Assignment - 2

Q1. What are the difference types of Network?

Ans. We have 11 types of Network.

1. Personal Area Network (PAN)

The smallest and most basic type of network, a PAN is made up of a wireless modem, a computer or two, phones, printers, tablets, etc., and revolves around one person in one building. These types of networks are typically found in small offices or residences, and are managed by one person or organization from a single device.

2. Local Area Network (LAN)

We're confident that you've heard of these types of networks before – LANs are the most frequently discussed networks, one of the most common, one of the most original and one of the simplest types of networks. LANs connect groups of computers and low-voltage devices together across short distances (within a building or between a group of two or three buildings in close proximity to each other) to share information and resources. Enterprises typically manage and maintain LANs.

Using routers, LANs can connect to wide area networks (WANs, explained below) to rapidly and safely transfer data.

3. Wireless Local Area Network (WLAN)

Functioning like a LAN, WLANs make use of wireless network technology, such as Wi-Fi. Typically seen in the same types of applications as LANs, these types of networks don't require that devices rely on physical cables to connect to the network.

4. Campus Area Network (CAN)

Larger than LANs, but smaller than metropolitan area networks (MANs, explained below), these types of networks are typically seen in universities, large K-12 school districts or small businesses. They can be spread across several buildings that are fairly close to each other so users can share resources.

5. Metropolitan Area Network (MAN)

These types of networks are larger than LANs but smaller than WANs – and incorporate elements from both types of networks. MANs span an entire geographic area (typically a town or city, but sometimes a campus). Ownership and maintenance is handled by either a single person or company (a local council, a large company, etc.).

6. Wide Area Network (WAN)

Slightly more complex than a LAN, a WAN connects computers together across longer physical distances. This allows computers and low-voltage devices to be remotely connected to each other over one large network to communicate even when they're miles apart.

The Internet is the most basic example of a WAN, connecting all computers together around the world. Because of a WAN's vast reach, it is typically owned and maintained by multiple administrators or the public.

7. Storage-Area Network (SAN)

As a dedicated high-speed network that connects shared pools of storage devices to several servers, these types of networks don't rely on a LAN or WAN. Instead, they move storage resources away from the network and place them into their own high-performance network. SANs can be accessed in the same fashion as a drive attached to a server. Types of storage-area networks include converged, virtual and unified SANs.

8. System-Area Network (also known as SAN)

This term is fairly new within the past two decades. It is used to explain a relatively local network that is designed to provide high-speed connection in server-to-server applications (cluster environments), storage area networks

(called “SANs” as well) and processor-to-processor applications. The computers connected on a SAN operate as a single system at very high speeds.

9. Passive Optical Local Area Network (POLAN)

As an alternative to traditional switch-based Ethernet LANs, POLAN technology can be integrated into structured cabling to overcome concerns about supporting traditional Ethernet protocols and network applications such as PoE (Power over Ethernet). A point-to-multipoint LAN architecture, POLAN uses optical splitters to split an optical signal from one strand of single mode optical fiber into multiple signals to serve users and devices.

10. Enterprise Private Network (EPN)

These types of networks are built and owned by businesses that want to securely connect its various locations to share computer resources.

11. Virtual Private Network (VPN)

By extending a private network across the Internet, a VPN lets its users send and receive data as if their devices were connected to the private network – even if they’re not. Through a virtual point-to-point connection, users can access a private network remotely.

Q2. Explain the shielded twisted pair (STP) and Unshielded twisted pair (UTP) ?

Ans. **Definition of UTPCable**

UNSHIELDED TWISTED-PAIR (UTP) CABLE is the most prevalent type of telecommunication medium in use today. Its frequency range is suitable for transmitting both data and voice. Therefore, these are most commonly used in telephone systems.

A twisted pair consists of two insulated conductors (usually copper) in a twisted configuration. Color bands are used in plastic insulation for identification. In addition, colors also identify the specific conductors in a cable and to indicate which wires belong in pairs and how

they relate to other pairs in a larger bundle.

The two wires are twisted in the twisted pair cable which significantly reduces the noise generated by the external source.
The **NOISE** here we are talking about is generated when two wires are parallel which causes an increase in voltage level in the wire closest to the source and also uneven load and damaged signal.

Definition of STP Cable

SHIELDED TWISTED-PAIR (STP) CABLE has an additional braided mesh coating or metal foil that wraps each set of insulated conductors. The metal casing intercepts the penetration

of **ELECTROMAGNETIC NOISE.** It also can eradicate a phenomenon called crosstalk, which is the unwanted effect of one circuit (or channel) on another circuit (or channel).

It occurs when one line (acting as a kind of receiving antenna) picks up some of the signals travelling down another line (acting as a kind of sending antenna). This effect can be experienced during telephone conversations when one can hear other conversations in the background. Shielding each pair of a twisted-pair cable can eliminate most crosstalk.

STP has the similar quality factor and uses the same connectors as UTP, but the shield must be connected to the **GROUND**.

1.2 KEY DIFFERENCES BETWEEN UTP AND STP CABLES

1. UTP and STP are the types of twisted pair cable where UTP is the unshielded type whereas STP is shielded, for doing so metal foil or braided mesh is used.
2. UTP reduces the crosstalk and noise as compared to the parallel arrangement of the wires but not at great extent. On the contrary, STP decreases the crosstalk, noise, and electromagnetic interference significantly.
3. UTP cables are easily installed while installation of STP cables is difficult are the cables are bigger, heavier and stiffer.
4. Grounding is not required in UTP cables. As against, STP cables requires grounding.

5. UTP cables are inexpensive whereas STP cables are costly comparatively due to additional material and manufacturing.
6. STP cables incorporate a conducting shield built of metallic foil enclosing the twisted wire pairs, which obstructs out electromagnetic interference, permitting it to carry data at an enhanced rate of speed. In contrast, UTP provides less speed of data transfer.

1.2.1 Conclusion

UTP and STP cables differ in the design and structure where STP cable has an additional metal foil wrapped in insulated conductors.

However, both STP and UTP cables have their respective merits and demerits, when it comes to proper installation and maintenance in a suitable situation for their use, both work finely.

What is difference between baseband and broadband transmission?

Ans.

TO DIFFERENCE BETWEEN BASEBAND AND BROADBAND TRANSMISSION

The baseband and broadband are the types of signaling techniques. These terminologies were developed to categories different types of signals depending on particular kind of signal formats or modulation technique.

The prior difference between baseband transmission and broadband transmission is that in the baseband transmission the whole bandwidth of the cable is utilized by a single signal. Conversely, in the broadband

transmission, multiple signals are sent on multiple frequencies simultaneously using a single channel.

CONTENT: BASEBAND AND BROADBAND TRANSMISSION

1. Comparison Chart
2. Definition
3. Key Differences
4. Conclusion

Comparison Chart

BASIS FOR COMPARISON	BASEBAND TRANSMISSION	BROADBAND TRANSMISSION
Type of signaling used	Digital	Analog

BASIS FOR COMPARISON	BASEBAND TRANSMISSION	BROADBAND TRANSMISSION
Application	Work well with bus topology.	Used with a bus as well as tree topology.
Encoding Used	Manchester and Differential Manchester encoding.	PSK encoding.
Transmission	Bidirectional	Unidirectional
Signal range	Signals can be travelled over short distances	Signals can be travelled over long distances without being attenuated.

Definition of Baseband Transmission

Baseband transmission uses whole frequency spectrum of the medium for the transmission. That is the reason frequency division multiplexing cannot be used in the transmission but time division multiplexing is used in this transmission as in TDM the link is not divided into multiple channels instead it provides each input signal with a time slot, in which the signal utilize whole bandwidth for a given time slot. The signals are carried by wires in the form of electrical pulse.

Signals transmitted at point propagated in both the directions hence it is bidirectional. The expansion of baseband signal is limited to shorter distances because at high frequency the attenuation of the signal is most strong and the pulse blur out, causing the large distance communication completely impractical.

Definition of Broadband Transmission

The Broadband transmission employs analog signals which include optical or electromagnetic wave form of signal. The signals are sent into multiple frequencies permitting multiple signals to be sent simultaneously. Frequency division multiplexing is possible in which the

frequency spectrum is divided into multiple sections of bandwidth. The distinct channels can support different types of signals of varying frequency ranges to travel simultaneously (at the same instance).

The signals propagated at any point are unidirectional in nature, in simple words the signal can be travelled at only one direction, unlike baseband transmission. It requires two data path that are connected at a point in the network refer to as headend. The first path is used for signal transmission from the station to the headend. And the other path is used for receiving propagated signals.

2.2 Key Differences Between Baseband and Broadband Transmission

1. Baseband transmission utilizes digital signalling while broadband transmission uses analog signalling.
2. Bus and tree topologies, both work well with the broadband transmission. On the other hand, for the baseband transmission bus topology is suitable.
3. Baseband involves manchester and differential manchester encoding. In contrast, broadband does not make use of any digital encoding instead it uses PSK (Phase shift keying) encoding.

4. The signals can be travelled in both the direction in baseband transmission whereas in broadband transmission the signals can travel in only one direction.
5. In baseband transmission, the signals cover shorter distances because at higher frequencies the attenuation is most pronounced which make a signal to travel short distances without reducing its power. As against, in broadband signals, the signals can be travelled at longer distances.

2.2.1 Conclusion

The baseband and broadband transmissions are the types of signalling. Baseband transmission uses digital signalling and involves digital signal or electrical impulse that can be carried in a physical media such as wires. The broadband transmission uses analog signalling which involves optical signals or signals in the form of an electromagnetic wave. Baseband transmission utilizes the whole bandwidth of the channel to transmit a signal whereas in broadband transmission the bandwidth is divided into variable frequency ranges to transmit the different signals at the same instant.

Q4. What is difference between a hub, modem, router and a switch ?

Ans. The Differences Between a Modem, a Router, a Switch and a Hub

Modem:	Stands for "modulating-demodulating": modems are hardware devices that allow a computer o another device, such as a router or switch, to connect t Internet. They convert or "modulate" an analog signal telephone or cable wire to digital data (1s and 0s) that computer can recognize. Simply send traffic from point A to piont B without fu manipulation.
Routers:	Are responsible for sending data from one network to another. Work at Layer 3 (Network) of the OSI model, which c with IP addresses. Typically, routers today will perform the functionality both a router and a switch - that is, the router will hav multiple ethernet ports that devices can plug into.
Switches:	They use the MAC address of a device to send data on the port the destination device is plugged into.

	Work at Layer 2 (Data Link) of the OSI model, which with MAC addresses.
Hubs:	Unlike switches, hubs broadcast data to all ports, whic inefficient, so hubs are basically a multiport repeaters.

Q5. When you move the NIC cards from one PC to another PC, does the MAC address gets transferred as well?

Ans. The Media Access Control address (MAC address) for any network adapter is hard coded into the card itself. Each manufacturer of network adapters has a group of characters assigned that refer specifically to that company. I believe that is the first 1/2 of the MAC address which is 12 hexadecimal characters long. But the MAC address is part and parcel of the network adapter, just as your internal organs are part of you. When you move to a new house, you take your liver with you. In the same way, when you move a NIC to a different computer, it takes its MAC address with it.

Q6. When troubleshooting Computer network problem's what common hardware-releted problems can occur?

Ans.
A large percentage of a network is made up of hardware. Problems in these areas can range from malfunctioning hard drives, broken NICs and even hardware startups. Incorrectly hardware configuration is also one of those culprits to look into

3.1

Q7. In a network that contains two servers and twenty workstation, where is the best place to install an Anti-virus program?

Ans. The best solution is to install anti-virus on all the computers in the network. This will protect each device from the other in case some malicious user tries to insert a virus into the servers or legitimate users.

Q8. Define static IP and dynamic IP? Discuss the difference between IPV4 and IPV6.

Ans. When a device is assigned a static IP address, the address does not change. Most devices use dynamic IP addresses, which are assigned

the network when they connect and change over time.

When static IPs are needed

Most users don't need static IP addresses. Static IP addresses normally matter more when external devices or websites need to remember your IP address. One example is VPN or other remote access solutions that trust (whitelists) certain IPs for security purposes. A static IP address is not required if you are hosting a server, although it can simplify the setup process. Google Fiber provides two options.

How to get a dynamic IP address

- Use advanced settings for your network to configure dynamic DNS. When your IP address changes, the DNS entry for your server is automatically updated with its new IP address, so outside users can use the same domain name. You can choose the Dynamic DNS provider and don't have to install additional software on your computer.

How to get a static IP address

- Use advanced settings to reserve an IP address for a device on your local network. Your

device keeps the same IP address until you cancel the reservation or remove the device from your network, even if the device is disconnected.

- When you sign up for Google Fiber for small business, you can choose to have no static IPs (that is, dynamic IPs for all your devices), one static IP, or multiple static IPs. The number of static IPs available is shown on the screen when you sign up for service. If you sign up for static IPs, we will assign addresses to you when your service is installed and activated.

If you're interested in Google Fiber for Small Business, you can read more information about static IP addresses.

If you are hosting your own server, review our accepted use policy.

Q9. Discuss TCP/IP model in detail ?

Ans. TCP/IP Reference Model is a four-layered suite of communication protocols. It was developed by the DoD (Department of Defence) in the 1960s. It is named after the two main protocols that are used in the model, namely, TCP and IP. TCP stands for Transmission Control Protocol and IP stands for Internet Protocol.

The four layers in the TCP/IP protocol suite are −

- **Host-to- Network Layer** −It is the lowest layer that is concerned with the physical transmission of data. TCP/IP does not specifically define any protocol here but supports all the standard protocols.
- **Internet Layer** −It defines the protocols for logical transmission of data over the network. The main protocol in this layer is Internet Protocol (IP) and it is supported by the protocols ICMP, IGMP, RARP, and ARP.
- **Transport Layer** − It is responsible for error-free end-to-end delivery of data. The protocols defined here are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
- **Application Layer** − This is the topmost layer and defines the interface of host programs with the transport layer services. This layer includes all high-level protocols like Telnet, DNS, HTTP, FTP, SMTP, etc.

Q10. What is a Web browser (Browser)? Give some example of browsers.

Ans. A web browser, or simply "browser," is an application used to access and view websites. Common web browsers include Microsoft Internet Explorer, Google Chrome, Mozilla Firefox, and Apple Safari.

The primary function of a web browser is to render HTML, the code used to design or "mark up" webpages. Each time a browser loads a web page, it processes the HTML, which may include text, links, and references to images and other items, such as cascading style sheets and JavaScript functions. The browser processes these items, then renders them in the browser window.

Early web browsers, such as Mosaic and Netscape Navigator, were simple applications that rendered HTML, processed form input, and supported bookmarks. As websites have evolved, so have web browser requirements. Today's browsers are far more advanced, supporting multiple types of HTML (such as XHTML and HTML 5), dynamic JavaScript, and encryption used by secure websites.

The capabilities of modern web browsers allow web developers to create highly interactive websites. For example, Ajax enables a browser to dynamically update information on a webpage without the need to reload the page. Advances in CSS allow browsers to display a responsive website layouts and a wide array of visual effects. Cookies allow browsers to remember your settings for specific websites.

While web browser technology has come a long way since Netscape, browser compatibility issues remain a problem. Since browsers use different rendering engines, websites may not appear the same across multiple browsers. In some cases, a website may work fine in one browser, but not

function properly in another. Therefore, it is smart to install multiple browsers on your computer so you can use an alternate browser if necessary.

Q11. What is a search engine? Give example?

Ans.

3 WHAT IS A SEARCH ENGINE?

A search engine is a web-based tool that enables users to locate information on the World Wide Web. Popular examples of search engines are Google, Yahoo!, and MSN Search. Search engines utilize automated software applications (referred to as robots, bots, or spiders) that travel along the Web, following links from page to page, site to site. The information gathered by the spiders is used to create a searchable index of the Web.

HOW DO SEARCH ENGINES WORK?

Every search engine uses different complex mathematical formulas to generate search results. The results for a specific query are then displayed on the SERP. Search engine algorithms take the key elements of a web page, including the page title, content and keyword density, and come up with a ranking for where to place the results on the pages. Each search engine's algorithm is unique, so a top ranking on Yahoo! does not guarantee a prominent ranking on Google, and vice versa. To make things more complicated, the algorithms used by search engines are not only closely guarded secrets, they are also constantly

undergoing modification and revision. This means that the criteria to best optimize a site with must be surmised through observation, as well as trial and error — and not just once, but continuously.

Gimmicks less reputable SEO firms tout as the answer to better site rankings may work at best for only a short period before the search engine's developers become wise to the tactics and change their algorithm. More likely, sites using these tricks will be labeled as spam by the search engines and their rankings will plummet.

Search engines only "see" the text on web pages, and use the underlying HTML structure to determine relevance. Large photos, or dynamic Flash animation mean nothing to search engines, but the actual text on your pages does. It is difficult to build a Flash site that is as friendly to search engines; as a result, Flash sites will tend not to rank as high as sites developed with well coded HTML and CSS (Cascading Style Sheets — a complex mechanism for adding styles to website pages above and beyond regular HTML). If the terms you want to be found by do not appear in the text of your website, it will be very difficult for your website to yield high placement in the SERPs.

Q12. What is the Internet & WWW? What are the uses of Internet in our daily life ?

Ans. The internet is the wider network that allows computer networks around the world run by companies, governments, universities and other organisations to talk to one another. The result is a mass of cables, computers, data centres, routers, servers, repeaters, satellites and wifi towers that allows digital information to travel around the world.

It is that infrastructure that lets you order the weekly shop, share your life on Facebook, stream Outcast on Netflix, email your aunt in Wollongong and search the web for the world's tiniest cat.

1. Uses of the **Internet** in Education. The **Internet** is a great platform for students to learn throughout their lifetime. ...
2. **Internet Use** to Speed Up **Daily** Tasks. ...
3. **Use** of the **Internet** for Shopping. ...
4. **Internet** for Research & Development. ...
5. Digital Transactions. ...
6. Money Management. ...
7. Tour & Travel.

The **World Wide Web** (**WWW**), commonly known as **the Web**, is an information system where documents and other web resources are identified by Uniform Resource Locators (URLs, such as which may be

interlinked by hypertext, and are accessible over the Internet.[1][2] The resources of the Web are transferred via the Hypertext Transfer Protocol (HTTP) and may be accessed by users by a software application called a *web browser* and are published by a software application called a *web server*. The World Wide Web is not synonymous with the Internet, which pre-existed the Web in some form by over two decades and upon whose technologies the Web is built.

Possible uses of the Internet and World Wide Web for business

- Publicity, Marketing and Advertising. ...
- Direct On-line Selling. ...
- Research and Development. ...
- **Communication**. ...
- Collaboration. ...
- Industrial Classification of the Sample Companies. ...
- Use of WWW Sites. ...
- Use of Multi-Media.

Q13. What is the Internet service provider ? Give some example ISP in India.

ANS. WHAT IS AN ISP?

The ISP, short for 'Internet Service Provider', is the company that connects your personal computer, notebook, netbook, PDA, mobile device, game station, etc. to the Internet. Another name for ISP is IAP, or Internet Access Provider.

INTERNET ACCESS TECHNOLOGIES

The connection between your Internet enabled device and the global network is executed through a specific digital data transmission technology. It represents the transfer of information packets through an Internet Protocol route.

According to the method of data transmission, the Internet access that ISPs provide to users can be divided into several types, the most popular of which are:

DIAL-UP INTERNET ACCESS

This is the oldest method of providing access to the Internet. It uses a telephone line to perform a modem-to-modem connection. For that purpose, the user's computer is attached to a telephone line enabled modem device, which dials into the node of the ISP and starts transferring data between the servers that store websites the user wants to see and their Internet connected device. The dial-up Internet is today considered outdated in most Internet societies due to the slow connection speed it ensures (about 40-50 kbit/s.). However, the wide availability of

telephone access makes this type of Internet access the only alternative for remote areas that remain off the broadband network. It is also the least expensive Internet access service and is preferred by users on a tight budget.

DSL

DSL, short for 'digital subscriber loop' or 'digital subscriber line', is an advanced version of the dial-up Internet access method. In contrast to dial-up, DSL uses high frequency to execute a connection over the local telephone network. This allows the Internet and the phone connections to be run on one and the same telephone line. The digital subscriber line technology ensures an Asymmetric Digital Subscriber Line (ADSL), where the upload speed is lower than the download speed, and a Symmetric Digital Subscriber Line (SDSL), offering equal upload and download speeds. Of them both, ADSL is much more popular and is even known as just DSL to users.

CABLE INTERNET

The cable Internet is among the most preferred methods for providing residential Internet access. Technically speaking, it represents a broadband Internet access method, using the high-bandwidth cable television network to transmit data between the global network and the households. To use cable Internet you will need a

cable modem at home that will be connected with the CMTS (Cable Modem Termination System) of your cable ISP. The cable Internet access can be offered together with a cable television subscription and separately, for customers' convenience. The second case incurs higher subscription fees due to the extra equipment installation costs.

WIRELESS BROADBAND (WIBB)

This is a new-generation broadband Internet access technology, allowing the delivery of high-speed wireless Internet within a large area. Wireless broadband ISPs (WISPs) ensure connection speeds that come close to the wired broadband speeds provided by DSL and cable ISPs. To get wireless broadband you need to place a specific dish on your house roof or apartment balcony and point it to the transmitter of your WISP. This type of Internet access is used as an alternative to the wired broadband connection in remote areas.

WI-FI INTERNET

Wi-Fi (from Wireless Fidelity) has become one of the most widely distributed Internet access methods, with the growing usage of portable computers and Internet enabled mobile devices, such as smart phones, PDAs, game consoles, etc. In this sense, it is the most mobile Internet access method, since you are able to use it everywhere as

long as you are located within the scope of coverage, i.e. within the range of an Internet connected wireless network. Due to its ability to serve mobile devices, Wi-Fi is used in public places such as airports, hotels and restaurants to provide Internet access to customers. There are also specialized Wi-Fi hotspots where the service is either free or paid. Some of the largest cities in the world are in the process of building Wi-Fi networks that cover all the public places in the central areas.

ISDN

Another online data transmission method worth considering is ISDN or the Integrated Services Digital Network. ISDN represents a telephone system network, integrating a high-quality digital transmission of voice and data over the ordinary phone line. Ensuring a much better data transmission over the phone line than an analog line could allow, the ISDN offers a fast upstream/downstream Internet connection speed of 128 kbit/s. This speed level can be considered as a broadband speed as opposed to the narrowband speed of standard analog 56k telephone lines.

ETHERNET

Another Internet access type worth mentioning is Ethernet - the most widespread wired LAN (local area network) technology, also used in wireless LANs. The Ethernet

technology may ensure various speed levels and can thus be divided into several types: regular Ethernet, providing transmission speeds of up to 10 mbits/s, fast Ethernet, offering up to 100 mbits/s, gigabit Ethernet, supporting 1 gbit/s and 10-Gbit Ethernet, coming at up to 10 gbits/s.

Q14. Discuss the difference between MAC address, IP address and Port address.

Ans. The main difference between MAC and IP address is that, MAC Address is used to ensure the physical address of computer. It uniquely identifies the devices on a network. While IP address are used to uniquely identifies the connection of network with that device take part in a network.

Let's see the difference between MAC Address and IP Address:

S.NO	MAC Address	IP Address
1.	MAC Address stands for Media Access Control Address.	IP Address stands for Internet Protocol Address.
2.	MAC Address is a six byte hexadecimal address.	IP Address is either four byte (IPv4) or six byte (IPv6) address.

3.	A device attached with MAC Address can retrieve by ARP protocol.	A device attached with IP Address can retrieve by RARP protocol.
4.	NIC Card's Manufacturer provides the MAC Address.	Internet Service Provider provides IP Address.
5.	MAC Address is used to ensure the physical address of computer.	IP Address is the logical address of the computer.
6.	MAC Address operates in the data link layer.	IP Address operates in the network layer.
7.	MAC Address helps in simply identifying the device.	IP Address identifies the connection of the device on the network.
8.	MAC Address of computer cannot be changed with time and environment.	IP Address modifies with the time and environment.
9.	MAC Address can't be found easily by third party.	IP Address can be found by third party

Q15. How do we view my Internet browser's history?

Ans. To view the web history in Google Chrome, click to open the menu ⋮ at the top-right of its window and select **History**, then click **History** a second time. Or press **Ctrl+H** on your keyboard.