**Network Foundations**

**Introduction to Networks**

**What is a Network?**

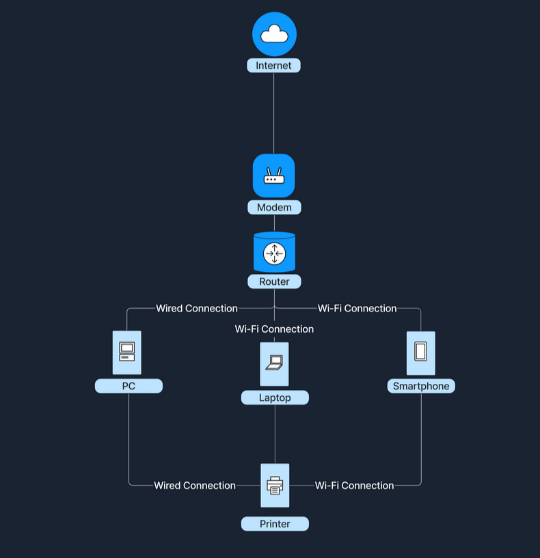
* A **network** is a collection of interconnected devices (nodes)—such as computers, smartphones, printers, and servers—that can share data and resources.
* Networks allow for data transfer and communication between nodes via **links** (wired or wireless connections).

| **Concept** | **Description** |
| --- | --- |
| Nodes | Individual devices on a network |
| Links | Wired or wireless pathways connecting nodes |
| Data Sharing | Primary function: enables data exchange between devices |

*Analogy: A group of friends chatting in a room, where each person is a node and their conversation forms the communication link (the data being shared).*

**Importance of Networks**

| **Function** | **Description** |
| --- | --- |
| Resource Sharing | Share hardware/software (e.g., printers, files) |
| Communication | Enables emails, instant messaging, video calls |
| Data Access | Retrieve files and databases from any connected device |
| Collaboration | Work together in real time regardless of location |



**Types of Networks**

**Local Area Network (LAN)**

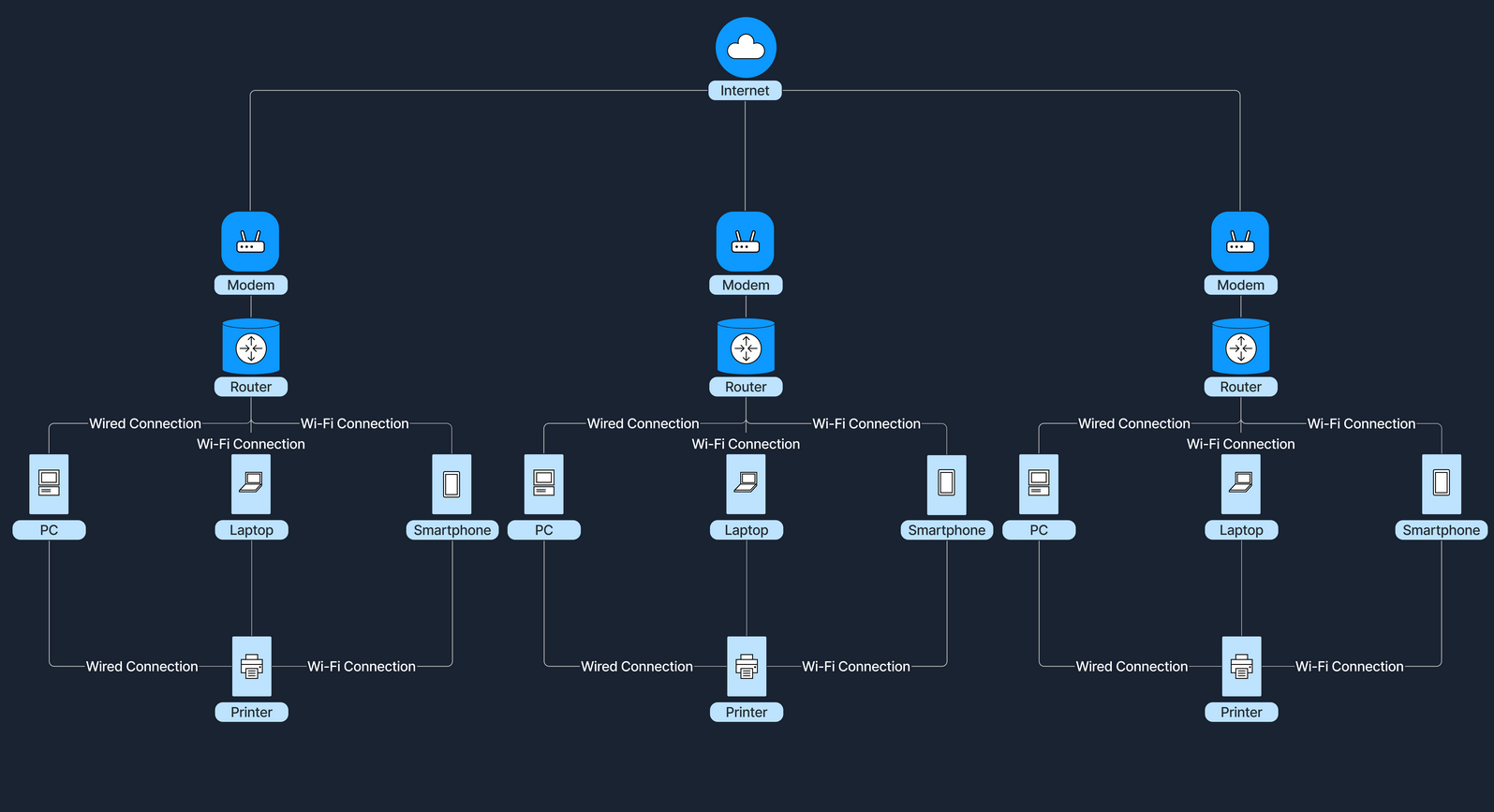
| **Characteristic** | **Description** |
| --- | --- |
| Geographical Scope | Small area: home, school, office building |
| Ownership | Single person/organization |
| Speed | High data transfer rates |
| Media | Wired (Ethernet), wireless (Wi-Fi) |

Example: Home Wi-Fi connecting laptops, smartphones, smart TVs.

**Wide Area Network (WAN)**

| **Characteristic** | **Description** |
| --- | --- |
| Geographical Scope | Large areas: cities, countries, continents |
| Ownership | Multiple organizations or ISPs |
| Speed | Lower than LAN due to longer distances |
| Media | Fiber optics, satellite, leased telecommunication lines |

Example: The Internet, which connects millions of LANs globally.



**LAN vs. WAN**

| **Aspect** | **LAN** | **WAN** |
| --- | --- | --- |
| Size | Small, localized area | Large, broad area |
| Ownership | Single entity | Multiple organizations/ISPs |
| Speed | High | Lower compared to LAN |
| Maintenance | Easier, less expensive | Complex, more costly |
| Example | Home or office network | The Internet |

**How LANs and WANs Work Together**

* **LANs** connect to **WANs** (e.g., Internet) for broader data sharing and communication.
* **Modem** bridges home LAN to ISP’s WAN, converting router signals for transmission over various media (phone lines, cable, fiber).
* **ISPs** provide Internet access to individual and organizational networks, extending each LAN’s reach to global online resources.
* **Business scenario:** Multiple office LANs connect over a WAN for unified communication and centralized resource access across regions.

**Real-World Example**

* Home devices (laptops, smartphones) form a LAN via the router.
* Router connects to ISP’s WAN with a modem, granting access to global online resources.
* In organizations, LANs in different locations connect using WAN, enabling collaboration and data sharing worldwide.

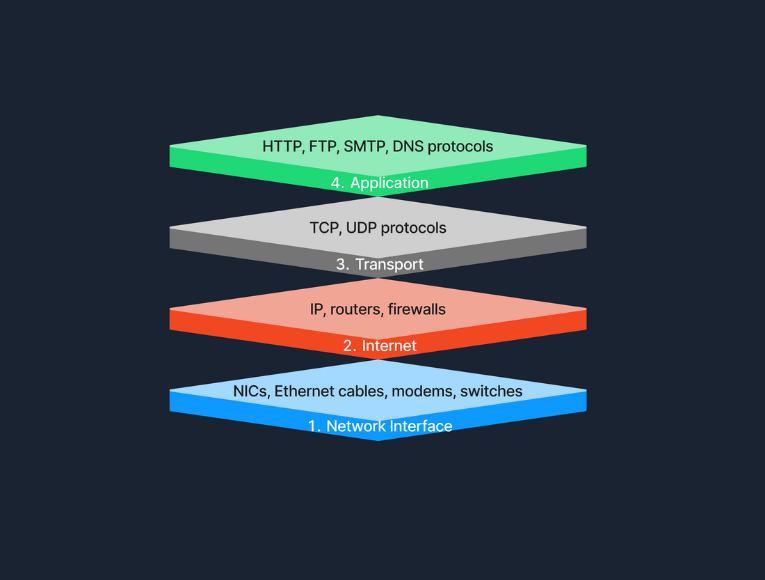
**Network Concepts**

**Introduction**

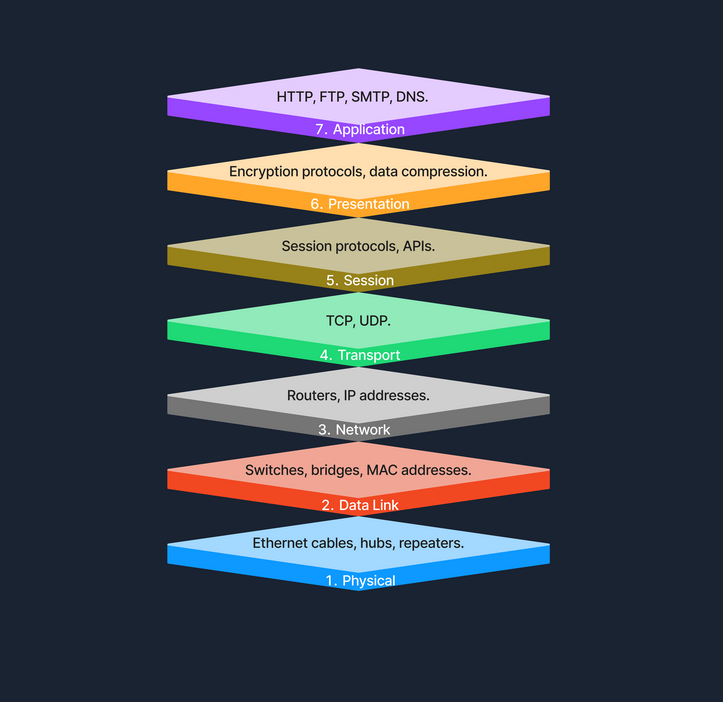
* Modern computing relies on complex networks built atop the **TCP/IP stack**.
* Understanding network models, protocols, and transmission methods is fundamental in technology and cybersecurity.

**OSI Model**

**The Open Systems Interconnection (OSI) Model**:

* Conceptual framework standardizing network functions into **seven layers**.

| **Layer** | **Description** | **Devices/Protocols** |
| --- | --- | --- |
| Physical (Layer 1) | Transmits raw bitstreams over the physical medium (cables, hubs, repeaters). | Ethernet cables, fiber, Wi-Fi |
| Data Link (L2) | Node-to-node transfer, error detection/correction, uses MAC addresses. | Switches, bridges |
| Network (L3) | Handles routing/forwarding of packets, logical addressing (IP). | Routers, IP addresses |
| Transport (L4) | Ensures reliable/unreliable communication (TCP/UDP), segmentation, error recovery. | TCP, UDP |
| Session (L5) | Manages, initiates, and terminates sessions (API coordination, session recovery). | NetBIOS, RPC |
| Presentation (L6) | Data translation, encryption/decryption, compression. | SSL/TLS, JPEG, MPEG, ASCII |
| Application (L7) | High-level APIs, app services (web, email, file transfer, DNS). | HTTP, FTP, SMTP, DNS, SSH |



*Example: Sending a file moves data from Application (L7) down to Physical (L1), with each layer handling specific functions like encryption, error control, and signaling.*

**TCP/IP Model**

**The Transmission Control Protocol/Internet Protocol (TCP/IP) Model:**

* Practical implementation, organizes into four layers:

| **TCP/IP Layer** | **Corresponding OSI Layers** | **Description / Protocols** |
| --- | --- | --- |
| Link | Physical + Data Link | Hardware/media, data framing; Ethernet |
| Internet | Network | Routing, logical addressing; IP, ICMP |
| Transport | Transport | Reliable/unreliable data delivery; TCP, UDP |
| Application | Session + Presentation + Application | End-user services; HTTP, SMTP, FTP |

*Example: Web browsing uses HTTP at the Application Layer, with TCP for reliable transfer, IP for routing, and physical network/media for connectivity.*

**OSI vs TCP/IP**

* OSI: Theoretical, comprehensive—used for understanding concepts.
* TCP/IP: Practical, widely implemented, internet-centric.
* TCP/IP combines higher OSI layers for implementation efficiency.

**Protocols**

| **Protocol** | **Layer(s)** | **Purpose** |
| --- | --- | --- |
| HTTP | Application | Web content delivery in browsers/servers |
| FTP | Application | File transfer between clients/servers |
| SMTP | Application | Email transmission |
| TCP | Transport | Reliable, ordered, error-checked communication |
| UDP | Transport | Fast, connectionless, used for streaming, DNS, etc. |
| IP | Internet | Addressing and routing packets across networks |

**Transmission**

**Types**

* **Analog:** Continuous signals (e.g., radio broadcasts).
* **Digital:** Discrete (binary) signals (e.g., computer networks).

**Modes**

* **Simplex:** One-way (keyboard to computer).
* **Half-Duplex:** Two-way, but not simultaneous (walkie-talkie).
* **Full-Duplex:** Two-way, simultaneous (telephone).

**Media**

| **Media Type** | **Examples** | **Use Case** |
| --- | --- | --- |
| Wired (Twisted Pair) | Ethernet, LAN | Office & home networks |
| Wired (Coaxial) | Cable TV, early LAN | Cable infrastructure, legacy networking |
| Wired (Fiber Optic) | Internet backbone | High-speed, long-distance networking |
| Wireless (Radio) | Wi-Fi, cellular | Wireless LAN, mobile connectivity |
| Wireless (Microwave) | Satellite links | Long-distance communication |
| Wireless (Infrared) | Remote controls | Short-range line-of-sight devices |

**Components of a Network**

**Overview**

* Networks enable devices to communicate, share resources, and access the internet reliably.
* Key components include End Devices, Intermediary Devices, Network Media and Software, and Servers.

**Components and Descriptions**

| **Component** | **Description** |
| --- | --- |
| End Devices | Computers, smartphones, tablets, IoT and smart devices that send/receive data. |
| Intermediary Devices | Switches, routers, modems, and access points that facilitate data flow between end devices. |
| Network Media & Software | Cables (Ethernet, fiber), protocols (TCP/IP, HTTP), network management and firewall software. |
| Servers | Web servers, file servers, mail servers, database servers providing resources and services. |

**Detailed Components**

**End Devices**

* Also called hosts.
* Primary interface for users to access web and resources.
* Connect via wired (Ethernet) or wireless (Wi-Fi).
* Example: A student using a laptop connected to school Wi-Fi to access learning materials.

**Intermediary Devices**

* Facilitate data flow between end devices locally or across networks.
* Perform packet forwarding and route data efficiently.
* Incorporate security features like firewalls.
* Operate at different OSI layers:
  + Routers at Network Layer (Layer 3)
  + Switches at Data Link Layer (Layer 2)
* Example: Home routers and switches connect all household devices to the internet.

**Network Interface Cards (NICs)**

* Hardware enabling network connection.
* Each NIC has a unique MAC address for device identification.
* Wired NICs use Ethernet cables, wireless NICs use Wi-Fi.
* Example: Desktop uses wired NIC; laptop uses wireless NIC.

**Routers**

* Forward data packets between different networks.
* Use routing tables and protocols (**O**pen **S**hortest **P**ath **F**irst, **B**order **G**ateway **P**rotocol) to find efficient paths.
* Manage traffic and enhance security via firewalls and access control.
* Example: Home router connects multiple devices to ISP and manages internet traffic.

**Switches**

* Connect devices within the same LAN.
* Forward data based on MAC addresses to reduce congestion.
* Improve network performance in offices or homes.

**Hubs**

* Basic, outdated devices that broadcast data to all ports.
* Operate at Physical Layer (Layer 1).
* Inefficient and prone to collisions compared to switches.

**Network Media and Software Components**

* **Network Media:** Physical cables (Ethernet, fiber optic) and wireless signals (Wi-Fi, Bluetooth).
* **Software Components:** Protocols and management tools ensuring data transmission and network security.
* Examples: TCP/IP, HTTP, FTP protocols; software firewalls and network monitoring tools.

**Cabling and Connectors**

* Physical cables and connectors (e.g., RJ-45).
* Quality affects performance and reliability.
* Common in office setups connecting computers, switches, and routers.

**Network Protocols**

* Set of rules for data formatting, transmission, reception, and interpretation.
* Examples:
  + TCP/IP: Universal internet communication protocol.
  + HTTP/HTTPS: Web page transfer.
  + FTP: File transfers.
  + SMTP: Email transmission.

**Network Management Software**

* Monitors and manages network performance, configuration, security, and faults.
* Helps administrators maintain efficient and secure networks.
* Example: IT department uses management software to monitor traffic and enforce policies.

**Software Firewalls**

* Security applications on individual devices.
* Monitor and control incoming/outgoing traffic based on rules.
* Protect against unauthorized access and malicious packets.
* Example: Built-in Windows Defender Firewall.

**Servers**

* Powerful machines offering services to clients over a network.
* Host websites, email, files, and applications.
* Enable resource sharing, centralized data management, and authentication.
* Follow client-server model: waiting for requests and responding accordingly.
* Example: Web server delivers a website to your browser on requesting access.

**Conclusion**

* Networking relies on multiple components working together:
  + **End Devices:** Interface for users.
  + **Intermediary Devices:** Manage connections and data flow.
  + **Servers:** Provide shared resources and services.
* This teamwork enables seamless communication powering modern digital interaction.

**Network Communication: Essential Components**

**Core Elements**

* **MAC Addresses:** Unique hardware IDs at Data Link Layer (Layer 2) for local device recognition.
* **IP Addresses:** Logical addresses at Network Layer (Layer 3) for global device identification/routing.
* **Ports:** Numeric identifiers at Transport Layer (Layer 4) for managing multiple services/applications per device.

**MAC Addresses**

**Definition**

* Media Access Control (MAC) address is a hardware-based, globally unique identifier assigned to a device’s network interface card (NIC).
* Format: 48 bits (six pairs of hex digits, e.g. 00:1A:2B:3C:4D:5E).
* First 24 bits: **Organizationally Unique Identifier (OUI)**—assigned to manufacturer.
* Last 24 bits: Unique to device.

**Role in Communication**

* Used within local networks (LAN) to deliver data frames to correct devices.
* Switches forward frames based on MAC address.
* **ARP (Address Resolution Protocol)** links IP addresses to physical MAC addresses.

**Command-Line Example**

* Windows: GETMAC shows MAC addresses of all NICs.

**Example Scenario**

* Computer A (IP: 192.168.1.2, MAC: 00:1A:2B:3C:4D:5E) sends data to Computer B (IP: 192.168.1.5, MAC: 00:1A:2B:3C:4D:5F):
  + Computer A uses ARP to discover B’s MAC.
  + Data sent with destination MAC set to B.
  + Switch delivers to B’s port.

**IP Addresses**

**Definition**

* Unique number assigned to devices for communication over IP-based networks.
* **Layer 3 – Network Layer** (OSI Model).
* Two main types:
  + **IPv4:** 32 bits (e.g. 192.168.1.1).
  + **IPv6:** 128 bits (e.g. 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

**Role in Communication**

* Used by routers to determine how to forward packets between networks.
* Not tied permanently; can be dynamic or static.

**Ports**

**Definition**

* Numeric endpoint for network traffic, identifying specific services/applications.
* **Layer 4 – Transport Layer** (TCP/UDP).
* Allow multiple services on one IP.

**Example**

* Browser to website: uses port 80 (HTTP); secure browsers use port 443 (HTTPS).

**Port Ranges**

| **Range** | **Type** | **Common Usage** |
| --- | --- | --- |
| 0-1023 | Well-Known Ports | Standard services (HTTP/FTP) |
| 1024-49151 | Registered Ports | Dedicated to third-party services |
| 49152-65535 | Dynamic/Private/Ephemeral | Temporary connections, custom use |

**Command-Line Example**

* netstat displays active connections and open ports.

**Example: Web Browsing Packet Flow**

1. **DNS Lookup:** Domain name resolves to IP (e.g. [example.com](http://example.com) → 93.184.216.34).
2. **Data Encapsulation:**
   * Browser makes HTTP request.
   * Encapsulates with TCP, sets port (80 or 443).
   * The packet includes the destination IP.
   * Uses ARP to get router’s MAC for LAN delivery.
3. **Data Transmission:**
   * Data frame sent to router MAC.
   * Router forwards to destination IP.
   * Intermediate routers continue to route by IP.
4. **Server Processing:**
   * Server accepts packet at listening port (80).
   * Handles HTTP request, prepares response.
5. **Response Transmission:**
   * Server sends response to client’s temporary (ephemeral) port chosen at session start.
   * Packet routed back through Internet based on source IP/port.

**Quick References**

* **MAC:** Hardware, local scope, Layer 2. Used for LAN delivery.
* **IP:** Logical, global scope, Layer 3. Used for routing between networks.
* **Ports:** Software, application/service ID, Layer 4. Facilitates multiple services per device.
* **Useful Tools:** GETMAC (Windows), netstat (view connections), ARP, DNS lookup utilities.

**Dynamic Host Configuration Protocol (DHCP)**

**Introduction**

* **DHCP** (Dynamic Host Configuration Protocol) automates the process of assigning IP addresses and other network configuration details (subnet mask, gateway, DNS) to devices on an IP network.
* Automates network setup, reduces manual errors, and simplifies administration—especially for large networks.
* Ensures each connected device receives a **unique IP address**, avoids conflicts, and dynamically reuses addresses when devices disconnect.

**How DHCP Works: The DORA Process**

**DHCP** exchanges between client and server follow a four-step sequence called DORA:

| **Step** | **Description** |
| --- | --- |
| Discover | Device broadcasts a “DHCP Discover” to locate DHCP servers and request network configuration. |
| Offer | DHCP server sends a “DHCP Offer” with an available IP address and network information. |
| Request | Client responds with a “DHCP Request” to accept the offered IP address. |
| Acknowledge | DHCP server sends a “DHCP Acknowledge” confirming the assignment of the IP address to the client. |

**Roles:**

* **DHCP Server:** Device (typically a router or dedicated server) that manages the pool of available IP addresses and settings.
* **DHCP Client:** Any device (e.g., computer, smartphone) that requests network configuration from the DHCP server.

**DHCP Lease and Renewal**

* **IP addresses are assigned for a limited "lease" time.** Configuration stays valid only within this period.
  + Example: A DHCP server gives a smartphone an IP for 24 hours.
* **Renewal:** Before the lease expires, the client must send a renewal request to keep using the IP.
  + Client communicates with the DHCP server and, if approved, extends the lease.
* **Addresses are recycled:** DHCP reclaims unused IPs and assigns them to new clients as needed.

**Example Scenario: DHCP in Action**

1. Alice brings a new laptop to work and connects to Wi-Fi. The laptop has no IP yet.
2. It broadcasts a "DHCP Discover" looking for a DHCP server.
3. The office DHCP server replies with a "DHCP Offer" (e.g., IP: 192.168.1.10).
4. Alice’s laptop sends a "DHCP Request" to accept.
5. The server sends a "DHCP Acknowledge", confirming assignment.
6. The laptop is now configured and network-ready.
7. Before the lease expires, the laptop must request a renewal—otherwise, it could lose network access or be assigned a new address.

**Key Takeaways**

* DHCP is critical for automated network configuration in modern IT environments.
* The DORA process underpins the client-server exchange for IP assignment.
* Leases prevent address exhaustion and help manage dynamic devices.
* **Tools/Commands:** On Linux/Windows, use ipconfig or dhclient to troubleshoot or view current DHCP-assigned details.

**Network Address Translation (NAT)**

**Purpose**

* **Solves IPv4 address exhaustion** by enabling many devices on a local (private) network to share a single public IP address.
* **Adds basic security** by preventing direct access to internal devices from the internet.

**IP Address Types**

| **Type** | **Use** | **Routable on Internet?** | **Example Range or Address** |
| --- | --- | --- | --- |
| Public IP | Global | Yes | 8.8.8.8, 142.251.46.174 |
| Private IP | Local only | No | 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16 |

*Private IP addresses help conserve public IP space and protect internal networks from direct external attacks.*

**What is NAT?**

* **Network Address Translation (NAT):**
  + Performed by routers/gateways.
  + Translates private (internal) IP addresses to a public IP address for packets leaving the local network.
  + Maintains a translation table to track which internal device each outgoing connection belongs to.
  + These Private IP’s are provide based on the RFC 1918

**How NAT Works: Example Flow**

1. Internal device (e.g., Laptop 192.168.1.10) requests an external site (e.g., [www.google.com](http://www.google.com/)).
2. Request goes to the router, which changes the private source IP to its public IP (e.g., 203.0.113.50).
3. Response from Google returns to router’s public IP.
4. Router uses NAT table to map the incoming packet back to the original device (192.168.1.10), using port numbers for session identification.

**Types of NAT**

| **Type** | **Description** | **Use Case** |
| --- | --- | --- |
| Static NAT | 1-to-1 mapping: Each private IP mapped to one public IP | Specific hosted services |
| Dynamic NAT | Many-to-many: Public IPs assigned from a pool as needed | Corporate environments |
| Port Address Translation (PAT/NAT Overload) | Many-to-one: Multiple private IPs share one public IP; sessions distinguished by port numbers | Most common (home/office) |

**Benefits**

* **Conserves IPv4 addresses**—fewer public IPs needed.
* **Security**—internal IPs are not directly visible from the internet.
* **Flexible private addressing**—can use any internal IP scheme.

**Trade-Offs**

* Running public servers behind NAT needs extra config (e.g., port forwarding).
* Some protocols (requiring true end-to-end communication) may break or need workarounds.
* Adds complexity for troubleshooting networking issues.

**Quick Commands/Notes**

* View NAT configuration/use: Check router settings or use firewall tools.
* Port forwarding: Required for hosting public services behind NAT.
* PAT is default for most home networks.

**Domain Name System (DNS)**

**What is DNS?**

* **DNS is the "phonebook" of the internet:** It translates easy-to-remember domain names (e.g., [www.google.com](http://www.google.com/)) into numerical IP addresses (e.g., 93.184.216.34), making websites accessible without memorizing IPs.
* Without DNS, users would need to enter IP addresses manually for every website.

**Domain Names vs. IP Addresses**

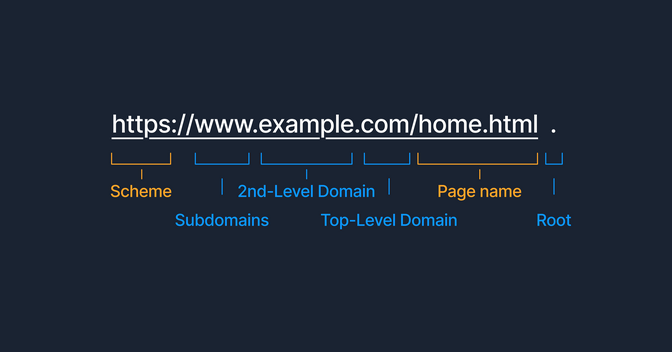
| **Term** | **Description** | **Example** |
| --- | --- | --- |
| Domain Name | Human-friendly website address | [www.example.com](http://www.example.com/) |
| IP Address | Numerical network identifier | 93.184.216.34 |

* **DNS bridges the gap**, letting us use readable names instead of numeric addresses.

**DNS Hierarchy**

DNS is structured like a tree:

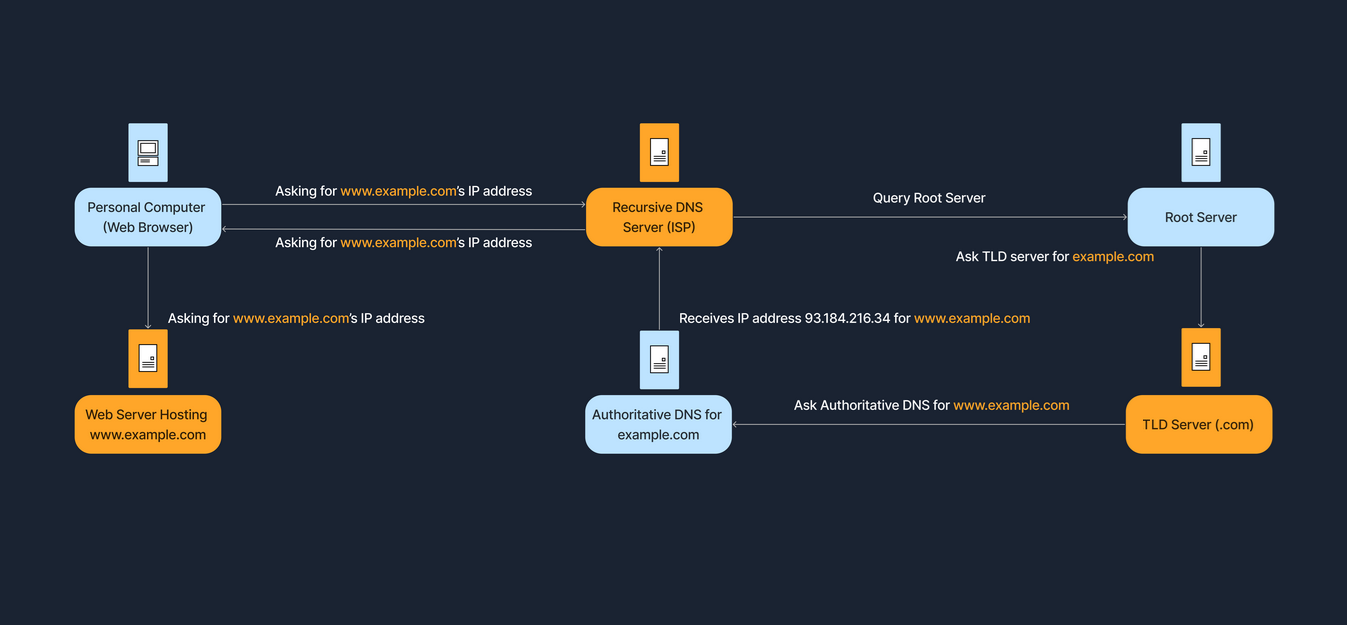
| **Layer** | **Description/Example** |
| --- | --- |
| Root Servers | Top of the hierarchy |
| Top-Level Domains (TLD) | .com, .org, .net, .uk, .de, etc. |
| Second-Level Domains | Domain within TLD ([example.com](http://example.com)) |
| Subdomains/Hostname | Additional levels ([www.example.com](http://www.example.com/), [accounts.google.com](http://accounts.google.com)) |



**DNS Resolution Process (“Domain Translation”)**

1. **User Action:** Type [www.example.com](http://www.example.com/) in the browser.
2. **Local DNS Cache Check:** Computer checks if IP is already stored locally.
3. **Recursive DNS Server Query:** If not cached, computer requests a recursive DNS server (provided by ISP or public DNS like Google).
4. **Root Server Query:** Recursive server queries a root DNS server for direction.
5. **TLD Name Server:** Root server directs to relevant TLD name server (.com, .net, etc.).
6. **Authoritative Name Server:** TLD server points to the authoritative name server for [example.com](http://example.com).
7. **IP Returned:** Authoritative server returns IP address for [www.example.com](http://www.example.com/).
8. **Connection Established:** Recursive server supplies IP to computer; website connection is made.

* **All steps occur within fractions of a second.**
* **Without DNS:** Users would manually enter complex IPs for every site.



**Key Takeaways**

* DNS enables seamless, intuitive access to online resources.
* Hierarchical structure improves scalability, organization, and efficiency.
* Local caching speeds up repeat queries.
* DNS queries can be analyzed for troubleshooting and cybersecurity (e.g., nslookup, dig, host commands).

**Internet Architecture: Models and Key Concepts**

**Overview**

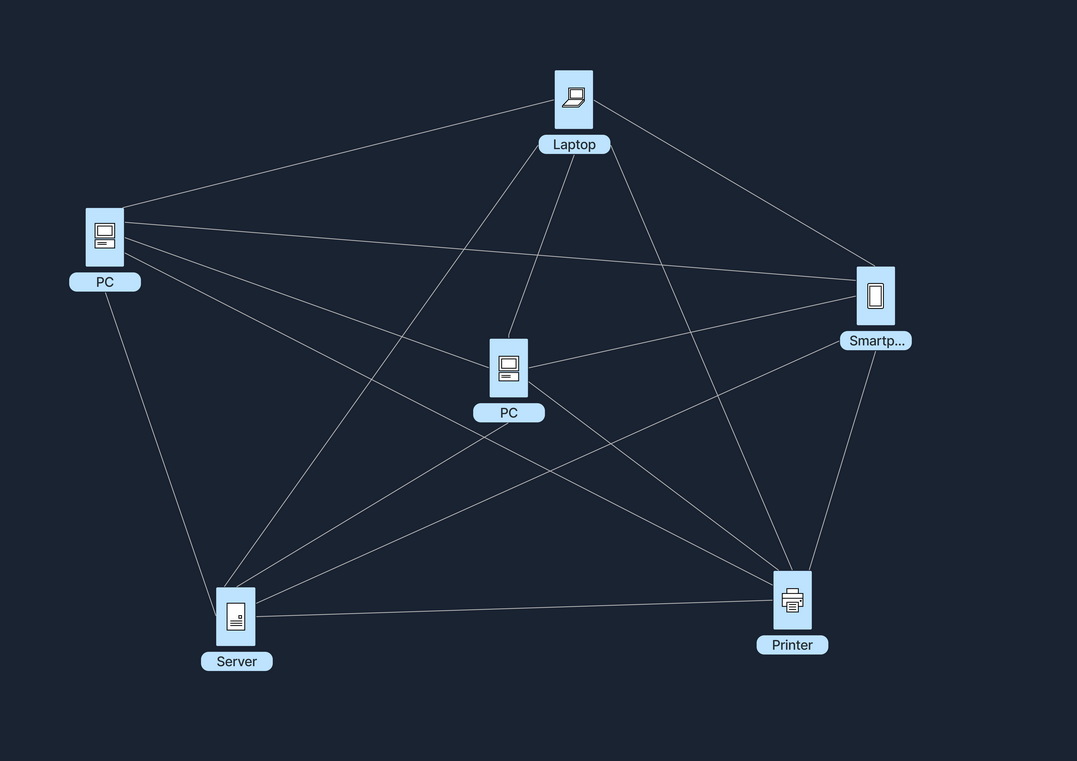
* **Internet Architecture:** Refers to how data is organized, transmitted, and managed. Different models address needs like scalability, security, resilience, and manageability.
* Architectures are often combined for hybrid solutions, each bringing specific strengths and trade-offs.

**1. Peer-to-Peer (P2P) Architecture**

* **Each node acts as both client and server.**
* Nodes share resources directly (files, bandwidth) with no need for a central server.
* Examples: BitTorrent, blockchain platforms.

| **Advantages** | **Description** |
| --- | --- |
| Scalability | Adding peers increases network resources |
| Resilience | No single failure stops the network |
| Cost Distribution | Bandwidth, storage, and load are shared |

| **Disadvantages** | **Description** |
| --- | --- |
| Management | Harder to manage security and updates |
| Reliability | Peer loss can reduce resource availability |
| Security | All peers are exposed to potential vulnerabilities |



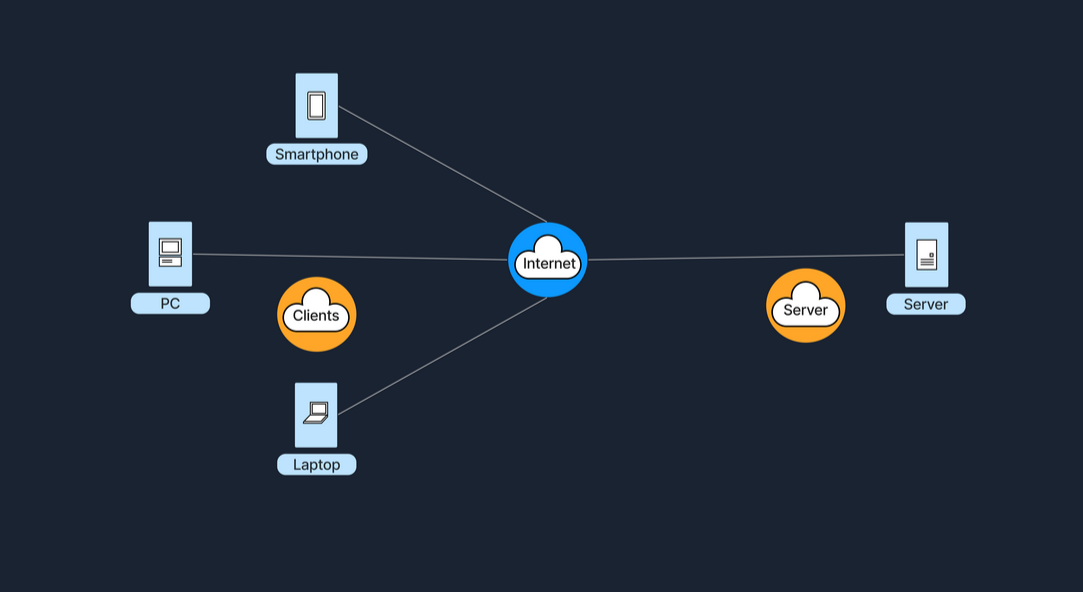
**2. Client-Server Architecture**

* **Clients request, servers respond; server is central hub.**
* Centralized storage, processing, and management.
* Widely used for web, email, business apps.

| **Tier Model** | **Description** |
| --- | --- |
| Single-tier | All roles on one machine; limited, rare |
| Two-tier | Client ↔ Server; common in desktop/database setups |
| Three-tier | Client ↔ Application Server ↔ Database Server; flexible, scalable |
| N-tier | Multiple tiers for large applications; high scalability, distributed |

| **Advantages** | **Description** |
| --- | --- |
| Central Control | Easier management, updates, and policy setting |
| Security | Central enforcement of security policies |
| Performance | Dedicated servers for optimized response |

| **Disadvantages** | **Description** |
| --- | --- |
| Single Point | Server failure impacts all clients |
| Cost | Expensive setup and operation, skilled maintenance required |
| Congestion | High load may overload the server/network |

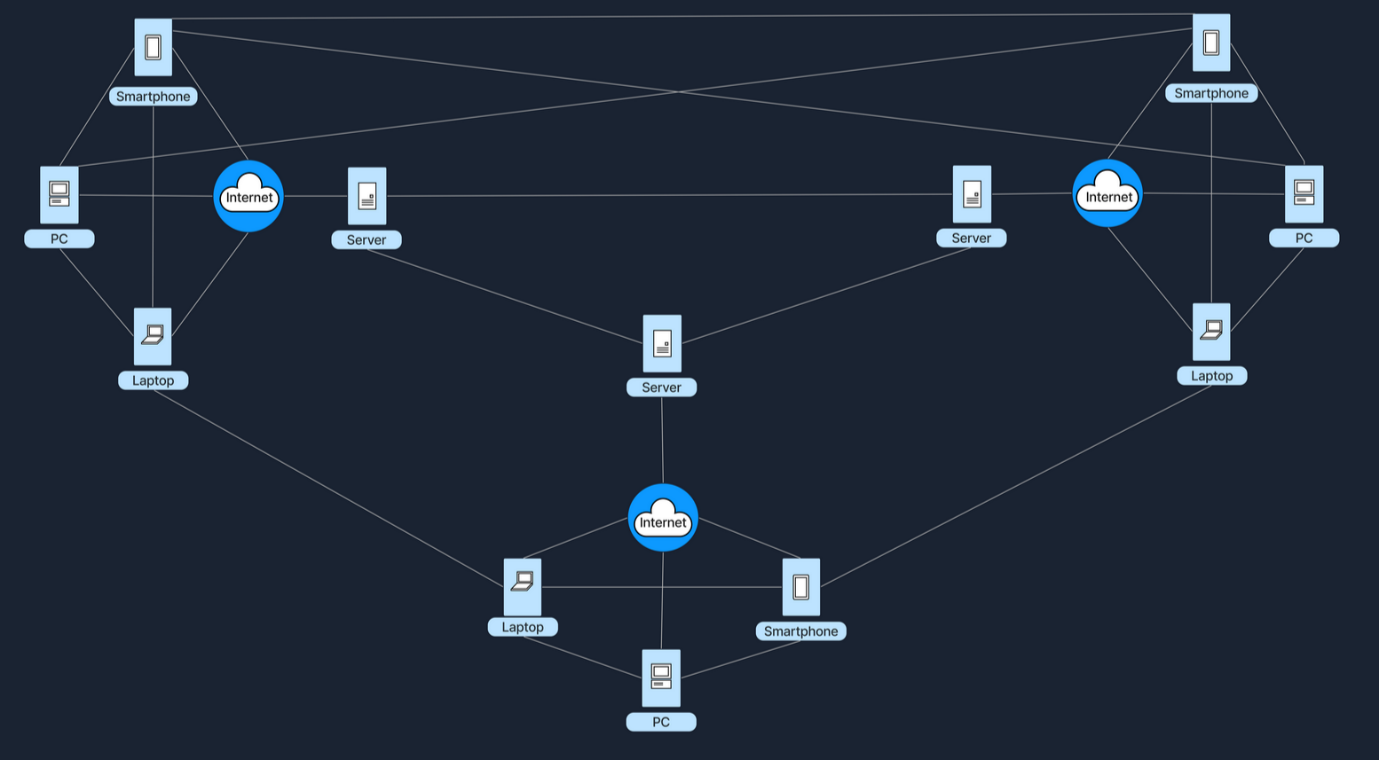


**3. Hybrid Architecture**

* **Mixes client-server (for control/authentication) with P2P (for data sharing).**
* Example: Video conferencing apps—authentication by server, media streams P2P.

| **Advantages** | **Description** |
| --- | --- |
| Efficiency | Peers handle bulk data, server less burdened |
| Central Control | Directory and authentication managed centrally |

| **Disadvantages** | **Description** |
| --- | --- |
| Complexity | Harder to design/implement |
| Partial Central | Central server still a critical point if coordination needed |



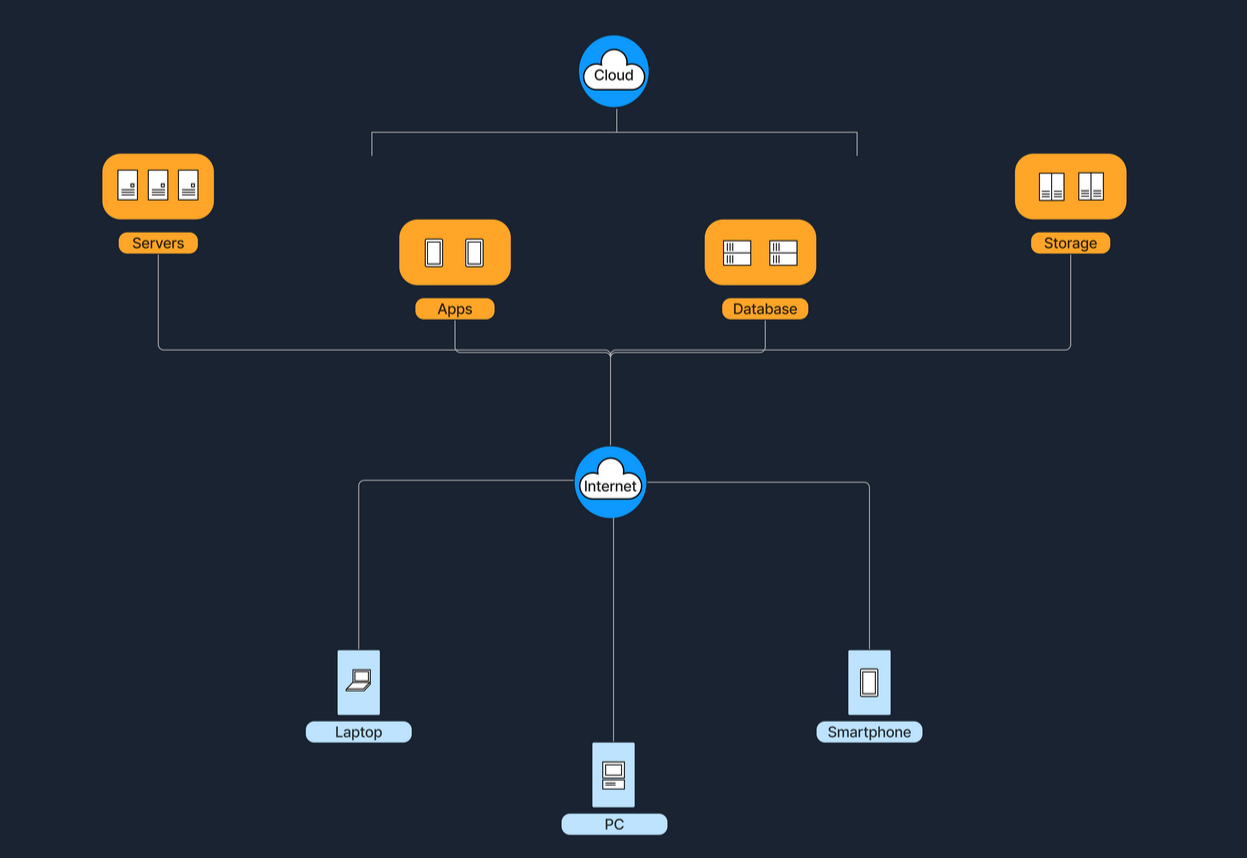
**4. Cloud Architecture**

* **Infrastructure hosted and managed by third-party providers (e.g., AWS, Azure).**
* Users access scalable resources on-demand via the internet.
* Follows a virtualized client-server model.

| **Defining Features** | **Description** |
| --- | --- |
| On-demand self-service | Instantly provision/manage resources |
| Broad network access | Accessible from anywhere on the internet |
| Resource pooling | Underlying resources shared by multiple users |
| Rapid elasticity | Scale up/down quickly as required |
| Measured service | Pay for what you use |

| **Advantages** | **Description** |
| --- | --- |
| Scalability | Add/remove resources easily |
| Cost/Maintenance | Provider handles hardware |
| Flexibility | Access from any internet connection |

| **Disadvantages** | **Description** |
| --- | --- |
| Vendor Lock-in | Difficult to migrate to another provider |
| Security/Compliance | Data privacy is in provider’s hands |
| Connectivity | Needs reliable internet |

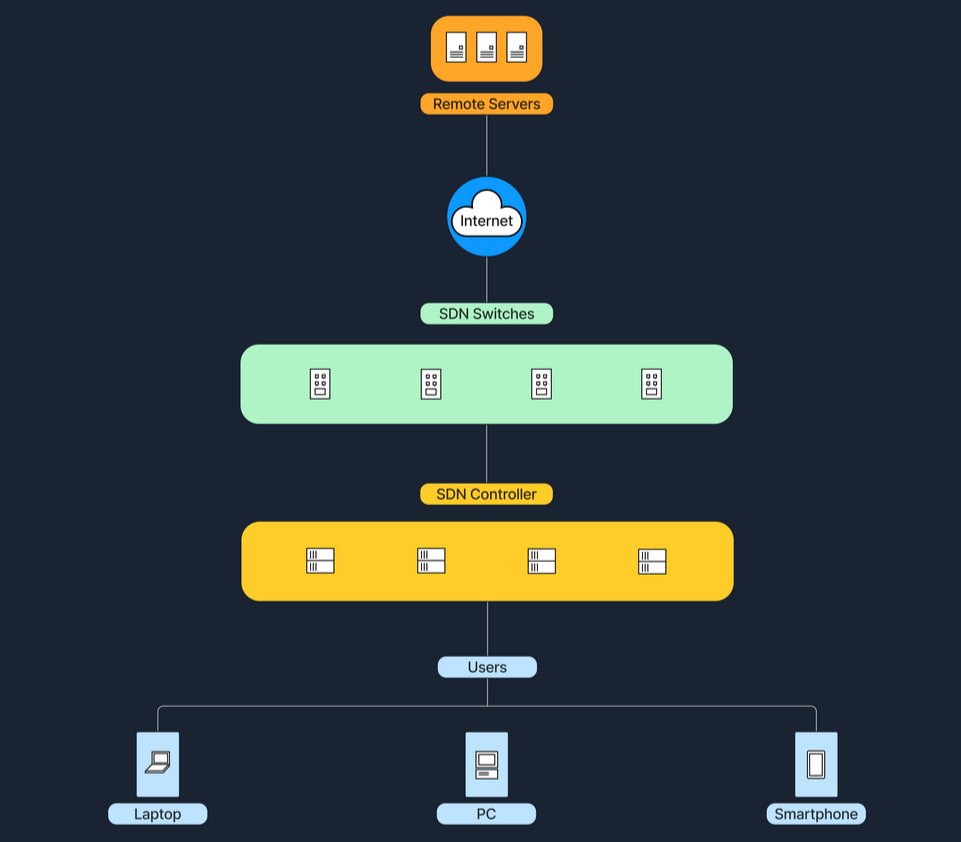


**5. Software-Defined Networking (SDN)**

* **Separates control plane from data plane; centralized programmable control.**
* Network devices follow instructions from a software controller.
* Used by large enterprises and data centers for flexible policy, automation, and scalability.

| **Advantages** | **Description** |
| --- | --- |
| Central Control | Easier to manage and automate the network |
| Programmability | Rapid changes via software, not hardware |
| Scalability | Optimize flows for efficiency and flexibility |

| **Disadvantages** | **Description** |
| --- | --- |
| Vulnerability | Controller failure can disrupt the whole network |
| Complexity | New tools, skills, and implementation needed |



**Key Architecture Comparison**

| **Architecture** | **Centralized?** | **Scalability** | **Ease of Management** | **Typical Use Cases** |
| --- | --- | --- | --- | --- |
| P2P | No/Partial | High | Complex | File-sharing, blockchain |
| Client-Server | Yes | Moderate | Easier (server-based) | Websites, email |
| Hybrid | Partial | Higher than C-S | Complex | Messaging, conferencing |
| Cloud | Centralized (provider) | High | Easier (outsourced) | Cloud apps, SaaS, storage |
| SDN | Centralized (controller) | High | Needs special skills | Datacenters, enterprises |

**Summary Notes**

* **P2P:** Decentralized resource sharing, high scalability, harder to manage.
* **Client-Server:** Centralized, easier admin/security, but costly and a single point of failure.
* **Hybrid:** Combines P2P and client-server; more efficient, but complex.
* **Cloud:** Highly scalable, managed for you, but reliant on providers and internet.
* **SDN:** Centralized, programmable, modern; enables rapid, flexible configuration.

**Wireless Networks**

**Overview**

* Wireless networks use radio waves or wireless signals to connect devices (computers, smartphones, IoT) without physical cables.
* Enable seamless data exchange, internet access, and file sharing with mobility and convenience.

**Advantages and Disadvantages**

| **Advantages** | **Description** |
| --- | --- |
| Mobility | Users can move freely within coverage area |
| Ease of Install | No complex cabling required |
| Scalability | Easier to add new devices than wired networks |

| **Disadvantages** | **Description** |
| --- | --- |
| Interference | Signals affected by walls, electronics, weather |
| Security Risks | Without strong protections, transmissions vulnerable to interception |
| Speed Limitations | Typically slower than wired connections |

**Wireless Router**

* Device combining **routing** and **wireless access point** functions.
* Connects local devices wirelessly and routes traffic to/from the internet.

| **Component** | **Function** |
| --- | --- |
| WAN Port | Connects to internet source (e.g., modem) |
| LAN Ports | Wired connections to local devices |
| Antennae | Transmit and receive wireless signals |
| Processor & Memory | Network management and routing tasks |

**Mobile Hotspot**

* Shares cellular data from a smartphone or dedicated device via Wi-Fi.
* Devices like laptops, tablets, connect to hotspot like normal Wi-Fi.
* Typical range limited to a few meters.
* Security: password protected access.
* Useful for internet access when traditional Wi-Fi unavailable.
* Battery drain can be significant when hotspot active.

**Cell Towers & Cellular Networks**

* **Cell Tower (Cell Site):** Structures with antennas providing cellular coverage in defined geographic “cells.”
* Cells overlap to provide continuous mobile coverage.
* Managed by Base Station Controllers (BSCs) that coordinate handoffs as users move between cells.
* Connected to core networks via backhaul links (fiber optic or microwave).

| **Cell Types** | **Description** |
| --- | --- |
| Macro Cells | Large towers providing wide coverage (rural areas) |
| Micro/Small Cells | Smaller towers filling coverage gaps in urban areas |

**Wireless Frequencies**

| **Frequency Band** | **Use Case** | **Characteristics** |
| --- | --- | --- |
| 2.4 GHz | Older Wi-Fi standards (802.11b/g/n) | Better wall penetration, prone to interference (microwave, Bluetooth) |
| 5 GHz | Newer Wi-Fi (802.11a/n/ac/ax) | Faster speeds, shorter range |
| Cellular Bands | 4G LTE, 5G; ranges from 700 MHz up to 28 GHz+ | Lower frequencies travel far, higher frequencies carry more data but shorter range |

* **Trade-offs:** Lower frequencies for wider range, higher for higher throughput.
* Frequency allocation regulated by authorities (e.g., FCC) to prevent interference.

**Summary: Common Daily Wireless Use**

* **At home:** Wi-Fi router provides internet on 2.4 GHz and 5 GHz to phones, laptops.
* **On the go:** Smartphones connect to internet via nearby cell towers over cellular networks (4G/5G).
* **Traveling:** Mobile hotspots share cellular data with other devices.

**Network Security**

**Core Objectives: The CIA Triad**

* **Confidentiality:** Only authorized users can access data.
* **Integrity:** Data remains accurate and unmodified.
* **Availability:** Network resources are available when needed.

**Firewalls**

**Definition**

* Security device (hardware, software, or both) that monitors and filters network traffic.
* Enforces **firewall policies** or **access control lists (ACLs)** to allow or block traffic.
* Comparable to a security guard verifying access based on rules.

**Operation**

* Analyzes data packets based on IP addresses, ports, protocols.
* Logs traffic, raises alerts on suspicious activity.
* Positioned between the internet and internal network (e.g., integrated in home router or dedicated device in enterprises).

**Types of Firewalls**

| **Type** | **Description** | **Example** |
| --- | --- | --- |
| Packet Filtering Firewall | Operates at Layer 3 & 4; filters via IP, port, protocol | Router ACL allowing only HTTP/HTTPS |
| Stateful Inspection | Tracks connection states; allows return traffic only if part of established session | Stateful firewall allowing inbound only if corresponding outbound request exists |
| Application Layer | Inspects up to Layer 7; analyzes actual content for malicious patterns | Web proxy filtering malicious HTTP requests |
| Next-Generation Firewall (NGFW) | Combines stateful inspection with deep packet inspection, intrusion detection, and application control | Modern firewall inspecting encrypted traffic and blocking malicious IPs |

**Intrusion Detection and Prevention Systems (IDS/IPS)**

**Definition**

* IDS: Monitors network/system activity, detects suspicious/malicious behavior, generates alerts without blocking.
* IPS: Detects and actively blocks malicious traffic in real-time.

**Detection Methods**

| **Technique** | **Description** |
| --- | --- |
| Signature-based | Matches traffic to known attack patterns/signatures |
| Anomaly-based | Detects deviations from normal behavior |

**Types of IDS/IPS**

| **Type** | **Description** | **Example** |
| --- | --- | --- |
| Network-Based (NIDS/NIPS) | Installed at key network points to inspect traffic for multiple devices | Sensor on core switch in data center |
| Host-Based (HIDS/HIPS) | Runs on individual hosts, monitors system and network activity locally | Antivirus or endpoint protection agent |

**Deployment**

* Placed behind firewalls to monitor filtered traffic.
* Deployed in DMZ to protect public-facing servers.
* Installed on endpoints to detect host-specific threats.

**Best Practices for Network Security**

| **Practice** | **Description** |
| --- | --- |
| Define Clear Policies | Use least privilege principle; limit traffic to necessary ports and protocols |
| Regular Updates | Keep firewalls, IDS/IPS signatures, and OS patched and updated |
| Monitor and Log Events | Continuously review logs and alerts for suspicious activity |
| Layered Security | Implement defense-in-depth: combine firewalls, IDS/IPS, antivirus, endpoint protection |
| Periodic Penetration Testing | Simulate attacks to validate and improve security posture |

**Data Flow Example: Accessing a Website**

**1. Connecting to the Internet (Wireless LAN)**

* Laptop discovers and identifies the wireless network (SSID).
* User authenticates using Wi-Fi security (e.g., WPA2/WPA3 password).
* Connection established and DHCP manages IP configuration.

**2. Local Network Configuration (DHCP)**

| **Step** | **Description** |
| --- | --- |
| IP Address Assignment | Laptop requests IP from router’s DHCP server if none assigned. |
| DHCP Acknowledgement | Router assigns a private IP (e.g., 192.168.1.10) with related network info (subnet mask, gateway, DNS server). |

**3. DNS Resolution**

| **Step** | **Description** |
| --- | --- |
| DNS Query | Laptop queries DNS server (ISP or third-party like Google DNS) to find IP for [www.example.com](http://www.example.com/). |
| DNS Response | DNS returns IP address (e.g., 93.184.216.34) for the domain. |

**4. Data Encapsulation and Local Transmission (OSI/TCP-IP Model)**

| **Layer** | **Description** |
| --- | --- |
| Application Layer | Browser creates HTTP/HTTPS request for the webpage. |
| Transport Layer | Request wrapped in TCP segment with source/destination ports (HTTP 80, HTTPS 443). |
| Internet Layer | TCP segment encapsulated into IP packet; source IP is laptop’s private IP, destination is server IP. |
| Link Layer | IP packet placed into Ethernet or Wi-Fi frame with MAC addresses (source: laptop MAC, destination: router MAC). |

* Laptop uses ARP to resolve router’s MAC address and sends frame to the router.

**5. Network Address Translation (NAT)**

* Router replaces the laptop's private IP with its own public IP (e.g., 203.0.113.45).
* Packet is forwarded to the ISP and routed across the internet to the destination server IP.

**6. Server Processing and Response**

* Server firewall checks incoming traffic on port 80/443, allowing legitimate requests.
* Web server software processes the request, assembles the webpage response.
* Response packet source IP: server IP, destination IP: router public IP.
* Router maps incoming packet back to laptop’s private IP using NAT translation.

**7. Decapsulation and Webpage Display**

* Laptop receives the response.
* Strips link-layer (Ethernet/Wi-Fi), IP, and TCP headers.
* Browser renders the webpage using HTML, CSS, JavaScript.

**Summary Data Flow Diagram (Conceptual)**

1. Laptop connects to WLAN → DHCP assigns IP
2. DNS query → DNS response with IP
3. HTTP request encapsulated and sent → ARP resolves MAC
4. Router performs NAT → Packet routed via ISP/internet
5. Server receives → Firewall checks → Web server responds
6. Response routed back → NAT reverses on router
7. Laptop decapsulates → Browser displays webpage

🡨 THE END 🡪