Module-1

Q-1 Difference Between Hardware and Software

A-1 Hardware and software are two fundamental components of a computer system. Hardware refers to the physical components of a computer system, while software refers to the programs and applications that run on the hardware.

Here are some key differences between hardware and software:

1.Nature: Hardware is a physical entity, while software is intangible.

2/Function: Hardware is responsible for processing data and executing commands, while software provides the instructions for hardware to execute.

3.Tangibility: Hardware can be seen and touched, while software is not visible to the naked eye.

4.Durability: Hardware is generally more durable than software since it is physical, while software can be easily damaged or corrupted.

5.Upgradability: Hardware can be upgraded by replacing or adding components, while software can be upgraded by downloading updates or patches.

6.Cost: Hardware is typically more expensive than software since it involves physical components, while software is relatively inexpensive to produce and distribute.

Overall, both hardware and software are essential components of a computer system, and they work together to enable various functions and tasks.

Q-2 Define IP address range and private address range.

A-2

A private address range refers to a range of IP addresses that are not publicly routable on the internet and are used for private networks. These addresses are reserved for use within private networks and are not allocated for use on the public internet. Private address ranges include:

10.0.0.0 to 10.255.255.255 (10.0.0.0/8)
172.16.0.0 to 172.31.255.255 (172.16.0.0/12)
192.168.0.0 to 192.168.255.255 (192.168.0.0/16)

These address ranges are commonly used for local area networks (LANs) in homes, businesses, and other organizations, and can be used for communication within the network. Private addresses are not globally unique and cannot be used for communication outside of the local network without the use of a network address translator (NAT) or other similar technologies.

Q-3 explain network protocol and port numbers

A-3

A network protocol is a set of rules that defines how data is transmitted and received over a network. It specifies how data is formatted, transmitted, and received, as well as how devices and applications communicate with each other. Examples of network protocols include TCP/IP (Transmission Control Protocol/Internet Protocol), HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), and SMTP (Simple Mail Transfer Protocol).

Port numbers are used to identify specific network services or applications within a device or server. A port number is a 16-bit unsigned integer that ranges from 0 to 65535. It is used in combination with an IP address to uniquely identify a specific network service or application on a device or server. When a device or server receives data, it uses the port number to identify the service or application to which the data should be forwarded.

Q-4 Explain types of network devices .

A-4

There are several types of network devices used to connect and manage computer networks. Here are some of the most common types of network devices:

1. Router: A router is a network device that connects multiple networks together and directs data traffic between them. Routers are used to connect LANs (local area networks) and WANs (wide area networks) to the Internet, and can be used to filter and forward network traffic.
2. Switch: A switch is a network device that connects devices together on a LAN and forwards data between them. Switches are used to create a network infrastructure by connecting computers, printers, and other devices on the same network, and can be used to manage and prioritize network traffic.

3. Hub: A hub is a basic network device that connects multiple devices together on a LAN. Hubs do not have any built-in intelligence to manage network traffic, and all data received on one port is broadcast to all other ports on the hub, which can lead to network congestion.
4. Modem: A modem is a device that connects a computer or network to the Internet over a phone line, cable line, or other communication channel. Modems convert digital signals to analog signals and vice versa to enable communication over the transmission medium.
5. Firewall: A firewall is a network security device that monitors and filters incoming and outgoing network traffic based on predefined security rules. Firewalls can be used to block unauthorized access to a network and protect against network threats such as viruses and malware.
6. Access Point: An access point is a device that enables wireless devices to connect to a wired network. Access points are used to create wireless networks and can provide wireless coverage over a specific area or building.
7. Repeater: A repeater is a network device that receives and amplifies network signals to extend the reach of a network. Repeaters are used to overcome signal attenuation or loss over long distances and can be used to increase the range of a network.

These are some of the most common types of network devices, but there are many other devices used in computer networking, such as network bridges, gateways, and network interface cards (NICs).