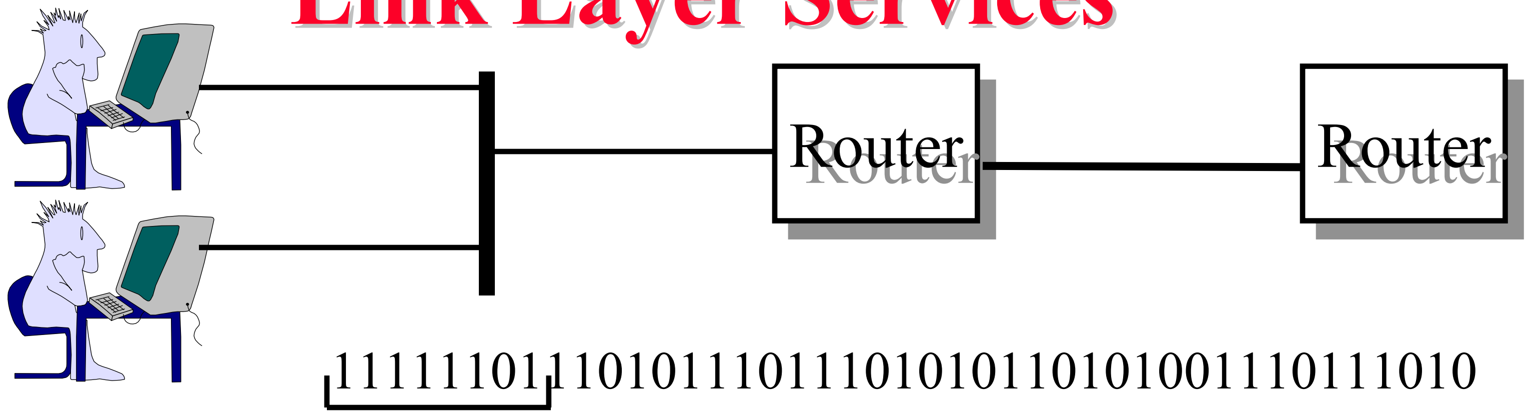
The Link Layer and LANs

1. Datalink Services
2. Error Detection
3. Multiple Access
4. Bridging
5. Point-to-Point Protocol and MPLS

Note: This class lecture is based on Chapter 5 of the textbook (Kurose and Ross) and the figures provided by the authors.

Link Layer Services

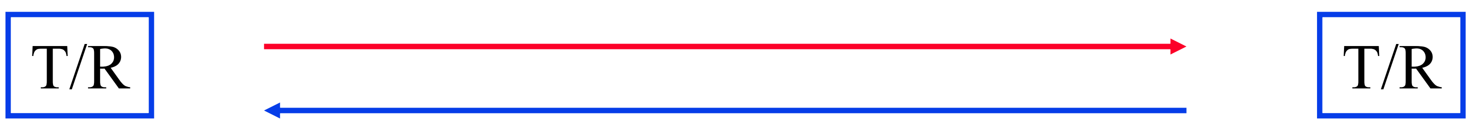


- Link = One hop
- Framing: Bit patterns at begin/end of a frame
- Multiple Access: Multiple users sharing a wire
- Flow Control
- Error Detection/Correction
- Reliable Delivery:
- Duplex Operation

Line Duplexity

- Simplex: Transmit or receive,
  e.g., Television

- Full Duplex: Transmit and receive simultaneously,
  e.g., Telephone



- Half-Duplex: Transmit and receive alternately,
  e.g., Police Radio

Error Detection

- Parity Checks
- Check Digit Method
- Modulo 2 Arithmetic
- Cyclic Redundancy Check (CRC)
- Popular CRC Polynomials

Parity Checks

1	2	3	4	5	6	7	8	9
1	0	1	1	1	0	1	0	

- Odd Parity

1	2	3	4	5	6	7	8	9
1	0	1	1	1	0	1	0	0

1	2	3	4	5	6	7	8	9
0	0	1	1	1	0	1	0	0

1-bit error

1	2	3	4	5	6	7	8	9
0	0	0	1	0	0	1	0	0

3-bit error

1	2	3	4	5	6	7	8	9
0	0	0	1	1	0	1	0	0

2-bit error

- Even Parity

1	2	3	4	5	6	7	8	9
1	0	1	1	1	0	1	1	0

Modulo 2 Arithmetic

```
  1111       11001          110
                      ___________
+1010     ×     11     11  | 1010
--------  --------          / 11
  0101      11001           --------    010   2
           11001              x11       011   3
          ---------            11       ----  --
          101011             --------   001   1  Mod 2
                                x00     101   5  Binary
                                 00
                              -----
                                 x0
```

Cyclic Redundancy Check (CRC)

- Binary Check Digit Method
- Make number divisible by P=110101 (n+1=6 bits)

Example: M=1010001101 is to be sent

1. Left-shift M by n bits 2^nM= 101000110100000
2. Divide 2^nM by P, find remainder: R=01110
3. Add the result of step 2 to step 1 :
   T=101000110101110
4. Check that the result T is divisible by P.

Modulo 2 Division

```
        Q=1101010110
P=110101)101000110100000=2^nM
         110101
          111011
          110101
           011101
           000000
            111010
            110101
             011111
             000000
              111110
              110101
               010110
               000000
                101100
                110101
                 110010
                 110101
                  001110
                  000000
                   01110 = R
```

Checking At The Receiver

```
        1101010110
110101)101000110101110
       110101
        111011
        110101
         011101
         000000
          111010
          110101
           011111
           000000
            111110
            110101
             010111
             000000
              101111
              110101
               110101
               110101
                00000
```

Error Detection: Review

1. Parity bits can help detect/correct errors
2. CRC uses mod 2 division

Homework 5A

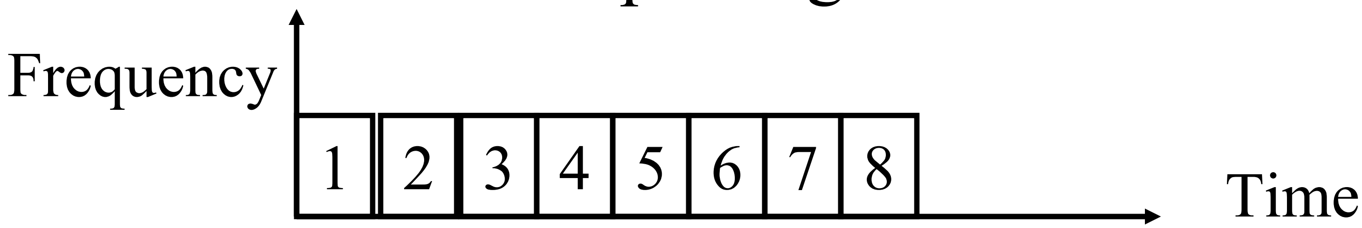
- Find the CRC of 1001100 using a generator *1011. Use mod 2 division. Show all steps.*

Ethernet and ARP

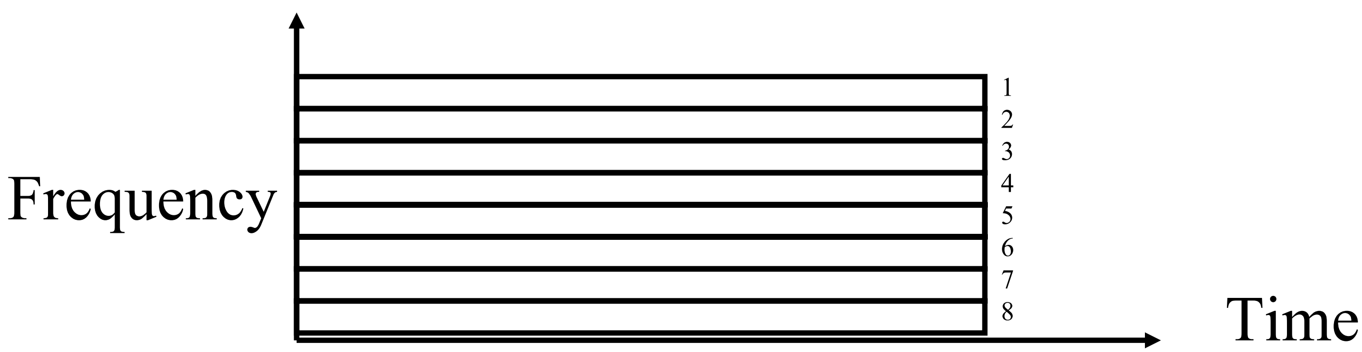
1. Multiple Access
2. CSMA/CD
3. IEEE 802.3 CSMA/CD
4. Ethernet Standards
5. CSMA/CD Performance
6. Distance-B/W Principle
7. Ethernet vs. Fast Ethernet
8. IEEE 802 Address Format
9. Address Resolution Protocol

Multiple Access

- How multiple users can share a link?
- Time Division Multiplexing



- Frequency Division Multiplexing



1-persistent: When the transmitting node is ready to transmit, it senses the transmission medium for idle or busy. If idle, then it transmits immediately. If busy, then it senses the transmission medium continuously until it becomes idle, then transmits the message (a frame) unconditionally (i.e. with probability=1). In case of a collision, the sender waits for a random period of time and attempts to transmit again unconditionally (i.e. with probability=1).

Non-persistent: When the transmitting node is ready to transmit data, it senses the transmission medium for idle or busy. If idle, then it transmits immediately. If busy, then it waits for a random period of time (during which it does not sense the transmission medium) before repeating the whole logic cycle (which started with sensing the transmission medium for idle or busy) again. This approach reduces collision, results in overall higher medium throughput but with a penalty of longer initial delay compared to 1–persistent.

P-persistent: When the transmitting node is ready to transmit data, it senses the transmission medium for idle or busy. If idle, then it transmits a frame with probability p. If the node does not transmit (the probability of this event is 1-p), it waits until the next available time slot. If the transmission medium is still not busy, it transmits again with the same probability p. P-persistent CSMA is used in CSMA/CA systems including Wi-Fi and other packet radio systems.

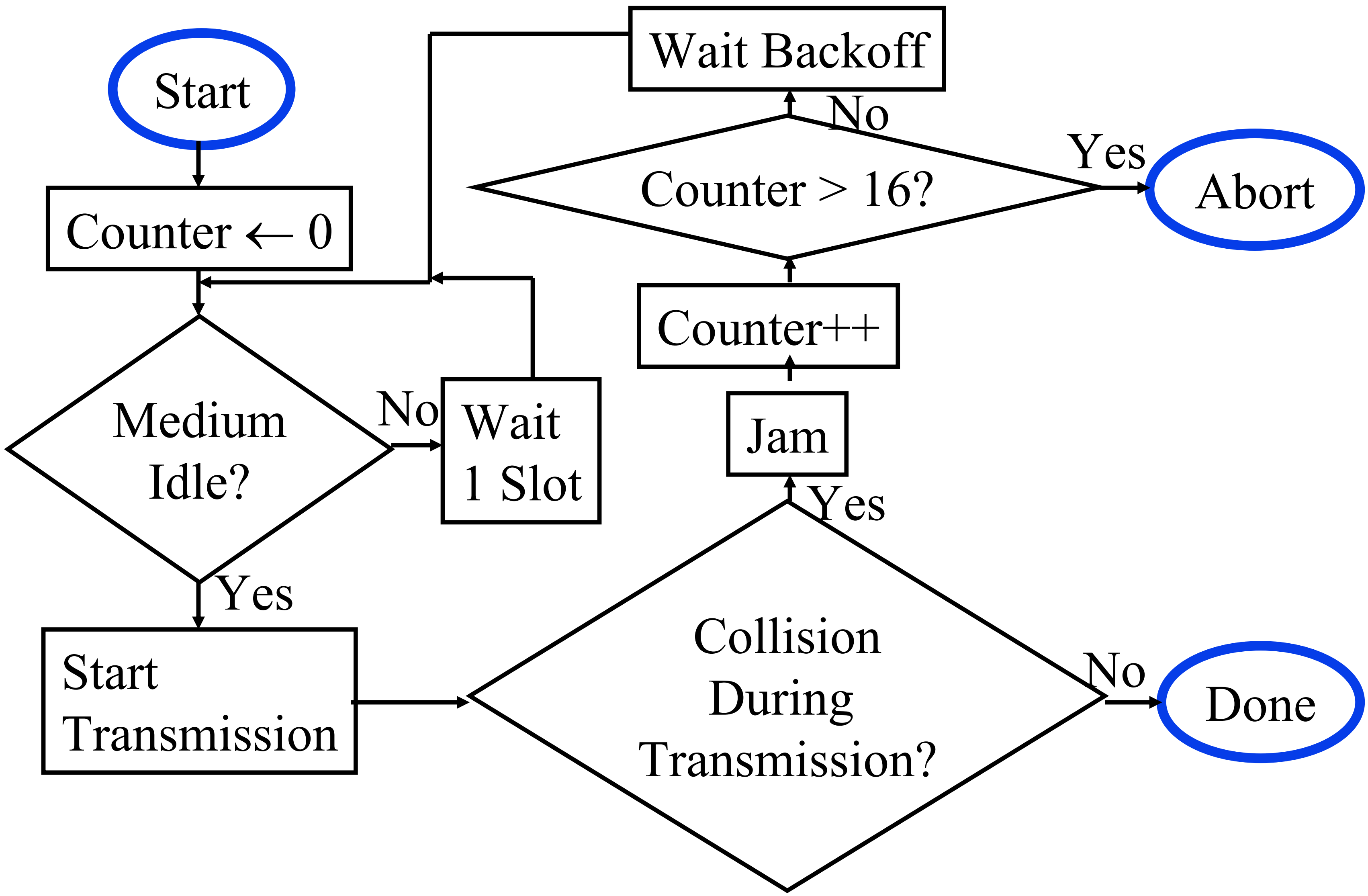
CSMA/CD

- Aloha at Univ of Hawaii:
  Transmit whenever you like
  Worst case utilization = 1/(2e) =18%
- Slotted Aloha: Fixed size transmission slots
  Worst case utilization = 1/e = 37%
- CSMA: Carrier Sense Multiple Access
  Listen before you transmit
- p-Persistent CSMA: If idle, transmit with probability p. Delay by one time unit with probability 1-p
- CSMA/CD: CSMA with Collision Detection
  Listen while transmitting. Stop if you hear someone else

IEEE 802.3 CSMA/CD

- If the medium is idle, transmit (1-persistent).
- If the medium is busy, wait until idle and then transmit immediately.
- If a collision is detected while transmitting,
  - Transmit a jam signal for one slot (= 51.2 μs = 64 byte times)
  - Wait for a random time and reattempt (up to 16 times)
  - Random time = Uniform[0,$2^{\min(k,10)}$-1] slots
- Collision detected by monitoring the voltage
  High voltage ⇒ two or more transmitters ⇒ Collision
  ⇒ Length of the cable is limited to 2 km

IEEE 802.3 CSMA/CD Flow Chart

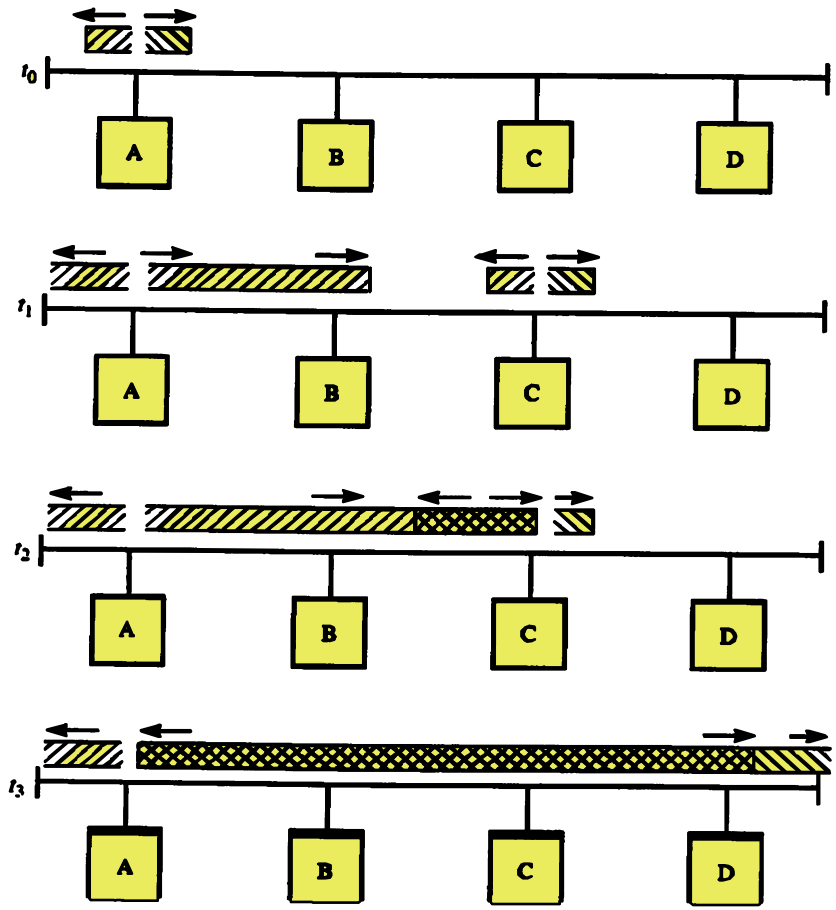


Exponential Backoff

- If a collision is detected, delay and try again
- Delay time is selected using binary exponential backoff
  - 1st time: choose K from {0,1} then delay = K * 51.2μs
  - 2nd time: choose K from {0,1,2,3} then delay = K * 51.2μs
  - *nth* time: delay = K x 51.2μs, for $K=0..2^n - 1$
    - Note max value for k = 1023
  - give up after several tries (usually 16)
    - Report transmit error to host
- If delay were not random, then there is a chance that sources would retransmit in lock step
- Why not just choose from small set for K
  - This works fine for a small number of hosts
  - Large number of nodes would result in more collisions

CSMA/CD Operation

- Collision window = 2 × One-way Propagation delay = 51.2 µs



One way delay
= 25.6 µs
Max Distance
<2.5 km

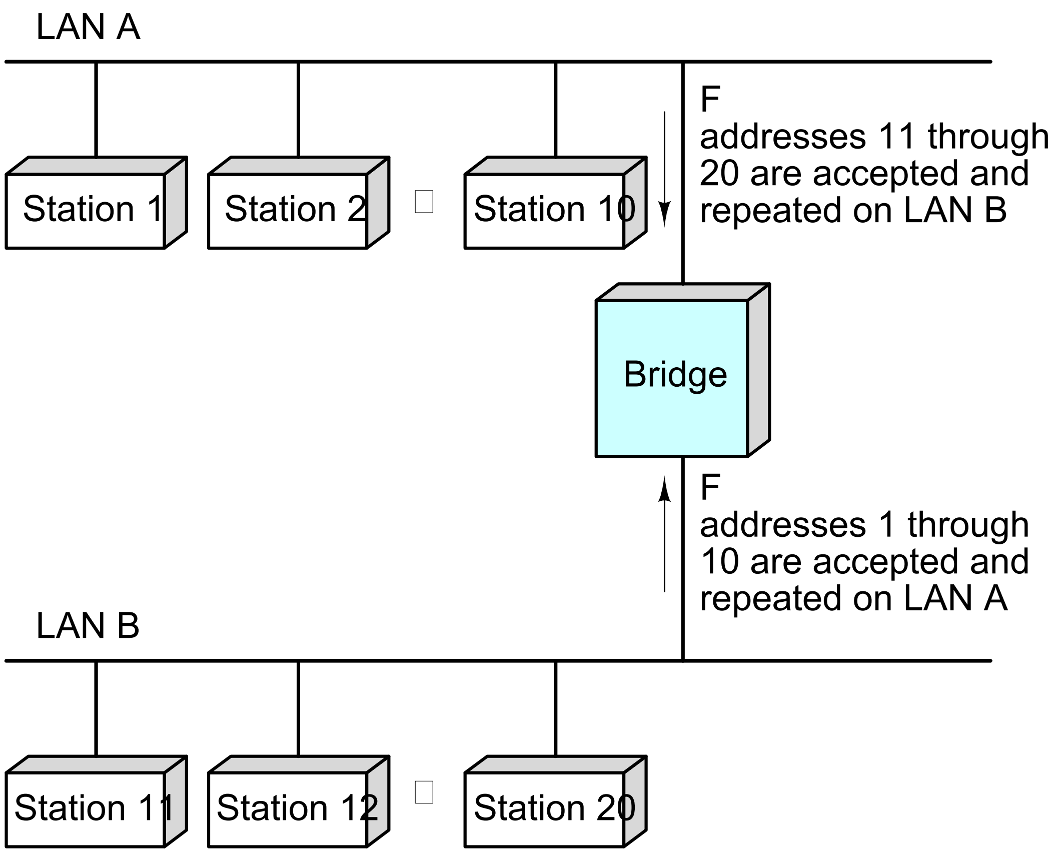
IEEE 802 Address Format

- 48-bit:1000 0000 : 0000 0001 : 0100 0011 : 0000 0000 : 1000 0000 : 0000 1100 = 80:01:43:00:80:0C

Organizationally Unique Identifier (OUI)			24 bits assigned by OUI Owner
Individual/ Group	Universal/ Local		
1	1	22	24

- Multicast = "To all bridges on this LAN"
- Broadcast = "To all stations" = 111111....111 = FF:FF:FF:FF:FF:FF

Bridges

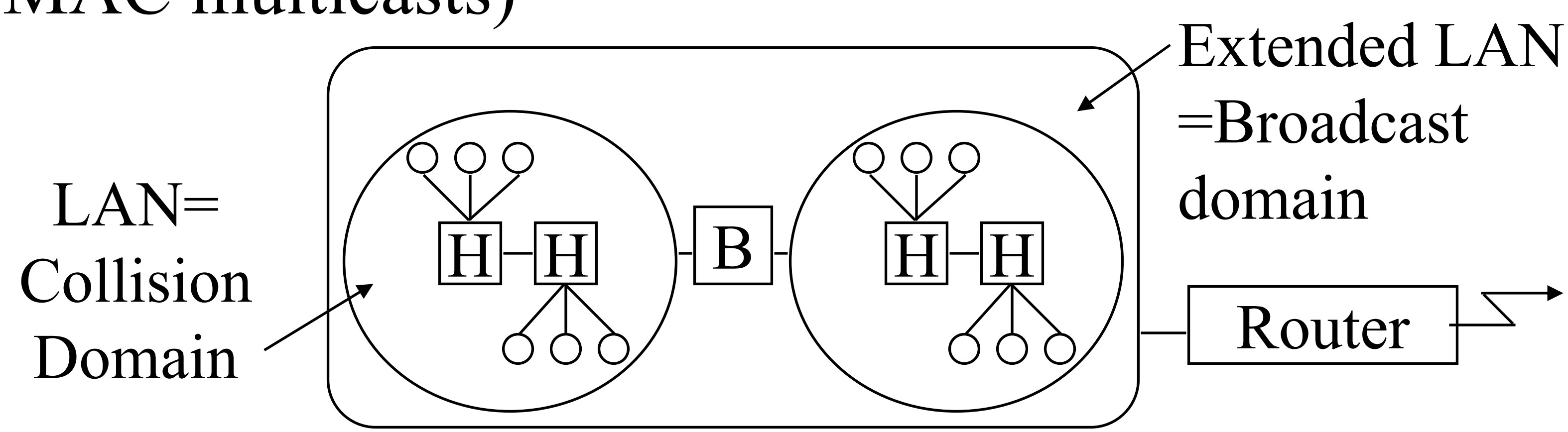

LAN A
Station 1
Station 2
Station 10
F
addresses 11 through
20 are accepted and
repeated on LAN B
Bridge
F
addresses 1 through
10 are accepted and
repeated on LAN A
LAN B
Station 11
Station 12
Station 20

Bridge: Functions

- Monitor all frames on LAN A
- Pickup frames that are for stations on the other side
- Retransmit the frames on the other side
- Knows or learns about stations are on various sides
  Learns by looking at source addresses⇒ **Self-learning**
- Makes no modification to content of the frames.
  May change headers.
- Provides storage for frames to be forwarded
- Improves reliability (less nodes per LAN)
- Improves performance (more bandwidth per node)
- Security (Keeps different traffic from entering a LAN)
- May provide flow and congestion control

Interconnection Devices

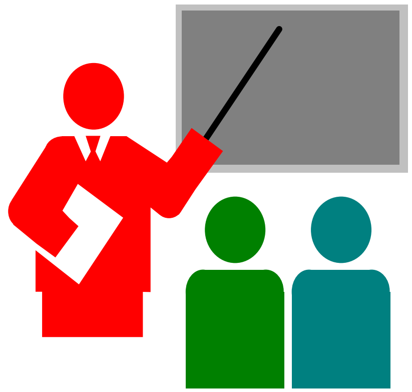
- **Repeater**: PHY device that restores data and collision signals
- **Hub:** Multiport repeater + fault detection, notification and signal broadcast
- **Bridge:** Datalink layer device connecting two or more collision domains
- **Router:** Network layer device (does not propagate MAC multicasts)



Address Resolution Protocol

- Problem: Given an IP address find the MAC address
- Solution: Address resolution protocol
- The host broadcasts a request:
  "What is the MAC address of 127.123.115.08?"
- The host whose IP address is 127.123.115.08 replies back:
  "The MAC address for 127.123.115.08 is 8A-5F-3C-23-45-56".

Ethernet and ARP: Review

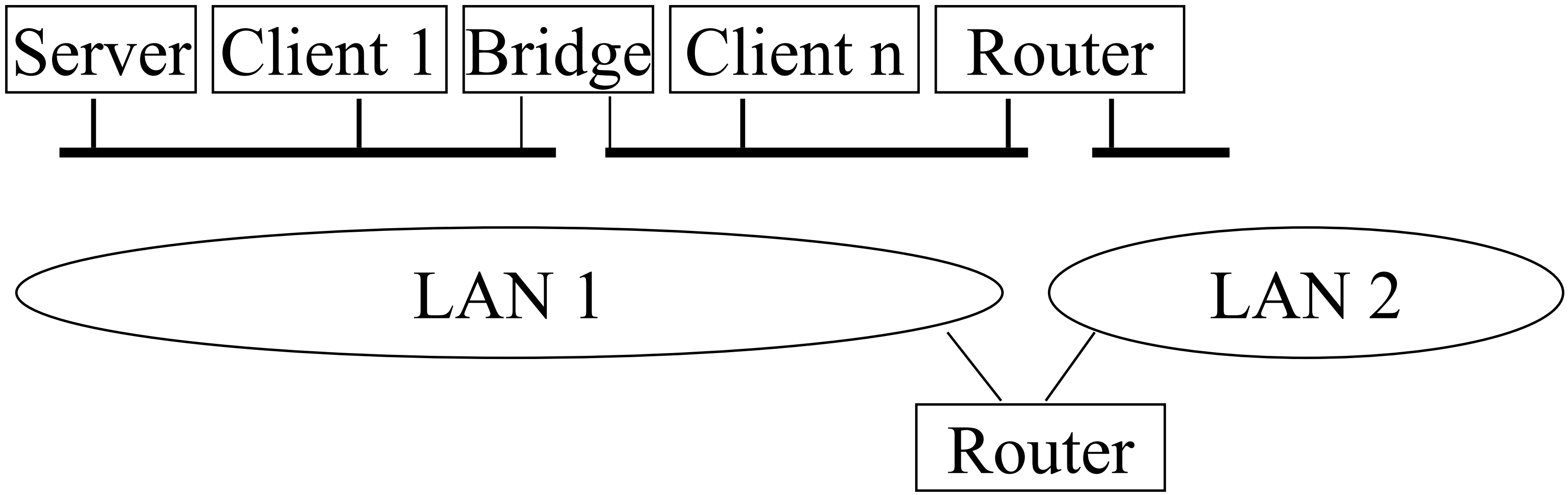


1. CSMA/CD = Listen while transmitting and stop on collision
2. IEEE 802.3 uses a *truncated binary exponential backoff*.
3. Ethernet uses 48-bit addresses of which the first bit is the unicast/multicast, 2^{nd} bit is universal/local, 22-bits are OUI (Organizationally unique identifier).
4. Address Resolution Protocol (ARP) is used to find the MAC address for a given IP address and vice versa.

LLC, VLANs, PPP, and MPLS

1. Virtual LAN
2. PPP
3. Multiprotocol Label Switching (MPLS)

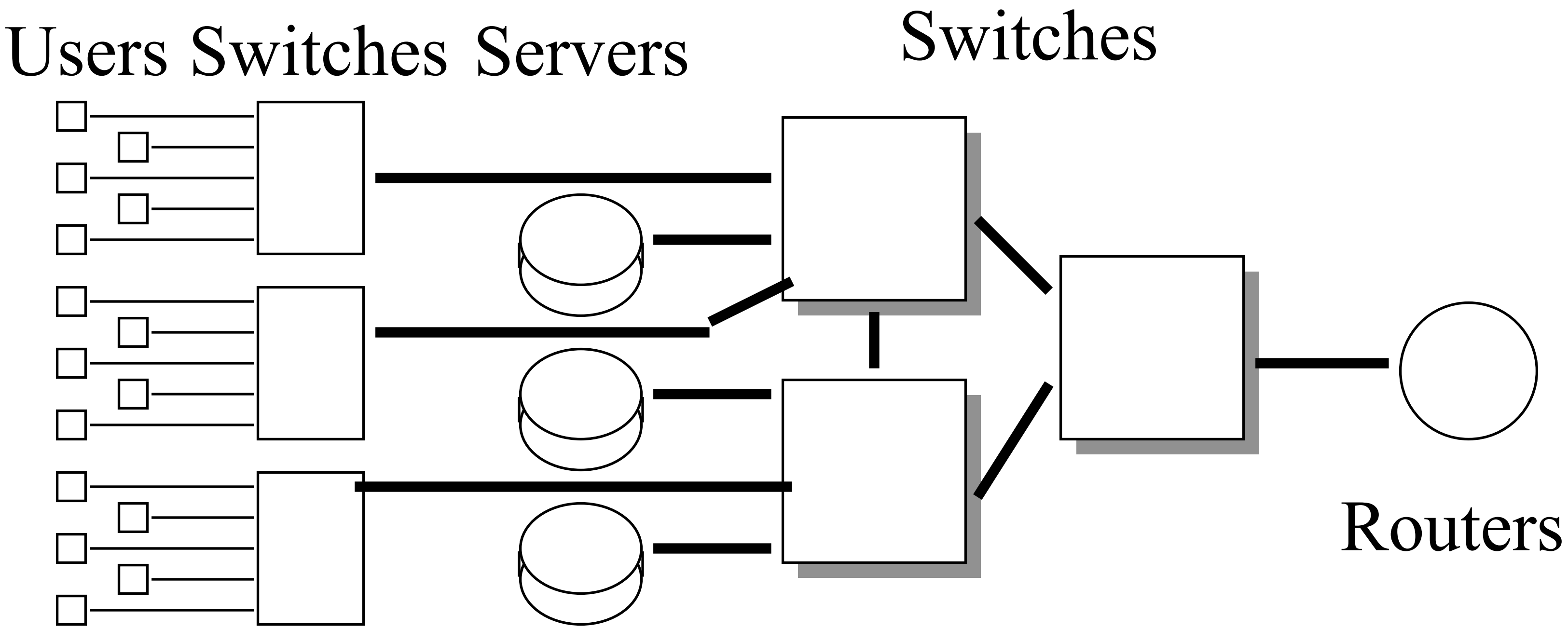
What is a LAN?



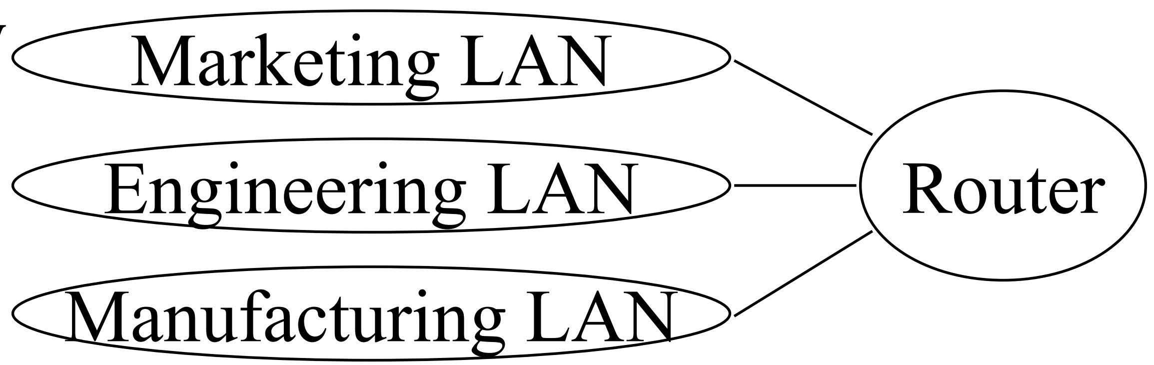
- LAN = Single broadcast domain
- No routing between members of a LAN
- Routing required between LANs

What is a Virtual LAN

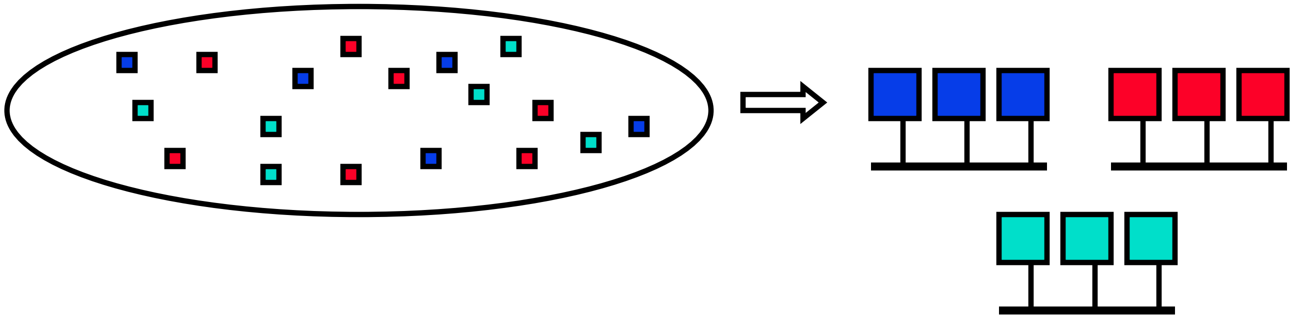
- **Physical View**



- **Logical View**



Virtual LAN

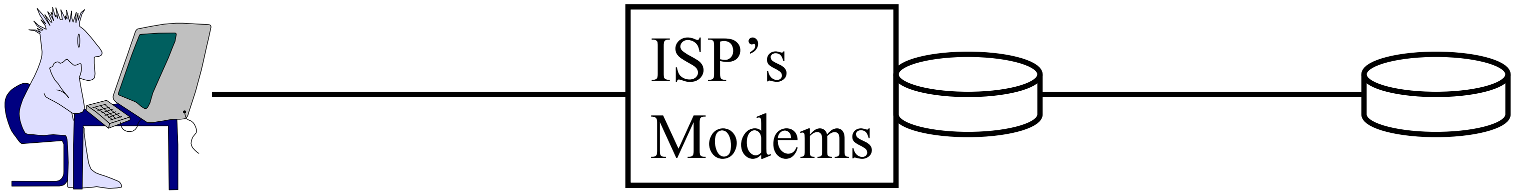


- Virtual LAN = Broadcasts and multicast goes only to the nodes in the virtual LAN
- LAN membership defined by the network manager $\Rightarrow$ Virtual

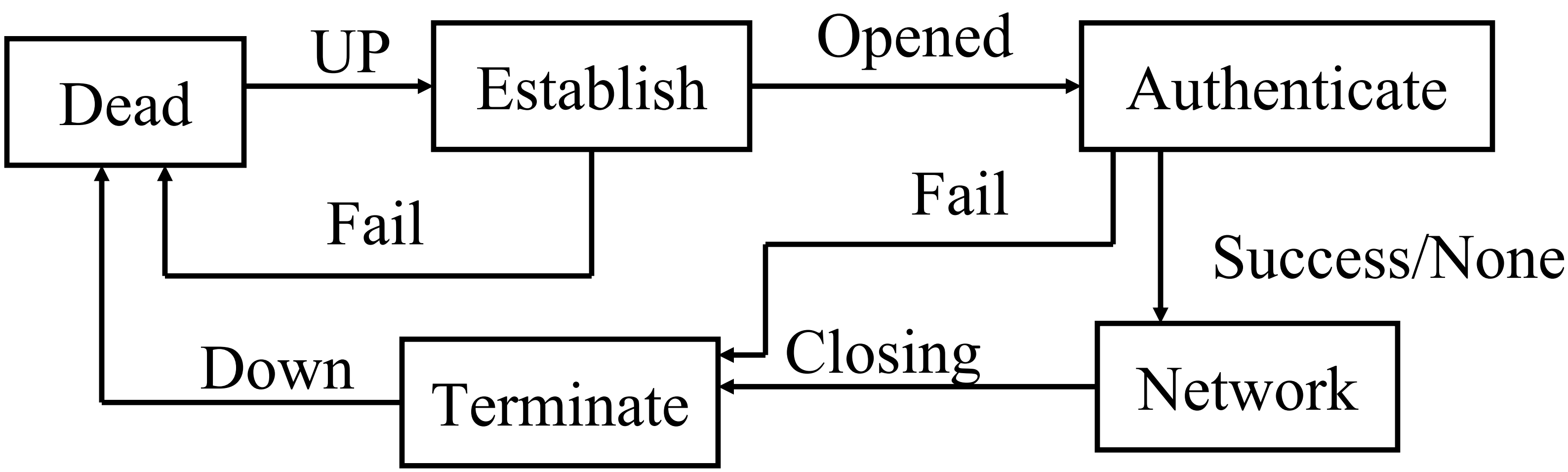
VLAN: Why?

- Virtual is Better than Real
  - Location-independent
    $\Rightarrow$ Marketing LAN can be all over the building
  - Users can move but not change LAN
  - Traffic between LANs is routed
    $\Rightarrow$ Better to keep all traffic on one LAN
  - Switch when you can, route when you must
  - Better security

PPP: Introduction



- Point-to-point Protocol
- Originally for User-network connection
- Now being used for router-router connection
- Three Components: Data encaptulation, Link Control Protocol (LCP), Network Control Protocols (NCP)



LCP packets are sent to determine the standards of the ensuing data transmission. it also used for establishing, configuring, and testing the data-link connection.
(NCPs) is used for establishing and configuring different network layer protocols.

PPP in HDLC-Like Framing

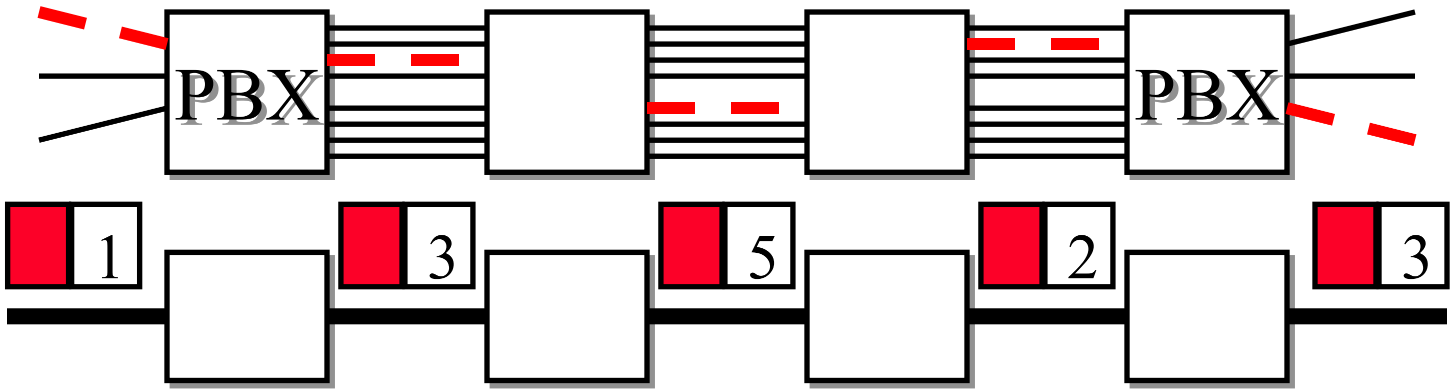
Flag	Address	Control	Protocol
01111110	11111111 (Broadcast)	00000011	

Info	Padding	CRC	Flag
			01111110

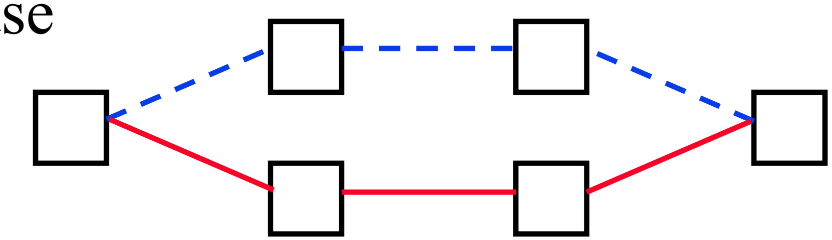
- Flag = 0111 1110 = 7E
- Byte Stuffing: 7E ⇒ 7D 5E
  7D ⇒ 7D 5D

HDLC (High-level Data Link Control) is a group of protocols or rules for transmitting data between network points (sometimes called nodes)

Multiprotocol Label Switching (MPLS)



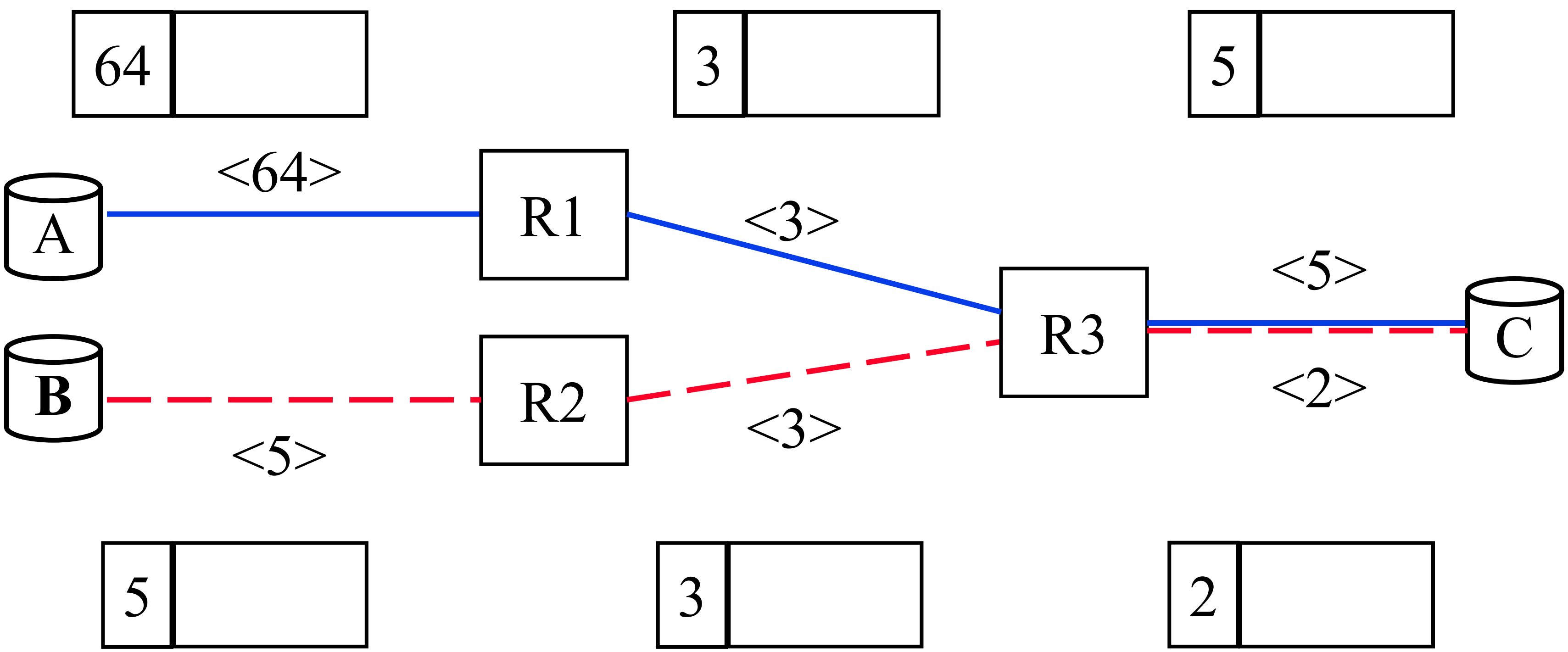
- Allows virtual circuits in IP Networks (May 1996)
- Each packet has a virtual circuit number called ‘label’
- Label determines the packet’s queuing and forwarding
- Circuits are called Label Switched Paths (LSPs)
- LSP’s have to be set up before use
- Allows traffic engineering

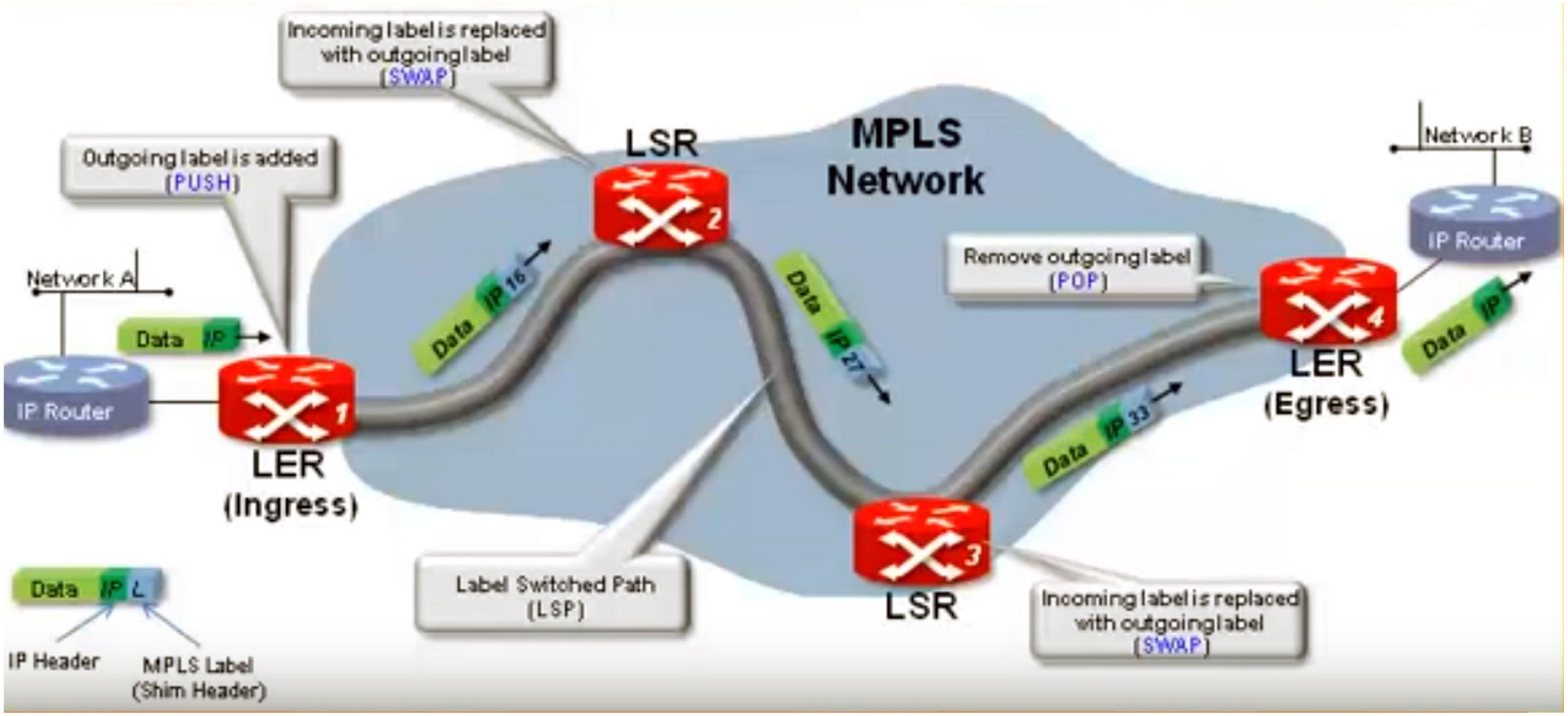


Label Switching Example

Ethernet Header	IP Header	Payload

Ethernet Header	Label	IP Header	Payload





MPLS is a “Layer 2.5 networking protocol”.

When an LSR (label switch router) receives a packet, it uses the label included in the packet header as an index to determine the next hop on the predetermined label-switched path (LSP) and a corresponding label for the packet from a lookup table. The old label is then removed from the header and replaced with the new label before the packet is routed forward.

A LER (label edge router) operates at the edge of an MPLS network and acts as the entry and exit points for the network. LER (ingress) does an IP lookup and pushes an MPLS label onto an incoming IP packet, and an egress LER pops it off the outgoing packet.

LLC, VLANs, PPP, MPLS:Review

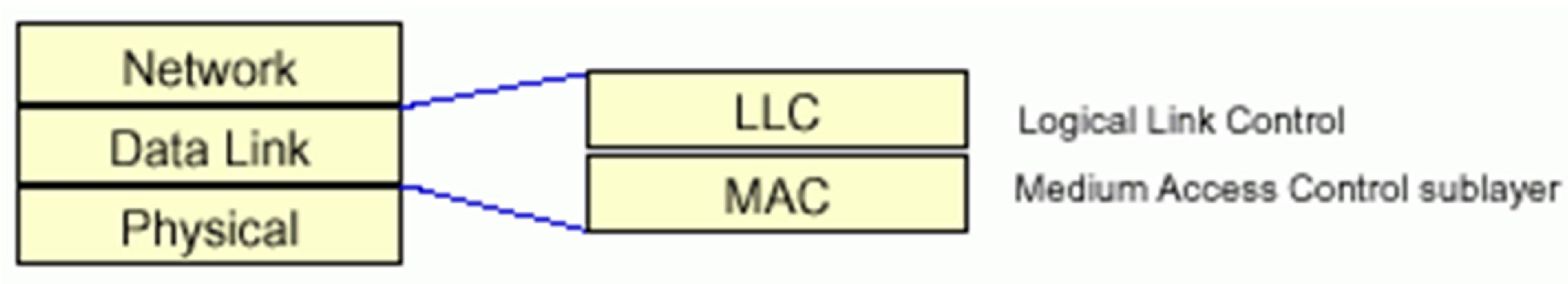
1. Virtual LANs allow hosts to be moved to different broadcast domains (subnets).
2. Point-to-Point protocol (PPP) is used for link and network layer configuration and framing
3. Multiprotocol Label Switching (MPLS) allows label-switched paths (LSPs) in IP networks.

IEEE LAN Standard

- 802.2 Logical Link Control
- 802.3 CSMA/CD (Ethernet)
- 802.4 Token Bus
- 802.5 Token Ring
- FDDI: Fiber Distributed Data Interface
- 802.11 Wireless LAN

IEEE 802.2 Logical Link Control

- Frame format of IEEE Standard does not specify upper layer protocol.
- LLC is used to specify upper layer protocol.



IEEE 802.5 Token Ring

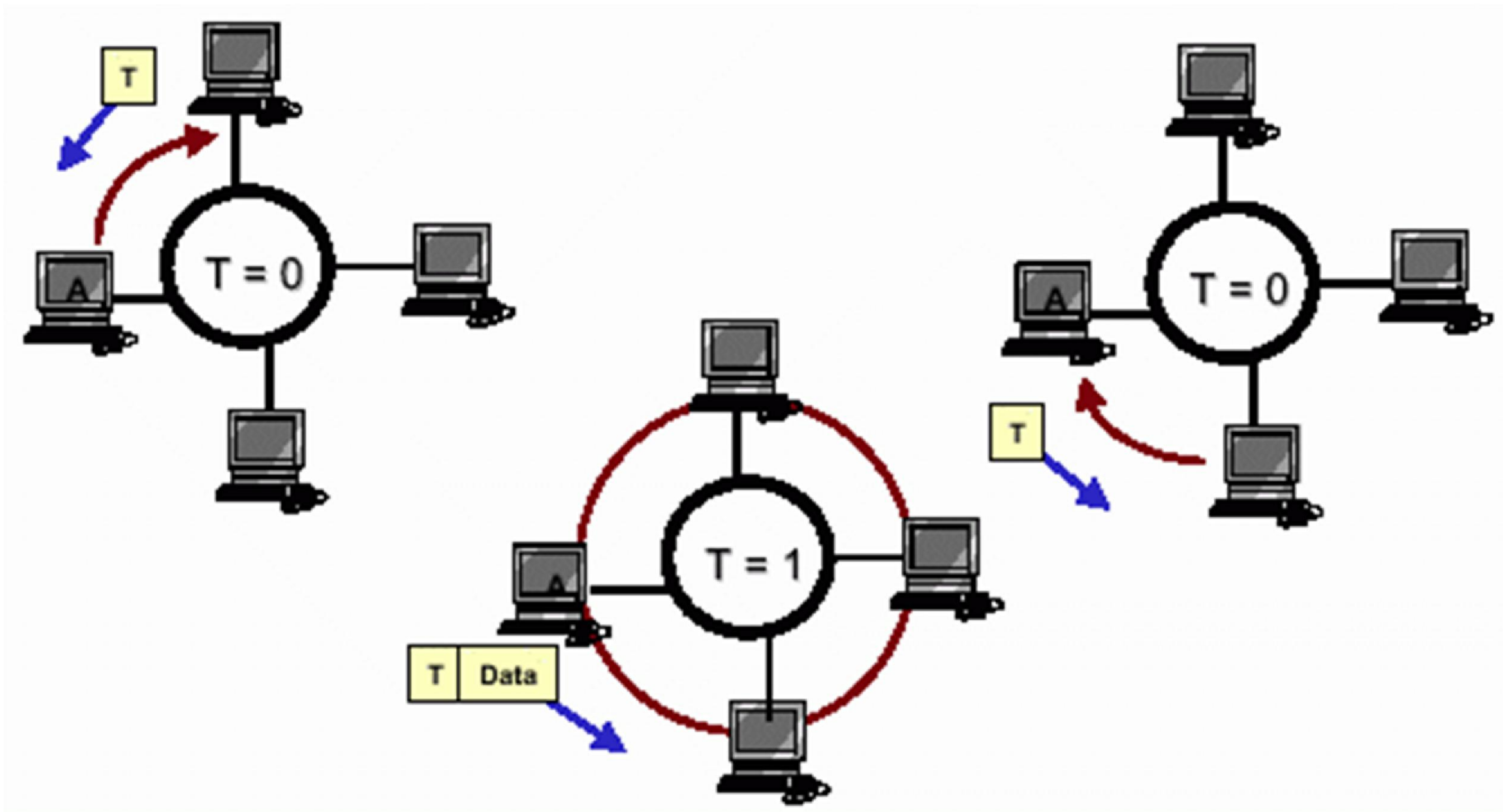
- Developed by IBM
- Use “token” to identify which node can transmit data

A Token Ring network is a local area network (LAN) in which all computers are connected in a ring or star topology and a bit- or token-passing scheme is used in order to prevent the collision of data between two computers that want to send messages at the same time. The Token Ring protocol is the second most widely-used protocol on local area networks after Ethernet. The IEEE 802.5 Token Ring technology provides for data transfer rates of either 4 or 16 megabits per second. Very briefly, here is how it works:

How Token Ring works?

1. Empty information frames are continuously circulated on the ring.
2. When a computer has a message to send, it inserts a token in an empty frame (this may consist of simply changing a 0 to a 1 in the token bit part of the frame) and inserts a message and a destination address in the frame.
3. The frame is then examined by each successive workstation. If the workstation sees that it is the destination for the message, it copies the message from the frame and changes the token back to 0.
4. When the frame gets back to the originator, it sees that the token has been changed to 0 and that the message has been copied and received. It removes the message from the frame.
5. The frame continues to circulate as an "empty" frame, ready to be taken by a workstation when it has a message to send.

Token Ring Operation

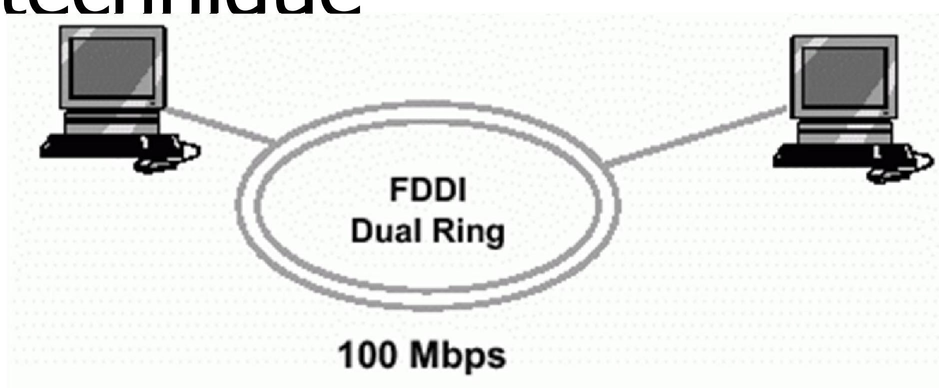


IEEE 802.4 Token Bus

- Same technique as Token Ring but implement in bus topology
- Because of complexity of implementation, token bus is not a popular.

FDDI

- Fiber Distributed Data Interface
- 100 Mbps
- LAN and MAN application
- Use Token Ring technique
- Dual rings



FDDI *V*s. Token Ring

Similarities:

(1) FDDI uses a rotating ring setup in the same way as the token ring protocol.

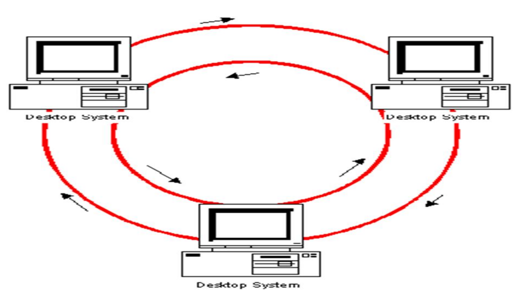
(2) FDDI's ring operation is basically very similar to the Token Ring early release operation in the way that tokens are passed on the network.

Differences:

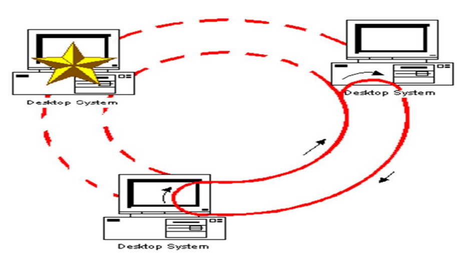
(1) As opposed to Token Ring's single ring, FDDI, uses two to achieve better reliability.

(2) FDDI uses a timed token protocol (fixed time to token handle) whereas Token Ring uses priority/ reservation token access.

(3) - In a basic Token Ring network, at any instant there is a single active ring monitor which supplies the master clock for the ring, whereas in FDDI this approach isn't ideal because of the high data rates. Instead, each ring interface has its own local clock, and outgoing data is transmitted using this clock.

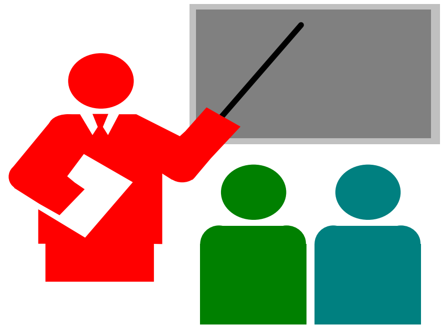


FDDI - all stations functioning



FDDI - one station is down

Summary



1. CRC uses mod-2 division using polynomial representation for binary numbers
2. IEEE 802.3 uses a *truncated binary exponential backoff*.
3. Address Resolution Protocol (ARP) is used to find the MAC address for a given IP address and vice versa.
4. PPP is used for configuration and framing on point-to-point links
5. MPLS allows virtual circuits (LSPs) on IP networks.