D. J. Sanghvi College of Engineering
Department of Electronics & Telecommunication Engineering
Rajus Nagwekar
60002180080
TE EXTC 2

Sem VI Computer Communication Network laboratory

Experiment No.: 1 Date: 5/3/21

Title: Study of various Hardware and Software Network components.

Aim: To study various components in computer communication networks.

Learning objectives: At the end of this experiment, students will able to

- Identify and Define essential components of networks.
- Distinguish between the various interfacing components and the network layers in which they are working.

Theory:

A system that carries a commodity between 2 or more entities is called a network. There are so many networks in our daily life like transport network, electrical network, computer network…etc. So a computer network is a network consists of devices (often referred to as nodes) connected by media links. Computer networks share common devices, functions, and features including servers, clients, transmission media, shared data, and other hardware and software resources. A detailed description of those hardware and software devices is given below.

Servers - Servers are computers that hold shared files, programs, and the network operating system. Servers provide access to network resources to all the users of the network. There are many different kinds of servers, and one server can provide several functions. For example, there are file servers, print servers, mail servers, communication servers, database servers, print servers, fax servers and web servers, to name a few.

Clients - Clients are computers that access and use the network and shared network resources. Client computers are basically the customers (users) of the network, as they request and receive services from the servers

Transmission Media - Transmission media are the facilities used to interconnect computers in a network, such as twisted-pair wire, coaxial cable, and optical fiber cable. Transmission media are sometimes called channels, links or lines.

Hub-Hubs are used to build a LAN by connecting different computers in a star/hierarchal network topology, the most common type on LANs now a day. A hub is a very simple (or dumb) device, once it gets bits of data sent from computer A to B, it does not check the destination, instead, it forwards that signal to all other computers (B, C, D…) within the network. B will then pick it up while other nodes discard it. This amplify that the traffic is shared. There are mainly two types of hubs:

Rajus Nagwekar
60002180080
TE EXTC 2

- **Passive**: The signal is forwarded as it is (so it doesn't need power supply).
- **Active:** The signal is amplified, so they work as repeaters. In fact they have been called multiport repeaters. (use power supply)

Hubs can be connected to other hubs using an uplink port to extend the network. Hubs work on the physical layer (lowest layer). That's the reason they can't deal with addressing or data filtering.

Switch-Switches on the other hand are more advanced. Instead of broadcasting the frames everywhere, a switch actually checks for the destination MAC address and forward it to the relevant port to reach that computer only. This way, switches reduce traffic and divide the collision domain into segments, this is very sufficient for busy LANs and it also protects frames from being sniffed by other computers sharing the same segment. They build a table of which MAC address belongs to which segment. If a destination MAC address is not in the table it forwards to all segments except the source segment. If the destination is same as the source, frame is discarded.

Switches have built-in hardware chips solely designed to perform switching capabilities, therefore they are fast and come with many ports. Sometimes they are referred to as intelligent bridges or multiport bridges. Different speed levels are supported. They can be 10 Mb/s, 100 Mb/s, 1 Gb/s or more.

Bridge-Bridges are used to extend networks by maintaining signals and traffic. They are on the data link layer so in principle they are capable to do what switches do like data filtering and separating the collision domain, but they are less advanced. They are known to be used to extend distance capabilities of networks. In a comparison with switches, they are slower because they use software to perform switching. They do not control broadcast domains and usually come with less number of ports.

Routers-They are used to connect different LANs or a LAN with a WAN (e.g. the internet). Routers control both collision domains and broadcast domains. If the packet's destination is on a different network, a router is used to pass it the right way, so without routers the internet could not functions. They use NAT (Network Address Translation) in conjunction with IP Masquerading to provide the internet to multiple nodes in the LAN under a single IP address. Now a day, routers come with hub or switch technology to connect computers directly. They work on the network layer so they can filter data based on IP addresses. They have route tables to store network addresses and forward packets to the right port.

Gateways-They are very intelligent devices or else can be a computer running the appropriate software to connect and translate data between networks with different protocols or architecture, so their work is much more complex than a normal router. For instance, allowing communication between TCP/IP clients and IPX/SPX or AppleTalk. Gateways

operate at the network layer and above, but most of them at the application layer. The term Gateway is used to refer to routers in some articles so beware. In this case, the router has gateway software. And Default Gateway is used to refer to the node (e.g. router) connecting the LAN to the outside (e.g. internet).

Repeaters- They are simple devices that work at the physical layer of the OSI. They regenerate signals (active hubs does that too).There is an important rule to obey while using repeaters/hubs to extend a local network and is called the 5-4-3 rule or the IEEE way. The rule forces that in a single collision domain there shouldn't be more than 5 segments, 4 repeaters between any two hosts in the network and only 3 of the segments can be populated (contain user connections).This rule ensures that a signal sent over the network will reach every part of it within an acceptable length of time. If the network is bigger, the collision domain can be divided into two parts or more using a switch or a bridge.

Modem- It is a contraction of the terms *modulator* and *demodulator*. Modems perform a simple function: They translate digital signals from a computer into analog signals that can travel across conventional phone lines. The modem modulates the signal at the sending end and demodulates at the receiving end. Modems provide a relatively slow method of communication. In fact, the fastest modem available on the market today has a maximum speed of 56kbps, compare that to the speed of a 10Mbps network connection, and it is found that the modem is approximately 180 times slower. That makes modems okay for browsing web pages or occasionally downloading small files but wholly unsuitable for downloading large files. As a result, many people prefer to use other remote access methods, including ISDN and DSL access.

Network Interface card– They are sometimes called NIC—are the mechanisms by which computers connect to a network. NICs come in all shapes and sizes, and they come in prices to suit all budgets. The NIC prepares (formats) and sends data, receives data, and controls data flow between the computer and the network. On the transmit side, the NIC passes frames of data on to the physical layer, which transmits the data to the physical link. On the receiver's side, the NIC processes bits received from the physical layer and processes the message based on its contents

Wireless access points-*This* referred to as either *WAPs* or *wireless APs,* are a transmitter and receiver (*transceiver*) device used for wireless LAN (WLAN) radio signals. A WAP is typically a separate network device with a built-in antenna, transmitter, and adapter. WAPs use the wireless infrastructure network mode to provide a connection point between WLANs and a wired Ethernet LAN. WAPs also typically have several ports allowing a way to expand the network to support additional clients. Depending on the size of the network, one or more WAPs may be required. Additional WAPs are used to allow access to more wireless clients

Rajus Nagwekar
60002180080
TE EXTC 2

and to expand the range of the wireless network. Each WAP is limited by a transmission range; the distance a client can be from a WAP and still get a useable signal. The actual distance depends on the wireless standard being used and the obstructions and environmental conditions between the client and the WAP.

Firewalls-Today, firewalls are an essential part of a network's design. A *firewall* is a networking device, either hardware or software based, that controls access to your organization's network. This controlled access is designed to protect data and resources from outside threat. To do this, firewalls are typically placed at entry/exit points of a network. For example, a firewall might be placed between an internal network and the Internet. After the firewall is in place, it can control access in and out of that point. Although firewalls typically protect internal networks from public networks, they are also used to control access between specific network segments within a network.

Result:We have seen and studied different types of computer networking components and hence we can compare and differentiate between them.

Conclusion:Hence we studied various hardware and software components in Computer Communication Network

Questions:

1. **Differentiate between switch and router.**

Ans:

Switch	Router
Device that uses packet switching to receive, process and forward data to the destination device.	Device that forwards data packets between computer networks
Creates a network by connecting several devices together and allows the exchange of data	Routes data from one network to another and connects different networks together
Uses MAC address for data transmission	Uses IP address for data transmission
Not fast as a router	Takes routing decisions faster
Works in data link layer of the OSI model (layer2)	Works in network layer of the OSI model (layer3)

Write down the specification of the transmission media used in your laboratory.

Ans: Impedance 75Ω
Capacitance 20pF, 25pF
Power rating 180
Watt Attenuation 5.60 dB and 9.708dB
Core 8mm and 13mm Double shielded

Tejas Nagvekar
60002180080
TE EXTC 2

CCN Experiment 1

1] Repeater: A repeater operates at the physical layer. The job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes very weak, they copy the signal bit by bit & regenerate it at the original strength. It is a 2 port device.

2] Hub: A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects ~~dif~~ different stations. ~~Hubs~~ Hubs cannot filter data, so data packets are sent to all connected devices. In other words, collision domain of all hosts connected through Hub remains one. Also, they do not have the intelligence to find out best path for data packets which leads to inefficiency & wastage.

Types of Hubs:

- Active Hub
- Passive Hub
- Intelligent Hub.

3] Bridge: A bridge operates at data link layer. It is a repeater, with add on the functionality of filtering content by reading the MAC address of source & destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input & single output port, thus making it a 2 port device.
Types of Bridges:
- Transparent Bridge
- Source Routing Bridge

4] Switch: A switch is a multiport bridge with buffer & a design that can boost its efficiency & performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors. & forwards good packets selectively to the correct port only. In other words, switch divides collision domain of hosts, but broadcast domain remains same.

5] Router: A router is a device like a switch that routes data packets based on their IP addresses. Router is mainly a network layer device. Routers normally connect ~~LANs~~ LANs & WANs together & have a dynamically updating routing table based on which they ~~make~~ make decisions on routing the data packets. Routers divide broadcast domains of hosts connected through it.

6] Gateway: A gateway is a passage to connect two networks together that may work upon different networking models. They basically works as the messenger agents that take data from one system, interpret it & transfer it to another system. Gateways are also called protocol converters & can operate at any network layer. Gateways are generally more complex than switch or router.

7] Firewalls: All the previous security measures are not enough for preventing harmful messages from creeping into the system. To control access to a system we need firewalls. A firewall is a device (usually a computer or a router) installed between the internal network of an organisation & the rest of the internet. It is designed to forward some packets & filter (not forward) others.