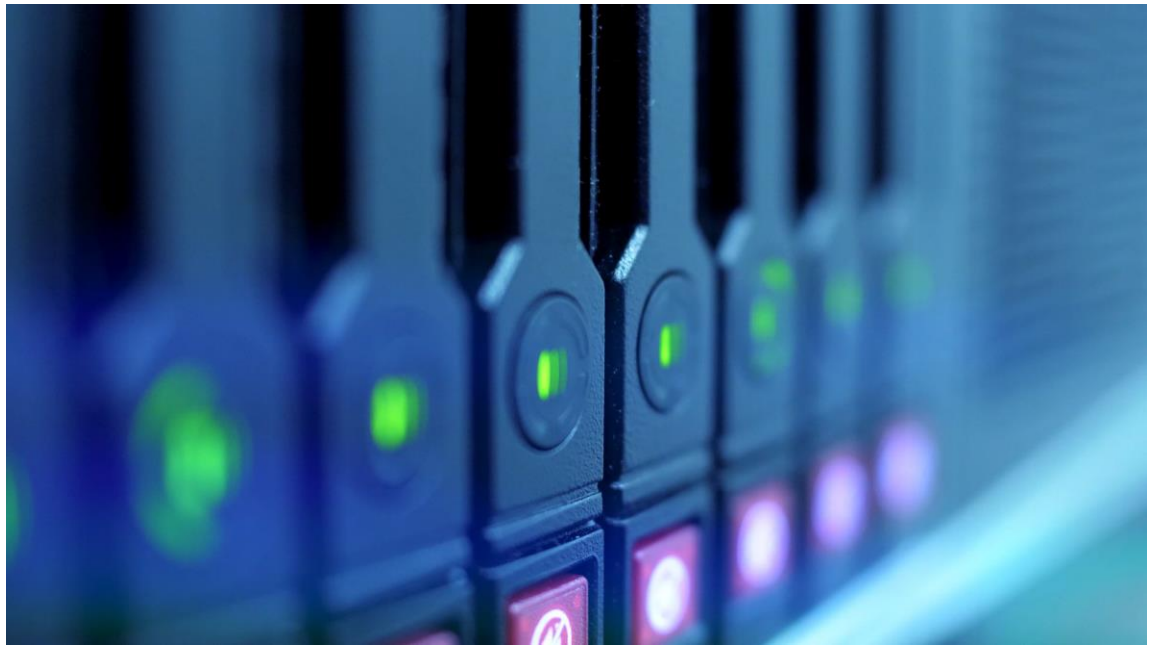
OSI

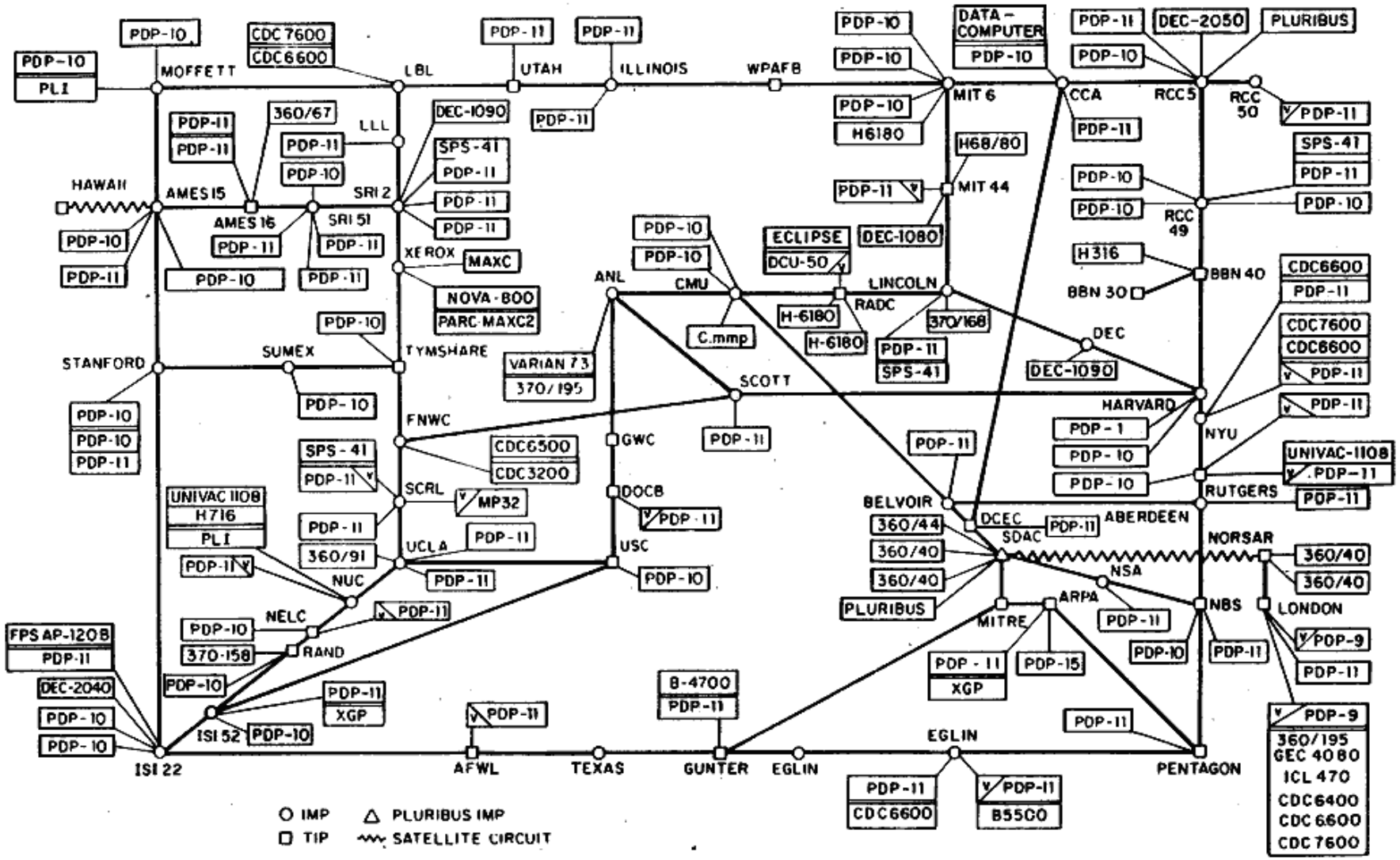
OPEN SYSTEMS INTERCONNECTION MODEL



DR. DARRYL J DSOUZA

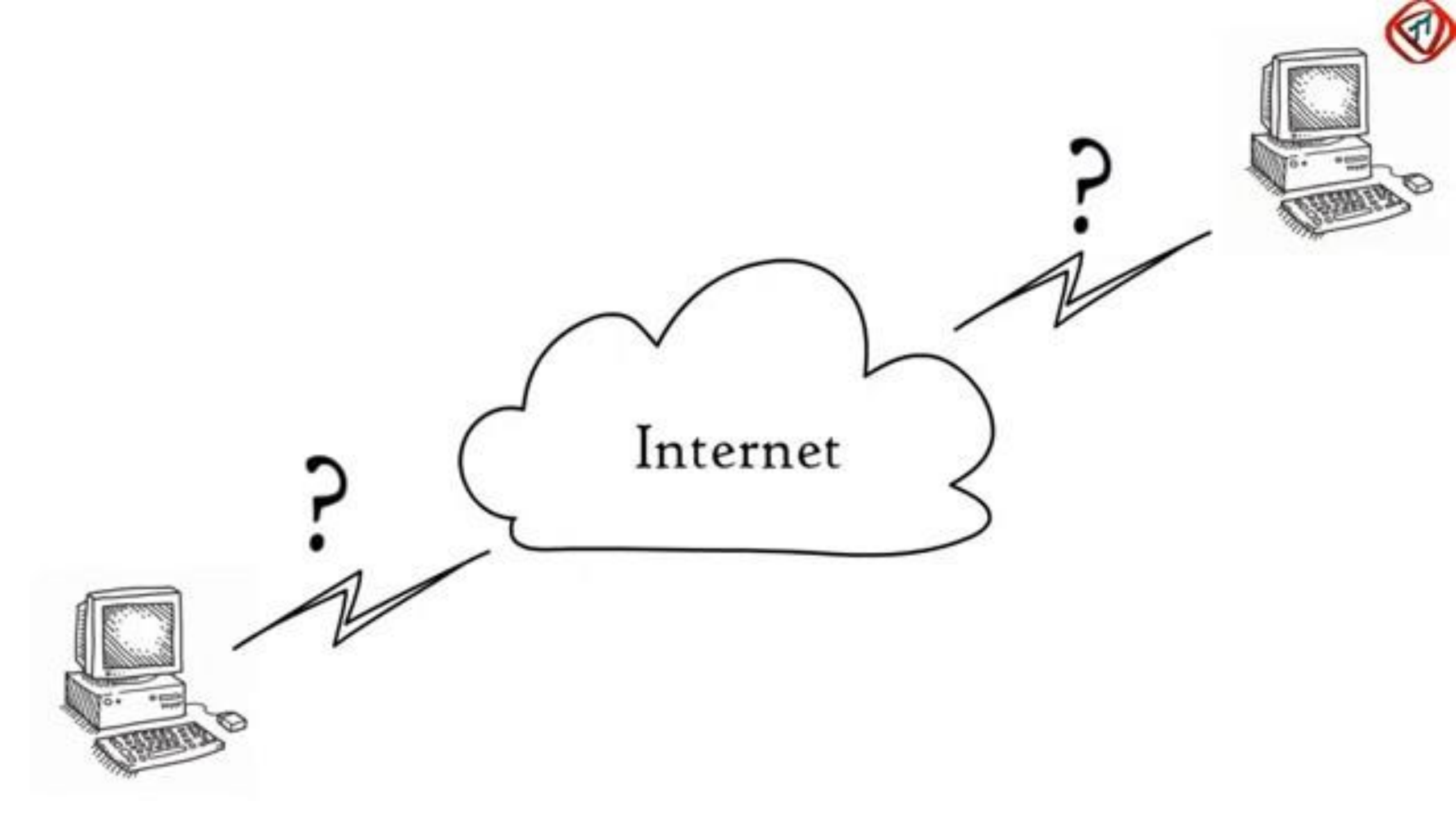
MOB NO: 9986382162

ARPANET LOGICAL MAP, MARCH 1977

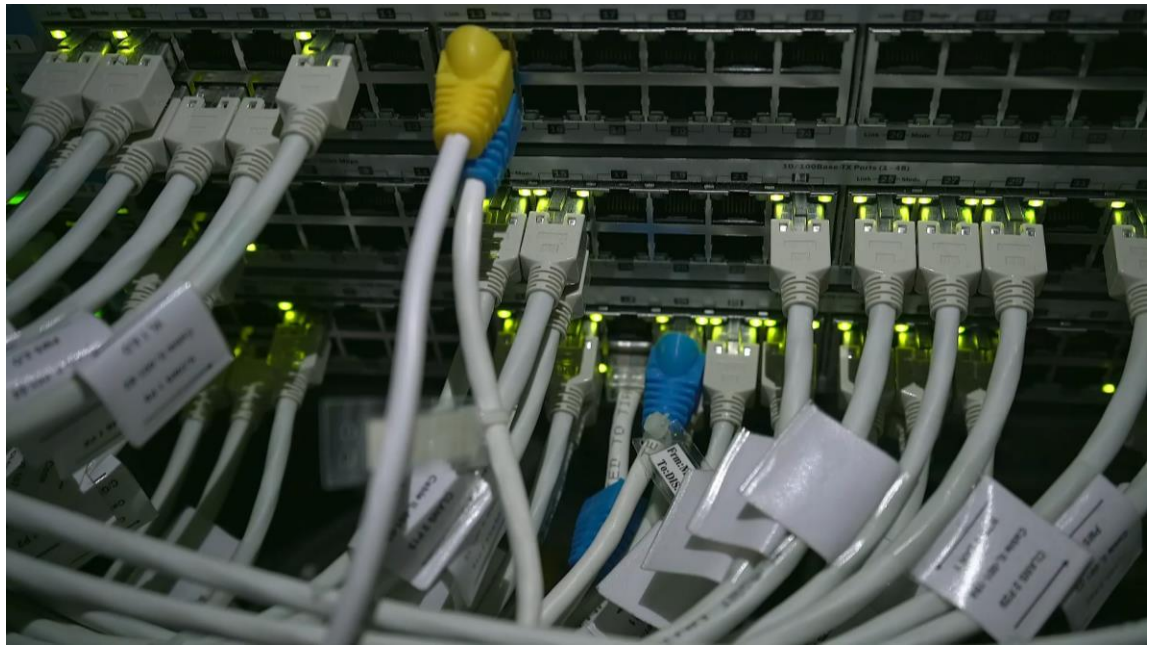


(PLEASE NOTE THAT WHILE THIS MAP SHOWS THE HOST POPULATION OF THE NETWORK ACCORDING TO THE BEST INFORMATION OBTAINABLE, NO CLAIM CAN BE MADE FOR ITS ACCURACY)

NAMES SHOWN ARE IMP NAMES, NOT (NECESSARILY) HOST NAMES


?
Internet
?

UNDERSTANDING NETWORK PROTOCOLS AND STANDARDS



Network Protocols

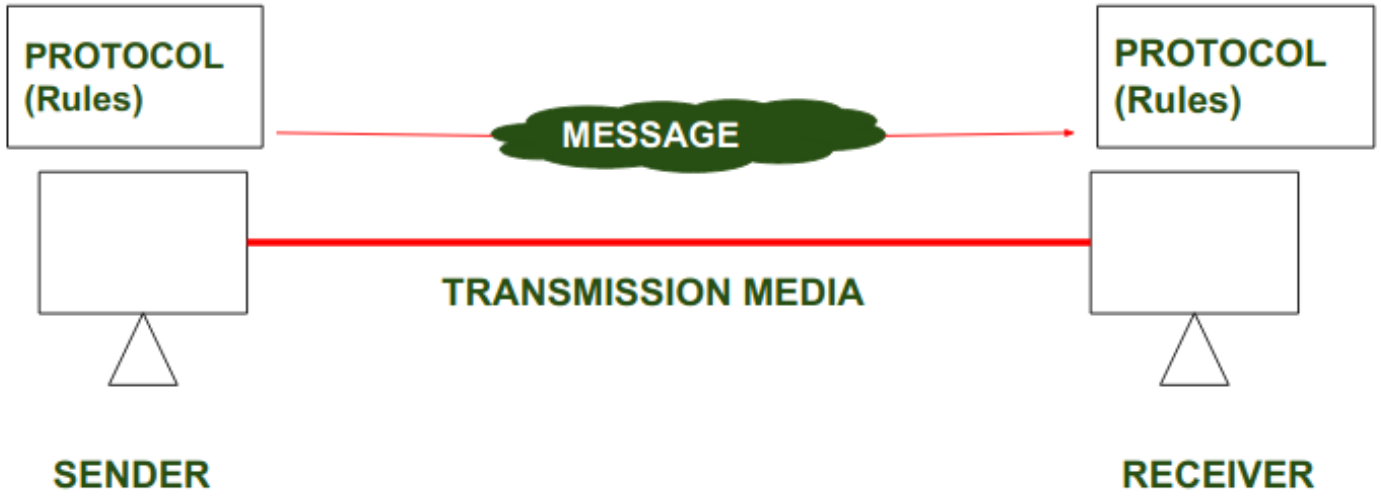
set of rules and conventions

- A protocol is a set of rules that enables effective communications to occur. Computer networks depend upon many different types of protocols in order to work. These protocols are very rigidly defined, and for good reason.
- Network cards must know how to talk to other network cards in order to exchange information, operating systems must know how to talk to network cards in order to send and receive data on the network, and application programs must know how to talk to operating systems in order to know how to retrieve a file from a network server.
- Protocols come in many different types. At the lowest level, protocols define exactly what type of electrical signal represents a one and what type of signal represents a zero. At the highest level, protocols allow a computer user in the United States to send an e-mail message to another computer user in New Zealand. And in between are many other levels of protocols. Example about these levels of protocols (which are often called layers), “The Seven Layers of the OSI Reference Model,”.

UNDERSTANDING PROTOCOLS

UNDERSTANDING PROTOCOLS

In Order to make communication successful between devices , some rules and procedures should be agreed upon at the sending and receiving ends of the system. Such rules and procedures are called as Protocols . Different types of protocols are used for different types of communication.



KEY ELEMENT OF PROTOCOL

- **Syntax :** syntax refers to the structure or the format of the data that gets exchanged between the devices. Syntax of message includes the type of data, composition of message and sequencing of message. The starting 8 bits of data is considered as the address of the sender. The next 8 bits is considered to be the address of the receiver. The remaining bits are considered as the message itself.
- **Semantics :** Semantics defines data transmitted between devices. It provides rules and norms for understanding message or data element values and actions.
- **Timing :** Timing refers to the synchronization and coordination between devices while transferring the data. Timing ensures at what time data should be sent and how fast data can be sent. For example, If a sender sends 100 Mbps but the receiver can only handle 1 Mbps, the receiver will overflow and lose data. Timing ensures preventing data loss, collisions and other timing related issues.
- **Sequence control :** Sequence control ensures the proper ordering of data packets. The main responsibility of sequence control is to acknowledge the data while it get received, and the retransmission of lost data. Through this mechanism the data is delivered in correct order.
- **Flow Control :** Flow control regulates device data delivery. It limits the sender's data or asks the receiver if it's ready for more. Flow control prevents data congestion and loss.
- **Error Control :** Error control mechanisms detect and fix data transmission faults. They include error detection codes, data resend, and error recovery. Error control detects and corrects noise, interference, and other problems to maintain data integrity.
- **Security :** Network security safeguards data confidentiality, integrity, and authenticity. which includes encryption, authentication, access control, and other security procedures. Network communication's privacy and trustworthiness are protected by security standards.

LAYERS OF PROTOCOLS

- Modern communication systems are very complex and many different organisations are involved in writing the software and developing the hardware that allow devices to communicate.
- To allow communication systems to be as open as possible, the different processes are divided up into layers, and each layer has a defined responsibility. The layers are ordered so that data moves from one layer to the next in its journey from the application (that the end-user interacts with) to the point at which it can be transmitted across a network.
- The specification for the interface between each layer is well documented. This means that software developers just need to make sure that the data is in the correct format (so that it can move from one layer to the next). The advantage of this is that each layer is independent of the others. For example, you can use the same web browser regardless of whether you connect to the internet using a local area network or through a mobile phone.

Various protocols tend to be used together in matched sets called protocol suites. The two most popular protocol suites for networking are TCP/IP and IPX/SPX. TCP/IP was originally developed for UNIX networks and is the protocol of the Internet. IPX/SPX was originally developed for NetWare networks and IPX/SPX was supported up to and including the era of Windows XP, with later operating systems moving to the modern TCP/IP protocol suite. A third important protocol is Ethernet, a low-level protocol that's used with both TCP/IP and IPX/SPX.

UNDERSTANDING PROTOCOLS

TYPES OF PROTOCOLS

Protocols can be broadly divided into the following two types:

- Proprietary Protocols
- Standard Protocols

PROPRIETARY PROTOCOLS

Proprietary protocols are developed by an individual organization for their specific devices. We have to take permission from the organization if we want to use their protocols.

It is not a standard protocol and it supports only specific devices. We may have to pay for these protocols.

Some of the examples of Proprietary Protocols are *IMessage, Apple Talk, etc.*

STANDARD PROTOCOLS

A standard protocol is a mandated protocol for all devices. It supports multiple devices and acts as a standard.

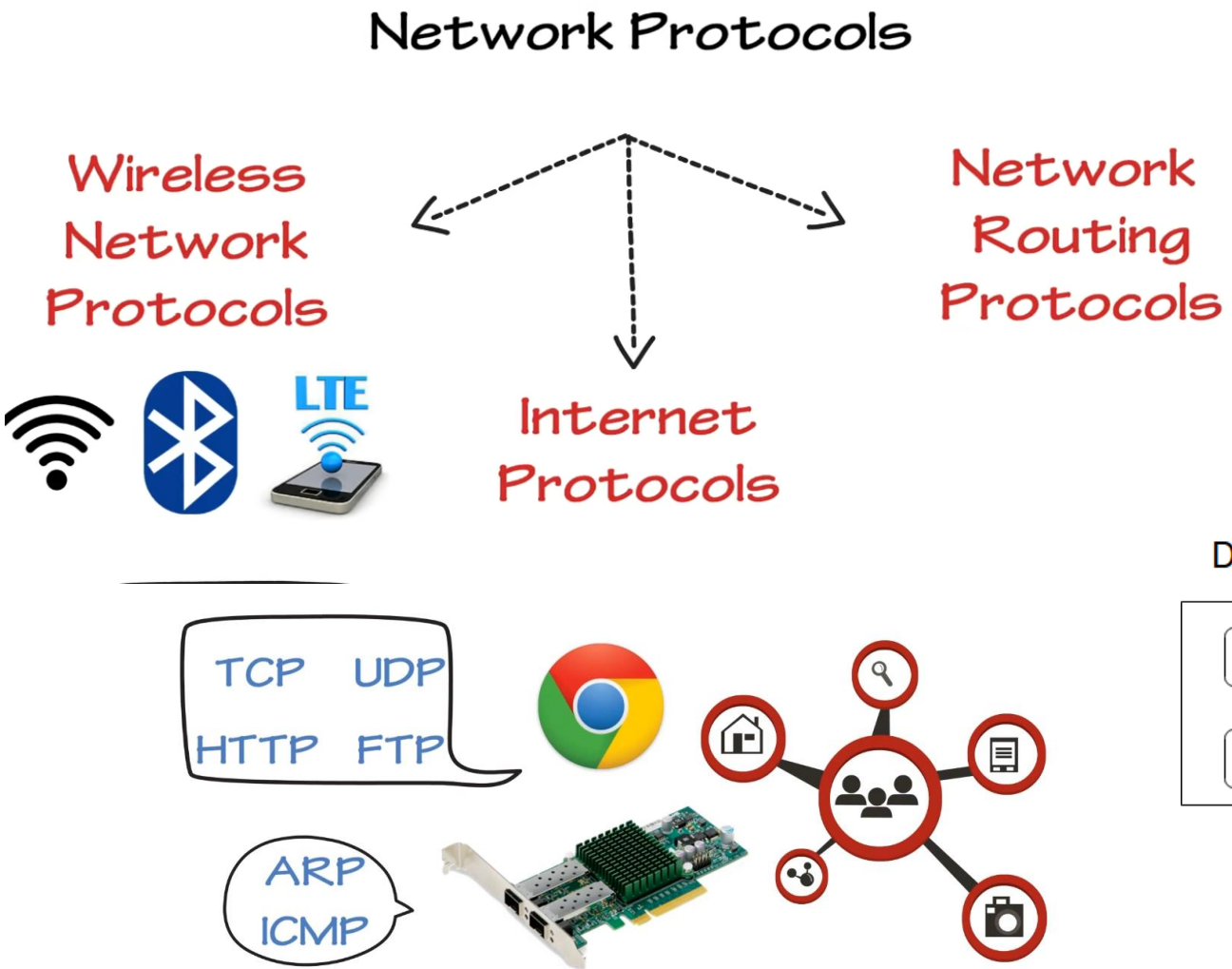
Standard protocols are not vendor-specific i.e. they are not specific to a particular company or organization. They are developed by a group of experts from different organizations .

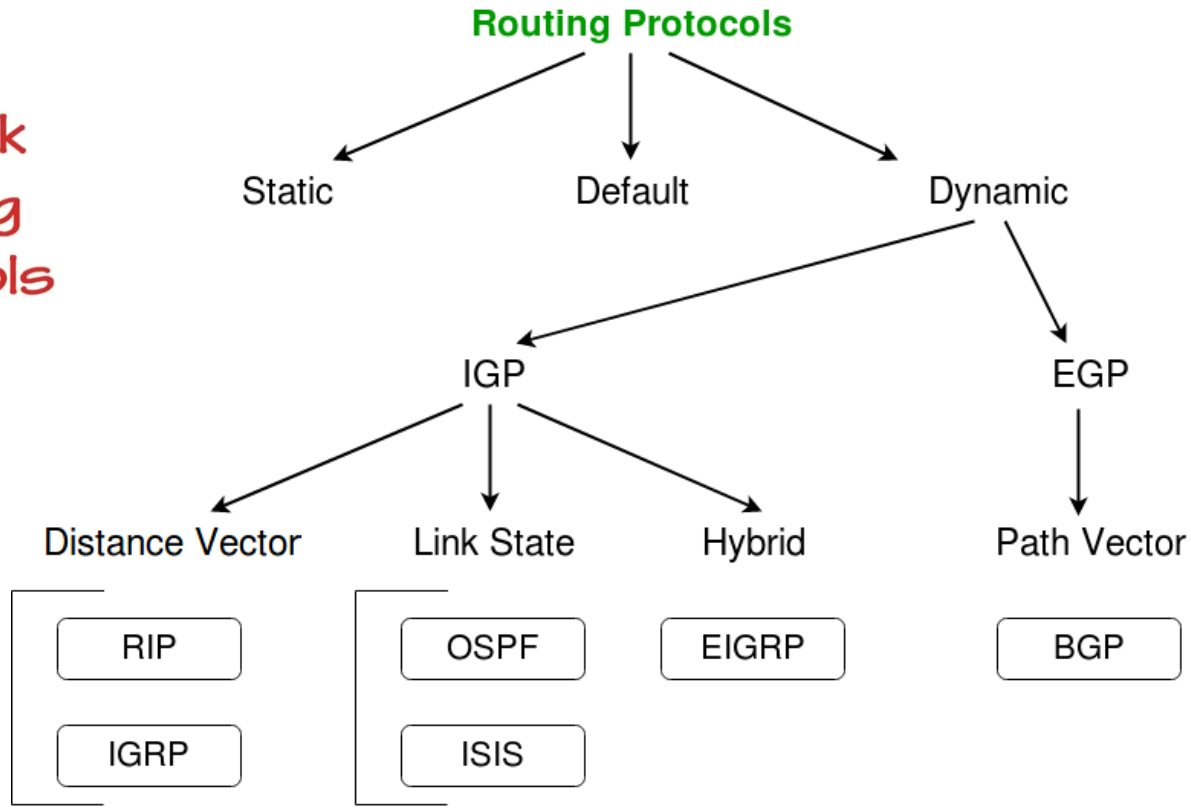
These protocols are publicly available, and we need not pay for them.

Some of the examples of Standard Protocols are FTP, DNS, DHCP, SMTP, TELNET, TFTP, etc.

Protocol	Layer	Full name and purpose
HTTP	Application	Hypertext Transfer Protocol. Used to make a request for a webpage. The server returns the page or an error code if there was a problem with the request.
HTTPS	Application	Hypertext Transfer Protocol Secure. Sends an encrypted request for a webpage. The server returns the encrypted page or an error code if there was a problem with the request.
FTP	Application	File Transfer Protocol. Used to upload or download a file. The server opens a data connection (over which the file will be transferred) or sends an error code if there was a problem with the request.
SMTP	Application	Simple Mail Transfer Protocol. Used to send an email to an email server. The server returns a code indicating whether or not the email could be delivered.
POP	Application	Post Office Protocol. Used to request any new emails for a specific email account. The server returns the emails (if there are any).
IMAP	Application	Internet Message Access Protocol. Used to synchronise a client email account with an account on a mail server. The server returns new emails (if there are any) and deletes any emails that were deleted locally on the client application. This allows a user to use multiple devices to access their email account.

Protocol	Layer	Full name and purpose
DHCP	Application	Dynamic Host Configuration Protocol. Used to assign IP addresses and other configuration options to devices in a network.
TCP	Transport	Transmission Control Protocol. When data is to be sent (whether from client or server), the data is split into packets and each packet is given a sequence number. This is a **reliable** transmission protocol. At the receiving end, the packets are checked. If any packets go missing, they will be resent.
UDP	Transport	User Datagram Protocol. Data is split into packets (as with TCP). However, this is an **unreliable** transmission protocol. If any packets arrive out of sequence or are missing, they are ignored. UDP is suitable where data does not have to be 100% accurate but speed is important, e.g. with some video streaming services or VOIP.
IP	Network (Internet)	Internet Protocol. Creates a new packet (imagine putting the packet from the transport layer into a new envelope). Adds the source and destination IP addresses to allow the packet to be delivered. These are the packets that are routed across the internet.
Ethernet and Wi-Fi protocols	Link (data link)	Encapsulates the data from the previous layer into frames (another kind of packet) with a source and destination MAC address, and manages multiple transmissions on the media.


Network Protocols
Wireless Network Protocols
Network Routing Protocols
Internet Protocols
LTE
TCP UDP
HTTP FTP
ARP
ICMP


Routing Protocols
Static
Default
Dynamic
IGP
EGP
Distance Vector
Link State
Hybrid
Path Vector
RIP
IGRP
OSPF
ISIS
EIGRP
BGP

- A standard is an agreed-upon definition of a protocol. In the early days of computer networking, each computer manufacturer developed its own networking protocols. As a result, you weren't able to easily mix equipment from different manufacturers on a single network.
- Then along came standards to save the day. Standards are industry-wide protocol definitions that are not tied to a particular manufacturer. With standard protocols, you can mix and match equipment from different vendors.
- As long as the equipment implements the standard protocols, it should be able to coexist on the same network.

UNDERSTANDING STANDARDS

NETWORK STANDARDS (DATA COMMUNICATIONS AND NETWORKING)

- **The Importance of Standards**
- **Standards are necessary in almost every business** and public service entity. For example, before 1904, fire hose couplings in the United States were not standard, which meant a fire department in one community could not help in another community. The transmission of electric current was not standardized until the end of the nineteenth century, so customers had to choose between Thomas Edison's direct current (DC) and George Westinghouse's alternating current (AC).
- **The primary reason for standards** is to ensure that hardware and software produced by different vendors can work together. Without networking standards, it would be difficult—if not impossible—to develop networks that easily share information. Standards also mean that customers are not locked into one vendor. They can buy hardware and software from any vendor whose equipment meets the standard. In this way, standards help to promote more competition and hold down prices.
- The use of standards makes it much easier to develop software and hardware that link different networks because software and hardware can be developed one layer at a time.

TYPES OF STANDARDS

- Standards are of two types :
- De Facto Standard.
- De Jure Standard.

De Facto Standard : The meaning of the work ” *De Facto* ” is ” By Fact ” or “By Convention”.These are the standard s that have not been approved by any Organization , but have been adopted as Standards because of it’s widespread use. Also , sometimes these standards are often established by Manufacturers.

- **For example :** Apple and Google are two companies which established their own rules on their products which are different . Also they use some same standard rules for manufacturing for their products.

De Jure Standard : The meaning of the word “*De Jure*” is “By Law” or “By Regulations”.Thus , these are the standards that have been approved by officially recognized body like ANSI , ISO , IEEE etc. These are the standard which are important to follow if it is required or needed.

- **For example :** All the data communication standard protocols like SMTP , TCP , IP , UDP etc. are important to follow the same when we needed them.

MANY ORGANIZATIONS ARE INVOLVED IN SETTING STANDARDS FOR NETWORKING. THE FIVE MOST IMPORTANT ORGANIZATIONS ARE

✦ **American National Standards Institute (ANSI):** The official standards organization in the United States. ANSI is pronounced *An-See*.

✦ **Institute of Electrical and Electronics Engineers (IEEE):** An international organization that publishes several key networking standards; in particular, the official standard for the Ethernet networking system (known officially as IEEE 802.3). IEEE is pronounced *Eye-triple-E*.

✦ **International Organization for Standardization (ISO):** A federation of more than 100 standards organizations from throughout the world.

✦ **Internet Engineering Task Force (IETF):** The organization responsible for the protocols that drive the Internet.

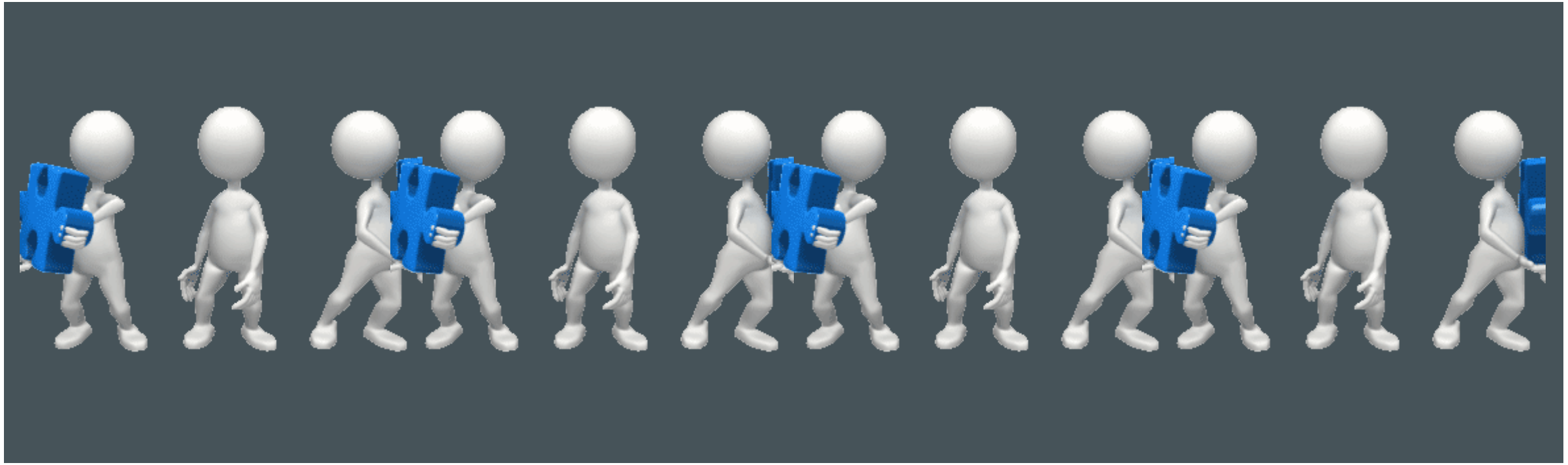
✦ **World Wide Web Consortium (W3C):** An international organization that handles the development of standards for the World Wide Web.

✦ **TIA (Telecommunications Industry Association) /EIA (Electronic Industries Association):** TIA/EIA structured cabling standards define how to design, build, and manage a cabling system that is structured

Table 2-1 Web Sites for Major Standards Organizations

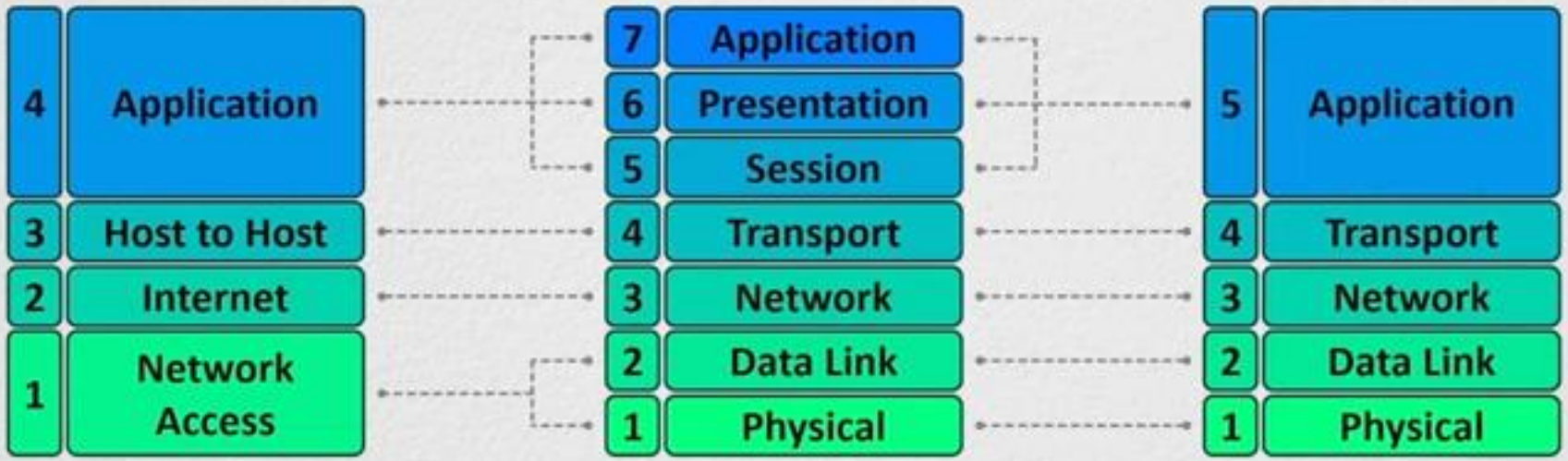
Organization	*Web Site*
ANSI (American National Standards Institute)	`www.ansi.org`
IEEE (Institute of Electrical and Electronic Engineers)	`www.ieee.org`
ISO (International Organization for Standardization)	`www.iso.org`
IETF (Internet Engineering Task Force)	`www.ietf.org`
W3C (World Wide Web Consortium)	`www.w3c.org`

OSI MODEL



Goal of Networking:

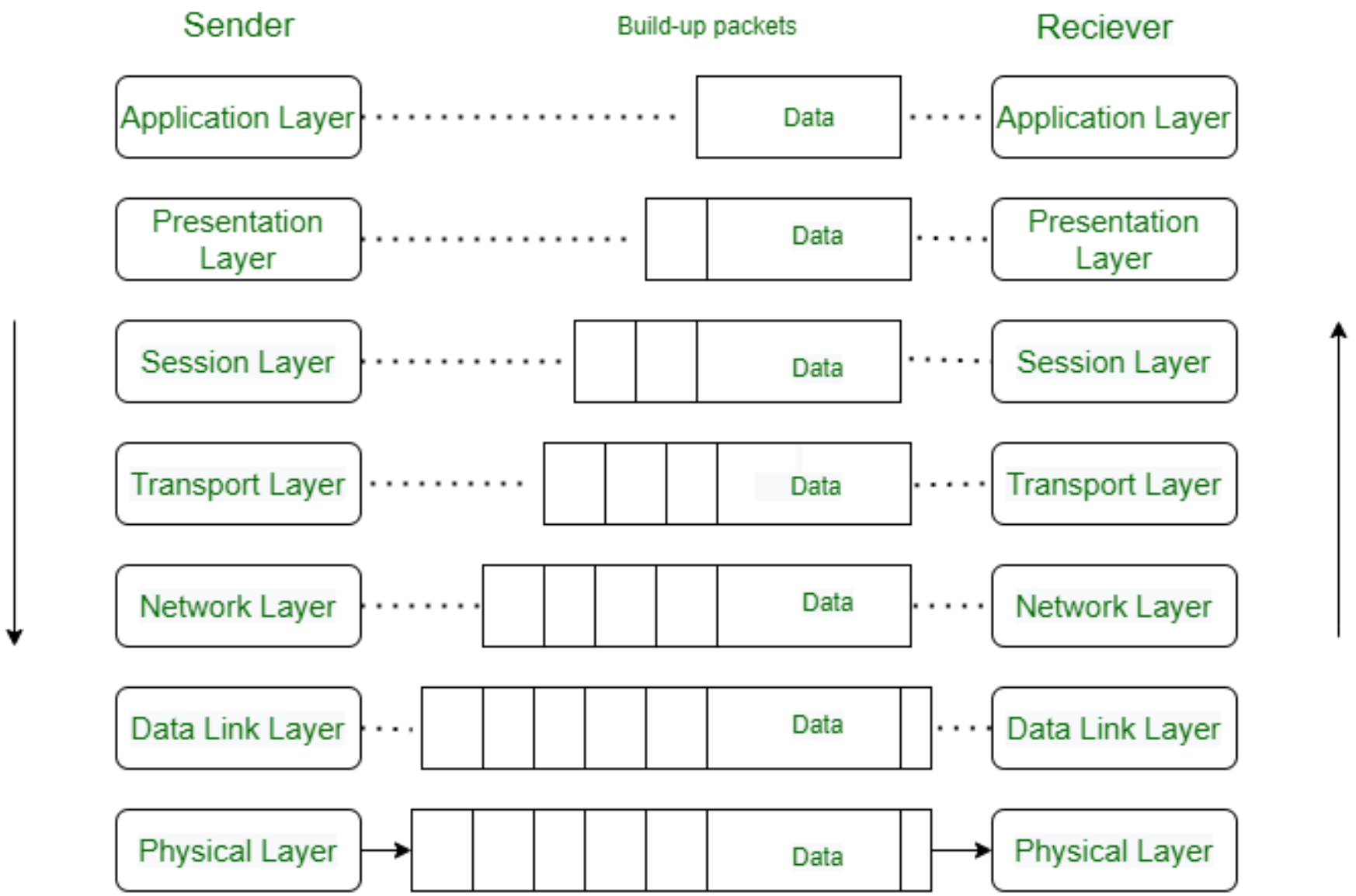
Allow two users to share data between computers



TCP/IP
Four Layer

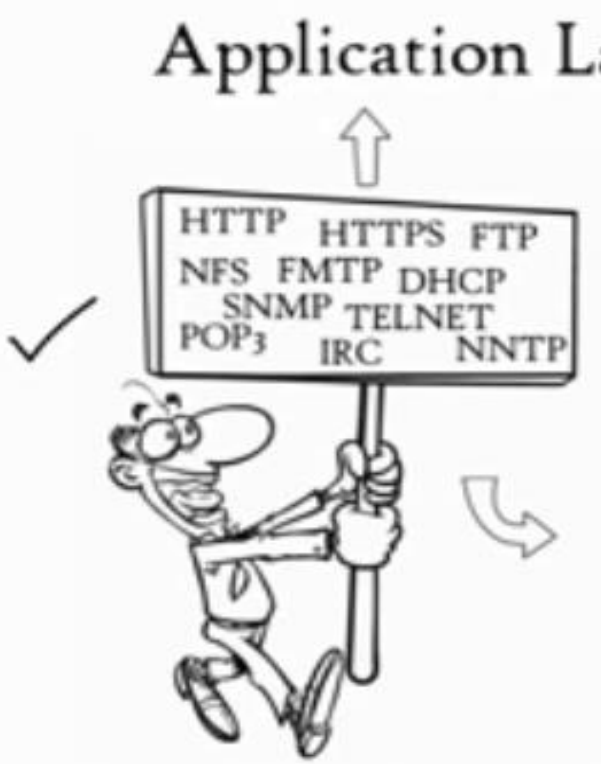
OSI Model
Seven Layer

TCP/IP
Five Layer


Sender
Build-up packets
Reciever
Application Layer
Data
Application Layer
Presentation Layer
Data
Presentation Layer
Session Layer
Data
Session Layer
Transport Layer
Data
Transport Layer
Network Layer
Data
Network Layer
Data Link Layer
Data
Data Link Layer
Physical Layer
Data
Physical Layer

LAYER 7 – APPLICATION LAYER

Application Layer: Network Applications



File Transfer

Web Surfing

Emails

Virtual Terminals

FTP

HTTP/S

SMTP

Telnet

FEATURES PROVIDED BY APPLICATION LAYER PROTOCOLS

To ensure smooth communication, application layer protocols are implemented the same on source host and destination host.
The following are some of the features which are provided by Application layer protocols-

- The Application Layer protocol defines process for both parties which are involved in communication.
- These protocols define the type of message being sent or received from any side (either source host or destination host).
- These protocols also define basic syntax of the message being forwarded or retrieved.
- These protocols define the way to send a message and the expected response.
- These protocols also define interaction with the next level.

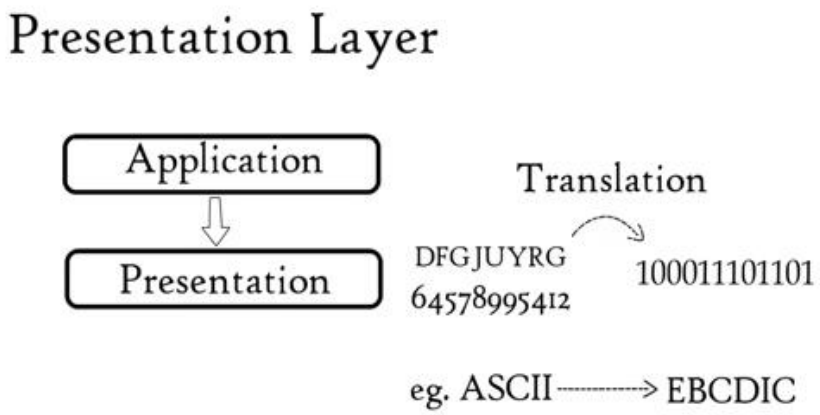
LAYER 6 – PRESENTATION LAYER

PRESENTATION LAYER

Translation

Data is sent from sender to receiver, but what if the sender device and receiver device understand different formats of code? For example, suppose one device understands ASCII code and another device understands EBCDIC code.

In that case, the data must be translated into a code that the recipient understands to determine what data has been sent. The presentation layer is responsible for translating ASCII codes to EBCDIC or vice versa. With the help of the presentation layer, the receiver understands the data effectively and uses it efficiently.



- Layer 7 determines what the interpreted characters do
  - i.e., application commands

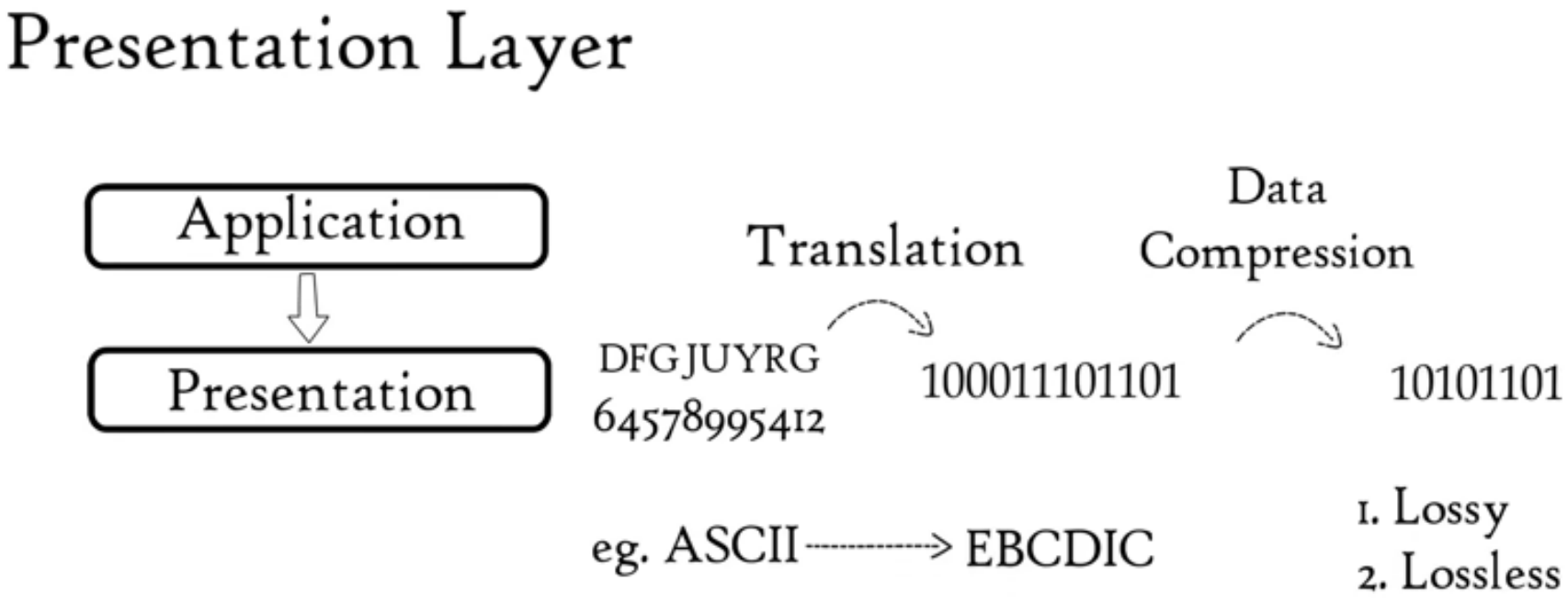
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

G	E	T	(space)	/	s	i	m
01000111	01000101	01010100	00100000	00101111	01110011	01101001	01101101

HTTP — **GET** Request a Webpage

```
GET /index.html HTTP/1.1
Host: hello.com
```

DATA COMPRESSION

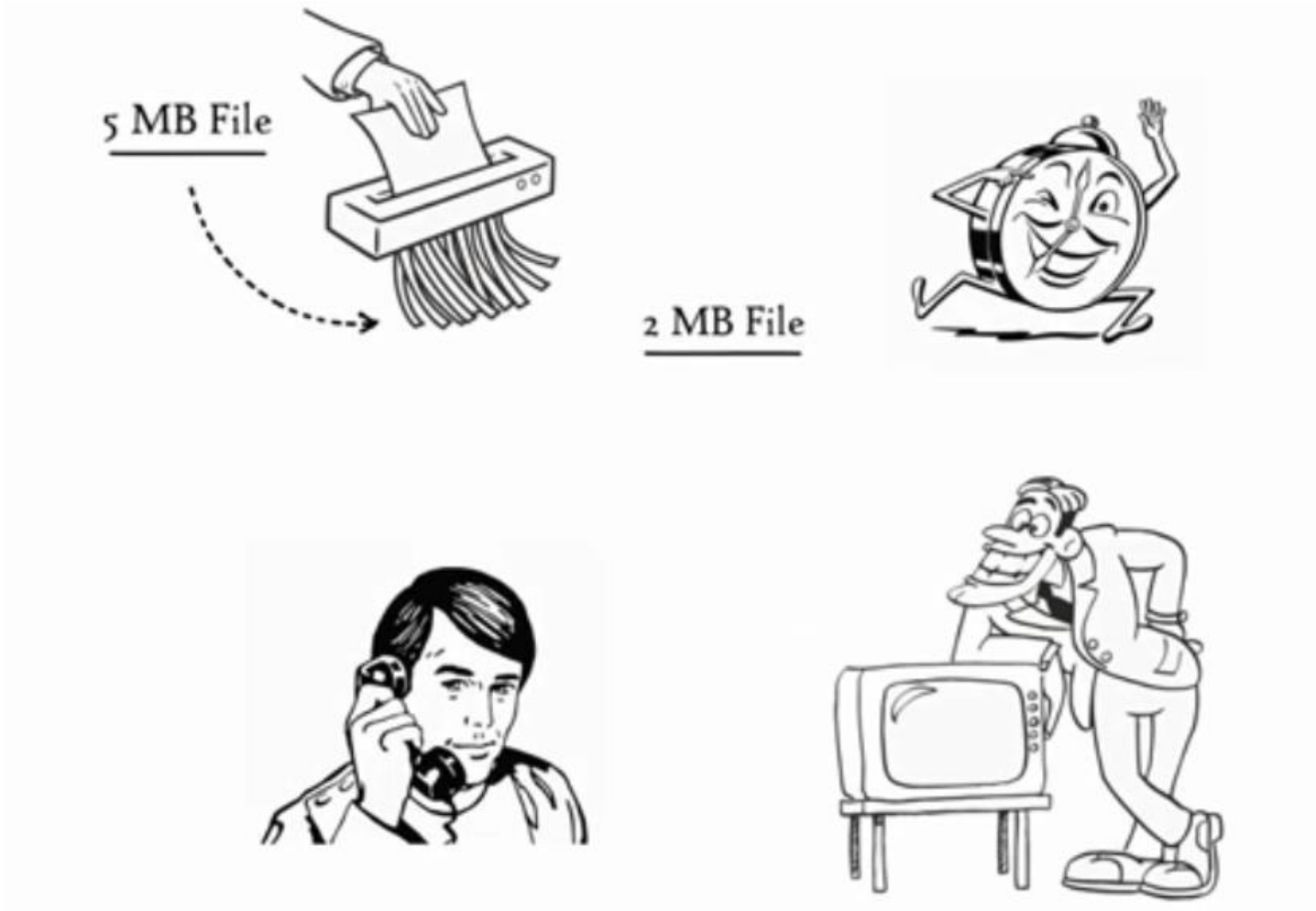


PRESENTATION LAYER

Compression and Decompression

If the file size is large, it becomes difficult to transmit the large file over the network. File size can be decreased by compressing the file for easy transmission of data.

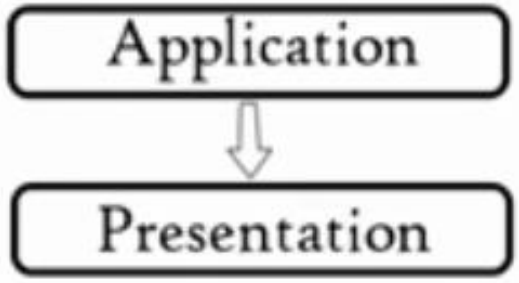
Compression is the method of diminishing the size of a file to transmit data easily in less time. When the compressed data reaches the receiver, the data is reconstructed back to the original size, and this process is called decompression.



Lossy compression is used in Images, audio, video.

Lossless Compression is used in Text, images, sound.

Presentation Layer



Translation

DFG JUYRG
64578995412

100011101101

eg. ASCII ⟶ EBCDIC

Data Compression

10101101

1. Lossy
2. Lossless

Encryption

10011011

SSL

Secure Sockets Layer

FEATURES OF PRESENTATION LAYER IN THE OSI MODEL

- Presentation layer could apply certain sophisticated compression techniques, so fewer bytes of data are required to represent the information when it is sent over the network.
- If two or more devices are communicating over an encrypted connection, then this presentation layer is responsible for adding encryption on the sender's end as well as the decoding the encryption on the receiver's end so that it can represent the application layer with unencrypted, readable data.
- This layer formats and encrypts data to be sent over a network, providing freedom from compatibility problems.
- This presentation layer also negotiates the Transfer Syntax.
- This presentation layer is also responsible for compressing data it receives from the application layer before delivering it to the session layer (which is the 5th layer in the OSI model) and thus improves the speed as well as the efficiency of communication by minimizing the amount of the data to be transferred.

EXAMPLES OF PRESENTATION LAYER PROTOCOLS AND STANDARDS

JPEG (Joint Photographic Experts Group)

- **Function**: A commonly used method of lossy compression for digital images.
- **Usage**: Used in digital cameras, websites, and various image-sharing platforms.
- **Advantages**: Reduces file size significantly while maintaining acceptable image quality for photographs and complex images.

GIF (Graphics Interchange Format)

- **Function**: A bitmap image format that supports both animated and static images.
- **Usage**: Popular for simple graphics and small animations on the web.
- **Advantages**: Supports up to 256 colors and allows for transparency and simple animation.

PNG (Portable Network Graphics)

- **Function**: A raster-graphics file format that supports lossless data compression.
- **Usage**: Commonly used for web graphics, supports transparency.
- **Advantages**: Retains high image quality and supports a wider color range than GIF.

MPEG (Moving Picture Experts Group)

- **Function**: Standards for the compression and transmission of audio and video data.
- **Usage**: Used in video streaming, digital television, DVDs, and video conferencing.
- **Advantages**: Provides high compression rates while maintaining video and audio quality.

ASCII (American Standard Code for Information Interchange)

Function: A character encoding standard for electronic communication.
Usage: Represents text in computers, telecommunications equipment, and other devices that use text.
Advantages: Simple and widely supported, allows for interoperability between different systems.

SSL/TLS (Secure Sockets Layer/Transport Layer Security)

Function: Provides encryption for secure data transmission over the internet.
Usage: Used in secure web browsing (HTTPS), email, VPNs, and other secure communications.
Advantages: Ensures data privacy, integrity, and authentication.

XDR (External Data Representation)

Function: A standard for data serialization.
Usage: Commonly used in network protocols and distributed systems to ensure data format interoperability.
Advantages: Facilitates the exchange of data between different types of computer systems.

XML (eXtensible Markup Language)

Function: A flexible text format used for structuring data.
Usage: Widely used in web services, configuration files, and data exchange between systems.
Advantages: Human-readable and machine-readable, supports complex data structures.

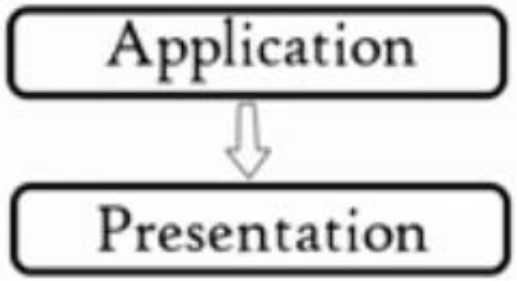
PRESENTATION LAYER

Encryption and Decryption

Whatever data is being transmitted between the sender and the receiver, that data must be secure because an intruder can hack the data passing between the sender and the receiver. Hackers can modify the data and send the modified data to the receiver to create false communication. The presentation layer is responsible for encrypting and decrypting data to avoid data leakage and data modification.

The plaintext data at the source is encrypted into ciphertext (unreadable format), then it is sent to the receiver, where the ciphertext is decrypted into plaintext. Now, if the hacker tries to hack the data, the hacker receives an encrypted, unreadable form, and if the hacker tries to send modified data, the receiver can detect the modification during decryption; thereby, the data remains safe.

Presentation Layer



Translation

DFGJUYRG
64578995412

100011101101

eg. ASCII ⟶ EBCDIC

Data Compression

10101101

1. Lossy
2. Lossless

Encryption/Decryption

10011011

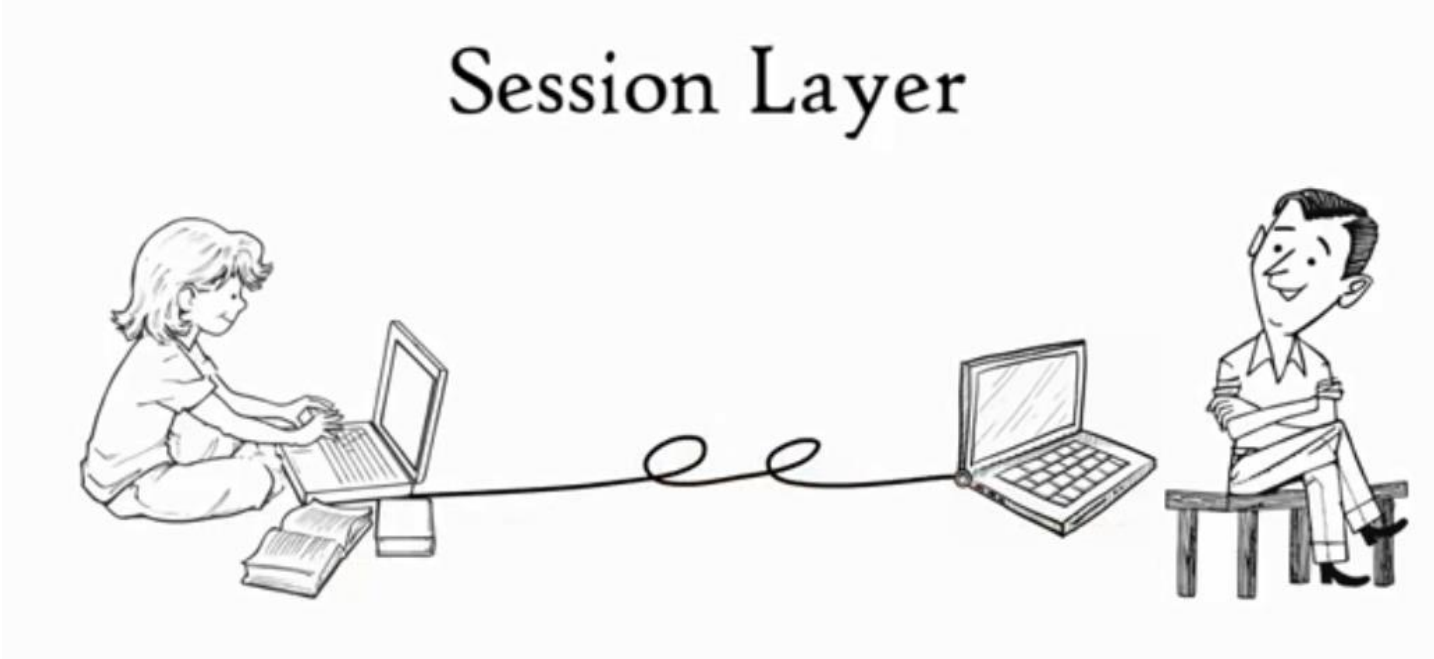
SSL

Secure Sockets Layer

LAYER 5 –SESSIONS LAYER

Sessions Layer

How your PC maintains a connection with the server? How does your PC know that the destination it communicates to is a legitimate one?

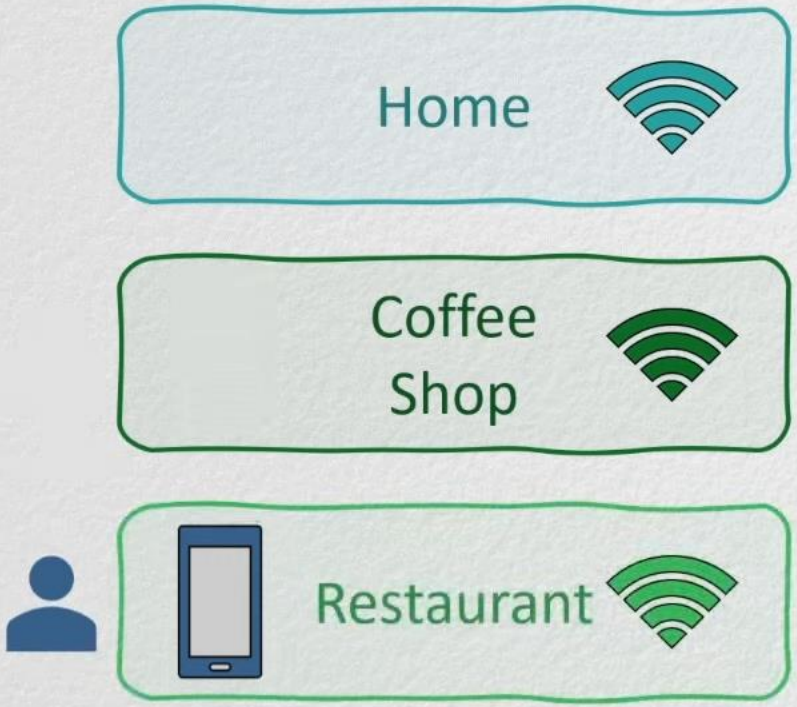


Note: AI Generated Images

- Create

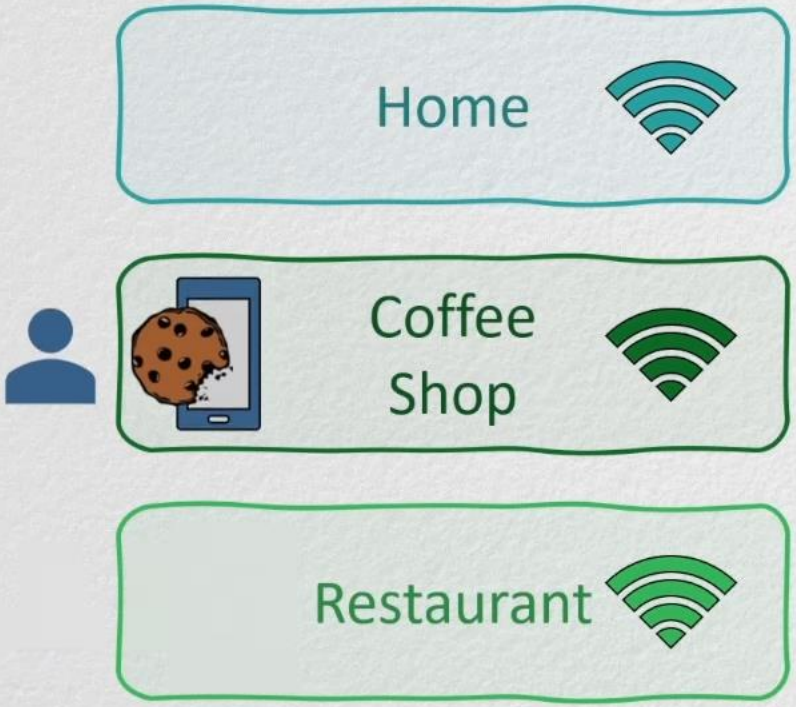
- Layer 5 distinguishes between **user sessions**
  - Identifies a user independent from L2, L3, or L4 addresses

7	Application
6	Presentation
5	**Session**
4	Transport
3	Network
2	Data Link
1	Physical



- Layer 5 distinguishes between **user sessions**
  - Identifies a user independent from L2, L3, or L4 addresses

7	Application
6	Presentation
5	**Session**
4	Transport
3	Network
2	Data Link
1	Physical



HTTP

HTTP Cookies

Arbitrary text strings that store user-specific information

FUNCTIONS OF THE SESSION LAYER

1. Session Establishment, Maintenance, and Termination:

- **Establishment**: The session layer establishes a connection (or session) between two devices or applications. This involves setting up and synchronizing the communication parameters such as port numbers and session IDs.
- **Maintenance**: Once established, the session layer maintains the session, keeping it alive for as long as needed. It manages the dialog between the two parties, ensuring that data is properly organized and synchronized.
- **Termination**: After the communication is complete, the session layer gracefully terminates the session, ensuring that all resources are released properly.

FUNCTIONS OF THE SESSION LAYER

2. Dialog Control

- The session layer controls the direction of communication between two devices, determining which device can send data at any given time. This is crucial in managing the communication flow in different modes:
  - **Simplex**: One-way communication where data flows in only one direction.
  - **Half-Duplex**: Two-way communication, but data can flow in only one direction at a time.
  - **Full-Duplex**: Two-way communication, where data can flow in both directions simultaneously.

3. Synchronization

- The session layer can insert **synchronization points** (also known as checkpoints) into the data stream. These points allow the session to be restarted from a specific point if a failure occurs. This is particularly useful in long or complex data transmissions, such as file transfers or database transactions, where you don't want to restart from the beginning in case of an interruption.

FUNCTIONS OF THE SESSION LAYER

4. Error Handling and Recovery

- If a session is interrupted or encounters an error, the session layer handles the recovery process. It can attempt to re-establish the session, resynchronize the communication, and ensure that data transmission can continue from the last successful synchronization point, minimizing data loss.

5. Token Management

- In certain types of communication protocols, the session layer may use a **token** system to manage access to the communication channel. The token acts as a permission slip, allowing only the holder to send data at any given time. This prevents collisions and ensures orderly communication.

PROTOCOLS AND TECHNOLOGIES THAT OPERATE AT THE SESSION LAYER

1. Session Initiation Protocol (SIP)

- **Purpose**: Used to initiate, maintain, modify, and terminate real-time sessions that involve video, voice, messaging, and other communications applications and services.
- **Applications**: VoIP (Voice over Internet Protocol), video conferencing, instant messaging.

2. NetBIOS (Network Basic Input/Output System)

- **Purpose**: Provides services related to the session layer of the OSI model allowing applications on separate computers to communicate over a local area network.
- **Applications**: File and printer sharing over a network, primarily used in Windows environments.

3. RPC (Remote Procedure Call)

- **Purpose**: Allows a program to cause a procedure to execute in another address space (commonly on another physical machine).
- **Applications**: Distributed systems and network management applications.

PROTOCOLS AND TECHNOLOGIES THAT OPERATE AT THE SESSION LAYER

5. RTCP (Real-Time Control Protocol)

- **Purpose**: Works with RTP (Real-Time Protocol) to provide control and monitoring of the data delivery for real-time applications.
- **Applications**: Audio and video streaming.

6. X Window System (X11)

- **Purpose**: Provides a framework for building graphical user interfaces and managing windows.
- **Applications**: Unix and Linux graphical user interface systems.

7. AppleTalk Session Protocol (ASP)

- **Purpose**: Manages the communication sessions in AppleTalk networking.
- **Applications**: AppleTalk network communications.

IMPORTANCE OF SESSION LAYER

- The session layer plays a crucial role in ensuring the reliability and integrity of data exchange. It serves as the pivotal bridge that ensures orderly communication between devices.
- This layer maintains the integrity and reliability of data exchange by managing session establishment, synchronization of data flow, and structured dialog control. Communication sessions might lack structure without this layer, leading to confusion and data corruption.
- Its presence enables error recovery, organized communication, and efficient data management, making it indispensable for seamless networking across diverse environments.

EXAMPLES OF USE CASES OF SESSION LAYER

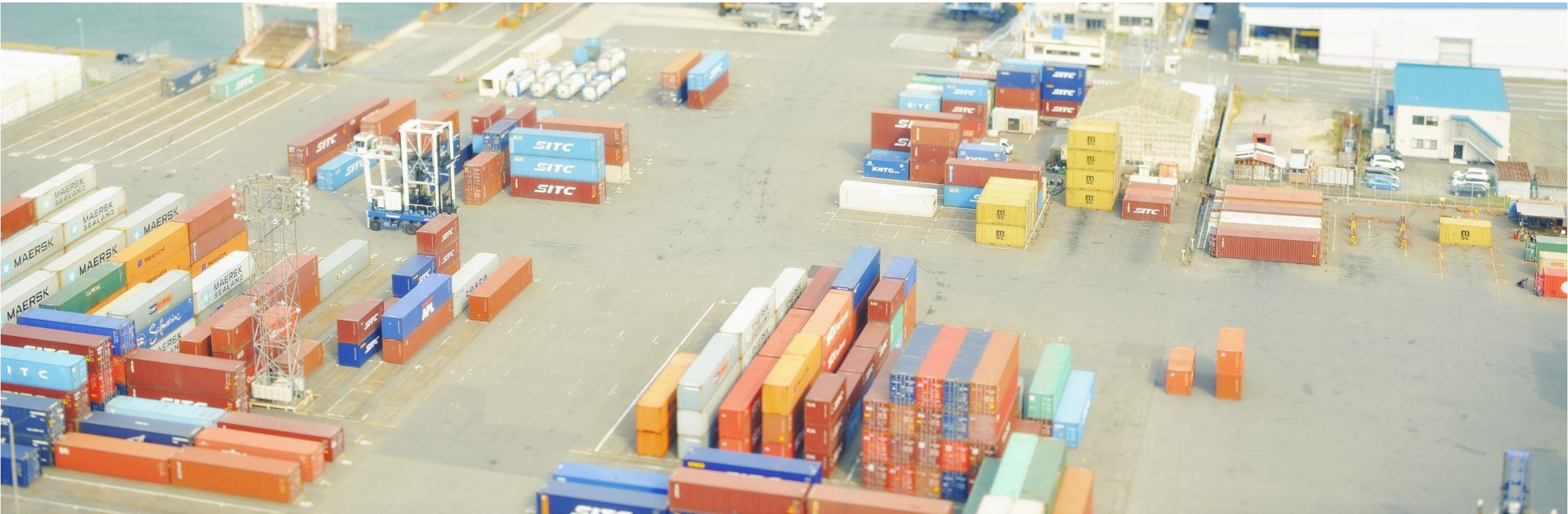
- **Video Conferencing**: The session layer ensures that the video and audio streams are synchronized and that the session remains active as long as the conference is ongoing.

- **Online Transactions**: In banking or e-commerce, the session layer ensures that the transaction is completed securely, even if interruptions occur.

- **File Transfers**: During large file transfers, the session layer can insert checkpoints to allow the transfer to resume from a specific point if a failure occurs.

LAYER 4 –TRANSPORT – SERVICE TO SERVICE

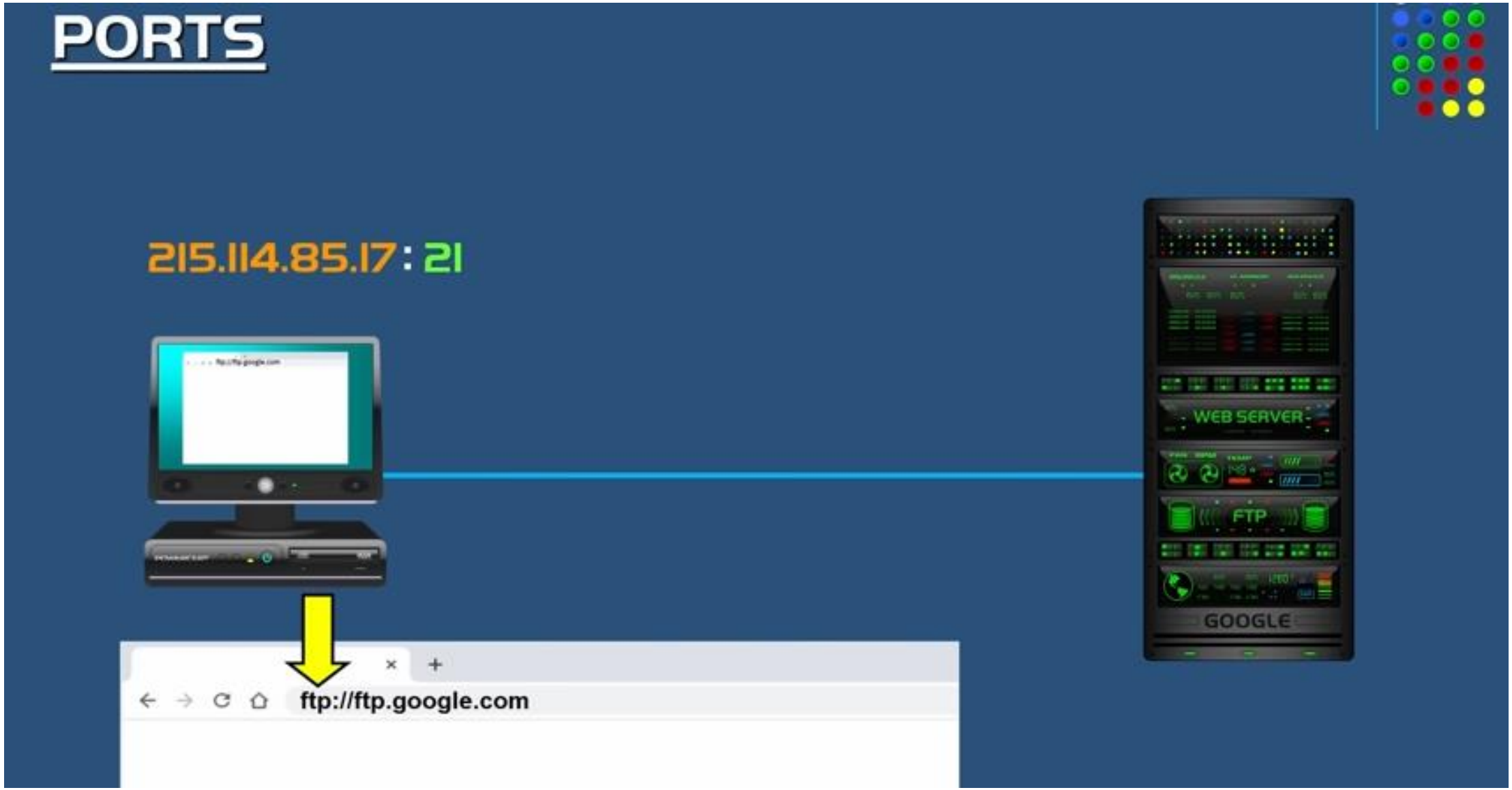
PORTS



All of this happens behind the scenes.

- You don't see the IP address or the port number that's being used.

PORTS



PORTS

SYSTAT	11	TACACS-DS	65	3COM-TXMUS	106	BL-IDM	142	BGP	179	SOFTPC	215
DAYTIME	13	SQL-NET	66	RTLNET	107	IMAP	143	RIS	180	CAILIC	216
QOTD	17	BOOTPS	67	SNAGAS	108	UMA	144	UNIFY	181	DBASE	217
MSP	18	TFTP	69	POP2	109	UAAC	145	AUDIT	182	MPP	218

Port numbers 49152 - 65535 are called Dynamic or Private ports.

These are client-side ports that are free to use.

These are ports that your computer assigns temporarily to itself during during a session.

Example: When viewing a web page.

NICNAME	43	SU-MIT-TG	89	NXEDIT	126	SNMPTRAP	162	SMUX	199	OPENPORT	260
MPM-FLAGS	44	DNSIX	90	LOCUS-CON	127	CMIP-MAN	163	SRC	200	NSIIOPS	261
MPM	45	MIT-DOV	91	GSS-XLICEN	128	CMIP-AGENT	164	AT-RTMP	201	ARCISDMS	262
MPM-SND	46	NPP	92	PWDGEN	129	XNS-COURIER	165	AT-NBP	202	HDAP	263
DOMAIN	53	SWIFT-RVF	97	INGRES-NET	134	PRINT-SRV	170	AT-7	207	TD-REPLICA	268
XNS-CH	54	TACNEWS	98	EPMAP	135	MULTIPLEX	171	AT-8	208	HTTPS	443

PORTS

CLIENT

Command Prompt

Microsoft Windows

C:\Users\Admin> netstat -an

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0 : 21	0.0.0.0 : 0	LISTENING
TCP	0.0.0.0 : 80	0.0.0.0 : 0	LISTENING
TCP	192.168.0.12 : 63510	215.114.85.17 : 80	ESTABLISHED
TCP	192.168.0.12 : 63562	215.114.85.17 : 1101	ESTABLISHED
TCP	192.168.0.12 : 63037	215.114.85.17 : 1527	ESTABLISHED

SERVER

PORTS

Command Prompt

Microsoft Windows

C:\Users\Admin> netstat -n

Active Connections

Proto	Local Address	Foreign Address	State
TCP	192.168.0.12 : 52913	74.125.44.25 : 443	ESTABLISHED
TCP	192.168.0.12 : 62976	22.134.45.78 : 443	ESTABLISHED
TCP	192.168.0.12 : 63510	42.33.44.55 : 21	ESTABLISHED

42.33.44.55

22.134.45.78

74.125.44.25

Port 80 and 443 are used for web pages.

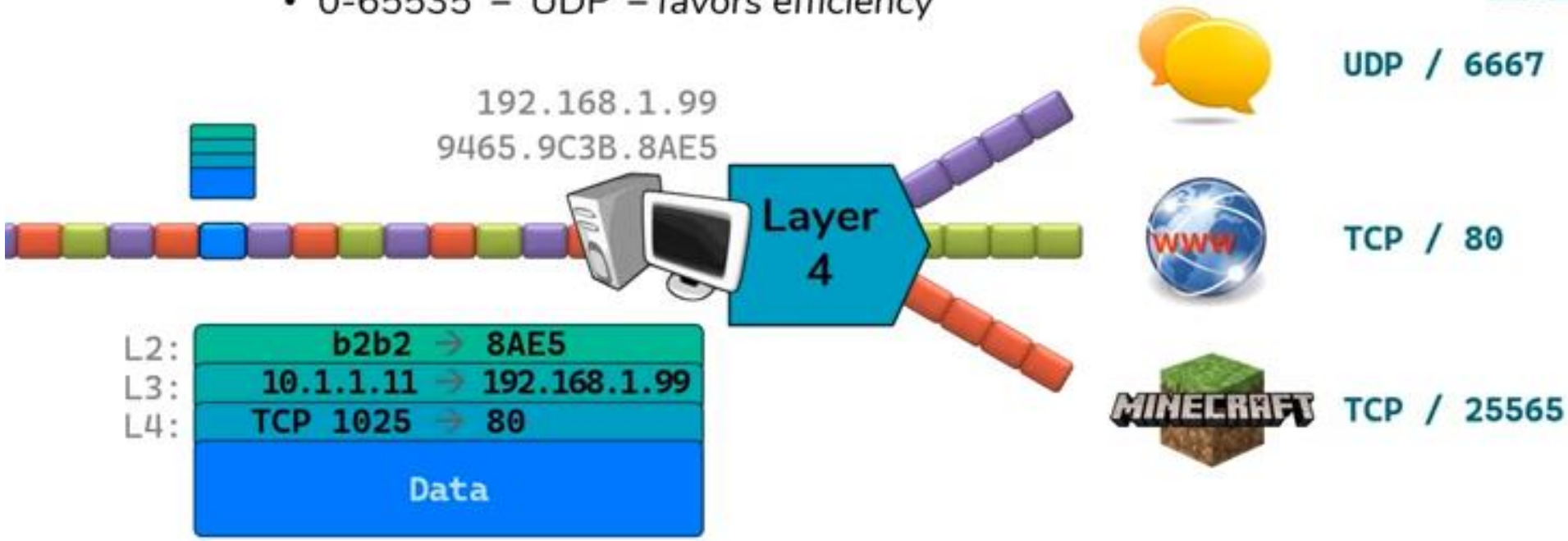
Port 80 uses HTTP (Hypertext Transfer Protocol).

Port 443 uses HTTPS (Hypertext Transfer Protocol Secure).

OSI Model

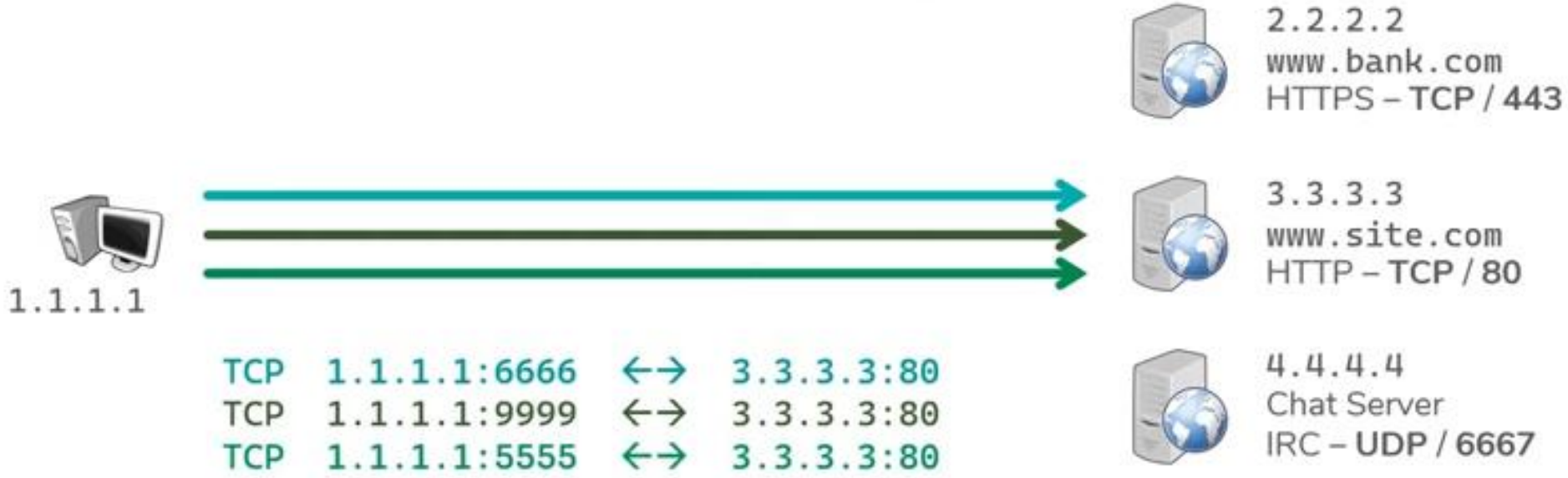
- **Layer 4 – Transport – Service to Service**
  - Distinguish data streams
  - Addressing Scheme – Ports
    - 0-65535 – TCP – *favors reliability*
    - 0-65535 – UDP – *favors efficiency*

7	Application
6	Presentation
5	Session
4	**Transport**
3	Network
2	Data Link
1	Physical



OSI Model

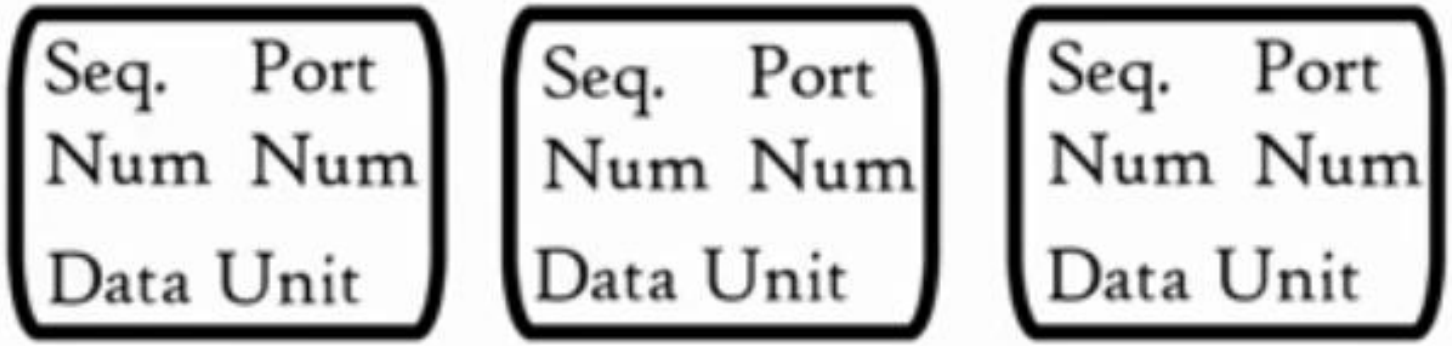
- **Layer 4 – Transport – Service to Service**
  - Distinguish data streams
  - Addressing Scheme – Ports – 0-65535, TCP or UDP
  - Servers listen for requests to pre-defined Ports
  - Clients select random Port for each connection



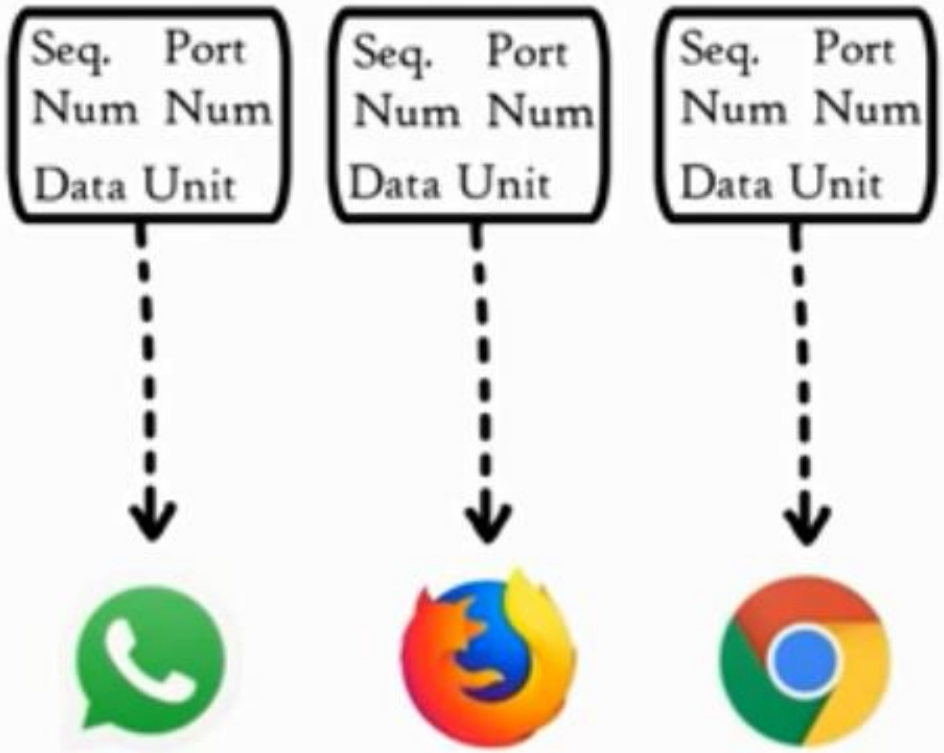
Transport layer controls the reliability of communication through

- Segmentation
- Flow control
- Error control

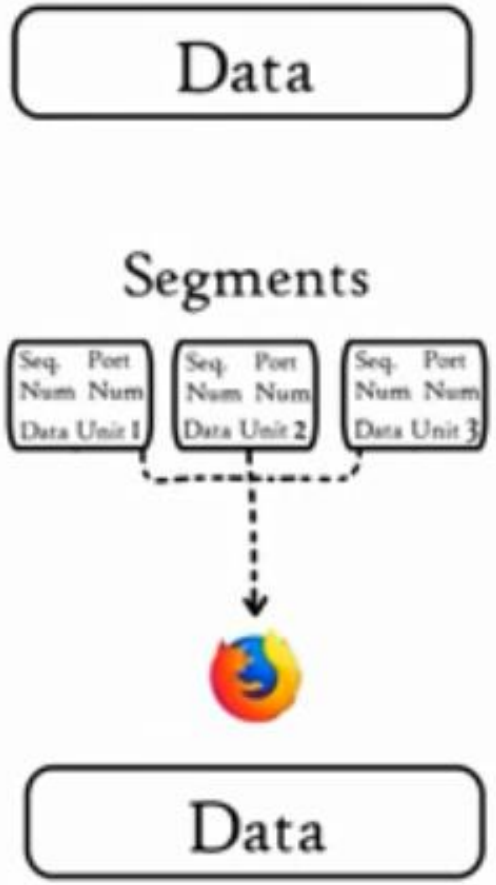
Segments


Seq. Num
Port Num
Data Unit
Seq. Num
Port Num
Data Unit
Seq. Num
Port Num
Data Unit

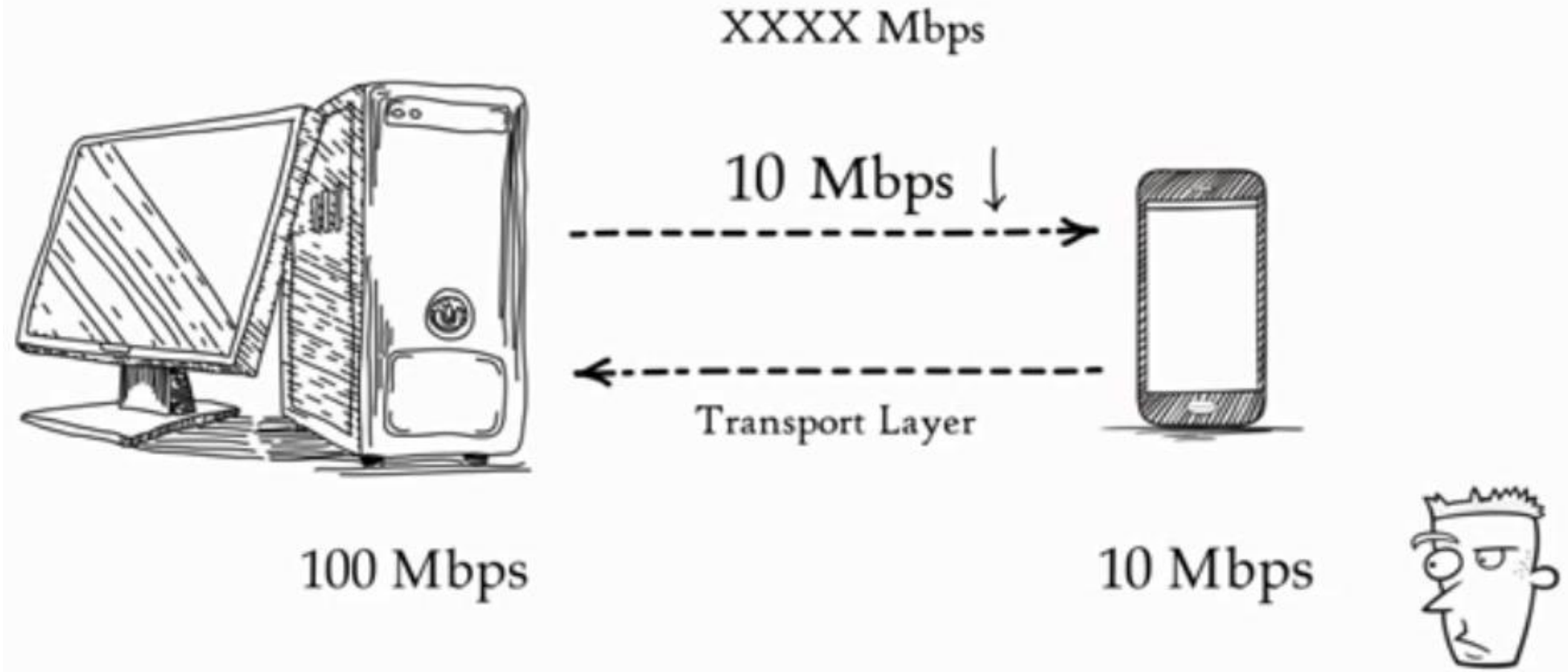
Segments


Seq. Num
Port Num
Data Unit
Seq. Num
Port Num
Data Unit
Seq. Num
Port Num
Data Unit

Segmentation:

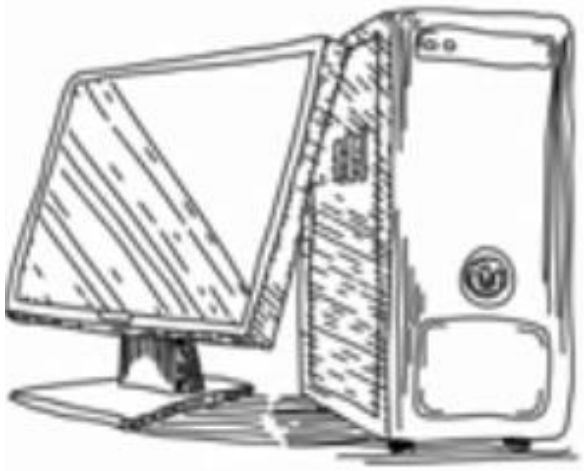


Flow Control:



Error Control:

Automatic Repeat Request



Data Unit 1

Data Unit 2

Data Unit 3

Data Unit 1 Checksum

Data Unit 2 Checksum

Data Unit 3 Checksum

Checksum → Corrupted

Transport Layer

Services:	Protocols:
- Connection-oriented Transmission	----------> Transmission Control Protocol (TCP)
- Connectionless Transmission	----------> User Datagram Protocol (UDP)

UDP

No feedback

TCP

Feedback

Transport Layer

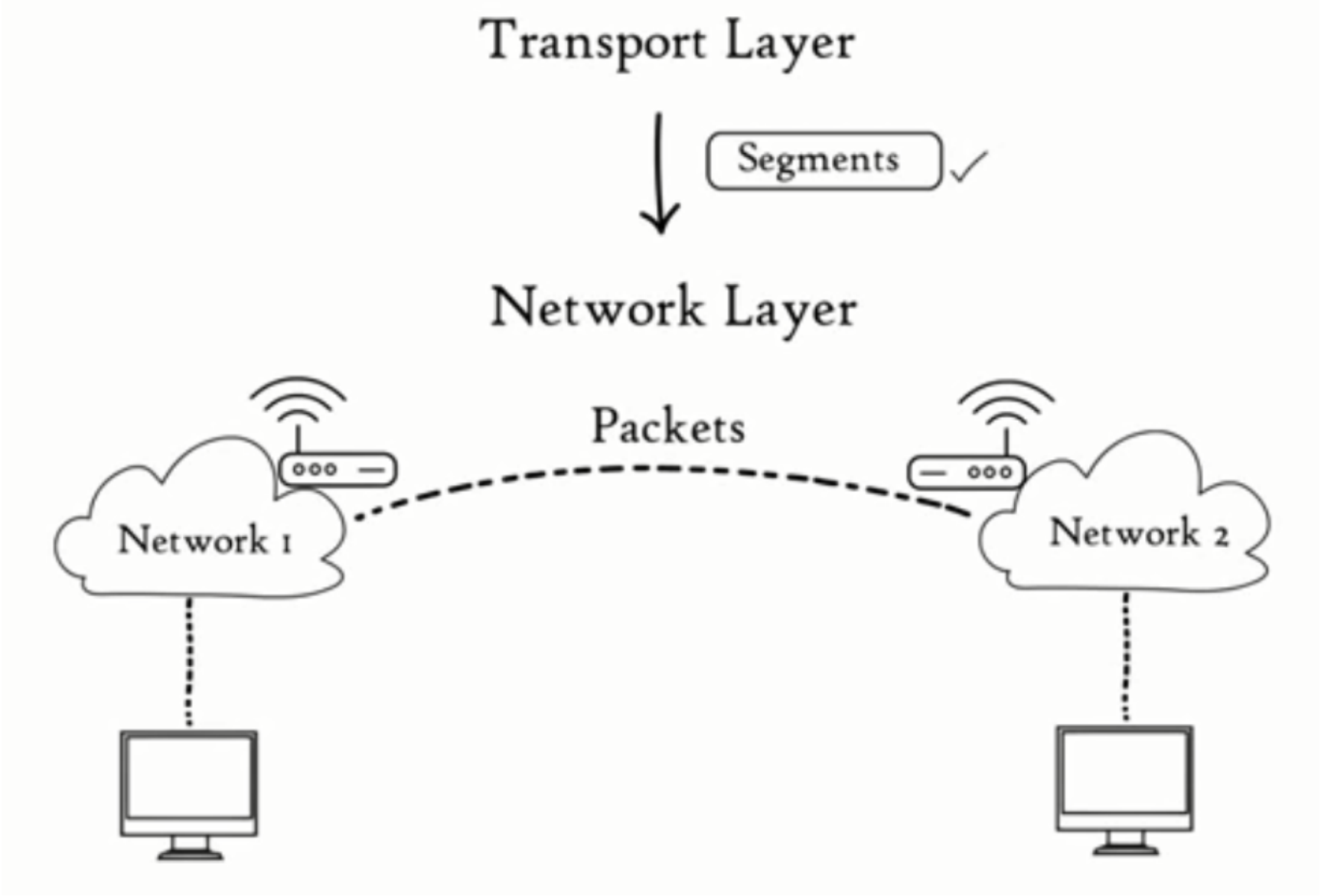
Segmentation

Flow Control

Error Control

Connection and Connectionless Tx

LAYER 3 – NETWORK – END TO END


Transport Layer
Segments
Network Layer
Packets
Network 1
Network 2

Network layer

Logical Addressing

IPv4 & IPv6

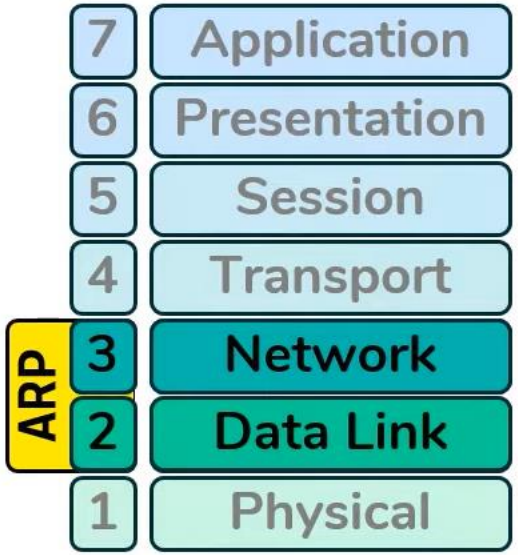
Path determination

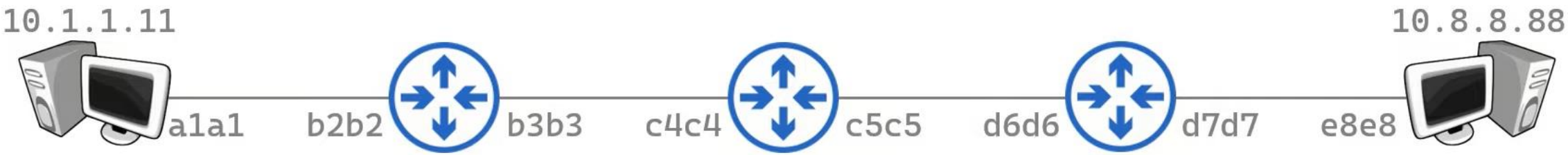
Routing

OSI Model

- **Layer 3 – IP Addresses**
- **Layer 2 – MAC Addresses**

- **ARP** – Address Resolution Protocol
  - Links a L3 address to a L2 address



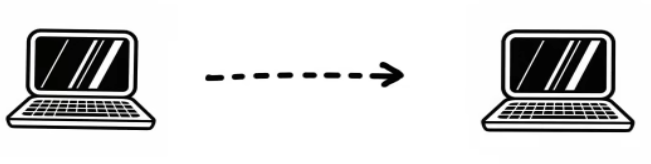


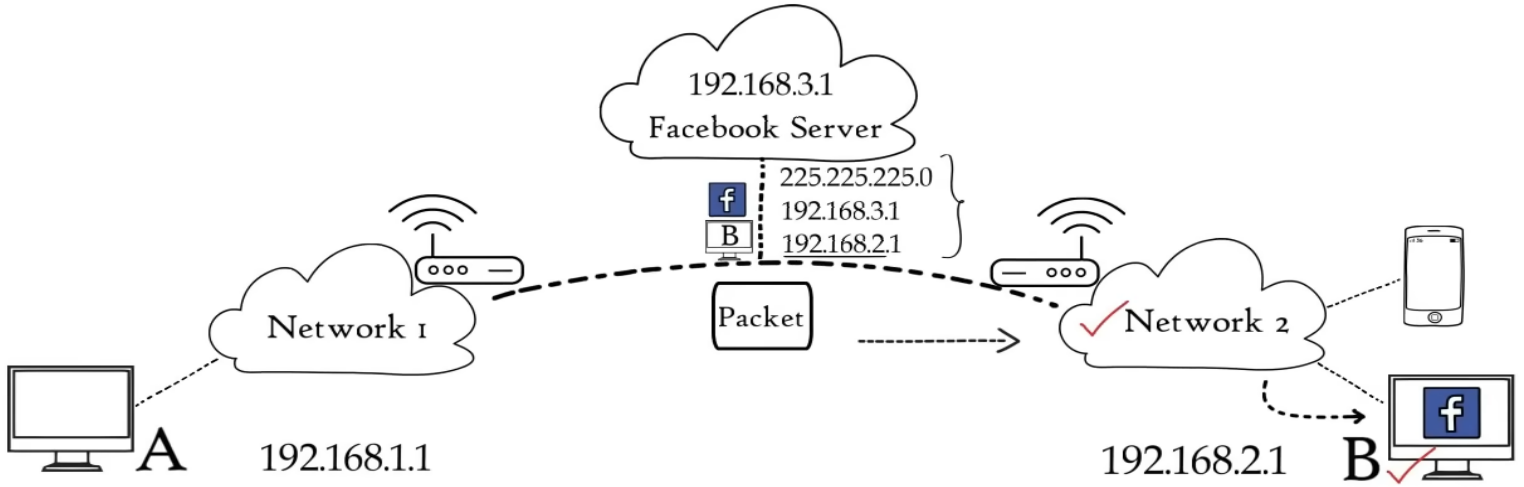
Logical Addressing

IPv4 & IPv6
+
Mask

Path determination

Routing



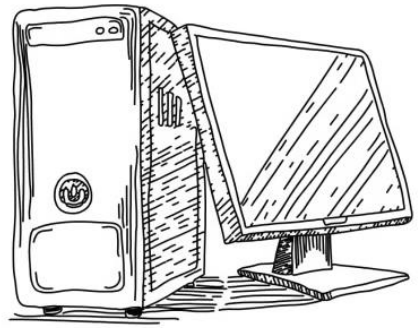


Path determination

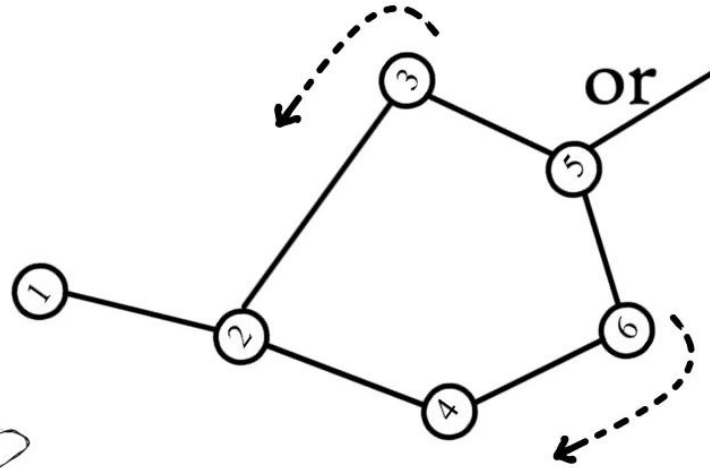
OSPF

BGP

IS-IS



Sender

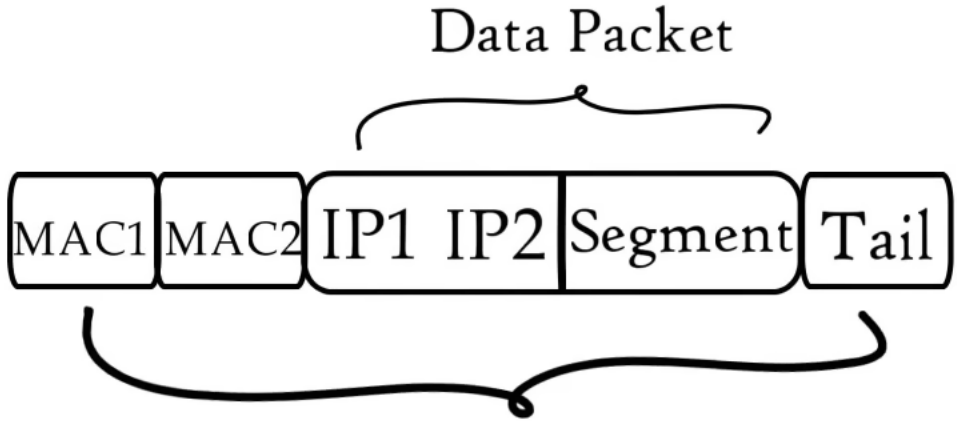


Receiver

LAYER 2 – DATA LINK – HOP TO HOP

MAC 1

62.34.DF.3A.87.C9



Frame

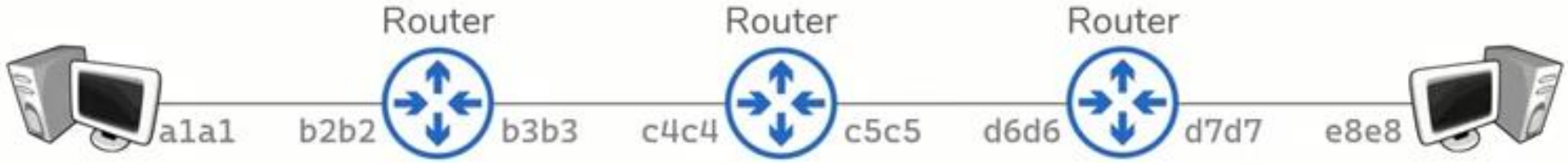
MAC 2

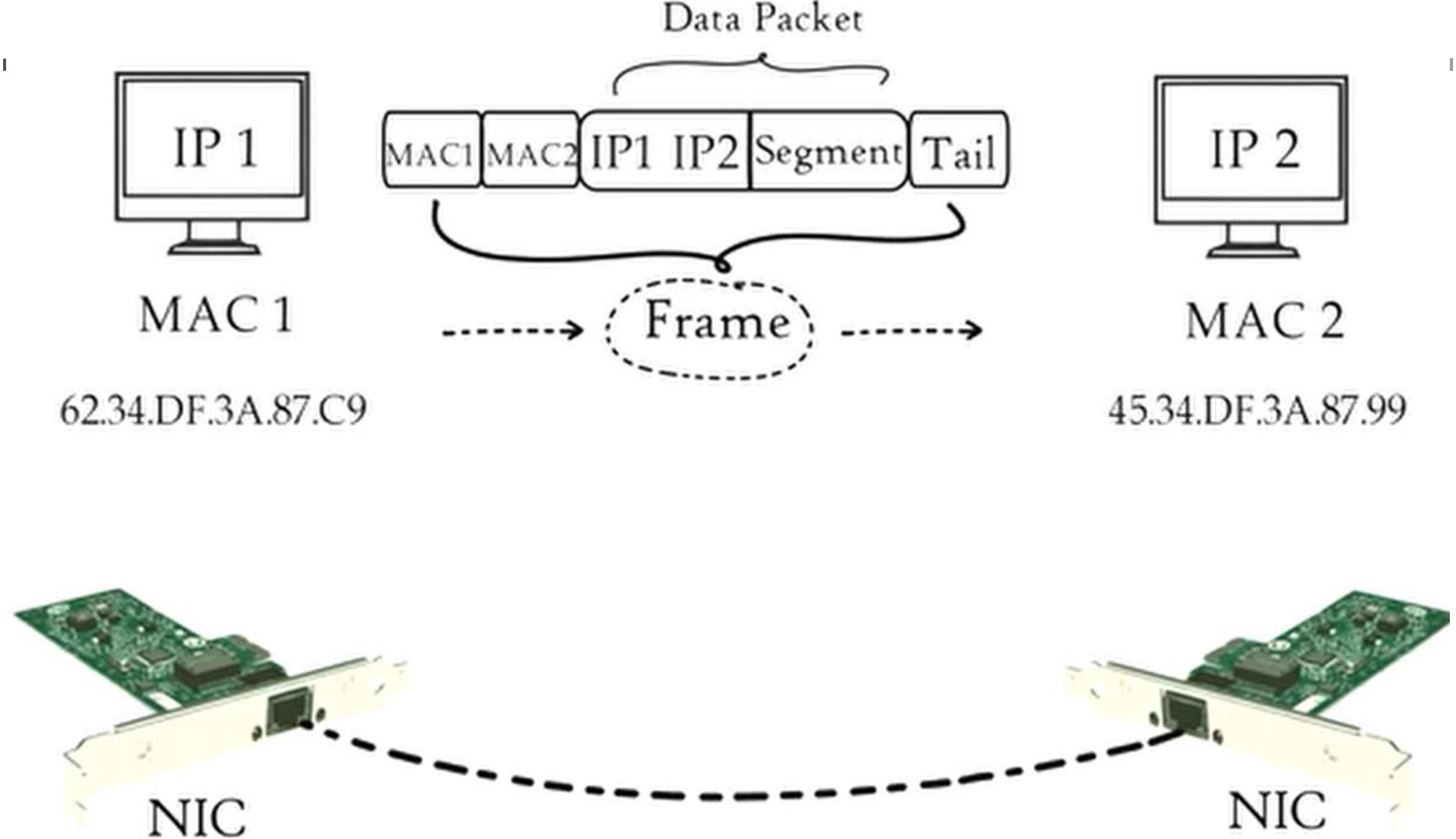
45.34.DF.3A.87.99

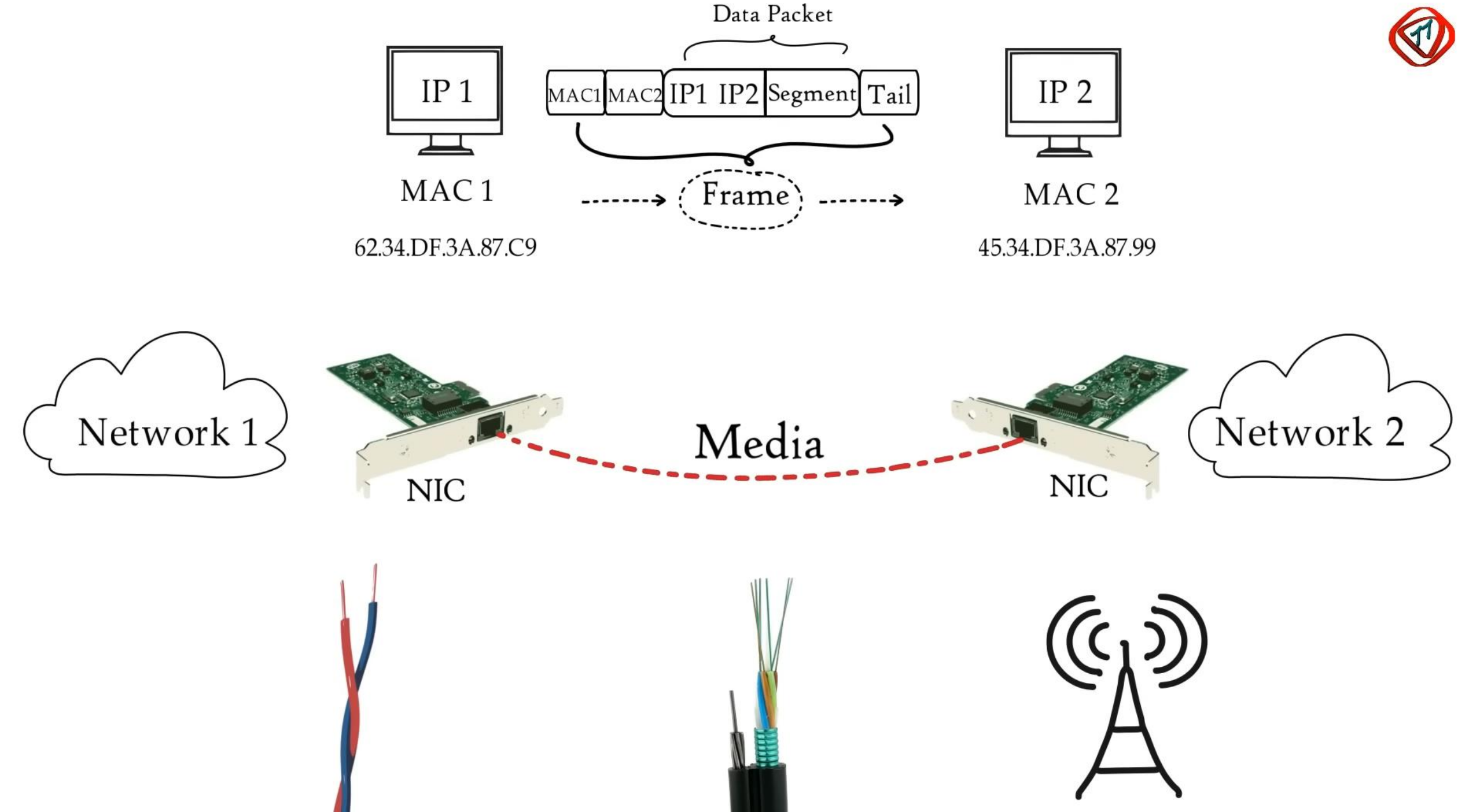
OSI Model

- **Layer 2 – Data Link – Hop to Hop**
  - Interacts with the Wire (i.e., Physical layer)
  - Addressing Scheme – MAC addresses
  - L2 Technologies: NICs, Switches
  - Often communication between hosts require multiple hops

7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	**Data Link**
1	Physical




Data Packet
IP 1
MAC1
MAC2
IP1 IP2
Segment
Tail
IP 2
MAC 1
Frame
MAC 2
62.34.DF.3A.87.C9
45.34.DF.3A.87.99
NIC
NIC


Data Packet
IP 1
MAC1
MAC2
IP1
IP2
Segment
Tail
IP 2
MAC 1
Frame
MAC 2
62.34.DF.3A.87.C9
45.34.DF.3A.87.99
Network 1
NIC
Media
NIC
Network 2

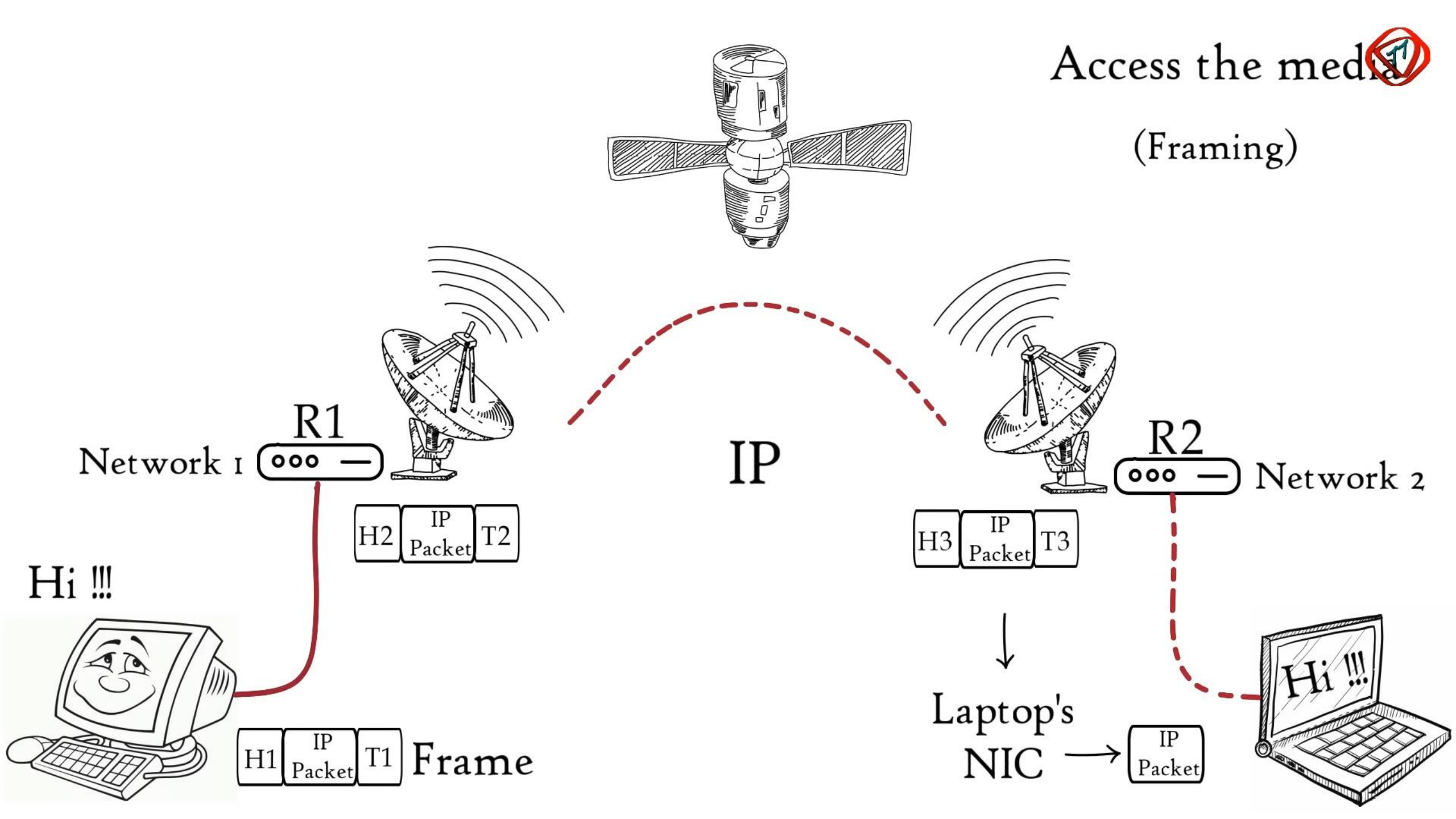
Data Link Layer

Access the media

(Framing)

Controls how data is placed
and received from the media

(Media Access Control)
(Error Detection)


Access the media
(Framing)
R1
Network 1
IP
R2
Network 2
H2
IP Packet
T2
H3
IP Packet
T3
Hi !!!
H1
IP Packet
T1
Frame
Laptop's NIC
IP Packet
Hi !!!

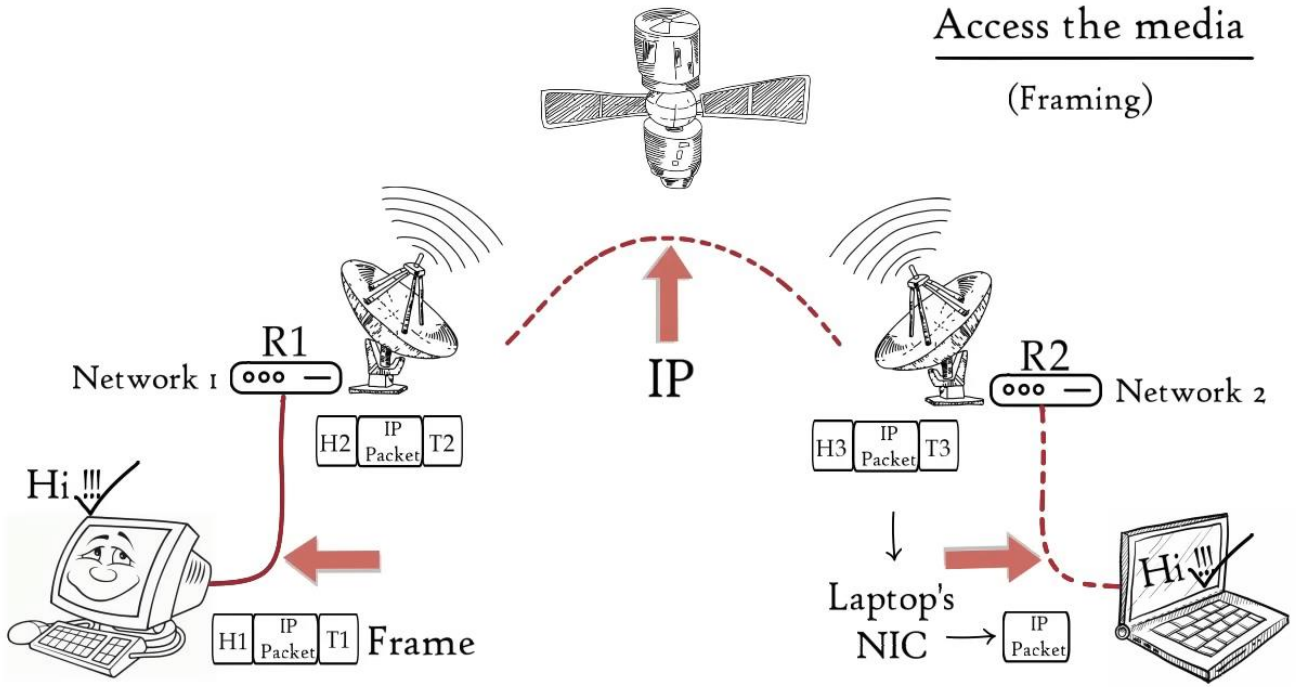
Data Link Layer

Access the media

(Framing)

Controls how data is placed and received from the media

(Media Access Control)
(Error Detection)

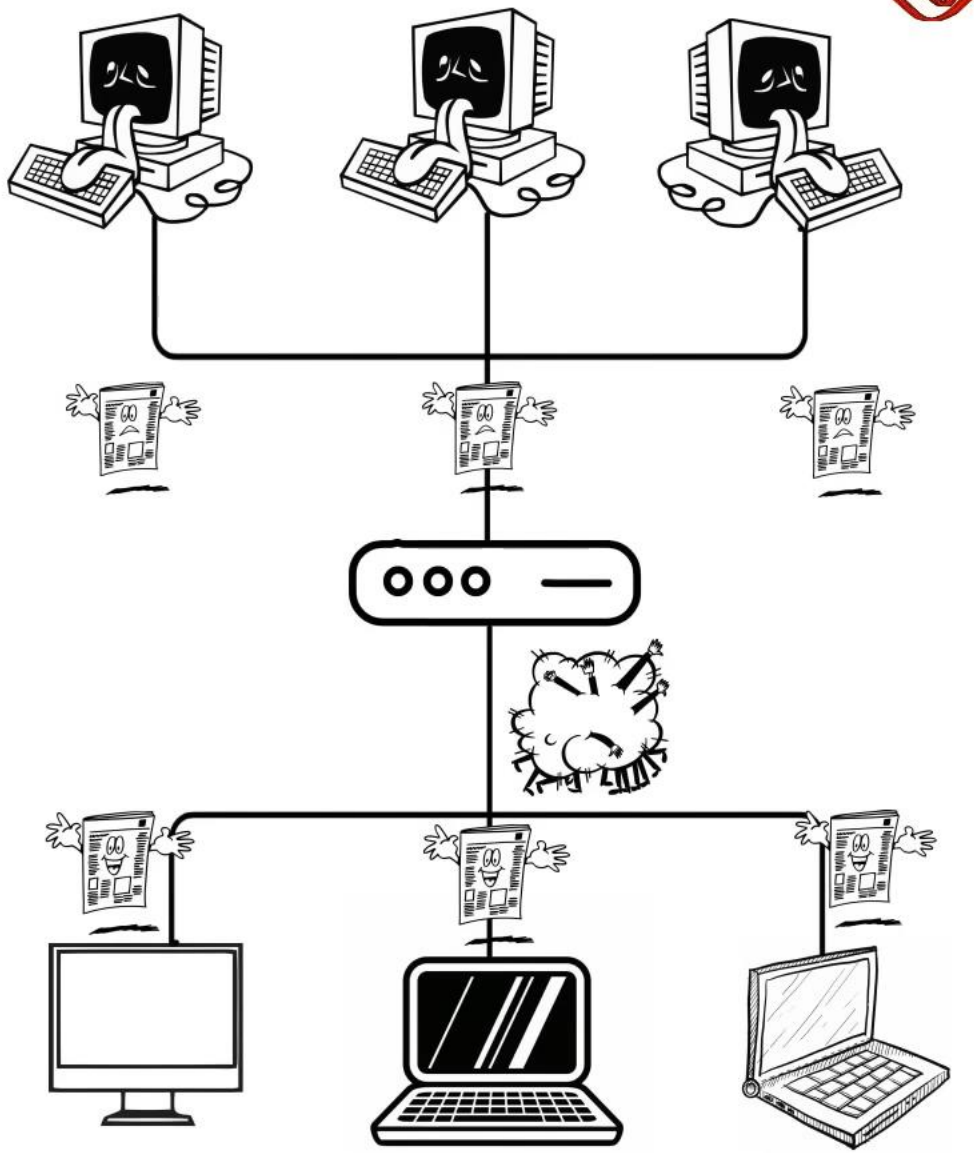


Controls how data is placed and received from the media

(Media Access Control)
(Error Detection)

DATA LINK LAYER

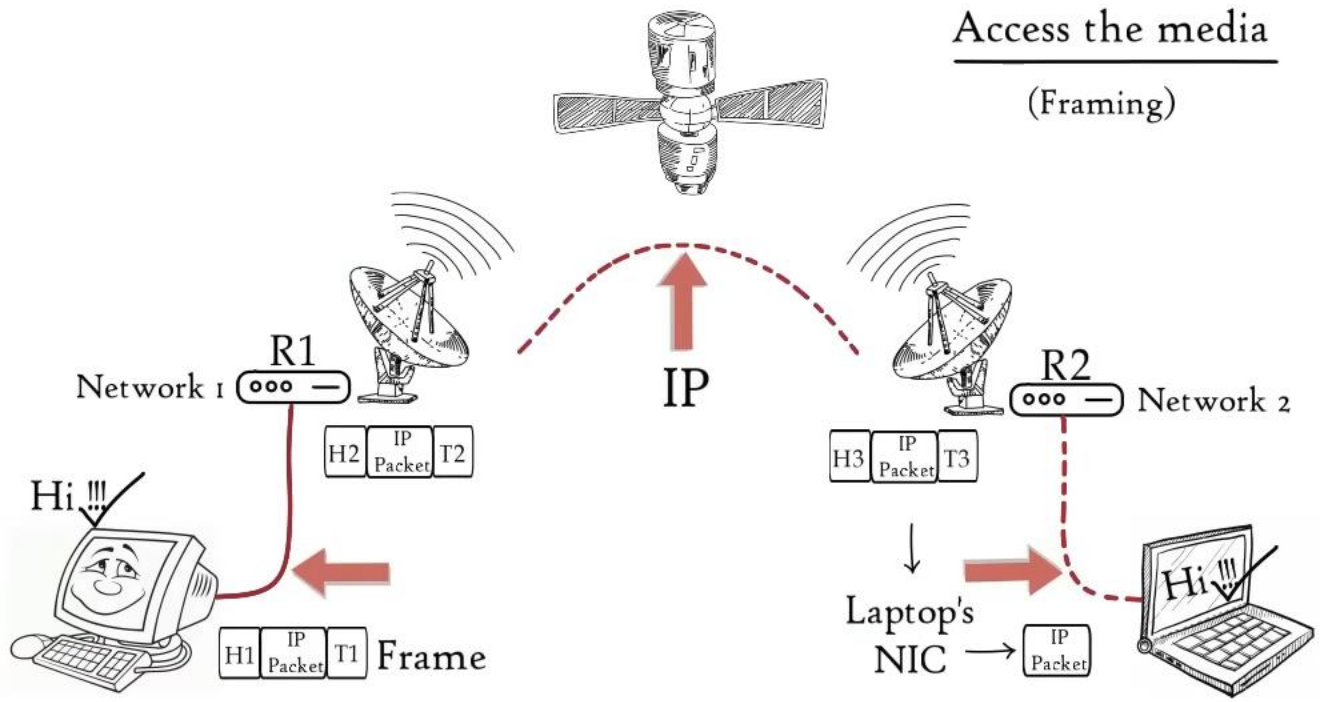
LAN Cable, Optical Fiber, Air



MEDIA ACCESS CONTROL METHODS

- This network channel through which data is transmitted between terminal nodes to avoid collision has three various ways of accomplishing this purpose. They include:
- Carrier sense multiple access with collision avoidance (CSMA/CA)
- Carrier sense multiple access with collision detection (CSMA/CD)
- Demand priority
- Token passing

Data Link Layer



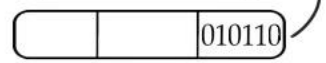
Access the media

(Framing)

Controls how data is placed and received from the media

(Media Access Control)

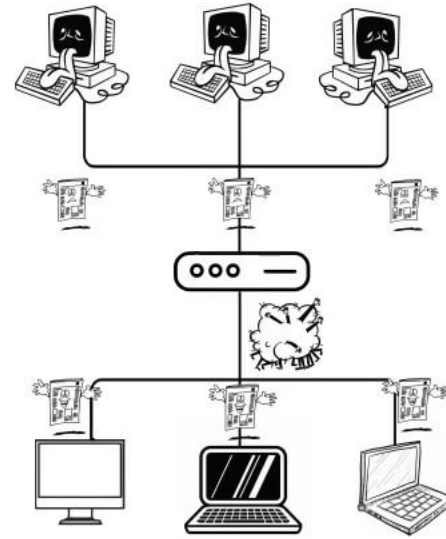
(Error Detection)



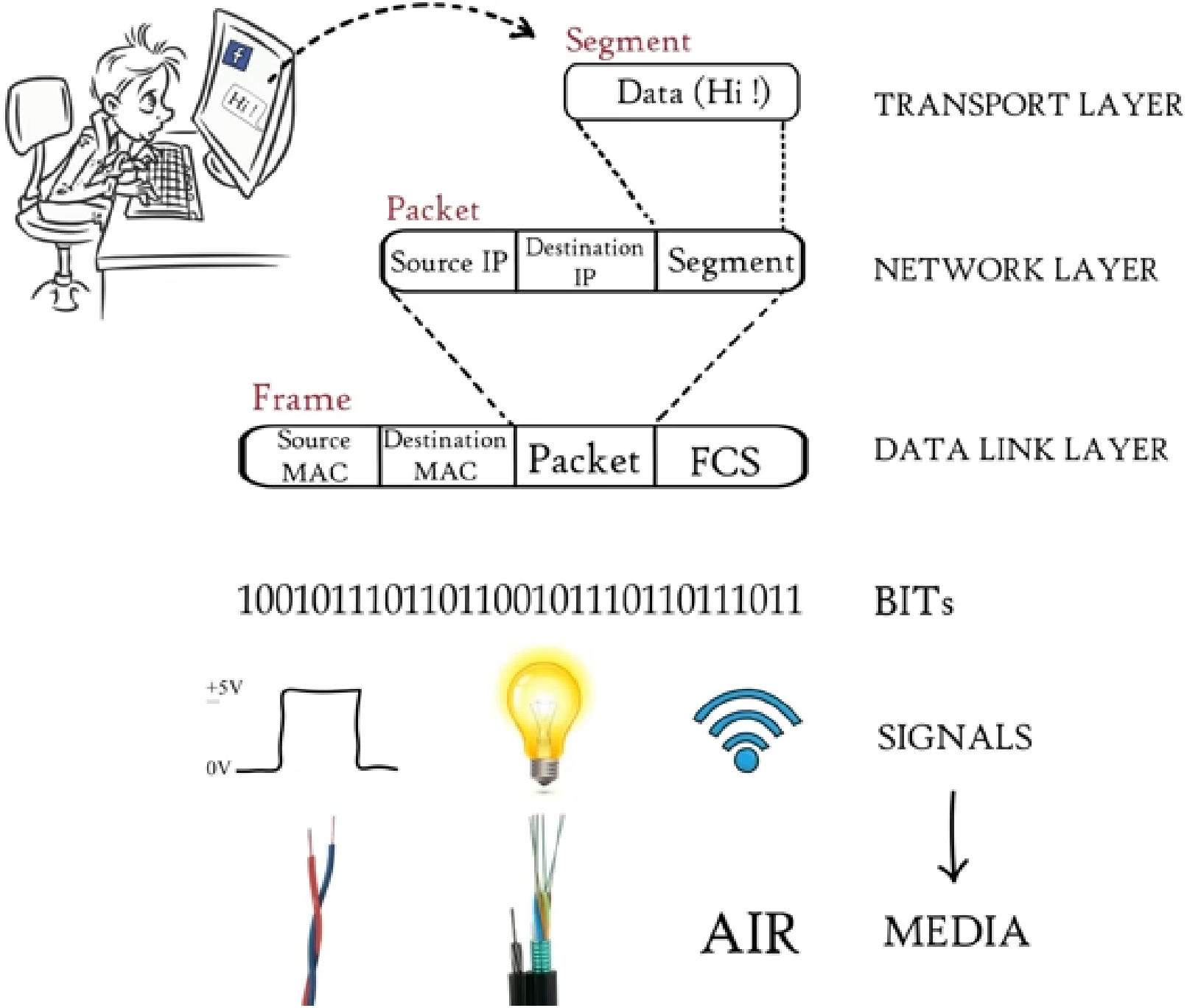
DATA LINK LAYER

CSMA

LAN Cable, Optical Fiber, Air



LAYER 1 – PHYSICAL – TRANSPORTING BITS


Segment
Data (Hi !)
TRANSPORT LAYER
Packet
Source IP
Destination IP
Segment
NETWORK LAYER
Frame
Source MAC
Destination MAC
Packet
FCS
DATA LINK LAYER
10010111011011001011011011011
BITs
+5V
0V
SIGNALS
AIR
MEDIA

OSI Model

- **Layer 1 – Physical – Transporting Bits**
  - Computer data exists in the form of Bits (1's and 0's)
  - Something has to transport those bits between hosts
  - L1 Technologies: Cables, Wifi, Repeaters, Hubs

7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	**Physical**

(Ethernet)

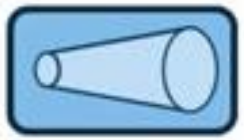
Twisted Pair

Coaxial

Fiber

Wi-Fi

Repeaters



Hub

Physical Layer

Segment

Data (Hi !)

TRANSPORT LAYER

Packet

Source IP	Destination IP	Segment

NETWORK LAYER

Frame

Source MAC	Destination MAC	Packet	FCS

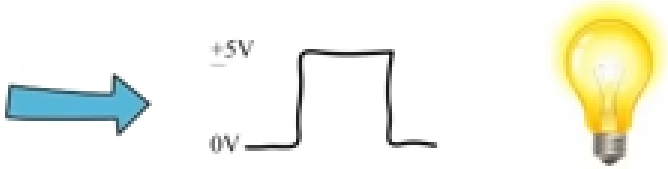
DATA LINK LAYER

APPLICATION LAYER

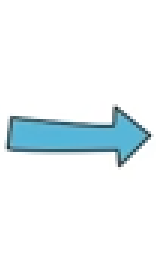
10010111011011001011101101110 11

BITs

BITs



SIGNALS



AIR

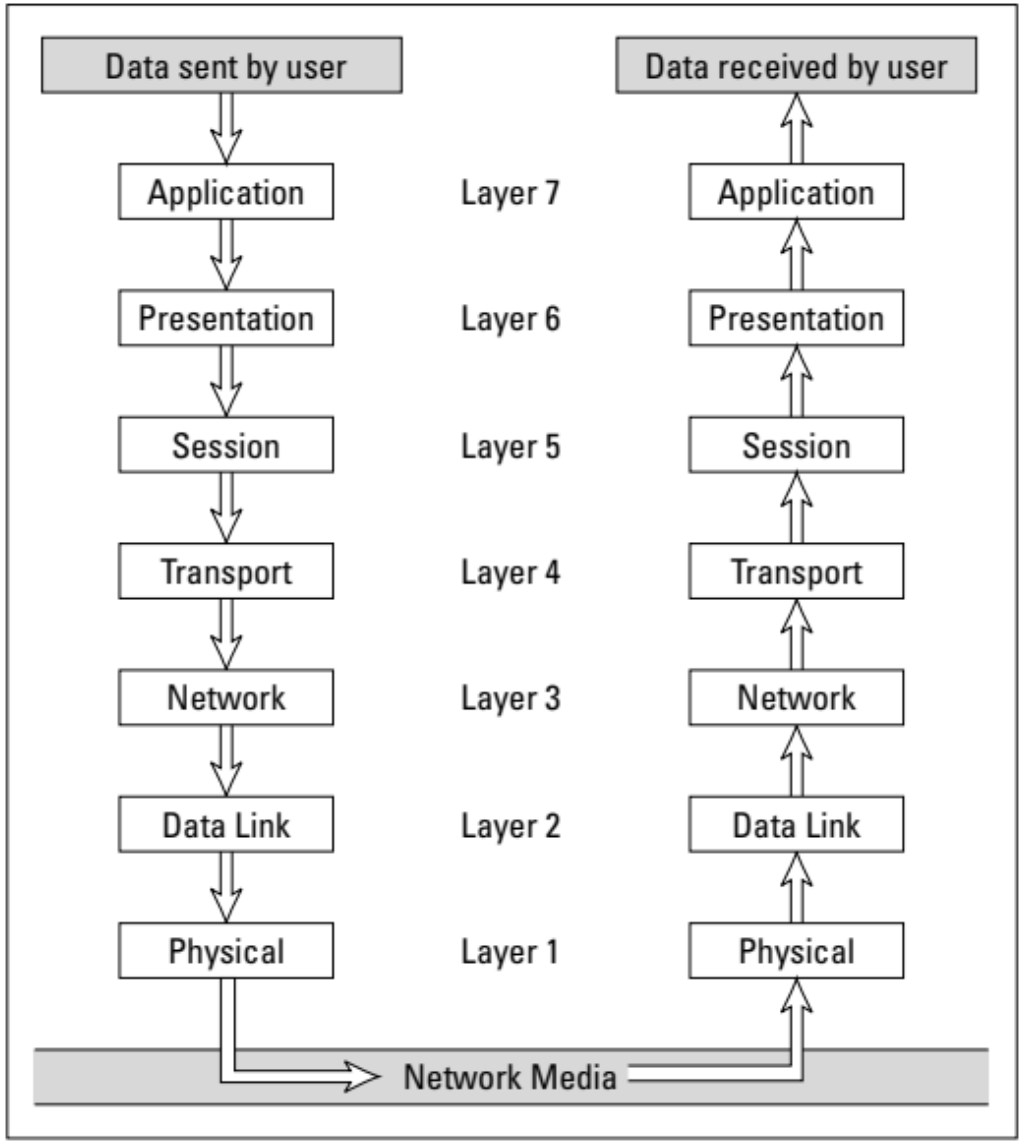
MEDIA

SIGNALS

OSI Model


Sending - Encapsulation
De-Encapsulation - Receiving
7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical
DATA
7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical

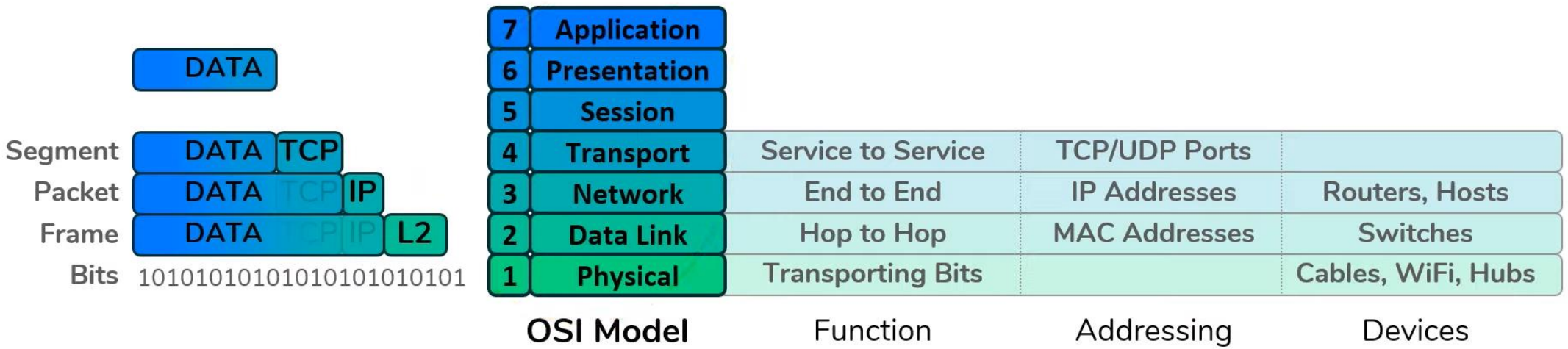
Following a Packet through the Layers

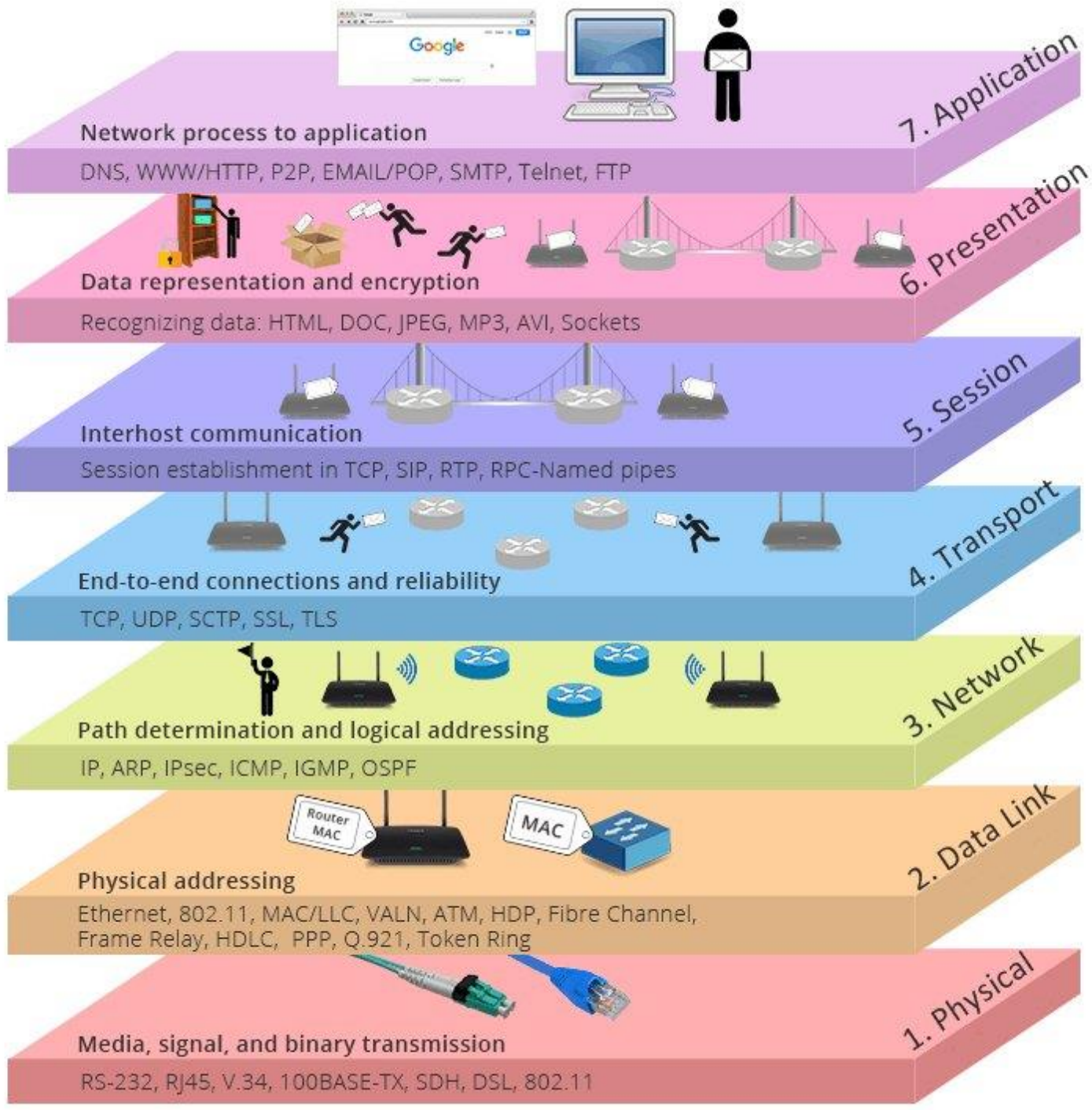


OSI Model

- Network Devices operate at specific layers
- Network Protocols operate at specific layers

- **Neither of these are strict rules** – exceptions exist
- **OSI Model is simply a model** – not rigid rules everything adheres to
  - Conceptualization of what is required for data to flow through the Internet




Google
7. Application
Network process to application
DNS, WWW/HTTP, P2P, EMAIL/POP, SMTP, Telnet, FTP
6. Presentation
Data representation and encryption
Recognizing data: HTML, DOC, JPEG, MP3, AVI, Sockets
5. Session
Interhost communication
Session establishment in TCP, SIP, RTP, RPC-Named pipes
4. Transport
End-to-end connections and reliability
TCP, UDP, SCTP, SSL, TLS
3. Network
Path determination and logical addressing
IP, ARP, IPsec, ICMP, IGMP, OSPF
Router MAC
MAC
2. Data Link
Physical addressing
Ethernet, 802.11, MAC/LLC, VALN, ATM, HDP, Fibre Channel,
Frame Relay, HDLC, PPP, Q.921, Token Ring
1. Physical
Media, signal, and binary transmission
RS-232, RJ45, V.34, 100BASE-TX, SDH, DSL, 802.11

THE ETHERNET PROTOCOL

The first two layers of the OSI model deal with the physical structure of the network and the means by which network devices can send information from one device on a network to another. By far, the most popular set of protocols for the Physical and Data Link layers is *Ethernet*.

Ethernet has been around in various forms since the early 1970s. The current incarnation of Ethernet is defined by the IEEE standard known as 802.3.

Various flavors of Ethernet operate at different speeds and use different types of media. However, all the versions of Ethernet are compatible with each other, so you can mix and match them on the same network by using devices such as bridges, hubs, and switches to link network segments that use different types of media.

- The actual transmission speed of Ethernet is measured in millions of bits per second, or Mbps.
- Ethernet comes in three different speed versions: 10Mbps, known as Standard Ethernet; 100Mbps, known as Fast Ethernet; and 1000Mbps, known as Gigabit Ethernet.
- However, that network transmission speed refers to the maximum speed that can be achieved over the network under ideal conditions. In reality, the actual throughput of an Ethernet network rarely reaches this maximum speed.

Ethernet operates at the first two layers of the OSI model — the Physical andthe Data Link layers. However, Ethernet divides the Data Link layer into two separate layers known as the Logical Link Control (LLC) layer and the Medium Access Control (MAC) layer.

ETHERNET AND THE OSI MODEL