LAB: Assignment 2

Objective: To understand the Networking Components (Hardware/Software)

Instructions: The instructor is required to discuss the following questions with the students.

Students are required to make note on these questions.

Name – Saransh

Roll no – 102103077

Class – 2/CO3

Q1. Network Interface Cards - their use, types and working.

Ans1: A Network Interface Card (NIC) is a hardware component that connects a computer or device to a network. It typically includes a network connector, such as an RJ-45 port, as well as a digital signal processor and other components. NICs can be used to connect computers to a wired Ethernet network, or to connect to wireless networks using Wi-Fi.

There are several types of NICs, including:

Ethernet NICs: These NICs use wired Ethernet connections and support speeds of 10Mbps, 100Mbps, and 1Gbps.

Wi-Fi NICs: These NICs use wireless connections to connect to wireless networks and support speeds of 11Mbps, 54Mbps, and faster.

Bluetooth NICs: These NICs use Bluetooth technology to connect to other devices wirelessly.

Fibre Channel NICs: These NICs use Fibre Channel technology to connect to storage area networks (SANs).

The working of NIC is as follows:

A NIC is installed in a computer, typically in a PCI or PCI Express slot on the motherboard.

When the computer is powered on, the NIC initializes and scans the network for available connections.

Once a connection is established, the NIC assigns the computer an IP address and configures other network settings.

The NIC then forwards data packets between the computer and the network, using the established connection.

It's worth noting that NICs can also have additional features such as VLAN tagging, Quality of Service (QoS), and support for virtualization technologies like SR-IOV, depending on the model.

Q2. Hub Device and its' working.

Ans2: A hub is a networking device that connects multiple computers or other network devices together. It is essentially a repeater that amplifies and sends incoming signals from one device to all other connected devices.

When a device connected to a hub sends data, the hub receives the data and retransmits it to all other connected devices. This means that all devices connected to the hub will receive all data sent by any other device.

There are two types of hubs: active and passive.

Active hubs contain electronics that amplify and regenerate the incoming signals, allowing them to travel farther and connect to more devices. Passive hubs do not contain any electronics and simply repeat the signals they receive.

The working of hub is as follows:

A hub is connected to a number of devices using Ethernet cables.

When a device connected to the hub wants to send data, it sends the data to the hub over the Ethernet cable.

The hub receives the data and amplifies it (if it's an active hub) and then sends the data to all other connected devices.

All other connected devices receive the data and process it if it is meant for them.

It's worth noting that hubs have limitations, such as a shared bandwidth among all connected devices, and no built-in method for handling collisions when multiple devices attempt to transmit data at the same time. These limitations have led to the development of more advanced networking devices such as switches and routers, which are more efficient and offer more features.

Q3. Switch Device and its' working.

Ans3: A switch is a networking device that connects multiple computers or other network devices together. It is similar to a hub in that it connects devices and allows them to communicate with each other, but it differs in how it handles the data.

Unlike a hub, which sends all incoming data to all connected devices, a switch uses MAC addresses to determine the intended recipient of the data and only sends the data to the specific device. This allows for more efficient use of bandwidth and reduces network congestion.

There are two types of switch: managed and unmanaged.

Managed switches are more advanced than unmanaged switches, they have an interface that can be accessed to configure advanced features such as VLANs, Quality of Service (QoS), and Port mirroring. Unmanaged switches, on the other hand, do not have an interface and are typically used for small home or office networks.

The working of switch is as follows:

A switch is connected to a number of devices using Ethernet cables.

When a device connected to the switch wants to send data, it sends the data to the switch over the Ethernet cable.

The switch receives the data and uses the destination MAC address to determine the intended recipient of the data.

The switch then sends the data only to the specific device that the data is intended for.

It's worth noting that switches also have built-in methods for handling collisions when multiple devices attempt to transmit data at the same time, and can also have features such as Port-based VLANs, Link aggregation, and Spanning Tree Protocol which helps to prevent network loops.

Q4. Router Device and its' working.

Ans4: A router is a networking device that connects multiple networks together and directs traffic between them. It determines the best path for data to travel and forwards it to the appropriate destination. Routers are typically used to connect a local network, such as a home or office network, to the Internet.

A router has multiple ports, some of which connect to other devices on the local network, such as a switch, and others that connect to the Internet, such as a modem.

There are two types of routers: wired and wireless.

Wired routers connect devices to the network using Ethernet cables, while wireless routers connect devices to the network using Wi-Fi.

The working of router is as follows:

A router is connected to a number of devices on a local network, as well as to the Internet.

When a device on the local network wants to send data, it sends the data to the router over the Ethernet cable or Wi-Fi.

The router receives the data and uses routing protocols and tables to determine the best path for the data to travel to its destination.

The router then sends the data to the next hop on the path, which could be another router or the final destination.

The router also performs Network Address Translation (NAT) to allow multiple devices on the local network to share a single public IP address.

It's worth noting that routers can also have additional features such as firewalls, Virtual Private Network (VPN) support, Quality of Service (QoS), and parental controls. Router firmware can also be upgraded to increase security, add new features and fix bugs.

Q5. Bridge device and its' working.

Ans5: A bridge is a networking device that connects two or more LANs (Local Area Networks) together. It is used to segment a larger network into smaller segments, allowing for more efficient use of network resources and improved network performance.

Bridges work at the Data Link Layer (layer 2) of the OSI model, and use MAC addresses to determine where to forward incoming data. They are transparent to the devices on the network, meaning that devices are unaware that the bridge is even there.

There are two types of bridges: local bridges and remote bridges.

A local bridge connects LAN segments that are in the same location, while a remote bridge connects LAN segments that are in different locations, such as over a WAN (Wide Area Network) connection.

The working of bridge is as follows:

A bridge is connected to two or more LANs using Ethernet cables.

When a device on one LAN sends data, the bridge receives the data and examines the destination MAC address.

If the destination device is on the same LAN as the sender, the bridge does not forward the data and discards it.

If the destination device is on a different LAN, the bridge forwards the data to the appropriate LAN.

The bridge also keeps a table of MAC addresses it has seen and the corresponding LAN, this is called the forwarding table.

The bridge updates the table by learning the MAC addresses of devices it sees.

It's worth noting that as bridges work at layer 2, they do not have the routing capabilities that routers have and are typically used in smaller networks or in conjunction with routers for network segmentation. Also, bridges can also have additional features such as VLAN tagging, Quality of Service (QoS), and Spanning Tree Protocol (STP) which helps to prevent network loops.

Q6. Types of networking wires and connectors, shapes and specifications.

Ans 6: There are several types of networking wires and connectors, each with their own unique characteristics and specifications:

Ethernet cables: These cables are used to connect devices to an Ethernet network. They come in several categories, such as Cat5, Cat5e, Cat6, and Cat6a, which determine the maximum speed and distance the cable can support. Ethernet cables have 8-wire connectors with RJ-45 connectors at each end.

Fiber-optic cables: These cables use light to transmit data and are often used in high-speed and long-distance networks. They come in single-mode and multi-mode varieties, which determine the distance the cable can support. Fiber-optic cables have connectors such as LC, SC, and ST.

Coaxial cables: These cables are used in cable television and broadband networks. They have a copper core surrounded by an insulating layer and a shield. Coaxial cables have connectors such as BNC, F-type, and RCA.

Twinaxial cables: These cables are used in high-speed, short-distance networks such as storage area networks (SANs). They have two copper conductors surrounded by an insulating layer and a shield. Twinaxial cables have connectors such as SFP and SFP+.

Power over Ethernet (PoE) cables: These cables have the same connectors as Ethernet cables, but also have the ability to transmit power over the cable, eliminating the need for an additional power source for devices such as IP phones and wireless access points.

USB cables: These cables are used to connect devices such as printers and external hard drives to computers. They have USB connectors at each end.

HDMI cables: These cables are used to connect devices such as computers, DVD players, and game consoles to televisions and monitors. They have HDMI connectors at each end.

DisplayPort cables: These cables are used to connect devices such as computers and graphics cards to monitors and televisions. They have DisplayPort connectors at each end.

It's worth noting that each type of cable has specific distance and speed limits, and it's important to choose the right cable to meet the specific needs of the network. Also, connectors are designed to fit specific cables and devices, so it's important to use the correct connector with the correct cable.

Q7. Wireless Access Points.

Ans 7: A wireless access point (WAP) is a networking device that allows wireless devices to connect to a wired network. It creates a wireless network, or "hotspot," which wireless devices such as smartphones, laptops, and tablets can connect to.

A wireless access point typically connects to a wired network using an Ethernet cable, and creates a wireless network using Wi-Fi technology, such as 802.11b, 802.11g, 802.11n, or 802.11ac. WAPs can be connected to a router to allow wireless devices to connect to the Internet, or can be used to create a standalone wireless network.

There are several types of wireless access points, including:

Standalone WAPs: These are standalone devices that can be connected to a wired network and create a wireless network.

Integrated WAPs: These are built-in to other devices such as routers and gateways, allowing them to create a wireless network in addition to their other functions.

Outdoor WAPs: These are designed to be used outdoors and have a weatherproof casing. They can be used to create wireless networks in outdoor areas such as parks and parking lots.

Enterprise WAPs: These are designed for use in large organizations and have advanced features such as support for multiple SSIDs, VLANs, and security features.

The working of wireless access point is as follows:

A WAP is connected to a wired network using an Ethernet cable.

The WAP creates a wireless network using Wi-Fi technology.

Wireless devices can connect to the wireless network using the appropriate SSID and security settings.

Once connected, the wireless devices can communicate with other devices on the wired network and access the Internet.

It's worth noting that wireless access points can also have additional features such as multiple SSIDs, support for different wireless standards, and support for wireless security protocols such as WPA and WPA2.

Q8. Proxy Servers and usages.

Ans 8: A proxy server is a server that acts as an intermediary between a client and one or more other servers. It is used to improve performance, provide anonymity, and implement security and access controls.

There are several types of proxy servers, including:

Forward proxy: A forward proxy is used to forward client requests to other servers on the Internet. It can be used to improve performance by caching frequently requested content, or to implement access controls by only allowing certain clients to access certain websites.

Reverse proxy: A reverse proxy is used to forward requests from the Internet to one or more servers on a private network. It can be used to improve performance by distributing the load among multiple servers, or to provide anonymity by hiding the IP addresses of the servers on the private network.

Transparent proxy: A transparent proxy is a forward proxy that is not configured on the client's device, but is transparently intercepting requests from the client to the Internet.

Anonymous proxy: An anonymous proxy is used to provide anonymity by hiding the client's IP address.

Distorting proxy: A distorting proxy is used to provide anonymity by returning a false IP address for the client.

High anonymity proxy: A high anonymity proxy is used to provide a high level of anonymity by returning no IP address for the client.

Usages:

Caching frequently requested content to improve performance

Filtering and blocking unwanted content

Implementing access controls by only allowing certain clients to access certain websites

Hiding the IP addresses of the servers on a private network

Providing anonymity by hiding the client's IP address

Implementing security by only allowing certain clients to access certain servers

Logging and monitoring client requests

Bypassing geographic restrictions

Helping with compliance and data protection regulations

It's worth noting that proxy servers can be used for legitimate purposes or for malicious purposes, such as to bypass restrictions or to steal sensitive information. It's important to ensure that the proxy server is from a reputable source and is properly configured to meet the needs of the network.

Q9. Firewall and working principle.

Ans 9: A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules and policies. It is used to prevent unauthorized access to or from a private network. Firewalls can be hardware-based, software-based, or a combination of both.

The working principle of a firewall is to inspect the incoming and outgoing network traffic, and allow or block it based on the security rules and policies that have been configured. These rules and policies can be based on various criteria such as source IP address, destination IP address, port number, and protocol.

There are several types of firewalls, including:

Packet-filtering firewall: This type of firewall examines each incoming and outgoing packet and decides whether to allow or block it based on the source and destination IP address and port number.

Circuit-level gateway firewall: This type of firewall examines the connection between the client and server and decides whether to allow or block it based on the source and destination IP address.

Application-level gateway firewall: This type of firewall examines the application data and decides whether to allow or block it based on the source and destination IP address, port number, and protocol.

Stateful inspection firewall: This type of firewall examines the entire connection, including the application data, and keeps track of the state of the connection. It then decides whether to allow or block it based on the source and destination IP address, port number, and protocol, as well as the state of the connection.

The working of firewall is as follows:

A firewall is connected to a network and configured with security rules and policies.

When a packet of data arrives at the firewall, it is inspected by the firewall and compared against the security rules and policies.

If the packet is determined to be safe, it is allowed to pass through the firewall and continue on to its destination.

If the packet is determined to be a security threat, it is blocked by the firewall and not allowed to pass through.

Firewalls can also send alerts when security threats are detected, and log information about all the traffic that is blocked or allowed, which can be useful for troubleshooting and security analysis.

It's worth noting that firewalls can also have additional features such as intrusion detection and prevention, VPN support, and content filtering. It's important to keep in mind that firewalls can block legitimate traffic if not configured correctly, and having a firewall alone is not sufficient for complete network security. It should be used in conjunction with other security measures such as antivirus and intrusion detection systems.