What is Networking

- Networking is the practice of connecting computers, devices, and systems so they can share resources, communicate, and exchange data

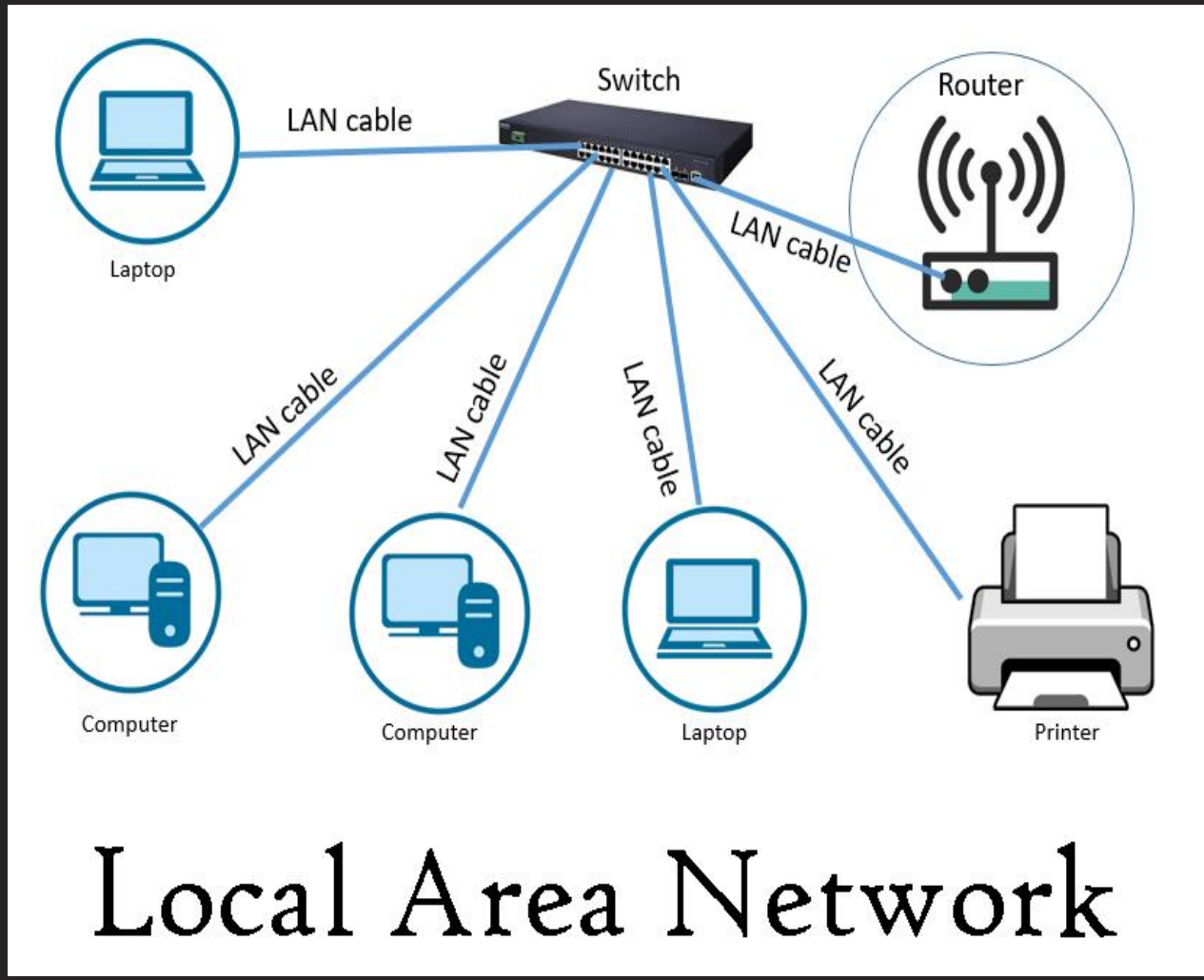
- Real Life example: you're in a bustling city like New York, where everyone is trying to deliver letters to specific destinations. How does this chaos stay organized?

Importance of Networking in Cybersecurity and SOC

1.A thief intercepts the letters (a hacker stealing data)?
2.Someone starts sending fake letters (malware or phishing emails)?

Types of Networking

1.LAN (Local Area Network)
2.WAN (Wide Area Network)
3.MAN (Metropolitan Area Network)
4.PAN (Personal Area Network)



1.LAN (Local Area Network):

A LAN connects devices within a small geographical area, like an office, home, or school.

Ex: A library where all computers are connected to a central server to access a shared database or printer.

Key Features:

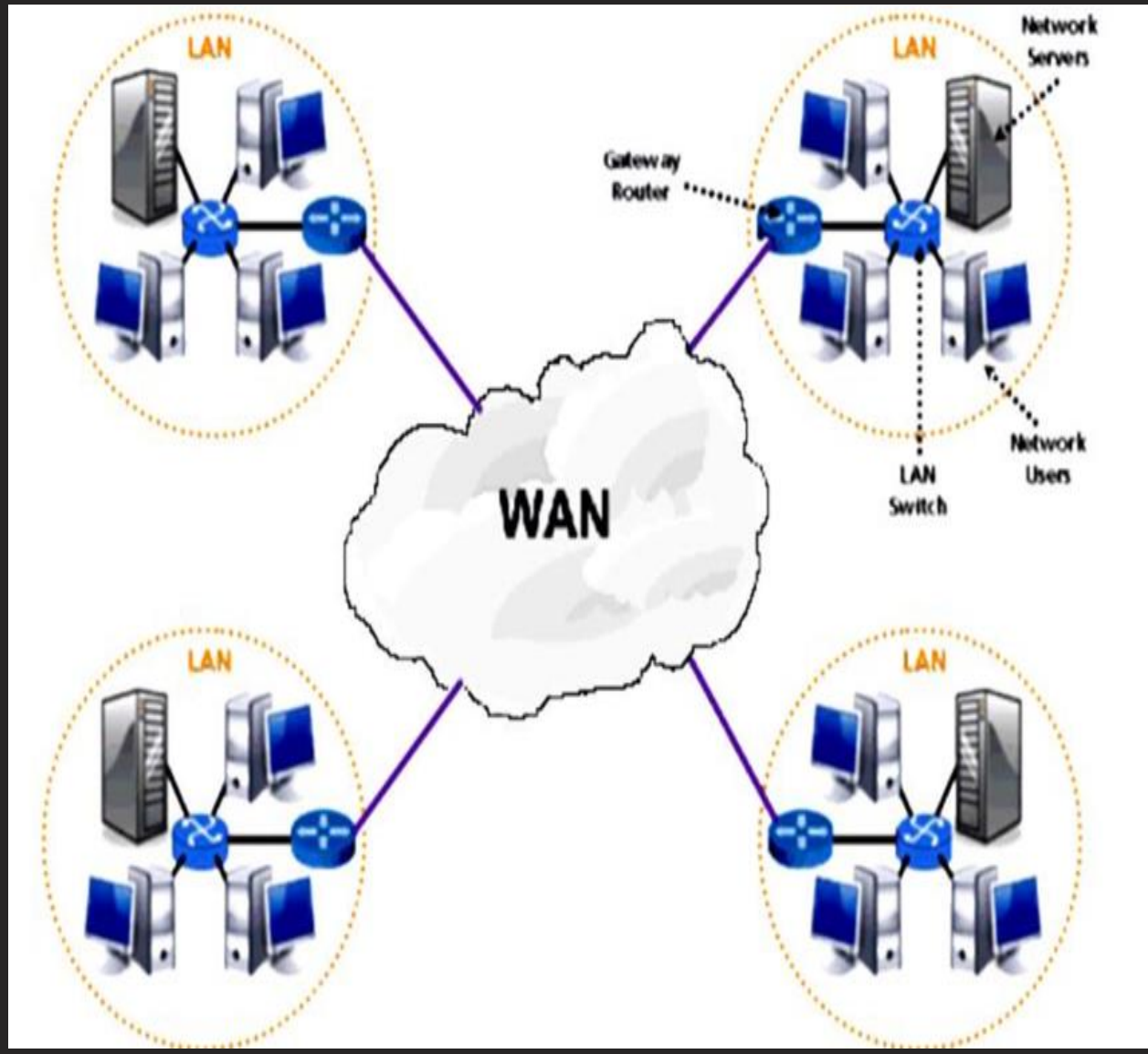
- High speed and low latency.
- Limited to a confined area, providing secure communication.

Types of Networking

WAN (Wide Area Network)

A WAN spans large geographical areas, often connecting multiple LANs. The internet is the largest example of a WAN

Imagine a multinational company with offices in New York, Tokyo, and London. A WAN allows these offices to communicate seamlessly

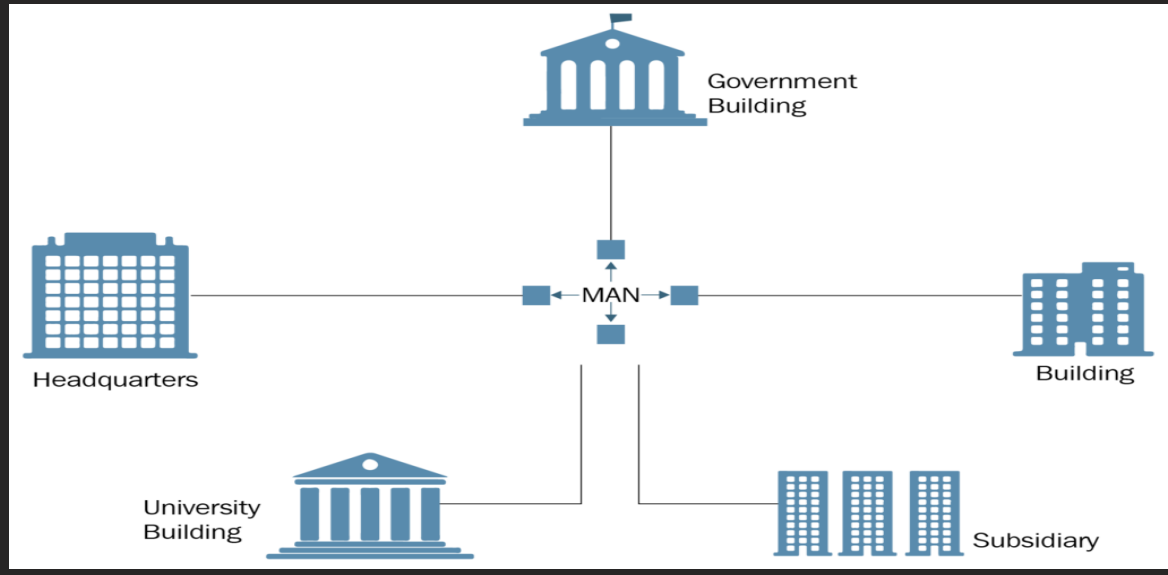


Types of Networking

MAN (Wide Area Network)

A WAN spans large geographical areas, often connecting multiple LANs. The internet is the largest example of a WAN

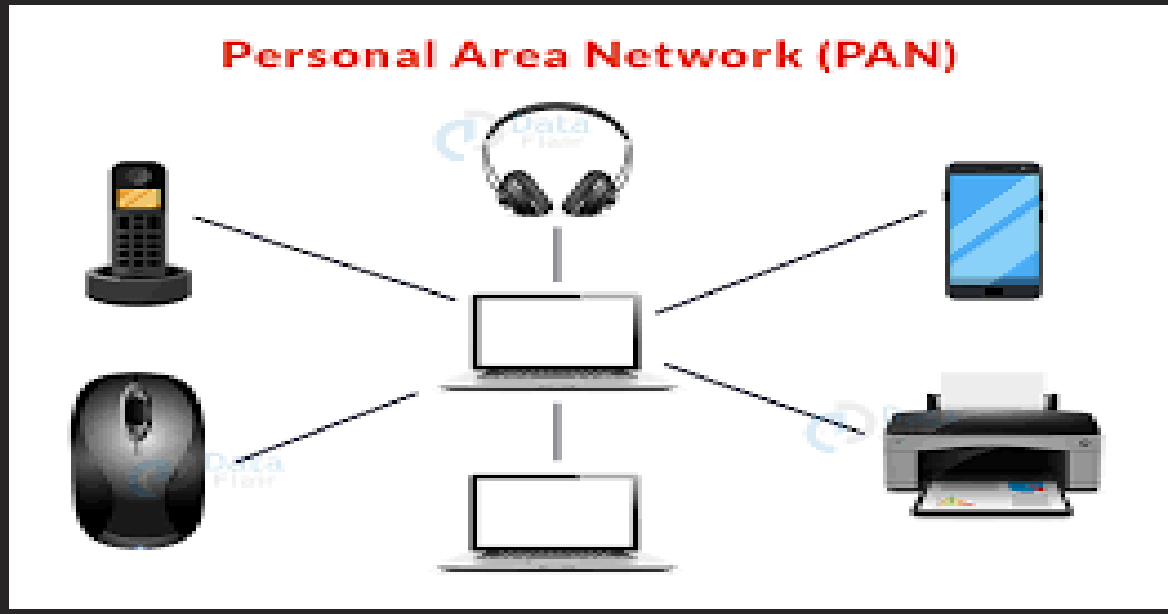
Imagine a multinational company with offices in New York, Tokyo, and London. A WAN allows these offices to communicate seamlessly



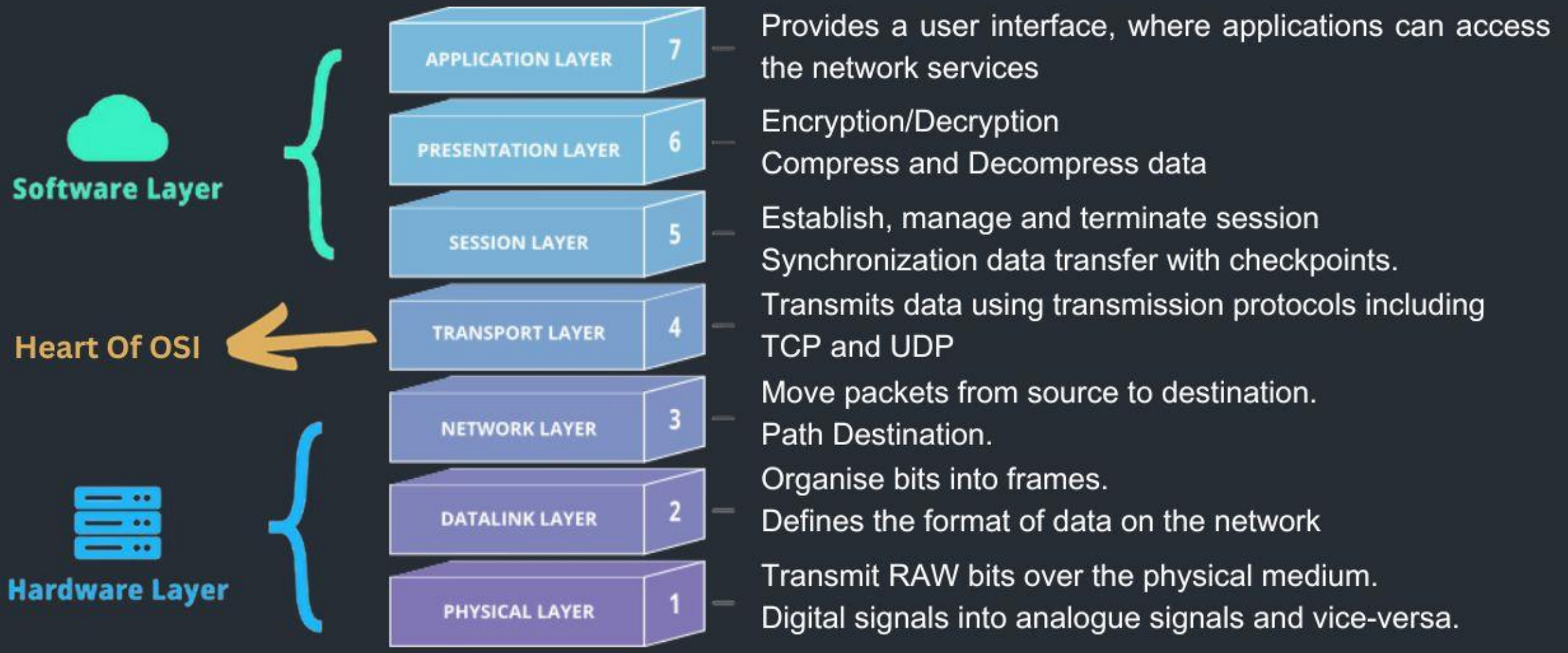
Personal Area Network (PAN

A PAN connects devices within a very short range, typically for a single user.

Your smartphone connected to Bluetooth headphones, a smartwatch, or a personal hotspot



7 Layers of the OSI Model

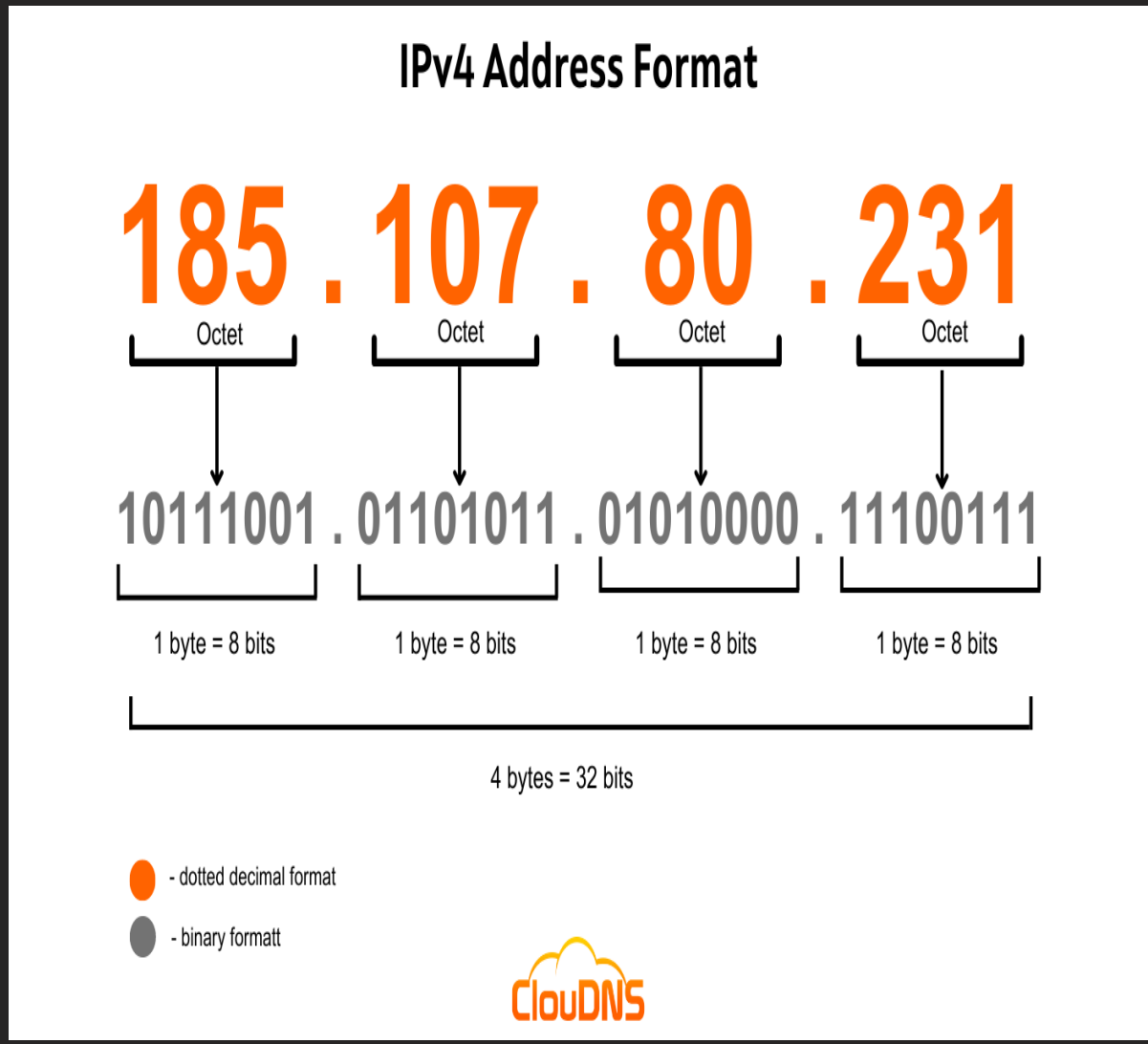


Key Networking terminologies : IP address

- IP address : IP address, or **Internet Protocol address**, is like the home address for your device on a network.
- Every device connected to the internet—whether it's your computer, smartphone, or even your smart fridge—needs a unique IP address to send and receive information

Types of IP Addresses

- **IPV4:** IPv4 stands for **Internet Protocol version 4**, and it's the fourth version of the Internet Protocol.
- It uses a **32-bit** addressing scheme, which means that each IPv4 address consists of 32 binary digits (bits)



Types of IP Addresses

IPV6:

IPv6, or **Internet Protocol version 6**, was introduced in the late 1990s to solve the problem of IPv4 exhaustion and to prepare for the future of internet growth.

IPv6 uses a 128-bit addressing scheme, which is much larger than IPv4.

An IPv6 address looks something like this: 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

IPv6 is 128-bit, it allows for a virtually **unlimited number of IP addresses**—specifically, 2^128 addresses, which equals around **340 undecillion addresses**.

Classes of IP address

Class A:
Range: 1.0.0.0 to 126.255.255.255
Purpose: Designed for **large networks** like big organizations or ISPs (Internet Service Providers

Class B
Range: 128.0.0.0 to 191.255.255.255
Purpose: Used by **medium-sized organizations**. It allows thousands of devices to connect to the network.

Class C
Range: 192.0.0.0 to 223.255.255.255
Purpose: Used by **small businesses or home networks**, supporting fewer devices than Class B.

Class D
Range: 224.0.0.0 to 239.255.255.255
Purpose: Reserved for **multicasting**. This is when a message is sent to multiple devices at once (e.g., live streaming).

Class E
Range: 240.0.0.0 to 255.255.255.255
Purpose: Reserved for **research and experimentation**. It's not used in regular networking.

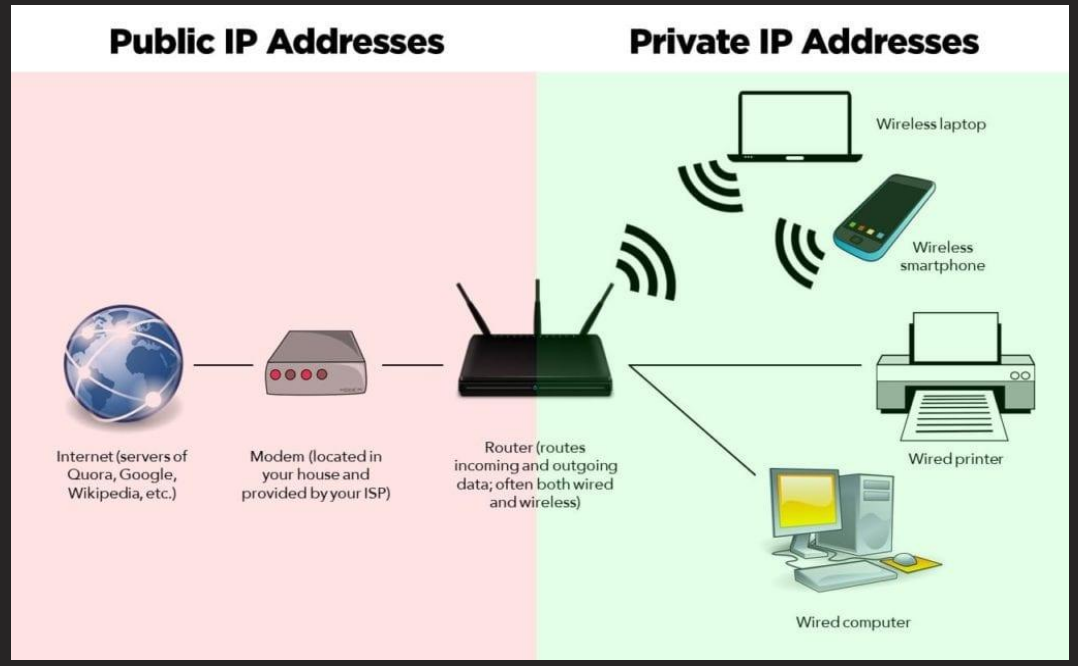
Private IP Address:

A private IP address is an IP address used within a private network (such as a home, office, or corporate LAN).

Example: A computer in your home might have a private IP like **192.168.1.5** that allows it to communicate with your home router but not the internet directly.

Assigned by: Private IP addresses are usually assigned by the local network's router using a system called **DHCP**.

Private IP address space	
From	**To**
10.0.0.0	10.255.255.255
172.16.0.0	172.31.255.255
192.168.0.0	192.168.255.255



Public IP Address:

A public IP address is an IP address that is assigned to a device for direct communication over the Internet.

Example: A web server hosting a website has a public IP address so users across the globe can connect to it.

Assigned by: Internet Service Providers (ISPs) assign public IP addresses to devices connected to

Static IP Address:

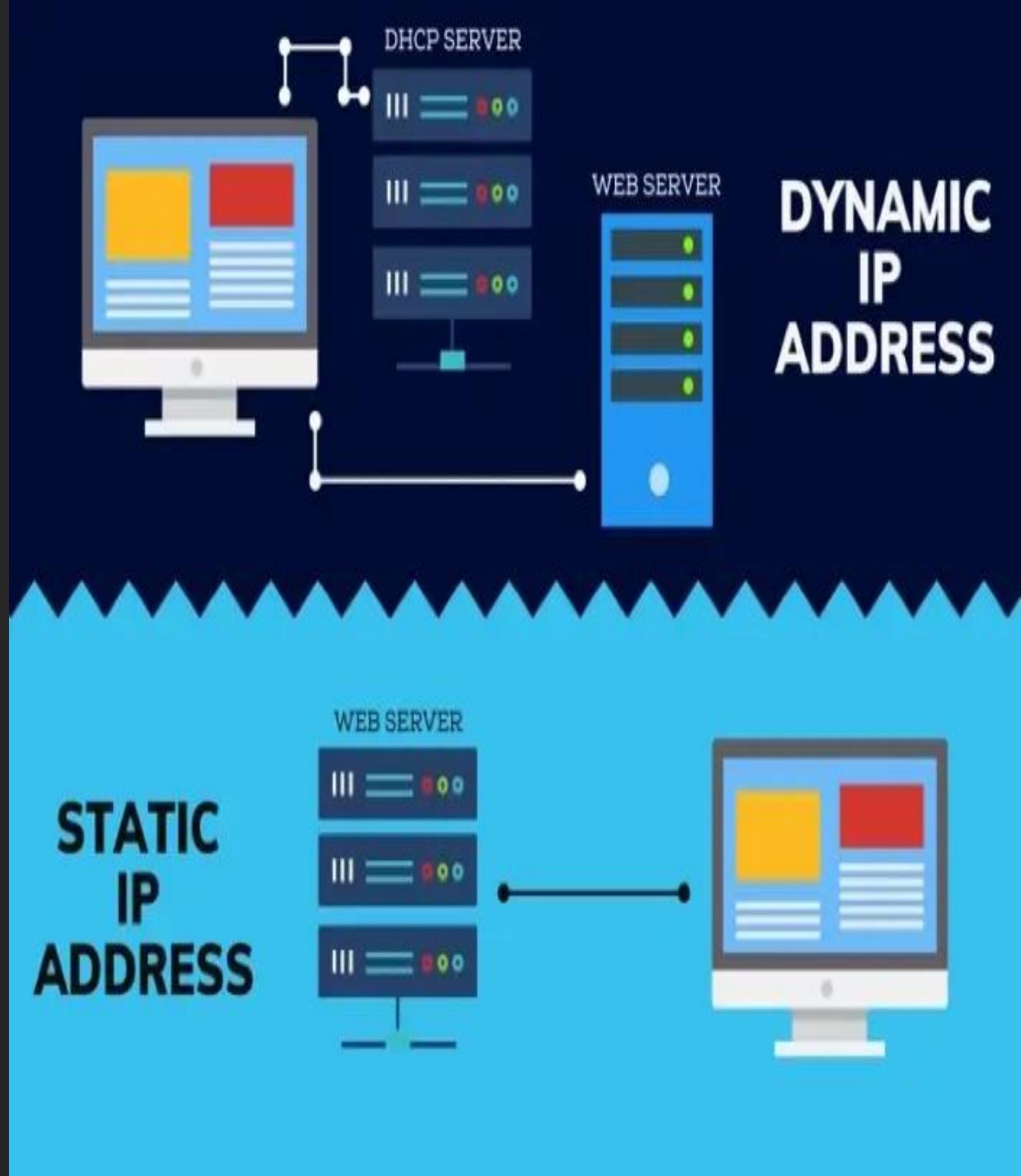
Definition: A static IP address is a permanent IP address assigned to a device. It does not change over time and remains constant unless manually altered by the network administrator.

Servers (like web, email, and database servers)
Network printers
Security cameras

Dynamic IP Address:

A dynamic IP address is assigned by a network when the device connects and may change over time. It is automatically allocated by a system called **DHCP** (Dynamic Host Configuration Protocol).

Personal computers, smartphones, or tablets connected to the Internet

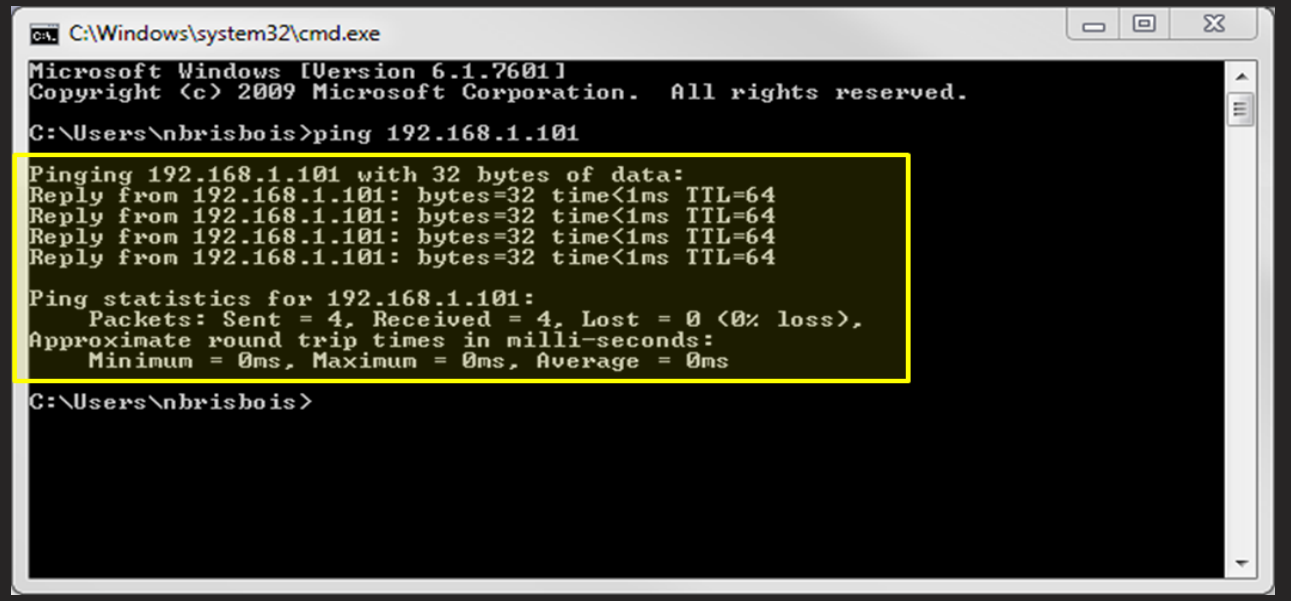


Key Network terminology:

PING:

Ping is a network utility used to test the reachability of a device on a network by sending an ICMP (Internet Control Message Protocol) Echo Request.

Helps troubleshoot network connectivity issues by checking if a device is online or reachable.



PORT:

A port is a logical endpoint in networking used for data exchange between devices. It is used by network protocols to identify specific processes or services.

Well-Known Ports (0-1023): For core services (e.g., HTTP – port 80).

- **Registered Ports (1024-49151)**: For user processes.
- **Dynamic/Private Ports (49152-65535)**: Used by temporary processes.

Key Network terminology:

Packet:

A packet is a unit of data transmitted over a network, containing both the data payload and information about its source, destination, and path.

Structure:

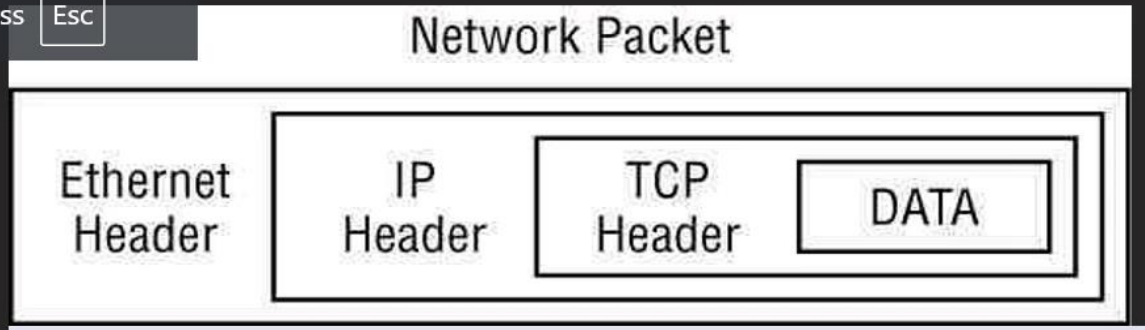
- **Header**: Metadata (IP address, source, destination).
- **Payload**: Actual data being sent.
- **Footer**: Error-checking information (CRC).

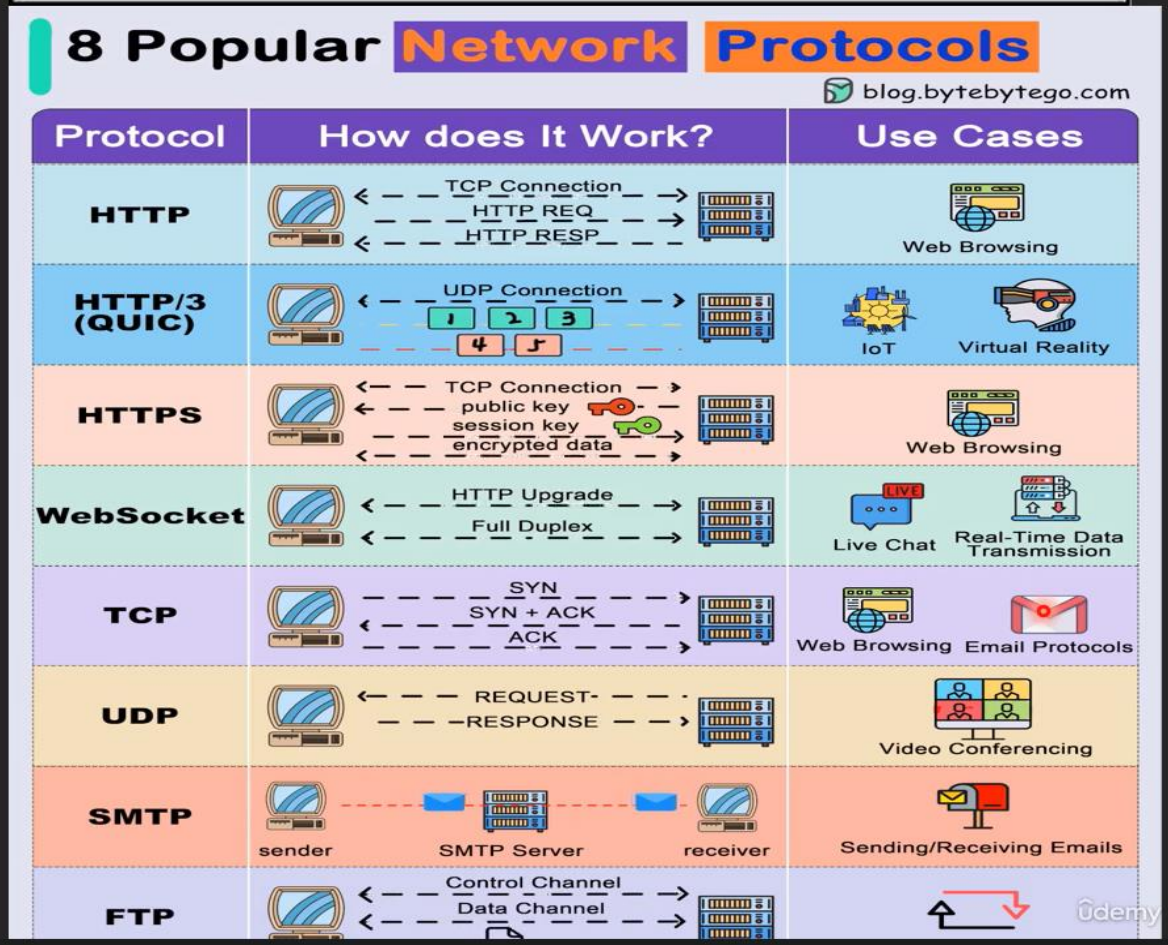
Protocol:

A protocol is a set of rules that govern how data is transmitted and received over a network.

Examples:

TCP (Transmission Control Protocol): Ensures reliable data transfer.
HTTP (Hypertext Transfer Protocol): Used for web communication.





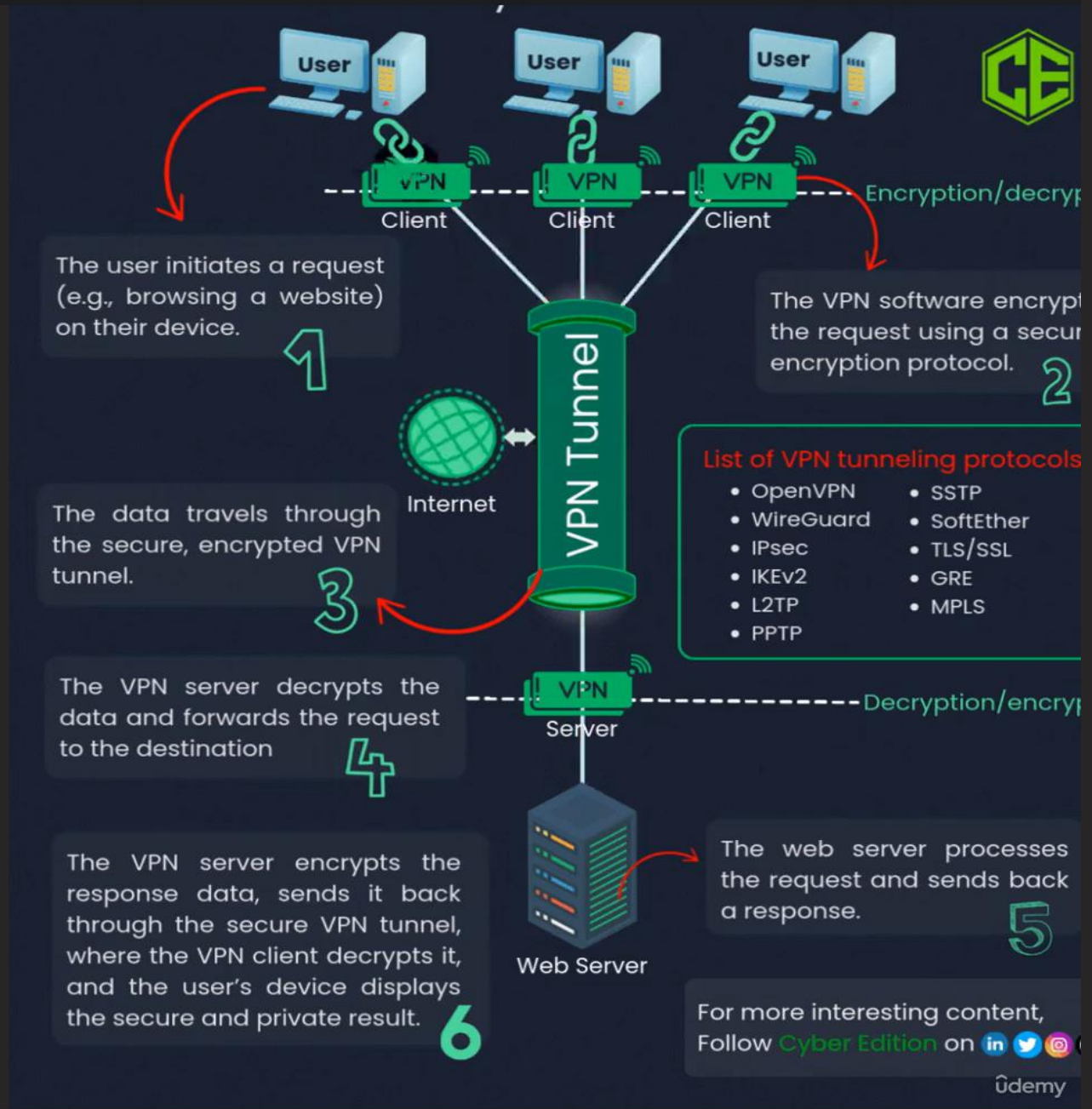
VPN (Virtual Private Network)

A VPN is a secure tunnel that encrypts data between a user and a network over the internet.

How It Works:

- Encrypts traffic and routes it through a secure server.
- Masks the user's IP address and enhances privacy.

Use Case: Used to securely access internal networks or browse the internet anonymously.



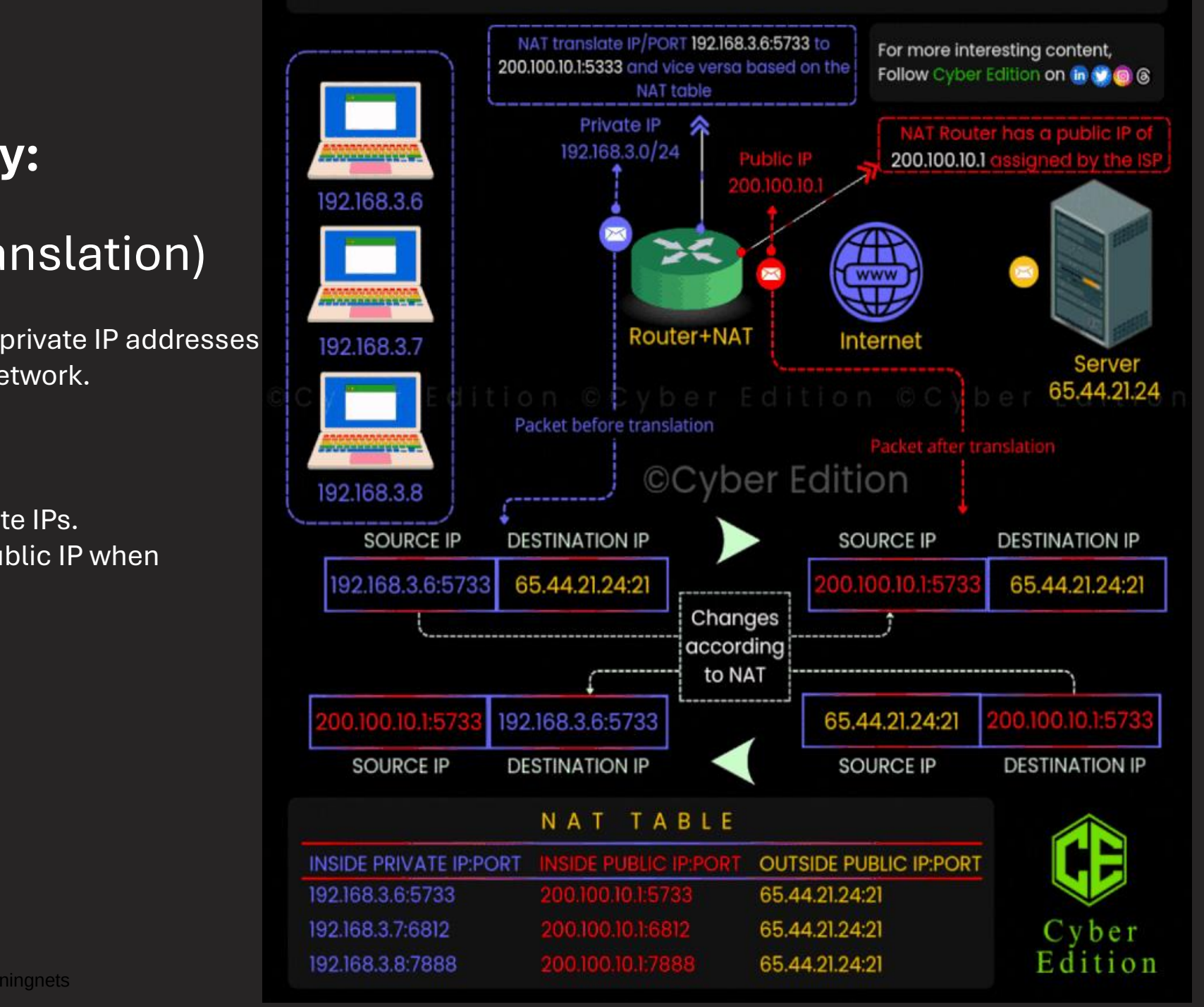
Key Network terminology:

NAT (Network Address Translation)

NAT is a method used by routers to translate private IP addresses to a public IP address for devices in a local network.

How It Works:

Devices in a local network are assigned private IPs.
The router translates these private IPs to a public IP when communicating with the internet.



Bandwidth

•**Definition**: Bandwidth refers to the maximum amount of data that can be transmitted over a network in a given period of time.

•**Measurement**: Typically measured in bits per second (bps), with common units like Mbps (Megabits per second) or Gbps (Gigabits per second).

•**Use Case**: Higher bandwidth allows for faster data transfer, essential for high-performance applications like streaming and gaming.

Latency

•**Definition**: Latency is the time delay between when a data packet is sent and when it is received at the destination.

•**Measurement**: Typically measured in milliseconds (ms).

•**Use Case**: Low latency is important for real-time applications like online gaming, video calls, and VoIP (Voice over IP).