UNIT III

MEDIUM ACCESS SUB LAYER AND TRANSPORT PROTOCOL

The Medium Access Sub Layer : The channel allocation problem, Multiple access Protocols, Ethernet, Wireless LANs, Broadband Wireless, Bluetooth, Data Link Layer Switching.

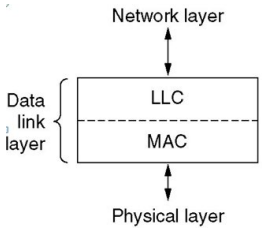
The Network Layer: Network Layer Design Issues, Routing Algorithms, Congestion Control Algorithms, Quality of Service.

The Transport Protocol: The Transport Service, Elements of transport protocol, Performance Issues

3.1 THE MEDIUM ACCESS SUB LAYER:

To coordinate the access to the channel, multiple access protocols are requiring. All these protocols belong to the MAC sub layer. Data Link layer is divided into two sub layers:

1. Logical Link Control (LLC)- is responsible for error control & flow control.
2. Medium Access Control (MAC)- MAC is responsible for multiple access resolutions



3.2 THE CHANNEL ALLOCATION PROBLEM

In broadcast networks, single channel is shared by several stations. This channel can be allocated to only one transmitting user at a time. There are two different methods of channel allocations:

1. **Static Channel Allocation**- a single channel is divided among various users either on the basis of frequency (FDM) or on the basis of time (TDM). In FDM, fixed frequency is assigned to each user, whereas, in TDM, fixed time slot is assigned to each user.
2. **Dynamic Channel Allocation-** no user is assigned fixed frequency or fixed time slot. All users are dynamically assigned frequency or time slot, depending upon the requirements of the user

3.3 MULTIPLE ACCESS PROTOCOLS

Many protocols have been defined to handle the access to shared link. These protocols are organized in three different groups:

- Random Access Protocols

- Controlled Access Protocols
- Channelization Protocols

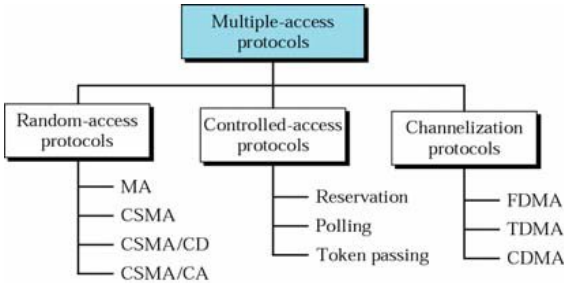


Fig 3.1 types of Multiple acess protocols

3.3.1 Random Access Protocols

There is no rule that decides which station should send next. If two stations transmit at the same time, there is collision and the frames are lost. The various random access methods are:

1. ALOHA
2. CSMA (Carrier Sense Multiple Access)
3. CSMA/CD (Carrier Sense Multiple Access with Collision Detection)
4. CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)

3.3.1.1 ALOHA

ALOHA was developed at University of Hawaii in early 1970s by Norman Abramson. It was used for ground based radio broadcasting. In this method, stations share a common channel. When two stations transmit simultaneously, collision occurs and frames are lost. There are two different versions of ALOHA:

- Pure ALOHA
- Slotted ALOHA

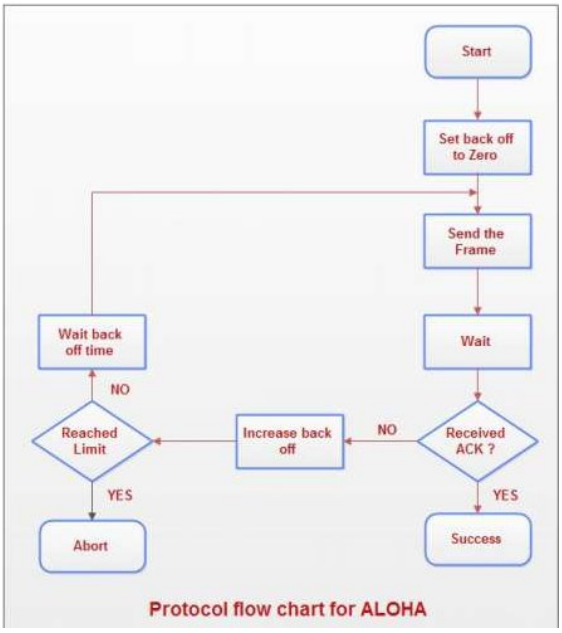


Fig 3.2 protocol flow chart for ALOHA

Pure ALOHA

In pure ALOHA, stations transmit frames whenever they have data to send. When two stations transmit simultaneously, there is collision and frames are lost. In pure ALOHA, whenever any station transmits a frame, it expects an acknowledgement from the receiver. If acknowledgement is not received within specified time, the station assumes that the frame has been lost. If the frame is lost, station waits for a random amount of time and sends it again. This waiting time must be random; otherwise, same frames will collide again and again. Whenever two frames try to occupy the channel at the same time, there will be collision and both the frames will be lost. If first bit of a new frame overlaps with the last bit of a frame almost finished, both frames will be lost and both will have to be retransmitted.

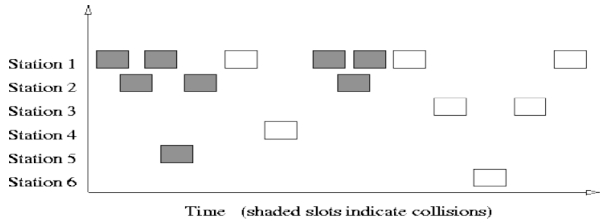


Fig 3.3 ALOHA Protocol

The probability of having *k* arrivals during a time interval of length *t* is given by:

$$P_k(t) = \frac{(\lambda t)^k e^{-\lambda t}}{k!}$$

where λ is the arrival rate. Note that this is a single-parameter model; all we have to know is λ.

Analysis of Pure ALOHA:

- Notation:
  - T_f = frame time (processing, transmission, propagation)
  - *S*: Average number of successful transmissions per T_f ; that is, the *throughput* or *efficiency*.
  - *G*: Average number of total frames transmitted per T_f
  - *D*: Average delay between the time a packet is ready for transmission and the completion of successful transmission.

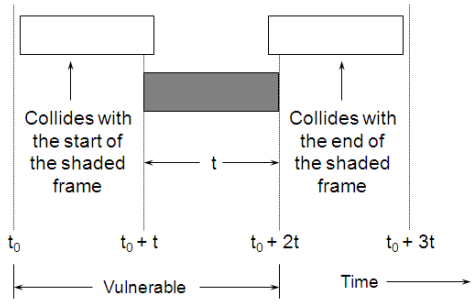
The following assumptions are

- All frames are of constant length
- The channel is noise-free; the errors are only due to collisions.
- Frames do not queue at individual stations
- The channel acts as a Poisson process.

Since *S* represents the number of "good" transmissions per *frame time*, and *G* represents the total number of attempted transmissions per *frame time*, then we have:

$S = G \cdot$ (Probability of good transmission)

- The vulnerable time for a successful transmission is $2T_f$
- So, the probability of good transmission is not to have an "arrival" during the vulnerable time .



Vulnerable period for the shaded frame

Fig 3.4 collision of frames

Using : $$P_k(t) = \frac{(\lambda t)^k e^{-\lambda t}}{k!}$$

And setting $t = 2T_f$ and $k = 0$, we get

$$P_0(2T_f) = \frac{(\lambda \cdot 2T_f)^0 e^{-\lambda 2T_f}}{0!} = e^{-2G}$$

$$\text{because } \lambda = \frac{G}{T_f}. \quad \text{Thus, } S = G \cdot e^{-2G}$$

If we differentiate $S = Ge^{-2G}$ with respect to G and set the result to 0 and solve for G, we find that the maximum occurs when $G = 0.5$, and for that $S = 1/2e = 0.18$. So, the maximum throughput is only 18% of capacity

Slotted ALOHA

Slotted ALOHA was invented to improve the efficiency of pure ALOHA. In slotted ALOHA, time of the channel is divided into intervals called slots. The station can send a frame only at the beginning of the slot and only one frame is sent in each slot. If any station is not able to place the frame onto the channel at the beginning of the slot, it has to wait until the next time slot. There is still a possibility of collision if two stations try to send at the beginning of the same time slot.

Analysis of Slotted ALOHA

Note that the vulnerable period is now reduced in half. Using:

$$P_k(t) = \frac{(\lambda t)^k e^{-\lambda t}}{k!}$$

And setting $t = T_f$ and $k = 0$, we get

$$P_0(T_f) = \frac{(\lambda \cdot T_f)^0 e^{-\lambda T_f}}{0!} = e^{-G}$$

$$\text{because } \lambda = \frac{G}{T_f}. \quad \text{Thus, } S = G \cdot e^{-G}$$

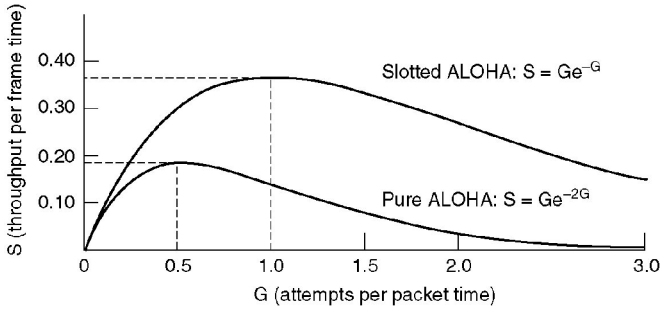


Fig 3.5 Throughput versus offered traffic for ALOHA systems.

3.3..2 Carrier Sense Multiple Access (CSMA)

` CSMA stands for Carrier Sense Multiple Access. Carrier Sense means, stations has an additional property with them, that they can sense the channel (carrier) and tell if the channel is in use or not. What we want, that at the start of the slot, stations should sense the channel first, and then act accordingly.

CSMA was developed to overcome the problems of ALOHA i.e. to minimize the chances of collision. The chances of collision reduces to a great extent if a station checks the channel before trying to use it.

There are three different types of CSMA protocols:

1. 1-Persistent CSMA
2. Non-Persistent CSMA
3. P-Persistent CSMA

3.3.2.1 1-Persistent CSMA

In this method, station that wants to transmit data, continuously senses the channel to check whether he channel is idle or busy. If the channel is busy, station waits until it becomes idle. When the station detects an idle channel, it immediately transmits the frame. This method has the highest chance of collision because two or more stations may find channel to be idle at the same time and transmit their frames.

3.3.2.2 Non-Persistent CSMA

A station that has a frame to send senses the channel. If the channel is idle, it sends immediately. If the channel is busy, it waits a random amount of time and then senses the channel again. It reduces the chance of collision because the stations wait for a random amount of time. It is unlikely that two or more stations will wait for the same amount of time and will retransmit at the same time.

3.3.2.3 P-Persistent CSMA

In this method, the channel has time slots such that the time slot duration is equal to or greater than the maximum propagation delay time. When a station is ready to send, it senses the channel. If the channel is busy, station waits until next slot. If the channel is idle, it transmits the frame. It reduces the chance of collision and improves the efficiency of the network.

3.3.2.4 CSMA with Collision Detection (CSMA/CD)

In this protocol, the station senses the channel before transmitting the frame. If the channel is busy, the station waits. Additional feature in CSMA/CD is that the stations can detect collisions. The stations abort their transmission as soon as they detect collision. This feature is not present in CSMA. The stations continue to transmit even though they find that collision has occurred.

In CSMA/CD, the station that sends its data on the channel, continues to sense the channel even after data transmission. If collision is detected, the station aborts its transmission and waits for a random amount of time & sends its data again. As soon as a collision is detected, the transmitting stations release a jam signal. Jam signal alerts other stations. Stations are not supposed to transmit immediately after the collision has occurred.

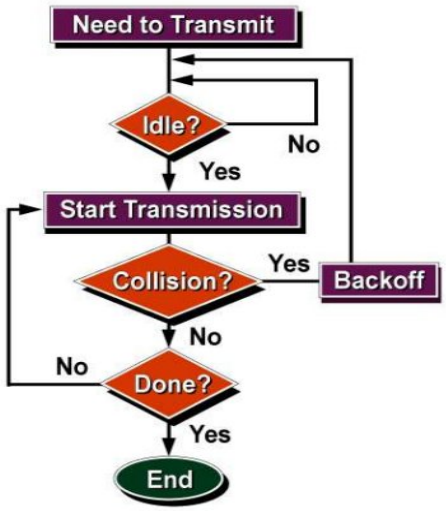


Fig 3.6 Flowchart for CSMA/CD

CSMA/CD can be in one of three states: contention, transmission, or idle.

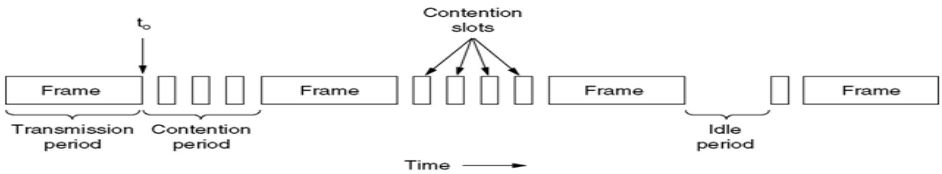


Fig 3.7 Frame format for CSMA/CD

3.3.2.5 CSMA with Collision Avoidance (CSMA/CA)

This protocol is used in wireless networks because they cannot detect the collision. So, the only solution is collision avoidance. It avoids the collision by using three basic techniques:

- Interframe Space
- Contention Window
- Acknowledgements

Interframe Space: Whenever the channel is found idle, the station does not transmit immediately. It waits for a period of time called Interframe Space (IFS). When channel is sensed idle, it may be possible that some distant station may have already started transmitting. Therefore, the purpose of IFS time is to allow this transmitted signal to reach its destination. If after this IFS time, channel is still idle, the station can send the frames.

Contention Window: Contention window is the amount of time divided into slots. Station that is ready to send chooses a random number of slots as its waiting time. The number of slots in the window changes with time. It means that it is set of one slot for the first time, and then doubles each time the station cannot detect an idle channel after the IFS time. In contention window, the station needs to sense the channel after each time slot.

Acknowledgment: Despite all the precautions, collisions may occur and destroy the data. Positive acknowledgement and the time-out timer help guarantee that the receiver has received the frame.

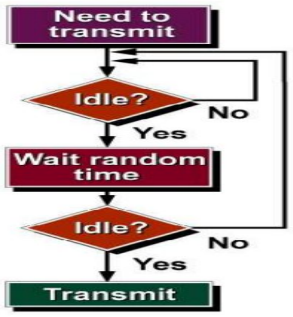


Fig 3.8 Flow chart for CSMA/CA

3.4 ETHERNET

Ethernet, developed in 1976, is the most widely-installed LAN technology, and typically uses coaxial or UTP cable. Ethernet technology uses broadcast topology with baseband signaling and a control method called Carrier Sense Multiple Access/Collision Detection (CSMA/CD) to transmit data. The IEEE 802.3 standard defines Ethernet protocols for (Open Systems Interconnect) OSI's Media Access Control (MAC) sublayer and physical layer network characteristics. The IEEE 802.2 standard defines protocols for the Logical Link Control (LLC) sublayer.

The most commonly installed Ethernet systems are called 10BASE-T, which provides transmission speeds up to 10 Mbps. 'Fast Ethernet' or 100BASE-T provides transmission speeds up to 100 megabits per second and is typically used for servers, LAN backbone systems and in workstations with high-bandwidth needs. Gigabit Ethernet provides an even faster level of backbone support at 1000 megabits per second (1 gigabit or 1 billion bits per second).

Ethernet is a passive, contention-based broadcast technology that uses baseband signaling. Baseband signaling uses the entire bandwidth of a cable for a single transmission. Only one signal can be transmitted at a time and every device on the shared network hears broadcast transmissions. Passive technology means that there is no one device controlling the network. Contention-based means that every device must compete with every other device for access to the shared network. In other words, devices take turns. They can transmit only when no other device is transmitting.

Physical layer configurations are specified in three parts
-Data rate (10, 100, 1,000) Mbps
-Signaling method –Baseband(Digital signaling) and Broadband(Analog signaling)
-Cabling (2, 5, T, F, S, L)

- 5 - Thick coax (original Ethernet cabling)
- F – Optical fiber
- S – Short wave laser over multimode fiber
- L – Long wave laser over single mode fiber

Frame format

Fig 3.9 Frame format of Ehernet

Preamble is a sequence of 7 bytes, each set to “10101010”. Used to synchronize receiver before actual data is sent
Addresses: -unique, 48-bit unicast address assigned to each adapter

- example: **8:0:e4:b1:2**
- Each manufacturer gets their own address range
  - broadcast: all **1**s
  - multicast: first bit is **1**

Type field is a demultiplexing key used to determine which higher level protocol the frame should be delivered to.
Body can contain up to 1500 bytes of data.

3.4.1 Ethernet working

When a node wants to communicate to another node, it transmits its frame. The frame travels to *every node on the segment*. Each node inspects the frame to see if it is addressed to him. If the frame is not addressed to the node, the node ignores it. If the frame *is* addressed to the node, the node opens the frame and reads its contents. The exception is a *broadcast address*, which is a special message intended to be read by every node (like a message on the P.A. as opposed to a comment from one person

to another).Token Ring, the main alternative to Ethernet, uses a different strategy to avoid computers talking at the same time.

Ethernet popularity is a result of several factors. Ethernet technology is:

- Inexpensive
- Easy to install, maintain, troubleshoot and expand
- A widely accepted industry standard, which means compatibility and
- equipment access are less of an issue
- Structured to allow compatibility with network operating systems
- (NOS)
- Very reliable

3.5 wireless LAN

wireless LAN technology based on IEEE 802.11 standard. Its predecessor the IEEE 802.3, commonly referred to as the Ethernet, is the most widely deployed member of the family. IEEE 802.11 is commonly referred to as wireless Ethernet because of its close similarity with the IEEE 802.3. Like IEEE 802.3, it also defines only two bottom levels of ISO's open system Interconnection (OSI) model. There are three media that can be used for transmission over wireless LANs. Infrared, radio frequency and microwave.

3.5.1 Framing

The frames can be categorized into three types; management frame, control frame and data frame. The management frames are used for association and disassociation of stations with at the AP, authentication and de-authentication, and timing and synchronization. Each frame consists of a MAC header, a frame body and a frame check sequence (FCS).

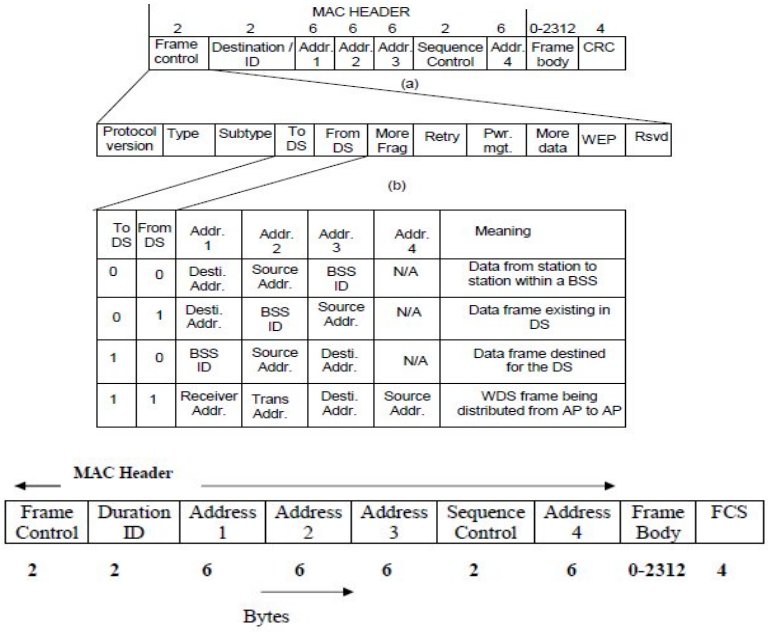


Fig3.10 The frame format of the IEEE 802.11

AC header will be described in a little while. Frame Body varies from 0-2312 bytes. At last is the FCS field. The *frame check sequence* is a 32-bit cyclic redundancy check which ensures there are no errors in the frame.

3.5.2 Frame Control Field (in MAC header)

The protocol version field is 2 bits in length and will carry the version of the 802.11 standard. The initial value of 802.11 is 0; all other bit values are reserved. Type and subtype fields are 2 and 4 bits, respectively. They work together hierarchically to determine the function of the frame. The remaining 8 fields are all 1 bit in length. The DS field is set to 1 if the frame is destined for the distribution system. From DS field is set to 1 when frames exit the distribution system. Note that frames which stay within their basic service set have both of these fields set to 0. The More Frag field is set to 1 if there is a following fragment of the current MSDU. Retry is set to 1 if this frame is a retransmission. Power Management field indicates if a station is in power save mode (set to 1) or active (set to 0). More data field is set to 1 if there is any MSDUs are buffered for that station. The WEP field is set to 1 if the information in the frame body was processed with the WEP algorithm. The Order field is set to 1 if the frames must be strictly ordered. The Duration/ID field is 2 bytes long. It contains the data on the duration value for each field and for control frames it carries the associated identity of the transmitting station. The address fields identify the basic service set, the destination address, the source address, and the receiver and transmitter addresses. Each address field is 6 bytes long. The sequence control field is 2 bytes and is split into 2 subfields, fragment number and sequence number. Fragment number is 4 bits and tells how many fragments the MSDU is broken into.

The sequence number field is 12 bits that indicates the sequence number of the MSDU. The frame body is a variable length field from 0 - 2312. This is the payload.

Advantages:

- **Availability of low-cost portable equipments:** Due to the technology enhancements, the equipment cost that are required for WLAN set-up have reduced a lot.
- **Mobility:** An increasing number of LAN users are becoming mobile. These mobile users require that they are connected to the network regardless of where they are because they want simultaneous access to the network. This makes the use of cables, or wired LANs, impractical if not impossible. Wireless LAN can provide users mobility, which is likely to increase productivity, user convenience and various service opportunities.
- **Installation speed and simplicity:** Wireless LANs are very easy to install. There is no requirement for wiring every workstation and every room. This ease of installation makes wireless LANs inherently flexible. If a workstation must be moved, it can be done easily and without additional wiring, cable drops or reconfiguration of the network.
- **Installation flexibility:** If a company moves to a new location, the wireless system is much easier to move than ripping up all of the cables that a wired system would have snaked throughout the building. This also provides portability. Wireless technology allows network to go anywhere wire cannot reach.
- **Reduced cost of ownership:** While the initial cost of wireless LAN can be higher than the cost of wired LAN hardware, it is envisaged that the overall installation expenses and life cycle costs can be significantly lower. Long-term cost-benefits are greater in dynamic environment requiring frequent moves and changes.
- **Scalability:** Wireless LAN can be configured in a variety of topologies to meet the users need and can be easily scaled to cover a large area with thousands of users roaming within it.

Limitation:

- Lower reliability due to susceptibility of radio transmission to noise and interference.
- Fluctuation of the strength of the received signal through multiple paths causing fading.
- Vulnerable to eavesdropping leading to security problem.
- Limited data rate because of the use of spread spectrum transmission techniques enforced to ISM band users.

3.6 BROADBAND WIRELESS

Wireless broadband is high-speed Internet and data service delivered through a wireless local area network (WLAN) or wide area network (WWAN). broadband means

"having instantaneous bandwidths greater than 1 MHz and supporting data rates greater than about 1.5 Mbit/s

As with other wireless service, wireless broadband may be either fixed or mobile. A fixed wireless service provides wireless Internet for devices in relatively permanent locations, such as homes and offices. Fixed wireless broadband technologies include LMDS (Local Multipoint Distribution System) and MMDS (Multichannel Multipoint Distribution Service) systems for broadband microwave wireless transmission direct from a local antenna to homes and businesses within a line-of-sight radius. The service is similar to that provided through digital subscriber line (DSL) or cable modem but the method of transmission is wireless. One particular access technology was standardized by IEEE 802.16, with products known as WiMAX.

A mobile broadband service provides connectivity to users who may be in temporary locations, such as coffee shops. WiMAX supports both fixed and mobile wireless and is often predicted to become the standard for wireless broadband.

3.6.1 WiMAX

WiMAX Acronym for Worldwide Interoperability for Microwave Access. It is Based on Wireless MAN technology. A wireless technology optimized for the delivery of IP centric services over a wide area. It is a scalable wireless platform for constructing alternative and complementary broadband networks. WiMAX is such an easy term that people tend to use it for the 802.16 standards and technology themselves, although strictly it applies only to systems that meet specific conformance criteria laid down by the WiMAX Forum.

The 802.16a standard for 2-11 GHz is a wireless metropolitan area network (MAN) technology that will provide broadband wireless connectivity to Fixed, Portable and Nomadic devices.

It can be used to connect 802.11 hot spots to the Internet, provide campus connectivity, and provide a wireless alternative to cable and DSL for last mile broadband access.

WiMax Speed and Range:

WiMAX is expected to offer initially up to about 40 Mbps capacity per wireless channel for both fixed and portable applications, depending on the particular technical configuration chosen, enough to support hundreds of businesses with T-1 speed connectivity and thousands of residences with DSL speed connectivity. WiMAX can support voice and video as well as Internet data.

WiMax developed to provide wireless broadband access to buildings, either in competition to existing wired networks or alone in currently unserved rural or thinly

populated areas. It can also be used to connect WLAN hotspots to the Internet. WiMAX is also intended to provide broadband connectivity to mobile devices. It would not be as fast as in these fixed applications, but expectations are for about 15 Mbps capacity in a 3 km cell coverage area.

With WiMAX, users could really cut free from today's Internet access arrangements and be able to go online at broadband speeds, almost wherever they like from within a Metro Zone. WiMAX could potentially be deployed in a variety of spectrum bands: 2.3GHz, 2.5GHz, 3.5GHz, and 5.8GHz. Support different application classes at the same time i.e Interactive gaming, VOIP & video conferencing, Streaming media (real time), Web browsing & instant messaging Media content download (store & forward).

3.7 BLUETOOTH

Bluetooth is a wireless technology standard for exchanging data over short distances (using short-wavelength UHF radio waves in the ISM band from 2.4 to 2.485 GHz) from fixed and mobile devices, and building personal area networks (PANs).

Wi-Fi and Bluetooth both occupy a section of the 2.4 GHz ISM band that is 83 MHz-wide. Bluetooth uses Frequency Hopping Spread Spectrum (FHSS) and is allowed to hop between 79 different 1 MHz-wide channels in this band.

3.7.1 Bluetooth Architecture

Bluetooth architecture defines two types of networks:

1. Piconet
2. Scattemet

1. Piconet

Piconet is a Bluetooth network that consists of one primary (master) node and seven active secondary (slave) nodes. Thus, piconet can have upto eight active nodes (1 master and 7 slaves) or stations within the distance of 10 meters. There can be only one primary or master station in each piconet. The communication between the primary and the secondary can be one-to-one or one-to-many. All communication is between master and a slave. Salve-slave communication is not possible. In addition to seven active slave station, a piconet can have upto 255 parked nodes. These parked nodes are secondary or slave stations and cannot take part in communication until it is moved from parked state to active state.

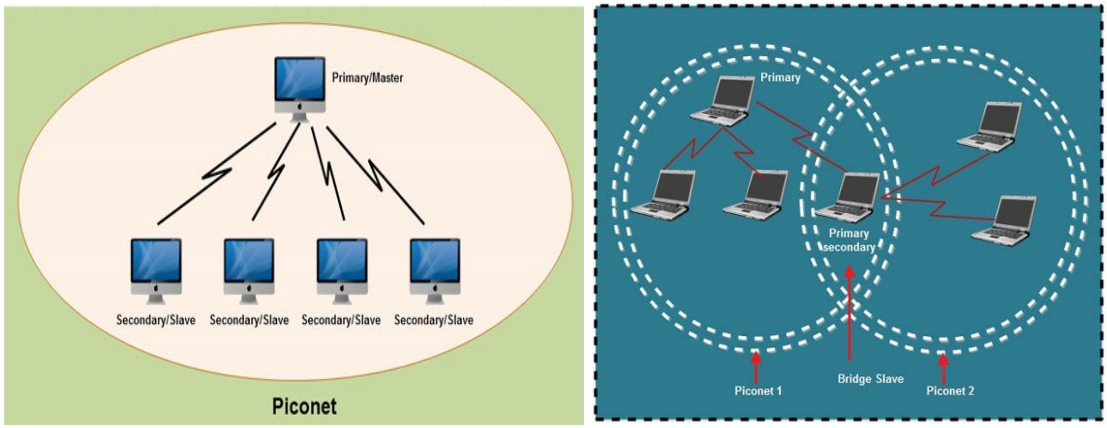


Fig 3.11 a)Bluetooth architecture a) piconet b) scatternet

3. Scatternet

Scattemet is formed by combining various piconets. A slave in one piconet can act as a master or primary in other piconet. Such a station or node can receive messages from the master in the first piconet and deliver the message to its slaves in other piconet where it is acting as master. This node is also called bridge slave. Thus a station can be a member of two piconets. A station cannot be a master in two piconets.

Bluetooth layers and Protocol Stack

Bluetooth standard has many protocols that are organized into different layers. The layer structure of Bluetooth does not follow OS1 model, TCP/IP model or any other known model.

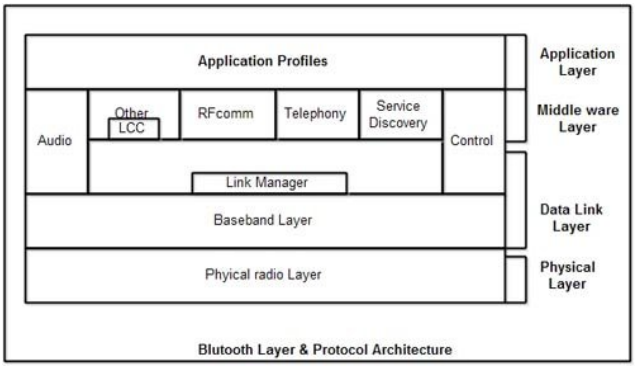


Fig 3.12 Different layers and Bluetooth protocol architecture.

Radio Layer

The Bluetooth radio layer corresponds to the physical layer of OSI model. It deals with ratio transmission and modulation. The radio layer moves data from master to slave or vice versa. It is a low power system that uses 2.4 GHz ISM band in a range of 10 meters. This band is divided into 79 channels of 1MHz each. Bluetooth uses the Frequency Hopping Spread Spectrum (FHSS) method in the physical layer to avoid interference from other devices or networks. Bluetooth hops 1600 times per

second, *i.e.* each device changes its modulation frequency 1600 times per second. In order to change bits into a signal, it uses a version of FSK called GFSK *i.e.* FSK with Gaussian bandwidth filtering.

Baseband Layer

Baseband layer is equivalent to the MAC sublayer in LANs. Bluetooth uses a form of TDMA called TDD-TDMA (time division duplex TDMA). Master and slave stations communicate with each other using time slots. The master in each piconet defines the time slot of 625 μsec. In TDD- TDMA, communication is half duplex in which receiver can send and receive data but not at the same time. If the piconet has only no slave; the master uses even numbered slots (0, 2, 4, ...) and the slave uses odd-numbered slots (1, 3, 5, ...). Both master and slave communicate in half duplex mode. In slot 0, master sends & secondary receives; in slot 1, secondary sends and primary receives. If piconet has more than one slave, the master uses even numbered slots. The slave sends in the next odd-numbered slot if the packet in the previous slot was addressed to it. In Baseband layer, two types of links can be created between a master and slave. These are:

1. Asynchronous Connection-less (ACL)

It is used for packet switched data that is available at irregular intervals. ACL delivers traffic on a best effort basis. Frames can be lost & may have to be retransmitted. A slave can have only one ACL link to its master. Thus ACL link is used where correct delivery is preferred over fast delivery. The ACL can achieve a maximum data rate of 721 kbps by using one, three or more slots.

2. Synchronous Connection Oriented (SCO)

sco is used for real time data such as sound. It is used where fast delivery is preferred over accurate delivery. In an sco link, a physical link is created between the master and slave by reserving specific slots at regular intervals. Damaged packet; are not retransmitted over sco links. A slave can have three sco links with the master and can send data at 64 Kbps.

Logical Link, Control Adaptation Protocol Layer (L2CAP)

The logical unit link control adaptation protocol is equivalent to logical link control sublayer of LAN. The ACL link uses L2CAP for data exchange but sco channel does not use it. The various function of L2CAP is:

1. Segmentation and reassembly

L2CAP receives the packets of upto 64 KB from upper layers and divides them into frames for transmission. It adds extra information to define the location of frame in the original packet. The L2CAP reassembles the frame into packets again at the destination.

2. Multiplexing

L2CAP performs multiplexing at sender side and demultiplexing at receiver side. At the sender site, it accepts data from one of the upper layer protocols frames them and

deliver them to the Baseband layer. At the receiver site, it accepts a frame from the baseband layer, extracts the data, and delivers them to the appropriate protocol1ayer.

3. Quality of Service (QOS)

L2CAP handles quality of service requirements, both when links are established and during normal operation. It also enables the devices to negotiate the maximum payload size during connection establishment.

Bluetooth Frame Format

The various fields of blue tooth frame format are:

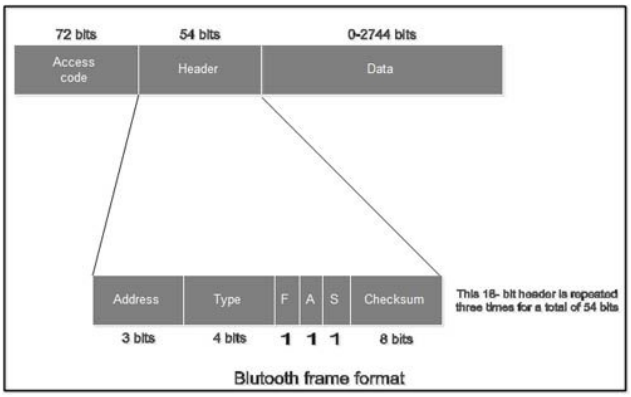


Fig 3.12 Bluetooth frame format

1. **Access Code**: It is 72 bit field that contains synchronization bits. It identifies the master.

2. **Header**: This is 54-bit field. It contain 18 bit pattern that is repeated for 3 time.

The header field contains following subfields:

(i) **Address**: This 3 bit field can define upto seven slaves (1 to 7). If the address is zero, it is used for broadcast communication from primary to all secondaries.

(ii)Type: This 4 bit field identifies the type of data coming from upper layers.

(iii) **F**: This flow bit is used for flow control. When set to 1, it means the device is unable to receive more frames.

(iv) **A**: This bit is used for acknowledgement.

(v) **S**: This bit contains a sequence number of the frame to detect retransmission. As stop and wait protocol is used, one bit is sufficient.

(vi) **Checksum**: This 8 bit field contains checksum to detect errors in header.

3. **Data**: This field can be 0 to 2744 bits long. It contains data or control information coming from upper layers.

3.8 Data Link Layer Switching.

LANs can be connected by devices called bridges, which operate in the data link layer. Bridges examine the data layer link addresses to do routing. Repeaters,

bridges, switches, hubs, routers, and gateways all of these devices are in common use, but they all differ in subtle. These devices operate in different layers. The layer matters because different devices use different pieces of information to decide how to switch. In a typical scenario, the user generates some data to be sent to a remote machine. Those data are passed to the transport layer, which then adds a header, for example, a TCP header, and passes the resulting unit down to the network layer. The network layer adds its own header to form a network layer packet, for example, an IP packet. Then the packet goes to the data link layer, which adds its own header and checksum (CRC) and gives the resulting frame to the physical layer for transmission, for example, over a LAN.

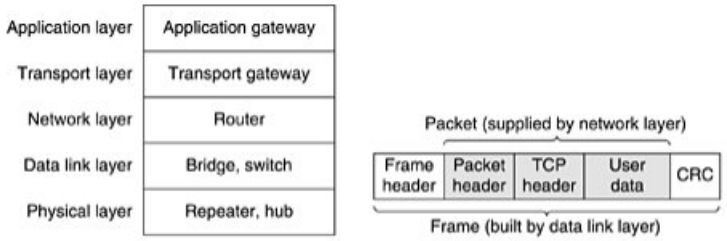


Fig 3.13 a) Device operated in each layer b) Frames, Packets and header

3.9 The Network Layer:

3.9.1 Network Layer Design Issues

The network layer design issues include

- Store-and-Forward Packet switching
- Provided service to the Transport Layer
- Implementation of Connectionless Service
- Implementation of Connection-Oriented Service

Store-and-Forward Packet switching

- Also known as packet switching.
- Packet Switching Data is divided into small parts (packets)
- Packets are transmitted from node to node, processed and forwarded.
- Two connection types
- Connectionless: datagram
- Connection-oriented:ν virtual circuit

Services Provided to Transport Layer

Services should be independent of router technology. Topology of network should be hidden. Network addresses available to transport layer should use be uniform, even across LANs and WANs. Network layer designers have freedom in writing specs of services to transport layer.

Connectionless Service

- No connection setup
- Message is broken into packets Called datagram (in analogy with telegram)
- Each packet is individually routed
- Routers decides line based on routing table
- Packets may follow different paths
- Not guaranteed to arrive in order

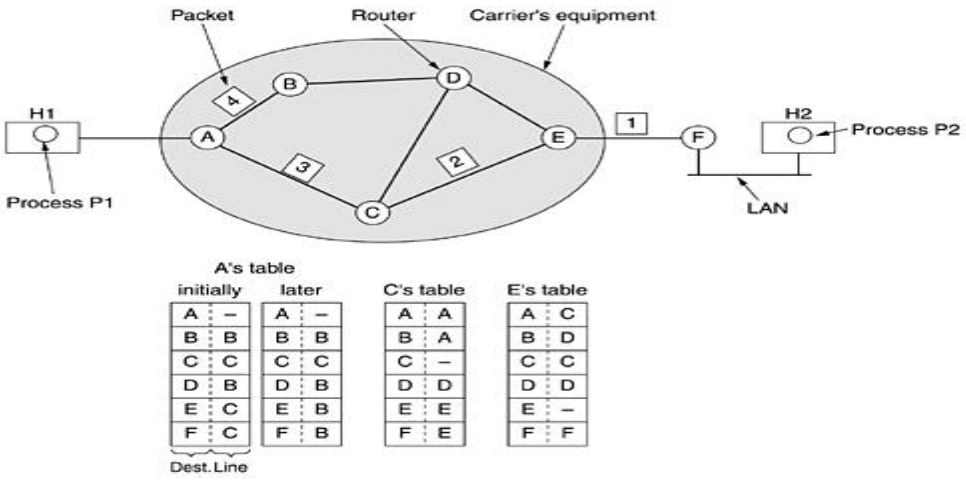


Figure 3.14 Routing within a Datagram-circuit subnet.

Connection-Oriented Service

- Path from source to destination must be established before any data can be sent
- Connection is called a VC (virtual circuit)
- analogy with physical circuit in phone system
- Avoid choosing new route for each packet
- Same route used for all packets in connection
- Each packet has ID for which VC it belongs to

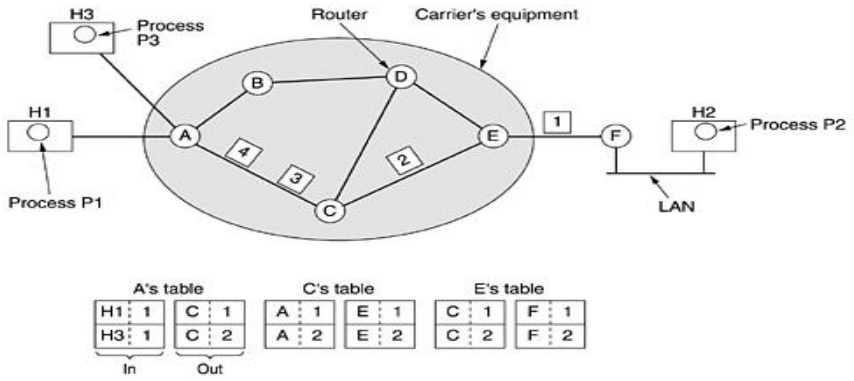


Fig 3.15 . Routing within a virtual-circuit subnet.

Table 1 comparison of virtual and datagram subnet

Issue	Datagram subnet	Virtual-circuit subnet
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC

3.10 Routing Algorithm

Network Layer Software responsible for deciding which output line an incoming packed should be transmitted on. The routing algorithms may be classified as follows:

Non-Adaptive Algorithms: Routing decision is based on pre-computed measurements or estimates and do not update the table based on current traffic and topology

Adaptive Algorithms: Change their routing decisions to reflect changes in the topology and traffic.

Optimization criterion are Distance, Bandwidth, Average Traffic Communication cost, Mean Queue Length, Measured Delay, e.t.c…

Algorithms:

3.10.1 Shortest Path Routing

The idea is to build a graph of the subnet, with each node of the graph representing a router and each arc representing a communication line (link).To choose a rout between a given pair of routers , the algorithm just finds the shortest path between them on the graph. The shortest path concept includes definition of the way of measuring path length. Deferent metrics like number of hops, geographical distance, the mean queuing and transmission delay of router can be used. In the most general case, the labels on the arcs could be computed as a function of the distance, bandwidth, average traffic, communication cost, mean queue length, measured delay, and other factors. There are several algorithms for computing shortest path between two nodes of a graph. One of them due to Dijkstra. The steps involved in this algorithm is shown below.

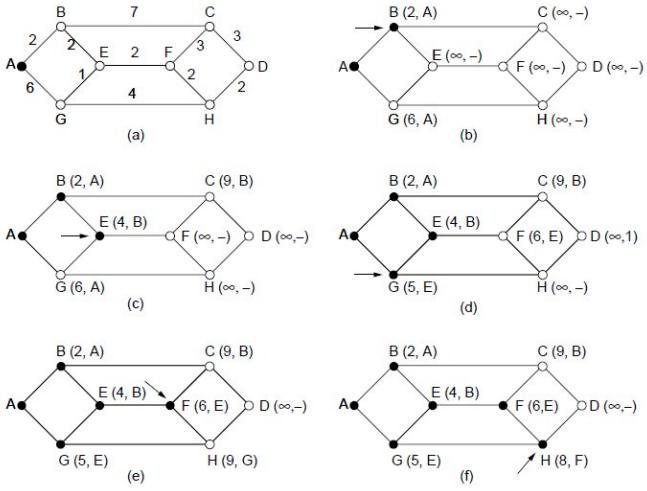


Fig 3.16 The first five steps used in computing the shortest path from *A to D.* The arrows indicate the working node.

3.10.2 Flooding

This is another static algorithm, in which every incoming packet is sent out on every outgoing line except the one it arrived on. Flooding generates infinite number of duplicate packets unless some measures are taken to damp the process.

One such measure is to have a hop counter in the header of each packet, which is decremented at each hop, with the packet being discarded when the counter reaches zero. Ideally, the hop counter is initialized to the length of the path from source to

destination. If the sender does not no the path length, it can initialize the counter to the worst case, the full diameter of the subnet.

An alternative technique is to keep track of which packets have been flooded, to avoid sending then out a second time. To achieve this goal the source router put a sequence number in each packet it receives from its hosts. Then each router needs a list per source router telling which sequence numbers originating at that source have already been seen. Any incoming packet that is on the list is not flooded. To prevent list form growing, each list should be augmented by a counter, k, meaning that all sequence numbers through k have been seen.

A variation of flooding named selective flooding is slightly more practical. In this algorithm the routers do not send every incoming packet out on every line, but only on those going approximately in the right direction.(there is usually little point in sending a westbound packet on an eastbound line unless the topology is extremely peculiar).

Flooding algorithms are rarely used, mostly with distributed systems or systems with tremendous robustness requirements at any instance.

3.10.3 Distance Vector Routing

It is a Dynamic Routing Algorithms in it take into account of actual network load. Each router maintains a table with the best known distance to each destination and which line to use to get there. Tables updated by exchanging information with the neighbors. The distance vector routing algorithm is sometimes called by other names including Bellman-Ford or Ford-Fulkerson. It was the original ARPANET routing algorithm and was also used in the Internet under the name RIP and in early versions of DECnet and Novell's IPX. AppleTalk & CISCO routers use improved distance vector protocols.

In that algorithm each router maintains a routing table indexed by and containing one entry for each router in the subnet. This entry contains two parts: the preferred outgoing line to use for that destination and an estimate of the time or distance to that destination. The metric used might be number of hops, time delay in milliseconds, total number of packets queued along the path or something similar.

The router is assumed to know the "distance" to each of its neighbors. In the hops metric the distance is one hop, for queue length metrics the router examines each queue, for the delay metric the route can measure it directly with special ECHO packets that the receiver just timestamps and sends back as fast as it can.

Distance vector routing works in theory, but has a serious drawback in practice: although it converges to the correct answer, it may be done slowly.

Count–to-Infinity Problem

- Slow Convergence to the correct answer.
- "Good news" Propagate fast
- "Bad news" Propagate slowly:
  - The core of the problem is that when X tells Y that I has a path somewhere, Y has no way of knowing whether it itself is on the path.

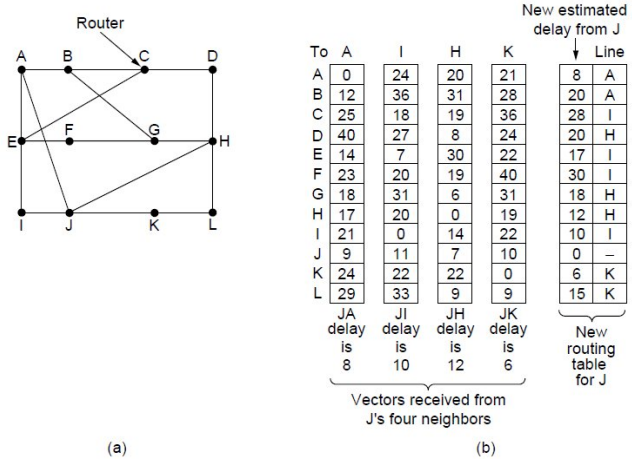


Fig 3.17 Distance vector routing algorithm

3.10.4 Link State Routing

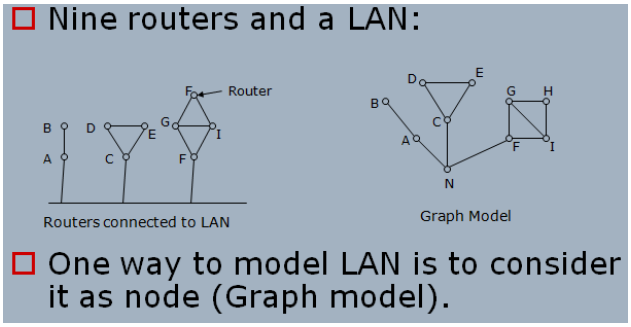
Each router must do the following:

1. Discover its neighbors and learn their network addresses.
2. Measure the delay or cost to each of its neighbors.
3. Construct a packet telling all it has just learned.
4. Send this packet to all other routers.
5. Compute the shortest path to every other router.

Complete topology and all delays are experimentally measured and distributed to every router. Dijkstra's algorithm can be run to find the shortest path to every other router.

Learning About the Neighbors

"HELLO" packed send on each point-to-point line from a booted router. Router on the other end must reply by sending its globally unique "name". Example of routers connected by a LAN.



3.18 Graph model for learning about neighbours

Measuring Line Cost

It is required by the Link State Routing algorithm that each router not have a reasonable estimate of the delay/cost to each of its neighbors. Send “ECHO” packet (ping) that the other side is required to send back immediately. Measure Round Trip time; Divide by 2 to get an estimate. More accurate estimate by repeating the process several times and by averaging estimates. Channel Load Issue when Measuring Delay to factor the load in: round trip timer must be started when the ECHO packed is queued. To ignore the load: round trip timer must be started when ECHO packed reaches front of the queue.

Building Link State Packets

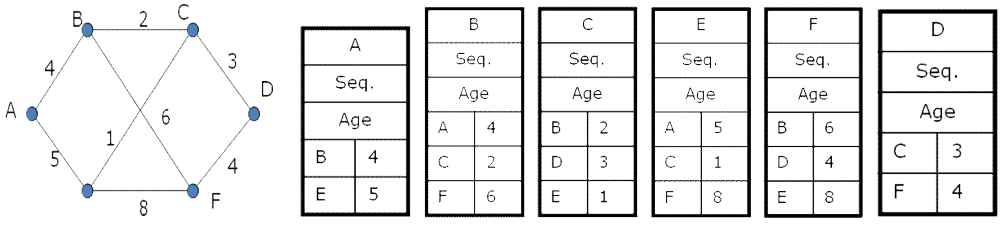


Fig 3.19 Packet Format:

Distributing the Link State Packets

The Basic Algorithm used for distributing the packet is Flooding. The Problems with basic algorithm are

1. Sequence Number wrap around.-Make a long precision number (e.g., 32-bit)
2. Crash of a router: losing track of sequence number.
3. Corruption of sequence number.

- Solution: Include Age of each packet.

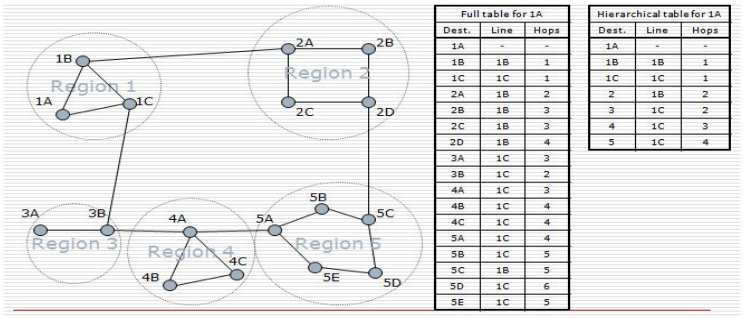
- Decrement this value once per second.
- When zero, this state information is disregarded.

3.10.5 Hierarchical Routing

It is used for Large Networks for such network the following problems acure:

- Proportionally large routing tables are required for each router
- More CPU time is needed to scan them
- More bandwidth is needed to send status reports.
- At certain point network may grow so large where it is no longer feasible for every router to have an entry for every other router.

In hierarchical routing the routers is divided in *Regions* (as in telephone network). Each router knows how to route packets to destinations within its own region. However, router does not have any information regarding the topology of the network of other regions. When different networks are interconnected they are regarded as a separate region in order to free the routers in one network from having to know the topological structure of the other ones. Huge networks will require more than two-level hierarchy.



Full table for 1A

Dest.	Line	Hops
1A	-	-
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

Hierarchical table for 1A

Dest.	Line	Hops
1A	-	-
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

Fig 3.20 Hierarchial Routing

3.10.6 Broadcast Routing

Sending a packed to all destinations simultaneously is called *Broadcasting*. There are many methods they are

Direct Method: Source sends a distinct packet to each destination routers in the subnet:

1. Wasteful of the bandwidth.
2. It requires source to have a list of all destinations.
3. In practice this may be the only feasible solution.

Flooding:

Ordinarily ill suited for point-to-point communication which Generates to many packets, and Consumes to much bandwidth**.**

Multi-destination Routing

Each packet contains a list of designations, or a bit map indicating the desired destinations. When packet arrives at a router the router checks all the destinations to determine the set of output lines that will be needed. Generates a new copy of the packed for each output line to be used and includes in each packet only those destinations that are to use the line. After a sufficient number of hops, each packed will carry only one destination and can be treated as normal packet. Multi-destination routing is like separately addressed packets, except that when several packets must follow the same rout, one of them pays full fare and the rest ride free.

Spanning Tree:

It is a subset of the subnet that includes all routers but contains no loops. Each router knows which of its lines belong to the spanning tree, it can copy an incoming broadcast packet onto all the spanning tree lines except the one it arrived on. Makes excellent use of bandwidth (generates absolute minimum number of packets necessary to do the job). Must have knowledge of some spanning tree for the method to be applicable: Information available in some instances (e.g., link state routing), Information not available (e.g., distance vector routing).

Reverse Path Forwarding:

Router checks if the broadcast packet arrived on the line that is normally used for sending packets *to* the source of the broadcast. If so, there is excellent chance that the broadcast packet itself followed the best route from the router and is therefore the first copy to arrive at the router. The router forwards copies of it onto all lines except the one it arrived on. If the broadcast packet arrived on a line other than the preferred one for reaching the source, the packet is discarded as a likely duplicate.

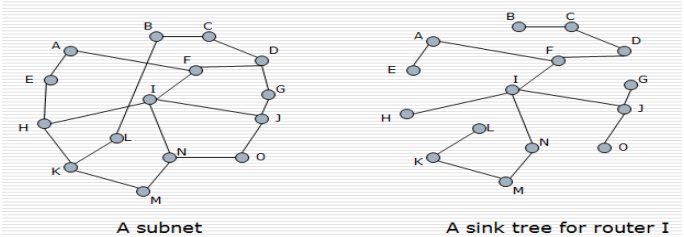


Fig 3.21 Example of Reverse path Forwarding

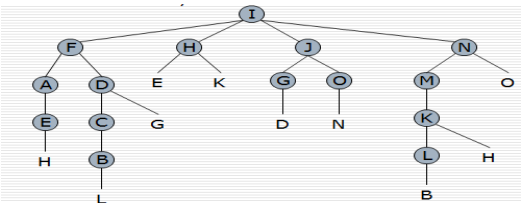


Fig 3.22 The tree build by reverse path forwarding

Multicast Routing

Application that require separate processes (i.e., each from separate location), access and ability to work on the same data. Small group can use point-to-point messaging to accomplish this task. Broadcasting can be used but communicating with 1000 "interested" machines out of million-node network is inefficient. Need a mechanism that would send messages to well-defined groups that are numerically large in size but small compared to the network as a whole. Sending a message to such a group is called *multicasting*. Corresponding routing algorithm is called *multicast routing*. Each Router Computes Spanning tree covering all other routers.

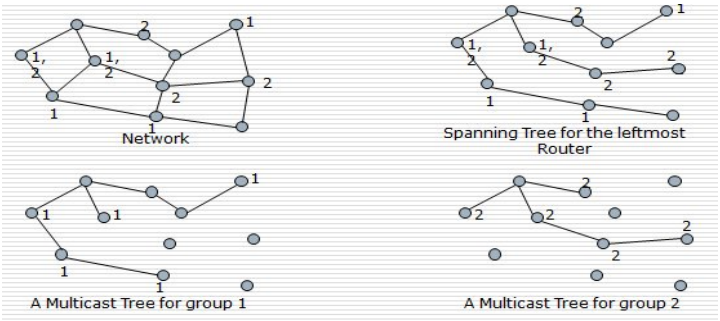


Fig 3.23 Example of a network with nodes belonging to two groups (1 & 2).

3.11 Congestion Control

When one part of the subnet (e.g. one or more routers in an area) becomes overloaded congestion results. Because routers are receiving packets faster than they can forward them, one of two things must happen: The subnet must prevent additional packets from entering the congested region until those already present can be processed. The congested routers can discard queued packets to make room for those that are arriving.

Factors that Cause Congestion

- Packet arrival rate exceeds the outgoing link capacity.
- Insufficient memory to store arriving packets
- Bursty traffic

- Slow processor

Several techniques can be employed. These include:

- Warning bit
- Choke packets
- Load shedding
- Random early discard
- Traffic shaping

The first three deals with congestion detection and recovery. The last two deal with congestion avoidance.

3.11.1 Warning Bit

A special bit in the packet header is set by the router to warn the source when congestion is detected. The bit is copied and piggy-backed on the ACK and sent to the sender. The sender monitors the number of ACK packets it receives with the warning bit set and adjusts its transmission rate accordingly.

3.11.2 Choke Packets

A more direct way of telling the source to slow down. A choke packet is a control packet generated at a congested node and transmitted to restrict traffic flow. The source, on receiving the choke packet must reduce its transmission rate by a certain percentage. An example of a choke packet is the ICMP Source Quench Packet.

3.11.3 Hop-by-Hop Choke Packets

Over long distances or at high speeds choke packets are not very effective. A more efficient method is to send to choke packets hop-by-hop. This requires each hop to reduce its transmission even before the choke packet arrive at the source.

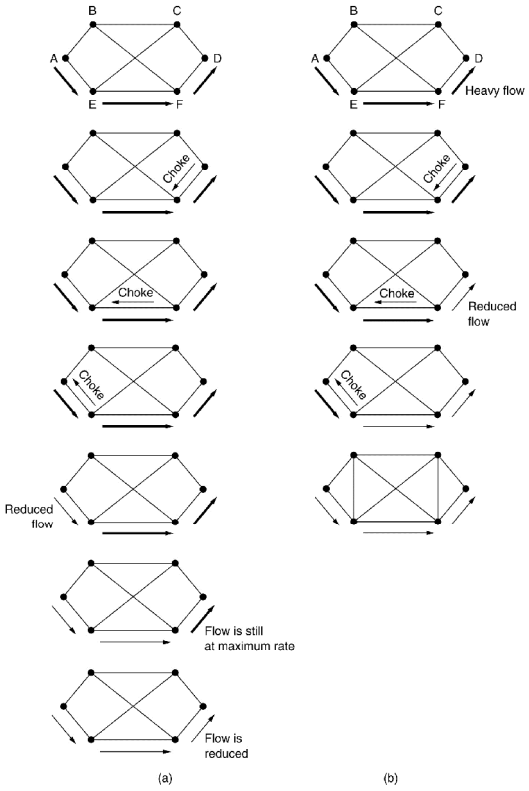


Fig 3.24 a) Choke packet method b) Hop by Hop choke packet method

3.11.4 Load Shedding

When buffers become full, routers simply discard packets. Which packet is chosen to be the victim depends on the application and on the error strategy used in the data link layer. For a file transfer, for, e.g. cannot discard older packets since this will cause a gap in the received data. For real-time voice or video it is probably better to throw away old data and keep new packets. Get the application to mark packets with discard priority.

3.11.5 Random Early Discard (RED)

This is a proactive approach in which the router discards one or more packets before the buffer becomes completely full. Each time a packet arrives, the RED algorithm computes the average queue length, avg. If avg is lower than some lower threshold, congestion is assumed to be minimal or non-existent and the packet is queued.

3.11.6 Traffic Shaping

Another method of congestion control is to “shape” the traffic before it enters the network. Traffic shaping controls the rate at which packets are sent (not just how

many). Used in ATM and Integrated Services networks. At connection set-up time, the sender and carrier negotiate a traffic pattern (shape). Two traffic shaping algorithms are: 1)Leaky Bucket 2)Token Bucket

The Leaky Bucket Algorithm

The Leaky Bucket Algorithm used to control rate in a network. It is implemented as a single-server queue with constant service time. If the bucket (buffer) overflows then packets are discarded. The leaky bucket enforces a constant output rate (average rate) regardless of the burstiness of the input. Does nothing when input is idle. The host injects one packet per clock tick onto the network. This results in a uniform flow of packets, smoothing out bursts and reducing congestion.

When packets are the same size (as in ATM cells), the one packet per tick is okay. For variable length packets though, it is better to allow a fixed number of bytes per tick. E.g. 1024 bytes per tick will allow one 1024-byte packet or two 512-byte packets or four 256-byte packets on 1 tick.

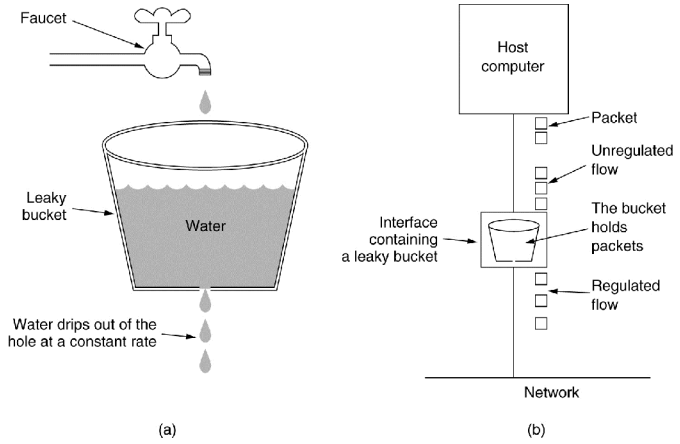


Fig 3.25 a) A leaky bucket with water. (b) a leaky bucket with packets.

Token Bucket Algorithm

In contrast to the LB, the Token Bucket Algorithm, allows the output rate to vary, depending on the size of the burst. In the TB algorithm, the bucket holds tokens. To transmit a packet, the host must capture and destroy one token. Tokens are generated by a clock at the rate of one token every t sec. Idle hosts can capture and save up tokens (up to the max. size of the bucket) in order to send larger bursts later.

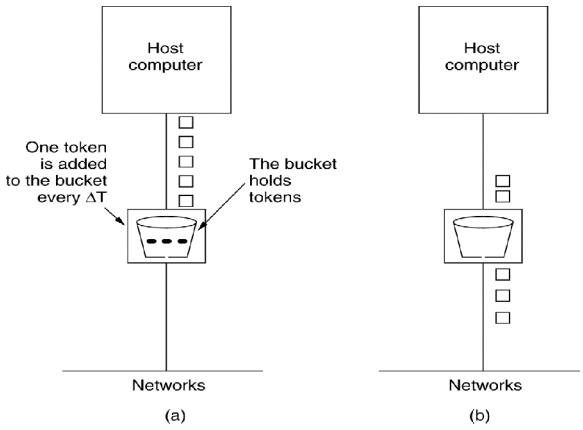


Fig 3.26 token bucket algorithm

3.12 Quality of Service

Quality of service is achieved by

- Requirements
- Techniques for Achieving Good Quality of Service
- Integrated Services
- Differentiated Services
- Label Switching and MPLS

3.13 The Transport layer

3.13.1 Transport Service

- Services provided to the upper layers. The Goal is to Provide efficient, reliable, and cost-effective services to its users (application/session layer processes).
- Transport entity which includes Hardware/software within transport layer to do the w work.
- To provide Connection-oriented E.g., TCP (Transmission Control Protocol) in TCP/IP and Connectionless services E.g., UDP (User Datagram Protocol) in TCP/IP.

3.13.2 Elements of Transport Protocols

- Addressing
- Connect
- Disconnect
- Flow control and buffering
- Multiplexing
- Crash recovery

3.13.3 Performance Issues

The performance issues include

- Performance problems in computer networks
- Network performance measurement
- System design for better performance which includes : Rules of thumb

    1. CPU speed more important than network speed
    2. Reduce packet count to reduce software overhead
    3. Minimize data touching
    4. Minimize context switches
    5. Minimize copying
    6. You can buy more bandwidth but not lower delay
    7. Avoiding congestion is better than recovering from it
    8. Avoid timeouts

- Fast TPDU processing
- Protocols for high-speed networks

Question for practice

Part A

1. Define LAN.
2. What is a peer-to- peer process?
3. What is need of NIC.?
4. Differentiate adaptive and non adaptive routing algorithms.
5. What is need for congestion control?
6. Explain briefly 10 Base-T, 10 Base 2, 10 Base 5.
7. Compare the throughput of pure ALOHA versus slotted ALOHA at low load. Which one is less? Explain your answer.
8. Differentiate between logical and physical addressing.
9. What are the various metrics for routing?
10. Narrate the necessity of routing algorithms.

PART B

1. Explain how congestion can be controlled in virtual circuit subnets and datagram subnets.

2. Explain the multiple access protocols
    a)pure ALOHA
    b)Slotted ALOHA
3. Explain any two routing algorithms with suitable examples.
4. Explain in detail about distance vector and link state routing algorithm

5. Explain in detail about Ethernet and its frame format.
6. Explain in detail about datagram and virtual subnet. Compare the performance of each.
7. Explain leaky bucket and token bucket algorithm
8. Mention the service provided by network layer. Explain in detail about hierarchial and shortest path routing algorithm.