ACT UNIT-2

Batch processing(one time at a time)

Time sharing(In computing, time-sharing is the sharing of a computing resource among many users at the same time by means of multiprogramming and multi-tasking.)

1. History of Internet?

The internet is a global network of connected computers and servers that allow people to share information and communicate with each other. It has its origins in the 1960s, when the US Department of Defense created a communication network called ARPANET. This network was designed to be decentralized and resilient, so that if one part of it was damaged or destroyed, the rest would continue to function.

In the 1980s, the internet began to grow rapidly as more universities and research institutions joined ARPANET and created their own networks. The development of the World Wide Web in the 1990s made the internet accessible to the general public, and it quickly became an essential tool for communication, commerce, and entertainment.

Today, the internet continues to evolve and grow, with new technologies and applications constantly being developed. It has become an indispensable part of modern life, connecting people from all over the world and providing access to a vast array of information and resources.

There are different networks like,Raind corporation America,National physical laborotory englad and Cyclades france these are the different networks helps to develop our modern internet.

What is the reason beyond ARPANET?

The Advanced Research Projects Agency Network (ARPANET) was created in the late 1960s by the United States Department of Defense as a means of enabling communication and collaboration among researchers and scientists working on military projects. The goal was to create a decentralized and fault-tolerant network that could continue to function even if some parts of it were damaged or destroyed in a military attack.

At the time, computers were large, expensive, and operated in isolation from each other. ARPANET was developed as a way to connect these computers together, allowing researchers to share data and resources, and collaborate on projects more easily. The technology developed for ARPANET laid the groundwork for the modern internet, which has become an essential tool for communication, commerce, education, and entertainment.

Uses of ARPANET?

The ARPANET was created as a research project to develop a decentralized and fault-tolerant communication network for the United States Department of Defense. The network was designed to be used by researchers and scientists working on military projects, but it eventually had a much broader impact on society. Some of the primary uses of ARPANET included:

Communication: ARPANET allowed researchers and scientists to communicate with each other over long distances using computers and the network. This was a significant improvement over traditional forms of communication, which were slower and more limited in scope.

Resource sharing: ARPANET enabled researchers to share computing resources and data with each other, allowing them to collaborate on projects more easily.

Remote access: ARPANET allowed researchers to access resources and data located at remote sites, making it easier to conduct research and collaborate with colleagues who were located far away.

Experimentation: ARPANET was a platform for experimentation and development of new networking technologies and protocols that eventually led to the creation of the modern internet.

Overall, the ARPANET played a critical role in the development of the internet and had a profound impact on how people communicate, collaborate, and access information today.

What was first message over internet?

The first message transmitted over the internet was sent on October 29, 1969, by a computer science professor named Leonard Kleinrock at the University of California, Los Angeles (UCLA). Kleinrock and his team sent a message from their computer at UCLA to a computer at the Stanford Research Institute (SRI) in Menlo Park, California.

The message was intended to be the word "login," but the system crashed after the first two letters were transmitted, so the full word was not sent. Nonetheless, this event marked the first successful transmission of data over what would eventually become the internet.

2. Internet Protocol Address:

An Internet Protocol (IP) address is a unique numerical identifier assigned to every device connected to the internet. It allows devices to communicate with each other and send and receive data packets over the internet.

IP addresses are either IPv4 (32-bit) or IPv6 (128-bit) numbers, which are typically represented as a series of four decimal numbers separated by periods (IPv4) or eight groups of four hexadecimal digits separated by colons (IPv6).

IP addresses are assigned to devices either statically or dynamically. In static addressing, an IP address is manually assigned to a device, while in dynamic addressing, an IP address is assigned automatically by a DHCP (Dynamic Host Configuration Protocol) server.

In summary, an IP address is a fundamental component of the internet that allows devices to communicate with each other and exchange data packets.

Ipv4 and ipv6:

IPv4 and IPv6 are two versions of the Internet Protocol, which is the set of rules that governs how data is transmitted over the internet.

IPv4 is the older of the two and uses a 32-bit addressing system, which means that it can support up to 4.3 billion unique IP addresses. However, due to the rapid expansion of the internet and

the increasing number of devices that need to be connected, the number of available IPv4 addresses has been exhausted, and the remaining ones are becoming increasingly scarce.

IPv6 is the newer version of the Internet Protocol and uses a 128-bit addressing system, which means that it can support an almost infinite number of unique IP addresses. This makes IPv6 much better suited to the needs of the modern internet, which requires a much larger pool of addresses to accommodate the growing number of devices and users.

Although IPv6 has been available since 1998, its adoption has been relatively slow due to various factors such as the cost of upgrading infrastructure and the compatibility issues with older systems that only support IPv4. However, many organizations and internet service providers are now beginning to adopt IPv6, and it is expected to eventually become the dominant protocol used on the internet.

Static and dynamic IP:

Static IP and Dynamic IP are two types of IP addresses that can be assigned to a device on a network.

A Static IP address is an IP address that is manually assigned to a device and does not change over time. It is typically used for devices that require a fixed IP address, such as servers, printers, or network storage devices. A static IP address can be more reliable for certain applications, as it does not change, but it can also be more difficult to manage and configure, especially in larger networks.

On the other hand, a Dynamic IP address is automatically assigned to a device by a Dynamic Host Configuration Protocol (DHCP) server on the network. Dynamic IP addresses can change over time, and are typically used for devices that do not require a fixed IP address, such as laptops, smartphones, or tablets. Dynamic IP addresses can be more flexible and easier to manage in larger networks, as the DHCP server can automatically assign addresses to devices as needed.

Binary and dotted decimal notations:

Binary and dotted decimal notations are two different ways of representing IP addresses, which are used to identify devices on a network.

In binary notation, an IP address is represented using a string of 32 bits, which are arranged in four groups of 8 bits each. Each group of 8 bits is then converted to its equivalent decimal value, which results in four numbers ranging from 0 to 255, separated by dots. For example, the IP address 192.168.0.1 in binary notation is 11000000.10101000.00000000.00000001.

In dotted decimal notation, an IP address is represented using four decimal numbers separated by dots, with each number ranging from 0 to 255. Each decimal number is then converted to its equivalent 8-bit binary representation, resulting in a string of 32 bits. For example, the IP address 192.168.0.1 in dotted decimal notation is represented in binary as 11000000.10101000.00000000.00000001.

Both notations are used interchangeably, but dotted decimal notation is more commonly used because it is easier for humans to read and remember. Binary notation is mainly used by network administrators and engineers for troubleshooting and network analysis.

who will control ip address:

The allocation and management of IP addresses is overseen by the Internet Assigned Numbers Authority (IANA), which is a department of the Internet Corporation for Assigned Names and Numbers (ICANN). However, IANA does not control IP addresses, rather they are responsible for allocating blocks of IP addresses to the five Regional Internet Registries (RIRs) around the world. These RIRs are responsible for managing and distributing IP addresses to internet service providers (ISPs) and other organizations within their respective regions. Ultimately, it is the individual organizations that control their own IP addresses, but they must adhere to the guidelines and policies set forth by the RIRs.

Examples:

Sure! Here's an example of an IP address:

IPv4 Address: 192.168.0.1

IPv6 Address: 2001:0db8:85a3:0000:0000:8a2e:0370:7334

In this example, the first IP address is an IPv4 address consisting of four decimal numbers separated by periods. The second IP address is an IPv6 address consisting of eight groups of four hexadecimal digits separated by colons.

Uses of IP addresses

IP addresses are used for several purposes, including:

Network communication: IP addresses are used to enable communication between devices on a network. Devices can send and receive data packets over the internet using IP addresses.

Identifying devices: IP addresses help in identifying devices on a network. Every device on a network has a unique IP address, which is used to identify it.

Routing: IP addresses are used in routing data packets across networks. Routers use IP addresses to direct data packets to the correct destination.

Security: IP addresses can be used for security purposes, such as identifying unauthorized access attempts, monitoring network activity, and enforcing access controls.

Geolocation: IP addresses can be used to determine the geographical location of a device. This can be used for various purposes such as advertising, content localization, and fraud detection.

3. ## Types of IP Addresses:

Private IP addresses: These are IP addresses that are used on private networks, such as local area networks (LANs) or home networks, and are not directly accessible from the internet. The most commonly used private IP addresses are in the ranges of 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, and 192.168.0.0 to 192.168.255.255.

Public IP addresses: These are IP addresses that are assigned to devices that are directly connected to the internet, such as web servers, email servers, or routers. Public IP addresses are unique and can be used to access these devices from anywhere on the internet.

Static IP addresses: These are IP addresses that are manually assigned to a device and do not change over time. Static IP addresses are commonly used for servers, printers, or other devices that need to be accessed consistently.

Dynamic IP addresses: These are IP addresses that are automatically assigned to a device by a server, and may change over time. Dynamic IP addresses are commonly used for home networks or devices that do not require a permanent IP address, like small businesses, and internet service providers (ISPs)

Reserved IP addresses: These are IP addresses that are reserved for special purposes, such as for use in private networks, for multicast communication (one to many or many to many communication, example online streaming, group messaging) Examples of reserved IP addresses include 127.0.0.1 (the loopback address) and 224.0.0.0 to 239.255.255.255 (for multicast communication).

Examples:

Private IP address: 192.168.0.1. This is a common default IP address used by many routers for their administration interface on a local network.

Public IP address: 205.251.242.54. This is an example of a public IP address assigned to a server that hosts a popular website.

Static IP address: 203.0.113.5. This is an example of a static IP address assigned to a server that needs to be accessible at the same address all the time.

Dynamic IP address: 192.168.1.100. This is an example of a dynamic IP address assigned to a device on a home network by the router's DHCP server.

Reserved IP address: 127.0.0.1. This is the loopback address that is reserved for a device to refer to itself, commonly used for testing network software.

Summary:

Type of IP Address	Description
Public IP	A public IP address is an address where one primary address is associated with your whole network.
Private IP	A private IP address is a unique IP number assigned to every device that connects to your home internet network.
Dynamic IP	Dynamic IP addresses always keep changing. It is temporary and are allocated to a device every time it connects to the web.
Static IP	Static IP address never changes, but it can be altered as part of routine network administration.
Shared IP	The IP address is not unique and it is shared with other websites.
Dedicated IP	Dedicated IP address is assigned uniquely to each website.

4. Domain Name System:

The Domain Name System (DNS) is a hierarchical naming system that is used to translate domain names (such as google.com) into IP addresses that computers can understand. DNS is essentially a phone book for the internet that translates human-readable domain names into IP addresses.

When a user types a domain name into their web browser, the browser sends a DNS query to a DNS resolver, which is a server that looks up the IP address associated with the domain name. The resolver then returns the IP address to the browser, which uses it to connect to the web server hosting the website.

DNS is divided into a hierarchy of domains, with each domain being managed by a different organization. The top-level domain (TLD) is the part of the domain name that appears after the last dot (e.g., .com, .org, .edu), and it is managed by the Internet Assigned Numbers Authority (IANA). Below the TLD, there are second-level domains (SLDs) and subdomains, which are managed by various domain registrars and domain name system providers.

DNS is critical to the functioning of the internet, as it enables users to access websites using easy-to-remember domain names, rather than having to remember the IP addresses of every website they want to visit.

Example:

Let's say you want to visit the website www.google.com. You type the domain name into your web browser, and the browser sends a DNS query to a DNS resolver. The resolver then looks up the IP address associated with the domain name by checking a series of DNS servers.

First, the resolver checks the root DNS servers to find the DNS server responsible for the .com TLD. Once it has the IP address of the .com TLD DNS server, it sends another query to that server to find the DNS server responsible for the google.com domain.

TLD: .com

SLD: google.com

Subdomains: mail.google.com, drive.google.com, maps.google.com

TLD: .org

SLD: wikipedia.org

Subdomains: en.wikipedia.org, fr.wikipedia.org, commons.wikipedia.org

TLD: .net

SLD: microsoft.net

Subdomains: outlook.microsoft.net, office365.microsoft.net, store.microsoft.net

TLD: .edu

SLD: harvard.edu

Subdomains: canvas.harvard.edu, extension.harvard.edu, library.harvard.edu

TLD: .gov

SLD: whitehouse.gov

Subdomains: petitions.whitehouse.gov, www2.whitehouse.gov, www3.whitehouse.gov

5. Uniform Resource Locator:

Uniform Resource Locator (URL) is a type of web address that is used to locate resources on the internet, such as web pages, images, videos, or any other file available on the World Wide Web. URLs are the addresses that you enter in your web browser to access a website.

Example URL: https://www.example.com:8080/path/to/page.html?

A URL contains the following information which is listed below:

Protocol name

A colon followed by double forward-slash (://)

Hostname (domain name) or IP address

A colon followed by port number (optional – unless specified otherwise, ":80" is the default when using HTTP, and ":443" is the default when using HTTPS)

Path of the file:

A typical URL consists of several parts, including:

Protocol: This specifies the communication protocol used to access the resource, such as HTTP, HTTPS, FTP, etc.

Domain Name: This identifies the domain name of the web server hosting the resource.

Path: This specifies the location of the resource on the web server, including the file name and directory structure.

Parameters: These are optional parameters that are used to pass additional information to the web server, such as search terms, page numbers, or user preferences.

For example, the URL for the homepage of Google is:

https://www.google.com/

Here, "https://" is the protocol, "www.google.com" is the domain name, and the "/" at the end indicates the root directory or homepage of the website.

What is HTTP?

HTTP stands for Hypertext Transfer Protocol, which is a protocol used to transfer data over the internet. It is a set of rules that govern how web browsers and servers communicate with each other. When you type a web address (URL) into your browser, the browser sends an HTTP request to the web server hosting the website. The web server then responds with an HTTP response, which contains the requested data (such as a webpage or an image).

HTTP is the foundation of the World Wide Web and is responsible for the transfer of web pages, images, videos, and other multimedia content. It uses a client-server model, where the client (usually a web browser) requests data from the server, and the server responds with the requested data. HTTP is an application-layer protocol, which means that it operates at the level of the application, rather than at the network or transport layers.

6. **Internet Services: Electronic Mail, File Transfer Protocol, Chatting, Internet Conferencing, Electronic Newspaper, World Wide Web, Online Shopping , Search Engine**

Electronic Mail: Electronic mail, commonly known as email, is a service that allows individuals to send and receive messages and files over the internet. Email is one of the most popular and widely used communication services on the internet, and it has become an integral part of many people's personal and professional lives.

Advantages:

Electronic Mail: Email is a quick, efficient, and cost-effective way to communicate with people all over the world. It allows for easy exchange of documents and files, and it provides a record of communication for future reference.

Disadvantages:

Electronic Mail: Email can be susceptible (influenced) to hacking, phishing, and spam. Users must take precautions to protect their email accounts and ensure the security of their messages and files.

File Transfer Protocol (FTP): File Transfer Protocol is a service that allows users to transfer files from one computer to another over the internet. FTP is commonly used for sharing large files or for managing websites, and it is a reliable and secure way to transfer data over the internet.

Advantages:

File Transfer Protocol (FTP): FTP provides a reliable and secure way to transfer large files over the internet. It is widely used for managing websites and sharing files with remote teams.

Disadvantages:

File Transfer Protocol (FTP): FTP can be vulnerable to security breaches if the connection is not properly secured. Care must be taken to ensure that sensitive information is not shared over an unsecured FTP connection.

Chatting: Chatting is a service that allows users to communicate with each other in real-time over the internet. Chatting can take place in a variety of formats, including text, voice, and video, and it is a popular way for people to socialize and connect with others online.

Advantages:

Chatting: Chatting allows people to connect with others in real-time, regardless of their location. It is an easy way to stay in touch with friends and family, and it is also a popular communication tool for businesses and organizations.

Disadvantages:

Chatting: Chatting can be distracting and can interfere with productivity. It is important to set boundaries and limit the time spent chatting to avoid being overwhelmed (have a strong emotional effect on).

Internet Conferencing: Internet conferencing is a service that allows users to participate in virtual meetings and presentations over the internet. Internet conferencing can include features like video and audio conferencing, screen sharing, and collaborative document editing, and it is commonly used for remote work and distance learning.

Advantages:

Internet Conferencing: Internet conferencing allows for virtual meetings and presentations, which can save time and money on travel expenses. It also makes it possible for people to work and learn remotely from anywhere in the world.

Disadvantages:

Internet Conferencing: Internet conferencing can be unreliable if the internet connection is not stable. Technical issues can also occur during a virtual meeting, which can disrupt the flow of communication.

Electronic Newspaper: An electronic newspaper, or e-newspaper, is a digital version of a traditional newspaper that can be accessed online. E-newspapers offer many of the same features as traditional newspapers, including news articles, opinion pieces, and classified ads, but they can also include multimedia content like videos and interactive graphics.

Advantages:

Electronic Newspaper: E-newspapers provide instant access to news and information from around the world. They can be accessed from anywhere with an internet connection, and they offer multimedia content like videos and interactive graphics.

Disadvantages:

Electronic Newspaper: E-newspapers may not be accessible to people who do not have access to the internet. They also may not provide the same level of in-depth reporting as traditional newspapers.

World Wide Web: The World Wide Web, often abbreviated as the Web, is a service that allows users to access and share information over the internet. The Web is based on a system of interlinked documents and pages, and it is accessed through web browsers like Chrome, Firefox, and Safari.

Advantages:

World Wide Web: The Web provides access to an almost infinite amount of information and resources. It allows people to connect with others, share ideas, and learn about new topics.

Disadvantages:

World Wide Web: The Web can be overwhelming and difficult to navigate, with a vast amount of information that can be inaccurate or unreliable. It is important to be cautious and verify the information found on the Web.

Online Shopping: Online shopping is a service that allows users to purchase goods and services over the internet. Online shopping has become increasingly popular in recent years, and it offers many benefits over traditional shopping, including convenience, selection, and price.

Advantages:

Online Shopping: Online shopping provides a convenient way to purchase goods and services from anywhere in the world. It allows for easy comparison of prices and products, and it can save time and money on travel and parking expenses.

Disadvantages:

Online Shopping: Online shopping can be risky if the website is not secure or if the product being purchased is counterfeit. It is important to shop from reputable websites and ensure that personal and financial information is protected.

Search Engine: A search engine is a service that allows users to search for information on the internet. Search engines use algorithms to crawl and index web pages, and they can return

relevant results based on a user's search query. Popular search engines include Google, Bing, and Yahoo.

Advantages:

Search Engine: Search engines provide quick and easy access to information on almost any topic. They can help people find answers to questions, learn new skills, and stay up-to-date on current events.

Disadvantages:

Search Engine: Search engines may not always return accurate or unbiased results. They can also be manipulated by businesses or organizations to promote certain products or ideas. It is important to evaluate the sources of information found through a search engine and to verify the accuracy of the information.

7. Web Security terminology: Virus, Malware, Ransom ware, Trojan Horse, Worm ,Bot/Botnet, Spy ware, Rootkit, DDos, Phishing, Clickjacking, Deepfake, White hat/Black hat, Firewall, Encryption, Decryption, Penetration testing.

1.Virus - A type of malicious software that can infect and spread itself to other computer systems. It typically attaches itself to legitimate (to rules or logic) programs and replicates when the program is executed.

Use:

Virus - A virus can infect a computer system and cause it to malfunction or steal data.

Adavantage:

Virus protection helps to prevent malware infections that can cause system crashes, data loss, and other disruptions.

2.Malware - An umbrella term for any malicious software that can harm computer systems, steal data, or gain unauthorized access. This can include viruses, Trojans, worms, spyware, and ransomware.

Use:

Malware - Malware can be used to gain unauthorized access to a computer system, steal sensitive information, or disrupt operations.

Advantages:

Malware protection helps to protect computer systems from a variety of malicious software, including viruses, Trojans, spyware, and ransomware.

3.Ransomware - A type of malware that encrypts(converts data into code) a victim's data and demands payment in exchange for the decryption (code into data) key.

Use:

Ransomware - Ransomware can encrypt a victim's data and demand payment in exchange for the decryption key.

Advantages:

Ransomware protection helps to prevent data encryption and loss of sensitive information.

4.Trojan Horse - A type of malware that disguises itself as a legitimate program or software, but once installed, it allows unauthorized access to the victim's computer.

Use:

Trojan Horse - A Trojan Horse can be used to gain unauthorized access to a computer system or to install other malware.

Advantages:

Trojan protection helps to prevent unauthorized access to computer systems and prevent the installation of other malware.

5.Worm - A self-replicating malware that spreads through computer networks by exploiting security vulnerabilities(state of being exposed to the possibility of being attacked or harmed).

Use:

Worm - A worm can spread through a computer network and cause widespread damage.

Advantages:

Worm protection helps to prevent the spread of malware through computer networks and disrupt operations.

6.Bot/Botnet - A bot is a software program that performs automated tasks, often without the user's knowledge. A botnet is a network of infected computers that are controlled by a single attacker.

Use:

Bot/Botnet - A botnet can be used to launch DDoS attacks, steal data, or send spam emails.

Advantages:

Bot/Botnet protection helps to prevent network breaches, data theft, and other malicious activities.

7.Spyware - A type of malware that is designed to collect personal information from a user's computer without their knowledge or consent.

Use:

Spyware - Spyware can be used to monitor a victim's computer activity and steal sensitive information.

Advantages:

Spyware protection helps to prevent the unauthorized monitoring of computer activity and theft of sensitive information.

8.Rootkit - A type of malware that can gain access to a computer system and remain hidden from detection by antivirus software and other security measures.

Use:

Rootkit - A rootkit can be used to gain persistent access to a computer system and remain hidden from detection.

Adavantages:

Rootkit protection helps to prevent unauthorized access to computer systems and persistent malware infections.

9.DDoS - Short for Distributed Denial of Service, a type of cyber attack where multiple compromised computer systems are used to flood a target system or network with traffic, making it unavailable to users.

Use:

DDoS - DDoS attacks can be used to take down websites or disrupt network operations.

Adavantages:

DDoS protection helps to prevent the disruption of network operations and prevent network downtime.

10.Phishing - A type of social engineering attack where attackers use emails, text messages, or websites to trick victims into giving away sensitive information such as passwords or credit card numbers.

Use:

Phishing - Phishing attacks can be used to steal sensitive information such as login credentials, credit card numbers, or social security numbers.

Adavantages:

Phishing protection helps to prevent the theft of sensitive information such as login credentials, credit card numbers, or social security numbers.

11.Clickjacking - A type of attack where attackers trick users into clicking on a disguised button or link that performs an unintended action, such as downloading malware or sharing personal information.

Use:

Clickjacking - Clickjacking can be used to trick users into performing unintended actions, such as downloading malware or sharing personal information.

Advantages:

Clickjacking protection helps to prevent users from being tricked into performing unintended actions, such as downloading malware or sharing personal information.

12.Deepfake - A type of synthetic media created using artificial intelligence techniques to manipulate images, video, or audio to make it appear real but is actually fake.

Use:

Deepfake - Deepfakes can be used to spread false information or manipulate public opinion.

Adavantages:

Deepfake protection helps to prevent the spread of false information and manipulative media.

13.White hat/Black hat - Terms used to describe ethical and unethical hackers, respectively. White hat hackers work to improve security by finding vulnerabilities in systems, while black hat hackers use these vulnerabilities for their own gain.

Use:

White hat/Black hat - White hat hackers can be hired by companies to test their security measures and identify vulnerabilities, while black hat hackers can use their skills for illegal activities.

Adavantages:

White hat/Black hat protection helps to ensure that ethical hackers use their skills for legal and ethical purposes and prevent illegal activities by black hat hackers.

14.Firewall - A network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

Uses:

Firewall - A firewall can be used to prevent unauthorized access to a computer network.

Adavantages:

Firewall protection helps to prevent unauthorized access to computer networks and prevent the spread of malware.

15.Encryption - The process of converting information into a secret code to protect it from unauthorized access.

Uses:

Encryption - Encryption can be used to protect sensitive information such as credit card numbers, social security numbers, or medical records.

Advantages:

Encryption helps to protect sensitive information from unauthorized access and ensure privacy.

16.Decryption - The process of converting encrypted data back into its original form.

Uses:

Decryption - Decryption is necessary to access encrypted data.

Adavantages:

Decryption helps authorized users to access encrypted data.

17.Penetration testing - The process of simulating an attack on a computer system to identify vulnerabilities and assess the effectiveness of security measures.

Uses:

Penetration testing - Penetration testing can be used to identify vulnerabilities in a computer system and improve its security measures.

Advantages:

Penetration testing helps to identify vulnerabilities in computer systems and improve security measures, preventing potential data breaches and disruptions.

Disadvantages of Web Security terminology:

1. Some security measures can be costly to implement, such as advanced firewalls or encryption software.
2. Security measures can sometimes slow down computer systems or websites, leading to decreased productivity or user frustration.
3. Some security measures require ongoing maintenance and updates to remain effective, which can be time-consuming and resource-intensive.
4. False positives can occur with some security measures, leading to legitimate actions being blocked or users being inconvenienced.
5. Security measures can sometimes be bypassed by sophisticated attackers, leaving systems vulnerable to attack.
6. Some security measures can require extensive training to use effectively, which can be costly and time-consuming.
7. Over-reliance on security measures can lead to a false sense of security, with users becoming complacent and neglecting other important security practices.
8. Penetration testing can sometimes cause unintended disruptions to computer systems or networks.
9. Some security measures can be difficult to configure or implement correctly, leading to vulnerabilities or other problems.
10. Security measures can sometimes conflict with other software or tools, leading to compatibility issues or decreased performance.

**what is firewalls? How does it works and types of firewalls?

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on a set of predetermined security rules. Its primary purpose is to prevent unauthorized access to or from a private network, such as a corporate network or a home network.

Firewalls work by inspecting the data packets that flow in and out of a network and enforcing predefined security policies based on the source, destination, and type of traffic. These policies can include rules that block certain types of traffic or allow it only to specific ports or IP addresses. The firewall can also perform other security functions such as packet filtering, intrusion detection, and content filtering.

There are different types of firewalls, including hardware and software firewalls. A hardware firewall is a physical device that sits between a network and the internet and filters traffic based on preconfigured

rules. A software firewall is a program that runs on a computer or server and monitors traffic coming in and out of that specific device.

Overall, a firewall is an essential component of network security, as it helps to protect against potential cyberattacks and unauthorized access to sensitive information.

There are several types of firewalls that are commonly used to protect networks and devices. Here are some of the most common types:

1. Packet-filtering firewall: This type of firewall examines the header information of each packet that passes through it and compares it against a set of predefined rules. If a packet meets the criteria specified in the rules, it is allowed to pass through the firewall. Otherwise, it is blocked.
2. Stateful firewall: This type of firewall is more advanced than a packet-filtering firewall. It not only examines the header information of each packet, but also the content of the packet and the state of the connection between the sender and receiver. This allows it to make more informed decisions about whether to allow or block traffic.
3. Proxy firewall: This type of firewall acts as an intermediary between a client and a server, and inspects traffic at the application layer. When a client sends a request to a server, the proxy firewall intercepts it and checks whether it meets the criteria specified in its rules. If it does, the proxy firewall forwards the request to the server on behalf of the client.
4. Next-generation firewall (NGFW): This type of firewall is designed to provide more advanced security features than traditional firewalls. It combines traditional firewall functionality with intrusion prevention, application awareness, and other security features to provide comprehensive protection against cyber threats.
5. Unified Threat Management (UTM) firewall: This type of firewall is a comprehensive security solution that includes several security features such as antivirus, anti-spam, content filtering, and intrusion detection and prevention. It provides a single platform for managing all aspects of network security.

** What is penetration testing and how does it works?

Penetration testing, also known as pen testing, is a simulated cyber attack on a computer system, network, or web application to identify vulnerabilities that attackers could exploit. The purpose of a penetration test is to evaluate the security of a system and determine whether it can be hacked or not.

Penetration testing typically follows a predefined methodology that includes the following steps:

1. Planning and reconnaissance: The pen tester gathers information about the target system, including its IP addresses, network architecture, and software applications.
2. Scanning: The pen tester uses various tools to scan the target system for vulnerabilities, such as open ports, unpatched software, and weak passwords.
3. Gaining access: Once vulnerabilities are identified, the pen tester attempts to exploit them to gain access to the target system. This could include using social engineering techniques, such as phishing emails, or exploiting software vulnerabilities, such as SQL injection or buffer overflow attacks.
4. Maintaining access: Once the pen tester has gained access to the target system, they attempt to maintain that access and escalate their privileges to gain deeper access to the system.

5. Analysis and reporting: The pen tester analyzes the results of the test and creates a report that outlines the vulnerabilities discovered, the methods used to exploit them, and recommendations for remediation.

What is the World Wide Web and how does it work?

The World Wide Web, commonly known as the web, is a system of interconnected documents and other resources, linked by hyperlinks and URLs (Uniform Resource Locators). It was invented by Sir Tim Berners-Lee in 1989 while working at CERN, the European Organization for Nuclear Research.

The web works by using a client-server model. A user accesses the web through a client, which is usually a web browser like Google Chrome or Mozilla Firefox. The client sends a request for a webpage to a server, which hosts the webpage, and the server responds by sending the requested webpage back to the client. The webpage may include text, images, videos, and other multimedia content.

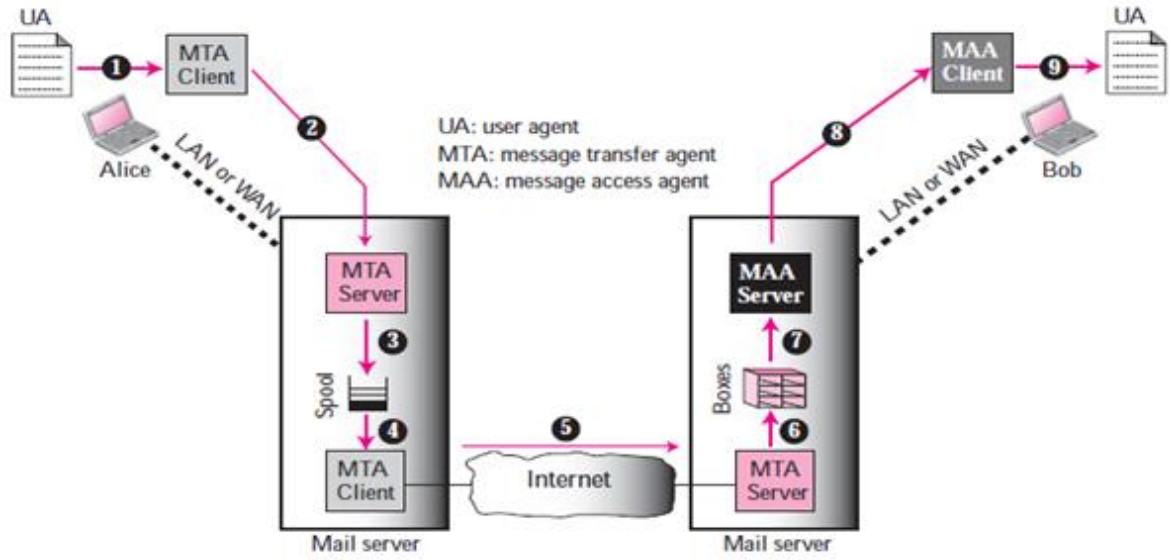
The web also uses a protocol called HTTP (Hypertext Transfer Protocol) to transfer data between the client and the server. HTTPS (HTTP Secure) is a more secure version of HTTP that uses encryption to protect data during transmission.

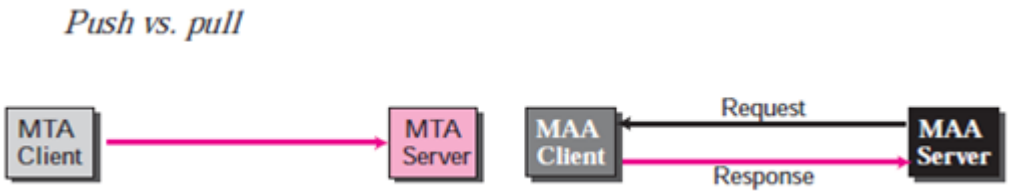
In addition to webpages, the web also includes other resources like email, online shopping, social media, and cloud computing. The web has revolutionized the way we access and share information, and has become an essential part of modern life.

Email Architecture:

Email architecture consists of three components:

- **User Agent (UA)**
- **Message Transfer Agent (MTA)(** Mail Transfer Agent)
- **Message Access Agent (MAA)(** Mailbox Access Agent)





User Agent:

A user agent is a Package "or in simple words a program" of a software that composes, Reads, Responds to, and forward messages. It also handles user computers with local mailboxes.

Sending Mail:

In order to send a mail, the user creates mail through the UA which looks very similar to Postal Mail.

Receiving Mail:

The User agent, or a timer, is triggered by the User. Where a user has mail, the UA will notify the user with a notice if the user is ready to read the mail, a list will be shown in which each line includes a description of a particular message's mailbox information.

Addresses:

A mail handling system must use a system address with unique addresses to deliver mails. Each user has a unique email address which is selected the time a person sign up for an email ID.

Mailing List or Group List:

Electronic mail allows for the one name, an alias, to represent several different email addresses; this is called a mailing list. The system checks the name of the recipient against the alias database whenever a message is to be sent; if there is a mailing list for the defined alias, separate messages, one for each entry in the list, must be prepared and given to the MTA.

Mail Transfer Agent "MTA":

The actual mail transmission is done through MTAs. A system must have the client MTA for sending mail, and a system must have a server MTA for

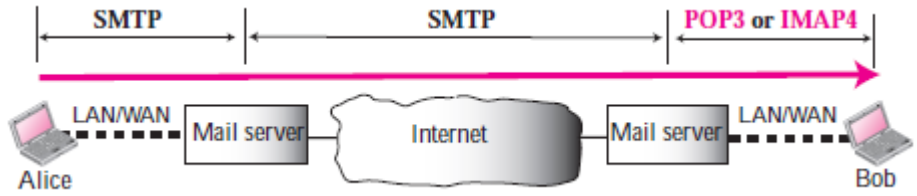
receiving mail. Simple Mail Transfer Protocol “SMTP” is the formal protocol that defines the MTA client and server within the internet.

Message Access Agent “MAA”:

MAA stands for "Mailbox Access Agent." It is a component of a mail server that is responsible for handling requests from email clients to access a user's mailbox.

When an email client, such as Microsoft Outlook or Apple Mail, wants to access a user's mailbox, it sends a request to the MAA on the mail server. The MAA then retrieves the user's emails and sends them back to the email client. The MAA also handles tasks such as creating, deleting, and moving emails within the user's mailbox.

Post Office Protocol version 3 “POP3” and Internet Mail Access Protocol “IMAP”.



Simple Mail Transfer Protocol (SMTP):

SMTP is used two times, between the sender and the sender’s mail server and between the two mail servers. SMTP simply defines how commands and responses must be sent back and forth between an MTA client and an MTA server.

ommands:

Hello e.g. Electroniclinic.com

Send from e.g. engrfahad@electroniclinic.com

Send to e.g. xyz@yahoo.com

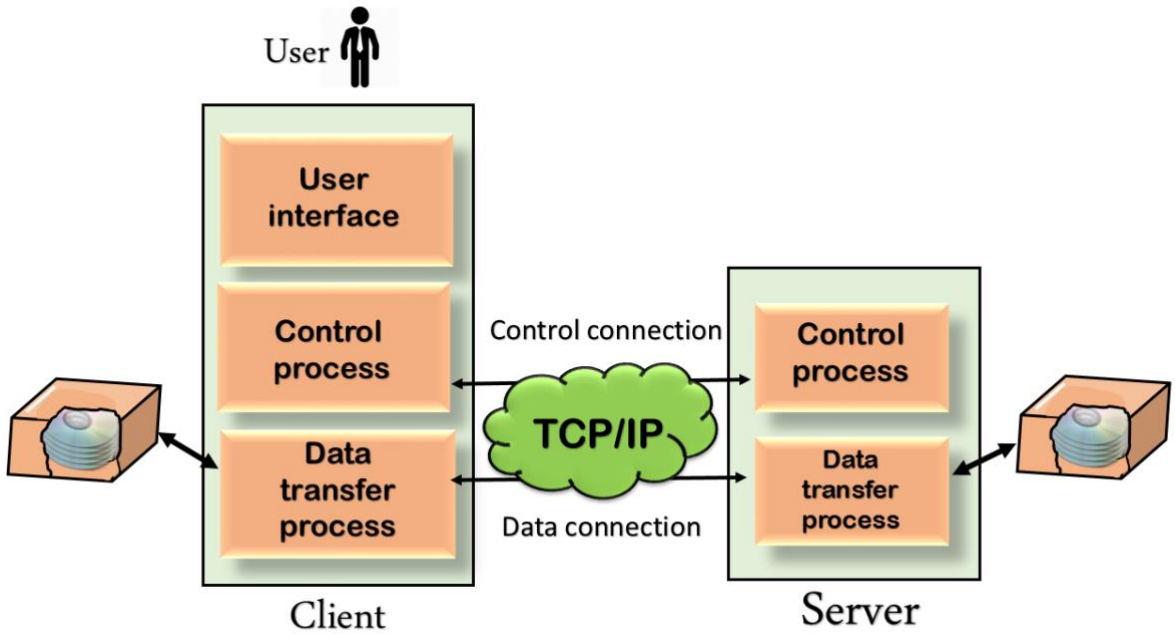
Data: e.g. “Hope you are fine” etc

Response:

- Services Ready
- User not local; the message will be forwarded
- The command is not executed; mailbox unavailable etc.

Mail Transfer Phases: The process of transmitting a mail message takes place in three phases: forming links, exchanging mail and terminating the connections.

File transfer Protocol



FTP

- FTP stands for File transfer protocol.
- FTP is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another.
- It is mainly used for transferring the web page files from their creator to the computer that acts as a server for other computers on the internet.
- It is also used for downloading the files to computer from other servers.

Objectives of FTP

- It provides the sharing of files.
- It is used to encourage the use of remote computers.
- It transfers the data more reliably and efficiently.

Why FTP?

Although transferring files from one system to another is very simple and straightforward, but sometimes it can cause problems. For example, two systems may have different file conventions. Two systems may have different ways to represent text and data. Two systems may have different directory structures. FTP protocol overcomes these problems by establishing two connections between hosts. One connection is used for data transfer, and another connection is used for the control connection.

Types of FTP

- **Control Connection:** The control connection uses very simple rules for communication. Through control connection, we can transfer a line of command or line of response at a time. The control connection is made between the control processes. The control connection remains connected during the entire interactive FTP session.
- **Data Connection:** The Data Connection uses very complex rules as data types may vary. The data connection is made between data transfer processes. The data connection opens when a command comes for transferring the files and closes when the file is transferred.

FTP Clients

- FTP client is a program that implements a file transfer protocol which allows you to transfer files between two hosts on the internet.
- It allows a user to connect to a remote host and upload or download the files.
- It has a set of commands that we can use to connect to a host, transfer the files between you and your host and close the connection.
- The FTP program is also available as a built-in component in a Web browser. This GUI based FTP client makes the file transfer very easy and also does not require to remember the FTP commands.

Advantages of FTP:

- **Speed:** One of the biggest advantages of FTP is speed. The FTP is one of the fastest way to transfer the files from one computer to another computer.
- **Efficient:** It is more efficient as we do not need to complete all the operations to get the entire file.

- **Security:** To access the FTP server, we need to login with the username and password. Therefore, we can say that FTP is more secure.
- **Back & forth movement:** FTP allows us to transfer the files back and forth. Suppose you are a manager of the company, you send some information to all the employees, and they all send information back on the same server.

Disadvantages of FTP:

- The standard requirement of the industry is that all the FTP transmissions should be encrypted. However, not all the FTP providers are equal and not all the providers offer encryption. So, we will have to look out for the FTP providers that provides encryption.
- FTP serves two operations, i.e., to send and receive large files on a network. However, the size limit of the file is 2GB that can be sent. It also doesn't allow you to run simultaneous transfers to multiple receivers.
- Passwords and file contents are sent in clear text that allows unwanted eavesdropping. So, it is quite possible that attackers can carry out the brute force attack by trying to guess the FTP password.
- It is not compatible with every system.