Biyani's Group of Girls' Colleges

Pre-University Exam

BCA III

Paper- Networking Technologies (SET -B)

Time: 3 Hrs. MM: 100

Part-I

A- Attempt all the questions (very short answer). Your answers should not exceed the maximum word limit of 40 for each question. Each question carries 2 marks

Q1. What is Transmission control protocol?

Ans. Transmission control protocol (TCP) is a network communication protocol designed to send data packets over the Internet.

TCP is a transport layer protocol in the OSI layer and is used to create a connection between remote computers by transporting and ensuring the delivery of messages over supporting networks and the Internet.

Q2. What is wireless transmission?

Ans. Wireless transmission is a form of unguided media. Wireless communication involves no physical link established between two or more devices, communicating wirelessly. Wireless signals are spread over in the air and are received and interpreted by appropriate antennas.

When an antenna is attached to electrical circuit of a computer or wireless device, it converts the digital data into wireless signals and spread all over within its frequency range. The receptor on the other end receives these signals and converts them back to digital data.

Q3. What is Star Topology?

Ans. A star topology is a topology for a Local Area Network (LAN) in which all nodes are individually connected to a central connection point, like a hub or a switch. A star takes more cable than e.g. a bus, but the benefit is that if a cable fails, only one node will be brought down.

Q4. What is Network interface?

Ans. A network interface is a system's (software and/or hardware) interface between two pieces of equipment or protocol layers in a computer network.

A network interface will usually have some form of network address. This may consist of a node ID and a port number or may be a unique node ID in its own right.

Network interfaces provide standardized functions such as passing messages, connecting and disconnecting, etc.

Q5. What is error correction?

Ans. The process of correcting errors in data that may have been corrupted during transmission or in storage. Data transmissions are always subject to corruption due to errors, but in videotransmissions, error correction needs to deal with the errors but not retransmit the corrupted data.

Q6. Explain protocol?

Ans .A protocol is a set of rules and guidelines for communicating data. Rules are defined for each step and process during communication between two or more computers. Networks have to follow these rules to successfully transmit data.

Q7. What is physical and logical address?

Ans. A physical address :- is the hardware-level address used by the Ethernet interface to communicate on the network. Every device must have a unique physical address. This is often referred to as its MAC (Media Access Control) address. An Ethernet physical address is six bytes long and consists of six hexadecimal numbers, usually separated by colon characters (:).

Logical addresses :- A logical address is a network-layer address that is interpreted by a protocol handler. Logical addresses are used by networking software to allow packets to be independent of the physical connection of the network, that is, to work with different network topologies and types of media. Each type of protocol has a different kind of logical address.

Q8. What is network layer?

Ans. The network layer is considered the backbone of the OSI Model. It selects and manages the best logical path for data transfer between nodes. This layer contains hardware devices such as routers, bridges, firewalls and switches, but it actually creates a logical image of the most efficient communication route and implements it with a physical medium.
Network layer protocols exist in every host or router. The router examines the header fields of all the IP packets that pass through it.

Q9. Define Switches and Bridges?

Ans. Bridging networks are generally always interconnected local area networks since broadcasting every message to all possible destinations would flood a larger network with unnecessary traffic. Switch :-A switch is a network device that selects a path or circuit for sending a unit of data to its next destination. A switch may also include the function of the router, a device or program that can determine the route and specifically what adjacent network point the data should be sent to. In general, a switch is a simpler and faster mechanism than a router, which requires knowledge about the network and how to determine the route.

Q10 .What do you mean by Guided and Un-guided Media?

Ans. Wired or Guided Media or Bound Transmission Media: Bound transmission media are the cables that are tangible or have physical existence and are limited by the physical geography. Popular bound transmission media in use are twisted pair cable, co-axial cable and fiber optical cable. Each of them has its own characteristics like transmission speed, effect of noise, physical appearance, cost etc.

Wireless or Unguided Media or Unbound Transmission Media: Unbound transmission media are the ways of transmitting data without using any cables. These media are not bounded by physical geography. This type of transmission is called Wireless **communication.** Nowadays wireless communication is becoming popular. Wireless LANs are being installed in office and college

campuses. This transmission uses Microwave, Radio wave, Infra red are some of popular unbound transmission media

Part-II

B- Attempt all the questions (short answers). Your answer should not exceed the maximum word limit of 80 words for each question. Each question carriers 4 marks.

Q1.Explain in brief:

a) **Simplex**
b) **Half-duplex**
c) **Full-Duplex**

Ans.**Simplex** :-A simplex communication channel only sends information in one direction. For example, a radio station usually sends signals to the audience but never receives signals from them, thus a radio station is a simplex channel. It is also common to use simplex channel in fiber optic communication. One strand is used for transmitting signals and the other is for receiving signals. But this might not be obvious because the pair of fiber strands are often combined to one cable. The good part of simplex mode is that its entire bandwidth can be used during the transmission.

2) Half duplex

In half duplex mode, data can be transmitted in both directions on a signal carrier except not at the same time. At a certain point, it is actually a simplex channel whose transmission direction can be switched. Walkie-talkie is a typical half duplex device. It has a "push-to-talk" button which can be used to turn on the transmitter but turn off the receiver. Therefore, once you push the button, you cannot hear the person you are talking to but your partner can hear you. An advantage of half-duplex is that the single track is cheaper than the double tracks.

3) Full duplex

A full duplex communication channel is able to transmit data in both directions on a signal carrier at the same time. It is constructed as a pair of simplex links that allows bidirectional simultaneous transmission. Take telephone as an example, people at both ends of a call can speak and be heard by each other at the same time because there are two communication paths between them. Thus, using the full duplex mode can greatly increase the efficiency of communication.

Q2.Explain Domain name space.

Ans.A domain namespace is a name service provided by the Internet for Transmission Control Protocol networks/Internet Protocol (TCP/IP). DNS is broken up into domains, a logical organization of computers that exist in a larger network. Below is an example of the hierarchy of domain naming on the Internet.

The naming system on which DNS is based is a hierarchical and logical tree structure called the domain namespace . Organizations can also create private networks that are not visible on the Internet, using their own domain namespaces. Figure 5.1 shows part of the Internet domain namespace, from the root domain and top-level Internet DNS domains, to the fictional DNS domain named reskit.com that contains a host (computer) named Mfgserver.

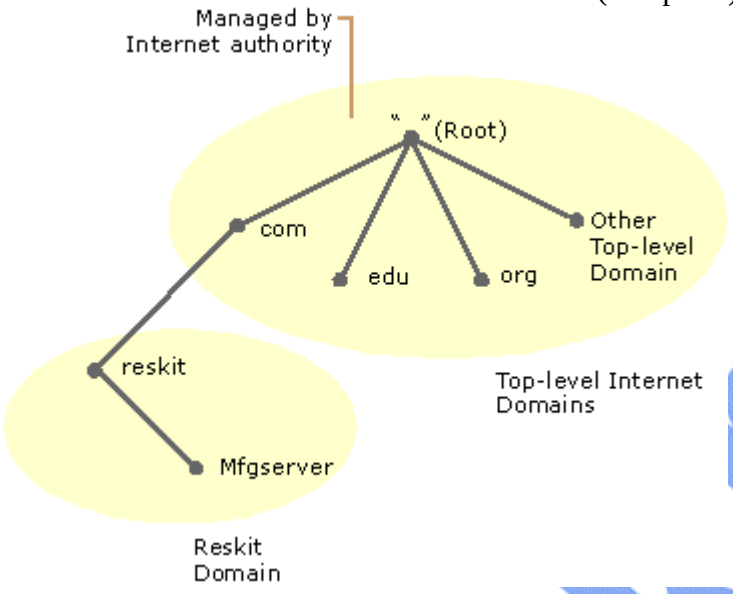
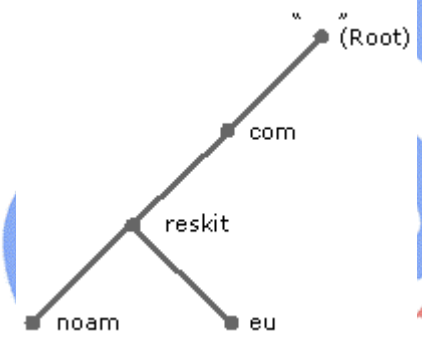


Figure 5.1 Domain Name System

Each node in the DNS tree represents a DNS name. Some examples of DNS names are DNS domains, computers, and services. A DNS domain is a branch under the node. For example, in Figure 5.1, reskit.com is a DNS domain. DNS domains can contain both hosts (computers or services) and other domains (referred to as subdomains). Each organization is assigned authority for a portion of the domain namespace and is responsible for administering, subdividing, and naming the DNS domains and computers within that portion of the namespace.



Q3. Explain ARP and RARP?

Ans.Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network. For example, in IP Version 4, the most common level of IP in use today, an address is 32 bits long. In an Ethernet local area network, however, addresses for attached devices are 48 bits long. (The physical machine address is also known as a Media Access Control or MAC address.) A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions.

RARP:-RARP (Reverse Address Resolution Protocol) is a protocol by which a physical machine in a local area network can request to learn its IP address from a gateway server's Address Resolution

Protocol (ARP) table or cache. A network administrator creates a table in a local area network's gateway router that maps the physical machine (or Media Access Control - MAC address) addresses to corresponding Internet Protocol addresses. When a new machine is set up, its RARP client program requests from the RARP server on the router to be sent its IP address. Assuming that an entry has been set up in the router table, the RARP server will return the IP address to the machine which can store it for future use.

Q4. How SNMP works in Internet Layer?

Ans. The Simple Network Management Protocol (SNMP) is a framework for managing devices in an internet using the TCP/IP protocol suite. It provides a set of fundamental operations for monitoring and maintaining an internet.

SNMP uses the concept of manager and agent. That is, a manager, usually a host, controls and monitors a set of agents, usually routers.

SNMP is an application-level protocol in which a few manager stations control a set of agents. The protocol is designed at the application level so that it can monitor devices made by different manufacturers and installed on different physical networks. In other words, SNMP frees management tasks from both the physical characteristics of the managed devices and the underlying networking technology. It can be used in a heterogeneous internet made of different LANs and WANs connected by routers or gateways made by different manufacturers.

Managers and Agents A management station, called a manager, is a host that runs the SNMP client program. A managed station, called an agent, is a router (or a host) that runs the SNMP server program. Management is achieved through simple interaction between a manager and an agent. The agent keeps performance information in a database. The manager has access to the values in the database. For example, a router can store in appropriate variables, the number of packets received and forwarded. The manager can fetch and compare the values of these two variables to see if the router is congested or not.

The manager can also make the router perform certain actions. For example, a router can periodically check the value of a reboot counter to see when it should reboot itself. It reboots itself, for example, if the value of the counter is 0. The manager can use this feature to reboot the agent remotely at any time. It simply sends a packet to force a 0 value in the counter.

Agents can also contribute to the management process. The Server program running on the agent can check the environment and, if it notices something unusual, it can send a warning message (called a trap) to the manager.

In other words, management with SNMP is based on three basic ideas.

1. A manager checks an agent by requesting information that reflects the behavior of the agent.
2. A manager forces an agent to perform a task by resetting values in the agent database.
3. An agent contributes to the management process by warning the manager of an unusual situation.

Components Management in the Internet is achieved not only through the SNMP protocol but also by using other protocols that cooperate with SNMP. At the top level, management is accomplished with two protocols.

1. Structure of management information (SMI)
2. Management information base (MIB)

Q5. What is Network Function and protocol Operations?

Ans. HTTP, FTP, SMTP and DNS (Session/Presentation/Application Layers)

There protocols listed below are a few of the more well-known:

- DNS - Domain Name System - translates network address (such as IP addresses) into terms understood by humans (such as Domain Names) and vice-versa
- DHCP - Dynamic Host Configuration Protocol - can automatically assign Internet addresses to computers and users
- FTP - File Transfer Protocol - a protocol that is used to transfer and manipulate files on the Internet
- HTTP - HyperText Transfer Protocol - An Internet-based protocol for sending and receiving webpages
- IMAP - Internet Message Access Protocol - A protocol for e-mail messages on the Internet
- IRC - Internet Relay Chat - a protocol used for Internet chat and other communications
- POP3 - Post Office protocol Version 3 - a protocol used by e-mail clients to retrieve messages from remote servers
- SMTP - Simple Mail Transfer Protocol - A protocol for e-mail messages on the Internet

Part-III

C- Attempt all the questions (long answer). Draw neat and comprehensive sketches wherever necessary to clearly illustrate your answer. Each question carries 12 marks.

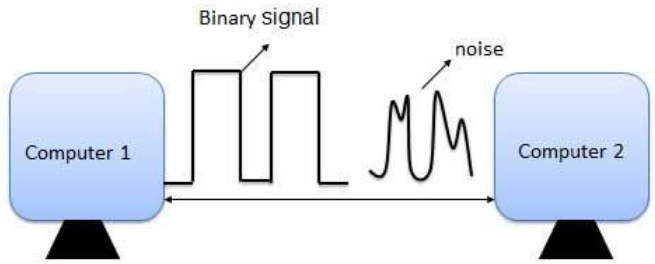
Q1.Differentiate between LAN, MAN, WAN?
Ans.

BASIS OF COMPARISON	LAN	MAN	WAN
Expands to	Local Area Network	Metropolitan Area Network	Wide Area Network
Meaning	A network that connects a group of	It covers relatively large region	It spans large locality and connects countries

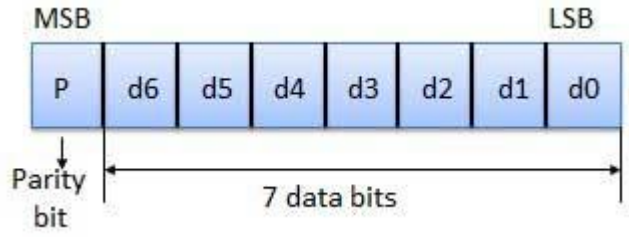
	computers in a small geographical area.	such as cities, towns.	together. Example Internet.
Ownership of Network	Private	Private or Public	Private or Public
Design and maintenance	Easy	Difficult	Difficult
Propagation Delay	Short	Moderate	Long
Speed	High	Moderate	Low
Fault Tolerance	More Tolerant	Less Tolerant	Less Tolerant
Congestion	Less	More	More
Used for	College, School, Hospital.	Small towns, City.	Country/Continent.

Q2.What is Error Correction and Detection? Explain.

Ans. Error is a condition when the output information does not match with the input information. During transmission, digital signals suffer from noise that can introduce errors in the binary bits travelling from one system to other. That means a 0 bit may change to 1 or a 1 bit may change to 0.



- Error-Detecting codes
- Whenever a message is transmitted, it may get scrambled by noise or data may get corrupted. To avoid this, we use error-detecting codes which are additional data added to a given digital message to help us detect if an error occurred during transmission of the message. A simple example of error-detecting code is parity check.
- Error-Correcting codes
- Along with error-detecting code, we can also pass some data to figure out the original message from the corrupt message that we received. This type of code is called an error-correcting code. Error-correcting codes also deploy the same strategy as error-detecting codes but additionally, such codes also detect the exact location of the corrupt bit.
- In error-correcting codes, parity check has a simple way to detect errors along with a sophisticated mechanism to determine the corrupt bit location. Once the corrupt bit is located, its value is reverted (from 0 to 1 or 1 to 0) to get the original message.
- How to Detect and Correct Errors?
- To detect and correct the errors, additional bits are added to the data bits at the time of transmission.
- The additional bits are called parity bits. They allow detection or correction of the errors.
- The data bits along with the parity bits form a code word.
- Parity Checking of Error Detection
- It is the simplest technique for detecting and correcting errors. The MSB of an 8-bits word is used as the parity bit and the remaining 7 bits are used as data or message bits. The parity of 8-bits transmitted word can be either even parity or odd parity.



- Even parity -- Even parity means the number of 1's in the given word including the parity bit should be even (2,4,6,....).
- Odd parity -- Odd parity means the number of 1's in the given word including the parity bit should be odd (1,3,5,....).
- Use of Parity Bit
- The parity bit can be set to 0 and 1 depending on the type of the parity required.
- For even parity, this bit is set to 1 or 0 such that the no. of "1 bits" in the entire word is even. Shown in fig. (a).

- For odd parity, this bit is set to 1 or 0 such that the no. of "1 bits" in the entire word is odd. Shown in fig. (b).

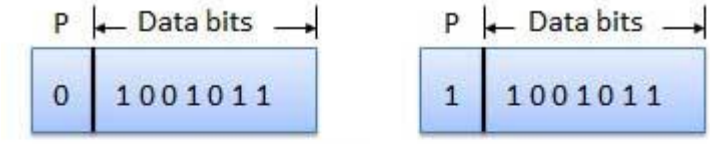


Fig. (a)

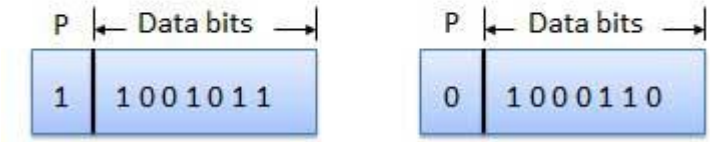
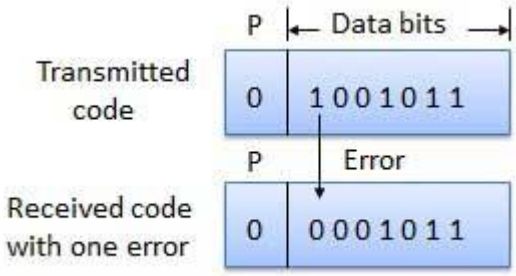


Fig. (b)

- How Does Error Detection Take Place?
- Parity checking at the receiver can detect the presence of an error if the parity of the receiver signal is different from the expected parity. That means, if it is known that the parity of the transmitted signal is always going to be "even" and if the received signal has an odd parity, then the receiver can conclude that the received signal is not correct. If an error is detected, then the receiver will ignore the received byte and request for retransmission of the same byte to the transmitter.



Q3. Explain Congestion control &Open loop algorithm?

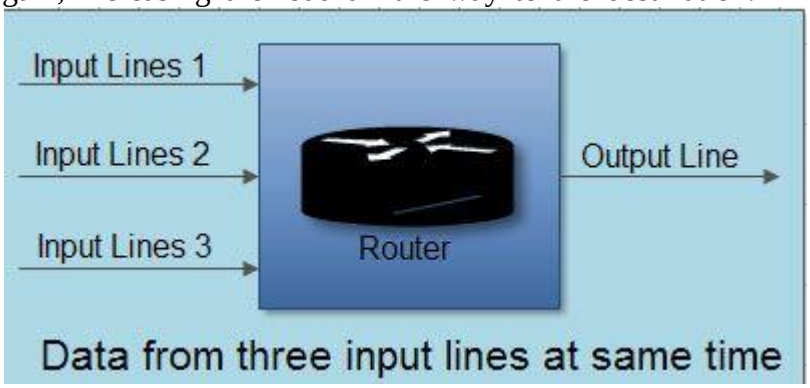
Ans. Congestion is an important issue that can arise in packet switched network. Congestion is a situation in Communication Networks in which too many packets are present in a part of the subnet, performance degrades. Congestion in a network may occur when the load on the network (i.e. the number of packets sent to the network) is greater than the capacity of the network (i.e. the number of packets a network can handle.

Causing of Congestion:

The various causes of congestion in a subnet are:

• The input traffic rate exceeds the capacity of the output lines. If suddenly, a stream of packet start arriving on three or four input lines and all need the same output line. In this case, a queue will be built up. If there is insufficient memory to hold all the packets, the packet will be lost. Increasing the memory to unlimited size does not solve the problem. This is because, by the time packets reach front of the queue, they have already timed out (as they waited the queue). When timer goes off source transmits duplicate packet that are also added to the queue. Thus same packets are added again and

again, increasing the load all the way to the destination.



• The routers are too slow to perform bookkeeping tasks (queuing buffers, updating tables, etc.).
• The routers' buffer is too limited.
• Congestion in a subnet can occur if the processors are slow. Slow speed CPU at routers will perform the routine tasks such as queuing buffers, updating table etc slowly. As a result of this, queues are built up even though there is excess line capacity.
• Congestion is also caused by slow links. This problem will be solved when high speed links are used. But it is not always the case. Sometimes increase in link bandwidth can further deteriorate the congestion problem as higher speed links may make the network more unbalanced.Congestion can make itself worse. If a route!" does not have free buffers, it start ignoring/discarding the newly arriving packets. When these packets are discarded, the sender may retransmit them after the timer goes off. Such packets are transmitted by the sender again and again until the source gets the acknowledgement of these packets. Therefore multiple transmissions of packets will force the congestion to take place at the sending end.

How to correct the Congestion Problem:

Congestion Control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened. Congestion control mechanisms are divided into two categories, one category prevents the congestion from happening and the other category removes congestion after it has taken place.

These two categories are:

1. Open loop

2. Closed loop

Open Loop Congestion Control

• In this method, policies are used to prevent the congestion before it happens.

• Congestion control is handled either by the source or by the destination.

• The various methods used for open loop congestion control are:

Q4. Explain the following terms
***FTP *HTTPS**

Ans.The File Transfer Protocol (FTP) is a standard network protocol used for the transfer of computer files between a client and server on a computer network.

FTP is built on a client-server model architecture and uses separate control and data connections between the client and the server.[1]FTP users may authenticate themselves with a clear-text sign-in

protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it. For secure transmission that protects the username and password, and encrypts the content, FTP is often secured with SSL/TLS (FTPS). SSH File Transfer Protocol (SFTP) is sometimes also used instead; it is technologically different.

HTTPS (HTTP Secure) is an adaptation of the Hypertext Transfer Protocol (HTTP) for secure communication over a computer network, and is widely used on the Internet. In HTTPS, the communication protocol is encrypted by Transport Layer Security (TLS), or formerly, its predecessor, Secure Sockets Layer (SSL). The protocol is therefore also often referred to as HTTP over TLS or HTTP over SSL.

The principal motivation for HTTPS is authentication of the accessed website and protection of the privacy and integrity of the exchanged data. It protects against man-in-the-middle attacks. The bidirectional encryption of communications between a client and server protects against eavesdropping and tampering of the communication.[5] In practice, this provides a reasonable assurance that one is communicating without interference by attackers with the website that one intended to communicate with, as opposed to an impostor.

Historically, HTTPS connections were primarily used for payment transactions on the World Wide Web, e-mail and for sensitive transactions in corporate information systems.[citation needed] Since 2018 HTTPS is more used on websites than the original non-secure HTTP; protecting page authenticity on all types of websites, securing accounts and keeping user communications, identity and web browsing private.

Q5. What is TCP/IP model? Explain layers with diagrams?
Ans.

Layer 4. Application Layer

Application layer is the top most layer of four layer TCP/IP model. Application layer is present on the top of the Transport layer. Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.

Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol) , DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

Layer 3. Transport Layer

Transport Layer is the third layer of the four layer TCP/IP model. The position of the Transport layer is between Application layer and Internet layer. The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation. Transport layer defines the level of service and status of the connection used when transporting data.

The main protocols included at Transport layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Layer 2. Internet Layer

Internet Layer is the second layer of the four layer TCP/IP model. The position of Internet layer is between Network Access Layer and Transport layer. Internet layer pack data into data packets known as IP datagrams, which contain source and destination address (logical address or IP address) information that is used to forward the datagrams between hosts and across networks. The Internet layer is also responsible for routing of IP datagrams.

Packet switching network depends upon a connectionless internetwork layer. This layer is known as Internet layer. Its job is to allow hosts to insert packets into any network and have them to deliver independently to the destination. At the destination side data packets may appear in a different order than they were sent. It is the job of the higher layers to rearrange them in order to deliver them to proper network applications operating at the Application layer.

The main protocols included at Internet layer are IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol) and IGMP (Internet Group Management Protocol).

Layer 1. Network Access Layer

Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.

The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

The most popular LAN architecture among those listed above is Ethernet. Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to access the media, when Ethernet operates in a shared media. An Access Method determines how a host will place data on the medium.

IN CSMA/CD Access Method, every host has equal access to the medium and can place data on the wire when the wire is free from network traffic. When a host wants to place data on the wire, it will check the wire to find whether another host is already using the medium. If there is traffic already in the medium, the host will wait and if there is no traffic, it will place the data in the medium. But, if two systems place data on the medium at the same instance, they will collide with each other, destroying the data. If the data is destroyed during transmission, the data will need to be retransmitted. After collision, each host will wait for a small interval of time and again the data will be retransmitted.