Chapter 4

The Medium Access Control Sublayer

The Channel Allocation Problem

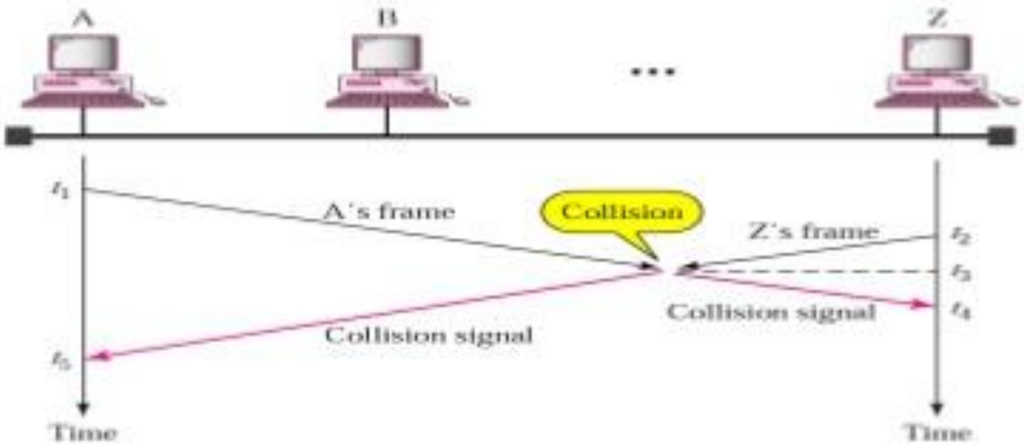
- Static Channel Allocation in LANs and MANs
- Dynamic Channel Allocation in LANs and MANs

Dynamic Channel Allocation in LANs and MANs

1. Station Model.
2. Single Channel Assumption.
3. Collision Assumption.
4. (a) Continuous Time.
   (b) Slotted Time.
5. (a) Carrier Sense.
   (b) No Carrier Sense.

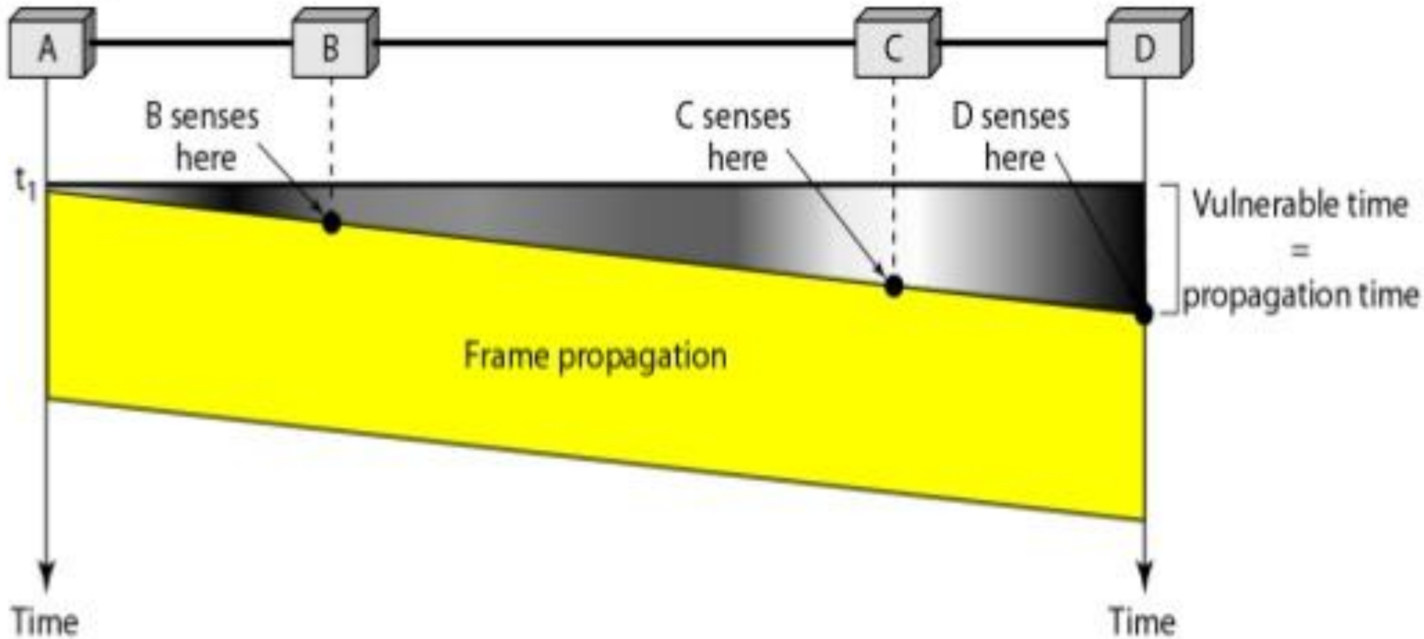
Random Access – Carrier Sense Multiple Access (CSMA)

- To improve performance, avoid transmissions that are certain to cause collisions
- Based on the fact that in LAN propagation time is **very small**
- ➔ If a frame was sent by a station, All stations knows immediately so they can **wait before start sending**
  - ➔ A station with frames to be sent, should **sense the medium** for the presence of another transmission (carrier) before it starts its own transmission
- This can **reduce** the possibility of collision but it <u>cannot eliminate</u> it.
  - Collision can only happen when more than one station begin transmitting within a short time (the **propagation time** period)



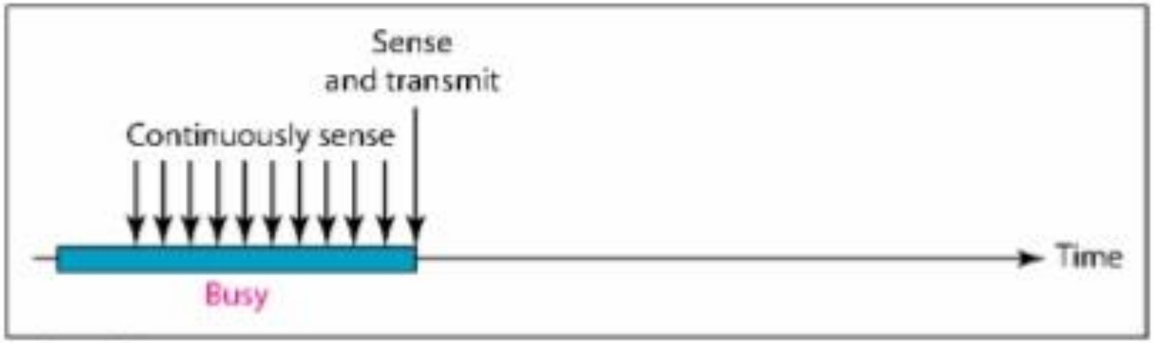
Random Access – Carrier Sense Multiple Access (CSMA)

- Vulnerable time for CSMA is the **maximum propagation time**
- The longer the propagation delay, the worse the performance of the protocol because of the above case.



1-persistent CSMA

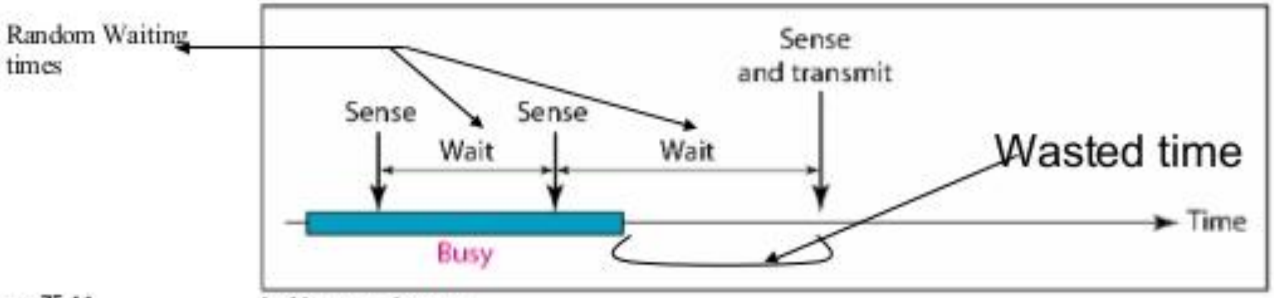
- To avoid idle channel time, 1-persistent protocol used
- Station wishing to transmit listens to the medium:
  1. If medium idle, **transmit** immediately;
  2. If medium busy, **continuously listen** until medium becomes idle; then transmit immediately with probability 1
- Performance
  - 1-persistent stations are **selfish**
  - If two or more stations becomes ready at the same time, **collision guaranteed**



a. 1-persistent

Nonpersistent CSMA

- A station with frames to be sent, should sense the medium
  1. If medium is idle, **transmit**; otherwise, go to 2
  2. If medium is busy, (**backoff**) wait a ***random* amount of time** and repeat **1**
- Non-persistent Stations are **deferential (respect others)**
- Performance:
  - Random delays reduces probability of collisions because two stations with data to be transmitted will wait for different amount of times.
  - Bandwidth is **wasted** if waiting time (backoff) is large because medium will remain idle following end of transmission even if one or more stations have frames to send

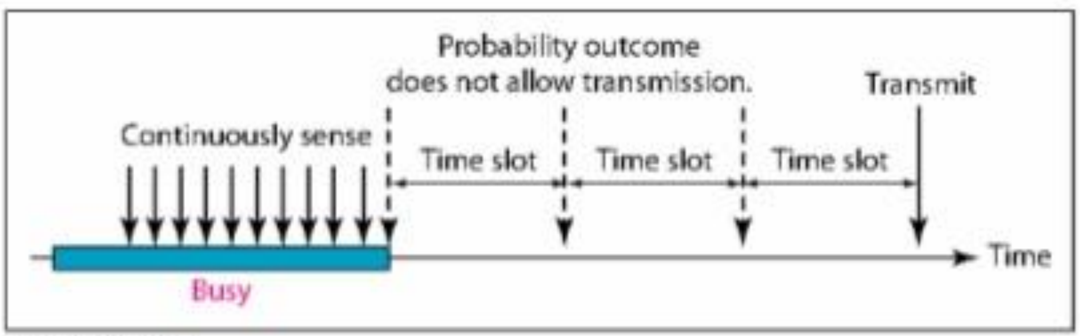


b. Nonpersistent

P-persistent CSMA

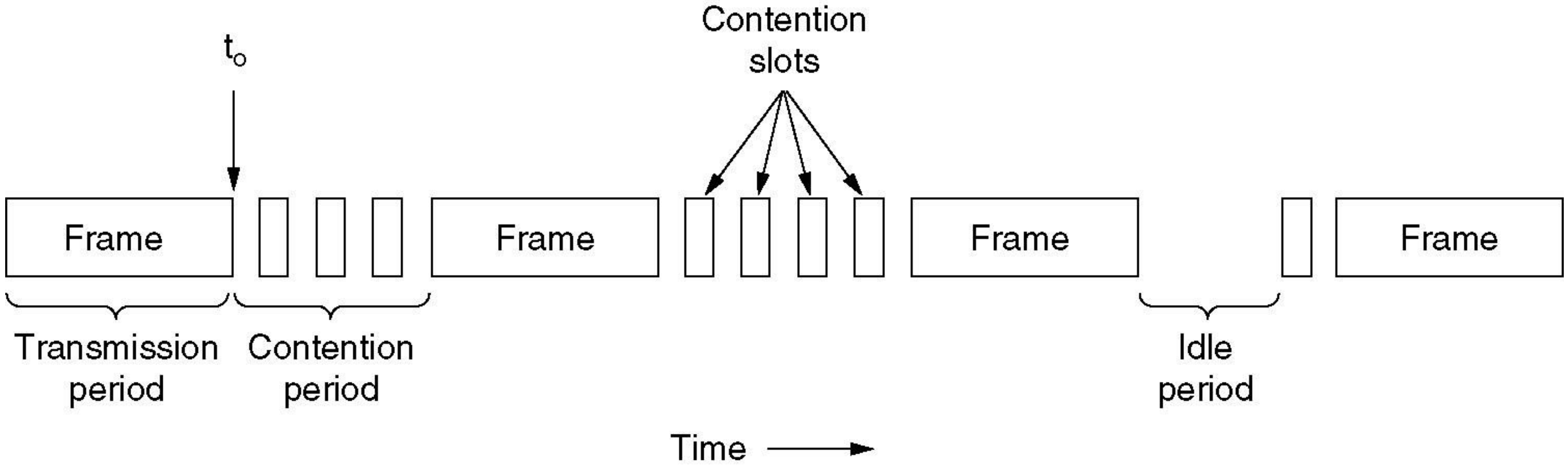
- Time is divided to slots where each Time unit (slot) typically equals **maximum propagation delay**
- Station wishing to transmit listens to the medium:

1. If medium idle,
   - transmit with probability (**p**), OR
   - wait **one time unit (slot)** with probability (**1 – p**), then repeat 1.
2. If medium busy, **continuously listen until idle** and repeat step **1**
3. Performance
   - Reduces the possibility of collisions like **nonpersistent**
   - Reduces channel idle time like **1-persistent**



c. p-persistent

CSMA with Collision Detection



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

Figure 12.12 *Collision of the first bit in CSMA/CD*

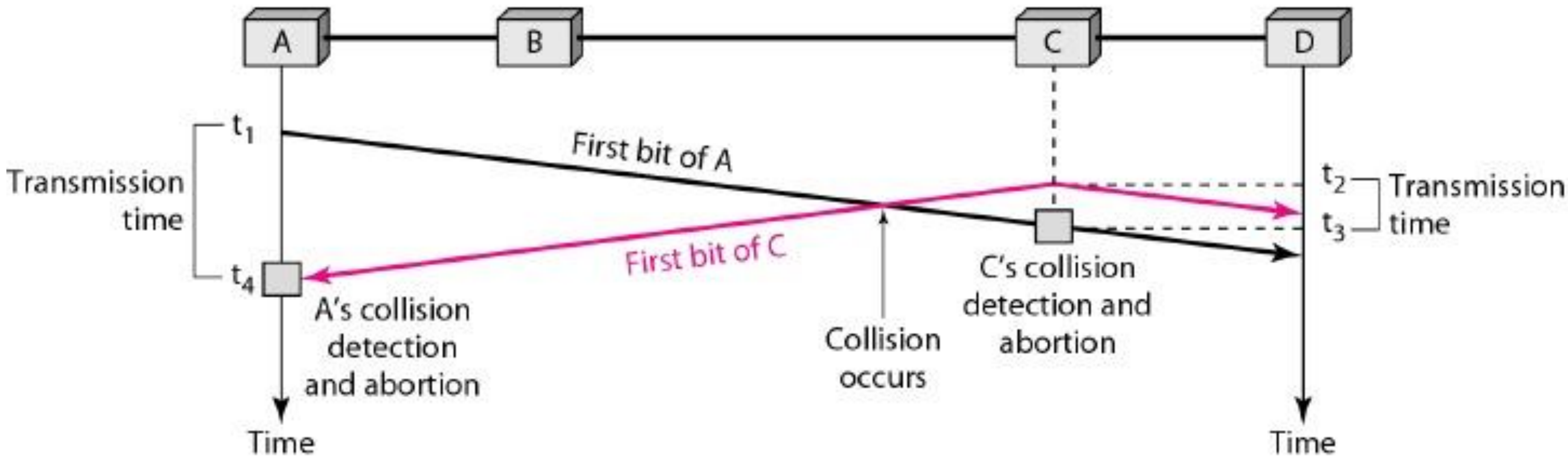
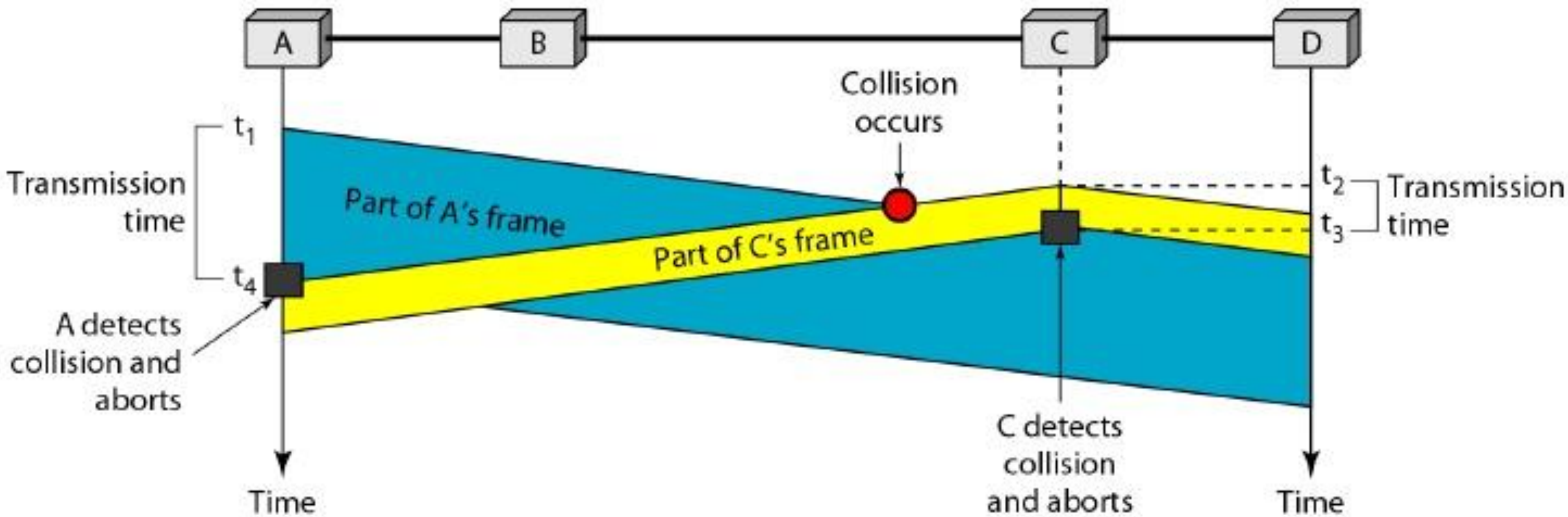


Figure 12.13 *Collision and abortion in CSMA/CD*



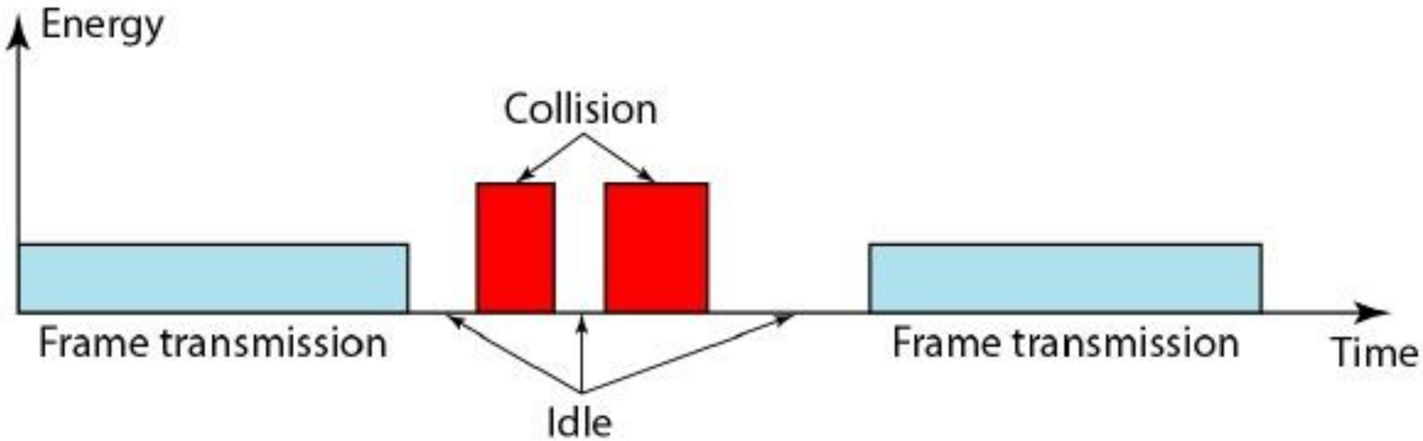
Example 12.5

A network using CSMA/CD has a bandwidth of 10 Mbps. If the maximum propagation time (including the delays in the devices and ignoring the time needed to send a jamming signal, as we see later) is 25.6 μs, what is the minimum size of the frame?

Solution

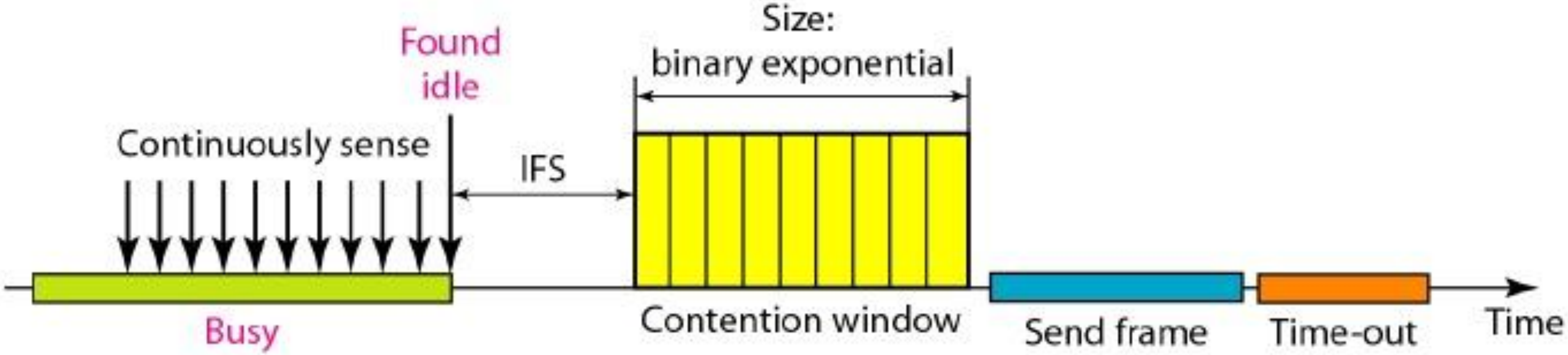
The frame transmission time is $T_{fr} = 2 \times T_p = 51.2\ \mu s$. This means, in the worst case, a station needs to transmit for a period of 51.2 μs to detect the collision. The minimum size of the frame is 10 Mbps × 51.2 μs = 512 bits or 64 bytes. This is actually the minimum size of the frame for Standard Ethernet.

Figure 12.15 ***Energy level during transmission, idleness, or collision***



12.27

Figure 12.16 *Timing in CSMA/CA*



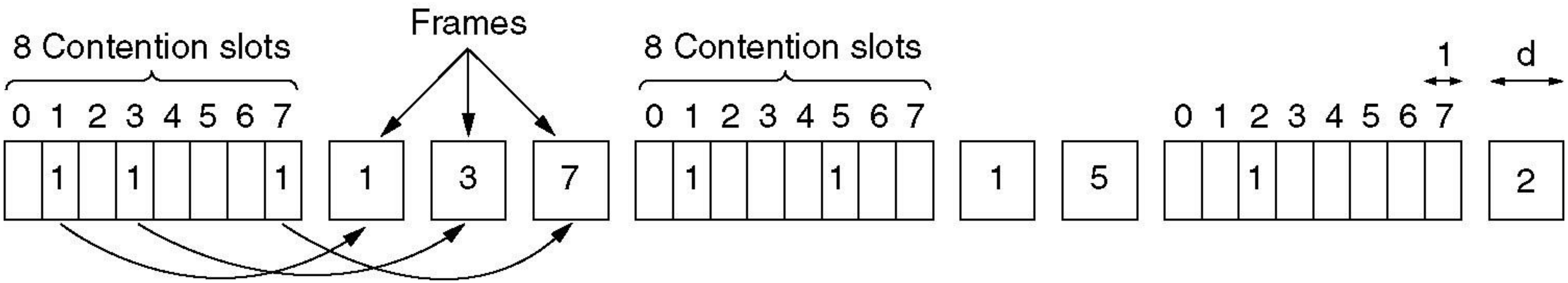
Note

In CSMA/CA, the IFS can also be used to define the priority of a station or a frame.

Note

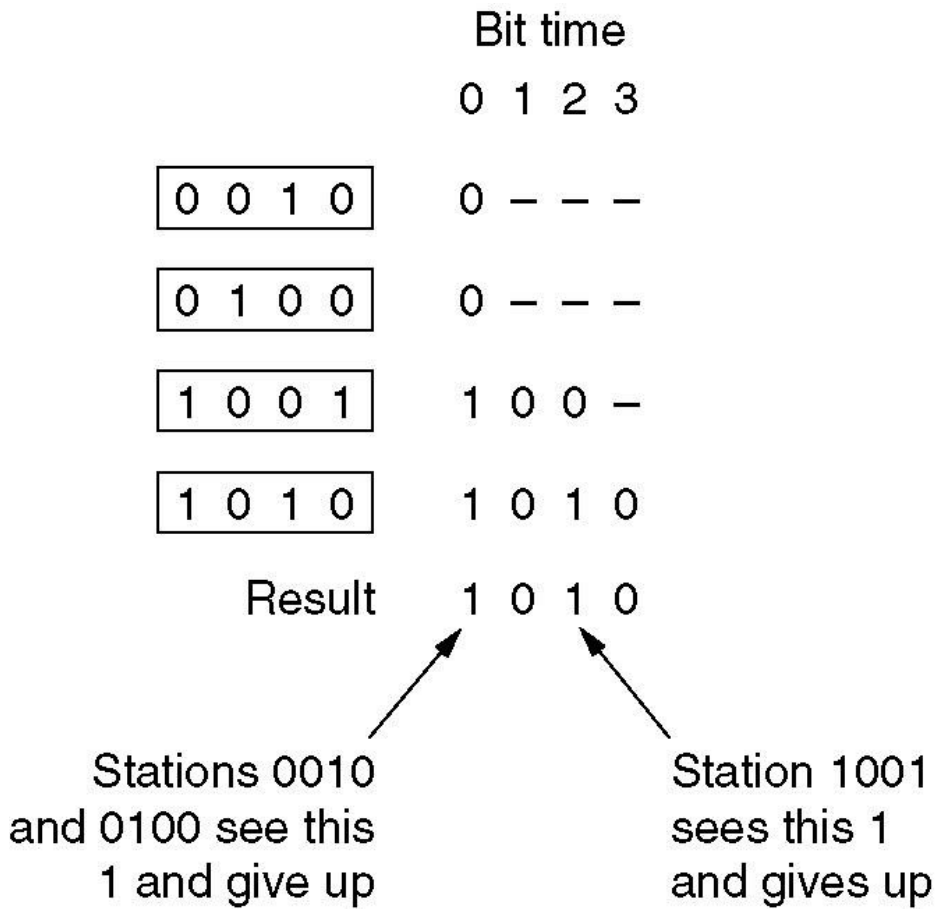
In CSMA/CA, if the station finds the channel busy, it does not restart the timer of the contention window; it stops the timer and restarts it when the channel becomes idle.

Collision-Free Protocols



The basic bit-map protocol.

Collision-Free Protocols (2)



The binary countdown protocol. A dash indicates silence.

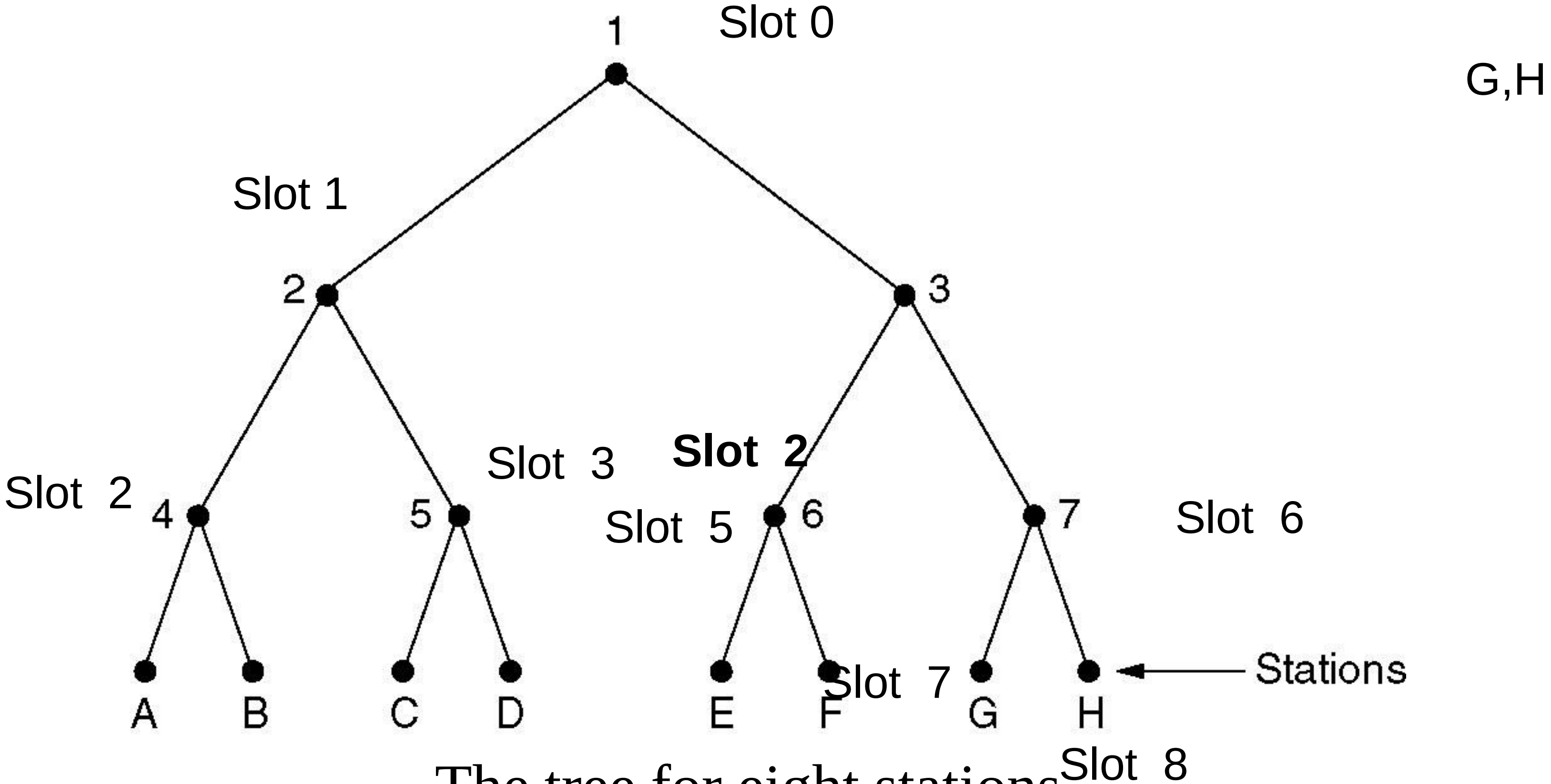
Improvements to the basic algorithm

Mok and Ward (1979) have described a variation of binary countdown

They suggest using virtual station numbers, with the virtual station numbers from 0 up to and including the successful station being circularly permuted after each transmission, in order to give higher priority to stations that have been silent unusually long.

For example, if stations *C, H, D, A, G, B, E, F have priorities 7, 6, 5, 4, 3, 2, 1, and 0, respectively, then a successful transmission by D puts it at the end of the list, giving a priority order of C, H, A, G, B, E, F, D. Thus, C remains virtual station 7, but A moves up from 4 to 5 and D drops from 5 to 0. Station D will now only be able to acquire the channel if no other station wants it.*

Limited contention protocols Adaptive Tree Walk Protocol



The tree for eight stations.

If the *q ready stations are uniformly distributed, the expected number of them below a specific node at level i is just* $q*2^{-i}$. *Intuitively, we would expect the optimal level to begin searching the tree as the one at which the mean number of contending stations per slot is 1, that is, the level at which* $q*2^{-i} = 1$. *Solving this equation, we find that* $i = \log_2 q$.

Improvements to the basic algorithm

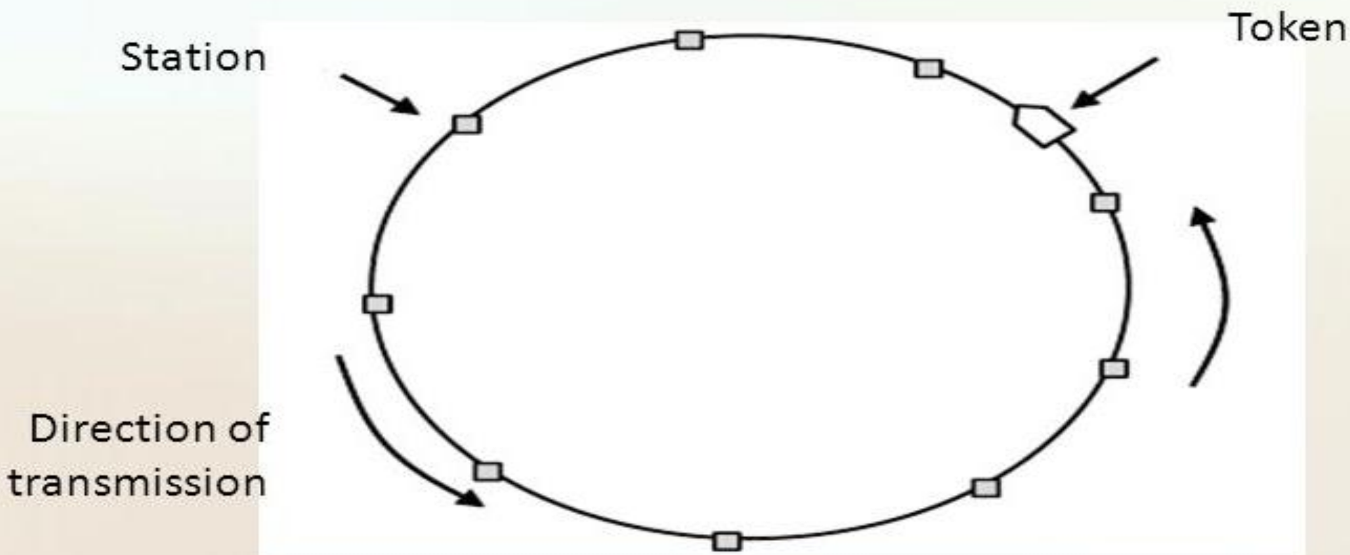
Bertsekas and Gallager (1992).

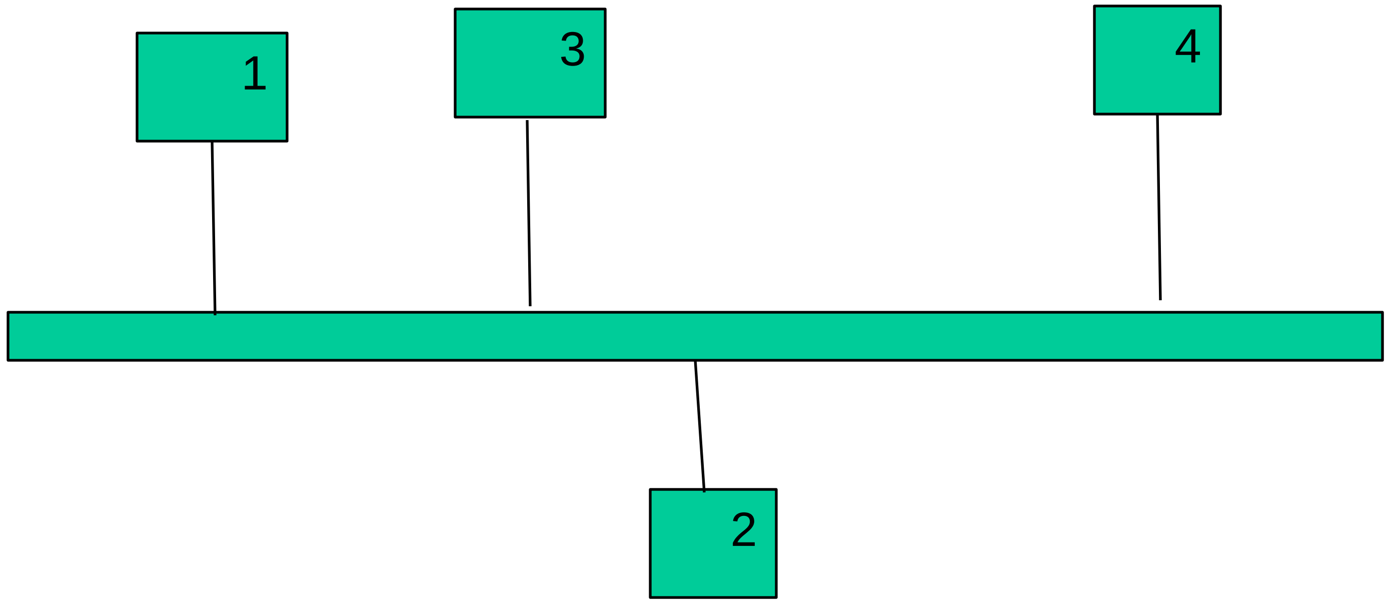
For example, consider the case of stations *G and H being the only ones wanting to transmit. At node 1 a collision will occur, so 2 will be tried and discovered idle. It is pointless to probe node 3 since it is guaranteed to have a collision (we know that two or more stations under 1 are ready and none of them are under 2, so they must all be under 3). The probe of 3 can be skipped and 6 tried next. When this probe also turns up nothing, 7 can be skipped and node G tried next.*

Collision-Free – Token Ring

Token sent round ring defines the sending order

- Station with token may send a frame before passing
- Idea can be used without ring too, e.g., token bus



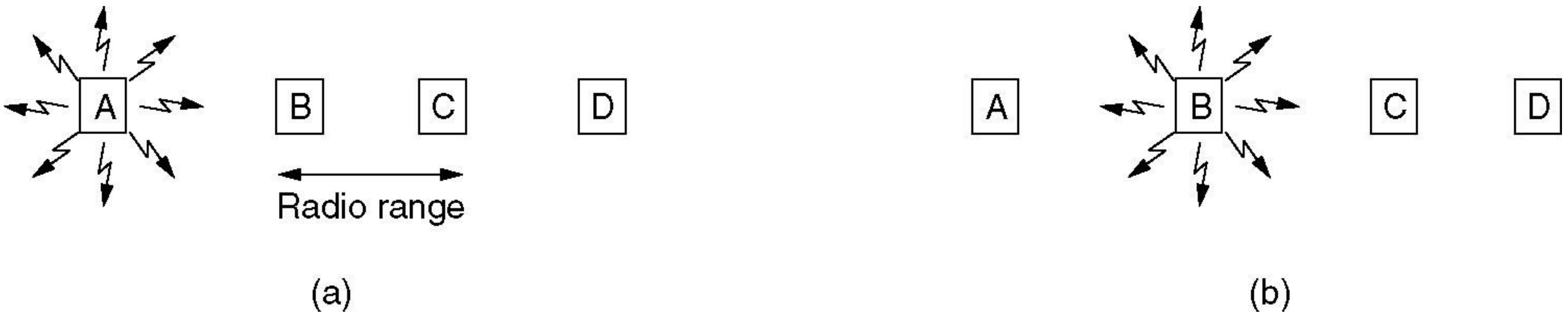


FDDI

WDMA

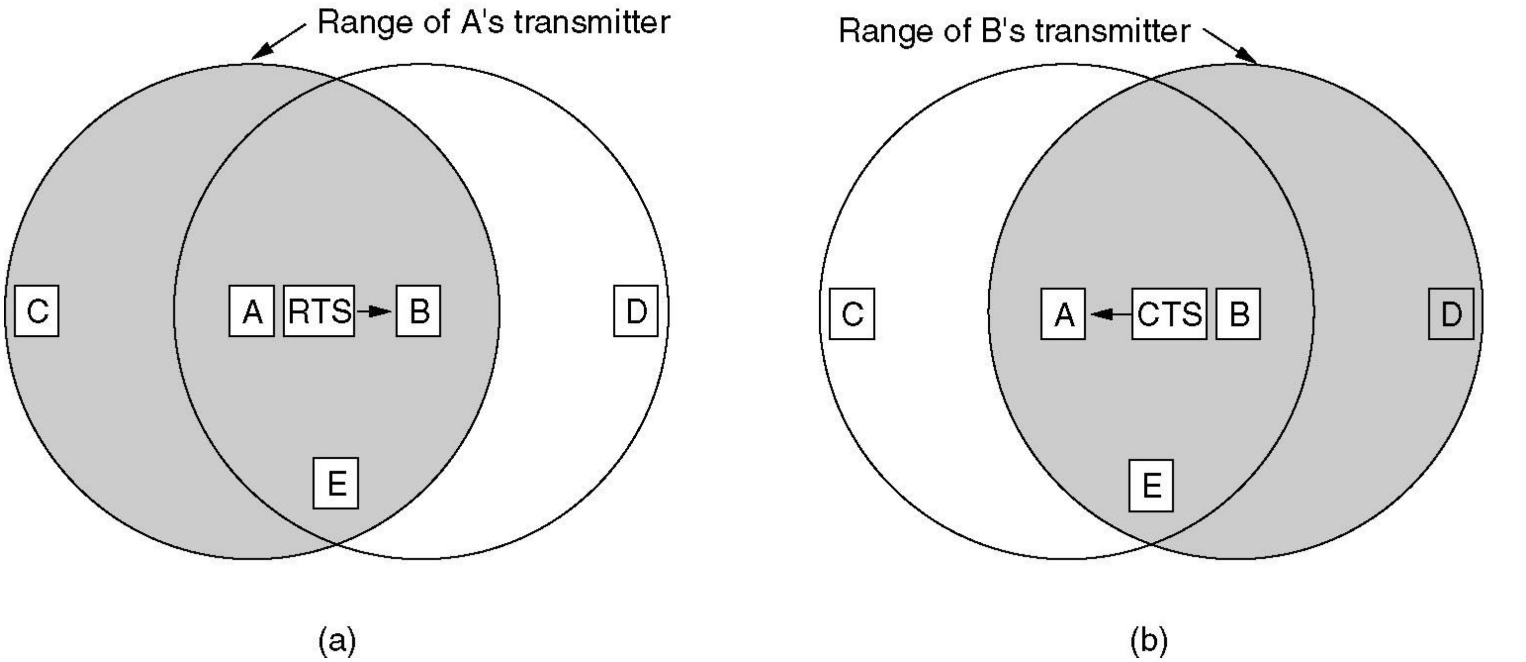
- Each station has:
  - A fixed-wavelength receiver for listening to its own control channel
  - A tunable transmitter for sending on other station's control channel
  - A fixed-wavelength transmitter for outputting data frames
  - A tunable receiver for selecting a data transmitter to listen to

Wireless LAN Protocols



A wireless LAN. (a) A transmitting. (b) B transmitting.

Wireless LAN Protocols (2)



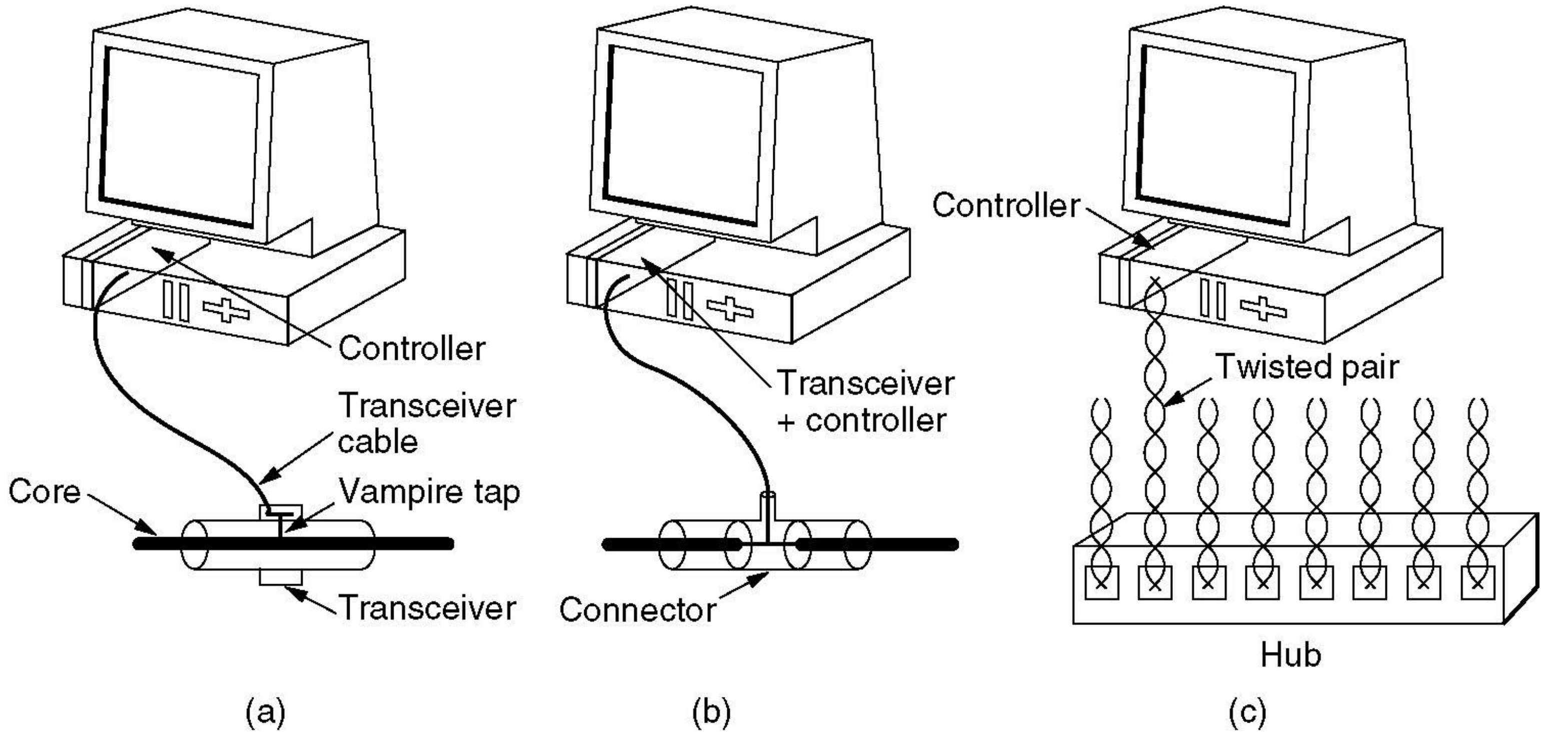
The MACA protocol. (a) A sending an RTS to B. (b) B responding with a CTS to A.

Ethernet Cabling

Name	Cable	Max. seg.	Nodes/seg.	Advantages
10Base5	Thick coax	500 m	100	Original cable; now obsolete
10Base2	Thin coax	185 m	30	No hub needed
10Base-T	Twisted pair	100 m	1024	Cheapest system
10Base-F	Fiber optics	2000 m	1024	Best between buildings

The most common kinds of Ethernet cabling.

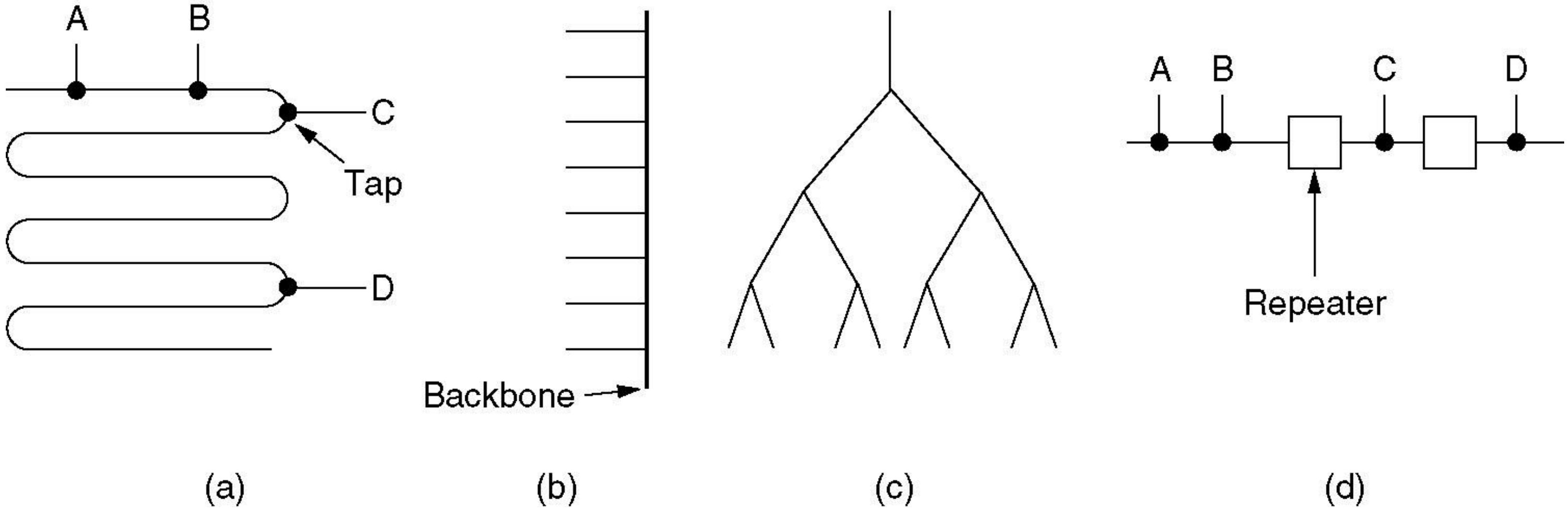
Ethernet Cabling (2)



Three kinds of Ethernet cabling.

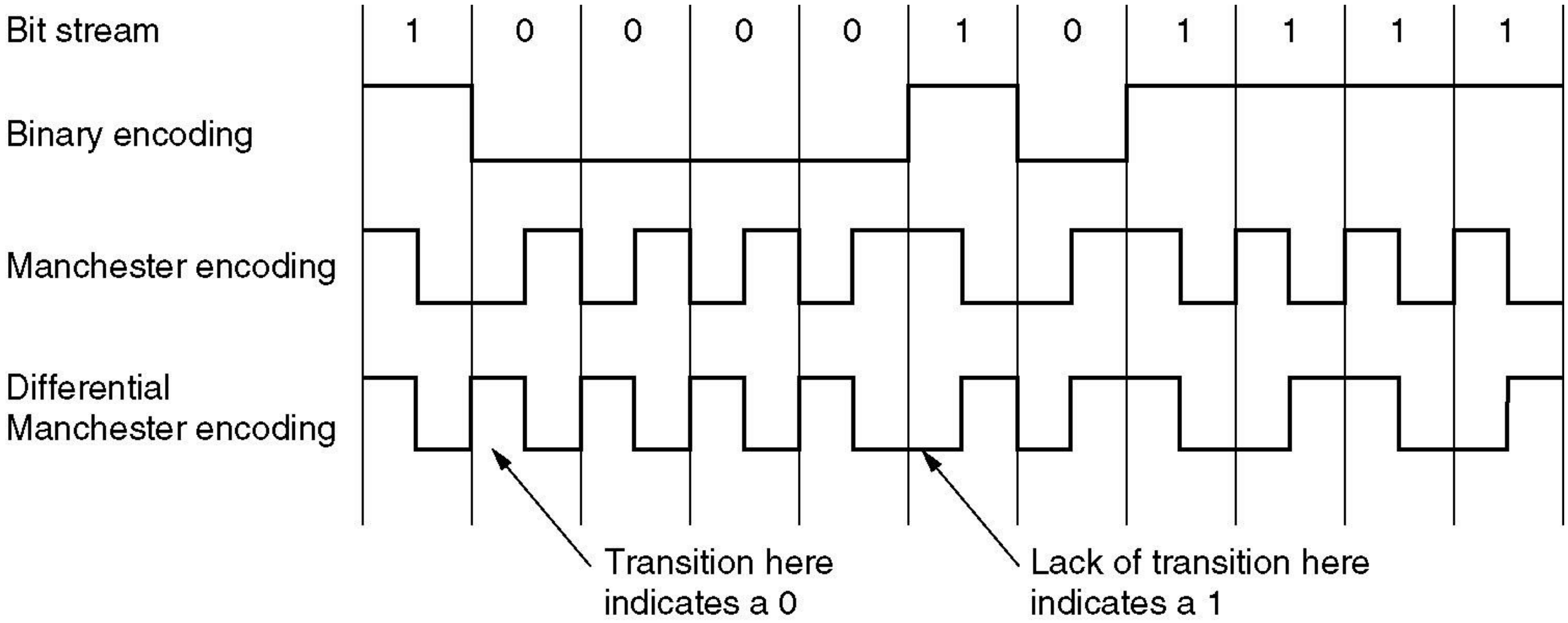
(a) 10Base5, (b) 10Base2, (c) 10Base-T.

Ethernet Cabling (3)



Cable topologies. (a) Linear, (b) Spine, (c) Tree, (d) Segmented.

Ethernet Cabling (4)



(a) Binary encoding, (b) Manchester encoding,
(c) Differential Manchester encoding.

Ethernet MAC Sublayer Protocol

Bytes	8	6	6	2	0-1500	0-46	4
(a)	Preamble	Destination address	Source address	Type	Data	Pad	Check-sum
(b)	Preamble SOF	Destination address	Source address	Length	Data	Pad	Check-sum

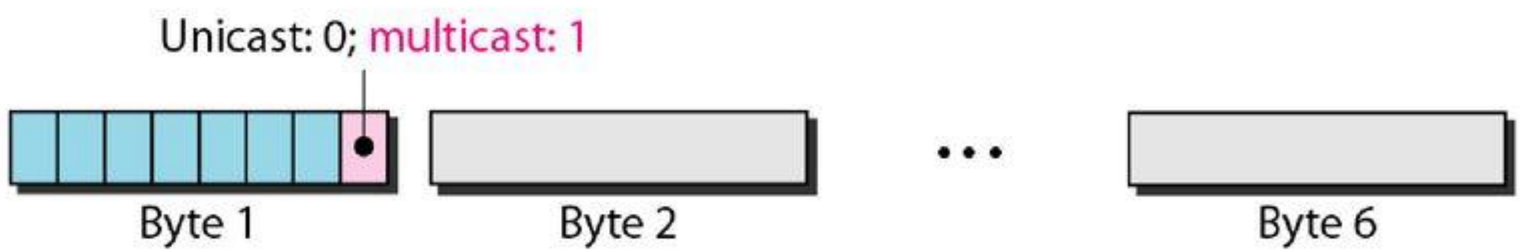
Frame formats. (a) DIX Ethernet, (b) IEEE 802.3.

1. addressing

Three types of addresses:

1. **Unicast MAC Address**: each host or each interface of a router is assigne unicast address. It allows each single transmitting device to send a pack to another single destination device. Unicasting means one-to-o communication. In the structure of Multicast MAC address the seco digit should be even. Example: A2:34:45:11:92:F1.

2. **Multicast MAC Address:** it allows a source device to send a packet to group of devices. Multicast means one-to-many communication. In t structure of Multicast MAC address the second digit should be od Example: A3:34:45:11:92:F1.



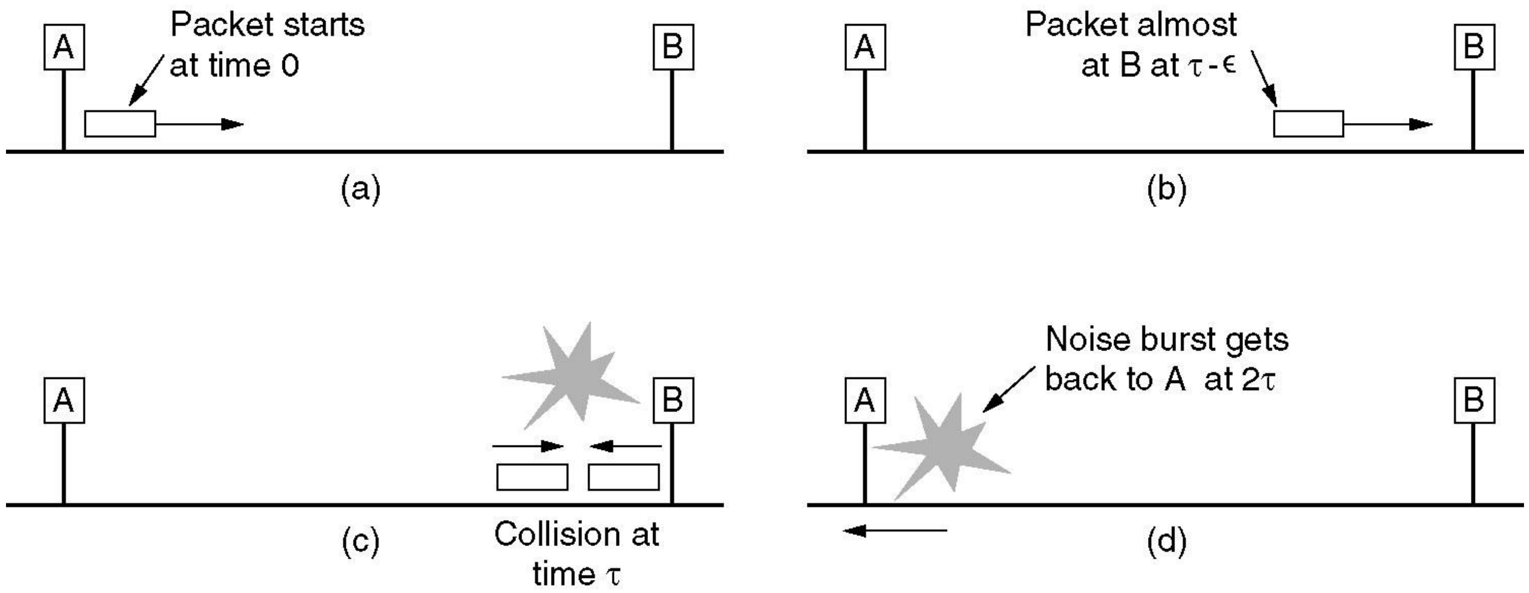
3. **Broadcast MAC Address**: A frame with a destination broadcast address sent to all entities in the link. Broadcasting means one-to communication. Example: FF:FF:FF:FF:FF:FF.

Show how the following address is sent out on line.
47:20:1B:2E:08:EE
01000111 0010 0000 00011011…. 11101110
Solution

The address is sent left-to-right, byte by byte; for each byte, it is sent right-to-Ieft, bit by bit, as
shown below:

🡐11100010 00000100 11011000 01110100 00010000
01110111

Ethernet MAC Sublayer Protocol (2)



Collision detection can take as long as 2τ.

The Binary Exponential Backoff Algorithm

After a collision, time is divided into discrete slots whose length is equal to the worst-case round-trip propagation time on the ether (2τ). To accommodate the longest path allowed by Ethernet, the slot time has been set to 512 bit times, or 51.2 μsec as mentioned above.

After the first collision, each station waits either 0 or 1 slot times before trying again. If two stations collide and each one picks the same random number, they will collide again.

After the second collision, each one picks either 0, 1, 2, or 3 at random and waits that number of slot times.

If a third collision occurs ,then the next time the number of slots to wait is chosen at random from the interval 0 to $2^3 - 1$.

The Binary Exponential Backoff Algorithm

In general, after *i collisions, a random number between 0 and* 2^i *- 1 is chosen, and that number of slots is skipped. However, after ten collisions have been reached, the randomization interval is frozen at a maximum of 1023 slots. After 16 collisions, the controller throws in the towel and reports failure back to the computer. Further recovery is up to higher layers.*

Fast Ethernet

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
100Base-FX	Fiber optics	2000 m	Full duplex at 100 Mbps; long runs

The original fast Ethernet cabling.

Fast Ethernet

Fast Ethernet was designed to compete with LAN protocols such as FDDI (Fiber Distributed Data Interface) or Fiber Channel.

IEEE created Fast Ethernet under the name 802.3u.

Fast Ethernet is backward-compatible with Standard Ethernet. It can transmit data 10 times faster at a rate of 100 Mbps

MAC: CSMA/CD for half duplex. Not needed in full duplex.

Auto nagotiation -It allows a station or a hub a range of capabilities. Auto negotiation allows two devices to negotiate the modeor data rate of operation.

Gigabit Ethernet

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

Gigabit Ethernet cabling.

Gigabit Ethernet

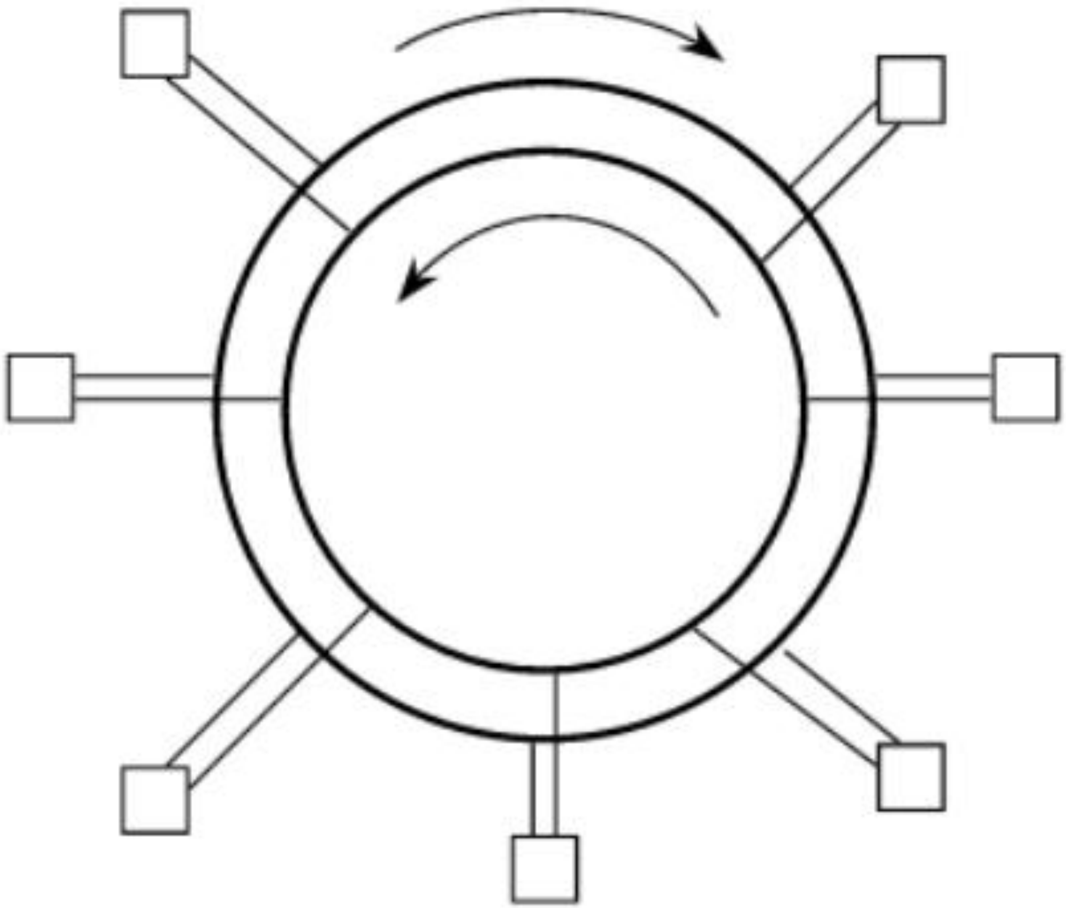
- The need for higher data rate resulted in the design of the Gigabit Ethernet (1000 Mbps).
- The IEEE committee calls the standard 802.3z.
- Upgraded to the data rate to 1 Gbps.
- Compatible with Standard or Fast Ethernet.
- Uses the same 48-bit address.
- Uses the same frame format.
- It permits to keep the same minimum and maximum frame lengths.
- It supports auto negotiation as defined in Fast Ethernet.
- For the star topology, there are two choices: half duplex and full duplex
- The access method is the same (CSMA/CD) for the half-duplex approach; mostly full duplex mode is used.

FDDI

a) The Fiber Distributed Data Interface (FDDI) specifies a 100-Mbps token-passing, dual-ring LAN using fiber-optic cable.

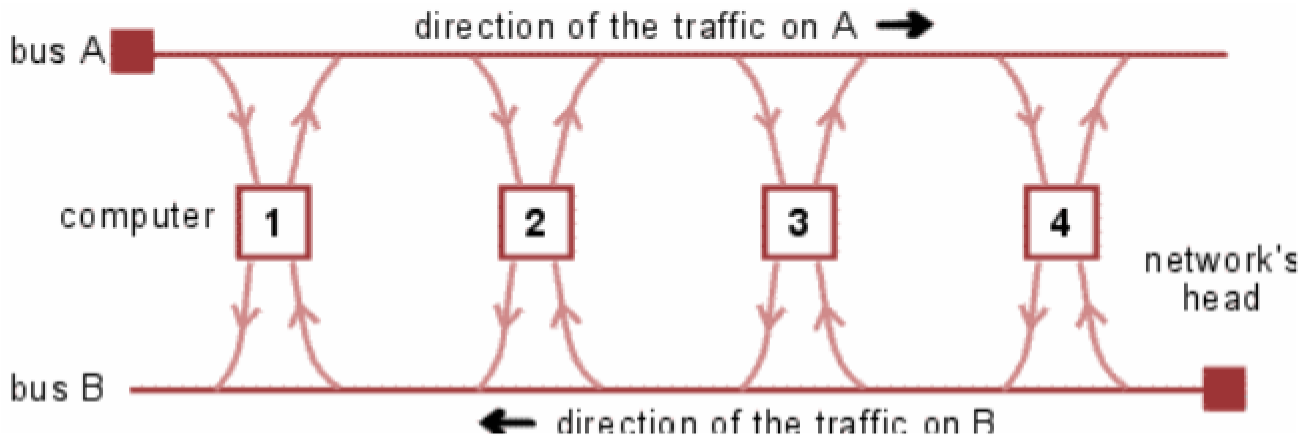
b) An FDDI network contains two token rings, one for possible backup in case the primary ring fails.

c) A FDDI dual ring supports up to 500 nodes per ring. The total maximum length for each of the cable rings is 100 km with nodes up to 2 km apart(max limit)on multimode fiber, and 10 km apart on single-mode fiber.

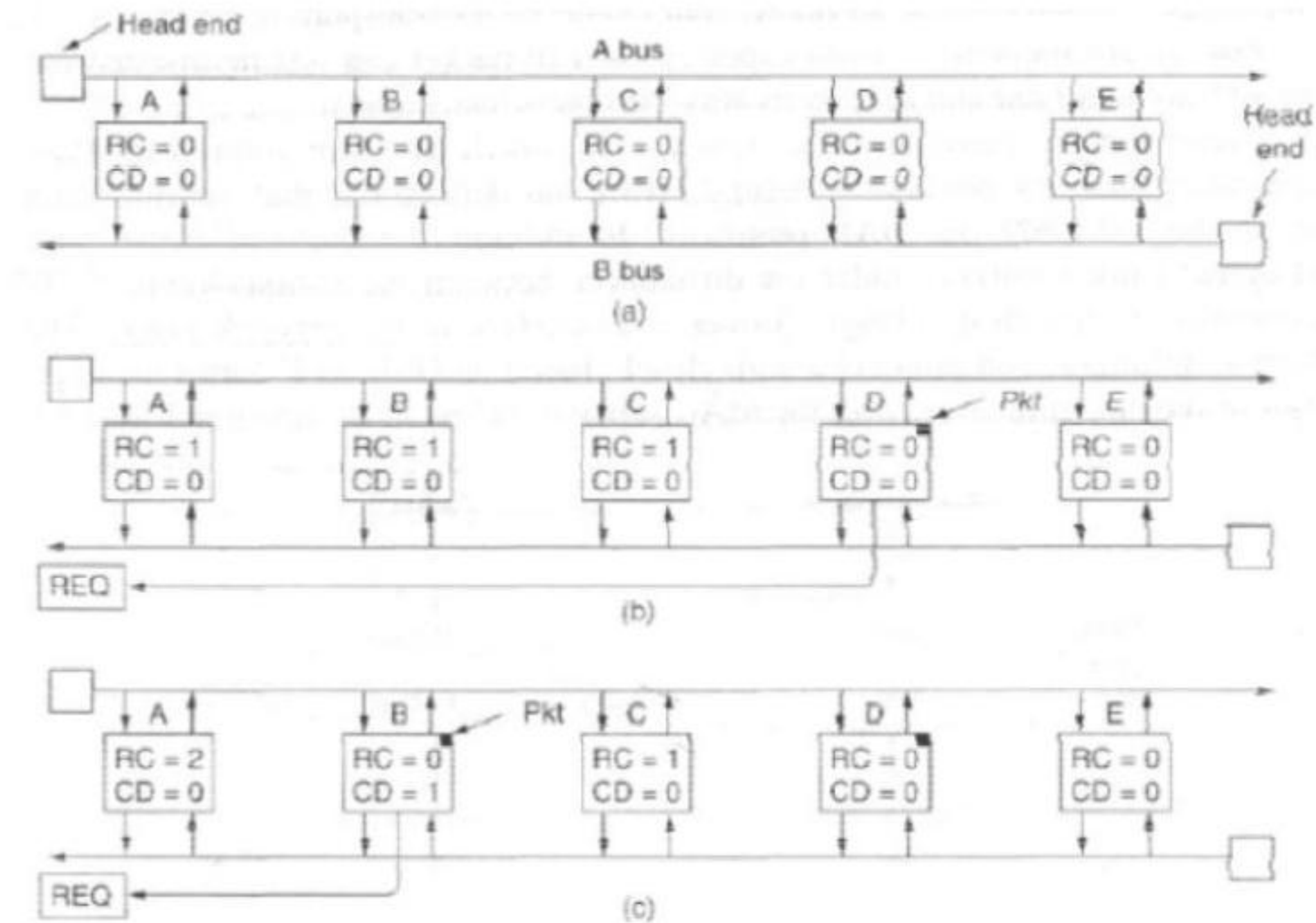


IEEE 802.6

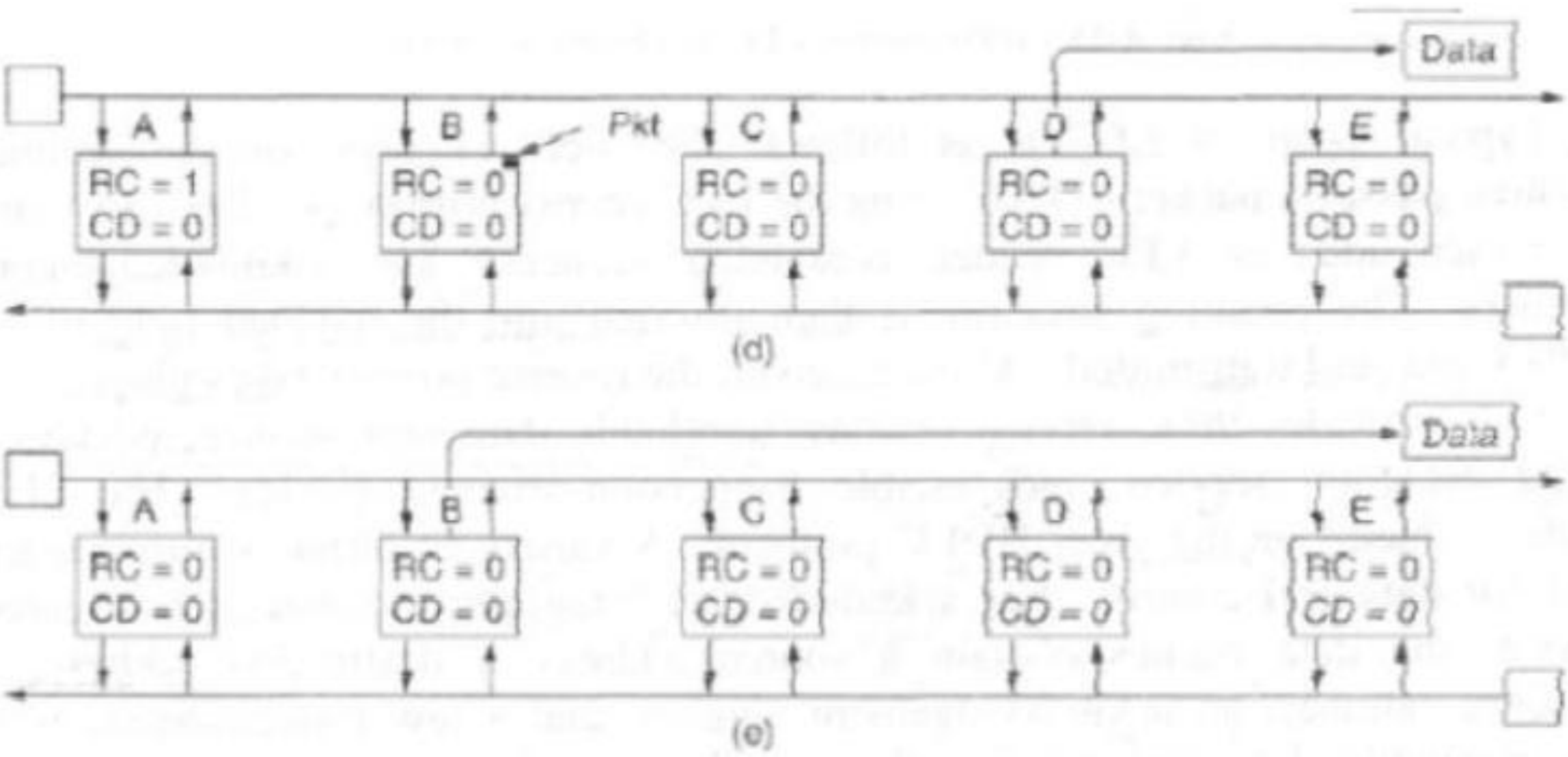
It is IEEE defined a MAN standard.
Distributed Queue Data Interface (DQDB).



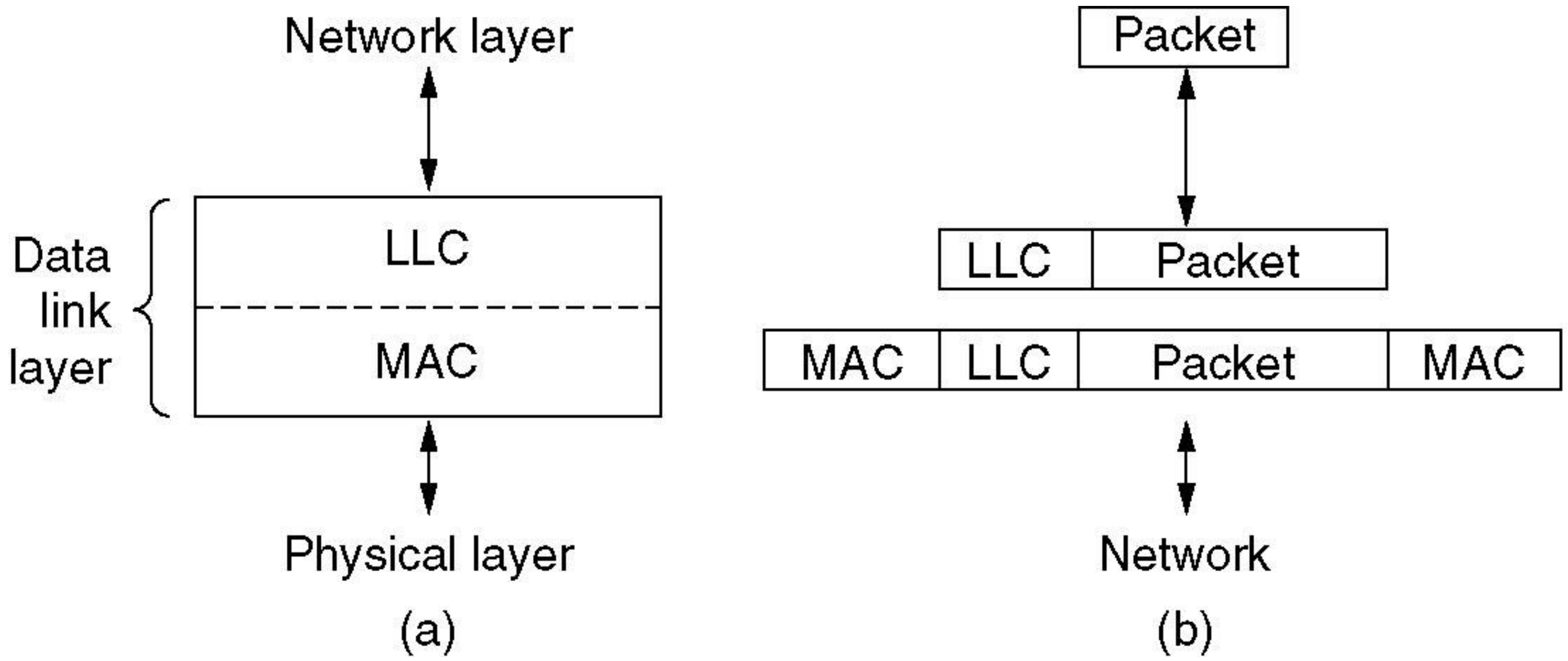
802.6


Head end
A bus
A
B
C
D
E
RC = 0
CD = 0
Head end
B bus
(a)
RC = 1
CD = 0
Pkt
REQ
(b)
RC = 2
CD = 0
RC = 0
CD = 1
Pkt
REQ
(c)

802.6


Data
A
B
Pkt
C
D
E
RC = 1
CD = 0
RC = 0
CD = 0
RC = 0
CD = 0
RC = 0
CD = 0
RC = 0
CD = 0
(d)
Data
A
B
C
D
E
RC = 0
CD = 0
RC = 0
CD = 0
RC = 0
CD = 0
RC = 0
CD = 0
RC = 0
CD = 0
(e)

IEEE 802.2: Logical Link Control



(a) Position of LLC. (b) Protocol formats.

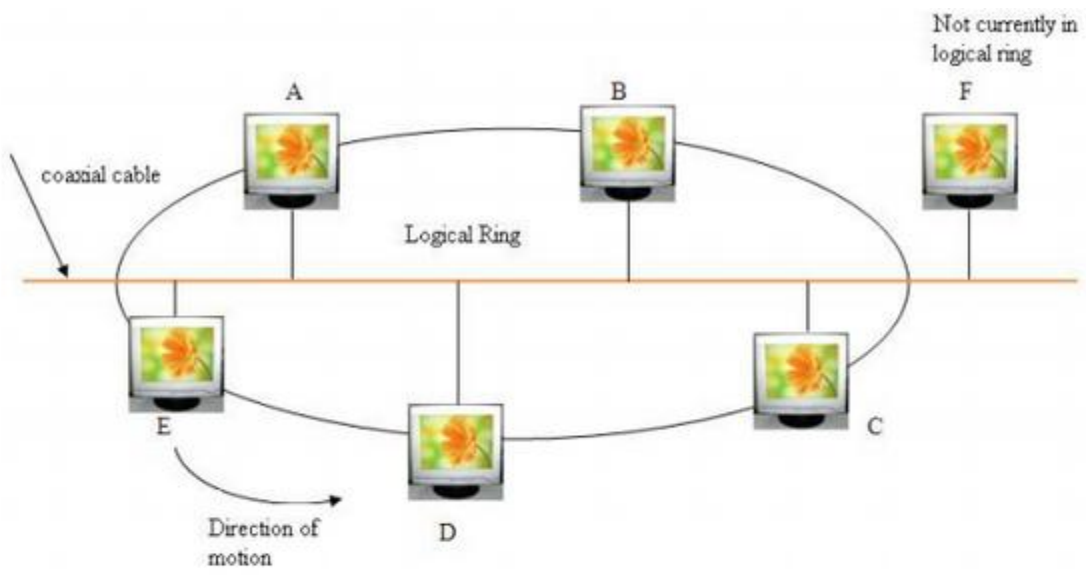
IEEE 802.2: Logical Link Control

The LLC header contains three fields: a destination access point, a source access point, and a control field.
The access points tell which process the frame came from and where it is to be delivered, replacing the DIX *Type field.*
The control field contains sequence and acknowledgement numbers.

IEEE 802.4

The 802.4 IEEE standard defines the Token Bus protocol for a token-passing access method on a bus topology.

IEEE 802.4 token bus networks are constructed with 75-ohm broadband coaxial cable using a bus topology employs analogue modulation. Speeds of 1, 5 and 10 Mbps are possible.



802.5

The IEEE 802.5 standard specifies the characteristics for Token Ring networks.

Token Ring was introduced by IBM in the mid-1980s and quickly became the network topology of choice until the rise in popularity of Ethernet.

The following is a list of the specific characteristics specified in the 802.5 standard:

Speed The 802.5 Token Ring specifies network speeds **of 4 and 16Mbps**.

Topology Token Ring networks use a **logical ring topology and most often a physical star.**

Media Token Ring networks use **unshielded twisted pair cabling or shielded twisted pair.**

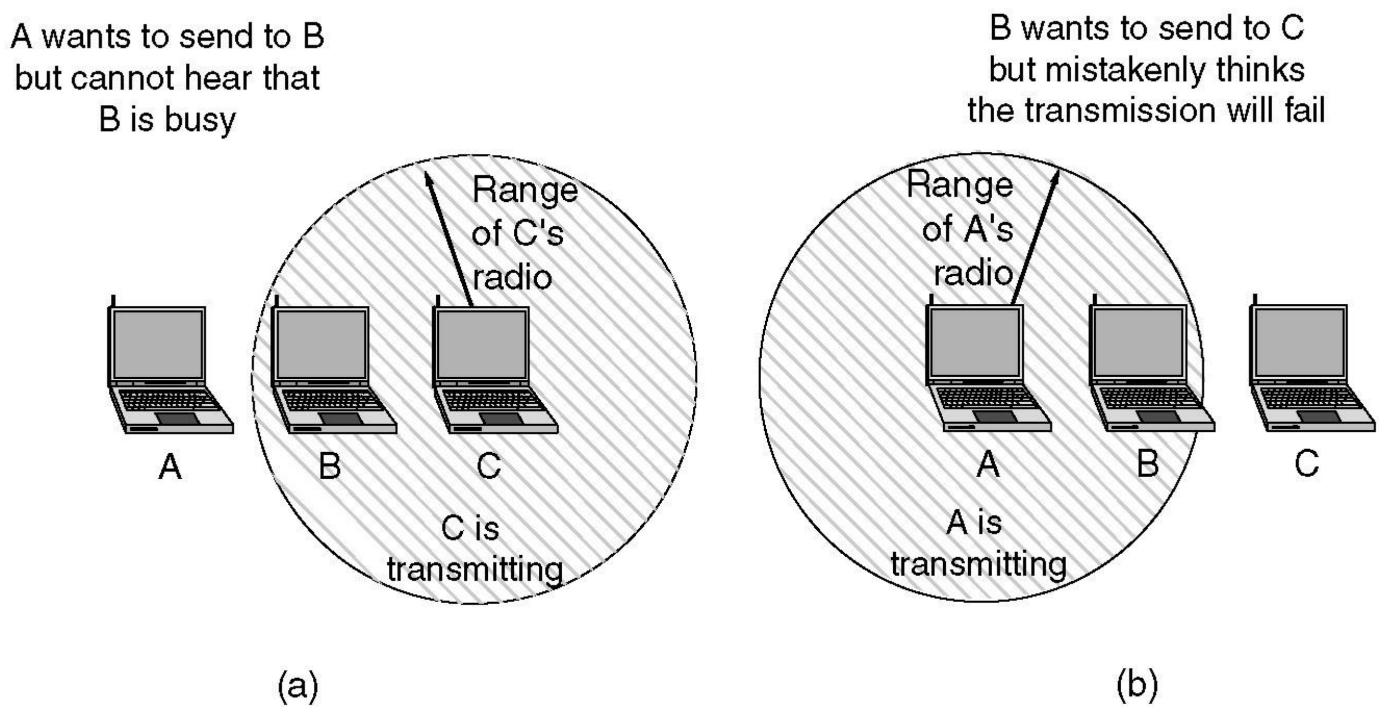
Encoding scheme used is **differential Manchester.**

Access method 802.5 specifies an access method known **as token passing**.

Wireless LANs

- The 802.11 Protocol Stack
- The 802.11 Physical Layer
- The 802.11 MAC Sublayer Protocol
- The 802.11 Frame Structure
- Services

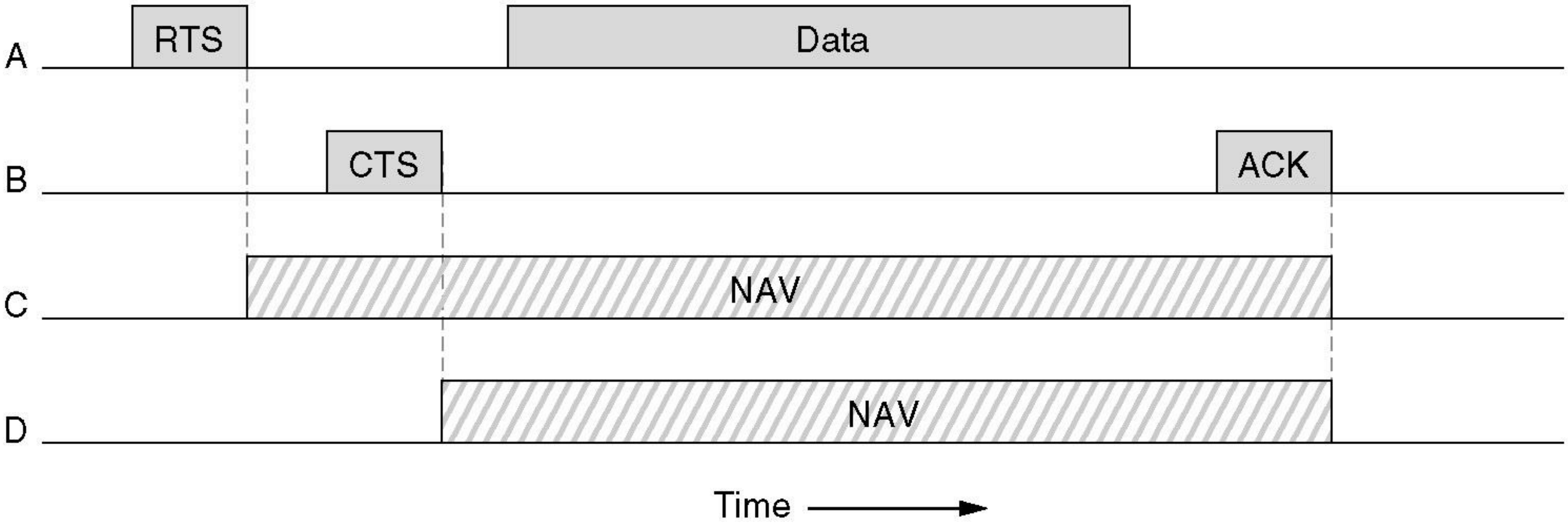
The 802.11 MAC Sublayer Protocol



(a) The hidden station problem.

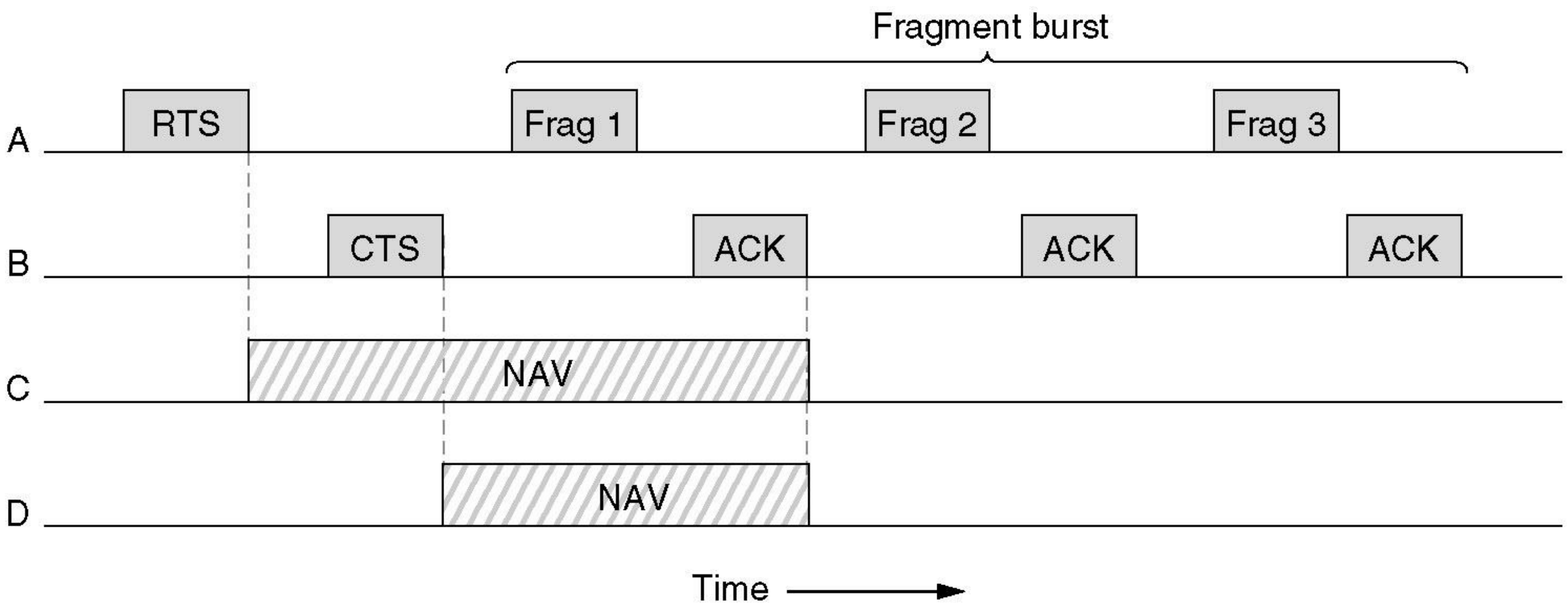
(b) The exposed station problem.

The 802.11 MAC Sublayer Protocol (2)



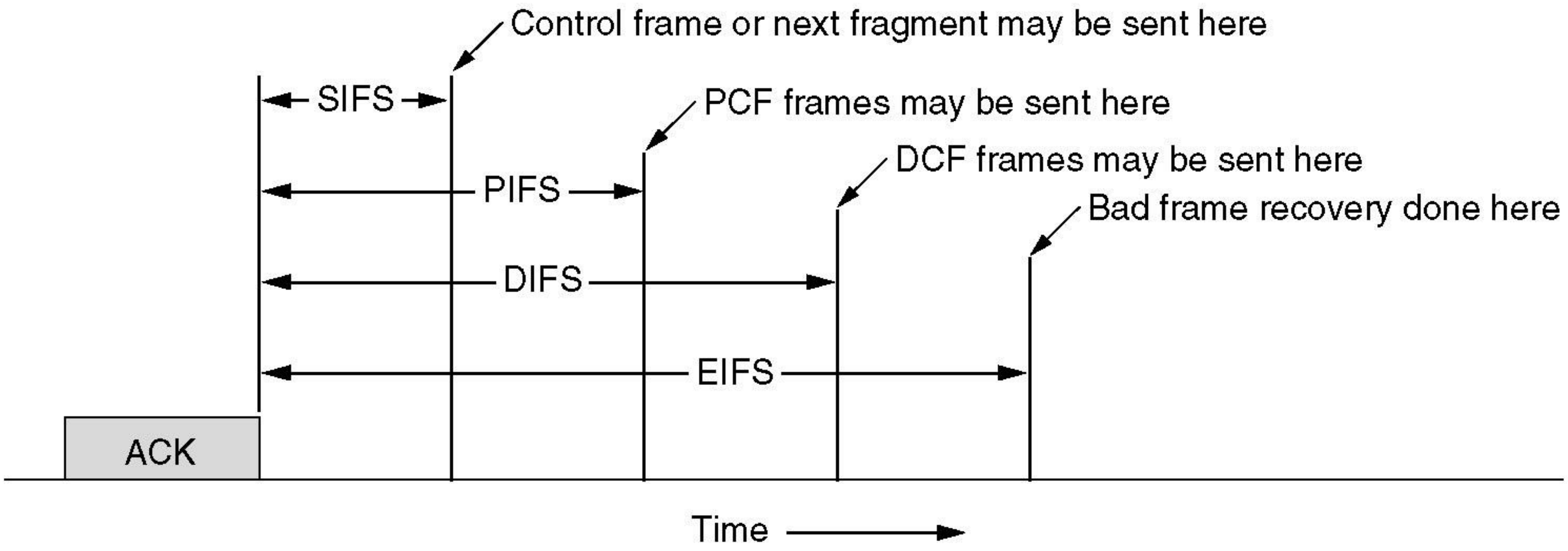
The use of virtual channel sensing using CSMA/CA.

The 802.11 MAC Sublayer Protocol (3)



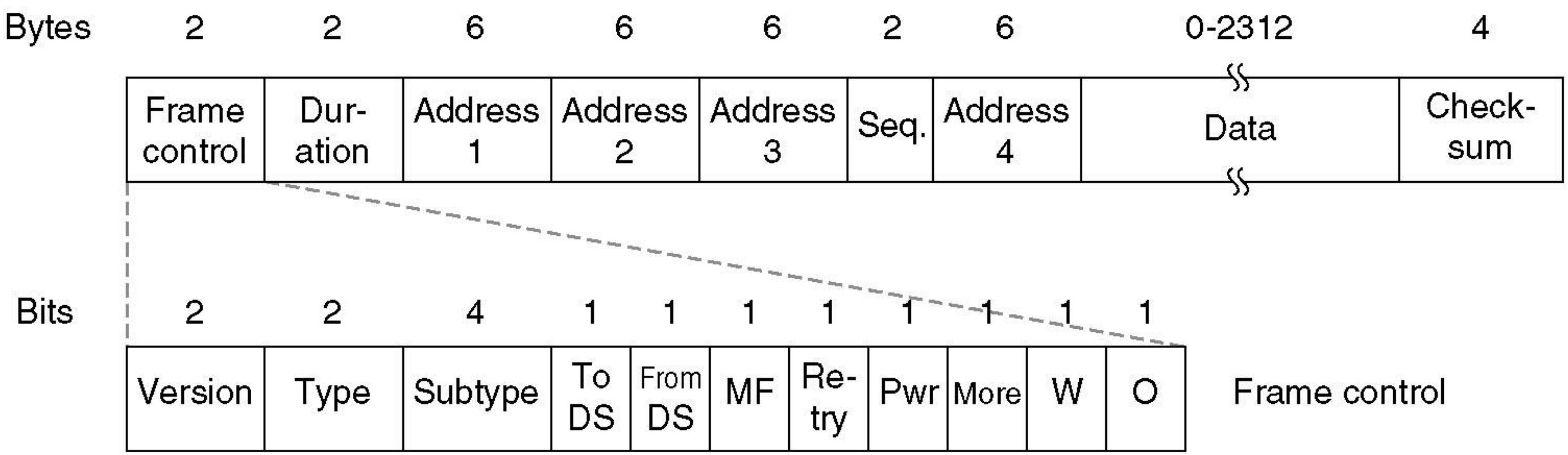
A fragment burst.

The 802.11 MAC Sublayer Protocol (4)



Interframe spacing in 802.11.

The 802.11 Frame Structure



The 802.11 data frame.

802.11 Services

Distribution Services

- Association
- Disassociation
- Reassociation
- Distribution
- Integration

802.11 Services

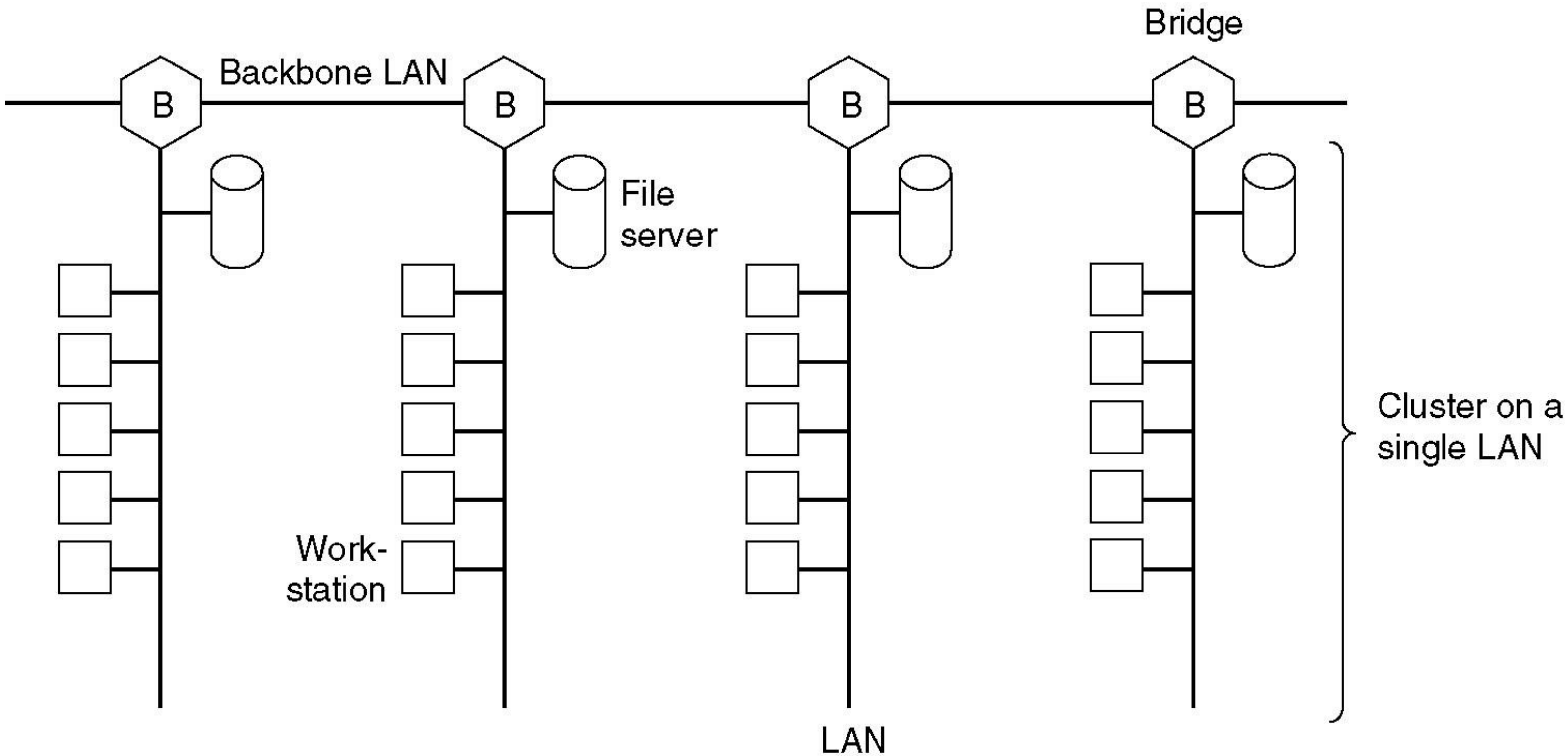
Intracell Services

- Authentication
- Deauthentication
- Privacy
- Data Delivery

Data Link Layer Switching

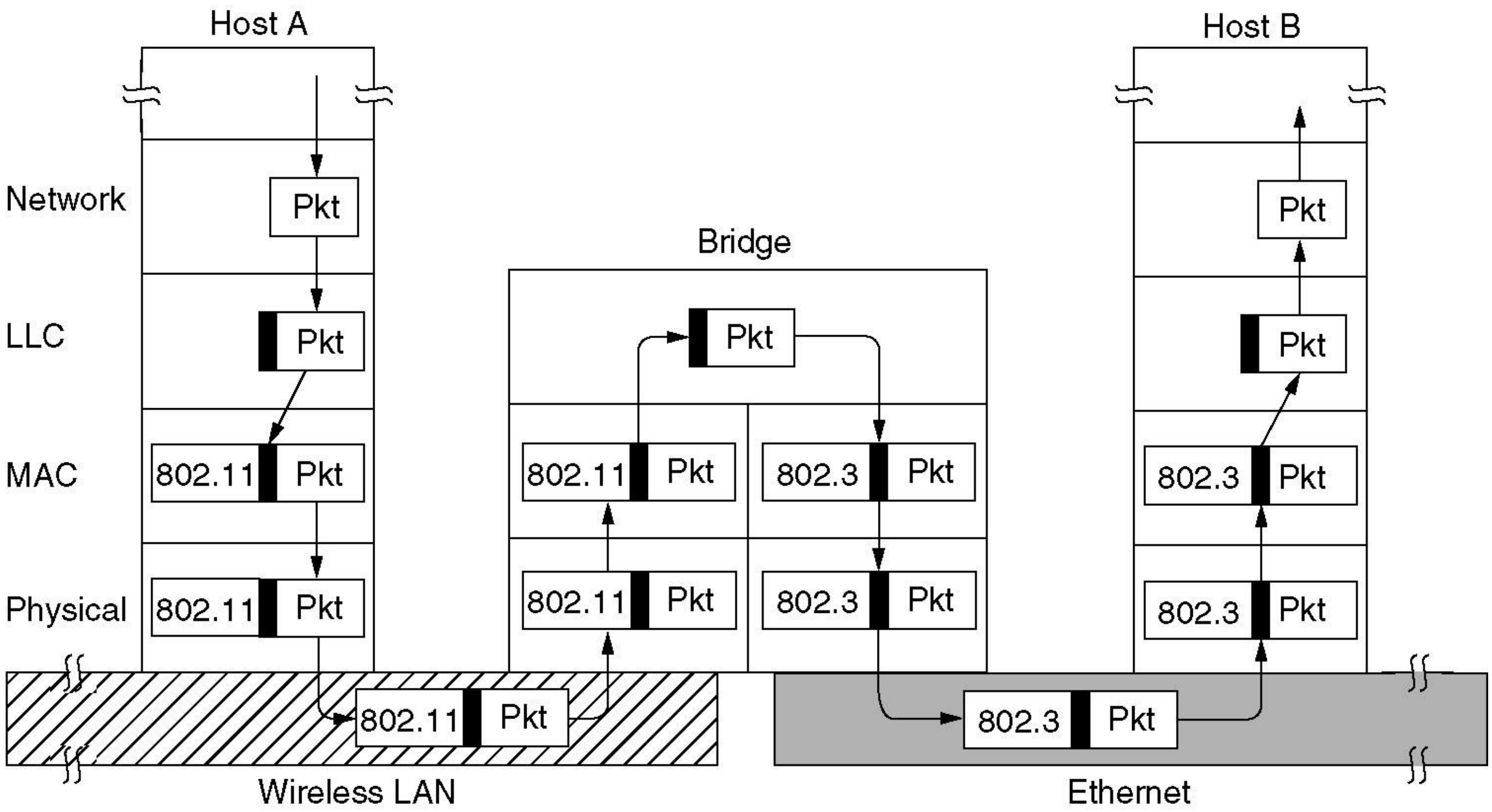
a) Geographical spread
b) Goals of the various departments of an organization are different
c) Splitting the load
d) Physical distance greater than 2.5 KM
e) Filtering garbage
f) promiscuous mode -Filtering sensitive information

Data Link Layer Switching



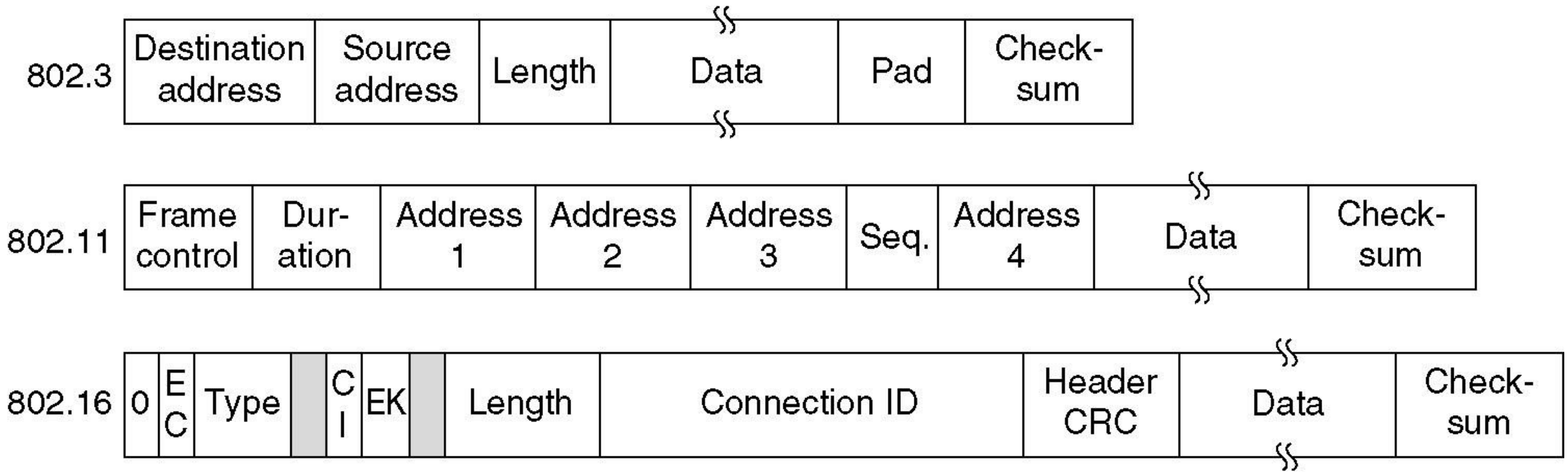
Multiple LANs connected by a backbone to handle a total load higher than the capacity of a single LAN.

Bridges from 802.x to 802.y



Operation of a LAN bridge from 802.11 to 802.3.

Bridges from 802.x to 802.y (2)

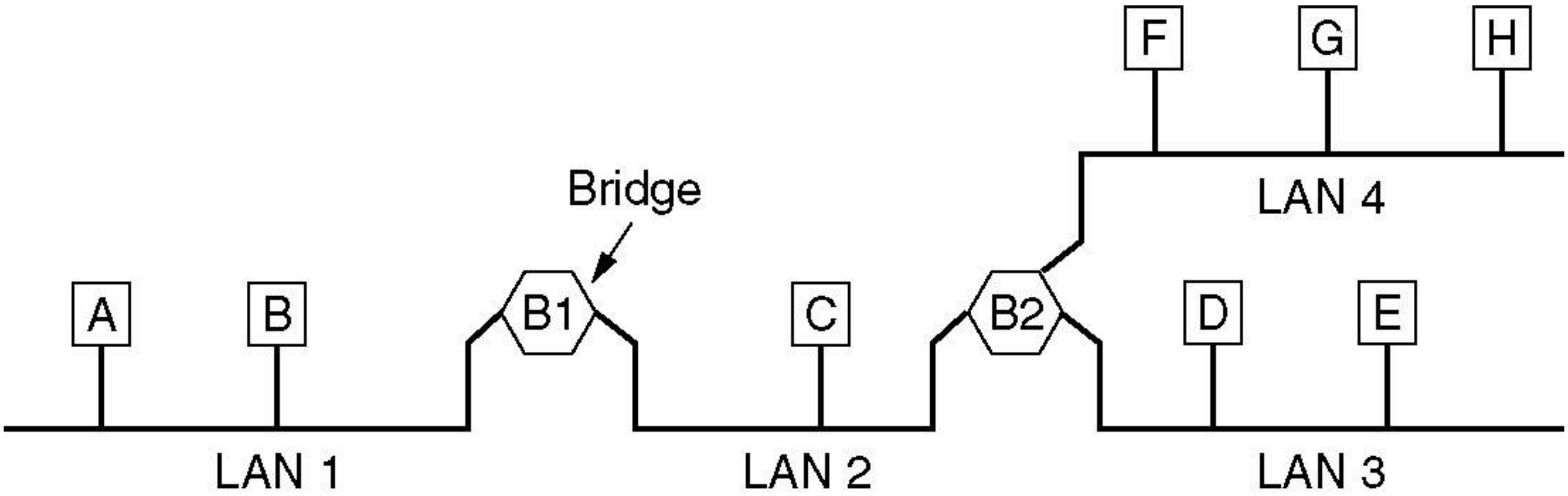


The IEEE 802 frame formats. The drawing is not to scale.

Not so easy!

a) Different frame format
b) Different data rate
c) Different maximum frame size
d) Security- encryption suppport
e) Qos support

Local Internetworking

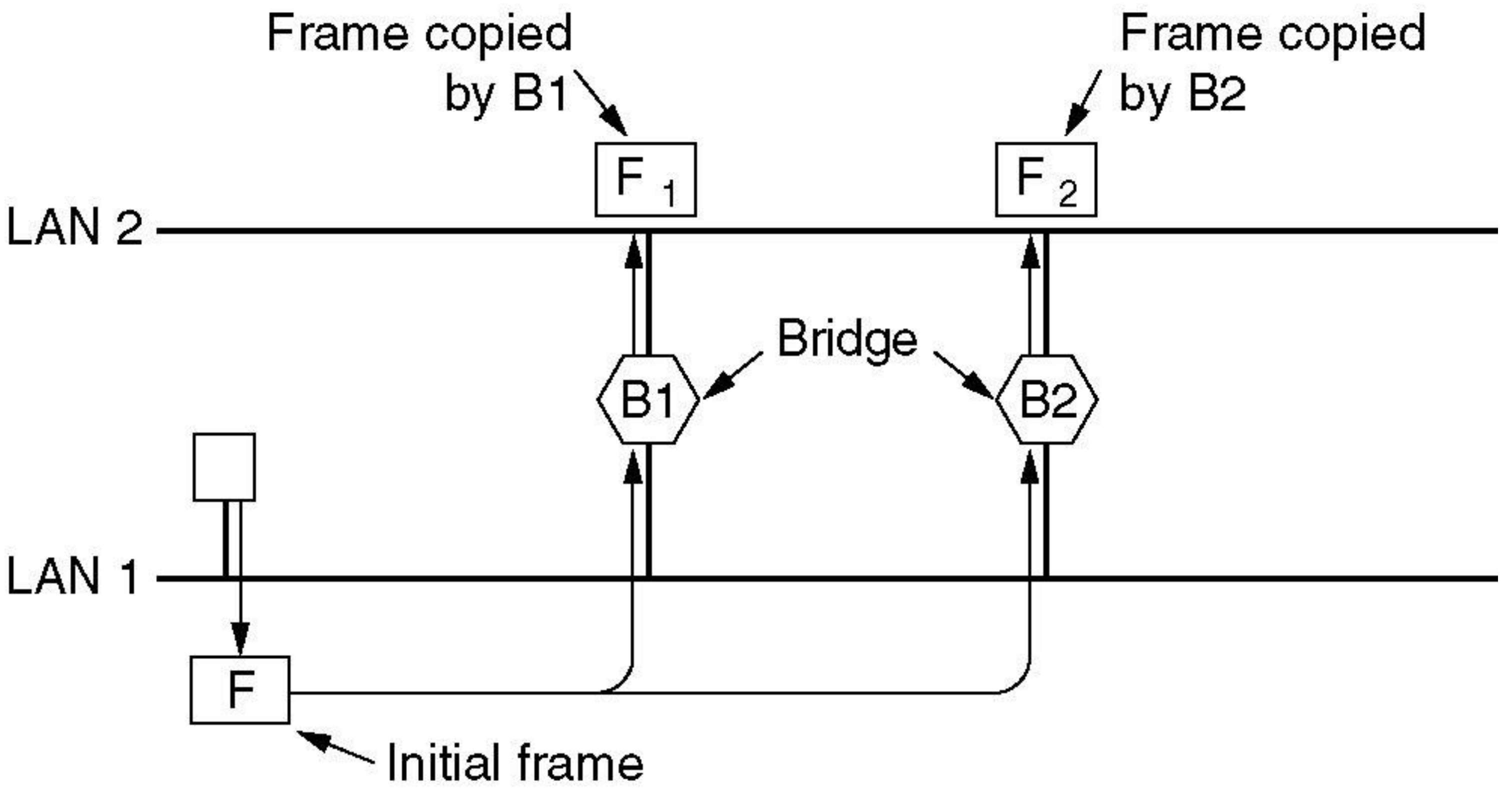


A configuration with four LANs and two bridges.

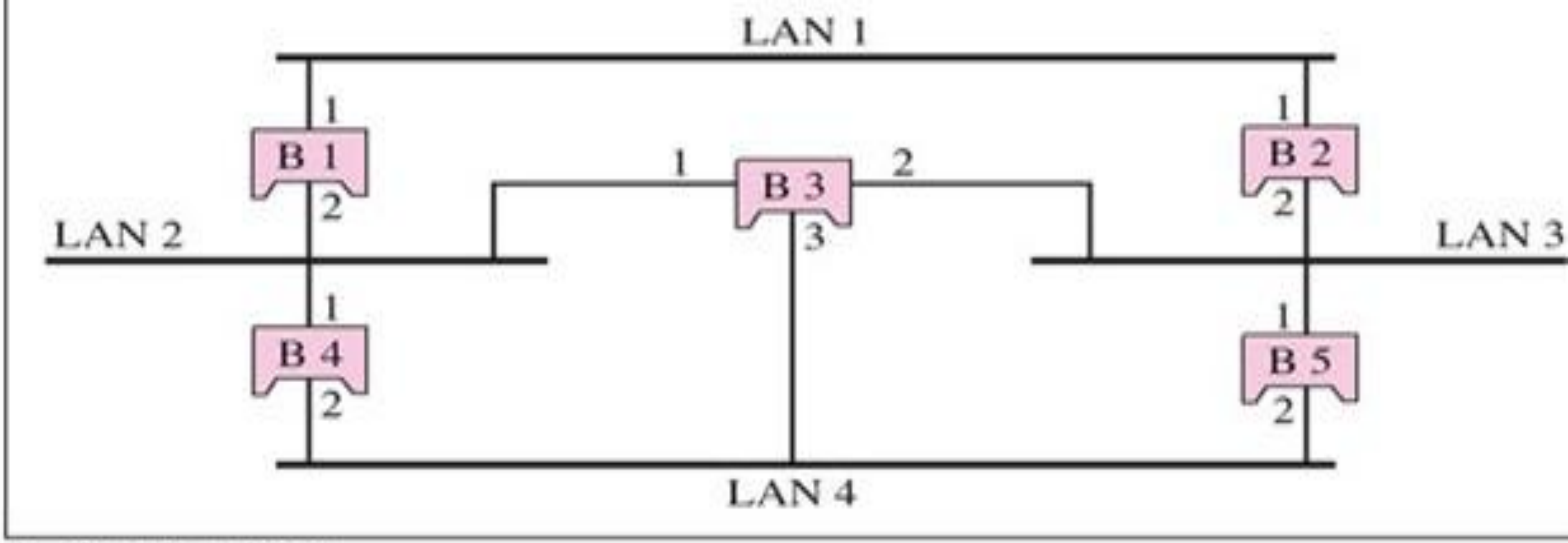
Bridges

a) Promiscuous mode
b) Transparent
c) Hash tables
d) Backward learning
e) Dynamic topology

Spanning Tree Bridges



Two parallel transparent bridges.



a. Actual system

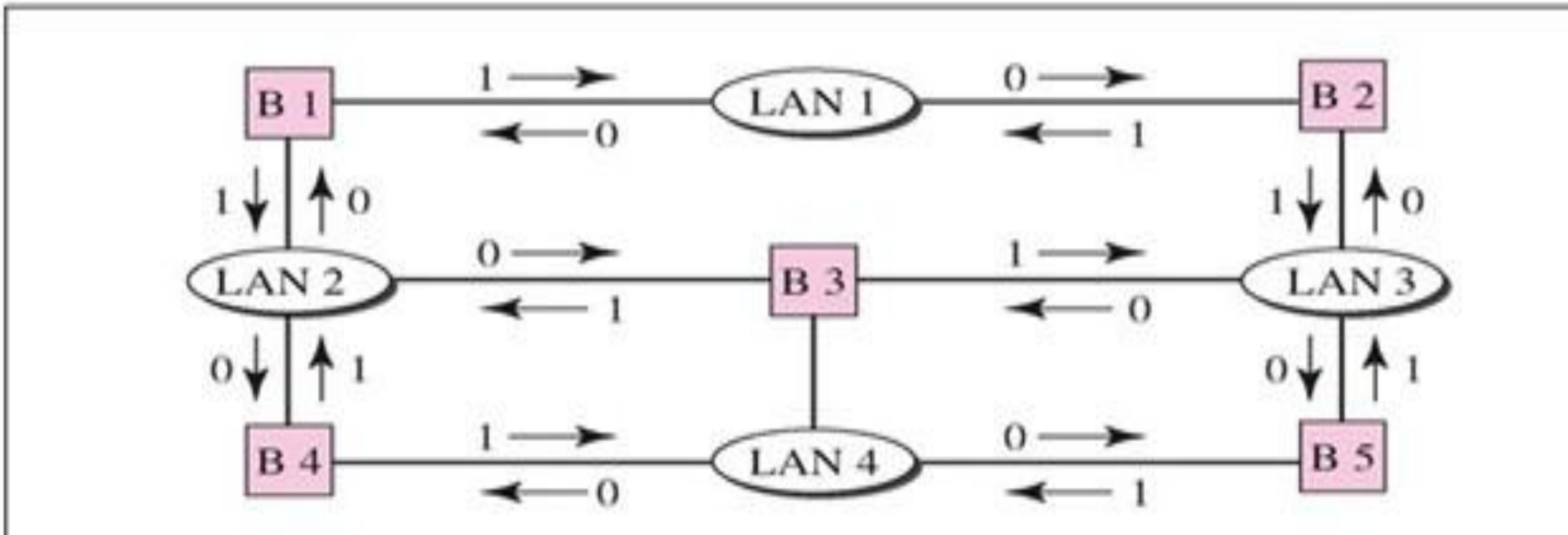
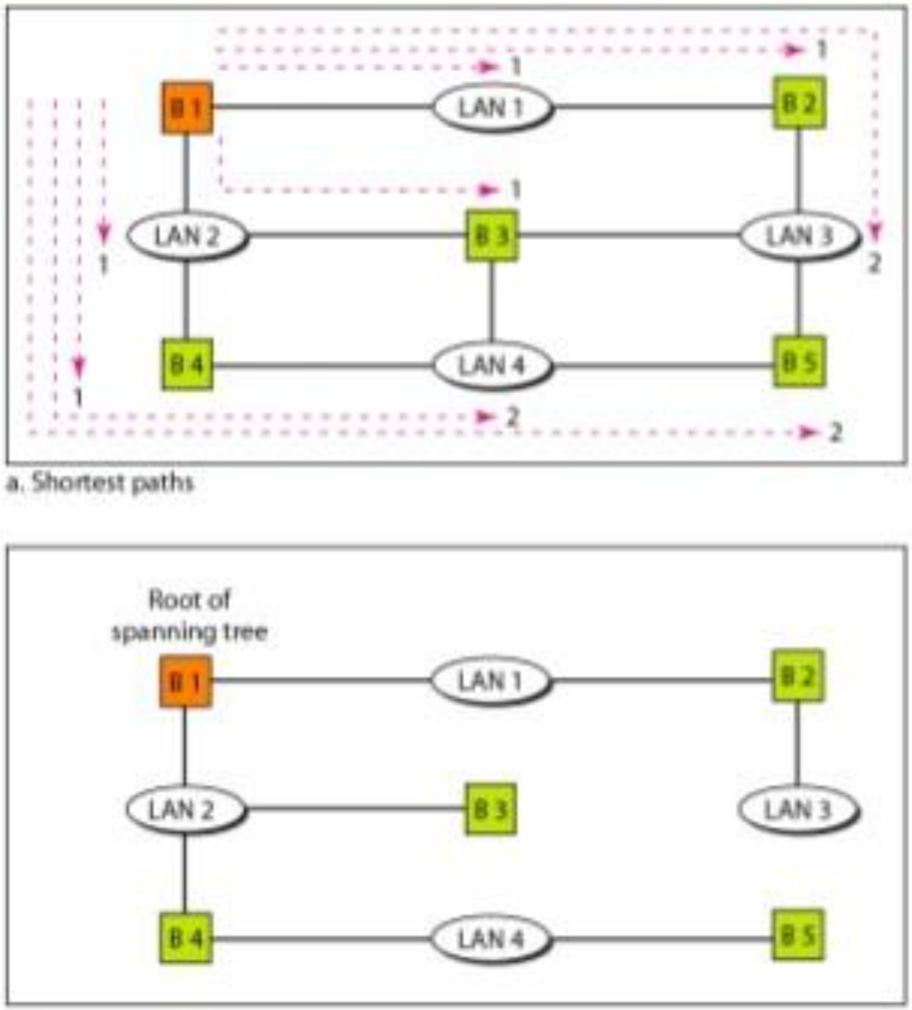
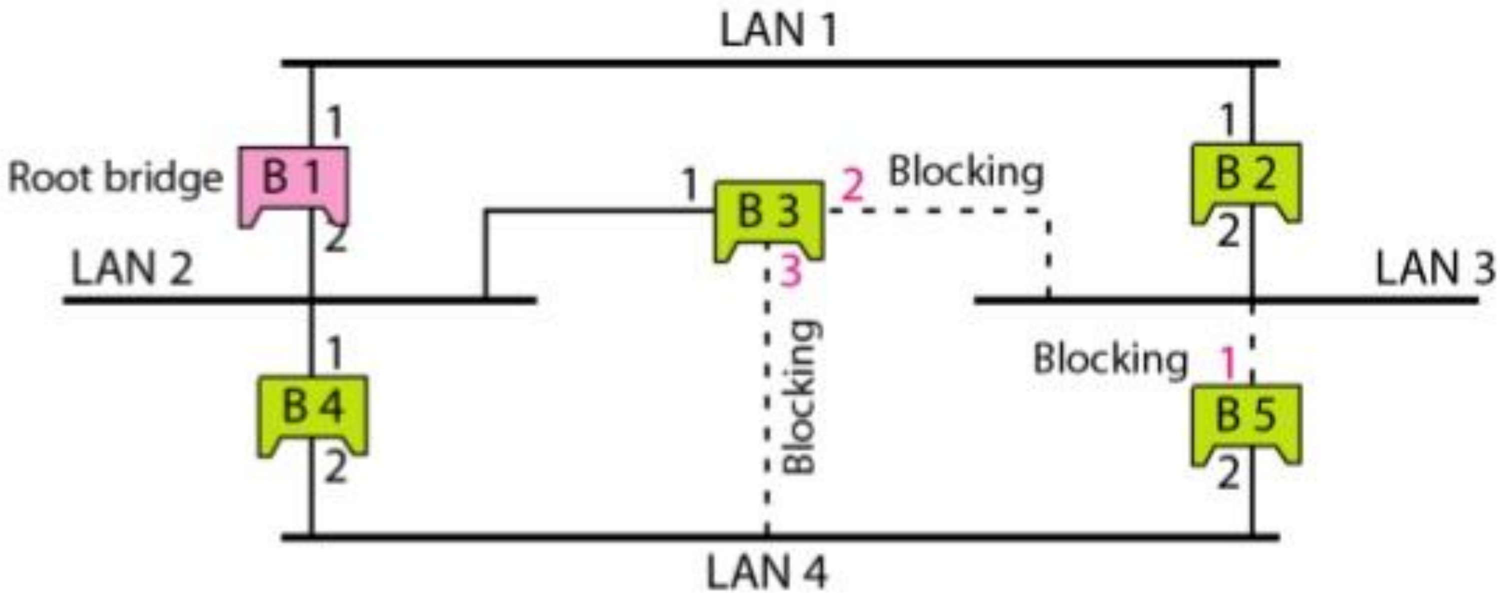


Figure 15.9 *Finding the shortest paths and the spanning tree in a system of bridges*



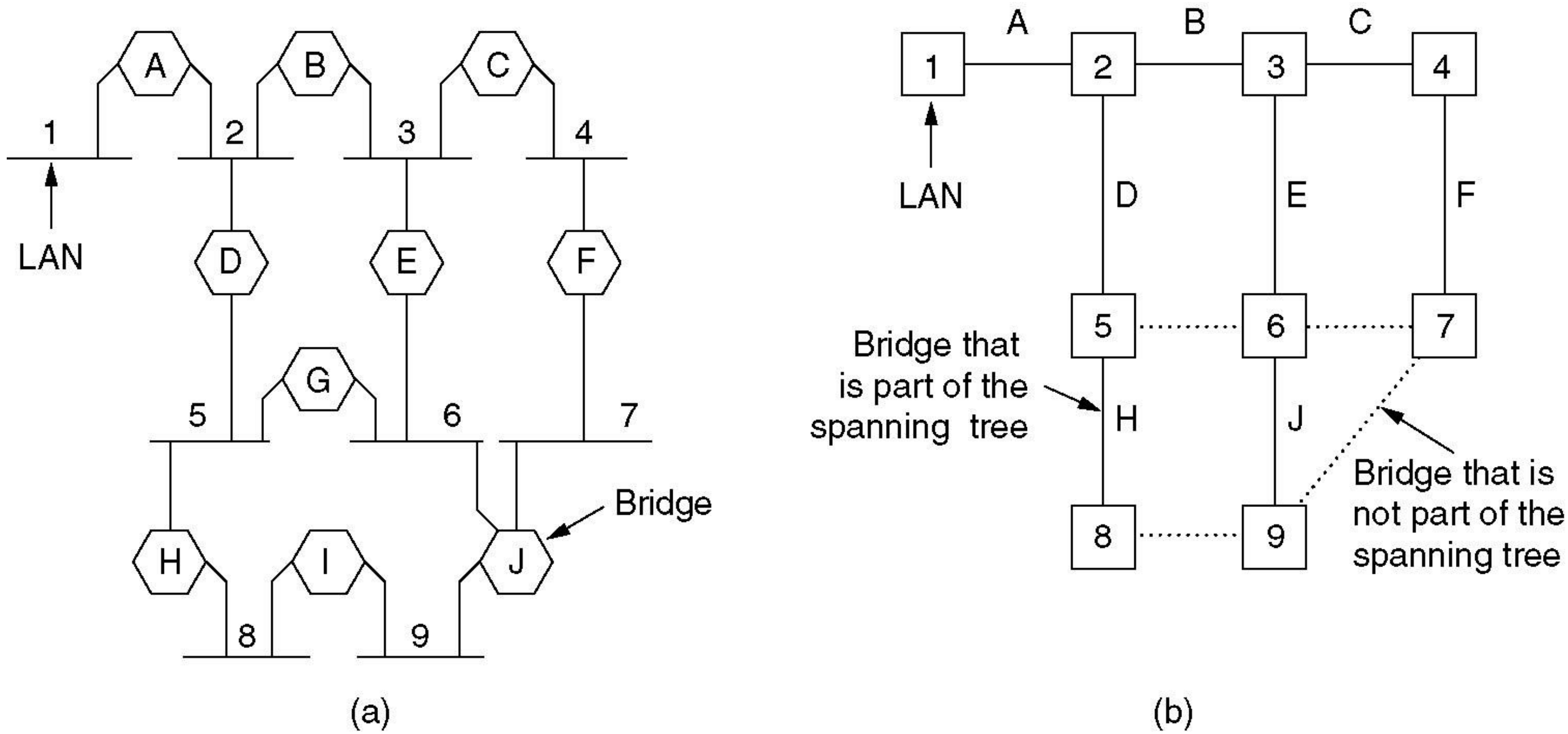
b. Spanning tree

Figure 15.10 ***Forwarding and blocking ports after using spanning tree algorithm***



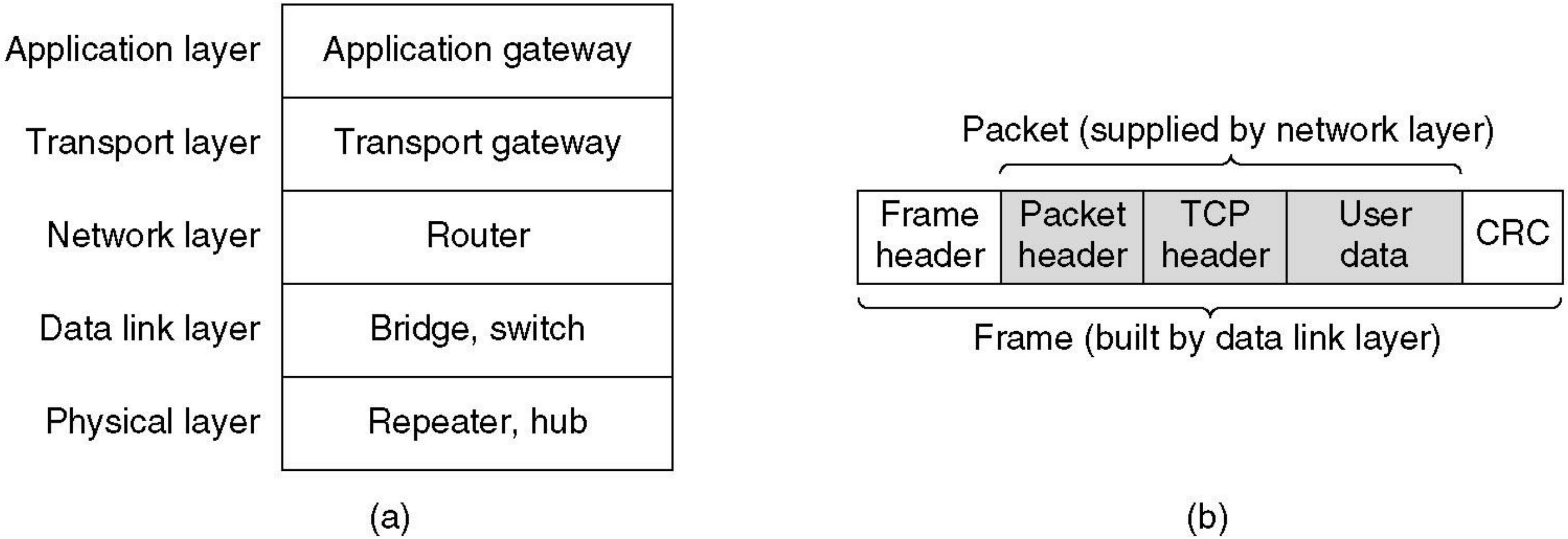
Ports 2 and 3 of bridge B3 are blocking ports (no frame is sent out of these ports).
Port 1 of bridge B5 is also a blocking port (no frame is sent out of this port).

Spanning Tree Bridges (2)



(a) Interconnected LANs. (b) A spanning tree covering the LANs. The dotted lines are not part of the spanning tree.

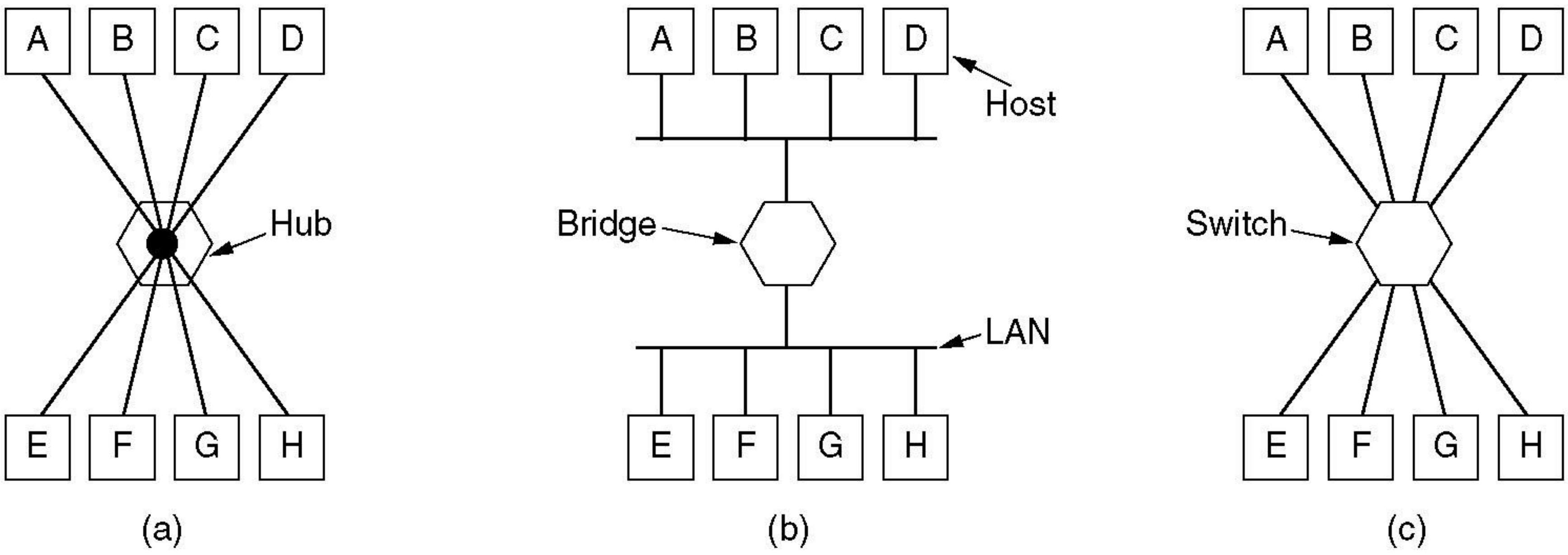
Repeaters, Hubs, Bridges, Switches, Routers and Gateways



(a) Which device is in which layer.

(b) Frames, packets, and headers.

Repeaters, Hubs, Bridges, Switches, Routers and Gateways (2)



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