Assignment

**ANS – 1 )**

**Personal Area Network (PAN):** The interconnection of devices within the range of an individual person, typically within a range of 10 meters. For example, a wireless network connecting a computer with its keyboard, mouse or printer is a PAN. Also, a PDA that controls the user’s hearing aid or pacemaker fits in this category. Another example of PAN is a Bluetooth. Typically, this kind of network could also be interconnected without wires to the Internet or other networks.

**Local Area Network (LAN):** Privately-owned networks covering a small geographic area, like a home, office, building or group of buildings (e.g. campus). They are widely used to connect computers in company offices and factories to share resources (e.g., printers) and exchange information. LANs are restricted in size, which means that the worst-case transmission time is bounded and known in advance. Knowing this bound makes it possible to use certain kinds of designs that would not otherwise be possible. It also simplifies network management. Traditional LANs run at speeds of 10 Mbps to 100 Mbps, have low delay (microseconds or nanoseconds), and make very few errors. Newer LANs operate at up to 10 Gbps.

Early LAN (Local Area Network) networks were formed using coaxial cable, coax is an electric cable and it is used to carry radio signals. **LAN (Local Area Network)** setup is developed by connecting two or more than two computers with each other using a physical connection in order to share files and data overtime.

**Metropolitan Area Network (MAN):** Covers a larger geographical area than is a LAN, ranging from several blocks of buildings to entire cities. MANs can also depend on communications channels of moderate-to-high data rates. A MAN might be owned and operated by a single organization, but it usually will be used by many individuals and organizations. MANs might also be owned and operated as public utilities. They will often provide means for internetworking of LANs. Metropolitan Area Networks can span up to 50km, devices used are modem and wire/cable.

Most widely used technologies to develop a MAN (Metropolitan Area Network) network are FDDI (fiber distribution data interface), **ATM (Asynchronous Transfer Mode)** and SMDS (switched multi megabit data service).**ATM (Asynchronous Transfer Mode)** is the most frequently used of all. ATM (Asynchronous Transfer Mode) is a digital data transfer technology. It was developed in 1980 to improve the transportation of real time data over a single network. ATM (Asynchronous Transfer Mode) works just like cell relay system, where data is separated in the form of fixed equal sized packets and is transferred overtime. The purpose of ATM (Asynchronous Transfer Mode) was to access clear audio and video results during a video conferencing.

**Wide Area Networks (WAN):** Computer network that covers a large geographical area, often a country or continent. (Any network 1 whose communications links cross metropolitan, regional, national boundaries). Less formally, a network that uses routers and public communications links. Routers will be discussed later.

**WAN (Wide Area Network)** networks are established often by seeking help from telecomm departments who provide the] facility of leased lines. Router is connected to the LAN at one side and a hub is attached at the other end.

ANS 2 )

The **OSI Model** we just looked at is just a reference/logical model. It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components. But when we talk about the TCP/IP model, it was designed and developed by Department of Defense (DoD) in 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol. The **TCP/IP model** is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model. The layers are:

1. Process/Application Layer
2. Host-to-Host/Transport Layer
3. Internet Layer
4. Network Access/Link Layer

The diagrammatic comparison of the TCP/IP and OSI model is as follows :

The first layer is the Process layer on the behalf of the sender and Network Access layer on the behalf of the receiver. During this article, we will be talking on the behalf of the receiver.

**1. Network Access Layer –**

This layer corresponds to the combination of Data Link Layer and Physical Layer of the OSI model. It looks out for hardware addressing and the protocols present in this layer allows for the physical transmission of data.  
We just talked about ARP being a protocol of Internet layer, but there is a conflict about declaring it as a protocol of Internet Layer or Network access layer. It is described as residing in layer 3, being encapsulated by layer 2 protocols.

**2. Internet Layer –**

This layer parallels the functions of OSI’s Network layer. It defines the protocols which are responsible for logical transmission of data over the entire network. The main protocols residing at this layer are :

1. **IP –** stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions:  
   IPv4 and IPv6. IPv4 is the one that most of the websites are using currently. But IPv6 is growing as the number of IPv4 addresses are limited in number when compared to the number of users.
2. **ICMP –** stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
3. **ARP –** stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP and Inverse ARP.

**3. Host-to-Host Layer –**

This layer is analogous to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The two main protocols present in this layer are :

1. **Transmission Control Protocol (TCP) –** It is known to provide reliable and error-free communication between end systems. It performs sequencing and segmentation of data. It also has acknowledgment feature and controls the flow of the data through flow control mechanism. It is a very effective protocol but has a lot of overhead due to such features. Increased overhead leads to increased cost.
2. **User Datagram Protocol (UDP) –** On the other hand does not provide any such features. It is the go-to protocol if your application does not require reliable transport as it is very cost-effective. Unlike TCP, which is connection-oriented protocol, UDP is connectionless.

**4. Application Layer –**

This layer performs the functions of top three layers of the OSI model: Application, Presentation and Session Layer. It is responsible for node-to-node communication and controls user-interface specifications. Some of the protocols present in this layer are: HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP, NFS, X Window, LPD. Have a look at [Protocols in Application Layer](https://www.geeksforgeeks.org/protocols-application-layer/) for some information about these protocols. Protocols other than those present in the linked article are :

* + 1. **HTTP and HTTPS –** HTTP stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL(Secure Socket Layer). It is efficient in cases where the browser need to fill out forms, sign in, authenticate and carry out bank transactions.
    2. **SSH –** SSH stands for Secure Shell. It is a terminal emulations software similar to Telnet. The reason SSH is more preferred is because of its ability to maintain the encrypted connection. It sets up a secure session over a TCP/IP connection.
    3. **NTP –** NTP stands for Network Time Protocol. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions. Assume the following situation without the presence of NTP. Suppose you carry out a transaction, where your computer reads the time at 2:30 PM while the server records it at 2:28 PM. The server can crash very badly if it’s out of sync.

ANS 3 )

A ) Architecture Of Internet

The architecture of the Internet is ever-changing due to continuous changes in the technologies as well as the nature of the service provided. The heterogeneity and vastness of the Internet make it difficult to describe every aspect of its architecture.

The overall architecture can be described in three levels −

1. Backbone ISP (Internet Service Provider)
2. Regional ISPs
3. Clients

B ) IP Addressing

An IP address (internet protocol address) is a numerical representation that uniquely identifies a specific interface on the network.

Addresses in IPv4 are 32-bits long. This allows for a maximum of 4,294,967,296 (232) unique addresses. Addresses in IPv6 are 128-bits, which allows for 3.4 x 1038 (2128) unique addresses.

The total usable address pool of both versions is reduced by various reserved addresses and other considerations.

IP addresses are binary numbers but are typically expressed in decimal form (IPv4) or hexadecimal form (IPv6) to make reading and using them easier for humans.

C ) URL And Their Applications

**URL** stands for Uniform Resource Locator. A URL is nothing more than the address of a given unique resource on the Web. In theory, each valid URL points to a unique resource. Such resources can be an HTML page, a CSS document, an image, etc. In practice, there are some exceptions, the most common being a URL pointing to a resource that no longer exists or that has moved. As the resource represented by the URL and the URL itself are handled by the Web server, it is up to the owner of the web server to carefully manage that resource and its associated URL.

D ) Network Utilities

Network utilities are software utilities designed to analyze and configure various aspects of computer networks. The majority of them originated on Unix systems, but several later ports to other operating systems exist. The most common tools include: ping, ping a host to check connectivity.