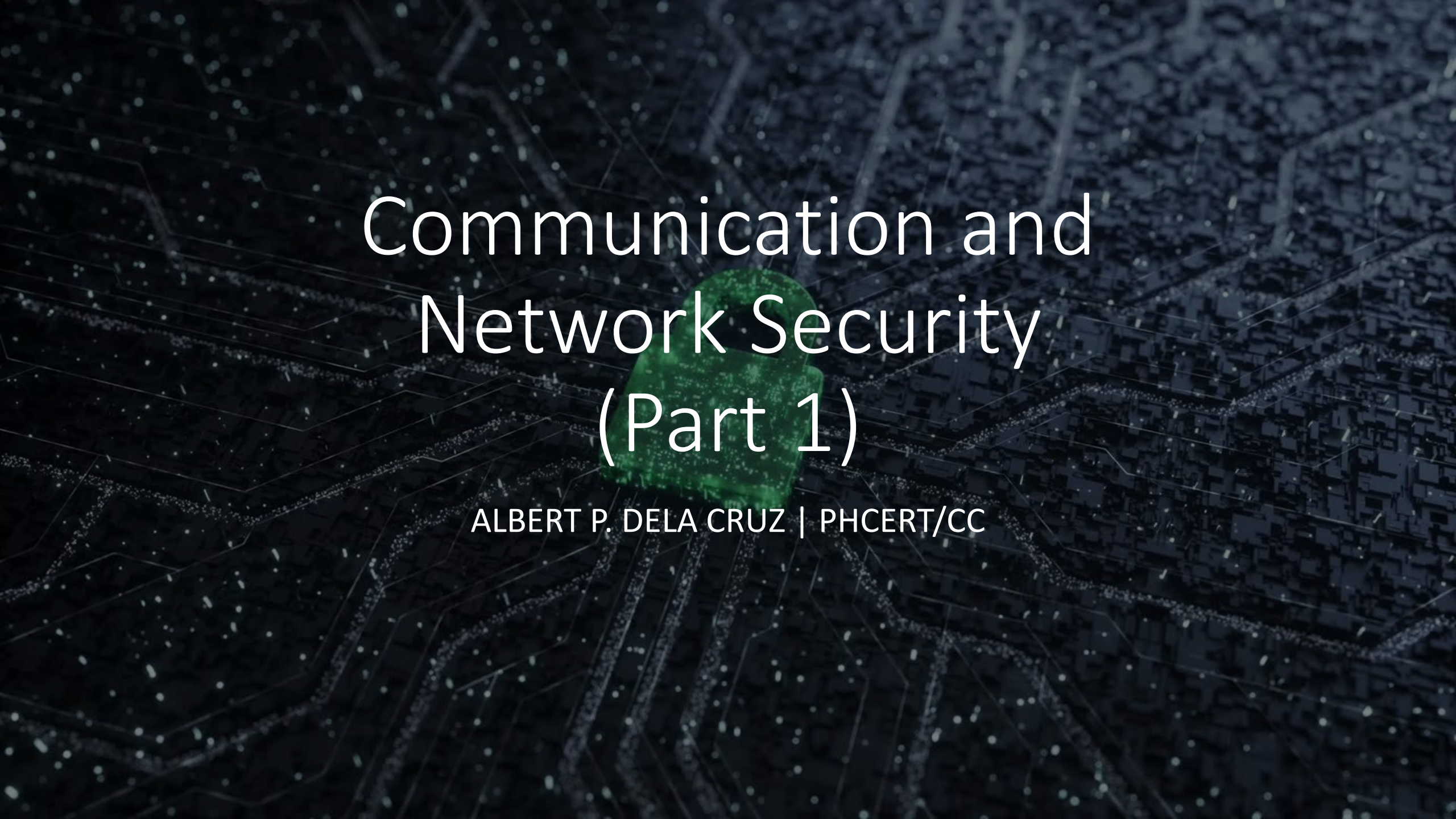
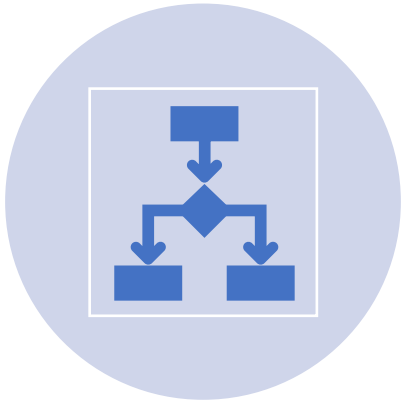


Communication and Network Security (Part 1)

ALBERT P. DELA CRUZ | PHCERT/CC

Communications and Network Security

COMMUNICATIONS IS HOW EVERYTHING IS INTERCONNECTED

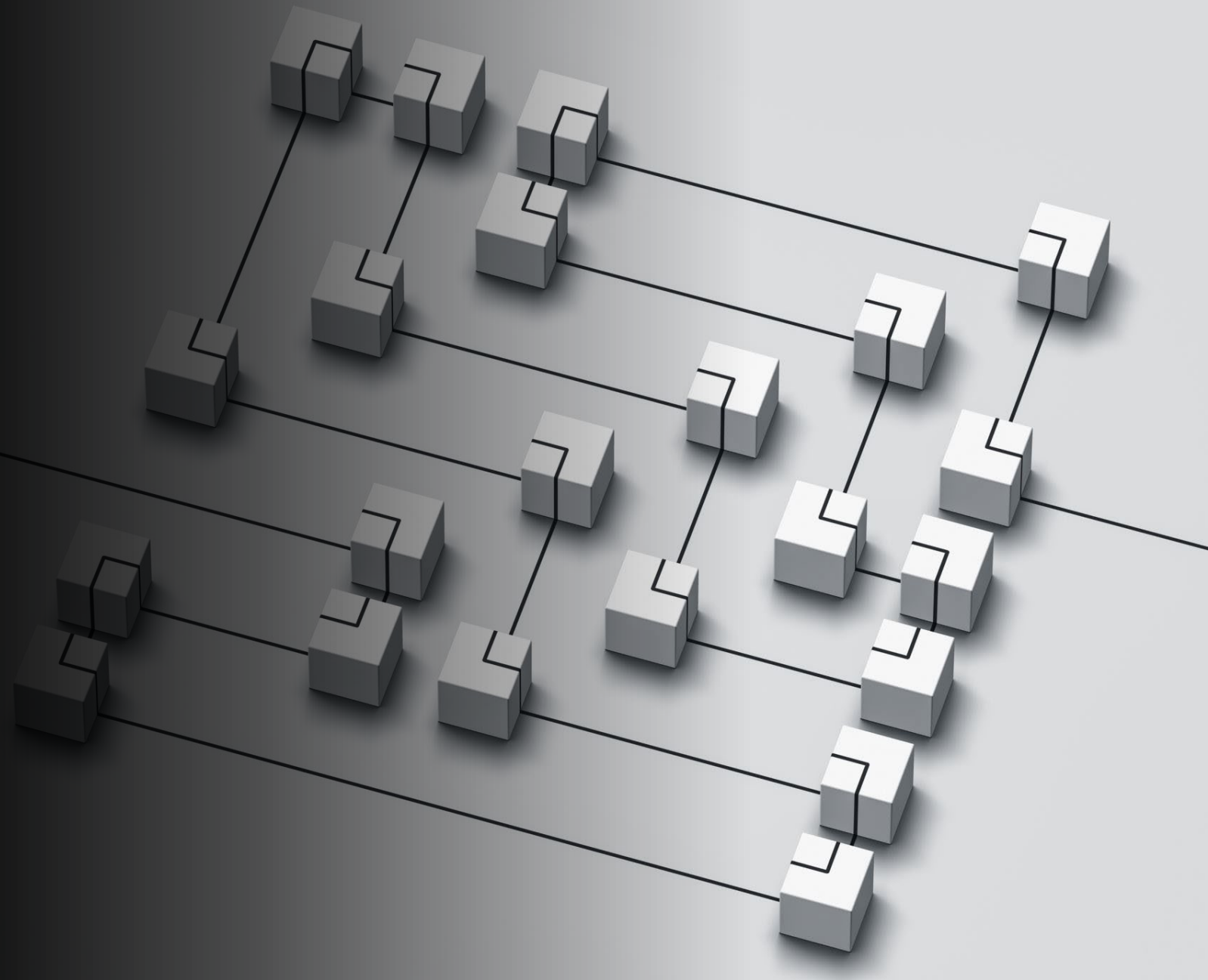


NETWORK SECURITY IS CONCERNED WITH PROTECTING THE C.I.A. OF “DATA IN MOTION”

ONE OF THE VERY LONG AND TECHNICAL INFORMATION SECURITY DOMAIN

Network Architecture and Design

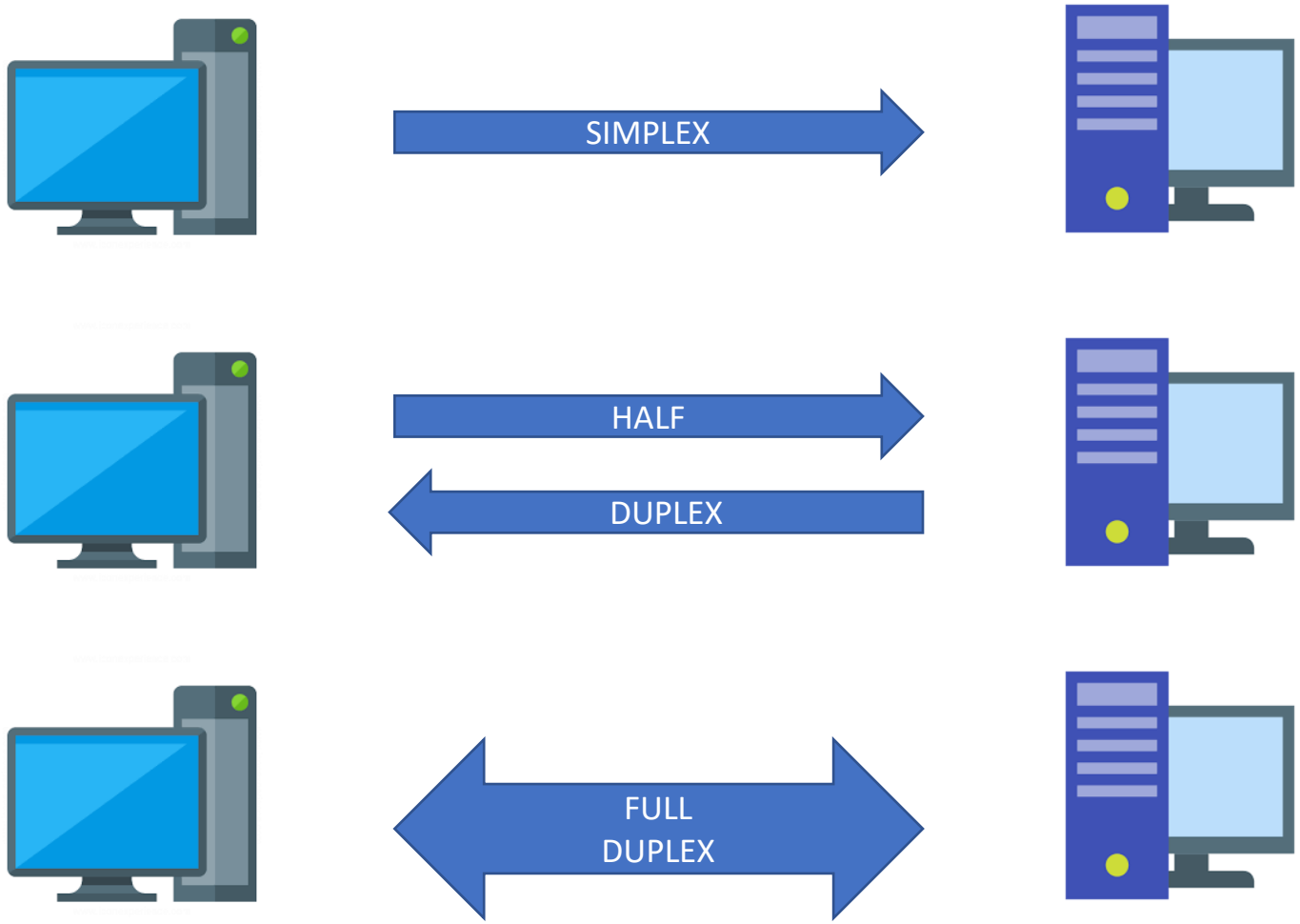
How networks should be designed, and the necessary controls needed



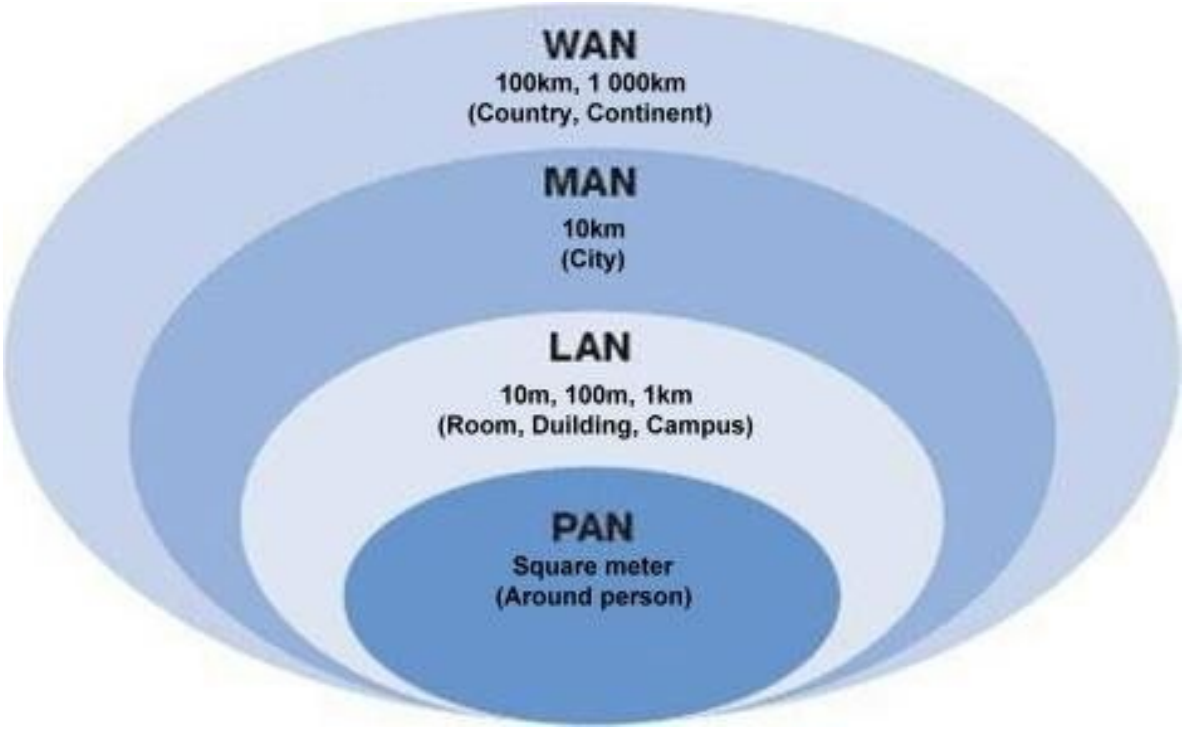
Transmission Modes

Simplex mode	Half-duplex mode	Full-duplex mode
The communication is unidirectional.	The communication is bidirectional, but one at a time.	The communication is bidirectional.
A device can only send data but cannot receive it or it can only receive data but cannot send it.	Both the devices can send and receive the data, but one at a time.	Both the devices can send and receive the data simultaneously.
The lowest performance among the mods.	The performance is better than simplex but less than full duplex.	The highest performance among the mods.
Examples are radio, keyboard, and monitor.	Example is Walkie-Talkies.	Example is a telephone or mobile network.

Transmission Modes

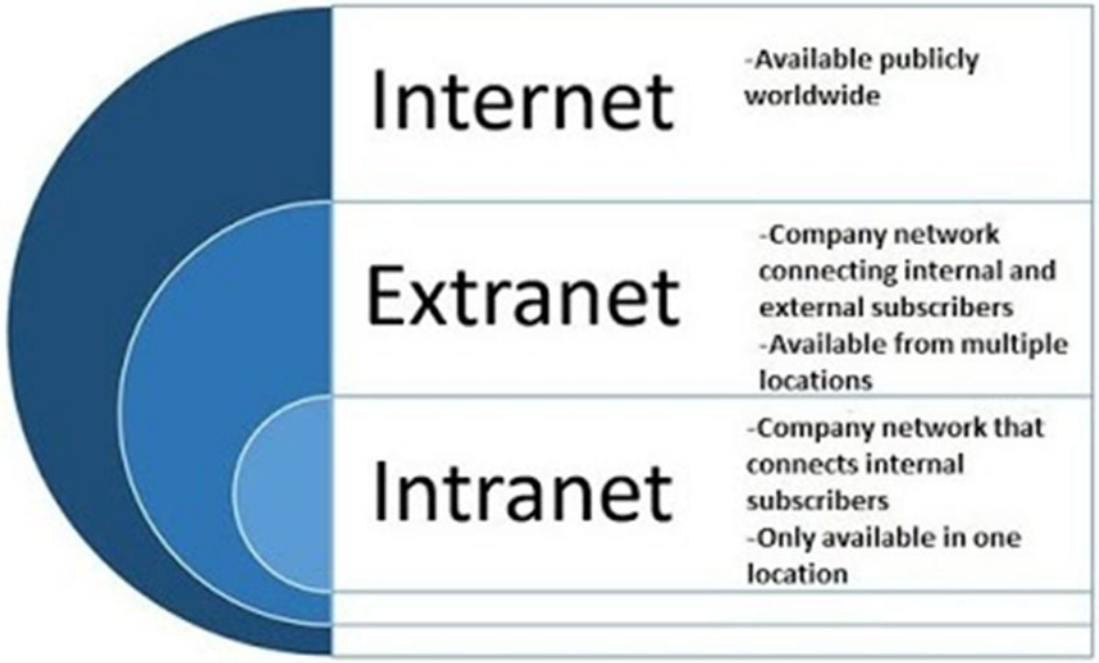


Network Types



* A GAN is a global area network, which is a global collection of WANs

Internet, Intranet, Extranet

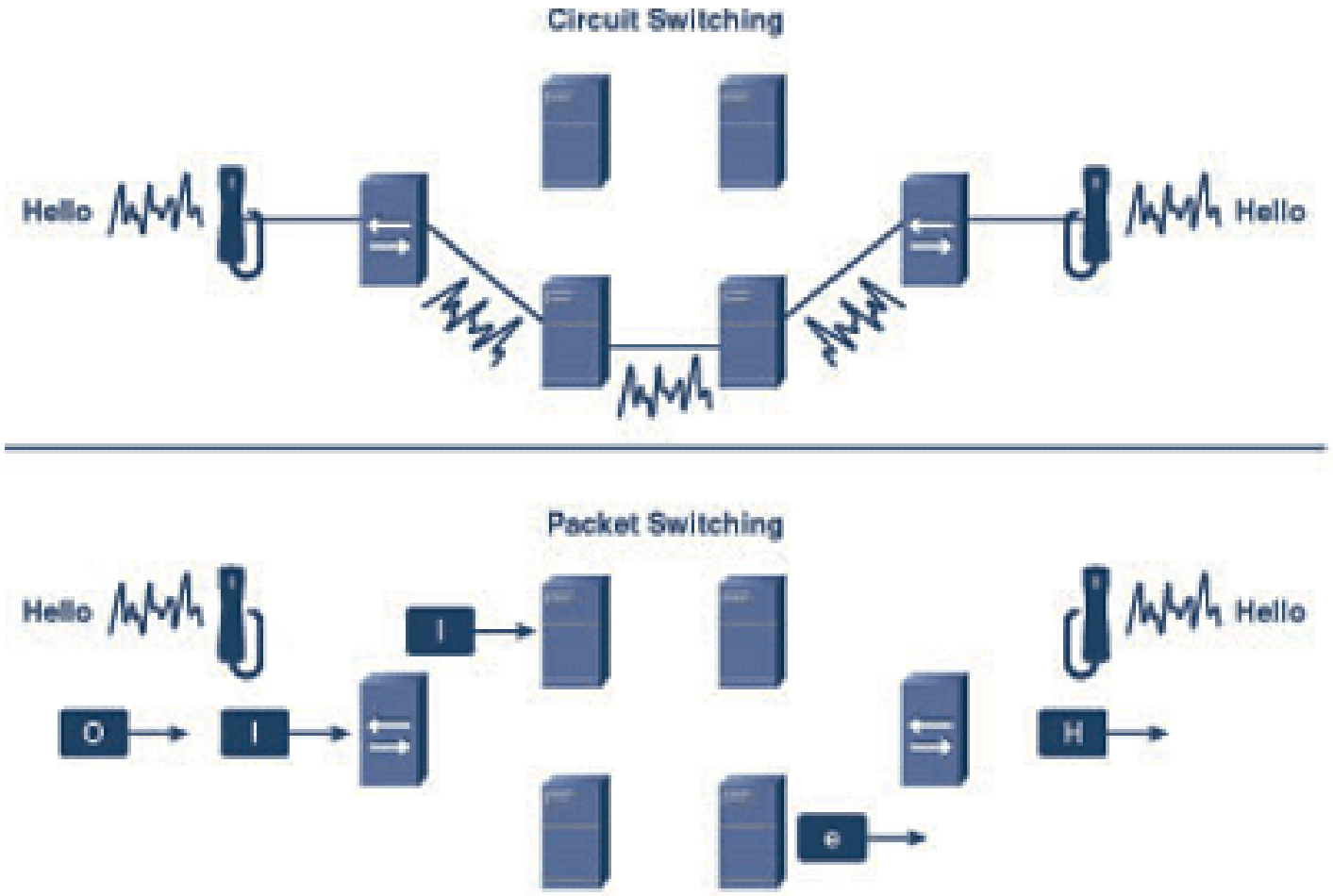


- Global Network of Computers that exchanges information
- Network of Networks with millions of private, public, academic, business and government networks.

- Intranet for outside (but authorized) users
- Inter-organizational information system
- Allows external parties to collaborate with company employees

- Internal Company Networks
- Accessed only by authorized persons or members of the organization

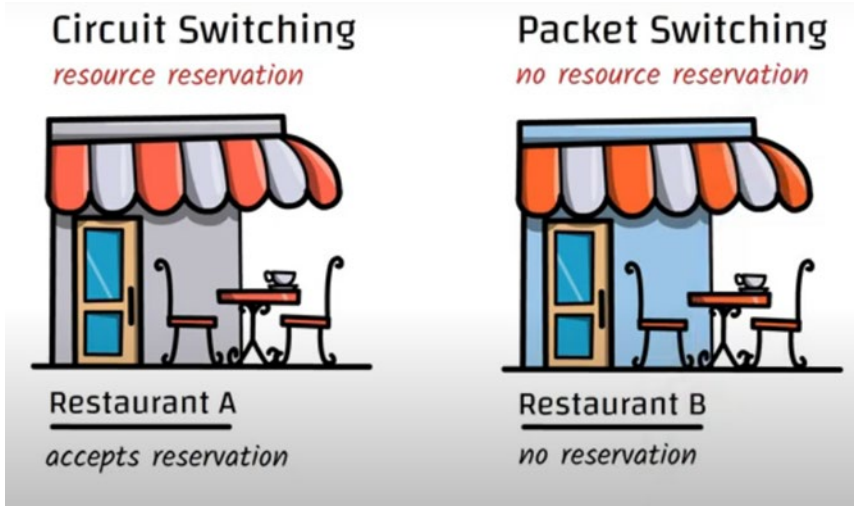
Circuit Switched, Packet Switched



Circuit Switched, Packet Switched

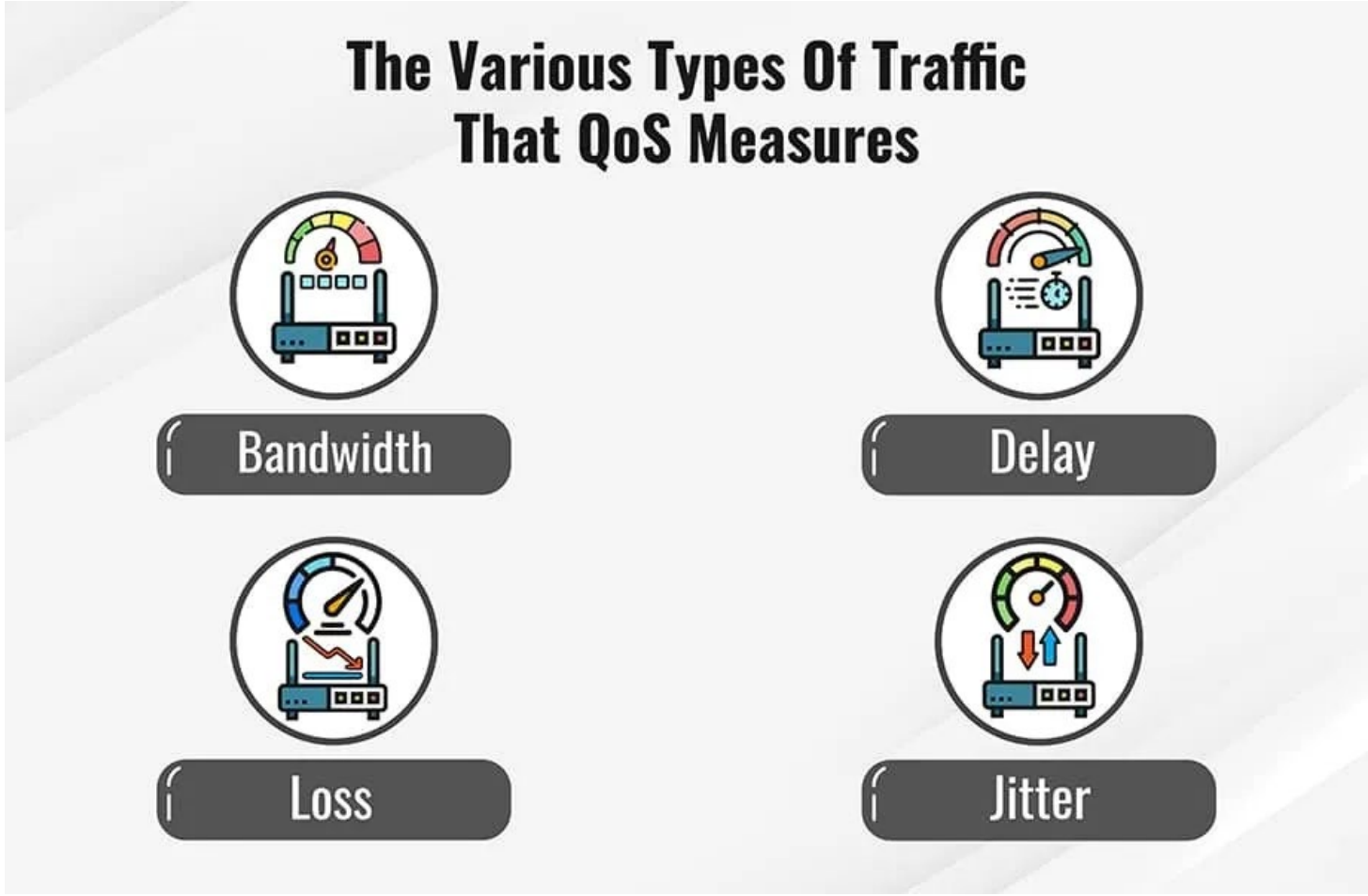
CIRCUIT SWITCHING	PACKET SWITCHING
Full capacity of circuit dedicated to conversation. When no data is transmitted, the circuit's capacity is unused, but still committed.	Conversations share connections, so the capacity available to any conversation can vary from moment to moment. It can carry more conversations, as most conversations have lulls during which little data is transmitted—what is unused capacity in a circuit-switched network is available to all other conversations.
No overhead for connections; data throughout the network identical to data as first encoded and sent.	Packets contain the sent data, plus various "envelopes" in the form of added data—e.g., headers to identify sender and destination, to direct routing, to encode metadata about the data, and to provide for error correction.
Fixed route for a conversation, defined by the circuit established to carry it.	Variable and dynamic routing; a packet may follow a different path than its predecessor to the same destination, based on changes in latency, packet loss and performance measures.
Constant latency defined by distance; excellent for real-time communications.	Variable latency dependent on both distance and network equipment load.
Fixed limit to number of conversations possibly determined by the number of strands of wire, optical fiber or separate radio channels in each segment of a network.	No simple, fixed limit on conversations. Conversations can be added as long as bandwidth remains and the network components have resources to cope with them. Some components will have fixed limits on how many conversations they can manage, but these limits tend to be very high.

Circuit Switching	Packet Switching
Physical path between source and destination	No physical path
All packets use same path	Packets travel independently
Reserve the entire bandwidth in advance	Does not reserve
Bandwidth Wastage	No Bandwidth wastage
No store and forward transmission	Supports store and forward transmission

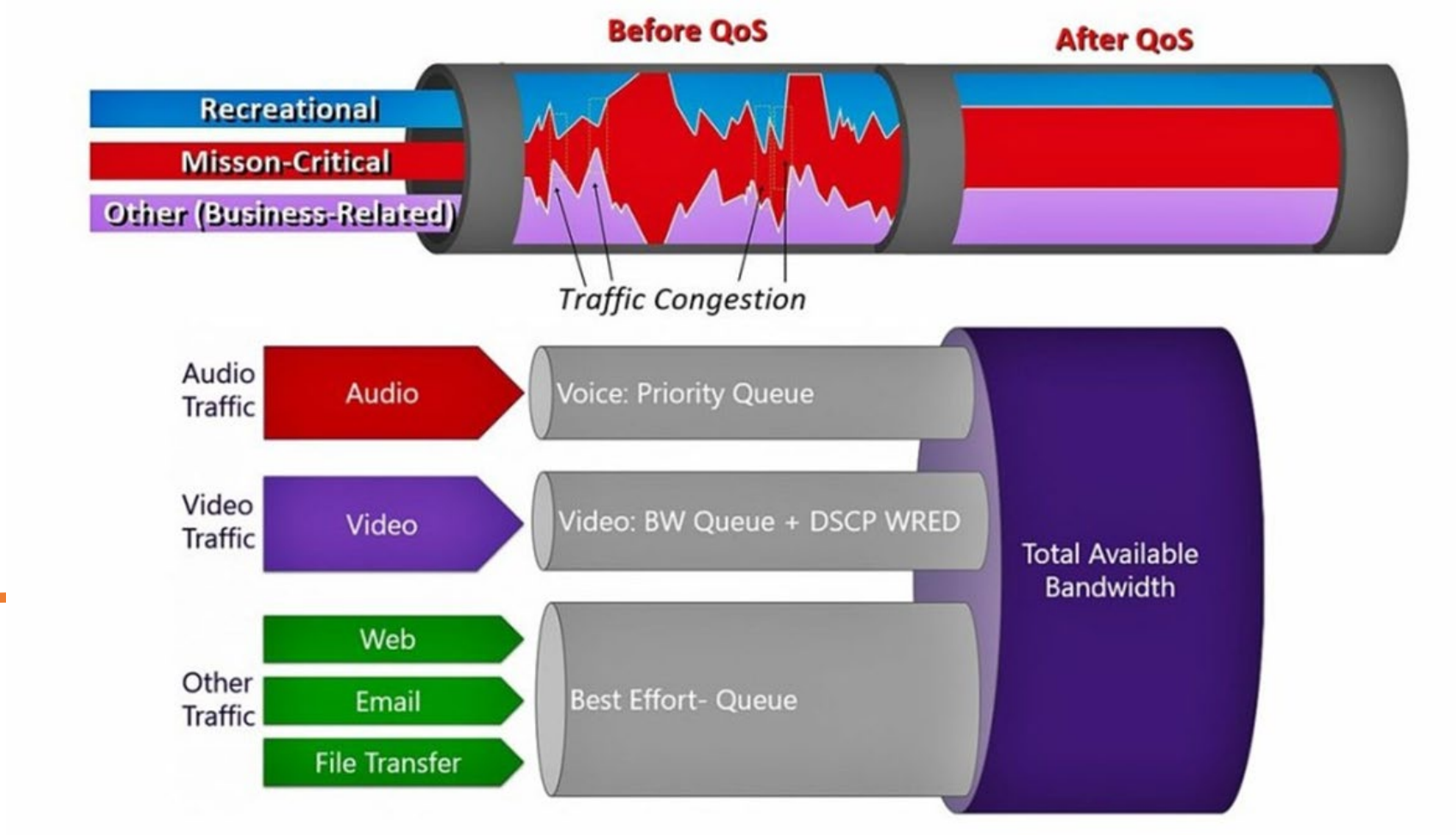


Quality of Service (QOS)

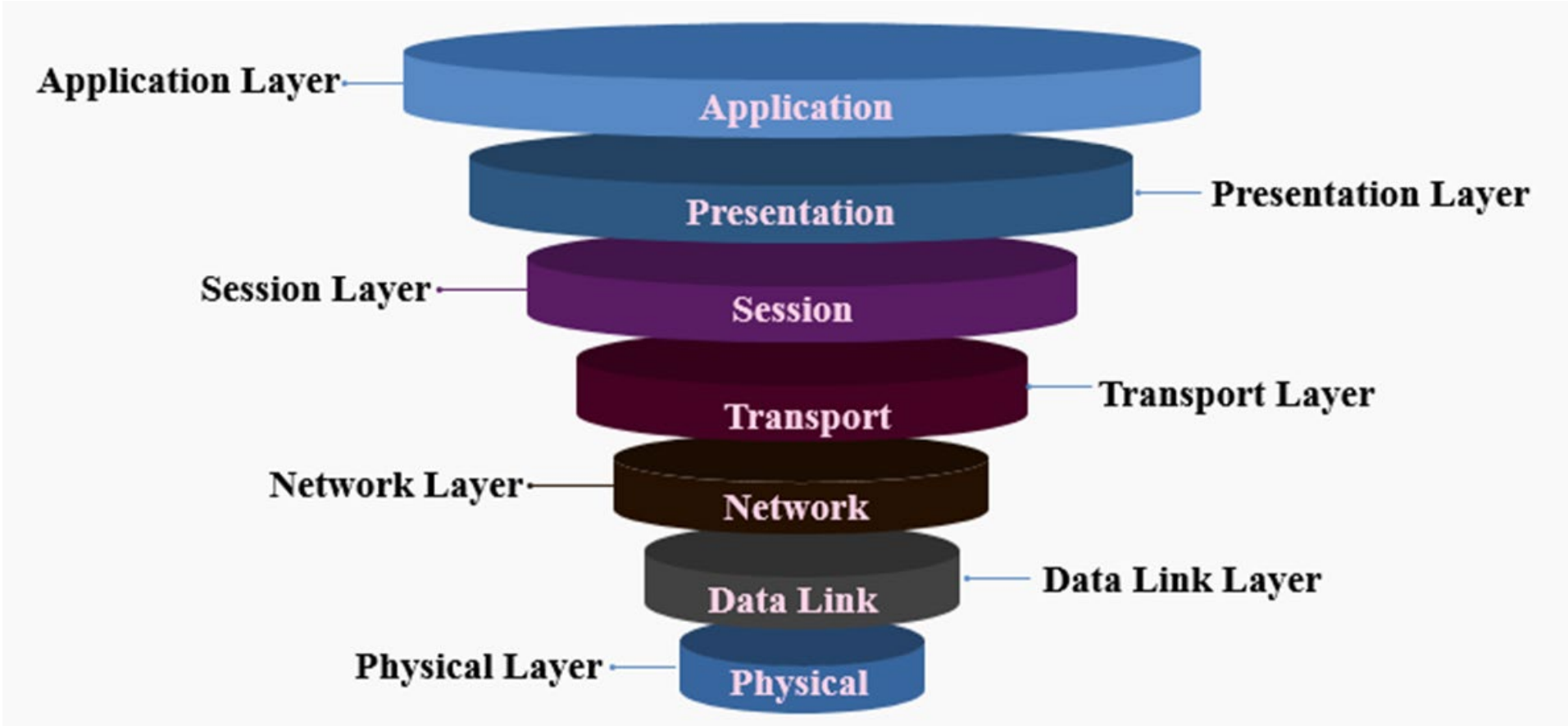
- Providing guaranteed delivery of service for applications that require prioritization. Done by guaranteeing sufficient bandwidth, controlling latency (lag) and jitter, as well as preventing data loss.



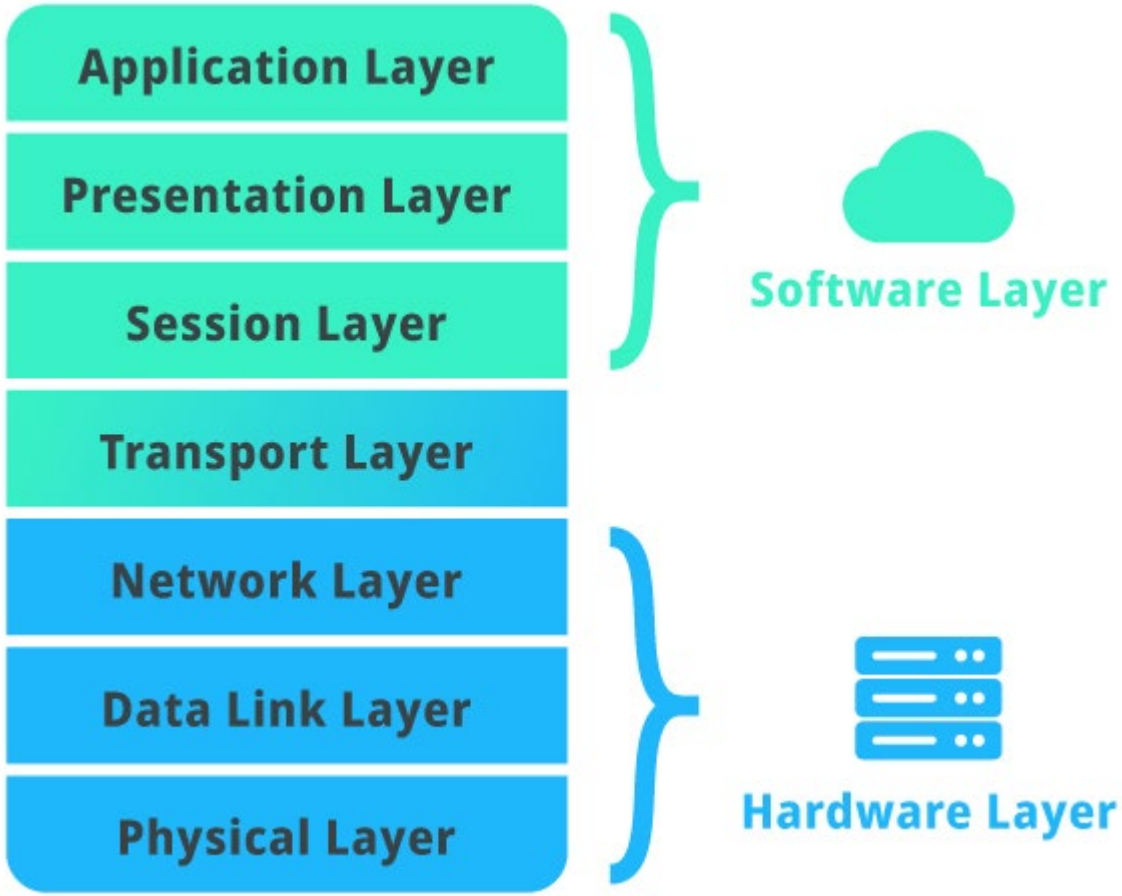
Quality of Service (QOS)



The ISO-OSI Model



The OSI Model

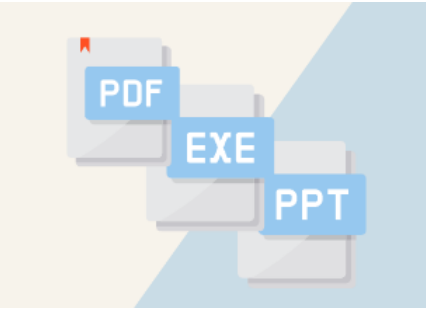


- The **OSI Model** or **Open Systems Interconnection model** is a conceptual model that is used to understand how data is communicated between one device to another within a computer network.
- It was developed by ISO (**International Organization of Standardization**) in 1984. OSI Model consists of 7 abstraction layers, wherein each layer is a package of standard communication protocols specifically designed to perform specific functionalities.

The OSI Model

LAYER 7: Application

- Provides an Interface for users to interact with the network.
  - i.e., Operating Systems, web browsers, email clients
- Provides capability for services to operate on the network.
  - Common Protocols: HTTP, DNS, FTP, Telnet, POP3/IMAP
  - Devices: PCs, Firewalls, IDS



LAYER 6: Presentation

- Negotiates and prepares how the data is presented to the user and the network.
- Handles Encryption, Decryption and File Compression
  - i.e., File Types, ASCII, etc.
  - Devices: PCs, Firewalls

LAYER 5: Application

- Overseas the setup, maintenance, and termination of sessions.
- Provides management of multiple sessions (each client connection is called a session)
- Assign Session ID numbers to each session to keep data streams separate.
  - Protocols: SIP, PPTP
  - Devices: Firewalls

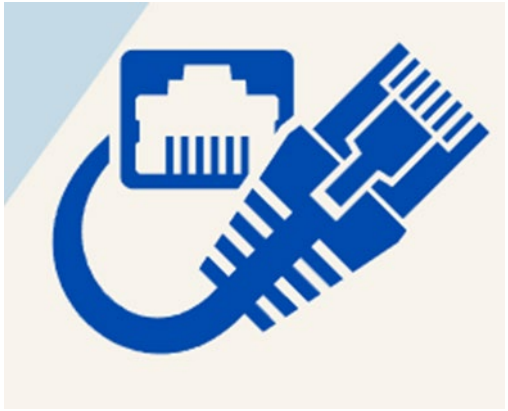
LAYER 4: Transport

- Provides a transition between the upper and lower layers.
- Determines if data delivery will be reliable/connection-oriented (TCP) or unreliable/connectionless (UDP) delivery of data.
- Data transferred at this layer are called '**segments**'
  - Protocols: TCP/UDP
  - Devices: Firewalls

The OSI Model

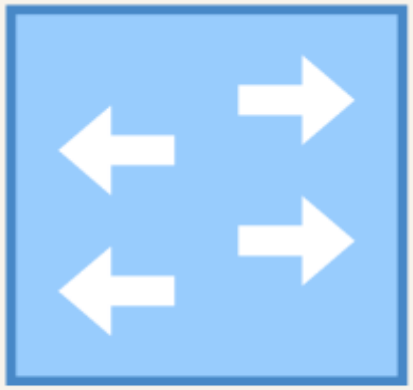
LAYER 3: Network

- Responsible for routing data across networks and on to the destination.
- Hosts are identified by their logical address (IP Address), determine the best path to send data.
- Data transferred at this layer is called '**Packets**'
  - Protocols: IPV4, IPV6, EIGRP, OSPF
  - Devices: Routers



LAYER 1: Physical

- Converts data into electrical signals to send over the wire.
- Data Transferred at this layer is called '**Bits**'.
- Provides management of multiple sessions (each client connection is called a session)
- Assign Session ID numbers to each session to keep data streams separate.
  - Devices: Cables, Hubs, Repeaters



LAYER 2: Data Link

- Sends and receives traffic on the same network segment (VLAN)
- Provides Flow Control, verifies data to and from the Physical Layer is error-free
- Devices are identified by their Physical Address (MAC Address).
- Data Transferred at this layer is called '**Frames**'.
  - Protocols: Ethernet, PPP, Frame Relay
  - Devices: Switch, Modems

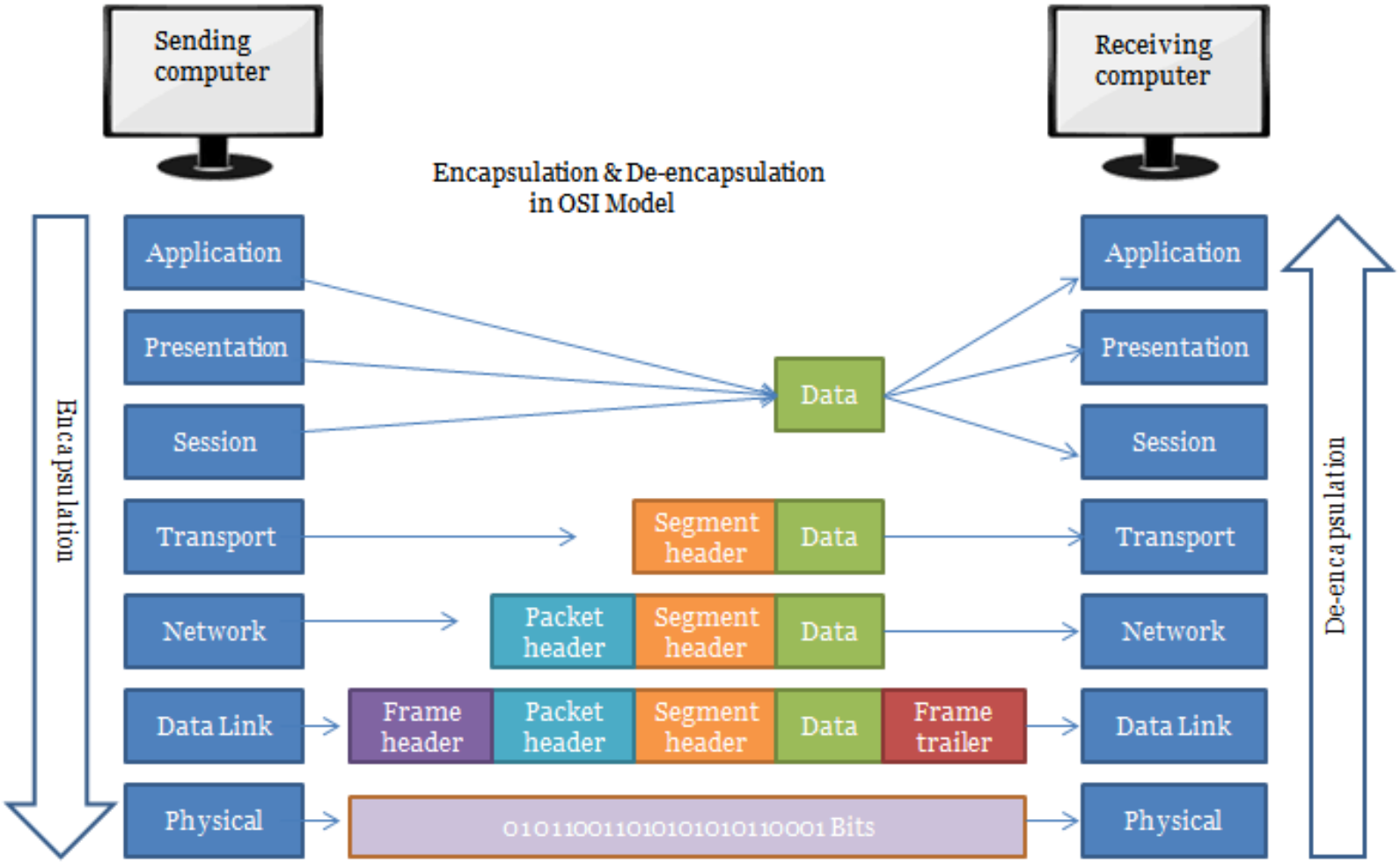
Encapsulation:
The process of adding additional headers to data. This is done by the sending host.

De-encapsulation:
The process of opening up encapsulated data. This is done by the receiving host.

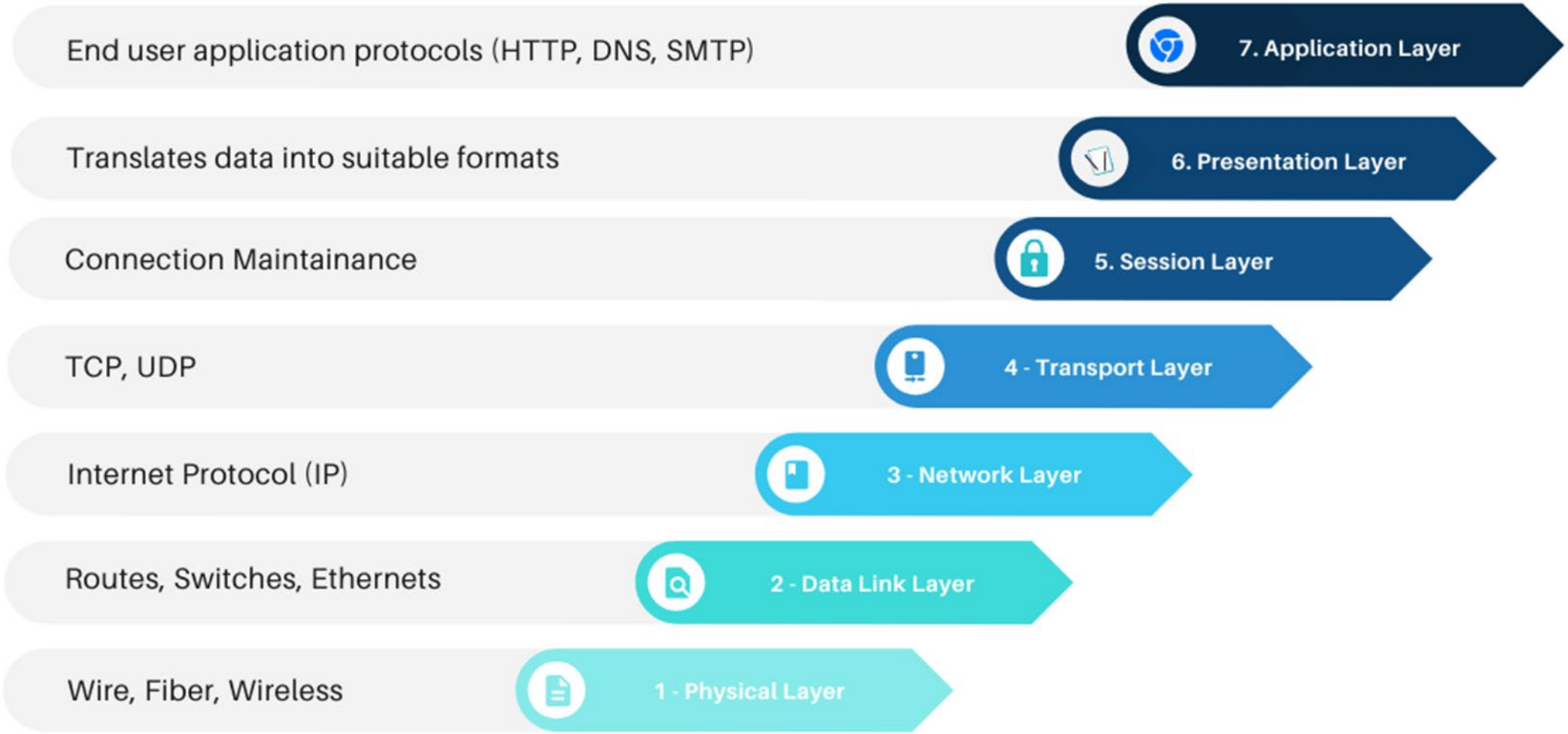
The OSI Model

Encapsulation:
The process of adding additional headers to data. This is done by the sending host.

De-encapsulation:
The process of opening up encapsulated data. This is done by the receiving host.



The OSI Model (Summary)

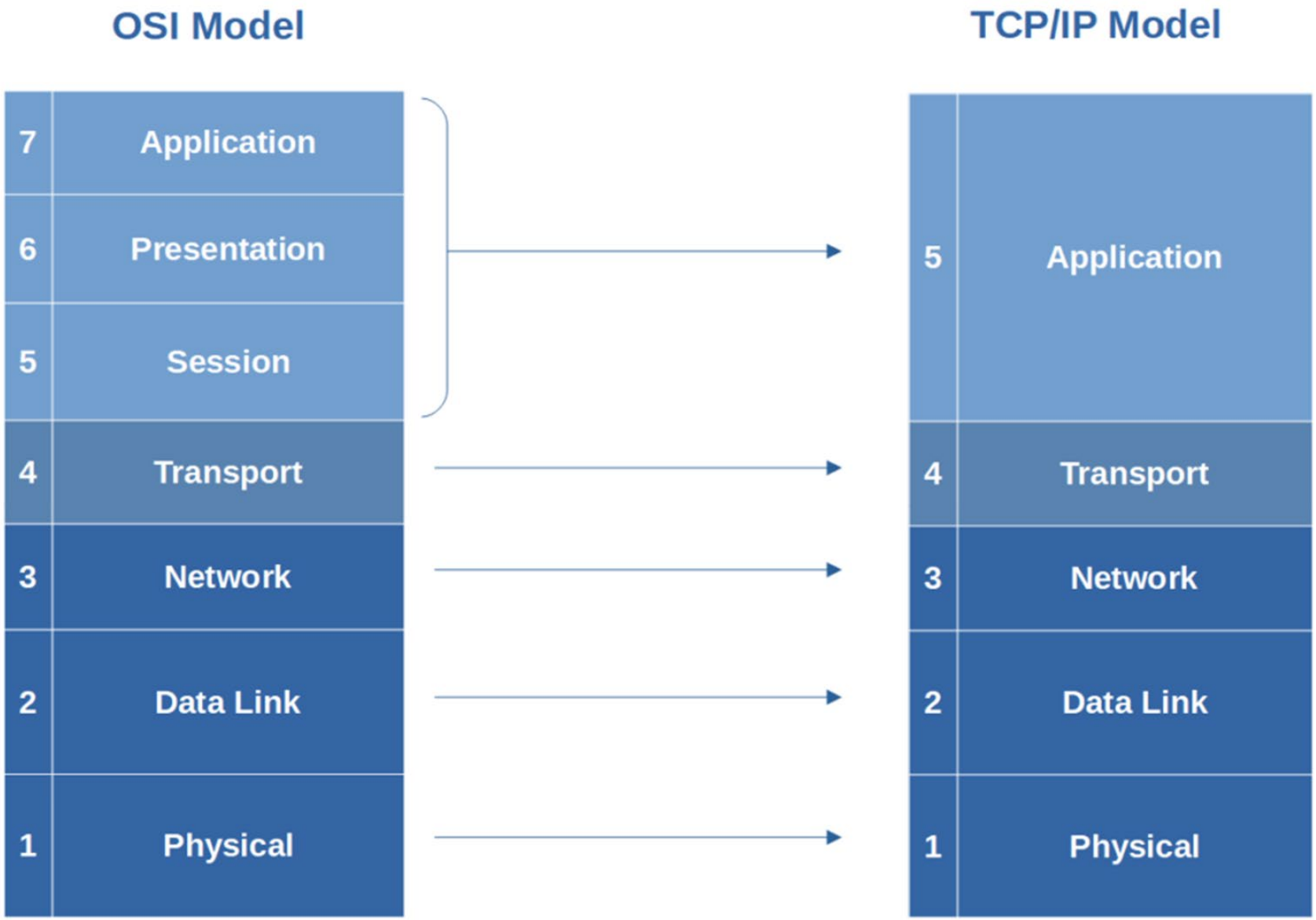


The TCP/IP Model

TCP/IP

- TCP/IP stands for Transmission Control Protocol/Internet Protocol and is a suite of communication protocols used to interconnect network devices on the internet.
- TCP/IP is also used as a communications protocol in a private computer network (an intranet or extranet).

TCP/IP vs OSI


OSI Model
7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical
TCP/IP Model
5 Application
4 Transport
3 Network
2 Data Link
1 Physical

TCP/IP (Layer 4)

Layer 4 **Application Layer**

This layer sends files such as a web page to the transport layer. Some common high-level protocols include:

- Web browsers and web servers that exchange information using HTTP & HTTPS protocols
- Email applications using POP (Post Office Protocol) and SMTP (Simple Mail Transfer Protocol) protocols
- Servers using FTP (File Transfer Protocol) protocols
- Telnet
- NFS (Network File System)
- RIP (Routing Information Protocol)

Layer by Layer Analogy: Mailing a Letter

You write a letter to your cousin and hand it to your friend

Your cousin reads the letter

TCP/IP (Layer 3)

Layer 3 **Transport Layer (TCP)**

This layer's main concern is with host-to-host communication, the source and destination in the network (e.g., web browser and web server). It breaks up data into packets, controls flow congestion, and establishes connections. This layer can also request retransmission if a packet is lost for reliable transmission of data.

The two protocols available in this layer include:

- TCP (Transmission Control Protocol)
- UDP (User Datagram Protocol)

C:\ _ Bonus: Try "ping" in your Command Prompt to see if your packet has been sent and received and "Tracert" (trace route) to see where your packets are being sent to arrive to its destination. Learn how to here: https://www.netgains.org/blog/how-to-do-ping-and-traceroute-for-windows-and-mac

Your friend puts the letter into an envelope, addresses it, stamps it, and drops it off at a mailbox

Your aunt opens the mail and passes the letter to your cousin

TCP/IP (Layer 2)

Layer 2 **Internet Layer (IP)**

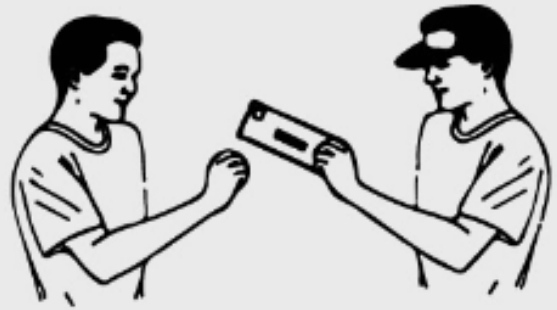
The Internet Layer (a.k.a. IP) addresses, routes a packet, and delivers packets from source to destination based only on its address. The primary protocol in this layer is the Internet Protocol, which uses IP addresses to transport packets to the next IP router that has connectivity to a network closer to the final data destination. It is referred to as a layer that establishes internetworking.

Other protocols in this layer include:

- ARP (Address Resolution Protocol)
- ICMP (Internet Control Message Protocol).

A mailman collects the letter, puts it in a mail bag and brings it to the post office

The letters are sorted by area and are given to a carrier for delivery



TCP/IP (Layer 1)

Layer 1 **Network Interface Layer**

The Network Interface layer transports a bit or a packet in the network medium. Examples of network mediums include:

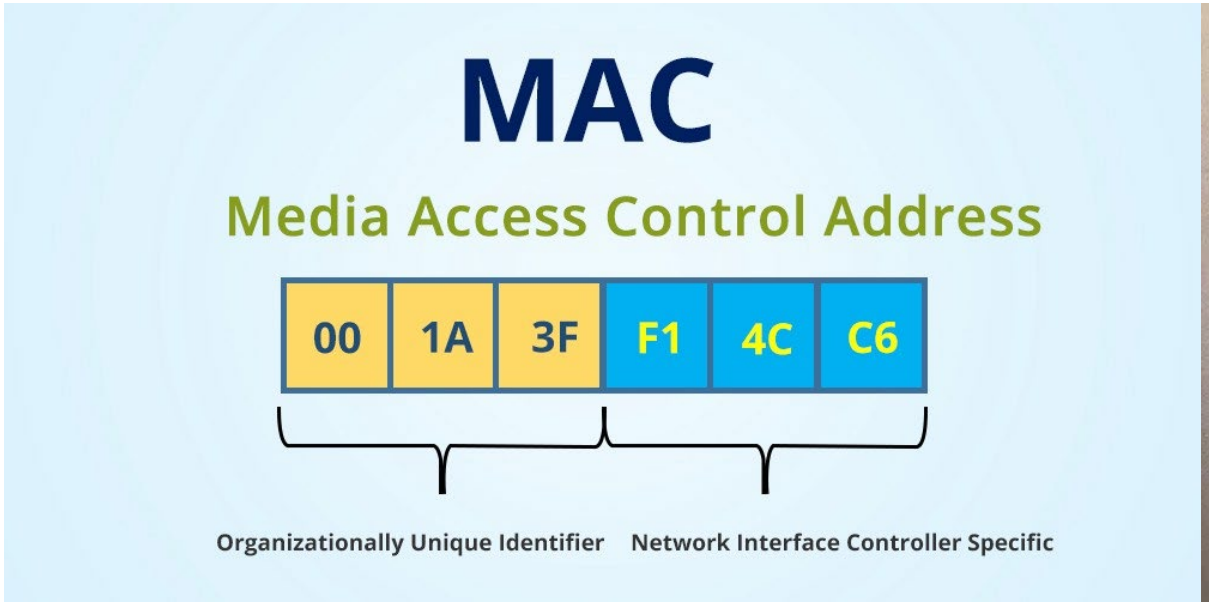
- Ethernet
- Wi-Fi
- DSL (Digital Subscriber Line)

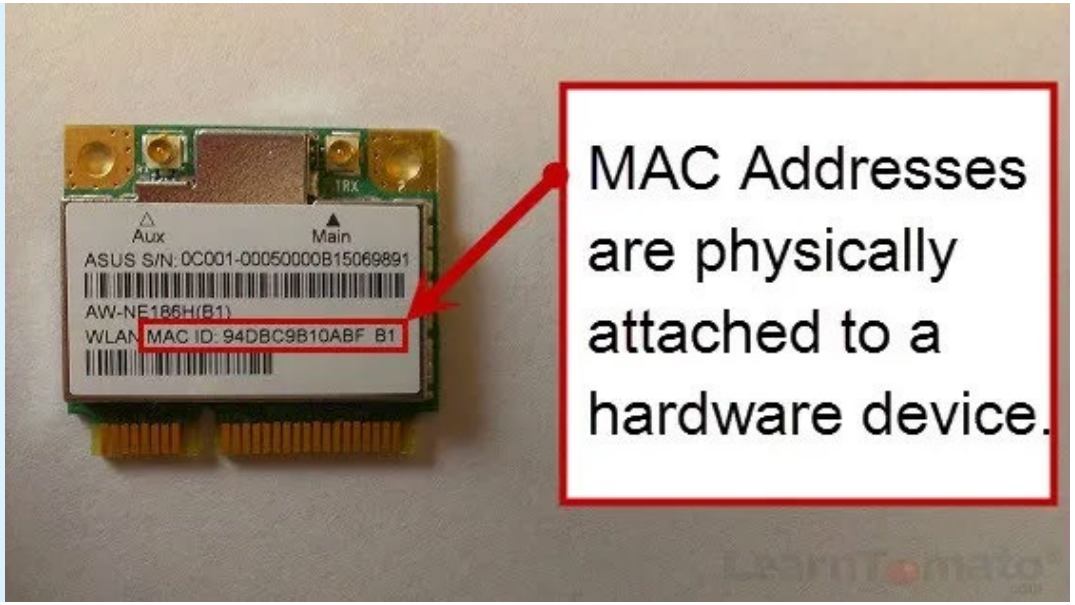
Network cables and hubs are also part of this layer. This physical layer standardizes the electrical signals that networks use. It also defines cable and wireless standards and how bits are placed on the physical media, thus dealing with how we send and receive 0s and 1s which represent our data.

The Postal service delivers the mail bag to a sorting office.

MAC Addresses

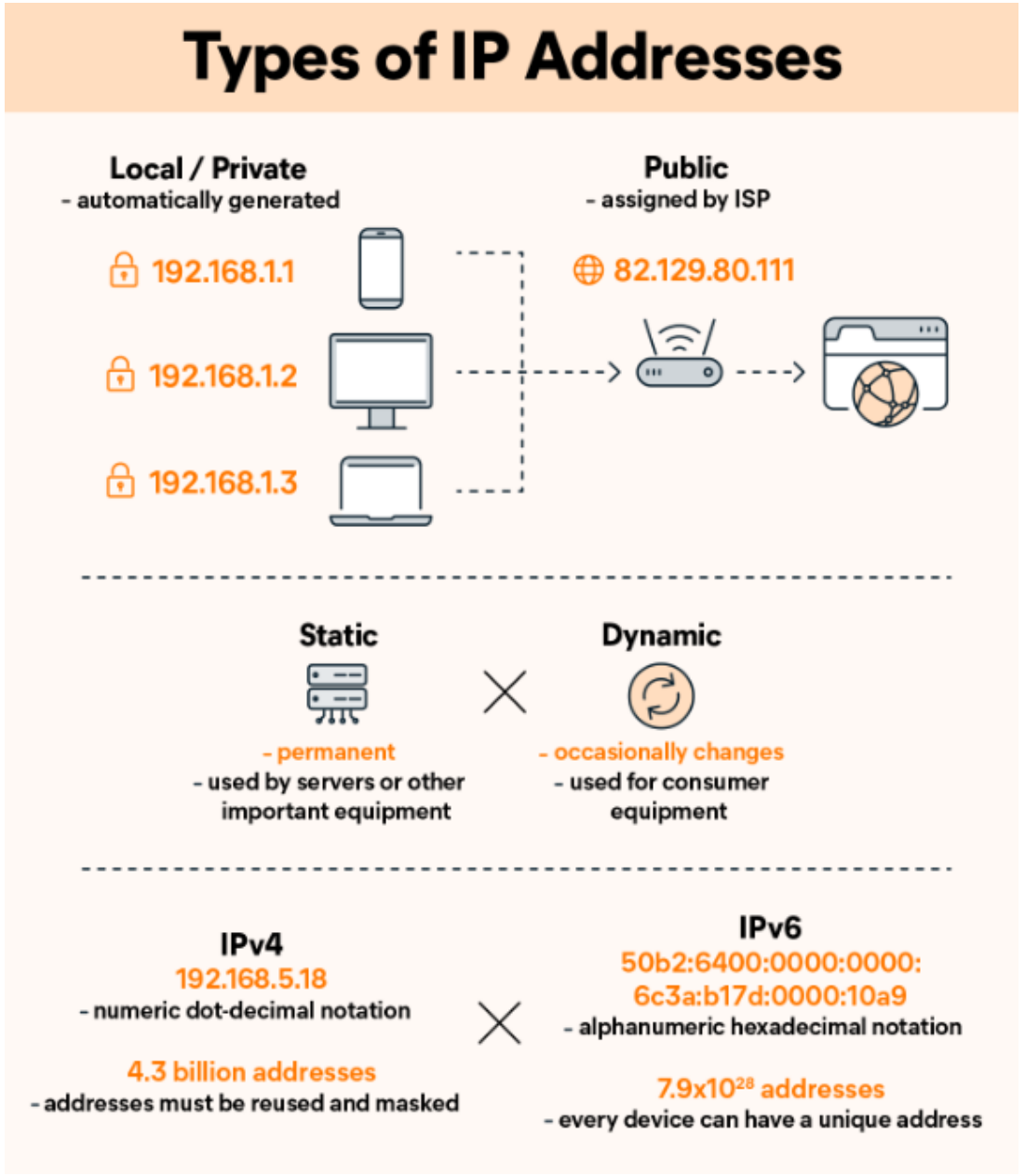
A media access control address (MAC address) is a unique identifier assigned to a network interface controller (NIC) for **use as a network address in communications within a network segment**.





IP Addresses

An Internet Protocol (IP) address is the unique number that gets assigned to your connected device. Every mobile phone, laptop, cable box, tablet, server along with thousands of other types of devices (IoT) that are connected to a computer network has one.



TCP vs UDP

What is TCP?

Transmission Control Protocol (TCP) is connection-oriented, meaning once a connection has been established, data can be transmitted in two directions. TCP has built-in systems to check for errors and to guarantee data will be delivered in the order it was sent, making it the perfect protocol for transferring information like still images, data files, and web pages.

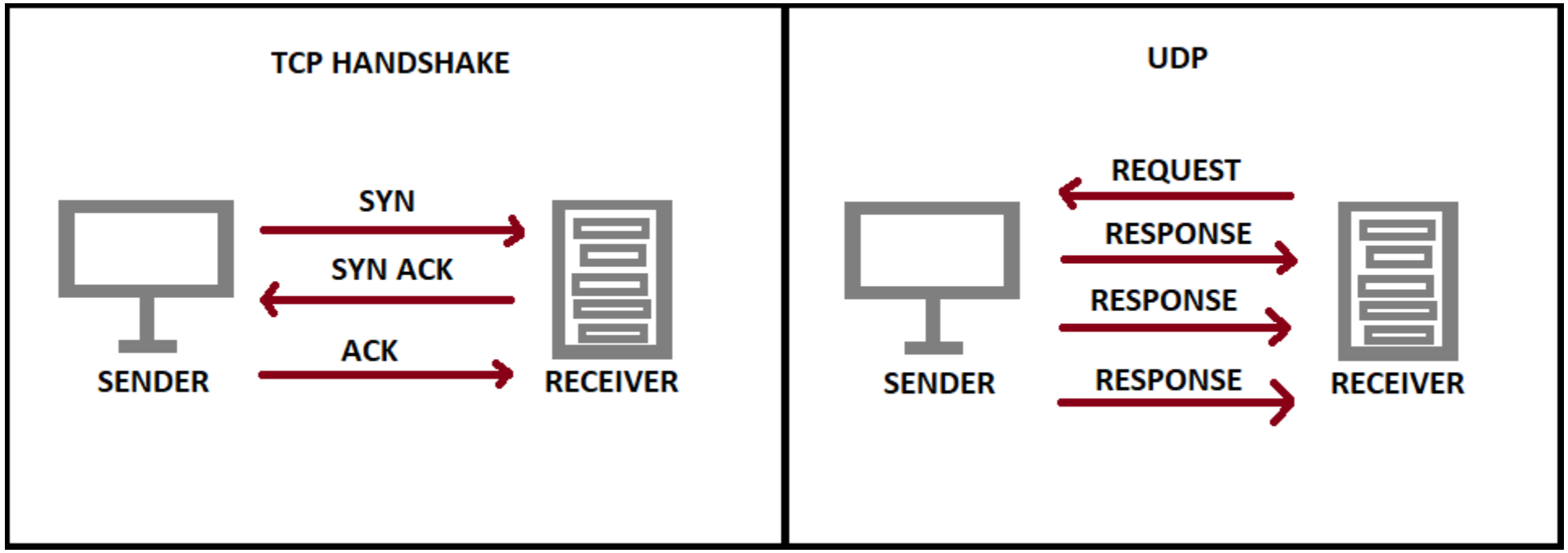
But while TCP is instinctively reliable, its feedback mechanisms also result in a larger overhead, translating to greater use of the available bandwidth on your network.

What is UDP?

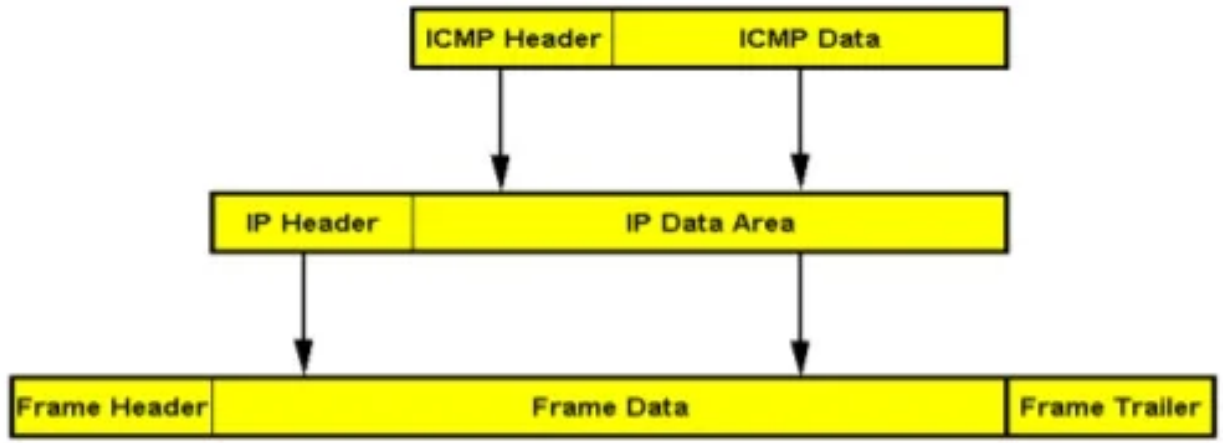
User Datagram Protocol (UDP) is a simpler, connectionless Internet protocol wherein error-checking and recovery services are not required. With UDP, there is no overhead for opening a connection, maintaining a connection, or terminating a connection; data is continuously sent to the recipient, whether or not they receive it.

Although UDP isn't ideal for sending an email, viewing a webpage, or downloading a file, it is largely preferred for real-time communications like broadcast or multitask network transmission.

TCP vs UDP


TCP HANDSHAKE
SYN
SYN ACK
ACK
SENDER
RECEIVER
UDP
REQUEST
RESPONSE
RESPONSE
RESPONSE
SENDER
RECEIVER

Internet Control Message Protocol ICMP



The Internet Control Message Protocol (ICMP) is a control protocol that is considered to be an integral part of IP, although it is architecturally layered upon IP - it uses IP to carry its data end-to-end. ICMP provides error reporting, congestion reporting, and first-hop router redirection.

Internet Control Message Protocol ICMP