**DATA COMMUNICATION & COMPUTER NETWORKS**

**4TH SEMESTER**

**ELECTRONICS & TELECOMMUNICATION**

**UNIT- 6 & 7**

COURSE CONTENT:

UNIT-6: LAN technology

* Topology & transmission medium.
* LAN protocol architecture.
* Medium access control.
* Bridges, HUB, switch.
* Ethernet (CSMA/CD), fiber channel.
* Wireless LAN technology.

UNIT-7: TCP/IP

* TCP/IP protocol suite.
* Basic protocol functions.
* Principles of internetworking.
* Internet protocol operations.
* Internet protocol.

UNIT-6

LAN Technology:

Introduction:

* A LAN consists of a shared transmission medium and a set of hardware & software for interfacing devices to the medium and regulating the orderly access to the medium.
* LANs have much greater capacity than WANs to carry greater internal communication load.
* The key elements of LAN are-
* Topology, Transmission medium, Wiring layout, Medium access control.

Topology & transmission medium:

* Topology refers to the way in which stations attached to the network are interconnected.
* The common topologies are- bus, tree, ring & star.

Bus & Tree topology:

* Use multipoint medium.
* In Bus, all stations are attached through a hardware interfacing known as tap, directly to the linear transmission medium, bus.



* Full duplex operation between station & tap allow data to be transmitted onto the bus and received from the bus.
* A transmission from any station propagates in both direction and received by all other station.
* At each end of bus is a terminator, which absorbs any signal, removing it from the bus.
* In Tree topology, the transmission medium is a branching cable with no closed loop.
* Transmission medium begins at a point known as headend. One or more cables start at the headend and each of these may have branches.
* Transmission from any propagates throughout the medium and received by all stations.



Disadvantage:

* Transmission from one station is received by all.
* Overlap of signal when two or more station transmit simultaneously.

Solution:

* Transmit data in frames which consists of header & control information.
* Each station assigned a unique address.

Ring topology:

* Network consists of repeaters joined by point-to-point link in a closed loop.
* Repeaters receive data on one link and transmit them bit by bit on another link.
* Links are unidirectional and transmitted in frames.
* As frame circulates through all stations, the destination station recognizes its address and copies the frame into the local buffer and then returns to the source where it is removed.



Star topology:

* Each station is directly connected to the common central node by two point-to-point link, one for transmission and another for reception.



* Central node operates in two ways-
1. Broadcast, i.e., frames transmitted on all ongoing links, referred as HUB.
2. Act as switch, i.e., incoming frame is buffered and then retransmitted on the outgoing link to the other destination address.

Choice of transmission medium:

* It is determined by- capacity, reliability, types of data supported & environmental scope.
* Cat3 UTP is most cost effective for single building, low traffic LAN installation.
* STP & baseband coaxial cable are more expensive, but provide greater capacity. Broadband cables are even more expensive and provide even greater capacity.
* Cat5 UTP supports high data rates for small no. of devices, but larger installation can be supported by use of star topology.
* Optical fiber has electromagnetic isolation, high capacity and small size, but high cost and lack of skilled personal to install and maintain.

LAN Protocol Architecture:

* Architecture of LAN is described in terms of layering of protocols that organize the basic function of LAN.

IEEE 802 reference model:

* Protocols define specifically for LAN & MAN transmission address issues relating to the transmission of blocks of data over the network.
* LAN protocol to OSI architecture was developed by IEEE 802 LAN standard committee adopted by all organization working on specification of LAN standards.
* It is generally referred as IEEE 802 reference model.



* The lowest layer is the physical layer.
* The layer above the physical layer, i.e., layer 2, provides services to LAN user such as-
1. On transmission, assemble data into frame with address and error detection fields.
2. On reception, disassemble frame, and perform address recognition and error detection.
3. Govern access to LAN transmission medium.
4. Provides an interface to higher layer and perform flow and error control.
* 1st three points are treated as Medium Access Control (MAC), and last point is Logical Link Control (LLC).



Logical Link Control:

* This layer is concerned with transmission of link level protocol data unit (PDU) between two stations, without any intermediate switching nodes.
* LLC involves addressing source and destination LLC user referred as Service Access Point (SAP).

LLC protocols:

* It has three protocols-
1. Type 1 operation is used to transfer data.
2. Type 2 operation establishes data link connection between two LLC SAPs prior to data exchange.
3. Type 3 operation acknowledges each transmitted PDU.
* LLC permits multiplexing by the use of LLC service access points (LSAPs).



* LLC PDU consists of four fields-

DSAP (Destination SAP) & SSAP (Source SAP) fields each contain 7-bit address which specifies the destination and source users of LLC.

1-bit of DSAP indicate whether DSAP is an individual or group (I/G).

1-bit of SSAP indicate whether PDU is command or response (C/R).

Medium Access Control:

* MAC protocol is used for controlling access to the transmission medium by providing orderly & efficient use of that capacity.
* Controlling may be centralized or distributed.
* In centralized scheme, a controller is assigned that has authority to grant access to the network.
* In distributed scheme, the stations collectively perform MAC function to determine dynamically the order in which station transmit.
* Access control techniques are categorized as synchronous and asynchronous.
* In synchronous technique, a specific capacity is dedicated to a connection. It is same as circuit switching, FDM & synchronous TDM.
* In asynchronous technique, capacity is allocated dynamically in response to immediate demand.
* Asynchronous technique is further divided into three categories-
1. Round Robin: each station in turn is given opportunity to transmit. The station may decline to transmit or may transmit depending upon maximum amount of data transmitted or time for the opportunity (upper bound). The station when finish, relinquish its turn, and passes to the next station in logical sequence. Control of sequence is centralized or distributed.
2. Reservation: used for stream traffic. Time on the medium is divided into slots. A station wishing to transmit reserves future slot for extended or indefinite period. Reservation may be centralized or distributed.
3. Contention: used for bursty traffic. No control is exercised to determine whose turn it is, all station contends for time. Contention is distributed. Main advantage is simple to implement and under light to moderate load, efficient.

MAC frame format:

* MAC layer receives a block of data from LLC layer and is responsible for performing function related to medium access for transmitting data.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| MAC control | Destination MAC address | Source MAC address | LLC PDU | CRC |

* MAC frame has 5 fields-
1. MAC control: contains protocol control information needed for functioning MAC protocol. Eg. Priority level.
2. Destination MAC address: destination physical attachment point on the LAN for this frame.
3. Source MAC address: source physical attachment point on the LAN for this frame.
4. LLC PDU: LLC data for higher layer.
5. CRC: cyclic redundancy check for error detection.

Bridges:

* Bridge is designed for use between LANs that use identical protocols for physical and link layers.
* Since all device use same protocol, amount of processing required is minimum.



* Consider two LANs A & B connected with a bridge.
* Since single bridge is used to connect both the LANs, it function as two half bridge, one for each LAN.
* Bridge read all frames transmitted on LAN A and accept those addressed to any station on LAN B.
* Then using MAC protocol for B, retransmit each frame on B.
* Same process is repeated for traffic from B to A.
* Bridges should contain enough buffer space because frames may arrive faster than they are transmitted.
* Bridge must know which address are on each network to know which frame to pass.

Bridge protocol architecture:

* IEEE 802.1D specification define the protocol architecture for MAC bridges.
* Bridge function at MAC level because station address is assigned at MAC level.
* A MAC frame whose destination is not an immediate LAN is copied by bridge, buffered and then retransmitted on other LAN.



* Bridge must have routing capability depending on topology and may be altered dynamically.
* Most common routing is fixed routing.
* Each bridge has a routing table, which shows, for each possible destination MAC address, the identity of the LAN to which the bridge should forward the frame.
* Spanning tree approach is a mechanism in which bridges automatically develop a routing table and update that table in response to changing topology.
* The algorithm consists of three mechanism-
1. Frame forwarding: Bridge maintains a forwarding database for each port attached to a LAN which indicates the station address for which frame should be forwarded through the port. If destination MAC address is found, then frame is forwarded through that port. If MAC address is not found, frame is transmitted to all ports except to the incoming port.
2. Address learning: when frame arrives on a particular port, the frame consists of source address field. Bridge can update its forwarding database for that port of source address field of each incoming frame.
3. Loop resolution: used when there are alternate route, i.e., closed loop. Destination receives two copies of frame. So, one bridge has to be removed, resulting in spanning tree.

HUB

* Hub is the active central element of star layout.
* Each station is connected to the hub by two lines, transmit and receive.
* Hub act as repeater. It receives signal from a station and repeats the signal on the outgoing line of each station.
* Lines consist of two UTP, length limited to about 100m. optical fiber link is also used, length maximum is about 500m.
* Transmission from two stations simultaneously causes collision.
* Multiple levels of hubs can be cascaded in a hierarchical configuration.



Where, HHUB is header hub & IHUB is intermediate hub.

Each hub may have a mixture of stations and other hubs attached to it.

Switch

Layer 2 switch:

* A new device, layer 2 switch, has a replaced the hub for high speed LANs.
* Layer two switch is also sometimes referred to as switching hub.
* With layer 2 switch, an incoming frame from a particular station is switched to the appropriate output lines to be delivered to the intended destination.
* At the same time, other unused lines can be used for switching other traffic.
* No change is required to the software or hardware of the attached devices to convert a bus LAN or a hub LAN to a switched LAN.
* Layer 2 switch scales easily. Additional devices can be attached to the layer 2 switch by increasing the capacity of the layer 2 switch correspondingly.
* Layer 2 switches are available as-
1. Store and forward switch: accept a frame on an input line, buffers it, and then routes it to appropriate output lines.
2. Cut-through switch: repeats the incoming frame onto the appropriate output lines as soon as it recognizes the destination address in the MAC frame.
* Layer 2 switch provide increased performance to meet the needs of high volume traffic generated by personal computers, workstations and servers.
* As no. of devices in a building or complex of buildings grows, layer 2 switches become inadequate.
* To overcome the problems, a large local network is logically broken into a no. of subnetworks connected by routers.
* A MAC broadcast frame is then limited to only the devices and switches contained in a single subnetwork.
* To accommodate such load, a no. of vendors have developed layer 3 switches, which implement a packet forwarding logic of the router in hardware.

Ethernet:

* The most widely used high speed LANs are based on Ethernet and were developed by IEEE 802.3 standard committee.
* This has both MAC layer and physical layer.

IEEE 802.3 MAC:

* Ethernet uses CSMA/CD approach.
* Earlier ALOHA technique was used.
* In ALOHA, a station transmit a frame at any time and listen for an amount of time equal to the maximum round trip propagation delay on the network and a small fixed time.
* If the station hears acknowledgement at this time, fine, otherwise it resend the frame.
* If two stations transmit at a time, collision occurs.
* To improve efficiency, slotted ALOHA was developed where the channel was divided into equal slots whose size equal to the frame transmission time.
* But, both ALOHA and slotted ALOHA exhibit poor utilization.
* Thus, CSMA (Carrier Sense Multiple Access) was developed.
* With CSMA, a station who wants to transmit, first listen to the medium to determine if another transmission is in progress (carrier sense).
* If medium is in use, station waits, and if medium is idle, station transmit.
* To avoid collision, station waits for an amount of time after transmitting for an acknowledgement.
* If there is no acknowledgement, station assumes collision has occurred and retransmits.
* Longer the frame or shorter the propagation time, higher the utilization.
* Three approaches with CSMA-
1. Non-persistent CSMA algorithm:
2. If medium is idle, transmit.
3. If medium is busy, wait for an amount of time and retransmit.
4. 1-persistent protocol:
5. If medium is idle, transmit.
6. If medium is busy, continue to listen until channel is isle, then transmit immediately.
7. P-persistent:
8. If medium is idle, transmit with probability ‘P’ and delay one time unit with (1-P).
9. If medium is busy, continue to listen until idle then repeat step 1.
10. If transmission is delayed one unit time, repeat step 1.
* With CSMA/CD:
1. If medium is idle, transmit.
2. If medium is busy, continue to listen until the channel is idle, then transmit immediately.
3. If collision is detected during transmission, transmit a brief jamming signal to assure that all station know that there has been a collision and then cease transmission.
4. After transmitting the jamming signal, wait a random amount of time, referred as back-off, then attempt to transmit again.

MAC frame:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Preamble | SFD | DA | SA | Length | LLC data  | Pad  | FCS |

7octet 1 6 6 2 ≥0 ≥0 4

1. Preamble: 7 octet pattern of alternating 0s and 1s used by receiver to establish bit synchronization.
2. SFD (Start Frame Delimiter): the sequence 10101011, which indicates actual start of frame and enables the receiver to locate the 1st and rest bit of frame.
3. DA (Destination Address): specifies the station for which the frame is intended. It may be global address, group address or unique physical address.
4. SA (Source Address): specifies the station that sent the frame.
5. Length/type: length of LLC data field in octet, or Ethernet type field, depending on whether the frame confirms IEEE 802.3 standard or earlier Ethernet specification.
6. LLC data: data unit supplied by LLC.
7. Pad: octets added to ensure that the frame is long enough for proper operation.
8. FCS (Frame Check Sequence): 32-bit CRC, based on all fields except preamble, SFD and FCS.

Ethernet with different speed:

* 10Mbps- standard Ethernet.
* 100Mbps- fast Ethernet.
* 1Gbps-10Gbps-gigabit Ethernet.

Addressing:

* Each station on an Ethernet network has its own Network Interface Card (NIC) which provides with link layer address.
* Ethernet address is 6 byte (48 bit) written in hex notation with colon. Example: 4A:30:10:21:10:1A

Fiber channel:

* Fibre Channel is designed to combine the best of both channel and network data communication.
* A channel is a direct or switched point-to-point connection. One benefit of a channel is that it is mostly hardware-intensive for speed and efficiency of data transport.
* This is compared to the higher overhead of network data transfer, which is slower because it is software-intensive.
* The benefit of networks is that they can handle a greater range of tasks because they operate in an environment of unanticipated connections.
* Fiber Channel avoids the downside of network data transfer by providing a way to transfer data from a buffer at the source device to a buffer at the destination device. Fibre Channel does not need to know what the data is or how it is formatted.
* What the individual protocols do with the data before or after it is in the buffer is independent of the function of Fibre Channel.
* All a Fibre Channel port has to do is to manage a simple point-to-point connection between itself and the Fabric.
* A Fabric is a circuit switch, active hub, or a loop.
* The transfer rates of Fibre Channel are currently (133 Mbps,266 Mbps,530 Mbps, and 1 Gbps).
* However, data rates of 2 to 4 Gbps should be available soon.
* Fibre Channel will allow simultaneous transmission of different protocols over a single optical-fiber pair and it can allow a number of existing services, such as network, point-to-point, and peripheral interfaces, to be accessed over a single medium using the same hardware connection.
* Fibre Channel also provides control and complete error checking.
* The Fibre Channel structure is defined as a multi-layered stack of functional levels, not unlike those used to represent network protocols, although not mapping directly to OSI layers.
* The layers of the Fibre Channel standard define the physical media and transmission rates, encoding scheme, framing protocol and flow control, common service, and the upper-level applications interfaces.
* The five layers are: FC-0, FC-1, FC-2, FC-3, FC-4.
* FC-0: the lowest layer, specifies the physical link in the system, including the media, transmitters, receivers, and connectors that can be used with Fibre Channel. This also includes electrical and optical characteristics, transmission rates, and other physical components of the standard. The physical level is designed to be able to use a large number of technologies to meet the widest range of system requirements. An end-to-end route can use different link technologies for increased performance and decreased cost, while at the same time, systems integrators can tailor an installation to meet the specific needs of their customers. FC-0 also specifies the (OFC) Open Fibre Control system, which is a safety system used to control the optical power level of SW laser data links in which an open fibre condition occurs. This safety feature is required because the optical power levels in this kind of system exceed the limits defined by the laser safety standards. Whenever this open fibre condition occurs in the link from the sending port, the receiver port detects it and pulses its laser at a low duty cycle within the laser safety requirements. The receiver at the other port detects the pulsing signal and itself sends pulses within the specified laser safety range. If the open fibre condition is restored, receivers from both ports receive the pulsing signals which will result in a double handshaking procedure to restore normal transmission after a couple of seconds.
* FC-1: defines all transmission protocols including serial encoding and decoding rules, special characters and error control. Every 8 bits of data are encoded into a 10 bit Transmission Character. A Transmission Word is composed of four contiguous Transmission Characters. The transmission code is DC balanced and the Transmission character is used to ensure that clock recovery is possible by having enough transitions present in the serial bit stream.
* FC-2: is called the signaling protocol level. It is responsible to break the data to be transmitted into frame size, and reassemble the frames after transport. It specifies the framing rules of the data to be sent from one port to another, ways for controlling the three service classes, and controlling the sequence in which the data is transferred. All frames in a transfer have a sequence number from 0 to N so that the receiver is able to tell if a frame is missing and exactly which frame(s) is missing.
* FC-3 is in the process of being defined for use by common services required for advanced features such as: striping - to multiply bandwidth ● hunt groups - the ability for more than one port to respond to the same alias address ● Multicast - which delivers a single transmission to multiple destination ports
* FC-4: This layer defines the application interfaces that can be run over Fibre Channel. Both network and channel protocols can concurrently run over the same physical interface providing seamless integration of standards.

Switched Fabric:

* The switched fabric topology gives the greatest connection capability and largest total combined throughput.
* Each device is connected to a switch and receives a non-blocking data path to any other connection on the switch.
* This would be equivalent to a dedicated connection to every device.
* As the number of devices increases to occupy multiple switches, the switches are in turn connected together.
* The switched fabric connection can interconnect large numbers of devices, sustain high bandwidth requirements, connect devices that run at different speeds, provide cable matching.

WIRELESS LAN TECHNOLOGY:

* Wireless LANs are generally categorized according to the transmission technique that is used. All current wireless LAN products fall into one of the following categories:
* Infrared (IR) LANs

• Spread spectrum LANs Infrared LANs

• Infrared LANs use infrared signals to transmit data. This is same technology used in products like remote controls for televisions and VCRs.

• These LANs can be setup using a point to point configuration is known as Directed- Beam IR.

• An omnidirectional configuration involves a single base station that is within Line of Sight of all other stations on the LAN. This station is mounted on the ceiling. The ceiling transmitter broadcasts an omnidirectional signal that can be received by all of the other IR Tran receivers in the area. These other Trans receivers transmit a directional beam aimed at the ceiling base unit.

• In a diffused configuration, all of the IR transmitters are focused and aimed at a point on a diffusely reflecting ceiling. IR radiation striking the ceiling is reradiated Omni directionally and picked up by all of the receivers in the area.

• Infrared equipment is inexpensive and simple.

• Many indoor environments experience rather intense infrared background radiation, from sunlight and indoor lighting. Spread Spectrum LANs

• Spread spectrum is currently the most widely used transmission technique for wireless LANs.

• It was initially developed by the military to avoid jamming.

• This is done by spreading the signal over a range of frequencies that consist of the industrial, scientific and medical bands of the electromagnetic spectrum.

• The first type of spread spectrum developed is known as frequency hopping spread spectrum.

• The other type of spread spectrum is called direct sequence spread spectrum.

• Frequency hopping radios currently use less power than direct sequence radios and generally cost less.

• While direct sequence data rate of 8 Mbps and frequency hopping have a limit of 2 Mbps.

UNIT-7: TCP/IP

TCP/IP PROTOCOL SUITE:

* The internet protocol suit is the conceptual model and set of communications protocols used in the internet and similar computer networks. It is known as TCP/IP because the foundational protocols in the suite are the Transmission Control Protocol (TCP) and the Internet Protocol (IP).
* The Internet Protocol suite provides end to end data communication specifying how data should be packetized, addressed, transmitted, routed and received.
* This functionality is organized into four abstraction layers.
* From lowest to highest, the layers are the link layer, containing communication methods for data that remains within a single network segment, the internet layer, providing inter networking between independent networks, the transport layer, handling host to host communication and the application layer, providing process to process data exchange for application.

BASIC PROTOCOL FUNCTIONS IN TCP/IP:

* The protocol functions are grouped into the following categories: • Encapsulation • Fragmentation and reassembly • Connection control • Ordered delivery • Flow control • Error control • Addressing • Multiplexing • Transmission services.

Encapsulation-

• For virtually all protocols, data are transferred in blocks, called Protocol Data Units (PDU).

• Each PDU contains not only data but also control information. The control information falls into three categories: Address, Error detecting code, protocol control. The addition of control information to data is referred to as encapsulation. Fragmentation and Reassembly-

• A protocol is concerned with exchanging data between two entities.

• Protocol may need to divide a block received from a higher layer into multiple blocks of some smaller bounded size. This process is called fragmentation. The counterpart of fragmentation is reassembly. Eventually, the segmented data must be reassembled into messages appropriate to the application level. If PDUs arrive out of order, the task is complicated

Connection Control-

• An entity may transmit data to another entity in such a way that each PDU is treated independently of all prior PDUs. This is known as connectionless data transfer, an example is the use of the datagram.

• Connection-oriented data transfer is preferred (even required) if stations anticipate a lengthy exchange of data. A logical association is established between the entities using three phases. • Connection establishment • Data transfer • Connection termination

Ordered Delivery-

• If two communicating entities are in different hosts2connected by a network, there is a risk that PDUs will not arrive in the order in which they were sent, because they may traverse different paths through the network.

• In connection-oriented protocols, it is generally required that PDU order always be maintained.

• If each PDU is given a unique number, and numbers are assigned sequentially, then it is a logically simple task for the receiving entity to reorder received PDUs on the basis of sequence number.

 Flow Control-

• Flow control is a function performed by a receiving entity to limit the amount or rate of data that is sent by a transmitting entity.

• The simplest form of flow control is a stop-and-wait procedure, in which each PDU must be acknowledged before the next can be sent.

• More efficient protocols involve some form of credit provided to the transmitter, which is the amount of data that can be sent without an acknowledgment. The HDLC sliding window technique is an example of this mechanism.

Error Control:

• Error control techniques are needed to guard against loss or damage of data and control information.

• Error control is implemented as two separate functions: 1) Error detection 2) Retransmission

Addressing:

The concept of addressing in a communications architecture is a complex one and covers a number of issues, including

• Addressing level • Addressing scope • Connection identifiers • Addressing mode • Addressing level refers to the level in the communications architecture at which an entity is named. • Another issue that relates to the address of an end system or intermediate system is addressing scope.

• The concept of connection identifiers comes into play when we consider connection oriented data transfer (e.g., virtual circuit) rather than connectionless data transfer (e.g., datagram).

• For connectionless data transfer, a global identifier is used with each data transmission.

• For connection-oriented transfer, it is sometimes desirable to use only a connection identifier during the data transfer phase.

• Another addressing concept is that of addressing mode. Most commonly, an address refers to a single system or port; in this case it is referred to as an individual or unicast address

• An address for multiple recipients may be broadcast.

Multiplexing:

One form of multiplexing is supported by means of multiple connections into a single system. For example, with frame relay, there can be multiple data link connections terminating in a single end system; we can say that these data link connections are multiplexed over the single physical interface between the end system and the network.

Transmission Services:

A protocol may provide a variety of additional services to the entities that use it. We mention here three common examples:

• Priority: Certain messages, such as control messages, may need to get through to the destination entity with minimum delay. An example would be a terminate-connection request. Thus, priority could be assigned on a message basis. Additionally, priority could be assigned on a connection basis.

• Quality of service: Certain classes of data may require a minimum throughput or a maximum delay threshold.

• Security: Security mechanisms, restricting access, may be invoked.

PRINCIPLE OF INTERNETWORKING:

Internet- A collection of communication networks interconnected by bridges and routers.

Intranet- An internet used by a single organization that provides the key internet applications. An internet operates within the organization for internal purposes.

End System- A device attached to one of the networks of an internet that is used to support end-user applications or services.

Intermediate System (ISs)- A device used to connect two networks and permit communication between end systems attached to different networks. Two types of ISs are bridges and routers.

Bridges- A bridges at layer 2 of the Open System Interconnection (OSI). An IS used to connect two LANs that use similar LAN protocols.

Routers- A router operates at layer 3 of the OSI architecture and routes packets between potentially different networks. Requirements

The overall requirements for an internetworking facility are as follows:

1. Provide a link between networks. At minimum, a physical and link control connection is needed.

2. Provide for the routing and delivery of data between processes on different networks.

3. Provide an accounting service that keeps track of the use of the various networks and routers and maintains status information.

4. Provide the services just listed in such a way as not to require modifications to the networking architecture. These include

• Different addressing schemes: The networks may use different endpoint names and addresses and directory maintenance schemes.

• Different maximum packet size: Packets from one network may have to be broken up into smaller pieces for another. This process is referred to as fragmentation.

• Different network access mechanisms: The network access mechanism between station and network may be different for stations on different networks.

• Different timeouts: Typically, a connection-oriented transport service will await an acknowledgment until a timeout expires, at which time it will retransmit its block of data. Internetwork timing procedures must allow successful transmission that avoids unnecessary retransmissions.

• Error recovery: Network procedures may provide anything from no error recovery up to reliable end-to-end (within the network) service.

• Status reporting: Different networks report status and performance differently. Yet it must be possible for the internetworking facility to provide such information on internetworking activity to interested and authorized processes.

• Routing techniques: Intra network routing may depend on fault detection and congestion control techniques. The internetworking facility must be able to coordinate these to route data adaptively between stations on different networks.

• User access control: Each network will have its own user access control technique (authorization for use of the network).

• Connection, connectionless: Individual networks may provide connection oriented (e.g., virtual circuit) or connectionless (datagram) service.

INTERNET PROTOCOL OPERATION:

* Operation of a connectionless internetworking scheme:
* IP provides a connectionless, or datagram, service between end systems. There are a number of advantages to this approach:
	+ A connectionless internet facility is flexible.
	+ A connectionless internet service can be made highly robust. This is basically the same argument made for a datagram network service versus a virtual circuit service.
	+ A connectionless internet service is best for connectionless transport protocols, because it does not impose unnecessary overhead. At each router, before the data can be forwarded, the router may need to fragment the datagram to accommodate a smaller maximum packet size limitation on the outgoing network. The router may also limit the length of its queue for each network to which it attaches so as to avoid having a slow network penalize a faster one. Once the queue limit is reached, additional data units are simply dropped. The destination end system recovers the IP datagram from its network wrapping. This service offered by IP is an unreliable one. With the Internet Protocol approach, each unit of data is passed from router to router in an attempt to get from source to destination. Design Issues Some design issues in greater detail:
	+ Routing • Datagram lifetime • Fragmentation and reassembly • Error control • Flow control

Routing-

* For the purpose of routing, each end system and router maintains a routing table that lists, for each possible destination network, the next router to which the internet datagram should be sent.
* Routing tables may also be used to support other inter-networking services, such as security and priority.
* Another routing technique is source routing.

Datagram lifetime-

* A simple way to implement lifetime is to use a hop count.
* Each time that a datagram passes through a router, the count is decremented.
* Alternatively, the life time could be a true measure of time.

Fragmentation and reassembly-

* Routers may need to fragment incoming datagrams into smaller pieces, called segments or fragments.
* To reassemble a datagram, there must be sufficient buffer space at the reassembly point.
* As fragments with the same ID arrive, their data fields are inserted in the proper position in the buffer until the entire data field is reassembled.

Error control-

* When a datagram is discarded by a router, the router should attempt to return some information to the source.
* The source Internet Protocol entity may use this information to modify its transmission strategy and may notify higher layers.

Flow control-

* Internet flow control allows routers and/or receiving stations to limit the rate at which they receive data. For the connectionless type of service we are describing, flow control mechanisms are limited.

INTERNET PROTOCOL:

* The Internet Protocol (IP) is part of the TCP/IP suite and is the most widely used internetworking protocol. As with any protocol standard, IP is specified in two parts:
* The interface with a higher layer (e.g., TCP), specifying the services that IP provides
* The actual protocol format and mechanisms

IP Services:

* The services to be provided across adjacent protocol layers (e.g., between IP and TCP) are expressed in terms of primitives and parameters. A primitive specifies the function to be performed, and the parameters are used to pass data and control information. The actual form of a primitive is implementation dependent. An example is a procedure call.
* IP provides two service primitives at the interface to the next higher layer. The Send primitive is used to request transmission of a data unit. The Deliver primitive is used by IP to notify a user of the arrival of a data unit. The parameters associated with the two primitives are as follows:
* Source address: Internetwork address of sending IP entity.
* Destination address: Internetwork address of destination IP entity.
* Protocol: Recipient protocol entity (an IP user, such as TCP).
* Type-of-service indicators: Used to specify the treatment of the data unit in its transmission through component networks.
* Identification: Used in combination with the source and destination addresses and user protocol to identify the data unit uniquely. This parameter is needed for reassembly and error reporting.
* Don’t fragment identifier: Indicates whether IP can fragment data to accomplish delivery.
* Time to live: Measured in seconds.
	+ Data length: Length of data being transmitted.
	+ Option data: Options requested by the IP user.
	+ Data: User data to be transmitted.

The currently defined options are as follows:

• Security: Allows a security label to be attached to a datagram.

• Source routing: A sequenced list of router addresses that specifies the route to be followed. Routing may be strict (only identified routers may be visited) or loose (other intermediate routers may be visited).

• Route recording: A field is allocated to record the sequence of routers visited by the datagram.

• Stream identification: Names reserved resources used for stream service. This service provides special handling for volatile periodic traffic (e.g., voice).

• Time stamping: The source IP entity and some or all intermediate routers add a timestamp (precision to milliseconds) to the data unit as it goes by.

Internet Protocol



 The protocol between IP entities is best described with reference to the IP datagram format. The fields are as follows:

* Version (4 bits): Indicates version number, to allow evolution of the protocol; the value is 4.
* Internet Header Length (IHL) (4 bits): Length of header in 32-bit words. The minimum value is five, for a minimum header length of 20 octets.
* Type of Service (8 bits): Prior to the introduction of differentiated services, this field was referred to as the Type of Service field and specified reliability, precedence, delay, and throughput parameters. This interpretation has now been superseded. The first six bits of this field are now referred to as the DS (Differentiated Services) field, the remaining 2 bits are reserved for an ECN (Explicit Congestion Notification) field, currently in the process of standardization. The ECN field provides for explicit signaling of congestion in a manner similar to that discussed for frame relay.
* Total Length (16 bits): Total datagram length, including header plus data, in octets.
* Identification (16 bits): A sequence number that, together with the source address, destination address and user protocol, is intended to identify a datagram uniquely. Thus, this number should be unique for the datagram’s source address, destination address, and user protocol for the time during which the datagram will remain in the internet.
* Flags (3 bits): Only two of the bits are currently defined. The More bit is used for fragmentation and reassembly, as previously explained. The Don’t Fragment bit prohibits fragmentation when set. This bit may be useful if it is known that the destination does not have the capability to reassemble fragments. However, if this bit is set, the datagram will be discarded if it exceeds the maximum size of an enroute network.
* Fragment Offset (13 bits): Indicates where in the original datagram this fragment belongs, measured in 64-bit units. This implies that fragments other than the last fragment must contain a data field that is a multiple of 64 bits in length.
* Time to Live (8 bits): Specifies how long, in seconds, a datagram is allowed to remain in the internet. Every router that processes a datagram must decrease the TTL by at least one, so the TTL is similar to a hop count.
* Protocol (8 bits): Indicates the next higher level protocol that is to receive the data field at the destination; thus, this field identifies the type of the next header in the packet after the IP header.
* Header Checksum (16 bits): An error-detecting code applied to the header only. Because some header fields may change during transit (e.g., Time to Live, fragmentation-related fields), this is reverified and recomputed at each router. The checksum is formed by taking the ones complement of the 16-bit ones complement addition of all 16-bit words in the header.  Source Address (32 bits): Coded to allow a variable allocation of bits to specify the network and the end system attached to the specified network, as discussed subsequently.  Destination Address (32 bits): Same characteristics as source address.
* Options (variable): Encodes the options requested by the sending user.
* Padding (variable): Used to ensure that the datagram header is a multiple of 32 bits in length.
* Data (variable): The data field must be an integer multiple of 8 bits in length. The maximum length of the datagram (data field plus header) is 65,535 octets.

IP Addresses:

* The source and destination address fields in the IP header each contain a 32-bit global internet address, generally consisting of a network identifier and a host identifier. Network Classes
* The address is coded to allow a variable allocation of bits to specify network and host. This encoding provides flexibility in assigning addresses to hosts and allows a mix of network sizes on an internet. The three principal network classes are best suited to the following conditions:

• Class A: Few networks, each with many hosts

• Class B: Medium number of networks, each with a medium number of hosts

• Class C: Many networks, each with a few hosts.

* Internet Control Message Protocol (ICMP)- ICMP provides a means for transferring messages from routers and other hosts to a host.
* ARP- The address resolution protocol (ARP) is a protocol used by the Internet Protocol (IP), specifically IPv4, to map IP network addresses to the hardware addresses used by a data link protocol. The protocol operates below the network layer as a part of the interface between the OSI network and OSI data link layer.