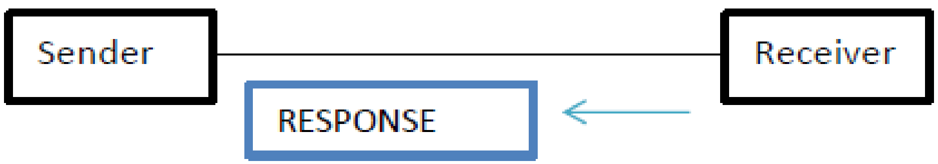
Module 2-Part2
The Data Link Layer
HDLC, MAC,
IEEE 802 Stds

Three types of stations

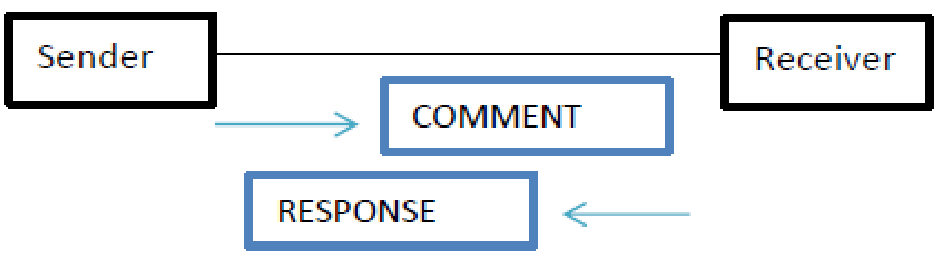
NODES in HDLC

1.Primary station: if particular node send COMMENT message

2.Secondary Station: if receiver sends RESPONSE message back



3.Combined Station: if it sends both COMMENT & RESPONSE



HDLC(high level data link control)

- bit oriented protocol for communication over point to point and multipoint links
  - All use bit stuffing for data transparency

  - All the bit-oriented protocols use the frame structure shown

Bits	8	8	8	≥ 0	16	8
	0 1 1 1 1 1 1 0	Address	Control	Data	Checksum	0 1 1 1 1 1 1 0

Frame format for bit-oriented protocols.

  - Control field is used for sequence numbers, acknowledgements, and other purposes
  - Data field may contain any information.
    - It may be arbitrarily long
  - Checksum field is a cyclic redundancy code (CRC)
  - Frame is delimited with another flag sequence (01111110)

HDLC

- On idle point-to-point lines, flag sequences are transmitted continuously
- minimum frame contains three fields and totals 32 bits, excluding the flags on either end
- Three kinds of frames:
  a) Information frame(**I frame**)-used to transport user data
  b) Supervisory frame **(S frame) -** used to transport control information
  c) Unnumbered frame(**U frame)-**is reserved for system management and information carried for managing the link.

Contents of the Control field for these three kinds are shown

Bits	1	3		1	3
(a)	0	Seq		P/F	Next
(b)	1	0	Type	P/F	Next
(c)	1	1	Type	P/F	Modifier

HDLC

- Protocol uses a sliding window, with a 3-bit sequence number.
- Up to seven unacknowledged frames may be outstanding at any instant.
- The Seq. field in Fig. (a) is the frame sequence number.
- The Next field is a piggybacked acknowledgement.
- The choice of using the last frame received or the next frame expected is arbitrary (subjective)
- P/F bit stands for Poll / Final
  - It is used when a computer is polling a group of terminals.
  - When used as P, the computer is inviting the terminal to send data.
  - All the frames sent by the terminal, except the final one, have the P/F bit set to P.
  - The final one is set to F.
  - P/F bit is used to force the other machine to send a Supervisory frame immediately rather than waiting for reverse traffic onto which to piggyback the window information.
  - Piggybacking-technique of temporarily delaying outgoing acknowledgements so that they can be hooked onto the next outgoing data frame

HDLC

- Various kinds of Supervisory frames are distinguished by the Type field.

  Type 0 (RECEIVE READY)

  - an acknowledgement frame used to indicate the next frame expected
  - This frame is used when there is no reverse traffic to use for piggybacking

  Type 1 (REJECT).

  - a negative acknowledgement frame used to indicate that a transmission error has been detected.
  - The Next field indicates the first frame in sequence not received correctly
  - The sender is required to retransmit all outstanding frames starting at Next.
  - This strategy is similar to Go back n

HDLC

- Type 2 (RECEIVE NOT READY)
  - . It acknowledges all frames up to without including Next
  - it tells the sender to stop sending.
  - intended to signal certain temporary problems with the receiver, such as a shortage of buffers

- Type 3 SELECTIVE REJECT.
- It calls for retransmission of only the frame specified.
- Similar to selective repeat protocol

HDLC

- Unnumbered frame
  - sometimes used for control purposes
  - but can also carry data when unreliable connectionless service is called for

Medium Access Control Sub Layer

- deals with broadcast networks and their protocols.
- In any broadcast network, the key issue is how to determine who gets to use the channel when there is competition for it.
- broadcast channels are sometimes referred to as **multiaccess channels or random access channels**
- protocols used to determine who goes next on a multiaccess channel belong to a sublayer of the data link layer called the **MAC (Medium Access Control) sublayer**
- MAC sublayer is especially important in LANs
- central theme:
  - how to allocate a single broadcast channel among competing users

Medium Access Control Sub Layer

- Two schemes:
  - static and dynamic schemes
- **Static Channel Allocation in LANs and MANs**
  - Frequency Division Multiplexing (FDM)
  - Time Division Multiplexing (FDM)

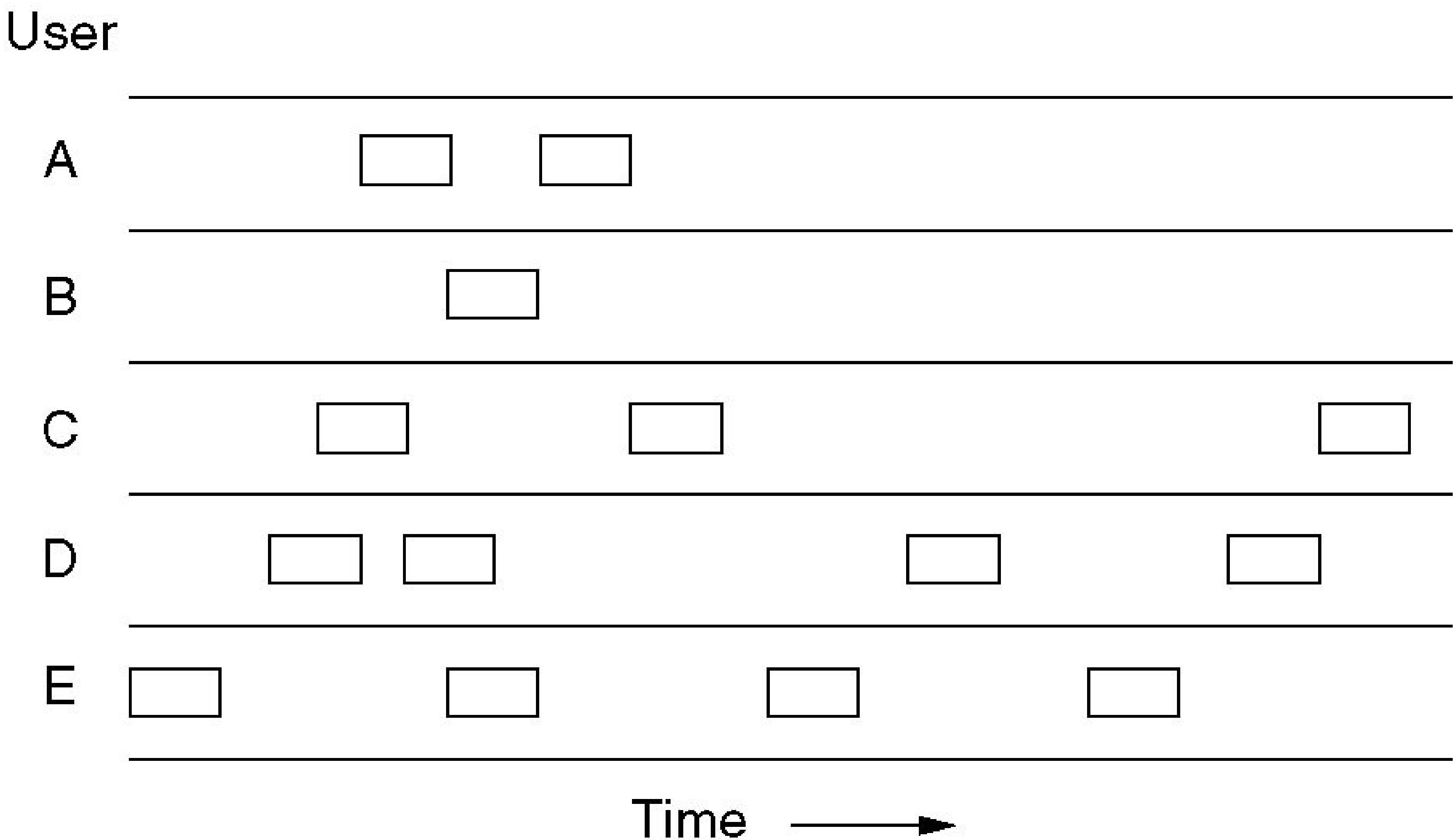
ALOHA

- **Dynamic Channel Allocation in LANs and MANs**
  - **Multiple Access Protocols**
  - Many algorithms for allocating a multiple access channel
    - **ALOHA**
      - basic idea is applicable to any system in which uncoordinated users are competing for the use of a single shared channel
      - used ground-based radio broadcasting
      - two versions of ALOHA : pure and slotted.
        - They differ with respect to whether time is divided into discrete slots into which all frames must fit.
        - Pure ALOHA does not require global time synchronization;
        - slotted ALOHA does.

Pure ALOHA

- ***Pure ALOHA***
  - basic idea of an ALOHA system is simple
  - let users transmit whenever they have data to be sent.
  - There will be collisions and the colliding frames will be damaged.
  - If the frame was destroyed, the sender just waits a random amount of time and sends it again.
  - The waiting time must be random or the same frames will collide over and over

Pure ALOHA

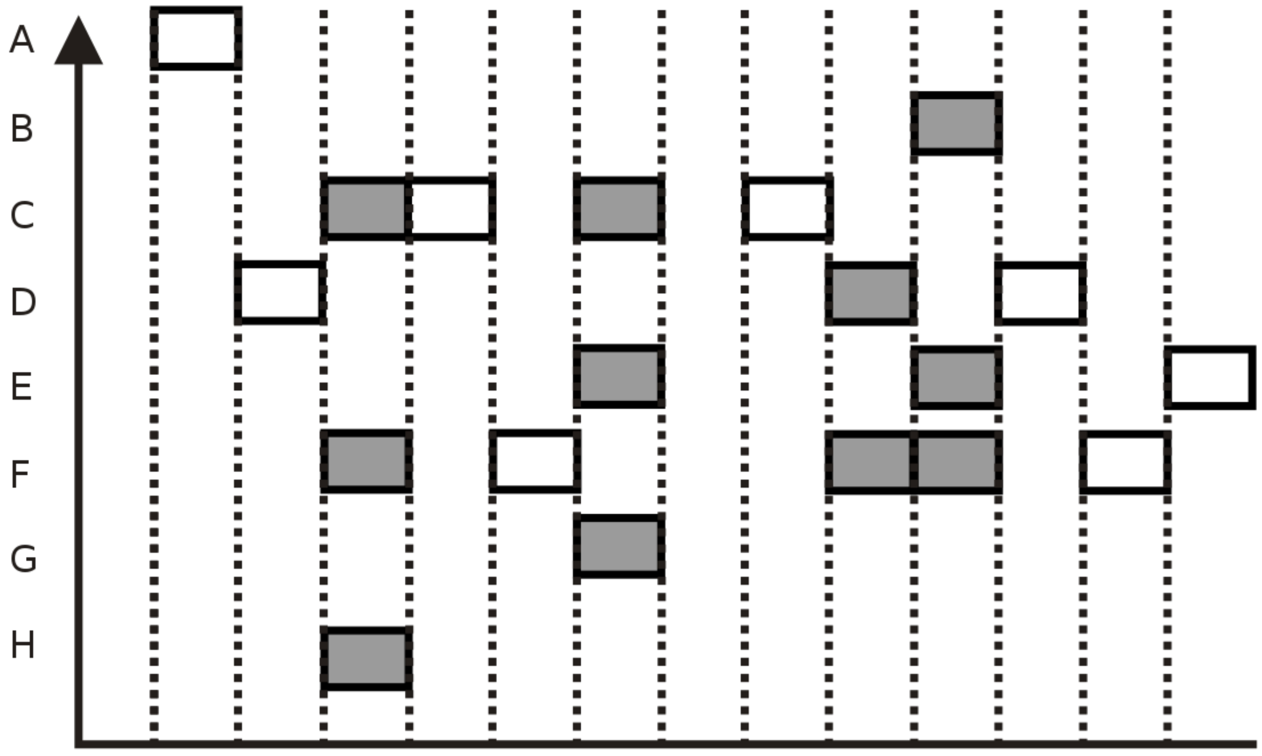


In pure ALOHA, frames are transmitted at completely arbitrary times.

Slotted ALOHA

- ***Slotted ALOHA***
  - method for doubling the capacity of an ALOHA system
  - to divide time into discrete intervals, each interval corresponding to one frame.
  - This approach requires the users to agree on slot boundaries.
  - it is required to wait for the beginning of the next slot

Slotted ALOHA



Slotted ALOHA protocol (shaded slots indicate collision)

CSMA

- **Carrier Sense Multiple Access (CSMA) Protocols**
  - Protocols in which stations listen for a carrier (i.e., a transmission) and act accordingly are called **carrier sense protocols**
  - **1-persistent CSMA**
    - When a station has data to send, it first listens to the channel to see if anyone else is transmitting at that moment.
    - If the channel is busy, the station waits until it becomes idle.
    - When the station detects an idle channel, it transmits a frame.
    - If a collision occurs, the station waits a random amount of time and starts all over again.
    - The protocol is called 1-persistent because the station transmits with a probability of 1 when it finds the channel idle.

CSMA

- **Nonpersistent CSMA**
  - Before sending, a station senses the channel.
  - If no one else is sending, the station begins sending.
  - However, if the channel is already in use, the station does not continually sense it for the purpose of seizing it immediately upon detecting the end of the previous transmission.
  - Instead, it waits a random period of time and then repeats the algorithm.
  - Consequently, this algorithm leads to better channel utilization but longer delays than 1-persistent CSMA.

CSMA

- **p-persistent CSMA**
  - When a station becomes ready to send, it senses the channel.
  - If it is idle, it transmits with a probability p.
  - With a probability q = 1 - p, it defers until the next slot.
  - If that slot is also idle, it either transmits or defers again, with probabilities p and q.
  - This process is repeated until either the frame has been transmitted or another station has begun transmitting
  - If the station initially senses the channel busy, it waits until the next slot and applies the above algorithm

CSMA/CD

- ***CSMA with Collision Detection (CSMA/CD)***
  - Persistent and nonpersistent CSMA protocols ensure that no station begins to transmit when it senses the channel busy
  - Another improvement is for stations to abort their transmissions as soon as they detect a collision
  - if two stations sense the channel to be idle and begin transmitting simultaneously, they will both detect the collision almost immediately.
  - Rather than finish transmitting their frames, they should stop transmitting as soon as the collision is detected
  - Advs: saves time and bandwidth
  - widely used on LANs in the MAC sublayer

IEEE 802 for LANS & MANS

- IEEE has standardized a number of local area networks and metropolitan area networks under the name of IEEE 802
  - 802.3 (Ethernet)
  - 802.4 (Token bus)
  - 802.5 (Token ring)
  - 802.11 (wireless LAN)
  - 802.15 (Bluetooth)
  - 802.16 (wireless MAN)

IEEE 802.3 (Ethernet)

- Ethernet is a **family of computer networking technologies for local area networks** (LANs).

- It was commercially introduced in 1980 and first standardized in 1983 as **IEEE 802.3** and has since been refined to support higher bit rates and longer link distances.

- Over time, Ethernet has largely replaced competing wired LAN technologies such as token ring, FDDI, and ARCNET

Ethernet Frame Format

Ethernet Frame Format

- **PREAMBLE:** The first field of the 802.3 frame contains 7 bytes(56bits)of alternating 0s and 1s that alerts the receiving system to coming frame and enables it to synchronize its input timing.
- **START FRAME DELIMITER(SFD)**:The second field (1byte:10101011)signals the beginning of the frame .
    - The last 2 bits is11 and alerts the receiver that the next field is the destination address.
- **DESTINATION ADDRESS** : The DA field is 6 bytes and contains the physical address of the destination station to receive the packet

Ethernet Frame Format

- **SOURCE ADDRESS** : The SA field is also 6 bytes and contains the physical address of the sender of the packet.
- **LENGTH/TYPE** : This field is defined as a type field or length field.The original Ethernet used this field as the type field to define the upper –layer protocol using the MAC frame.
- If the **data** portion of a frame is less than 46 bytes, **the Pad** field is used to fill out the frame to the minimum size.It can have a maximum of 1500 bytes
- **FCS/Checksum** field used for error detection.
- minimum(64 bytes) and maximum(1518 bytes) length of frame.

Properties of Ethernet

- ***shared bus topology*** –all stations connect to a single, shared communication channel
- ***broadcast technology -*** all stations receive every transmission, making it possible to transmit a packet to all stations at the same time
- ***distributed access control -***no central authority to grant access
- ***best-effort delivery*** mechanism - the hardware provides no information to the sender about whether the packet was delivered.
- access scheme is ***Carrier Sense Multiple Access*** with ***Collision Detect (CSMA/CD).***

Ethernet Hardware Addresses

- Ethernet defines a 48-bit addressing scheme.
- Each computer attached to an Ethernet network is assigned a unique 48-bit number known as its ***Ethernet address(MAC address or physical address)***
- To assign an address, Ethernet hardware manufacturers purchase blocks of Ethernet addresses assign them in sequence as they manufacture Ethernet interface hardware.
- Thus, no two hardware interfaces have the same Ethernet address.
- The Ethernet address is 6 bytes (48 bits), normally written in hexadecimal notation, with a colon between the bytes.

  06:01 :02:01:2C:4B

High Speed LANs

	Fast Ethernet	Gigabit Ethernet	Fibre Channel	Wireless LAN
Data Rate	100 Mbps	1 Gbps, 10 Gbps	100 Mbps - 3.2 Gbps	1 Mbps - 2 Gbps
Transmission Mode	UTP,STP, Optical Fiber	UTP, shielded cable, optical fiber	Optical fiber, coaxial cable, STP	2.4 GHz, 5 GHz Microwave
Access Method	CSMA/CD	CSMA/CD	Switched	CSMA/CA Polling
Supporting Standard	IEEE 802.3	IEEE 802.3	Fibre Channel Association	IEEE 802.11

Fast Ethernet (802.3u)

- Fast Ethernet refers to a set of specifications developed by the IEEE 802.3 committee to provide a low-cost, Ethernet-compatible LAN operating at 100 Mbps.
- keep all the old frame formats, interfaces, and procedural rules, but just reduce the bit time from 100 nsec to 10 nsec

Name	Cable	Max. segment	Advantages
100Base-T4	Twisted pair	100 m	Uses category 3 UTP
100Base-TX	Twisted pair	100 m	Full duplex at 100 Mbps (Cat 5 UTP)
100Base-FX	Fiber optics	2000 m	Full duplex at 100 Mbps; long runs

Gigabit Ethernet **(802.3z)**

- Gigabit Ethernet is a term describing various technologies for transmitting Ethernet frames at a rate of a gigabit per second (1,000,000,000 bits per second), as defined by the IEEE 802.3-2008 standard.
- make Ethernet go 10 times faster yet remain backward compatible with all existing Ethernet standards

  - 1000BASE-X - Optical Fibre
  - 1000BASE-T- Twisted Pair Cable

Gigabit Ethernet Technology

Name	Cable	Max. segment	Advantages
1000Base-SX	Fiber optics	550 m	Multimode fiber (50, 62.5 microns)
1000Base-LX	Fiber optics	5000 m	Single (10 μ) or multimode (50, 62.5 μ)
1000Base-CX	2 Pairs of STP	25 m	Shielded twisted pair
1000Base-T	4 Pairs of UTP	100 m	Standard category 5 UTP

1000 BASE SX *fiber* - *short wavelength*

1000 BASE LX *fiber* - *long wavelength*

1000 BASE CX *copper* - *shielded twisted pair*

1000 BASE T *copper* - *unshielded twisted pair*

* Based on Fiber Channel physical signaling technology.

Gigabit Ethernet cabling.

IEEE 802.4 -Token Bus

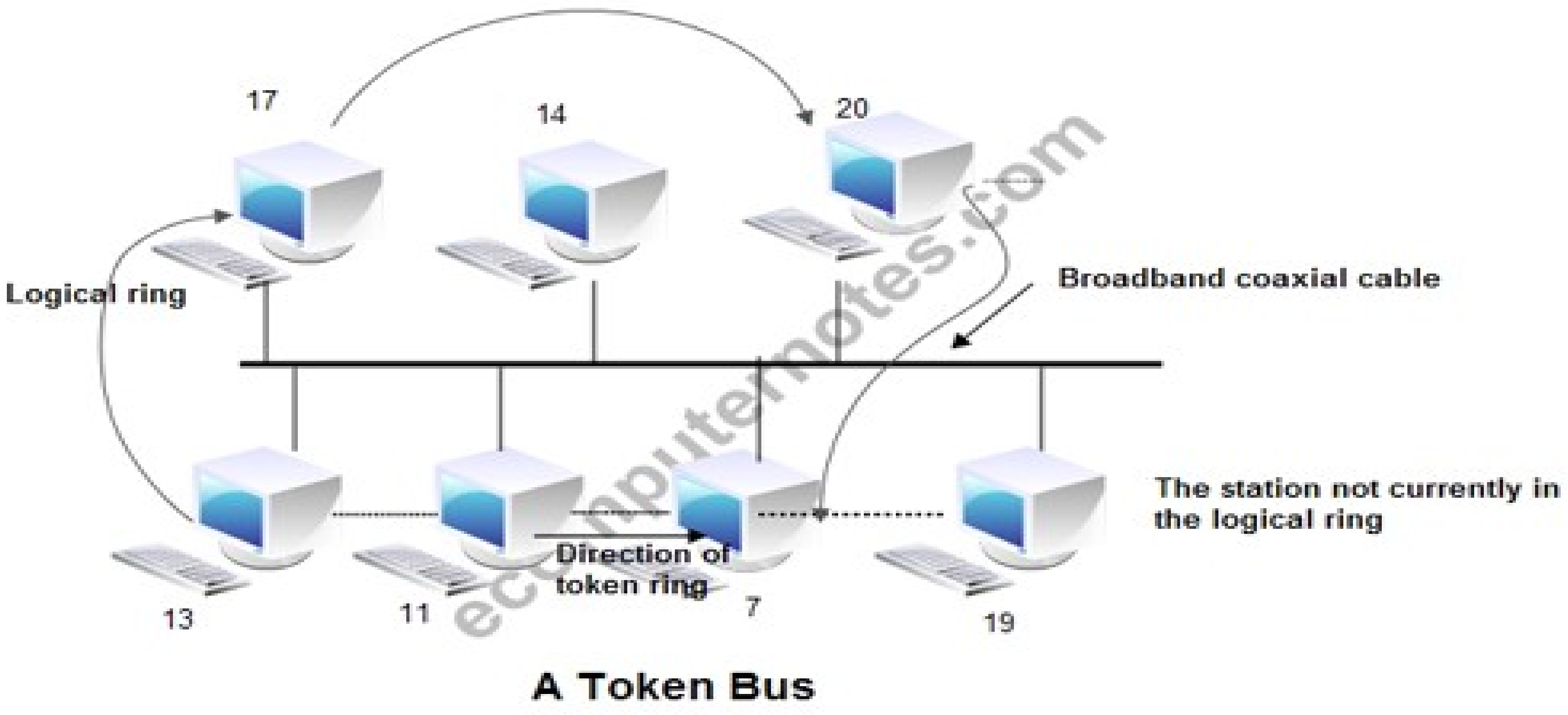
- Computer network station must possess a token before it can transmit on the computer network.
- They are broadband computer networks, as opposed to Ethernet's baseband transmission technique.
- Physically, the token bus is a linear or tree-shape cable to which the stations are attached
- Logically, the stations are organized into a ring.
- Token bus topology is well suited to groups of users that are separated by some distance.
- token bus networks are constructed with 75-ohm coaxial cable using a bus topology.

IEEE 802.4 -Token Bus

- The broadband characteristics of the 802.4 standard support transmission over several different channels simultaneously.
- When the logical ring is initialized, the highest numbered station may send the first frame.
- The token and frames of data are passed from one station to another following the numeric sequence of the station addresses.
- Thus, the token follows a logical ring rather than a physical ring.
- The last station in numeric order passes the token back to the first station.

IEEE 802.4 -Token Bus

- The token does not follow the physical ordering of workstation attachment to the cable.
- Station 1 might be at one end of the cable and station 2 might be at the other, with station 3 in the middle.



IEEE 802.4 -Token Bus

- In such a case, there is no collision as only one station possesses a token at any given time.
- In token bus, each station receives each frame;
- the station whose address is specified in the frame processes it and the other stations discard the frame.
- Working:
  - When the ring is initialized, stations are inserted into it in order of station address, from highest to lowest.
  - Token passing is done from high to low address.
  - Whenever a station acquires the token, it can transmit frames for a specific amount of time.
  - If a station has no data, it passes the token immediately upon receiving it.

IEEE 802.4 -Token Bus

1 byte	1 byte	1 byte	2-6 byte	2-6 byte	0-8182	4 byte	1 byte
Preamble	Start Delimiter	Frame Control	Destination Address	Source Address	Data	Checksum	End Delimiter

Frame format of IEEE 802.4

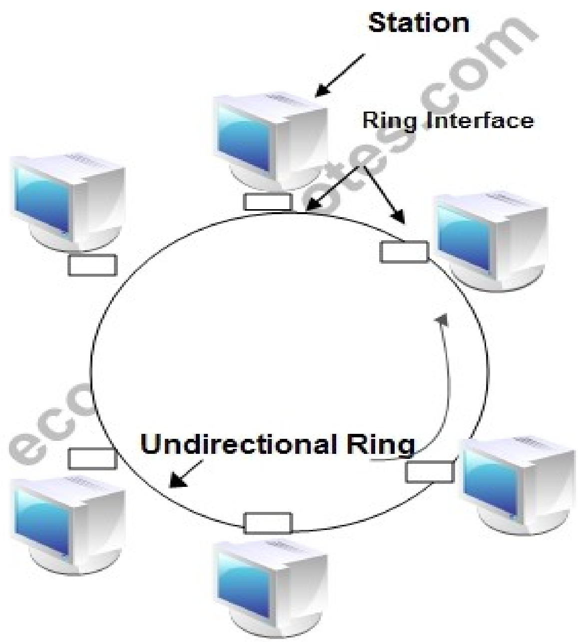
1. **Preamble**: This. Field is at least 1 byte long. It is used for bit synchronization.
2. **Start Delimiter**: This one byte field marks the beginning of frame.
3. **Frame Control:** This one byte field specifies the type of frame. It distinguishes data frame from control frames.
4. **Destination address**: It specifies 2 to 6 bytes destination address.
5. **Source address**: It specifies 2 to 6 bytes source address.
6. **Data**: This field may be up to 8182 bytes long when 2 bytes addresses are used & up to 8174 bytes long when 6 bytes address is used.
7. **Checksum**: This 4 byte field detects transmission errors.
8. **End Delimiter**: This one byte field marks the end of frame

IEEE 802.5 -Token Ring

- **IEEE 802.5 (Token Ring)**
  - A ring consists of a collection of ring interfaces connected by point-to-point lines
  - *i.e.* ring interface of one station is connected to the ring interfaces of its left station as well as right station.
  - Internally, signals travel around the Communication network from one station to the next in a ring.
  - These point-to-point links can be created with twisted pair, coaxial cable or fiber optics.

IEEE 802.5 -Token Ring

- all stations are connected in a ring and each station can directly hear transmissions only from its immediate neighbor.
- Permission to transmit is granted by a message (token) that circulates around the ring.
- A token is a special bit pattern (3 bytes long).
- There is only one token in the network



A Ring Network

IEEE 802.5 -Token Ring

- Token-passing networks move a small frame, called a token, around the network.
- Possession of the token grants the right to transmit.
- Since only one station can possess the token and transmit data at any given time, there are no collisions
- two operating modes of ring interfaces.
  - listen and transmit.

IEEE 802.5 -Token Ring

- In listen mode, the input bits are simply copied to output with a delay of 1- bit time.
- In transmit mode, the connection between input and output is broken by the interface so that is can insert its own data.
- The station comes in transmit mode when it captures the token
- The frames are acknowledged by the destination in a very simple manner.
  - The sender sends frames to receiver with ACK bit 0.
  - The receiver on receiving frames, copies data into its buffer, verifies the checksum and set the ACK bit to 1.
  - The verified frames come back to sender, where they are removed from the ring

IEEE 802.5 -Token Ring

- The information frame circulates the ring until it reaches the intended destination station, which copies the information for further processing.
- The information frame continues to circle the ring and is finally removed when it reaches the sending station.
- The sending station can check the returning frame to see whether the frame was seen and subsequently copied by the destination
- A station can hold a token for a specific duration of time.
- During this time, it has to complete its transmission and regenerates the token in ring.
- Whenever a station finishes its transmissions, the other station grabs the token and starts its own transmission

Differentiate 802.3, 802.4 & 802.5

Sl. No.	Parameter of comparison	802.3 Ethernet	802.4 Token Bus	802.5 Token Ring
1	Physical topology	Linear	Linear	Ring
2	Logical topology	None	Ring	Ring
3	Contention	Random chance	By token	By token
4	Adding stations	A new station can be added almost anywhere on the cable at any time.	Distributed algorithms are needed to add new stations.	Must be added between two specified stations.

Differentiate 802.3, 802.4 & 802.5

Sl. No.	Parameter of comparison	802.3 Ethernet	802.4 Token Bus	802.5 Token Ring
5	Performance	Stations often transmit immediately under light loads, but heavy traffic can reduce the effective data to nearly 0.	Stations must wait for the token even if no other station is transmitting. Under heavy load, token passing provides fair access to all stations.	Stations must wait for the token even if no other station is transmitting. Under heavy loads, token passing provides fair access to all stations.

Differentiate 802.3, 802.4 & 802.5

Sl. No.	Parameter of comparison	802.3 Ethernet	802.4 Token Bus	802.5 Token Ring
6	Maximum delay before transmitting	None	Bounded, depending on distance spanned and number of stations.	Bounded, depending on distance spanned and number of stations. However, if priorities are used, a low priority station may have no maximum delay.

Differentiate 802.3, 802.4 & 802.5

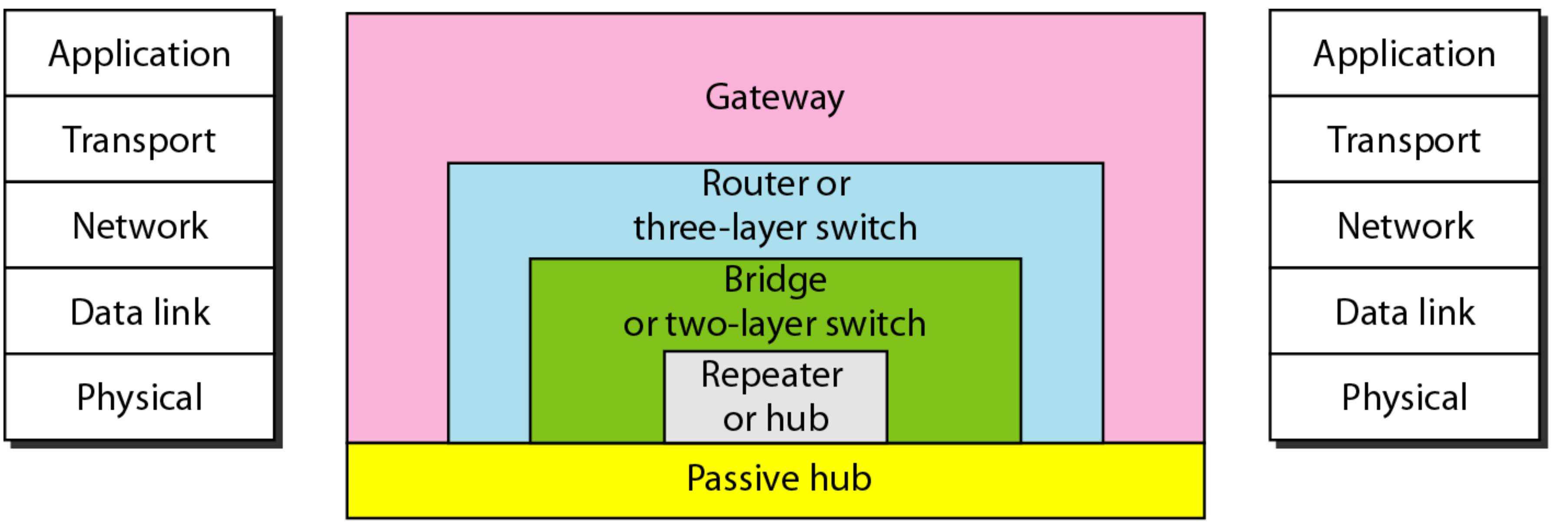
Sl. No.	Parameter of comparison	802.3 Ethernet	802.4 Token Bus	802.5 Token Ring
7	Maintenance	No central maintenance	Distributed algorithm provide maintenance	A designated monitor station performs maintenance.
8	Cable used	Twisted pair, co-axial fiber optic	Co-axial	Twisted pair and fiber optic.
9	Cable length	50 to 2000 m	200 to 500 m	50 to 2000 m
10	Frame	l0Mbps to 100 Mbps	10Mbps	4 to l00Mbps
11	Structure	1500 bytes	8191 bytes	5000 bytes

CONNECTING DEVICES

- LANs do not normally operate in isolation but they are connected to one another or to the Internet.
- To connect LANs, connecting devices are needed and various connecting devices are such as bridge, switch, router, hub, repeater.

CONNECTING DEVICES

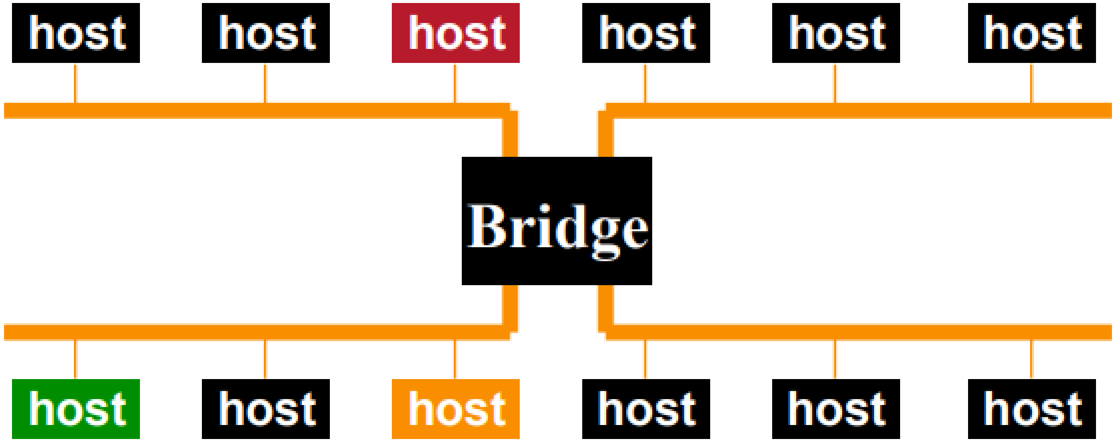
- Connecting devices into five different categories based on the layer in which they operate in a network.



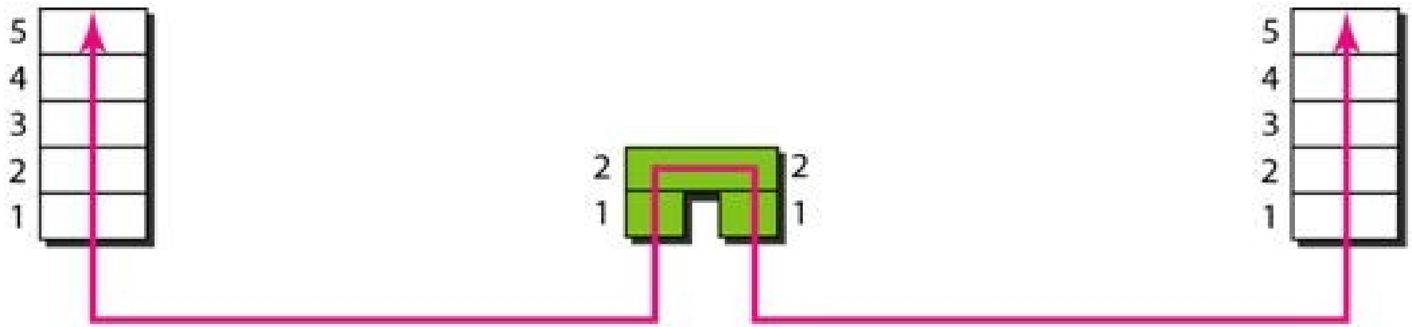
Bridges and Switches

Bridges

- Connects two or more LANs at the link layer
  - – Extracts destination address from the frame.
  - – Looks up the destination in a table.
  - – Forwards the frame to the appropriate LAN segment .
- Each segment can carry its own traffic.

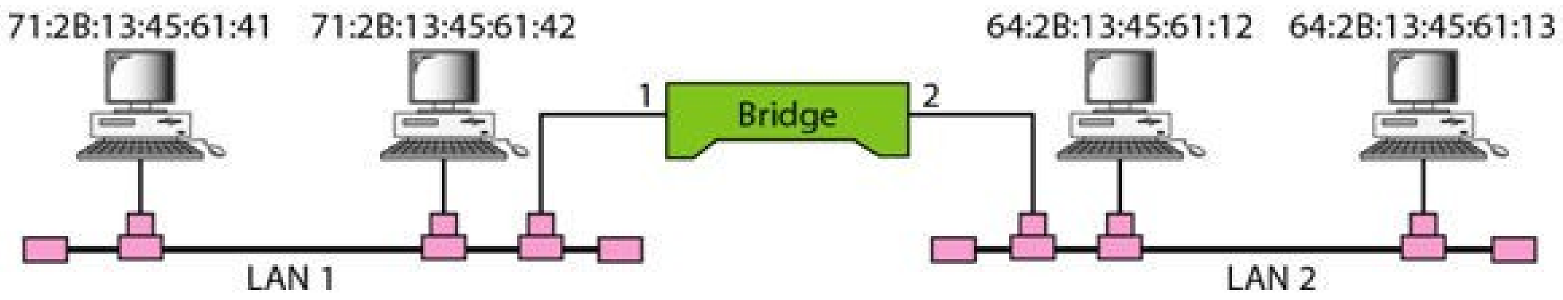


A bridge connecting two LANs



Address	Port
71:2B:13:45:61:41	1
71:2B:13:45:61:42	1
64:2B:13:45:61:12	2
64:2B:13:45:61:13	2

Bridge Table



- When bridge receives a frame:
- The routing procedure for an incoming frame depends on the LAN it arrives on (the source LAN) and the LAN its destination is on (the destination LAN), as follows:
  - If destination and source LANs are the same, discard the frame
  - If the destination and source LANs are different, forward the frame
  - If the destination LAN is unknown, use flooding

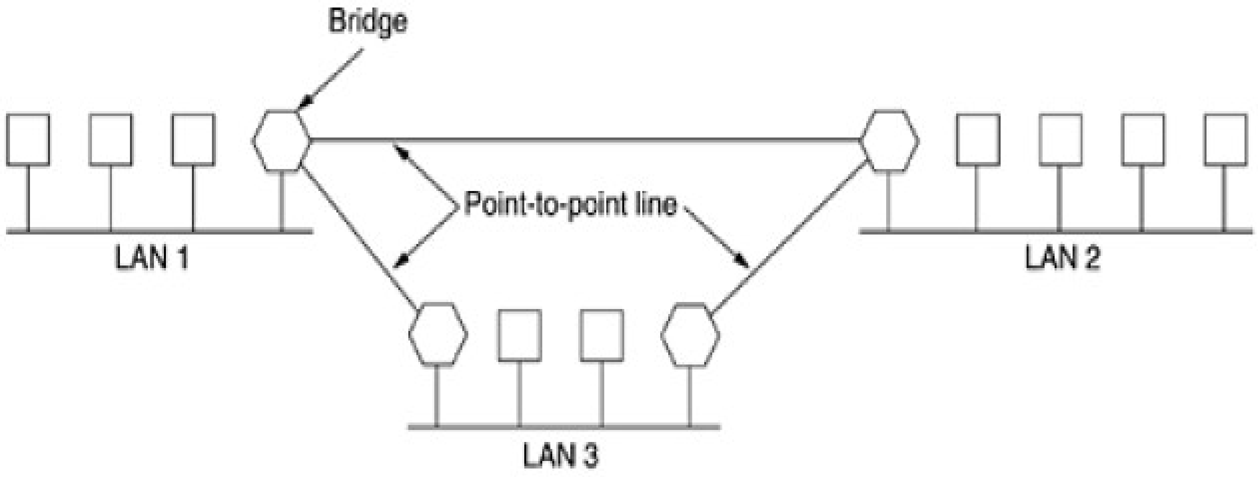
Features

- MAC layer (Data Link Layer) device
- stores and forwards Ethernet frames
- operate on Ethernet frames, examining frame header and selectively forwarding frame based on MAC dest address
- When frame is to be forwarded on segment, bridge uses CSMA/CD to access segment and transmit
- Can connect different type Ethernet since it is a store and forward device.
- Limitless number of nodes and geographical coverage
- Transparent: hosts are unaware of presence of bridges

Remote Bridges

- A common use of bridges is to connect two (or more) distant LANs.
- For example, a company might have plants in several cities, each with its own LAN.
- Ideally, all the LANs should be interconnected, so the complete system acts like one large LAN.
- This goal can be achieved by putting a bridge on each LAN and connecting the bridges pairwise with point-to-point lines (e.g., lines leased from a telephone company).

Remote Bridges

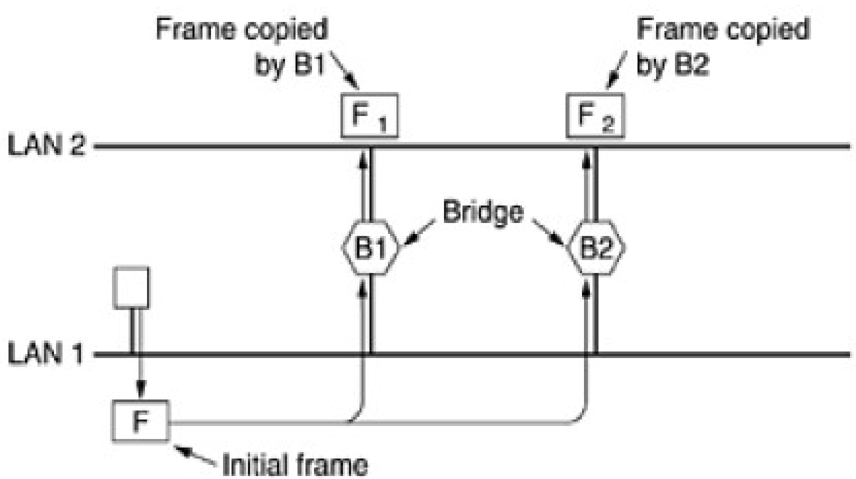


Spanning Tree Bridges

To increase reliability, some sites use two or more bridges in parallel between pairs of LANs, as shown in Fig.

This arrangement, however, also introduces some additional problems because it creates loops in the topology

Two parallel transparent bridges.



Spanning Tree Bridges

The solution to this difficulty is for the bridges to communicate with each other and overlay the actual topology with a spanning tree that reaches every LAN.

To build the spanning tree, first the bridges have to choose one bridge to be the root of the tree.

Next, a tree of shortest paths from the root to every bridge and LAN is constructed.

This tree is the spanning tree.

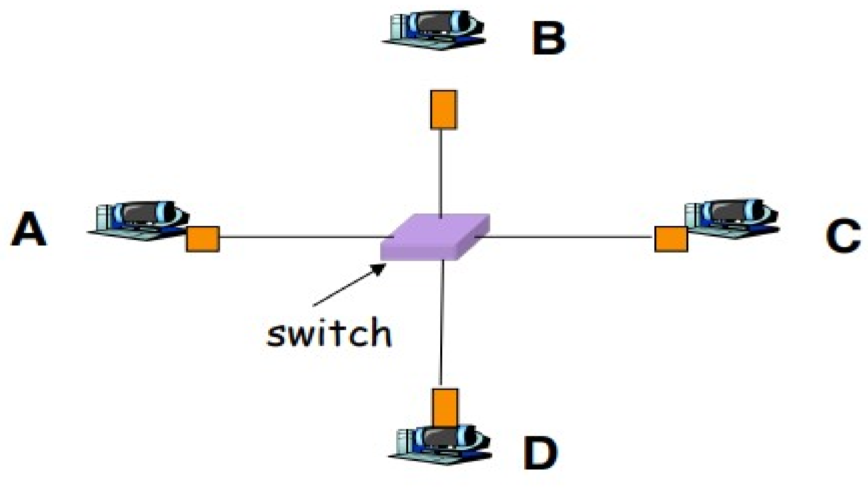
If a bridge or LAN fails, a new one is computed.

The result of this algorithm is that a unique path is established from every LAN to the root and thus to every other LAN.

Even after the spanning tree has been established, the algorithm continues to run during normal operation in order to automatically detect topology changes and update the tree.

Switches

a) Typically connects individual computers
  – – A switch is essentially the same as a bridge
  – – though typically used to connect hosts, LANs
b) Like bridges, support concurrent communication
c) – Host A can talk to C, while B talks to D

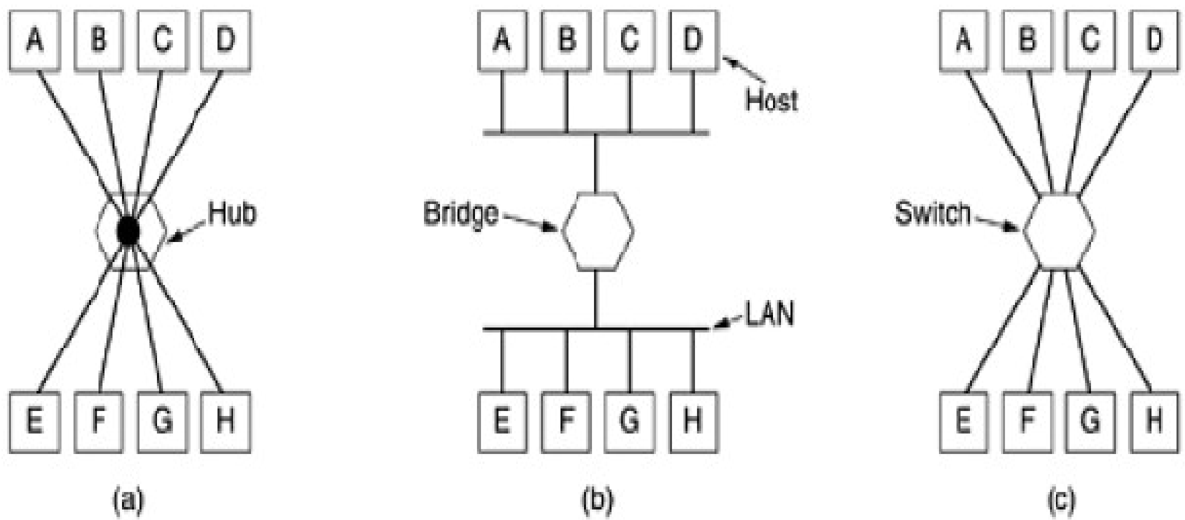


SWITCHES

Switches are similar to bridges in that both route on frame addresses. In fact, many people uses the terms interchangeably.

The main difference is that a switch is most often used to connect individual computers, as shown in Fig. (c).

(a) A hub. (b) A bridge. (c) A switch.



SWITCHES

As a consequence, when host *A* in Fig. (b) wants to send a frame to host *B*, the bridge gets the frame but just discards it.

In contrast, in Fig.(c), the switch must actively forward the frame from *A* to *B* because there is no other way for the frame to get there.

Since each switch port usually goes to a single computer, switches must have space for many more line cards than do bridges intended to connect only LANs.