How does the Internet Work?

As a web developer, it’s important to have a solid understanding of what the internet is and how it works. To build effective, secure, and scalable applications and services, you need to have a solid understanding of how the internet works and how to leverage its power and connectivity.

Introduction to the internet

Before understanding the internet, it’s important to know what a *Network* is. Network is a group of computers or other devices connected to each other, and all these networks connected together form the internet.

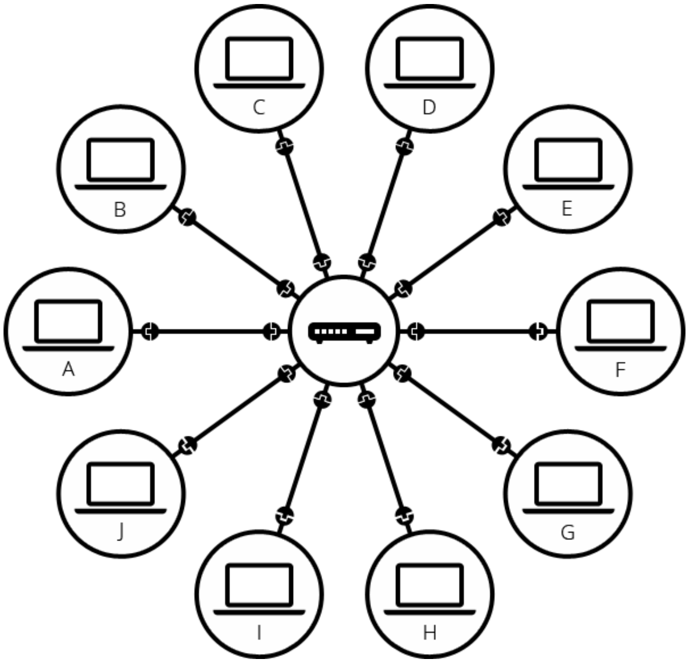

Figure 1 - Network, in the middle we have the router, and the router is connected with other ten devices listed from A to J.

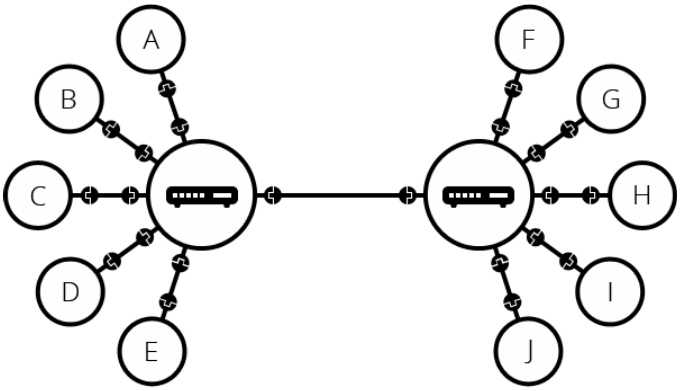

Figure 2 - Here we have two networks, and the two networks are connected with each other;

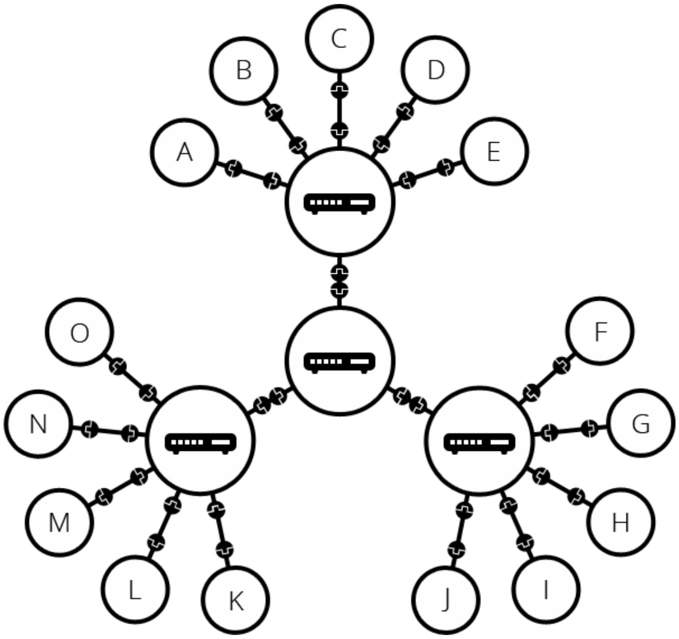

Figure 3 - Here we have three networks connected to a router, making one network of three other networks, all these networks connected together form the internet;

Today, the internet is an essential part of modern life, used by billions of peoples, to access information, communicate with friends and family, conduct business, and more.

How the Internet Works: Overview

At a high level, the internet works by connecting devices and computer systems together using a set of protocols. These protocols define how information is exchanged between devices and ensure that data is transmitted reliably and securely.

The core of the internet is a global network of interconnected routers, which are responsible for directing traffic between different devices and systems. When you send data over the internet, it’s broken up into small packets that are sent from your device to a router. The router examines the packet and forwards it to the next router in the path towards its destination. This continues until the packet reaches its final destination.

To ensure that packets are sent and received, the internet uses a variety of protocols, including the Internet Protocol (IP) and Transmission Control Protocol (TCP). IP is responsible for routing packets to their correct destination, while TCP ensures that packets are transmitted reliably and in the correct order.

In addition to these core protocols, there are a wide range of other technologies and protocols that are used to enable communication and data exchange over the internet, including the Domain Name System (DNS), the Hypertext Transfer Protocol (HTTP), and the Secure Sockets Layer / Transport Layer Security (SSL/TLS) protocol.

Basics Concepts and Terminology

To understand the internet, it’s important to be familiar with basics concepts and terminology:

- **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;

The Role of Protocols in Internet

Protocols play a critical role in enabling communication and data exchange over the internet. A protocol is a set of rules and standards that define how information is exchanged between devices and systems.

There are many different protocols used in internet communication, including the Internet Protocol (IP), the Transmission Control Protocol (TCP), the User Datagram Protocol (UDP), the Domain Name System (DNS), and many others.

IP is responsible for routing packets of data to their correct destination, while TCP and UDP ensure that packets are transmitted reliably and efficiently. DNS is used to translate domain names into IP addresses, and HTTP is used to transfer data between clients and servers.

One of the key benefits of using standardized protocols is that they allow devices and systems from different manufacturers and vendors to communicate with each other seamlessly. For example, a web browser developed by one company can communicate with a web server developed by another company, as long as they both adhere to the HTTP protocol.

Understanding IP Addresses and Domain Names

IP addresses and domain names are both important concepts to understand when working with the internet.

An IP address is a unique identifier assigned to each device on a network. It’s used to route data to the correct destination, ensuring that information is sent to the intended recipient. IP addresses are typically represented as a series of four numbers separated by periods, such as “192.168.1.1”.

Domain names, on the other hand, are human-readable names used to identify websites and other internet resources. They’re typically composed of two or more parts, separated by periods. The “google.com” is a good example of a domain name. Domain names are translated into IP addresses using the Domain Name System (DNS).

DNS is a critical part of the internet infrastructure, responsible for translating domain names into IP addresses. When you enter a domain name into your 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.

Introduction to HTTP and HTTPS

HTTP (Hypertext Transfer Protocol) and HTTPS (Hypertext Transfer Protocol Secure), are two of the most commonly used protocols in internet-based applications and services.

HTTP is the protocol used to transfer data between a client and a server. When you visit a website, your web browser sends an HTTP request to the server, asking for the webpage or other resource you’ve requested. The server then sends an HTTP response back to the client, containing the requested data.

HTTPS is a more secure version, which encrypts the data being transmitted between the client and server using SSL/TLS encryption. This provides an additional layer of security, helping to protect sensitive information such as login credentials, payment information, and other personal data.

When you visit a website that uses HTTPS, your web browser will display a padlock icon in the address bar, indicating that the connection is secure. You may also see the letters “https” at the beginning of the website address, rather than “http”.

Building Applications with TCP/IP

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;

When building applications with TCP/IP, you'll need to ensure that your application is designed to work with the appropriate ports, sockets, and connections. You'll also need to be familiar with the various protocols and standards that are commonly used to TCP/IP, such as HTTP, FTP (File Transfer Procotol), and SMTP (Simple Mail Transfer Protocol). Understanding these concepts and protocols is essential for building effective, scalable, and secure internet-based applications and services.

Securing Internet Communication with SSL/TLS

As we discussed earlier, SSL/TLS is a protocol used to encrypt data being transmitted over the internet. It is commonly used to provide secure connections for applications such as web browsers, email clients, and file transfer programs.

When using SSL/TLS to secure internet communication, there are a few key concepts to understand:

- **Certificates:** SSL/TLS certificates are used to establish trust between the client and server. They contain information about the identity of the server and are signed by a trusted third party (a Certificate Authority) to verify their authenticity;
- **Handshake:** During the SSL/TLS handshake process, the client and server exchange information to negotiate the encryption algorithm and other parameters for the secure connection;
- **Encryption:** Once the secure connection is established, data is encrypted using the agreed-upon algorithm and can be transmitted securely between the client and server;

When building internet-based applications and services, it’s important to understand how SSL/TLS works and to ensure that your application is designed to use SSL/TLS when transmitting sensitive data such as login credentials, payment information, and other personal data. You’ll also need to ensure that you obtain and maintain valid SSL;TLS certificates for your servers, and that you follow best practices for configuring and securing your SSL/TLS connections. By doing so, you can help protect your users data and ensure the integrity and confidentiality of your application’s communication over the internet.

The Future: Emerging Trends and Technologies

The internet is constantly evolving, and new technologies and trends are emerging all the time. As a developer, it’s important to stay up-to-date with the latest developments in order to build innovative and effective applications and services.

Here are some of the emerging trends and technologies that are shaping the future of the internet:

- **5G:** 5G is the latest generation of mobile network technology, offering faster speeds, lower latency, and greater capacity than previous generations. It is expected to enable new use cases and applications, such as autonomous vehicles and remote surgery.
- **Internet of Things (IoT):** IoT refers to the network of physical devices, vehicles, home appliances, and other objects that are connected to the internet and can

exchange data. As IoT continues to grow, it is expected to revolutionize industries such as healthcare, transportation, and manufacturing.

- **Artificial Intelligence (AI):** AI technologies such as machine learning and natural language processing are already being used to power a wide range of applications and services, from voice assistants to fraud detection. As AI continues to advance, it is expected to enable new use cases and transform industries such as healthcare, finance, and education.
- **Blockchain:** Blockchain is a distributed ledger technology that enables secure, decentralized transactions. It is being used to power a wide range of applications, from cryptocurrency to supply chain management.
- **Edge computing:** Edge computing refers to the processing and storage of data at the edge of the network, rather than in centralized data centers. It is expected to enable new use cases and applications, such as real-time analytics and low-latency applications.

Conclusion

We've covered a lot of ground, so let's take a moment to review what we've learned:

- The internet is a global network of interconnected computers that uses a standard set of communication protocols to exchange data.
- The internet works by connecting devices and computer systems together using standardized protocols, such as IP and TCP.
- The core of the internet is a global network of interconnected routers that direct traffic between different devices and systems.
- Basic concepts and terminology that you need to familiarize yourself with include packets, routers, IP addresses, domain names, DNS, HTTP, HTTPS, and SSL/TLS.
- Protocols play a critical role in enabling communication and data exchange over the internet, allowing devices and systems from different manufacturers and vendors to communicate seamlessly.

References

How does the internet work?

How Does the Internet Work? MDN Docs