N+ Assignment

DATE:
PAGE:

Module-1

1) What is network?

→ A Computer Network is a group of interconnected nodes or Computing devices that exchange data and resources with each other.

→ Network Connection between these devices can be established using Cable or Wireless media.

→ once a connection is established, Communication protocols -- such as a TCP/IP, Simple Mail Transfer Protocol and Hypertext Transfer protocol are used to exchanges data between the networked devices.

2) Explain type of Network - LAN, MAN, WAN

* LAN (Local Area Network)

→ LAN interconnect endpoint in a single domain.

→ Network is a group of two or more connected computers and a LAN is a network contained within a small geographic area, usually within the same building.

DATE:
PAGE:

* MAN

→ Metropolitan area network is a computer network that connects computers within metropolitan area, which could be a single large city, multiple cities and town, or any given large area with multiple buildings.

* WAN

→ Wide Area network is a large computer over large distance. WANs are often used by large businesses to connect their office networks.

3) What is Internet?

→ Internet is global Network that connects billions of computers across the world with each other and to the world wide web.

→ It uses standard internet protocol suite 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, internet is the fastest mean of sending or exchanging Information and data between compiteers across the Woorld.

4) Define Network Topologies ?

→ Network topology refers to the Physical and logical arrangement of nodes and connections in a Computing network.

→ Physical topology describes the layout of devices and Cables. and logical topology describes the way in which data is transmitted within the network regardless of the physical layout.

- Bus Network
- Star Network
- Ring Network
- Mesh Network
- Tree Network
- Hybrid Network

5) Define list of Cables in use of Network - Twisted Pair, Fiber optic

→ Cable is the medium through which information usually moves from one network devic to another.

There are several types of Cable which are commonly used with LANs.

- Unshielded Twisted pair (UTP) Cable
- Shielded Twisted pair (STP) Cable
- Coaxial Cable.
- Fiber optic Cable.
- [redacted]

⇒ Twisted Pair Cables.

- Twisted Pair cables have two conductors that are generally made up of copper and each conductor has insulation.

- These two conductors are twisted together. thus giving the name twisted Pair cables.

- one of the conductors is used to carry the signal and the other is used as a ground reference only.

→ The receiver uses the difference of signals between these two conductors

DATE:
PAGE:

Unshieleded UTP

These are apair of two insulated copper wires twisted together without any other insulation or shielding and hence are called Unshielded twisted pair cables.

Shielded (STP) :-

→ These types of cable have extra insulation or protective covering over the conductors in the form of a copper braid covering.

Fiber optics

→ An optical fiber is a cylindrical fiber of glass which is hair thin size or any transparent dielectric medium.

→ The fiber which is used for Optical communication is waveguides made of transparent dielectries

6) Straight Cable Standard Sequence 568 A and 568 B.

→ T568A and T568B the main difference between these two standard is the position of the orange and green wire pairs.

→ Make sure that the copper strips should be toward your face when you match the connection same as.

7) What is fiber optics module and fiber connector.

→ optical module, also called fiber optic transceiver or optical transeeiver, is a typically hot-pluggable device used in high-bandwidth data communicetions applications.

→ An optical module functions as a photoelectric converter which converts the electrical signal into light and vice versa.

→ Fiber optic connectors is a detachable device between optical fibers.

→ It precisely connects the two end faces of the optical fiber so that the optical energy output by the transmitting fiber can be coupled to the receiving fibers to the maximum extent.

8) Explain Switch.

→ Switches are networking devices operating at layer 2 or a data link layer of the OSI model.

→ They connect devices in a network and use packet switching to send, receive or forward data packets or data frames over the network.

→ Switch has many ports to which computers are plugged in. When a data frame arrives at any port of a network switch, it examines the destination address, performs necessary checks and sends the frame to the corresponding device. It supports unicast, multicast, as well as boadcast comm

9) Explain Router.

→ The router is a physical or virtual internetworking device that is designed to receive, analyze, and forward data packets between computer networks.

→ A router examines a destination IP address of a given data packet, and it uses the headers and forwarding table to decide the best way to transfer the packets.

→ Router works on the third layer of the OSI model. router is a intelligent device as it can calculate the best route to pass the network packets from source to the destination automatically.

10) Explain MODEM ?

→ A modem is a hardware which connects to a computer, broadband network or wireless router.

→ Modem converts information between analogue and digital formats in real time making seamless two-way network communication

→ The full form of Modem stands for Modulator - demodulator.

→ Modulation is performed to extend the frequency of the signal for propagation at production purpose, whereas demodulation is performed at receiving purpose to bring down the signal to its original level.

11) Explain DHCP: Dynamic host Configuration Protocol.

→ DHCP is a network management protocol used to dynamically assign an IP address to any device, or node, on a network so it can communicate using IP.

→ DHCP automates and centrally manages these configurations rather then requiring network administrator to manually assign IP addresses to all network devices.

→ DHCP can be implemented on small local Network, as well as large enterprise networks.

→ DHCP assigns new IP addresses in each location when device are moved from place to place.

12) Explain Domain Nameing Services.

→ An application layer Protocol defines how the application process es running on different system, pass the messeges to each other.

→ DNS - Domain Name System.

- DNS is directory Serivce that provides a mapping between the name of a host on the Network and its Numerical address.

→ DNS is required for the functioning of the internet.

13) What is Protocol ?

→ Protocol is a set of rules for formatting and Processing data.

→ Network Protocols are like a common language for computers. The Computers within a network may use vastly different software and hardware.

→ However, the use of protocols enable them to communicate with each other regardless.

14) What is Unicast multicast and broadcast

⇒ In Unicast transmission, the data is transferred from a single sender to a single receiver.

⇒ In Broadcast transmission, the data is transmitted from one or more senders to all the receivers within the same network or in other Networks.

→ This type of transmission is useful in network management Packets such as ARP and RIP where all the devices must see the data.

⇒ Multicast Transmission

→ When the data is transmitted from a single source host to a specific group of hosts having the interest to receive the data, it is known as multicast transmission.

→ Multicast can be more efficient then Unicast.

15) What IS OSI Model?

→ The open systems Interconnection model describes seven layers that computer systems use to communicate over a network.

→ It was the first standard model for network communications, adopted by all major computer and telecommunication companies in the early 1980s.

→ OSI Model Contained 7 layers

7. application layer
6. Presentation layer
5. Session layer
4. Transport layer
3. Network layer
2. Data link layer
1. Physical layer

→ We'll describe OSI layers "top down" from the application layer that directly serves the end user, down to the physical layer.

16) What is Port Number?

→ 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.

→ The reason why they are reserved is for certain protocols and their associated function.

→ Hypertext Protocol (HTTP) Messages for example, always go to port 80 one of the most commonly used ports.

→ Advanced Research Project Agency Network, is an informal co-operation of system administrator and software authors, developers of proposed the concept of Port Numbers.

→ Previously Port Numbers were known as Socket Numbers. the early interconnection of Port Numbers is similar to the IP add. class

1.1) Difference between TCP vis UDP Communications.

TCP → TCP is a connection-oriented Protocol.

UDP → UDP is the datagram-oriented Protocol.

TCP → TCP is reliable as it guarantees the delivery of data to the destination router.

UDP → The delivery of data to the destination cannot be guaranteed in UDP.

TCP → TCP Provides extensive error-checking mechanisms. It is because it Provides flow control and acknowledgment of data.

UDP → UDP has only the basic error-Checking mechanism Using checksums.

TCP- An acknowledgment Segment is Present.

UDP → NO Acknowledgment Segment.

TCP → TCP is comparatively slower the UDP.

UDP- UDP is faster, simple, and more efficient than TCP.

TCP- TCP has a 20 bytes Variable length header.

UDP- UDP has an 8 bytes fixed-length header.

TCP- TCP is heavy-weight

UDP- UDP is lightweight.

TCP- TCP doesn't Support Broadcasting

UDP- UDP Supports Broadcasting.

TCP- The TCP connection is a byte stream

UDP- UDP Connection is a message stream.

18) What is Session development?

→ A session development is total time devoted to an activity. In Computer systems, a User session begins when a User logs in to or accesses a particular Computer Network or Software service.

→ A session can temporarily store information related to the activities of the user connected.

19) What is flow control?

→ In a network, the sender sends the data and the receiver receives the data.

→ But suppose a situation where the sender is sending the data a speed higher than the receiver is able to receive and process it, then the data will get lost.

→ Flow-control methods will help in ensuring this. The flow control method will keep a check that the senders send the data only at a speed that the receiver is able to receive and process.

→ [illegible]

20) Difference between TCP [illegible]
communications

20) What is the difference between TCP IP Model and OSI Model ?

OSI → OSI represents open system Interconnection.

TCP/IP → TCP/IP Model represents the transmission control protocol Internet protocol.

OSI → It provides quality services

TCP/IP → It does not provide quality services.

OSI → The OSI model was developed first and then protocols were created to fit the network architecture's needs.

TCP/IP → The protocols were created first and then built the TCP/IP model.

OSI → It is difficult as distinguished to TCP/IP.

TCP/IP → It is simpler then OSI.

OSI → It uses a Vertical approach.

TCP-IP → It uses a horizontal approach

OSI → The Smallest Size of the OSI header is 5 bytes.

TCP/IP → The Smallest Size of the TCP/IP header is 20 bytes.

OSI → Protocols are Unknown in the OSI model and are returned while the technology modifies.

TCP/IP → In TCP/IP, returning protocol is not difficult.

21) What is arp broadcast?

→ ARP broadcasts a request Packet to all the machines on the LAN and asks if any of the machines are using that particular IP address.

→ When a machine recognizes the IP address as its own, it sends a reply so ARP can update the cache for future reference and proceed with the communication.

22) What is mac - address ?

→ Mac address is the Physical address, which Uniquely identifies each device on a given network.

→ To make Communication between Make Communication between two networked devices, we need two addresses : IP address and Mac address.

→ It is assigned to the NIC of each device that can be connected to the internet.

→ It stands for Media Access Control, and also known as Physical address, hardware address.

→ It is 12-digit and 48 bits long. first 24 bits are used for OUI and 24 bits are NIC vendor Specific.

→ two device Cannot have the same Mac address. It is represented in a hexadecimal format on each device such as 00:0a:95:9d:68:16.

→ It works on the data link layer of the OSI Model.

23) What is ip address ? Difference between ipv4 addr

→ IP Stands four internet protocol. An IP address is assigned to each device uses an IP address for communication.

→ It also behaves as an identifies as this address is used to identify the device on a network. It defines the technical format of the packets.

IPV4	IPV6
→ IPv4 is Version 4 of IP	→ IPv6 is the next generation of IP addresses
→ IPv4 is a 32-bit address	→ IPv6 is a 128 bit address.
→ IPv4 is a numeric address that consists of 4 fields which are separated by dot(.).	→ IPv6 is an alphanumeric address that consists of 8 fields, which are separated by colon.
→ IPv4 has a limited number of IP addresses	→ IPv6 has a huge number of IP addresses.

IPV4	IPV6
→ It Supports VLSM Here VLSM means that IPV4 converts IP address into a subnet of different sizes	→ It does not Support VLSM.
→ It Supports manual and DHCP configuration	→ It Supports manual, DHCP, auto-configuration and renumbering.
→ It generates 4 billion Unique addresses	→ It generates 340 Undecillion Unique addresses.
→ end to end connection integrity is Unachievable	→ end to end connection integrity is achievable.
→ IP address is represented in decimal.	→ IP address is represented in hexadecimal.
→ It does not provide encryption and authentication.	→ It Provides encryption and authentication
→ IPV4 is broadcasting	→ IPV6 is multicasting which Provides efficient network operation.

DATE:
PAGE:

24) Assign multiple IPV4 in single network in PC.

→ Double click the Ethernet or wifi connection.

→ In the Status Windows press Properties.

→ Select Internet Protocol Version 4 (TCP\IPV4) in the list and Press Properties.

→ Switch the selector to use the following IP address.

→ Manually specify IP, Subnet mask, Default gateway and preferred DNS Server.

→ The Press Advanced.

→ click Add button.

→ Specify additional IP addresses with Subnet masks and Press Add.

→ Press Ok!

→ Press ok once more.

→ Press close.

In such a way you can add a bunch of IP addresses to single network

25) What are network Vulnerabilities

→ A network Vulnerability is a weakness or flaw in software, hardware, or organizational processes which when compromised by a threat, can result in a security breach.

→ Nonphysical network Vulnerabilities typically involve software or data.

→ Physical Network Vulnerabilities involve the physical protection of an asset such as locking a server in a rack closet or securing an entry point with a turnstile.

26) What is a firewall to use for?

→ A firewall is a security system designed to prevent unauthorized access into or out of a Computer Network.

→ firewalls are often used to make sure internet users without access are not able to interface with private networks, or intranets, connected to the internet.

→ A firewall is positioned between a network or a computer and a different network, like the internet.

27) Wireless router Configure four internet connection and wireless security.

→ Purchase a Wireless router.

→ Connect the Cables.

→ Connect it to your existing Internet modem.

→ Connect an Ethernet Cable from your modem to the Wireless router.

→ Plug in the Power Cable For the wireless router.

→ Wait at least 30 to 60 seconds, and make sure the lights on your router are working correctly.

→ Using your Web browser, enter the router's default IP address into the address bar then Press Enter.

→ The router's sign-in page will appear. Sign in using Admin and Password.

→ Locate and select the Network Name setting, then enter a unique network name.

→ Locate and select the Network Password setting, and choose an Encryption option.

→ Enter your desired Password. Make sure to use a strong password to help ensure no one else can access your network.

→ Locate and select the Save button to save your settings.

→ That's it! Now you're ready to connect to your wi-fi Network and make sure it's working.

→ Locate your computer's Network Settings, and search for nearby wi-fi networks.

→ Select your Network, and enter your Password.

→ If the connection is successful.

DATE:
PAGE:

28) What is Wireless access point?

→ A wireless Access point is a network device that allows Connecting the devices with the wired Network.

→ A Wireless Access Point (WAP) is used to Create the WLAN.

→ It is Commonly Used in large offices and buildings which have expanded businesses.

→ A WAP connect the Wired Networks to the Wireless Client. It casses access to the network for mobile users which increases Productivity and reduces the infrastructure cost.

29) What is Wireless extender?

→ Wireless extender is a device between base router or wireless LAN access point and Client Computer or device that is outside the signal range or blocked by signal barriers.

→ The extender work as a wireless relay or repeater by receiving access point signals which retransmitted the client.