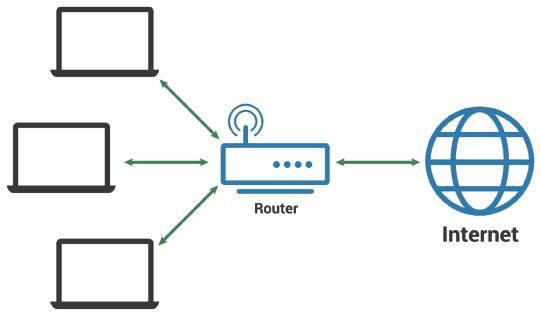
Cybersecurity & Networking Basics: Foundations

Day 2: Networking Fundamentals

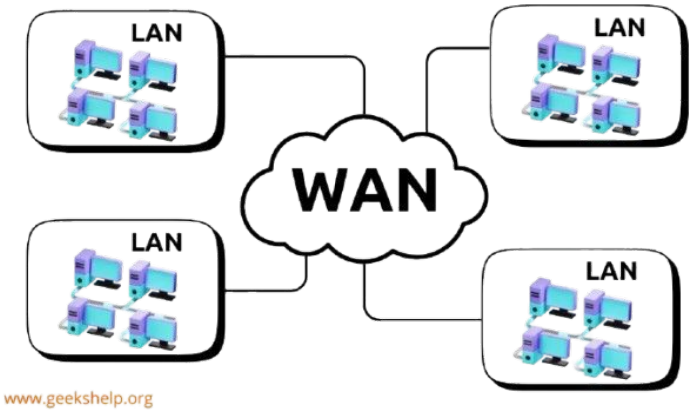
Introduction to Computer Networking

- **What is a network?**
  - Computer networking is the practice of connecting computers and other devices to share resources and information.
- **Purpose:**
  - To facilitate communication, share resources, and provide access to information
- **Key components:**
  - Devices, communication medium, and protocols.

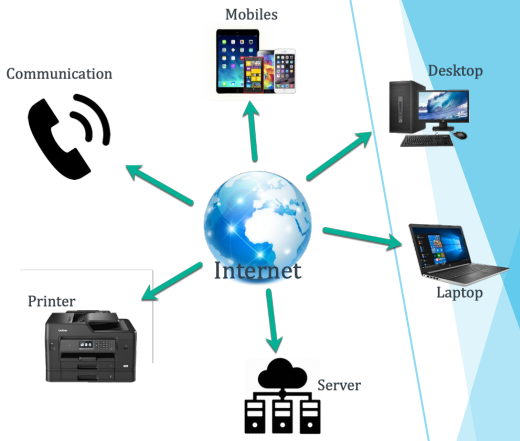
Types of networks: LAN, WAN, Internet



LAN (Local Area Network)
Connects devices within a limited geographical area, such as a home, office, or school. High-speed and privately owned.

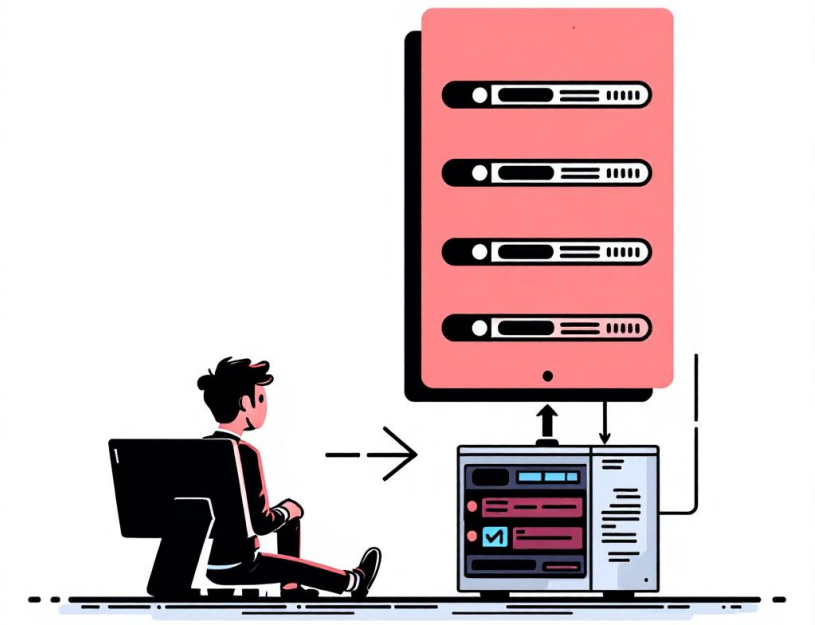


WAN (Wide Area Network)
Spans a larger geographical area, connecting multiple LANs over long distances. Often uses telecommunication links.



The Internet
A global network of interconnected computer networks, utilizing a standardized set of communication protocols. It's the largest WAN.

The Client-Server Model



The client-server model is a distributed application framework that partitions tasks between service providers (servers) and service requesters (clients).

Clients: Devices or applications that request information or services (e.g., your web browser, email client).

Servers: Powerful computers that provide resources, data, or services to clients (e.g., web servers, database servers).

Interaction: Clients initiate communication, and servers listen for requests and respond accordingly.

Why Networking Matters in Cybersecurity

Networks are the backbone of modern digital operations, making them a prime target for attackers.

- **Attackers need Network Access**
  - **Entry Point:** Most cyberattacks leverage network vulnerabilities to gain initial access.
  - **Lateral Movement:** Once inside, attackers use network paths to move between systems.
  - **Exfiltration:** Stolen data is typically exfiltrated over the network

Visibility Empowers Defenders

- **Detection:**
  - Monitoring network traffic helps identify suspicious activities and intrusions early.
- **Prevention:**
  - Proper network segmentation and firewall rules block unauthorized access.
- **Response:**
  - Understanding network architecture is key to containing and eradicating threats.
- **Forensics:**
  - Network logs provide crucial evidence for incident investigation.

The Network as a Battlefield

- Security is about the pathways, not just the devices.
- Data integrity is won or lost within the network.
- Mastery of network fundamentals is essential for success.
- Every packet and connection tells a unique story.

Common Network Devices (with Examples)

- **Router**

  A router connects **different networks together** and decides the best path for data to travel. It is usually the gateway between a local network and the internet.

- **Example:** A home or office router that connects internal computers to the internet.
- Blocks or allows traffic based on rules and helps prevent unauthorized access.

Common Network Devices (with Examples)

- **Switch**

  A switch connects devices within the same network and forwards data only to the intended device using MAC addresses.

- **Example:** An office switch connecting computers, printers, and servers.

- Reduces unnecessary traffic and supports features like VLANs for network segmentation.

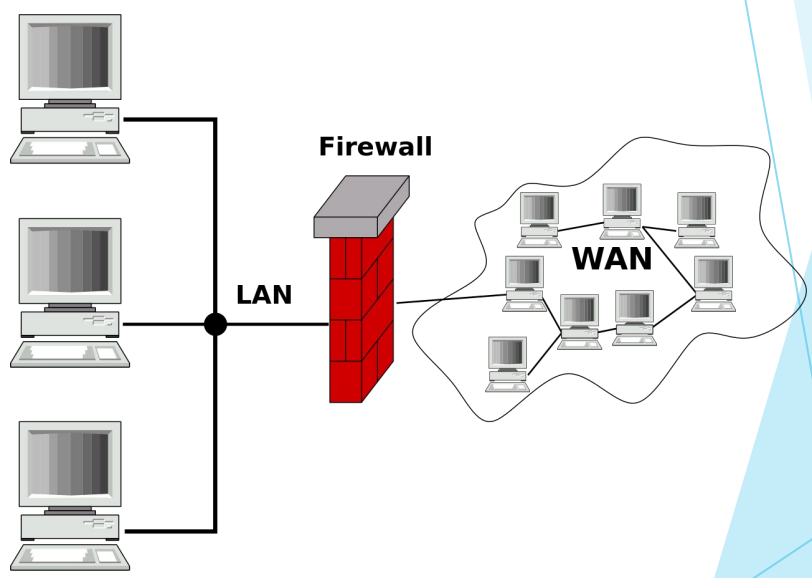
Common Network Devices (with Examples)

- **Firewall**

  A firewall monitors and controls incoming and outgoing network traffic based on security rules. It acts as a barrier between trusted and untrusted networks.

- **Example:** A firewall blocking suspicious traffic from the internet.

- Prevents unauthorized access, malware communication, and attacks like port scanning.



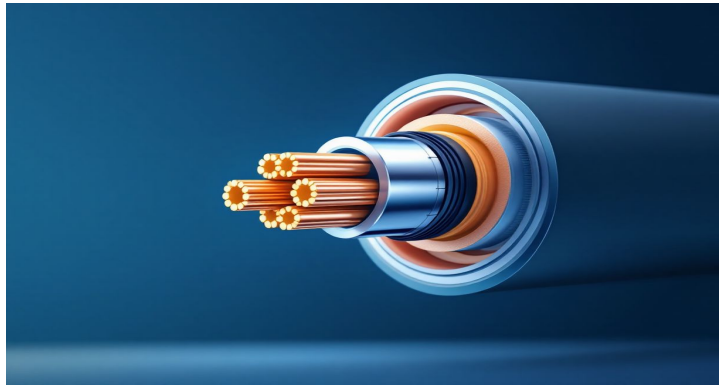
Common Network Devices (with Examples)

- **Modem**

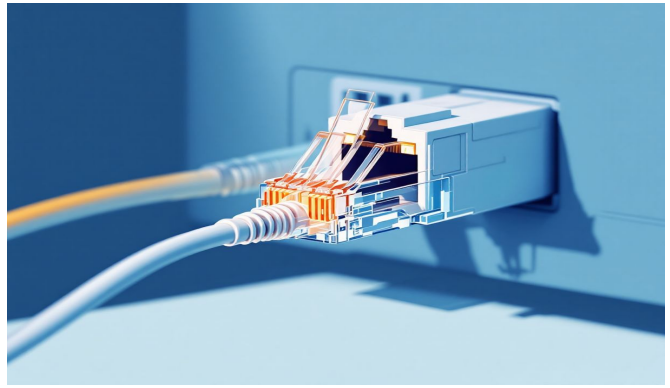
  A modem connects a local network to an Internet Service Provider (ISP) by converting signals into a usable digital format.

- **Example:** Cable or fiber modem provided by an ISP.
- Security role: Works with firewalls and routers to protect the internal network.

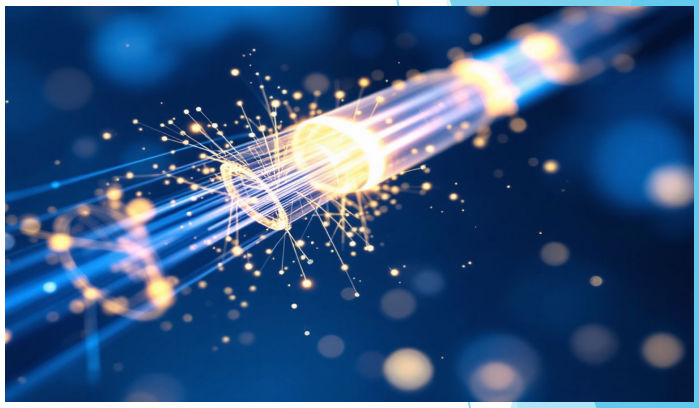
Network Transmission Media



- **Coaxial Cable**
  - Cable TV connections
  - Cable internet modems
  - **Cybersecurity:** Physical access can enable signal tapping, but the cable's shielding provides more resistance than simpler copper wiring.



- **RJ45 Connector (Ethernet)**
  - PC connected to a switch
  - Router connected to a modem
  - **Cybersecurity:** Physical access to an Ethernet port can allow unauthorized network entry, making robust port security and access control vital.



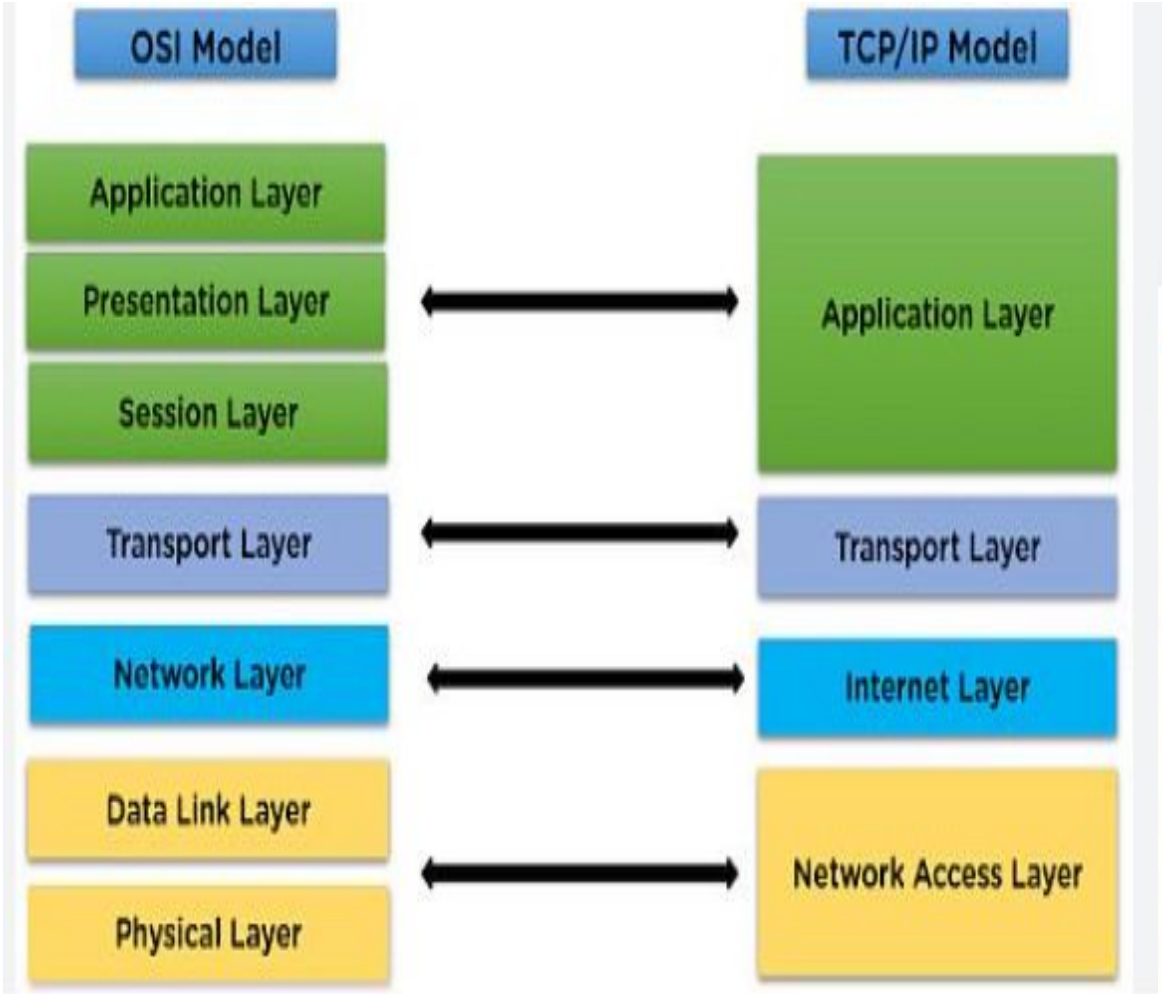
- **Fiber Optic Cable**
  - ISP backbone networks
  - Data centers and cloud providers
  - **Cybersecurity:** Fiber optics are inherently more secure than copper, as tapping into them is extremely difficult to do without detection, safeguarding critical data.

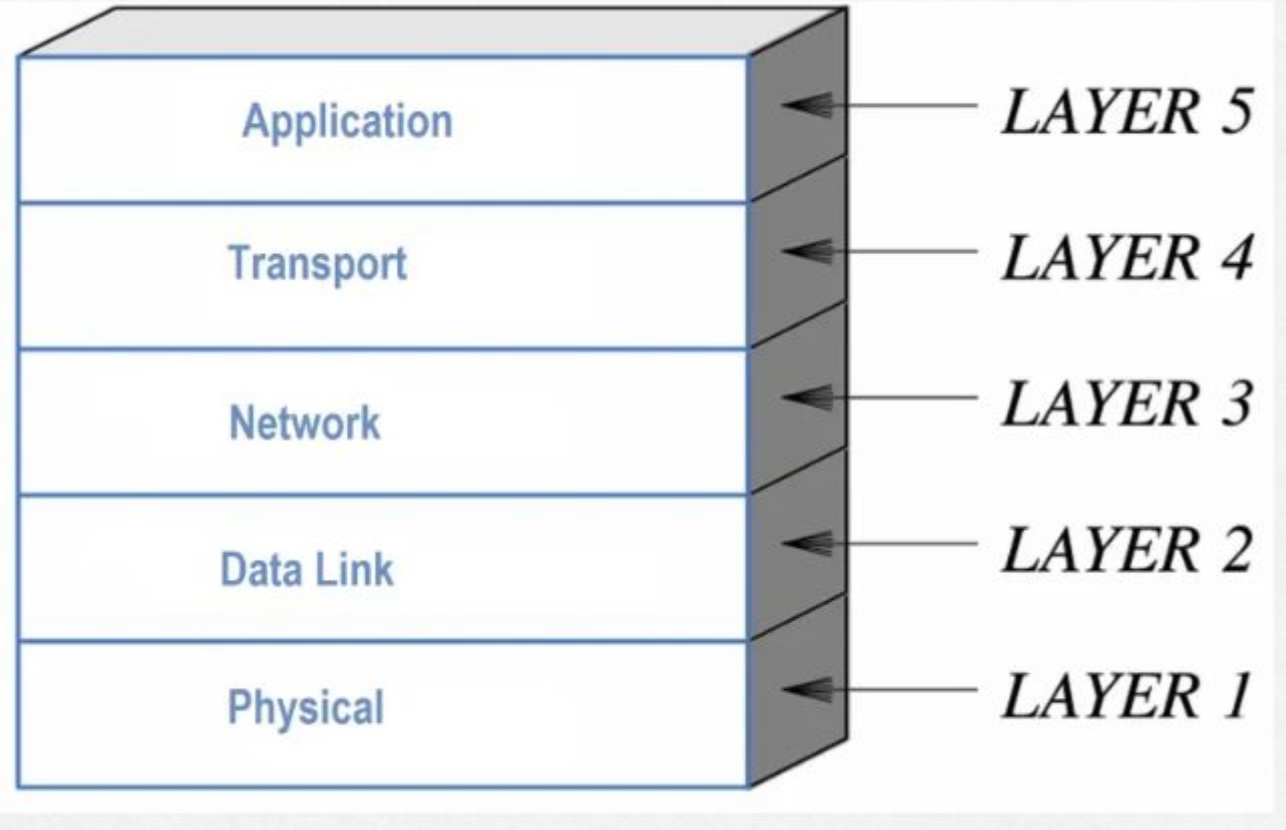
The OSI Model: A 7-Layer Framework

7	**Application Layer**	Human-computer interaction layer, where applications can access the network services
6	**Presentation Layer**	Ensures that data is in usable format and is where data encryption occurs
5	**Session Layer**	Maintains connections and is responsible for controlling ports and sessions
4	**Transport Layer**	Transmits data using transmission protocols including TCP and UDP
3	**Network Layer**	Decides which physical path the data will take
2	**Data Link Layer**	Defines the format of data on the network
1	**Physical Layer**	Transmits raw bit stream over the physical medium

The OSI Model: A 7-Layer Framework

TCP/IP Model	Protocols
Application	HTTP, HTTPS, FTP
Transport	TCP, UDP
Network	IP
Data Link	MAC Address
Physical	Cables, Wi-Fi


OSI Model
TCP/IP Model
Application Layer
Presentation Layer
Session Layer
Application Layer
Transport Layer
Transport Layer
Network Layer
Internet Layer
Data Link Layer
Physical Layer
Network Access Layer


Application
Transport
Network
Data Link
Physical
LAYER 5
LAYER 4
LAYER 3
LAYER 2
LAYER 1

IP Addresses: Your Digital Fingerprint

- Every device connected to a network needs a unique identifier
  - IP (Internet Protocol) address.

IPv4 vs. IPv6

IPv4: Uses 32-bit addresses (e.g., 192.168.1.1). Offers about 4 billion unique addresses. Still widely used but exhausting supply.
IPv6: Uses 128-bit addresses (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334). Offers virtually limitless addresses, designed to replace IPv4.

Public vs. Private IPs

Public: Internet-routable addresses, unique globally. Used for devices directly accessible from the internet (e.g., web servers).
Private: Non-routable addresses, used within local networks. Many devices can use the same private IP ranges without conflict, relying on NAT for internet access.

Static vs. Dynamic IPs

Static: Manually assigned and fixed. Ideal for servers or network devices that need a consistent address.
Dynamic: Automatically assigned by a DHCP server. Common for most client devices (laptops, phones), which receive a temporary address from a pool.

IP Addresses

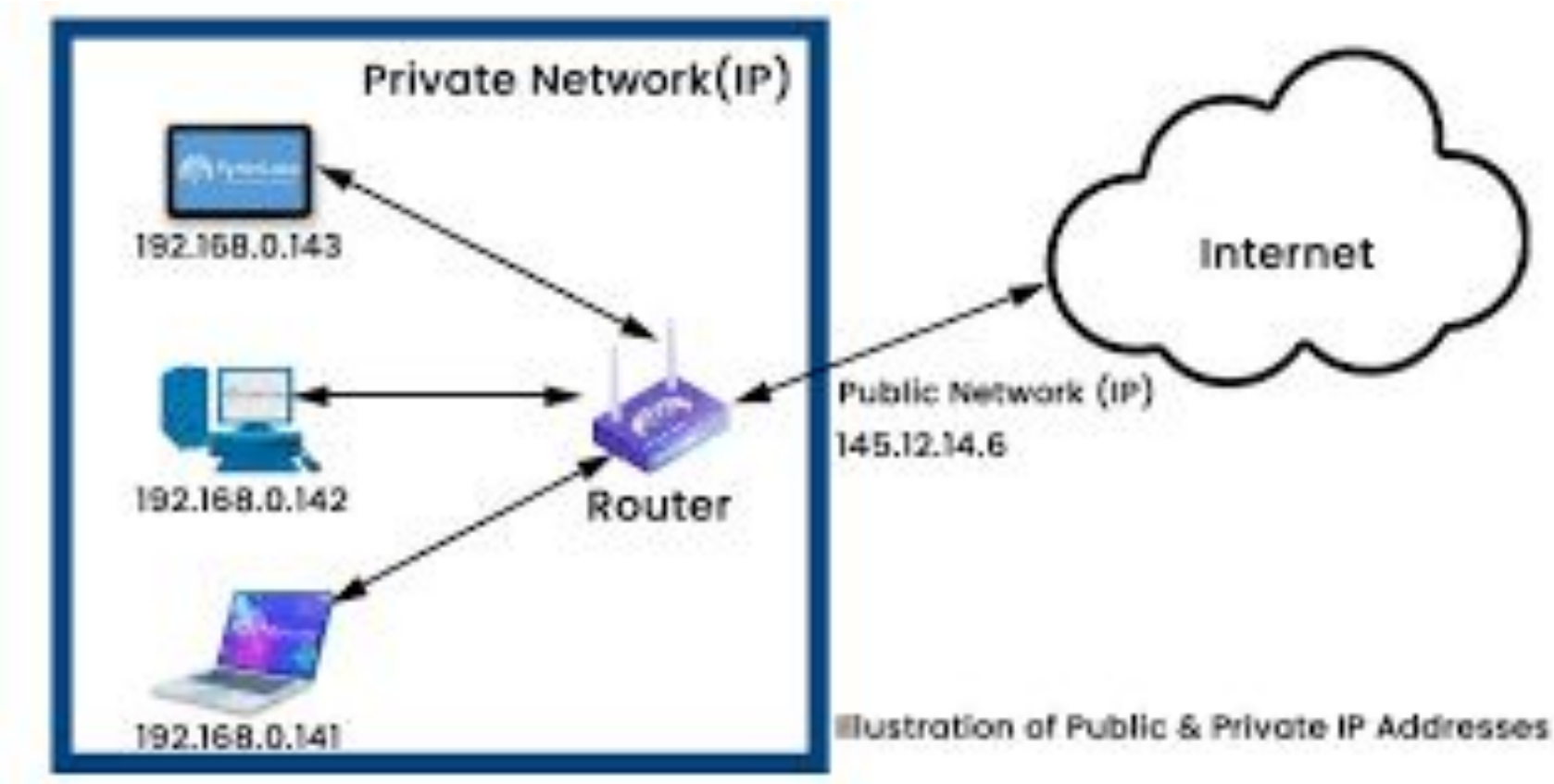


Illustration of Public & Private IP Addresses

IPv4 Address Classes

Class A

Range: 1.0.0.0 to 126.255.255.255
Networks: 128 potential networks (2 reserved).
Hosts per Network: 16,777,214 hosts.
Default Mask: 255.0.0.0 (/8).

Class B

Range: 128.0.0.0 to 191.255.255.255
Networks: 16,384 networks.
Hosts per Network: 65,534 hosts.
Default Mask: 255.255.0.0 (/16).

Class C

Range: 192.0.0.0 to 223.255.255.255
Networks: 2,097,152 networks.
Hosts per Network: 254 hosts.
Default Mask: 255.255.255.0 (/24).

Class D (Multicast)

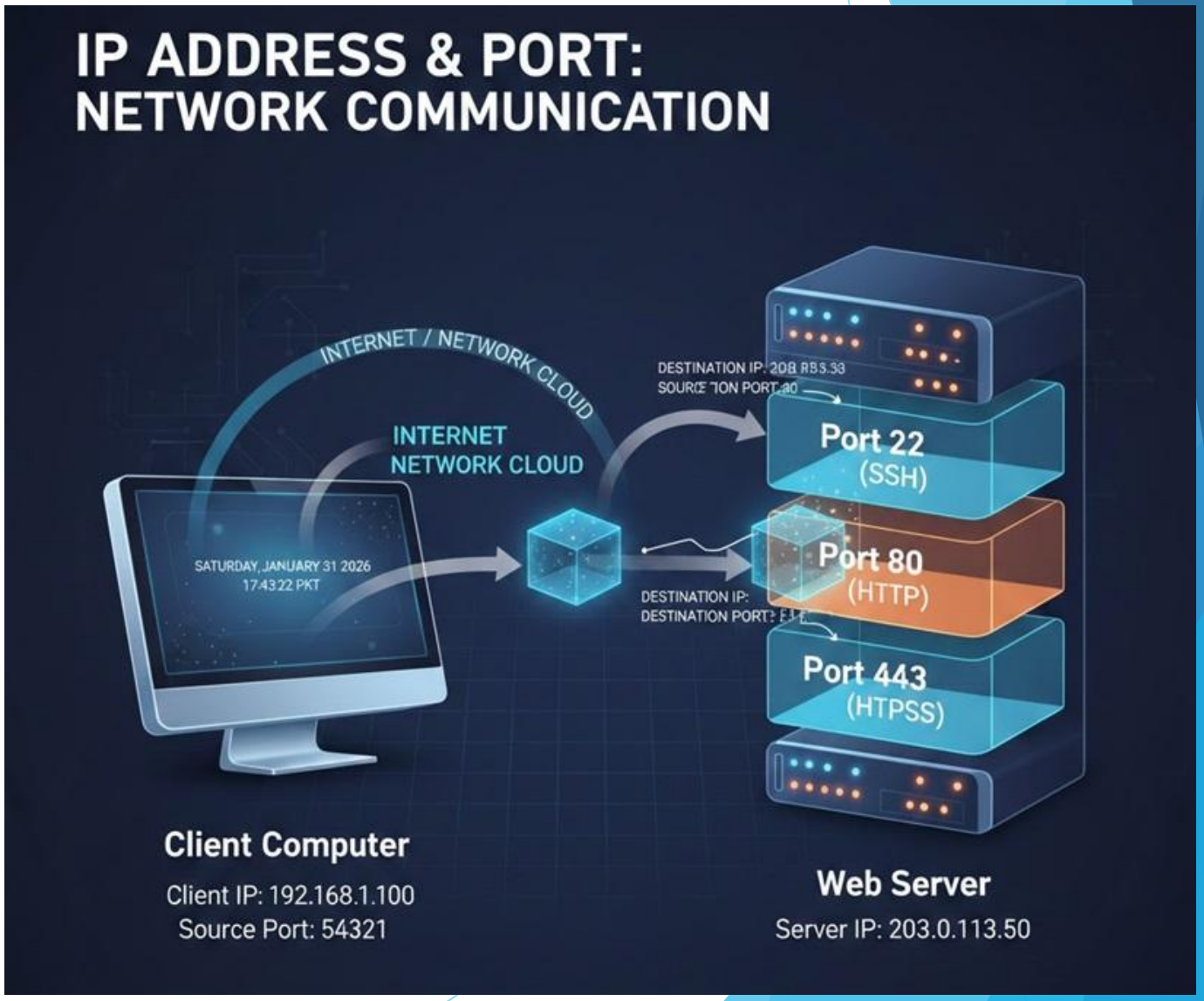
Range: 224.0.0.0 to 239.255.255.255
Usage: No host or network bits; used for broadcasting to a group of hosts simultaneously.

Class E (Experimental)

Range: 240.0.0.0 to 255.255.255.255
Usage: Reserved by IETF for research and future study.

What is a Network Port?

- **Virtual point** where network connections start and end.
- If IP is the building, the Port is the specific door.
- Ensures data reaches the correct application on a device.

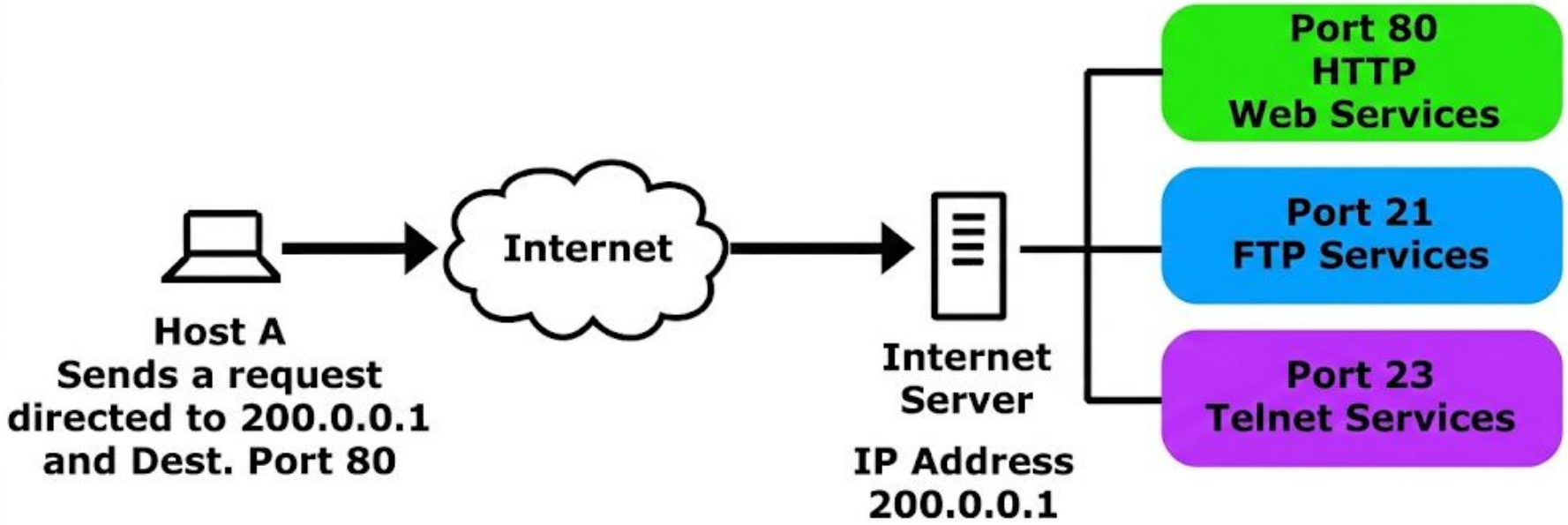


Port Categories

- **65,536 Total Ports:** Port numbers range from 0 to 65535.
- **Well-Known Ports (0–1023):** Reserved for universal, standard services like web browsing and file transfers.
- **Registered Ports (1024–49151):** Assigned by the IANA* for specific applications or software vendors.
- **Dynamic/Private Ports (49152–65535):** Temporary ports used by your computer to talk to a server.

***IANA** stands for the **Internet Assigned Numbers Authority**.

Using Ports To Identify Services



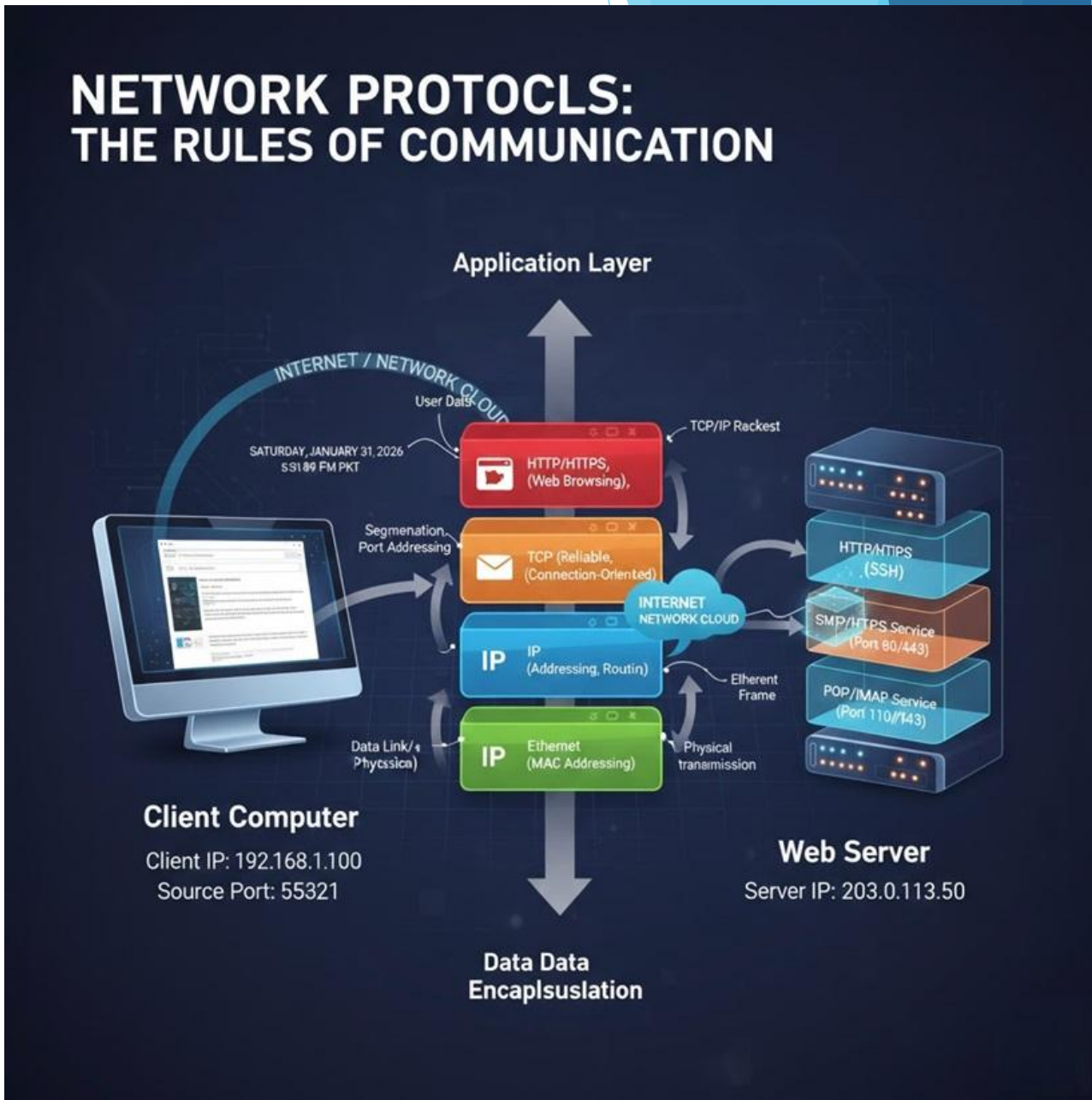
In this example, Host A sends a request to a server on the Internet.
The Destination Port is set to 80, indicating a HTTP request

Ports in Cybersecurity

- Open ports represent the 'Attack Surface' of a system.
- Port Scanning is used by attackers to find vulnerabilities.
- Firewalls secure networks by closing unnecessary ports.
- Specific attacks often target common ports like SQL (1433) or RDP (Remote Desktop Protocol) (3389)

Network Protocols

- Formal rules for data transmission between devices.
- Ensures different hardware and software can communicate.
- Handles addressing, routing, and error detection.



Common Application Protocols

- HTTPS: Secure web browsing.
- DNS: Translating URLs to IP addresses.
- FTP: Dedicated file transfers.
- SSH: Secure remote server management.

Core Protocols: TCP vs. UDP

- **TCP:** Reliable, connection-oriented, and checks for errors.
  - Use TCP for accuracy (Email)
- **UDP:** Fast, connectionless, and used for real-time streaming.
  - use UDP for speed (Gaming).

Protocols in Cybersecurity

- Secure protocols (HTTPS/SSH) protect data from sniffing.
- Plaintext protocols (HTTP/Telnet) are high-security risks.
- Firewalls filter traffic based on protocol types.
- Attackers scan protocols to find unpatched vulnerabilities.

Common Well-Known Ports & Protocols

- Understanding standard port assignments is essential for network troubleshooting and security configuration.

Port	Protocol	Types
80	TCP	HTTP (Hypertext Transfer Protocol) - Used for unencrypted web traffic.
443	TCP	HTTPS (Hypertext Transfer Protocol Secure) - Used for encrypted web traffic.
22	TCP	SSH (Secure Shell) - Used for secure remote access to computers and servers.
21	TCP	FTP (File Transfer Protocol) - Used for transferring files between computers.
23	TCP	Telnet - Used for unencrypted remote access. Largely deprecated due to security concerns.
25	TCP	SMTP (Simple Mail Transfer Protocol) - Used for sending email messages.
53	TCP/UDP	DNS (Domain Name System) - Translates domain names into IP addresses.
3389	TCP	RDP (Remote Desktop Protocol) - Allows a user to connect to another computer over a network.