How the Internet Works

- **Packet:** A small unit of data that is transmitted over the internet.
- **Router:** A device that directs packets of data between different networks.
- **IP Address:** A unique identifier assigned to each device on a network, used to route data to the correct destination.
- **Domain Name:** A human-readable name that is used to identify a website, such as google.com.
- **DNS:** The Domain Name System is responsible for translating domain names into IP addresses.
- **HTTP:** The Hypertext Transfer Protocol is used to transfer data between a client (such as a web browser) and a server (such as a website).
- **HTTPS:** An encrypted version of HTTP that is used to provide secure communication between a client and server.
- **SSL/TLS:** The Secure Sockets Layer and Transport Layer Security protocols are used to provide secure communication over the internet.

IP is responsible for routing packets to their correct destination, while TCP ensures that packets are transmitted reliably and in the correct order.

When you enter a domain name into your web browser, your computer sends a DNS query to a DNS server, which returns the corresponding IP address. Your computer then uses that IP address to connect to the website or other resource you've requested.

TCP/IP (Transmission Control Protocol/Internet Protocol) is the underlying communication protocol used by most internet-based applications and services. It provides a reliable, ordered, and error-checked delivery of data between applications running on different devices.

When building applications with TCP/IP, there are a few key concepts to understand:

- Ports: Ports are used to identify the application or service running on a device. Each application or service is assigned a unique port number, allowing data to be sent to the correct destination.
- Sockets: A socket is a combination of an IP address and a port number, representing a specific endpoint for communication. Sockets are used to establish connections between devices and transfer data between applications.
- Connections: A connection is established between two sockets when two devices want to communicate with each other. During the connection establishment process, the devices negotiate various parameters such

as the maximum segment size and window size, which determine how data will be transmitted over the connection.

- Data transfer: Once a connection is established, data can be transferred between the applications running on each device. Data is typically transmitted in segments, with each segment containing a sequence number and other metadata to ensure reliable delivery.
- (80 for HTTP and 443 for HTTPS)
-
- Companies called registrars use domain name registries to keep track of technical and administrative information connecting you to your domain name.

HTTP status codes are 3-digit codes most often used to indicate whether an HTTP request has been successfully completed. Status codes are broken into the following 5 blocks:

1. 1xx Informational
2. 2xx Success
3. 3xx Redirection
4. 4xx Client Error
5. 5xx Server Error

The “xx” refers to different numbers between 00 and 99.

Status codes starting with the number ‘2’ indicate a success. For example, after a client requests a webpage, the most commonly seen responses have a status code of ‘200 OK’, indicating that the request was properly completed.

If the response starts with a ‘4’ or a ‘5’ that means there was an error and the webpage will not be displayed. A status code that begins with a ‘4’ indicates a client-side error (it is very common to encounter a ‘404 NOT FOUND’ status code when making a typo in a URL). A status code beginning in ‘5’ means something went wrong on the server side. Status codes can also begin with a ‘1’ or a ‘3’, which indicate an informational response and a redirect, respectively.

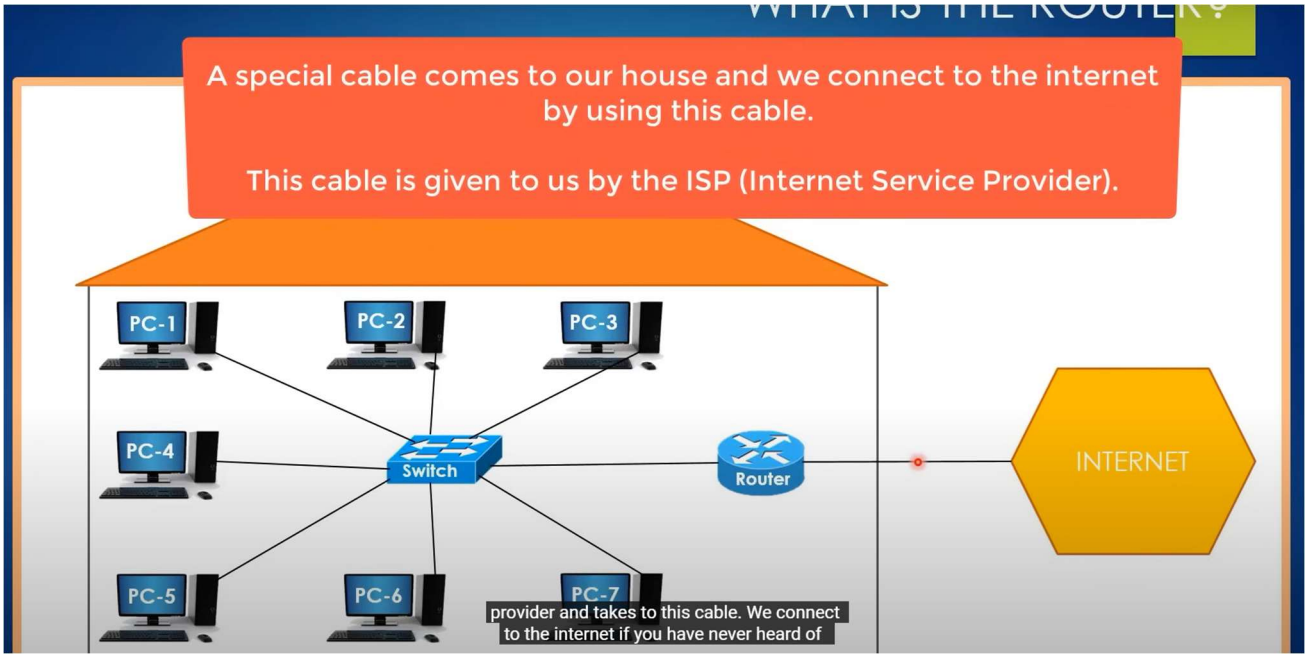
Types of Web Hosting:

1. **Shared Hosting**: In shared hosting, multiple websites are hosted on a single server. Resources such as CPU, RAM, and bandwidth are shared among all the websites on that server. It's a cost-effective option suitable for small websites with low to moderate traffic.
2. **Virtual Private Server (VPS) Hosting**: VPS hosting provides a virtualized server environment where each website is hosted on its own virtual server with dedicated resources. It offers more control, flexibility, and scalability compared to shared hosting, making it suitable for websites that require more resources or customization.
3. **Dedicated Server Hosting**: With dedicated server hosting, you get an entire physical server dedicated to your website. This provides maximum control, performance, and security but comes at a higher cost. Dedicated hosting is ideal for large websites with high traffic volumes and resource-intensive applications.
4. **Cloud Hosting**: Cloud hosting utilizes a network of virtual servers to distribute resources and load across multiple servers. It offers scalability, reliability, and flexibility, as resources can be scaled up or down based on demand. Cloud hosting is suitable for websites with fluctuating traffic or those that require high availability.
5. **Managed Hosting**: Managed hosting services provide comprehensive support and management of the server infrastructure, including software updates, security monitoring, backups, and more. It allows website owners to focus on their content or business while the hosting provider takes care of the technical aspects.
6. **WordPress Hosting**: WordPress hosting is optimized specifically for hosting WordPress websites. It often includes features such as one-click WordPress installation, automatic updates, caching, and specialized support for WordPress-related issues.
7. **E-commerce Hosting**: E-commerce hosting is tailored for hosting online stores and comes with features such as SSL certificates, payment gateway integration, shopping cart software, and scalability to handle high volumes of transactions.

The use of switch or an access point

If pc 1 can send a packet to pc6 then it means that these two computer can communicate with each other and they are on the same network.

The Router is a device for a computer to be connected to the internet.



Wi-fi is also known as wireless router.

A LAN may use a switch but a WAN uses Rogers.

Bandwidth – Maximum Transmission Capacity Of A Device

There are 4 DNS servers involved in loading a webpage:

- DNS recursor - The recursor can be thought of as a librarian who is asked to go find a particular book somewhere in a library. The DNS recursor is a server designed to receive queries from client machines through applications such as web browsers. Typically the recursor is then responsible for making additional requests in order to satisfy the client's DNS query.

- **Root nameserver** - The root server is the first step in translating (resolving) human readable host names into IP addresses. It can be thought of like an index in a library that points to different racks of books - typically it serves as a reference to other more specific locations.

- TLD nameserver - The top level domain server (TLD) can be thought of as a specific rack of books in a library. This nameserver is the next step in the search for a specific IP address, and it hosts the last portion of a hostname (In example.com, the TLD server is "com").

- Authoritative nameserver - This final nameserver can be thought of as a dictionary on a rack of books, in which a specific name can be translated into its definition. The authoritative nameserver is the last stop in the nameserver query. If the authoritative name server has access to the requested record, it will return the IP address for the requested hostname back to the DNS Recursor (the librarian) that made the initial request.

5 major types of browser on Desktop

- Chrome
- Internet Explorer
- Firefox
- Safari
- Opera

5 major types of browser on Mobile

- Android Browser
- iPhone - Safari
- Opera Mini
- Opera Mobile
- UC Browser

How a message is sent over the internet

Sending a message over the Internet involves several steps and components working together to ensure the data reaches its destination correctly. Here's a detailed breakdown:

1. Creation and Preparation

- **Application Layer:** The message is created using an application (e.g., email client, messaging app). The application formats the message into a protocol like HTTP, SMTP, or FTP.
- **Transport Layer:** The message is broken into smaller chunks called packets. The Transmission Control Protocol (TCP) is commonly used to ensure reliable transmission. Each packet is numbered and includes source and destination ports.

2. Addressing and Routing

- **Network Layer:** Each packet is assigned an IP address, which includes the sender's IP address and the recipient's IP address. The Internet Protocol (IP) is used for this purpose.
- **Data Link Layer:** Each packet is encapsulated into a frame, which includes MAC addresses for physical network interface identification.

3. Transmission

- **Physical Layer:** The frames are converted into electrical, optical, or wireless signals and transmitted over the network medium (e.g., Ethernet cable, fiber optics, Wi-Fi).

4. Routing through Networks

- **Local Network:** The packets travel through the local network, passing through switches and possibly routers.
- **ISP Network:** The packets reach the ISP, which uses routers to direct the packets to their destination based on the IP addresses.
- **Internet Backbone:** The packets may traverse multiple interconnected networks and backbone providers. Routers at each hop decide the best path based on routing tables and protocols like BGP (Border Gateway Protocol).

5. Delivery and Reconstruction

- **Recipient's ISP:** The packets reach the recipient's ISP, which directs them to the appropriate local network.
- **Local Network and Device:** The packets travel through the local network to the recipient's device.
- **Transport Layer:** TCP reassembles the packets in the correct order, checks for errors, and requests retransmission of any missing packets.
- **Application Layer:** The reassembled message is passed to the application layer, where it is interpreted and displayed to the user.

6. Acknowledgement (for TCP)

- **ACK Packets:** The recipient's device sends acknowledgment packets back to the sender to confirm successful receipt.

Example: Sending an Email

1. **Compose Email:** You write and send an email using an email client.
2. **SMTP Protocol:** The email client uses the SMTP protocol to send the email to the email server.
3. **Packetization:** The email is broken into packets, each containing part of the message and control information.
4. **Routing:** The packets are routed through various networks and ISPs, guided by routers that determine the best path to the destination.
5. **Reassembly:** The recipient's email server reassembles the packets into the original email.
6. **POP/IMAP Protocol:** The recipient retrieves the email using POP or IMAP protocols.

This process involves multiple layers of the OSI (Open Systems Interconnection) model, ensuring that data is transmitted efficiently and accurately across the complex web of interconnected networks that make up the Internet.

The *Internet* is an infrastructure, whereas the *Web* is a service built on top of the infrastructure

Sandboxing

It isolates websites from a user's operating system and other programs. If a website tries to run malicious code, it remains within the sandbox environment, protecting the user's device and data.

Networking Basics

1. Servers and Clients:

- **Server:** A computer or system that provides resources, data, services, or programs to other devices (clients) over a network.
- **Client:** A device (like your computer or phone) that requests resources or services from a server.
- Example: When you type a URL, your browser (client) sends a request to the website's server.

2. Protocols:

- Rules that govern data exchange over a network.
- Common protocols:
  - **HTTP/HTTPS:** For web page communication.
  - **FTP:** For transferring files.
  - **SMTP/IMAP:** For sending/receiving emails.
  - **TCP/IP:** The foundation of all internet communication, ensuring reliable data delivery.

DNS & IPs

1. DNS (Domain Name System):

- Translates human-readable domain names (like google.com) into IP addresses (like 142.250.72.14) so that computers can understand and connect to them.
- Analogy: Think of DNS as a phonebook for the internet.

2. IP (Internet Protocol):

- The unique address assigned to each device on the internet.
    - **IPv4:** 32-bit addresses (e.g., 192.168.1.1).
    - **IPv6:** 128-bit addresses to accommodate the growing number of devices.

How DNS Works:

1. You type www.example.com in your browser.
2. The browser contacts a DNS server to get the corresponding IP.
3. Once the IP is found, your device connects to the server hosting the website.

Data Flow

1. HTTP/HTTPS:

- **HTTP (Hypertext Transfer Protocol):** The protocol for transferring web pages.
- **HTTPS (Secure HTTP):** Encrypted HTTP using SSL/TLS for secure communication.
    - Ensures data integrity, encryption, and authentication.

2. Packets:

- Data sent over the internet is broken into smaller units called packets.
- Each packet includes:
    - **Header:** Contains metadata like source, destination, and sequence number.
    - **Payload:** The actual data being transmitted.

3. Firewalls:

- Security systems that monitor and control incoming and outgoing network traffic based on security rules.
- Protects networks from unauthorized access and cyber threats.

Why is this essential for web development?

1. **Debugging:** Understanding how data flows helps troubleshoot network errors.
2. **Optimization:** Optimize your websites for faster loading and better security.
3. **Security:** Knowledge of protocols like HTTPS ensures safe user experiences.

4. **Scalability:** Build robust systems by understanding client-server architecture.