**DESCRIBE HUB, SWITCH AND ROUTER**

Hub, switch, and router are three types of networking devices used to facilitate communication and data transfer between devices in a computer network.

1. Hub:

A hub is the simplest and oldest networking device among the three. It operates at the Physical Layer (Layer 1) of the OSI (Open Systems Interconnection) model. When a device sends data to the hub, it broadcasts that data to all other devices connected to the hub. This means that all devices connected to the hub receive the data, even if it is intended for a specific device only. Hubs are considered "dumb" devices because they lack the ability to make intelligent decisions about where to send data. They suffer from inefficiencies, as all data transmissions share the same bandwidth, leading to collisions and reduced network performance. For this reason, hubs are rarely used in modern networks, having been largely replaced by switches.

2. Switch:

A switch is a more advanced networking device that operates at both the Physical Layer (Layer 1) and Data Link Layer (Layer 2) of the OSI model. Unlike a hub, a switch can make intelligent decisions about where to send data. It maintains a table called a MAC address table, which maps the MAC addresses (hardware addresses) of devices connected to its ports. When a device sends data to the switch, the switch examines the destination MAC address and forwards the data only to the port where the destination device is connected. This significantly reduces collisions and improves network efficiency since data is sent only to the intended recipient. Switches are widely used in modern networks and are the preferred choice for connecting devices within a local area network (LAN).

3. Router:

A router is a networking device that operates at the Network Layer (Layer 3) of the OSI model. Its primary function is to connect multiple networks together, such as connecting a local network (LAN) to the internet. Routers use routing tables to determine the best path for data to reach its destination network. These tables are based on IP addresses. When a device sends data to a router, the router reads the destination IP address and forwards the data to the appropriate network, making sure it reaches its destination efficiently. Routers are also equipped with Network Address Translation (NAT) capabilities, allowing multiple devices in a local network to share a single public IP address. This is essential for conserving IP address space and enhancing security.

In summary:

- Hubs are basic networking devices that broadcast data to all connected devices, resulting in inefficient data transmission.

- Switches are smarter devices that use MAC address tables to forward data only to the intended recipient, improving network efficiency.

- Routers are advanced networking devices that connect different networks, using routing tables and IP addresses to forward data between them. They also perform Network Address Translation to share a single public IP address among multiple devices in a local network.

**WHAT IS THE OSI MODEL?**

The OSI (Open Systems Interconnection) model is a conceptual framework that standardizes the functions of a telecommunication or computing system into seven distinct layers. It was developed by the International Organization for Standardization (ISO) in 1984 to facilitate interoperability between different vendors' networking and communication technologies. The OSI model is not an actual protocol or implementation; instead, it serves as a reference model to help understand how different networking components interact and communicate with each other.

**EXPLAIN THE DIFFERENT LAYERS OF THE OSI MODEL**

The seven layers of the OSI model, from the bottom (Physical Layer) to the top (Application Layer), are as follows:

1. Physical Layer (Layer 1):

The Physical Layer deals with the physical medium over which data is transmitted. It defines the electrical, mechanical, and procedural aspects of communication, such as cables, switches, network interface cards (NICs), and their specifications. It's responsible for converting bits into electrical signals or light pulses and transmitting them over the physical medium.

2. Data Link Layer (Layer 2):

The Data Link Layer is responsible for the reliable transmission of data frames between devices on the same network segment. It deals with MAC (Media Access Control) addresses and performs error detection and correction. This layer ensures that data can move from one device to another within the same local network without errors or collisions.

3. Network Layer (Layer 3):

The Network Layer is responsible for the logical addressing and routing of data packets between different networks. It deals with IP (Internet Protocol) addresses and determines the best path for data to reach its destination across multiple interconnected networks.

4. Transport Layer (Layer 4):

The Transport Layer ensures reliable end-to-end communication between two devices. It provides mechanisms for segmenting and reassembling data and handles flow control, error recovery, and data sequencing. TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are common examples of transport layer protocols.

5. Session Layer (Layer 5):

The Session Layer establishes, maintains, and terminates communication sessions between applications on different devices. It manages session synchronization, checkpointing, and recovery, allowing data exchange to occur in an organized manner.

6. Presentation Layer (Layer 6):

The Presentation Layer is responsible for data translation, encryption, and compression, ensuring that data is in a format that can be understood by the application layer. It deals with data format conversions, making sure that data sent by one system can be interpreted correctly by another system.

7. Application Layer (Layer 7):

The Application Layer is the topmost layer and represents the interface between the network and the user's applications. It enables communication and data exchange between software applications, such as web browsers, email clients, and file transfer programs.

Each layer of the OSI model has its specific functions and protocols, and the model's layered approach allows for modularity and easier troubleshooting of networking issues. When data is transmitted through a network, it passes through each layer sequentially, with each layer's functionalities being carried out at both the sending and receiving devices.

**WHAT IS THE MEANING OF NETWORK PROTOCOLS?**

Network protocols refer to a set of rules and conventions that govern the communication and interaction between devices and systems in a computer network. These protocols define the format, timing, sequencing, and error handling of data transmitted over the network. They play a crucial role in enabling devices to understand and interpret the data exchanged with each other.

Network protocols are essential for ensuring reliable and efficient data transfer between devices from different manufacturers and running different software applications. Without standardized protocols, it would be challenging for devices to communicate effectively and consistently.

**WRITE BRIEFLY ON THE DIFFERENT PROTOCOLS**

- Hypertext Transfer Protocol (HTTP): Used for web browsing, fetching web pages, and transmitting data between web servers and browsers.

-HTTPS stands for Hypertext Transfer Protocol Secure. It is a secure version of the standard HTTP protocol used for transmitting data over the internet. HTTPS employs encryption to protect the data exchanged between a user's web browser and a website's server, ensuring confidentiality and data integrity.

- Transmission Control Protocol (TCP): Ensures reliable data delivery and establishes connections between devices.

- Internet Protocol (IP): Provides addressing and routing for data packets on the internet.

- Simple Mail Transfer Protocol (SMTP): Used for sending and receiving emails.

- User Datagram Protocol (UDP): A connectionless protocol that provides faster but less reliable data transmission.

- File Transfer Protocol (FTP): Used for transferring files between a client and a server.

- Domain Name System (DNS): Resolves human-readable domain names into IP addresses.

**WHAT IS A FIREWALL?**

A firewall is a network security device or software that acts as a barrier between a trusted internal network (such as a company's private network) and an untrusted external network (such as the internet). Its primary purpose is to monitor and control incoming and outgoing network traffic based on a set of predetermined security rules.

The firewall serves as a gatekeeper for the network, allowing or blocking specific types of traffic based on the rules defined by network administrators. It helps prevent unauthorized access to the internal network, protects against malicious activities, and safeguards sensitive data.

**EXPLAIN DNS**

DNS stands for Domain Name System. It is a fundamental component of the internet that acts as a distributed database and translates human-readable domain names into their corresponding numerical IP addresses. This translation is crucial for enabling users to access websites and services by typing user-friendly domain names in web browsers rather than remembering the complex numerical IP addresses associated with each site.

In simple terms, DNS functions as a phone book for the internet. When you enter a domain name (e.g., www.example.com) into your web browser's address bar, the browser needs to find the IP address of the web server hosting that domain to establish a connection. This is where DNS comes into play:

1. Domain Name Resolution: When you enter a domain name, your computer first checks its local DNS cache to see if it already has the corresponding IP address. If the information is not found locally, your computer sends a DNS query to a DNS resolver.

2. DNS Resolver: A DNS resolver is a server that your computer contacts to request the IP address associated with the domain name. This resolver could be provided by your internet service provider (ISP) or a public DNS resolver like Google's 8.8.8.8 or Cloudflare's 1.1.1.1.

3. Recursive Query: If the DNS resolver doesn't have the IP address in its cache, it starts the process of recursive query. It first checks the root DNS servers to find the authoritative DNS server for the top-level domain (TLD) of the requested domain name (e.g., .com, .org, .net).

4. Authoritative DNS Server: The authoritative DNS server is responsible for the specific domain name in question (e.g., example.com). It holds the mapping between the domain name and its corresponding IP address.

5. DNS Response: The authoritative DNS server sends the IP address back to the DNS resolver, which, in turn, sends it to your computer.

6. Accessing the Website: Armed with the IP address, your computer can now establish a connection to the web server hosting the website associated with the domain name. The web server returns the requested web page, and your browser displays it for you to view.

DNS operates in a hierarchical and distributed manner, meaning there are multiple DNS servers worldwide, and the responsibility for managing different domains is delegated to various authorities. This distributed architecture ensures efficient and reliable domain name resolution across the internet.

Overall, DNS plays a crucial role in making the internet user-friendly, as it allows us to access websites using human-readable domain names rather than remembering the corresponding IP addresses for each site.

**DEFINE LATENCY**

Latency refers to the time delay or the amount of time it takes for data to travel from its source to its destination in a computer network or a computing system. It is one of the critical factors that affect the responsiveness and performance of network communication.

**DEFINE CACHING**

Caching is a technique used in computing and computer networks to store frequently accessed data or resources in a temporary storage location called a cache. The primary purpose of caching is to improve the efficiency and speed of data retrieval and reduce the load on the original data source or server.

When a request for data is made, instead of directly accessing the original source (e.g., a website server, a database), the system first checks the cache to see if the requested data is already available there. If the data is found in the cache, it is quickly retrieved, avoiding the need to fetch it from the original source, which can be slower and resource-intensive.

**DEFINE WIDE AREA NETWORK**

A Wide Area Network (WAN) is a type of computer network that spans a large geographical area, typically covering cities, states, countries, or even continents. WANs are designed to connect multiple local area networks (LANs) or other smaller networks together, allowing devices and users in different locations to communicate and share resources seamlessly.

**WHAT IS AN IP ADDRESS?**

An IP address, short for Internet Protocol address, is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. It serves as a unique identifier for the device and allows it to be located and communicated with on the network.

IP addresses are essential for enabling data transmission across the internet and other computer networks. When you send a request to access a website, send an email, or perform any online activity, your device uses its IP address to route the data to the intended destination.

**DEFINE A ROUTING INFORMATION PROTOCOL.**

The Routing Information Protocol (RIP) is one of the oldest interior gateway protocols (IGPs) used for dynamic routing within computer networks. It is primarily designed for small to medium-sized networks and operates within a single autonomous system (AS). RIP uses distance-vector routing algorithms to determine the best path for data packets to reach their destination.

**"193.16.20.35/29" What is the Network IP, number of hosts, range of IP addresses and broadcast Ip from this subnet?**

Network IP: 193.16.20.0

Number of Hosts: 6 (usable IP addresses for devices)

Range of IP addresses: 193.16.20.1 to 193.16.20.6

Broadcast IP: 193.16.20.7