SUNBEAM
Institute of Information Technology

PreCAT
Data Communication And Networking

CONTENTS

NETWORK:

A **network** is a collection of computers, network devices, servers, mainframes, devices, peripherals, or other devices connected to each other to allow the sharing of resources, data.

Internet is good example of a network which is global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols.

Centralized Computing is a multiple client-single server like architecture where the server computer is the one where all of the major processing is done. It even has more computing resources than its clients. Client machines connect to the server computer and submit their requests.

Decentralized Computing is the one where there is no single server machine that is solely responsible for all the processing. The architecture allows to distribute the workload among multiple compute nodes, and each of them is equally capable of servicing requests.

Server-client can provide various functionalities, often called "services", such as sharing data or resources among multiple clients, or performing computation for a client. A single server can serve multiple clients, and a single client can use multiple servers.

Cloud computing allows clients with various computing capabilities to store and process data either in a privately-owned cloud, or on a third-party server located in a data centre., thus making data-accessing mechanisms more efficient and reliable. Cloud computing relies on sharing of resources.

Common types of networks are:

- LAN - Local Area Network
- WAN - Wide Area Network
- WLAN – Wireless Local Area Network
- MAN - Metropolitan Area Network
- SAN - Storage Area Network, Server Area Network
- CAN - Campus Area Network, Cluster Area Network
- PAN - Personal Area Network

Primary and main types of networks:

LAN:

The local area network is a network which is designed to operate over a small physical area such as an office, factory or a group of buildings. LANs are very widely used in a variety of applications.

In LAN all the machines are connected to a single cable. Different types of. Topologies such as Bus, Ring, Star, Mesh etc. are used for LANs.

LAN uses a layered architecture and they are capable of operating at hundreds of Mbits/sec.

A local area network (LAN) is usually a privately owned and links the devices in a single office, building or campus of up to a few kilometres in size.

WAN:

Wide area networks (WAN) are often established with leased telecommunication circuits. A wide area network is a computer network that extends over a large geographical distance. It interconnects multiple local area networks (LANs).

WAN infrastructure typically leased by a third-party service provider, such as a telecommunications carrier, Internet service provider, private IP network operator or cable company.

Basic types of LAN:

Token Ring:

It is the token passing method developed and copyright by IBM. Token Ring controls the medium by passing a control frame (token) from one device to the next. Only the computer possessing the token may transmit. Its topology is a logical ring but usually a physical star. And speed is limited at 4mbps and 16 mbps.

Ethernet:

It is developed at the PARC in Palo Alto CA in the early 70's by Robert Metcalf.

It is a Carrier Sense Multiple Access transmission method. This means if the channel is available then any device connected to the medium can transmit. Carrier Sense Multiple Access/Collision Detect (CSMA/CD) is the protocol for carrier transmission access in Ethernet networks. On Ethernet, any device can try to send a frame at any time. Each device senses whether the line is idle and therefore available to be used. If it is, the device begins to transmit its first frame. If another device has tried to send at the same time, a collision is said to occur and the frames are discarded. Each device then waits a random amount of time and retries until successful in getting its transmission sent. It transmits data in the form of 1's &0's. It uses +5V for sending 1, +2V for sending 0, and 0.5V for carrier sense i.e. basic voltage required. It is the most common LAN technology today well suited for any and all types of applications.

A standard Ethernet cable is slightly thicker than a phone cable and has an RJ45 connector on each end. Ethernet ports look similar to telephone jacks, but are slightly wider. You can plug or unplug devices on an Ethernet network while they are powered on without harming them.

Like usb, Ethernet has multiple standards that all use the same interface. These include:

- 10BASE-T - supports up to 10 Mbps
- 100BASE-T - supports up to 100 Mbps
- 1000BASE-T (also called "Gigabit Ethernet") - supports up to 1,000 Mbps

MAC Address

MAC addresses are 12-digit (48 bits) hexadecimal numbers. By convention, they are usually written in one of the following three formats:

- MM:MM:MM:SS:SS:SS
- MM-MM-MM-SS-SS-SS
- MMM.MMM.SSS.SSS

The leftmost 6 digits (24 bits) called a "prefix" is associated with the adapter manufacturer. Each vendor registers and obtains MAC prefixes as assigned by the IEEE. Vendors often possess many prefix numbers associated with their different products.

The rightmost digits of a MAC address represent an identification number for the specific device. Among all devices manufactured with the same vendor prefix, each is given their own unique 24-bit number.

Frame Structure:

(4 Bytes) CRC	(1500 Bytes) IP/ IPX/ AT	(2 Bytes) OPTIONS FIELD	(6 Bytes) SOURCE ADDRESS	(6 Bytes) DESTINATION ADDRESS

Total frame size = 1518 Bytes

An Ethernet frame starts with a header (from right), which contains the source and destination MAC addresses, among other data. The middle part of the frame is the actual data. The frame ends with a field called Cyclic Redundancy Check (CRC)

The Ethernet frame structure is defined in the IEEE 802.3 standard

- Destination MAC –MAC address of the receiving system.
- Source MAC – MAC address of the sending system.
- Options field – It defines the type of protocol inside the frame, for example IPv4 or IPv6.
- CRC – Cyclic Redundancy Check (CRC) which allows detection of corrupted data.

In the LAN, machine will process the data in frame in two conditions:

1. When the destination MAC is matching with its own MAC address.
2. When there is broadcast (i.e. when destination address is all 1's/ all FF.).

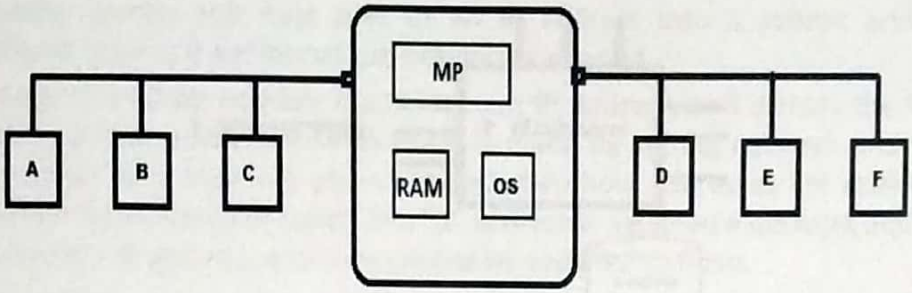
A **network collision** occurs when more than one device attempts to send a packet on a network segment at the same time. Only one device in the collision domain may transmit at any one time, and the other devices in the domain listen to the network and refrain from transmitting while others are already transmitting in order to avoid collisions. Because only one device may be transmitting at any one time, total network bandwidth is shared among all devices on the collision domain. Collisions also decrease network efficiency.

In Ethernet, collisions are eliminated using carrier sense multiple access with collision detection (CSMA/CD) in which the competing packets are discarded and re-sent.

Modern wired networks use a **switch** to reduce or eliminate collisions. By connecting each device directly to a port on the switch, either each port on a switch becomes its own collision domain (in the case of half duplex links) or the possibility of collisions is eliminated entirely in the case of full-duplex links. In a network, a switch is a device that forward incoming data from any of multiple input ports to the specific output port that will take the data toward its intended destination.

On an Ethernet local area network (LAN), a switch determines from the physical device (MAC) address in each incoming message frame which output port to forward it to and out of.

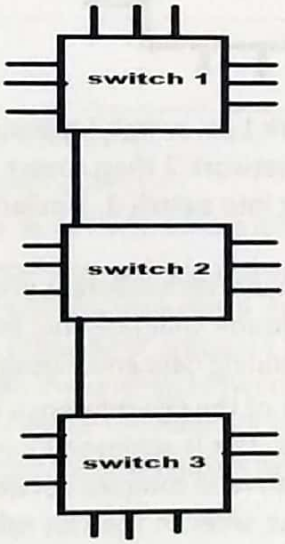
Switches are used to avoid collision. In the following structure the machine A,B,C are connected at one port of the switch and D,E,F are connected at another port of same switch. Now MAC addresses of A,B,C,D,E,F are learned on their respective ports. So collisions are reduced by 50%.



Switch/Bridge

As no of ports on switch are increased, possibility of collision is reduced. One machine per port allows full duplex communication and eliminates collisions totally.

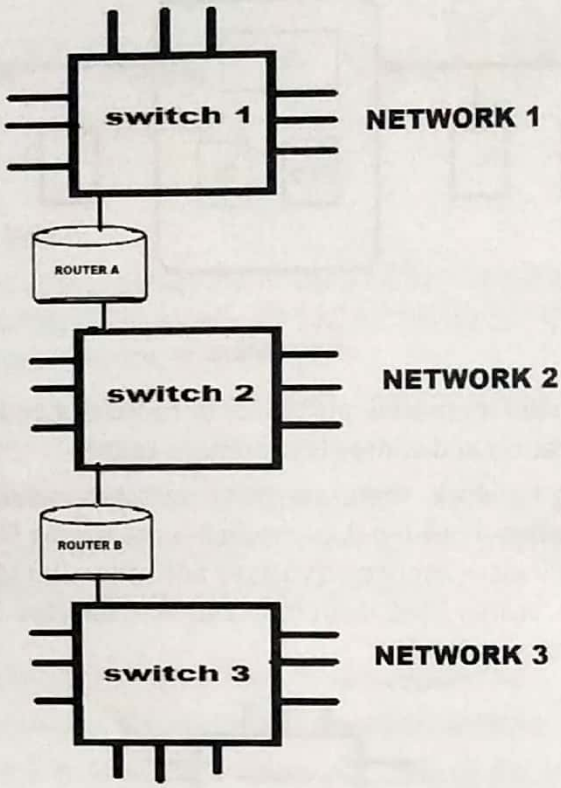
Let's consider following network, there are three switches, switch 1, switch 2 and switch 3 connected. Suppose each switch-1, switch-2 and switch-3 are having 50 machines connected each. So switch-1 learn 50 MAC addresses connected to itself and other 100 MAC addresses also which are connected to switch 2&3. i.e. switch 1 will learn total 150 MAC address. Similarly switch 2 and switch 3 also have 150 MAC addresses learned.



Now due to this process, following drawbacks of the switch are raised:

1. Every MAC address in the network is learned on switch. So as no. of switches increases, delay in process increases. In above example, it requires more time to search destinations MAC address in 150 MAC addresses, so delay gets increases.
2. Switches can not control broadcast. Broadcast consumes more processing power. Hence machine goes slow down.

So to control broadcast, an intelligent device is used called as **Router**. The primary function of a routers to connect networks together and keep certain kinds of broadcast traffic under control. A router is a specialized networking device connected to two or more networks running software that allows the router to move data from one network to another.



When there is broadcast in Network 1 i.e. switch 1 broadcast, the router A prevents it from going into switch 2. If there is broadcast in network 2 then router A prevents it from entering in switch 1 and router B prevents it from entering into switch 3. Similarly network 3 broadcast is prevented by router B from entering into network 2.

A network consists of several segments with different protocols and architectures a switch might be inadequate. The network needs a router that not only knows the address of each segment, but can also determine the best path for sending data and filtering broadcast traffic to the local segment.

Routers work at the network layer of the OSI reference model. This means they can switch and route packets across multiple networks. This is achieved by exchanging protocol specific information between separate networks. Routers can read complex network addressing information in the packet and, because they function at a higher layer in the OSI reference model than bridges, they have access to additional information. Routers can provide the filtering and isolating of traffic and the connection of network segments.

IP Addressing:

An Internet Protocol address (IP address) is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication.

An IP address has two components : Network Id & Host Id.

It is full 32 bit number and its grouped into 4 octets (for understanding purpose only). When machines are connected physically, they must be connected logically in the same network then only they can communicate with each other.

IP address always comes with additional parameter called as **Subnet Mask.**

A subnet mask separates the IP address into the network and host addresses (<network><host>).

Sub netting further divides the host part of an IP address into a subnet and host address (<network><subnet><host>) if additional sub network is needed.

A Subnet mask is a 32-bit number that masks an IP address, and divides the IP address into network address and host address. Subnet Mask is made by setting network bits to all "1"s and setting host bits to all "0"s. Within a given network, two host addresses are reserved for special purpose, and cannot be assigned to hosts. The "0" address is assigned a network address and "255" is assigned to a broadcast address, and they cannot be assigned to hosts.

IP address classes:

There are five classes of available IP ranges: Class A, Class B, Class C, Class D and Class E, while only A, B, and C are commonly used. Classes are distributed according to first octet in IP address. Each class allows for a range of valid IP addresses, shown in the following table:

Class	Range	Subnet Mask	Application
Class A	1 to 127	255.0.0.0	Large
Class B	128 to 191	255.255.0.0	Medium
Class C	192 to 223	255.255.255.0	Small
Class D	224 to 239		Reserved for Multicasting
Class E	240 to 255		Reserved for experimental , R&D

Ranges 127.x.x.x are reserved for the loopback.

For example, 127.0.0.1 is the loopback address.

Range 255.255.255.255 broadcasts to all hosts on the local network.

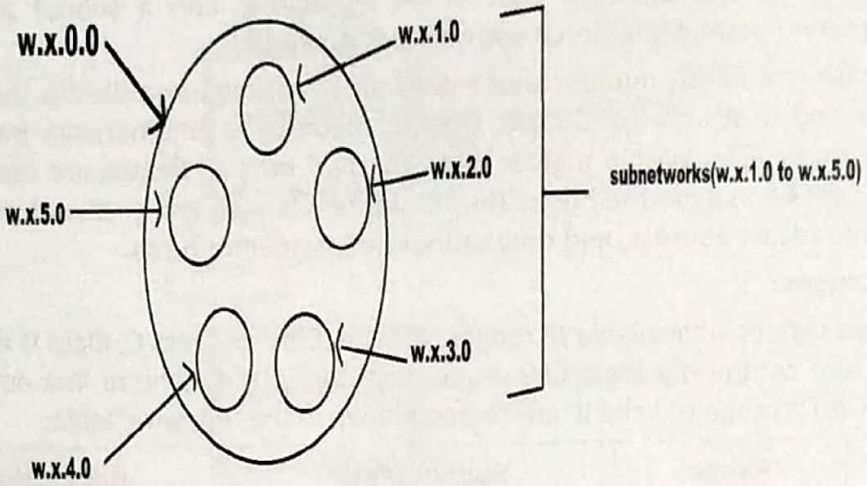
Sub netting is the strategy used to partition a single physical network into more than one smaller logical sub-networks (subnets). An IP address includes a network segment and a host segment. Subnets are designed by accepting bits from the IP address's host part and using these bits to assign a number of smaller sub-networks inside the original network. Sub netting allows an organization to add sub-networks. Sub netting helps to reduce the network traffic and conceals network complexity.

In the host part , the ON bits are used for internal Sub netting.

To calculate no. of subnets: 2 N

To calculate no. of Host: 2 N-2

Where N= No. of Bits



For example, In the above fig. there is network w.x.0.0. This network is divided in the small-small subnet works. W.X. is a fixed part and is used as network part, third octet is used for internal Sub netting. Above W.X.1.0 to W.X.5.0 are the subnet works in the W.X.0.0 network.

In the subnet W.X.1.0, W.X.1.1 is the first port in first subnet, 1.2 is second port and so on up to 254. 255 is the broadcast ID. Same thing is used for other subnets W.X.1.0 to 5.0.

OSI MODEL:

The International organization for Standardization developed the OSI model. OSI (Open Systems Interconnection) is reference model for how applications can communicate over a network. A reference model is a conceptual framework for understanding relationships. It defines a networking framework to implement protocols in seven layers.

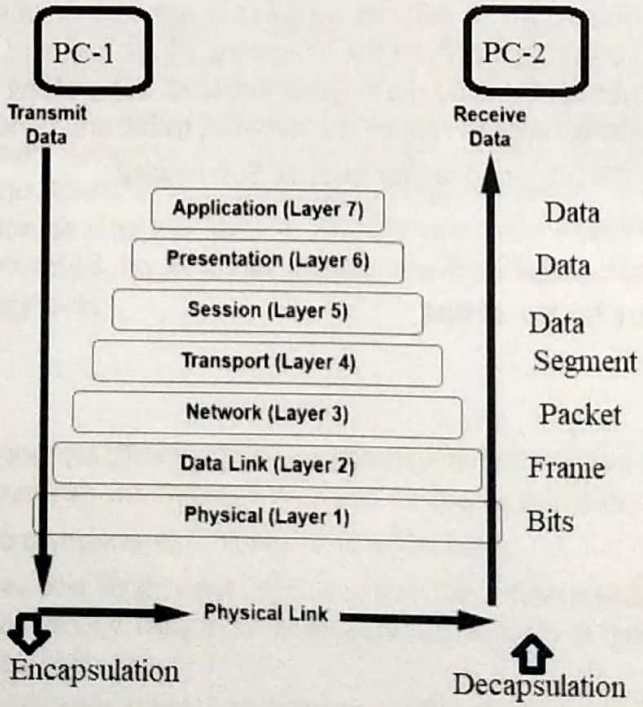


Fig. OSI Model

Physical layer:

At Layer 1, the Physical layer of the OSI model is responsible for transmission of digital data bits from the Physical layer of the source over network communications media to the Physical layer of the destination. It includes Ethernet cable, hubs and repeaters, crimps, cable connectors. At the Physical layer, data are transmitted using the type of signalling supported by the physical medium: electric voltages, radio frequencies, or pulses of infrared or ordinary light.

Examples: Ethernet, FDDI, RJ45.

Data Link layer:

Layer 2 is the data-link layer. This layer sets up links across the physical network, putting packets into network frames. This layer has two sub-layers, the Logical Link Control Layer and the Media Access Control Layer. Ethernet is the main data link layer in use. The Data Link layer also manages physical addressing schemes such as MAC addresses for Ethernet networks, controlling access of any various network devices to the physical medium.

Example: PPP, FDDI, ATM, IEEE 802.5/ 802.2, IEEE 802.3/802.2, HDLC, Frame Relay.

Network layer:

The Network layer adds the concept of routing above the Data Link layer. When data arrives at the Network layer, the source and destination addresses contained inside each frame are examined to determine if the data has reached its final destination. If the data has reached the final destination, this Layer 3 formats the data into packets delivered up to the Transport layer. Otherwise, the Network layer updates the destination address and pushes the frame back down to the lower layers.

To support routing, the Network layer maintains logical addresses such as IP addresses for devices on the network. The Network layer also manages the mapping between these logical addresses and physical addresses. In IP networking, this mapping is accomplished through the Address Resolution Protocol (ARP).

Example: AppleTalk DDP, IP, IPX.

Transport Layer:

The Transport Layer delivers data across network connections. TCP is the most common example of a Transport Layer 4 network protocol. Different transport protocols may support a range of optional capabilities including error recovery, flow control, and support for re-transmission. This layer manages packetization of data, then the delivery of the packets, including checking for errors in the data once it arrives. On the Internet, TCP and UDP provide these services for most applications as well.

TCP is connection oriented – once a connection is established, data can be sent bidirectional. UDP is a simpler, connectionless Internet protocol. Multiple messages are sent as packets in chunks using UDP.

Example: SPX, TCP, UDP.

Session Layer:

This layer sets up, coordinates and terminates conversations. Services include authentication and reconnection after an interruption. The Session Layer manages the sequence and flow of events

that initiate and tear down network connections. At Layer 5, it is built to support multiple types of connections that can be created dynamically and run over individual networks. It deals with session and connection coordination.

Example: NFS, Net Bios names, RPC, SQL.

Presentation Layer:

This layer provides independence from differences in data representation (e.g., encryption) by translating from application to network format, and vice versa. The presentation layer works to transform data into the form that the application layer can accept. This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems.

Example: encryption, ASCII, EBCDIC, TIFF, GIF, PICT, JPEG, MPEG.

Application Layer:

The Application layer supplies network services to end-user applications. Network services are typically protocols that work with user's data. For example, in a Web browser application, the Application layer protocol HTTP packages the data needed to send and receive Web page content. This Layer 7 provides data to (and obtains data from) the Presentation layer.

Example: WWW browsers, NFS, SNMP, Telnet, HTTP, FTP

Common TCP/IP stack Protocols:

- **ARP (Address Resolution Protocol)** – used to convert an IP address to a MAC address.
- **IP (Internet Protocol)** – used to deliver packets from the source host to the destination host based on the IP addresses.
- **ICMP (Internet Control Message Protocol)** – used to detects and reports network error conditions. Used in ping.
- **TCP (Transmission Control Protocol)** – a connection-oriented protocol that enables reliable data transfer between two computers.
- **UDP (User Datagram Protocol)** – a connectionless protocol for data transfer. Since a session is not created before the data transfer, there is no guarantee of data delivery.
- **FTP (File Transfer Protocol)** – used for file transfers from one host to another.
- **Telnet (Telecommunications Network)** – used to connect and issue commands on a remote computer.
- **DNS (Domain Name System)** – used for host names to the IP address resolution.
- **HTTP (Hypertext Transfer Protocol)** – used to transfer files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web.

Objective Questions

Q.1. A BSS with an AP in wireless LAN is called _____ architecture

a. Ad-hoc architecture
b. Infrastructure
c. ESS
d. NAV

Q.2. In a network, after the load reaches the capacity, throughput _____

a. Increases sharply
b. Increases proportionally with the load
c. declines sharply
d. declines proportionally with the load

Q.3. The topology which requires a central controller or hub is _____.

a. Mesh
b. Star
c. Bus
d. Ring

Q.4. Frames from one LAN can be transmitted to another LAN via the device

a. Router
b. Bridge
c. Repeater
d. Modem

Q.5.Which multiplexing technique transmits digital signals?

a. FDM
b. TDM
c. WDM
d. None of the above

Q.6. You have a class A network address 10.0.0.0 with 40 subnets, but are required to add 60 new subnets very soon. You would like to still allow for the largest possible number of host IDs per subnet. Which subnet mask should you assign?

a. 255.240.0.0
b. 255.248.0.0
c. 255.252.0.0
d. 255.254.0.0

Q.7. The Ipv4 header size

a. is 20 to 60 bytes long
b. is always 20 bytes long
c. is always 60 bytes long
d. depends on the MTU

Q.8. What is the size (in terms of bits) of header length field in IPv4 header ?

a. 2
b. 4
c. 8
d. 16

Q.9. Which field determines the lifetime of IPv6 diagram?

a. Hop Limit
b. TTL
c. Next Header
d. Fragmentation

Q.10. What is CRC in cyclic redundancy checking ?

a. the divisor
b. The quotient
c. The dividend
d. The remainder

Q.11. Which of the internet working device takes data sent from one network device and forwards it to the destination node based on MAC address ?

a. Switch
b. Router
c. Hub
d. Bridge

Q.12. The Routing Information Protocol (RIP) is an infra-domain routing based on _____ routing algorithm.

a. distance vector
b. link state
c. path vector
d. OSPF

Q.13.Which of the following event is not possible in wireless LAN ?

a. collision detection
b. Acknowledgement of data frames
c. multi mode data transmission
d. collision avoidance

Q.14. _____ is a subset of a network that includes all the routers but contains no loops.

a. Spanning Tree
b. LEACH
c. Spider Structure
d. Spider Tree

Q.15. The _____ address must be referred to deliver a message to the correct application program running on a host

a. PORT
b. IP
c. Physical
d. Logical

Q.16. _____ is class based Qos model designed for IP?

a. Integrated services
b. Differentiated services
c. Connectionless
d. Connection-oriented

Q.17. The space which is provided to avoid overlap with other burst is known as _____

a. Frequency space
b. Guard space
c. Information Space
d. Bandwidth Space

Q.18. The standard TCP port assigned for SSH server is _____

a. port 20
b. port 21
c. port 22
d. port 23

Q.19. In FTP, the port _____ is used for the control connection and the port _____ for the data connection.

a. 21;22
b. 21;20
c. 20;21
d. 22;21

Q.20. The typical range of Ephemeral port is _____

a. 1 to 80
b. 1 to 1024
c. 80 to 1024
d. 1024 to 65535

Q.21. The services of _____ is used by DNS at well-known port 53.

a. TCP
b. UDP
c. SCTP
d. TCP or UDP

Q.22. If 10 files are transferred from server A to client B in the same session through FTP. the number of TCP connections between A and B is

a. 9
b. 10
c. 11
d. 12

Q.23. The network availability calculated as

a. (Total Time Available + Downtime) * Total Time Available
b. (Total Time Available - Downtime)
c. (Total Time Available + Downtime)
d. (Total Time Available + Downtime) / Total Time Available

Q.24. A bluetooth network consists of_____ primary devices and upto _____ devices secondary devices.

a. One;five
b. three;five
c. two;six
d. one;seven

Q.25. In IEE 802.11, the architecture where a BSS is without as AP called an _____

a. Ad-hoc architecture
b. infrastructure architecture
c. ESS
d. NAV

Q.26. The IEEE 802 project of the 1980s involved further defining the lower two layers of the OSI model. A number of standards were agreed upon during that time. Which of the following is the standard for Ethernet?

a. 802.2
b. 802.3
c. 802.4
d. 802.5

Q.27. The DHCP server assigns an IP address to a client

a. for unlimited period
b. for limited period
c. not dependent on time
d. daily basis

Q.28. _____ uses distance vector routing algorithm in Internet.

a. OSPF
b. ARP
c. RIP
d. RARP

Q.29. _____ method is used by HTTP request line to request a document from the server.

a. GET
b. PUT
c. COPY
d. PUSH

Q.30. Short message service is a message consisting of maximum of alphanumeric characters

a. 100
b. 150
c. 160
d. 170

Q.31. A mobile station can communicate with two base stations at the same time in a _____ handoff.

a. Hard
b. Soft
c. Medium
d. Moderate

Q.32. A connection device that operates in all five layers of the internet model or seven layers of OSI model is called _____.

a. Repeater
b. Bridge
c. Router
d. Gateway

Q.33. The _____ layer adds a header that includes the logical addresses of the sender and receiver to the packet coping from the upper layer

a. Physical Layer
b. Data Link
c. Network
d. Transport

Q.34. The physical, data link, and network layers are the _____ support layers.

a. user
b. network
c. both (a) and (b)
d. neither (a) nor (b)

Q.35. The slowest transmission speeds are those of

a. twisted-pair wire
b. coaxial cable
c. fiber-optic cable
d. microwaves

ANSWER KEY FOR OBJECTIVE QUESTIONS							
Q.1	B	**Q.11**	A	**Q.21**	D	**Q.31**	B
Q.2	D	**Q.12**	A	**Q.22**	C	**Q.32**	D
Q.3	B	**Q.13**	A	**Q.23**	D	**Q.33**	C
Q.4	B	**Q.14**	A	**Q.24**	D	**Q.34**	B
Q.5	B	**Q.15**	C	**Q.25**	A	**Q.35**	A
Q.6	D	**Q.16**	B	**Q.26**	B		
Q.7	A	**Q.17**	B	**Q.27**	B		
Q.8	B	**Q.18**	C	**Q.28**	C		
Q.9	A	**Q.19**	A	**Q.29**	A		
Q.10	D	**Q.20**	D	**Q.30**	C		