UFV

Networks

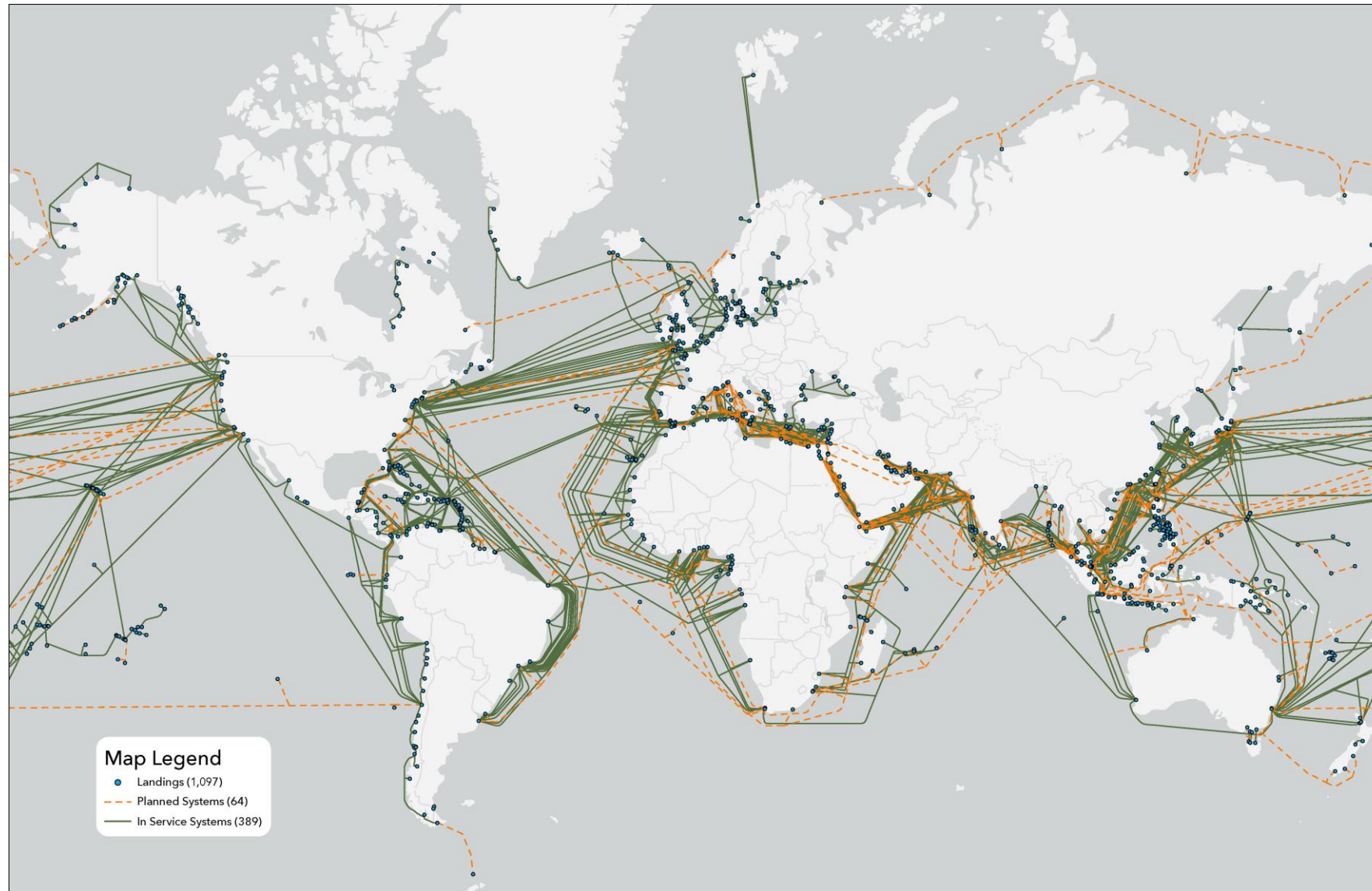## MODULE 2 / UNIT 7 / 0.9

MOISES M. MARTINEZ

FUNDAMENTALS OF COMPUTER ENGINEERING
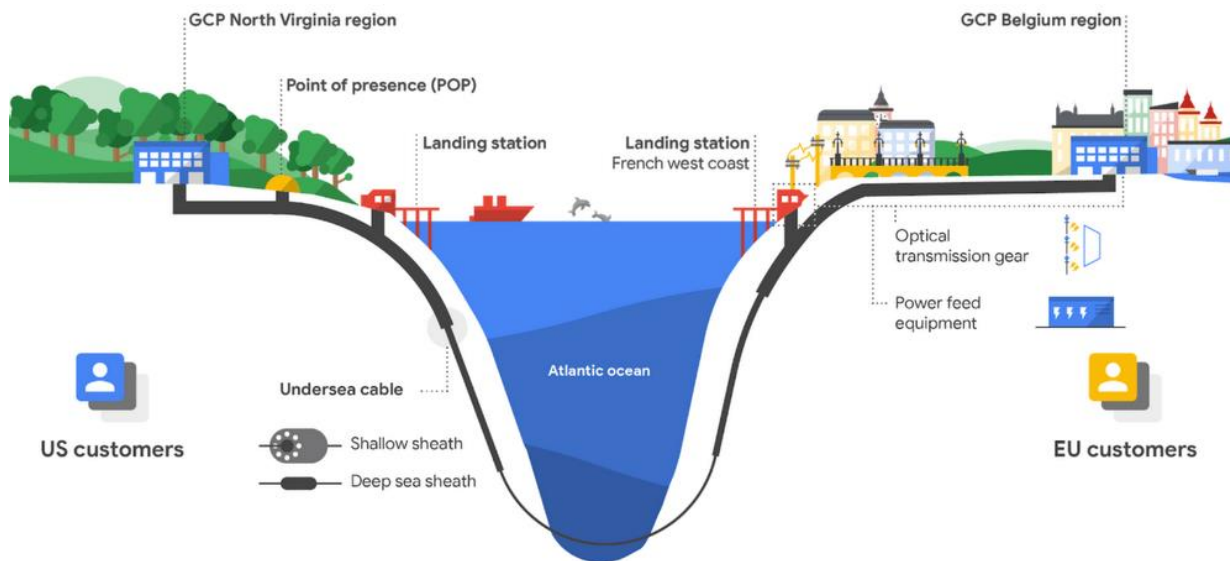
2025/2026

What is a Network?

What is a network?

Map Legend
- Landings (1,097)
- Planned Systems (64)
- In Service Systems (389)
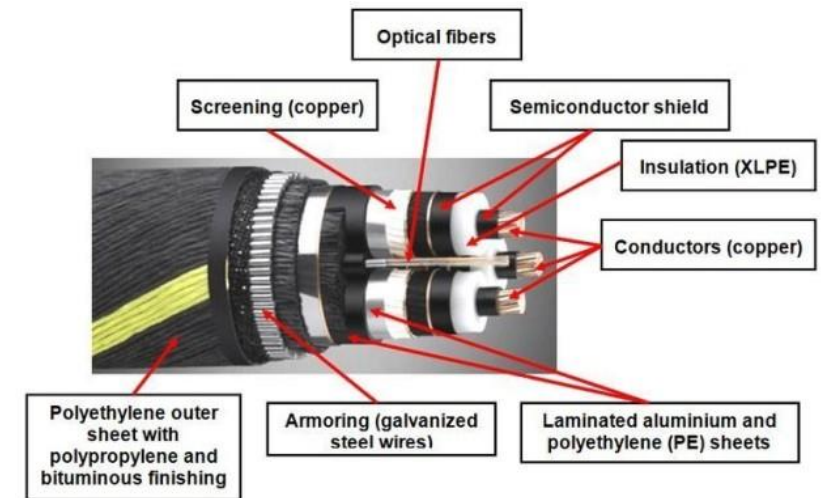
A telecommunications submarine cable is an undersea fibber-optic cable used to transmit data signals across bodies of water, typically oceans or seas. These cables are laid along the seabed and are essential for global communications, serving as the backbone of the internet by connecting continents and countries.

Google Cloud submarine cable infrastructure
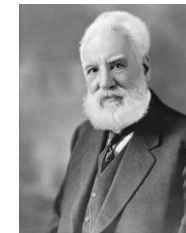
Structure of a Submarine Cable

The path to Internet

01

HIGHER POLYTECHNIC SCHOOL

A network refers to the combination of two or more devices and the interconnecting links facilitating the transmission of information among them.

- Telegraph (Samuel Morse, 1832 - 1844): Message communication network.

- Telephone (Alexander Graham Bell, 1876): telephone (voice) communication network.

- Radio (Guglielmo Marconi, 1896): Wireless communication network.

UFV

Voice and data communications were traditionally based on circuit-switching techniques, as exemplified by the conventional telephone network, where each call was assigned a dedicated end-to-end electronic connection between the two communicating parties.

The initial version of the Internet, known as **ARPANET**, was established in 1969 and connected four universities:

- UCLA.

- Stanford (UCSB).

- University of California-Santa Barbara (SRI).
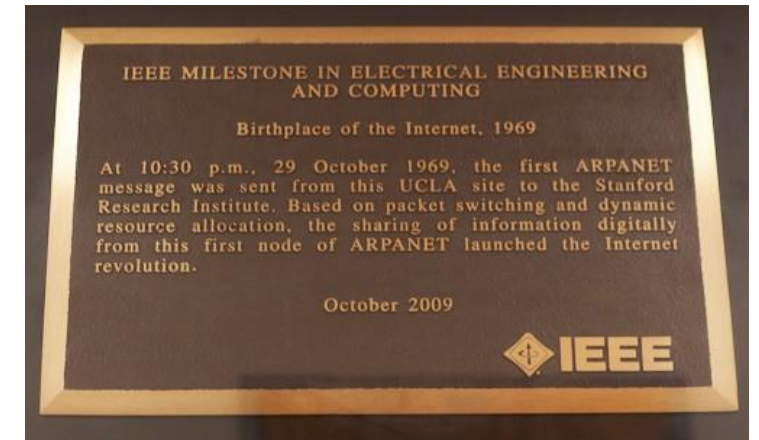
- University of Utah.

The ARPANET in December 1969

Voice and data communications were traditionally based on circuit-switching techniques, as exemplified by the conventional telephone network, where each call was assigned a dedicated end-to-end electronic connection between the two communicating parties.
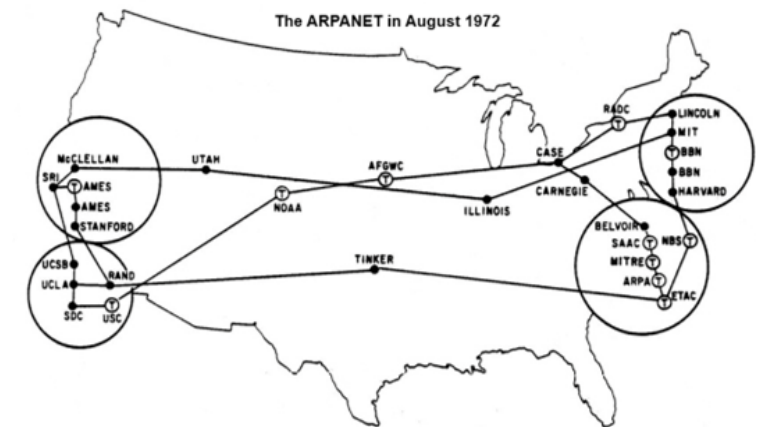
The inaugural network, ARPANET, connected UCLA, Stanford, the University of California-Santa Barbara, and the University of Utah.

This network made history by sending its first message, "LO", which was an initial attempt to transmit the word **LOGIN**.

IEEE MILESTONE IN ELECTRICAL ENGINEERING AND COMPUTING

Birthplace of the Internet, 1969

At 10:30 p.m., 29 October 1969, the first ARPANET message was sent from this UCLA site to the Stanford Research Institute. Based on packet switching and dynamic resource allocation, the sharing of information digitally from this first node of ARPANET launched the Internet revolution.
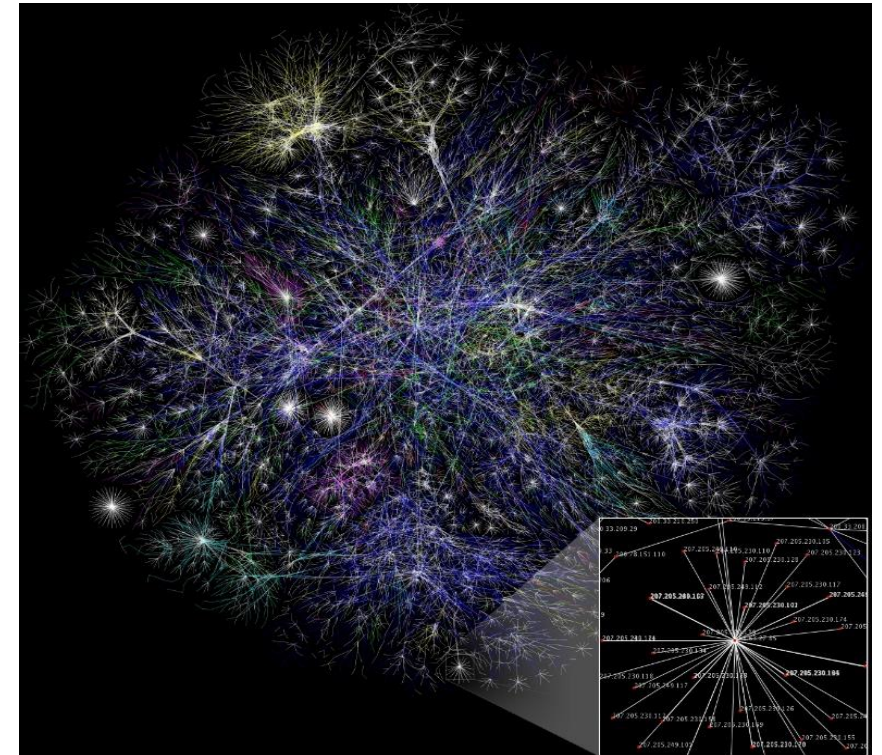
October 2009

IEEE

ARPANET was introduced to the public during the First International Conference on Computers and Communication in Washington, D.C., in 1972. At this event, ARPANET showcased a network consisting of 40 interconnected nodes spread across various geographical regions in the United State.

- Telenet (1974): Commercial version of ARPANET.
- Usenet (1979): Open system focused on e-mail and still works.
- Bitnet (1981): Linked American universities using IBM systems.
- Eunet (1982): It united the United Kingdom, Scandinavia and the Netherlands.

The ARPANET in August 1972

The path to Internet

The Internet, established in 1990, is a decentralized network of interconnected systems that operate on the TCP/IP protocol suite. This model enables diverse physical networks to function together as a single, cohesive logical network with global reach, ensuring seamless communication and data exchange across the world.

- Rapid Expansion of Client/Server Applications.

- Proliferation of Web-Based Services and Applications.

- Emergence of New Service Types Requiring Distributed Systems like e-commerce, streaming, and cloud computing.

UFV

The World Wide Web (WWW), commonly known as the Web, is an information system that allows users to access and navigate interconnected hypertext documents and various web resources via the Internet.

- Web 1.0 was the "read-only web".
- Web 2.0 was the "read-write". We can create content and interact with other web users in real time.
- Web 3.0 is the "read-write-execute". It is called the semantic web.

World Wide Web

The WorldWideWeb (W3) is a wide-area hypermedia information retrieval initiative aiming to give universal access to a large universe of documents.

Everything there is online about W3 is linked directly or indirectly to this document, including an executive summary of the project, Mailing lists , Policy , November's W3 news , Frequently Asked Questions .

What's out there?
 Pointers to the world's online information, subjects , W3 servers, etc.
Help
 on the browser you are using
Software Products
 A list of W3 project components and their current state. (e.g. Line Mode ,X11 Viola , NeXTStep , Servers , Tools , Mail robot , Library)
Technical
 Details of protocols, formats, program internals etc
Bibliography
 Paper documentation on W3 and references.
People
 A list of some people involved in the project.
History
 A summary of the history of the project.
How can I help ?
 If you would like to support the web..
Getting code
 Getting the code by anonymous FTP , etc.

Copy of the original page taken in 1992: info.cern.ch

The World Wide Web was devised by Tim Berners-Lee, a British computer scientist, while he was working at CERN. **It was initially conceived as a system for managing and sharing documents within the organization, providing a way to easily access and interlink research information.**

What is the volume of data generated by the world every minute?
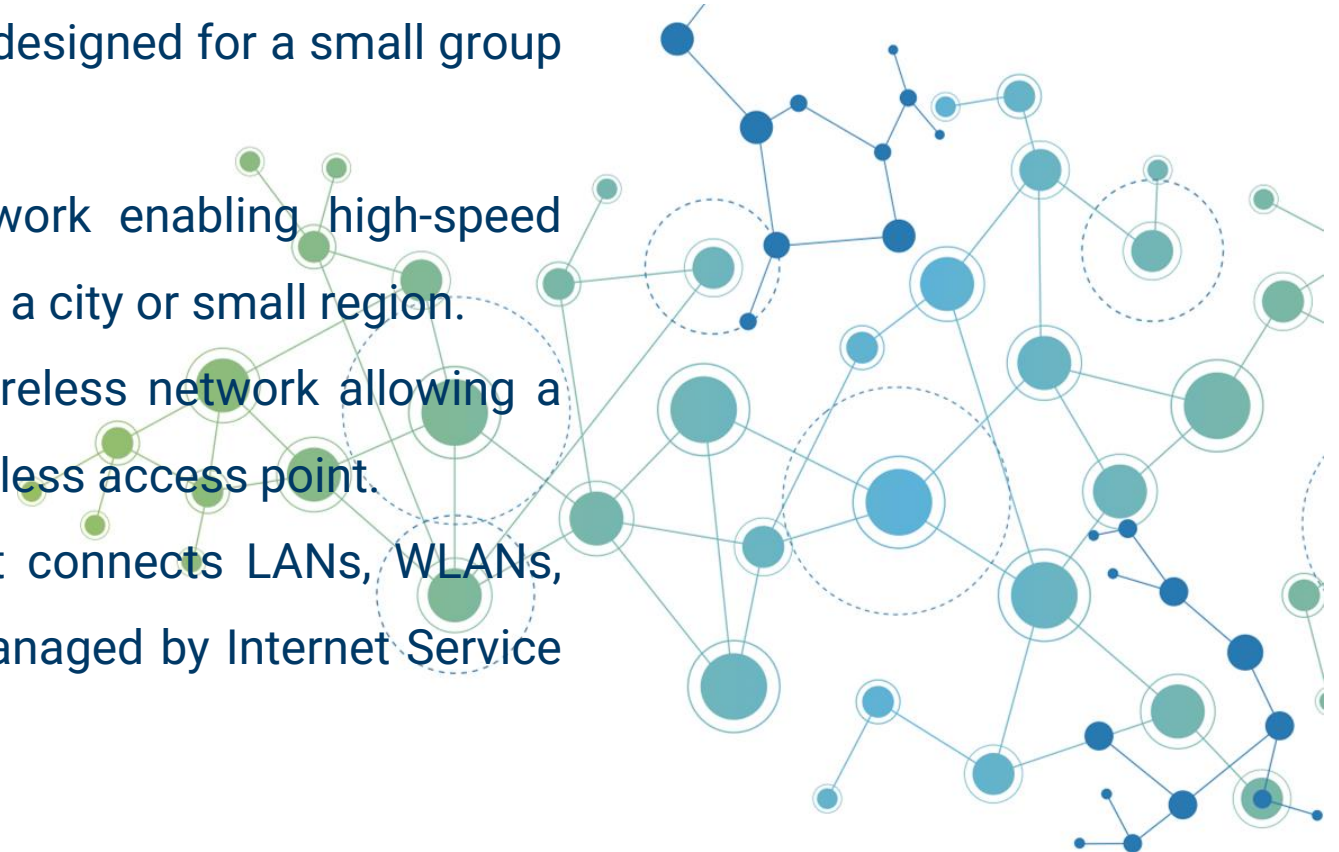

2021

2022

2023

Created by: eDiscovery Today & LTMG

Networks

02

HIGHER POLYTECHNIC SCHOOL
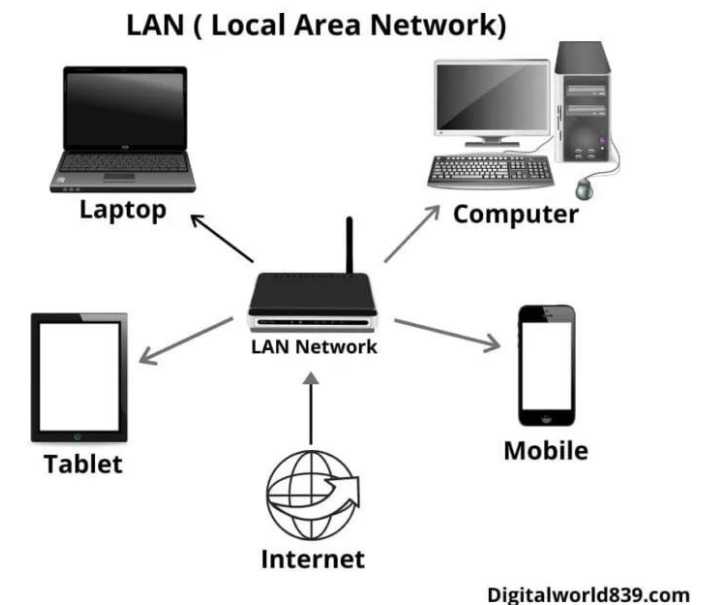
Fundamentals of Computer Engineering

UFV

A computer network **is a group of interconnected computers that enables communication between devices**, allowing them to share resources, data, and applications seamlessly.

- LAN (Local Area Network): A wired network designed for a small group of computers within a localized area.

- MAN (Metropolitan Area Network): A network enabling high-speed connections between LANs or WLANs within a city or small region.

- WLAN (Wireless Local Area Network): A wireless network allowing a small group of systems to connect via a wireless access point.

- WAN (Wide Area Network): A network that connects LANs, WLANs, and MANs over large distances, typically managed by Internet Service Providers (ISPs).

A LAN (Local Area Network) network is a wired network designed for a small group of computers within a localized area.

- Coverage Area: It is typically employed to interconnect multiple personal computers within a limited geographic area, usually spanning 10 to 1500 meters.
- Transmission Medium: LANs utilize various mediums such as twisted pair cables, coaxial cables, and others for data transmission.
- Cost-Effectiveness: LANs are cost-effective, using economical hardware components like hubs, network adapters, and Ethernet cables.
- Data Transmission Speed: Data transmission within LANs occurs at significantly higher speeds compared to other network types.
- Security: LANs offer enhanced security measures, providing better protection compared to other network configurations.

LAN (Local Area Network)
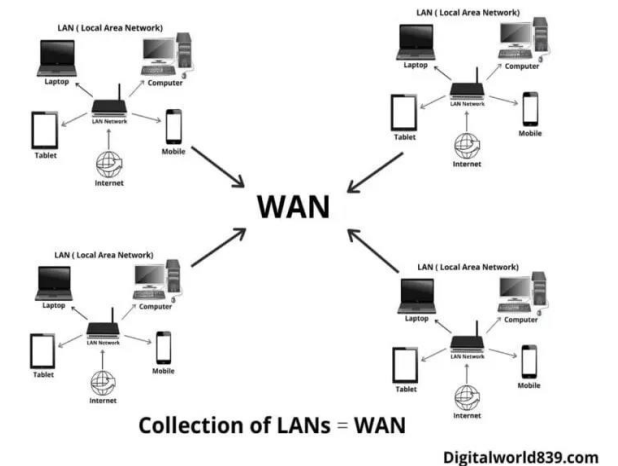Laptop — Computer — Tablet — LAN Network — Mobile — Internet
Digitalworld839.com

WLAN extends the LAN network by utilizing wireless technologies like WiFi and Bluetooth to enable connectivity without the need for physical cables.

A MAN (Metropolitan Area Network) network enables high-speed connections between LANs or WLANs within a city or small region.
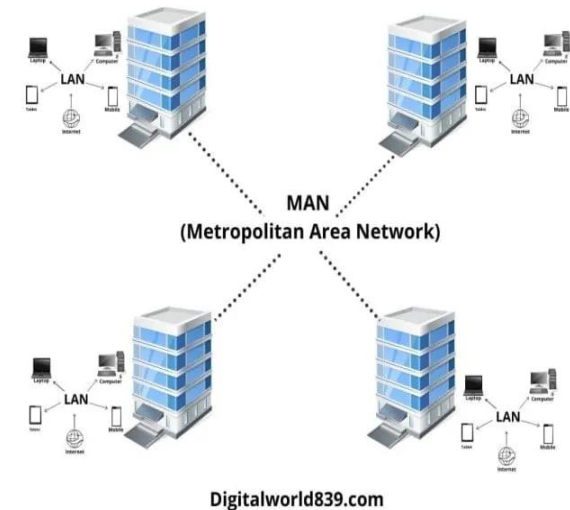
- Coverage Area: It typically spans a city or a large campus, covering distances that exceed the range of a Local Area Network (LAN).
- Transmission Medium: MANs use a variety of transmission mediums, including fibber-optic cables and wireless connections, to achieve high-speed communication over relatively large distances.
- Cost-Effectiveness: MANs involve moderate costs due to the need for more extensive infrastructure and sophisticated networking equipment.
- Data Transmission Speed: MANs provide high data transmission speeds, sufficient for handling the communication needs of a city-wide network.
- Security: MANs offer robust security features, though they may require more complex security management due to the broader area and the potential for diverse users compared to LANs.
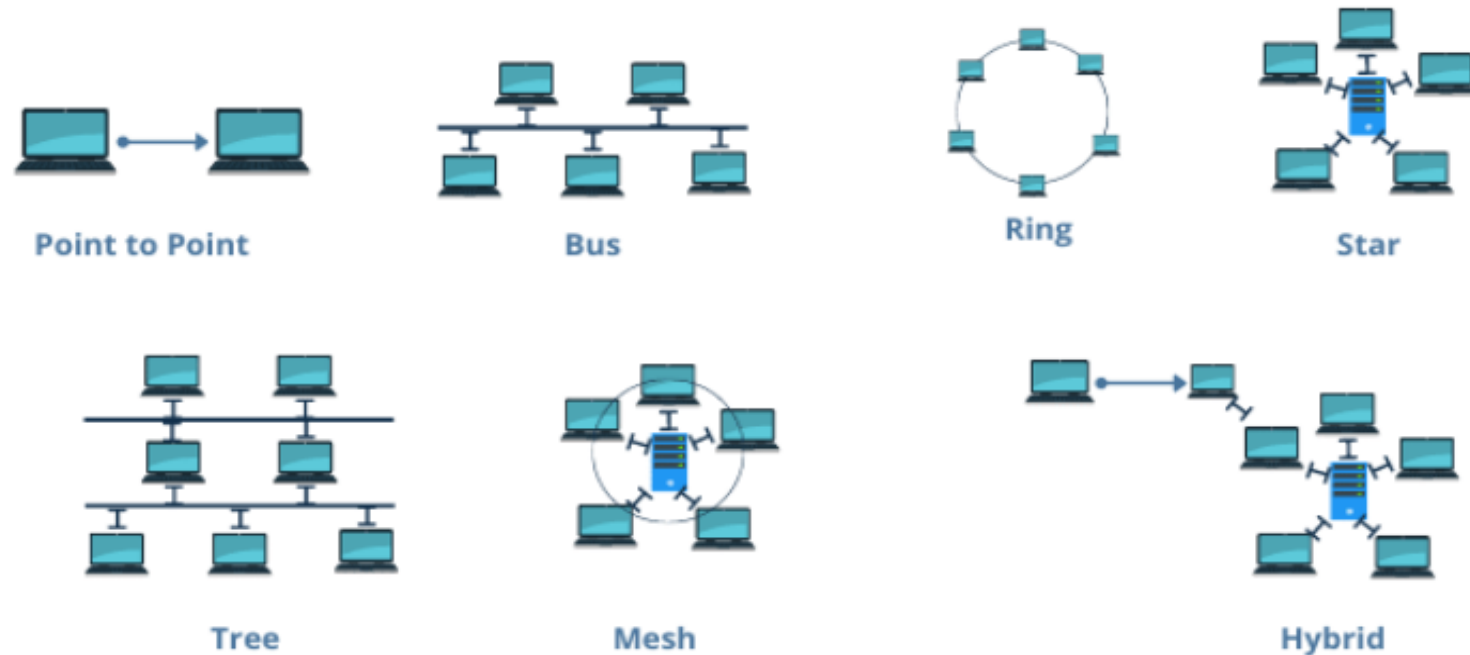
A WAN (Wide Area Network) is a big network that connects LANs, WLANs, and MANs over large distances, typically managed by Internet Service Providers (ISPs).

- Coverage Area: It covers extensive geographic regions, ranging from large cities and countries to global connections, interconnecting networks across vast distances.

- Transmission Medium: WANs utilize a variety of transmission mediums, including fiber optic cables, satellite links, and undersea cables, to facilitate communication across large distances.

- Cost-Effectiveness: WANs involve significant costs, often higher than LANs and MANs, due to the extensive infrastructure, advanced networking equipment, and service fees from Internet Service Providers (ISPs).

- Data Transmission Speed: WANs support long-distance communication; data transmission speeds can vary based on the medium used and the distance involved.

- Security: WANs require advanced security measures due to the complexity and scope of the network, with a focus on protecting data as it travels across public and private infrastructure.

MAN
(Metropolitan Area Network)

Digitalworld839.com

Network topology refers to the schematic layout of a network's structural configuration. A network can have a single physical topology while simultaneously supporting multiple logical topologies, reflecting different patterns of data flow and connectivity.

- Point to point.
- Bus.
- Ring.
- Star.
- Mesh.
- Tree.
- Hybrid.

Point to Point

Bus

Ring

Star

Tree

Mesh

Hybrid

Network models

03

HIGHER POLYTECHNIC SCHOOL

The execution of tasks related to information communication within networks is organized into **a layered structure**, where each layer is responsible for **specific functions and operates according to the protocols** defined by the layer directly below it. This hierarchical approach ensures that complex network operations are handled efficiently and systematically.

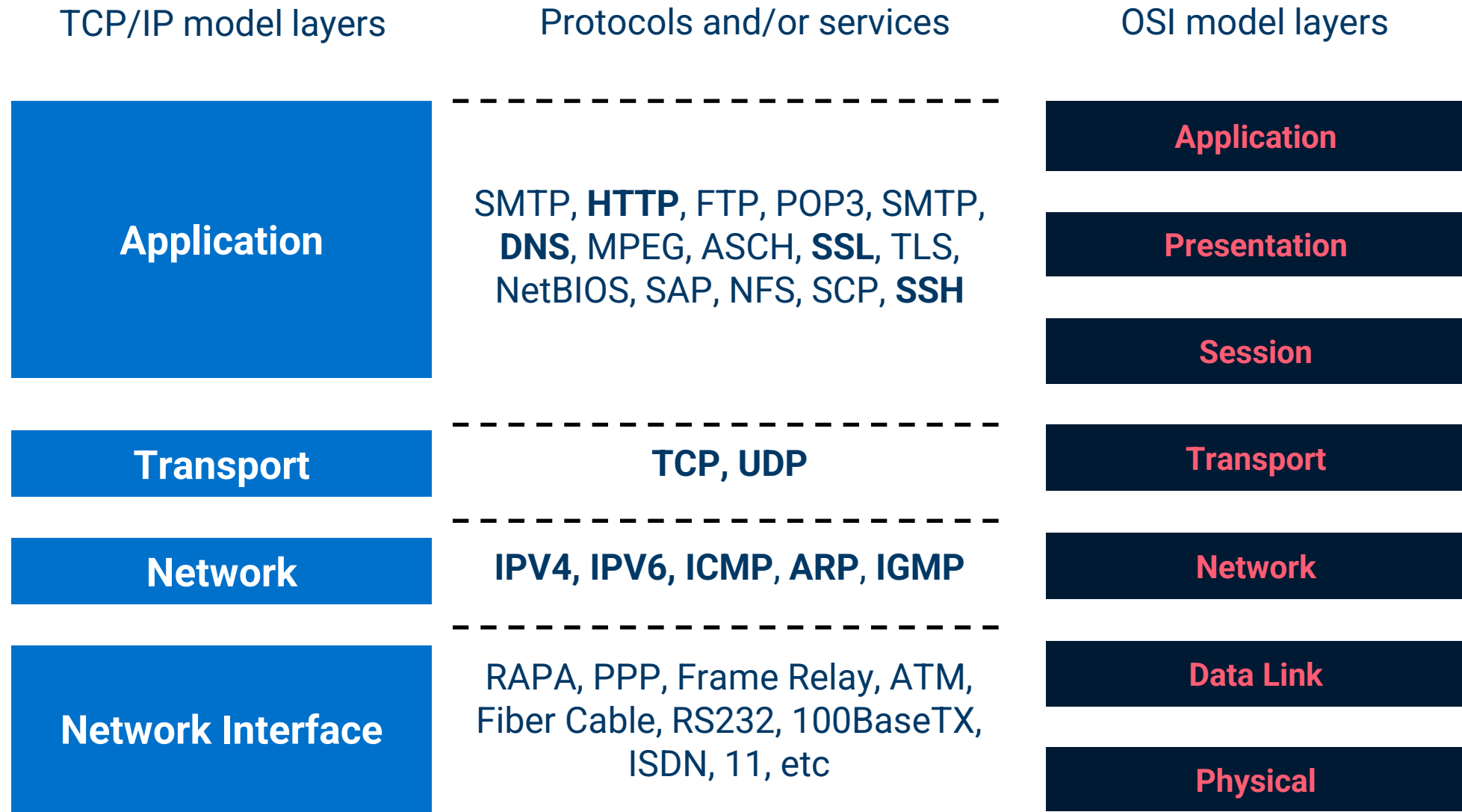There are two primary models for this layered structure:

- OSI (Open Systems Interconnection) Model: A conceptual framework that standardizes the functions of a telecommunication or computing system into seven different layers.

- TCP/IP Model: A more practical framework that simplifies the layered approach into four layers, specifically designed for the Internet and related networks.

Network models

The Open System Interconnection (OSI) model is a conceptual framework developed by the International Organization for Standardization (ISO). It provides a standardized foundation for the coordination and development of networking protocols and standards, with the primary goal of enabling seamless interconnection and communication between diverse systems.

	Layer	Name	Protocols
Application	Layer 7	Application	SMTP, **HTTP**, FTP, POP3, **DNS**, **SSH**
Presentation	Layer 6	Presentation	MPEG, ASCH, **SSL**, TLS
Session	Layer 5	Session	NetBIOS, SAP, NFS, SCP
Transport	Layer 4	Transport	**TCP, UDP**
Network	Layer 3	Network	**IPV4, IPV6, ICMP**, IPSEC, **ARP**, MPLS, **IGMP**
Data Link	Layer 2	Data Link	RAPA, PPP, Frame Relay, ATM, Fiber Cable, etc
Physical	Layer 1	Physical	RS232, 100BaseTX, ISDN, 11

The Internet Protocol framework, commonly known as TCP/IP model, is the set of communication protocols used for the Internet and similar computer networks. It functions as **the de facto standard framework** for all networked applications, enabling reliable data transmission and communication across diverse systems and platforms.

Layer	Name	Protocols
Layer 4	Application	SMTP, **HTTP**, FTP, POP3, SMTP, **DNS**, MPEG, ASCH, **SSL**, TLS, NetBIOS, SAP, NFS, SCP, **SSH**
Layer 3	Transport	**TCP, UDP**
Layer 2	Network	**IPV4, IPV6, ICMP**, IPSEC, **ARP**, MPLS, **IGMP**
Layer 1	Interface	RAPA, PPP, Frame Relay, ATM, Fiber Cable, RS232, 100BaseTX, ISDN, 11, etc

Application

Transport

Network

Network Interface

Network models

TCP/IP model layers	Protocols and/or services	OSI model layers
Application	SMTP, **HTTP**, FTP, POP3, SMTP, **DNS**, MPEG, ASCH, **SSL**, TLS, NetBIOS, SAP, NFS, SCP, **SSH**	**Application**
		Presentation
		Session
Transport	**TCP, UDP**	**Transport**
Network	**IPV4, IPV6, ICMP, ARP, IGMP**	**Network**
Network Interface	RAPA, PPP, Frame Relay, ATM, Fiber Cable, RS232, 100BaseTX, ISDN, 11, etc	**Data Link**
		Physical

Network hardware

04

HIGHER POLYTECHNIC SCHOOL
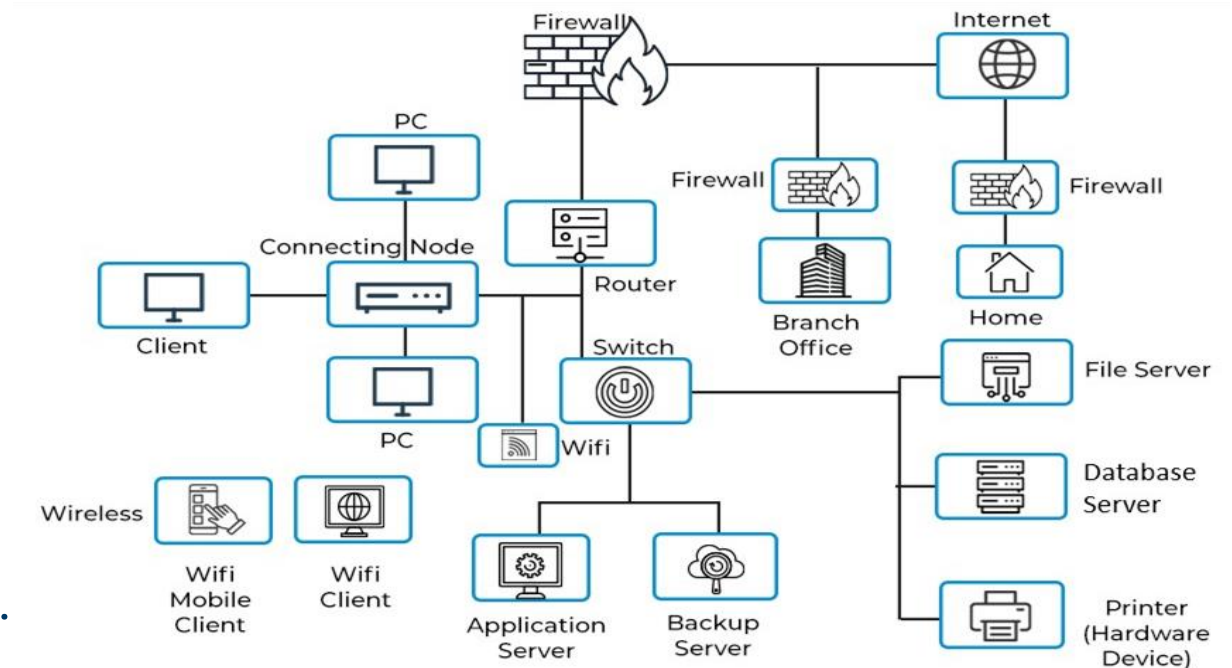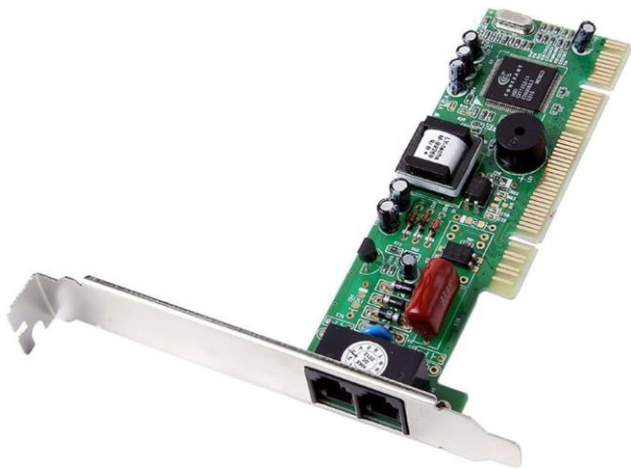
Network hardware includes a range of physical devices that are crucial for enabling interaction and communication between computers within a network. These devices are integral to managing data transmission, connectivity, and the overall operation of the network.

- Modems.

- Hubs, bridges, and switches.

- Routers.

- Network interface cards.

- Network cables.

- Firewalls (excluding software-based ones).

Modems

A modulator-demodulator, commonly known as a modem, is a network hardware device that enables a computer to connect to the internet via a telephone line.

The modem converts the digital signals produced by the computer into analogy signals, which are then transmitted over the telephone line to establish the connection.

Hubs, bridges, and switches

Hubs, bridges, and switches are network hardware devices that facilitate the connection of multiple devices within a network and manage the transmission of data across these devices. These devices work alongside a router to ensure that data is efficiently distributed to all devices in the network, enabling seamless communication, resource sharing, and internet access.

- A hub broadcasts data to all devices within a network.
- A bridge connects two separate LAN networks, allowing them to communicate as a single network.
- A switch, offering greater efficiency and functionality than a hub or bridge, manages data traffic by directing it specifically to the intended devices within the network.

network switch
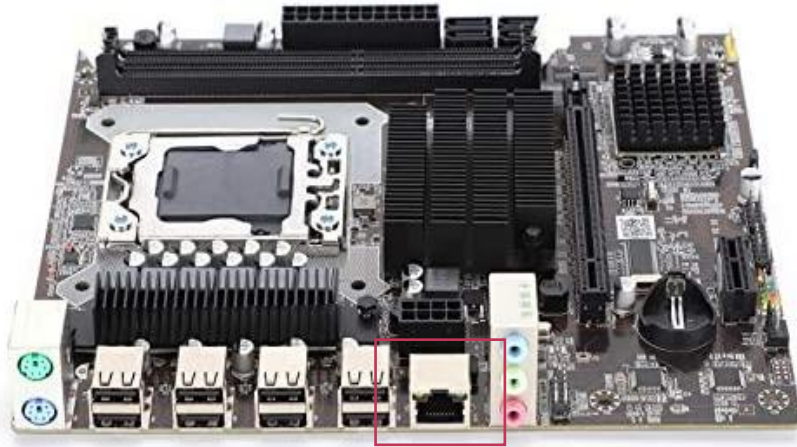
network hub

Routers

A router is a network hardware device that acts as an interface between two or more networks. A common use of a router is to connect a local area network (LAN) in a home or office to the wider internet (WAN), facilitating communication and data exchange between these networks.

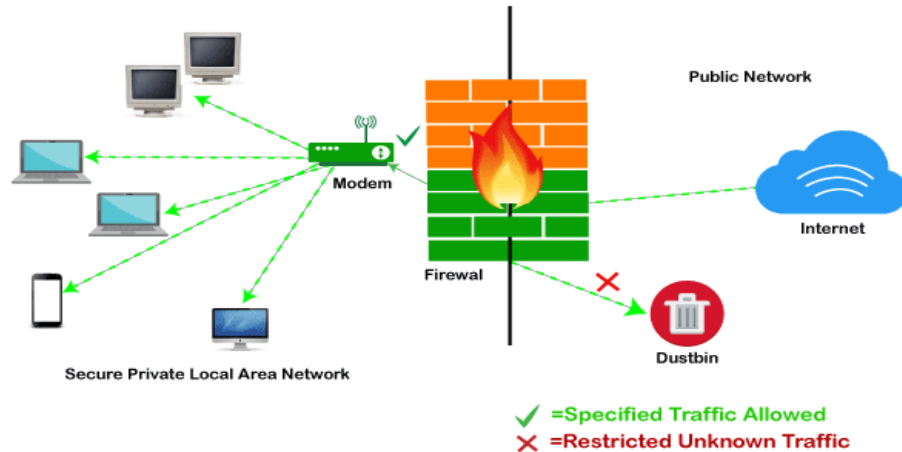**HIGHER POLYTECHNIC SCHOOL**

Network Interface Card

A Network Interface Card (NIC) is a hardware component installed in a computer that allows it to connect to and communicate with a network.

• Network interface cards (NICs) are often integrated directly into the motherboard.

• NICs can be added externally by installing an additional expansion card, which is a small circuit board that provides network connectivity.

Firewalls

A firewall is a hardware device that acts as a barrier between a computer and the broader network, protecting it from potential attacks or intrusion attempts by hackers.

LAN networks can improve their security against hackers by placing a hardware firewall between the LAN and the internet connection. This firewall acts as a protective barrier, monitoring and controlling incoming and outgoing network traffic to prevent unauthorized access.
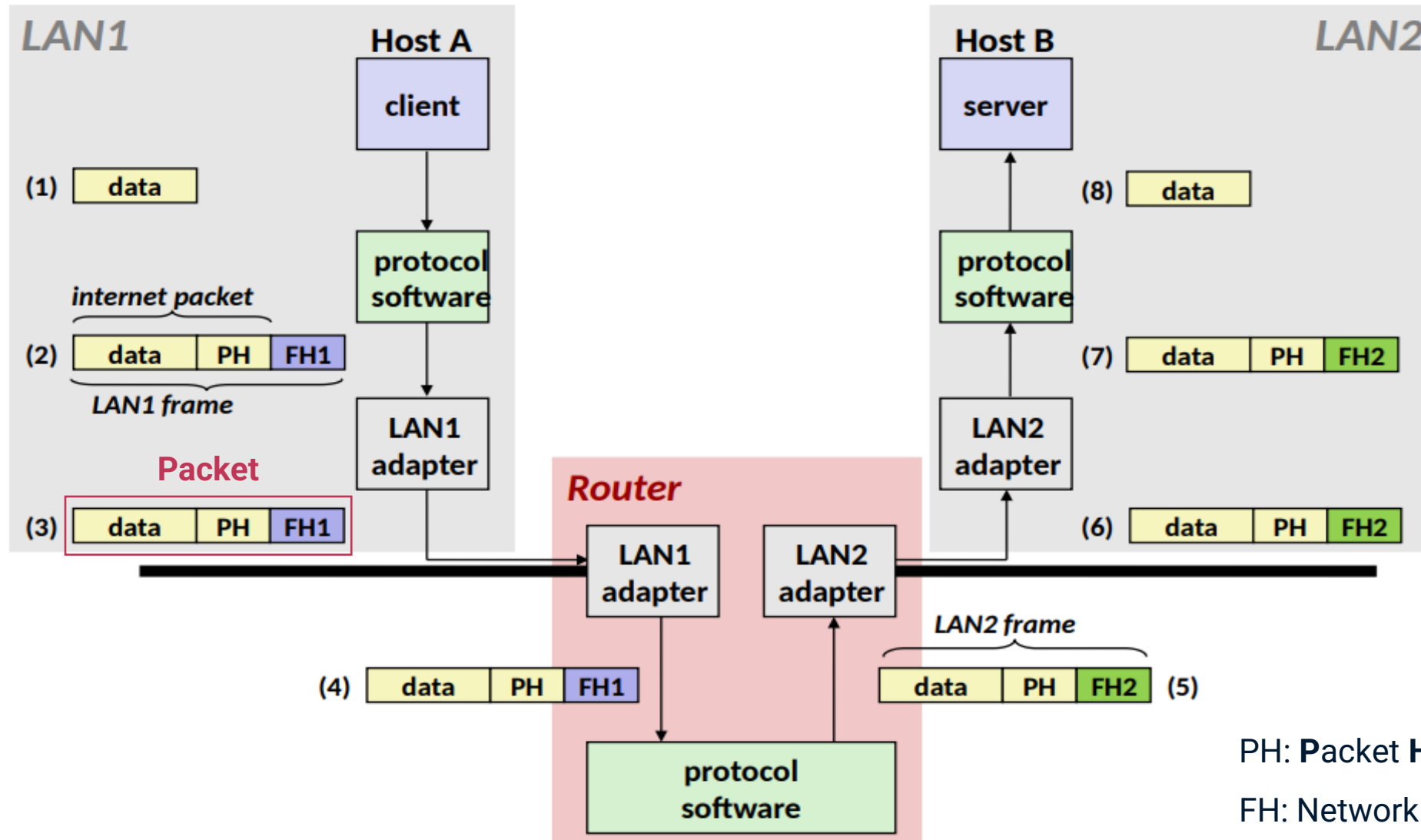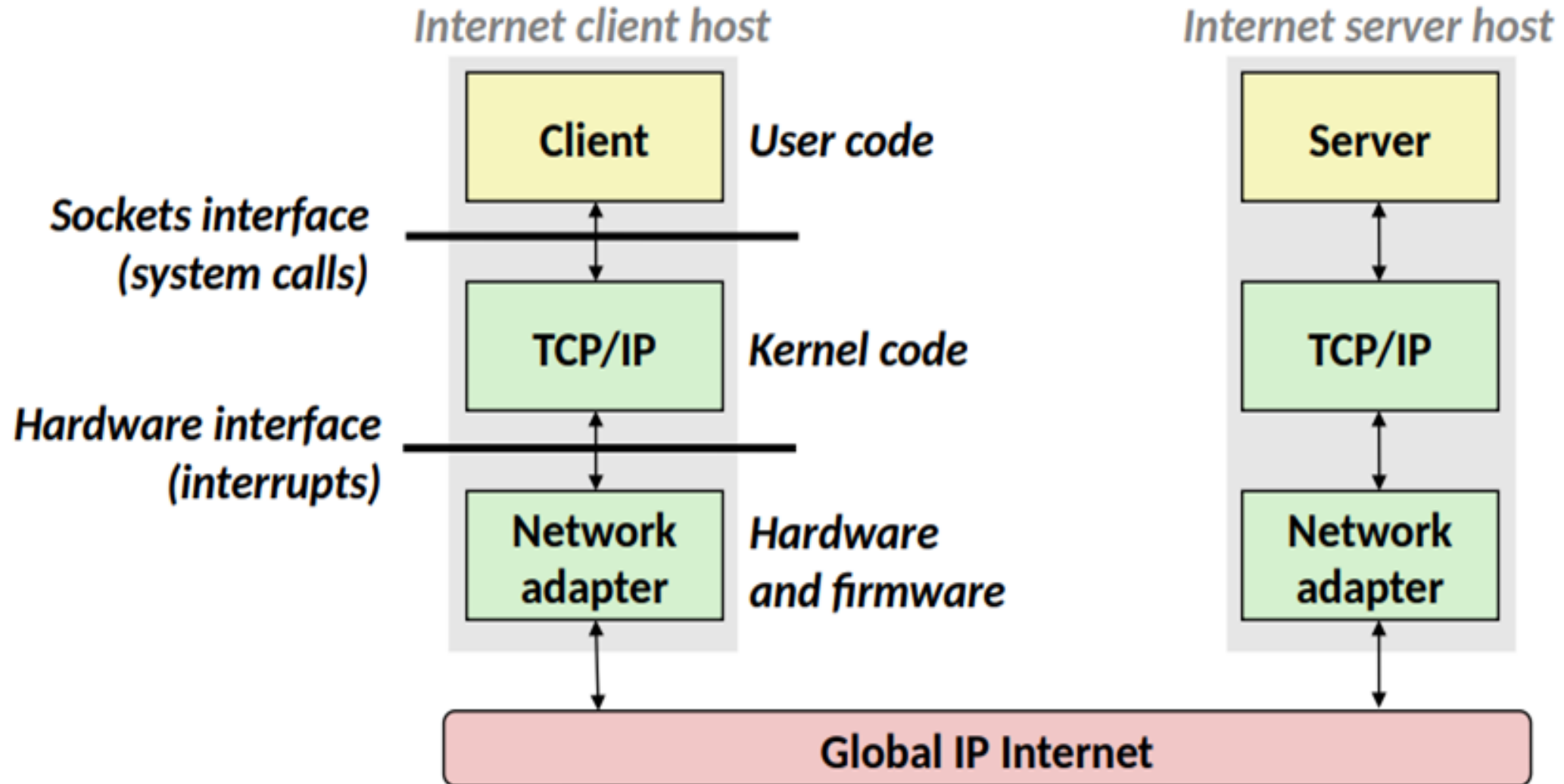
Network software

05

How is information transmitted across different types of networks?

HIGHER POLYTECHNIC SCHOOL

A **protocol** is a defined **set of rules that governs how hosts and routers collaborate to transmit data** across different networks.

The **Internet Protocol** (IP) is a set of rules that governs how data is transmitted over the internet and similar networks.
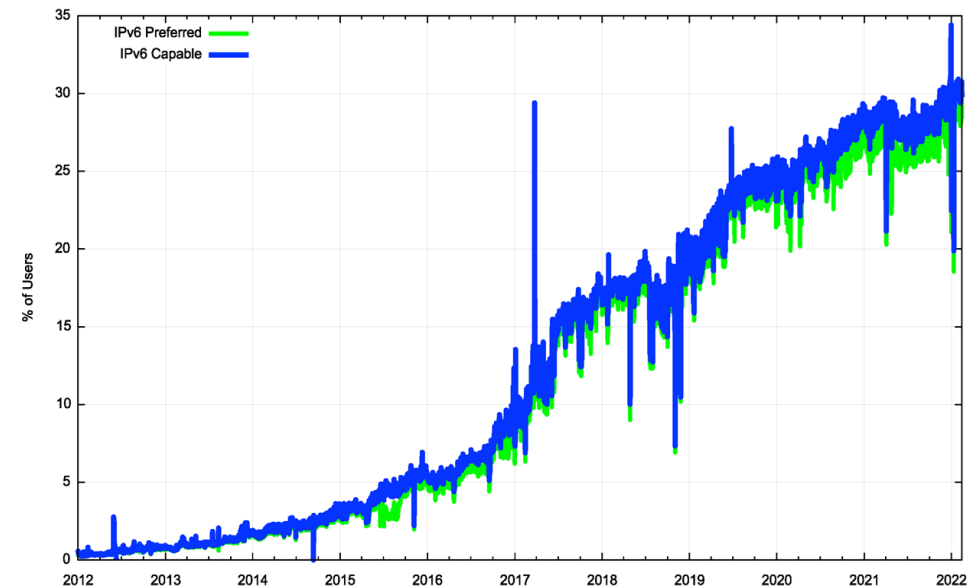
• It specifies a standardized format for host addresses, commonly known as a naming scheme, where each host and router is assigned at least one of these internet addresses, which uniquely identifies them within the network.

• It defines a standard unit of data transfer called a "**packet**". A packet consists of two primary components: a **header**, which contains control information, and a **payload**, which carries the actual data being transmitted.
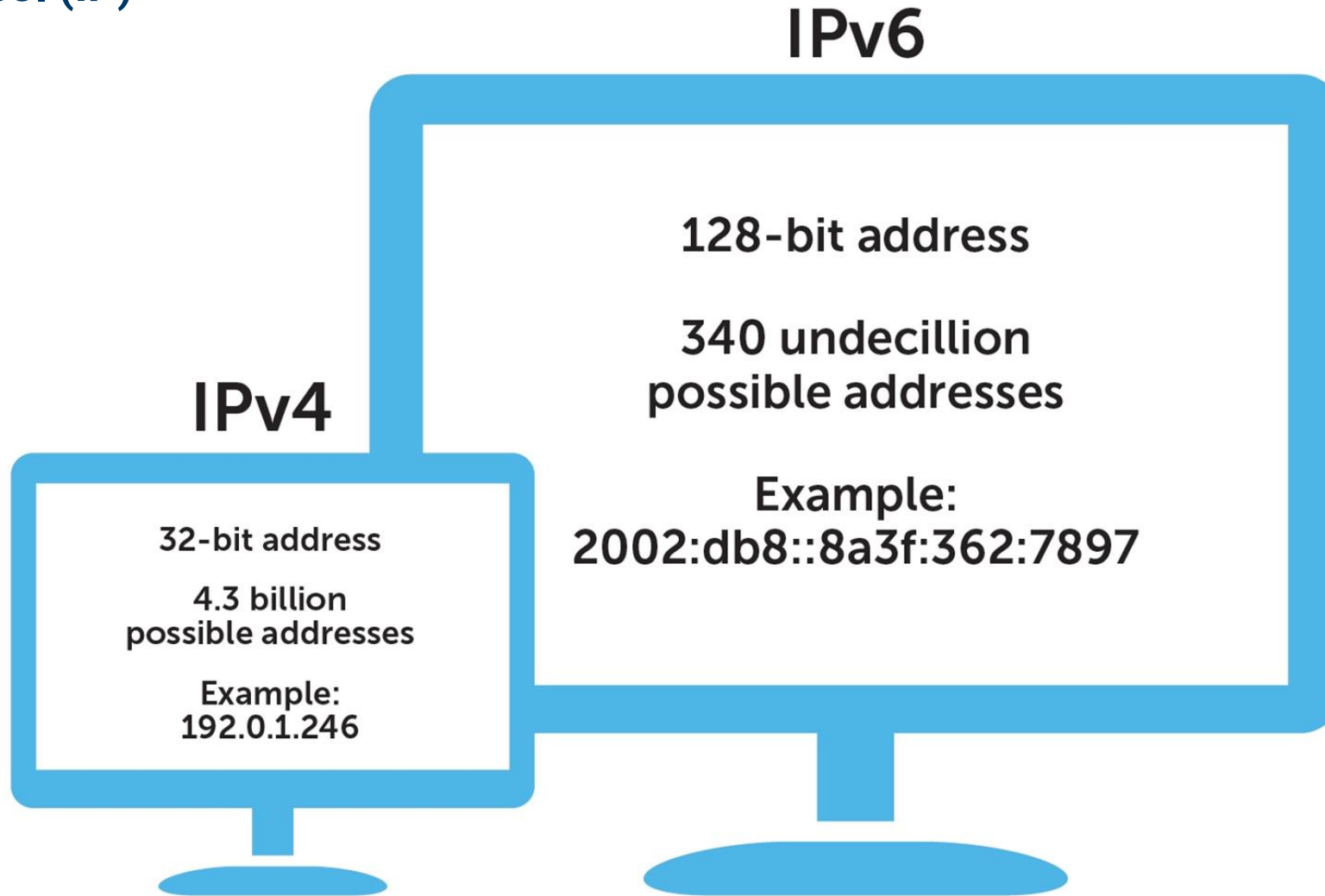
An **Internet Protocol** (IP) is a set of rules that governs how data is transmitted over the internet and similar networks. The original version of the Internet Protocol, which uses **32-bit addresses**, is officially known as Internet Protocol Version 4 (IPv4).

In 1998, Internet Protocol Version 6 (IPv6) was introduced, utilizing **128-bit addresses** as a strategic solution to the problem of **IP address depletion**. This new version significantly expanded the available address space, accommodating the growing number of devices connected to the internet.

UFV

Internet Protocol (IP)

IPv6

128-bit address

340 undecillion
possible addresses

Example:
2002:db8::8a3f:362:7897

IPv4

32-bit address

4.3 billion
possible addresses

Example:
192.0.1.246

UFV

Network address

A network address is a unique identifier assigned to a device (such as a computer, router, NIC, or printer) within a computer network. It allows the device to be recognized and located within the network, enabling communication and data exchange between devices. There are different types of network addresses depending on the context:

- Physical Address (network hardware) is a unique identifier assigned to a network hardware device and is used for communication within the local network segment.
- IP Address (TCP/IP network, such as the Internet) is a primary network address, uniquely identifying each device on the network.
- Domain Name (Internet) are human-readable addresses (e.g., www.example.com) that are linked to IP addresses, making it easier to locate and access resources online.
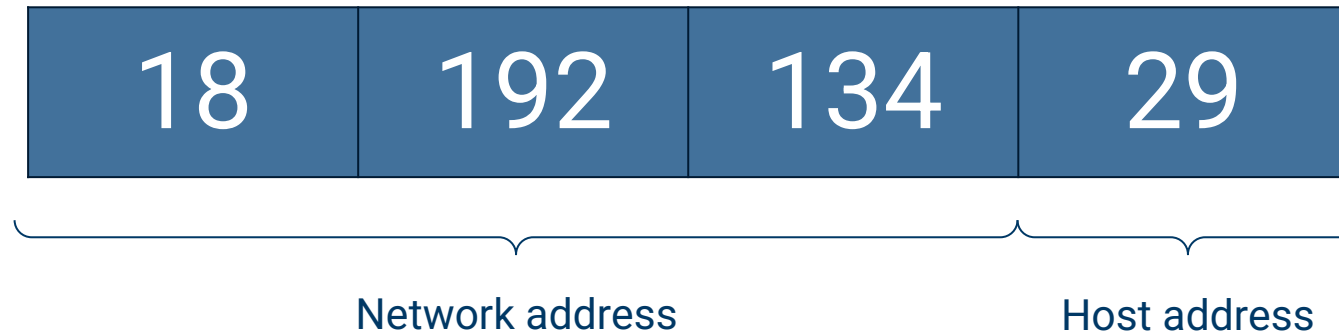
UFV

Physical address

A Media Access Control (MAC) address, also known as a hardware or physical address, is a unique 12-character alphanumeric string assigned to each electronic device on a network. Its primary function is to uniquely identify individual devices within the network, ensuring accurate communication and data transfer between them.

| C8 | 69 | CD | BA | 95 | 65 |

Organizationally Unique Identifier

Network Interface Controller specific

C8-69-CD is one of the Organizationally Unique Identifier assigned to Apple devices.

IP address

An IP address (Internet Protocol address) is a unique numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. It serves two main purposes: (1) identifying the host or network interface, (2) and providing the location of the device within the network.

18	192	134	29

Network address   Host address

The initial segment of an IP address is designated as the network address, identifying the specific network to which the device belongs, while the terminal segment is reserved for specifying the host address, uniquely identifying a device within that network.

IP address

There are public and private IP addresses:

- Private IP addresses are used within local networks and must be translated into public IP addresses to connect to the internet. This translation is handled by the NAT (Network Address Translation) service, which is typically performed by the router or proxy that provides internet access for the local network.
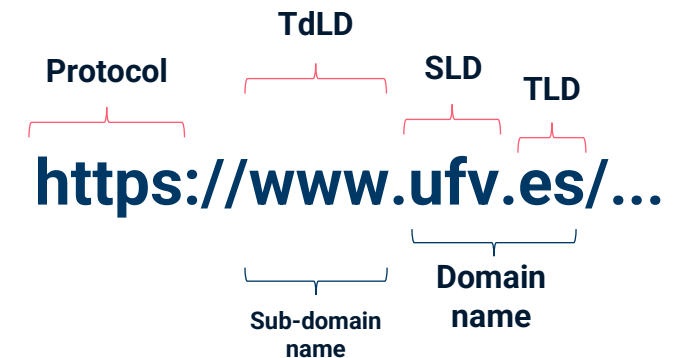
  Private addresses range: 10.x.x.x, 172.16.x.x to 172.31.x.x and 192.168.x.x

- Public IP addresses are unique addresses assigned to devices that are directly accessible on the internet. Unlike private IP addresses, which are limited to internal networks, public IPs allow devices to communicate across the internet.

Domain name

A domain name is a human-readable address used to identify and access websites or other resources on the internet. It serves as an easy-to-remember alternative to the numerical IP addresses that computers use to identify each other on the network.
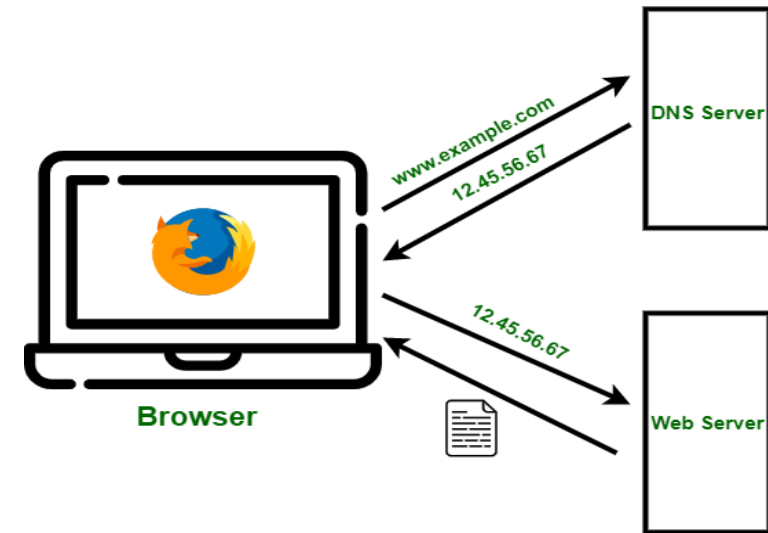
- The Top-Level Domain is the last part of the domain name, appearing after the final dot. Common TLDs include .com, .org, .net, and country-specific TLDs like .es or .uk.

- The Second-Level Domain (SLD) is the part of the domain name that directly precedes the TLD. For example, in ufv.es "ufv" is the SLD. It typically represents the name of a business, organization, or individual.

- The Third-Level Domain (TdLD) is an additional part of the domain name that precedes the SLD. For example, in www.ufv.es, "www" is the Third-Level Domain or sub-domain.

Protocol   **TdLD**   **SLD**   **TLD**

https://www.ufv.es/...

Sub-domain name   **Domain name**

The Domain Name System

The global Internet infrastructure maintains a comprehensive mapping system between IP addresses and domain names, implemented through a vast, globally distributed database known as the Domain Name System (DNS).

- Every domain name is associated with a corresponding IP address.

- Multiple domain names can be linked to a single IP address, allowing different websites or services to be hosted on the same server.
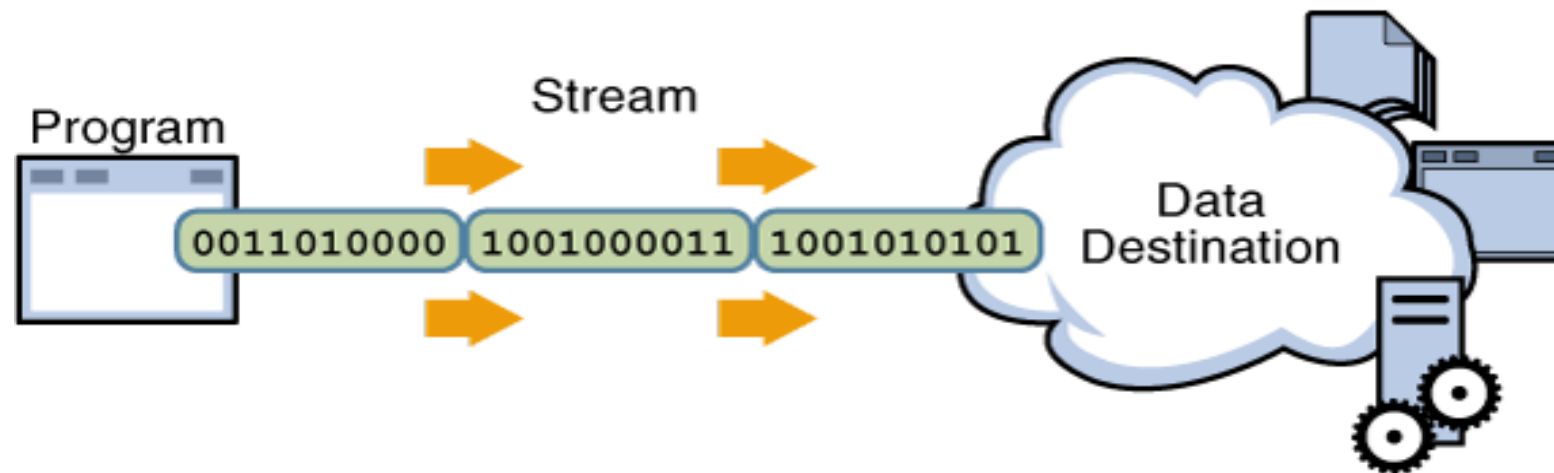

DNS can be considered like the phonebook of the Internet because it translates human-readable domain names into the numerical IP addresses that computers use.

How do computers communicate in the Internet?

HIGHER POLYTECHNIC SCHOOL

Comunication - Components

Clients and servers communicate by exchanging streams of data over network connections.

- Point-to-Point Communication: Each connection is established between a specific pair of processes, allowing direct communication between the client and the server.

- Full-Duplex Communication: Data can flow in both directions simultaneously on the same connection, enabling efficient two-way communication between the client and server.

Comunication - Components

The communication between clients and servers happens through endpoints called **sockets**. A socket is defined by **a unique combination of an IP address and a port number** that identifies one end of a connection:

- A socket address is a unique combination of an IP address and a port number (IP address). For example, 192.168.1.10:8085 represents a socket with IP 192.168.1.10 and port 8085.
- A port is **a 16-bit number that identifies a specific process or service on a computer**. Ports allow multiple network services to run on a single IP address (computer) by assigning each service a unique port number.
  - Ephemeral Ports are **temporary ports automatically assigned by the client's operating system** when a client initiates a connection to a server. Ephemeral ports typically range from 49152 to 65535.
  - Well-Known Ports are **pre-assigned to specific services and are recognized globally**. For example, port 80 is commonly used for HTTP web traffic, and port 443 is used for HTTPS (secure web traffic). **Well-known ports range from 0 to 1023.**

Comunication - Components

The communication between clients and servers happens through endpoints called **sockets**. A socket is defined by **a unique combination of an IP address and a port number** that identifies one end of a connection:
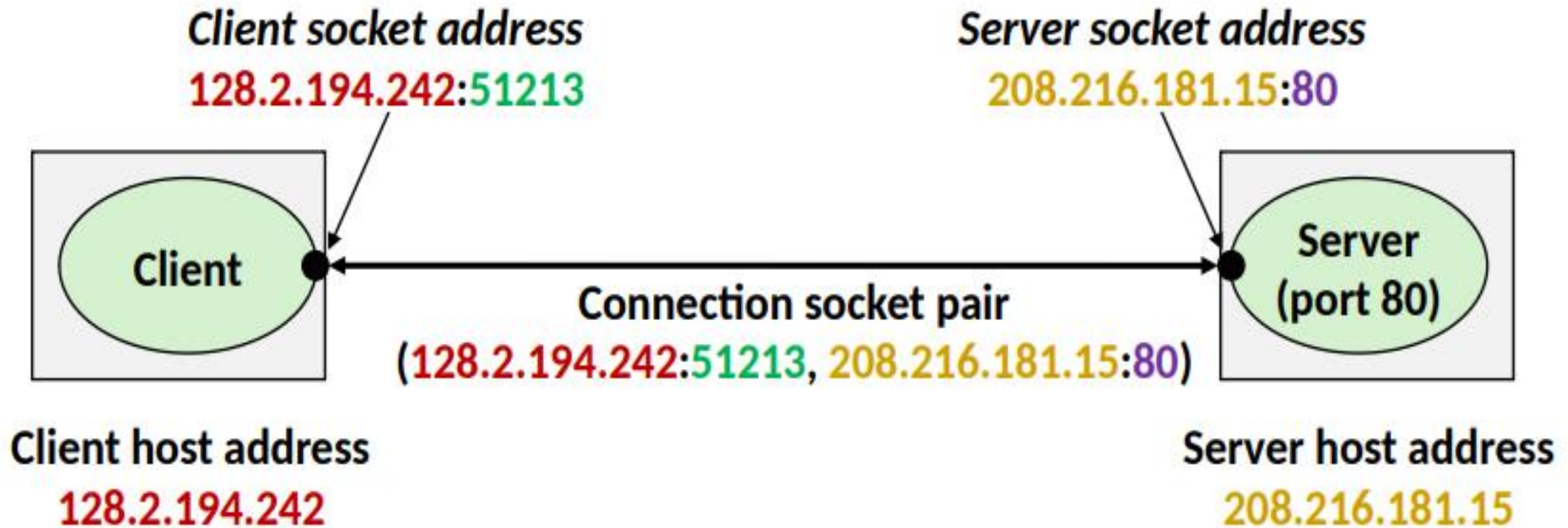
For example, 192.168.1.10:8085 represents a socket with IP 192.168.1.10 and port 8085.

A port is **a 16-bit number that identifies a specific process or service on a computer**. Ports allow multiple network services to run on a single IP address (computer) by assigning each service a unique port number.

- Ephemeral Ports are **temporary ports automatically assigned by the client's operating system** when a client initiates a connection to a server. Ephemeral ports typically range from 49152 to 65535.
- Well-Known Ports are **pre-assigned to specific services and are recognized globally**. For example, port 80 is commonly used for HTTP web traffic, and port 443 is used for HTTPS (secure web traffic). **Well-known ports range from 0 to 1023.**
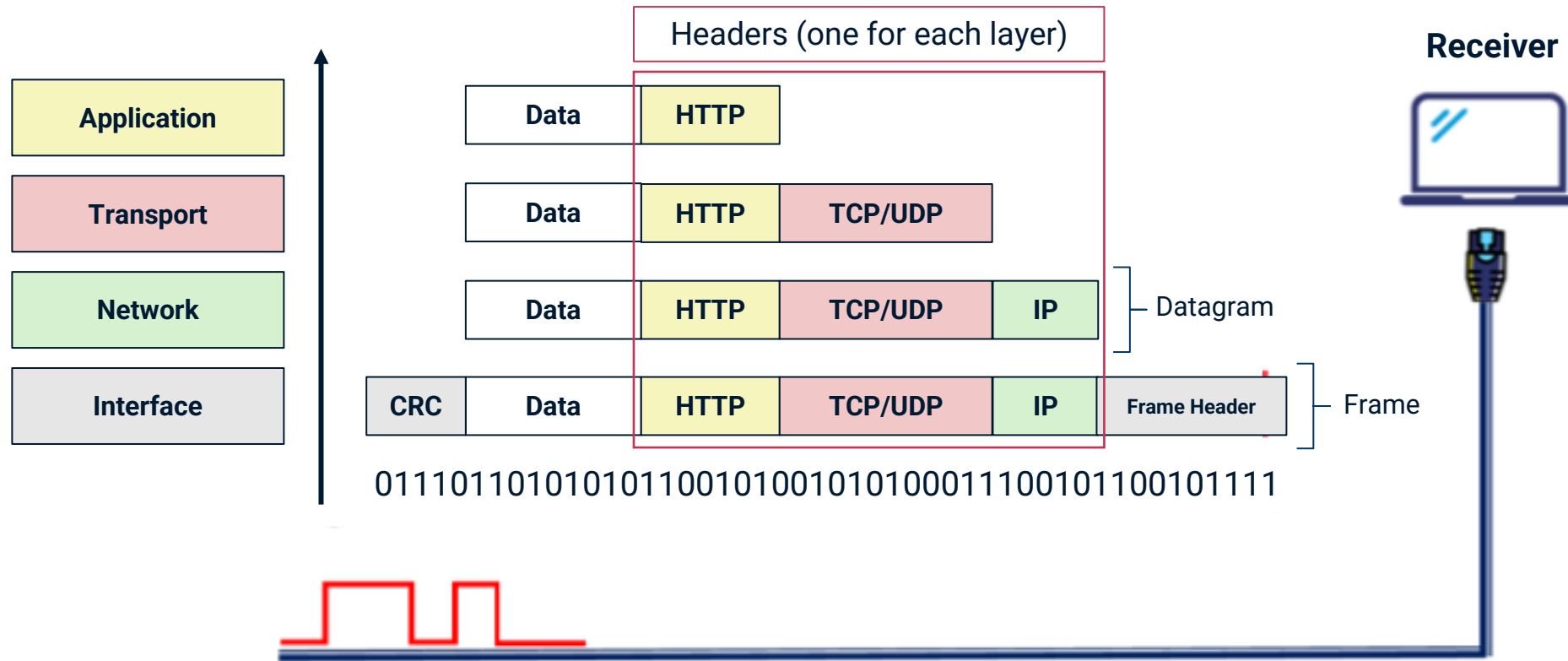
Comunication

A connection is uniquely identified by the socket addresses of its endpoints (connection socket pair).

Client socket address
128.2.194.242:51213

Server socket address
208.216.181.15:80

Client

Server
(port 80)

Connection socket pair
(128.2.194.242:51213, 208.216.181.15:80)

Client host address
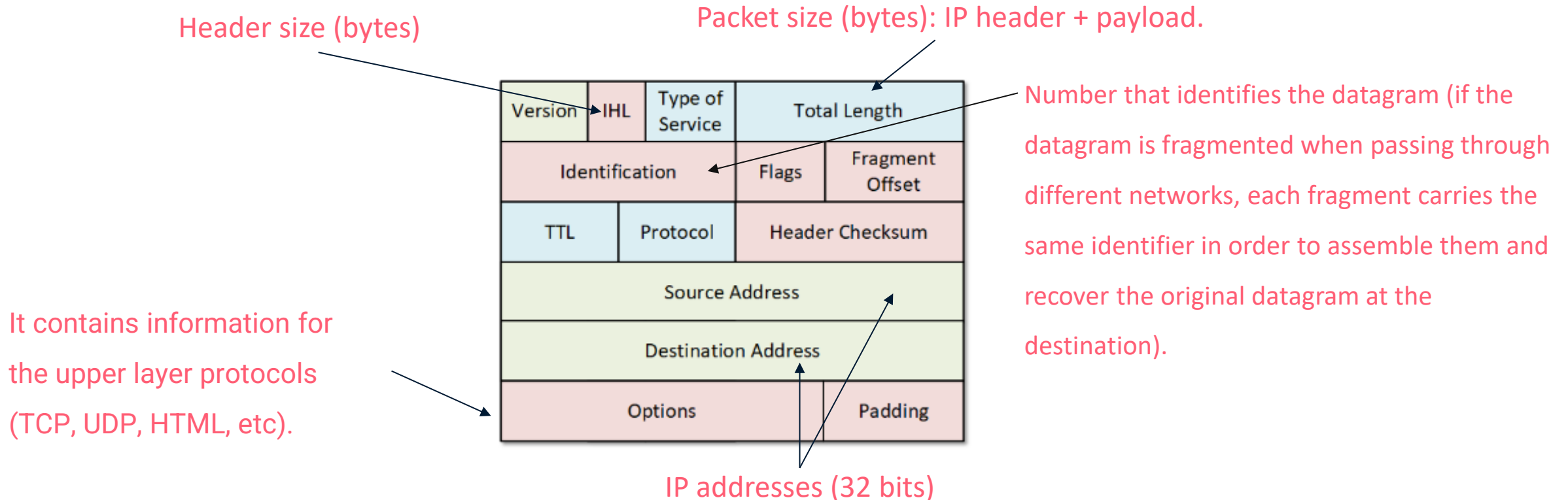128.2.194.242

Server host address
208.216.181.15

Comunication - Datagrams

Packets are referred to as datagrams at the network layer and as frames at the data link layer (also known as the interface layer).

01110110101010110010100101010001110010110010111

Network software

Comunication – Network datagrams

An IPv4 datagram is a basic unit of data that is transmitted across an IPv4 (Internet Protocol version 4) network. It encapsulates the information that needs to be sent from one device to another over the Internet or other IP-based networks.

Header size (bytes)

Packet size (bytes): IP header + payload.

Number that identifies the datagram (if the datagram is fragmented when passing through different networks, each fragment carries the same identifier in order to assemble them and recover the original datagram at the destination).

It contains information for the upper layer protocols (TCP, UDP, HTML, etc).

Version	IHL	Type of Service	Total Length	
Identification			Flags	Fragment Offset
TTL		Protocol	Header Checksum	
Source Address				
Destination Address				
Options			Padding	

IP addresses (32 bits)

Network software

Comunication – Network datagrams

IPv4 datagram

Version	IHL	Type of Service	Total Length	
Identification			Flags	Fragment Offset
TTL		Protocol	Header Checksum	
Source Address				
Destination Address				
Options			Padding	

IPv6 datagram

Version	Traffic Class	Flow Label	
Payload Length		Next Header	Hop Limit
Source Address			
Destination Address			

- Fields kept in IPv6.
- Fields kept in IPv6, but name and position changed.
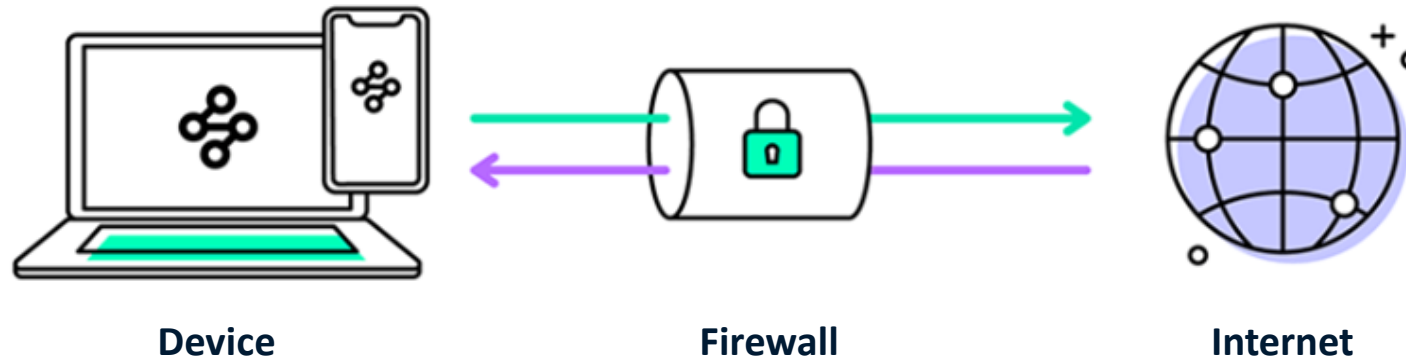- Fields removed in IPv6.
- Fields are new in IPv6.

HIGHER POLYTECHNIC SCHOOL

Fundamentals of Computer Engineering

Network applications

06

HIGHER POLYTECHNIC SCHOOL

Fundamentals of Computer Engineering
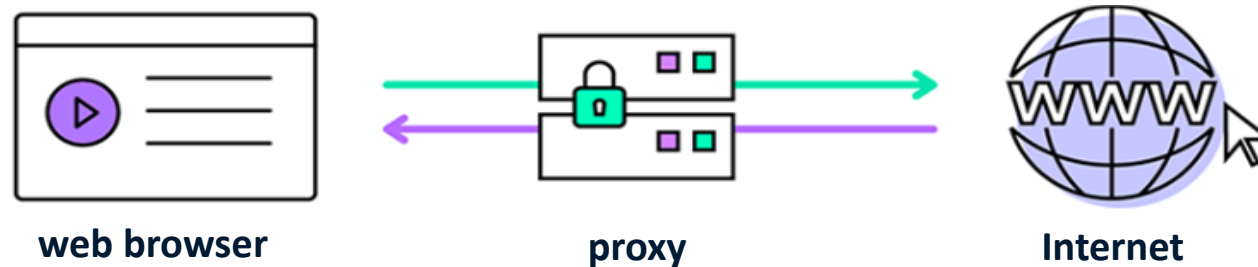
Firewall (software)

A firewall is a security application that acts as a barrier between a trusted internal network and untrusted external networks, such as the internet.

Device   **Firewall**   **Internet**

- It inspects incoming and outgoing network traffic, allowing or blocking data packets based on predefined security rules.

- It enforce access control policies by specifying which users, devices, or applications can access network resources.

- It can detect and block malicious activities, such as malware or hacking attempts, by identifying suspicious patterns in network traffic and stopping them before they can cause harm.
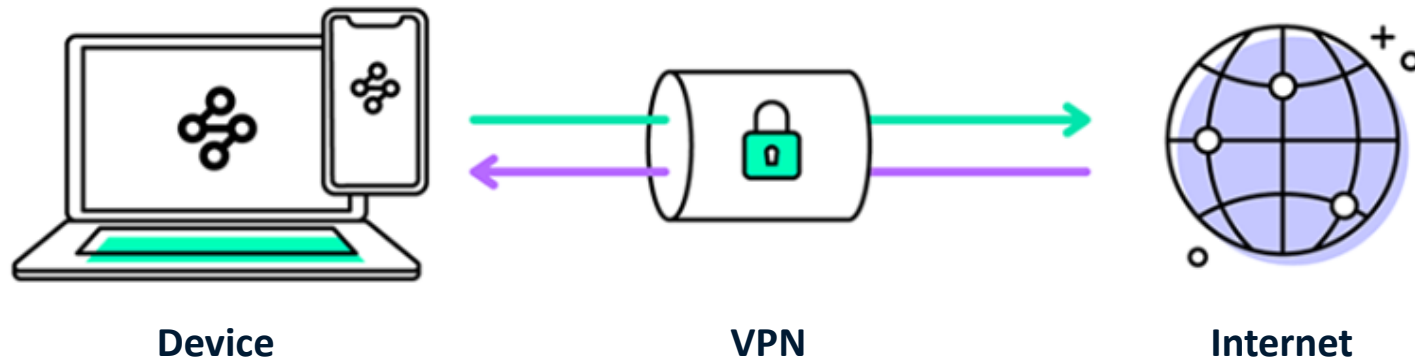
Proxy

A proxy server is a server-based application that acts as an intermediary between a client requesting a specific resource and the server that provides that resource. It manages and forwards client requests to the appropriate server, often enhancing security, privacy, or performance in the process.

web browser   **proxy**   **Internet**

- It facilitates caching functionality to improve response times and reduce bandwidth usage by storing copies of frequently accessed resources.
- It enforces access control and enhances security, often working alongside a firewall to regulate and protect network traffic.
- It offers address translation services, commonly known as Network Address Translation (NAT), allowing multiple devices on a local network to share a single public IP address.

Virtual Private Network (VPN)

A virtual private network (VPN) extends the reach of a private network over a public network infrastructure, enabling users to transmit and receive data across shared or public networks as if their devices were directly connected to the private network.

Device　　　　　**VPN**　　　　　**Internet**

- It creates a secure and encrypted connection, ensuring privacy and data integrity while using public networks.
- It circumvents geographically restricted content, allowing users to access websites and services that may be blocked or limited based on their location.
- It ensures safety via anonymity, masking the user's IP address and encrypting their data.

UFV

HIGHER POLYTECHNIC SCHOOL

Fundamentals of Computer Engineering