UNIT II

Medium access – CSMA – Ethernet – Token ring – FDDI - Wireless LAN – Bridges and Switches.

Medium Access

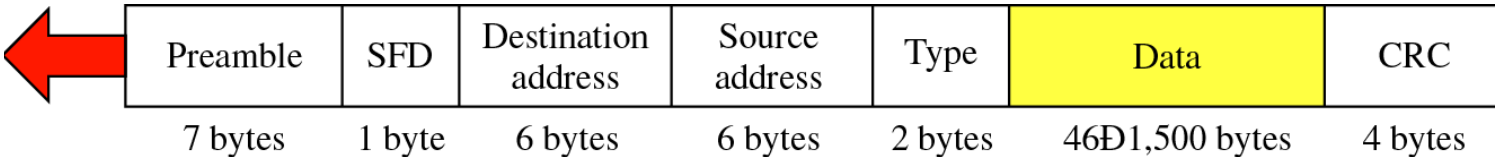
- Some network topologies share a common medium with multiple nodes. At any one time, there may be a number of devices attempting to send and receive data using the network media.
- When two or more nodes are sending data at the same time, data may be unusable due to collsion. There are rules that govern how these devices share the media to solve the collision problem.
- Here are two basic media access control methods for shared media: Controlled - Each node has its own time to use the medium. Network devices will take turns, in sequence, to access the medium. One example is Token Ring.
- Contention-based - All nodes compete for the use of the medium.
- CSMA is usually implemented in conjunction with a method for resolving the media contention. The two commonly used methods are:

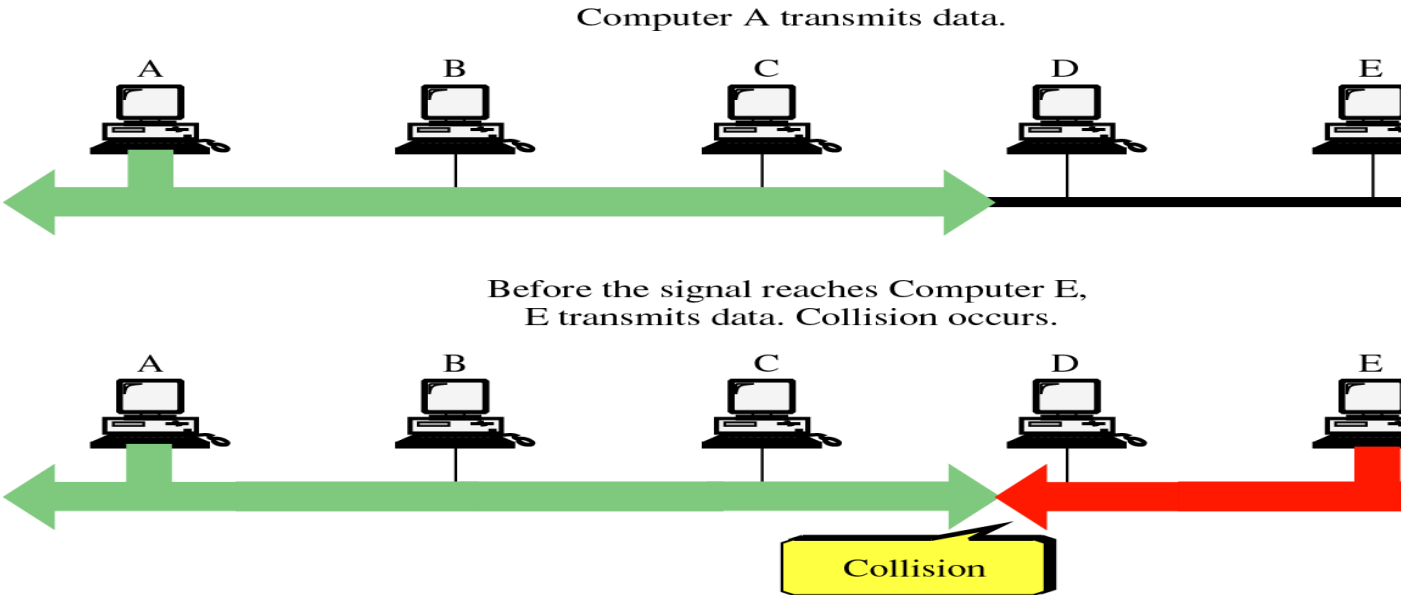
CSMA/CollisionDetection
CSMA/Collision Avoidance

Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

The basic idea:
When a station has a frame to transmit:
1) Listen for Data Transmission on Cable (Carrier Sense)
2) When Medium is Quiet (no other station transmitting):
a) Transmit Frame, Listening for Collision
b) If collision is heard, stop transmitting, wait random time, and transmit again.

Frame format

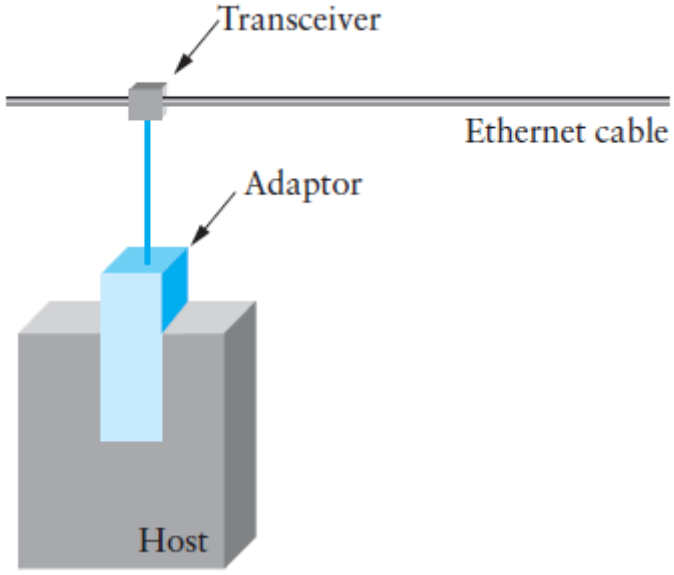




Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

▸ CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) is a protocol for carrier transmission in 802.11 networks. ▸ Unlike CSMA/CD which deals with transmissions after a collision has occurred, CSMA/CA acts to prevent collisions before they happen. In CSMA/CA, as soon as a node receives a packet that is to be sent, it checks to be sure the channel is clear (no other node is transmitting at the time). ▸ If the channel is clear, then the packet is sent. If the channel is not clear, the node waits for a randomly chosen period of time, and then checks again to see if the channel is clear. ▸ This period of time is called the backoff factor, and is counted down by a backoff counter. ▸ If the channel is clear when the backoff counter reaches zero, the node transmits the packet.

Ethernet (802.3) ▸ The Ethernet is easily the most successful local area networking technology of the last 20 years. ▸ Developed in the mid-1970s by researchers at the Xerox Palo Alto Research Center (PARC), the Ethernet is a working example of the more general Carrier Sense Multiple Access with Collision Detect (CSMA/CD) local area network technology.



- Ethernet is a multiple-access network, meaning that a set of nodes send and receive frames over a shared link.
- The fundamental problem faced by the Ethernet is how to mediate access to a shared medium fairly and efficiently.
- Digital Equipment Corporation and Intel Corporation joined Xerox to define a 10-Mbps Ethernet standard in 1978. This standard then formed the basis for IEEE standard 802.3.
- 100-Mbps version called Fast Ethernet.
- and a 1000-Mbps version called Gigabit Ethernet.
- Both 100-Mbps and 1000-Mbps Ethernets are designed to be used in full-duplex, point-to-point configurations, which means that they are typically used in switched networks.

Physical Properties

- An Ethernet segment is implemented on a coaxial cable of up to 500m. This cable is similar to the type used for cable TV, except that it typically has an impedance of 50 ohms instead of cable TV‟s 75 ohms.
- Hosts connect to an Ethernet segment by tapping into it; taps must be at least 2.5 m apart.

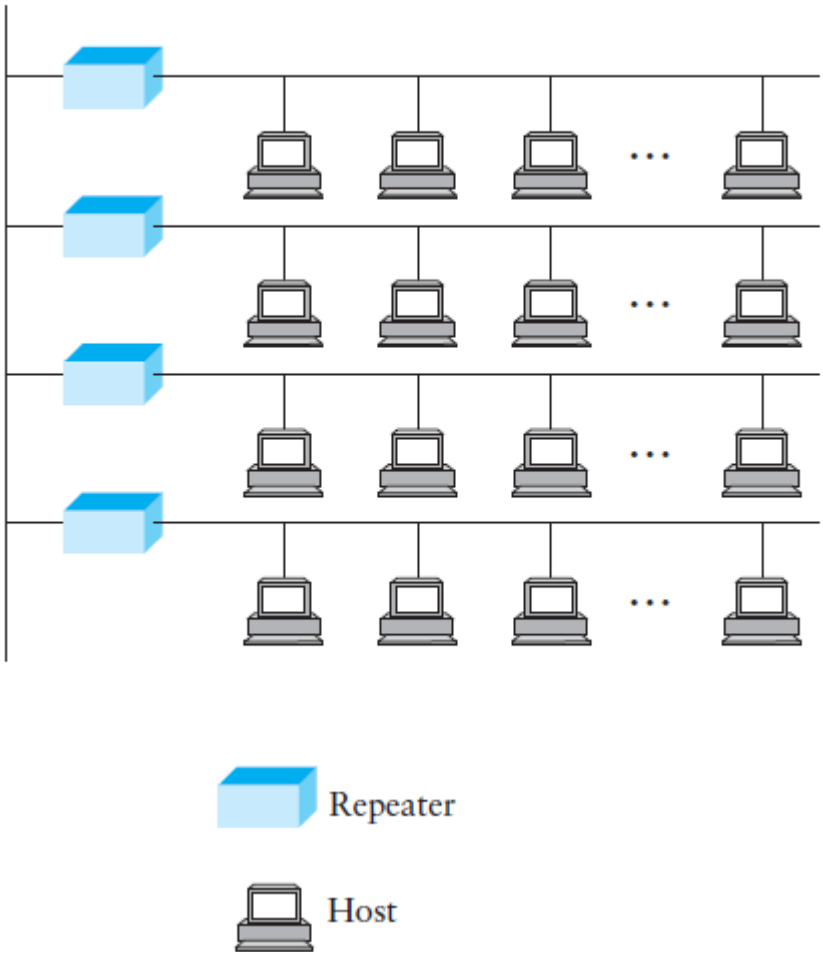
- A *transceiver—a small device directly* attached to the tap—detects when the line is idle and drives the signal when the host is transmitting.
- It also receives incoming signals.
- The transceiver is, in turn, connected to an Ethernet adaptor, which is plugged into the host.

Ethernet Transceiver and adaptor

- Multiple Ethernet segments can be joined together by *repeaters.A repeater is a device* that forwards digital signals, much like an amplifier forwards analog signals.
- However, no more than four repeaters may be positioned between any pair of hosts, meaning that an Ethernet has a total reach of only 2500 m.

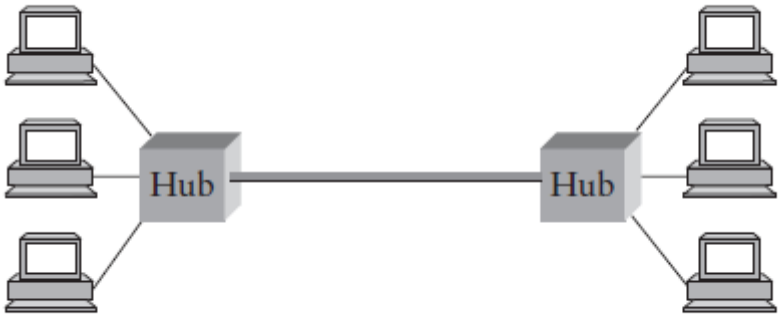
Ethernet is limited to supporting a maximum of 1024 hosts.

Ethernet Repeater



- Any signal placed on the Ethernet by a host is broadcast over the entire network; that is, the signal is propagated in both directions, and repeaters forward the signal on all outgoing segments.
- Terminators attached to the end of each segment absorb the signal and keep it from bouncing back and interfering with trailing signals.
- The Ethernet uses the Manchester encoding scheme.
- Ethernet can be constructed from a thinner cable known as10Base2; the original cable is called 10Base5 (the two cables are commonly called *thin-net and thick-net, respectively).*
- *The "10" in 10Base2 means that the network operates* at 10 Mbps, "Base" refers to the fact that the cable is used in a *baseband system, and* the "2" means that a given segment can be no longer than 200 m.
- Today, a third cable technology is predominantly used, called 10BaseT, where the "T" stands for twisted pair. Typically, Category 5 twisted pair wiring is used.
- A 10BaseT segment is usually limited to under100 m in length.

Ethernet Hub

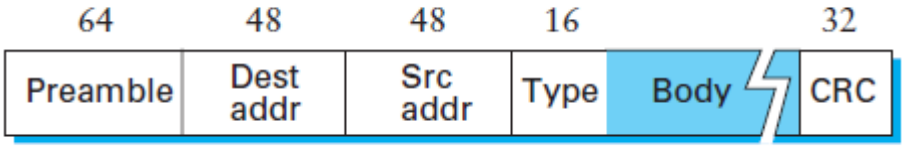


Access Protocol

- We now turn our attention to the algorithm that controls access to the shared Ethernet link. This algorithm is commonly called the Ethernet's *media access control (MAC)*.
- It is typically implemented in hardware on the network adaptor.

Frame Format

- The 64-bit preamble allows the receiver to synchronize with the signal; it is a sequence of alternating 0sand 1s.
- Both the source and destination hosts are identified with a 48-bit address.
- The packet type field serves as the demultiplexing key; that is, it identifies to which of possibly many higher-level protocols this frame should be delivered.
- Each frame contains up to 1500 bytes of data. Minimally, a frame must contain at least 46 bytes of data, even if this means the host has to pad the frame before transmitting it.
- The reason for this minimum frame size is that the frame must be long enough to detect a collision.
- Each frame includes a 32-bit CRC.
- The Ethernet is a bit-oriented framing protocol.



- Ethernet frame has a 14-byte header: two 6-byte addresses and a 2-byte type field.
- The frame format just described is taken from the Digital-Intel-Xerox Ethernet standard.
- The 802.3 frame format is exactly the same, except it substitutes a 16-bit length field for the 16-bit type field.

Addresses

- Each host on an Ethernet—in fact, every Ethernet host in the world—has a unique Ethernet address.
- Technically, the address belongs to the adaptor, not the host; it is usually burned into ROM.
- Ethernet addresses are typically printed in a form humans can read as a sequence of six numbers separated by colons.
- Each number corresponds to 1 byte of the 6-byte address and is given by a pair of hexadecimal digits, one for each of the 4-bit nibbles in the byte; leading 0s are dropped.
- For example, 8:0:2b:e4:b1:2 is the human-readable representation of Ethernet address

00001000 00000000 00101011 11100100 10110001 00000010

- To ensure that every adaptor gets a unique address, each manufacturer of Ethernet devices is allocated a different prefix that must be prepended to the address on every adaptor they build.
- For example, Advanced Micro Devices has been assigned the

24-bit prefix x080020 (or 8:0:20).

- Each frame transmitted on an Ethernet is received by every adaptor connected to that Ethernet.

Each adaptor recognizes those frames addressed to its address and passes only those frames on to the host

Ethernet adaptor receives all frames and accepts

- frames addressed to its own address

- frames addressed to the broadcast address
- frames addressed to a multicast address, if it has been instructed to listen to that address.
- all frames, if it has been placed in promiscuous mode

Transmitter Algorithm

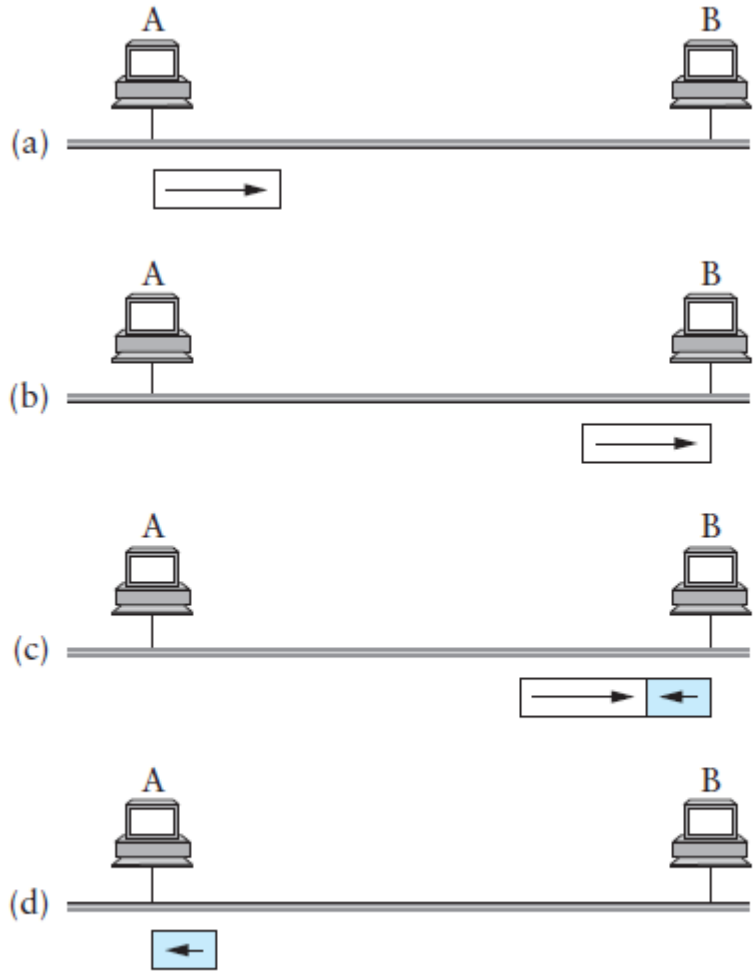
When the adaptor has a frame to send and the line is idle, it transmits the frame immediately; there is no negotiation with the other adaptors.

- The upper bound of 1500 bytes in the message means that the adaptor can occupy the line for only a fixed length of time.
- When an adaptor has a frame to send and the line is busy, it waits for the line to go idle and the transmits immediately.
- The Ethernet is said to be a *1-persistent protocol* because an adaptor with a frame to send transmits with probability 1 whenever a busy line goes idle.
- In general, a *p-persistent algorithm transmits with probability* $0 \leq p \leq 1$ after a line becomes idle, and defers with probability $q = 1 - p$.
- *The reasoning behind* choosing a $p < 1$ *is that there might be multiple adaptors waiting for the busy line* to become idle.

Collison Handling

- Returning to our discussion of the Ethernet, because there is no centralized control it is possible for two (or more) adaptors to begin transmitting at the same time, either because both found the line to be idle or because both had been waiting for a busy line to become idle.
- When this happens, the two (or more) frames are said to *collide on the network. Each sender, because the Ethernet supports collision detection, is* able to determine that a collision is in progress.
- At the moment an adaptor detects that its frame is colliding with another, it first makes sure to transmit a 32-bit jamming sequence and then stops the transmission. Thus, a transmitter will minimally send 96 bits in the case of a collision: 64-bit preamble plus 32-bit jamming sequence.
- One way that an adaptor will send only 96 bits—which is sometimes called a *runt frame.*

Worst-case scenario: (a) A sends a frame at time *t*; (b) *A's frame arrives at* B at time *t + d*; (c) *B begins transmitting at time t + d and collides with A's frame*; (d) *B's* runt (32-bit) frame arrives at A at time *t +2d.*



- Once an adaptor has detected a collision and stopped its transmission, it waits a certain amount of time and tries again. Each time it tries to transmit but fails, the adaptor doubles the amount of time it waits before trying again.
- This strategy of doubling the delay interval between each retransmission attempt is a general technique known as *exponential backoff*.

Experience with Ethernet

DRAWBACKS

- Utilization - 30%.
- Too much of the network‟s capacity is wasted by collisions.

- Most Ethernets have fewer than 200 hosts.
- Similarly, most Ethernets are far shorter than 2500 m.
- provide an end-to-end flow-control mechanism.

ADVANTAGES

- Ethernet is extremely easy to administer and maintain: There are no switches that can fail, no routing or configuration tables that have to be kept up-to-date, and it is easy to add a new host to the network.
- It is inexpensive: Cable is cheap, and the only other cost is the network adaptor on each host.

Token Rings

- Token rings are the other significant class of shared-media network.

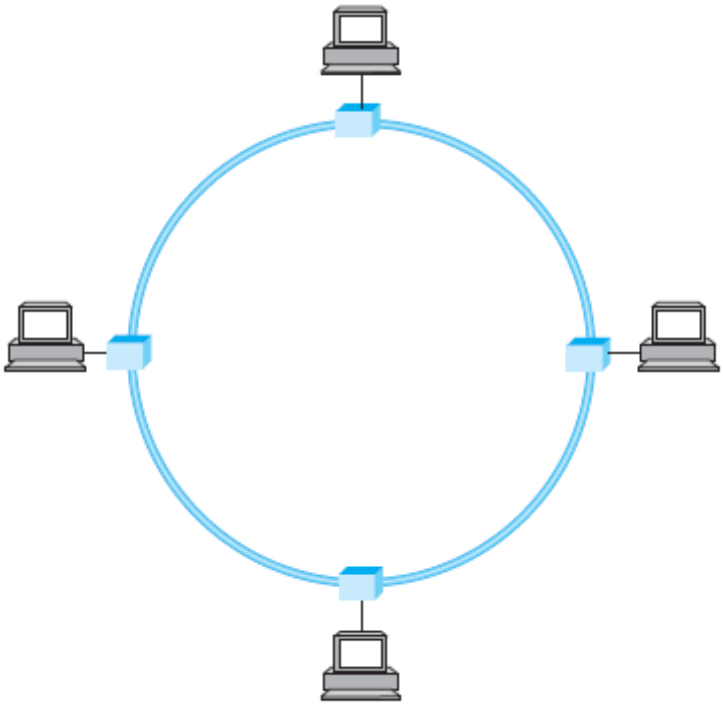
There are more different types of token rings available.
IBM Token Ring. Like the Xerox Ethernet, IBM"s Token Ring has a nearly identical IEEE standard, known as 802.5.

- However, the FDDI (Fiber Distributed Data Interface) standard—a newer, faster type of token ring.
- Another token ring standard, called Resilient Packet Ring or 802.17.

Construction

- As the name suggests, a token ring network consists of a set of nodes connected in a ring. Data always flows in a particular direction around the ring, with each node receiving frames from its upstream neighbor and then forwarding them to its downstream neighbor.
- This ring-based topology is in contrast to the Ethernet"s bus topology. Like the Ethernet, however, the ring is viewed as a single shared medium.

Token Ring Network



Features

- Thus, a token ring shares two key features with an Ethernet: First, it involves a distributed algorithm that controls when each node is allowed to transmit.
- and second, all nodes see all frames, with the node identified in the frame header as the destination saving a copy of the frame as it flows past.

Working Strategy

- The word "token" in token ring comes from the way access to the shared ring is managed. The idea is that a token, which is really just a special sequence of bits, circulates around the ring; each node receives and then forwards the token.
- When a node that has a frame to transmit sees the token, it takes the token off the token and instead inserts its frame into the ring.
- Each node along the way simply forwards the frame, with the destination node saving a copy and forwarding the message onto the next node on the ring.

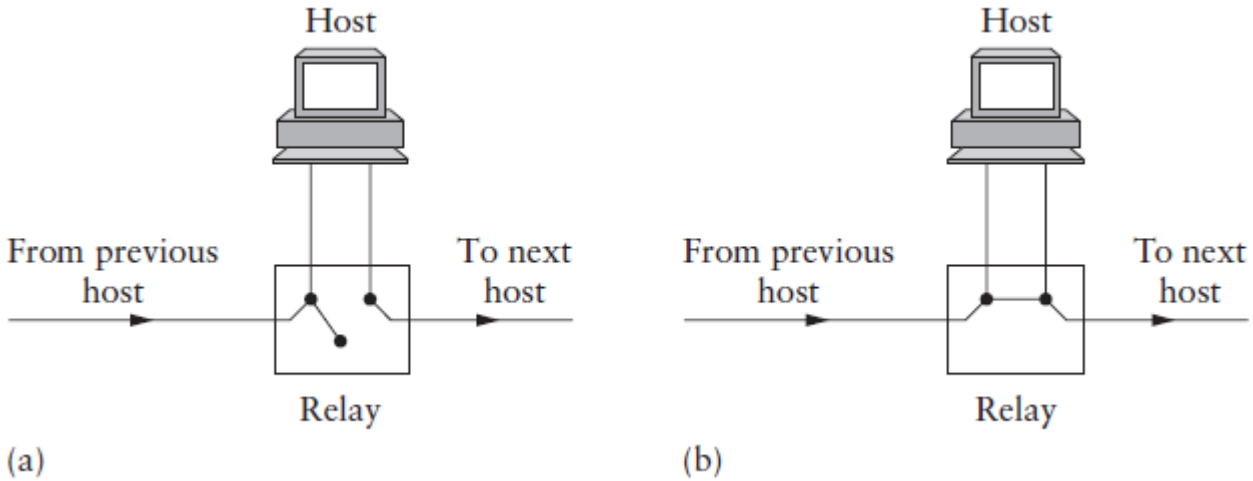
Physical Properties

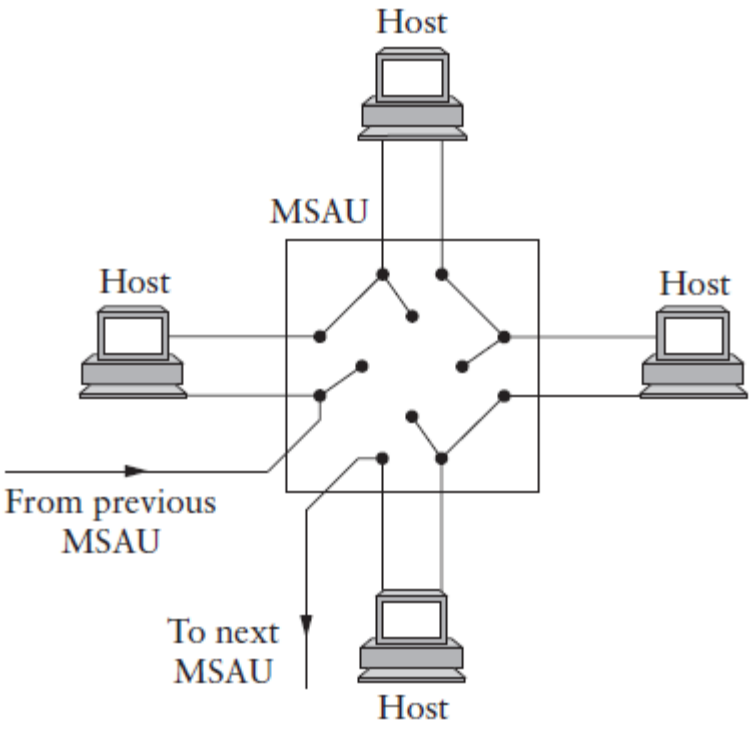
- One of the first things you might worry about with a ring topology is that any link or node failure would render the whole network useless.
- This problem is addressed by connecting each station into the ring using an electromechanical relay.
- As long as the station is healthy, the relay is open and the station is included in the ring. If the station stops providing power, the relay closes and the ring automatically bypasses the station.
- Several of these relays are usually packed into a single box, known as a multi station access unit (MSAU).
- This has the interesting effect of making a token ring actually look more like a star topology.

Relay used on a token ring: (a) relay open—host active; (b) relay closed—host bypassed.

Multi station access unit

- It also makes it very easy to add stations to and remove stations from the network, since they can just be plugged into or unplugged from the nearest MSAU, while the overall wiring of the network can be left unchanged.





- IBM Token Ring specification and 802.5 is that the former actually requires the use of MSAUs,while the latter does not allow MSAU.
- MSAU allows robustness and ease of station addition and removal.
- The data rate may be either 4 Mbps or 16 Mbps.
- It uses differential Manchester encoding.
- 260 stations per ring.

Token Ring Media Access Control

- When none of the stations connected to the ring has anything to send, the token circulates around the ring. Obviously, the ring has to have enough "storage capacity" to hold an entire token.
- As the token circulates around the ring, any station that has data to send may "seize" the token, that is, drain it off the ring and begin sending data. In 802.5 networks, the seizing process involves simply modifying 1 bit in the second byte token; the first 2 bytes of the modified token now become the preamble for the subsequent data packet.
- Once a station has the token, it is allowed to send one or more packets—exactly how many more depends on some factors.
- Each transmitted packet contains the destination address of the intended receiver;it may also contain a multicast (or broadcast) address if it is intended to reach more than one (or all) receivers.
- As the packet flows past each node on the ring, each node looks inside the packet to see if it is the intended recipient. If so, it copies the packet into a buffer as it flows through the network adaptor.
- One issue we must address is how much data a given node is allowed to transmit each time it possesses the token, or said another way, how long a given node is allowed to hold the token.
- We call this the *token holding time (THT)*.
- In 802.5 networks, the default THT is10 ms.
- Before putting each packet onto the ring, the station must check that the amount of time it would take to transmit the packet would not cause it to exceed the token holding time.
- From the token holding time we can derive another useful quantity, the *token rotation time (TRT), which is the amount of time it takes a token to traverse the ring* as viewed by a given node.

TRT ≤ Active Nodes × THT + Ring Latency

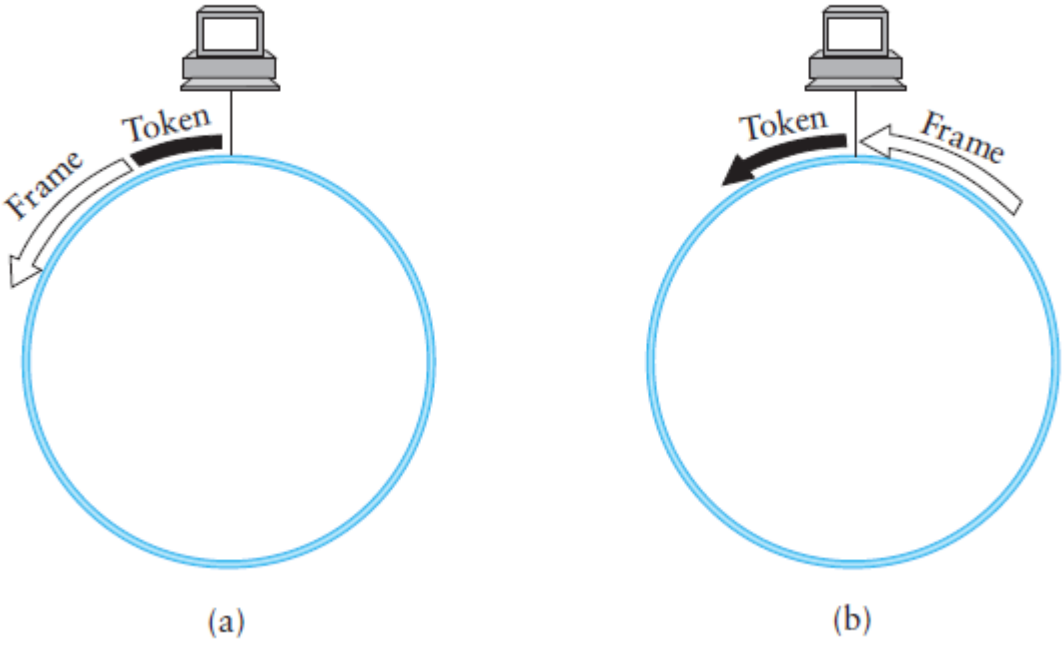
- RingLatency denotes how long it takes the token to circulate around the ring when no one has data to send.
- ActiveNodes denotes the number of nodes that have data to transmit.
- The 802.5 protocol provides a form of reliable delivery using 2 bits in the packet trailer, the A and C bits. These are both 0 initially.
- When a station sees a frame for which it is the intended recipient, it sets the A bit in the frame. When it copies the frame into its adaptor, it sets the C bit.
- If the sending station sees the frame come back over the ring with the A bit still 0, it knows that the intended recipient is not functioning or absent.
- If the A bit is set but not the C bit, this implies that for some reason (e.g.,lack of buffer space) the destination could not accept the frame. Thus, the frame might reasonably be retransmitted later in the hope that buffer space had become available.

Priority Based Transmission

- Another detail of the 802.5 protocol concerns the support of different levels of priority.
- The token contains a 3-bit priority field, so we can think of the token having a certain priority *n at any time.*
- *Each device that wants to send a packet assigns a* priority to that packet, and the device can only seize the token to transmit a packet if the packet"s priority is at least as great as the token"s.
- The priority of the token changes over time due to the use of three *reservation bits in the frame header.*
- Note that this is a *strict priority scheme, in the sense that no lower-priority packets* get sent when higher-priority packets are waiting.
- This may cause lower-priority packets to be locked out of the ring for extended periods if there is a sufficient supply of high-priority packets.

Token release: (a) early versus (b) delayed.

- The sender can insert the token back onto the ring immediately following its frame (this is called *early release) or after the frame it transmits has gone all the way* around the ring and been removed (this is called *delayed release)* .



(a) (b)

Token Ring Maintenance

- As we noted above, token rings have a designated monitor station.
- Any station on the ring can become the monitor, and there are defined procedures by which the monitor is elected when the ring is first connected or on the failure of the current monitor.
- A healthy monitor periodically announces its presence with a special control message; if a station fails to see such a message for some period of time, it will assume that the monitor has failed and will try to become the monitor.
- When a station decides that a new monitor is needed, it transmits a "claim token" frame, announcing its intent to become the new monitor. If that token circulates back to the sender, it can assume that it is OK for it to become the monitor.
- If some other station is also trying to become the monitor at the same instant, the sender might see a claim token message from that other station first. In this case, it will be necessary to break the tie using some well-defined rule like "highest address wins."

- Once the monitor is agreed upon, it plays a number of roles. We have already seen that it may need to insert additional delay into the ring. It is also responsible for making sure that there is always a token somewhere in the ring, either circulating or currently held by a station. It should be clear that a token may vanish for several reasons, such as a bit error, or a crash on the part of a station that was holding it.
- To detect a missing token, the monitor watches for a passing token and maintains a timer equal to the maximum possible token rotation time.
- This interval equals

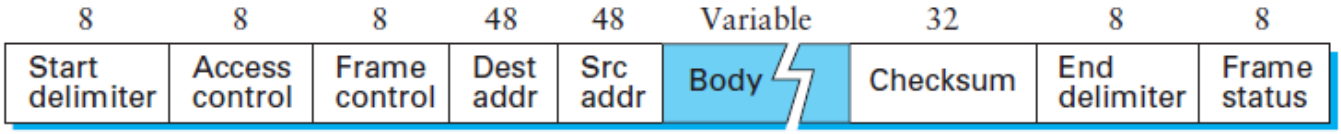
NumStations × THT + Ring Latency

- where NumStations is the number of stations on the ring, and RingLatency is the total propagation delay of the ring. If the timer expires without the monitor seeing a token it creates a new one.

- The monitor also checks for corrupted or orphaned frames. The former have checksum errors or invalid formats, and without monitor intervention, they could circulate forever on the ring.
- The monitor drains them off the ring before reinserting the token.
- An orphaned frame is one that was transmitted correctly onto the ring but whose "parent" died; that is, the sending station went down before it could remove the frame from the ring.
- These are detected using another header bit, the "„monitor" bit. This is 0 on transmission and set to 1 the first time the packet passes the monitor. If the monitor sees a packet with this bit set, it knows the packet is going by for the second time and it drains the packet off the ring.
- One additional ring maintenance function is the detection of dead stations. The relays in the MSAU can automatically bypass a station that has been disconnected
or powered down, but may not detect more subtle failures. If any station suspects a failure on the ring, it can send a *beacon frame to the suspect destination.*

802.5 Token Ring Frame Format

- Start delimiter, End delimiter-Manchester encoding bits.
- control byte-which includes the frame priority and the reservation priority.
- The frame control byte is a demux key.
- This is followed by the frame status byte, which includes the A and C bits for reliable delivery.



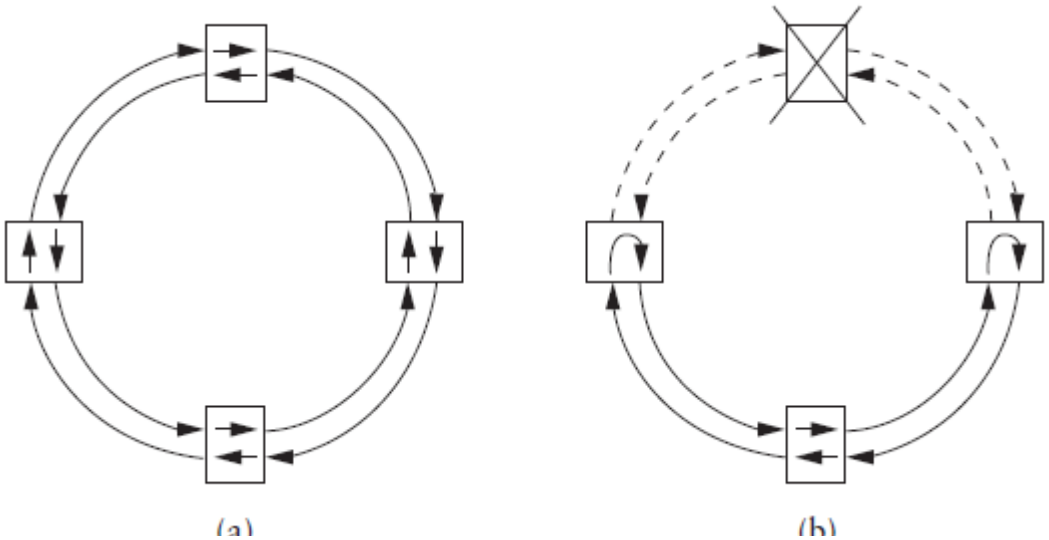
Fddi(Fiber Distributed Data Interface)

- FDDI is similar to 802.5 and IBM Token Rings but it uses optical fiber cable instead of copper cables.

Physical Properties

- Unlike 802.5 networks, an FDDI network consists of a dual ring—two independent rings that transmit data in opposite directions.
- The second ring is not used during normal operation but instead comes into play only if the primary ring fails.

Dual-fiber ring: (a) normal operation; (b) failure of the primary ring.

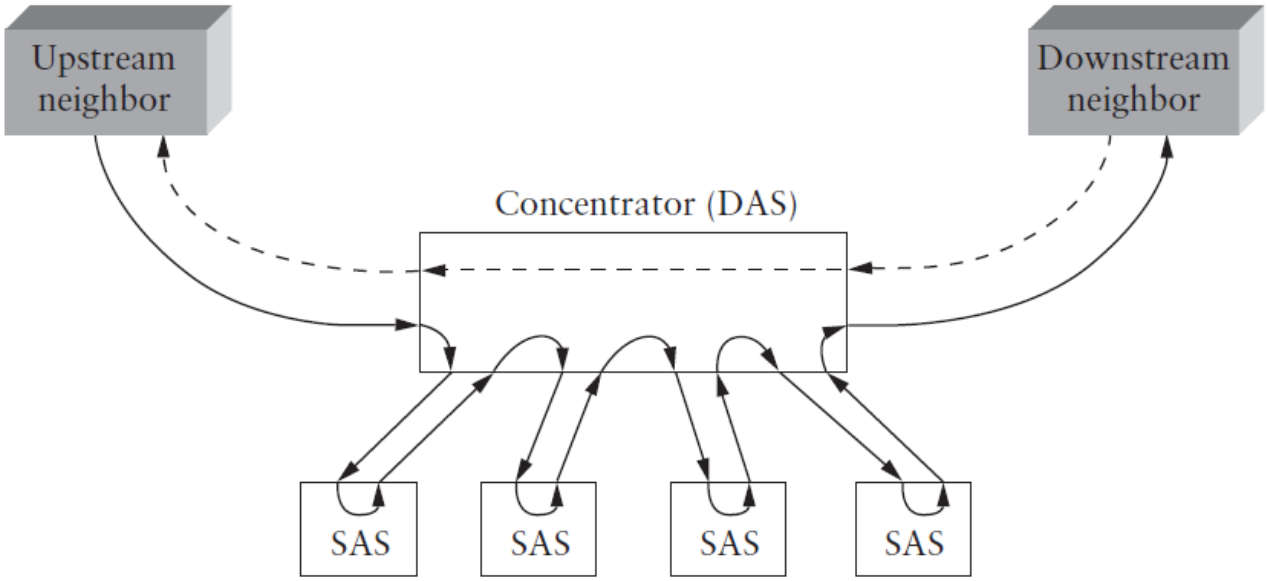


- That is, the ring loops back on the secondary fiber to form a complete ring, and as a consequence, an FDDI network is able to tolerate a single break in the cable or the failure of one station.

- Because of the expense of the dual-ring configuration, FDDI allows nodes to attach to the network by means of a single cable. Such nodes are called *single attachment stations (SAS); their dual-connected counterparts are called, not surprisingly, dual attachment stations (DAS).*

- Should this SAS fail, the concentrator detects this situation and uses an *optical bypass to isolate the failed SAS,*thereby keeping the ring connected.

SAS Connected to ma Concentrator



- As in 802.5, each network adaptor holds some number of bits between its input and output interfaces. Unlike 802.5, however, the buffer can be of different sizes in different stations, although never less than 9 bits nor more than 80 bits.
- It is also possible for a station to start transmitting bits out of this buffer before it is full. Of course, the total time it takes for a token to pass around the network is a function of the size of these buffers.
- For example, because FDDI is a 100-Mbps network, it has a 10-nanosecond (ns) bit time (each bit is 10 ns wide). If each station implements a 10-bit buffer and waits for the buffer to be half full before starting to transmit, then each station introduces a 5 × 10 ns = 50-ns delay into the total ring rotation time.

FDDI has other physical characteristics

- at most 500 stations.
- maximum distance of 2 km between any pair of stations .
- Overall, the network is limited to a total of 200 km of fiber, which means that, because of the dual nature of the ring, the total amount of cable connecting all stations is limited to 100 km.
- FDDI uses 4B/5B encoding.

Timed Token Algorithm

- *Target token rotation time (TTRT).(max TRT)*
- Specifically, each node measures the time between successive arrivals of the token. We call this the node"s *measured TRT*.
- If this measured TRT is greater than the agreed-upon TTRT, then the token is late, and the node does not transmit any data.
- If this measured TRT is less than the TTRT, then the token is early, and the node is allowed to hold the token for the difference between TTRT and the measured TRT.
- FDDI defines two classes of traffic: *synchronous an asynchronous*.

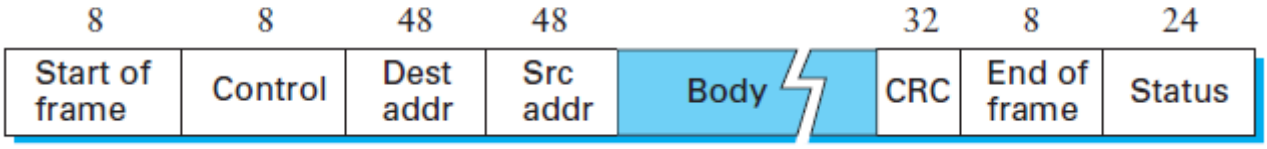
- When a node receives a token, it is always allowed to send synchronous data, without regard for whether the token is early or late. In contrast, a node can send asynchronous traffic only when the token is early.
- Synchronous is delay sensitive used to send voice or video data.

Asynchronous means that the application is more interested in throughput than delay. It is used for file transfer application.

Token Maintenance

- First, all nodes on an FDDI ring monitor the ring to be sure that the token has not been lost.
- Observe that in a correctly functioning ring, each node should see a valid transmission—either a data frame or the token—every so often.
- The greatest idle time between valid transmissions that a given node should experience is equal to the ring latency plus the time it takes to transmit a full frame, which on a maximally sized ring is a little less than 2.5 ms.
- Therefore, each node sets a timer event that fires after 2.5 ms. If this timer expires, the node suspects that something has gone wrong and transmits a "claim" frame.
- Every time a valid transmission is received, however, the node resets the timer back to 2.5 ms.
- The claim frames in FDDI differ from those in 802.5 because they contain the node's *bid for the TTRT, that is, the token rotation time that the node needs so that the* applications running on the node can meet their timing constraints.
- If this claim frame makes it all the way around the ring, then the sender removes it, knowing that its TTRT bid was the lowest.
- That node now holds the token—that is, it is responsible for inserting a valid token on the ring—and may proceed with the normal token algorithm.
- When a node receives a claim frame, it checks to see if the TTRT bid in the frame is less than its own. If it is, then the node resets its local definition of the TTRT to that contained in the claim frame and forwards the frame to the next node.
- If the bid TTRT is greater than that node's minimum required TTRT, then the claim frame is removed from the ring and the node enters the bidding process by putting its own claim frame on the ring.
- Should the bid TTRT be equal to the node's required TTRT, the node compares the address of the claim frame's sender with its own and the higher address wins.

Frame Format



Wireless (802.11)LAN

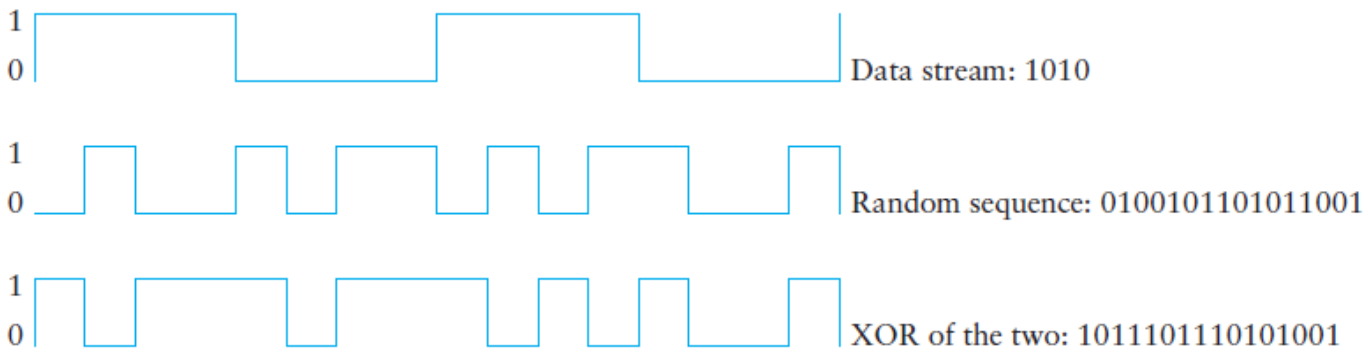
- Wireless networking is a rapidly evolving technology for connecting computers.
- standard IEEE 802.11.

Physical Properties:

- 802.11 was designed to run over three different physical media—two based on spread spectrum radio and one based on diffused infrared.
- The radio-based versions currently run at 11 Mbps, but may soon run at 54 Mbps.
- The idea behind spread spectrum is to spread the signal over a wider frequency band than normal, so as to minimize the impact of interference from other devices.
- For example, *frequency hopping is a spread* spectrum technique that involves transmitting the signal over a random sequence of frequencies; that is, first transmitting at one frequency, then a second, then a third, and so on.
- The sequence of frequencies is not truly random, but is instead computed algorithmically by a pseudorandom number generator.
- The receiver uses the same algorithm as the sender—and initializes it with the same seed—and hence is able to hop frequencies in sync with the transmitter to correctly receive the frame.
- A second spread spectrum technique, called *direct sequence, achieves the same* effect by representing each bit in the frame by multiple bits in the transmitted signal.
- For each bit the sender wants to transmit, it actually sends the exclusive-OR of that bit and *n random bits.*
- As with frequency hopping, the sequence of random bits is generated by a pseudorandom number generator known to both the sender and the receiver.
- The transmitted values, known as an *n-bit chipping code, spread the signal* across a frequency band that is *n times wider than the frame would have otherwise* required.
- 802.11 defines one physical layer using frequency hopping (over 79 1-MHz-wide frequency bandwidths) and a second using direct sequence (using an 11-bit chipping sequence). Both standards run in the 2.4-GHz frequency band of the electromagnetic spectrum.
- The third physical standard for 802.11 is based on infrared signals. The transmission is diffused, meaning that the sender and receiver do not have to be aimed at each other and do not need a clear line of sight. This technology has a range of up to about 10 m and is limited to the inside of buildings only.

Example 4-bit chipping sequence.

- Collision AvoidanceAt first glance, it might seem that a wireless protocol would follow exactly the same algorithm as the Ethernet—wait until the link becomes

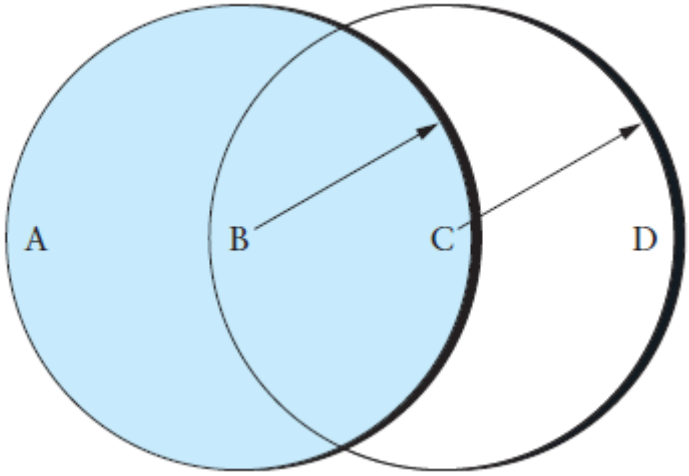


idle before transmitting and back off should a collision occur—and to a first approximation, this is exactly what 802.11 does.

- where each of four nodes is able to send and receive signals that reach just the nodes to its immediate left and right. For example, B can exchange frames with A and C but it cannot reach D, while C can reach B and D but not A.

- Suppose both A and C want to communicate with B and so they each send it a frame. A and C are unaware of each other since their signals do not carry that far. These two frames collide with each other at B, but unlike an Ethernet, neither A nor C is aware of this collision. A and C are said to be *hidden nodes with respect to each other.*

Example wireless network



- 802.11 addresses these two problems with an algorithm called Multiple Access with Collision Avoidance (MACA). The idea is for the sender and receiver to exchange control frames with each other before the sender actually transmits any data.

- This exchange informs all nearby nodes that a transmission is about to begin. Specifically, the sender transmits a *Request to Send (RTS) frame to the receiver; the RTS frame* includes a field that indicates how long the sender wants to hold the medium (i.e., it specifies the length of the data frame to be transmitted).

- The receiver then replies with a *Clear to Send (CTS) frame; this frame echoes this length field back to the sender.*
- Any node that sees the CTS frame knows that it is close to the receiver, and therefore cannot transmit for the period of time it takes to send a frame of the specified length. Any First, the receiver sends an ACK to the sender after successfully receiving a frame. All nodes must wait for this ACK before trying to transmit.

- Second, should two or more nodes detect an idle link and try to transmit an RTS frame at the same time, their RTS frames will collide with each other.

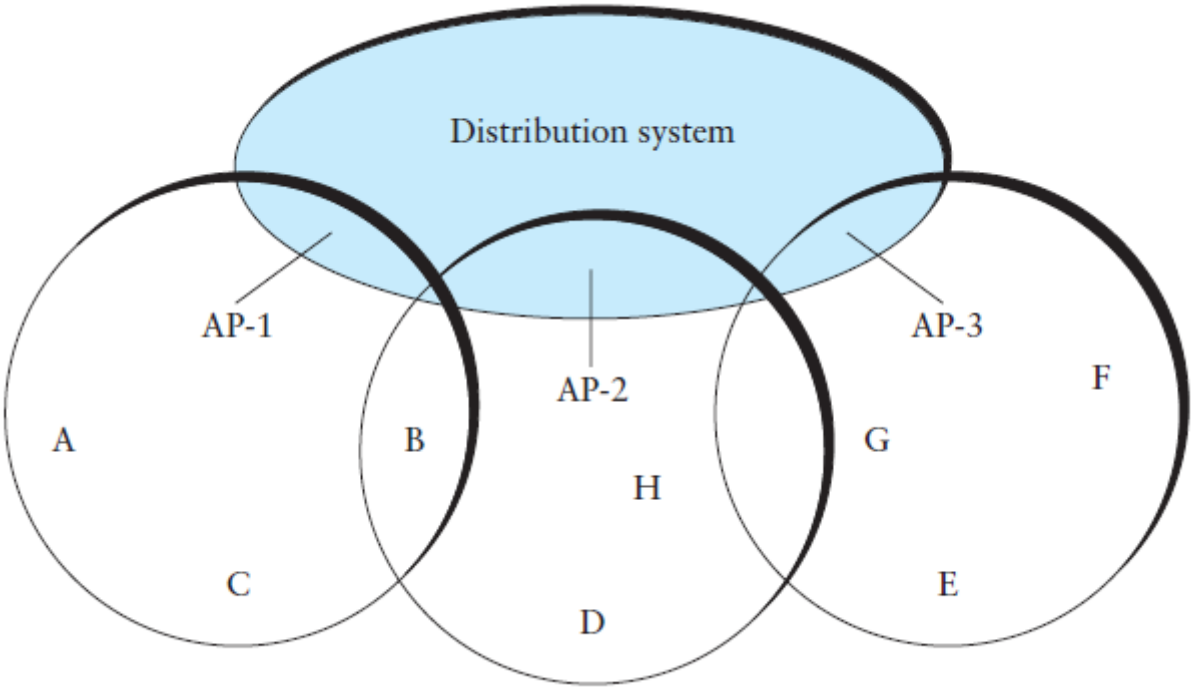
- 802.11 does not support collision detection, but instead the senders realize the collision has happened when they do not receive the CTS frame after a period of time, in which case they each wait a random amount of time before trying again.

- The amount of time a given node delays is defined by the same exponential backoff algorithm used on the Ethernetnode that sees the RTS frame but not the CTS frame is not close enough to the receiver to interfere with it, and so is free to transmit.

Distribution System

- As described so far, 802.11 would be suitable for an adhoc configuration of nodes that may or may not be able to communicate with all other nodes, depending on how far apart they are.
- Moreover, since one of the advantages of a wireless network is that nodes are free to move around—they are not tethered by wire—the set of directly reachable nodes may change over time.
- Nodes are free to directly communicate with each other as just described, but in practice, the operate within this structure.
- Instead of all nodes being created equal, some nodes are allowed to roam (e.g., your laptop) and some are connected to a wired network infrastructure.
- The latter are called *access points (AP), and they are connected to each other by a so-called* distribution system.

Access points connected to a distribution



- In this example distribution system that connects three access points, each of which services the nodes in some region. Each of these regions is analogous to a cell in a cellular phone system, with the APs playing the same role as a base station.
- Distribution network runs at layer 2 of the ISO architecture; that is,it does not depend on any higher-level protocols.
- Although two nodes can communicate directly with each other if they are within reach of each other, the idea behind this configuration is that each node associates itself with one access point.
- For node A to communicate with node E, for example, A first sends a frame to its access point (AP-1), which forwards the frame across the distribution system to AP-3, which finally transmits the message to node E. In this example distribution system that connects three access points, each of which services the nodes in some region. Each of these regions is analogous to a cell in a cellular phone system, with the APs playing the same role as a base station.

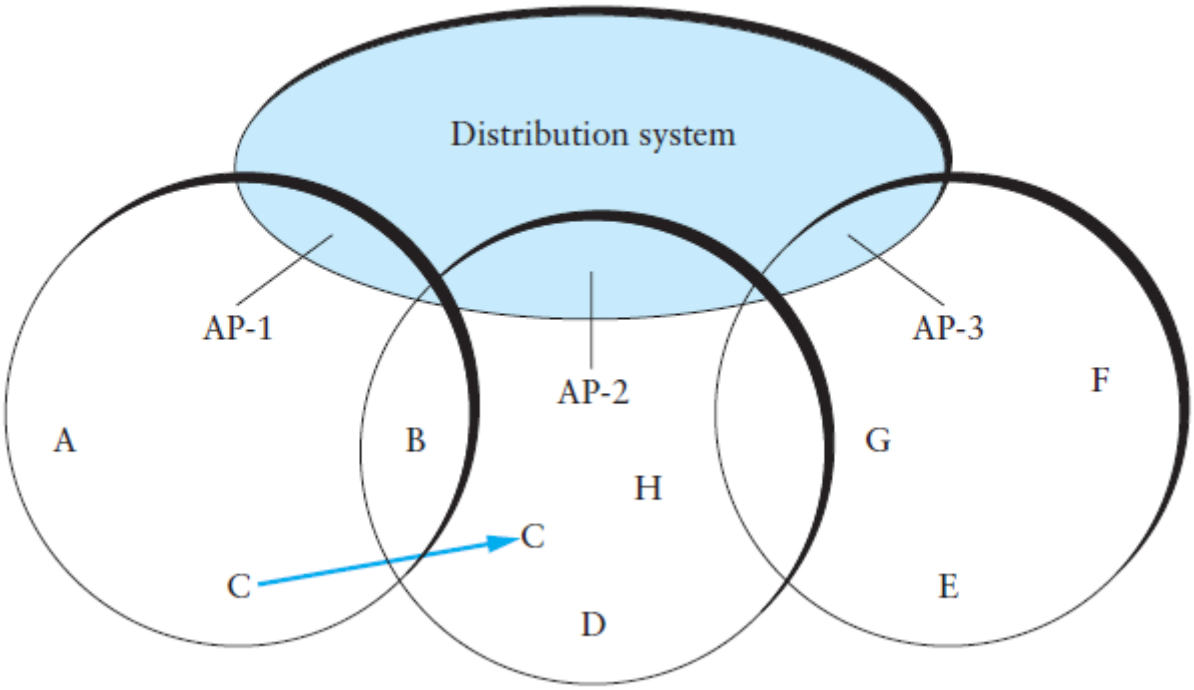
The technique for selecting an AP is called *scanning and involves the following* four steps:
1 .The node sends a Probe frame.

2 .All APs within reach reply with a Probe Response frame.
3. The node selects one of the access points and sends that AP an Association Request frame.
4. The AP replies with an Association Response frame

- A node engages this protocol whenever it joins the network, as well as when it becomes unhappy with its current AP. This might happen, for example, because the signal from its current AP has weakened due to the node moving away from it.

- Whenever a node acquires a new AP, the new AP notifies the old AP of the change (this happens in step 4)via the distribution system.

Node Mobility

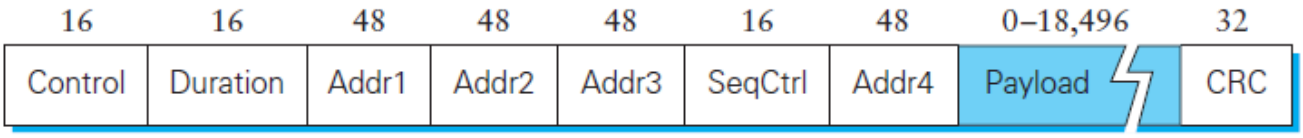


- where node C moves from the cell serviced by AP-1 to the cell serviced by AP-2. As it moves, it sends Probe frames, which eventually result in Probe Response frames from AP-2. At some point, C prefers AP-2 over AP-1, and so it associates itself with that access point.

- The mechanism just described is called *active scanning since the node is actively* searching for an access point.

- APs also periodically send a Beacon frame that advertises the capabilities of the access point; these include the transmission rates supported by the AP. This is called *passive scanning, and a node can change to this AP based on the* Beacon frame simply by sending it an Association Request frame back to the access point.

Frame Format



- The frame contains the source and destination node addresses, each of which are 48 bits long; up to 2312 bytes of data;
- and a 32-bit CRC.
- The Control field contains three subfields of interest (not shown): a 6-bit Type field that indicates whether the frame carries data, is an RTS or CTS frame, or is being used by the scanning algorithm.
- and a pair of 1-bit fields—called ToDS and FromDS—that are described below.
- In the simplest case, when one node is sending directly to another, both the DS bits are 0, Addr1 identifies the target node, and Addr2 identifies the source node. In the most complex case, both DS bits are set to 1, indicating that the message went from a wireless node onto the distribution system, and then from the distribution system to another wireless node. With both bits set, Addr1 identifies the ultimate destination, Addr2 identifies the immediate sender.
- Addr3 identifies the intermediate destination (the one that accepted the frame from a wireless node and forwarded it across the distribution system),and Addr4 identifies the original source.
- Addr1 corresponds to E, Addr2 identifies AP-3, Addr3 corresponds to AP-1, and Addr4 identifies A.

Bridges and LAN Switches

1. switch that is used to forward packets between shared-media LANs such as Ethernets.

2. It is also called as LAN switches.
3. historically they have also been referred to as bridges.

4. a pair of Ethernets interconnected by using repeater.

5. An alternative way is to put a node between the two Ethernets and have the node forward frames from one Ethernet to the other, this node is called bridge.

6. And a collection of LANs connected by one or more bridges is usually said to form an *extended LAN*.

7. This node would be in promiscuous mode.

8. For example, while a single Ethernet segment can carry only 10 Mbps of total traffic, an Ethernet bridge can carry as much as 10*n Mbps, where n is the number* of ports (inputs and outputs) on the bridge.

Learning Bridges

1. Whenever the bridge receives a frame on port 1 that is addressed to host A, it would not forward the frame out on port 2; there would be no need because host A would have already directly received the frame on the LAN connected to port 1.

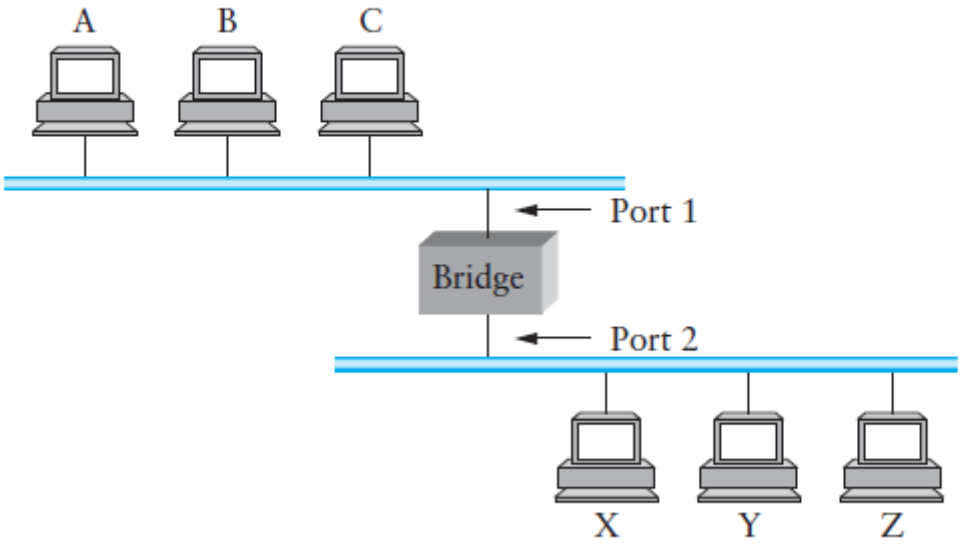
2. Anytime a frame addressed to host A was received on port 2, the bridge would forward the frame out on port 1.

3. Bridges forward frames on datagram model.

4. It also uses forwarding table to forward the incoming frames to the output node.

5. The idea is for each bridge to inspect the *source* address in all the frames it receives.

Illustration Of A Learning Bridge.



Forwarding Table

1. When a bridge first boots, this table is empty; entries are added over time.

2.Also, a timeout is associated with each entry, and the bridge discards the entry after a specified period of time.

Forwarding table maintained by a bridge

Host	Port
A	1
B	1
C	1
X	2
Y	2
Z	2

Implementation

1. Structure Bridge Entry defines a single entry in the bridge‟s forwarding table.

2. These are stored in a Map structure.

3. (which supports mapCreate, mapBind, and MapResolve operations.

4. The constant MAX TTL specifies how long an entry is kept in the table.

Table Creation Routine

```
#define BRIDGE_TAB_SIZE  1024 /* max. size of bridging table */
#define MAX_TTL           120 /* time (in seconds) before an
                                 entry is flushed */

typedef struct {
    MacAddr     destination;  /* MAC address of a node */
    int         ifnumber;     /* interface to reach it */
    u_short     TTL;          /* time to live */
    Binding     binding;      /* binding in the Map */
} BridgeEntry;

int     numEntries = 0;
Map     bridgeMap = mapCreate(BRIDGE_TAB_SIZE,
                              sizeof(BridgeEntry));
```

- The routine that updates the forwarding table when a new packet arrives is given by updateTable.
- The arguments passed are the source MAC address containedin the packet and the interface number on which it was received.
- shown here, is invoked at regular intervals, scans the entries in the forwarding table,
- and decrements the TTL (time to live) field of each entry, discarding any entries whose TTL has reached 0. Note that the TTL is reset to MAX TTL every time a packet arrives .

Table Updation when new Entries added

```
void
updateTable (MacAddr src, int inif)
{
   BridgeEntry      *b;

   if (mapResolve(bridgeMap, &src, (void **)&b) == FALSE)
   {
       /* this address is not in the table, so try to add it */
       if (numEntries < BRIDGE_TAB_SIZE)
       {
           b = NEW(BridgeEntry);
           b->binding = mapBind( bridgeMap, &src, b);
           /* use source address of packet as dest. address in
              table */
           b->destination = src;
           numEntries++;
       }
       else
       {
           /* can't fit this address in the table now, so give
              up */
```

```
            return;
        }
    }
    /* reset TTL and use most recent input interface */
    b->TTL = MAX_TTL;
    b->ifnumber = inif;
}
```

Spanning Tree Algorithm

1) Loops in a extended LAN,purpose—to provide redundancy in case of failure.

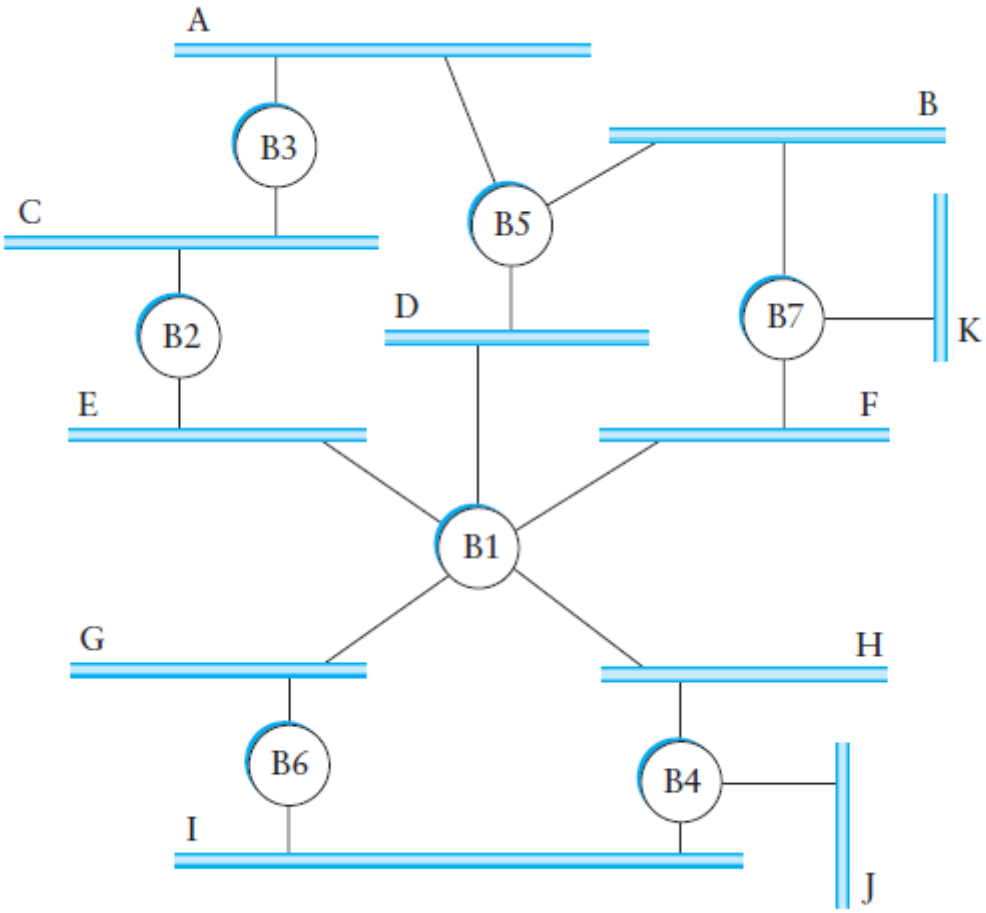
2) bridges must be able to correctly handle loops.

3) This problem is addressed by having the distributed *spanning tree algorithm.*

4) *If you* think of the extended LAN as being represented by a graph that possibly has loops (cycles).

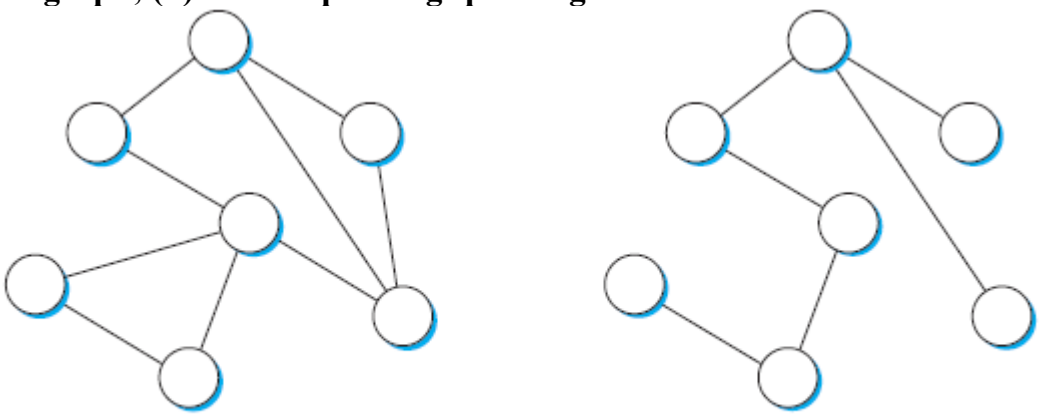
5) then a spanning tree is a subgraph of this graph that covers (spans) all the vertices, but contains no cycles.

6) That is, a spanning tree keeps all of the vertices of the original graph, but throws out some of the edges.



Extended LAN with loops

a) **a cyclic graph; (b) a corresponding spanning tree**



1. The spanning tree algorithm, which was developed by Radia Perlman at Digital.

2. is a protocol used by a set of bridges to agree upon a spanning tree for a particular extended LAN.

3. The main idea of the spanning tree is for the bridges to select the ports over which they will forward frames.

4. The algorithm selects ports as follows. Each bridge has a unique identifier; for our purposes, we use the labels B1, B2, B3, and so on.
5. The algorithm first elects the bridge with the smallest id as the root of the spanning tree; exactly how this election takes place is described below.

6. The root bridge always forwards frames out over all of its ports.

Path Selection

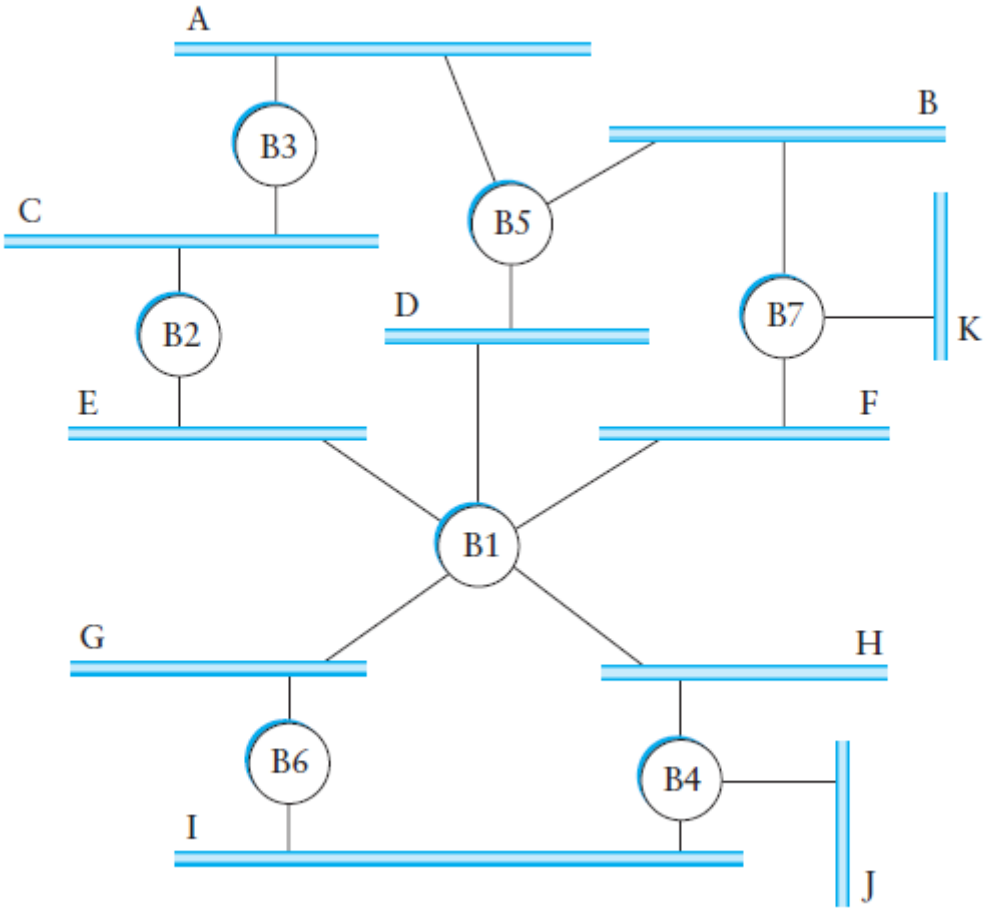
1. each bridge computes the shortest path to the root and notes which of its ports is on this path

2. This port is also selected as the bridge"s preferred path to the root.

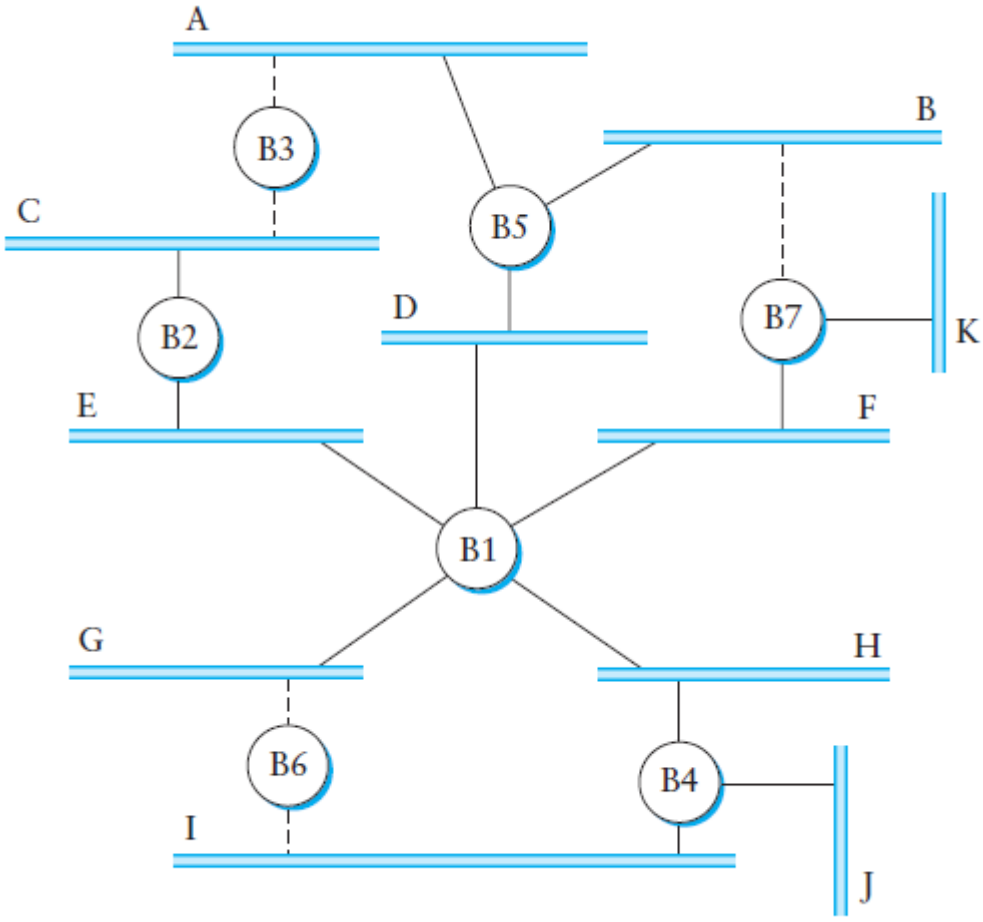
3. Finally, all the bridges connected to a given LAN elect a single *designated bridge that will be responsible for forwarding frames toward* the root bridge.

4. designated bridge is the one that is closest to the root, and if two or more bridges are equally close to the root, then the bridges" identifiers are used to break ties; the smallest id wins.

Extended LAN with loops.



Spanning tree with some ports not selected



1. B1 is the root bridge, since it has the smallest id.

2. Notice that both B3 and B5 are connected to LAN A, but B5 is the designated bridge since it is closer to the root.

3. Similarly, both B5 and B7 are connected to LAN B, but in this case, B5 is the designated bridge since it has the smaller id; both are an equal distance from B1.

4. the bridges in an extended LAN do not have the luxury of being able to see the topology of the entire network.

5. Instead, the bridges have to exchange configuration messages with each other and then.

6. Based on this the root or a designated bridge will be decide.

- The configuration messages contain three pieces of information.

1. the id for the bridge that is sending the message

2. the id for what the sending bridge believes to be the root bridge

3. the distance, measured in hops, from the sending bridge to the root bridge.

1. Initially, each bridge thinks it is the root.

2. and so it sends a configuration message out on each of its ports identifying itself as the root.

3. and giving a distance to the root of 0.
4. Upon receiving a configuration message over a particular port, the bridge checks to see if that new message is better than the current best configuration message recorded for that port.

5. The new configuration message is considered “better” than the currently recorded information if

- it identifies a root with a smaller id or
- it identifies a root with an equal id but with a shorter distance or
- the root id and distance are equal, but the sending bridge has a smaller id.
- If the new message is better than the currently recorded information, the bridge discards the old information and saves the new information.
- However, it first adds 1 to the distance-to-root field since the bridge is one hop farther away from the root than the bridge that sent the message.

1. B3 receives (B2, 0, B2).

2. Since 2 < 3, B3 accepts B2 as root.

3. B3 adds one to the distance advertised by B2 (0) and thus sends (B2, 1, B3)toward B5.

4. Meanwhile, B2 accepts B1 as root because it has the lower id, and it sends (B1, 1, B2) toward B3.

5. B5 accepts B1 as root and sends (B1, 1, B5) toward B3.

6. B3 accepts B1 as root, and it notes that both B2 and B5 are closer to the root.

7. than it is. Thus B3 stops forwarding messages on both its interfaces.

Broadcast and Multicast

- Bridges must also support these broadcast and multicast transmissions.
- Broadcast is simple—each bridge forwards a frame with a destination broadcast address out on each active (selected) port other than the one on which the frame was received.
- Multicast can be implemented in exactly the same way, with each host deciding for itself whether or not to accept the message.
- Not all the LANs in an extended LAN necessarily have a host that is a member of a particular multicast group.

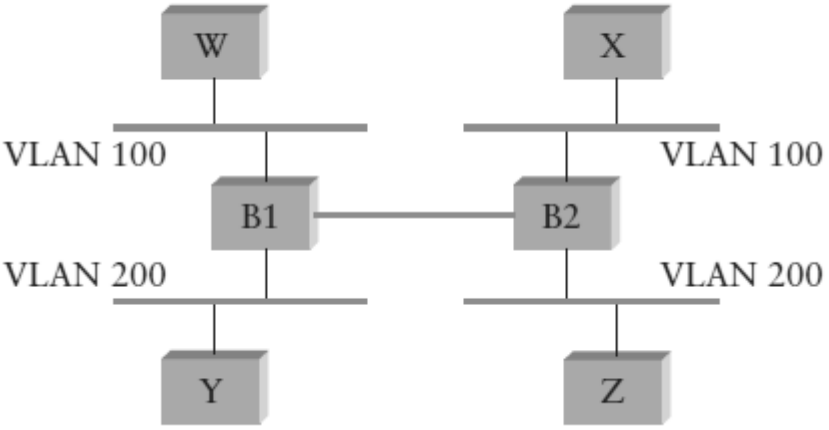
Consider the figure spanning tree with some ports are not selected.

- In that a frame sent to group M by a host on LAN A , If there is no host on LAN J that belongs to group M, then there is no need for bridge B4 to forward the frames over that network.
- On the other hand, not having a host on LAN H that belongs to group M does not necessarily mean that bridge B1 can avoid forwarding multicast frames onto LAN H. It all depends on whether or not there are members of group M on LANs I and J.
- It learns exactly the same way that a bridge learns whether it should forward a unicast frame over a particular port—by observing the *source addresses that it* receives over that port.
- In particular, each host that is a member of group M must periodically send a frame with the address for group M in the source field of the frame header. This frame would have as its destination address the multicast address for the bridges.

Limitations of Bridges

- On the issue of scale, it is not realistic to connect more than a few LANs by means of bridges, where in practice "few" typically means "tens of.
- One reason for this is that the spanning tree algorithm scales linearly; that is, there is no provision for imposing a hierarchy on the extended LAN.
- A second reason is that bridges forward all broadcast frames.
- One approach to increasing the scalability of extended LANs is the *virtual LAN*(VLAN). VLANs allow a single extended LAN to be partitioned into several seemingly separate LANs.
- Each virtual LAN is assigned an identifier (sometimes called a *color),*and packets can only travel from one segment to another if both segments have the same identifier.

Two virtual LANs share a common backbone



- shows four hosts on four different LAN segments. In the absence of VLANs, any broadcast packet from any host will reach all the other hosts.
- Now let"s suppose that we define the segments connected to hosts W and X as being in one VLAN, which we"ll call VLAN 100. We also define the segments that connect to hosts Y and Z as being in VLAN 200.
- To do this, we need to configure a VLAN ID on each port of bridges B1 and B2.

The link between B1 and B2 is considered to be in both VLANs.

- When a packet sent by host X arrives at bridge B2, the bridge observes that it came in a port that was configured as being in VLAN 100.
- It inserts a VLAN header between the Ethernet header and its payload. The interesting part of the VLAN header is the VLAN ID; in this case, that ID is set to 100.
- The bridge now applies its normal rules for forwarding to the packet, with the extra restriction that the packet may not be sent out an interface that is not part of VLAN 100.
- Thus, under no circumstances will the packet—even a broadcast packet—be sent out the interface to host Z, which is in VLAN 200. The packet is, however, forwarded to bridge B1, which follows the same rules, and thus may forward the packet to host W but not to host Y.
- Their *main advantage* is that they allow multiple LANs to be transparently connected; that is, the networks can be connected without the end hosts having to run any additional protocols.
- Disadvantage: The latency between any pair of hosts on an extended LAN becomes both larger and more highly variable.