What is internet?

The internet is a global network of interconnected computers and devices that allows people to communicate, exchange data, and access resources from anywhere in the world. It works as the underlying infrastructure that makes services like the web, email, social media, and cloud storage possible by letting devices talk to each other using standardized protocols.

In web development, the Internet is essential because it enables:

- Hosting and accessing websites and web applications
- Communication between clients and servers
- Use of protocols such as HTTP/HTTPS to transfer web pages and resources

Key points for a web developer:

- The Internet is the backbone, and the **Web(World Wide Web)** is a system of interlinked HTML documents accessed via browsers using the Internet.
- You build websites that are stored on servers; users access these sites through browsers over the Internet.
- Understanding terms like **IP address**, **DNS**, **clients, servers**, and **protocols** (especially **TCP/IP**, **HTTP**, **HTTPS**) is crucial for web development.

if you meant “intranet” that’s a private network used within an organization, different from the public Internet but based on similar technology.

What is HTTP?

- HTTP(Hypertext Transfer Protocol) is the foundational protocol for the web.
- It allows web browsers (clients) and web servers to communicate, exchanging data like HTML pages, images, scripts, etc.
- When you enter a URL starting with http:// , your browser uses HTTP to send a request to the server, then the server responds with the necessary resources to render the web page.
- HTTP works as a strict set of rules a client sends requests (for resources), the server sends back responses (with the requested data).

- Communication over HTTP is in plaintext, meaning data in not encrypted or protected against interception.

What is HTTPS?

- HTTPS(Hypertext Transfer Protocol Secure) builds on HTTP by adding a layer of security using TLS(Transport Layer Security) or the older SSL(Secure Sockets Layer).
- URLs start with https:// the “S” stands for “Secure”.
- HTTPS encrypts all data exchanged between the browser and the server. This protects sensitive information (like logins, payment details, personal data) from eavesdropping or tampering while in transit.
- Websites needing login, forms, payments, or any sensitive data should always use HTTPS. Most browsers now label HTTP-only sites as “Not Secure”.
- Websites prove their identity to users by providing a digital certificate (SSL/TLS certificate), typically verified by a trusted Certificate Authority (CA).
- Technically, the only difference between HTTP and HTTPS is the encryption layer, but it makes a huge impact on security and trust online.

Key Differences

Feature	HTTP	HTTPS
Security	None (plaintext)	TLS/SSL encryption
Data Privacy	Not protected	Protected
Website Identity	No verification	Certificate-based identity
Default Port	80	443
Browser Indicator	None/"Not Secure"	Padlock icon in address bar
Best For	Non-sensitive sites	All sites, especially sensitive data

In modern web development, always use HTTPS for any public facing website, and redirect HTTP traffic to HTTPS. This is best practice for user security and SEO.

What is IP address?

An **IP address (Internet Protocol address)** is a unique numerical identifier assigned to each device connected to a network that uses the Internet Protocol for communication. It serves two primary roles: identifying the device (host) and locating it so that data can be appropriately routed between devices.

How it works in detail:

- **Format and Versions**:

- IPv4 addresses are 32-bit numbers, typically shown as four decimal numbers (octets) separated by dots, e.g., 192.168.1.1.
- IPv6 addresses are 128-bit numbers, shown as eight groups of hexadecimal characters separated by colons, e.g., 2001:0db8:85a3::8a2e:0370:7334. IPv6 was introduced to solve the shortage of IPv4 addresses.

- **Structure**:

  An IP address consists of two parts:
  - **Network portion**: Identifies the specific network on which the device resides.
  - **Host portion**: Identifies the specific device within that network.

    This helps routers determine how to deliver packets efficiently.
- **Types of IP addresses**:
  - **Public IP addresses**, assigned by ISPs, are globally unique and allow devices to communicate over the internet.
  - **Private IP addresses**, used within local networks (homes, offices), are unique only within that network and are managed by routers using Network Address Translation (NAT).
  - IP addresses can be **static** (fixed) or **dynamic** (assigned temporarily via DHCP).
- **Data routing**:

  When a device sends data, it breaks it into packets with headers containing the source and destination IP addresses. Routers read these headers to forward packets across multiple networks toward the destination device. Each router uses routing tables and protocols to find the most efficient path.
- **Management and allocation**:

  The global IP address space is managed by the Internet Assigned Numbers Authority (IANA) and delegated to regional registries, ISPs, and organizations to ensure uniqueness and prevent conflicts.
- **Additional concepts**:
  - **CIDR notation** is used to specify the network size, e.g., 192.0.2.1/24 means the first 24 bits define the network, and remaining bits define hosts.
  - IPv4 supports broadcasting (sending data to all devices on a network), while IPv6 replaces this with multicast and anycast addressing types for efficiency.

For web development, understanding IP addresses is crucial because servers hosting websites have IPs through which clients (browsers) connect. DNS translates domain names people use into these IP addresses, enabling access to websites without needing to remember numerical addresses.

This system is fundamental for reliable, efficient, and unique communication on both local and global networks.

What is DNS?

The **Domain Name System (DNS)** is a hierarchical and distributed system that translates human-readable domain names (like www.example.com) into numerical IP addresses that computers use to locate each other on the internet. This translation allows users to access websites by typing easy-to-remember names instead of complex IP addresses.

Here's how it works for web access:

- When you enter a domain name in your browser, a DNS server looks up the corresponding IP address.
- This IP address directs your browser to the correct web server hosting the website.
- DNS servers operate in a hierarchy: root servers direct requests to top-level domain (TLD) servers (e.g., .com, .org), which then point to authoritative servers that hold the actual records for the domain.

For web development, DNS is crucial because it connects your domain to the IP address of your hosting server, making your website reachable via its domain name.

In essence, DNS is the internet's "phonebook" that simplifies navigation by mapping memorable domain names to technical IP addresses so users can effortlessly access websites.

What is TCP/IP?

TCP/IP (Transmission Control Protocol/Internet Protocol) is a suite of communication protocols used to interconnect network devices on the Internet and other networks. It defines how data is packaged, addressed, transmitted, routed, and received to ensure reliable communication between computers.

- **TCP (Transmission Control Protocol)** is responsible for breaking data into packets, establishing a reliable connection between sender and receiver, ensuring all packets arrive in order and without errors, and managing data flow and retransmissions if packets

are lost. It uses mechanisms like the three-way handshake to establish connections and acknowledgments to confirm delivery.
- **IP (Internet Protocol)** handles addressing and routing packets to their destination across different networks. It ensures that each packet is sent to the correct IP address, though it does not guarantee delivery or order.

Together, TCP/IP provides a standardized, reliable way for devices on diverse networks to communicate, which is fundamental for web browsing, email, file transfers, and virtually all internet applications.

The TCP/IP model breaks communication into layers, allowing data to travel correctly through networks and be reassembled properly at the destination.

For web development, TCP/IP is the underlying technology that enables browsers and servers to send and receive data reliably over the Internet.

What is SSL/TLS?

SSL (Secure Sockets Layer) and **TLS (Transport Layer Security)** are cryptographic protocols used to secure communications over the Internet by encrypting data sent between a client (like a web browser) and a server (such as a website). SSL is the original protocol developed by Netscape in the mid-1990s, but it has since been succeeded by TLS, which is more secure and efficient.

They work by:

- Encrypting data to keep it private and protect it from eavesdropping.
- Authenticating the server (and optionally the client) to ensure identity.
- Ensuring data integrity so the information is not tampered with during transmission.

The process begins with a handshake where the client and server agree on encryption methods and exchange keys for secure communication. This enables HTTPS (HTTP secured by SSL/TLS), which is indicated by a padlock icon in browsers and uses port 443.

In summary, TLS is the modern, improved version of SSL used almost universally today to safeguard sensitive information like passwords, credit card numbers, and personal data during online communication.