Ethernet standards

Ethernet standard definition

- **Ethernet** is the **standard** network technology that connects computers to each other and to the Internet via cables.
- It is **Defined** as the 802.3 **standard** by the IEEE, the **Ethernet** access method is the global **standard**.

Introduction

- The most common Ethernet standards (such as 10Base5, 10BaseT, 100BaseFX, 802.5-Token ring, 802.11b-Wireless, CSMA CD, etc.
- IEEE shorthand identifiers, such as ***10Base5, 10Base2, 10BaseT, and 10BaseF*** include three pieces of information:
- **The number 10:** At the front of each identifier, 10 denotes the standard data transfer speed over these media - ten megabits per second (10Mbps).
- **The word Base:** Short for Baseband, this part of the identifier signifies a type of network that uses only one carrier frequency for signaling and requires all network stations to share its use.
- **The segment type or segment length:** This part of the identifier can be a digit or a letter:
- **Digit -** shorthand for how long (in meters) a cable segment may be before attenuation sets in. For example, a 10Base5 segment can be no more than 500 meters long.
- **Letter -** identifies a specific physical type of cable. For example, the
- **T** at the end of 10BaseT stands for twisted-pair.

Ethernet standards

10BaseT

- One of the most common types of Ethernet in use today is **10BaseT.** This particular implementation uses four-pair UTP wiring (Cat3 or higher, but most commonly you will see Cat5) using RJ-45 connectors. Each cable is connected from each network device to a central hub in a physical star topology. Within the hub, the signals are repeated and forwarded to all other nodes on the network because it is a logical bus topology. Older network interface cards are configured with jumpers to set addresses and interrupts.
- Today's network interface cards can be managed through a diagnostic program, or automatically configure themselves through plug and play technology. There is a limit of 1024 devices on an Ethernet segment, plus you can have a maximum of 1024 network segments. A UTP cable has a maximum distance of 100 meters, which is equivalent to 328 feet.

Ethernet standards

10BaseF

- **10BaseF** is an implementation of Ethernet 802.3 over fiber optic cabling. 10BaseF offers only 10 Mbps, even though the fiber optic media has the capacity for much faster data rates. One of the implementations of 10BaseF is to connect two hubs as well as connecting hubs to workstations. The best time to use 10BaseF is in the rewiring of a network from copper to fiber optic, when you need an intermediate protocol using the new wiring. 10BaseF is not often a permanent solution because the data rate is so low and the cabling so expensive in comparison to using UTP.

10Base2

- **10Base2,** also called ThinNet, is one of the two Ethernet specifications that use coaxial cable. (One of the best ways to remember that***10Base2*** is ThinNet, and 2 is smaller than 10Base5, which is ThickNet.)

Ethernet standards

10Base5

- ***10Base5*** is nearly identical to **10Base2,** except that it uses a different type of cabling and media connector. 10Base5 is known as ThickNet because it uses the RG-8 coaxial cable.
- It requires an external transceiver to attach to the network interface card on each device. The transceiver is a device that translates the workstation's digital signal to a baseband cabling format.
- ThinNet and UTP network interface cards have built-in transceivers. Only 10Base5 ThickNet network interfaces use external transceivers.
- In the 10Base5 configuration, the NIC attaches to the external transceiver using an **AUI connector**. The transceiver then clamps into the ThickNet cabling, which is why it is usually called a *vampire tap*.
- 10Base5 can also use **BNC connectors**.

Ethernet standards

100BaseFX

- **100BaseFX** is simply ***Fast Ethernet*** over fiber. Originally, the specification was known as *100Base-X over CDDI (Copper Data Digital Interface) or FDDI (Fiber Data Digital Interface).*
- Because the signaling is so vastly different, these two technologies were split into ***100BaseFX*** *and* ***100BaseTX***.
- 100BaseFX runs over **multimode fiber**.
- There are two types of fiber in use. **Multimode fiber optic** cables use LEDs to transmit data and are thick enough that the light signals bounce off the walls of the fiber. The dispersion of the signal limits the length of multimode fiber.
- **Single mode fiber optic** cables use injected lasers to transmit the data along fiber optic cable with an extremely small diameter. Because the laser signal can travel straight without bouncing and dispersing, the signal can travel much farther than multimode.

Ethernet standards

100BaseT4

- **100BaseT4** was the specification created to upgrade 10BaseT networks over Cat3 wiring to 100 Mbps without having to replace the wiring.
- Using four pairs of twisted pair wiring, two of the four pairs are configured for half-duplex transmission (data can move in only one direction at a time). The other two pairs are configured as simplex transmission, which means data moves only in one direction on a pair all the time.

Ethernet standards

100BaseTX

- **100BaseTX,** Fast Ethernet, transmits data at 100 Mbps. Leveraging the existing IEEE 802.3u standard rules, Fast Ethernet works nearly identically to 10BaseT, including that it has a physical star topology using a logical bus.
- 100BaseTX requires Cat5 UTP.

Gigabit Ethernet

- The fastest form of Ethernet is currently Gigabit Ethernet, also known as **1000BaseT** over Cat5 or highergrade cable, using all four pairs of the cable.
- It uses a physical star topology with logical bus.
- There is also **1000BaseF**, which runs over multimode fiber optic cabling. Data transmission is full-duplex, but half-duplex is also supported.

Ethernet standards

Summary characteristics of some Ethernet standards

Designation	Supported Media	Maximum Segment Length	Transfer Speed	Topology
10Base-5	Coaxial	500m	10Mbps	Bus
10Base-2	ThinCoaxial (RG-58 A/U)	185m	10Mbps	Bus
10Base-T	Category3 or above unshielded twisted-pair (UTP)	100m	10Mbps	Star,using either simple repeater hubs or Ethernet switches
1Base-5	Category3 UTP, or above	100m	1Mbps	Star,using simple repeater hubs
10Broad-36	Coaxial(RG-58 A/U CATV type)	3600m	10Mbps	Bus(often only point-to-point)
10Base-FL	Fiber-optic- two strands of multimode 62.5/125 fiber	2000m (full-duplex)	10Mbps	Star(often only point-to-point)

Ethernet standards

802.5 (token ring)

- The IEEE 802.5 Token Ring standards define services for the OSI physical layer and the MAC sublayer of the data link layer.
- Token Ring computers are situated on a continuous network loop.
- A Token Ring controls access to the network by passing a token, from one computer to the next. Before they can transmit data they must wait for a free token, thus token passing does not allow two or more computers to begin transmitting at the same time.

Ethernet standards

802.11b (wireless)

- 802.11b is a wireless Ethernet technology operating at 11MB.
- 802.11b devices use Direct Sequence Spread Spectrum (DSSS) radio technology operating in the 2.4GHz frequency band.
- An 802.11b wireless network consists of wireless NICs and access points. Access points act as wireless hubs to link multiple wireless NICs into a single subnet. Access points also have at least one fixed Ethernet port to allow the wireless network to be bridged to a traditional wired Ethernet network. Wireless and wired devices can coexist on the same network. 802.11b devices can communicate across a maximum range of 50-300 feet from each other.

Ethernet standards

FDDI networking technologies

- Fiber Distributed Data Interface, shares many of the same features as token ring, such as a token passing, and the continuous network loop configuration. But FDDI has better fault tolerance because of its use of a dual, counter-rotating ring that enables the ring to reconfigure itself in case of a link failure.
- FDDI also has higher transfer speeds, 100 Mbps for FDDI, compared to 4 - 16 Mbps for Token Ring.
- Unlike Token Ring, which uses a star topology, FDDI uses a physical ring. Each device in the ring attaches to the adjacent device using a two stranded fiber optic cable. Data travels in one direction on the outer strand and in the other direction on the inner strand. When all devices attached to the dual ring are functioning properly, data travels on only one ring. FDDI transmits data on the second ring only in the event of a link failure.

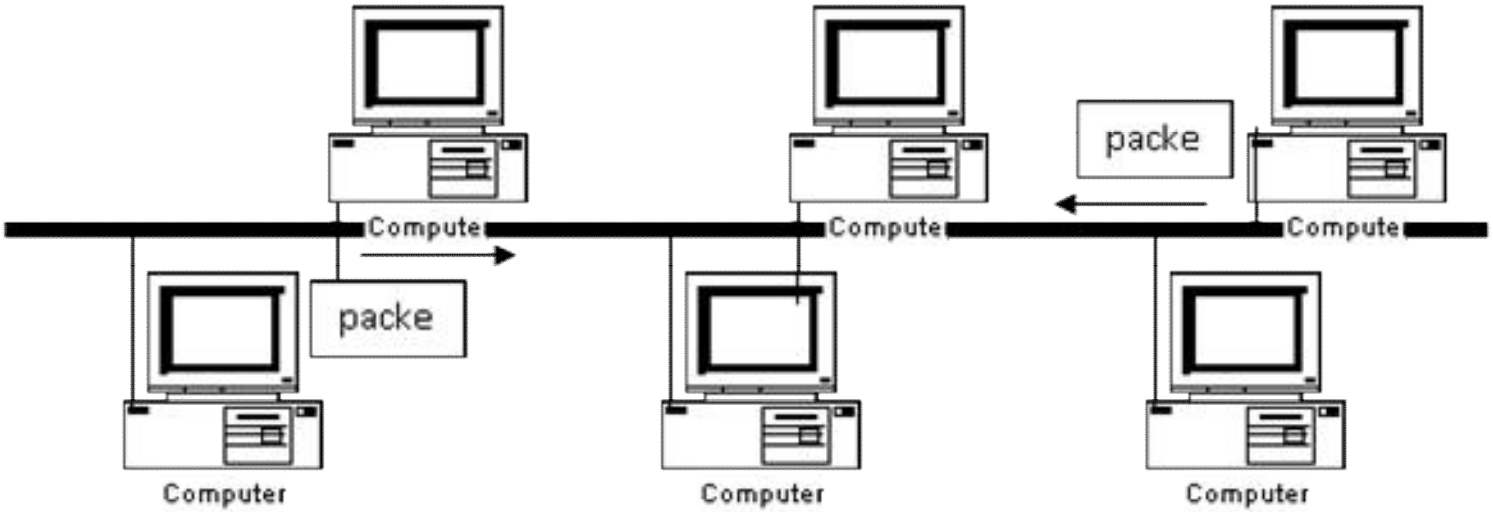
Media Access control methods

Gaining Access to the Media

- Media access methods are independent of the physical and logical topologies. You will find that there are usually just a few combinations that seem to work well, however.
- Media access methods are simply the rules that govern how a device can submit data to the network. Each access method will have a different effect on network traffic.

1. Contention based network

- In contention based network, computers sent data whenever they had data to send. This might work well in a small environment when little data is being sent along the cable. But as more computers send data, the messages collide more frequently, must be resend, and then collide again. Soon there will be a communication breakdown.



Collision in Contention Method

1. Contention as a Method of Media Access

- Contention, often called random access, is the media access method that acts as an open door to anyone who wants to walk in.
- Two types of contention methods exist for media access; they are similar, but a single difference between them changes how efficiently they operate. They are:
- CSMA/CD (Carrier Sense Multiple Access / Collision Detection)
- CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)

Contention cont...d

- To organize contention based network, two carrier access method were created:
- **Carrier Sense multiple Access with Collision detection (CSMA/CD):** is one of the most popular ways to regulate network traffic. Used by Ethernet, this access method prevents collision *by listening to the channel to see if another computer is sending data. If the computer does not sense data on the line, it sends its message. If another computer is using the channel, the computer waits a random amount of time and then checks again*. *This process is continued until the channel is free and the computer can send the data.*

Advantages:

- Inexpensive to implement.
- Fast in a small network with low traffic.

Disadvantages:

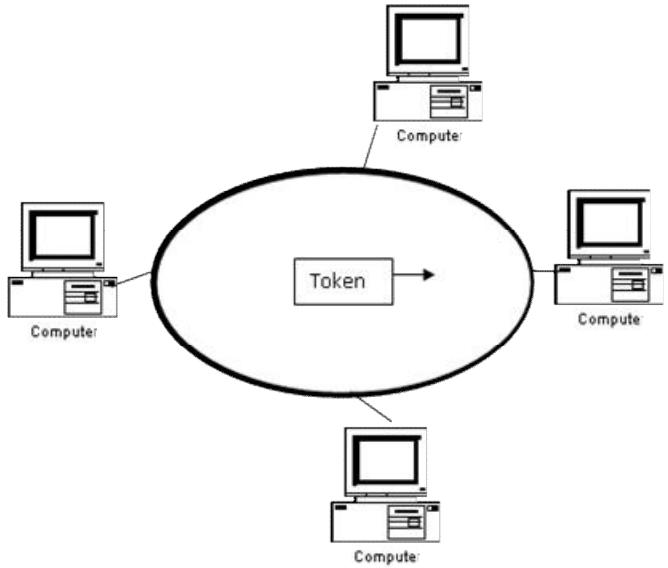
- Slow in a large network with high traffic.
- Does not support priority. A single computer can block all other computer if it has very long message to send.

Contention cont...d

- **Carrier sense multiple access with collision avoidance (CSMA/CA):** It uses collision avoidance, rather than detection, to prevent collision. With CSMA/CA, *once the computer senses that no other computer is using the network, it signals its intent to transmit data. Any other computer with data to send wait when they receive the "intent-to-transmit" signal and send their intent-to-transmit signals when they see that channel is free*. Although this method is more reliable than CSMA/CD in avoiding collision, the additional overhead created by the "intent-to-transmit" packets significantly reduces the speed of any network using this method.

2. Token Passing

- Using this channel access method, a special packet called the “token” is passed from one computer to the next sequentially.
- Only the computer holding token can send data. A computer can keep token only a specific amount of time.
- If the computer with the token has no data to send, it passes the token to the next computer.



Token Passing cont...d

Advantages:

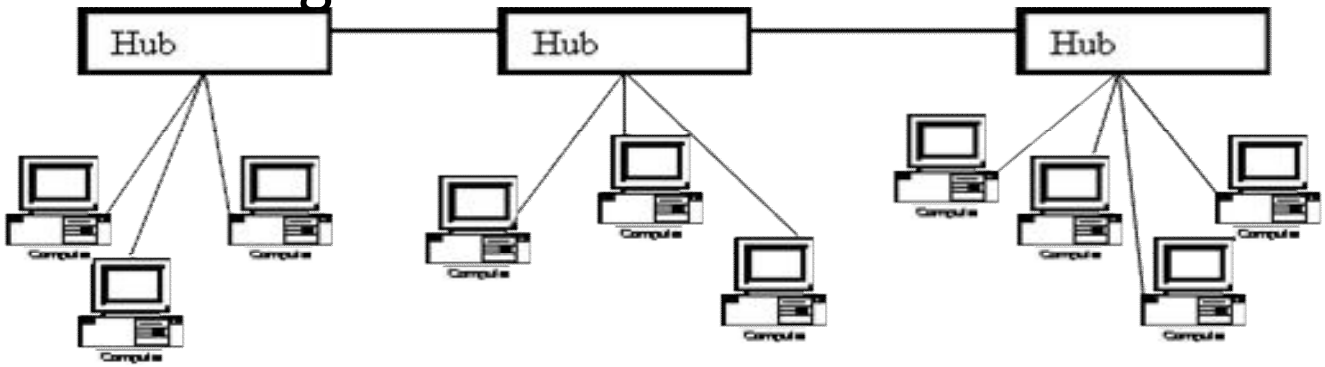
- Because only the computer with the token can transfer data, collisions are avoided with this method.
- All the computers have equal access to the channel. Because of this equality, token passing network is best suited for time-sensitive environment. For example banking transaction and database queries.

Token Passing cont...d

- **Disadvantages:**
- Even if only one computer on the network has data to send, it must wait until it receives the token. If its data is large enough it will wait more than one turns of token to finish the transmission, means further delay.
- The process of creating and passing the token is complicated and requires more expensive equipment than contention based network.

3. Demand Priority

- Demand priority is a recent channel access method and relies on following method.



- Intelligent hubs are used to control access to the network. The hub searches all connections in a round robin fashion *(**Round-robin** (RR) is one of the algorithms employed by process and network schedulers in computing. As the term is generally used, **time slices are assigned to each process in equal portions and in circular order, handling all processes without priority** (also known as cyclic executive))*.
- When an end node (computer) has data to send, it transmits a “demand signal” to the hub. The hub then sends and acknowledgement that the node can start transmitting its data.

Demand Priority cont...d

- Unlike other channel access methods, demand priority allows for certain computers to be assigned a higher priority than other.
- If multiple computers make simultaneous demands, the computer with highest priority is allowed to transmit first.
- Demand priority makes the most efficient use of the available network media. Rather than wasting time addressing computers that do not have data to send, hubs using demand priority channel access respond only when computers signal the hub for service.
- Also packets are not broadcast in demand priority network as they are in CSMA/CD and CSMA/CA network but, instead, are sent from the computer to the hub and from the hub directly to the destination. This eliminates traffic on the network.

Demand Priority cont...d

Advantages:

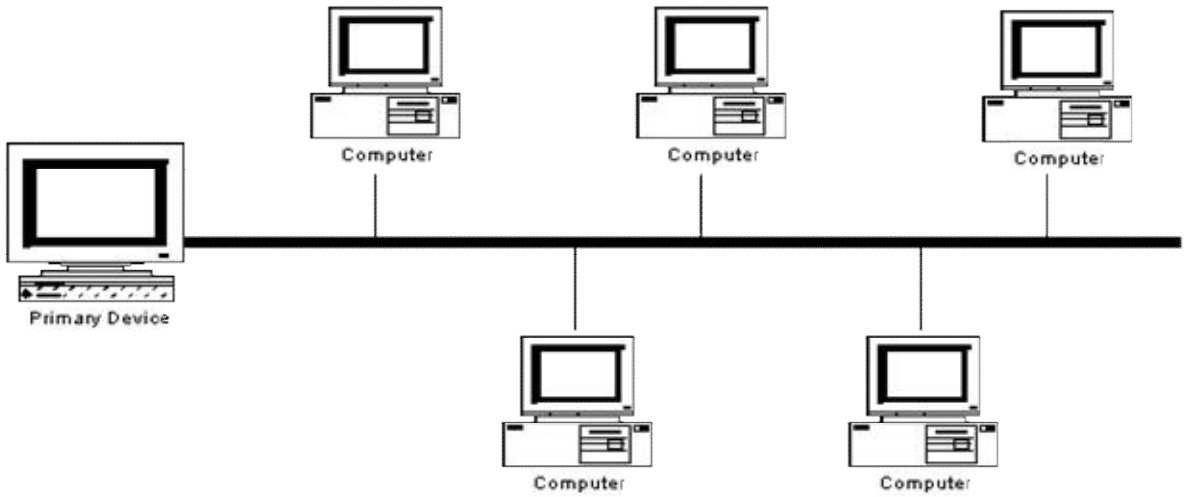
- Very fast in high and low traffic environments
- No collision
- Provide priority

Disadvantages:

- Expensive because special equipment is required.
- Lower priority may starve for service.

4. Polling

- Polling is one of the oldest ways of controlling access to the network.
- A central controller, often referred to as the “primary device”, ask each computer (the secondary device) on the network if it has data to send. If so, the computer is allowed to send data, up to a certain amount of time; then it is the next computer’s turn.



Polling cont...d

Advantages:

- Like token passing, it allows all computers equal access to the channel, and no single computer can monopolize the media.
- The central controller allows for centralized management, and certain computers can receive priority over other computers; they can be polled more often or be allowed to send data for longer period of time than the remaining computers.

Disadvantages:

- Does not make efficient use of the media.
- If the primary device fails, the whole network fails.
- Increased expenses because of the primary device.

Switching Techniques

- The main objective of networking is to connect all the devices so that resources and information can be shared efficiently.
- Whenever we have multiple devices, we have problem of connect them to make one-to-one connection possible.
- One solution is to install a point to point link between each pair of devices such as in mesh topology or between a central device and every other device as in star topology.
- These methods, however, are impractical and wasteful when applied to very large network.
- The number and length of the links require too many infrastructures to be cost efficient; and majority of those links would be idle most of the time.

Switching Techniques cont...d

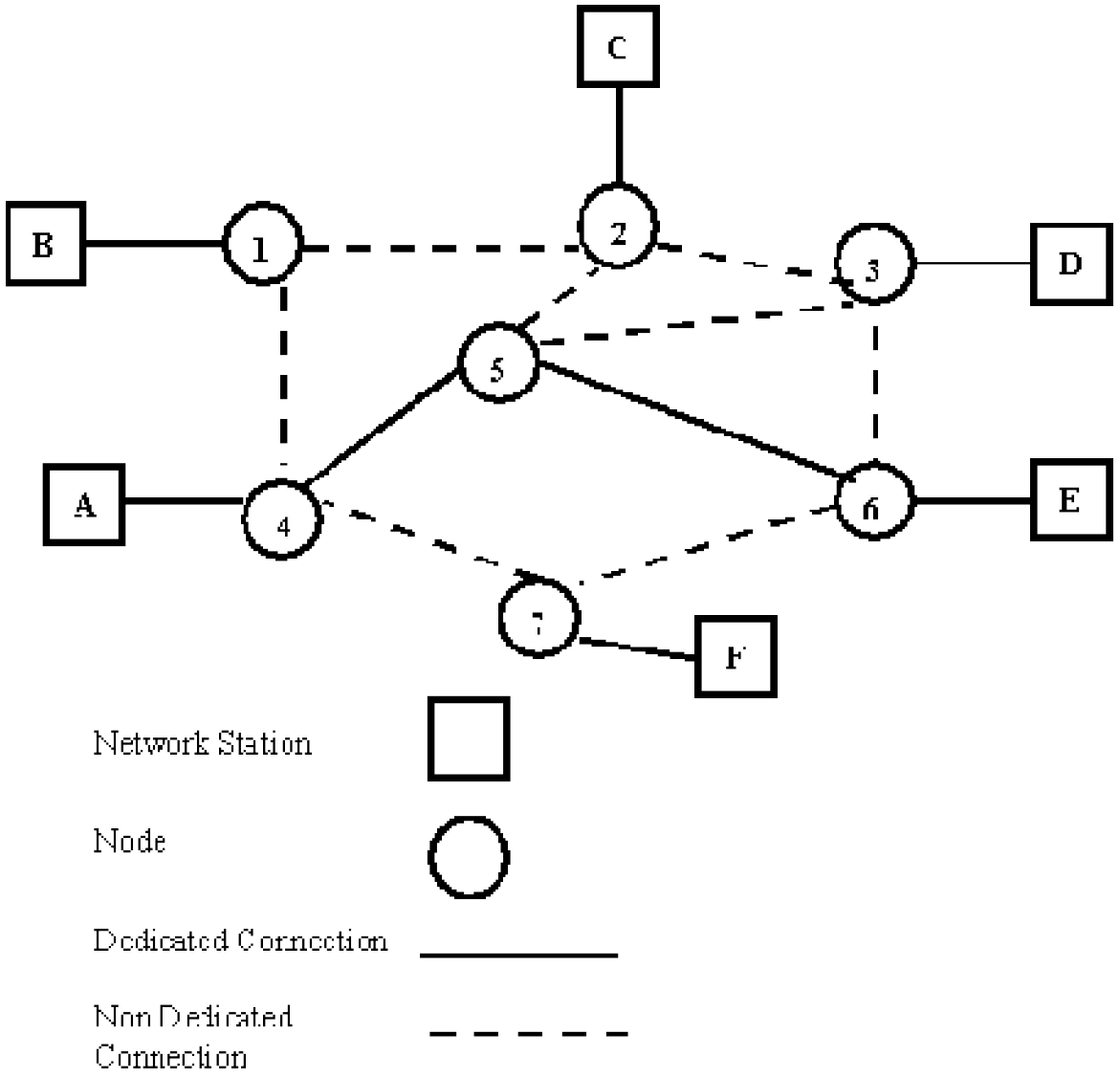
- A better solution is to use switching.
- A switch network consists of a series of inter-linked node, called ***switches***.
- Switched are hardware and/or software capable of creating temporary connection between two or more devices linked to switch but not to each other.
- Traditionally, three methods of switching have been important:

    1. Circuit switching
    2. Packet switching and
    3. Message switching

1. Circuit Switching

- Communication via circuit switching implies that there is a *dedicated communication path between two stations*. The path is a connected sequence of links between network nodes. On each physical link, a channel is dedicated to the connection. A common example of circuit switching is the *telephone network.*
- Communication via circuit switching involves three phases:
    i. Circuit Establishment
    ii. Information Transfer
    iii. Circuit Disconnection

Circuit Switching cont...d



Circuit Switching Network

i. Circuit Establishment

- Before any signals can be transmitted, an end-to-end (station to station) circuit must be established.
- For example, station A wants to communicate with station E. station A sends a request to node 4 requesting a connection to station E. typically, the link from A to 4 is a dedicated line, so that part of connection already exists.
- On the basis of routing information and measures availability and perhaps cost, lets assume that node 4,5, and 6 are used to complete the connection.
- In completing the connection, a test is made to determine if station E is busy or is prepared to accept the connection.

ii. Information Transfer

- Information now can transmit from A through the network to E the transmission may be analog voice, or binary data. Generally the connection is full duplex, and signals may be transmitted in both direction simultaneously.

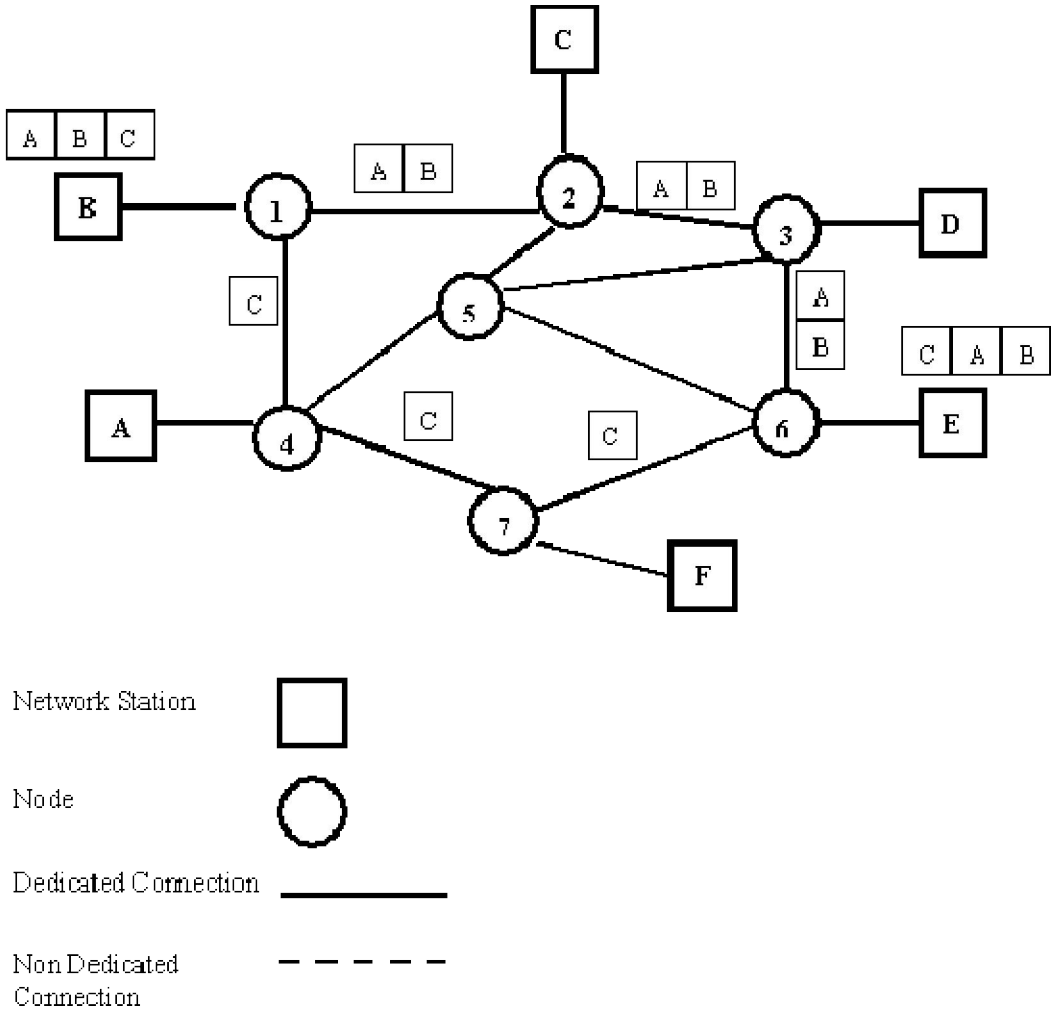
iii. Circuit Disconnection

- One the transmission is completed, the connection is terminated, usually by the action of one of the two station. Signals must be propagated to the nodes 4,5, and 6 to deallocate the dedicated resources.
- Circuit switching can be rather inefficient. Channel capacity is dedicated for the duration of a connection, even if no data are being transferred. The connection provides for transmission at a constant data rate. Thus, each of the devices that are connected must transmit and receive at the same data rate as the other.

2. Packet Switching

- In a packet switching data are transmitted in short packets. A typical packet length is 1000 byte.
- If a source has longer message to send, the message is broken up into a series of packets.
- Each packet contains a portion (or the entire short message) of the user's data plus some control information.
- These packets are routed to the destination via different available nodes.

Packet Switching cont...d



Packet Switching Networks

Packet Switching cont...d

- Above figure illustrate the basic operation.
- A transmitting computer or other device sends a message as a sequence of packets. Each packet includes control information including the destination station.
- The packets are initially sent to the node to which the sending station attaches. As each packet arrives at these nodes, the node stores the packet briefly, and determines the next available link. When the link is available, the packet is transmitted to the next node. The entire packet eventually delivered to the intended node.
- There are two popular approaches to packet switching:
  a. Datagram and
  b. Virtual circuit.

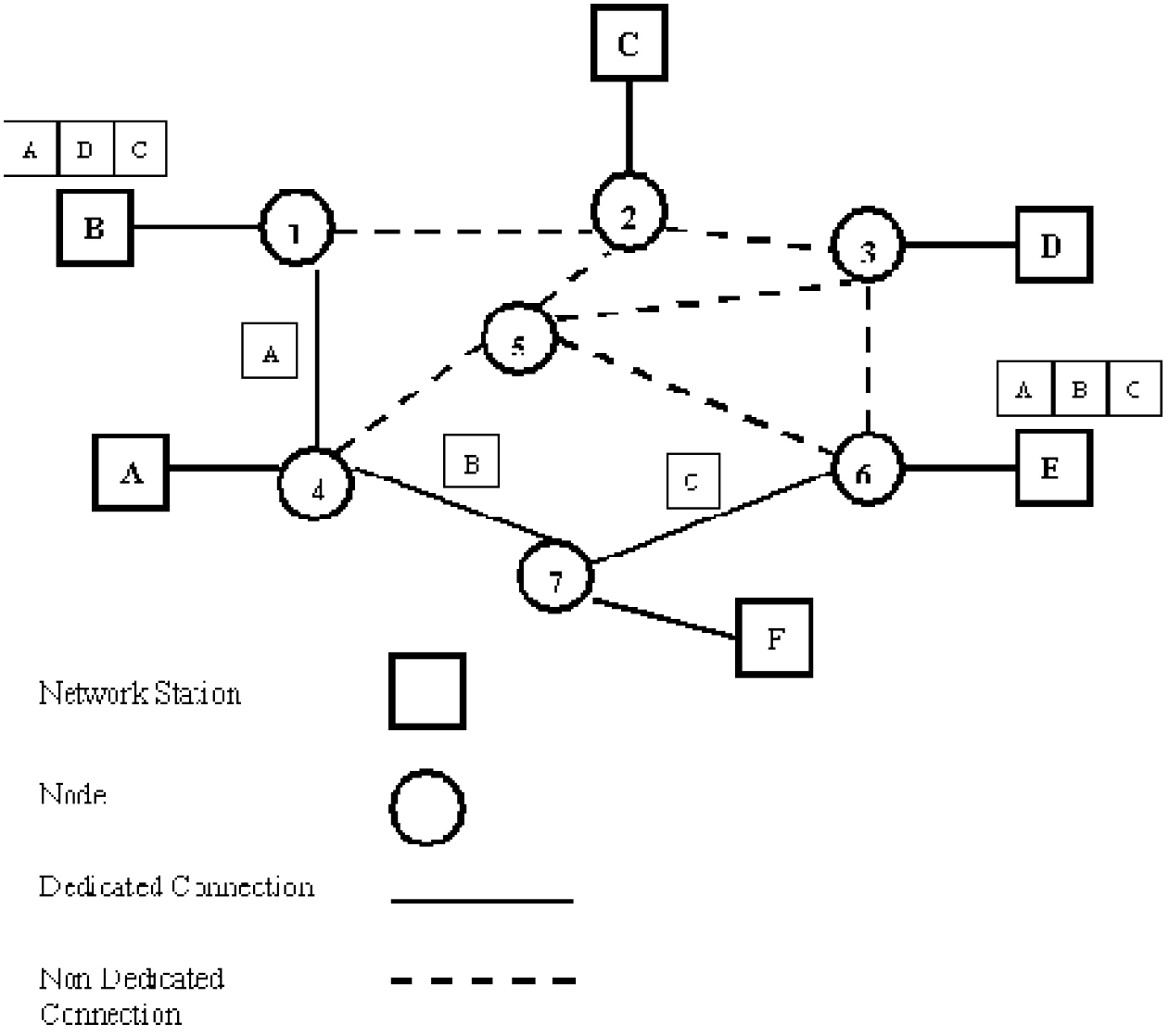
a. Datagram Approach

- In the datagram approach to packet switching, each packet is treated independently from all others and each packet can be sent via any available path, with no reference to packet that have gone before.
- In the datagram approach, packets with the same destination address do not all follow the same route, and they may arrive out of sequence at the exit point.

b. Virtual Circuit

- In this approach, a preplanned route is established before any packets are sent.
- Once the route is established, all the packets between a pair of communicating parties follow this same route through the network.
- Each packet now contains a virtual circuit identifier as well as the data.
- Each node on the pre-established route knows where to direct such packet.
- No routing decisions are required.
- At any time, each station can have more than one virtual circuit to any other station and can have virtual circuits to more than one station.

Virtual Circuit cont...d



Virtual Switching Network

3. Message Switching

- The descriptive term store and forward best know message switching.
- In this mechanism, a node (usually a special computer with number of disks) receives a message, stores it until the appropriate route is free, then send it along.
- Note that in message switching the messages are stored and relayed from the secondary storage (disk), while in packet switching the packets are stored and forward from primary storage (RAM).

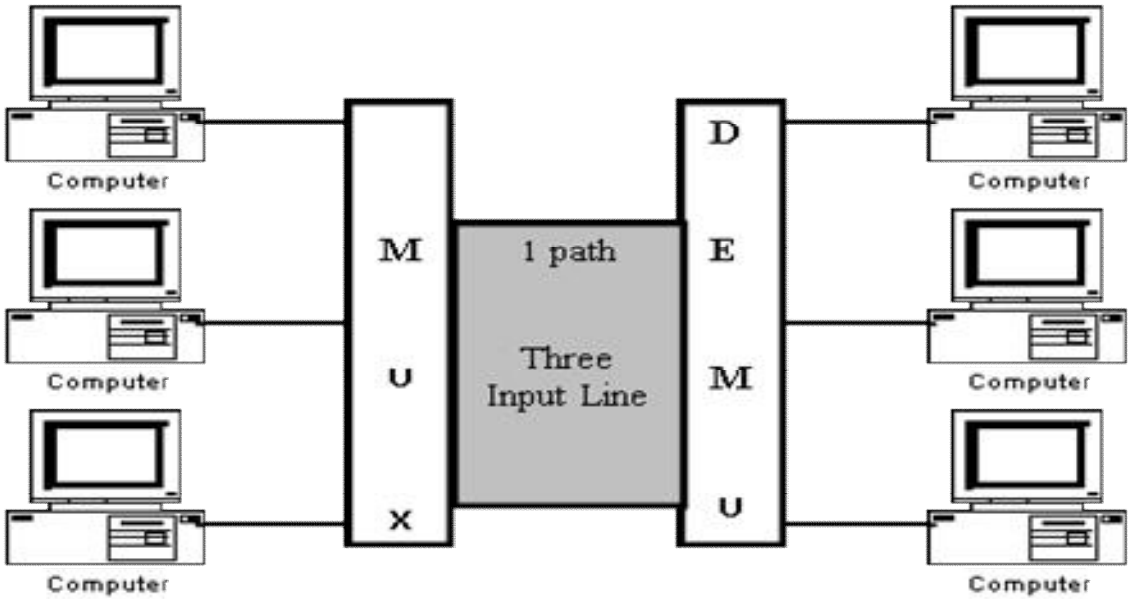
3. Message Switching

- The primary uses of message switching have been to provide high-level network service (e.g. delayed delivery, broadcast) for unintelligent devices.
- Since such devices have been replaced, message switching has virtually disappeared.
- Also delays inherent in the process, as well as the requirement for large capacity storage media at each node, make it unpopular for direct communication.

Multiplexing

- **Multiplexing** is the process of combining separate signal channels into one composite stream. *It is carried out to increase the utilization of transmission channel*.
- In a multiplexed system, *n devices* stare the capacity of one link.
- In the following figure, three devices on the left direct their transmission stream to a multiplexer (MUX) which combines them into a single stream (many to one).
- At the receiving end, the stream is fed into a demultiplexer (DEMX), which separates the stream back into its component transmissions (one to many) and directs them to their receiving devices

Multiplexing cont...d

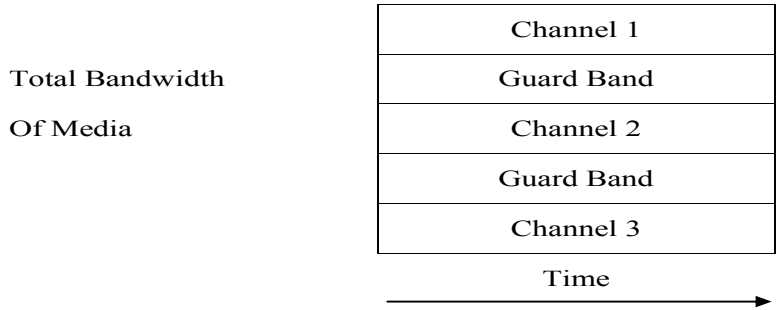


There are two major methods of multiplexing:

a) Frequency Division Multiplexing (FDM) and
b) Time Division Multiplexing (TDM). TDM is further subdivided into:
   i. synchronous-TDM and
   ii. Asynchronous TDM. Asynchronous TDM also called statistical TDM.

a) Frequency Division Multiplexing (FDM)

- FDM is an analog technique that works by *dividing slicing the total bandwidth of a media into a number of narrow bandwidth units known as channels*.

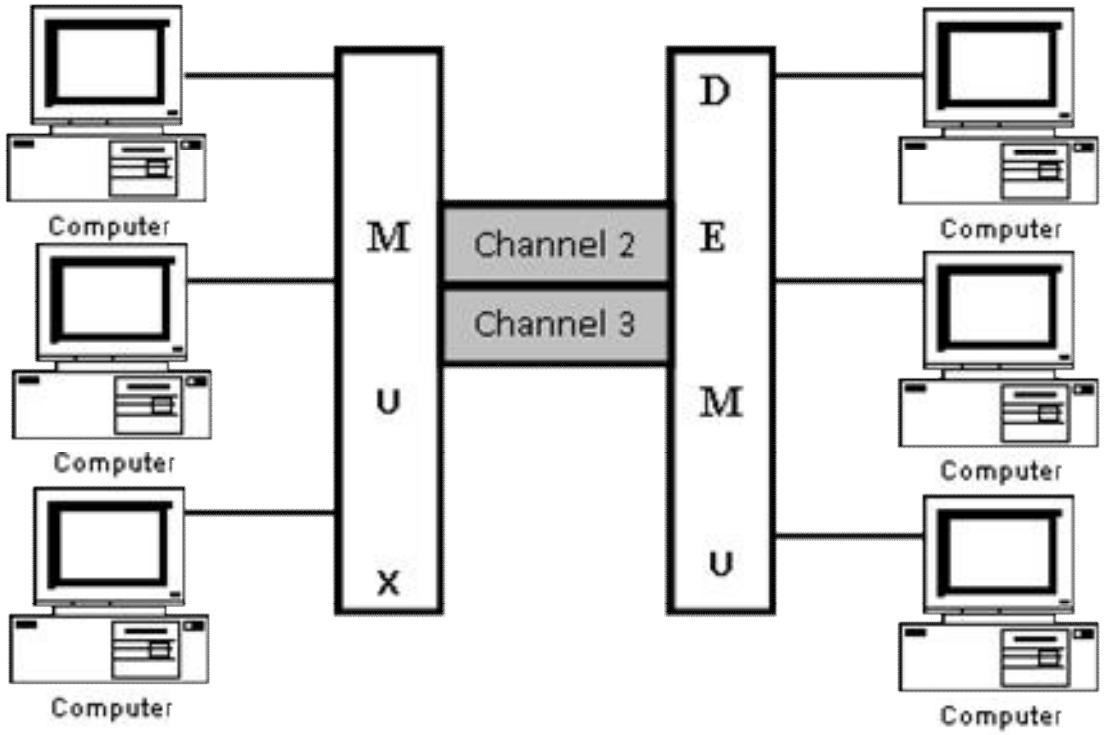


Frequency Division of Media Bandwidth

- These *channels are separated by further narrower slices, known as **guard bands**, to prevent inter-channel interface*.
- This actual waste of bandwidth is offset by the lower costs of the filter (frequency selection device). The closer the channels are together (the narrower the guard bands) the more critical and expensive the channel filter become.

a) Frequency Division Multiplexing (FDM)

- Bellow figure gives a conceptual view of FDM. In this illustration, the transmission path is divided into three parts (based on different frequencies), each representing a channel to carry one transmission.



Frequency Division Multiplexing

a) Frequency Division Multiplexing (FDM)

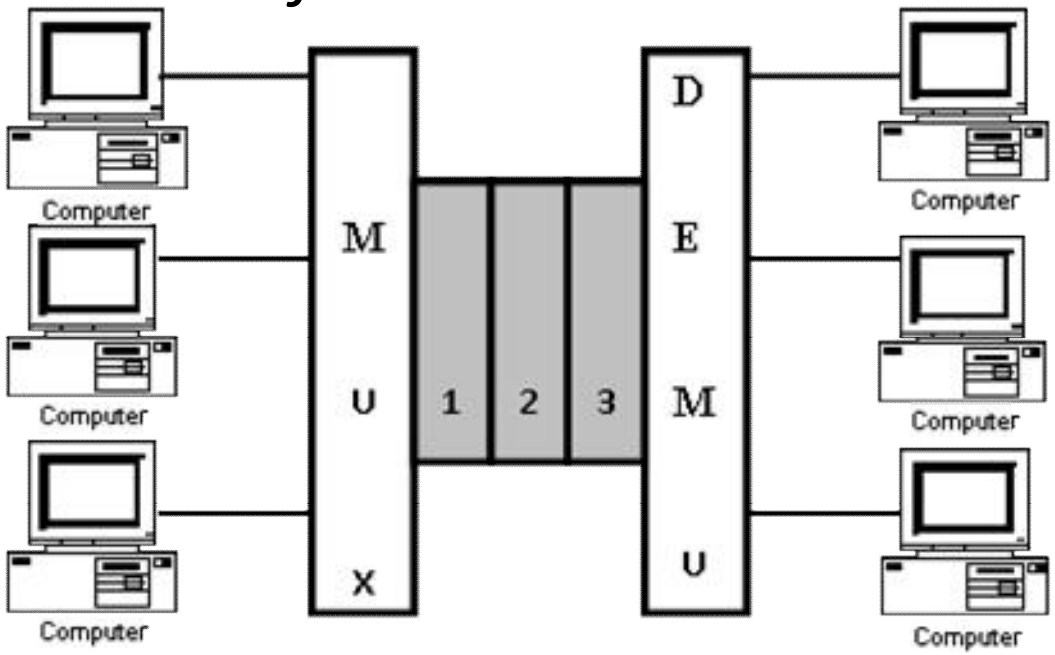
- As an analogy, imagine a point where three separate narrow roads merge to form a three-lane highway. Each of the three roads corresponds to a lane of the highway. Each car merging into the highway from one of the road still has its own lane and can travel without interfering with cars in other lane.

Example: Cable Television

- A familiar application of FDM is cable television. The coaxial cable used in a cable television system has a bandwidth of approximately 500 MHz.
- An individual television channel requires about 6 MHz of bandwidth for transmission. The coaxial cable, therefore, can carry many multiplexed channels (theoretically 83 channels, but actually fewer to allow for guard band). A demultiplexer at your television allows you to select which of those channels you wish to receive.

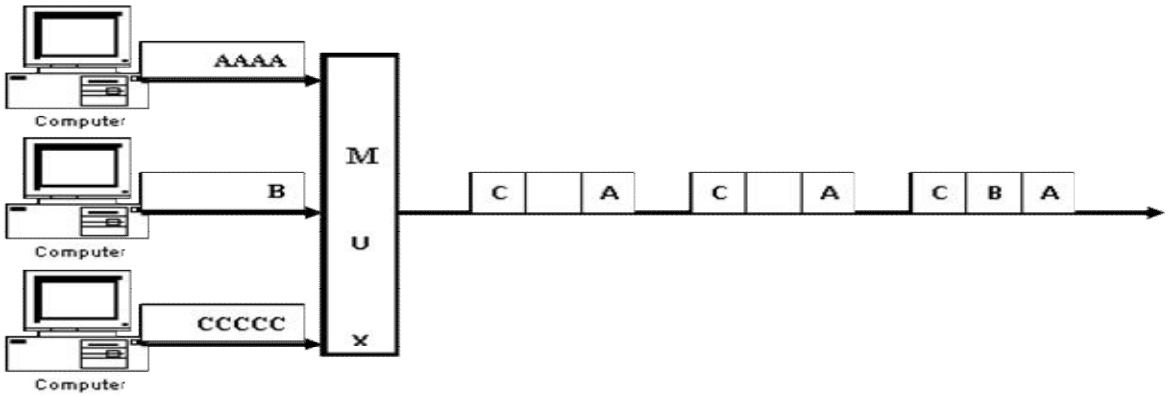
b) Time Division Multiplexing (TDM)

- *TDM is a digital process that can be applied when the data rate capacity of the transmission medium is greater than the data rate required by the sending and receiving devices. Each channel is allocated a pre-defined amount of time to transmit information over the whole of the media.*



- TDM can be implemented in two ways: **synchronous TDM and asynchronous TDM.**

i) synchronous TDM

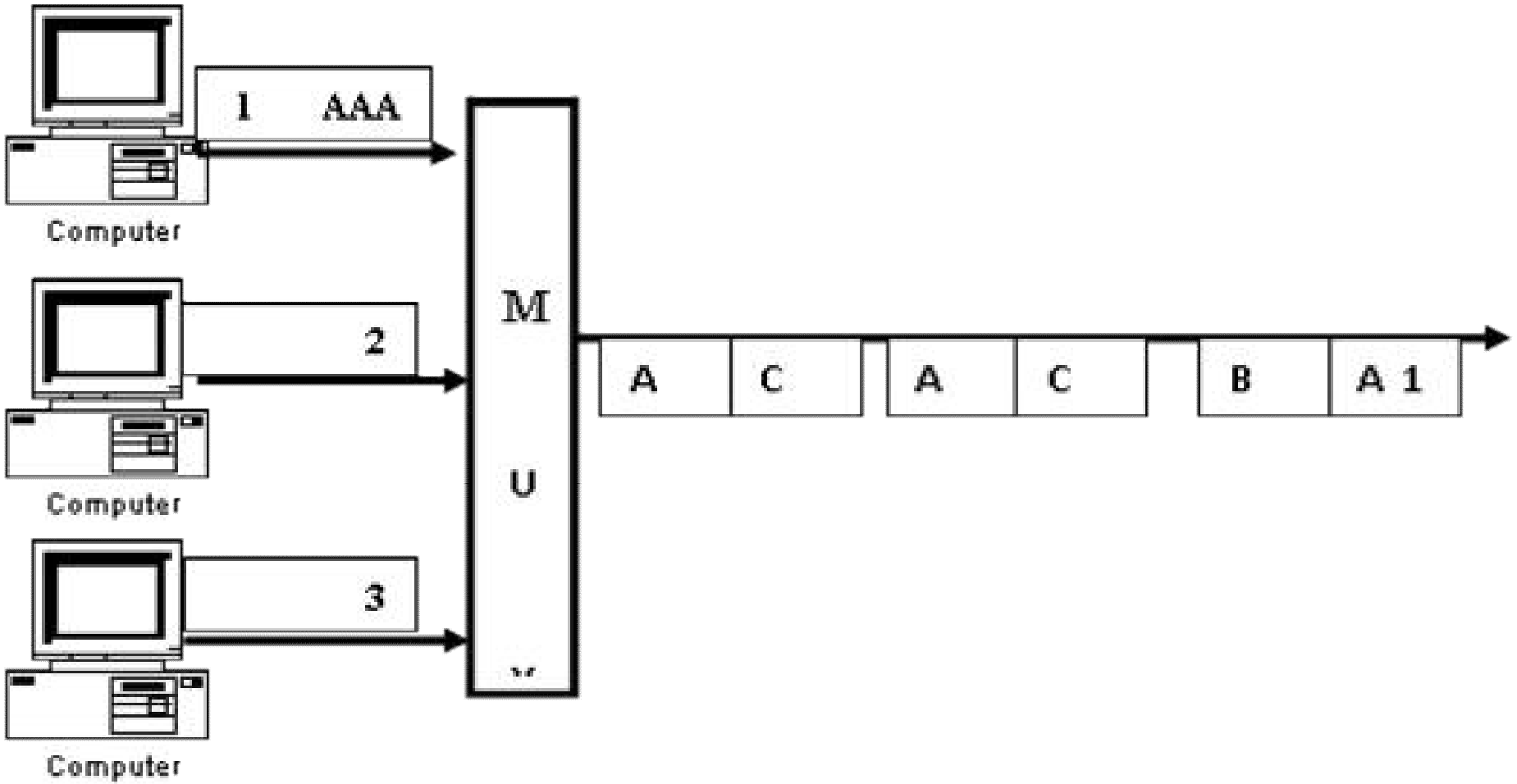


- In this method, *multiplexer allocates the same time slot to each device at all time, whether or not a device has anything to transmit.* IF there are *n* input line than there must be *n* time slots in the frame (time slots are grouped into frames). Time slot (lets say T), for example, is assigned to device (lets say D) alone and can not be used by any other device. Each time its allocated time slot comes in (in a round robin fashion), Device D has the opportunity to send a portion of its data for time slot T. If the device D is unable to transmit or does not have data to send, its time slot remains empty and no other device can use it, in other words it is wasted.

ii. Asynchronous TDM

- Asynchronous TDM provide better utilization of media. Like synchronous TDM, *asynchronous TDM allows a number of lower speed input lines to be multiplexed to a single higher speed line*. Unlike synchronous TDM, however, in asynchronous TDM the total speed of input line can be greater than the capacity of the media. *In asynchronous TDM the number of slots in the frame are less than numbers of input lines. Slots are not preassigned, each slot is available to any of the attached input lines that has data to send. The multiplexer scans the input line, accepts the portion of data until a frame is filed, and then sends the frame across the link.*
- Since the slots are not preassigned for each input line, line address must be added along with the data to send.

Asynchronous TDM cont...d



Asynchronous TDM