حوضي من عدن ... إلى عمان البلقاء

جامعة البلقاء التطبيقية

Al Balqa Applied University

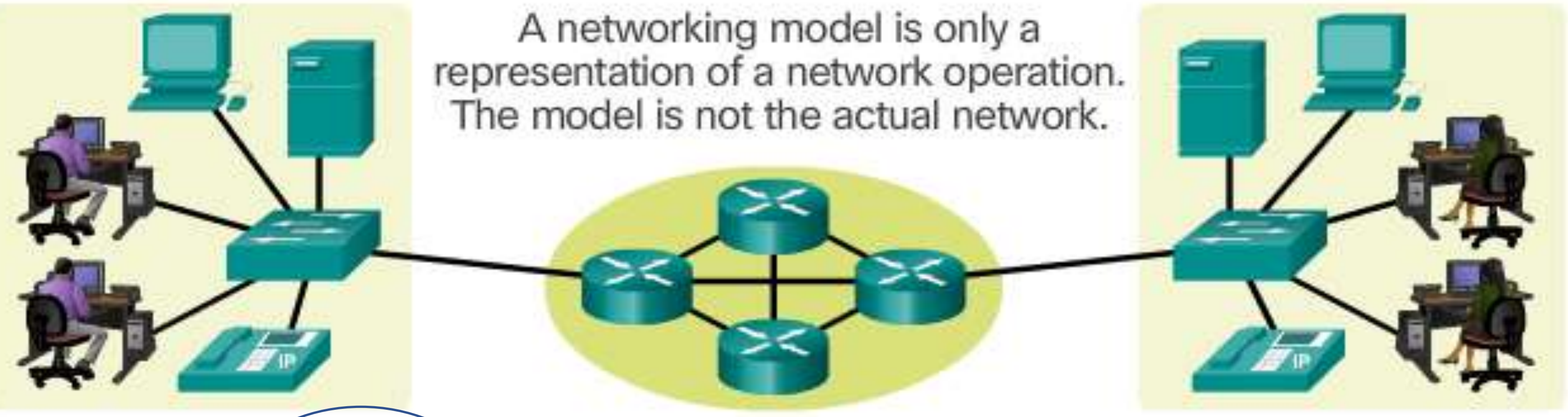
Computer Networks Protocols

Network Protocol

A protocol is a set of rules that governs the communications between computers on a network. These rules include guidelines that regulate the following characteristics of a network: access method, allowed physical topologies, types of cabling, and speed of data transfer.

What is a Protocol?

- Protocol is a controlled sequence of messages that is exchanged between two or more systems to accomplish a given task.
- Protocol specifications define this sequence together with the **format or layout** of the messages that are exchanged.



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	PPP, Frame Relay, Ethernet	Network Access
Physical		

Protocol development

For communication to take place, protocols have to be agreed upon. Recall that in digital computing systems, the rules can be expressed by algorithms and data structures, raising the opportunity of hardware independence. Expressing the algorithms in a portable programming language, makes the protocol software operating system independent. The source code could be considered a protocol specification. This form of specification, however is not suitable for the parties involved.

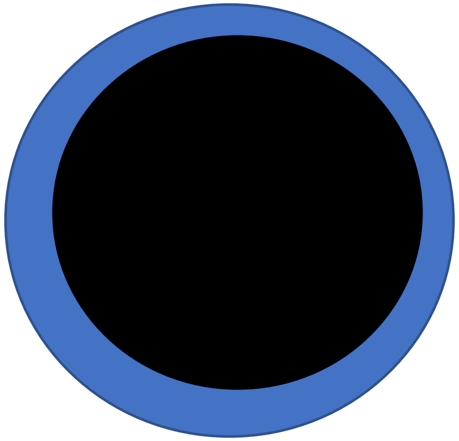
Common types of protocols

The Internet Protocol is used in concert with other protocols within the Internet Protocol Suite. Prominent members of which include:

- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Internet Control Message Protocol (ICMP)
- Hypertext Transfer Protocol (HTTP)
- Post Office Protocol (POP)
- File Transfer Protocol (FTP)
- Internet Message Access Protocol (IMAP)

•Types of Network Protocols

- ⍰ Ethernet
- ⍰ Local Talk
- ⍰ Token Ring
- ⍰ FDDI
- ⍰ ATM



Benefits

Communicating over a network is a complicated task. Different hardware elements in the network need to be informed of the process in hand and instructed in their role. Each element has its own requirements and a set format for receiving instructions. Both the sender and receiver must communicate in the same language and all connecting hardware and software must be able to exchange control information. The benefits of using network protocols are that all these tasks have already been mapped out by someone else, and they have published their knowledge for others to share.

Needs

 Human intercommunication (in pairs or larger groups) requires rules of conversation (do not speak if someone else is speaking) to function effectively.

 Computers are no different. Consider the following simplistic analogy:

 Therefore, we need regulations and rules to how we communicate over a computer network. For example to remote login (telnet), FTP or email.

 The set of rules and regulations is called a Protocol.

Functions

The function of protocols in a network and how each protocol works in one or more layers of the open systems interconnection (OSI) model, why protocols are needed to enable computer communications, and describe common protocol suites.

Objectives

 Appreciate the role of measurement in building and maintaining high-performance TCP/IP networks

 Explain the types of tools available for performance measurement

 Familiarize with freely available performance measurement and testing tools

 Select an appropriate tool for a given task

Advantages

1. Many computers from all the world can connect together, because they are using the international standard.
2. Easier maintenance and installation because you get used on the standard.

Disadvantages

1. Problems Occur in Standards, it will be international problem.
2. All companies and manufactures must follow the standards instead of developing new techniques.

CONCLUSION

While the age-old concept of the network is foundational in virtually all areas of society, Computer Networks and Protocols have forever changed the way humans will work, play, and communicate. Forging powerfully into areas of our lives that no one had expected, digital networking is further empowering us for the future. New protocols and standards will emerge, new applications will be conceived, and our lives will be further changed and enhanced

CONCLUSION

While the age-old concept of the network is foundational in virtually all areas of society, Computer Networks and Protocols have forever changed the way humans will work, play, and communicate. Forging powerfully into areas of our lives that no one had expected, digital networking is further empowering us for the future. New protocols and standards will emerge, new applications will be conceived, and our lives will be further changed and enhanced

CH2

The OSI Model

Why do we need the OSI Model?

- To address the problem of networks increasing in size and in number, the International Organization for Standardization (ISO) researched many network schemes and recognized that there was a need to create a network model

- This would help network builders implement networks that could communicate and work together

- ISO therefore, released the OSI reference model in 1984.

Don’t Get Confused.

ISO - International Organization for Standardization

OSI - Open System Interconnection

IOS - Internetwork Operating System

To avoid confusion, some people say “International Standard Organization.”

The OSI Reference Model

7 Application

6 Presentation

5 Session

4 Transport

3 Network

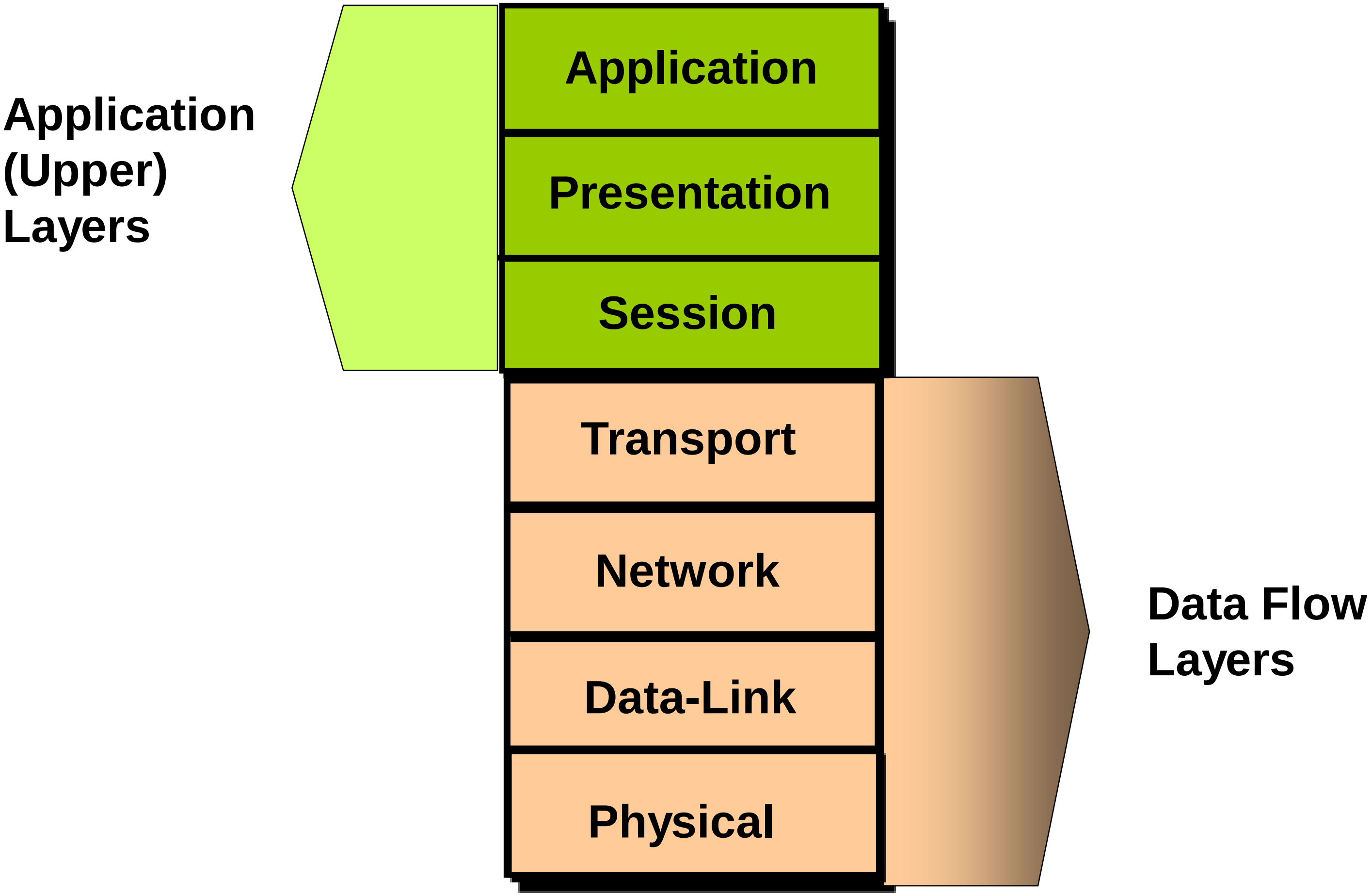
2 Data Link

1 Physical

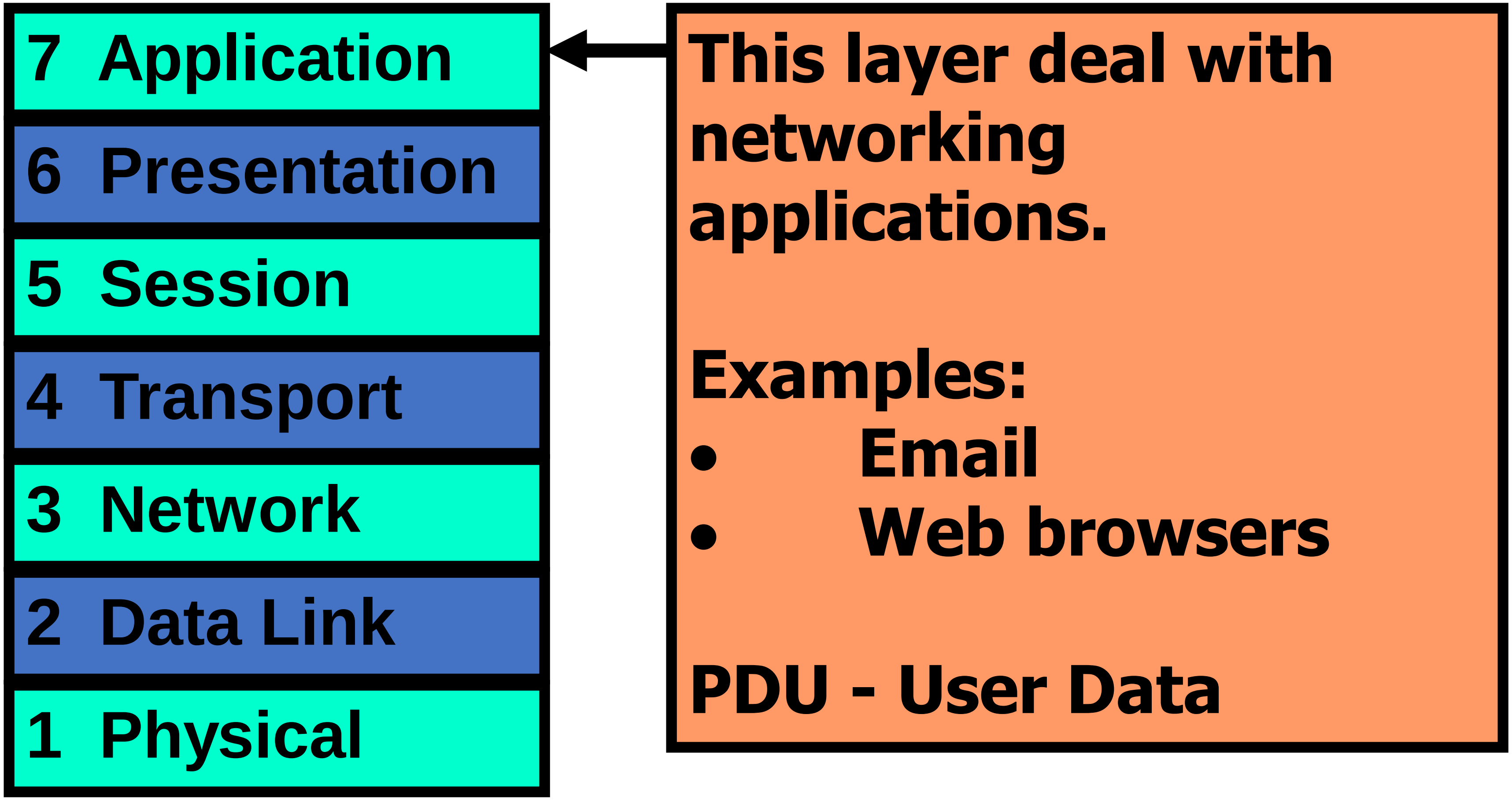
The OSI Model will be used throughout your entire networking career!

Memorize it!

OSI Model


Application
(Upper)
Layers
Application
Presentation
Session
Transport
Network
Data-Link
Physical
Data Flow
Layers

Layer 7 - The Application Layer



7 Application

6 Presentation

5 Session

4 Transport

3 Network

2 Data Link

1 Physical

This layer deal with networking applications.

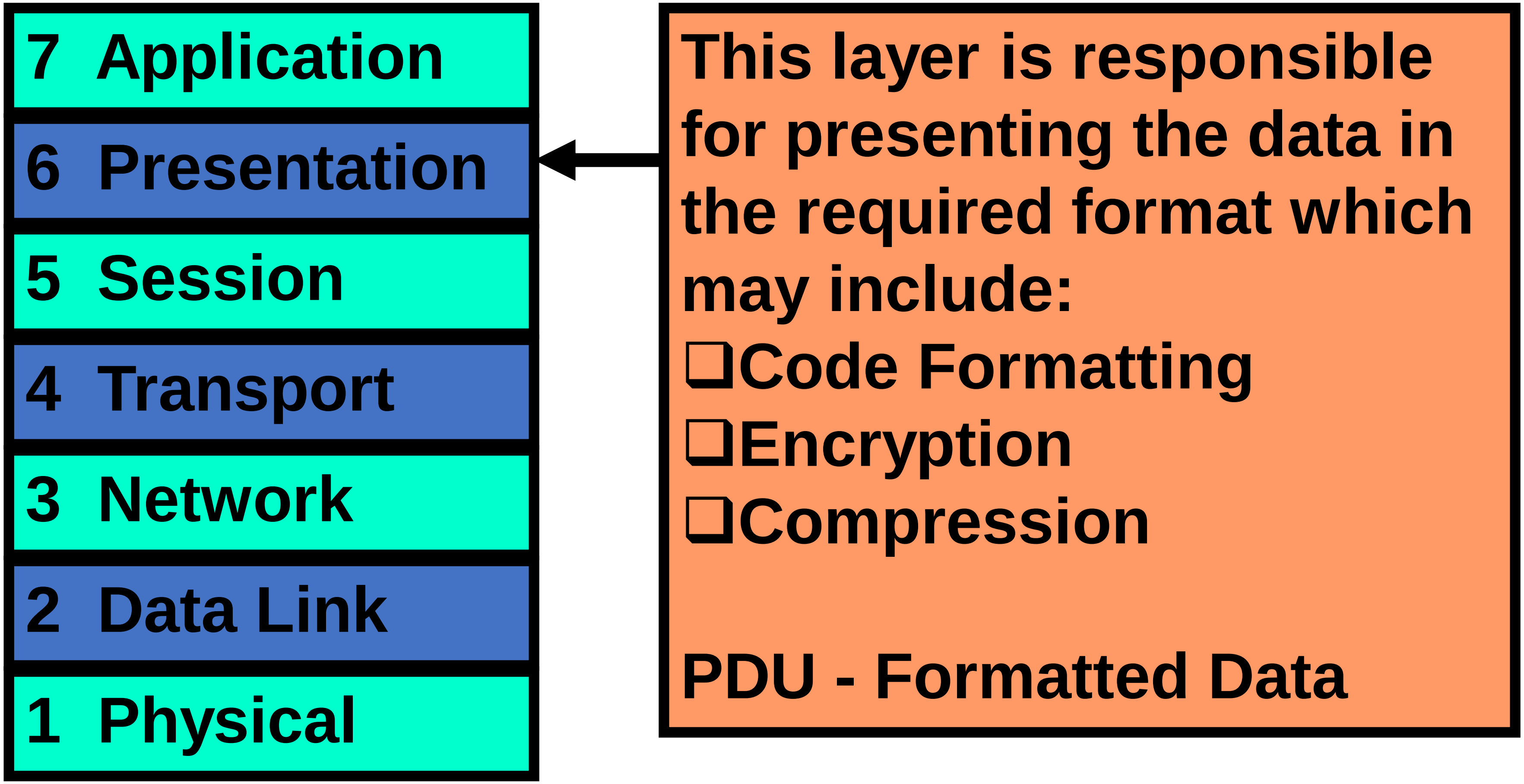
Examples:

- **Email**
- **Web browsers**

PDU - User Data

Each of the layers have Protocol Data Unit (PDU)

Layer 6 - The Presentation Layer



7 Application

6 Presentation

5 Session

4 Transport

3 Network

2 Data Link

1 Physical

This layer is responsible for presenting the data in the required format which may include:

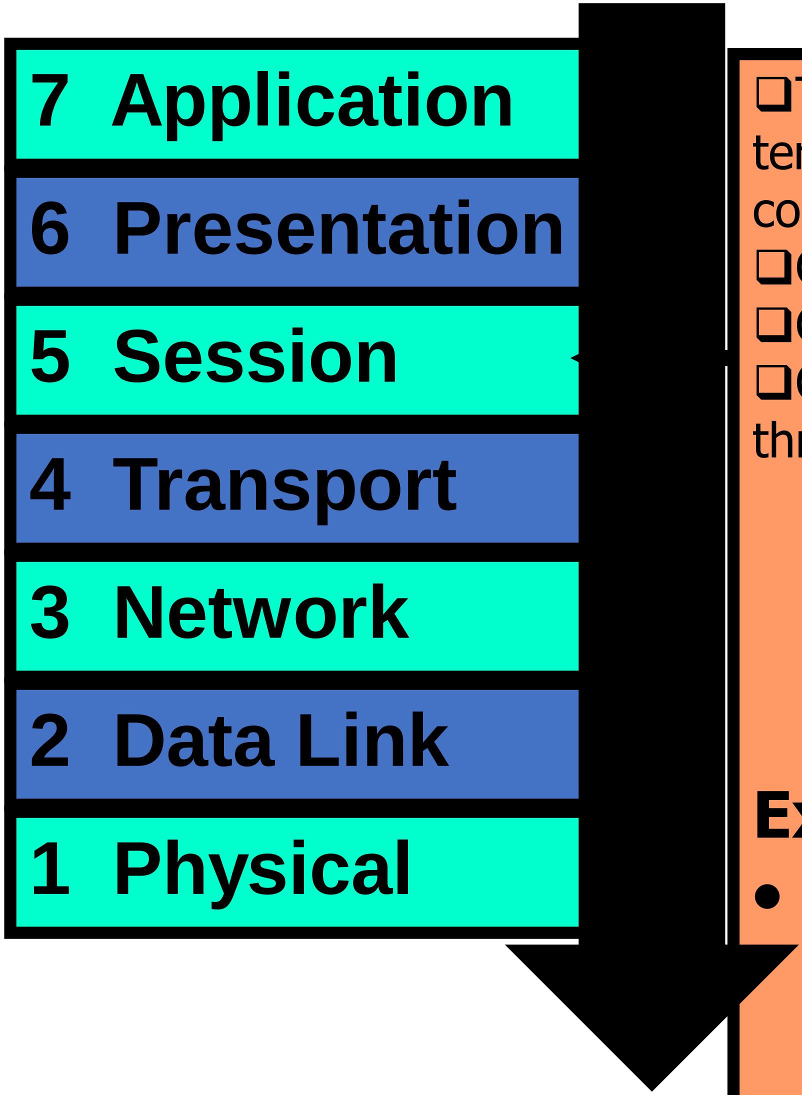
□ Code Formatting

□ Encryption

□ Compression

PDU - Formatted Data

Layer 5 - The Session Layer



7 Application

6 Presentation

5 Session

4 Transport

3 Network

2 Data Link

1 Physical

- ❑This layer establishes, manages, and terminates sessions between two communicating hosts.
- ❑Creates Virtual Circuit
- ❑Coordinates communication between systems
- ❑Organize their communication by offering three different modes
  - ❑Simplex
  - ❑Half Duplex
  - ❑Full Duplex

Example:

- **Client Software**
  (Used for logging in)

PDU - Formatted Data

Half Duplex

- It uses only one wire pair with a digital signal running in both directions on the wire.

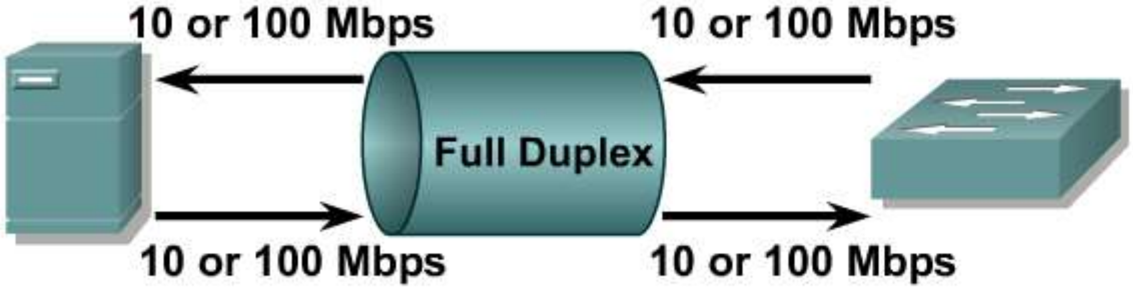
- It also uses the CSMA/CD protocol to help detect collisions and to permit retransmitting if a collision does occur.

- If a hub is attached to a switch, it must operate in half-duplex mode because the end stations must be able to detect collisions.

- Half-duplex Ethernet—typically 10BaseT—is only about 30 to 40 percent efficient because a large 10BaseT network will usually only give you 3 to 4Mbps—at most.

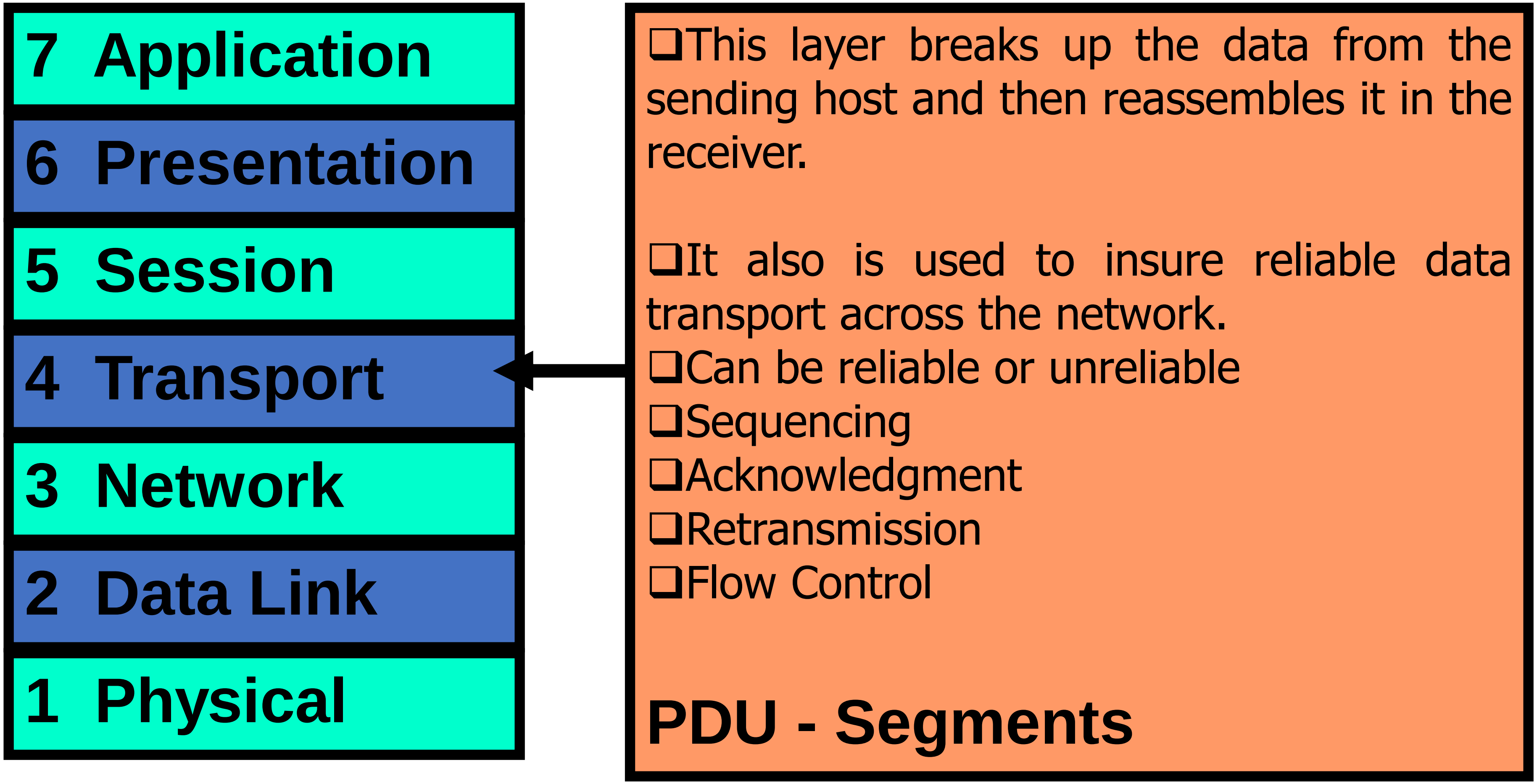
Full Duplex

In a network that uses twisted-pair cabling, one pair is used to carry the transmitted signal from one node to the other node. A separate pair is used for the return or received signal. It is possible for signals to pass through both pairs simultaneously. The capability of communication in both directions at once is known as full duplex.



- Doubles bandwidth between nodes
- Collision-free transmission
- Two 10- or 100- Mbps data paths

Layer 4 - The Transport Layer



7 Application

6 Presentation

5 Session

4 Transport

3 Network

2 Data Link

1 Physical

❑This layer breaks up the data from the sending host and then reassembles it in the receiver.

❑It also is used to insure reliable data transport across the network.

❑Can be reliable or unreliable

❑Sequencing

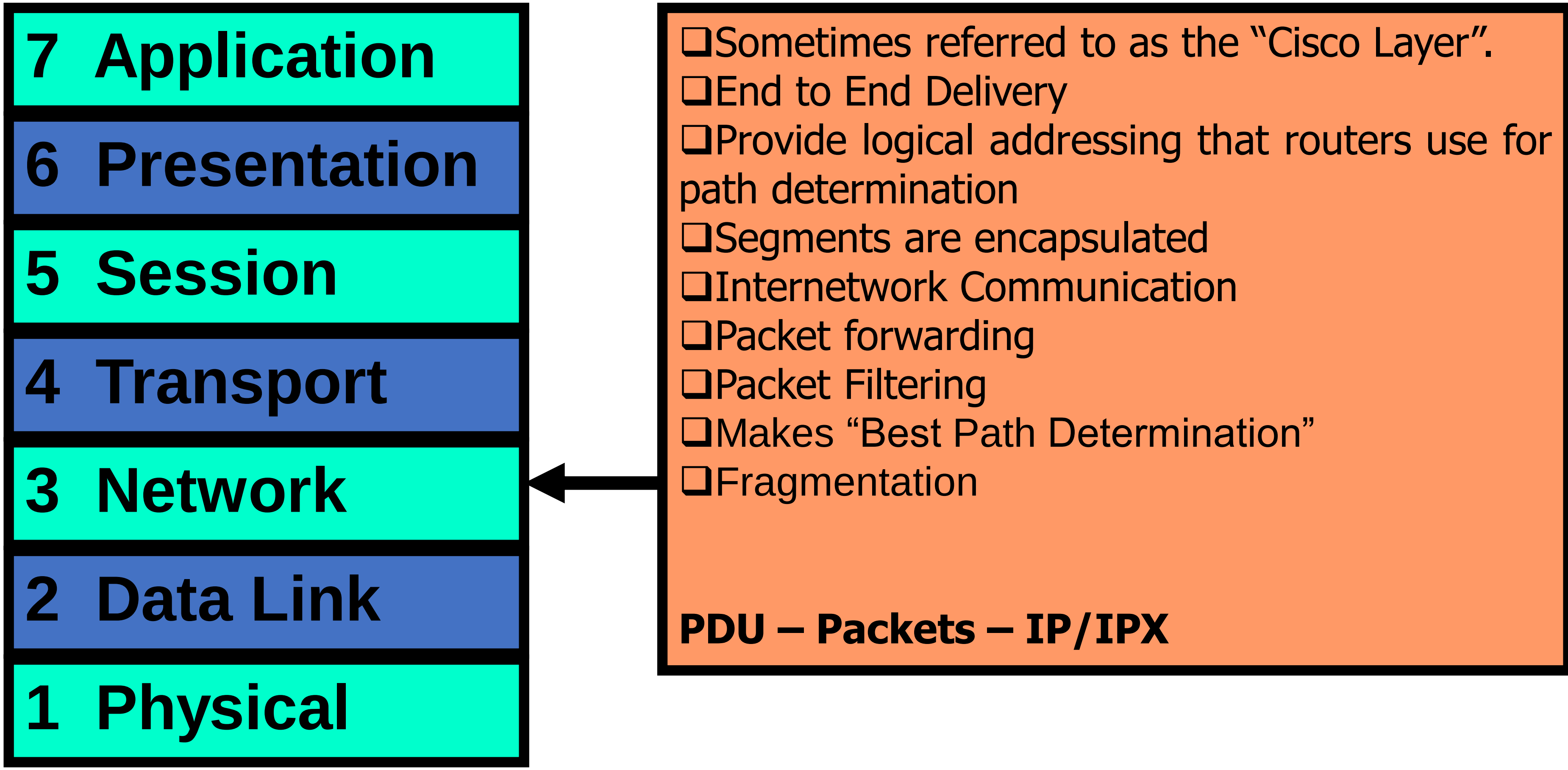
❑Acknowledgment

❑Retransmission

❑Flow Control

PDU - Segments

Layer 3 - The Network Layer



7 Application

6 Presentation

5 Session

4 Transport

3 Network

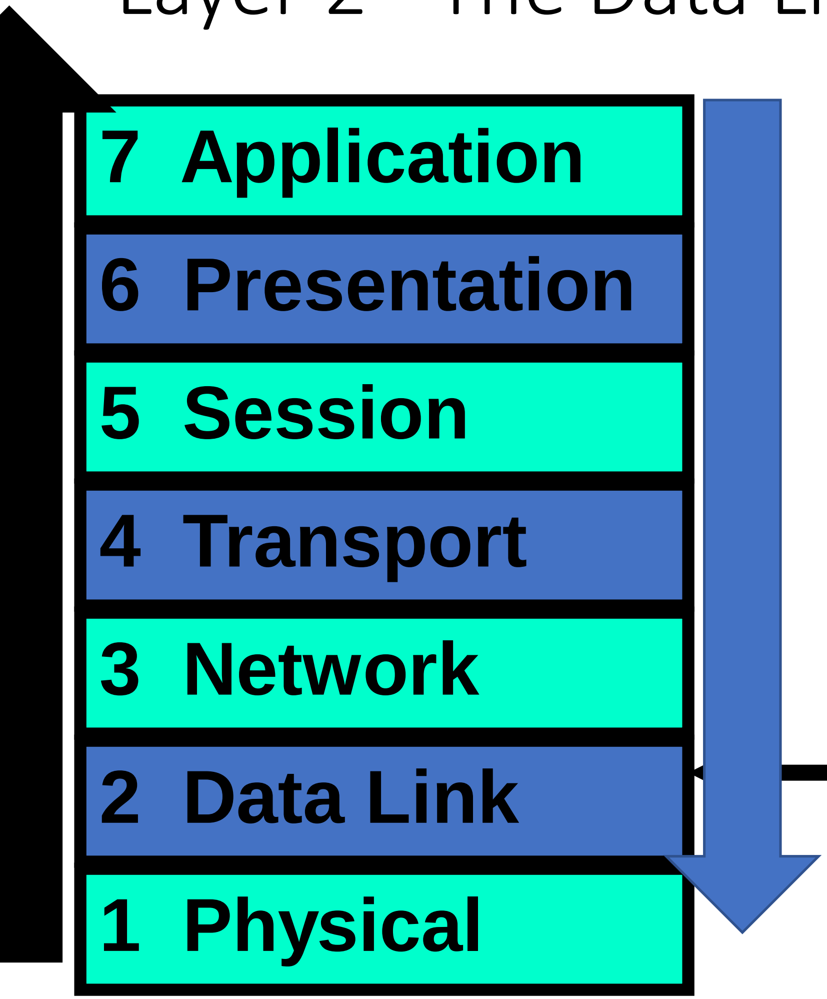
2 Data Link

1 Physical

❑Sometimes referred to as the “Cisco Layer”.
❑End to End Delivery
❑Provide logical addressing that routers use for path determination
❑Segments are encapsulated
❑Internetwork Communication
❑Packet forwarding
❑Packet Filtering
❑Makes “Best Path Determination”
❑Fragmentation

PDU – Packets – IP/IPX

Layer 2 - The Data Link Layer

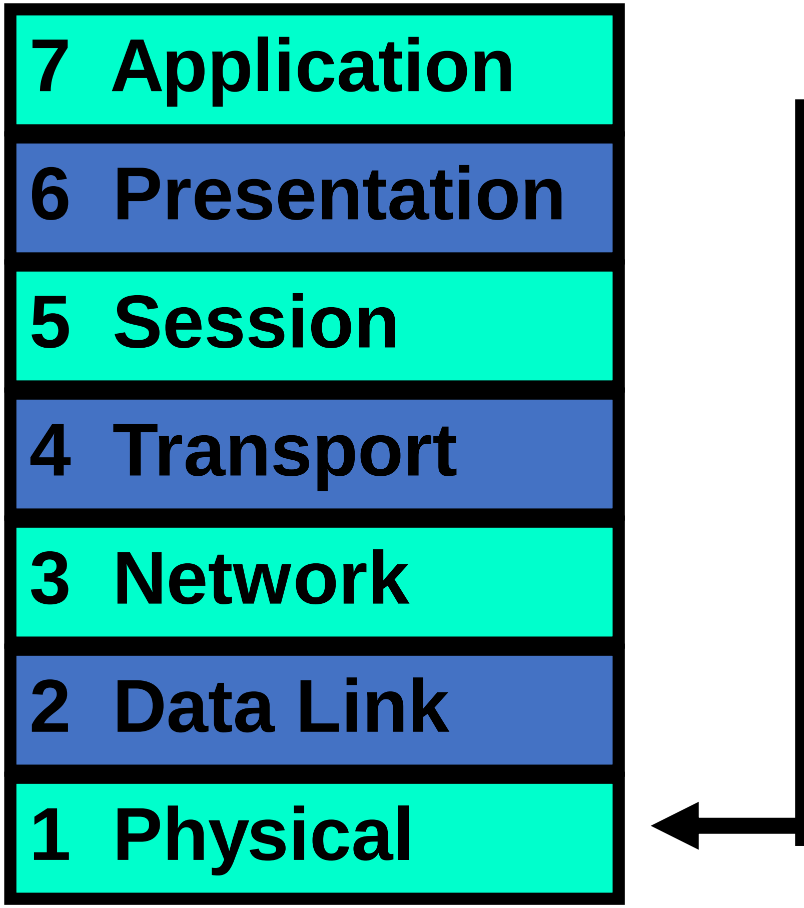


❑Performs Physical Addressing
❑This layer provides reliable transit of data across a physical link.
❑Combines bits into bytes and bytes into frames
❑Access to media using MAC address
❑Error detection, not correction
❑LLC and MAC
❑Logical Link Control performs Link establishment
❑MAC Performs Access method

PDU - Frames

Preamble	DMAC	SMAC	Data length	DATA	FCS

Layer 1 - The Physical Layer



7 Application

6 Presentation

5 Session

4 Transport

3 Network

2 Data Link

1 Physical

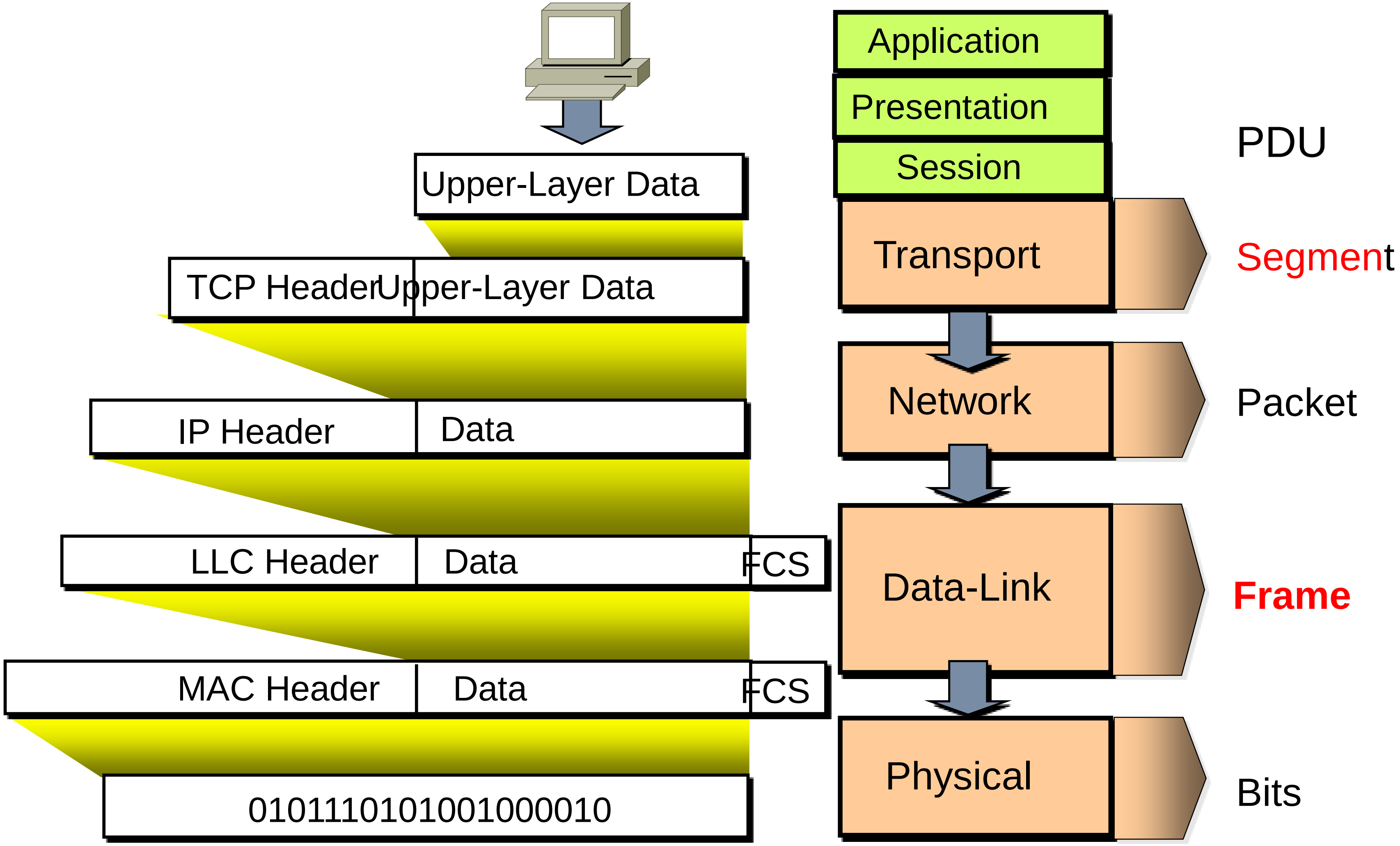
- This is the physical media through which the data, represented as electronic signals, is sent from the source host to the destination host.

- Move bits between devices
- Encoding

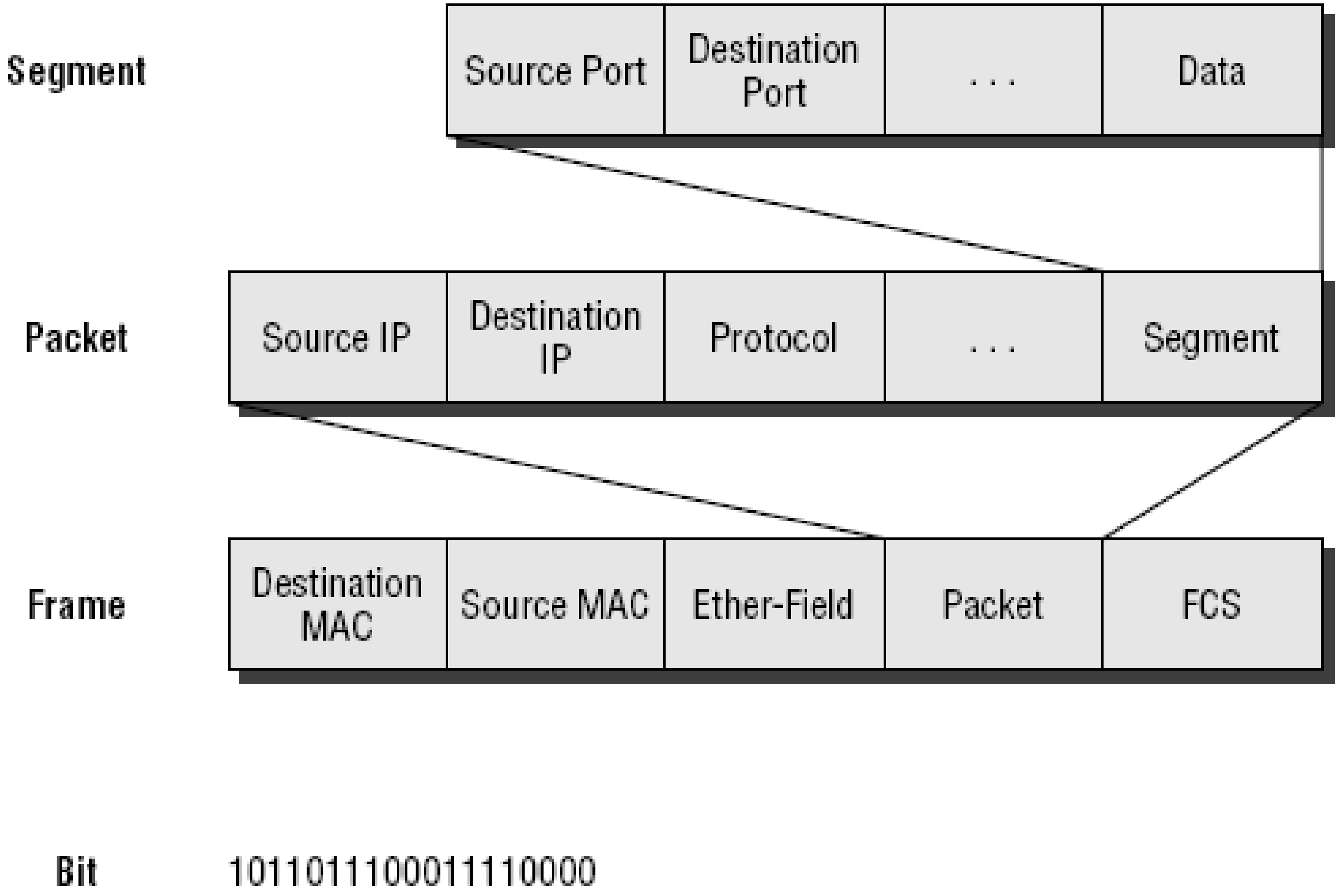
PDU - Bits

11111111010101010101010

Data Encapsulation



Data Encapsulation



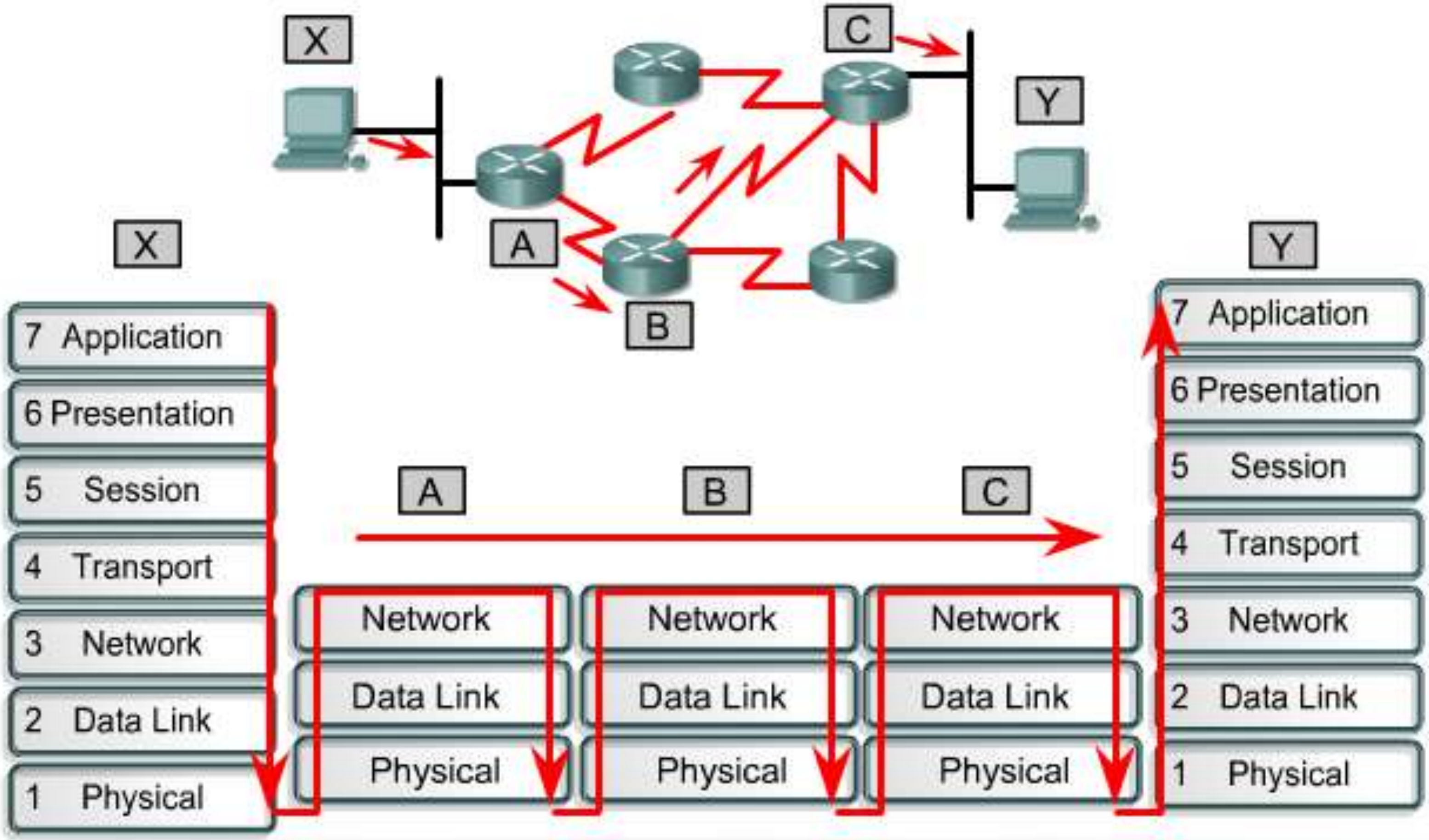
Segment: Source Port | Destination Port | . . . | Data

Packet: Source IP | Destination IP | Protocol | . . . | Segment

Frame: Destination MAC | Source MAC | Ether-Field | Packet | FCS

Bit: 1011011100011110000

Data Flow Through a Network



Data flow in a network focuses on layers one, two and three of the OSI model. This is after being transmitted by the sending host and before arriving at the receiving host.

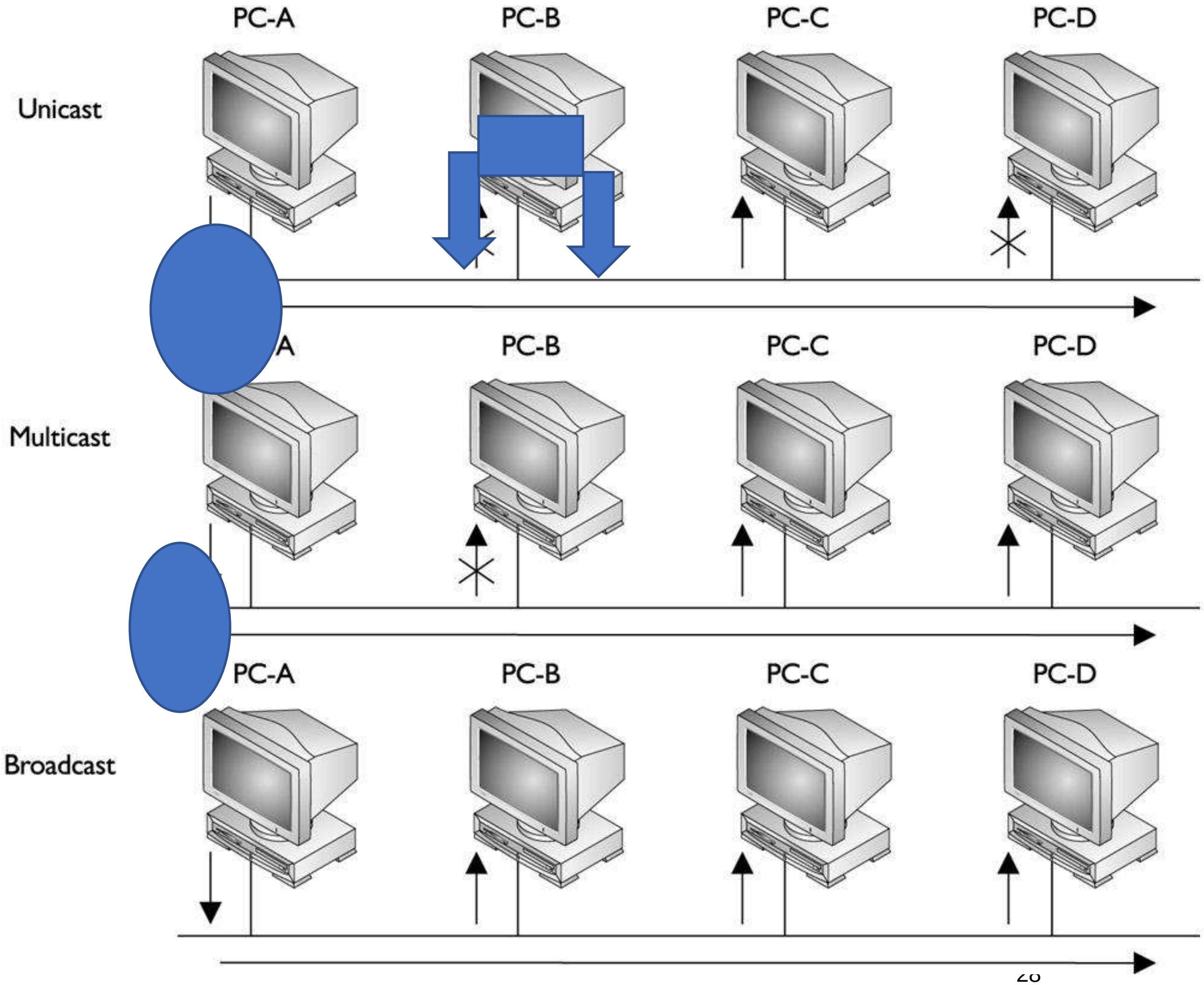
Type of Transmission

❑Unicast

❑Multicast

❑Broadcast

Type of Transmission



Broadcast Domain

❑A group of devices receiving broadcast frames initiating from any device within the group

❑Routers do not forward broadcast frames, broadcast domains are not forwarded from one broadcast to another.

Collision

- The effect of two nodes sending transmissions simultaneously in Ethernet. When they meet on the physical media, the frames from each node collide and are damaged.

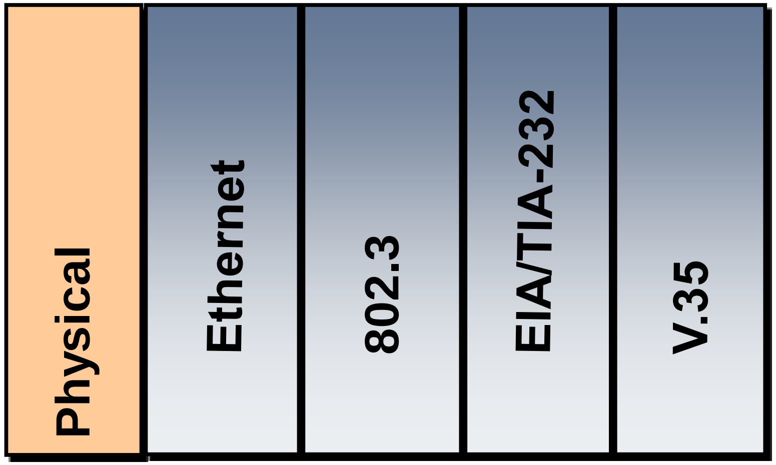
Collision Domain

- ❑The network area in Ethernet over which frames that have collided will be detected.
- ❑Collisions are propagated by hubs and repeaters
- ❑Collisions are **Not** propagated by switches, routers, or bridges

Physical Layer

Defines

- **Media type**
- **Connector type**
- **Signaling type**



Physical

Ethernet

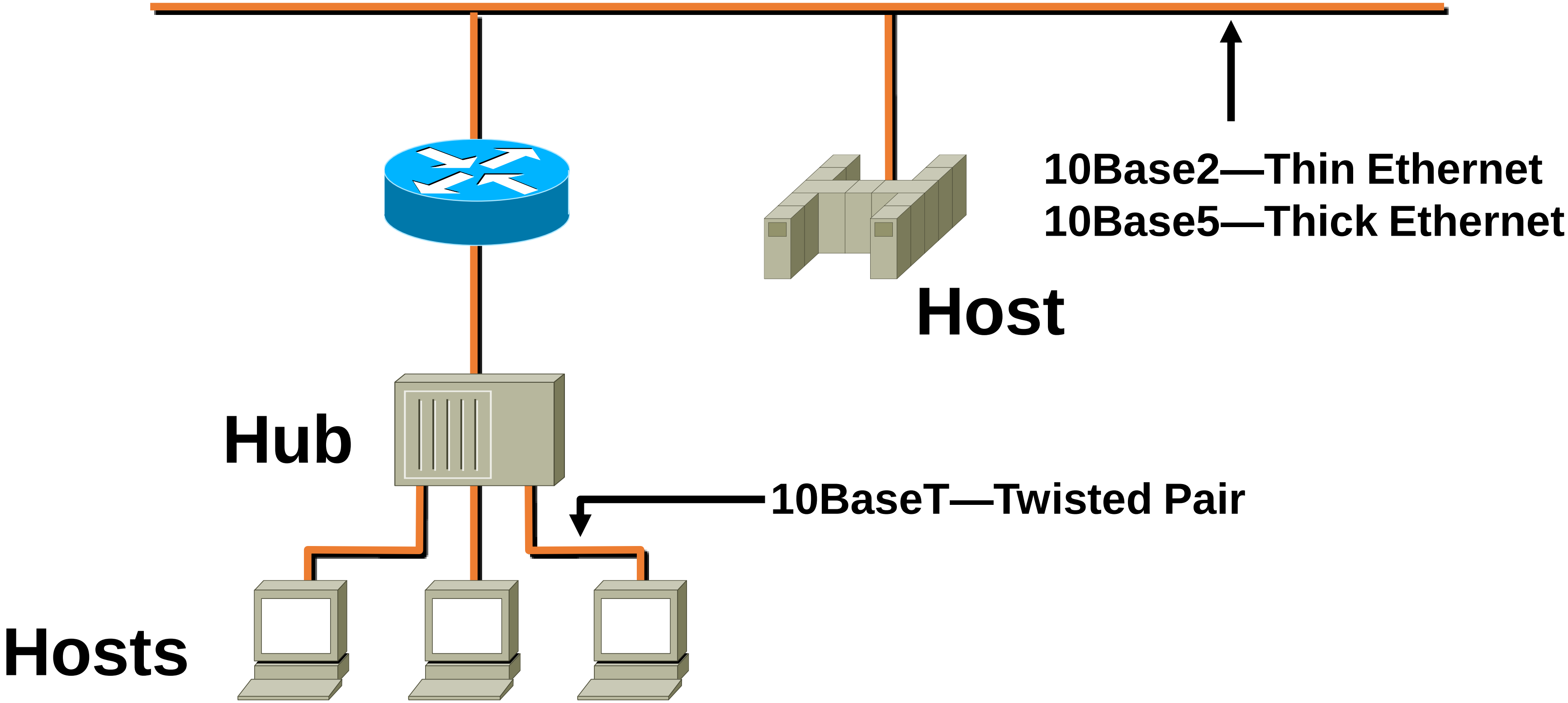
802.3

EIA/TIA-232

V.35

802.3 is responsible for LANs based on the carrier sense multiple access collision detect (CSMA/CD) access methodology. Ethernet is an example of a CSMA/CD network.

Physical Layer: Ethernet/802.3



10Base2—Thin Ethernet
10Base5—Thick Ethernet

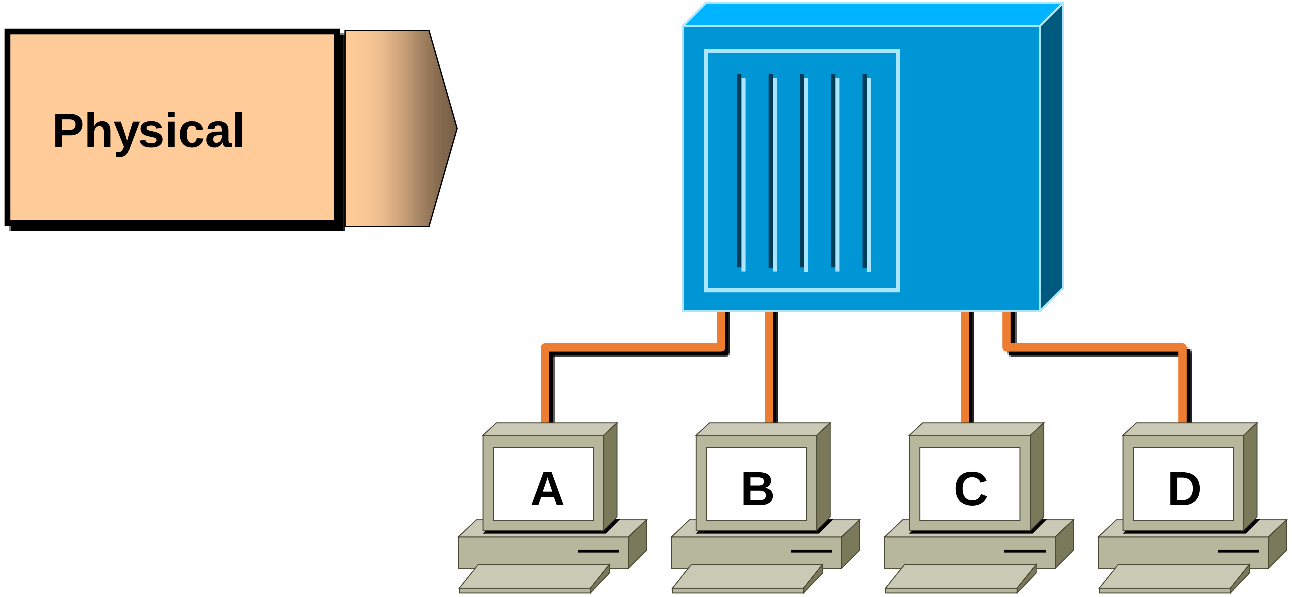
Host

Hub

10BaseT—Twisted Pair

Hosts

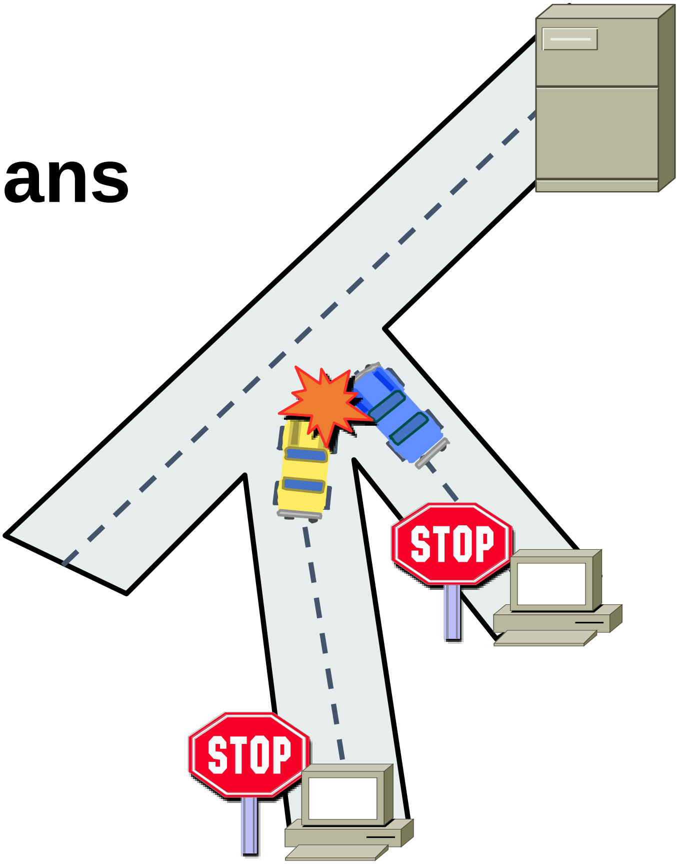
Device Used At Layer 1



- **All devices are in the same collision domain.**
- **All devices are in the same broadcast domain.**
- **Devices share the same bandwidth.**

Hubs & Collision Domains

- **More end stations means more collisions.**
- **CSMA/CD is used.**

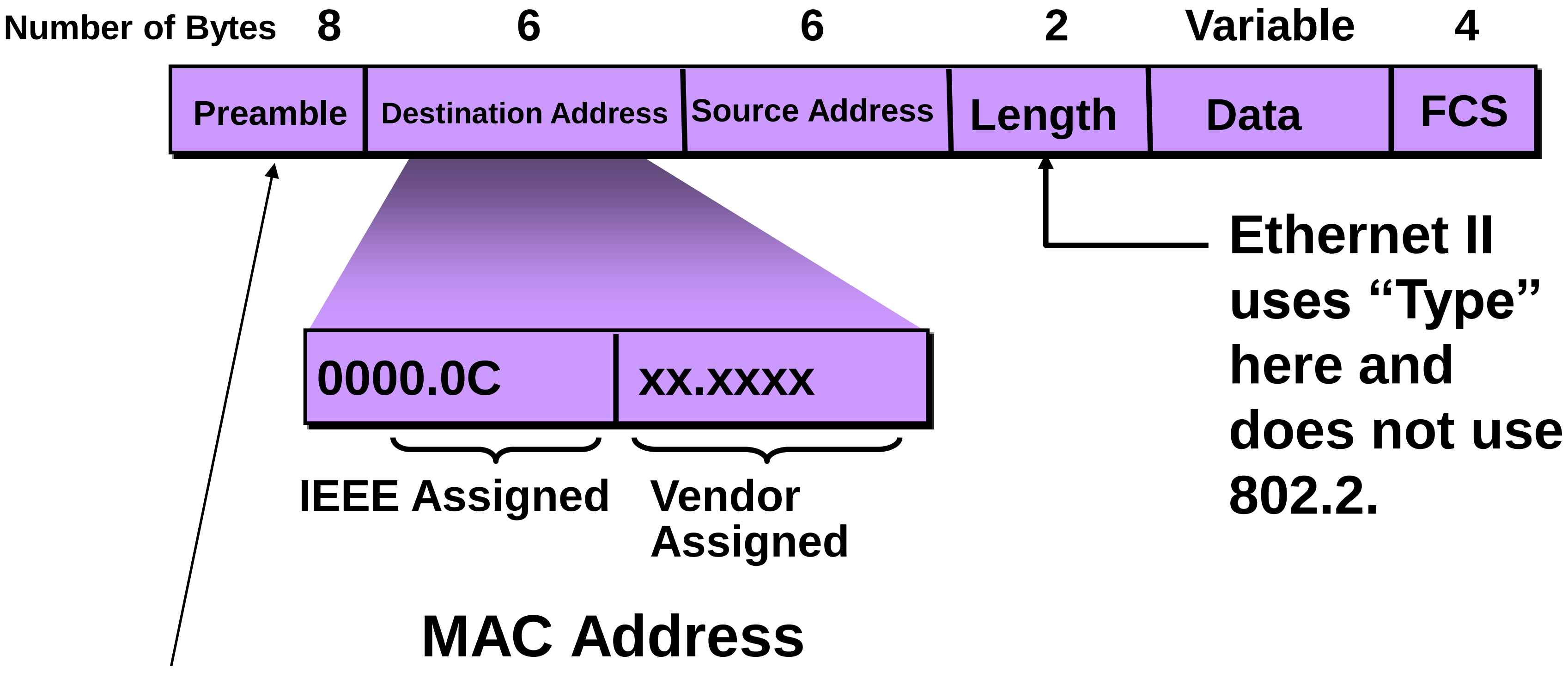


Difference Between Collision and Broadcast Domain

Collision Domain	Broadcast Domain
The Collision domain is a network section that allows traffic to flow forward and backward.	A Broadcast domain is a type of Domain wherein traffic flows all over the network.
The Collision domain refers to a set of devices in which packet collision could occur.	Broadcast domain refers to a logical set of reachable computer systems without using a router.
The devices might include the devices of other IP subnetworks.	Broadcast Domain is never limited to the specific IP subnetwork for all types of IP broadcasts.
Packet collision occurs as multiple devices transmit data on a single wire link.	The broadcast domain mostly uses a switched environment to broadcast, so no collision occurs.
Switches will break in the collision domain.	Switches will never break in the broadcast domain.
In, collision domain, every port on a router are in the separate broadcast domains.	All ports on a switch or a hub likely to be in the same broadcast domain.

Layer 2

MAC Layer—802.3



Number of Bytes	8	6	6	2	Variable	4
	Preamble	Destination Address	Source Address	Length	Data	FCS

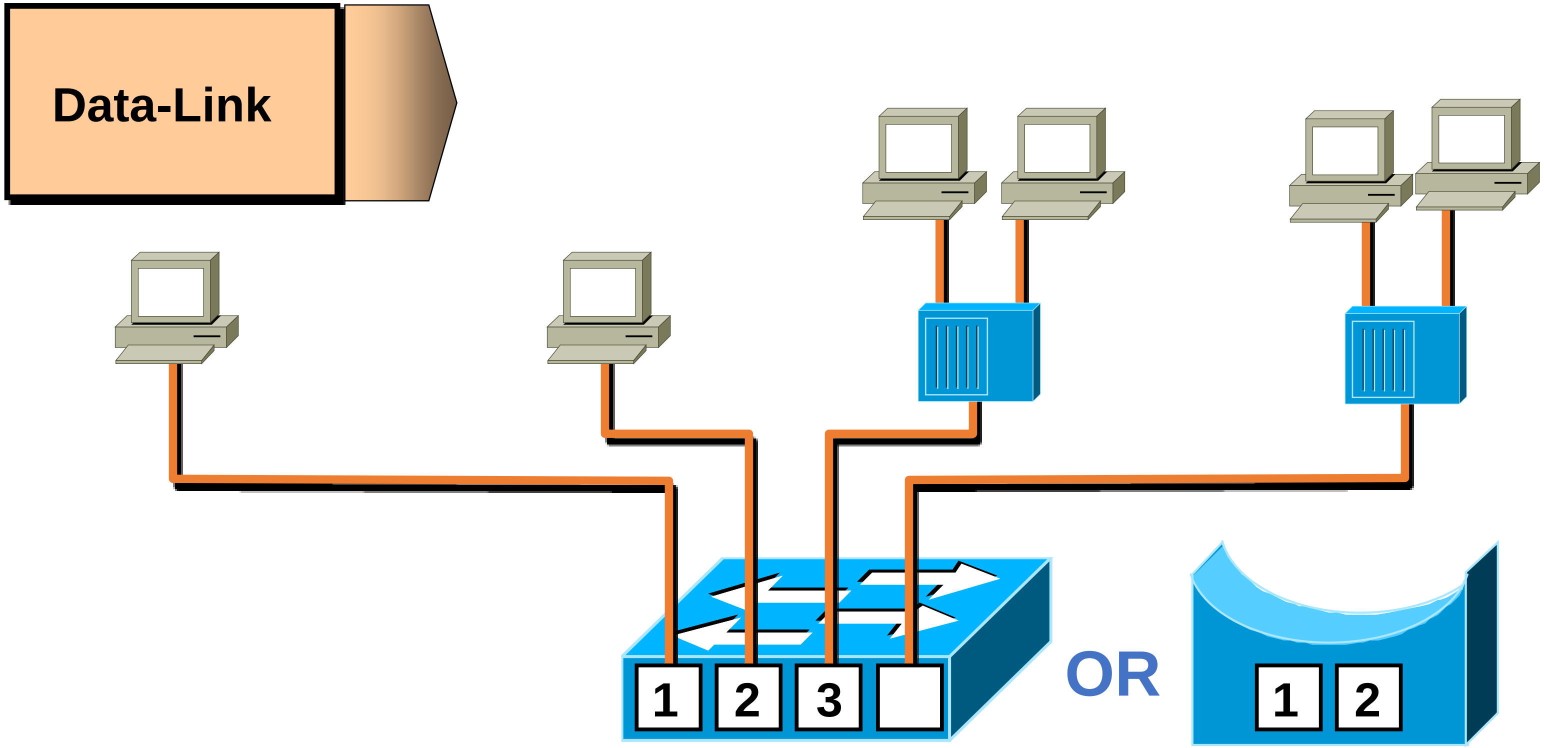
0000.0C	xx.xxxx
IEEE Assigned	Vendor Assigned

MAC Address

Ethernet II uses “Type” here and does not use 802.2.

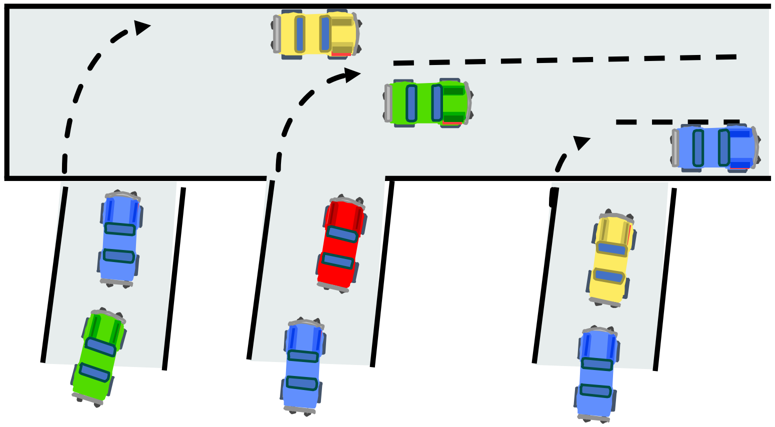
synchronize senders and receivers

Devices On Layer 2
(Switches & Bridges)

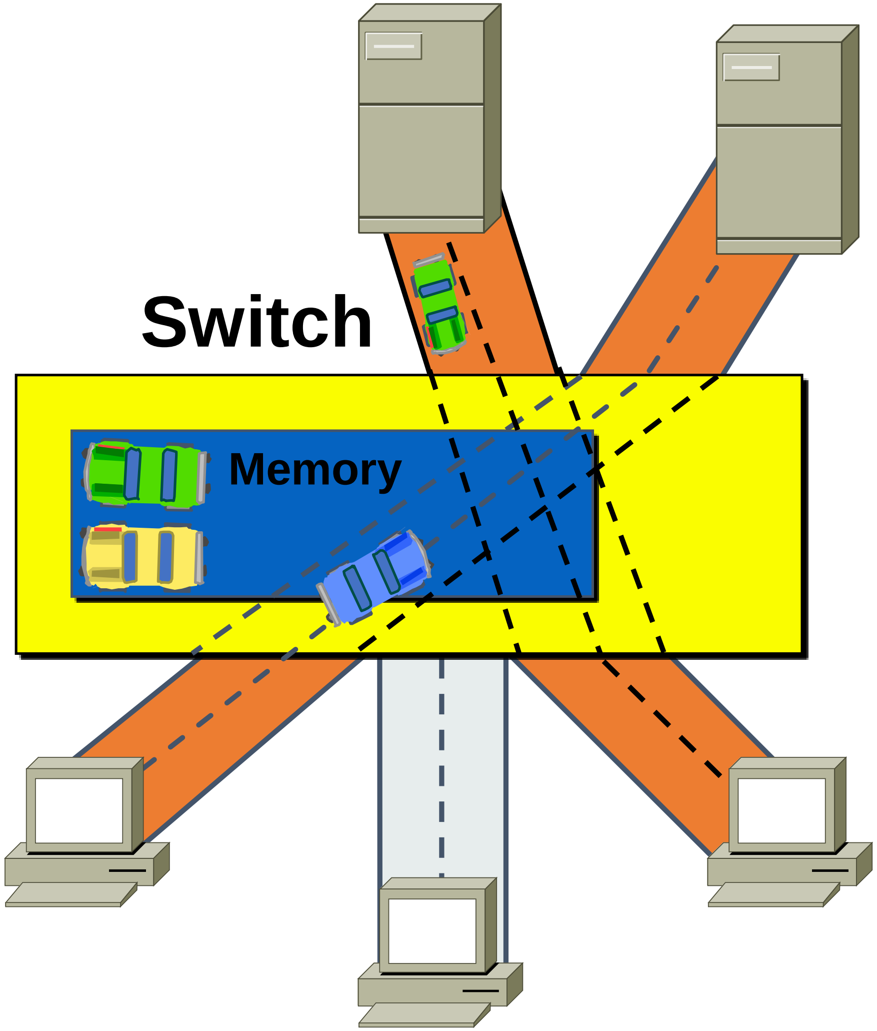


- **Each segment has its own collision domain.**
- **All segments are in the same broadcast domain.**

Switches

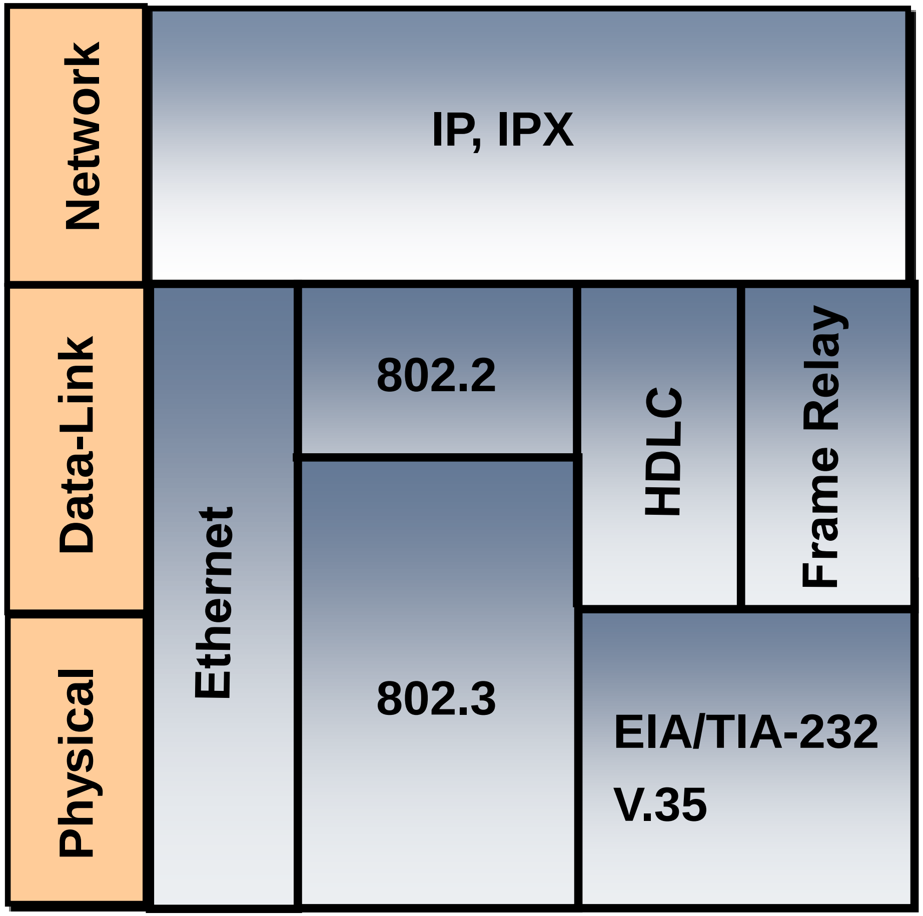


- **Each segment is its own collision domain.**
- **Broadcasts are forwarded to all segments.**



Layer 3 : Network Layer

- **Defines logical source and destination addresses associated with a specific protocol**
- **Defines paths through network**



Network

IP, IPX

Data-Link

Physical

Ethernet

802.2

802.3

HDLC

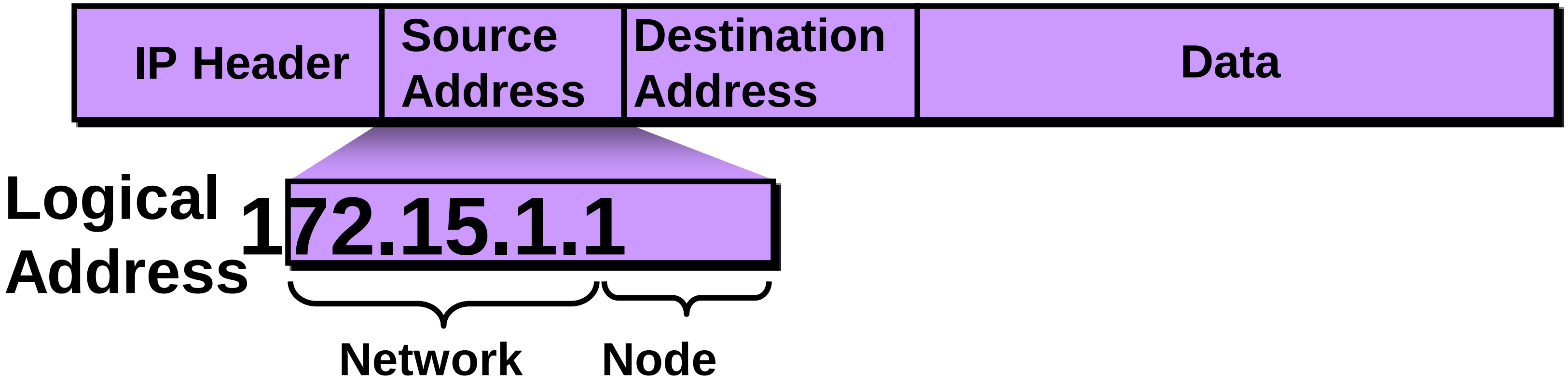
Frame Relay

EIA/TIA-232

V.35

Layer 3 : (cont.)

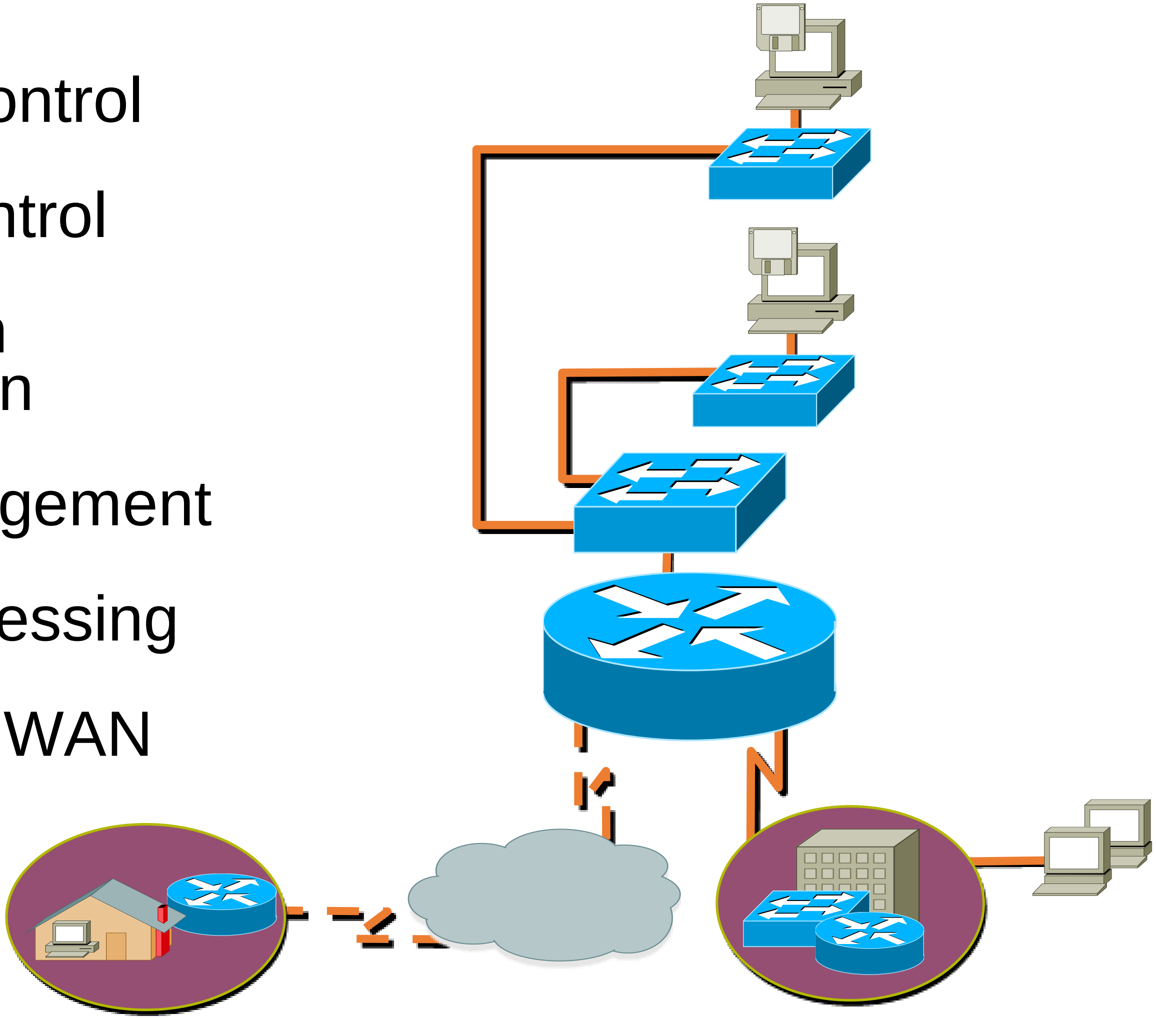
Network Layer End-Station Packet



- Route determination occurs at this layer, so a packet must include a source and destination address.
- Network-layer addresses have two components: a network component for internetwork routing, and a node number for a device-specific address. The example in the figure is an example of an IP packet and address.

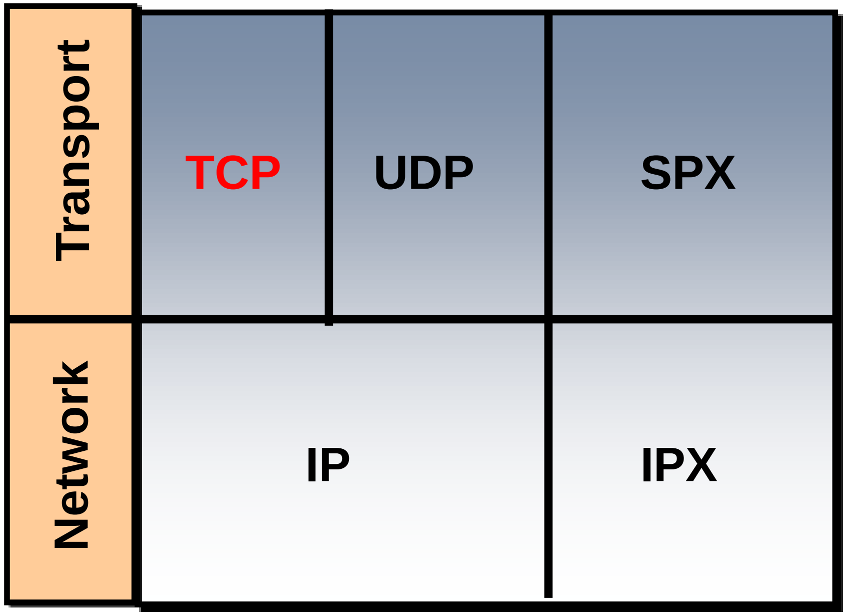
Device On Layer 3
Router

- Broadcast control
- Multicast control
- Optimal path determination
- Traffic management
- Logical addressing
- Connects to WAN services



Layer 4 : Transport Layer

- **Distinguishes between upper-layer applications**
- **Establishes end-to-end connectivity between applications**
- **Defines flow control**
- **Provides reliable or unreliable services for data transfer**



Transport

TCP

UDP

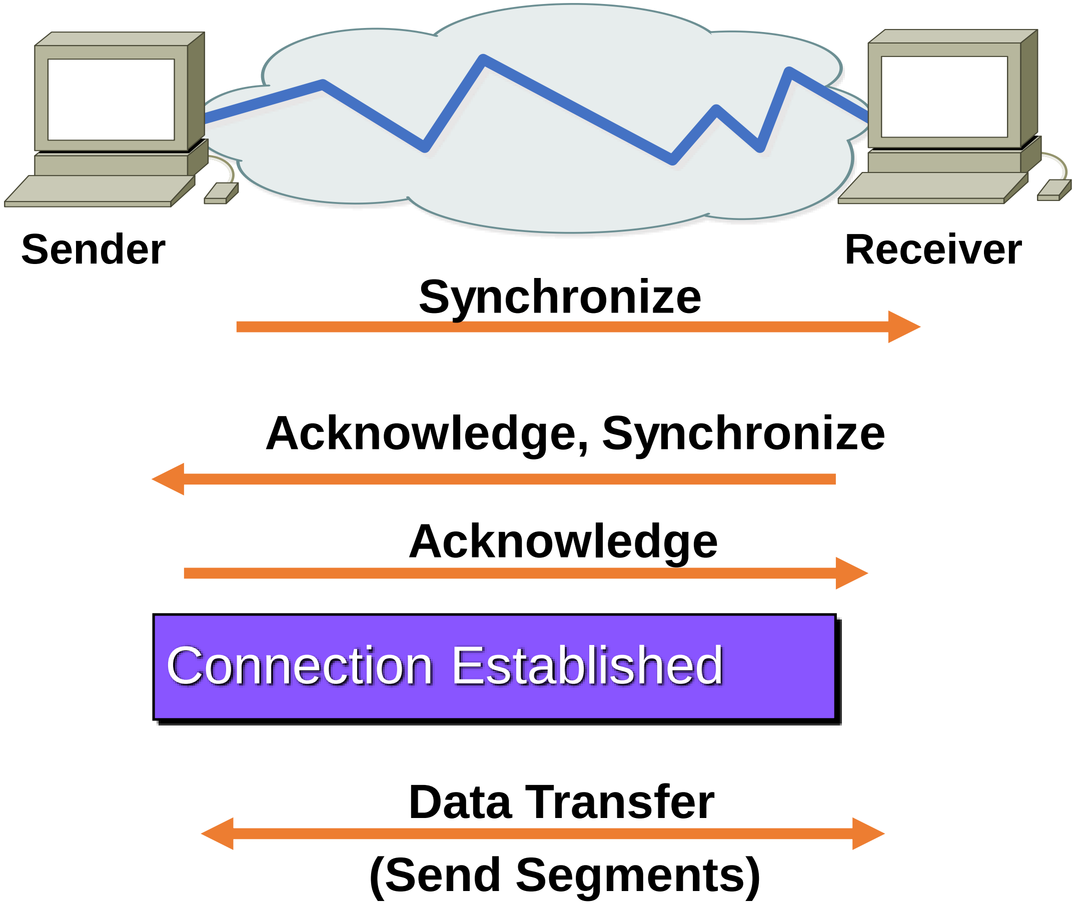
SPX

Network

IP

IPX

Reliable Service



Sender

Receiver

Synchronize

Acknowledge, Synchronize

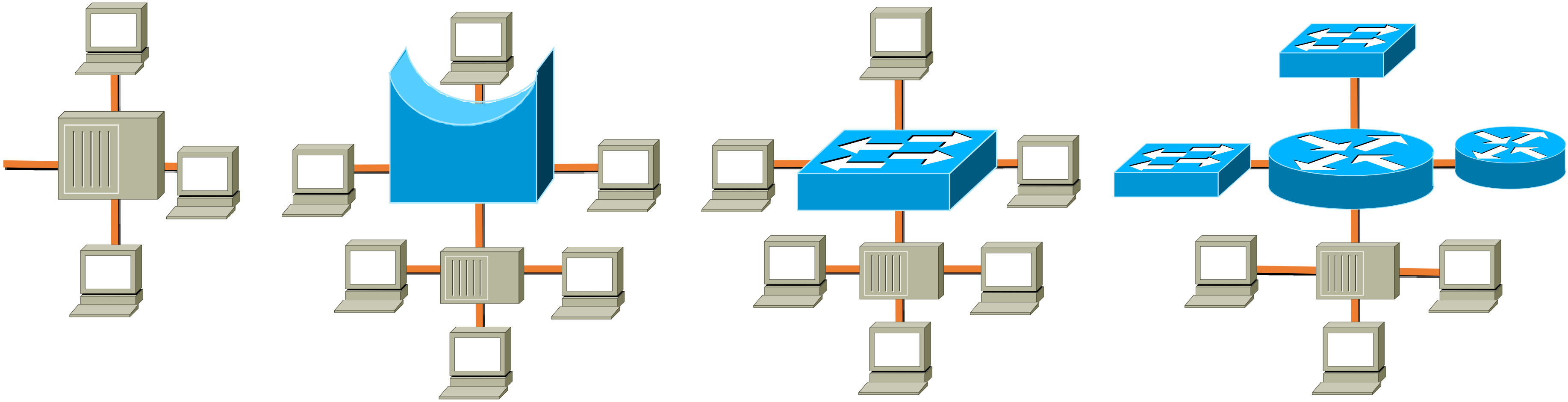
Acknowledge

Connection Established

Data Transfer

(Send Segments)

How They Operate



	Hub	Bridge	Switch	Router
Collision Domains:	1	4	4	4
Broadcast Domains:	1	1	1	4

TCP/IP MODEL

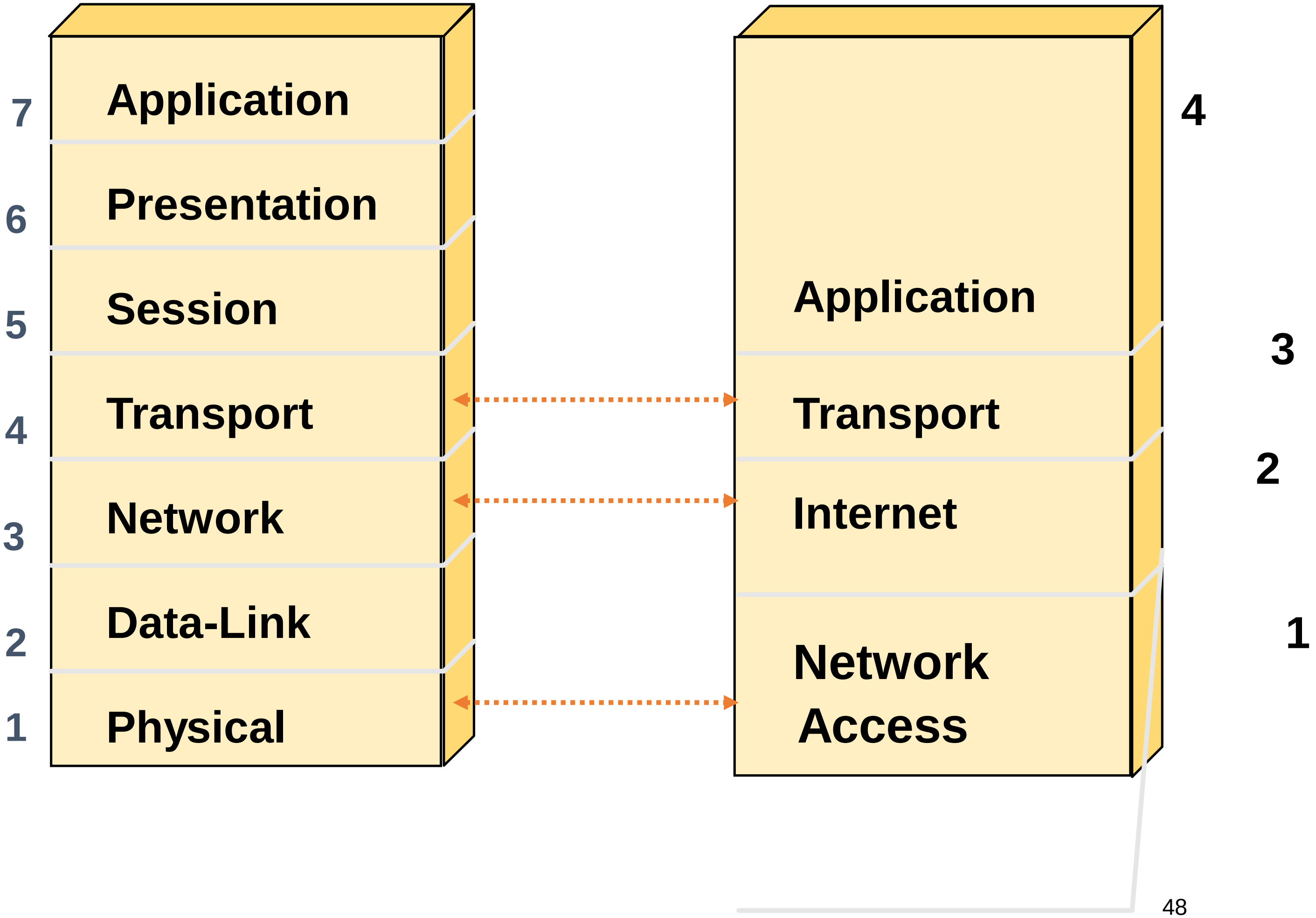
Why Another Model?

Although the OSI reference model is universally recognized, the historical and technical open standard of the Internet is Transmission Control Protocol / Internet Protocol (TCP/IP).

The TCP/IP reference model and the TCP/IP protocol stack make data communication possible between any two computers, anywhere in the world, at nearly the speed of light.

The U.S. Department of Defense (DoD) created the TCP/IP reference model because it wanted a network that could survive any conditions, even a nuclear war.

TCP/IP Protocol Stack



App verview

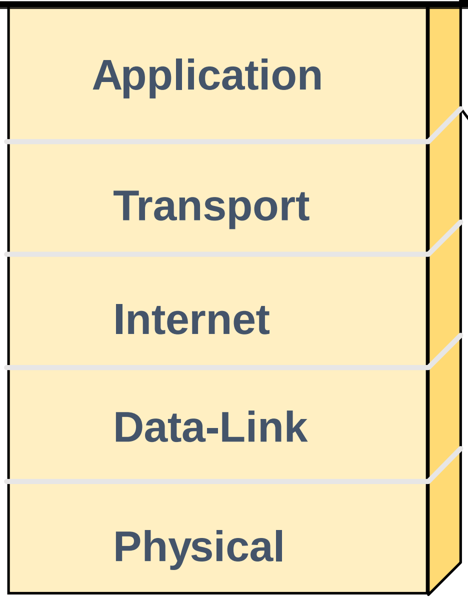
- TFTP*
- FTP*
- NFS

E-Mail
- SMTP

Remote Login
- Telnet*
- rlogin*

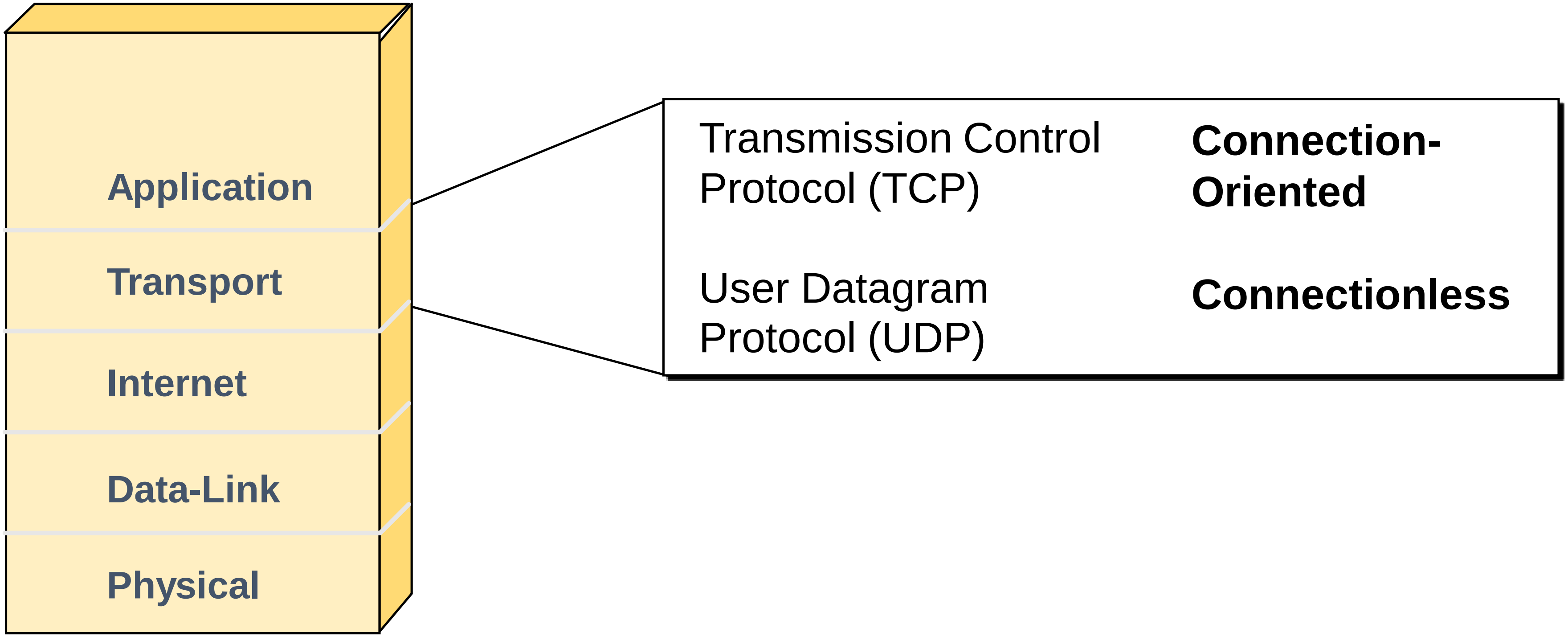
Network Management
- SNMP*

Name Management
- DNS*



***Used by the Router**

Transport Layer Overview



Application

Transport

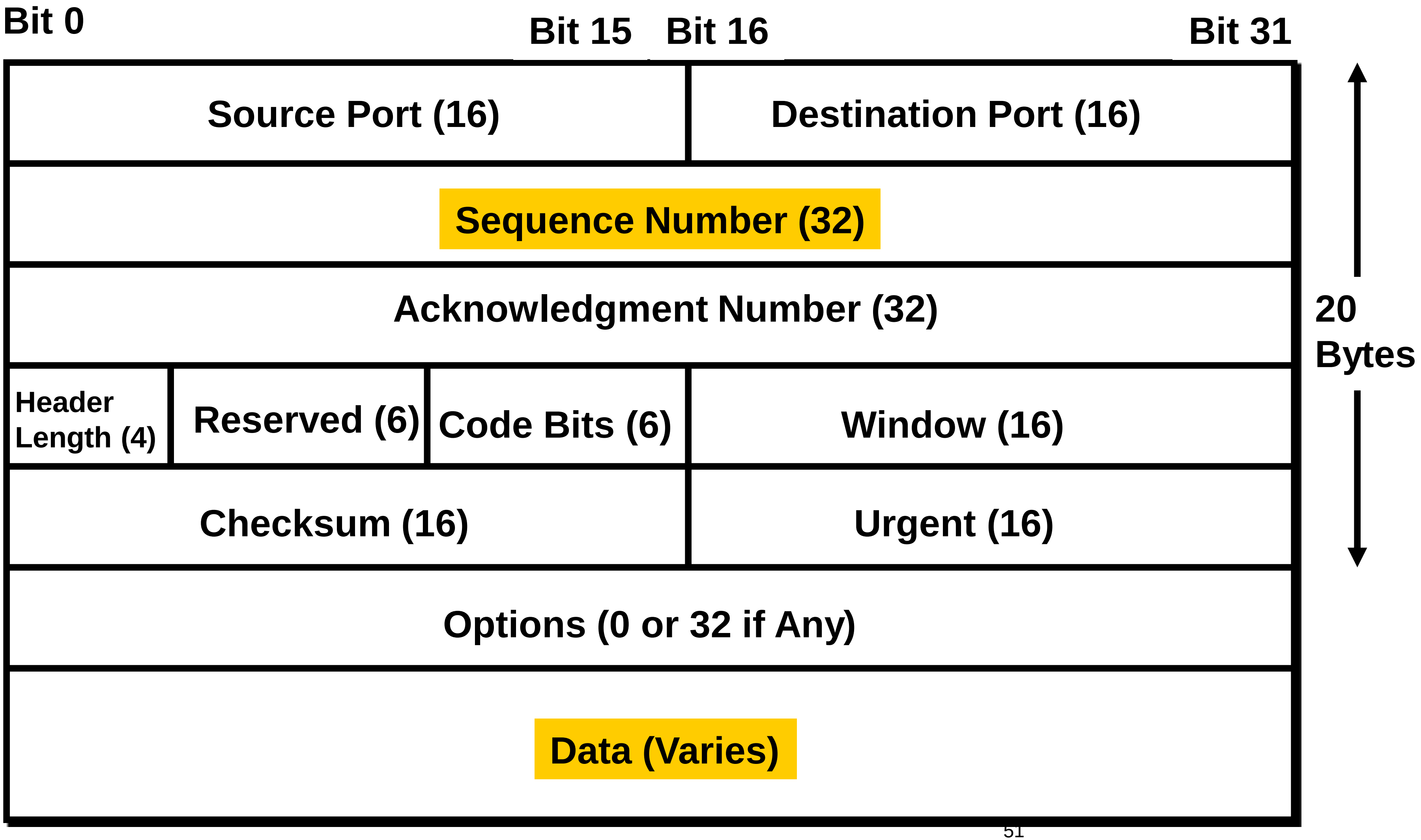
Internet

Data-Link

Physical

Transmission Control Protocol (TCP)	**Connection-Oriented**
User Datagram Protocol (UDP)	**Connectionless**

TCP Segment Format



Bit 0

Bit 15 Bit 16

Bit 31

Source Port (16) | Destination Port (16)

Sequence Number (32)

Acknowledgment Number (32)

Header Length (4) | Reserved (6) | Code Bits (6) | Window (16)

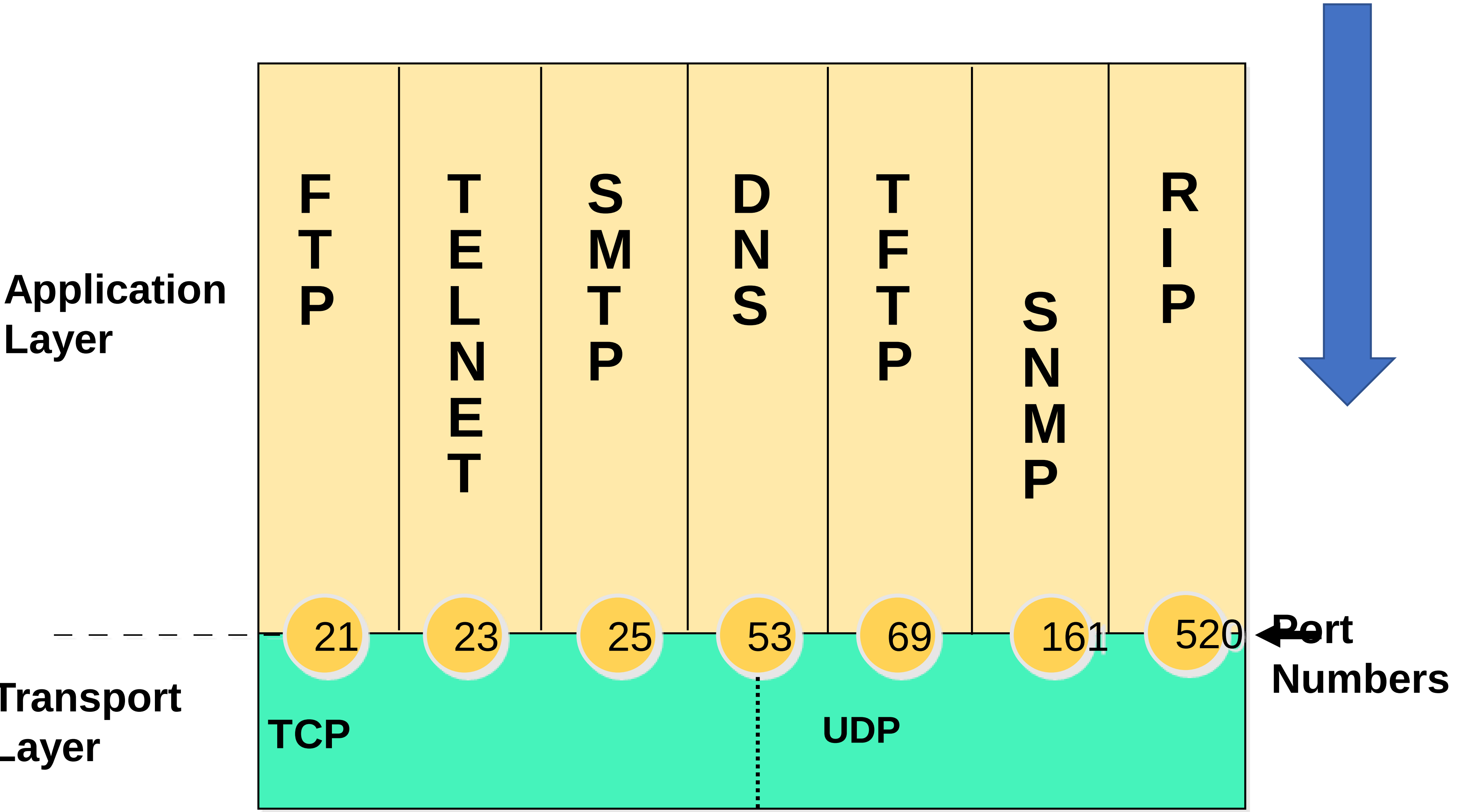
Checksum (16) | Urgent (16)

Options (0 or 32 if Any)

Data (Varies)

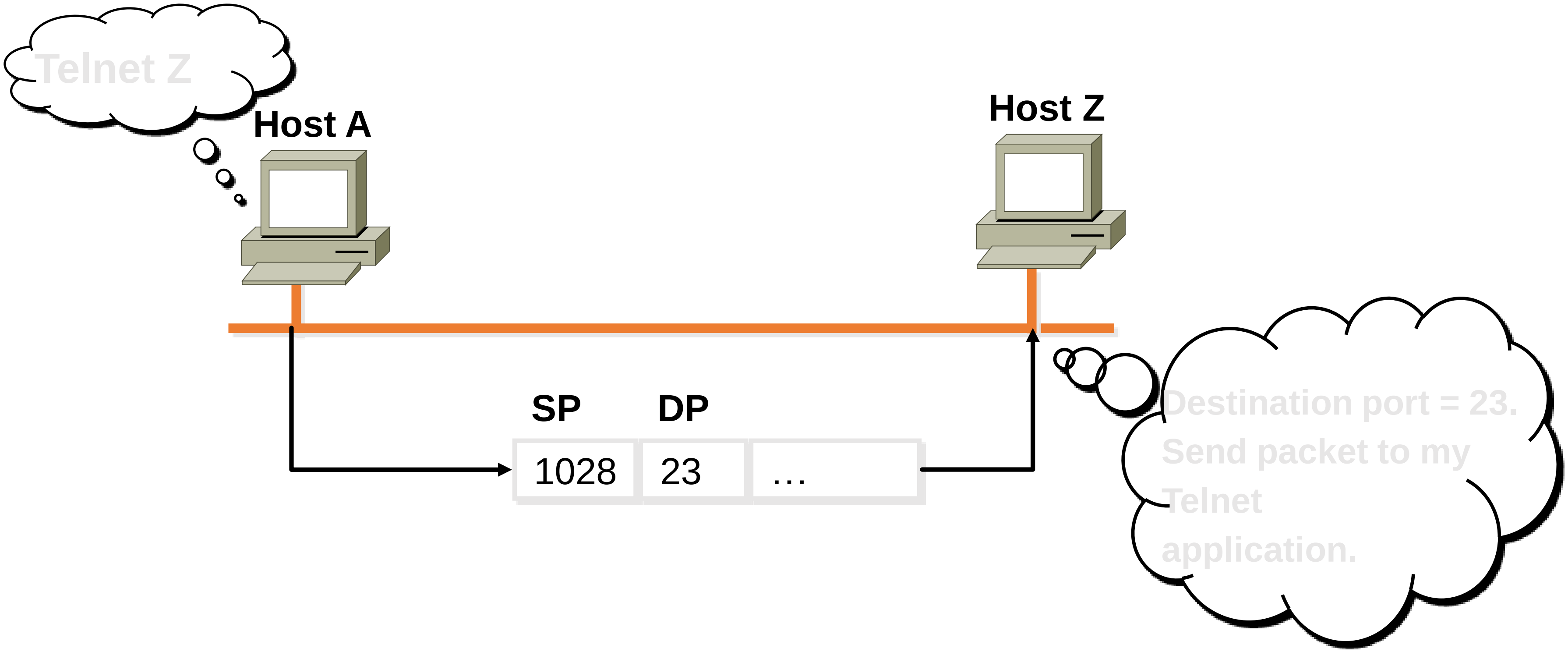
20 Bytes

Port Numbers

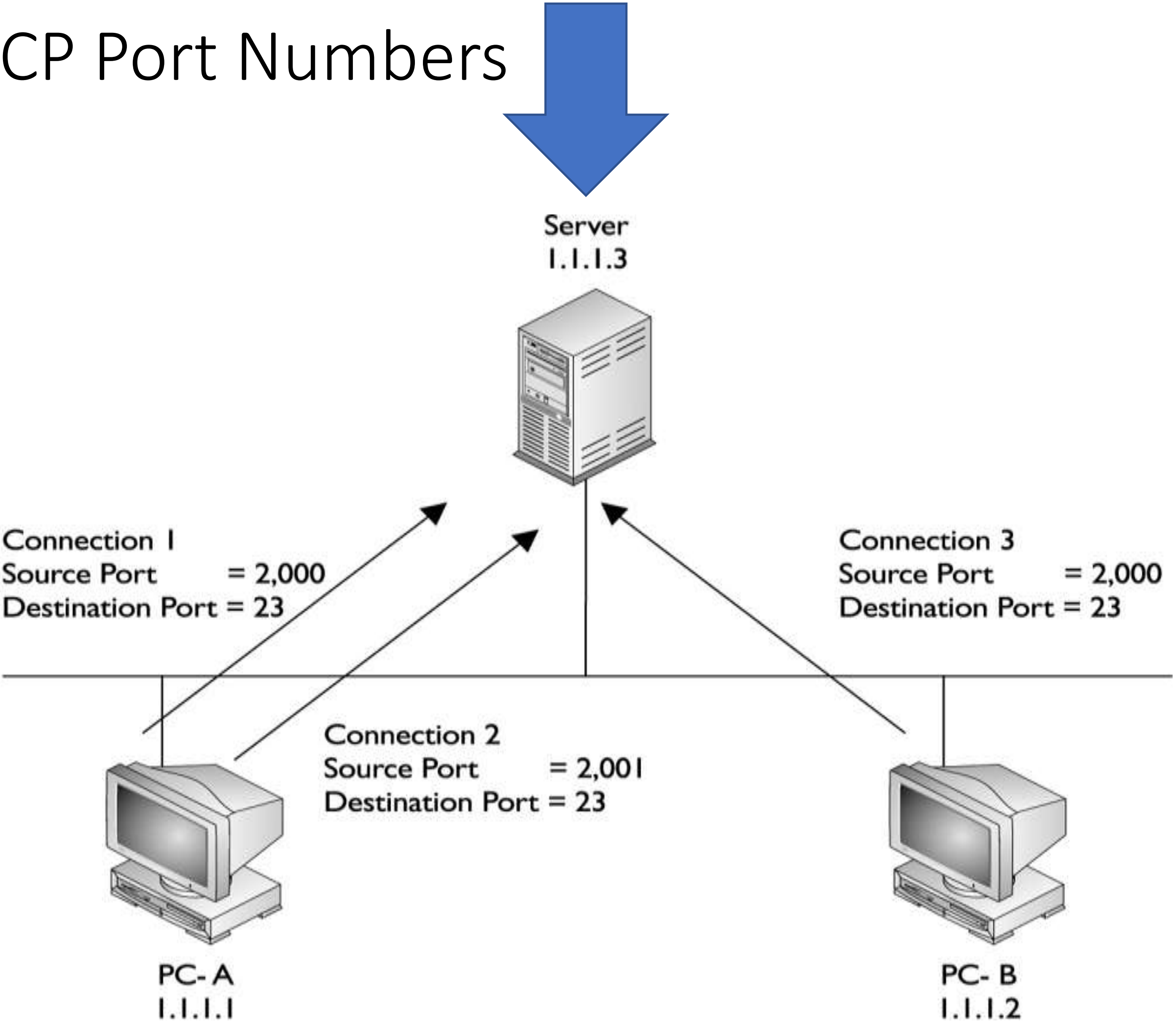


TCP Port Numbers

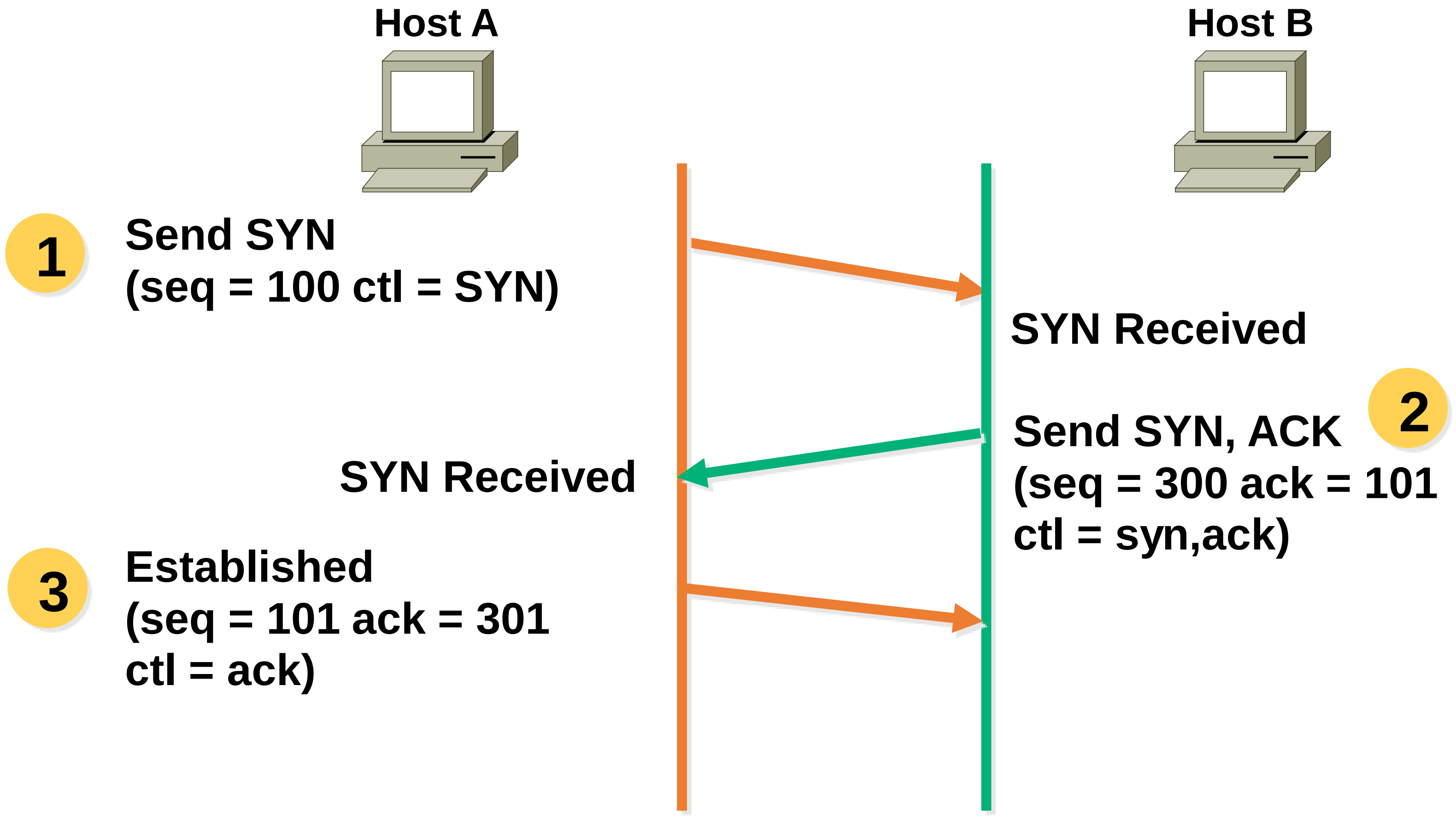
Source Port	Destination Port	…


Telnet Z
Host A
Host Z
SP
DP
1028
23
…
Destination port = 23. Send packet to my Telnet application.

TCP Port Numbers



TCP Three-Way Handshake/Open Connection



Host A

Host B

1 Send SYN
(seq = 100 ctl = SYN)

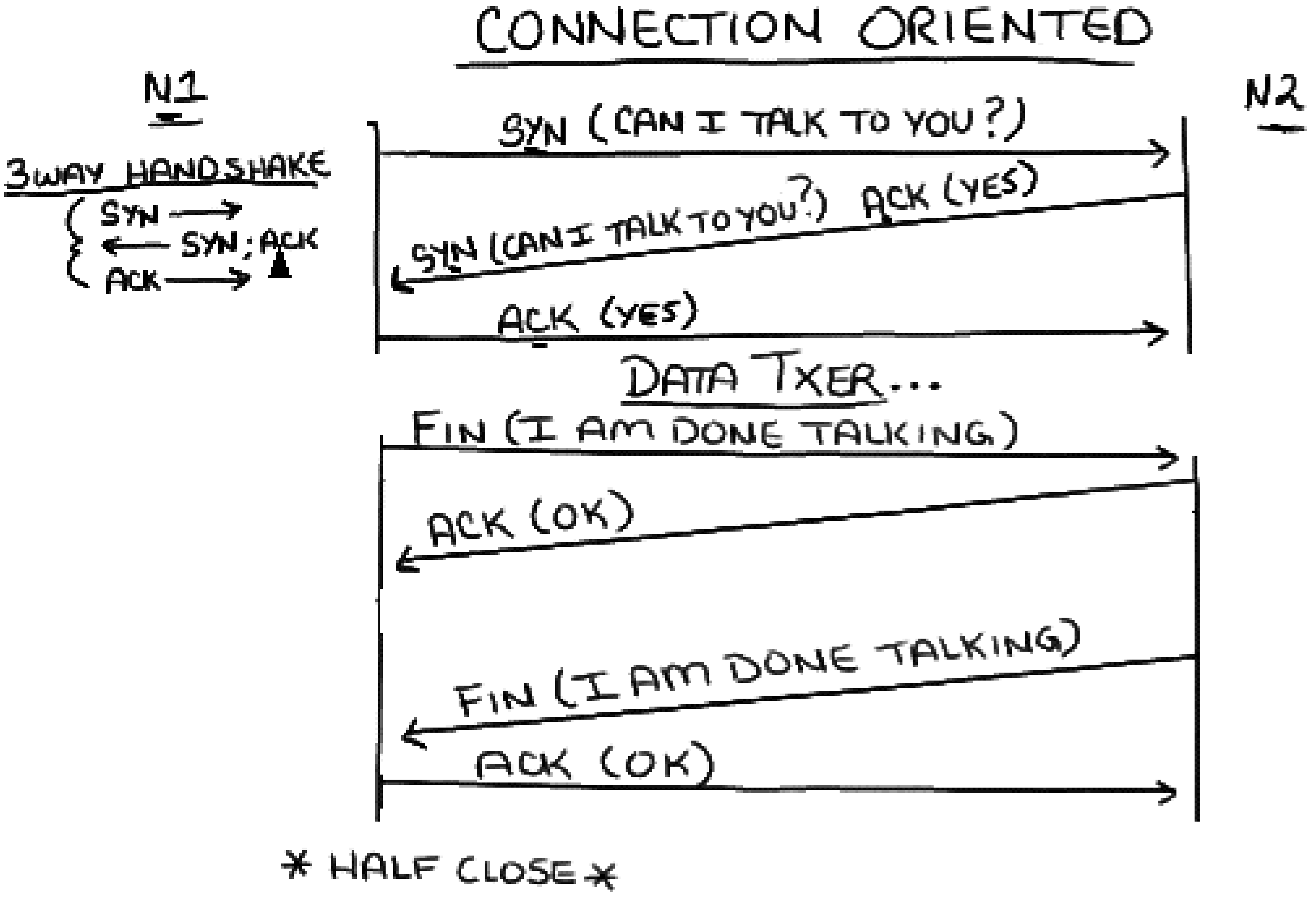
SYN Received

2 Send SYN, ACK
(seq = 300 ack = 101
ctl = syn,ack)

SYN Received

3 Established
(seq = 101 ack = 301
ctl = ack)

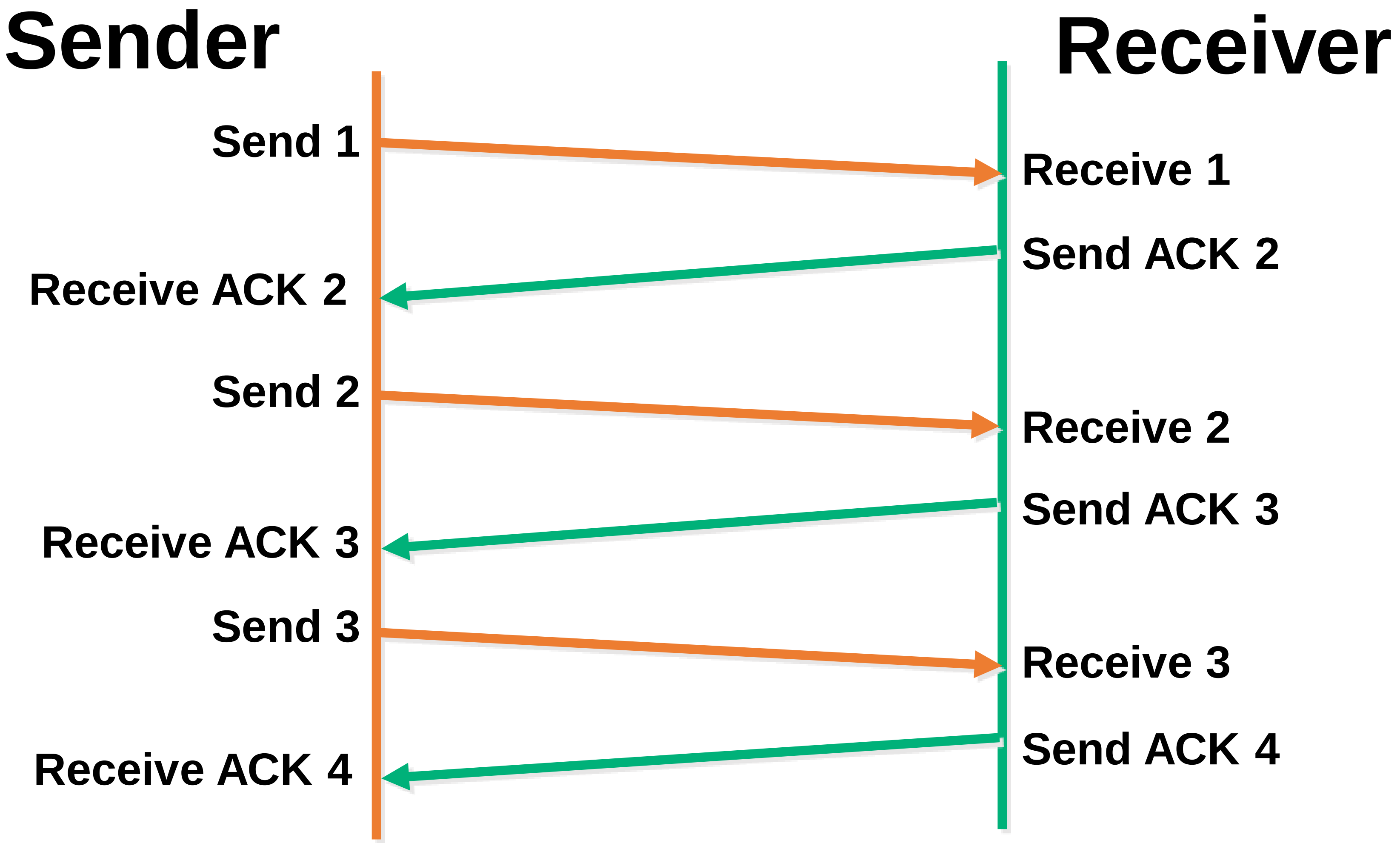
Opening & Closing Connection



Windowing

- Windowing in networking means the quantity of data segments which is measured in bytes that a machine can transmit/send on the network without receiving an acknowledgement

TCP Simple Acknowledgment



Sender

Receiver

Send 1

Receive 1

Send ACK 2

Receive ACK 2

Send 2

Receive 2

Send ACK 3

Receive ACK 3

Send 3

Receive 3

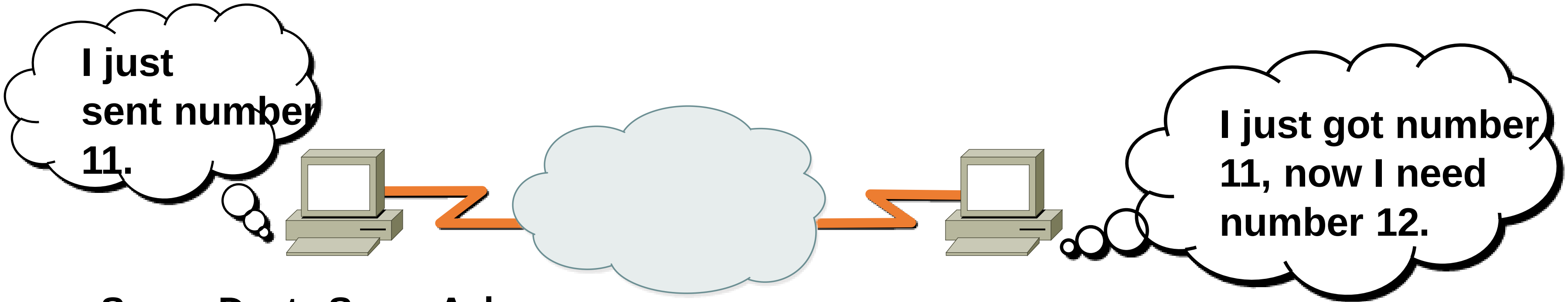
Send ACK 4

Receive ACK 4

- Window Size = 1

TCP Sequence and Acknowledgment Numbers

Source Port	Destination Port	Sequence	Acknowledgment	…



Source	Dest.	Seq.	Ack.
1028	23	10	100

→

Source	Dest.	Seq.	Ack.
23	1028	100	11

←

Source	Dest.	Seq.	Ack.
1028	23	11	101

→

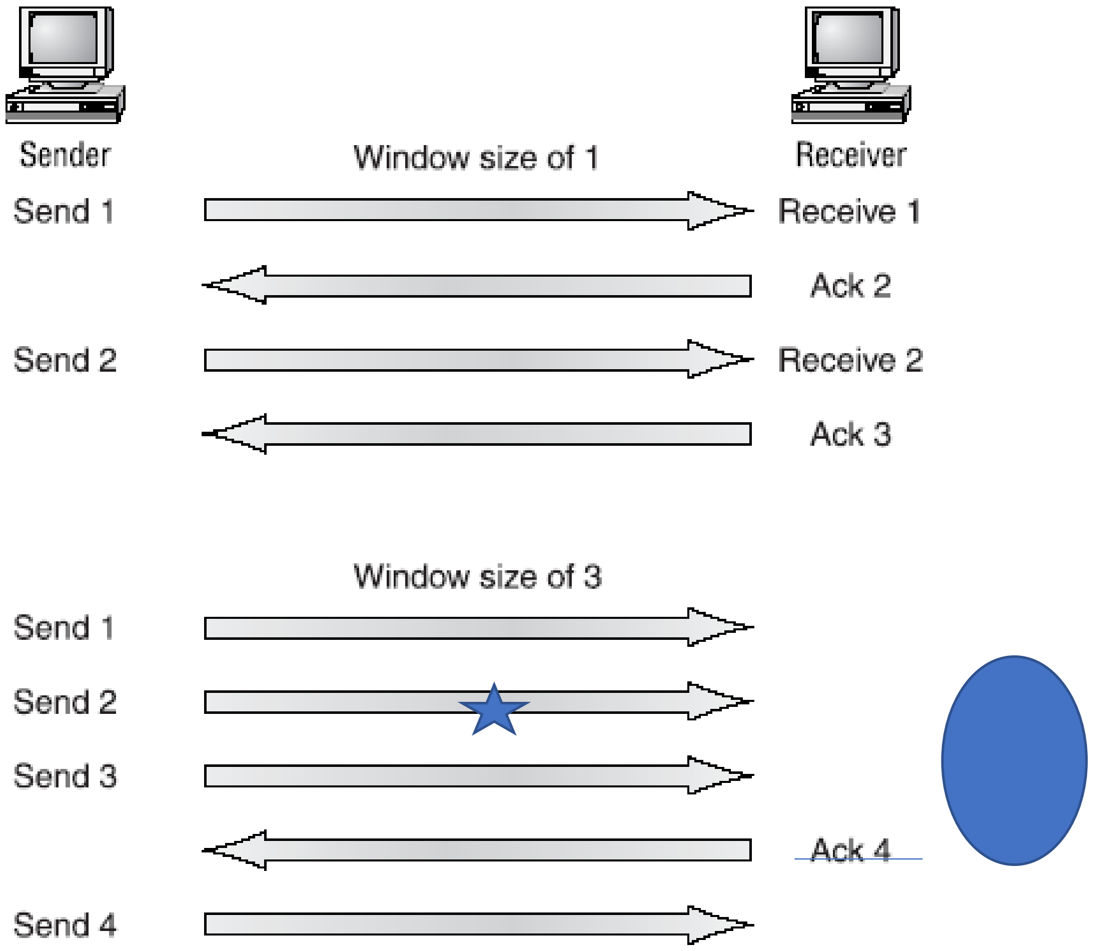
←

Source	Dest.	Seq.	Ack.
23	1028	101	12

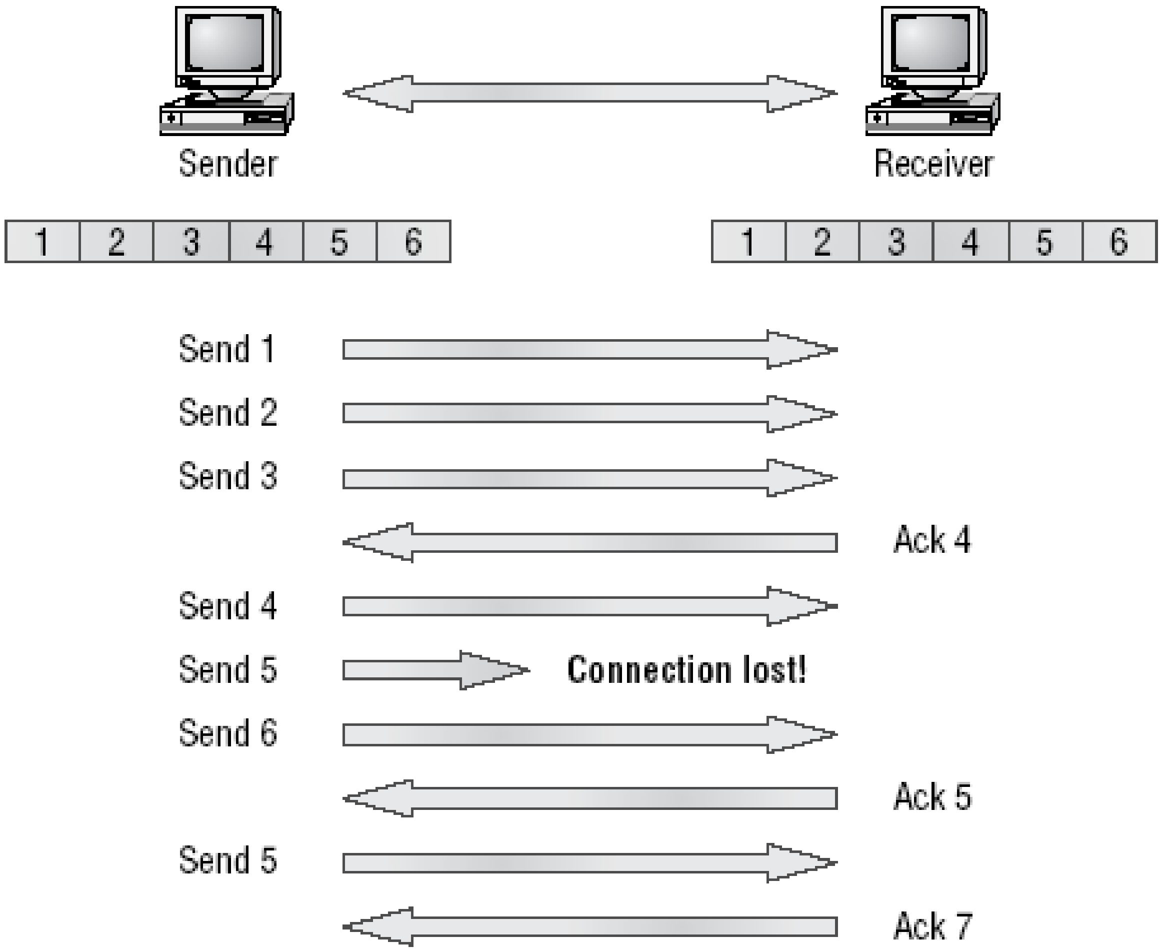
Windowing

- There are two window sizes—one set to 1 and one set to 3.
- When you’ve configured a window size of 1, the sending machine waits for an acknowledgment for each data segment it transmits before transmitting another
- If you’ve configured a window size of 3, it’s allowed to transmit three data segments before an acknowledgment is received.

Windowing


Sender
Receiver
Window size of 1
Send 1
Receive 1
Ack 2
Send 2
Receive 2
Ack 3
Window size of 3
Send 1
Send 2
Send 3
Ack 4
Send 4

Transport Layer Reliable Delivery



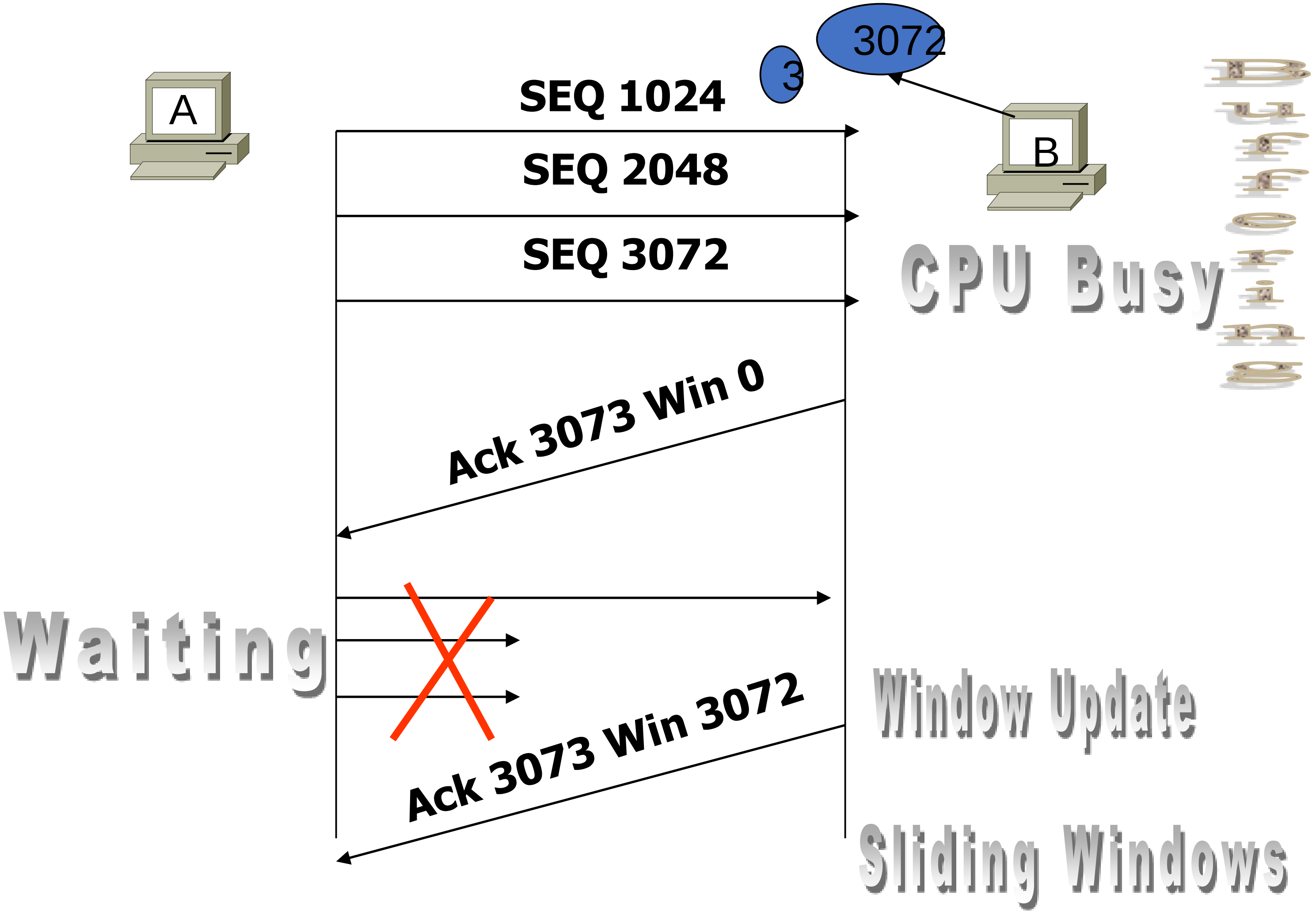
Flow Control

❑Another function of the transport layer is to provide optional flow control.

❑Flow control is used to ensure that networking devices don’t send too much information to the destination, overflowing its receiving buffer space, and causing it to drop the sent information

❑The purpose of flow control is to ensure the destination doesn't get overrun by too much information sent by the source

Flow Control



3072

3

A

SEQ 1024

SEQ 2048

SEQ 3072

B

CPU Busy

Buffering

Ack 3073 Win 0

Waiting

Ack 3073 Win 3072

Window Update

Sliding Windows

User Datagram Protocol (UDP)

User Datagram Protocol (UDP) is the connectionless transport protocol in the TCP/IP protocol stack.

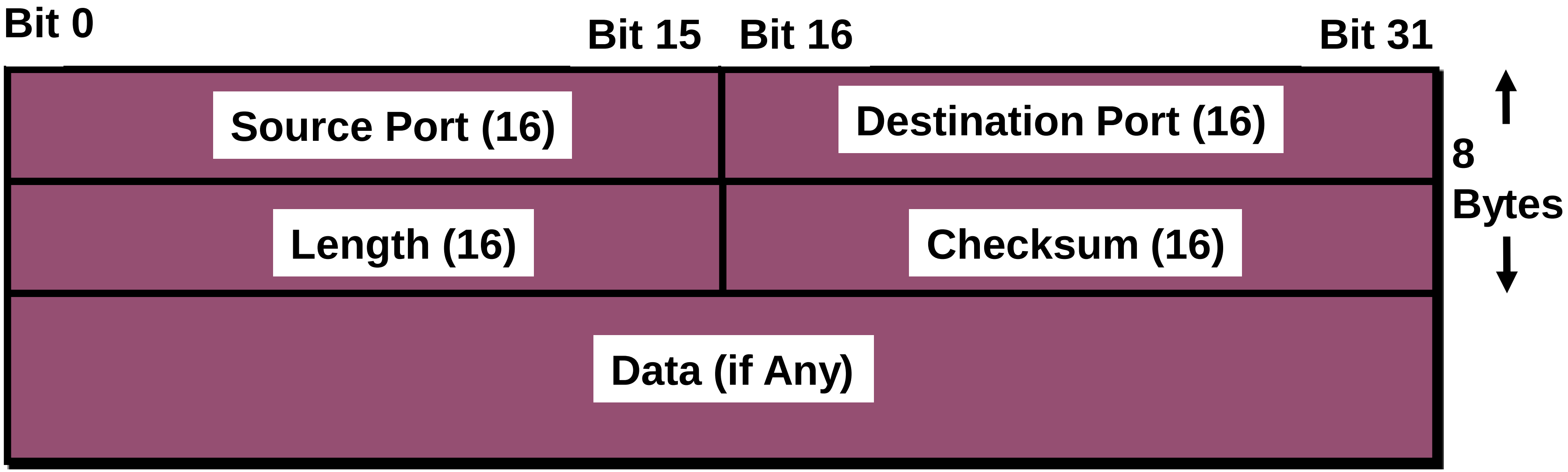
UDP is a simple protocol that exchanges datagrams, without acknowledgments or guaranteed delivery. Error processing and retransmission must be handled by higher layer protocols.

UDP is designed for applications that do not need to put sequences of segments together.

The protocols that use UDP include:

- TFTP (Trivial File Transfer Protocol)
- SNMP (Simple Network Management Protocol)
- DHCP (Dynamic Host Control Protocol)
- DNS (Domain Name System)

UDP Segment Format



Bit 0

Bit 15

Bit 16

Bit 31

Source Port (16)

Destination Port (16)

Length (16)

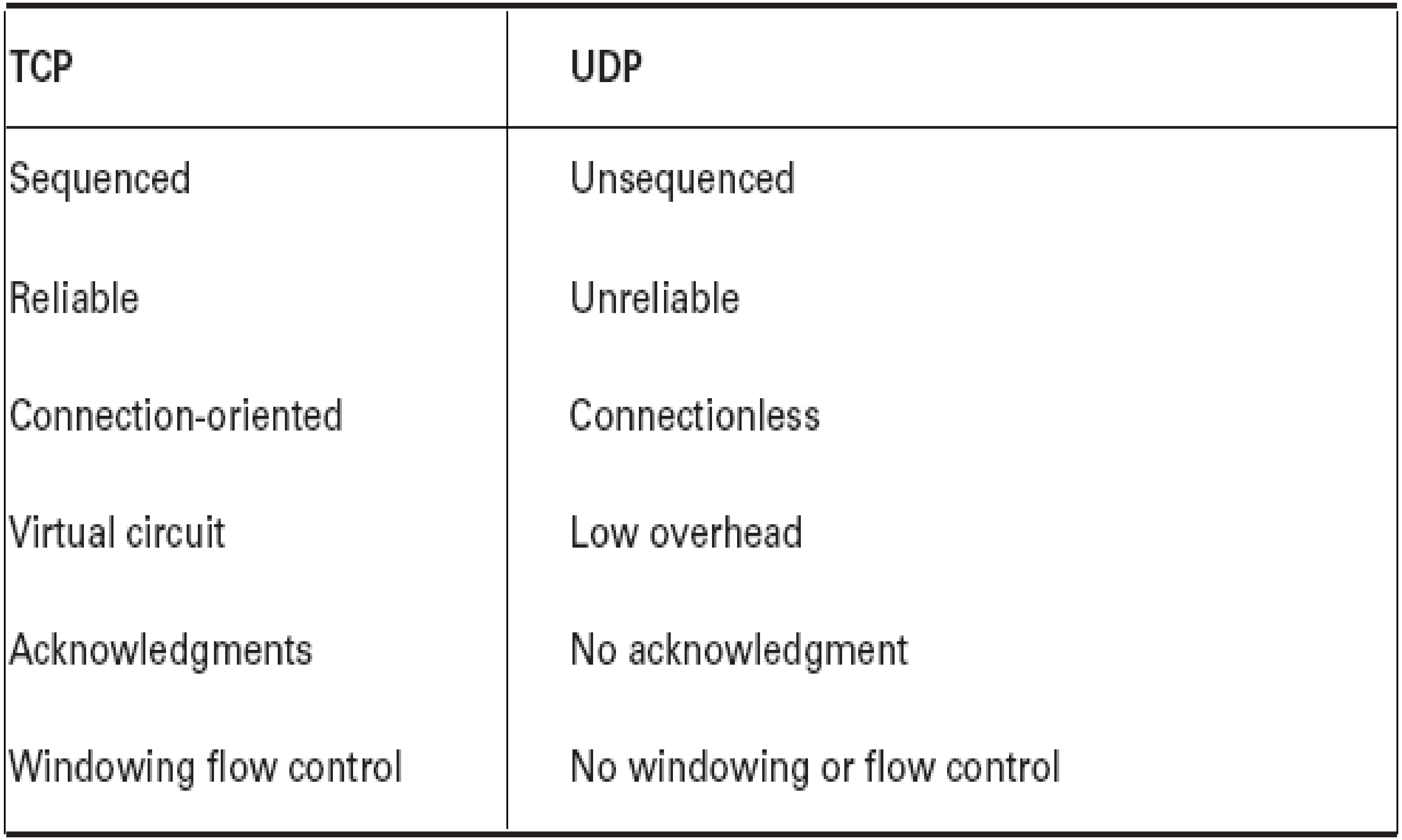
Checksum (16)

Data (if Any)

8 Bytes

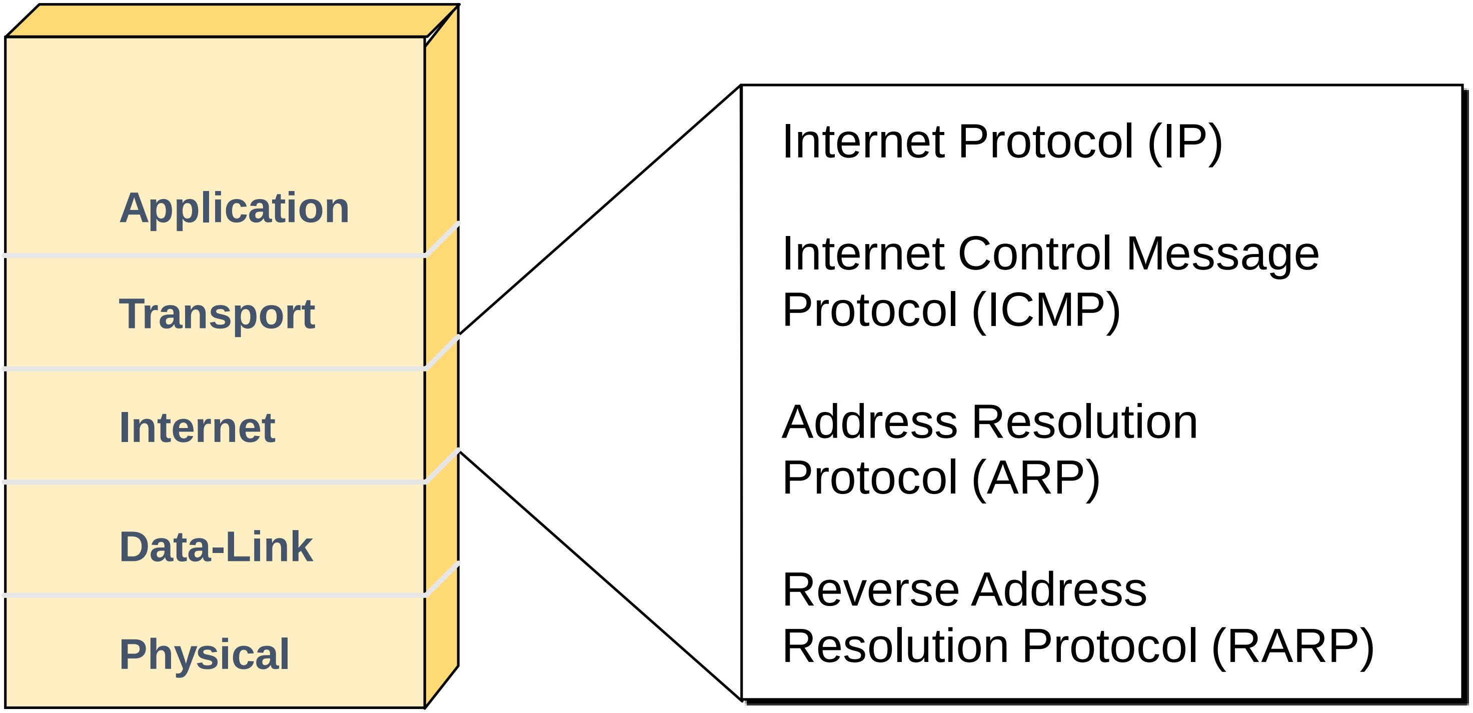
- No sequence or acknowledgment fields

TCP vs UDP



TCP	UDP
Sequenced	Unsequenced
Reliable	Unreliable
Connection-oriented	Connectionless
Virtual circuit	Low overhead
Acknowledgments	No acknowledgment
Windowing flow control	No windowing or flow control

Internet Layer Overview



Application

Transport

Internet

Data-Link

Physical

Internet Protocol (IP)

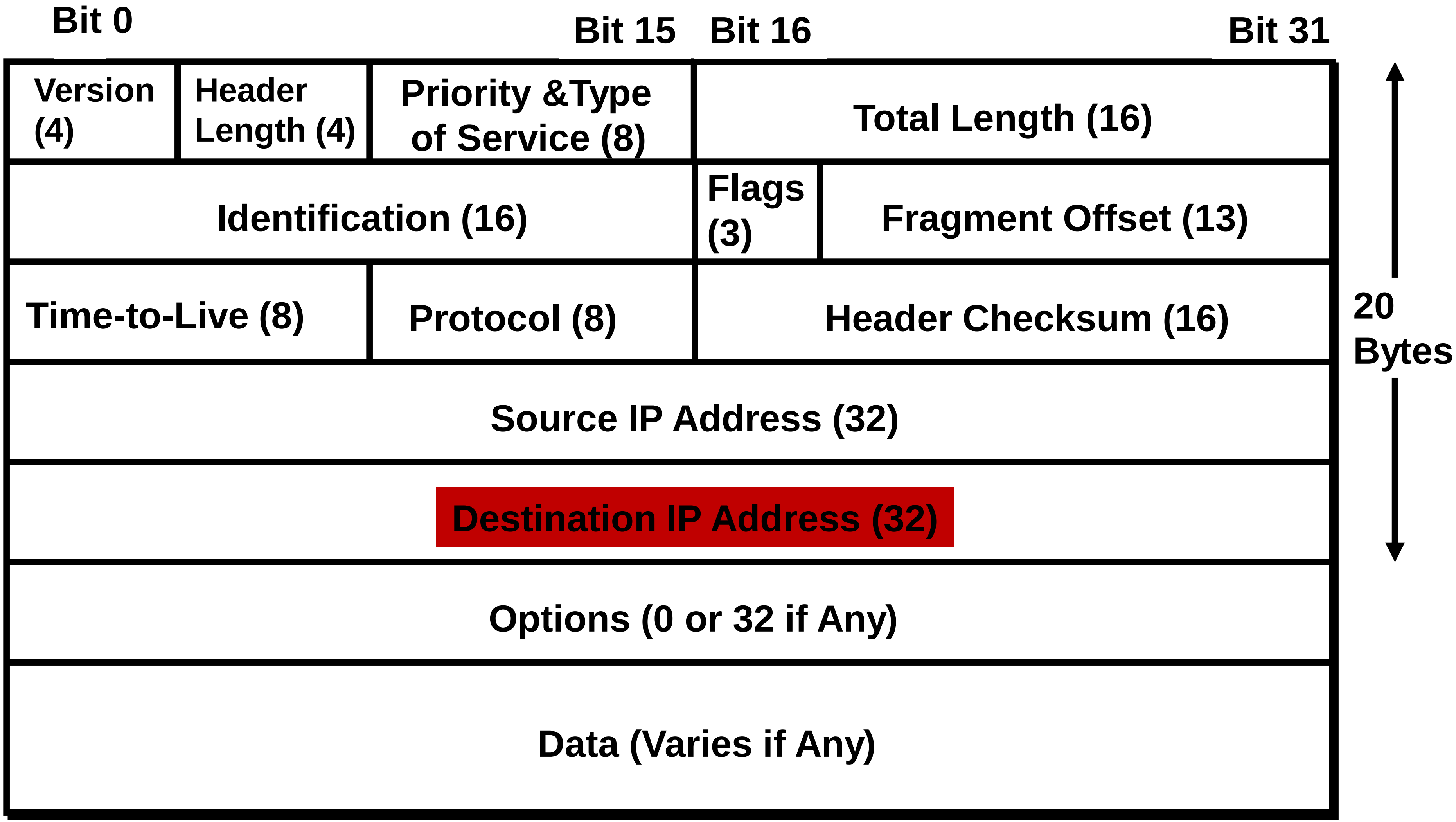
Internet Control Message Protocol (ICMP)

Address Resolution Protocol (ARP)

Reverse Address Resolution Protocol (RARP)

- In the OSI reference model, the network layer corresponds to the TCP/IP Internet layer.

IP Datagram



Bit 0

Bit 15

Bit 16

Bit 31

Version (4)

Header Length (4)

Priority &Type of Service (8)

Total Length (16)

Identification (16)

Flags (3)

Fragment Offset (13)

Time-to-Live (8)

Protocol (8)

Header Checksum (16)

Source IP Address (32)

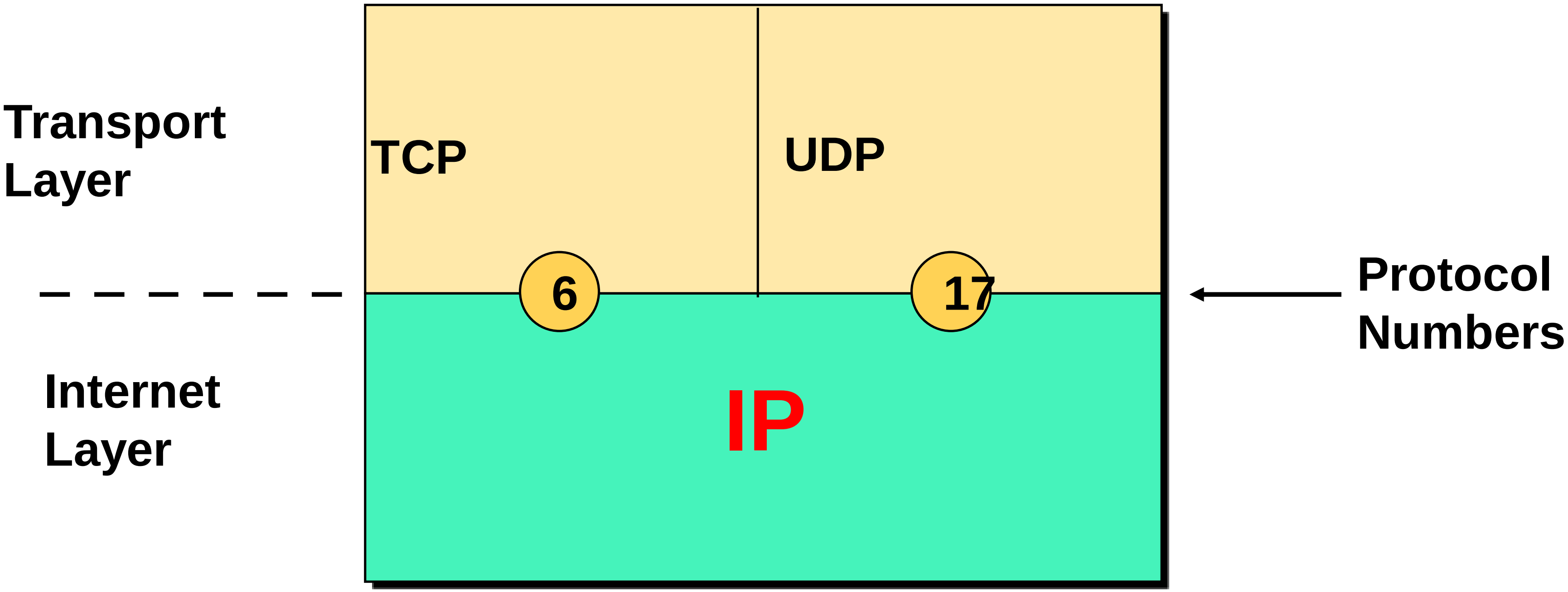
Destination IP Address (32)

Options (0 or 32 if Any)

Data (Varies if Any)

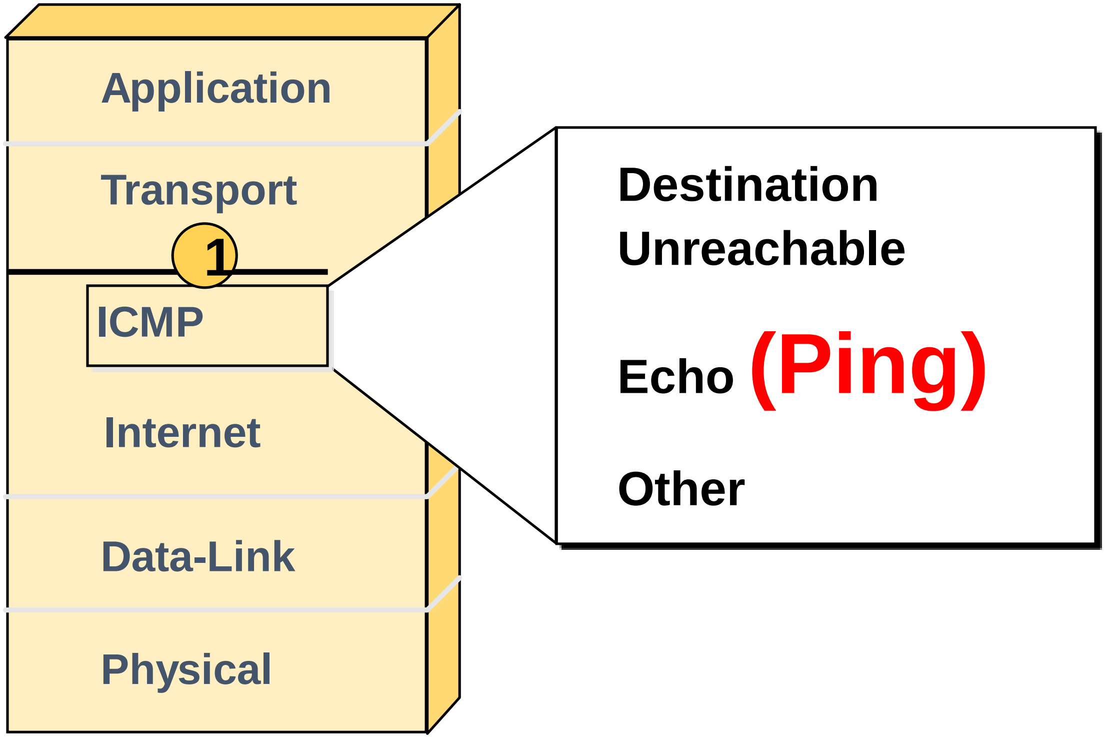
20 Bytes

Protocol Field



- Determines destination upper-layer protocol

Internet Control Message Protocol

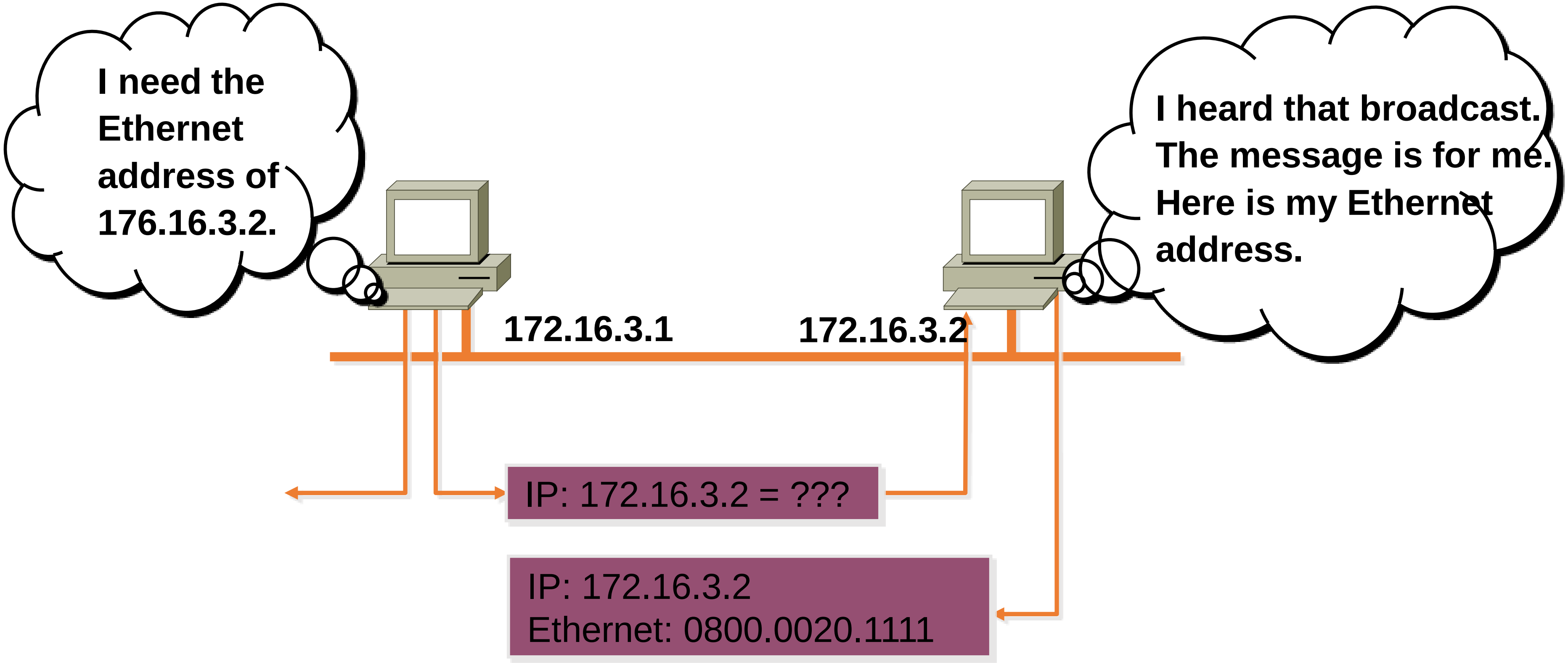


Destination Unreachable

Echo (Ping)

Other

Address Resolution Protocol



I need the Ethernet address of 176.16.3.2.

I heard that broadcast. The message is for me. Here is my Ethernet address.

172.16.3.1

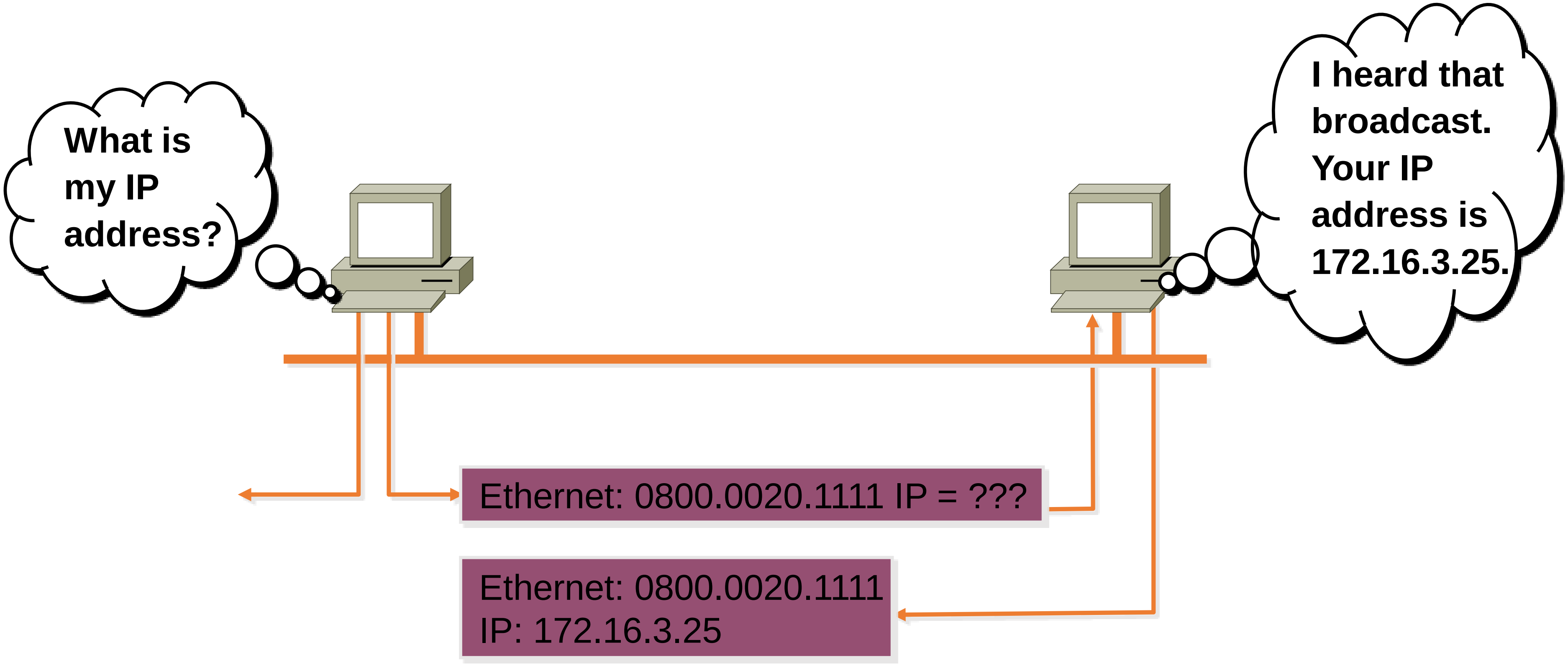
172.16.3.2

IP: 172.16.3.2 = ???

IP: 172.16.3.2
Ethernet: 0800.0020.1111

- Map IP → MAC
- Local ARP

Reverse ARP



What is my IP address?

I heard that broadcast. Your IP address is 172.16.3.25.

Ethernet: 0800.0020.1111 IP = ???

Ethernet: 0800.0020.1111
IP: 172.16.3.25

- Map MAC → IP