COMPUTER NETWORKS

ASSIGNMENT-2

1. **Network Interface Cards - their use, types and working**.

Network Interface Card (NIC) is a hardware unit, which is inbuilt inside a computer provided with a slot, it connects the computer to a computer network for communication with other devices via buses. There are many synonyms for network interface card like, network adapter, local area network (LAN) card or physical network interface card, ethernet controller or ethernet adapter, network controller, and connection card. Network interface card supports almost all standard buses for data transfer between the computers or devices. The connectors or buses act as an intermediator for communication converts the communication between various devices from serial communication to parallel communication or parallel communication to serial communication. It also formats data based on the architecture of the network.

USES

- It acts like a translator, which converts data into a digital signal.
- Communication can be either by using cable wire or by the router which is wireless over the server network
- To communicate over a long distance a network adapter is used.

TYPES

- **Ethernet NIC** : Ethernet NIC card is a slot for a cable where we have to plug one end of the ethernet cable into the slots of the computer and another end of the cable is plugged into the modem, likewise, various devices are connected to make a communication set up between them.
- **Wireless Network NIC**: Wireless network NIC cards consist of a small antenna integrated onto the card, where the communication between various devices is set up wirelessly using the router and various network protocols.

WORKING

NIC works on the physical layer and data link layer. Actually, NIC collects the data from the computer and sends it to the transmission Channel. It acts as a middleman between your computer and the data network. It is responsible to exchange the computer’s data with a network. Any incoming data that comes from the network medium received by the NIC.

2. Hub Device and its’ working.

A hub is a common connection point, also known as a network hub, which is used for connection of devices in a network. It works as a central connection for all the devices that are connected through a hub. The hub has numerous ports. If a packet reaches at one port, it is able to see by all the segments of the network due to a packet is copied to the other ports. A network hub has no routing tables or intelligence (unlike a network switch or router), which is used to send information and broadcast all network data across each and every connection.

WORKING

Hubs work as a central connection between all network equipment and handle a data type, which is called frames. If a frame is received, it is transmitted to the port of the destination computer after amplifying it. A frame is passed to each of its ports in the hub, whether it is destined only for one port. It does not include the way of deciding a frame to which port it should be sent. Therefore, a frame has to transmit to every port, which ensures that it will reach its intended destination that generates a lot of traffic on the network and can be caused to damage the network. The hub is slower as compared to standard switch as it is not able to send or receive information at the same time, but a switch is more costly than a hub.

3. Switch Device and its’ working

A network switch is a hardware component responsible for relaying data from networks to the destination endpoint through packet switching, MAC address identification, and a multiport bridge system.

A network switch connects and transmits data packets to and from devices on a local area network (LAN). Far from a router, a switch only distributes information to the one device for which it was designed, including some other switch, a router, or a user's computer, rather than to several devices in a network.

WORKING

Once a device is connected to a switch, the switch notes its media access control (MAC) address, a code that's baked into the device's network-interface card (NIC).The NIC attaches to an Ethernet cable that connects to the switch. The switch uses the MAC address to identify which device's outgoing packets are being sent, and where to deliver incoming packets.

The MAC address identifies the physical device and doesn't change, while the network layer (Layer 3) IP address, can be assigned dynamically to a device and change over time. (Think of a MAC address as the VIN number on a car, and the IP address as the license plate.)

When a packet enters the switch, the switch reads its header, then matches the destination address or addresses and sends the packet out through the appropriate ports that lead to the destination devices.

To reduce the chance for collisions between network traffic going to and from a switch and a connected device at the same time, most switches offer full-duplex functionality in which packets coming from and going to a device have access to the full bandwidth of the switch connection. (Picture two people talking on smartphones as opposed to a walkie-talkie).

While it's true that switches operate at Layer 2, they can also operate at Layer 3, which is necessary for them to support virtual LANs (VLANs), logical network segments that can span subnets. In order for traffic to get from one subnet to another it must pass between switches, and this is facilitated by routing capabilities built into the switches.

4. Router Device and its' working

A Router is a networking device that forwards data packets between computer networks. One or more packet switched networks or subnetworks can be connected using a router. By sending data packets to their intended IP addresses, it manages traffic between networks and permits several devices to share an internet connection.

WORKING

Routers connect computers and other devices to the Internet. A router acts as a dispatcher, choosing the best route for your information to travel. It connects your business to the world, protects information from security threats, and can even decide which computers get priority over others.

A router helps you connect multiple devices to the internet and connect the devices to each other. Also you can use routers to create local networks of devices. These local networks are useful if you want to share files among devices or allow employees to share software tools.

5. **Bridge device and its' working.**

A bridge in a computer network is one kind of network device, used to separate a network into sections. Every section in the network represents a collision domain that has separate bandwidth. So that network performance can be improved using a bridge. In the OSI model, a bridge works at layer-2 namely the data link layer. The main function of this is to examine the incoming traffic and examine whether to filter it or forward it.

WORKING

The working principle of a bridge is, it blocks or forwards the data depending on the destination MAC address and this address is written into every data frame.
In a computer network, a bridge separates a LAN into different segments like segment1 & segment2, etc and the MAC address of all the PCs can be stored into the table. For instance, PC1 transmits the data to PC2, where the data will transmit to the bridge first. So the bridge reads the MAC address & decides whether to transmit the data to segment1 or segment2. Therefore, the PC2 is accessible in segment1, which means the bridge transmits the data in segment1 only & eliminates all the

connected PCs in segment2. In this way, the bridge reduces traffic in a computer network.

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

There are several types of network cables. Each type of network cable uses specific types of connectors to connect to another network cable or network interface card.

- **Barrel connectors** are used to join two cables. Barrel connectors are female connectors on both sides. They allow you to extend the length of a cable.
- **An F connector** is used to attach a coaxial cable to a device. **F** connectors are mostly used to install home appliances such as dish TV, cable internet, CCTV camera, etc.
- **A terminator connector** is used to terminate the endpoint of a coaxial cable.
- **A T connector** creates a connection point on the coaxial cable. The connection point is used to connect a device to the cable.
- **RJ-11 connectors** have the capacity for six small pins. However, in many cases, only two or four pins are used.
- **RJ-45 connectors** look likes RJ-11 connectors, but they are different. They have 8 pins. They are also bigger in size than RJ-11. RJ-45 connectors are mostly used in computer networks.
- **DB-9 or RS-232 connector** connects a device over a serial port. It has 9 pins. It is available in both male and female connectors. It is used for asynchronous serial communication. The other side of the cable can be connected to any popular connector type.
- **USB connectors** are the most popular. They support 127 devices in the series. All modern computers have USB ports. Most devices that you can connect to the system have USB ports. Some examples of devices that support or have USB ports are mice, printers, network cards, mobiles
- **SC connectors** are also known as **subscriber connectors**, **standard connectors**, or **square connectors**. An SC connector connects to a terminating device by pushing the connector into the terminating device, and it can be removed by pulling the connector from the terminating device.

- **Straight tip (ST) connectors** are also known as **bayonet connectors**. They have a long tip extending from the connector. They are commonly used with MMF cables. They use a half-twist bayonet type of lock.
- **LC connectors** are known as **Lucent Connectors**. For a secure connection, they have a flange on top, similar to an RJ-45 connector. An LC connector connects to a terminating device by pushing the connector into the terminating device, and it can be removed by pressing the tab on the connector and pulling it out of the terminating device.
- An **MTRJ connector** connects to a terminating device by pushing the connector into the terminating device, and it can be removed by pulling the connector from the terminating device. It includes two fiber strands: a transmit strand and a receive strand in a single connector.

7. Wireless access Points

Wireless access points (WAP) may be used to provide network connectivity in office environments, allowing employees to work anywhere in the office and remain connected to a network. In addition, WAPs provide wireless Internet in public places, like coffee shops, airports and train stations.

A wireless access point (WAP) is a networking device that allows wireless-capable devices to connect to a wired network. It is simpler and easier to install WAPs to connect all the computers or devices in your network than to use wires and cables.

8. Proxy Servers and usages

A proxy server acts as a gateway between you and the internet. It’s an intermediary server separating end users from the websites they browse. Proxy servers provide varying levels of functionality, security, and privacy depending on your use case, needs, or company policy.

If you’re using a proxy server, internet traffic flows through the proxy server on its way to the address you requested. The request then comes back through that same proxy server (there are exceptions to this rule), and then the proxy server forwards the data received from the website to you.

USES

- **To control internet usage of employees and children:** Organizations and parents set up proxy servers to control and monitor how their employees or kids use the internet. Most organizations don't want you looking at specific websites on company time, and they can configure the proxy server to deny access to specific sites.
- **Bandwidth savings and improved speeds:** Organizations can also get better overall network performance with a good proxy server. Proxy servers can cache (save a copy of the website locally) popular websites – so when you ask for www.varonis.com, the proxy server will check to see if it has the most recent copy of the site, and then send you the saved copy.
- **Improved security:** Proxy servers provide security benefits on top of the privacy benefits. You can configure your proxy server to encrypt your web requests to keep prying eyes from reading your transactions. You can also prevent known malware sites from any access through the proxy server.
- **Get access to blocked resources:** Proxy servers allow users to circumvent content restrictions imposed by companies or governments. Is the local sportsball team's game blacked out online? Log into a proxy server on the other side of the country and watch from there.

9. Firewall and working principle

A firewall is a system that provides network security by filtering incoming and outgoing network traffic based on a set of user-defined rules. In general, the purpose of a firewall is to reduce or eliminate the occurrence of unwanted network communications while allowing all legitimate communication to flow freely.

Firewalls filter the network traffic within a private network. It analyses which traffic should be allowed or restricted based on a set of rules. Think of the firewall like a gatekeeper at your computer's entry point which only allows trusted sources, or IP addresses, to enter your network.

A firewall welcomes only those incoming traffic that has been configured to accept. It distinguishes between good and malicious traffic and either allows or blocks specific data packets on pre-established security rules.