N+ assignment

Module - 1

Que- What is network?

Ans: A network is a collection of computers, servers, mainframes, peripherals, or other devices connected to facilitate communication and data sharing.

Que Define network topology.

Ans: A network topology is the physical and logical arrangement of nodes and connection in a network.

Que What is the internet?

Ans: The internet is a global network that connects billions of computer across the world with each other and to the world wide web. It uses the standard internet protocol suite (TCP/IP) to connect billions of computer users worldwide. It is set up by using cables such as optical fibers and other wireless and networking technologies. At present, the internet is the fastest means of sending or exchanging information and data between computers across the world.

Page No.:
Date:

Que. What is the optical fiber module and connector?

Ans: A fiber-optic module is a component that is used to connect a fiber-optic cable to an electronic device. There are a number of different parts of a fiber-optic module and different modules are designed with different specifications. The parts of the module are attached to a board which can be installed as a single unit in an electronic device.

An optical fiber connector is a flexible device that connects fiber cables requiring a quick connection fiber cables requiring a quick connection and disconnection. Optical fibers terminate fiber-optic connections to fiber equipment or join two fiber connections without splicing. Hundreds of optical fiber connector types are available, but the key differentiator is defined by the mechanical coupling techniques and dimensions. Optical fiber connectors ensure stable connections, as they ensure the fiber ends are optically smooth and the end-to-end positions are properly aligned.

Que Explain Switch

Ans: A network switch connects devices in a network to each other, enabling them to talk by exchanging data packets. Switches can be hardware devices that manage physical networks or software-based virtual devices.

A network switch operates on the data-link layer, or layer 2, of the open system interconnection (OSI) model. In a local area network (LAN) using ethernet, a network switch determines where to send each incoming message frame by looking at the media access control (mac) address. Switches maintain tables that match each MAC address to the port receiving the MAC address.

Several types of switches in networking:

(i) Virtual switches
(ii) Routing Switches
(iii) Managed switches
(iv) Unmanaged switches
(v) Smart switches
(vi) stackable switches
(vii) Modular switches

Page No.:
Date:

Que Explain Router.

Ans:- A router receives and sends data on computer networks. Routers are sometimes confused with network hubs, modems, or network switches. However routers can combine the functions of these components, and connects with these devices, to improve internet access or help create business network.

Several types of routers :-

(i) Core router
(ii) Edge router
(iii) Distribution router
(iv) wireless router
(v) Virtual router

Que: Explain MODEM

Ans: Modem stands for modulator / demodulator. The modem is defined as a networking device that is used to connects devices connected in the network to the internet. A modem convert analog signal from telephone wires into digital form, stored in 0s and 1s. It performs modulation and demodulation simultaneously, transfering digital data in personal system. Modems also function as signal translators, converting analog signals into digital ones.

Types of modem

(i) optical modem

(ii) Digital modem

(iii) Cable modem

(iv) Satellite modem

(v) Dial modem

Que:- What is flow control?

Ans:- Flow Control is a technique used to regulate data transfer between computers or other nodes in a network. Flow Control ensures that the transmitting device does not send more data to the receiving device that it can handle. If a device receives more data than it can process or store in memory at any given time, the data is lost and needs to be retransmitted.

Que:- What is arp broadcast?

Ans:- Address Resolution protocol (ARP) is a protocol that maps dynamic IP address to permanent Physical machine addresses in a local area network (LAN). The physical machine address is also called media access control (MAC) address.

ARP translates 32-bit addresses to 48-bit addresses and vice versa, which is necessary because IP addresses in IP version 4 (IPV4) are 32 bits but MAC addresses are 48 bits.

ARP works between layer 2 and layer 3 of the open System Interconnection model (OSI model). The MAC address exists on layer 2 of the OSI ~~layer~~ model, the data link layer. The IP address exists on layer 3, the network layer.

ARP can also be used for IP over other LAN technologies, such as token ring, Fiber Distributed Data interface and IP over Asynchronous Transfer Mode.

Que: What is a mac-address?

Ans: A MAC (Media Access control) address, sometimes referred to as a hardware or physical address is a unique 12-character alphanumeric attribute that is used to identify individual electronic ~~value~~ devic on a network. An example of a MAC address is: 00-B0-D0-63-C2-26.

Que: What is a firewall to use for?

Ans: Firewalls provide protection against outside cyber attacks by shielding your computer or network from malicious or unnecessary network traffic. Firewalls can also prevent malicious software from accessing a computer or network via the internet. Firewalls can be configured to block data from certain locations (i.e. computer network addresses), applications, or ports while allowing relevant and necessary data

Page No.:
Date:

Que:- What is the port number?

Ans:- A port number is a way to identify a specific process to which an internet or other network message is to be forwarded when it arrives at a server. All network-connected devices come equipped with standardized ports that have an assigned number. These numbers are reserved for certain protocols and their associated function. Hypertext Transfer protocol (HTTP) messages for example, always go to port 80.

Que:- Explain DHCP Dynamic host configuration protocol, Explain Domain naming services and what is protocol?

Ans:- Dynamic Host Configuration protocol (DHCP):- DHCP is a network protocol that automates the assignment of IP addresses and configuration settings to devices, allowing them to join a network seamlessly without manual intervention.

Domain Name System (DNS):- DNS is a system translating human-readable domain names into IP addresses, facilitating user-friendly web browsing by providing a directory for internet resources

Protocol:- A protocol is a set of rules defining how data is transmitted and received over a network, ensuring standardized and effecient

Communication between devices in various networking contents.

Que: Inlirless router configure for internet connection and wireless security? what is a wireless access point? what is a wireless extender?

Ans: Wireless router configuration:- Configure a router for internet connection by accessing its web interface, setting up WAN settings, and configuring wireless parameters for security. Ensure firmware is updated for optimal functionality.

Wireless Access point (WAP): A wireless access point facilitates wireless device connection to a wired network, extending coverage. It operates by receiving and retransmitting wi-fi signals, enabling devices to access the network without physical cables.

Wireless extender :- A wi-fi range extender amplifies and rebroadcasts existing wi-fi signals, expanding coverage to areas with weak reception. It's useful in eliminating dead zones and improving connectivity in larger spaces where the router's signal is insufficient.

Que: Straight cable standard sequence 568 A and 568 B

Ans: 568 A :-

white - Green
Green
White - orange
Blue
White - Blue
Orange
White - Brown
Brown

568 B :-

White - Orange
Orange
White - Green
Blue
White - Blue
Green
White - Brown
Brown

Que: Define list of cables in use of network - Twisted pair, fiber optics.

Ans: Twisted Pair :-

- Twisted pair is a physical media consisting of a twisted pair of cables.
- Compared to other transmission media, a twisted cable is inexpensive. The twisted cable is easy to mount and is lightweight cable.

- The frequency range for twisted pair cable is from 0 to 3.5KHz.

Types of twisted pair cables:

Unshielded twisted pair :- An unshielded twisted pair is widely used in telecommunication. Following are the categories of an unshielded twisted pair cable:

Category 1 : Category 1 is used for telephone line that have low-speed data.

Category 2 : It can support upto 4 Mbps.

Category 3 : It can support upto 16 Mbps.

Category 4 : It can support upto 20 Mbps. Therefore, it can be used for long-distance communication.

Category 5 : It can support upto 200 Mbps.

Advantage:

- It is Cheap
- Installation of the unshielded twisted pair is easy.
- It can be used for high-speed LAN.

Disadvantage:

This cable can only be used for short distances because of attenuation.

Shielded Twisted Pair: A shielded twisted pair is a cable that contains the mesh surrounding the wire that allows the higher transmission rate.

Characteristics of shielded twisted pair:-

- The cost of the shielded twisted pair cable is not very high and not very low.
- An installation of STP is easy.
- It has higher capacity.
- It has higher attenuation.
- It is shielded that provides the higher data transmission rate.

Disadvantage:

- It is more expensive as compared to UTP and coaxial cable.
- It has a higher attenuation rate.

Fiber optic:-

- Fiber optic cable is a communication cable which uses electrical signals
- Fiber optics is a cable containing the plastic coated fibres that transmit the data through light pulses
- The plastic layer avoids heat, cold, electromagnetic of the optical fibres from other cables.
- Fiber optics provide faster data than copper wires.

Date:

Que: Explain types of network - LAN, MAN, WAN?

Ans: LAN :- A local area network (LAN) is a network contained within a small geographic area, usually within the same building. Home wifi networks and small business networks are common examples of LANs.

LANs can also be fairly large, although if they take up multiple buildings, it is usually more accurate to classify them as wide area network (WAN) or metropolitan area network (MAN).

WAN :- A wide-area network is a technology that connects offices, data centers, cloud applications, and storage across a specific geographic area or the world. It spans beyond a single building or large campus, making it useful for businesses with international branch offices. The world's largest WAN is the internet, which consist of many international networks.

MAN :- A metropolitan area network is a computer network connecting computers within a metropolitan area, larger than a local area network but smaller than

Que: What is unicast, multicast and broadcast?

Ans: Unicast : In unicast communication, data is sent from a single sender to a specific

receiver over a dedicated connection. This method ensures that the intended recipient receives and processes the information, making it suitable for applications like web browsing, email and file transfers.

Multicast: Multicast enables one to many or many to many communication by sending a single copy of data to a predefined multicast group. Devices interested in the data can join the group, optimizing bandwidth usage. Common application includes video streaming, online conferencing, and online gaming.

Broadcast: In broadcast communication, data is sent from one sender to all devices in the network, irrespective of their interest in the information. While broadcast was more prevalent in older network technologies like Ethernet, it is now less commonly used in modern network due to its potential for causing unnecessary network congestion.

Que: Difference between TCP/IP and OSI layer.

Ans:

TCP/IP	OSI Model.
• Full form of TCP/IP is Transmission Control protocol / Internet protocol.	• Full form of OSI is Open System Interconnection.

• It is a communication protocol that is based on standard protocol and allows the connection of hosts over a network.	• It is a structured model which deals which the functioning of a network.
• It comprises of four layers : Network interface, Internet, Transport, Application.	• It comprises seven layers : Physical, Data link, Network, Transport, session, presentation, Application.
• It follows a horizontal approach.	• It follows a vertical approach
• It is protocol dependent.	• It is protocol independent.

Que: Difference between TCP and UDP. What is session development?

~~Ans~~:

Ans: Session development involves creating, managing and securing communication sessions, ensuring that data exchange between entities is efficient and reliable. It can encompass various protocol, including both TCP and UDP, depending on the requirements of the application.

TCP	UDP
· Transmission control protocol	· User datagram protocol.
· Connection oriented	· Connection less.
· Support ACK's	· No support for ACK's
· Reliable communication	· Unreliable communication.
· Slower data transportation.	· Faster data transportation.
· Protocol No. is 6	· Protocol No. is 17.
· Eg:- HTTP, FTP, SMTP	· Eg:- DNS, DHCP, TFTP.

Que: What is OSI model?

Ans: The OSI model is a conceptual framework that standardize the function of a telecommunication or computing system into seven abstraction layers. It was developed by International organization for standardization (ISO).

(i) physical layer: This layer deals with the physical connection between devices. It defines the hardware elements such as cables, connectors and electrical signals.

(ii) Data link layer: Responsible for creating a reliable link between two directly connected nodes. It includes sublayers for addressing (MAC addresses) and error detection.

(iii) Network layer: This layer handles the routing of data between devices across different networks. It is concerned with logical addressing and determining the optimal path for data transfer.

(iv) Transport layer: Responsible for end-to-end communication and data flow control. It ensures that data is delivered reliably and in correct order.

(v) Session layer: Manages sessions or connection between application on different devices.

(vi) Presentation layer: Concerned with the format and representation of data during communication. It translates between the application layer and the lower layers, handling issues such as encryption, compression and data formatting.

(vii) Application layer: This is the topmost layer and is closest to the end user. It provides network services directly to applications.

Page No.:
Date:

Que: What is an ip address? Difference between ipv4 address and ipv6 address? Assign multiple ipv4 in a single network adapter in pc? what are network vulnerabilities?

Ans: IP address: An IP address is a unique numerical identifier assigned by an ISP to every device or network connected to the internet, used for communication across the internet.

IPV4	IPV6
• IPV4 has a 32 bit address length.	• IPV6 has a 128 bit address length.
• It supports manual and DHCP address configuration.	• It supports Auto and renumbering address configuration.
• It can generate 4.29 x 109 address space.	• The address space of IPV6 is quite large it can produce 3.4 x 1038 address space.
• The security feature is dependent on the application	• IPSEC is an inbuilt security protocol. feature in the IPV6 ~~network~~.
• Address representation of IPV4 is in decimal.	• Address representation of IPV6 is in hexa decimal.

• In IPV4 packet flow identification is not available.	• In IPV6 packet flow identification are available and uses the flow label field in the header.
• In IPV4 checksum field is available.	• In IPV6 checksum field is not available.
• It has broadcast message transmission scheme.	• In IPV6 multicast and anycast message transmission scheme is available.
• In IPV4 encryption and authentication facility not provided.	• In IPV6 encryption and authentication are provided.
• IPV4 can be converted to IPV6.	• Not all IPV6 can be converted to IPV4.

Steps to add second IP address to existing network:

→ Use the Start menu to open the control panel.

→ On windows XP, you may need to open Network and Internet Connections.

→ Open Network (and Dial-up) connections.

→ Open your network adapter.

→ Click properties.

→ Click Internet protocol (TCP/IP) then click properties.

→ Click Advanced.

→ On the IP setting tab, click Add

→ Type in the new IP address then click Add.

→ Click ok to close the Advanced TCP/IP setting window.

→ Click ok to close the internet protocol (TCP/IP) properties window.

→ Click ok to close ~~the internet protocol (TCP/IP)~~ your network adapter properties window.

Network Vulnerabilities :- A network vulnerability is a weakness or flaw in software, hardware or organizational process, which when compromised by a threat, can result in a security breach.