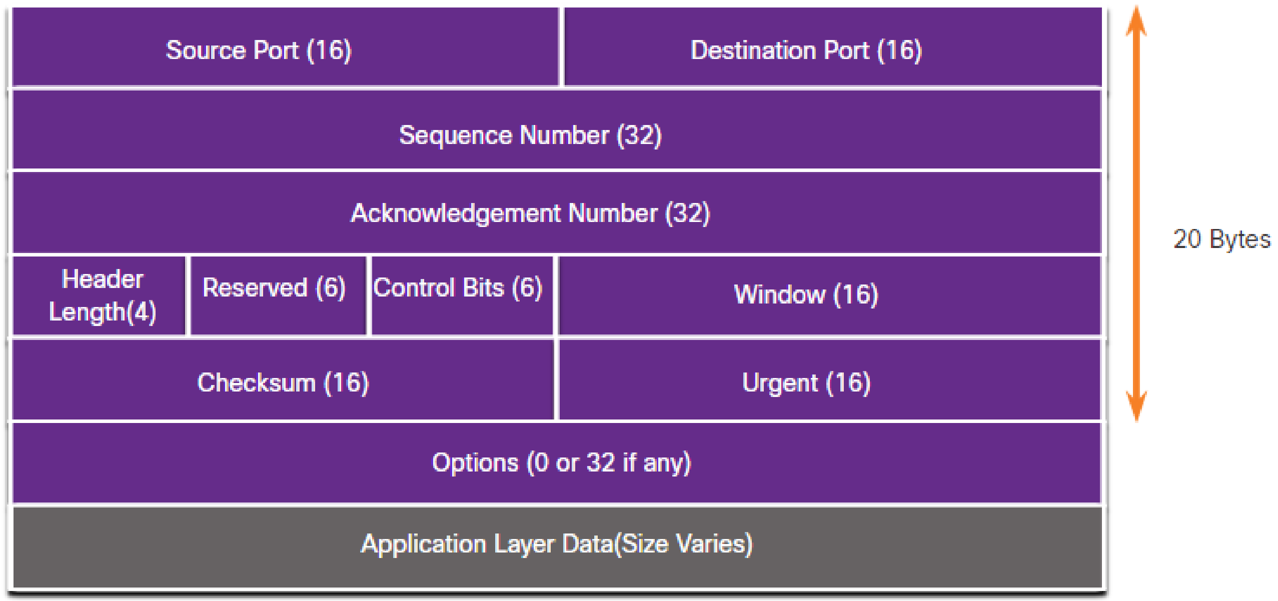
- If it is important that all the data arrives and that it can be processed in its proper sequence, TCP is used as the transport protocol.



TCP Overview
TCP Header

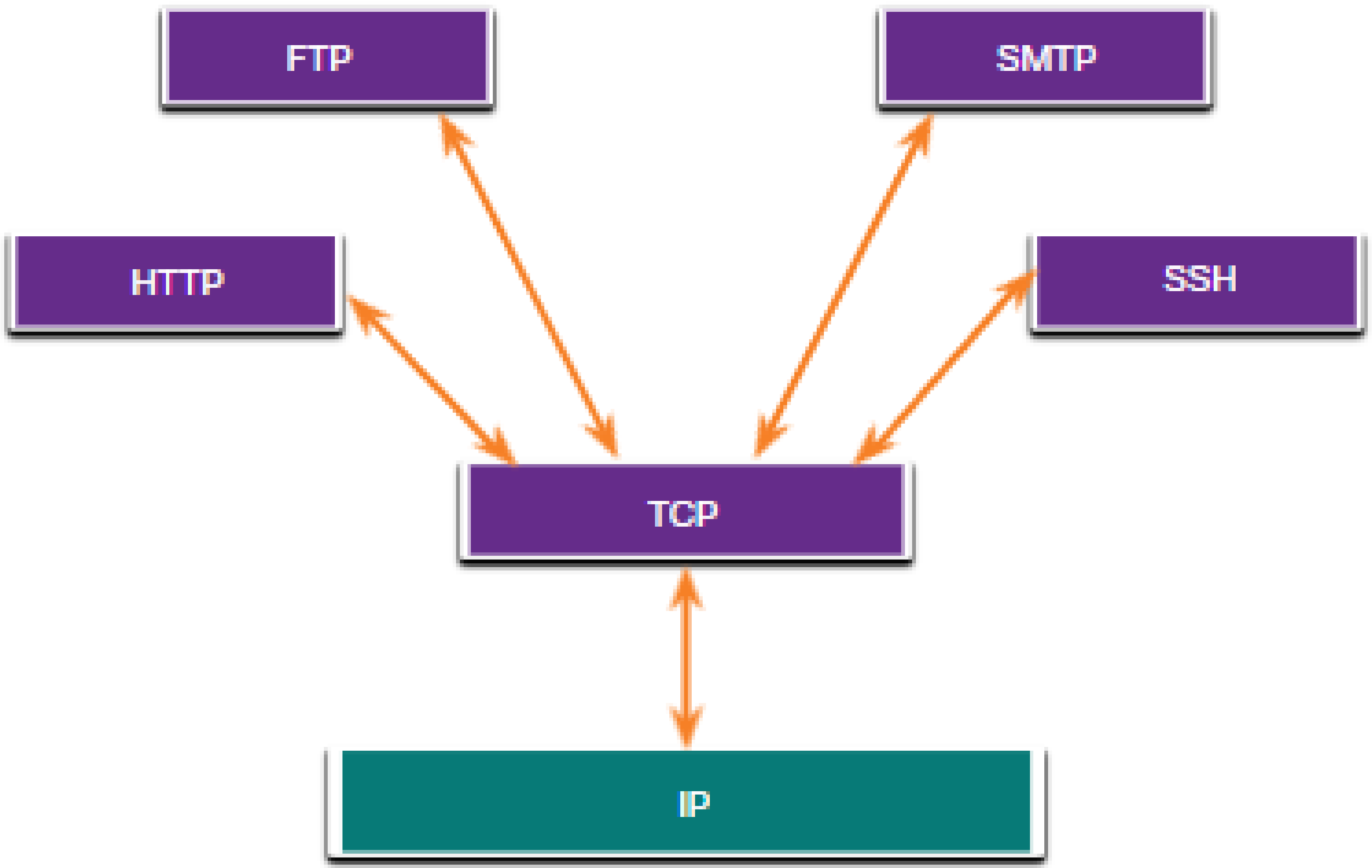
- TCP is a stateful protocol which means it keeps track of the state of the communication session.

- TCP records which information it has sent, and which information has been acknowledged.



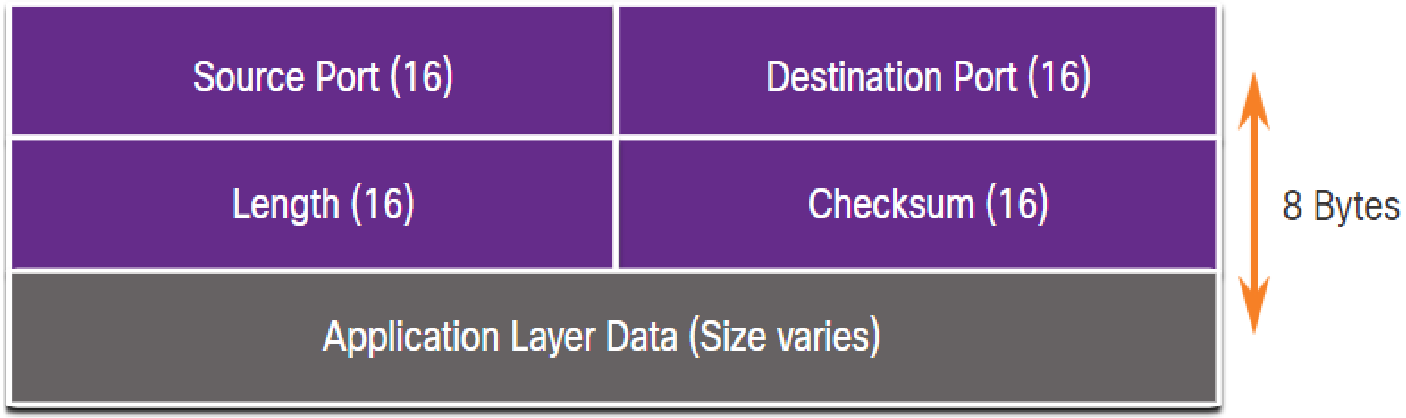
TCP Overview Applications that use TCP

TCP handles all tasks associated with dividing the data stream into segments, providing reliability, controlling data flow, and reordering segments.



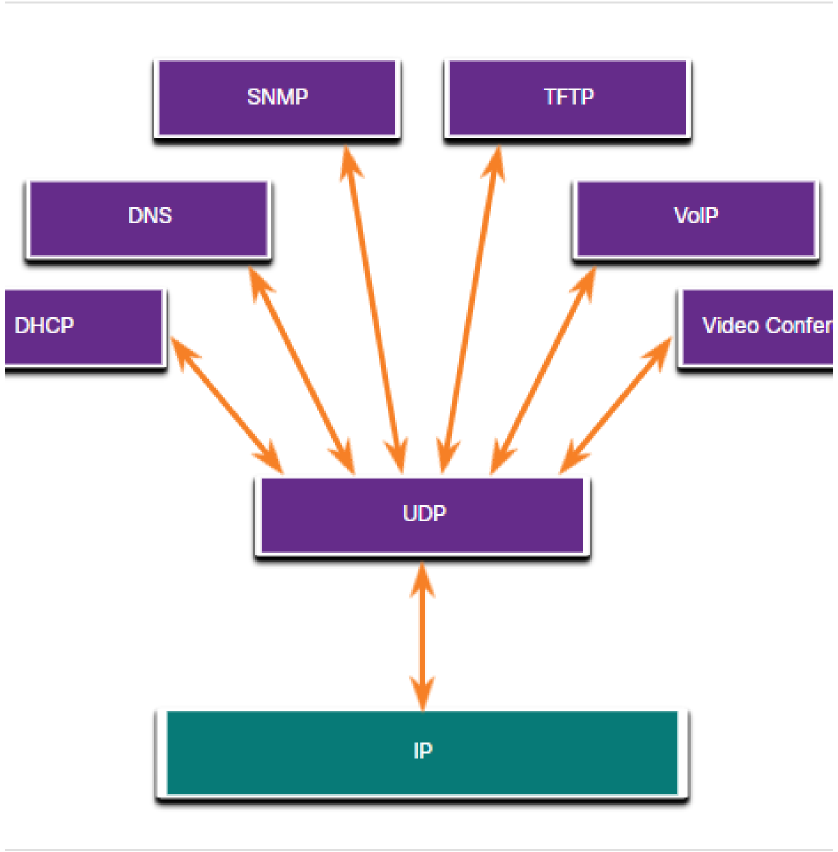
UDP Overview
UDP Header

- The UDP header is far simpler than the TCP header because it only has four fields and requires 8 bytes (i.e. 64 bits).

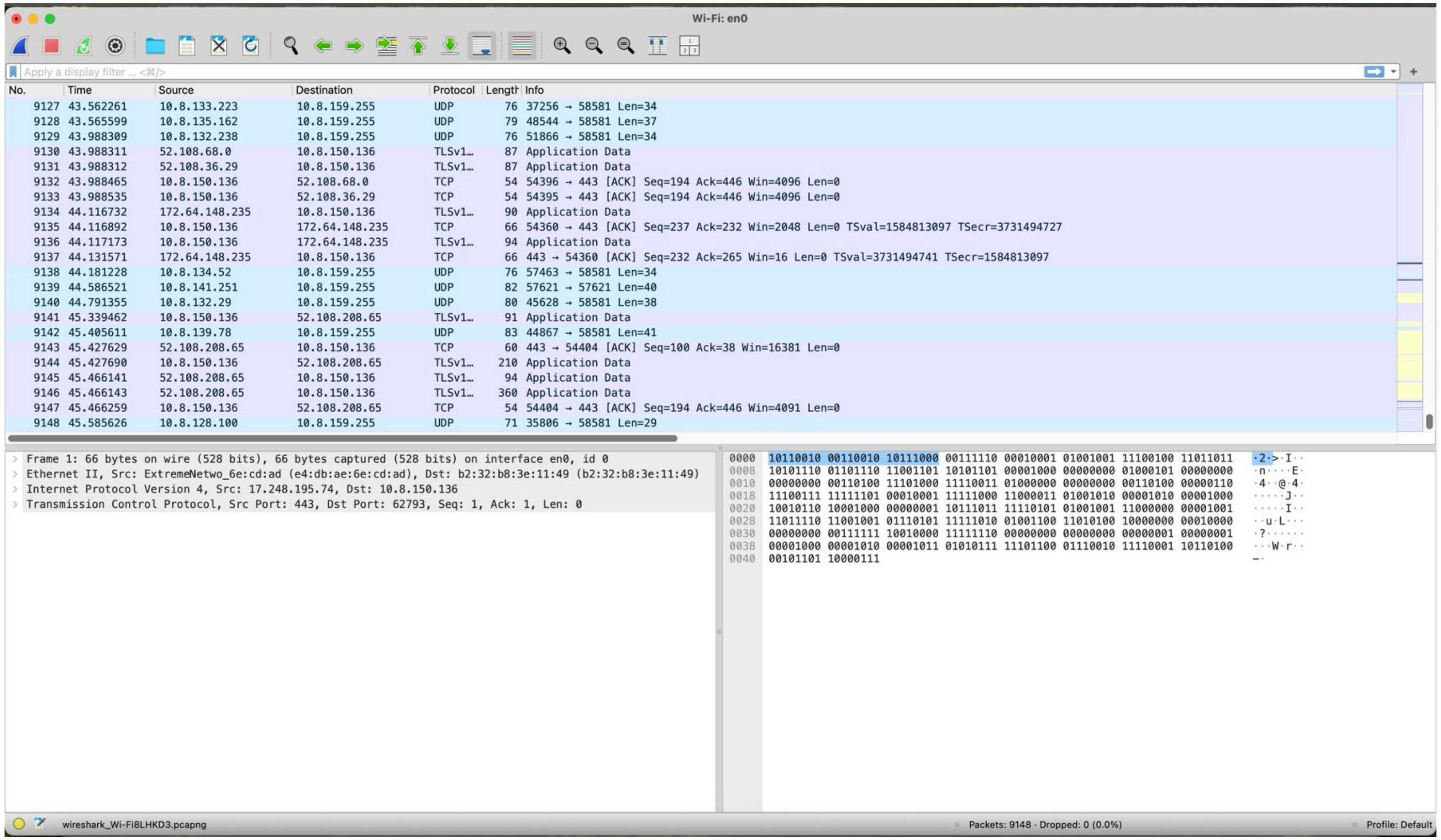


UDP Overview
Applications that use UDP

- Live video and multimedia applications - These applications can tolerate some data loss but require little or no delay. Examples include VoIP and live streaming video.
- Simple request and reply applications - Applications with simple transactions where a host sends a request and may or may not receive a reply. Examples include DNS and DHCP.
- Applications that handle reliability themselves - Unidirectional communications where flow control, error detection, acknowledgments, and error recovery is not required, or can be handled by the application. Examples include SNMP and TFTP.



Wireshark Demo!!!!

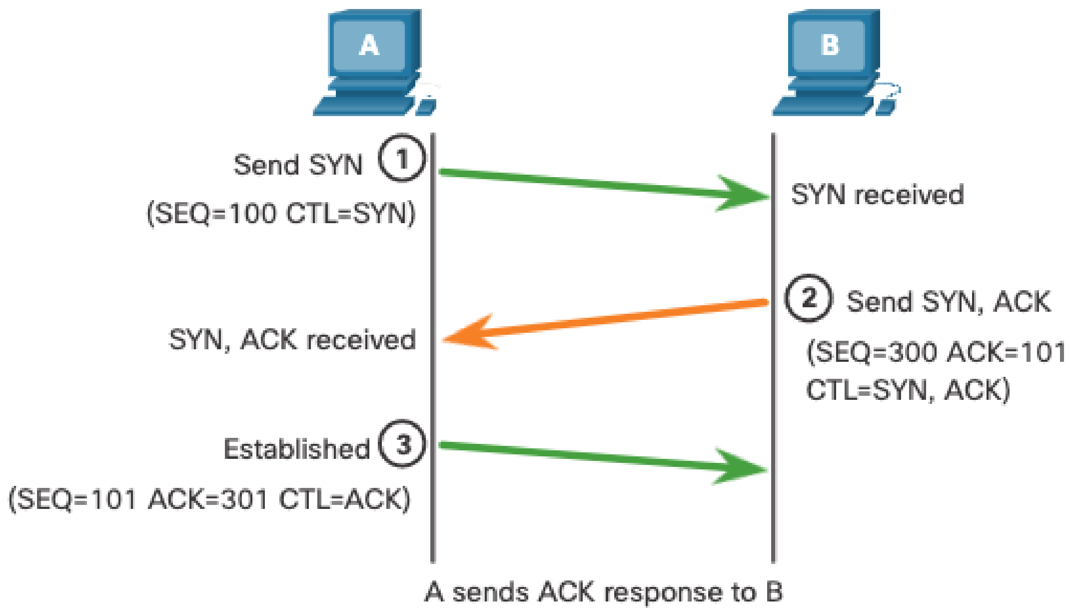


TCP Communication Process
TCP Connection Establishment

Step 1: The initiating client requests a client-to-server communication session with the server.

Step 2: The server acknowledges the client-to-server communication session and requests a server-to-client communication session.

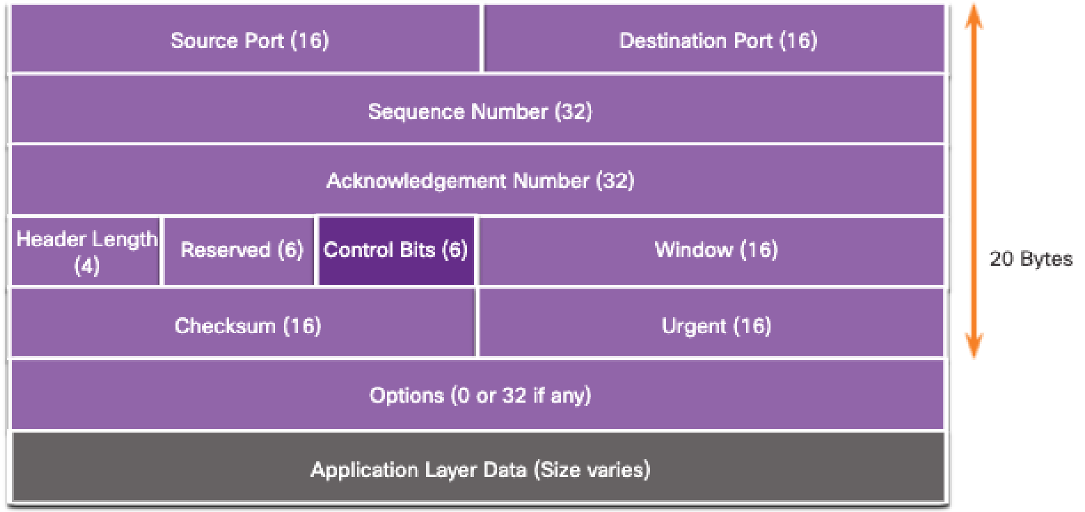
Step 3: The initiating client acknowledges the server-to-client communication session.



TCP Communication Process
TCP Three-Way Handshake Analysis (Cont.)

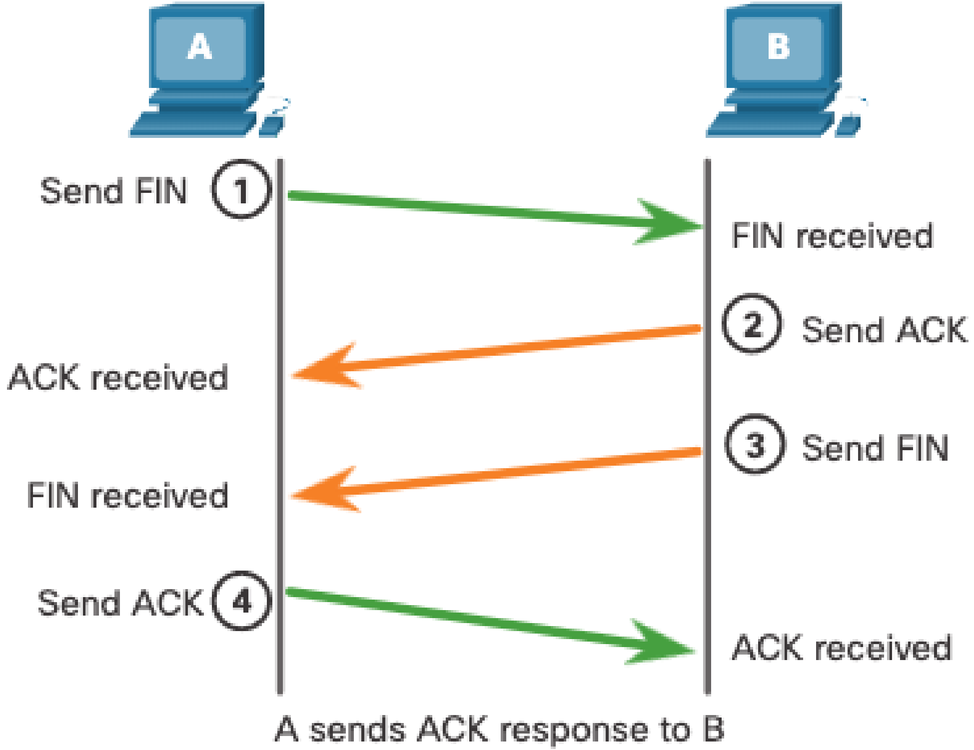
The six control bit flags are as follows:

- **URG** - Urgent pointer field significant
- **ACK** - Acknowledgment flag used in connection establishment and session termination
- **PSH** - Push function
- **RST** - Reset the connection when an error or timeout occurs
- **SYN** - Synchronize sequence numbers used in connection establishment
- **FIN** - No more data from sender and used in session termination



TCP Communication Process
Session Termination

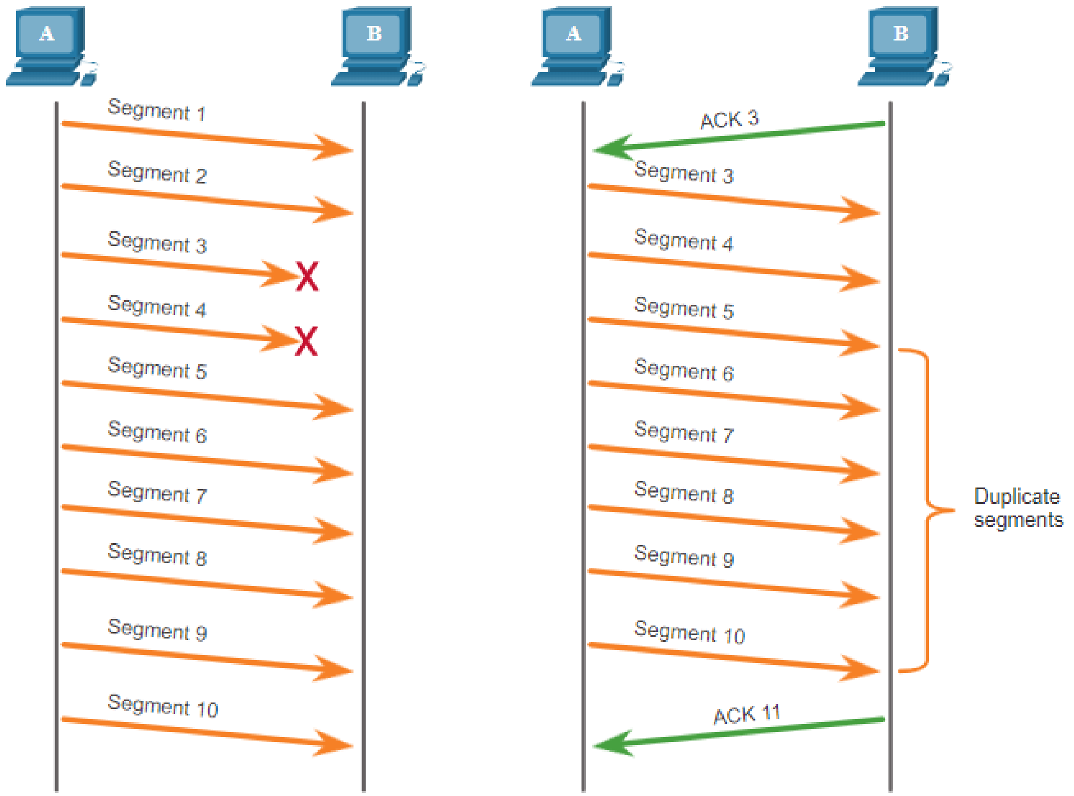
- Step 1: When the client has no more data to send in the stream, it sends a segment with the FIN flag set.
- Step 2: The server sends an ACK to acknowledge the receipt of the FIN to terminate the session from client to server.
- Step 3: The server sends a FIN to the client to terminate the server-to-client session.
- Step 4: The client responds with an ACK to acknowledge the FIN from the server.



Reliability and Flow Control
TCP Reliability – Data Loss and Retransmission

No matter how well designed a network is, data loss occasionally occurs.

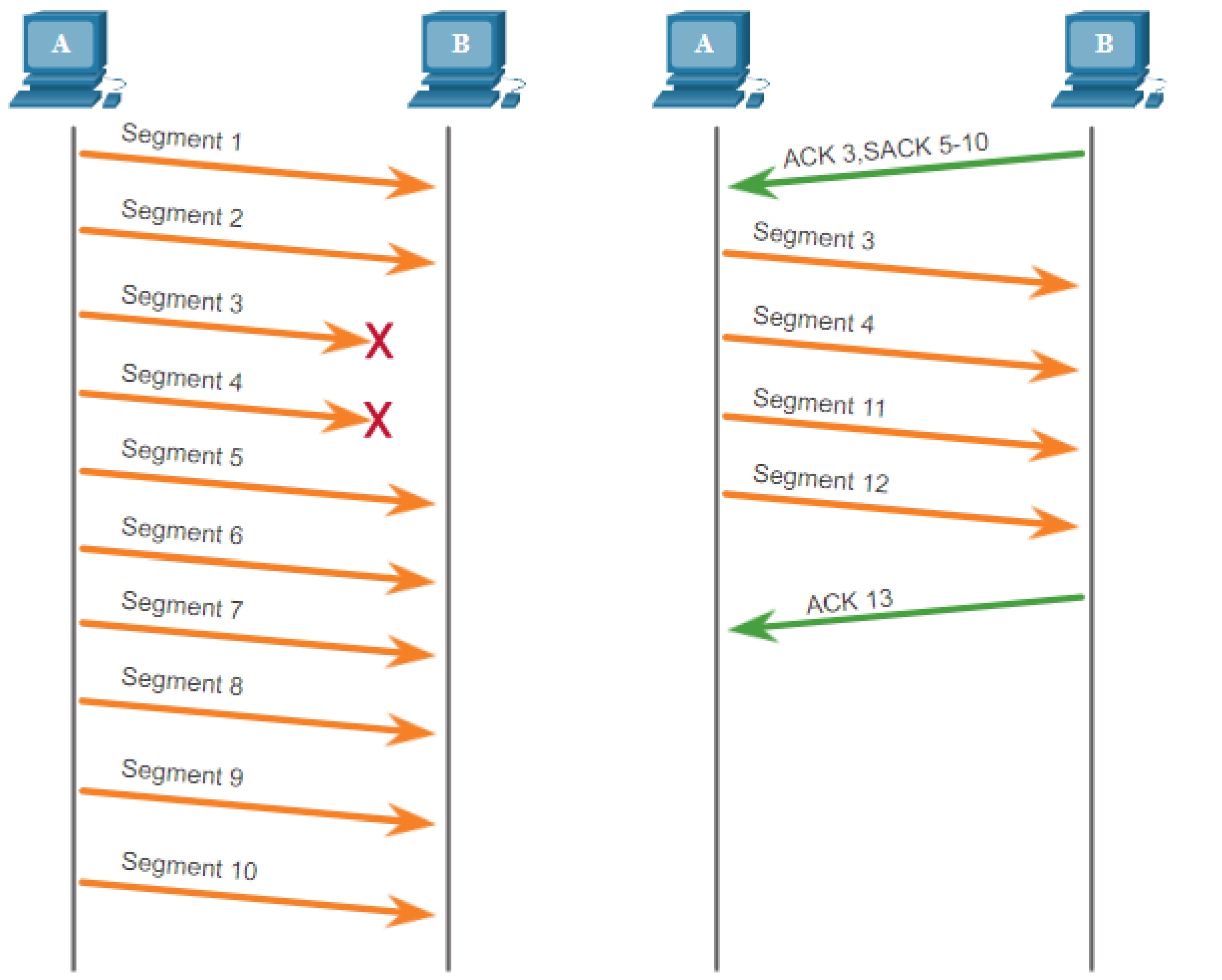
TCP provides methods of managing these segment losses. Among these is a mechanism to retransmit segments for unacknowledged data.



TCP Reliability – Data Loss and Retransmission (Cont.)

Host operating systems today typically employ an optional TCP feature called selective acknowledgment (SACK), negotiated during the three-way handshake.

If both hosts support SACK, the receiver can explicitly acknowledge which segments (bytes) were received including any discontinuous segments.



Directory Service (DS)

Software system that organizes, manages, administers, and locates network resources/objects.

Identifies every network resource (users, computers, printers, servers, email addresses, etc.).

Netware directory services (NDS) - Novell Netware uses NDS. NDS maintains information about all network resources (users, groups, servers, and volumes) in a hierarchical tree structure.

Active directory services (ADS) - Microsoft uses ADS. ADS was developed after NDS and is Microsoft's version of NDS.

LDAP

LDAP (Lightweight Directory Access Protocol)

- Accesses and maintains distributed directory information services over an IP network.
- Provides a central location for storing **usernames and passwords**.
- Applications and services use LDAP to **validate users**.
- Example: Active Directory in Windows Server 2019 uses LDAP.
- Uses **TCP or UDP port 389**.

Security of LDAP

- LDAP traffic is **not secure** (transmitted in cleartext).

LDAPS (LDAP Secure / LDAP over SSL)

- Uses **SSL/TLS** to secure LDAP transmissions.
- Client and server establish SSL/TLS connection **before transmitting LDAP messages**.
- LDAPS connection ends when the underlying SSL/TLS connection closes.
- Uses **TCP port 636** by default.

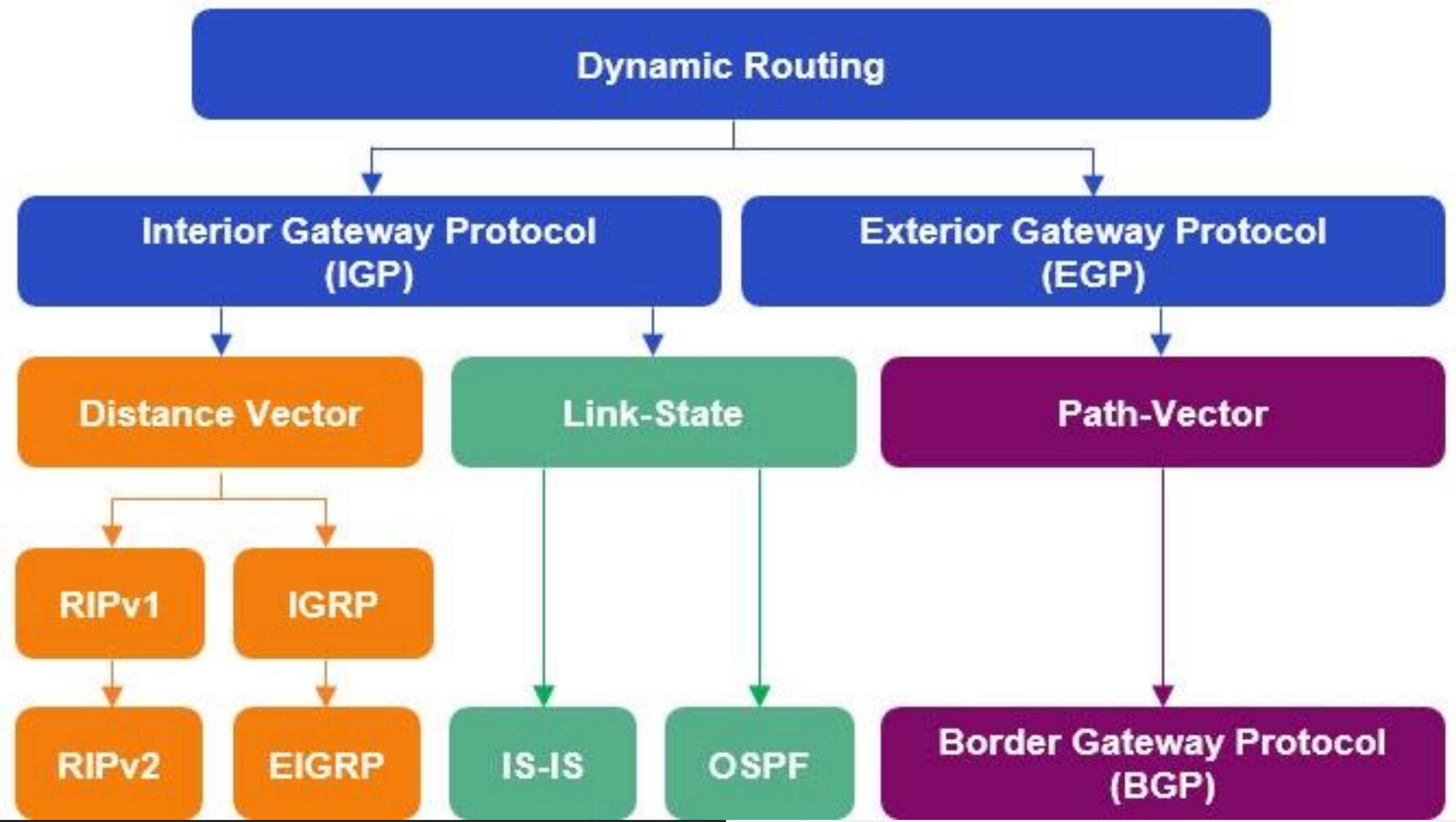
Routing Protocols

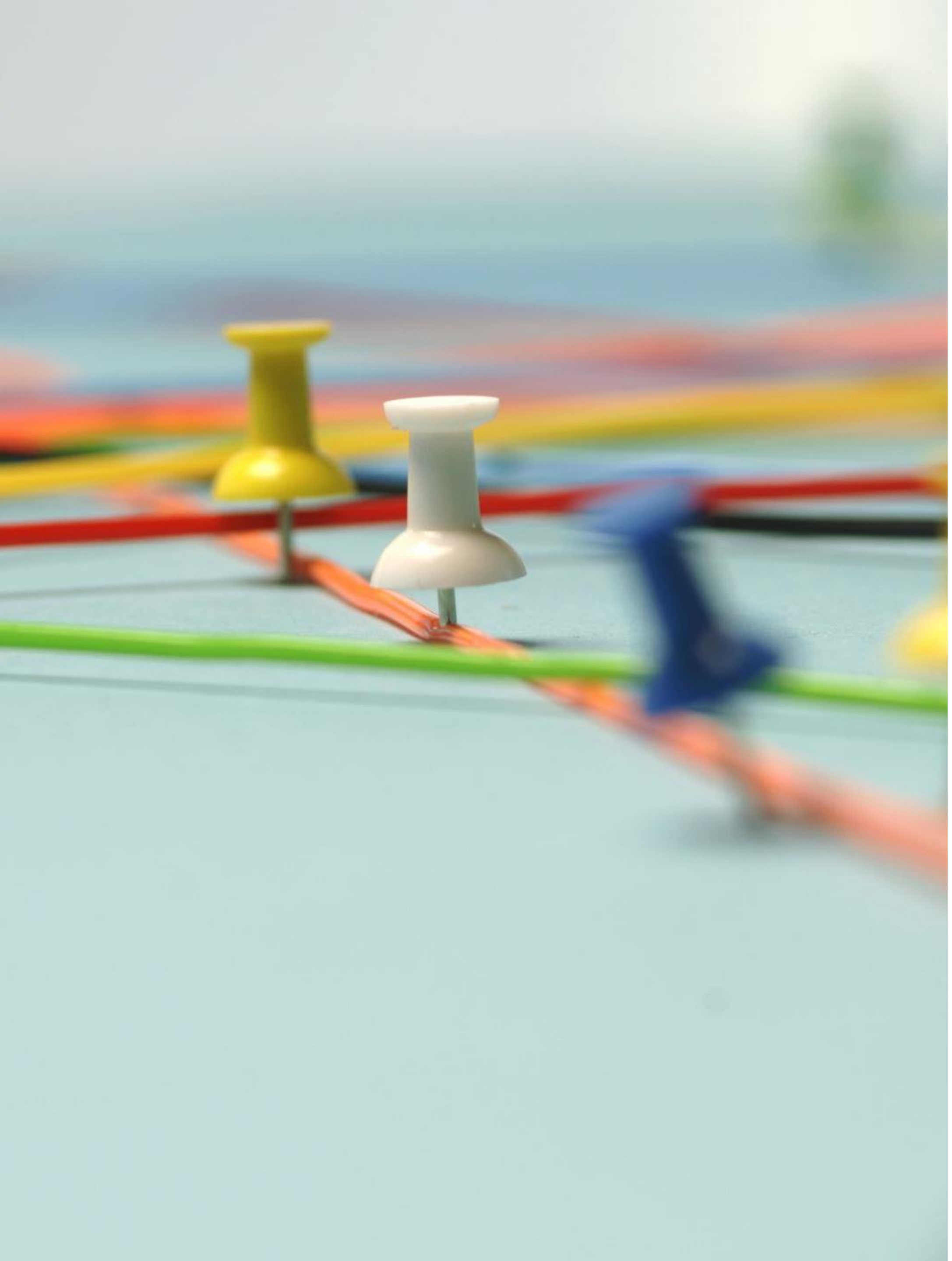
WE have a packet now what!!!!!

Routing Basics

This material was developed with funding from the National Science Foundation under Grant # DUE 1601612

Restart 1/12 Back Next

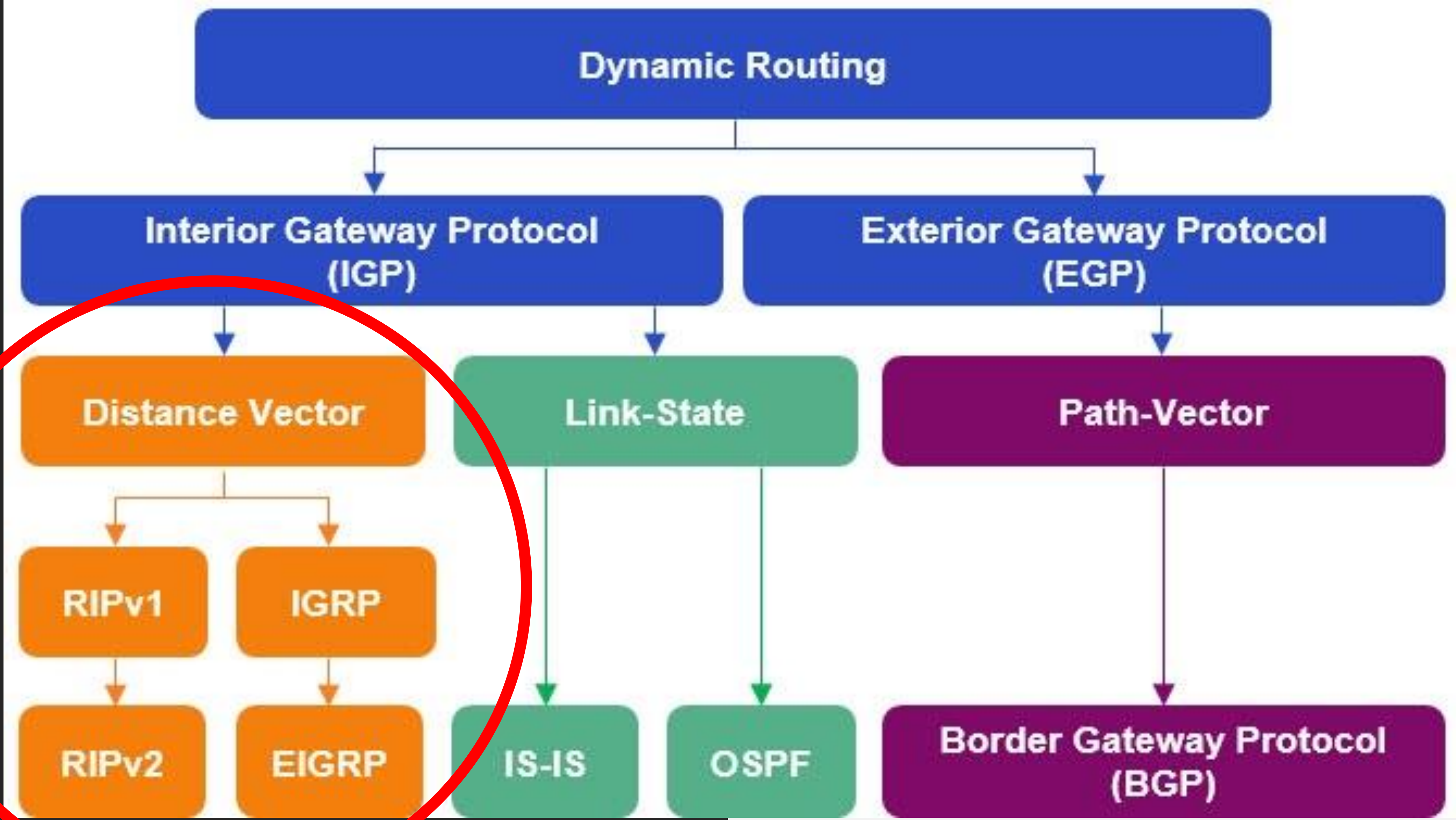

Dynamic Routing
Interior Gateway Protocol (IGP)
Exterior Gateway Protocol (EGP)
Distance Vector
Link-State
Path-Vector
RIPv1
IGRP
RIPv2
EIGRP
IS-IS
OSPF
Border Gateway Protocol (BGP)



6.2 Distance vector protocol

- A ***distance vector protocol*** is a routing protocol that uses distance vectors or hop count as a primary metric to determine a packet's destination route.

- **Characteristics of a distance vector protocol:**
  - Routinely sends routing table information to neighboring routers.
  - Determines the best path using hop count. Hop count is the number of routers the data passes through to get to the destination device.
  - Uses the Bellman-Ford algorithm to calculate the best route.


Dynamic Routing
Interior Gateway Protocol (IGP)
Exterior Gateway Protocol (EGP)
Distance Vector
Link-State
Path-Vector
RIPv1
IGRP
RIPv2
EIGRP
IS-IS
OSPF
Border Gateway Protocol (BGP)

Routing Information Protocol (RIP)

- Ch
  - ses
  - s.
  - ers

R.I.P.

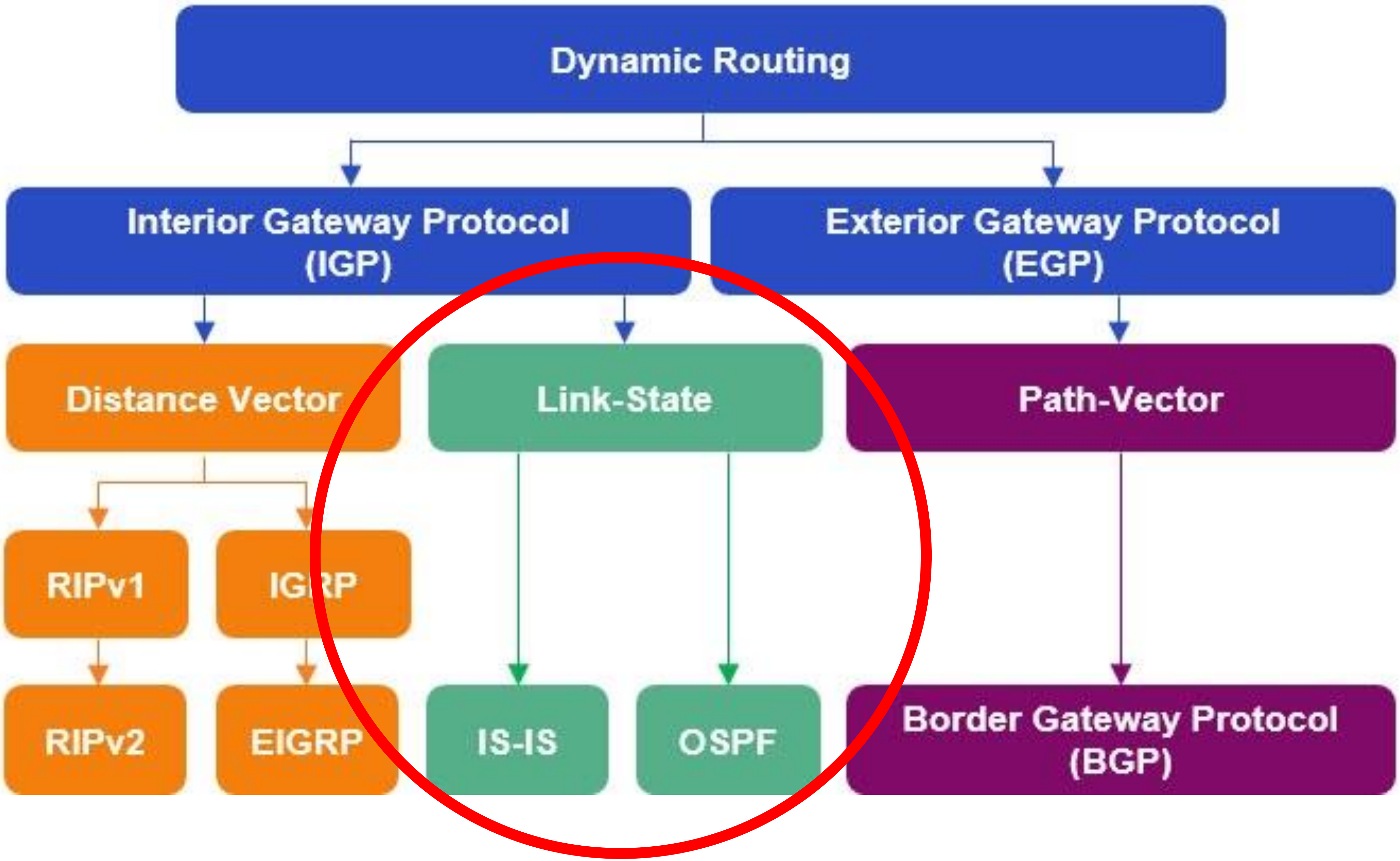
RIP

(RIP is dead!)

IGRP Cisco

Interior Gateway Routing Protocol (IGRP) is a proprietary distance vector routing protocol used to send routing information within an autonomous system. To avoid routing loops, IGRP updates the occurring network changes and uses error management. IGRP is a network layer protocol (Layer 3). IGRP uses IP protocol 9 directly.

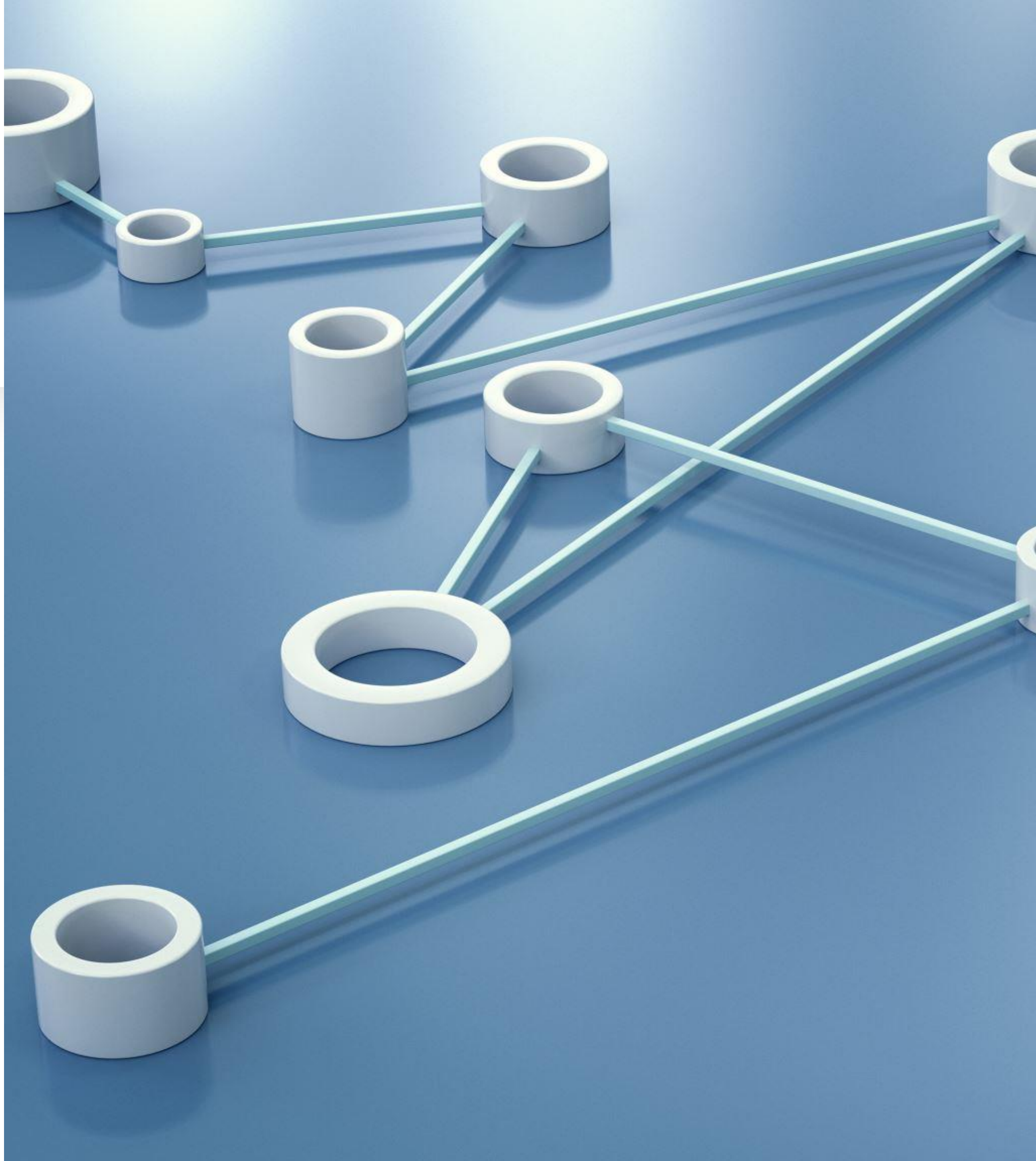
- IGRP characteristics:
  - Routers send updates to neighboring routers every 90 seconds.
  - The maximum hop count is 255.
  - Metric parameters:
    - Delay
    - Bandwidth
    - Reliability
    - Load

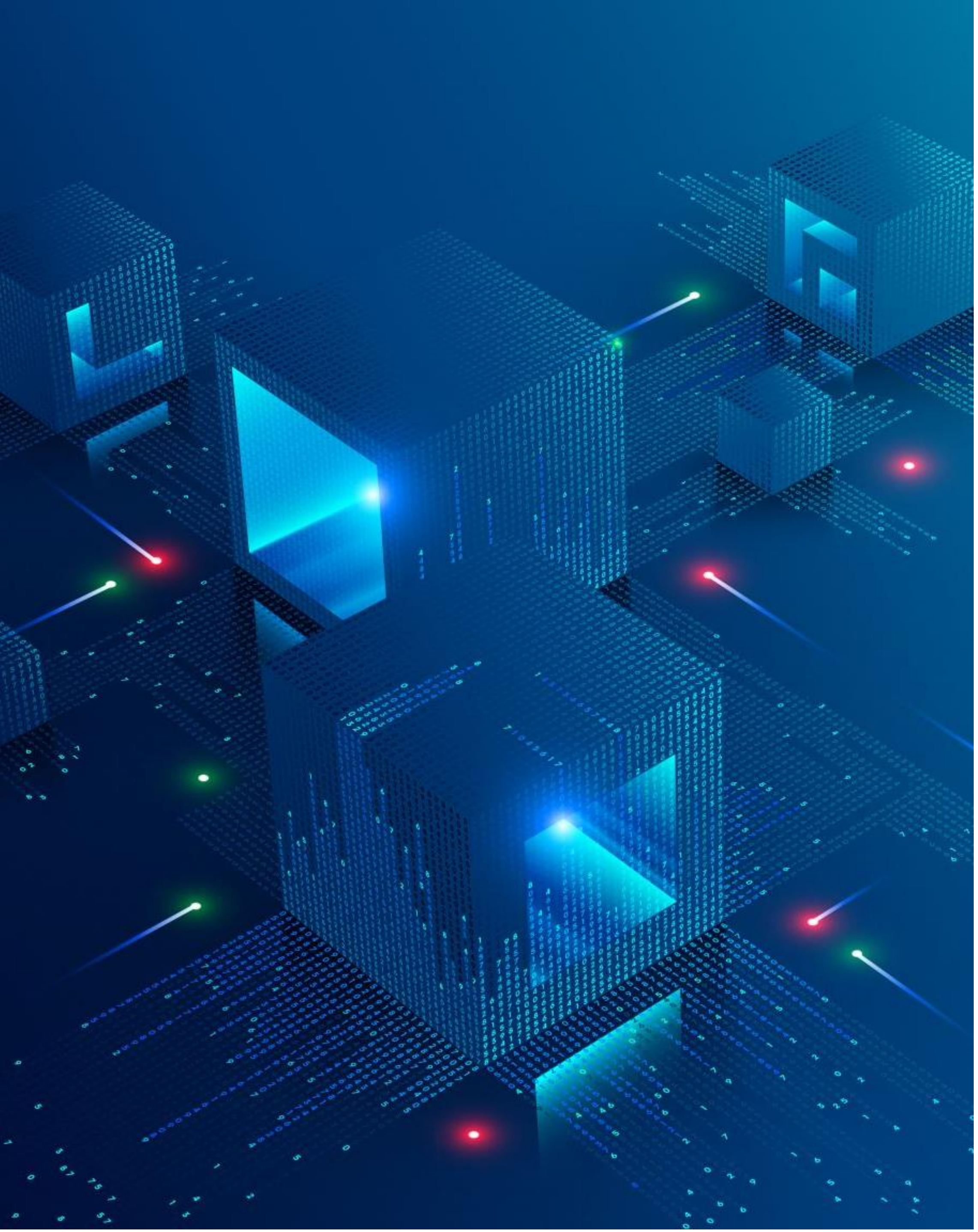


Dynamic Routing
Interior Gateway Protocol (IGP)
Exterior Gateway Protocol (EGP)
Distance Vector
Link-State
Path-Vector
RIPv1
IGRP
RIPv2
EIGRP
IS-IS
OSPF
Border Gateway Protocol (BGP)

6.3 Link state (OSPF) Open Shortest Path First

- A ***link state protocol***, also known as ***shortest path first protocol***, is an IGP routing protocol used in packet switching networks. A link state routing protocol has a full network topology picture by using three tables per enabled router. Using the topology and neighbor connectivity information, each router calculates the best path to each network destination. Each calculated best path forms the router's routing table.
- **Link-state protocol characteristics:**
    - Floods information to each router about the state of routers directly connected links.
    - Uses link state information to build a link-state database, providing a full network topology picture.
    - Uses bandwidth efficiently.
    - Intensive use of CPU and memory.

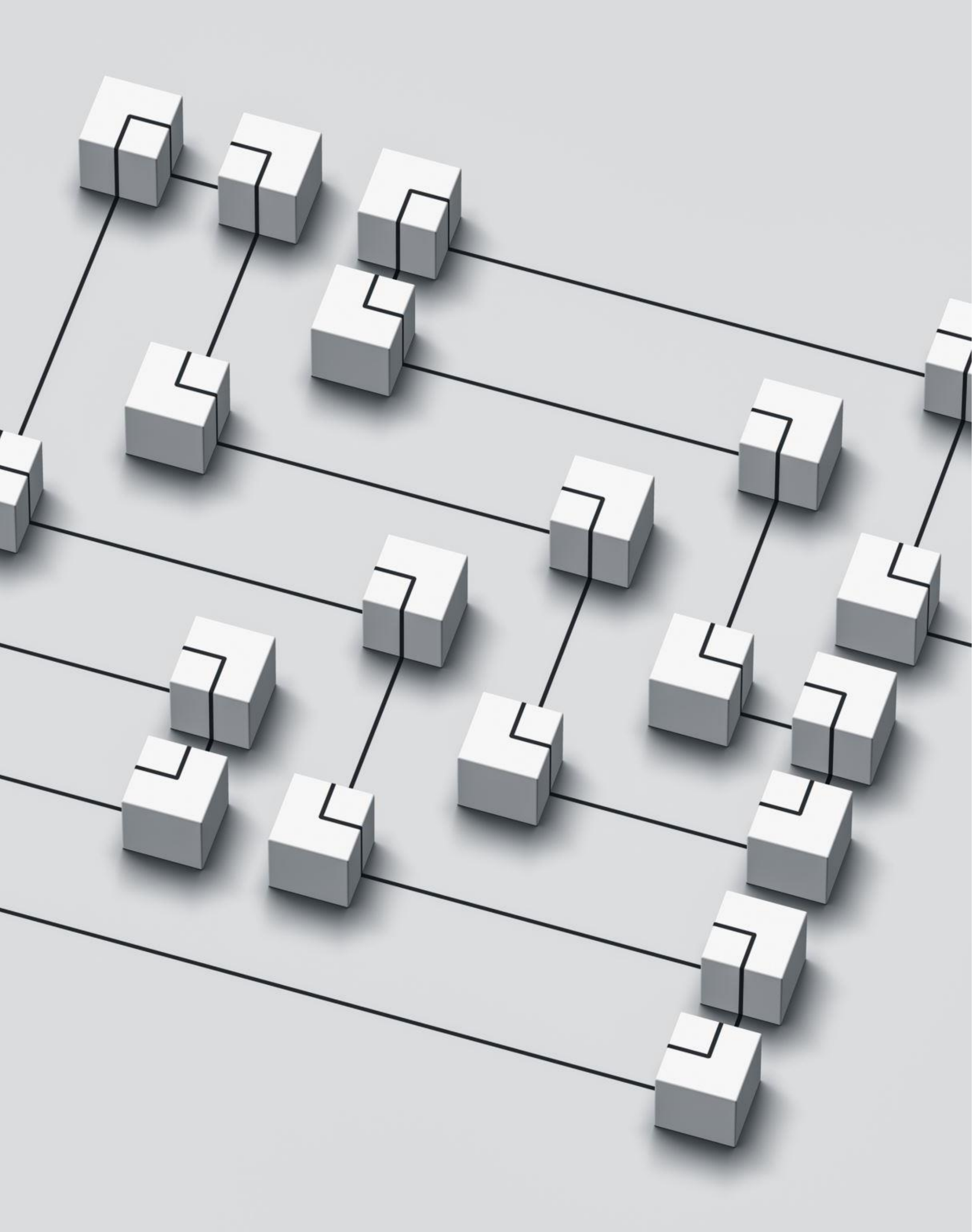




6.3 BGP

Border Gateway Protocol (BGP) is an exterior gateway protocol enabling the internet to exchange routing information between autonomous systems. The internet has thousands of smaller autonomous systems connected together. BGP is the protocol for routing the data path through multiple autonomous systems. BGP is an application layer protocol (Layer 7). BGP uses TCP port 179.

USED BY ISP (internet Service Providers) and WAN ports on enterprise routers.



6.3 *Enhanced Interior Gateway Routing Protocol (EIGRP)*

- EIGRP advantages over IGRP:
  - Provides faster convergence.
  - Exchanges router information more efficiently.
  - Addresses scalability problem.
  - Improves voice and video quality.
  - Updates neighboring routers with changes only, not an entire routing table.
  - Uses a Hello packet to notify neighboring routers the router is operative. If no Hello packet is sent after a certain time, the router is considered offline.

CDP and LLDP

- ***Cisco Discovery Protocol (CDP)***
- ***Link Layer Discovery Protocol (LLDP)***

Layer 2 *discovery protocols used to learn and share information about neighboring devices. Ex: Switches and firewalls. CDP is a Cisco-proprietary protocol whereas LLDP is a non-proprietary or standards-based protocol. CDP and LLDP are compatible. However, exclusively Cisco-based networks typically use CDP instead of LLDP.*

6.4 Common protocols

Network Management Protocol (NMP)

- Internet Control Message Protocol (ICMP)
- Simple network management protocol (SNMP).
- Suite of protocols defining processes, procedures, and policies to manage a network.

Server Message Block (SMB) Protocol

a client-server communication protocol, is used for sharing access to files, printers, and serial ports. SMB can also carry transaction protocols for interprocess communication and is implemented in Microsoft Windows.

Simple network management protocol (SNMP)

SNMP

- Network protocol for monitoring and managing networked devices in an IP network.
- Operates at the **application layer (Layer 7)**.
- Uses **TCP ports 161 and 162**.

Key Components

- **Managed Device / Network Element**:
  - Any device with an SNMP interface (switch, router, modem, printer, IP phone, host, etc.).
- **SNMP Manager**:
  - System that monitors and controls network elements.
- **SNMP Agent**:
  - Software running on the device that collects and maintains device information.

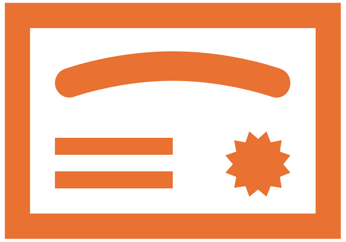
6.5 Secure protocols

Secure Sockets Layer (SSL)

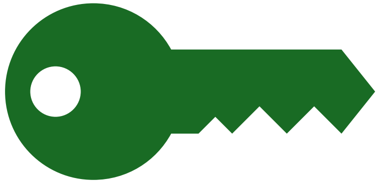
Transport Layer Security (TLS)

cryptography protocols used to provide secure communication between devices over a network.

6.5 Certificates



Security certificate (often called **SSL certificate**) issued by a Certificate Authority (CA).



Authenticates a website and provides a secure connection.

Encryption

This material was developed with funding from the
National Science Foundation under Grant # DUE 1601612

Restart 1/17 Back Next

SSL/TLS OSI Layer & Operation

SSL, TLS, and SSL/TLS operate at **OSI Layer 6 (Presentation Layer)**.

TLS is implemented **on top of TCP** to encrypt Application Layer protocols.

Uses **encryption algorithms** to scramble data.

Destination device **decrypts** data for application use.

Applications Using SSL/TLS

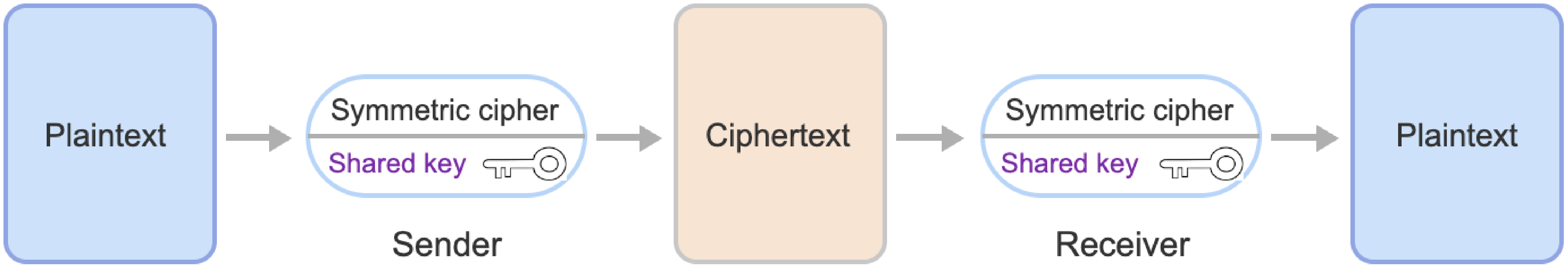
Email

Instant Messaging

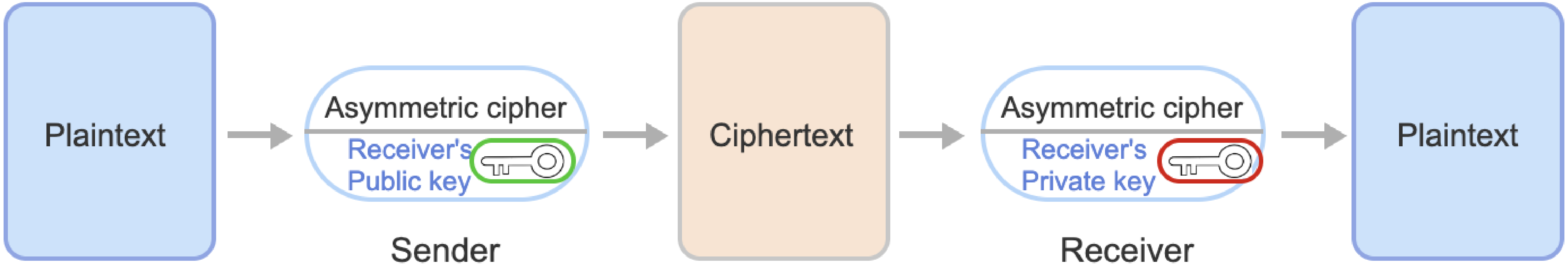
Voice over IP (VoIP)

HTTPS (Hypertext Transfer Protocol Secure)

Symmetric cryptography



Asymmetric cryptography



Diffie–Hellman
Key Exchange

E-MATE 2.0

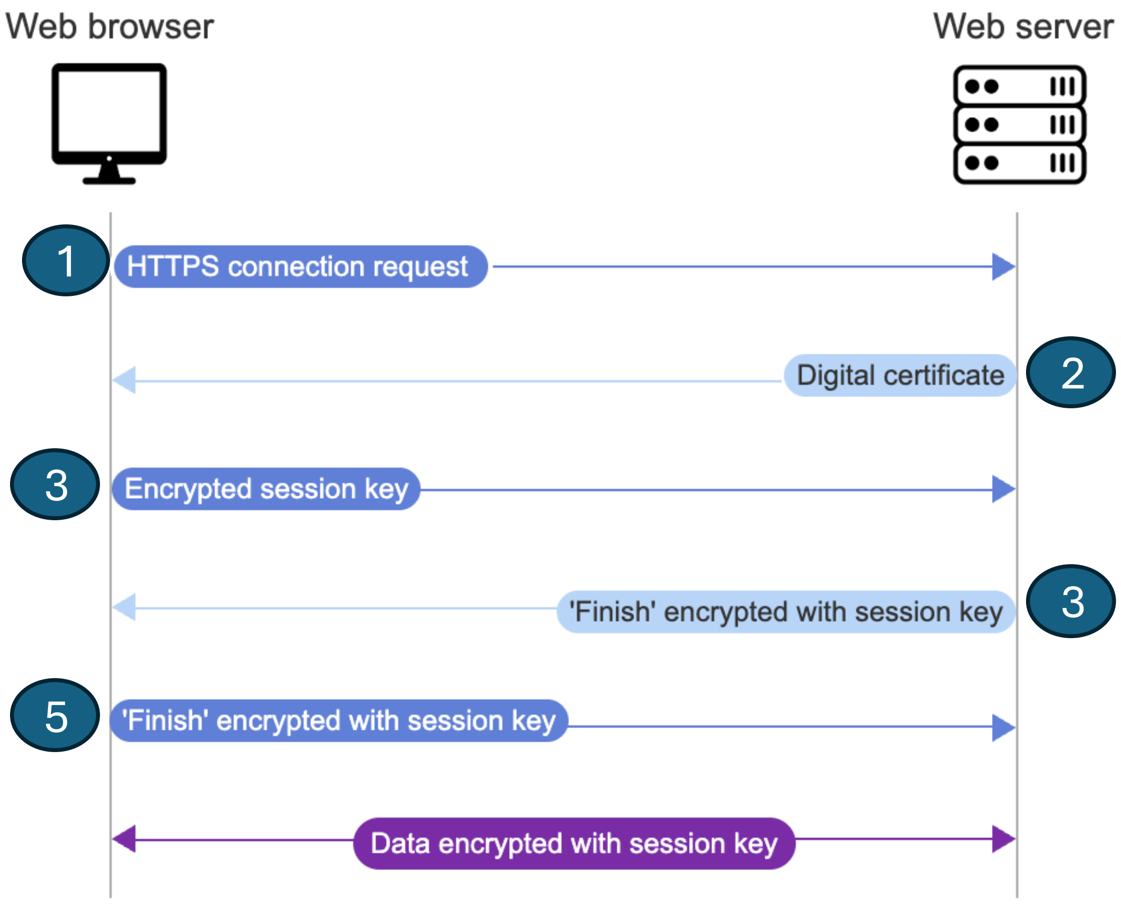
Building Capacity for Interactive Teaching and Learning

This material was developed with funding from the National Science Foundation under Grant # DUE 1601612

Restart 1/12 Back Next

6.6.3: HTTPS SSL/TLS handshake.

1. Web browser (HTTPS client) requests an HTTPS session from a web server.
2. Web server sends its digital certificate
3. Session key (symmetric key) and encrypts the session key with the web server's public key obtained from the digital certificate.
4. Server decrypts the session key with the web server's private key, encrypts "Finish" with the session key, and sends the encrypted message to the web browser.
5. Web browser encrypts "Finish" with the session key and sends the encrypted message to the web server. The HTTPS session data is encrypted with the session key.



Secure shell (SSH)

SSH (Secure Shell)

- Cryptographic network protocol for secure operation over an unsecured network.
- Uses **client-server model** (SSH client connects to SSH server).
- Replacement for **Telnet** and other insecure remote shell protocols.
- Uses **TCP port 22** by default.

6.6 Mail, web and remote access protocol

- ***Simple Mail Transfer Protocol (SMTP)*** is a network protocol for sending, receiving, and relaying outgoing emails. SMTP is an application layer protocol (Layer 7). SMTP uses TCP port 25 and SMTPS uses port 587.
- ***Hyper text transfer protocol (HTTP)*** is a network protocol for distributing graphics, audio, video, text, and hyperlinks on networks. HTTP is an application layer protocol (Layer 7). HTTP uses TCP port 80.
- ***Hypertext transfer protocol secure (HTTPS)***, also known as ***HTTP over SSL*** or ***HTTP over TLS***, is an extension of the hypertext transfer protocol (HTTP) that uses SSL/TLS to establish an authenticated and encrypted connection between a client and a server. HTTPS is used for secure data exchange between a web browser and a web server. HTTPS is an application layer protocol (Layer 7). HTTPS uses TCP port 443 by default.

File transfer protocol (FTP)

FTP (File Transfer Protocol)

Network protocol for transferring files between devices.

Operates at the **Application Layer (Layer 7)**.

Uses **TCP ports 20 (data) and 21 (command)**.

Client/Server Model

Uses **two channels**: command channel and data channel.

Transfers files between two devices.

Common FTP Uses

Backup – move data at regular intervals for safekeeping.

Replication – duplicate data in real time for availability/resilience.

Data Loading – transfer/load data to a remote device (often cloud-based).

TFTP (Trivial File Transfer Protocol)

Simplified version of FTP.

Primarily used for transferring **network device configurations**.

Uses **UDP port 69**.

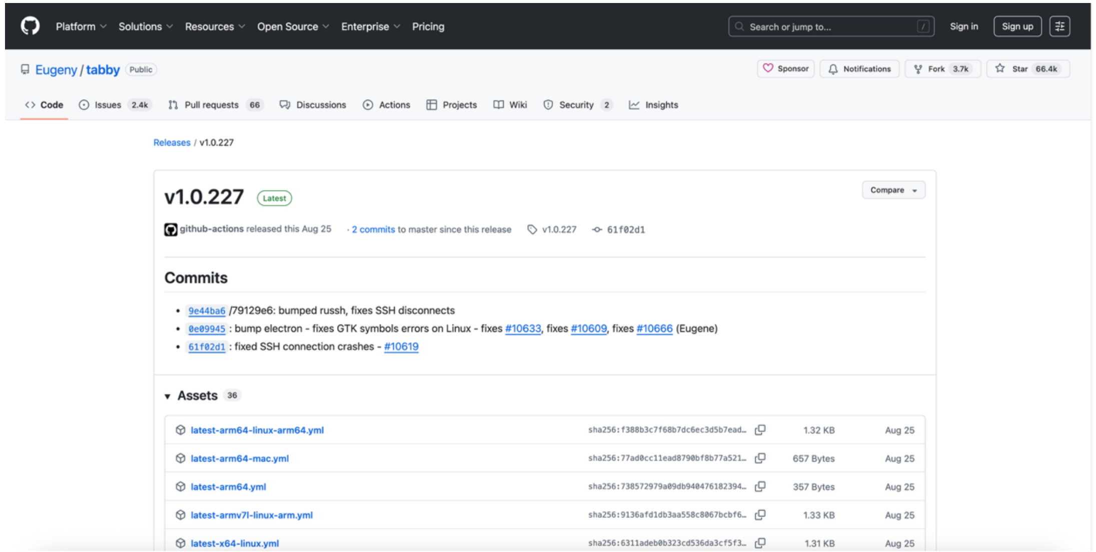
Commonly used in **PXE boot** to download network software.

Table 6.6.1: File transfer protocols.

Protocol	Security mechanism	Port
FTP	None	TCP 20 (data channel) TCP 21 (control channel)
FTPS	FTP over SSL/TLS	TCP 989 (data channel) TCP 990 (control channel)
SFTP	SSH	TCP 22

Today you should download these programs

- Windows download



SSH Practice

[SDF Public Access UNIX System .. Est. 1987]

join welcome faq status members store tour gopher abuse dialup minecraft
social tilde europa webmail gallery usermap irc tutorials telnet git ssh

-=- a community platform for inspiring, facilitating and implementing new ideas -=-

Create a Free UNIX Shell Account

Your E-Mail:
Preferred Login:
Confirm

Alternative methods

- **MacOS X** users, click here: ssh://new@sdf.org
- **Web Browser** users may use our HTML5 SSH client: https://ssh.sdf.org
- **Linux/UNIX** users can type 'ssh new@sdf.org' at their shell prompts.

For Microsoft Windows we highly recommend the free SSH client putty.exe.

If you have any questions or cannot figure out how to use **SSH**, live help is available on IRC via **irc.sdf.org** in the **#helpdesk** channel.

Make a Donation

Please be sure fill in the description with your login and membership option.

Chapter 6: Protocols

Chapter 7: Switches and Routers

7. Switches and Routers

7.1 Network transmission

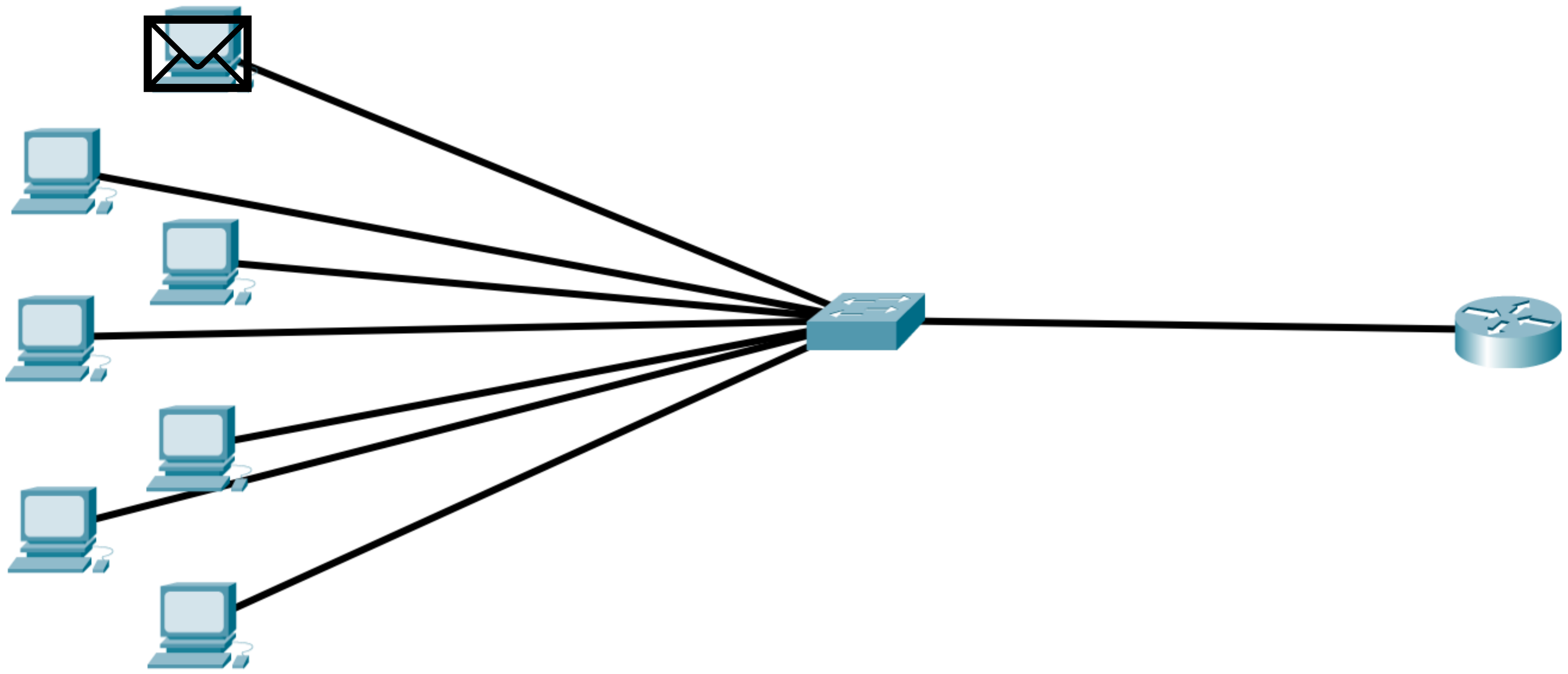
Broadcast, multicast, and unicast

A ***cast*** is the transmission of packets across network media.

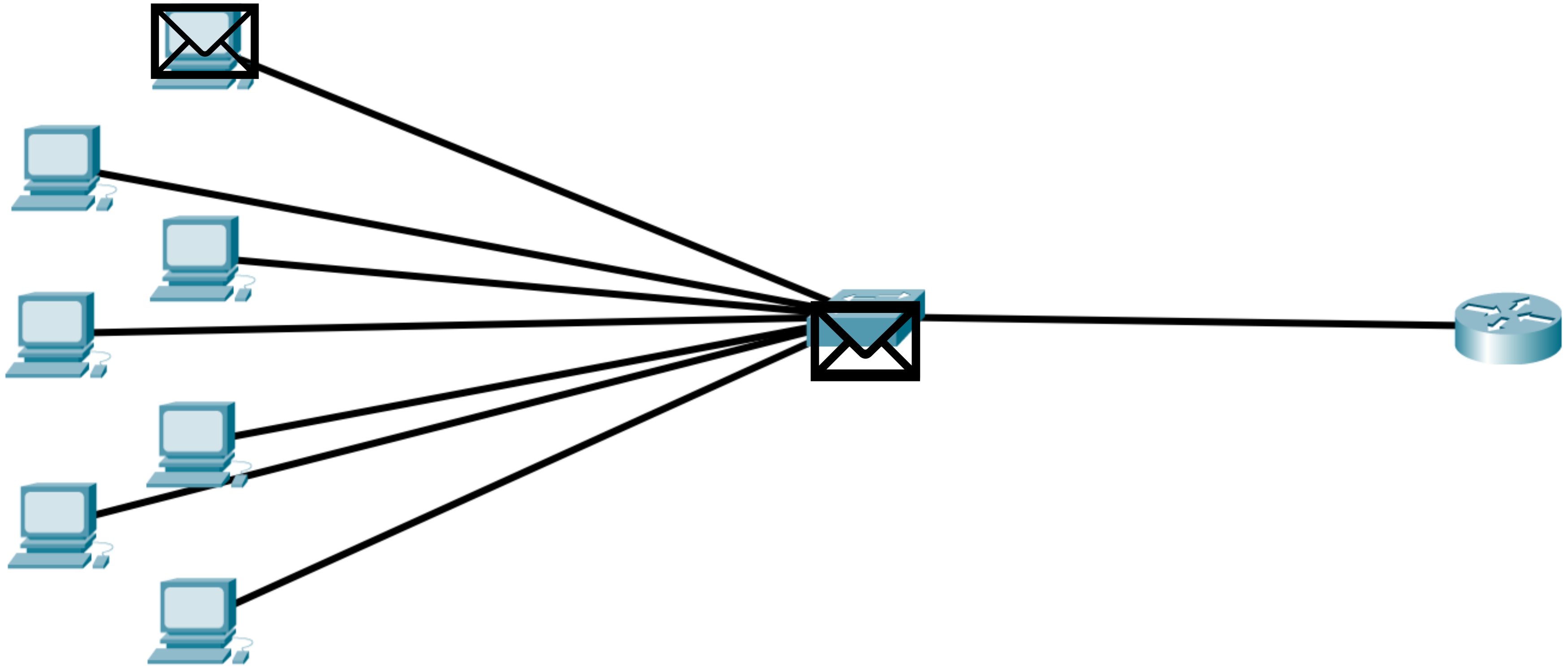
Three cast types:

- Unicast - ***Unicast*** is a cast to a single network device.
- Multicast - ***Multicast*** is a cast to a group of network devices simultaneously.
- Broadcast - ***Broadcast*** is a cast to all devices on the network simultaneously.

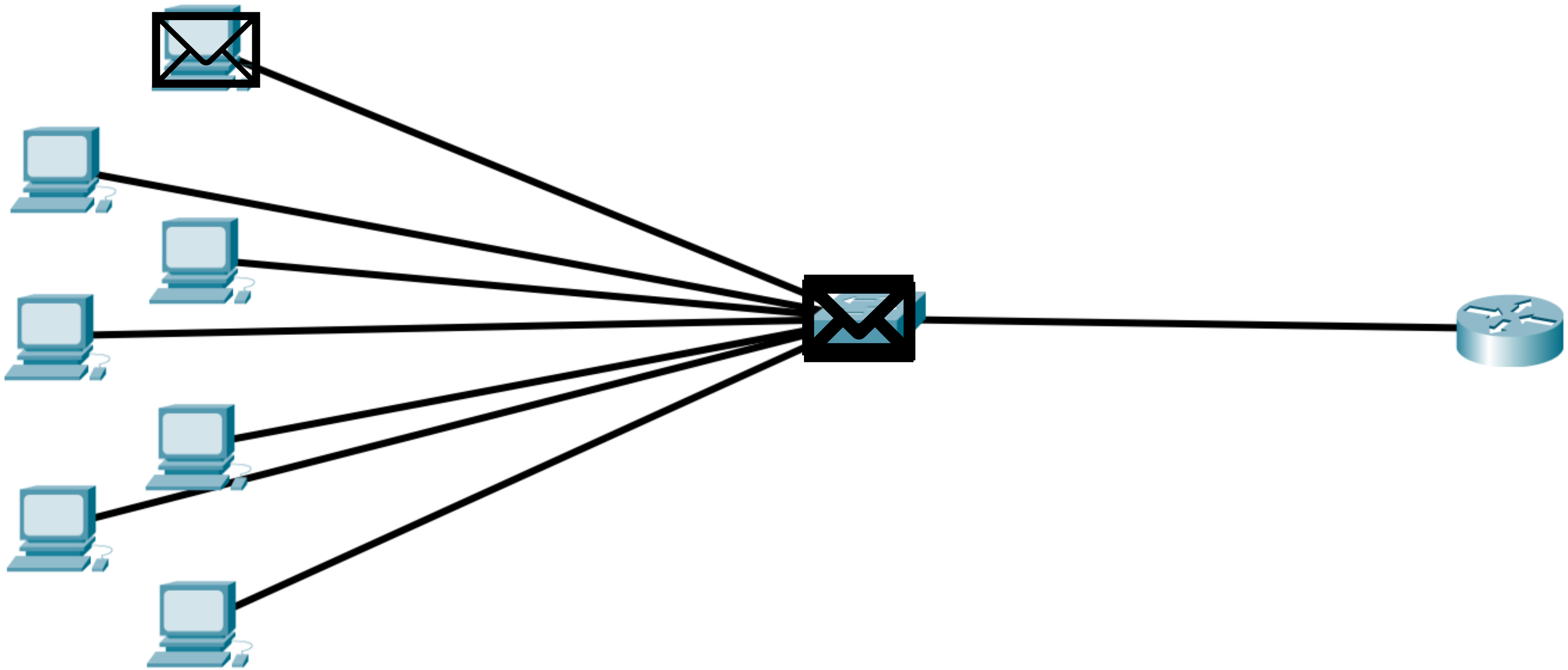
Unicast (One to one)



Multicast (One to many)



Broadcast (One to everyone)



Broadcast and collision domains

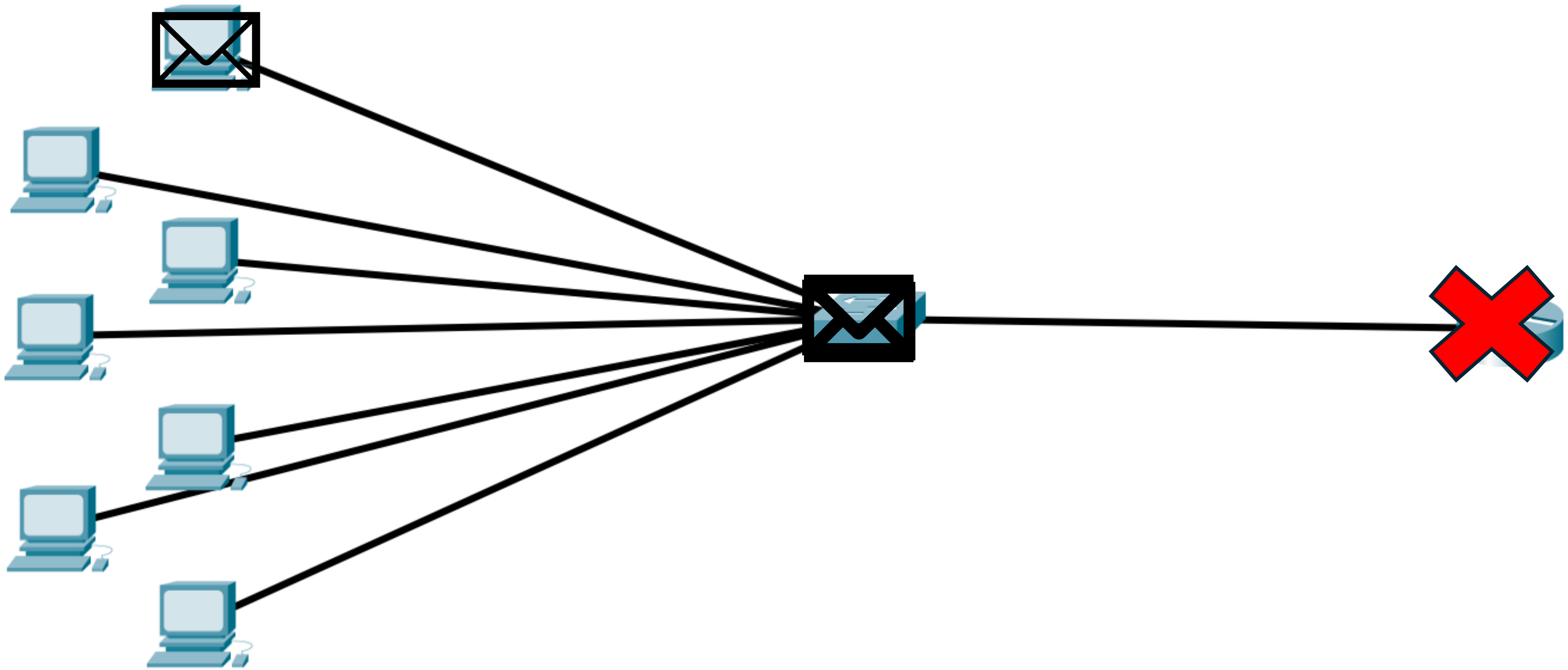
Broadcast domain:

- Logical Layer 2 network segment where all devices receive broadcast traffic.
- By default, all switch ports share one broadcast domain.
- Each router port forms a separate broadcast domain.

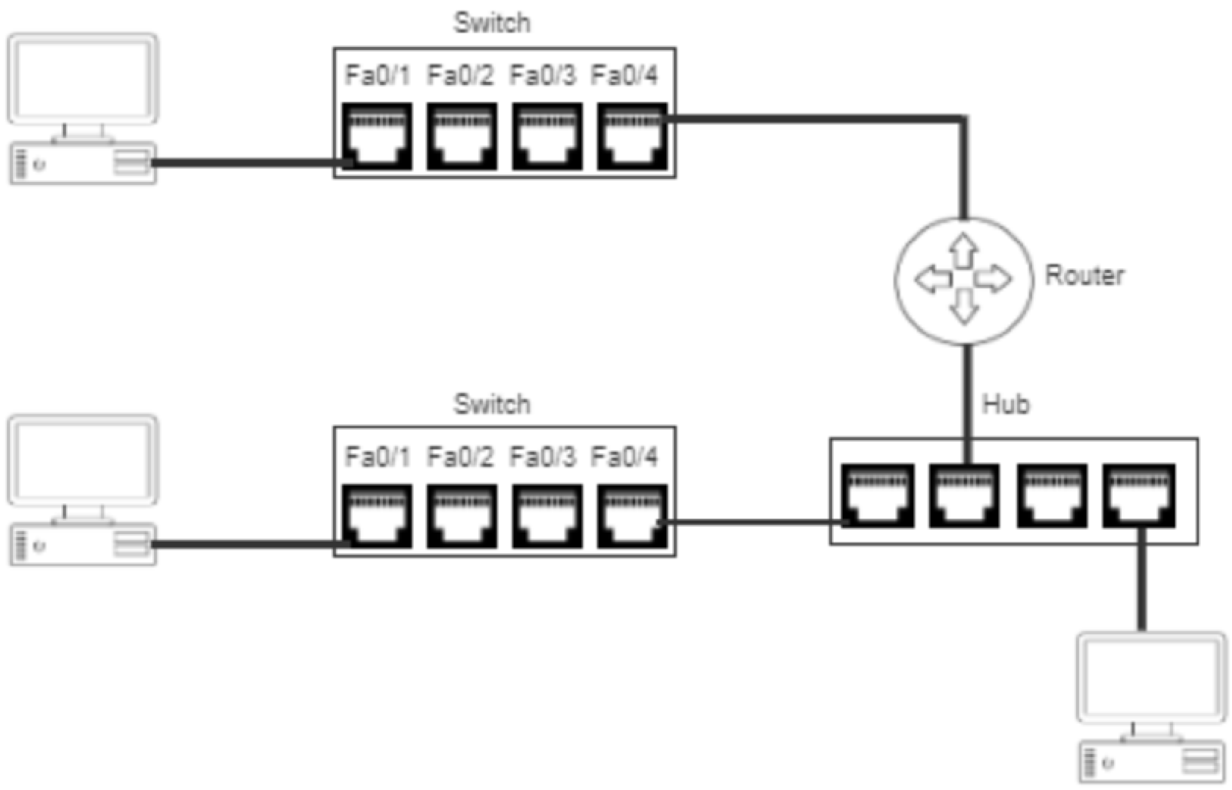
Collision domain:

- Area where packet/frame collisions can occur at Layer 2.
- Collisions happen when two devices transmit simultaneously.
- Each switch, bridge, or router port is its own collision domain.
- All **hub ports** share a **single collision domain**.

Broadcast domains



Collision domain



Maximum Transmission Unit (MTU):

- Largest Layer 3 protocol data unit (PDU) that can be transmitted.
- Smaller MTU → lower delay; larger MTU → less overhead.
- Measured in bytes; Ethernet MTU = **1,500 bytes**.

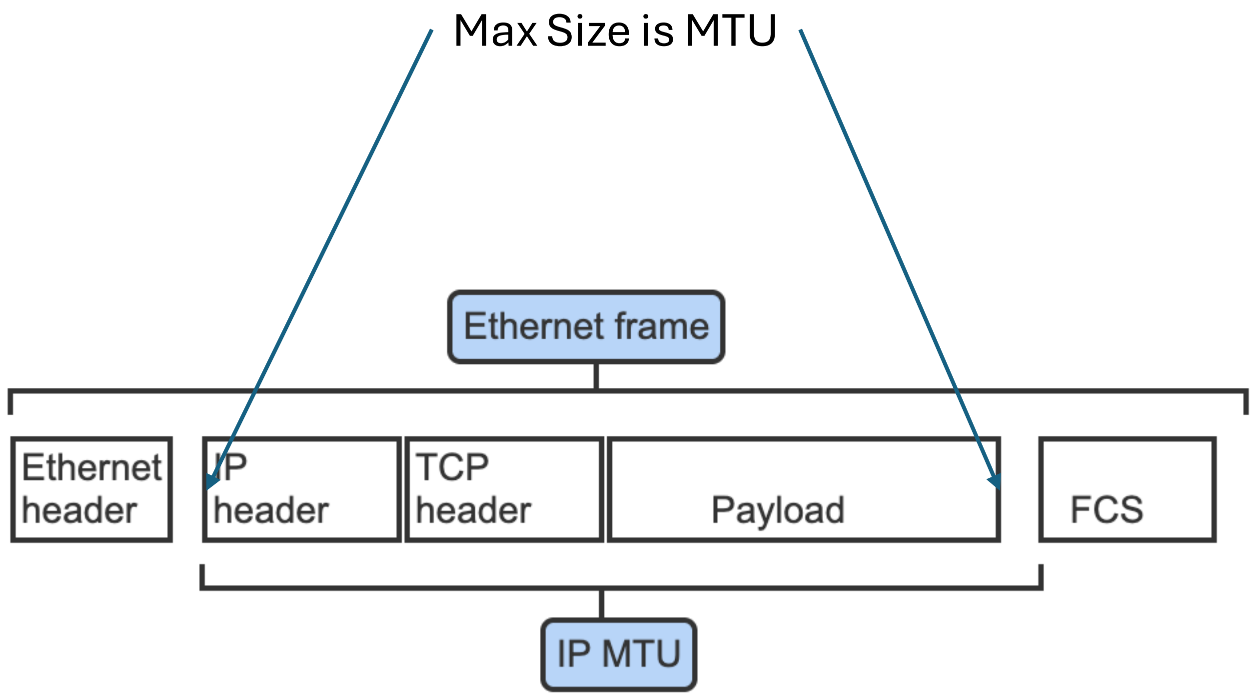
Overhead:

- MTU = maximum frame size – overhead.
- Ethernet frame = **1,518 bytes total**, with **18 bytes** of overhead.

Jumbo Frame:

- Ethernet frame with payload >1,500 bytes.
- Used on **1 Gbps LANs**.
- Maximum size = **9,000 bytes**.

Maximum Transmission Unit (MTU):



Carrier Sense Multiple Access (CSMA):

- MAC protocol designed to **reduce network collisions**.
- Collisions slow performance due to retransmissions.
- Device **listens for a carrier signal** before transmitting.
- If another transmission is detected, it **waits until the channel is clear**.

Two types of **Carrier Sense Multiple Access (CSMA):**

CSMA/CD (Collision Detection):	**CSMA/CA (Collision Avoidance):**
• Used on **wired networks** (e.g., Ethernet). • Detects collisions and sends a **jam signal** to stop transmissions.	• Used on **wireless networks**. • Avoids collisions using **RTS (Request to Send)** and **CTS (Clear to Send)** signals before sending data.

7.2 Network traffic

- Bandwidth management technique that **controls and prioritizes traffic flow**.
- Ensures **high-priority traffic** moves before lower-priority traffic.

Traffic shaping

- **Quality of Service (QoS):** Layer 3; prioritizes traffic for resource-intensive applications.
- **Class of Service (CoS):** Layer 2; prioritizes traffic by group (e.g., **VoIP > HTTP**).

VPN (Virtual Private Network):

- A tunneling protocol that encrypts data for secure transmission.
- Commonly used due to its **ease of use and security benefits**.

- **Full Tunnel:**
  - **All traffic** is routed and encrypted through the VPN.
  - **Most secure** option—protects all network communication.
  - Recommended for handling **confidential data**.
- **Split Tunnel:**
  - Only **non-internet traffic** goes through the VPN.
  - **Internet traffic** (e.g., Google, Yahoo) bypasses the VPN.
  - Useful for accessing **local and remote resources simultaneously**, but **less secure**.

VPN Demo

Network Loop (Layer 2 / Bridge Loop):

Occurs when **multiple paths** exist between two network endpoints.

Happens at the **data link layer (Layer 2)**.

Example: Two hosts connected by more than one switch path.

Spanning-Tree Protocol

Spanning Tree Protocol (STP) is a **loop-prevention** network protocol that allows for redundancy while creating a loop-free Layer 2 topology.

STP **logically** blocks physical loops in a Layer 2 network, preventing frames from circling the network forever.

Spanning-Tree Protocol

Bridge Protocol Data Unit (BPDU):

Packets exchanged between switches to **detect network loops**.

Used by **Spanning Tree Protocol (STP)** to build a **loop-free topology**.

Only switches should send BPDUs; **end devices** should not.

Security Risk:

Attackers can inject **malicious BPDUs** to alter the STP topology.

This manipulation can **redirect or disrupt Layer 2 traffic**.

BPDU Guard:

Prevents BPDUs from entering switch ports connected to end devices.

Protects STP topology from BPDU-based attacks.

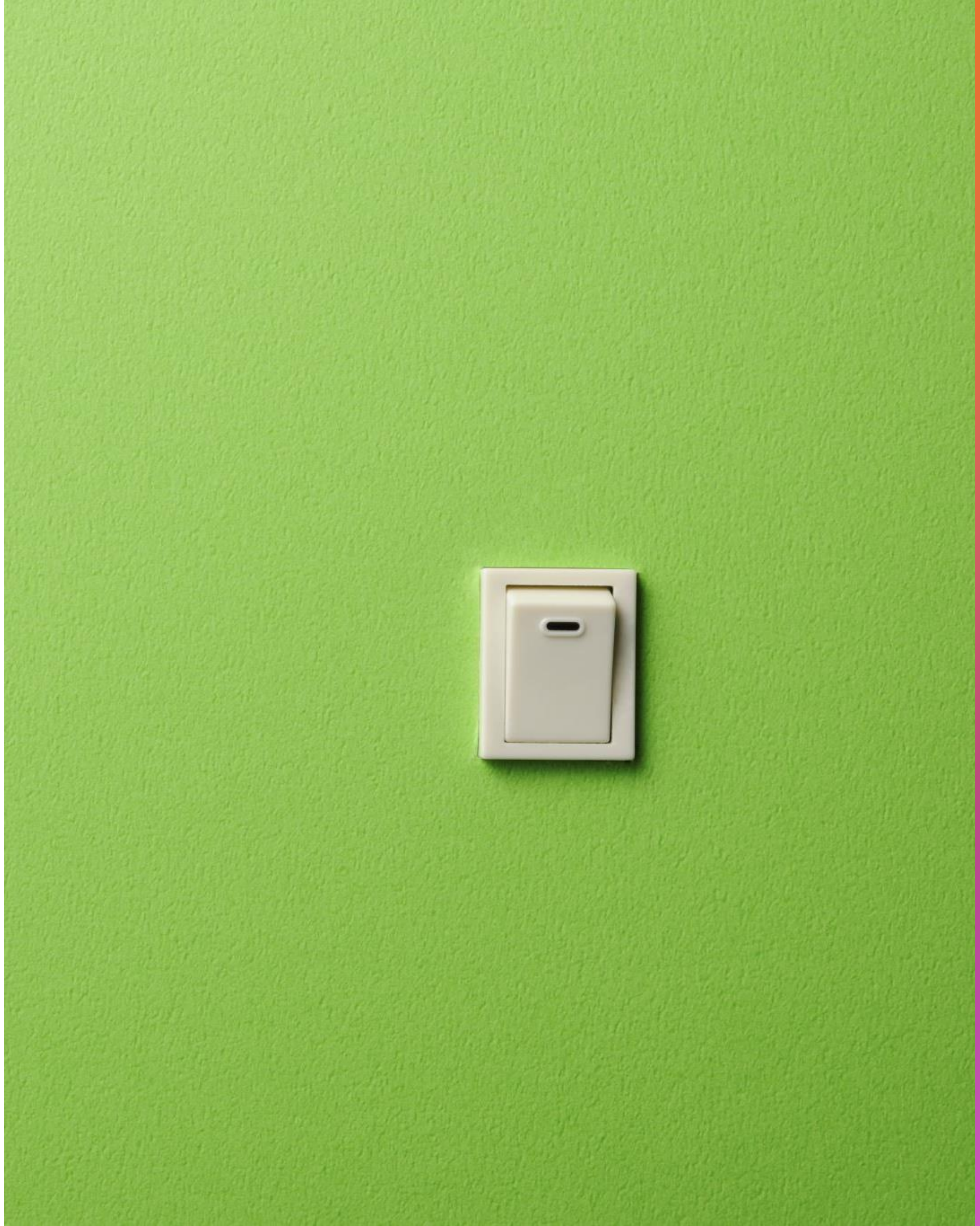
Spanning-Tree Operations

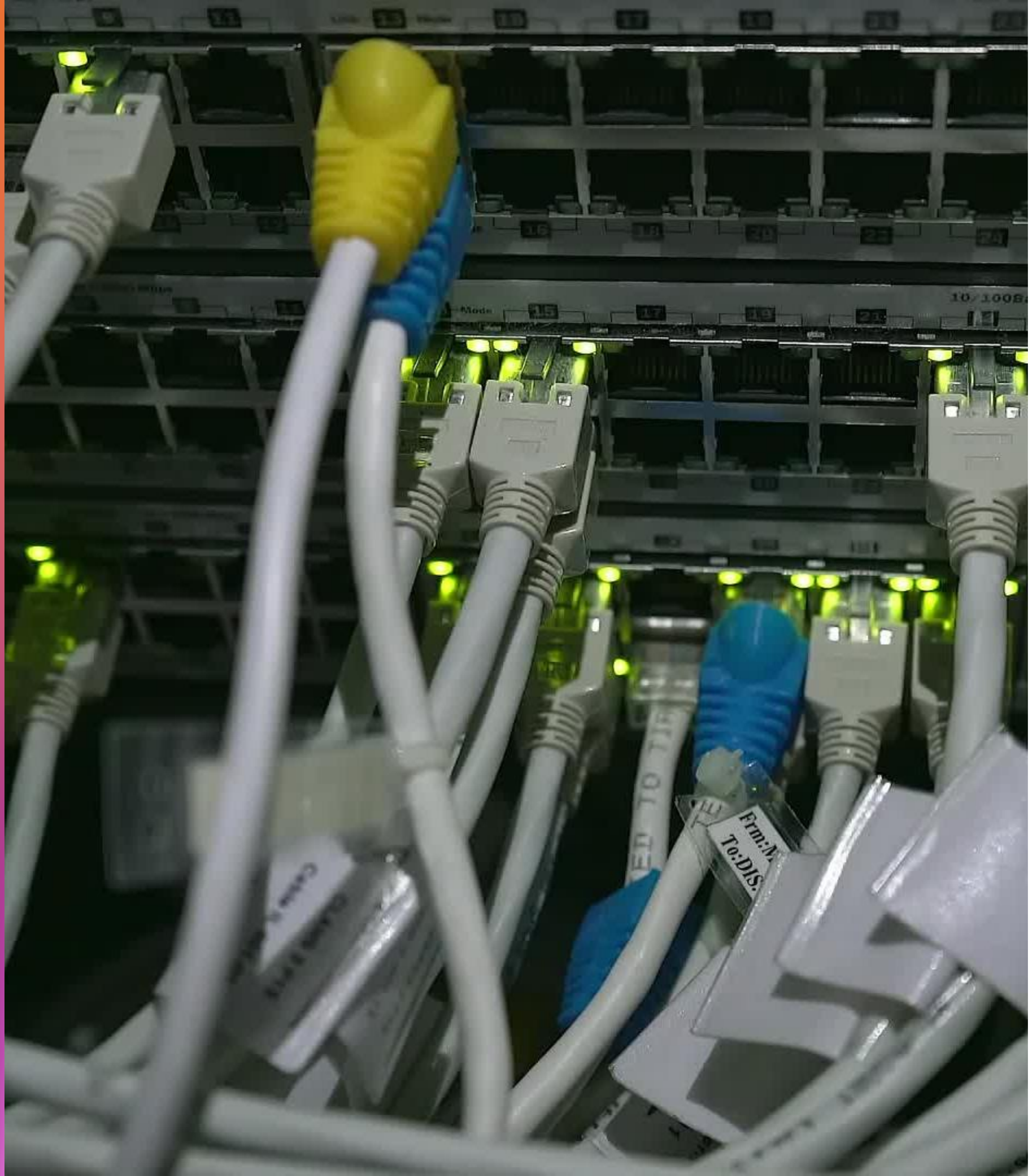
Using the Spanning Tree Algorithm (STA), Spanning tree process (STP) builds a loop-free topology in a four-step process:

1. Elect the root **bridge**.
2. Elect the root **ports**.
3. Elect **designated** ports.
4. Elect **alternate** (blocked) ports.

Spanning-Tree Demo

7.3 Switch features





Network Switch:

  - Acts as a **multiport bridge** using **packet switching**.
  - Forwards packets based on **MAC addresses**.
  - Ports can be **access**, **trunk**, or **hybrid**.
- **Switch Port:**
  - Each port is **individually configurable** to suit connected devices.

Common Switchport configurations

Speed	Speed – Defines data rate (e.g., 100 Mbps, 1 Gbps).
Duplex	Duplex – Sets half or full duplex communication.
Flow	Flow Control – Manages congestion and packet loss.
Port	Port Security – Limits access based on MAC addresses.
Port	Port Aggregation – Combines multiple ports for higher bandwidth.
Port	Port Mirroring - Switch feature that copies traffic from one or more ports to another port.

Tagged and untagged ports

Tagged Port (Trunk Port):

- Carries traffic from **multiple VLANs**.
- Uses **802.1Q (Dot1Q)** encapsulation to insert a **4-byte VLAN tag** into Ethernet frames.
- Allows VLAN traffic to travel between switches.

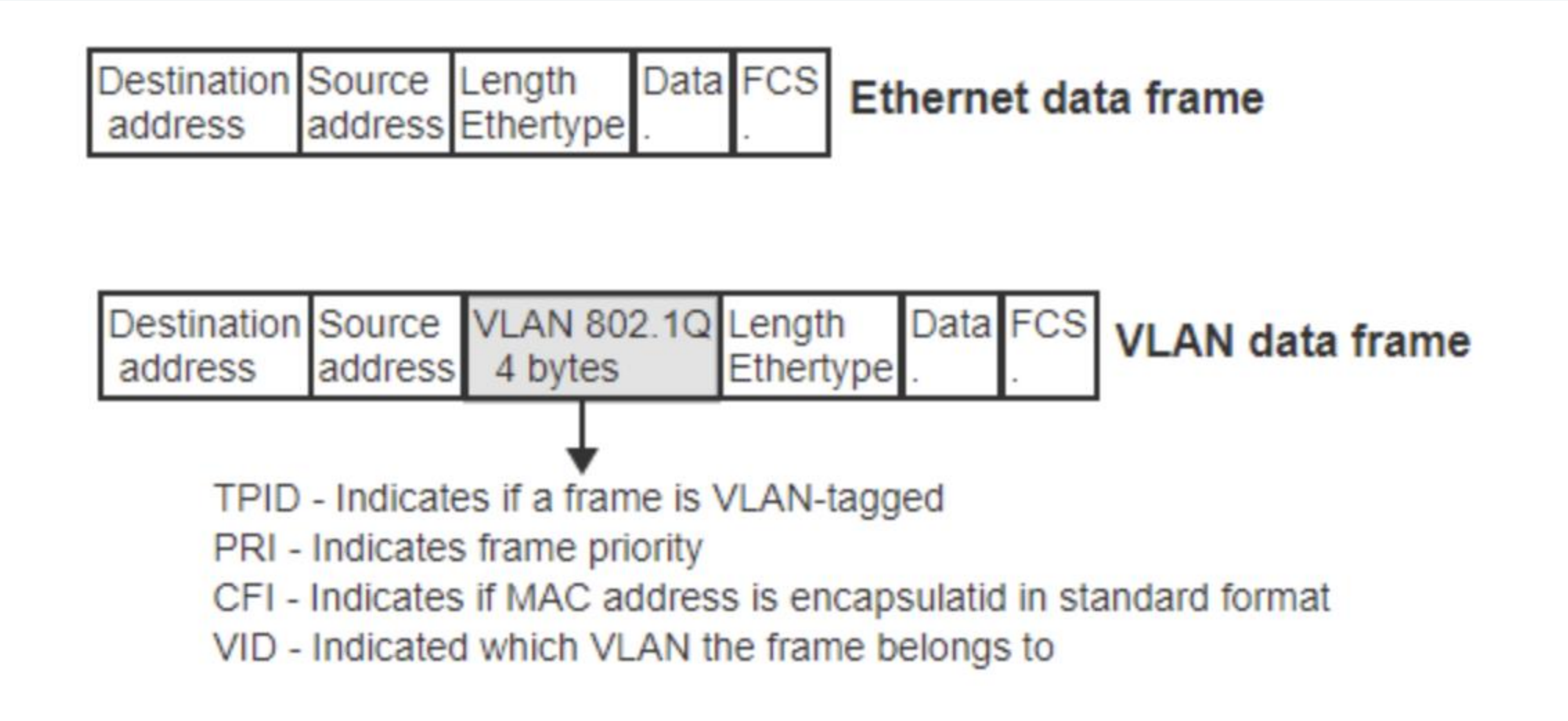
Untagged Port (Access Port):

- Carries traffic from **a single VLAN**.
- Typically connects to **end devices** (e.g., PCs, printers).

Native VLAN:

- Used to handle **untagged frames** from legacy or non-VLAN-aware devices.
- Should be an **unused VLAN** for security and isolation.

Tagging traffic



7.4 Switch configuration

- Power over Ethernet (PoE)
- Tagged ports
- VLAN tunneling
- Port duplex
- Port speed
- Auto medium dependent interface (MDI)/medium dependent interface crossover (MDI-X) port feature

Power over Ethernet (PoE)

Power over Ethernet (PoE):

- Delivers **power and data** over the same Ethernet cable.
- Provided by **PoE-enabled switches** or **add-on modules**.
- Eliminates the need for separate power outlets, offering **flexibility and cost savings**.

Common PoE Devices:

- **Wireless access points** (with antennas)
- **Security cameras**
- **VoIP phones**

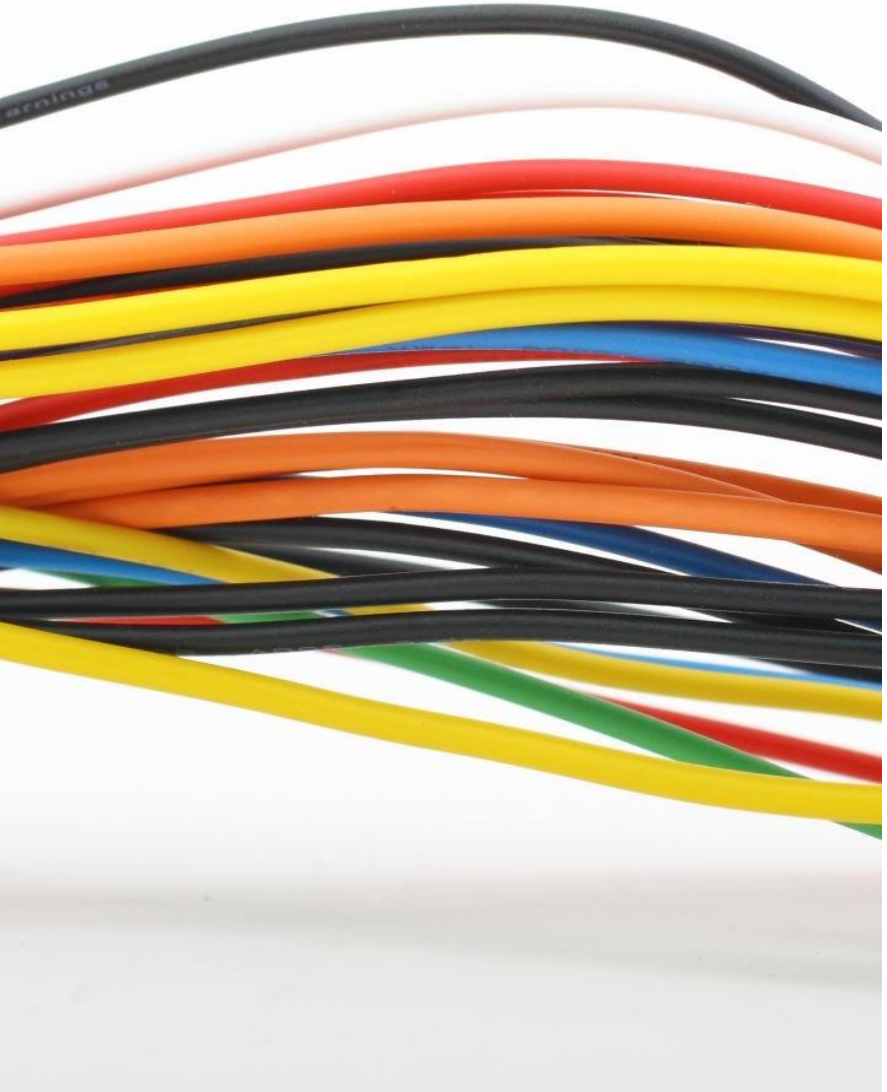
Power over Ethernet Plus (PoE+):

Power over Ethernet Plus (PoE+):	Enhanced version of PoE with **higher power capacity**. Provides up to **30 watts** per port for high-power devices. **PoE++** extends power beyond 30 W for devices like **TVs and laptops**.
Common PoE+ Devices:	**Wireless access points** (four or more antennas) **Pan/tilt/zoom security cameras** **Video IP phones** **Alarm systems**

Table 7.4.1: IEEE PoE and PoE+ standards.

Table 7.4.1: IEEE PoE and PoE+ standards.

IEEE standard	Maximum power rating	Device power available	Supported cable
802.3af Type 1 - PoE	15.4 W	12.95 W	CAT3 and above
802.3at Type 2 - PoE+	30 W	25.5 W	CAT5 and above
802.3bt Type 3 - 4PPoE/PoE++	60 W	51 W	CAT5 and above
802.3bt Type 4 - 4PPoE/ PoE++/UPoE	100 W	71 W	CAT5 and above



Auto-MDI-X.

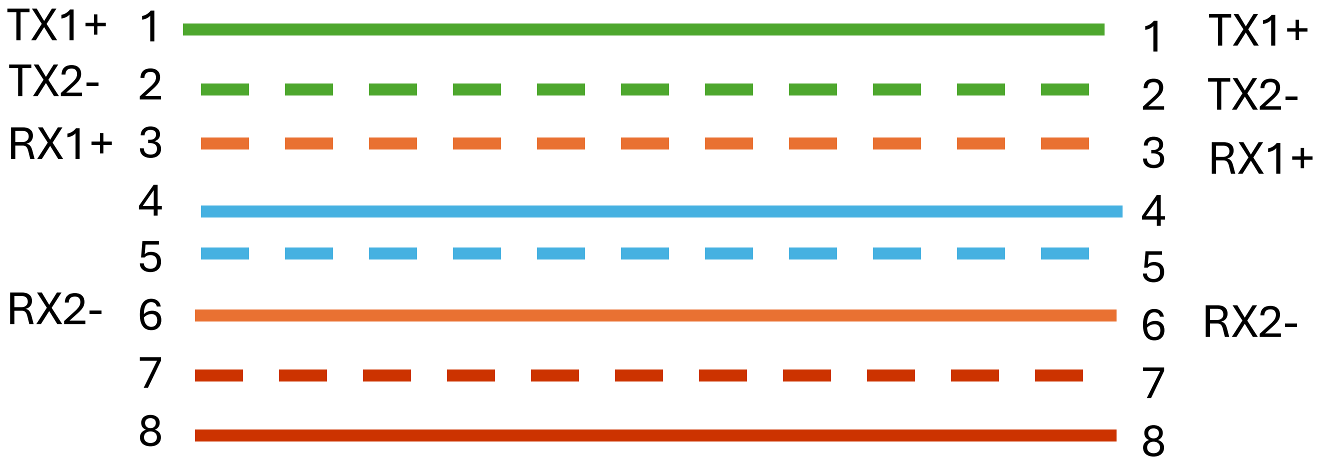
Auto-MDI-X configures the cable connection automatically, eliminating the need for a crossover cable. A straight thru cable connects a MDI to MDI-X port connection, or a MDI-X to MDI-X. A crossover cable is used for a MDI to MDI port connection.

Straight Through cable with Like devices

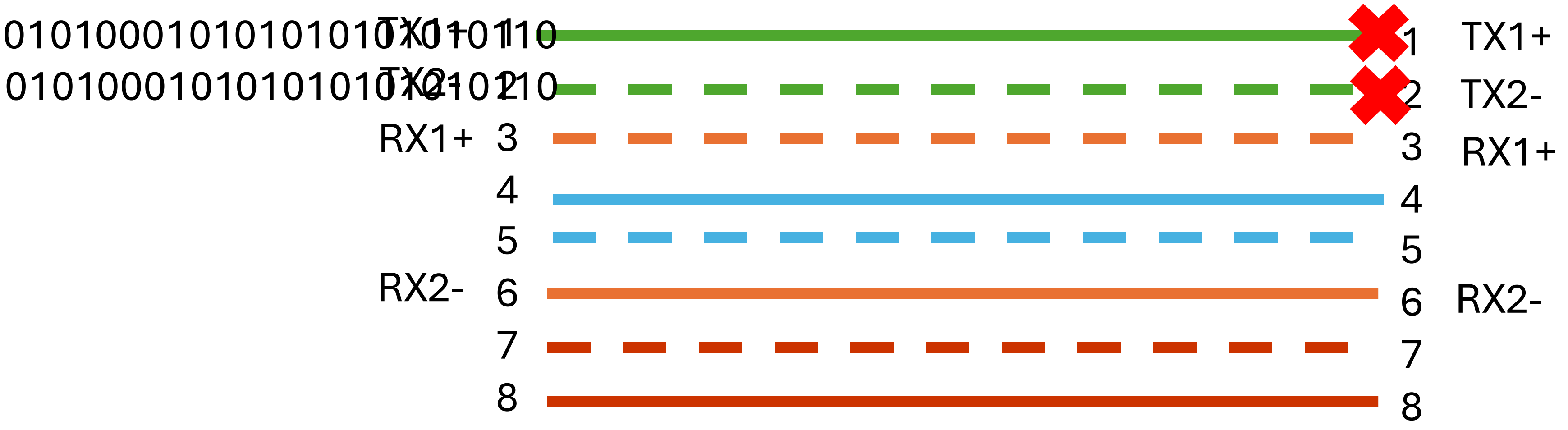
Switches use Pin

1 and 2 Transmit

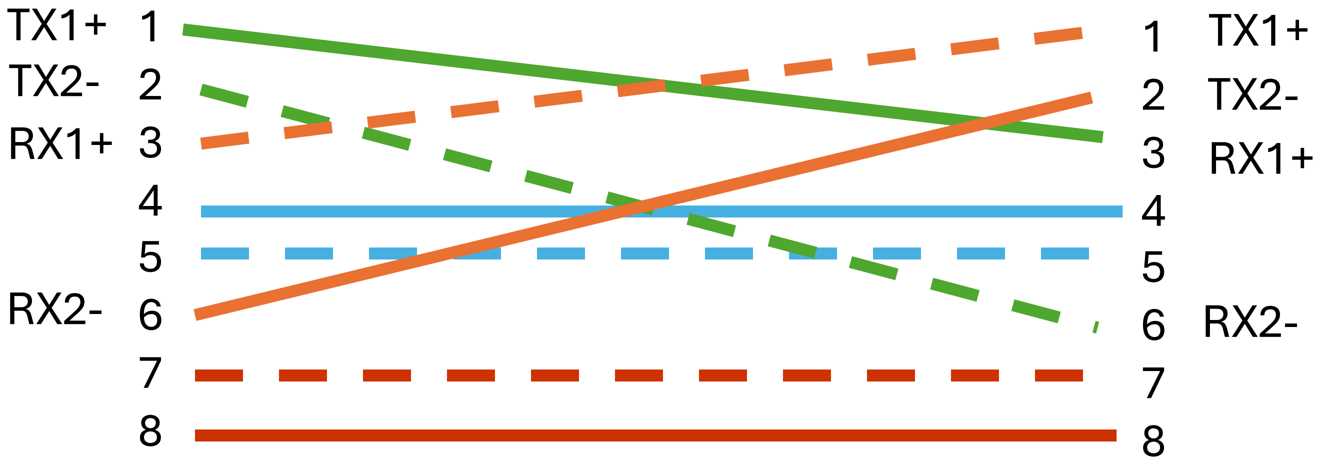
3 and 6 Receive



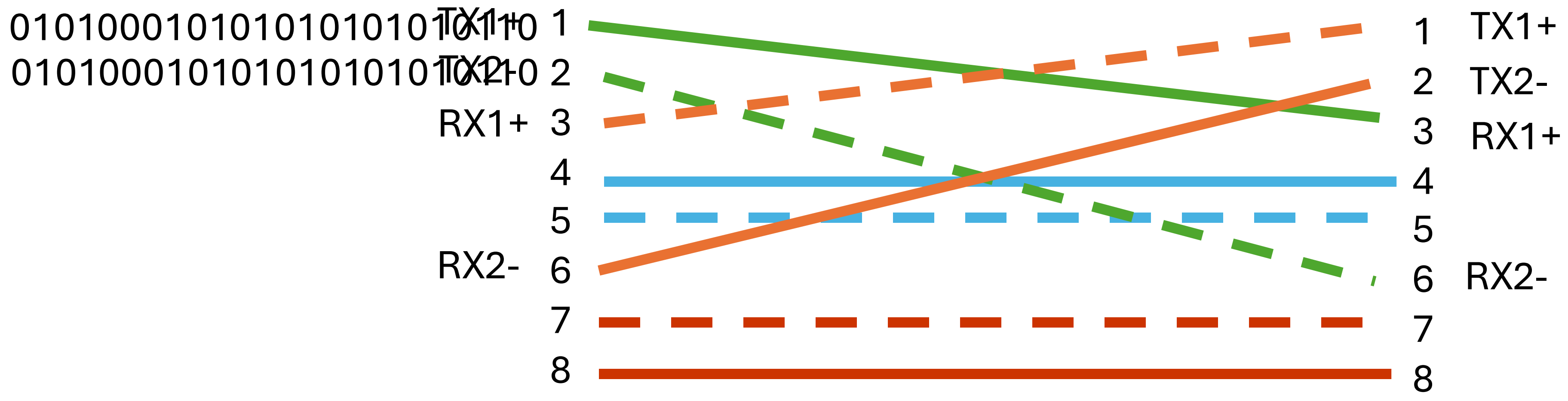
Straight Through cable with Like devices



Crossover cable with Like devices

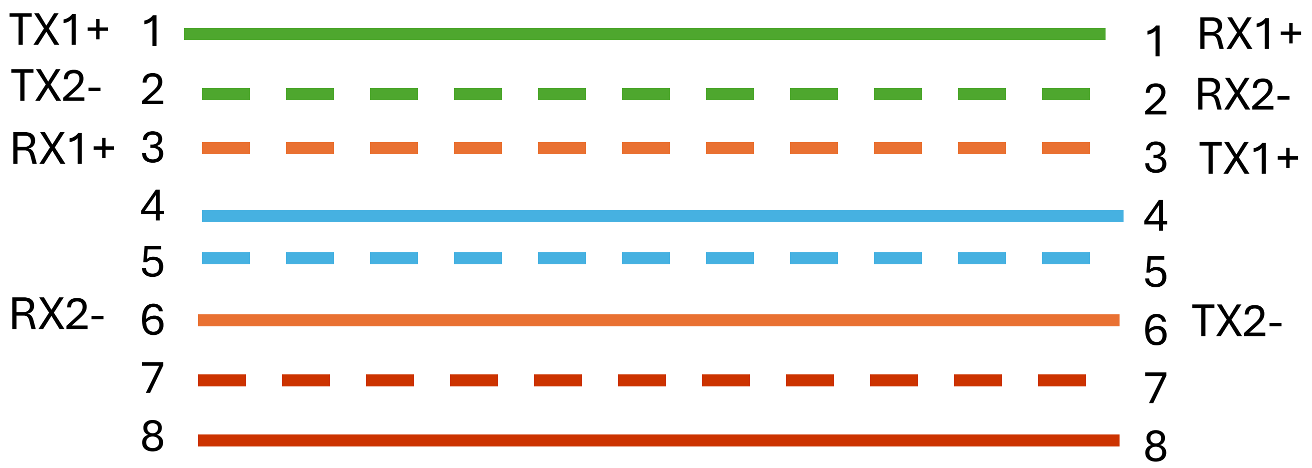


Crossover cable with Like devices



Dislike devices

Switches

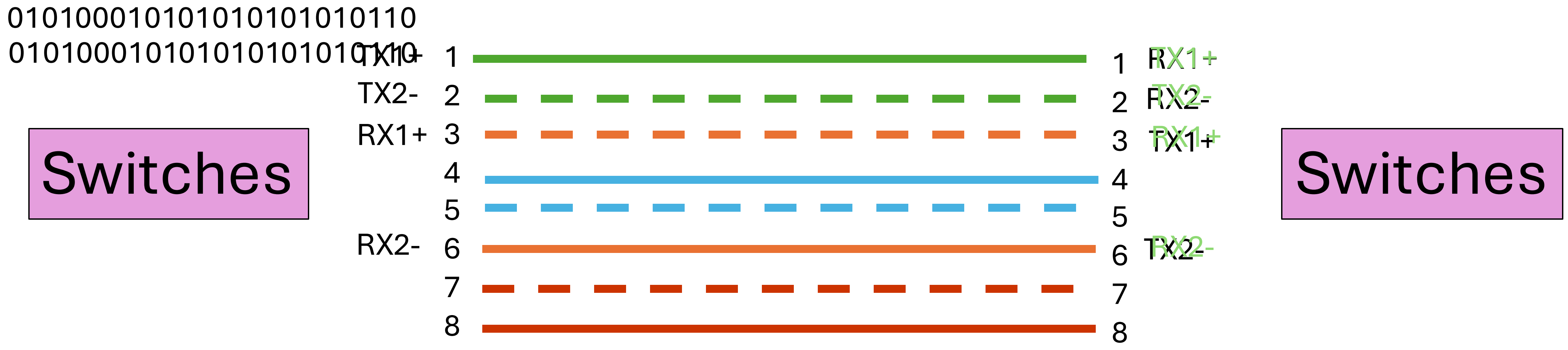


Routers
PCs
Hubs
Access Points

Switches use Pin
1 and 2 Transmit
3 and 6 Receive

Everything else
3 and 6 Transmit
1 and 2 Receive

Auto MDIX



0101000101010101010110
0101000101010101010110
Switches
TX1+
TX2-
RX1+
RX2-
1
2
3
4
5
6
7
8
1
2
3
4
5
6
7
8
RX1+
RX2-
TX1+
TX2-
TX1+
TX2-
RX1+
RX2-
Switches

Link Aggregation Control Protocol (LACP)

- **Link Aggregation:**
  - Combines **multiple physical links** into one for **higher bandwidth** and **redundancy**.
  - Commonly used between **switches, servers, NAS devices, or multi-port access points**.

- **Logical Aggregation Group (LAG):**
  - The **single logical channel** formed by combining multiple physical connections.

- **Link Aggregation Control Protocol (LACP):**
  - Defined by **IEEE 802.3ad**.
  - Provides a **standardized negotiation method** for forming and managing LAGs.

- **LACP Concepts:**
  - **System Priority:** Determines the order devices select active interfaces for aggregation.
  - **Interface Priority:** Assigns values to select which interfaces are active (lower = higher priority).
  - **LACP Mode (M:N):** Specifies **M active** and **N backup links** for **reliability and load balancing**.

LACP Demo

7.5 VLANs

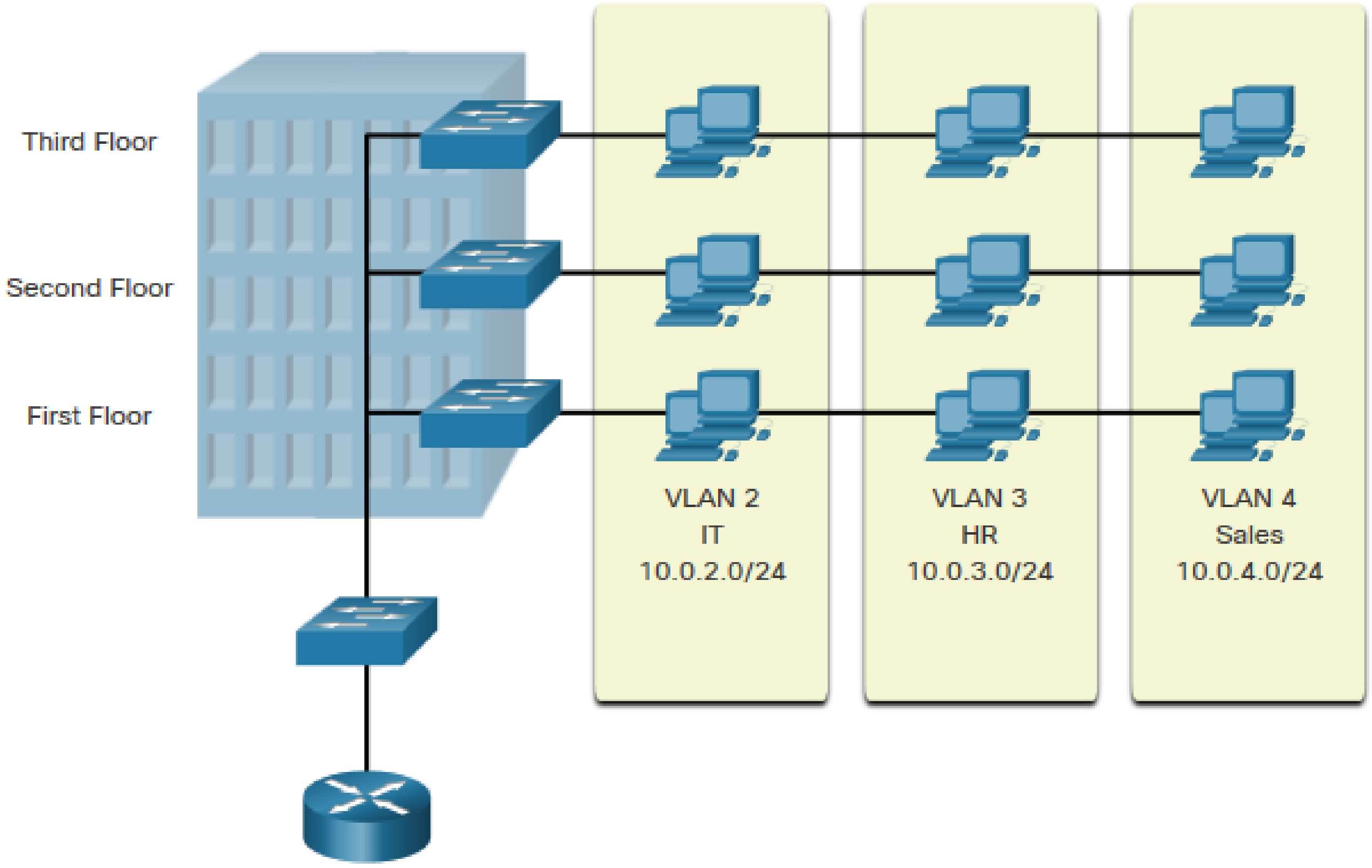
Provides **logical segmentation** of a network independent of physical layout.

Enhances **access control** and **network performance**.

Allows grouping by **department or resource needs**.

Use Case Example:

- Multi-floor office with departments spread across floors.
- Physical layout no longer matches departmental organization.
- Accounting users on different floors need access to accounting resources only.



VLAN Benefits:

Creates multiple broadcast domains to reduce traffic.

Limits broadcast traffic within and between VLANs.

Groups users logically by department, not location.

Maintains consistent access control across the network.

VLAN Demo

VLAN membership types

Port-based VLAN (Static VLAN):

- Assigns a VLAN to a **specific switch port**.
- The host connected to that port automatically joins the VLAN.

MAC-based VLAN:

- Assigns VLAN membership based on the device's **MAC address**.
- Allows VLAN assignment regardless of the physical switch port used.

Protocol-based VLAN:

- Uses **network protocol types** (e.g., IPv4, IPv6) to assign VLAN membership.
- Enables traffic separation based on **protocol** rather than hardware or port.

Table 7.5.1: Membership types.

Membership type	OSI layer	Description
Port	Layer 1	Membership is defined by a switch port VLAN number.
MAC address	Layer 2	Membership is defined by MAC address.
Protocol type	Layer 3	Membership is defined by the network IP subnet address.

VLAN connection types

VLAN-aware Device:

Understands VLAN tags and membership information.

VLAN-unaware Device:

Does **not recognize VLAN tags** or VLAN formats.

VLAN Connection Types:

Trunk Line: Connects only **VLAN-aware devices**; carries traffic for multiple VLANs.

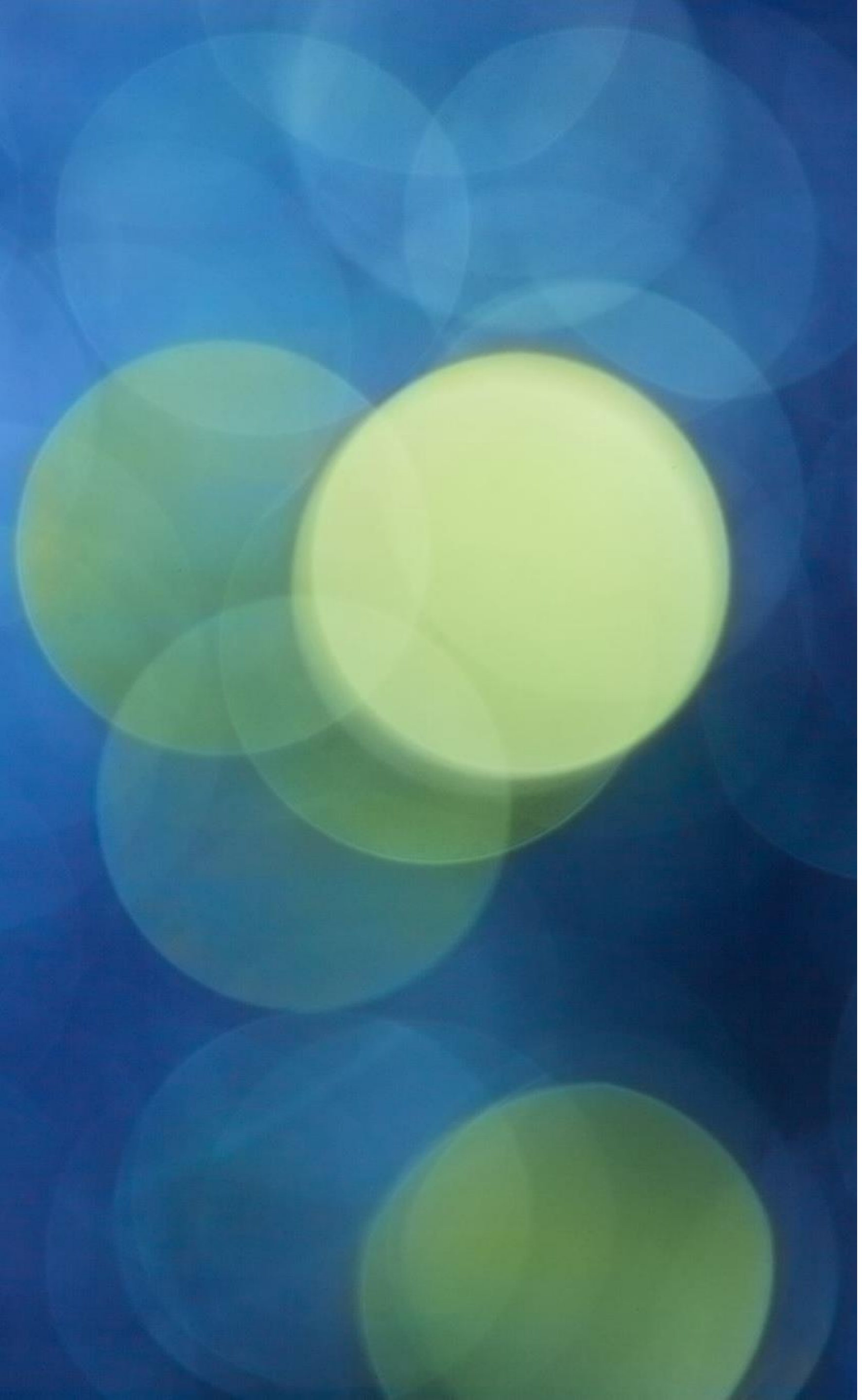
Access Link: Connects a **VLAN-unaware device** to a VLAN-aware port; carries one VLAN.

Hybrid Link: Combines trunk and access features; supports **both VLAN-aware and VLAN-unaware devices**.

Spanning Tree Demo

7.6 VLAN design and configuration

- **VLAN Advantages:**
  - Improves **network performance** and **administration**.
  - Enhances **resource access control** and segmentation.
- **Requirements and Costs:**
  - **Layer 3 device** (router or Layer 3 switch) needed for inter-VLAN communication.
  - **Additional hardware and configuration** increase deployment cost.
- **Security Considerations:**
  - VLAN devices (e.g., routers) can become **attack targets**.
- **VLAN-specific threats:**
  - **VLAN Hopping:** Attacker moves from one VLAN to another via a breached VLAN.
  - **Switch Spoofing:** Attacker pretends to be a trunking switch to access multiple VLANs.
  - **Double-Tagging:** Attacker inserts **two VLAN tags** to bypass VLAN protections.
- **Key Takeaway:**
  - VLAN deployment improves efficiency but requires **careful security and cost planning**.



VLAN security

VLAN Security Purpose:

- Creates **virtual boundaries** to prevent unauthorized access.
- **Segments sensitive devices** and data for better isolation.
- Provides **protocol separation**, limiting traffic to specific VLANs.
- Extends security to **wireless devices**, maintaining consistent policies.

Key Point:

True VLAN security depends on **following best practices**, not just configuration.

Best practice	Justification
Assign one VLAN per access port	An access port should only carry traffic for a single VLAN
Exclude all other VLANs from an access port	Ensures a single VLAN uses an access port
Configure an access port as untagged	Mitigates double-tagging
Exclude unwanted VLANs from a trunk port	Unwanted VLANs should not traverse a trunk port
Configure a trunk port as tagged for all VLANs except one	Tagging ensures traffic reaches the correct VLANs - only the native VLAN receives untagged traffic
Configure a management VLAN	Segregates user traffic from administrative traffic
Do not use VLAN 1	VLAN 1 is a preconfigured VLAN an attacker can exploit
Assign all ports to at least one VLAN	Unused ports can be exploited
Supplement VLAN routing with an access control list (ACL)	Provides an additional layer of packet filtering, limiting unwanted traffic
Assign the correct VLAN type to a port	Improves both performance and security

Table 7.6.1: VLAN security best practices

VLAN switch configurations

Most VLAN switch configurations require five steps:

1. Enter configuration mode
2. Enter VLAN mode to create a VLAN or range of VLANs
3. Exit VLAN mode
4. Confirm VLAN/VLAN range creation
5. Save the VLAN configuration to the VLAN database

VLAN Router Configurations (Inter-VLAN Routing):

Enables communication **between VLANs.**

Method depends on device type and available interfaces.

Inter-VLAN Routing Methods:

One-Port-Per-VLAN: Each VLAN connects to a **dedicated physical router port**.

Router-on-a-Stick:

- Uses **one physical port** divided into **multiple subinterfaces**.
- Each subinterface handles a separate VLAN.

Layer 3 Switch (SVIs):

- Uses **Switched Virtual Interfaces (SVIs)** to route traffic between VLANs.

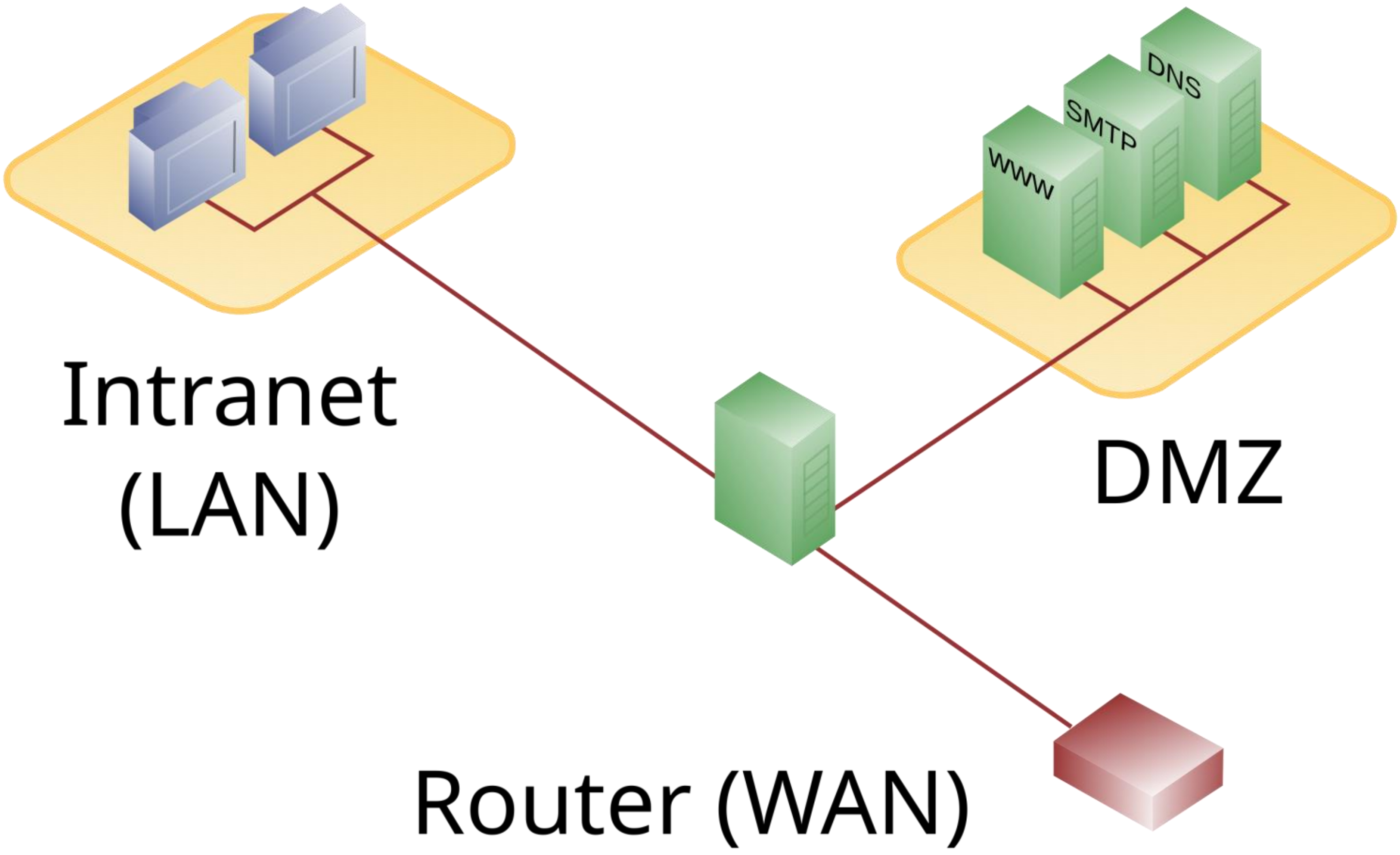
7.7 Security zones and IP support

Types of Security Zones:

- **Trusted Zone (Private Zone):**
  - Contains internal, authorized resources.
  - Resources **trust one another** (e.g., internal servers and clients).
- **Untrusted Zone (Public Zone):**
  - Contains resources **outside organizational control** (e.g., the internet).
  - Trusted zone resources **do not trust** untrusted zone resources.
- **Demilitarized Zone (DMZ / Screened Subnet):**
  - Sits **between trusted and untrusted zones**.
  - Hosts **public-facing resources** (e.g., web, email, DNS servers).
  - Protects the internal network from external threats.

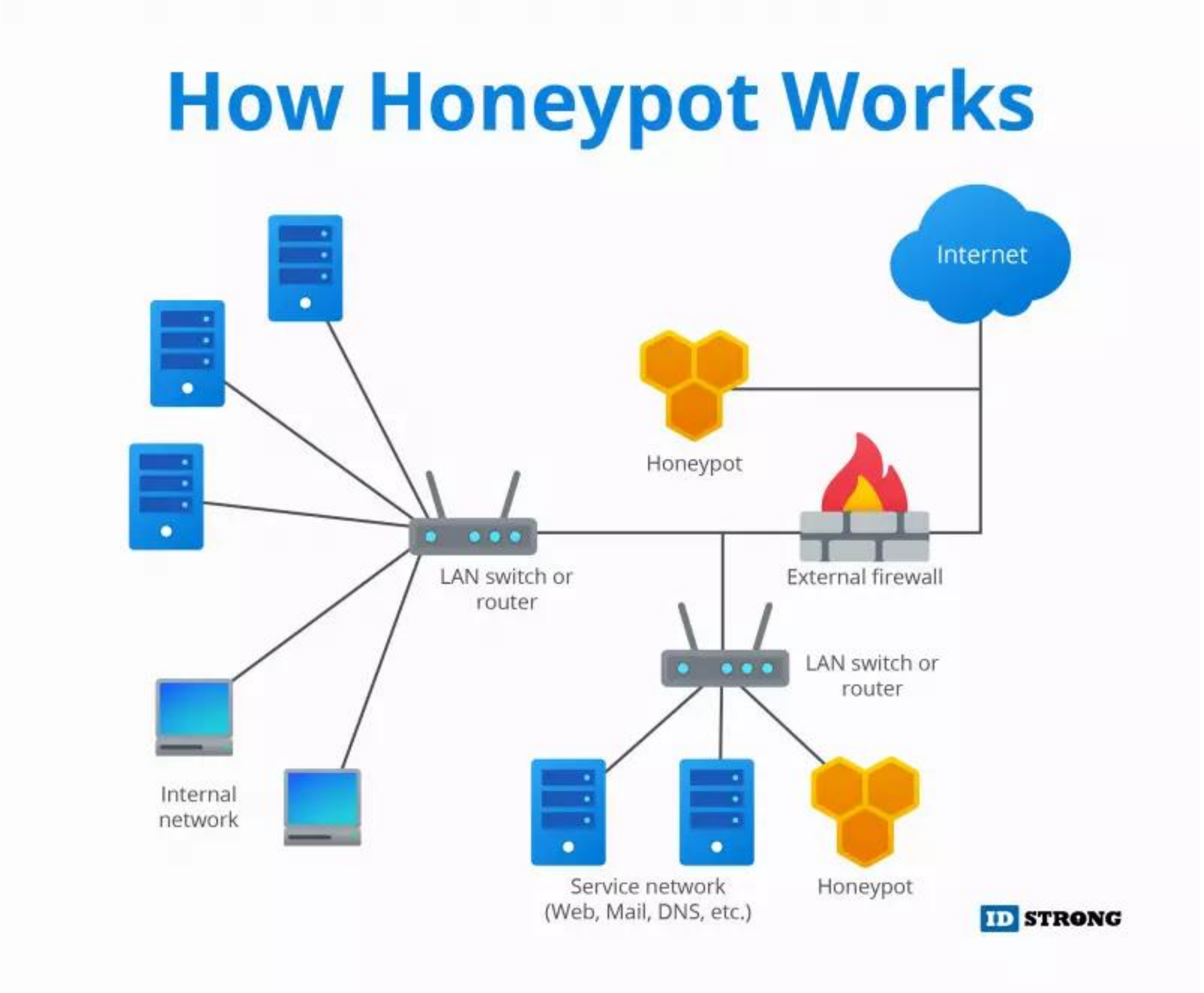
Demilitarized zone

- Sits **between trusted and untrusted zones**.
- Hosts **public-facing resources** (e.g., web, email, DNS servers).
- Protects the internal network from external threats.



Honeypot

- **Decoy system** placed in the DMZ to attract attackers.
- Collects data on attack methods to **strengthen network defenses**.



Zero Trust Network Architecture (ZTA):

- Also known as **perimeter-less security**.
- Based on the principle of **"never trust, always verify."**
- Assumes the network is **always compromised** with **internal and external threats**.
- **No automatic trust** is granted to any device or user.
- **Access control** is enforced **at every access attempt**, regardless of location or trust level.

Network Address Translation (NAT):

- Converts **private (inside)** IP addresses to **public (outside)** IP addresses.
- Operates at **OSI Layer 3**, typically on a **router or firewall**.
- Provides **security** and **IP address conservation** by masking internal devices.
- Commonly used in **homes and organizations** to share one public IP.

NAT Demo

Types of NAT:

Port Address Translation (PAT):

- Maps **multiple private devices** to one public IP using **unique port numbers**.
- Hides internal IPs for **added security**.

Static NAT (One-to-One):

- Permanently maps one private IP to one public IP.
- Entries remain in the **NAT table** until manually removed.

Dynamic NAT:

- Temporarily maps private IPs to available public IPs.
- **Mappings expire** after a timeout period.

Source NAT (SNAT):

- Translates **source IPs** (private → public).
- Most common form used for outbound internet access.

Dual stack

Why Run Dual Stack:

- Ensures **compatibility** during the transition from IPv4 to IPv6.
- Allows **IPv4 and IPv6 to operate simultaneously** without disruption.
- Supports communication with both **legacy IPv4** and **modern IPv6** networks.

Dual Stack Technology:

Dual Stack Technology:

- Enables devices and networks to **send and receive** both IPv4 and IPv6 packets.
- Used by ISPs to provide **seamless connectivity** during the migration period.
- Implemented on **routers, servers, firewalls, and other network equipment**.

Dual Stack Devices and Networks:

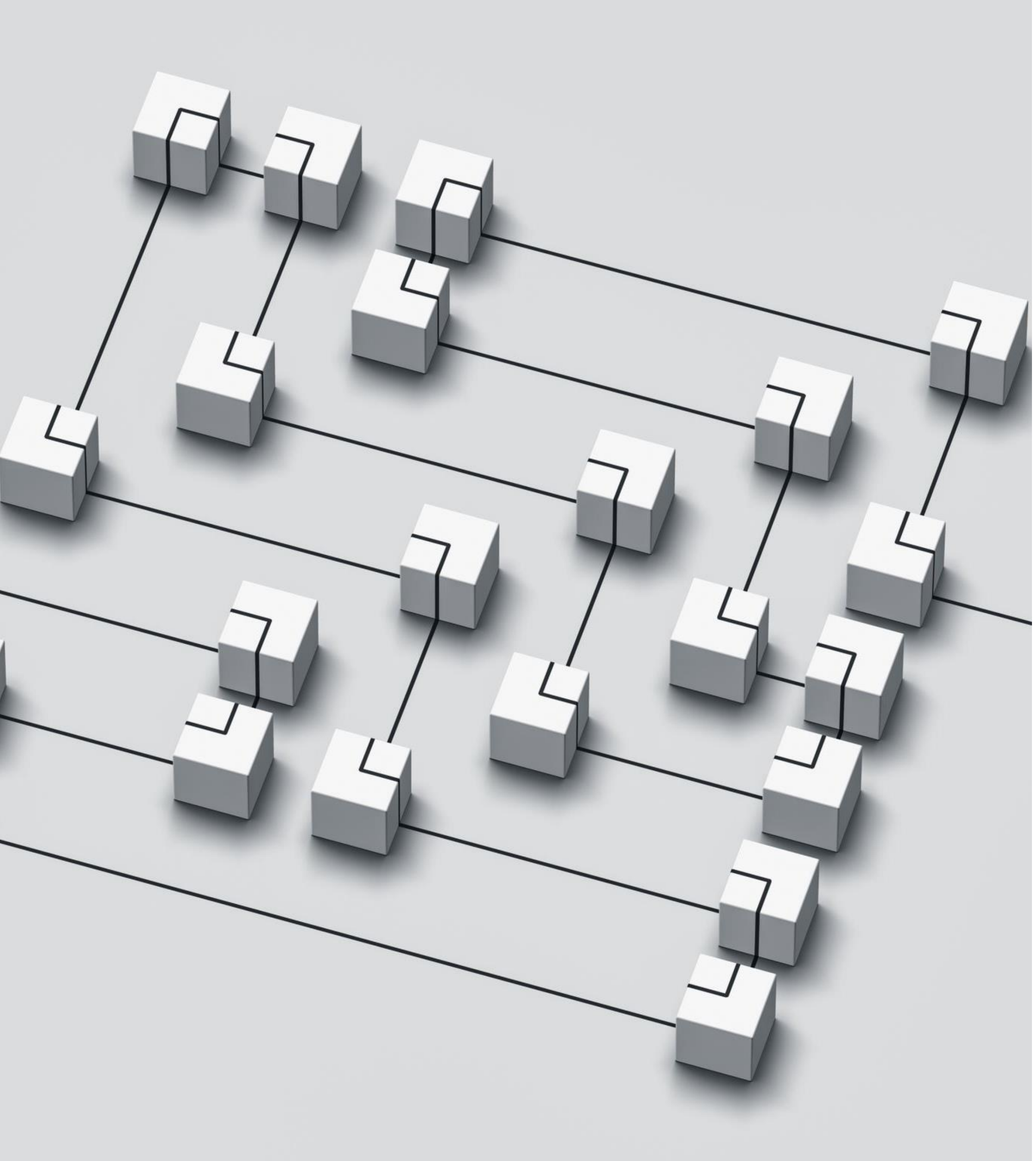
- **Dual-stack device:** Can process both IPv4 and IPv6 traffic at the same time.
- **Dual-stack network:** All devices understand and operate with both protocols concurrently.

7.8 Routers

Router basics

Router Purpose:

- Connects **two or more networks or subnetworks**.
- **Forwards packets** to their destination IP addresses.
- Allows multiple devices to share a **single internet connection**.
- Commonly connects a **LAN to a WAN**.



Router basics

Routing Table:

- Used to determine the **best path** for forwarding data.
- Default route destination: **0.0.0.0** (represents any network).

Router basics

Time to Live (TTL) / Hop Limit:

- Defines how long a packet can exist in the network before being discarded.
- **Decreases by 1** each time the packet passes a router.
- If TTL reaches **zero**, the packet is dropped to prevent endless looping.

Types of routers

Wireless Router:

- Connects to a **modem via Ethernet cable**.
- Creates a **WLAN (Wireless Local Area Network)** for multiple wireless devices.
- Provides **internet access** without physical cabling to end devices.

Wired Router:

- Connects to a **modem and network devices using Ethernet cables**.
- Creates a **LAN (Local Area Network)** through wired connections.
- Provides **reliable internet access** to connected devices.

Router Types and Functions:

- **Core Router:** Operates within the **backbone of a network**, managing high-speed data.
- **Edge Router:** Connects **internal networks to external networks** (e.g., ISPs).
- **Virtual Router:** Software-based; runs routing functions **without dedicated hardware**.

Table 7.8.1: Router types

Specialized router type	Characteristic
Edge router	Installed at the boundaries of a network. Distributes packets across multiple networks.
Core router	Distributes packets within the same network rather than across multiple networks.
VPN router	Is a normal router with VPN client software installed. Every VPN connected device is protected by the VPN.

Routing Function:

Builds a **map of the network** using **static or dynamic routing**.

Static Routing: Manually configured; does **not adapt** to network changes.

Dynamic Routing: Uses **protocols** to automatically share topology updates with other routers.

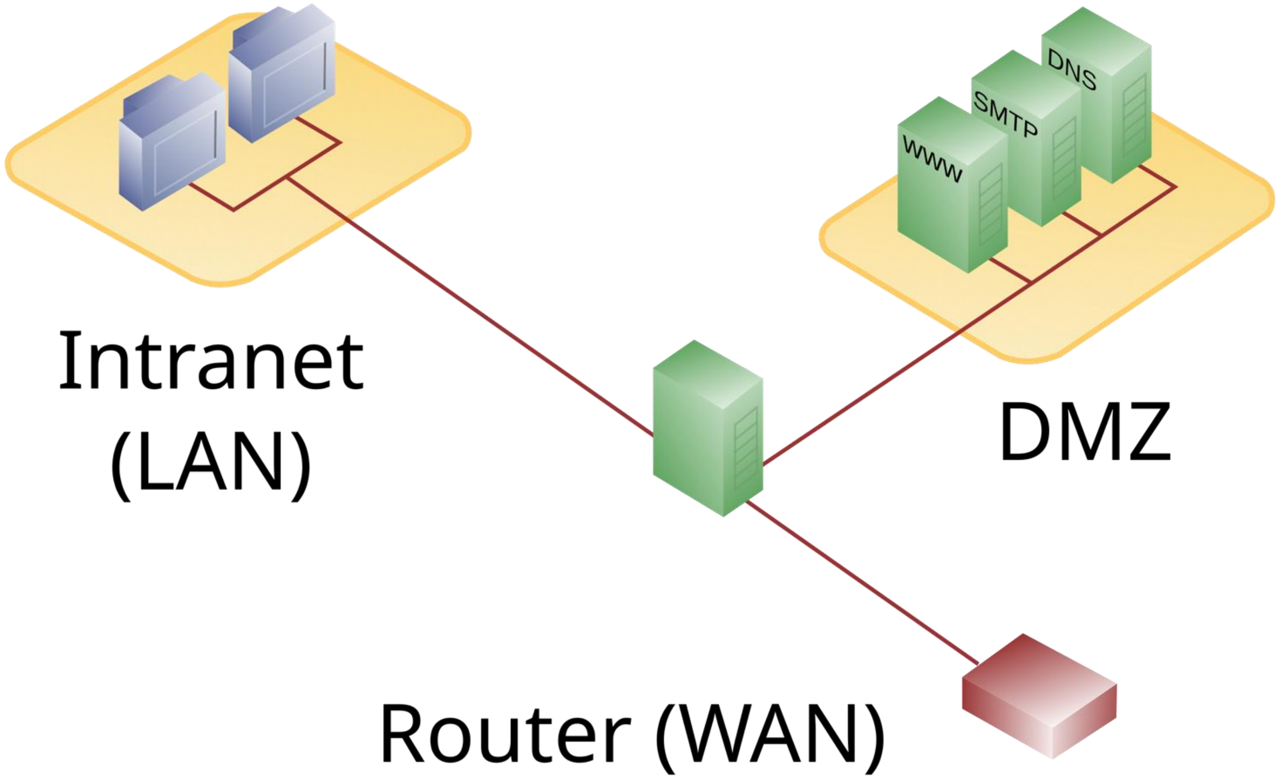
Both methods populate the **routing table**, which guides packet forwarding.

Router Advertisement (RA):

- Broadcasts a router's **IP address** on the local network.
- Helps hosts **discover available routers** automatically.
- **Security Risk:** Rogue RAs can redirect traffic to a malicious device.
- **RA Guard:** Blocks or rejects **unauthorized RA transmissions** to prevent spoofing attacks.

Access Control List (ACL): security

- A set of filtering rules used by routers, switches, and firewalls.
- Determines whether network traffic is allowed or denied.
- Evaluates packets based on IP address, protocol, or port number.
- Used to enhance security, control access, and manage traffic flow.



ACL Types:

Standard ACL: Filters traffic based only on the **source IP address.**

Extended ACL: Filters traffic using **source and destination IPs**, **ports**, and **protocols.**

Chapter 7: Switches and Routers

Chapter 14: Network Troubleshooting

Chapter 10: Wireless Networking

Chapter 11: Network Services

Chapter 12: Network Architecture

Chapter 13: Network Operations

Chapter 13: Network Troubleshooting