**Tops Technology**

**Q1. What is network ?**

Ans. Two or more computer connected together, which can communicate with each other.

**Q2. Explain types of network - LAN, MAN, WAN ?**

Ans.

1. LAN - (Local Area Network) LAN is a group of computer connected together usually in the same building, these connections are relatively fast and inexpensive.
2. MAN - (Metropolitan Area Network) MAN is a larger network consisting many buildings in the same area. Basically MAN is a group of several LAN network.
3. WAN - (Wide Area Network) WAN is a network which is not restricted to a geographical location. Connecting many organizations and institutions together across the continent. WAN is a group several LAN network combined together. It is fast speed and relatively expensive.

**Q3. What is Internet ?**

Ans. Internet is a vast group of computers interconnected with each other through which they can communicate with each other using internet protocol suite i.e TCP/IP.

**Q4. What is OSI model ?**

Ans. OSI Model (Open System Interconnection) is a architecture consist of 7 layers, in which first three layers are Software layer (Application, Presentation, Session layer) after it comes the core layer that is Transport layer, and the third ad the last stage is Hardware layer (Network, Data Link, Physical layer) :

1. Application layer : this layer is responsible for providing an interface to the user to interact with the system. For example web browser, telnet.
2. Presentation layer : it is responsible for defining a standard format to the data. It deals with data presentation. As well as it is responsible for the “encoding-decoding”, “encrypt-decrypt”, “compress-decompress”.
3. Session layer : this layer is responsible for establishing and terminating the session between to devices. For example RPC(Remote procedural call), SQL(Structured query language).
4. Transport Layer : this layer is responsible for deciding if the data should be on single or parallel path; multiplexing, segmenting and splitting of the data is done on this layer as well. Transport layer makes segments of the data for the better handling and efficiency. Moreover, It is also responsible for providing any packet of data lost during the transmission or in case of any error again to the data link layer. As well as it also provides header for the data for recognition and categorization of the data.
5. Network Layer : this layer routes the data from one node to another node, it is also responsible for deciding the fastest route for the data to travel. This layer also divides the outgoing data into packets and assembles the incoming packets into messages for higher level.
6. Data Link layer : it responsible synchronizing the information which is to be transmitted over the physical layer; The most important feature of this layer is to make sure that data is error free from one node to another node over the physical layer. Acknowledgments are also conveyed through this layer.
7. Physical Layer : the last layer of the OSI model it activates, maintains and deactivates the physical connection. It also converts digital and analog signals to electrical or optical signals. As well as data encoding is also done in this layer.

**Q5. Explain Switch ?**

Ans. Switches are very similar to a hub, but they are much more advance when it comes to manage the internet traffic, it learns the incoming internet traffic and then directs the packets to the specified computer through specified ports.

**Q6. What is MAC-address ?**

Ans. MAC address (Media Access Control) is a physical identification 48 bit hardware number provided to the NIC (Network Interface Card) and during manufacturing process. Its works at the data link layer.

**Q7. Explain Router ?**

Ans. Router is a hardware device designed to receive, analyze and move incoming packets to and from another network. It can also be used to convert the packets to another network interface, drop them as well as it can perform other actions related to network. Unlike switches and hub which are not able to analyze the incoming and outgoing traffic, routers can analyze the packets being sent over a network and can also change how it is packed, and send it to a different network.

**Q8. What is 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 comes equipped with standardized ports that have an assigned number. These numbers are reserved for certain protocols and their associated function.

**Q9. Explain Modem ?**

Ans. Modem is a device that allows computer to connect to internet and communicate with other computers by converting digital signals into analog signals and vice versa. It is also known as “Modulator-Demodulator”.

**Q10. What is Flow Control ?**

Ans. A flow control mechanism to avoid a fast transmitter from running a slow receiver by buffering the extra bit is provided by flow control. This prevents traffic jam at the receiver side. It works on the data link layer.

**Q11. What is ARP Broadcast ?**

Ans. ARP(Address Resolution Protocol) is a request packet which is send over the network to a specific IP to check if that IP is available on the network or not.

**Q12. Define list of cables in use of network—Twisted pair , fiber optics ?**

Ans.

1. Twisted pair : This type of cable is most commonly used type of cable and also this is the cheapest available cable among other options. In Twisted pair cable there are two types of cable available.

* Unshielded Twisted Pair - This is the most common type of telecommunication cable consisting of two conductors usually copper, each with its own colour plastic insulator. The identification is the reason behind the coloured plastic insulation. It comes in 2 or 4 pair of twisted cable. Cable with two pair is for Rj11; whereas, 4 pair is for Rj45 connector respectively. Advantages of the cable are easy to use, cheap, flexible, high speed. However, there are disadvantages as well low bandwidth, less protection from interference, not weather proof.
* Shielded Twisted Pair - This type of cable is similar to the unshielded twisted pair, except for the part that in this each twisted pair is covered in metal foil or braided mesh covering which prevents “Electromagnetic noise penetration” as well as “Crosstalk”. Advantages of this type are adequate performance, increased signal rate eliminates crosstalk, higher capacity than UNTP. However, there is only one disadvantage that it is difficult to manufacture due to added weight to it.

1. Fiber Optics : These are similar to coaxial cable. It uses electric signals to transmit data. Except it is made up of different material. At the center of the cable it’s a glass core through which light travels. There are two types of fiber cables “multi mode” and “Single mode”. There are both advantages and disadvantages of the fiber optic cable, it provides high quality transmission of signals at very high speed, not affected by the electromagnetic signals so no chances of interference, used for both analog and digital signals; however, it is very expensive and difficult to install and maintain, it has its limitations as it cannot completely route light signals.

**Q13. What is unicast multicast and broadcast?**

Ans.

* Unicast : this is a one to one transmission of data from one sender to one receiver in a network. The sender and receiver are identified by network addresses, and other devices on the network do no participate. The internet uses unicast to route messages from one IP address to another, insuring that the information reached the intended destination. In basic terms it takes packet from the host Ip which has the destination Ip into it and then unicast will only deliver the packet to that particular Ip.
* Multicast : multicast can be one-to-many or many-to-many distribution. For example, a single source can send to multiple recipients on a network when the receiver broadcasts a signal for acceptance.
* Broadcast : Broadcasting is a method used in computer networking that allows a message to be sent simultaneously to every member of the network. It is the most thorough and all-encompassing kind of communication. Similar to a mailing list where the recipients are hidden, broadcasting operates in a similar way. The data must be received and processed by the network's component parts.

**Q14. What is the difference between TCP/IP model and OSI model?**

Ans.

|  |  |
| --- | --- |
| **TCP/IP** | **OSI** |
| * TCP/IP model is based on standard protocols around which the internet has developed. It is a communication protocol, which allows connection of hosts over a network. | * OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user. |
| * In TCP/IP model the transport layer doesn’t guarantees delivery of packets. Still the TCP/IP model is more reliable. | * In OSI model the transport layer guarantees the delivery of the packet. |
| * TCP/IP doesn’t have a separate presentation layer or session layer. | * OSI model has a separate presentation layer. |
| * Follows horizontal approach. | * Follows vertical layer. |

**Q15. Straight cable standard sequence 568 A and 568 B ?**

Ans. The only difference between T568A and T568B is the order in which the wires connect to the RJ45 jack. In T568A, the green wire connects to pin three and the orange wire connects to pin six. In T568B, the orange wire connects to pin three and the green wire connects to pin six. All the other wires connect to the same pins in both standards. From a technical standpoint, there is no difference between T568A and T568B. Both standards have the same transmission performance and can support the same Ethernet protocols, including Gigabit Ethernet.

* 568-A :

1. white green
2. green
3. white orange
4. blue
5. white blue
6. orange
7. white brown
8. Brown

* 568-B :

1. white orange
2. orange
3. white green
4. blue
5. white blue
6. green
7. white brown
8. Brown

**Q16. What is fiber optics module and fiber connector ?**

Ans.

* Fiber optic module -  is a small, self-contained device that transmits and receives light pulses over optical fiber cables. It's a key component in fiber optic communication systems, converting electrical signals into light pulses that can be transmitted over long distances.
* Fiber connector - is a device that links optical fibers to allow for efficient light signal transmission. They are often used to terminate optical fiber cables and provide removable fiber joints between fiber-coupled devices.

**Q17. Difference between TCP V/S UDP communications. What is session**

**development?**

Ans.

* TCP - is a connection-oriented protocol. Connection orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data.
* UDP - is the Datagram-oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, or terminating a connection. UDP is efficient for broadcast and multicast types of network transmission.
* Session Development - is a temporary, two-way link between two or more devices that communicate over a network. Sessions are a layer in the TCP/IP protocol that allow devices to exchange information and interact. A session is established at a certain time and then ended at a later time.

|  |  |
| --- | --- |
| **TCP** | **UDP** |
| TCP is reliable as it guarantees the delivery of data to the destination router. | The delivery of data to the destination cannot be guaranteed in UDP. |
| TCP provides extensive error-checking mechanisms.  It is because it provides flow control and acknowledgment of data. | UDP has only the basic error-checking mechanism using checksum. |
| An acknowledgment segment is present. | No acknowledgment segment. |
| Sequencing of data is a feature of Transmission Control  Protocol (TCP). this means that packets arrive in order at the receiver. | There is no sequencing of data in UDP. If the order is required, it has to be managed by the application layer. |
| TCP is comparatively slower than UDP. | UDP is faster, simpler, and more efficient than TCP. |
| Retransmission of lost packets is possible in TCP, but not in UDP. | There is no retransmission of lost packets in the User Datagram Protocol (UDP). |
| TCP has a (20-60) bytes variable length header. | UDP has an 8 bytes fixed-length header. |
| TCP doesn’t support Broadcasting. | UDP supports Broadcasting. |
| TCP is used by [HTTP, HTTPs](https://www.geeksforgeeks.org/difference-between-http-and-https-2/),[FTP](https://www.geeksforgeeks.org/file-transfer-protocol-ftp/), [SMTP](https://www.geeksforgeeks.org/simple-mail-transfer-protocol-smtp/) and [Telnet](https://www.geeksforgeeks.org/introduction-to-telnet/). | UDP is used by [DNS](https://www.geeksforgeeks.org/details-on-dns/), [DHCP](https://www.geeksforgeeks.org/dynamic-host-configuration-protocol-dhcp/), TFTP, [SNMP](https://www.geeksforgeeks.org/simple-network-management-protocol-snmp/), [RIP](https://www.geeksforgeeks.org/routing-information-protocol-rip/), and [VoIP](https://www.geeksforgeeks.org/voice-over-internet-protocol-voip/). |

**Q18. What is the use of firewall?**

Ans. A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It's a barrier between a trusted network and an untrusted network, such as the internet. As well as it used to protect networks from cyberattacks, such as malware attacks and hacking attempts. They can also be used to control and block access to certain websites and online services. Firewalls can be hardware, software, or a virtual private cloud. They can be used in both corporate and consumer settings.

**Q19. Define Network Topologies ?**

Ans. There are total 7 types of network topologies :

1. Point to point - It is a protocol which is used as a communication link between two devices. It is a simple setup. The most common example for (PPP) is a computer connected by telephone line.
2. Bus - Bus topology is a network type in which every computer and network device is connected to single cable. When it has two endpoints, then it’s called Linear bus topology. It Transmit data in one direction only, it is also cheap. Used in small networks. However, if something happens to the cable then the whole network will fail, if network traffic is heavy then the performance of the network will also decrease, cable has limited length.
3. Star - Is a type of topology in which all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node. Fast performance, easy to troubleshoot, can be easily upgraded. However, cost of installation is high, expensive to use, performance is based on the hub that depends upon the hub capacity.
4. Ring - It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first PC. Exactly two neighbors for each device. Cheap to install and expand, transmitting network is not affected by high traffic or by adding more nodes as only the nodes having tokens can transmit data. However, troubleshooting is difficult in ring topology, adding or deleting the computers disturb the network activity.
5. Mesh - It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. Mesh has n(n-2)/2 physical channels to link n devices. There are two techniques to transmit data over the Mesh topology, they are :

* Routing - In routing, the nodes have a routing logic, as per the network requirements. Like routing logic to direct the data to reach the destination using the shortest distance. Or, routing logic which has information about the broken links, and it avoids those node etc. We can even have routing logic, to re-configure the failed nodes.
* Flooding - In flooding, the same data is transmitted to all the network nodes, hence no routing logic is required. The network is robust, and the its very unlikely to lose the data. But it leads to unwanted load over the network.

1. Tree - It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy. It is ideal if workstation are located in groups, used in WAN, it is also easy to maintain and manage as well as error detection becomes easier. However, there are quite some disadvantages as well like it is heavily cabled so it becomes costly, if central hub fails then the whole networks fail.
2. Hybrid - It is a mixture of two or more topologies combined together. This also inherits the advantages and disadvantages of the topologies included. For example, if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in hybrid topology(ring and star topology). These are some of the advantages of the Hybrid setup, scalable as size can be increased easily, it is also flexible. However there is one disadvantage of this setup is that it is complex in design.

**Q20. Explain DHCP Dynamic host configuration protocol. Explain Domain**

**Naming Services. What is protocol?**

Ans. DHCP is a network management protocol that once configured it will automatically assigns IP address to devices connected on that particular network, as well as it also provides the gateway IP of the router to the connected devices. DHCP stands for Direct Host Configuration Protocol (DHCP). DNS is a distributed naming service that translates domain name into IP addresses, which then further are used by browser to load internet pages, in simple terms DNS is used for giving a name to IP addresses so that it becomes easy for us humans to memorize needed pages, DNS stands for Domain Name Server (DNS). Protocols are set of rules for formatting and processing data, in networks there are many types of protocols, such as “FTP(File Transfer Protocol), HTTP(Hypertext Transfer Protocol), SMTP(Simple Mail Transfer Protocol). These are some of the protocols, all of these have their own purposes in a network.

**Q21. What is IP address? Difference between IPv4 address and IPv6 address.**

**Assign multiple IPv4 in single network adapter in PC. What are network**

**vulnerabilities?**

Ans. An IP address is a unique numerical value identification given to each and every device which can connect to the internet, IP addresses are made up of four numbers each ranging from 0 to 255.

Differences between IPv4 and IPv6 :

|  |  |
| --- | --- |
| **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 |
| In IPv4 end to end, connection integrity is Unachievable | In IPv6 end-to-end, connection integrity is Achievable |
| It can generate 4.29×10 to the power 9 address space | The address space of IPv6 is quite large it can produce 3.4×10 to the power 38 address space |
| Address representation of IPv4 is in decimal | Address Representation of IPv6 is in hexadecimal |
| In IPv4 Packet flow identification is not available | In IPv6 packet flow identification are Available and uses the flow label field in the header |
| IPv4 has a header of 20-60 bytes. | IPv6 has a header of 40 bytes fixed |
| IPv4 can be converted to IPv6 | Not all IPv6 can be converted to IPv4 |
| IPv4’s  IP addresses are divided into five different classes. Class A , Class B, Class C, Class D , Class E. | IPv6 does not have any classes of the IP address. |
| IPv4 supports VLSM | IPv6 does not support VLSM. |
| Example of IPv4:  192.168.30.2 | Example of IPv6: 2001:0000:3238:DFE1:0063:0000:0000:FEFB |

Assigning multiple IPv4 in single network adapter in PC :

Control panel > network and sharing > Ethernet/Wi-Fi > properties > IPv4 (TCP/IPv4) > click on it and select properties > Alternate > User Configuration. In here one can assign multiple IP address.

Network vulnerabilities are weaknesses or flaw in a network that can be exploited to gain unauthorized access and launch an attack. These weaknesses can be in hardware, software, or configuration settings. Such as, insecure wireless networks, removable media devices, outdated software, weak passwords, poorly configured firewall.

**Q22. Configure wireless router for internet connection and wireless security.**

**What is wireless access point? What is wireless extender?**

Ans.

Configuration of a wireless router :

1. Take one WRT300N router
2. Click on it and open GUI panel
3. Now go into wireless section of the router and select Basic wireless settings
4. Now give SSID name and then,
5. Go to wireless security panel and select security mode (WPA2 Personal) and enter your desired pass-phrase
6. Now save all the settings.
7. Now take Laptop-PT and remove its Ethernet port and add this module (PT-LAPTOP-NM-1W).
8. Now go to PC wireless in desktop
9. In the PC wireless
10. there it will show the configured router ready for connection.
11. Just add appropriate credentials and the laptop will just connect fine.
12. The end.

Wireless Access Point is a wireless communication hardware device that creates a central point of wireless connectivity. A wireless access point behaves much like a “hub” in that the total bandwidth is shared among all users for which the device is maintaining an active network connection.

A wireless extender, also known as Wi-Fi range extender, is a device which improves Wi-Fi by repeating and rebroadcasting router’s wireless signal to areas with weak or no Wi-Fi. Extenders are often used in larger homes or spaces with reduced coverage areas.