

Introduction to IT Systems for Beginners

Maciej Gowin @ [CoderBrother](#)

All rights reserved

What is the Internet?

The Internet is a **global network of interconnected computers and devices** that communicate using standard protocols (like TCP/IP) to exchange data and information.

Internet: Key Components

- **Networks**

- A collection of smaller networks (e.g., home networks, enterprise networks) connected together.

- **Servers**

- Powerful computers that host websites, applications, and services, allowing clients (like browsers) to access data.

- **Clients**

- Devices like computers, smartphones, and tablets that connect to the Internet to request and retrieve information.

Internet: How It Works

- Data is sent over the Internet in small units called packets.
- Routers and Switches direct packets between devices across different networks.
- DNS (Domain Name System) translates human-readable domain names (like google.com) into IP addresses that computers use to identify servers.

Internet: Key Features

- **Global Connectivity**

- Provides access to resources, information, and services from anywhere in the world.

- **Communication**

- Facilitates services like email, social media, and video conferencing.

- **Information Sharing**

- Allows people and organizations to share knowledge, resources, and media instantly.

Network

- A network is a group of two or more devices connected to share resources and information.
 - Examples include computers, smartphones, printers, and other devices.
- Networks enable communication and resource sharing (e.g., files, internet, printers) between devices.

Basic Types of Networks

- **LAN (Local Area Network):** Connects devices in a small area, like a home or office.
- **WAN (Wide Area Network):** Connects devices across large distances, often using multiple LANs (e.g., the internet).

Basic Components of a Network

Key Devices

- **Router:** Directs data between networks; connects LAN to the internet.
- **Switch:** Connects multiple devices in a LAN, allowing them to communicate with each other.
- **Modem:** Connects to the internet by converting data for transmission over different media (e.g., cable, fiber).

Basic Components of a Network

Types of Connections

- **Wired (Ethernet):** Uses cables for fast and stable connections.
- **Wireless (Wi-Fi):** Allows devices to connect without cables; convenient for mobile devices.

Network Security

- Protects data and devices on a network.
- Common measures include strong passwords, firewalls, and encryption.

IP Address

- An IP (Internet Protocol) Address is a unique identifier assigned to each device on a network. It functions like a mailing address, allowing devices to send and receive data.
- They help route data to the correct device, enabling communication across networks, whether it's local or over the internet.

Types of IP Addresses

IPv4	The most common format, uses four sets of numbers (e.g., 192.168.1.1).
IPv6	Newer format with longer addresses to support more devices (e.g., 2001:0db8:85a3::8a2e:0370:7334).

Public vs. Private IPs

Public IP	Assigned by an Internet Service Provider (ISP) and is visible on the internet.
Private IP	Used within local networks (e.g., home or office) and not accessible directly from the internet.

TCP/IP Model

- TCP/IP (Transmission Control Protocol/Internet Protocol) is a set of networking protocols that governs how data is transmitted over the Internet.
- It is the foundational protocol suite for the modern Internet and is used to connect network devices and ensure data communication.
- It is a simplified version of the ISO/OSI model.

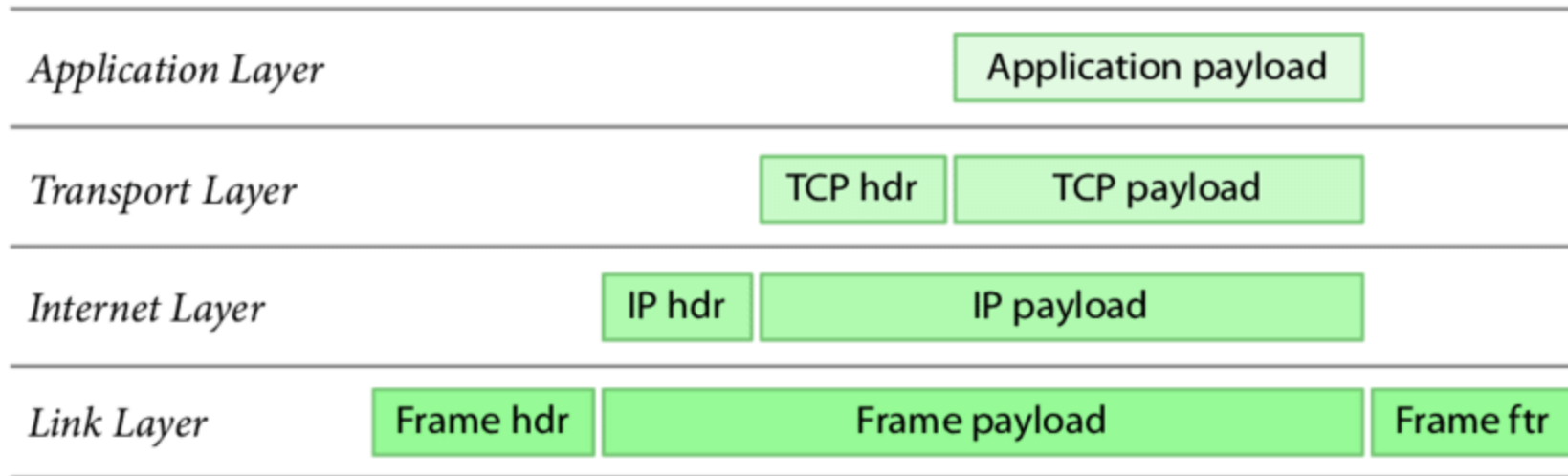
The 4 Layers of the TCP/IP Model

Application Layer

Transport Layer

Internet Layer

Link Layer



TCP/IP Model: Link Layer

- Corresponds to the physical and data link layers in the OSI model.
- Deals with the physical connection between devices and local data transmission (e.g., Ethernet, Wi-Fi).

TCP/IP Model: Internet Layer

- Responsible for addressing, packaging, and routing data.
- IP (Internet Protocol) is the primary protocol used for sending packets across networks (IPv4, IPv6).
- Devices are identified by IP addresses.

TCP/IP Model: Transport Layer

- Provides end-to-end communication and data reliability.
- Key protocols:
 - TCP (Transmission Control Protocol): Ensures reliable, ordered delivery of data.
 - UDP (User Datagram Protocol): Allows faster, connectionless communication without guaranteed delivery.

TCP/IP Model: Application Layer

- Interfaces directly with user applications to provide data services.
- Key protocols:
 - HTTP (web browsing)
 - SMTP (email)
 - FTP (file transfer)
 - DNS (domain name resolution)

TCP/IP Model: Key Features

- **Scalability:** Supports large-scale, global networks like the Internet.
- **Reliability:** Ensures data is transmitted accurately (using TCP) with error checking.
- **Interoperability:** Provides a standardized framework for communication between diverse devices and networks.

What is HTTP?

- HTTP (Hypertext Transfer Protocol) is the foundation of data communication on the World Wide Web.
- It defines how messages are formatted and transmitted, and how web servers and browsers should respond to various commands.
- HTTP typically uses port 80, while its secure counterpart, HTTPS, uses port 443.

FLIGHTS | CAR HIRE | HOTELS | GIFT CARDS

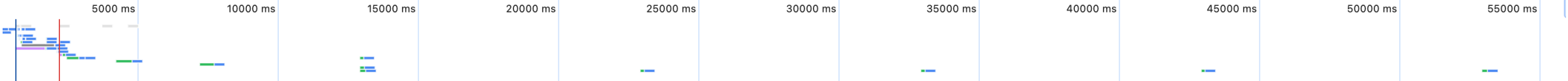
Return trip | One way | Apply promo code



From **Warsaw Chopin** To **Destination**

Search

Filters: Price range | Times | Type of trip



Name	Headers	Preview	Response	Initiator	Timing	Cookies
en	▼ General					
?features=intersectionObserver,cssVars,objectFit	Request URL:	https://www.ryanair.com/gb/en				
runtime.0c9c7f81239711c9.js	Request Method:	GET				
main.9c9f8a83d861b49b.js	Status Code:	● 200 OK				
js?id=UA-153938230-2&l=GTAGdataLayer	Remote Address:	108.138.51.91:443				
i18n.frontend.a11y.accessibility.auth.common-head...	Referrer Policy:	same-origin				
1633.0738771c968efd9f.js	▼ Response Headers					
injected.js	Accept-Ranges:	bytes ✎				
pixels-config.json	Age:	58				

HTTP Characteristics

- **Stateless:** Each request-response cycle is independent, meaning the server does not retain information between requests.
- **Protocol of the Web:** Used to load web pages by transferring hypertext (HTML, CSS, JavaScript, images, etc.).

HTTP Request-Response Model

Request

- A web client (browser) sends an HTTP request to the server.
- Components of a request:
 - **Method** (e.g., GET, POST, PUT, DELETE)
 - **URL (Uniform Resource Locator)**: Specifies the resource being requested.
 - **Headers**: Additional information like browser type, accepted content, etc.
 - **Body**: Contains data (for methods like POST).

HTTP Request-Response Model

Response

- The server processes the request and sends back an HTTP response.
- Components of a response:
 - **Status Code** (e.g., 200 OK, 404 Not Found, 500 Internal Server Error)
 - **Headers:** Metadata (e.g., content type, length).
 - **Body:** The content requested (e.g., HTML file).

Common HTTP Methods

- **GET:**
 - Retrieves data from the server.
 - Example: A user requests a web page or image.
- **POST:**
 - Sends data to the server to create/update resources.
 - Example: Submitting a form (login data, comments).
- **PUT:**
 - Updates an existing resource or creates a new one if it doesn't exist.
- **DELETE:**
 - Requests the server to delete a specified resource.

HTTP Status Codes

Status group	Usage	Example
1xx (Informational)	The request was received, and the process is continuing.	100 Continue
2xx (Success)	The request was successfully received and processed.	200 OK
3xx (Redirection)	The client must take additional action to complete the request.	301 Moved Permanently
4xx (Client Errors)	The request contains bad syntax or cannot be fulfilled.	404 Not Found
5xx (Server Errors)	The server failed to fulfill a valid request.	500 Internal Server Error

HTTP vs. HTTPS

HTTP (Hypertext Transfer Protocol)

- Data is transferred in plain text, which makes it vulnerable to interception.

HTTPS (Hypertext Transfer Protocol Secure)

- A secure version of HTTP that encrypts data using SSL/TLS protocols.
- Provides confidentiality, integrity, and authentication.
- Common for websites handling sensitive data (e.g., banking, login systems).

What is SSL?

SSL (Secure Sockets Layer) is a security protocol that establishes an encrypted link between a web server and a client (typically a browser).

Ensures that all data transmitted remains confidential and integral.

Common Use

- Websites with HTTPS (Hypertext Transfer Protocol Secure) use SSL/TLS to secure online transactions, login credentials, and sensitive information.

How SSL Works

1. Handshake Process

The client and server initiate an SSL connection by exchanging certificates and keys.

2. Encryption

SSL uses asymmetric encryption (public and private keys) to share a symmetric session key, which is then used to encrypt data.

3. Data Transmission

Encrypted data is securely transmitted over the established SSL session.

SSL vs. TLS

TLS (Transport Layer Security) is the successor to SSL with enhanced security features. SSL is often used to refer generically to both SSL and TLS.

SSL Key Benefits

- **Confidentiality:** Encrypts data to prevent unauthorized access.
- **Integrity:** Protects data from being altered during transmission.
- **Authentication:** Uses digital certificates to verify the identity of the server.

SSH (Secure Shell)

SSH (Secure Shell) is a network protocol that allows secure, encrypted communication between two systems over an unsecured network (like the internet).

SSH does not use SSL/TLS for traffic encryption. Even though both protocols have much in common, under the hood SSH has its own transport protocol, independent from SSL.

How SSH Works

- Uses public-key cryptography to authenticate users and encrypt data.
- Typically operates on port 22 by default.

Key Uses of SSH

- **Remote Access:** Securely log into another computer or server remotely.
- **File Transfer:** Securely transfer files between systems (using tools like SCP or SFTP).
- **Tunneling:** Encrypt other network protocols using SSH tunnels for added security.

SSH Example

Basic SSH Command

- Example: ssh `user@192.168.1.10` to log into a server with IP 192.168.1.10.

```
ssh username@hostname
```

SSH: Advantages

- **Security:** All communication is encrypted, protecting data from eavesdropping and man-in-the-middle attacks.
- **Authentication:** Uses passwords or more secure SSH keys for user authentication.
- **Widely Supported:** SSH is available on most operating systems (Linux, macOS, Windows with third-party clients).

What is Remote Desktop?

- Remote Desktop is a technology that allows users to connect to and control a computer from a remote location as if they were physically present.
- Commonly used for remote work, technical support, and accessing resources on another device.

Key Features of Remote Desktop

- **Full Control Over Remote System:** Users can view the remote desktop, open files, run applications, and perform tasks just as they would on a local machine.
- **Cross-Platform Access:** Supports connections across different operating systems, allowing users to connect between Windows, macOS, and Linux, as well as from mobile devices.
- **Secure Connections:** Many remote desktop solutions use encryption protocols (like RDP or VNC with SSL) to ensure secure data transmission.

Key Features of Remote Desktop

- **Resource Sharing:** Enables access to local resources on the remote machine, such as printers, drives, and clipboard sharing, improving productivity.
- **Collaboration:** Allows IT support, troubleshooting, or remote training by enabling multiple users to view or control a session.
- **Popular Remote Desktop Tools:** Examples include Microsoft Remote Desktop (RDP), TeamViewer, AnyDesk, and Chrome Remote Desktop.

Domain Names

A domain name is a unique, human-readable address for a website (e.g., example.com) that maps to an IP address.

Structure

- Top-Level Domain (TLD): The last part (e.g., .com, .org, .net).
- Second-Level Domain: The main part of the domain (e.g., example in example.com).
- Subdomain: Optional prefix before the domain (e.g., www in www.example.com).

Domain Registration

- Domain names are purchased and registered with domain registrars (e.g., GoDaddy, Namecheap), and assigned to IP addresses through DNS records.

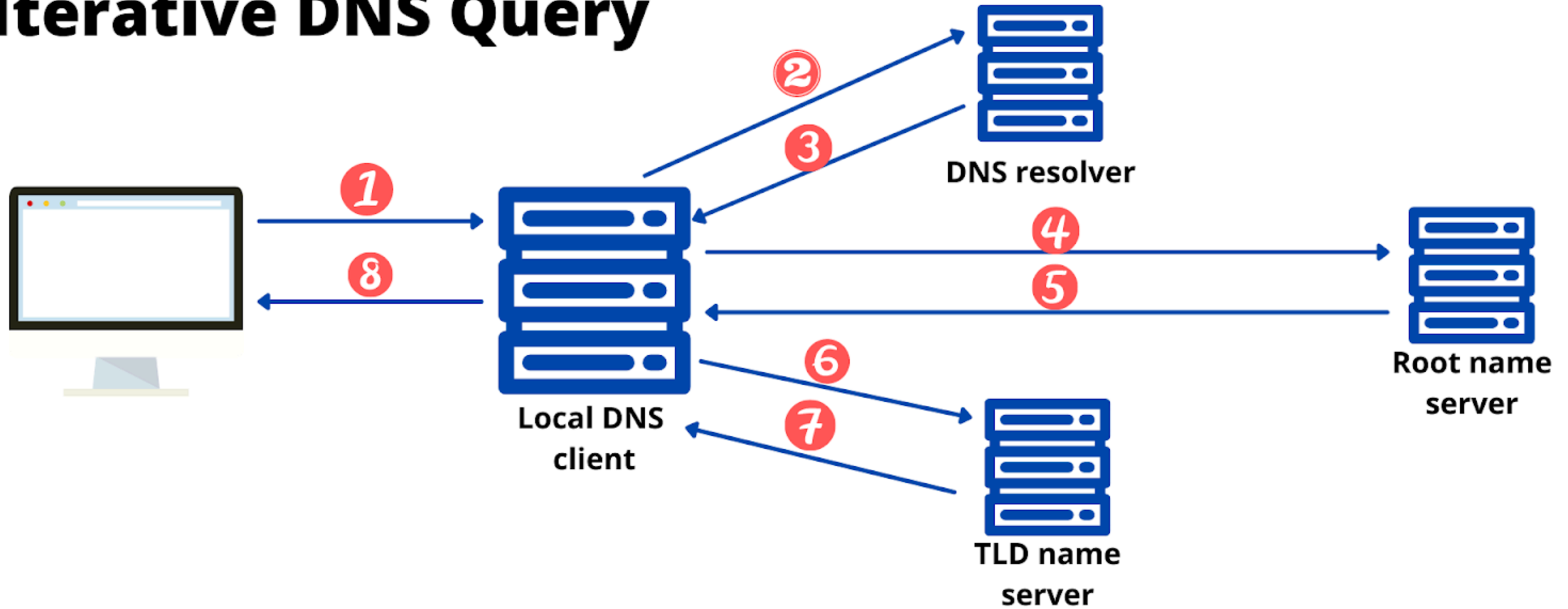
What is DNS (Domain Name System)?

- The Domain Name System (DNS) is a hierarchical system that **translates human-readable domain names** (e.g., example.com) into IP addresses that computers use to identify each other on the internet.
- Allows users to access websites using **memorable domain names** instead of numerical IP addresses.

DNS Key Components:

- **DNS Servers:** Store and manage domain name records.
- **DNS Resolver:** Queries DNS servers to resolve domain names into IPs.
- **Records:** DNS entries that specify how domain names are handled (e.g., A records, CNAMEs).

Iterative DNS Query



How DNS Works

1. User Request

- User types a domain (e.g., `www.example.com`) into a browser.

2. DNS Query

- The DNS resolver contacts DNS servers to find the corresponding IP address for the domain.

How DNS Works

3. Resolution

- DNS Servers check their records:
 - Root DNS: Directs the query to top-level domain servers (e.g., .com, .org).
 - Top-Level Domain (TLD) Server: Directs to the domain's authoritative DNS server.
 - Authoritative DNS Server: Provides the final IP address.

4. IP Address Returned

- The resolver returns the IP address to the browser, which connects to the web server and loads the site.

DNS Records

A Record	Maps a domain name directly to an IP address (IPv4).
AAAA Record	Maps a domain name to an IPv6 address.
MX Record	Directs email to the server specified for the domain.
TXT Record	Holds additional text information, often used for domain verification and security (e.g., SPF, DKIM).
CNAME Record	Maps a domain alias (like <code>www.example.com</code>) to another domain (like <code>example.com</code>).

```
gowinm:~> nslookup www.google.com
Server:          100.64.0.1
Address:         100.64.0.1#53
```

```
Non-authoritative answer:
Name:   www.google.com
Address: 142.250.186.196
```

```
gowinm:~> nslookup www.ryanair.com
Server:          100.64.0.2
Address:         100.64.0.2#53
```

```
Non-authoritative answer:
www.ryanair.com canonical name = d37en9p9pf4plz.cloudfront.net.
Name:   d37en9p9pf4plz.cloudfront.net
Address: 108.138.51.91
Name:   d37en9p9pf4plz.cloudfront.net
Address: 108.138.51.77
Name:   d37en9p9pf4plz.cloudfront.net
Address: 108.138.51.19
Name:   d37en9p9pf4plz.cloudfront.net
Address: 108.138.51.37
```

What is a VPN (Virtual Private Network)?

A VPN (Virtual Private Network) is a technology that **creates a secure, encrypted connection over the internet**, allowing users to access private networks and protect their data.

How VPN Works

- The user's device connects to a VPN server, which encrypts all internet traffic and routes it through a secure tunnel to the internet or a private network.
- The VPN masks the user's IP address, making it appear as if they're accessing the internet from the VPN server's location.

Benefits of VPN

- **Enhanced Security:** Encrypts data, protecting sensitive information from hackers.
- **Privacy:** Hides the user's IP address, providing anonymity online.
- **Remote Access:** Allows secure access to internal network resources from anywhere.
- **Bypass Geo-Restrictions:** Enables access to content restricted by location by making it appear as if the user is connecting from another region.

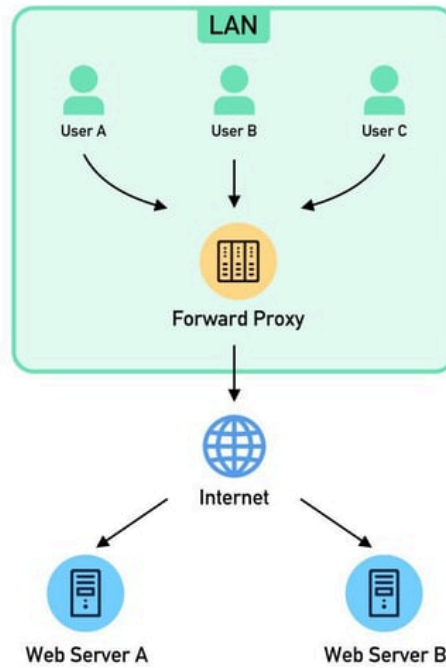
What is a Proxy Server?

A Proxy Server acts as an **intermediary between a user's device and the internet**, forwarding requests from clients to external servers. It masks the user's IP address, providing an additional layer of privacy and control.

Forward Proxy v.s. Reverse Proxy

Forward Proxy

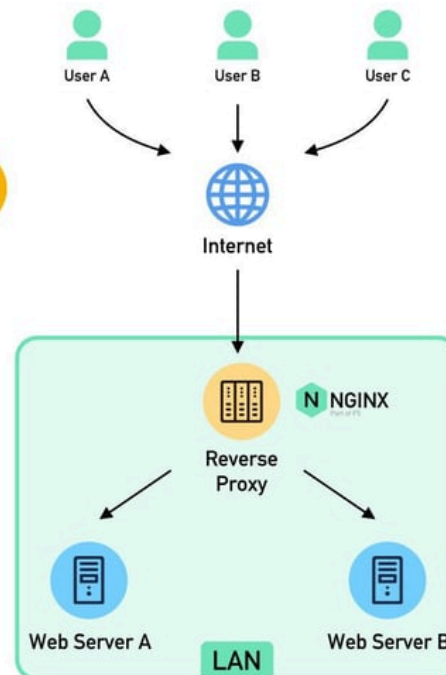
- Avoid browsing restrictions
- Block access to certain content
- Protect user identity online



VS

Reverse Proxy

- Load balancing
- Protect from DDos attacks
- Cache static content
- Encrypt and decrypt SSL communications



Key Functions of a Proxy

- **Privacy and Anonymity:** Hides the client's IP address, allowing anonymous browsing and providing protection against tracking.
- **Content Filtering:** Can block or allow access to specific websites or content, commonly used in organizational or educational networks.
- **Caching:** Stores frequently requested content to speed up access and reduce bandwidth usage.
- **Load Balancing:** Distributes incoming requests across multiple servers, optimizing network performance and preventing server overload.
- **Security:** Filters incoming and outgoing traffic, offering protection against malicious sites and potential threats.

Advantages of Using a Proxy

- **Enhanced Privacy:** Masks user IP addresses for greater anonymity.
- **Access Control:** Allows organizations to control and monitor internet usage.
- **Improved Performance:** Caches frequently accessed content, reducing load times.
- **Security:** Adds a layer of protection against external threats.

Client-Server Model

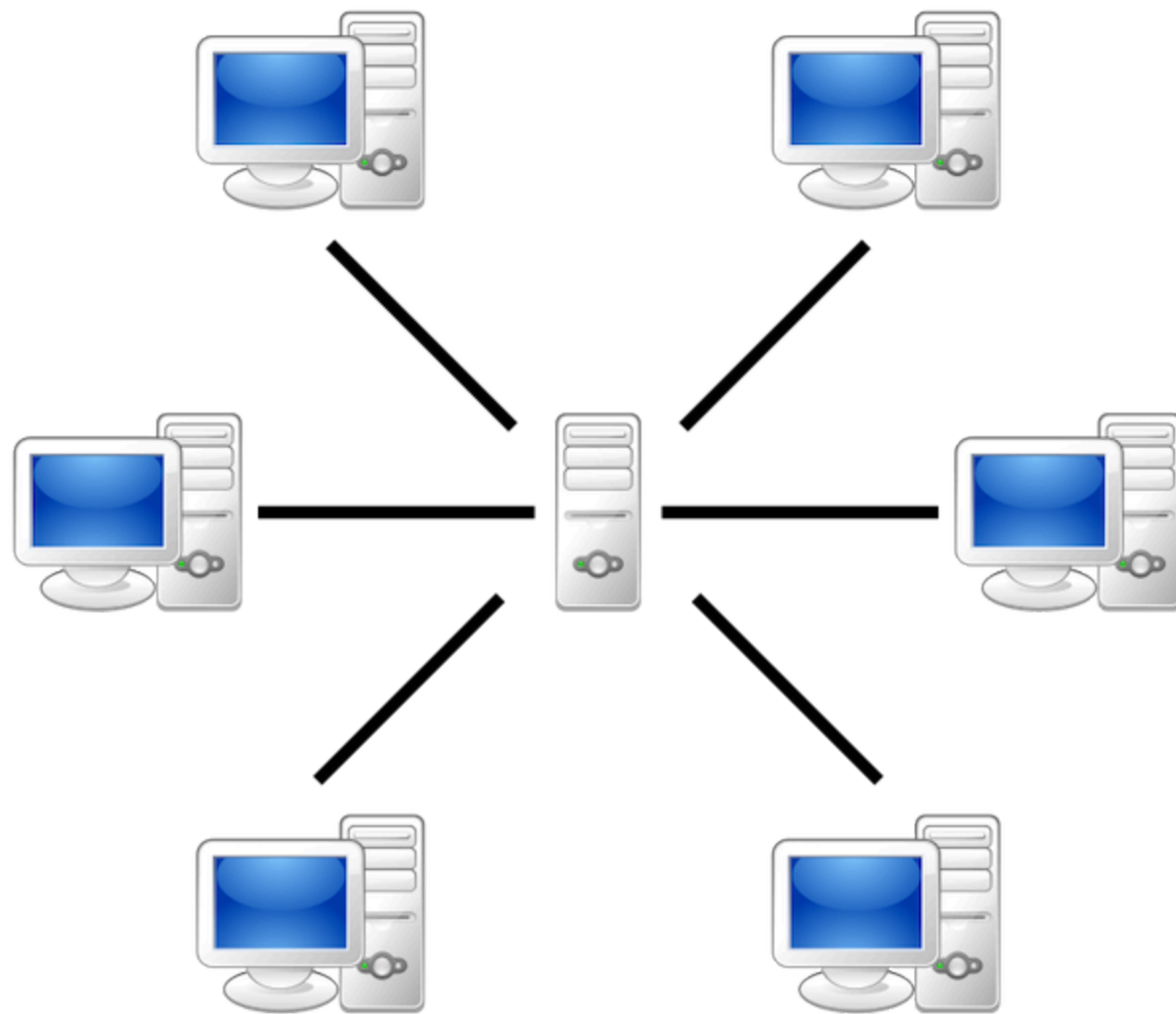
A centralized network architecture where clients (users' devices) request services from a server (central device).

How It Works

- Clients send requests to the server, which processes and responds. Servers manage resources and data storage.
- **Pros:** Reliable, secure, easier to manage and scale.
- **Cons:** Higher setup cost, potential single point of failure.

Examples

- Websites, email servers, cloud services.



Peer-to-Peer (P2P) Model

A decentralized network architecture where all devices, or peers, have equal roles and can both request and provide services.

How It Works

- Peers connect directly to each other, sharing resources without a central server.
- **Pros:** Cost-effective, flexible, efficient for sharing data among users.
- **Cons:** Less secure, harder to manage, reliability depends on peer availability.

Examples

- File-sharing networks (e.g., BitTorrent), local network gaming.

