Department of Computer and IT Engineering
University of Kurdistan

Computer Networks I

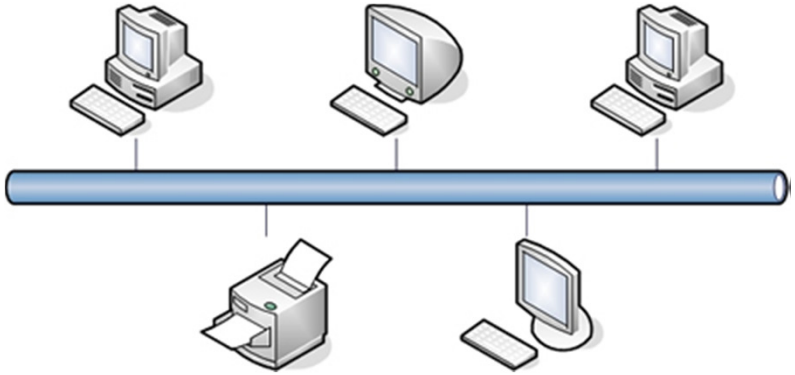
Media Access Control (MAC)

(with some IEEE 802 standards)

By: Dr. Alireza Abdollahpouri

Media Access Control

Multiple access links



There is 'collision' if more than one node sends at the same time only one node can send successfully at a time

Media Access Control

- When a "collision" occurs, the signals will get distorted and the frame will be lost ⟹ the link bandwidth is wasted during collision
- Question: How to coordinate the access of multiple sending and receiving nodes to the **shared link** ?
- Solution: We need a protocol to determine how nodes share channel ⟹ Medium Access control (MAC) protocol
- The main task of a MAC protocol is to minimize collisions in order to utilize the bandwidth by:
  - Determining when a node can use the link (medium)
  - What a node should do when the link is busy
  - What the node should do when it is involved in collision

Ideal Multiple Access Protocol

1. When one node wants to transmit, it can send at rate R bps, where R is the channel rate.

2. When M nodes want to transmit, each can send at average rate R/M (fair)

3. fully decentralized:
   - No special node to coordinate transmissions
   - No synchronization of clocks, slots

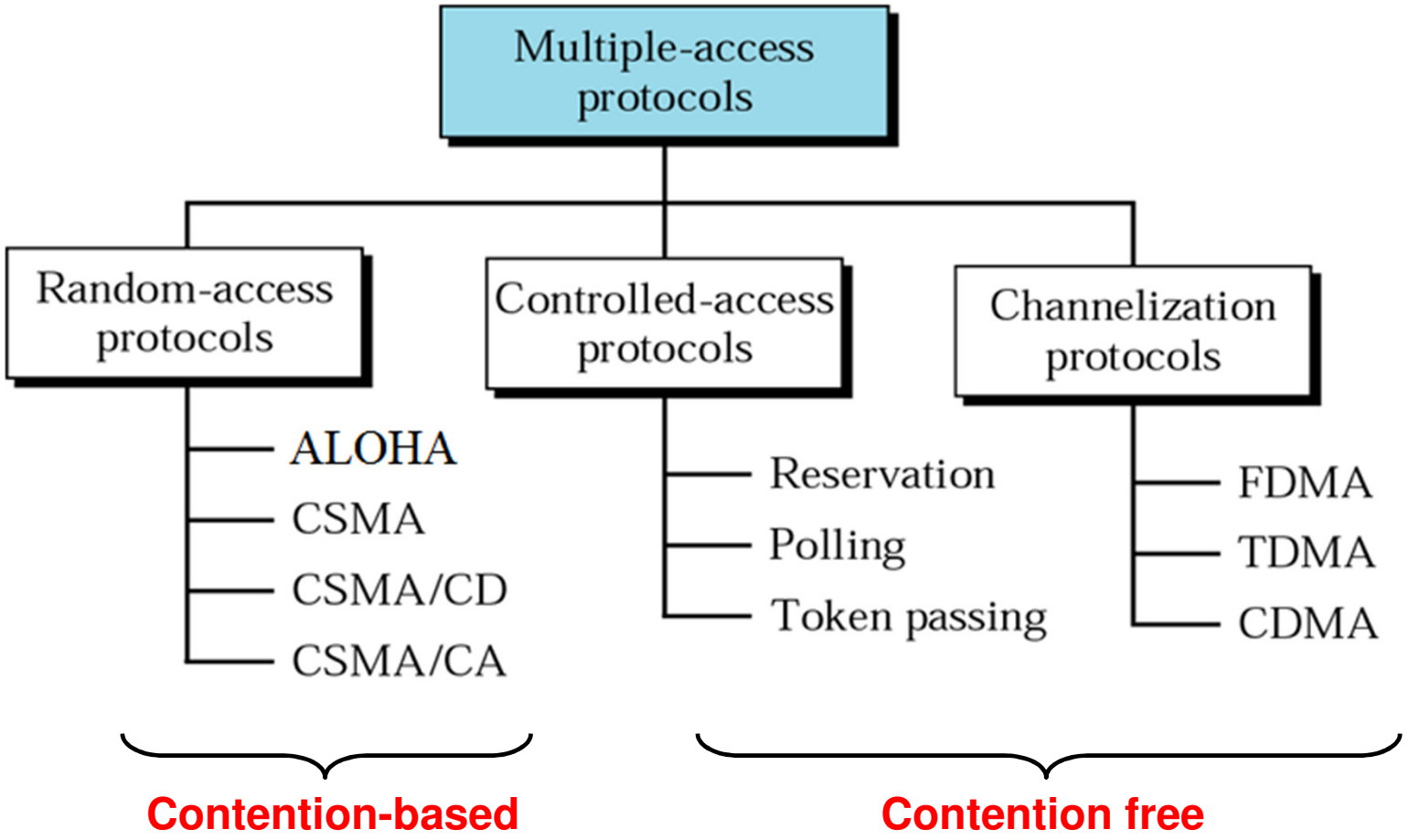
4. Simple

Does not exist!!

Three Ways to Share the Media

- **Channel partitioning MAC protocols:**
  - Share channel efficiently and fairly at high load
  - Inefficient at low load: delay in channel access, 1/N bandwidth allocated even if only 1 active node!
- **"Taking turns" protocols**
  - Eliminates empty slots without causing collisions
  - Vulnerable to failures (e.g., failed node or lost token)
- **Random access MAC protocols**
  - Efficient at low load: single node can fully utilize channel
  - High load: collision overhead

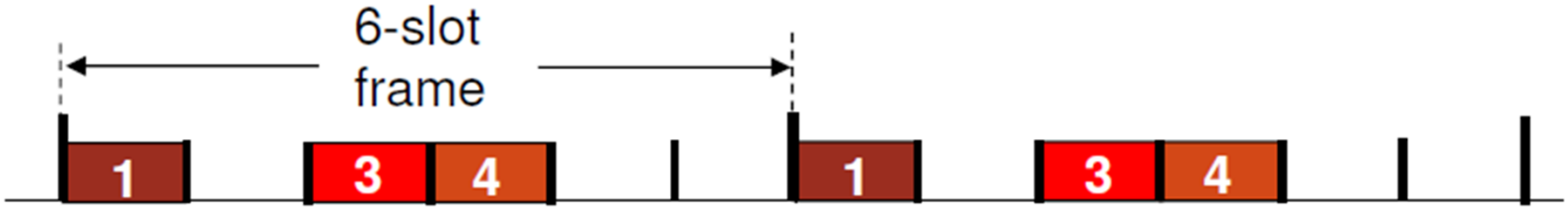
Multiple Access Protocols



Channel Partitioning: TDMA

TDMA: time division multiple access

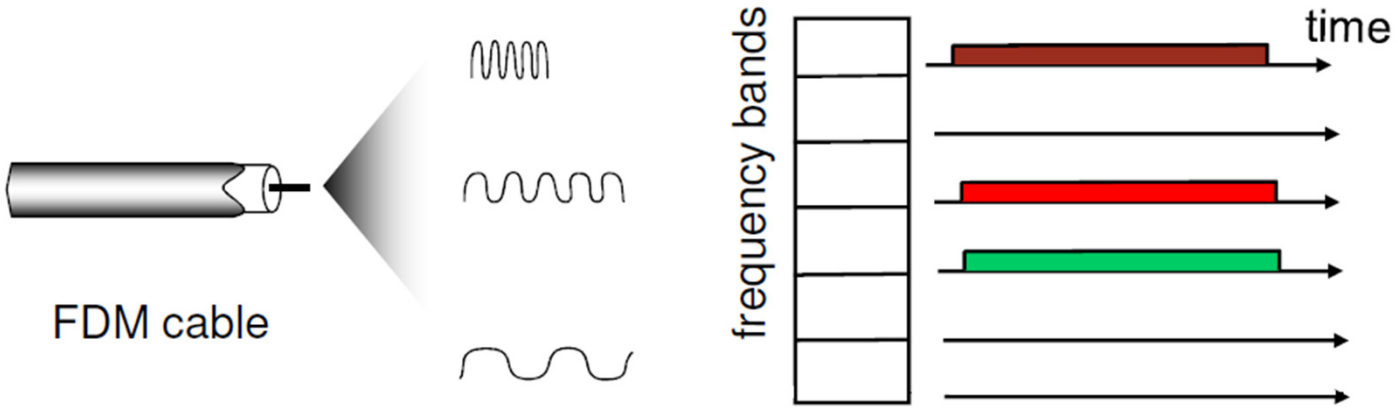
- Access to channel in "rounds"
  - Each station gets fixed length slot in each round
- Time-slot length is packet transmission time
  - Unused slots go idle
- Example: 6-station LAN with slots 1, 3, and 4



Channel Partitioning: FDMA

FDMA: frequency division multiple access

- Channel spectrum divided into frequency bands
  - Each station assigned fixed frequency band
- Unused transmission time in bands go idle
- Example: 6-station LAN with bands 1, 3, and 4

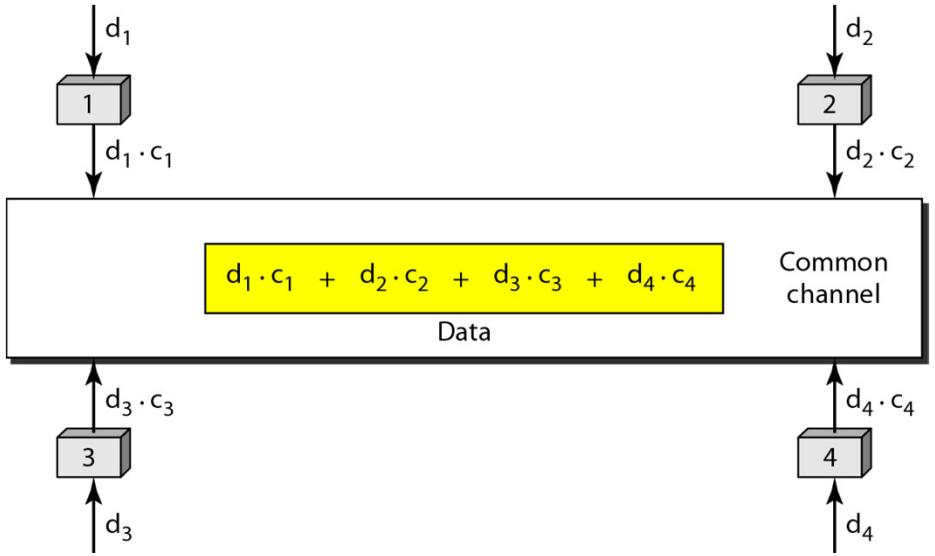


Channel Partitioning: CDMA

CDMA: Code division multiple access

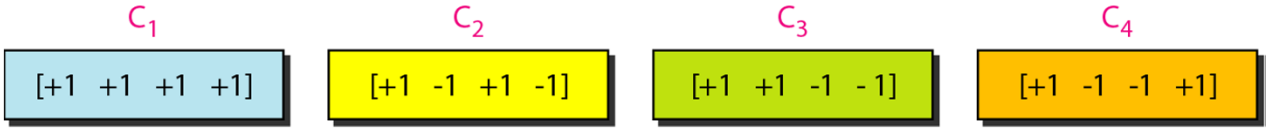
- One channel carries all transmissions simultaneously
- Two properties: If we multiply each code by another, we get 0.
  If we multiply each code by itself, we get 4
- Data = $(d_1 \cdot c_1 + d_2 \cdot c_2 + d_3 \cdot c_3 + d_4 \cdot c_4) \cdot c_1$

  $= d_1 \cdot c_1 \cdot c_1 + d_2 \cdot c_2 \cdot c_1 + d_3 \cdot c_3 \cdot c_1 + d_4 \cdot c_4 \cdot c_1 = 4 \cdot d_1$

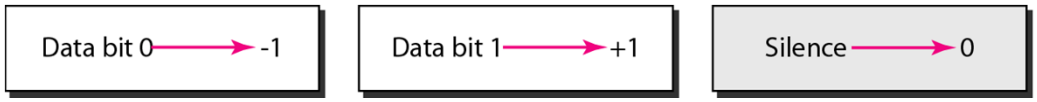


CDMA: Chips

- Sequence of numbers called **chips**

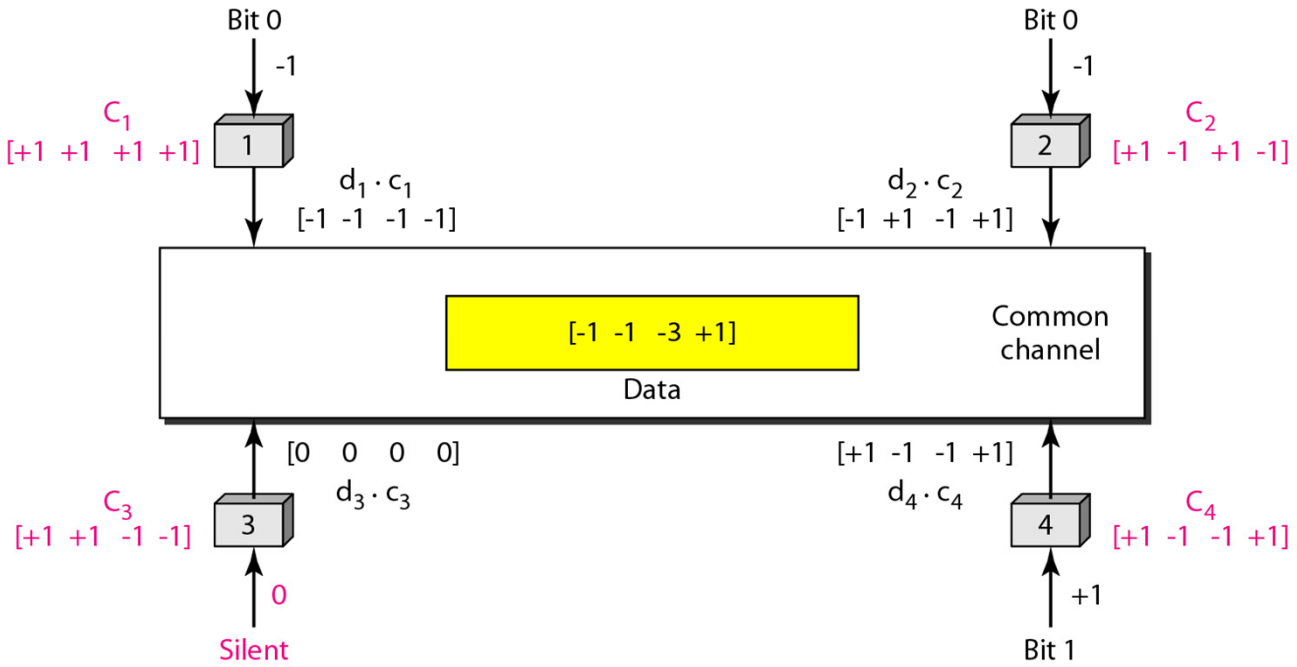


- **Orthogonal sequences have the following properties:**
  - **Each sequence is made of N elements, where N is the number of stations**
  - **If we multiply a sequence by a number, every element in the sequence is multiplied by that element (scalar multiplication)**
  - **If we multiply two equal sequence, element by element, and add the results, we get N (inner product)**
  - **If we multiply two different sequence, element by element, and add the results, we get 0**
  - **Adding two sequence means adding the corresponding elements. The result is another sequence**
- **Data representation in CDMA**



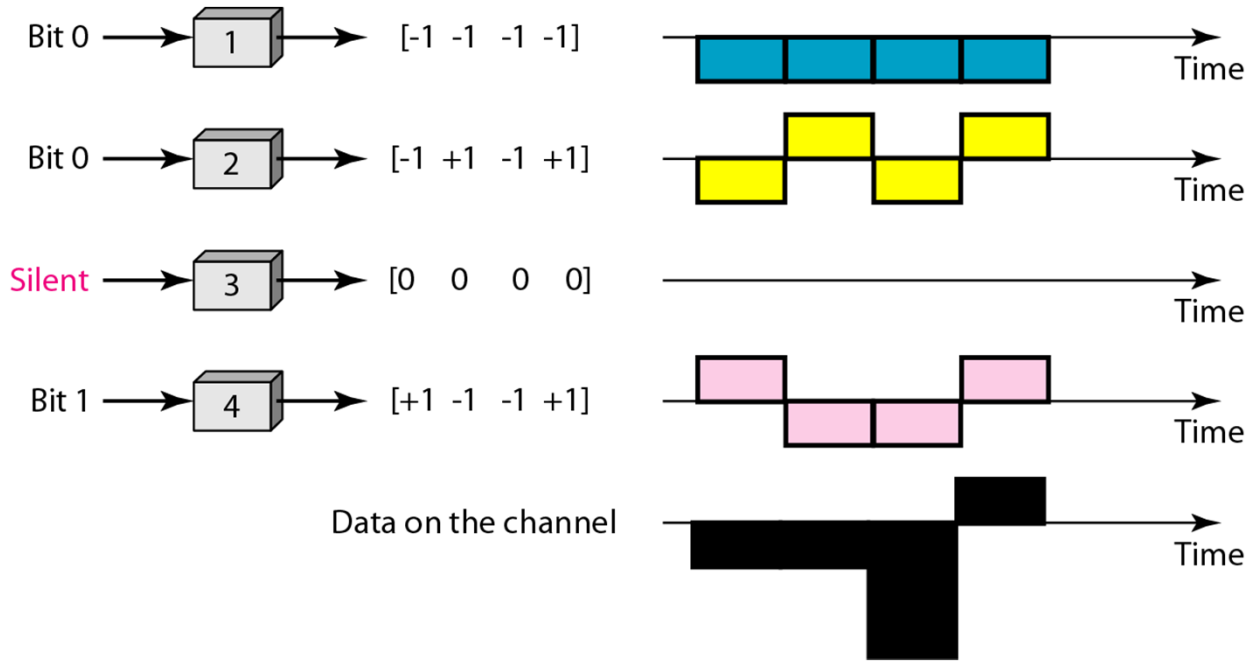
CDMA: Encoding and Decoding

- Show how four stations share the link during a 1-bit interval



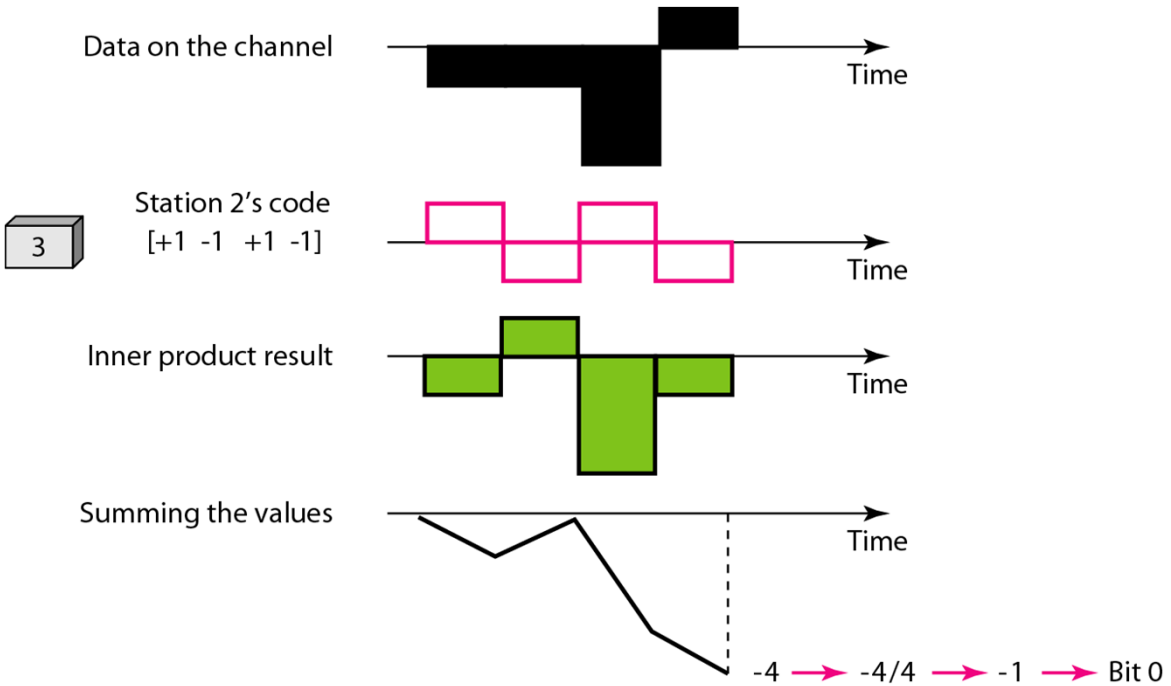
CDMA: Signal Level

- Digital signal created by four stations in CDMA using NRZ-L for simplicity

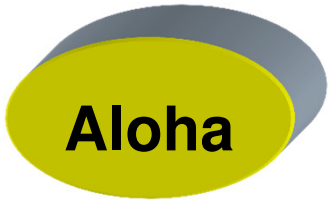


CDMA: Decoding

- Show how station 3 can detect the data by station 2 by using the code for station 2
- Decoding of the composite signal for one in CDMA



Evolution of Contention Protocols



Developed in the 1970s for a packet radio network

Improvement: Start transmission only at fixed times (slots)

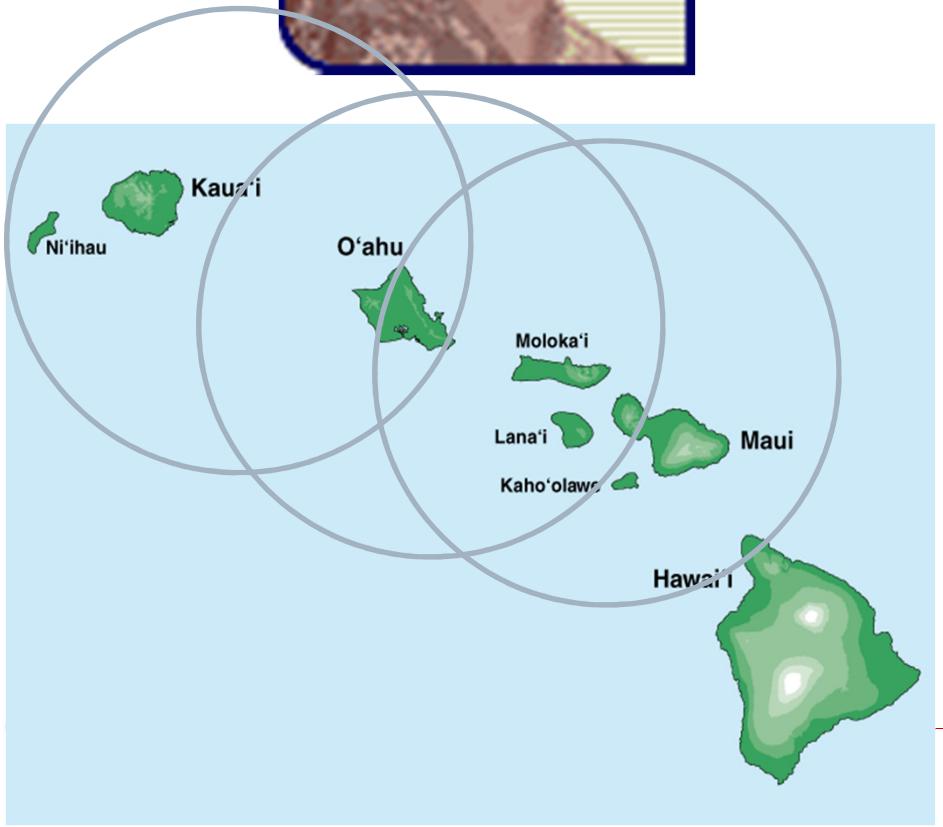
CSMA = Carrier Sense Multiple Access
Improvement: Start transmission only if no transmission is ongoing

CD = Collision Detection
Improvement: Stop ongoing transmission if a collision is detected (e.g. Ethernet)

ALOHA

- **Pure ALOHA**
  - Developed by Abramson in the 1970s for a packet radio network by Hawaii University.
  - Whenever a station has a data, it transmits immediately. Sender finds out whether transmission was successful or experienced a collision by listening to the broadcast from the destination station. Sender retransmits after some random time if there is a collision.
- **Slotted ALOHA**
  - Improvement: Time is slotted and a packet can only be transmitted at the beginning of one slot. Thus, it can reduce the collision duration.

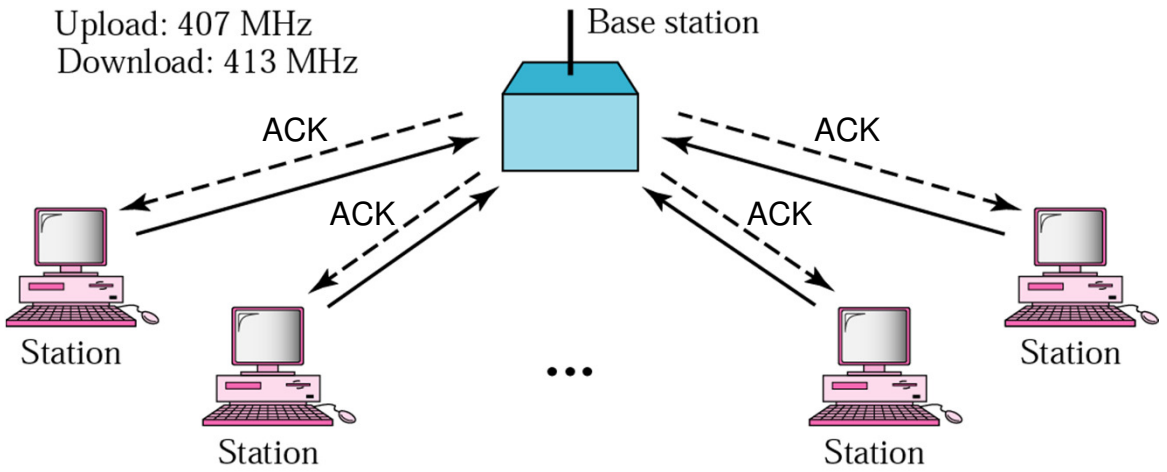
Where it all Started: AlohaNet



- Norm Abramson left Stanford in 1970 (***so he could surf!)***
- Set up first data communication system for Hawaiian islands
- Central hub at U. Hawaii, Oahu

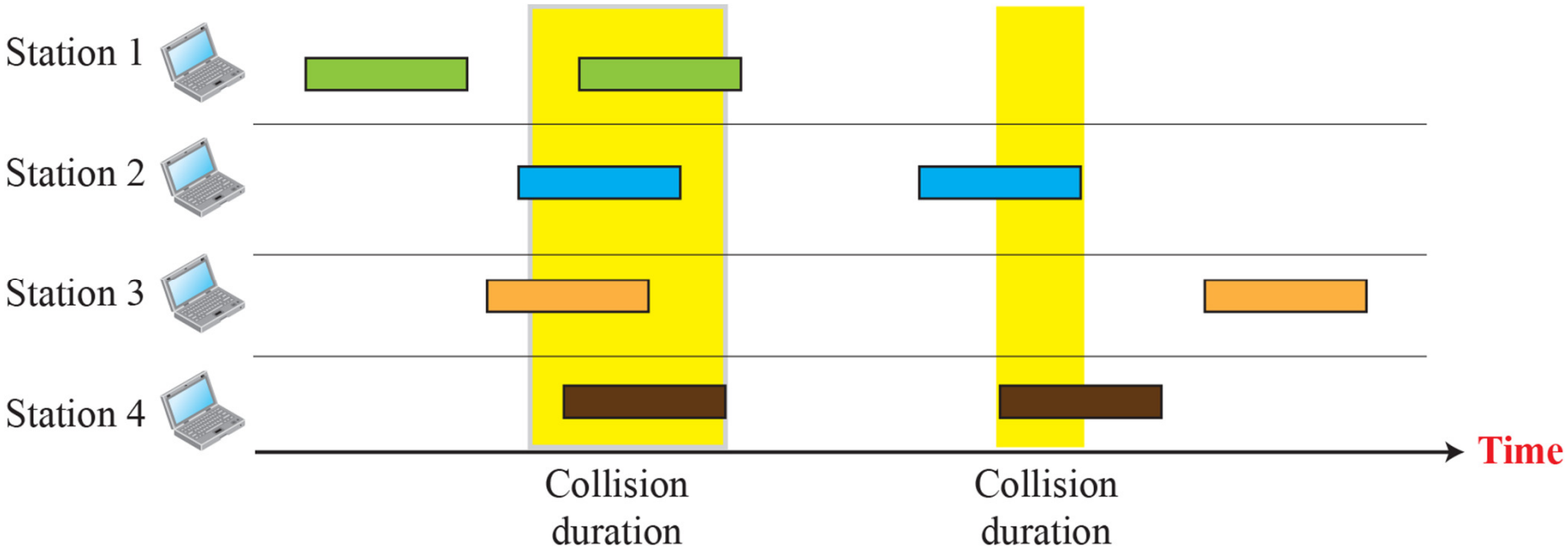
ALOHA

- Mountainous islands – land network difficult to install
- Fully decentralized protocol



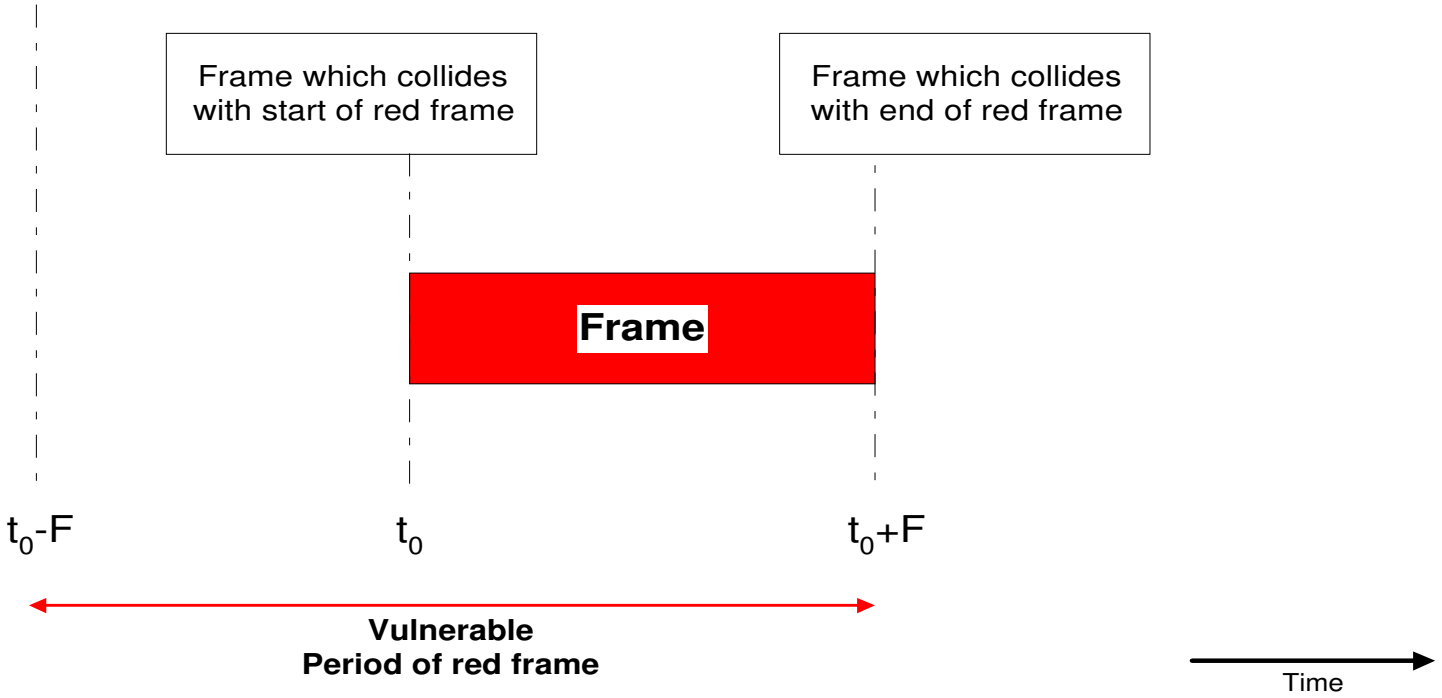
The node waits for an ACK for time-out equals to the maximum round-trip propagation delay = 2* t_{prop}

Frame Transmission in pure ALOHA



If the frame is collided (no ACK was received) the stations wait for a random time and retransmit the frame again.

Throughput Analysis



- A frame (red frame) will be in a collision if and only if another transmission begins in the vulnerable period of the frame
- Vulnerable period has the **length of 2 frame times**

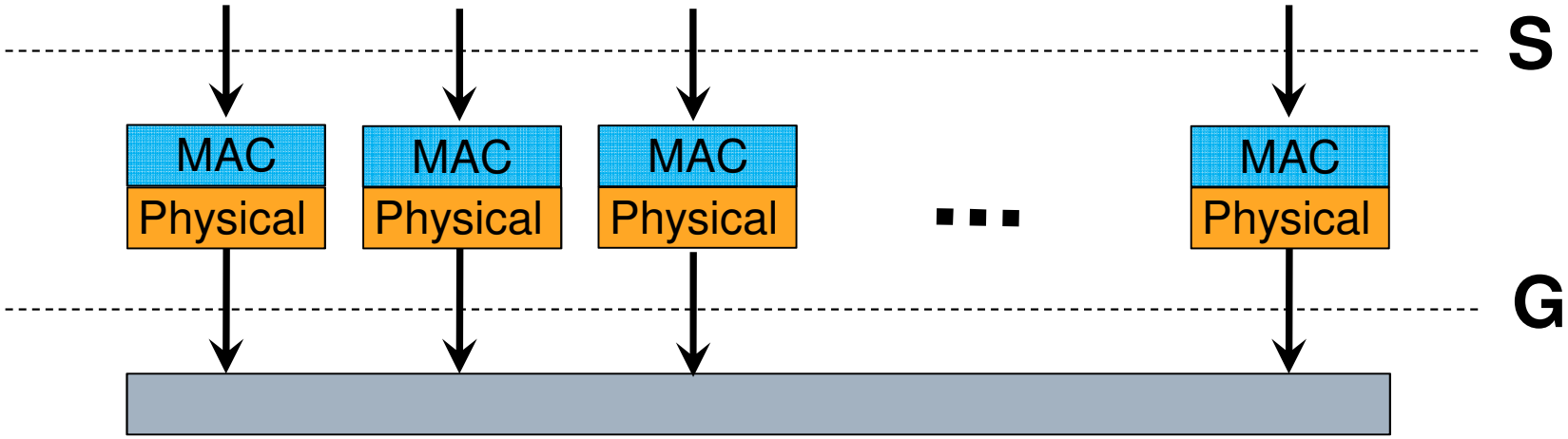
Vulnerable time- example

A pure ALOHA network transmits 200-bit frames on a shared channel of 200 kbps. What is the requirement to make this frame collision-free?

Solution

Average frame transmission time T_{fr} is 200 bits/200 kbps or 1 ms. The vulnerable time is 2×1 ms = 2 ms. This means no station should send later than 1 ms before this station starts transmission and no station should start sending during the one 1-ms period that this station is sending.

Throughput Analysis



S: throughput, average number of successful frame transmissions per second

G: load, average number of transmission attempts by all nodes **during one frame transmission time**

Throughput Analysis

$P_{success}$: Probability that a frame transmission is successful
= Probability that there are no additional transmissions in the vulnerable period

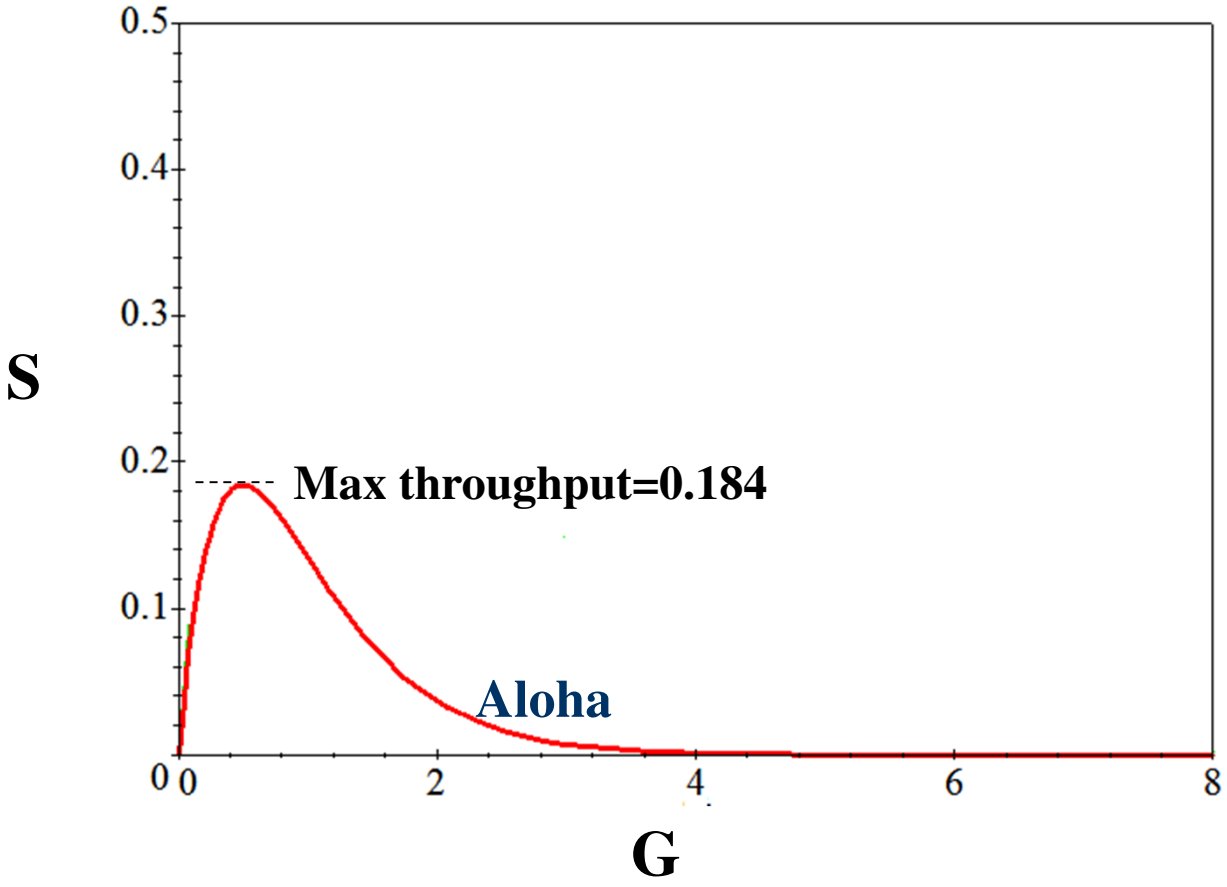
The probability of ***k*** transmission-attempts during the vulnerable period:

$$P(k) = \frac{(2G)^k e^{-2G}}{k!}$$

$P_{success} = P(0) = e^{-2G}$

$S = GP_{success} = Ge^{-2G}$

Throughput Analysis



For small G: S ≈ G, there is nearly no collision, S is small because the load is small

For large G: G >> S, there are many backlogged users, S is small because there are many collisions

ALOHA Throughput - example

A pure ALOHA network transmits 200-bit frames on a shared channel of 200 kbps. What is the throughput if the system (all stations together) produces

a. 1000 frames per second b. 500 frames per second

c. 250 frames per second.

Solution

The frame transmission time is 200/200 kbps or 1 ms.

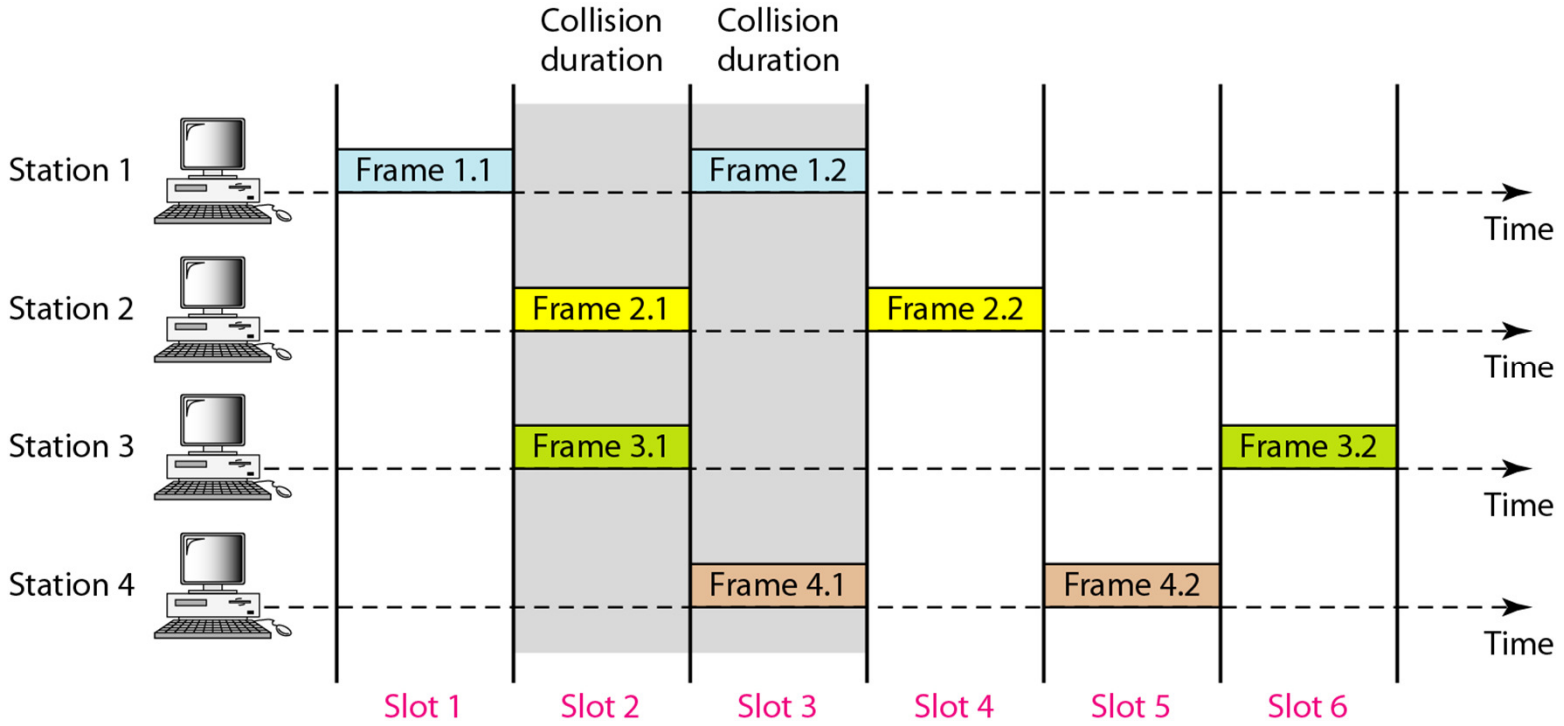
a. If the system creates 1000 frames per second, this is 1 frame per millisecond. The load is 1. In this case $S = G \times e^{-2G}$ or $S = 0.135$ (13.5 percent). This means that the throughput is $1000 \times 0.135 = 135$ frames. Only 135 frames out of 1000 will probably survive.

ALOHA Throughput - example

b. If the system creates 500 frames per second, this is (1/2) frame per millisecond. The load is (1/2). In this case $S = G \times e^{-2G}$ or $S = 0.184$ (18.4 percent). This means that the throughput is $500 \times 0.184 = 92$ and that only 92 frames out of 500 will probably survive. Note that this is the maximum throughput case, percentagewise.

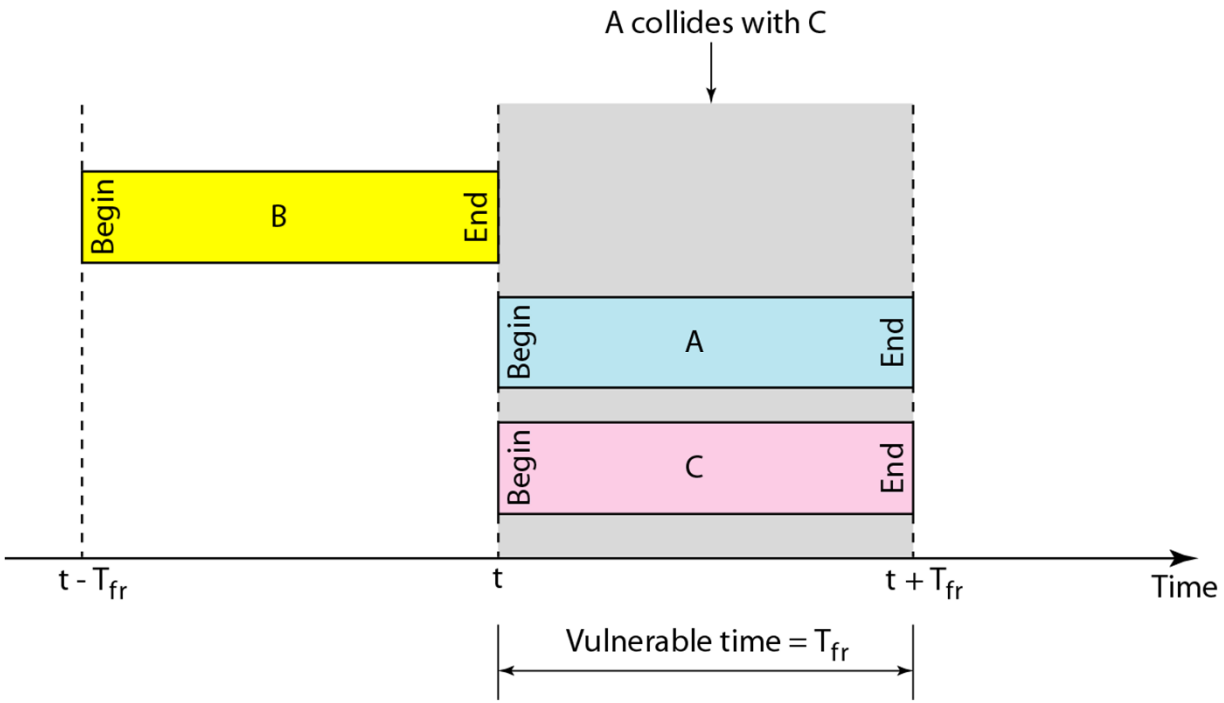
c. If the system creates 250 frames per second, this is (1/4) frame per millisecond. The load is (1/4). In this case $S = G \times e^{-2G}$ or $S = 0.152$ (15.2 percent). This means that the throughput is $250 \times 0.152 = 38$. Only 38 frames out of 250 will probably survive.

Slotted ALOHA



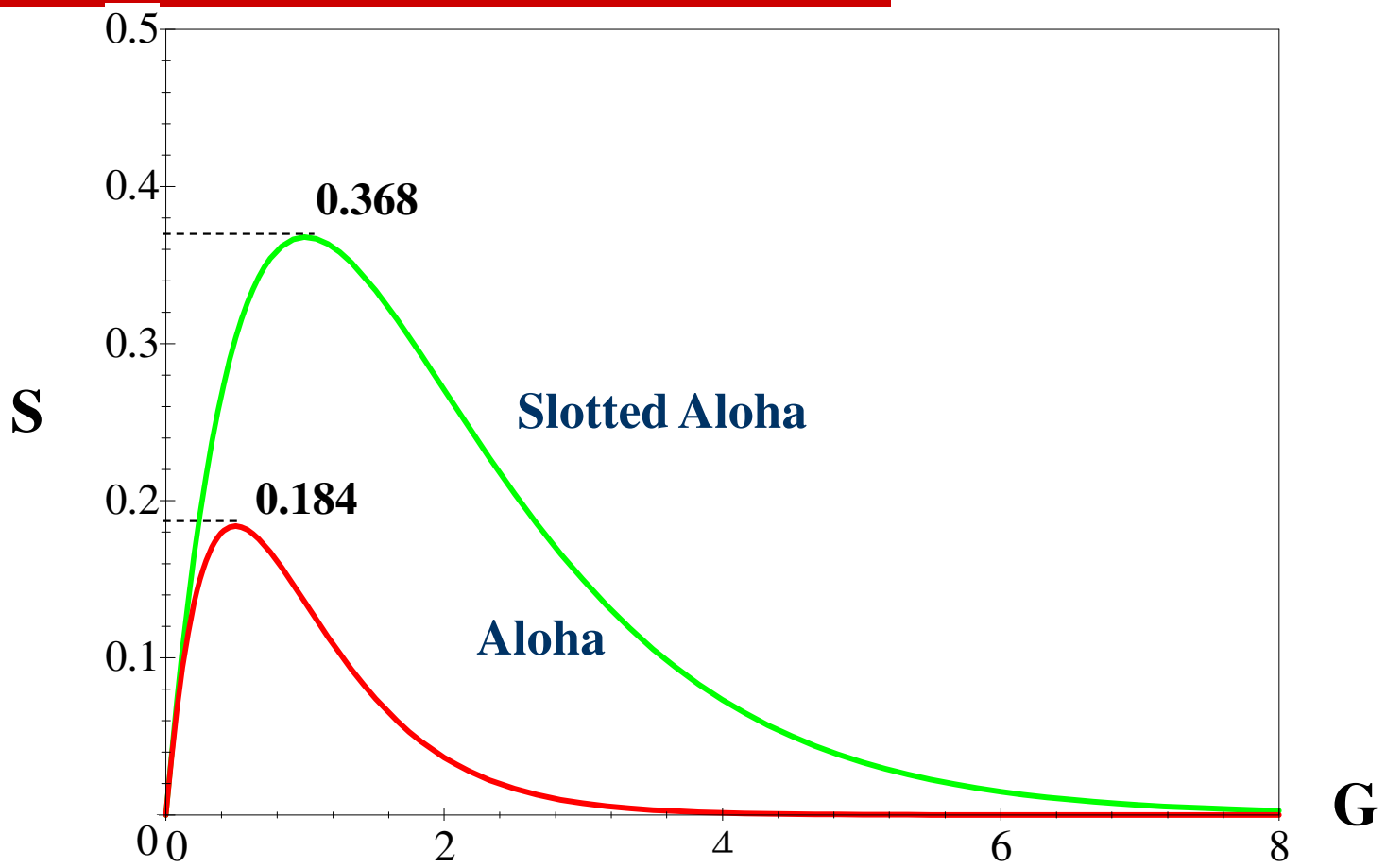
- time divided into discrete intervals (1 interval = 1 frame)
- the sending station waits until the beginning of the next discrete interval

Throughput for slotted ALOHA



$$S=Ge^{-G}$$

Pure and Slotted ALOHA Throughput



Simple improvement but big impact

Slotted ALOHA Throughput - example

A slotted ALOHA network transmits 200-bit frames on a shared channel of 200 kbps. What is the throughput if the system (all stations together) produces

a. 1000 frames per second b. 500 frames per second

c. 250 frames per second.

Solution

The frame transmission time is 200/200 kbps or 1 ms.

a. If the system creates 1000 frames per second, this is 1 frame per millisecond. The load is 1. In this case $S = G \times e^{-G}$ or $S = 0.368$ (36.8 percent). This means that the throughput is $1000 \times 0.0368 = 368$ frames. Only 386 frames out of 1000 will probably survive.

Slotted ALOHA Throughput - example

b. If the system creates 500 frames per second, this is (1/2) frame per millisecond. The load is (1/2). In this case $S = G \times e^{-G}$ or $S = 0.303$ (30.3 percent). This means that the throughput is $500 \times 0.0303 = 151$. Only 151 frames out of 500 will probably survive.

c. If the system creates 250 frames per second, this is (1/4) frame per millisecond. The load is (1/4). In this case $S = G \times e^{-G}$ or $S = 0.195$ (19.5 percent). This means that the throughput is $250 \times 0.195 = 49$. Only 49 frames out of 250 will probably survive.

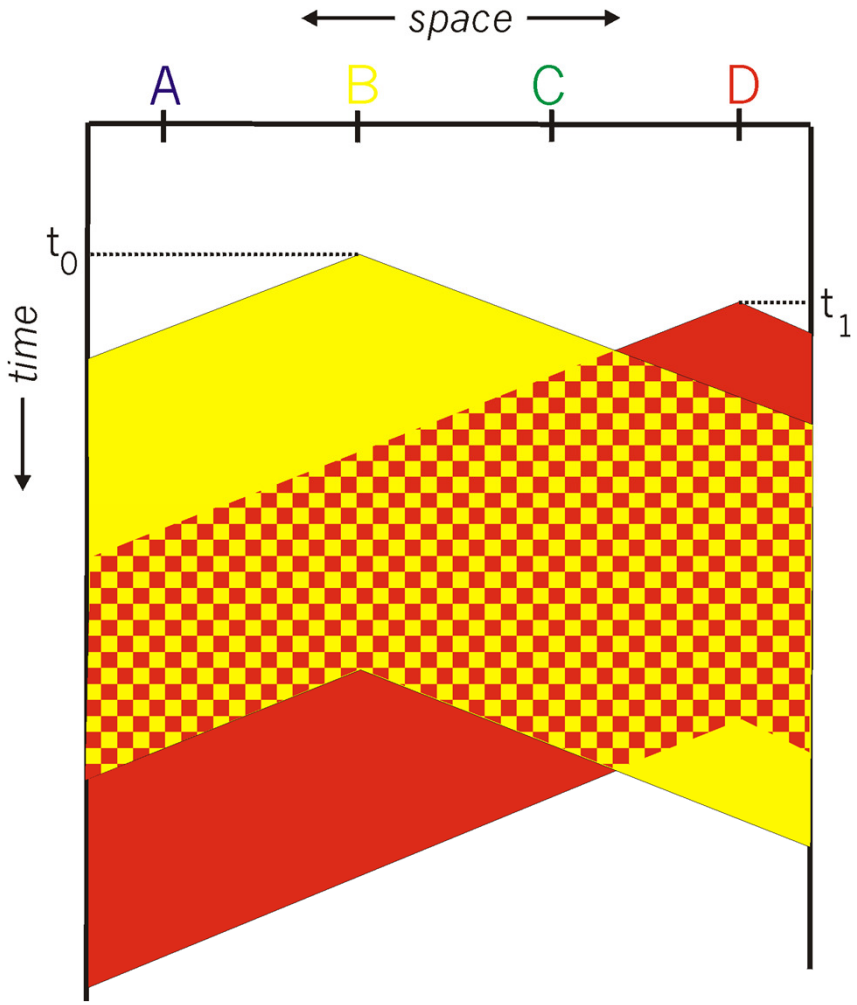
CSMA (Carrier Sense Multiple Access)

- Collisions hurt the efficiency of ALOHA protocol
  - At best, channel is useful 37% of the time
- CSMA gives improved throughput compared to Aloha protocols.
- CSMA: **listen before transmit**
  - If channel sensed idle: transmit entire frame
  - If channel sensed busy, defer transmission
- Human analogy: don't interrupt others!

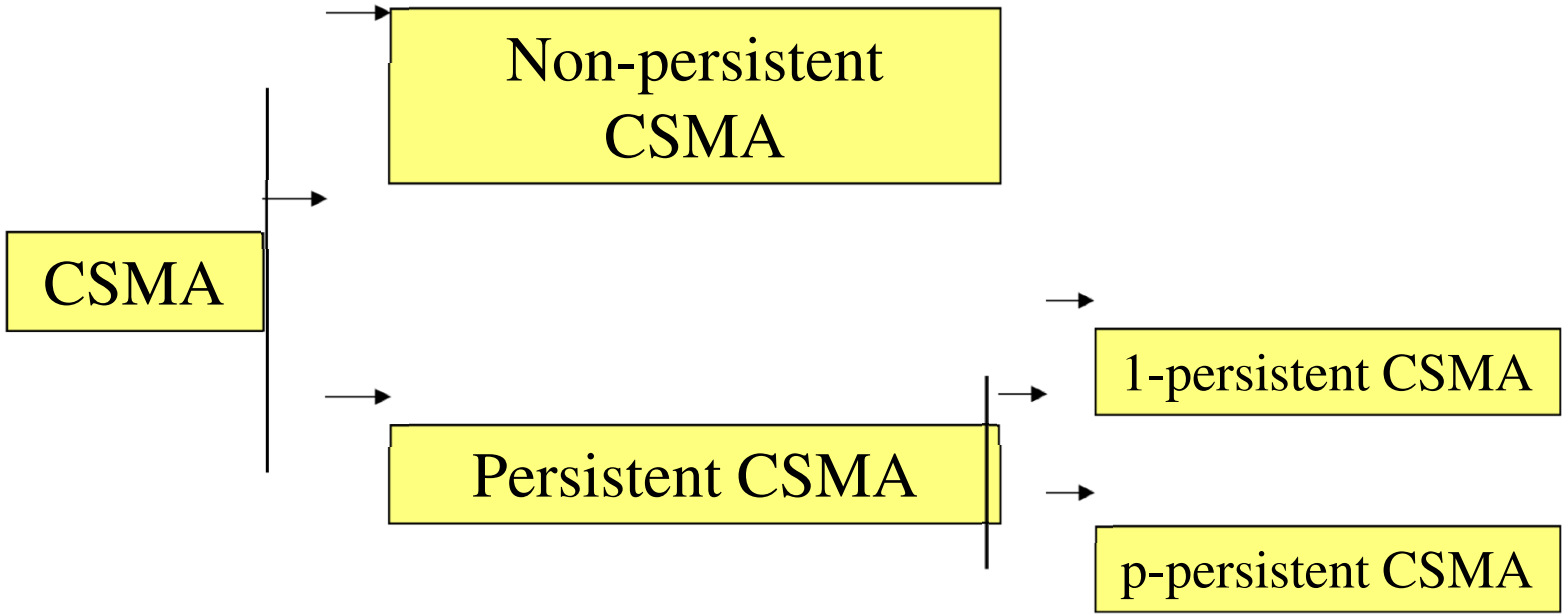
CSMA Collisions

Collisions *can* still occur:
propagation delay means two nodes may not hear each other's transmission

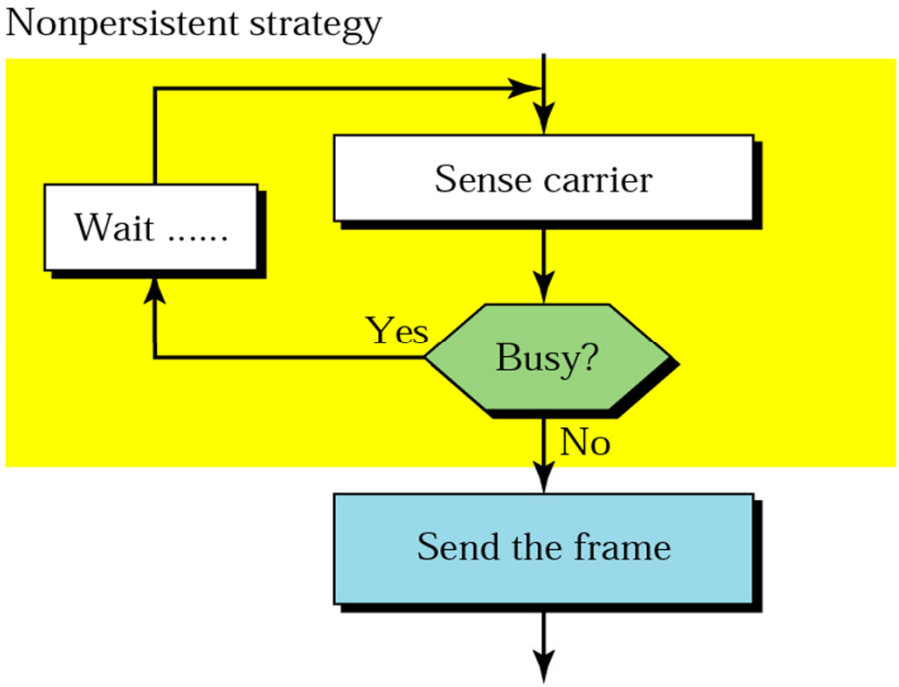
Collision:
entire packet transmission time wasted

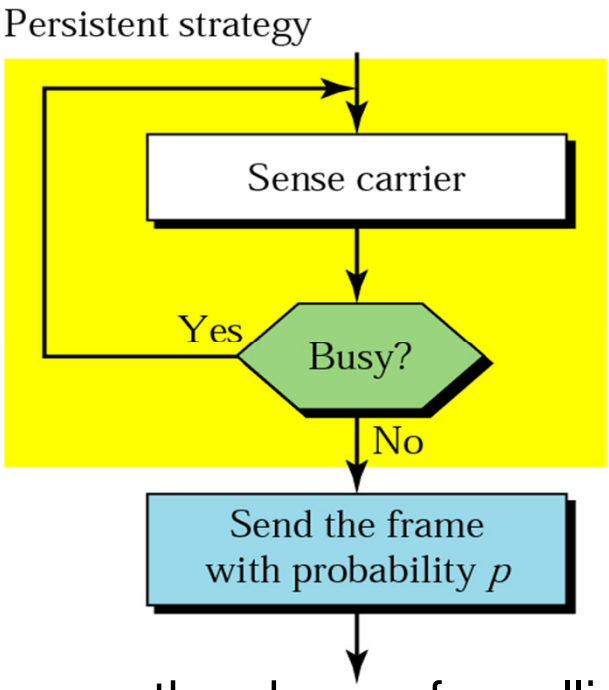


Kinds of CSMA



Nonpersistent vs. persistent





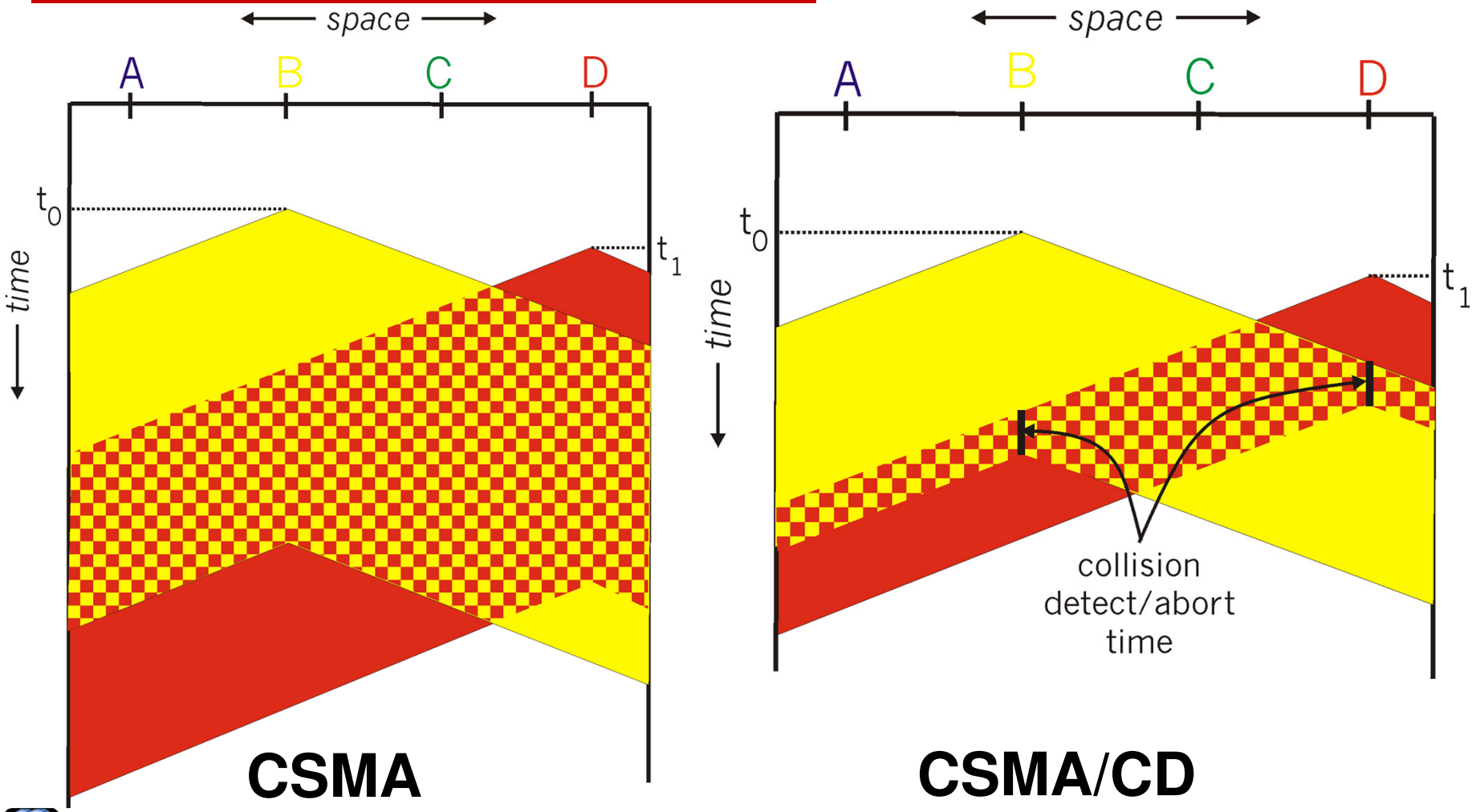
- reduces chance of collisions
- reduces the efficiency

- increases the chance for collisions
  - 1-persistant
- p-persistent
  - Decrease the chance for collisions
  - Improves efficiency

CSMA/CD (Collision Detection)

- CSMA/CD: carrier sensing, deferral as in CSMA
  - Collisions detected within short time
  - Colliding transmissions aborted, reducing wastage
- Collision detection
  - Easy in wired LANs: measure signal strengths, compare transmitted, received signals
  - Difficult in wireless LANs: receiver shut off while transmitting
- Human analogy: the polite conversationalist

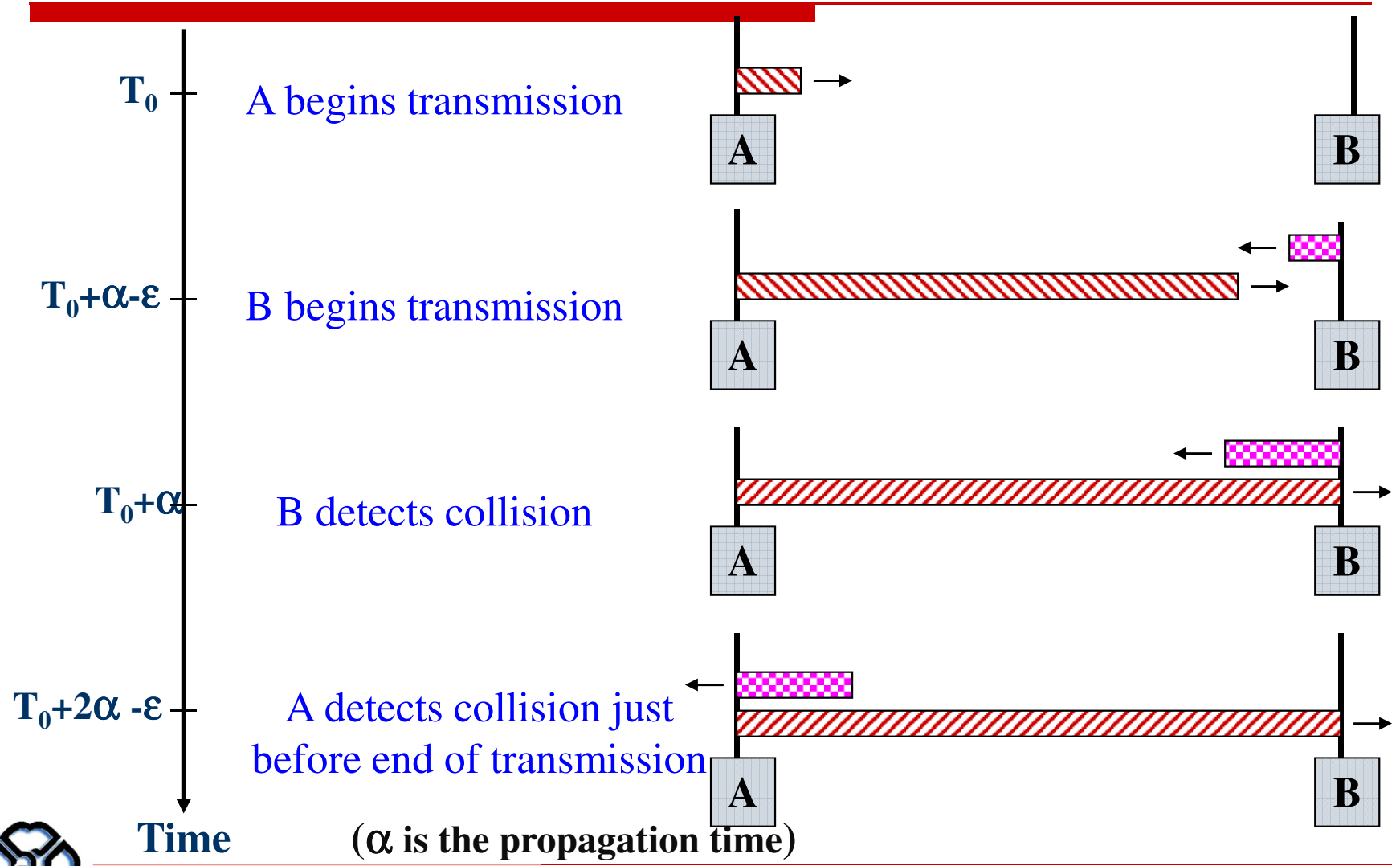
CSMA/CD Collision Detection



Minimum Packet Size

- Why put a minimum packet size?
- Give a host enough time to detect collisions
- In Ethernet, minimum packet size = 64 bytes (two 6-byte addresses, 2-byte type, 4-byte CRC, and 46 bytes of data)
- If host has less than 46 bytes to send, the adaptor pads (adds) bytes to make it 46 bytes
- What is the relationship between minimum packet size and the length of the LAN?

CSMA/CD- Collision detection interval



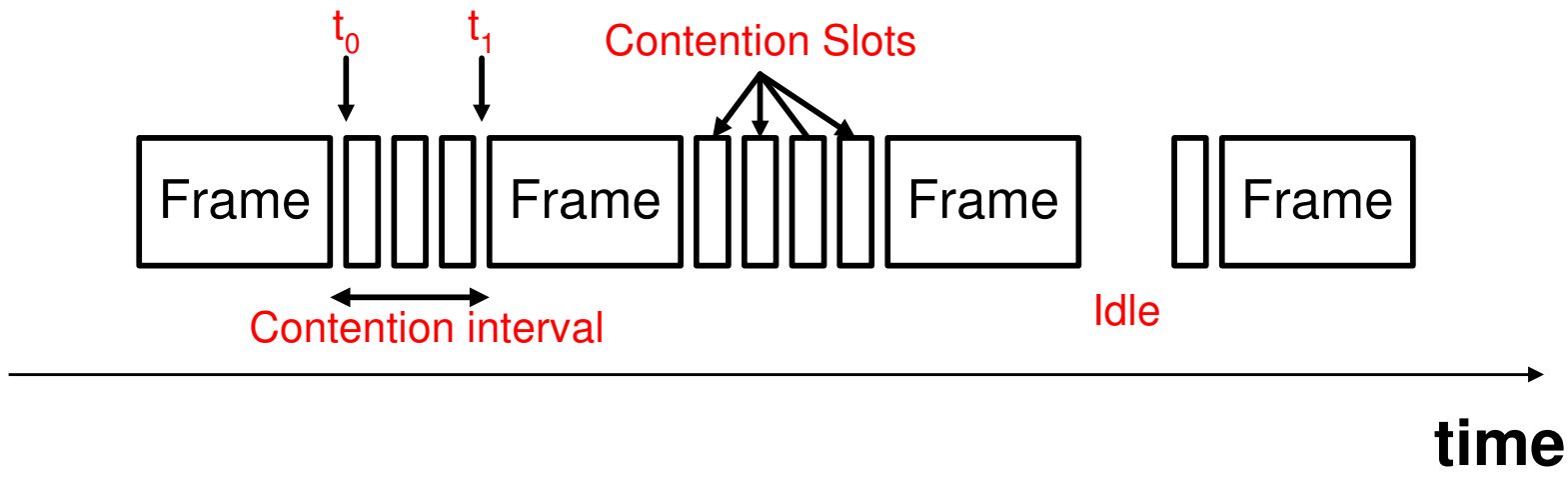
Collision detection

- How the station detects a collision?
- There are many collision detection methods!
- Most of them are analog processes

Examples:

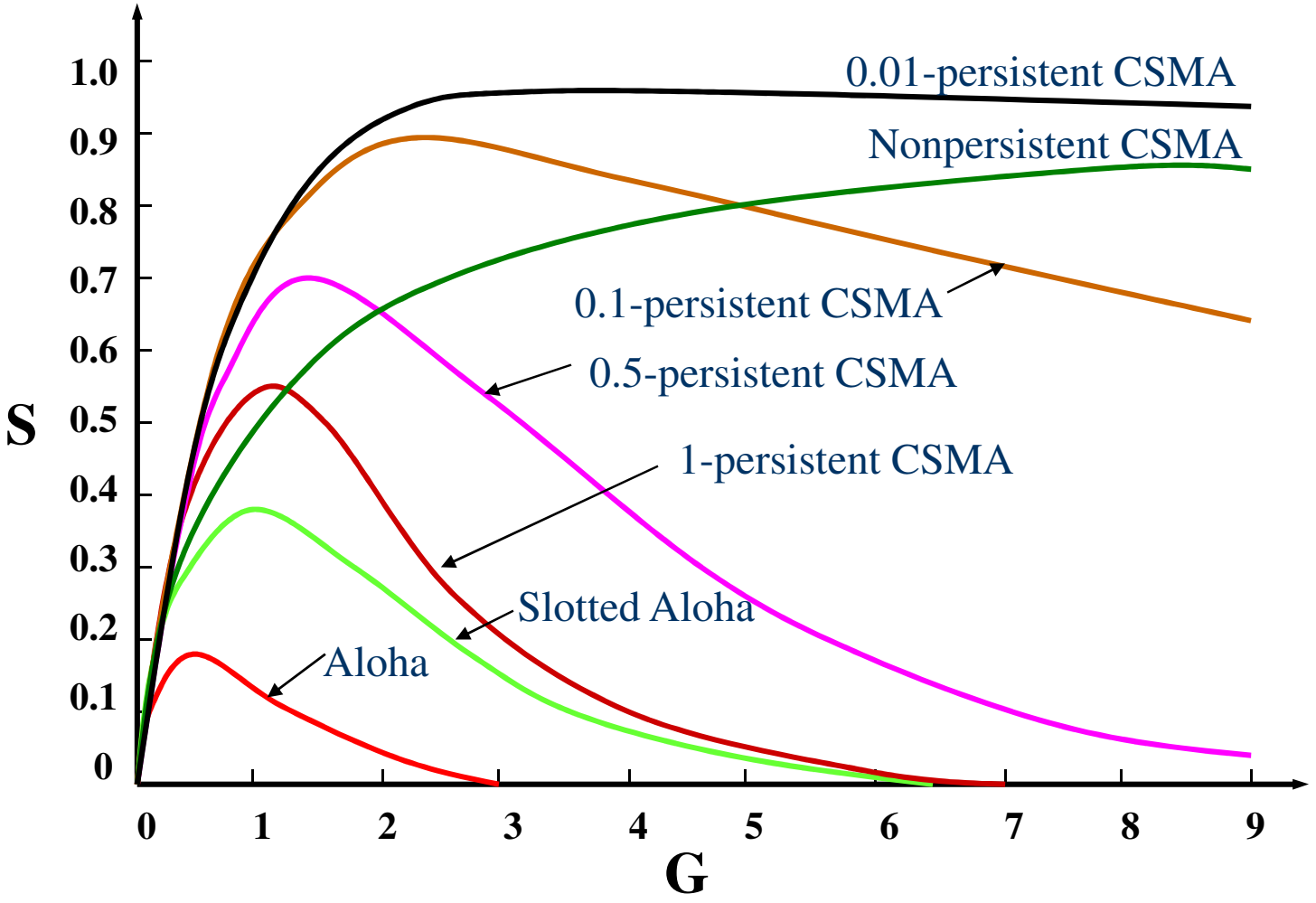
- detecting voltage level on the line
- detecting power level
- detecting simultaneous transmission & reception

CSMA/CD Contention Interval



- Contention slots end in a collision
- Contention interval is a sequence of contention slots
- Length of a slot in contention interval is 512 bit time

Throughput Comparison



Controlled Access Protocols

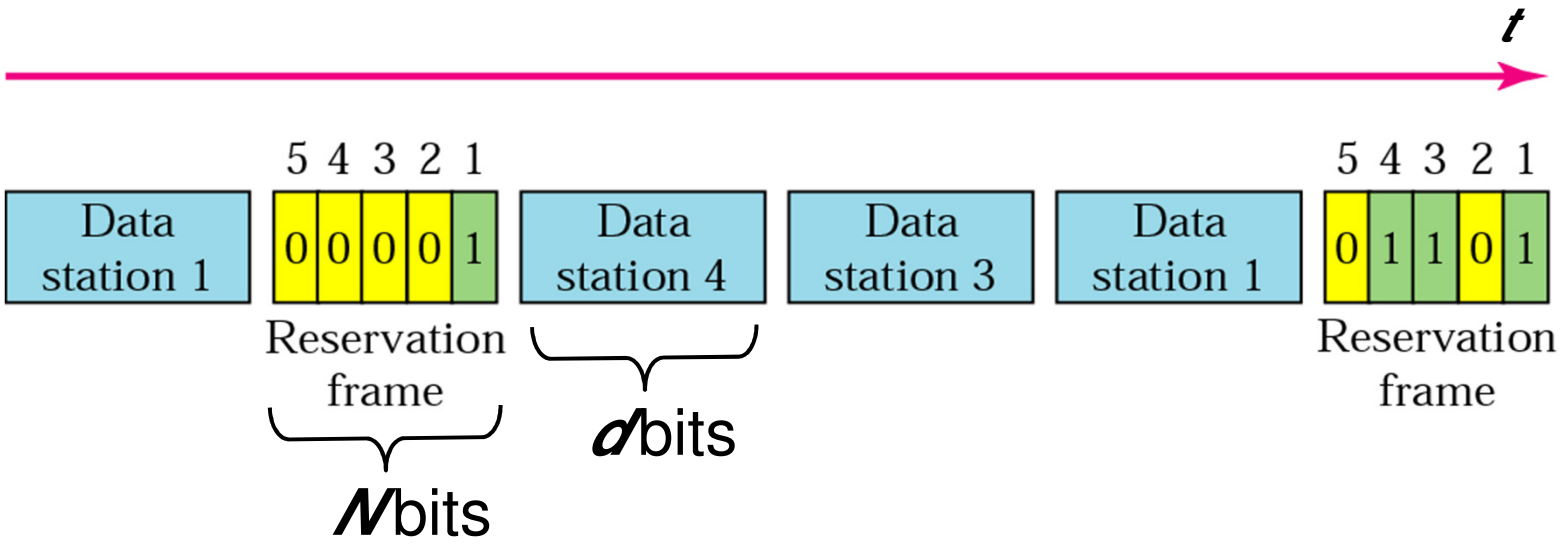
In controlled access, the stations consult one another to find which station has the right to send. A station cannot send unless it has been authorized by other stations.

Topics discussed in this section:

- **Reservation**
- **Polling**
- **Binary Countdown**
- **Token Passing**

Reservation access method

- No collisions
- reservation is made before sending

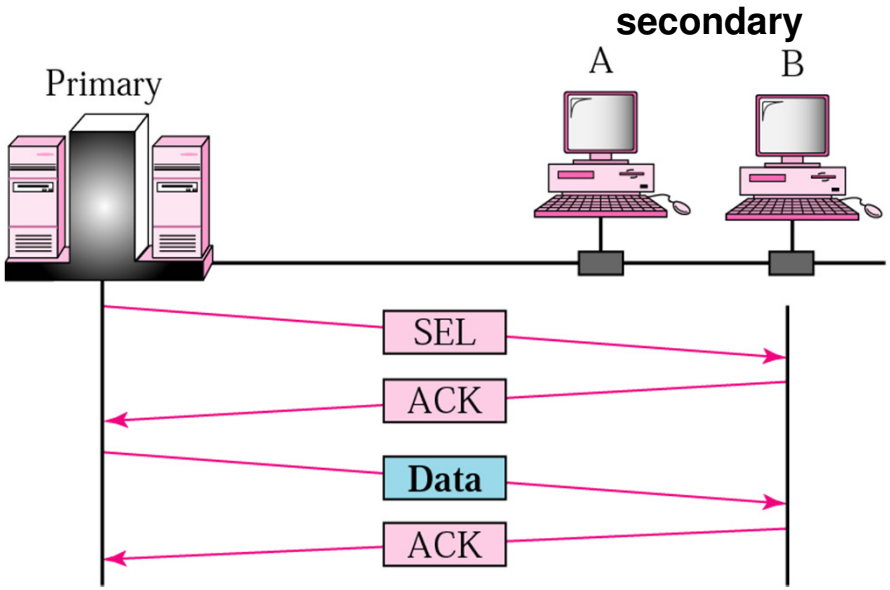


- average waiting time before transmission is N
- low load utilization: d/(d+N) – not good if N is large
- high-load utilization d/(d+1)

Polling

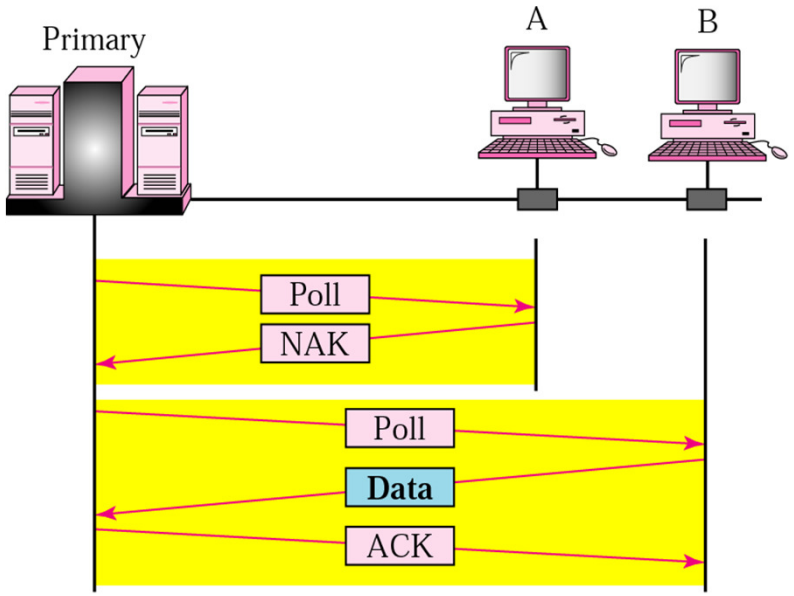
Poll

primary device wants to send data



Select

primary device is ready to receive



- All data exchanges made through the primary device
- primary device controls the channel and is initiator of the session

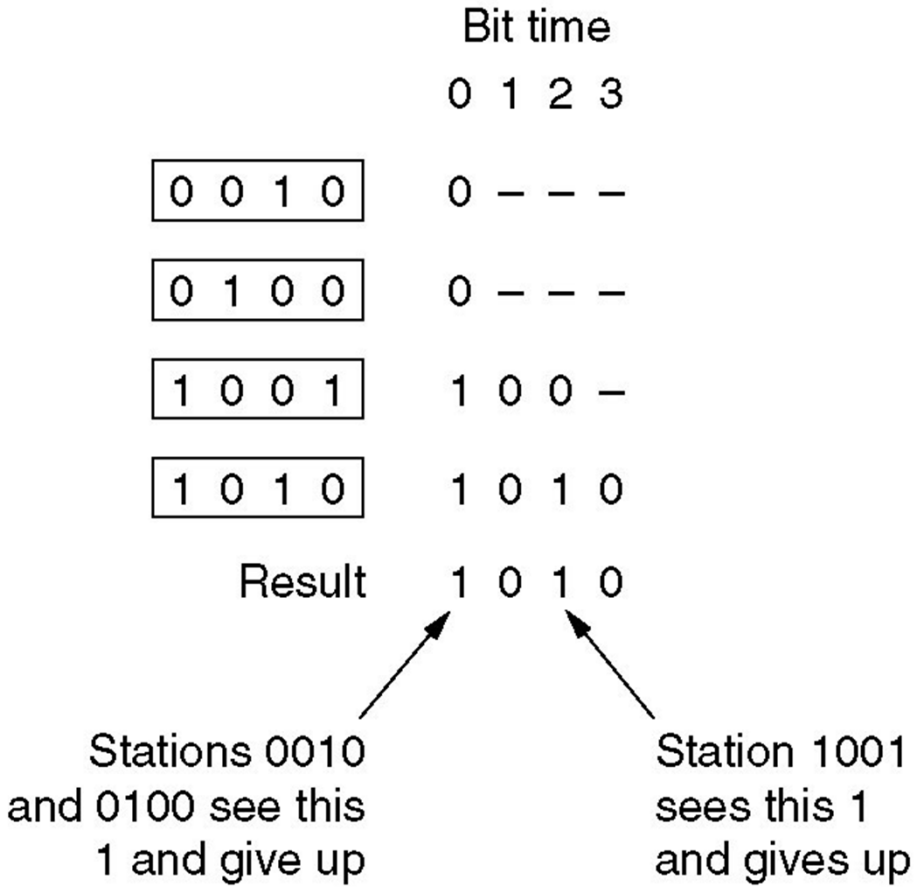
Polling (cnt'd)

- Offers higher efficiency than the random access protocols
- Drawbacks:
  - polling delay
  - node transmits at rate less than *R* bps
  - channel becomes inoperative if master device fails

Remember 4 protocol issues?

- ✓ - if only 1 node is sending than the throughput is *R*
- ✓ - when *M* nodes have data to send than the throughput is *R/M*
- ✓ - decentralized protocol
- ✓ simple & inexpensive to implement

The binary countdown protocol



- A dash indicates silence
- Channel efficiency $d/(d+\log_2 N)$
- If the source address is at the beginning than efficiency is 100 %!
- stations with larger numbers have better chances to access the medium

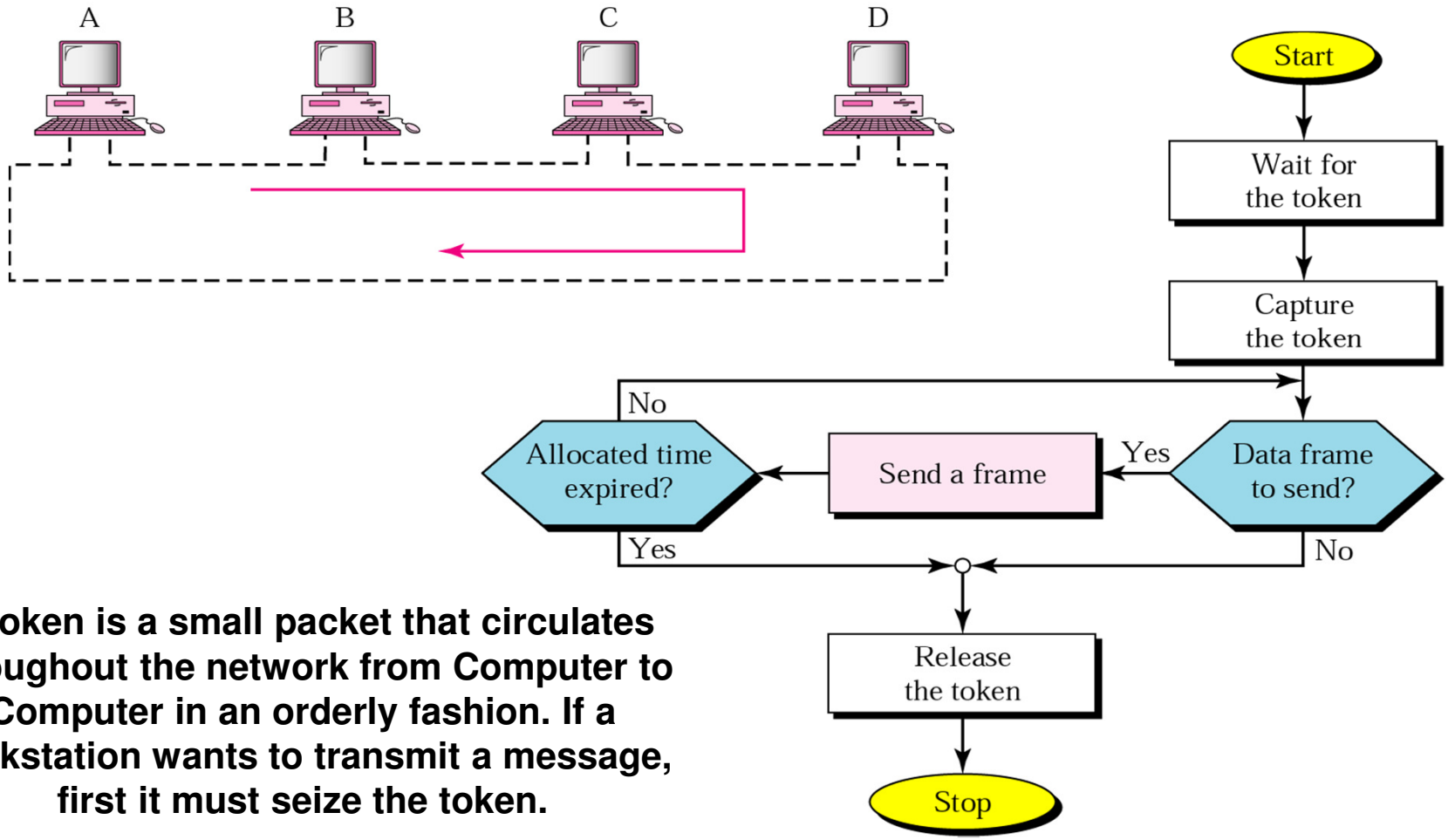
The binary countdown protocol-variation

- Stations D, E, A, F, B, G
  with priorities 6, 5, 4, 3, 2, 1

- If station D has sent a frame than the new order is
  E, A, F, B, G, D
  with priorities 6, 5, 4, 3, 2, 1

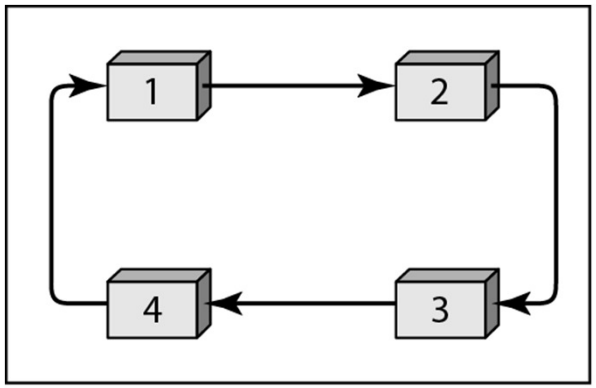
- **Stations get more equal chance to access the medium**

Token passing

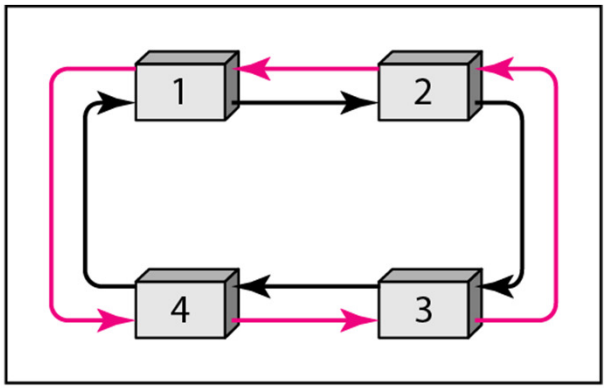


A token is a small packet that circulates throughout the network from Computer to Computer in an orderly fashion. If a workstation wants to transmit a message, first it must seize the token.

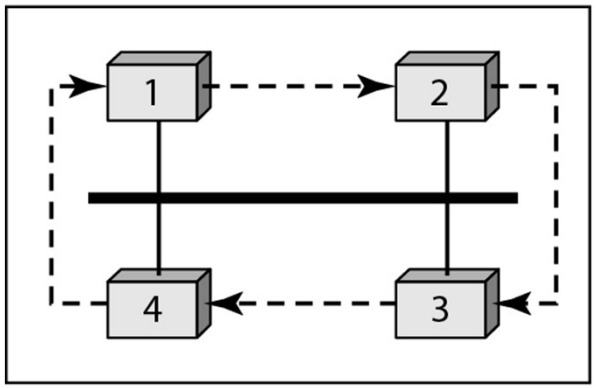
Token passing



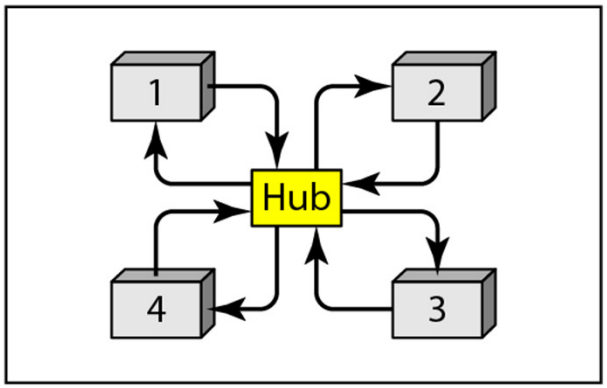
a. Physical ring



b. Dual ring



c. Bus ring



d. Star ring

Logical ring and physical topology in token-passing access method

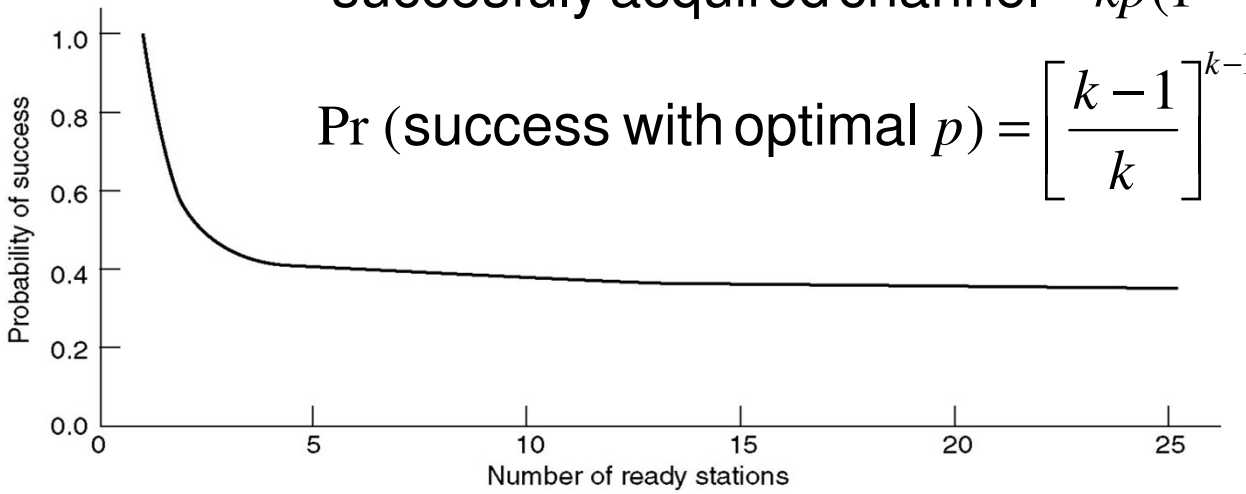
Limited-contention protocols

- performance measures:
  - delay @ low load (ALOHA – CS method)
  - channel efficiency @ high load (collision-free protocols)
- the best is to have a combined performance

decrease the amount of competition

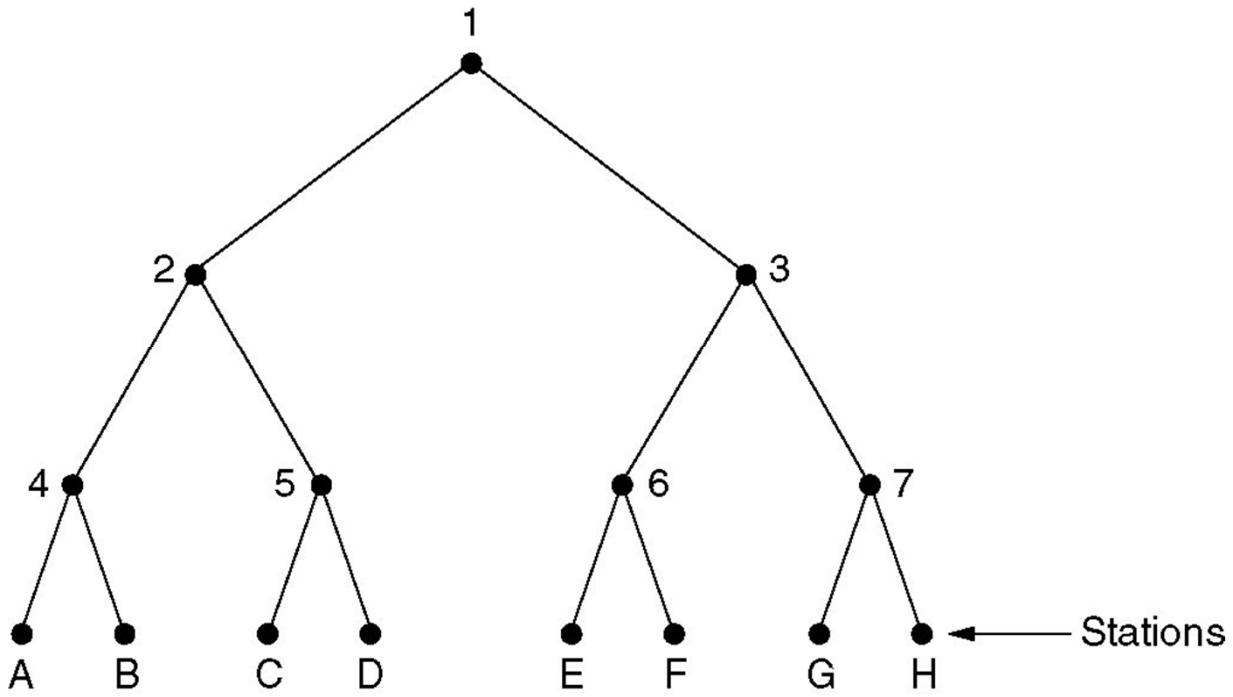
succesfuly acquired channel $kp(1-p)^{k-1}$

$$\Pr(\text{success with optimal } p) = \left[\frac{k-1}{k}\right]^{k-1}$$



Adaptive Tree Walk Protocol

- U.S. Army test for Syphilis
  - Test group, if negative all ok
  - If positive, then split in two and re-test

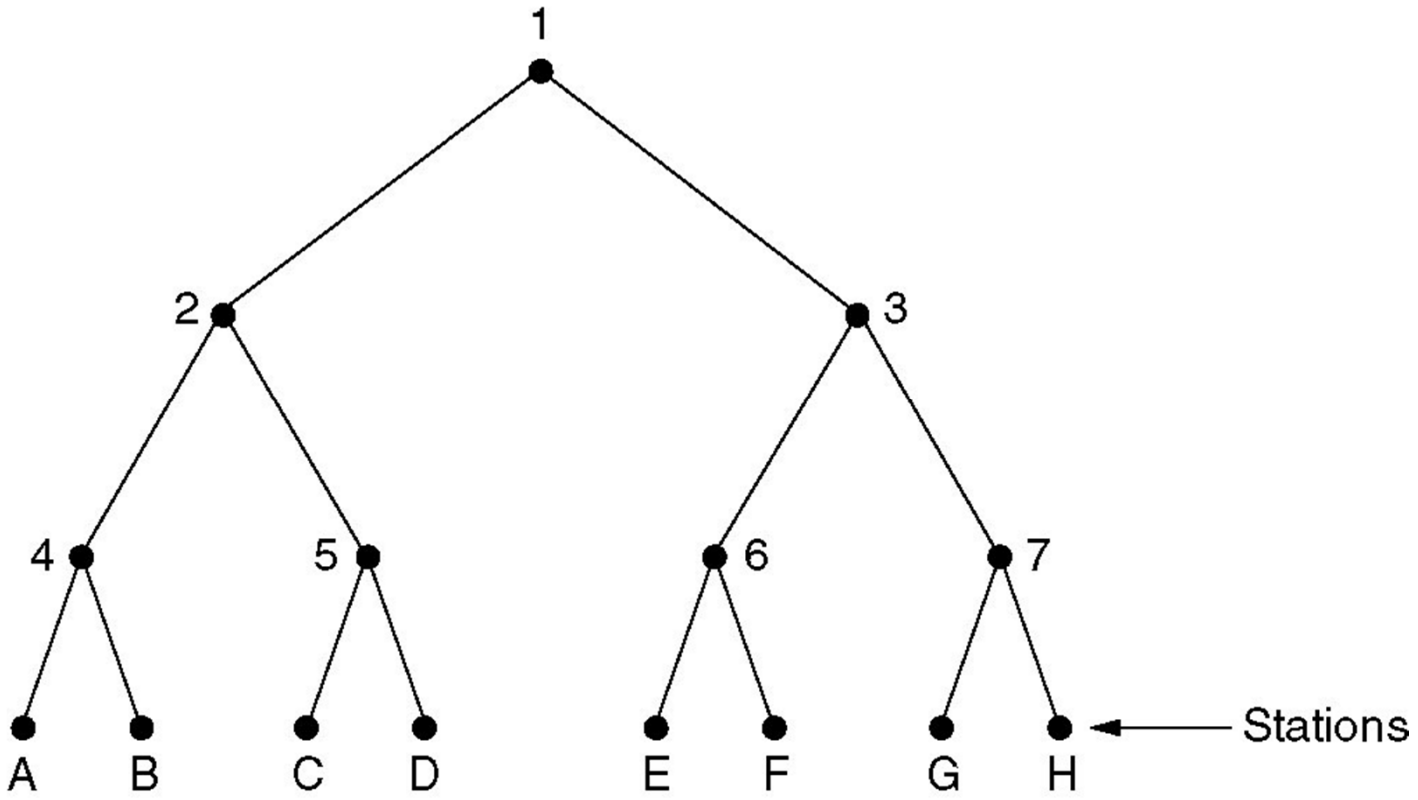


Adaptive Tree Walk Protocol

- Where to begin searching (entire army?)
  - if heavily loaded, not at the top since there will always be a collision
- Number levels 0, 1, 2 …
- At level i, $1/2^i$ stations below it
  - ex: level 0, all stations below it, 1 has 1/2 below…
- If q stations want to transmit, then $q/2^i$ below
- Want number below to be 1 (no collisions)
  - $q/2^i = 1$, $i = \log_2 q$

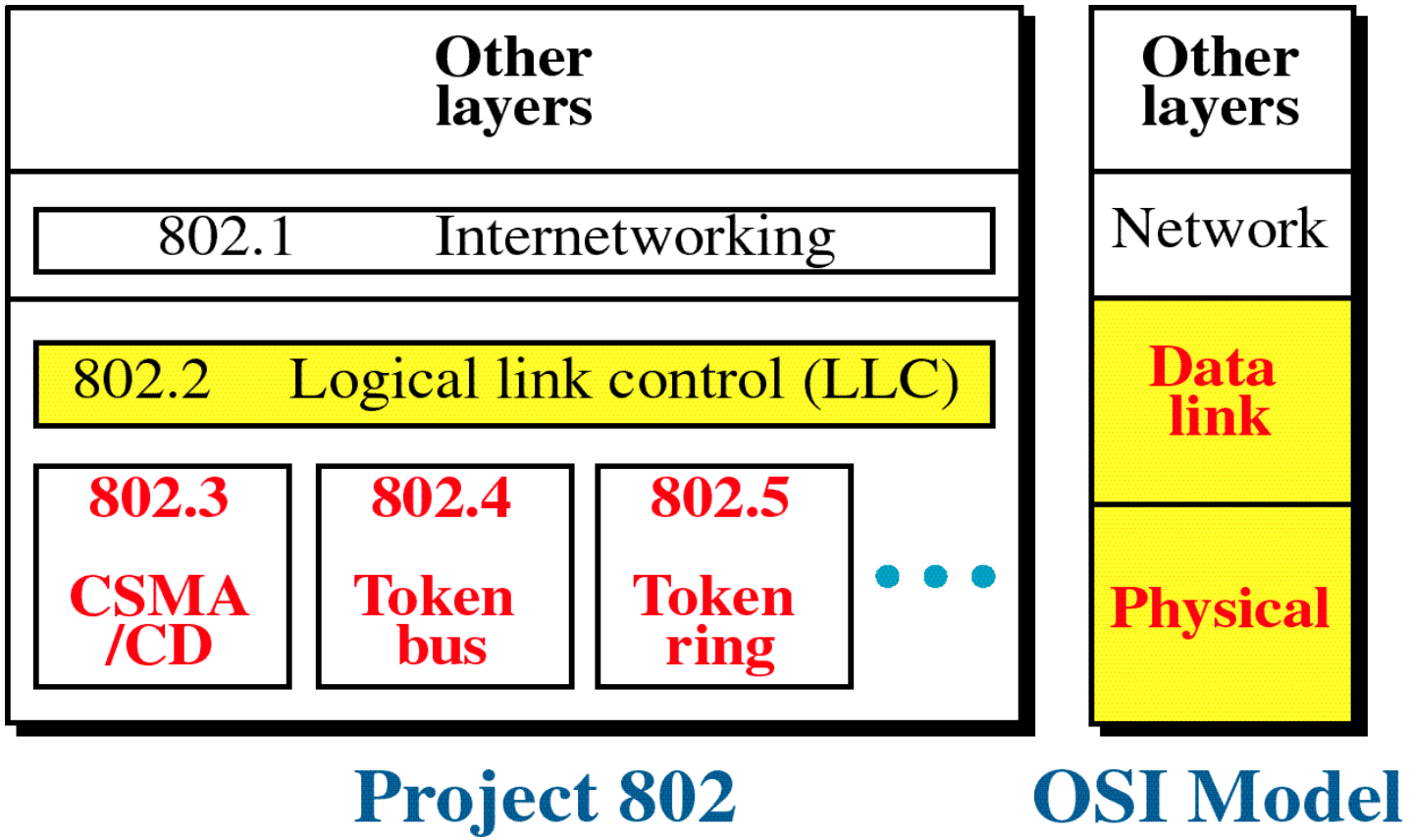
ATWP- Improvement

If collision at 1, 2 idle, do we need to search 3?



IEEE Standards for LANs

IEEE 802 Project for DL and Phy. Layers



IEEE 802 standards

802	Overview and Architecture
802.1	Network Management
802.2	Logical Link Control (LLC)
802.3	CSMA/CD - Ethernet
1802.3	Conformance Test Methodology for IEEE 802.3
802.4	Token Passing Bus
802.5	Token Ring
802.6	Metropolitan Area Network (MAN) : DQDB

802.7	Broadband LAN
802.8	Fiber Optic
802.9	Isochonous LAN
802.10	Integrated Service Security
802.11	Wireless LAN
802.12	Demand Priority
802.15	Wireless PAN
802.16	Broadband Wireless Access (Wireless MAN)
802.17	Resilient Packet Ring
802.18	Radio Regulatory

IEEE 802 Standards

(Ethernet: 802.3)

Ethernet (IEEE 802.3)

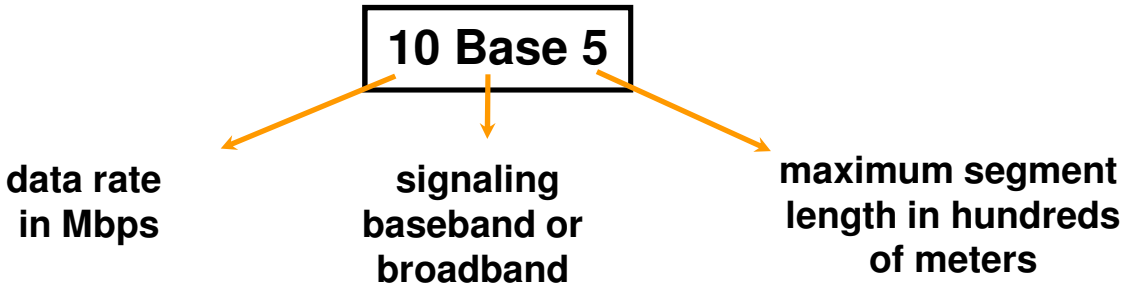
- The Ethernet is **the most successful** local area networking technology.
- Ethernet provides Unreliable Connectionless service
- 1973- Developed at Xerox Park by **Robert Metcalfe** and David Boggs, it is a general form of the **Carrier Sense Multiple Access with Collision Detection (CSMA/CD)** technology.

Ethernet (IEEE 802.3)

- Digital Equipment Corporation (DEC), Intel and Xerox joined to form the 10 Mbps Ethernet standard in 1978.
- This standard formed the basis of the IEEE standard 802.3
- It has recently been extended to include a 100 Mbps version, called **Fast Ethernet** and a 1000 Mbps version called **Gigabit Ethernet**.

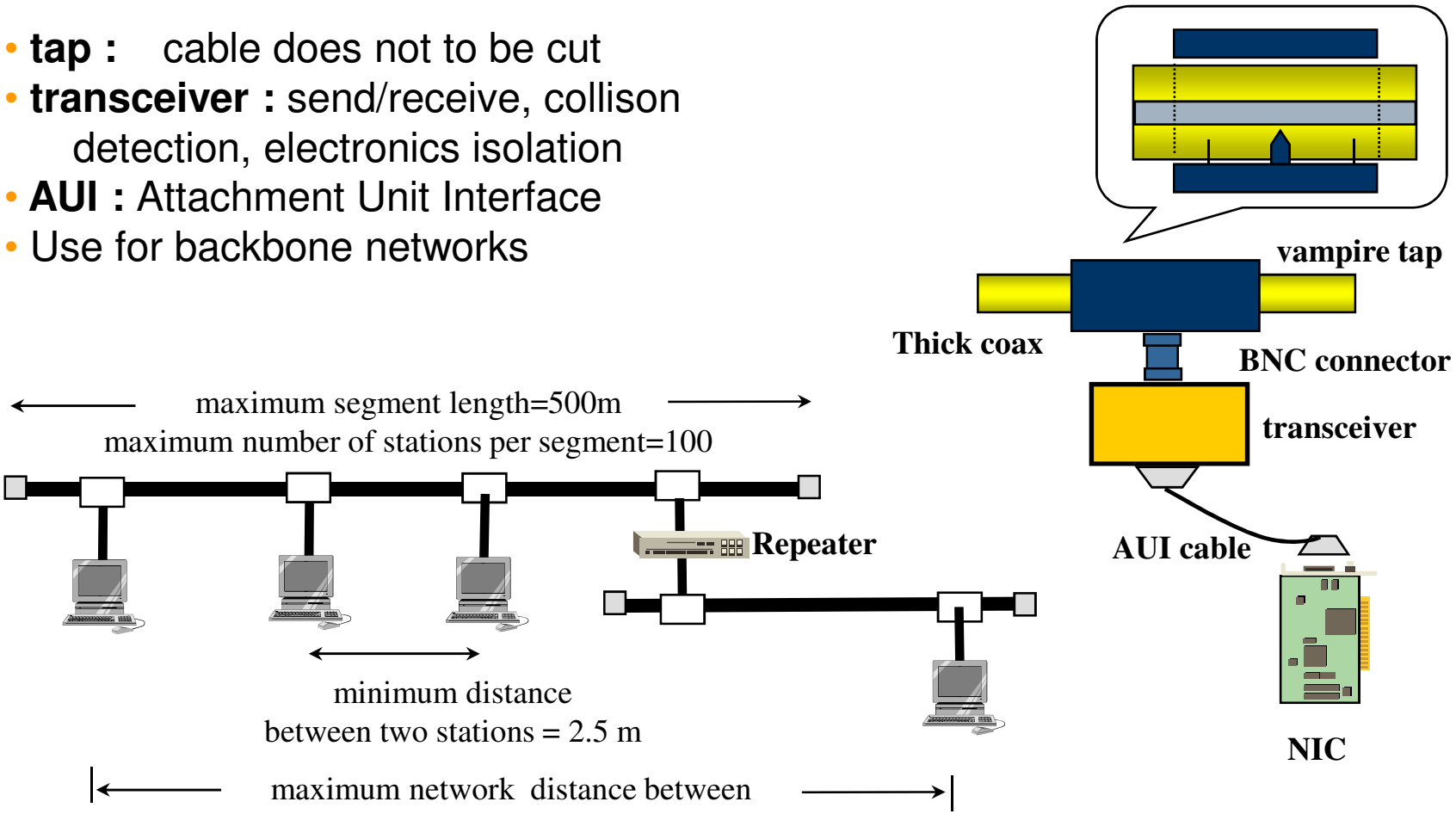
IEEE 802.3 specification

- **Various standard defined for IEEE802.3**
  - 10Base5 -- thick coaxial (BUS topology)
  - 10Base2 -- thin coaxial (BUS topology)
  - 10BaseT -- twisted pair (Star topology)
  - 10BaseF -- fiber optics (Star topology)
- **Fast Ethernet**
  - 100BaseTX, 100BaseT4, 100BaseF and 100 VG-AnyLAN
- **Gigabit Ethernet**
  - 1000BaseX, 1000BaseTX, 1000BaseSX, 1000BaseLX



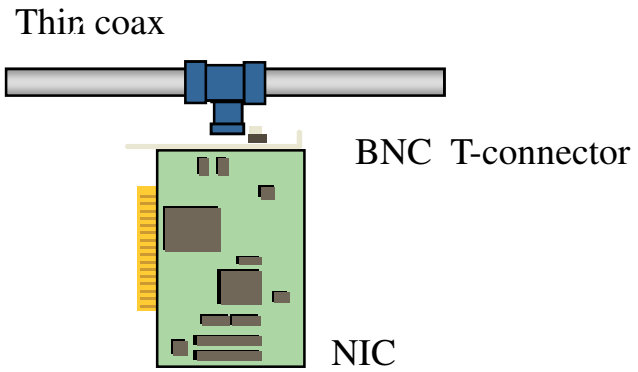
10Base5

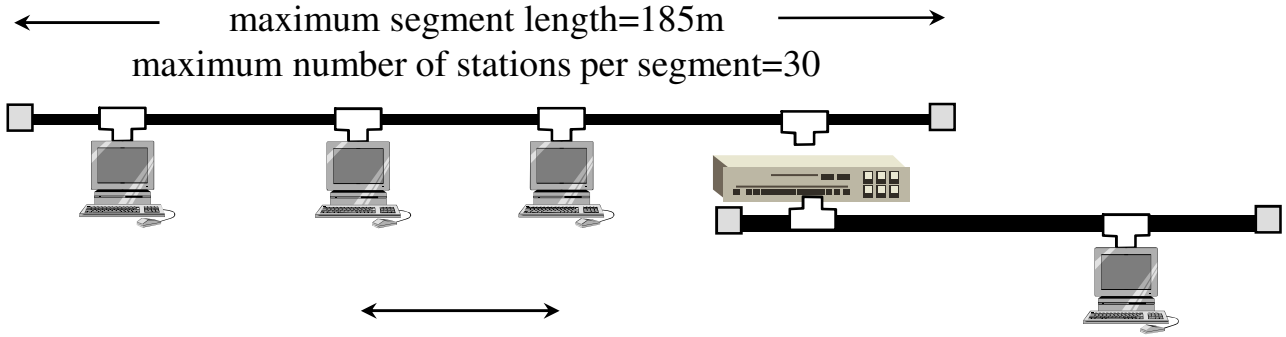
- **tap :** cable does not to be cut
- **transceiver :** send/receive, collison detection, electronics isolation
- **AUI :** Attachment Unit Interface
- Use for backbone networks



10Base2

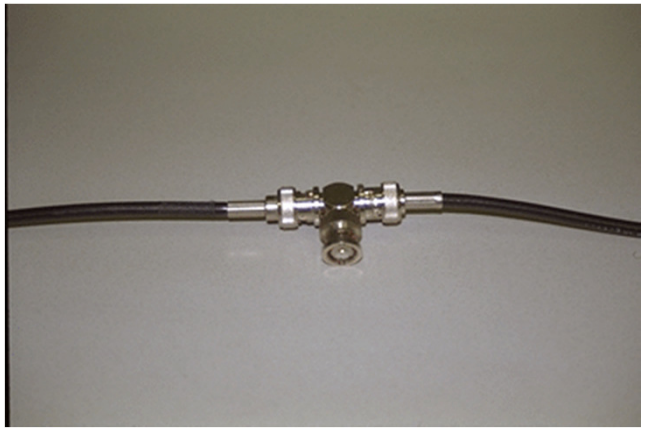
- **BNC connector**
- **No drop cable**
- **use for office LAN**

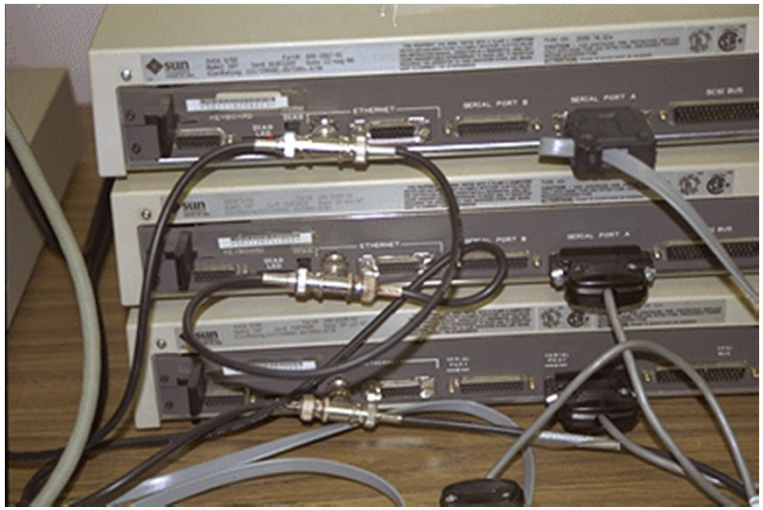




10Base2

- **Uses thin coax that is cheaper and easier to install than thick Ethernet coax**
- **Transceiver electronics built into NIC; NIC connects directly to network medium**

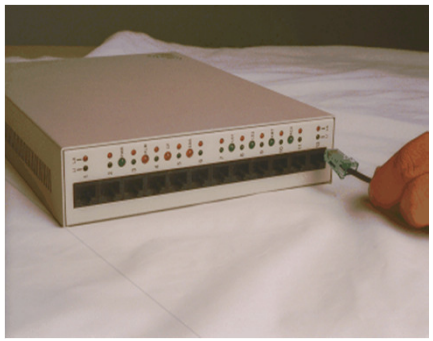


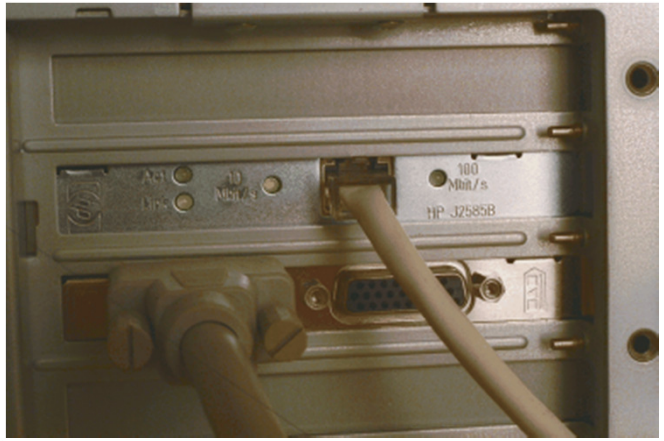


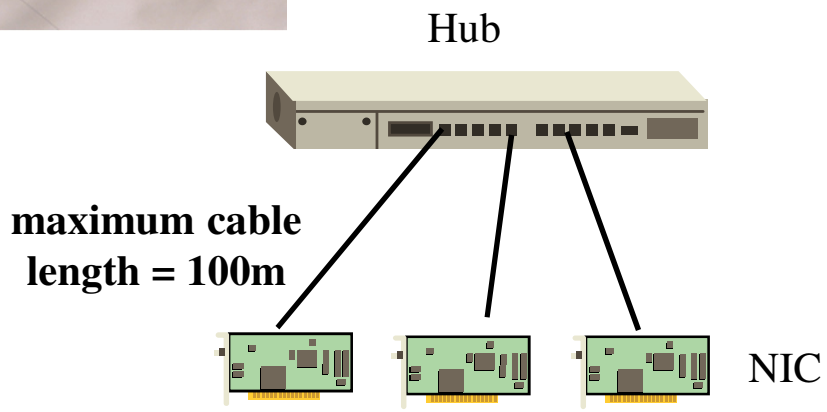
- Useful when many computers are located close to each other
- May be unreliable - any disconnection disrupts entire net

10BaseT

- Replaces AUI cable with twisted pair cable
- Replaces thick coax with hub
- Use for office LAN

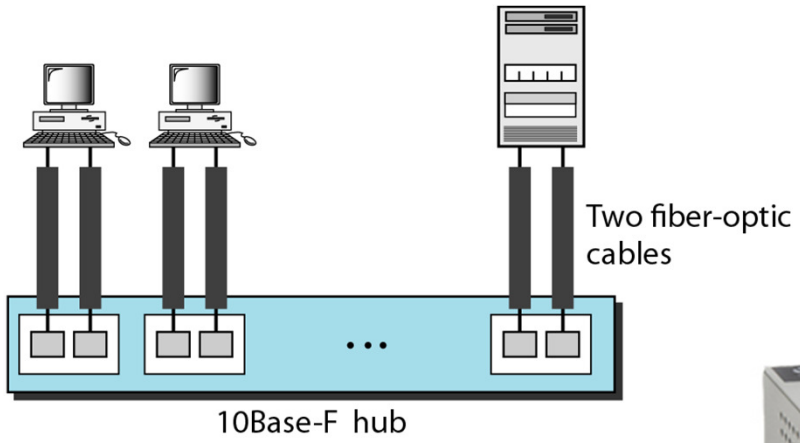






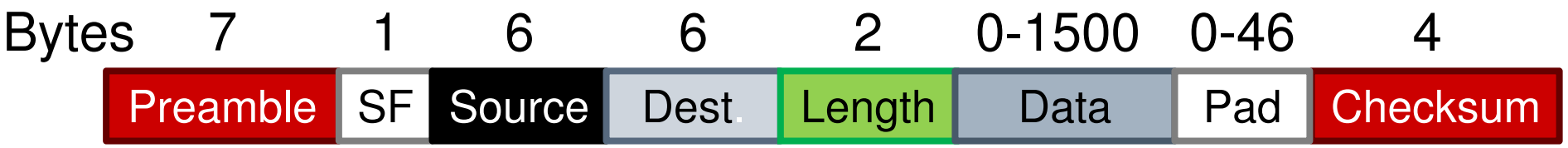
10BaseF

10BaseF specification enable long distance connections with the use of optical fiber.



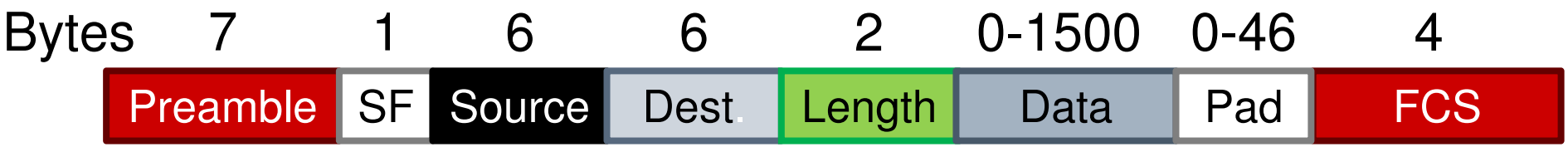
Fiber port

Ethernet Frame Format



- **Preamble:** 7 bytes of 10101010. (used for synchronization)
- **Start Frame (SF):** 10101011
- **Source and destination:** MAC addresses
  - E.g. 00:45:A5:F3:25:0C
  - Broadcast: FF:FF:FF:FF:FF:FF

Ethernet Frame Format



- **Length:** defines the length of the Data field.
- **Minimum packet length of 64 bytes (to detect collision)**
- **PAD**: Frame must be at least 64 bytes long, so if the data is shorter than 46 bytes, the pad field must compensate
- **FCS (Frame Check Sequence):** for error detection
  - Checked at receiver. If error is detected, the frame is simply dropped

Ethernet Uses CSMA/CD

- **Carrier sense: wait for link to be idle**
  - Channel idle: start transmitting
  - Channel busy: wait until idle
- **Collision detection: listen while transmitting**
  - No collision: transmission is complete
  - Collision: abort transmission, and send jam signal
- **Random access: exponential back-off**
  - After collision, wait a random time before trying again

Exponential Backoff Algorithm

Ethernet uses the exponential backoff algorithm to determine when a station can retransmit after a collision

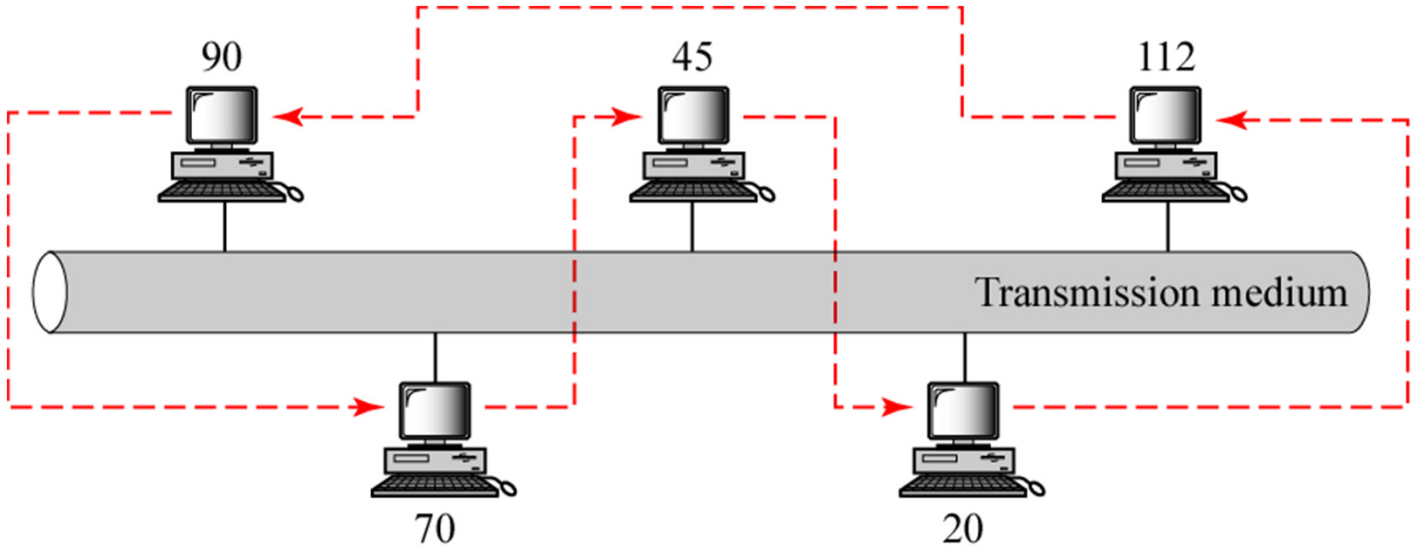
Algorithm:

- Set “slot time” equal to 512bit time
- After first collision wait 0 or 1 slot times
- After i-th collision, wait a random number between 0 and 2^i-1 time slots
- Do not increase random number range, if =10
- Give up after 16 collisions

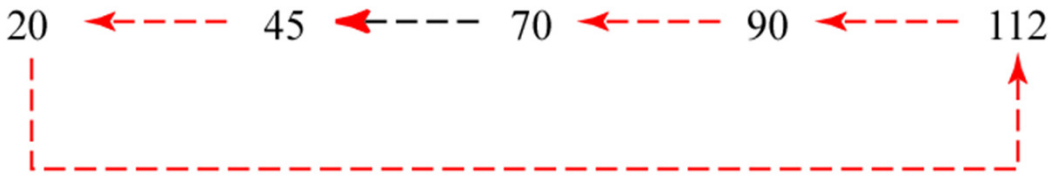
IEEE 802 Standards

(Token Bus: 802.4)

IEEE 802.4: Token Bus



a. Bus and ring

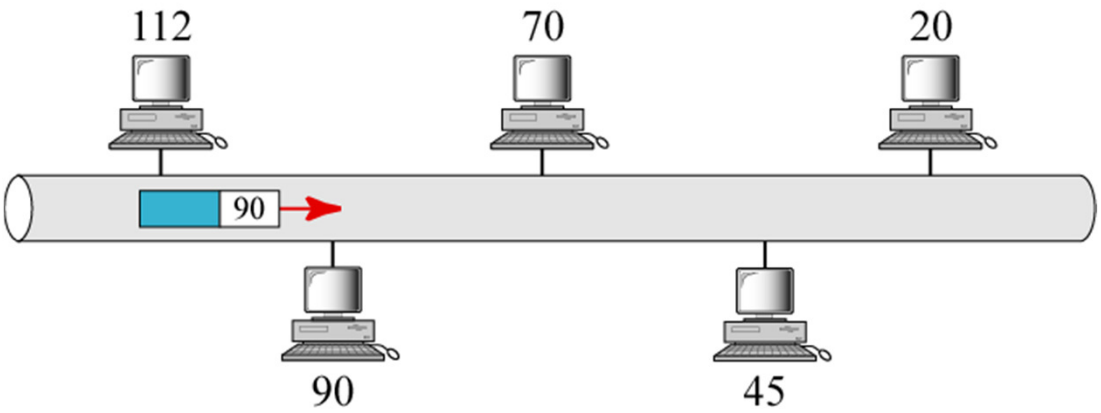


b. Descending ordering

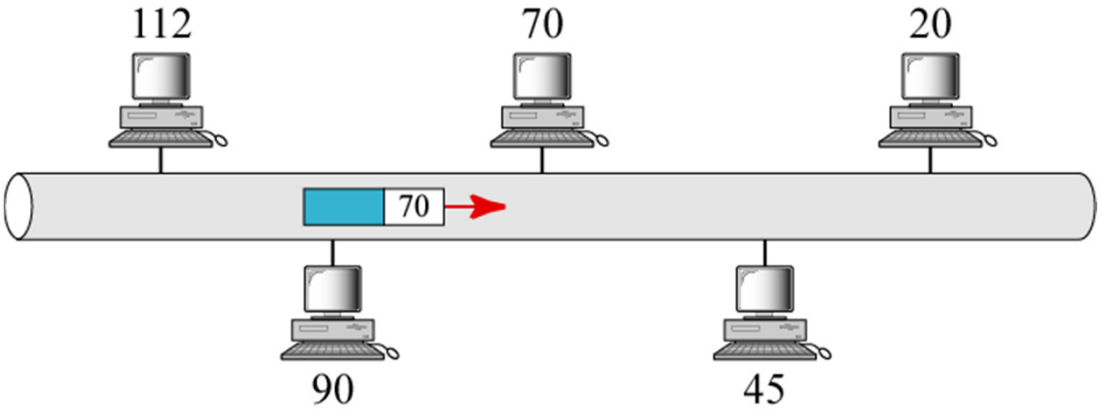
Physical topology:
BUS

Logical topology:
Ring

Token Passing in a Token Bus Network

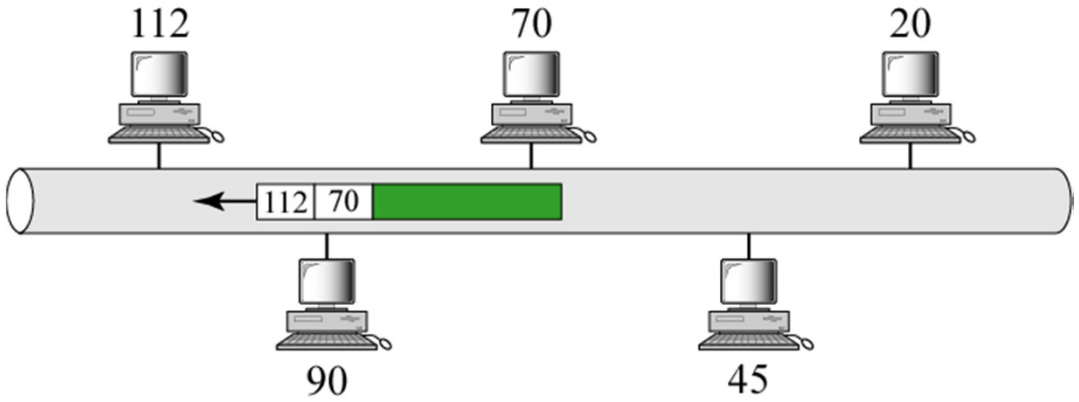


a. Station 112 does not have data; it sends the token to 90

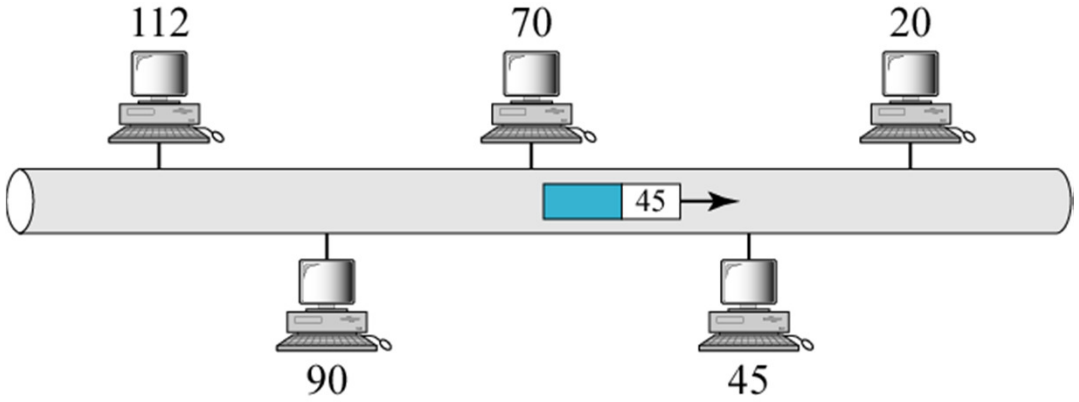


b. Station 90 does not have data; it sends the token to 70

Token Passing in a Token Bus Network

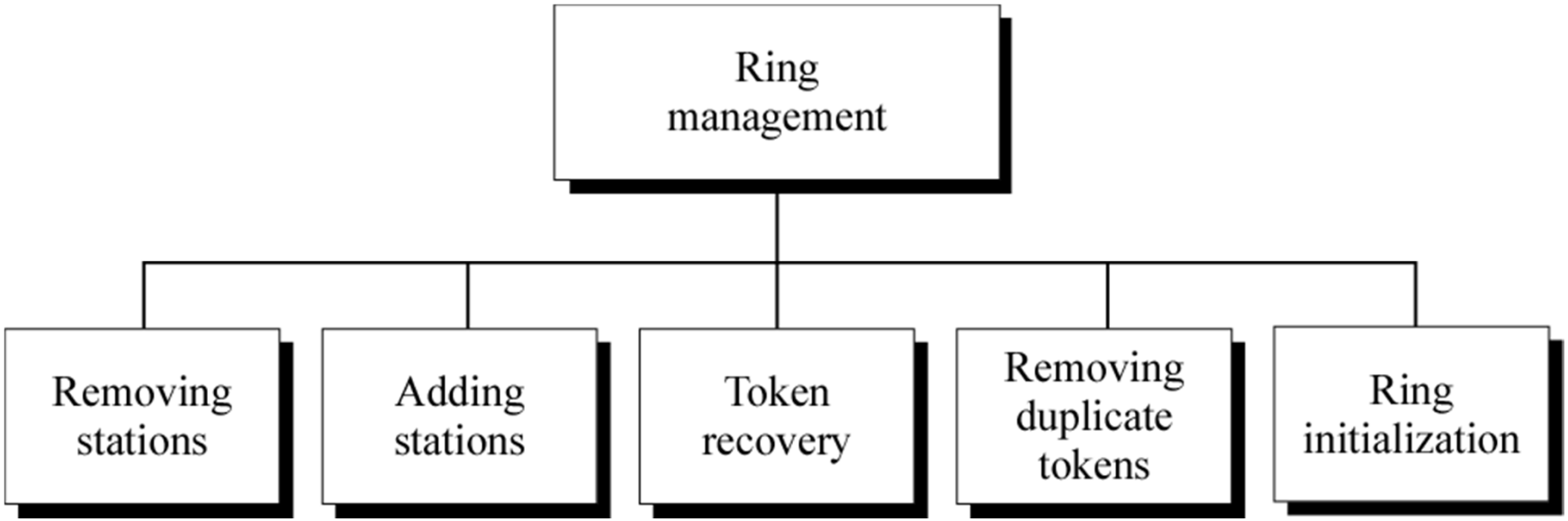


c. Station 70 sends a data frame to station 112



d. Station 70 sends the token to station 45

Ring Management



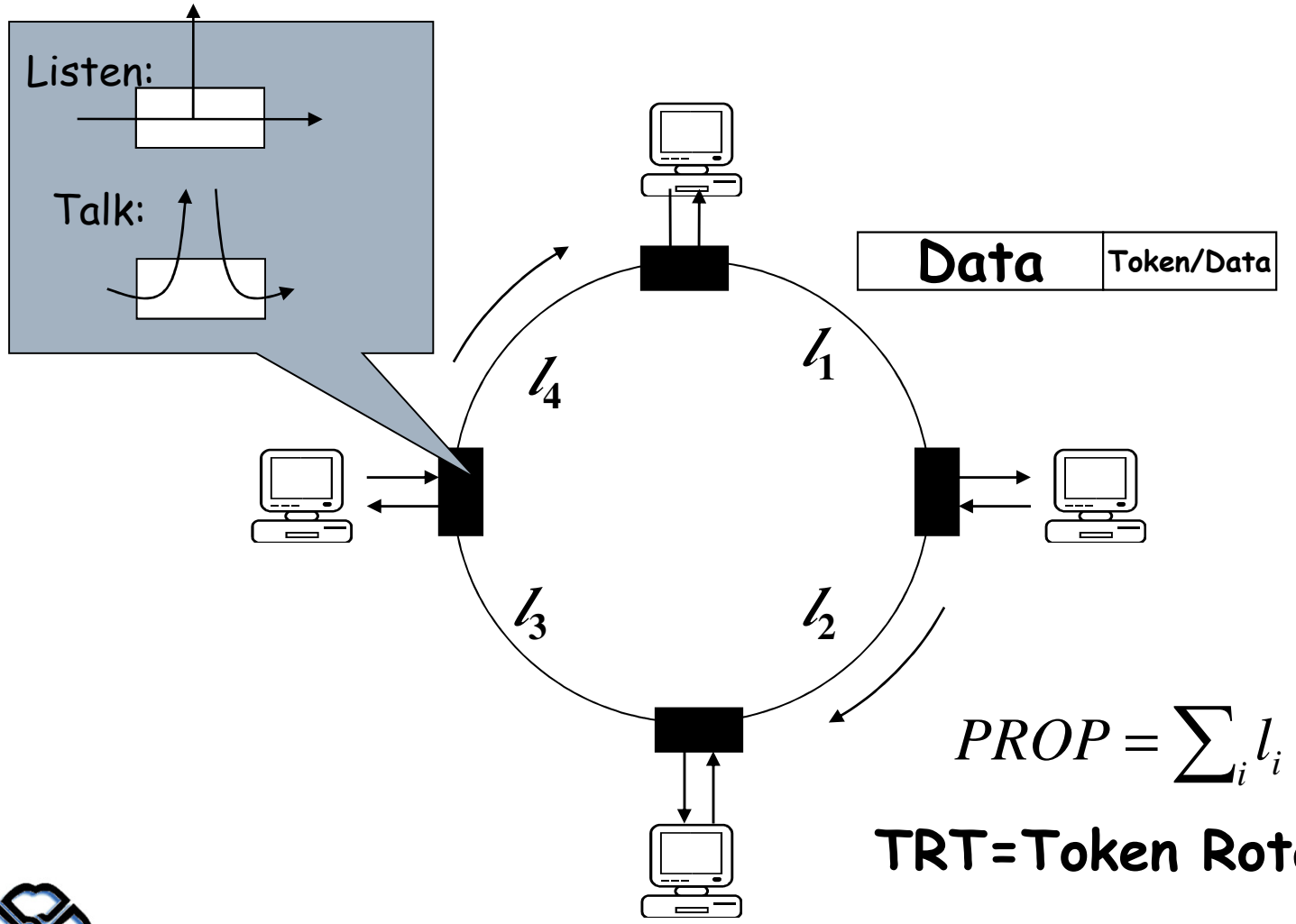
IEEE 802 Standards

(Token Ring: 802.5)

IEEE 802.5: Token Ring

- Proposed in 1969 and initially referred to as a ***Newhall ring.***
- Token ring :: a number of stations connected by transmission links in a ring topology. Information flows ***in one direction along the ring*** from source to destination and back to source.
- Medium access control is provided by a small frame, **the token**, that circulates around the ring when all stations are idle. ***Only the station possessing the token is allowed to transmit at any given time.***

Token Ring IEEE 802.5

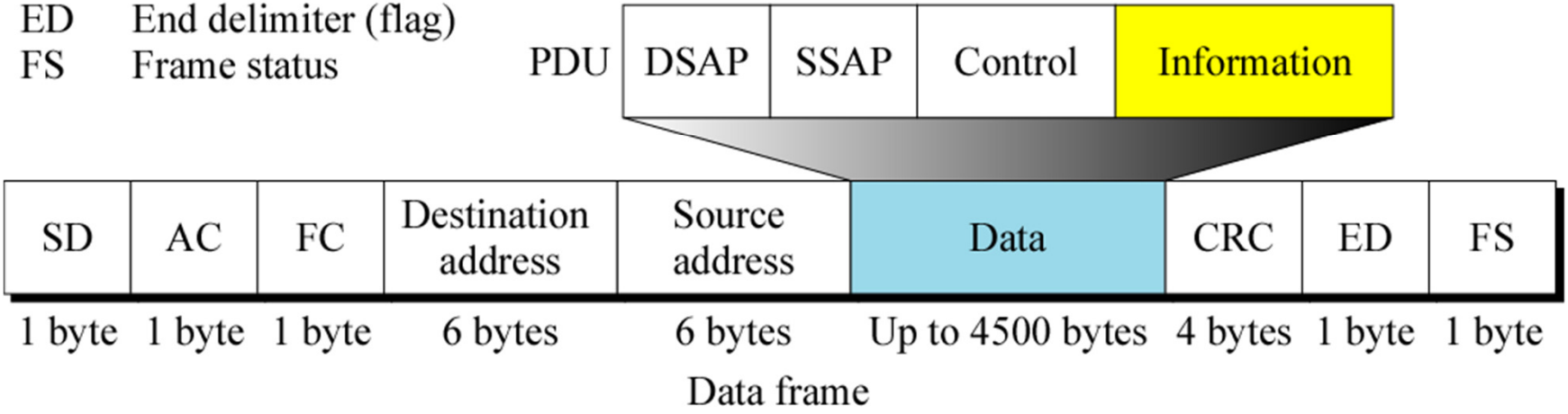


$$PROP = \sum_i l_i / c = TRT_{\min}$$

TRT=Token Rotation Time

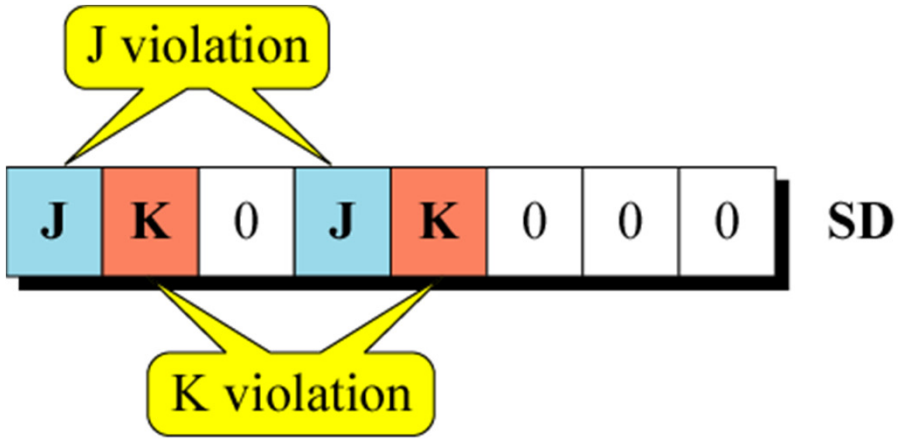
Data Frames

SD Start delimiter (flag)
AC Access control (priority)
FC Frame control (frame type)
ED End delimiter (flag)
FS Frame status



Data frame

SD (Start Delimiter) Field



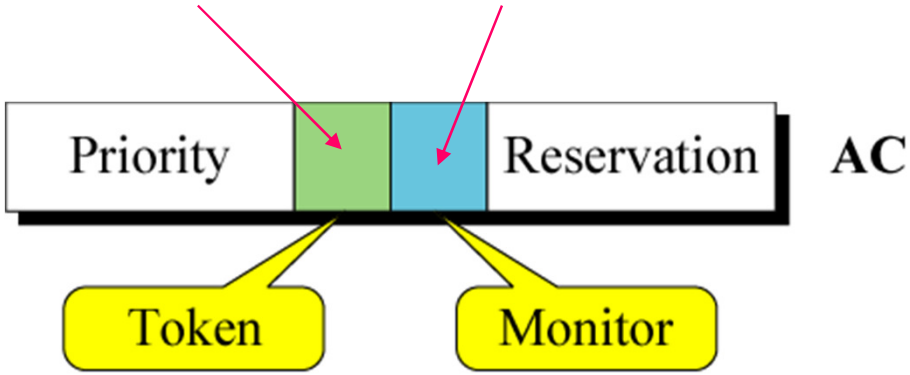
The J and K violations are created at the physical layer

* **Differential encoding: each bit has two transitions:**
  one at the beginning of the bit
  the second at the middle of the bit
* **J violation: both transitions are cancelled**
* **K violation: the middle transition is cancelled**

AC (Access Control) Field

0: token
1: data frame

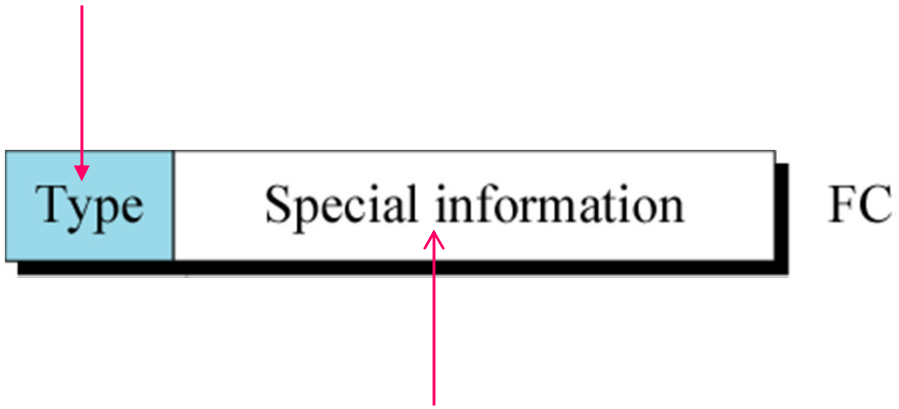
Set to 0 by the sending station
Changed to 1 by the monitor station
to remove an errant frame if it happens



IEEE 802.5 provides a procedure for the selection of a station to become an active monitor

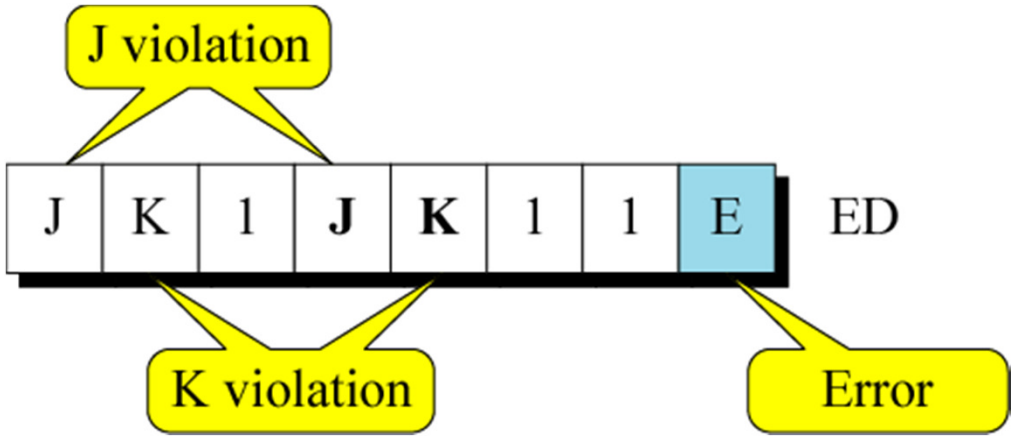
FC (Frame Control) Field

To indicate if it is control information or data in the PDU

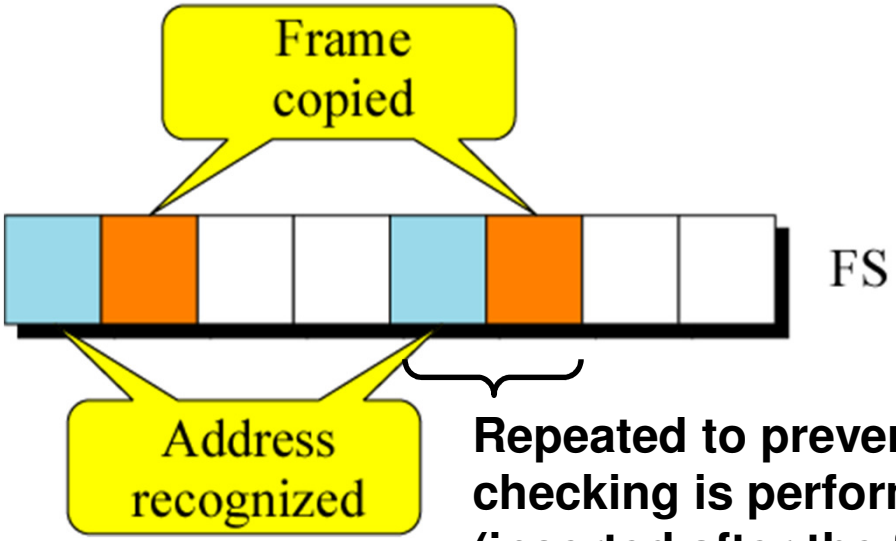


Determines how to use the info in the AC field

ED (End Delimiter) Field



FS (Frame Status) Field



Repeated to prevent errors because no error checking is performed on this part (inserted after the frame leaves the sender)

Can be set

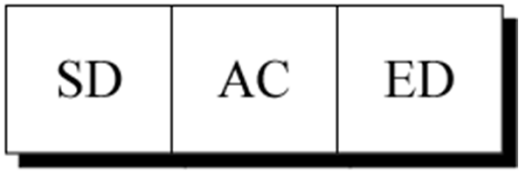
* **by the receiver to indicate that the frame has been read or**
* **by the monitor to indicate that the frame has been around the ring**

Not an ACK, but it does tell the sender that the frame can now be discarded

Token Frame

Really a placeholder and reservation frame, only 3 bytes long

SD	Start delimiter (flag)
AC	Access control (priority)
ED	End delimiter (flag)



Token

SD: a frame is coming
AC: indicates the frame is a token and includes priority and reservation fields
ED: the end of the frame

Token Ring Operation

- Whenever the network is unoccupied, it circulates a simple three-byte token.
- This token is passed from NIC to NIC in sequence until it encounters a station with data to send.
- That station waits for the token to enter its network board. If the token is free the station may send a data frame.
- This data frame proceeds around the ring regenerated by each station.

Token Ring Operation

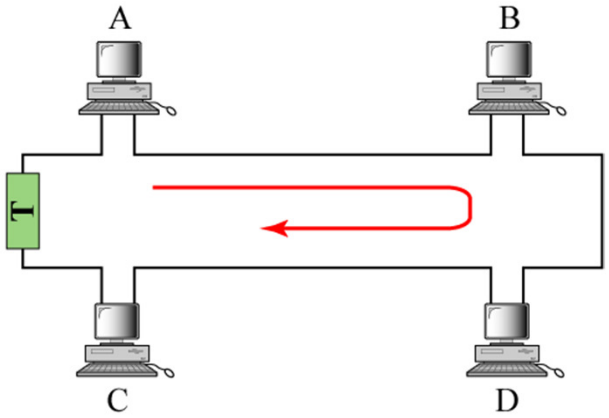
- Each intermediate station examines the destination address, if the frame is addressed to another station, the station relays it to its neighbor.
- If the station recognizes its own address, copies the message, checks for errors, and changes four bits in the last byte of the frame to indicate address recognized and frame copied.
- The full packet then continues around the ring until it returns to the station that sent it.

Token Ring Operation

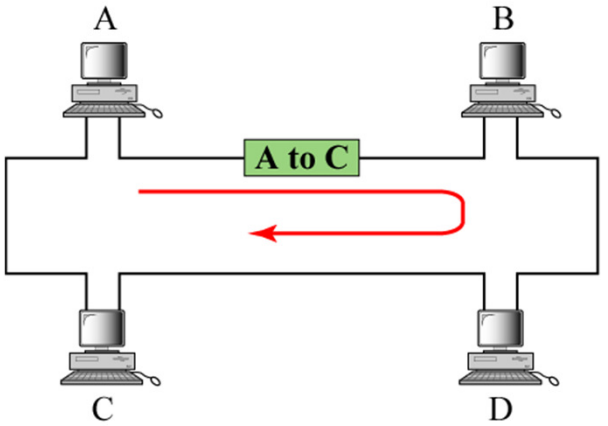
- The sender receives the frame and recognizes itself in the source address field. It then checks the **address-recognized** and **frame copied** bits. If they are set, it knows that the frame was received.

- The sender then discards the used data frame and releases the token back to the ring.

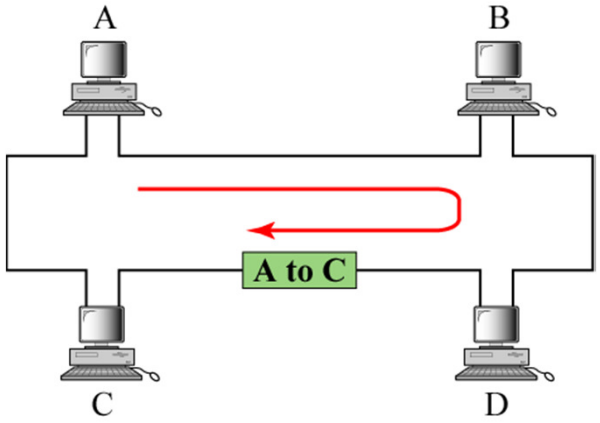
Token Ring Operation



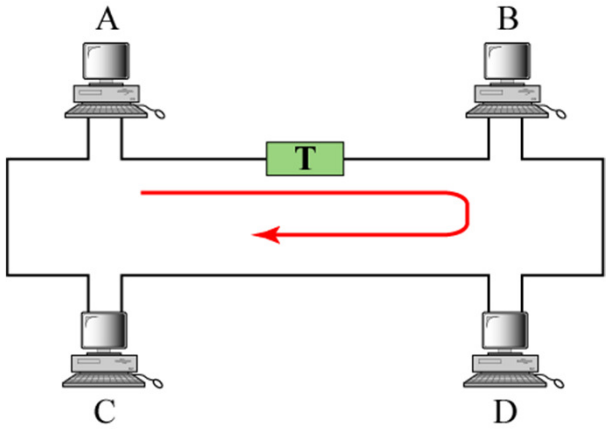
a. Station A captures the token



b. Station A sends data to station C



c. Station C copies data and sends frame back to A



d. Station A releases the token

Priority and reservation

- A busy token can be reserved by a station waiting to transmit regardless of that station's location on the ring.
- Each station has a priority code. As a frame passes by, a station waiting to transmit it may reserve the next open token by entering its priority code in the **access control (AC) field** of the token or data frame.
- A station with a higher priority may remove a lower priority reservation and replace it with its own.

Monitor station

Several problems may occur to disrupt the operation of a token ring network.

1. A station may neglect to retransmit a token
2. A token may be destroyed by noise
3. A sending station may not release the token once its turn has ended
4. A sending station may neglect to remove its used data frame from the ring

To handle these situations, one station on the ring is designated as **monitor station**.

Monitor station

- The monitor sets a timer each the token passes. If the token does not reappear in the allotted time, it is presumed to be lost and the monitor generates a new token and introduces it into the ring.

- The monitor guards against perpetually recirculating data frames by setting a bit (status bit) in the AC (access control) field of each frame.

- If the status bit has been set, it knows that the packet has already been around the ring and should be discarded. The monitor destroys the frame and puts a token into the ring.

IEEE 802 Standards

(WiFi: 802.11)

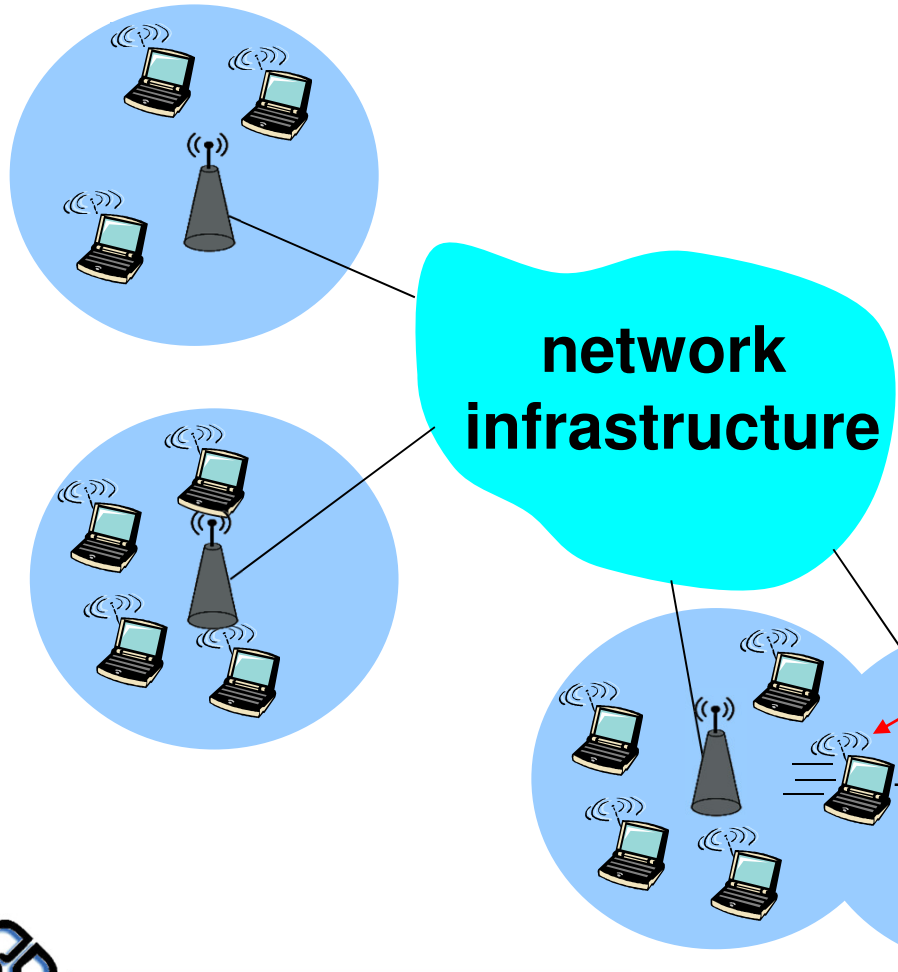
Wireless Link Characteristics

Differences from wired link ….

- decreased signal strength: radio signal attenuates as it propagates through matter (path loss)
- interference from other sources: standardized wireless network frequencies (e.g., 2.4 GHz) shared by other devices (e.g., phone); devices (motors) interfere as well
- multipath propagation: radio signal reflects off objects ground, arriving ad destination at slightly different times

…. make communication across (even a point to point) wireless link much more “difficult”

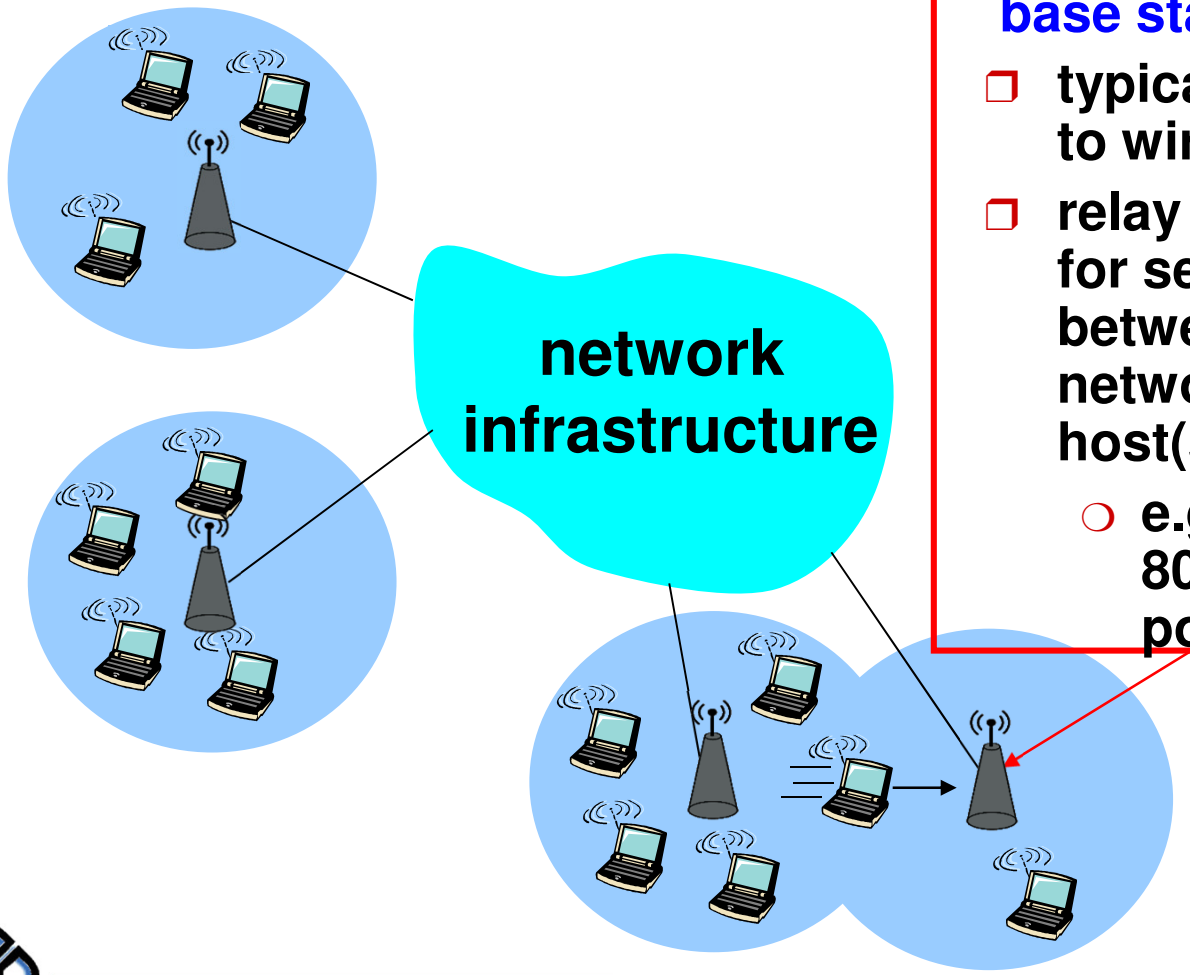
Elements of a Wireless Network

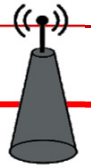


wireless hosts

- laptop, PDA, IP phone
- run applications
- may be stationary (non-mobile) or mobile
  - wireless does *not* always mean mobility

Elements of a Wireless Network

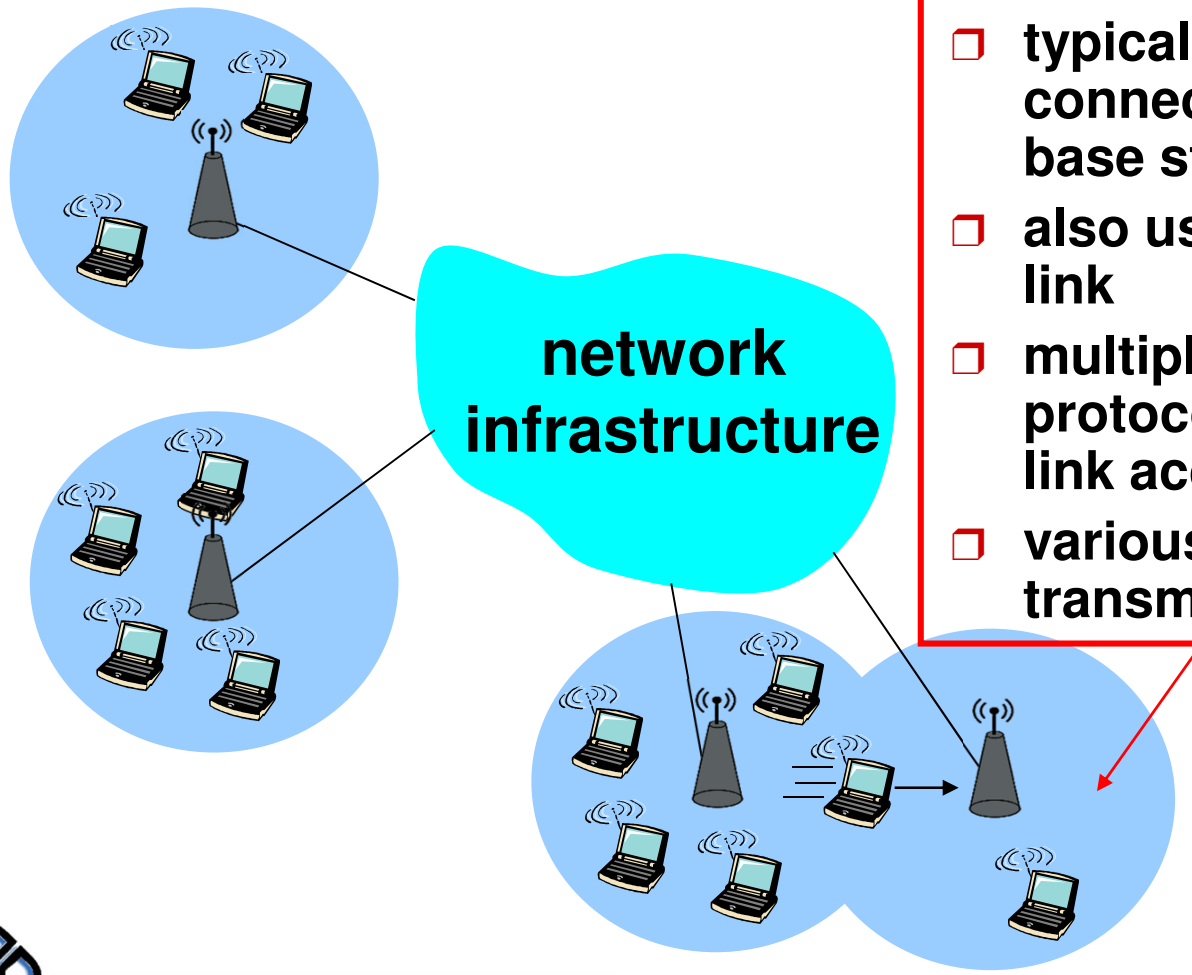




base station

- typically connected to wired network
- relay - responsible for sending packets between wired network and wireless host(s) in its "area"
  - e.g., cell towers, 802.11 access points

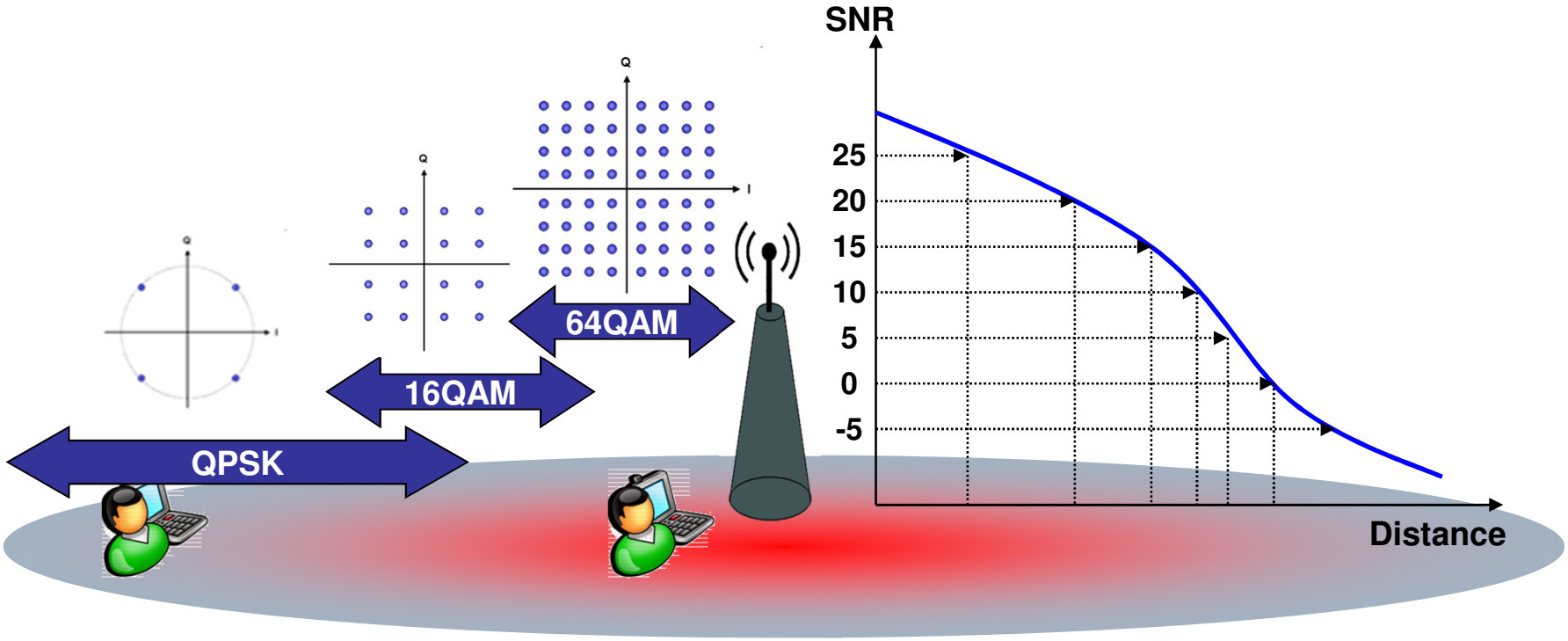
Elements of a Wireless Network



wireless link

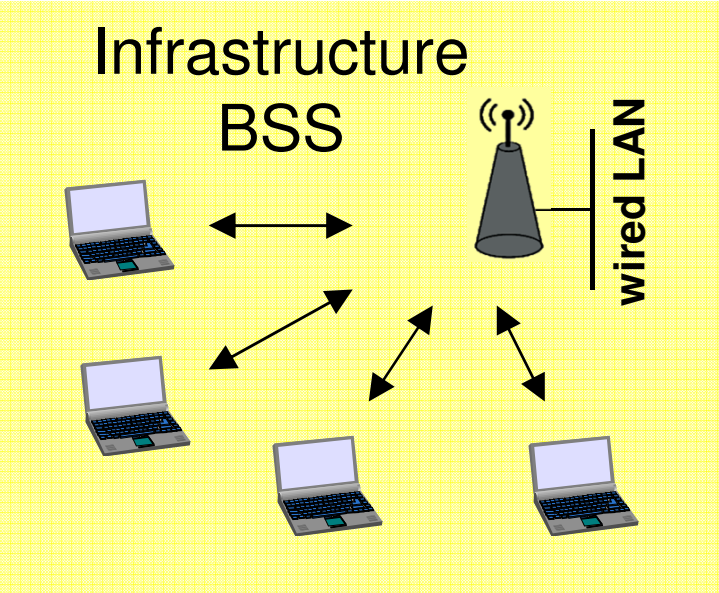
- typically used to connect mobile(s) to base station
- also used as backbone link
- multiple access protocol coordinates link access
- various data rates, transmission distance

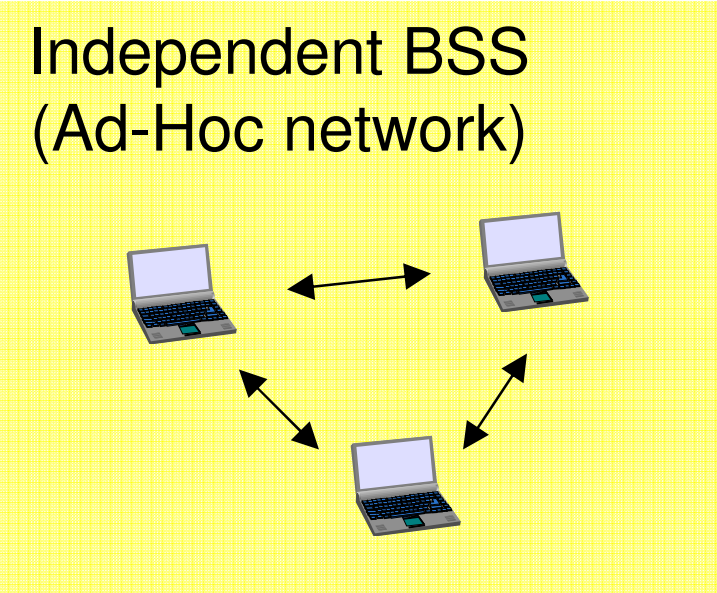
Distance Sensitivity in Wireless Networks



IEEE 802.11 WLAN architecture

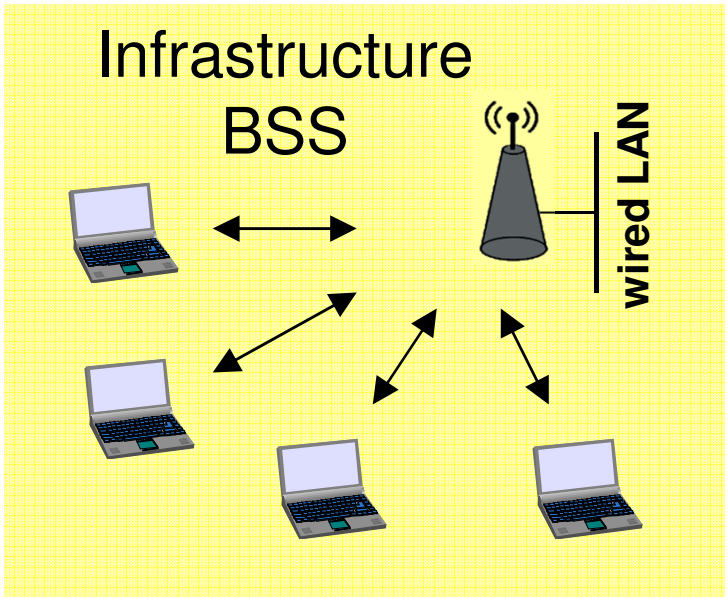
802.11 defines two BSS (Basic Service Set) options:





Infrastructure BSS

This is by far the most common way of implementing WLANs.



The base stations connected to the wired infrastructure are called access points (AP).

Wireless stations in an Infrastructure BSS must always communicate via the AP (never directly).

Before stations can use the BSS: Association.

Independent BSS (Ad-Hoc configuration)

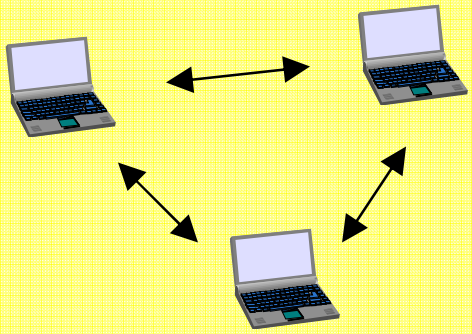
Very hot topic for research- So many new applications

No access point is required, stations can communicate directly.

Efficient routing of packets is not a trivial problem
(routing is not a task of 802.11).

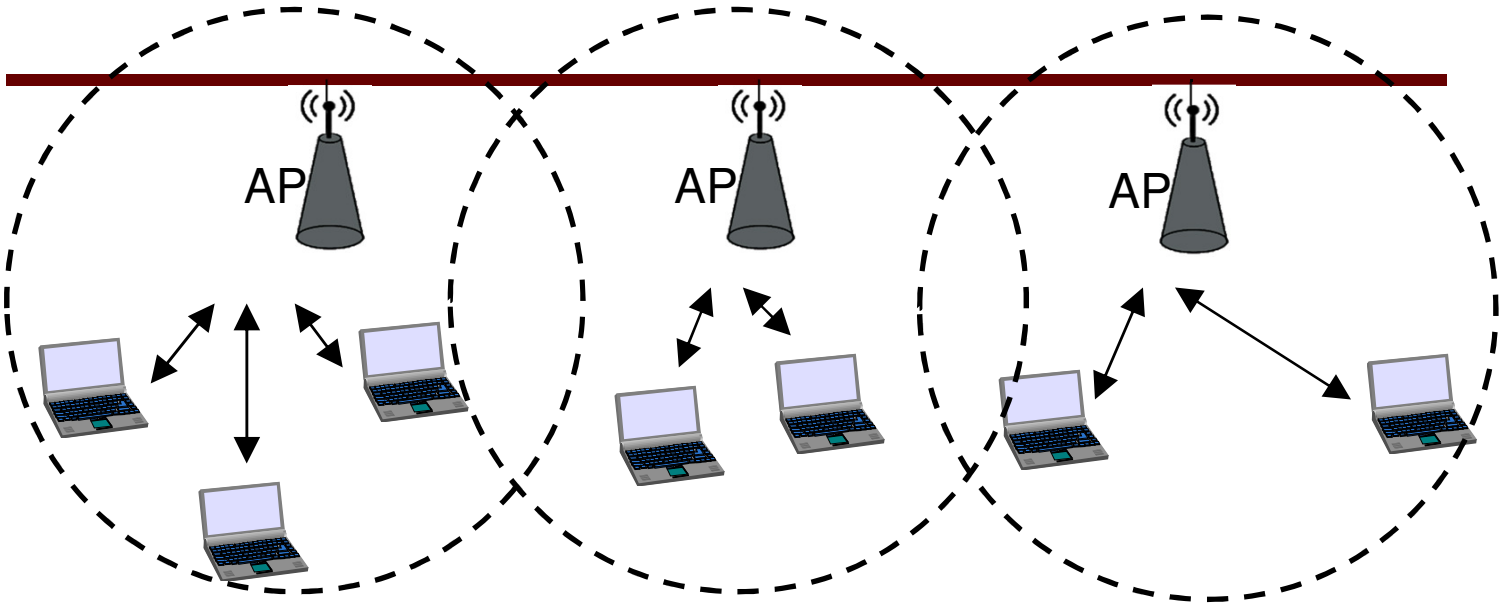
Ad-Hoc WLAN networks are outside the scope of this course.

Independent BSS
(Ad-Hoc network)



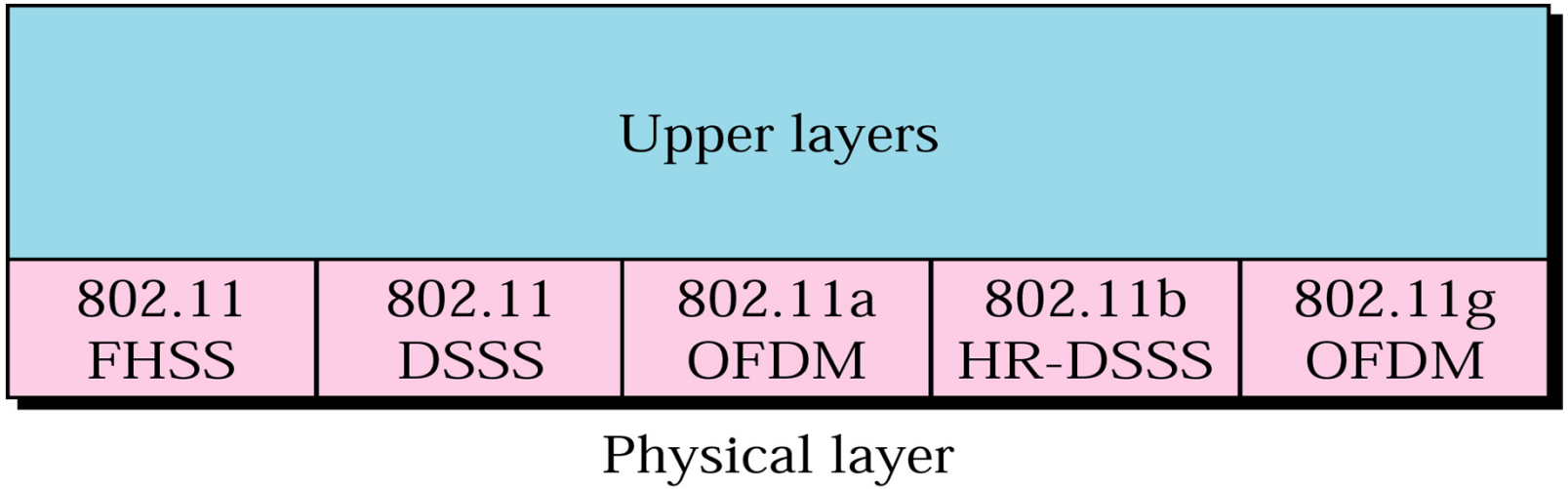
Extended Service Set (ESS)

This is a larger WLAN network consisting of a number of BSS networks interconnected via a common backbone



802.11 supports link-layer mobility within an ESS (but not outside the ESS)

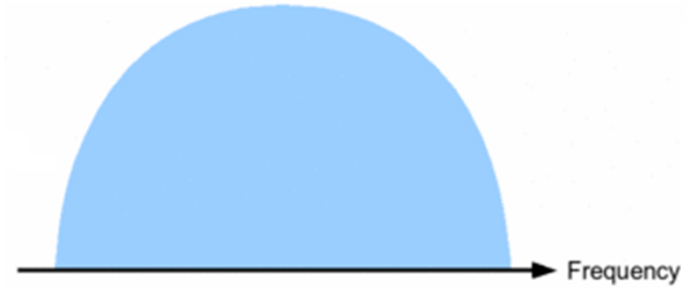
IEEE 802.11 Physical Layer



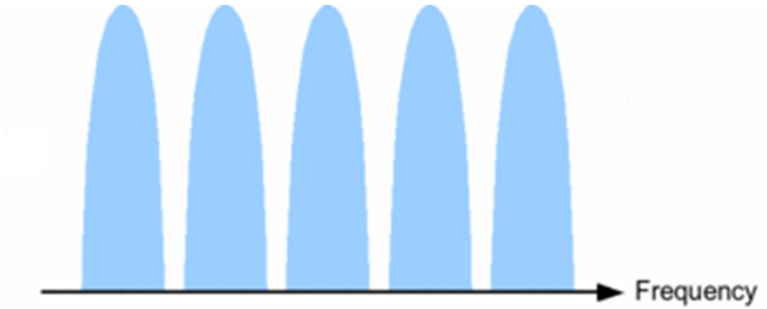
IEEE specifies different Physical layer techniques for 802.11

Multi-carrier transmission

Single carrier



Multi carrier

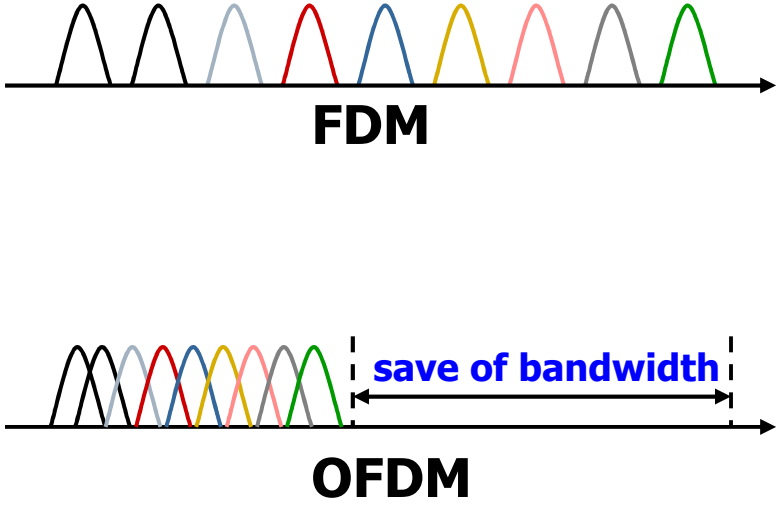


Convert a serial high rate data stream on to multiple parallel low rate sub-streams.

OFDM vs. FDM

High spectral efficiency:

- The sub-channels are made **orthogonal** to each other over the OFDM symbol duration.
- Spacing is carefully selected.
- Allow the sub-channels to overlap in the frequency domain.
- Allow sub-carriers to be spaced as close as theoretically possible.



OFDM: Orthogonal Frequency Division Multiplexing

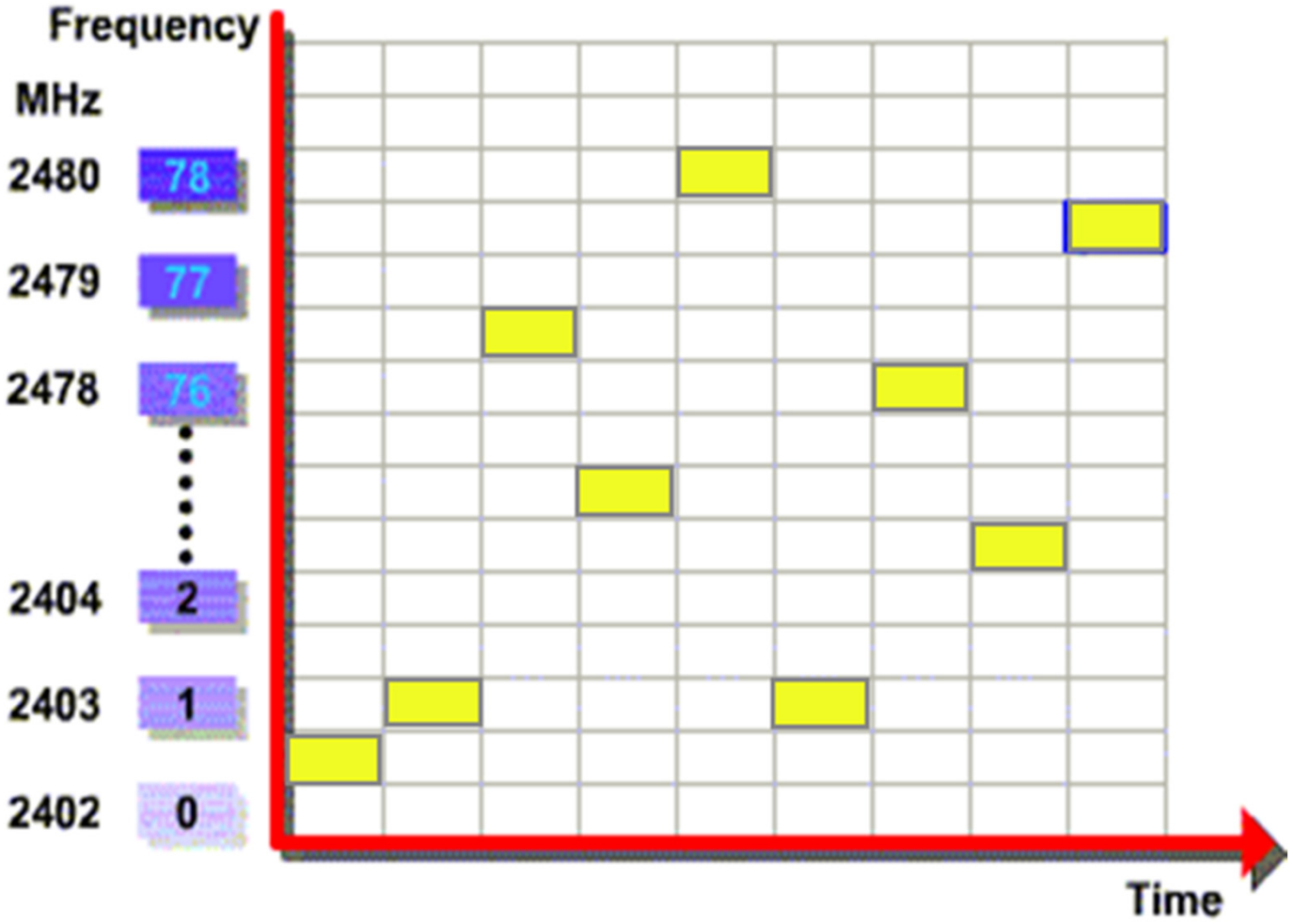
Frequency hopping Spread Spectrum (FHSS)

- This dilemma was recognized prior to WWII.
- In 1942, Hedy Lamarr and pianist George Antheil patented a “Secret Communication System”.
- Their scheme was for a **frequency hopping** remote control for torpedo guidance.

Hedy Lamarr

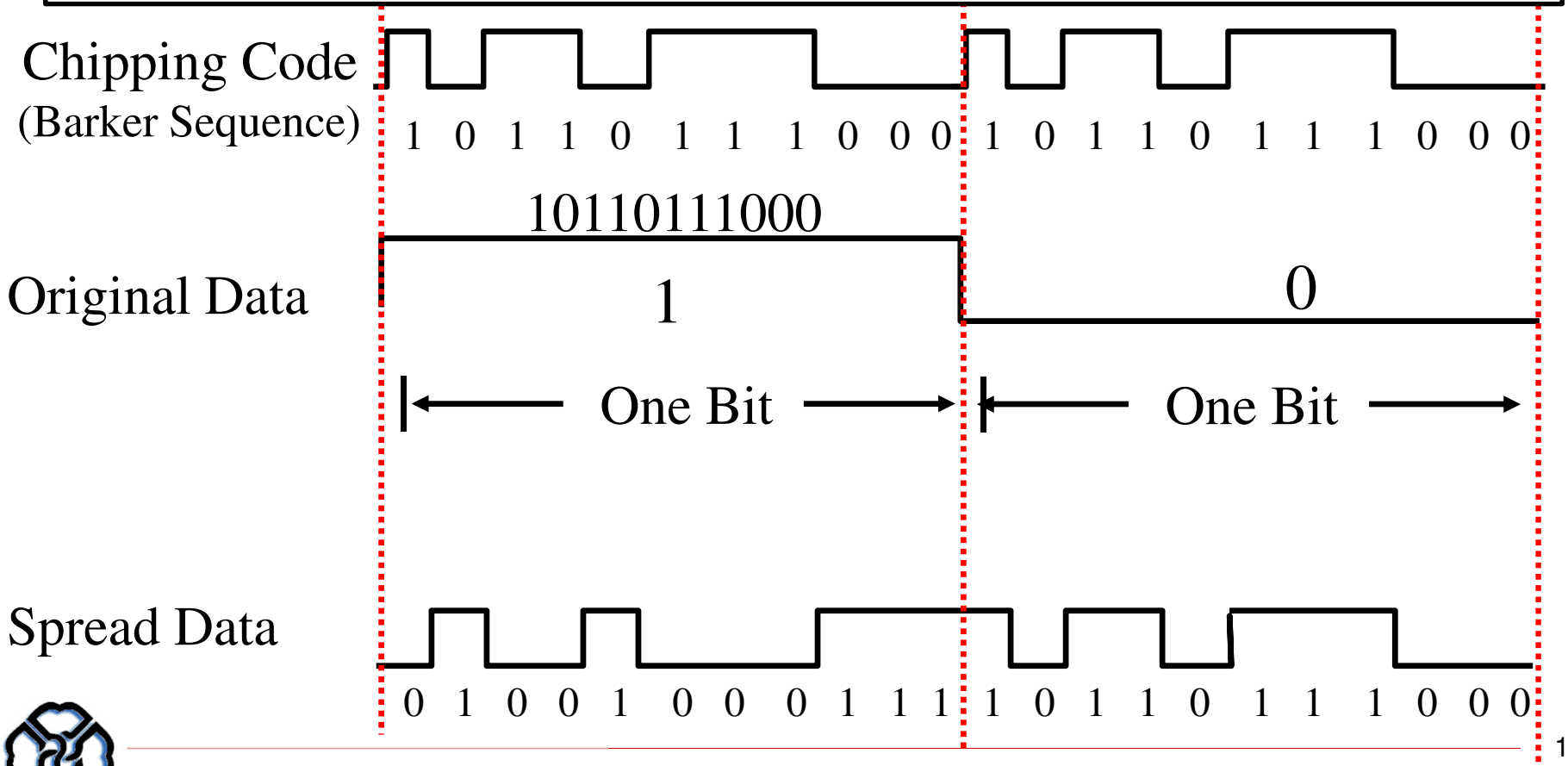
Actress and co-inventor of frequency hopping spread spectrum

FHSS

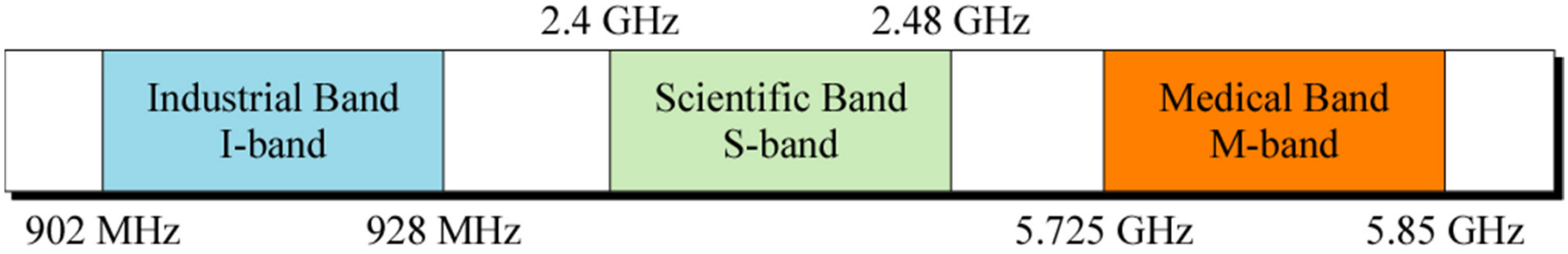


Direct Sequence Spread Spectrum (DSSS)

In a DSSS system the message bit stream is modified by a higher rate sequence (called a chip sequence).



ISM Bands (Unlicensed)



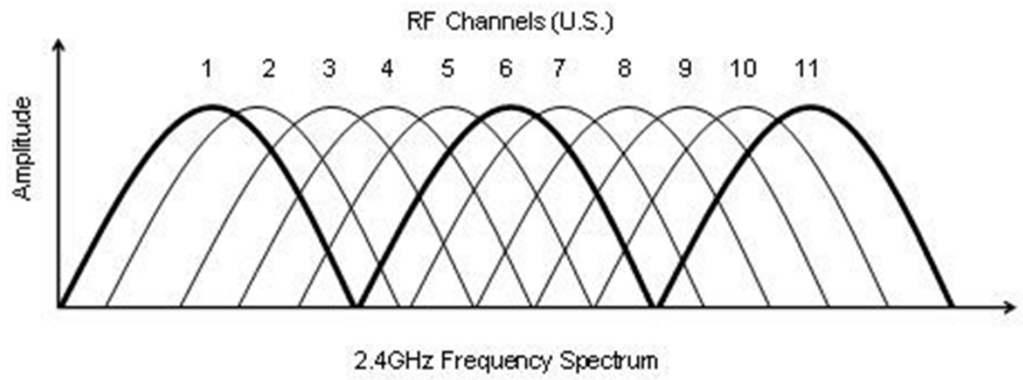
802.11b
(up to 11Mbps)

802.11a
(up to 54 Mbps)

802.11g
(up to 54 Mbps)

802.11b

- Introduced in 1999
- Uses the unlicensed 2.4 GHz band
  - Same band as cordless phones, microwave ovens
- 5.5 and 11 Mbps data rates
  - Practical throughput with TCP is only 5.9 Mbps
- 11 channels (in the US). Only 1, 6, and 11 are non-overlapping



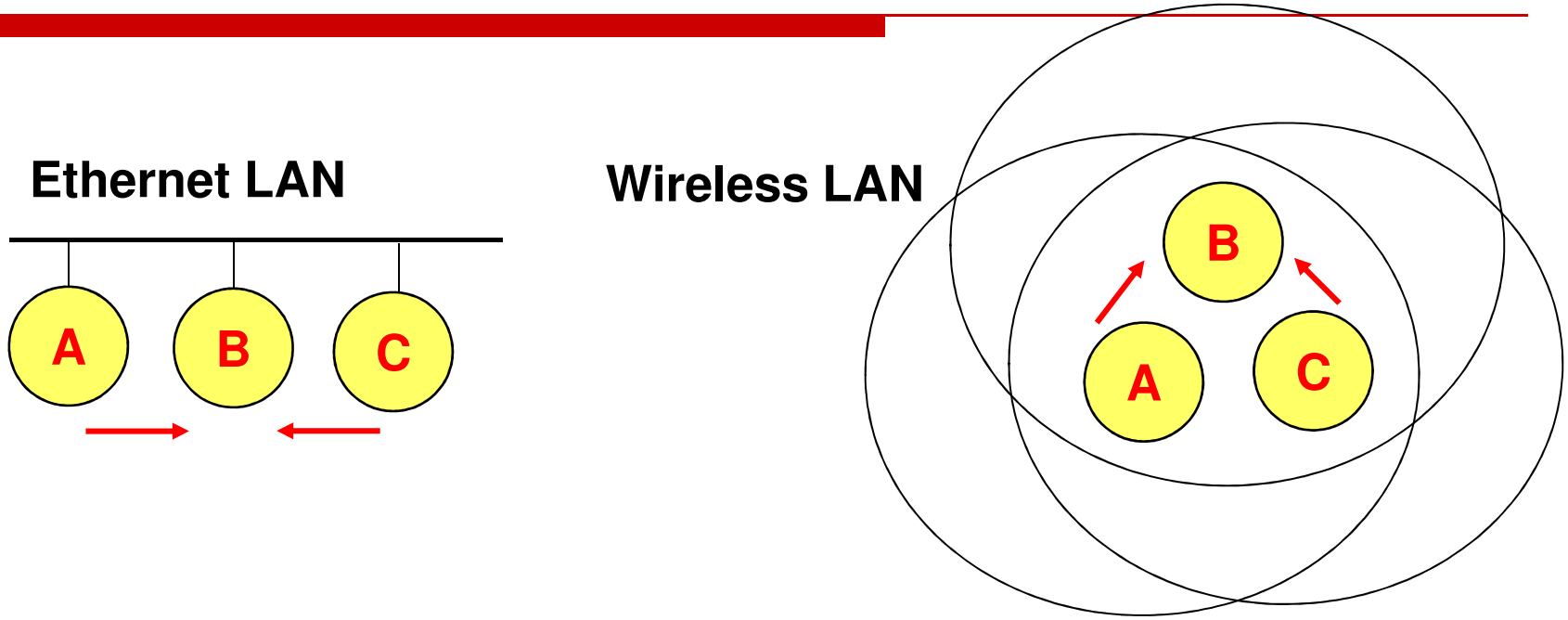
802.11a/g

- 802.11a
  - Uses the 5 GHz band
  - 6, 9, 12, 18, 24, 36, 48, 54 Mbps
  - Switches from CCK to Orthogonal Frequency Division Multiplexing (OFDM)
    - Each frequency is orthogonal
- 802.11g
  - Introduced in 2003
  - Uses OFDM to improve performance (54 Mbps)
  - Backwards compatible with 802.11b

802.11n/ac

- 802.11n
  - Introduced in 2009
  - Multiple Input Multiple Output (MIMO)
    - Multiple send and receive antennas per devices (up to four)
    - Data stream is multiplexed across all antennas
  - Maximum 600 Mbps transfer rate (in a 4x4 configuration)
  - 300 Mbps is more common (2x2 configuration)
- 802.11ac
  - Almost finished, draft standard
  - 8x8 MIMO in the 5 GHz band, 500 Mbps – 1 GBps rates

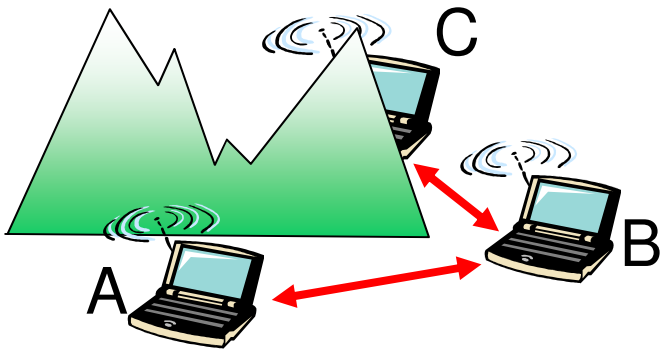
Difference Between Wired and Wireless

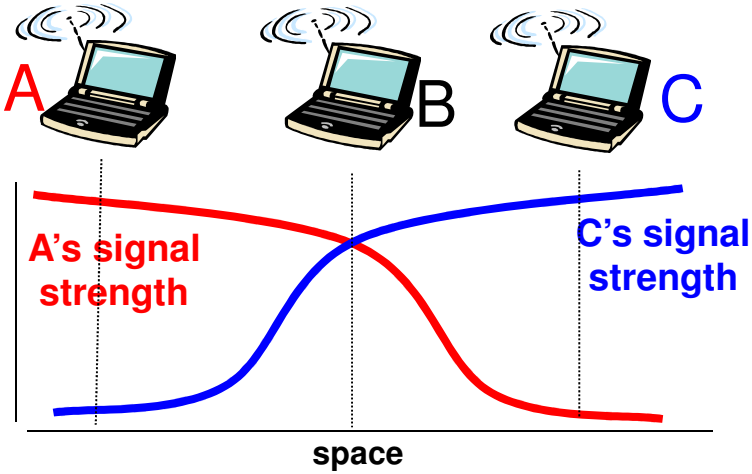


- If both A and C sense the channel to be idle at the same time, they send at the same time.
- Collision can be detected **at sender** in Ethernet.
- Half-duplex radios in wireless cannot detect collision at sender.

Hidden terminal problem

Multiple wireless senders and receivers create additional problems (beyond multiple access):





Hidden terminal problem

- B, A hear each other
- B, C hear each other
- A, C can not hear each other

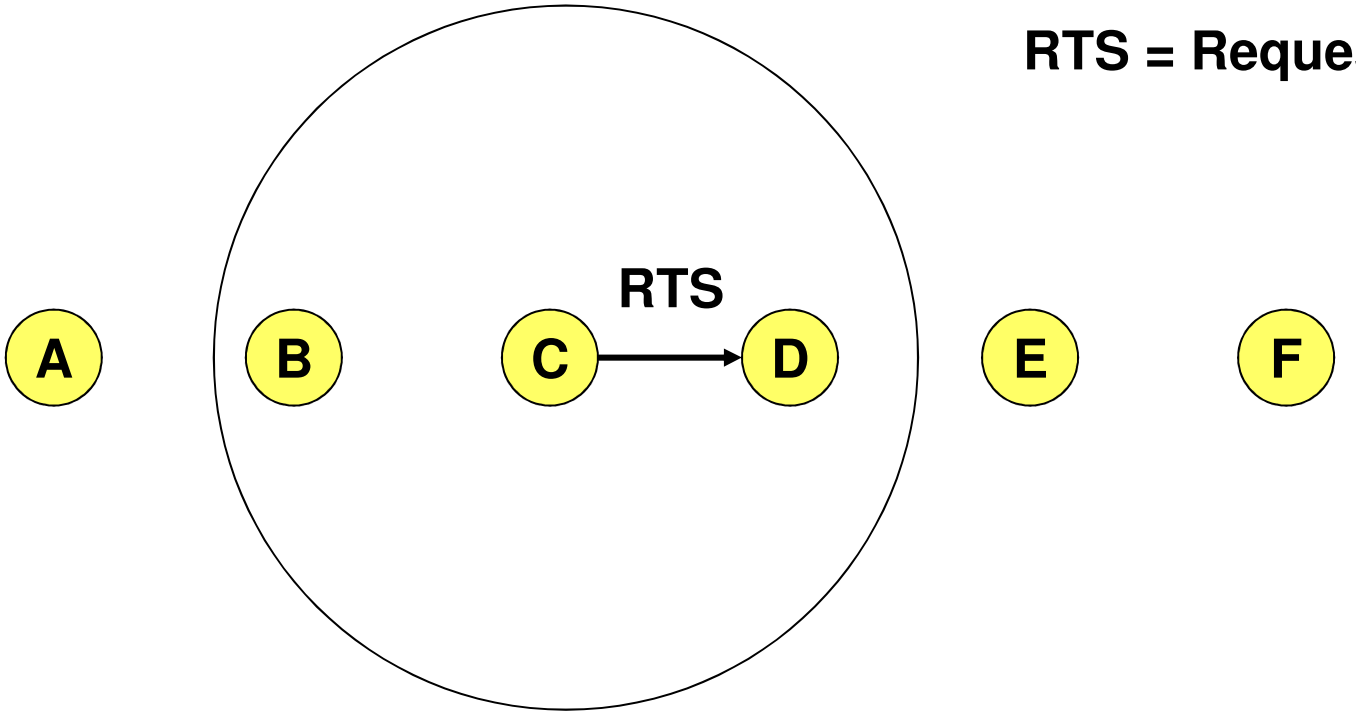
means A, C unaware of their interference at B

Signal attenuation:

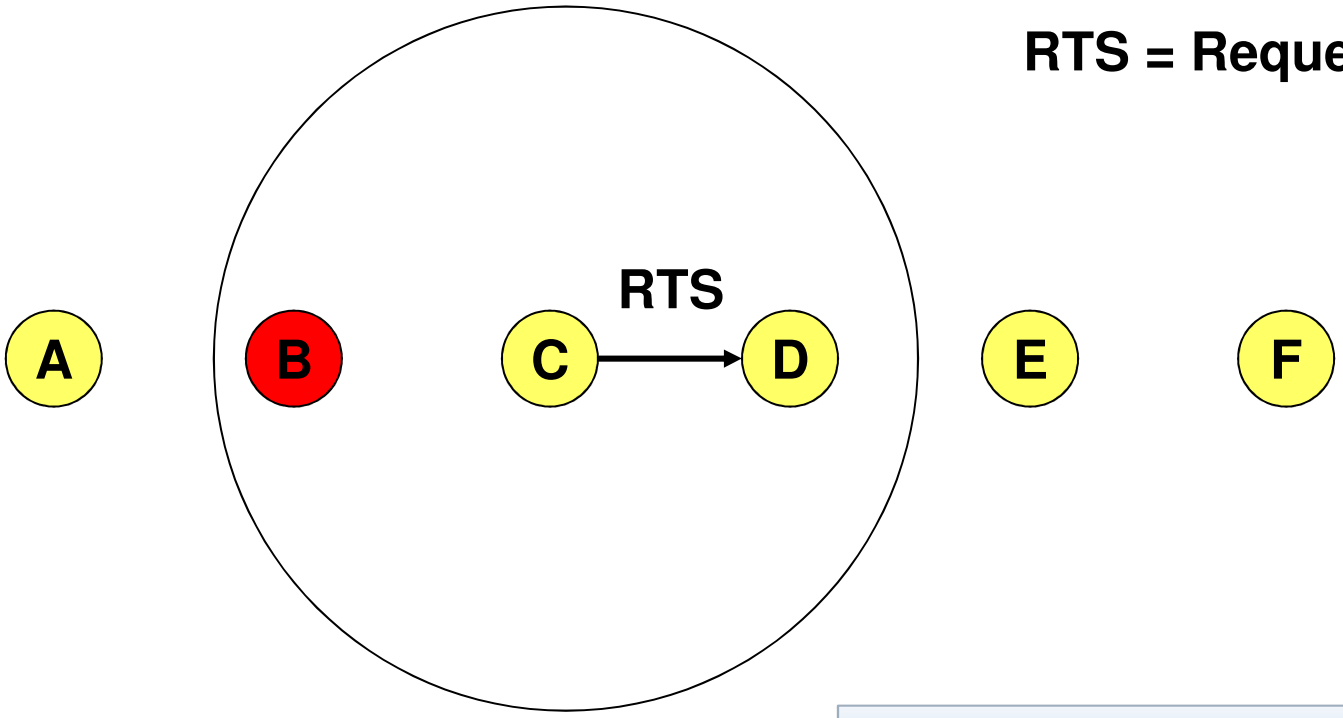
- B, A hear each other
- B, C hear each other
- A, C can not hear each other interfering at B

Virtual carrier sensing (with RTS and CTS)

idea: allow sender to “reserve” channel rather than random access of data frames: avoid collisions of long data frames

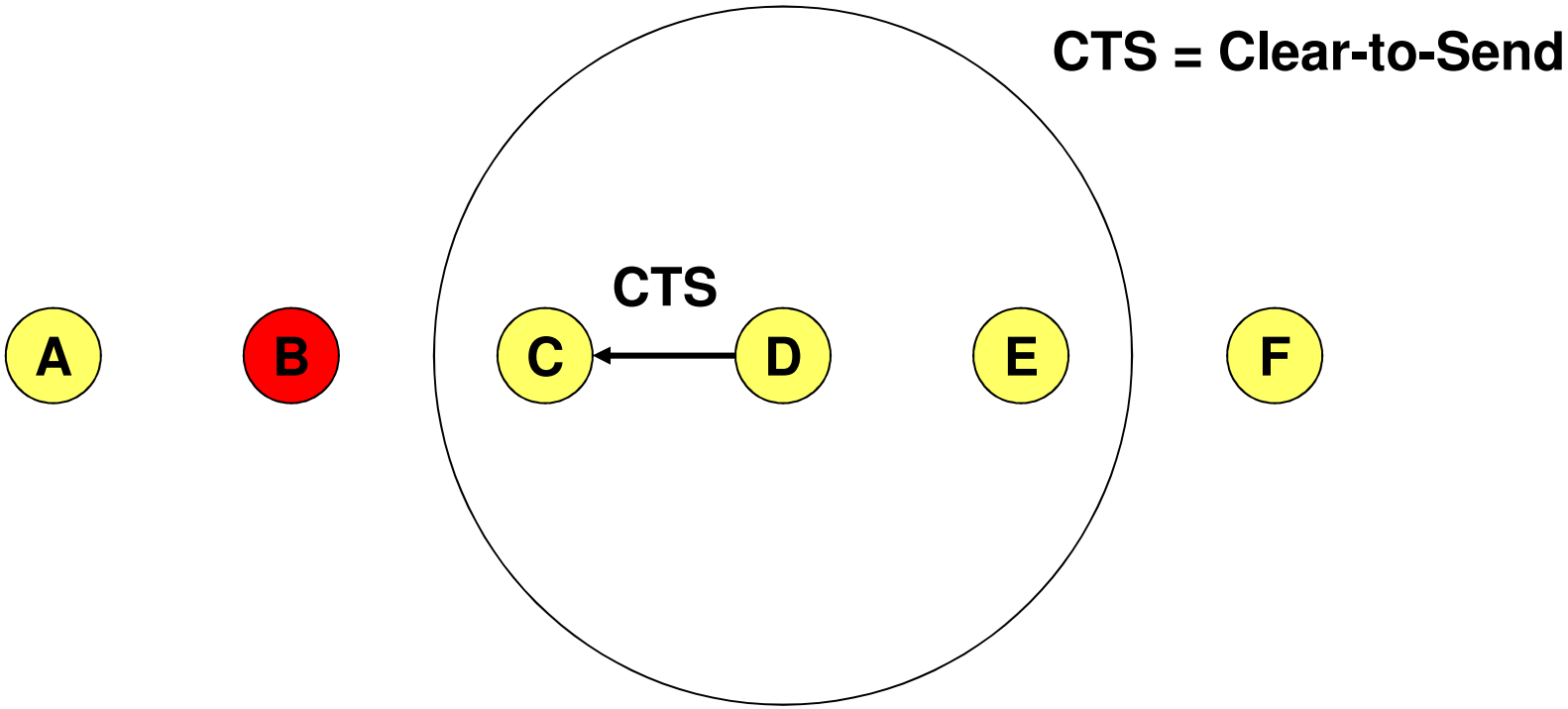


Virtual carrier sensing (with RTS and CTS)

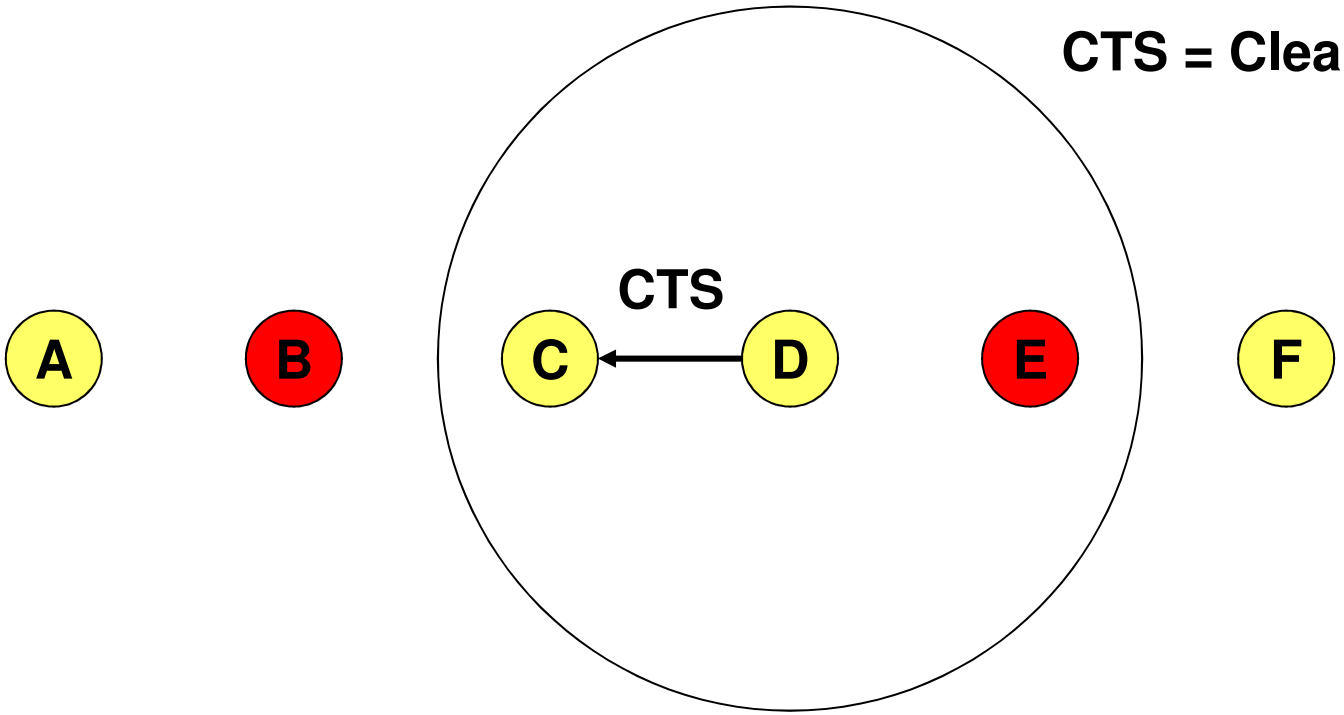


B hears RTS, becomes silent

Virtual carrier sensing (with RTS and CTS)

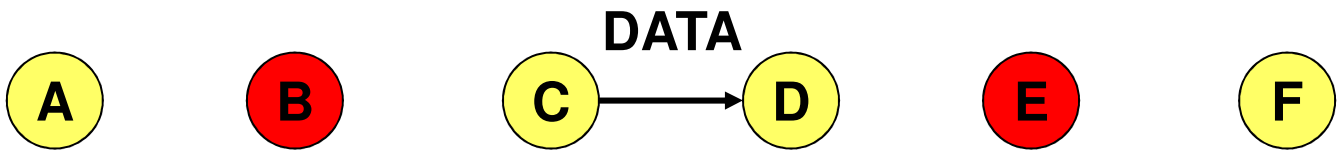


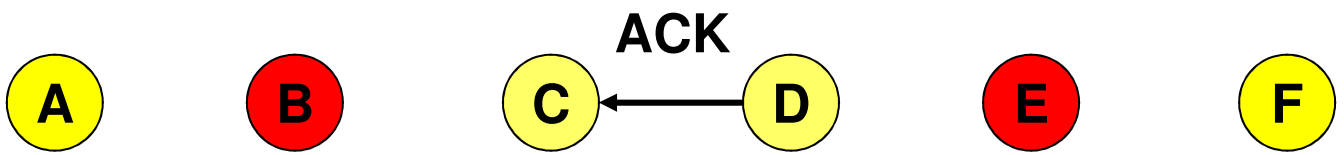
Virtual carrier sensing (with RTS and CTS)



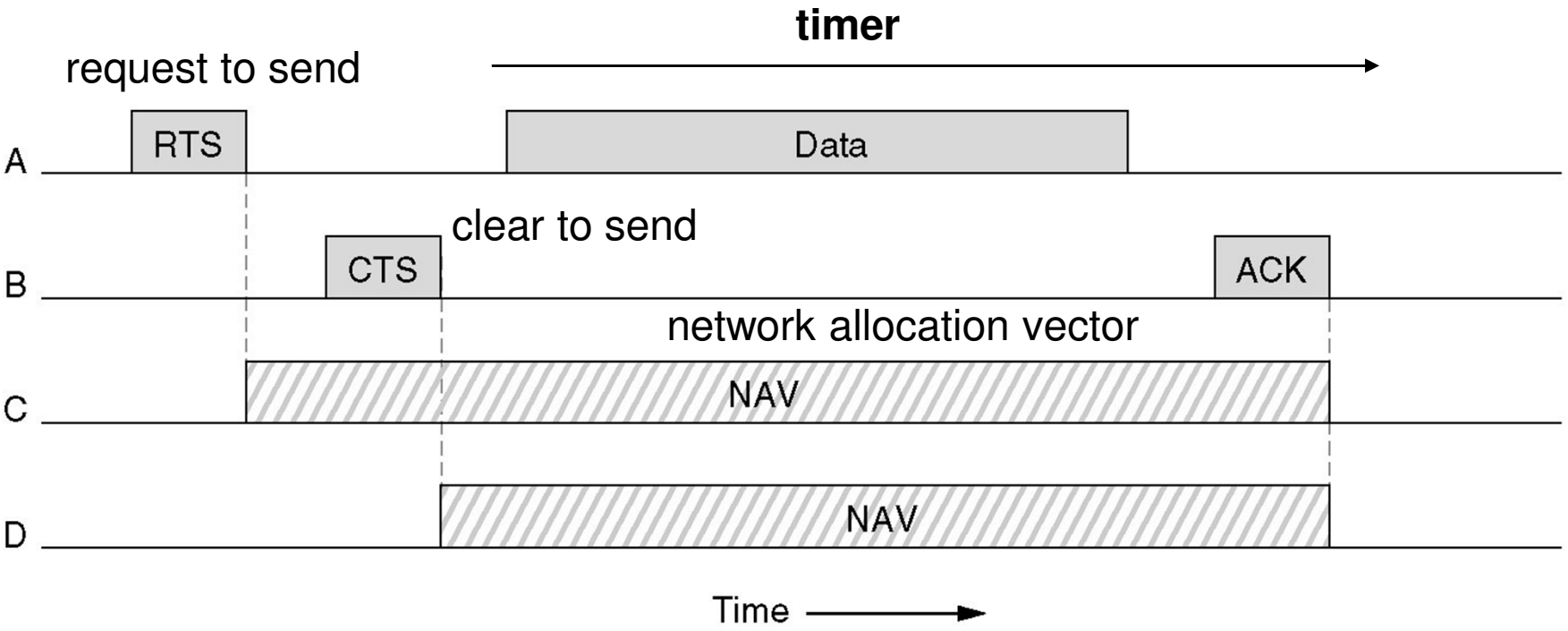
E hears CTS, becomes silent

Virtual carrier sensing (with RTS and CTS)





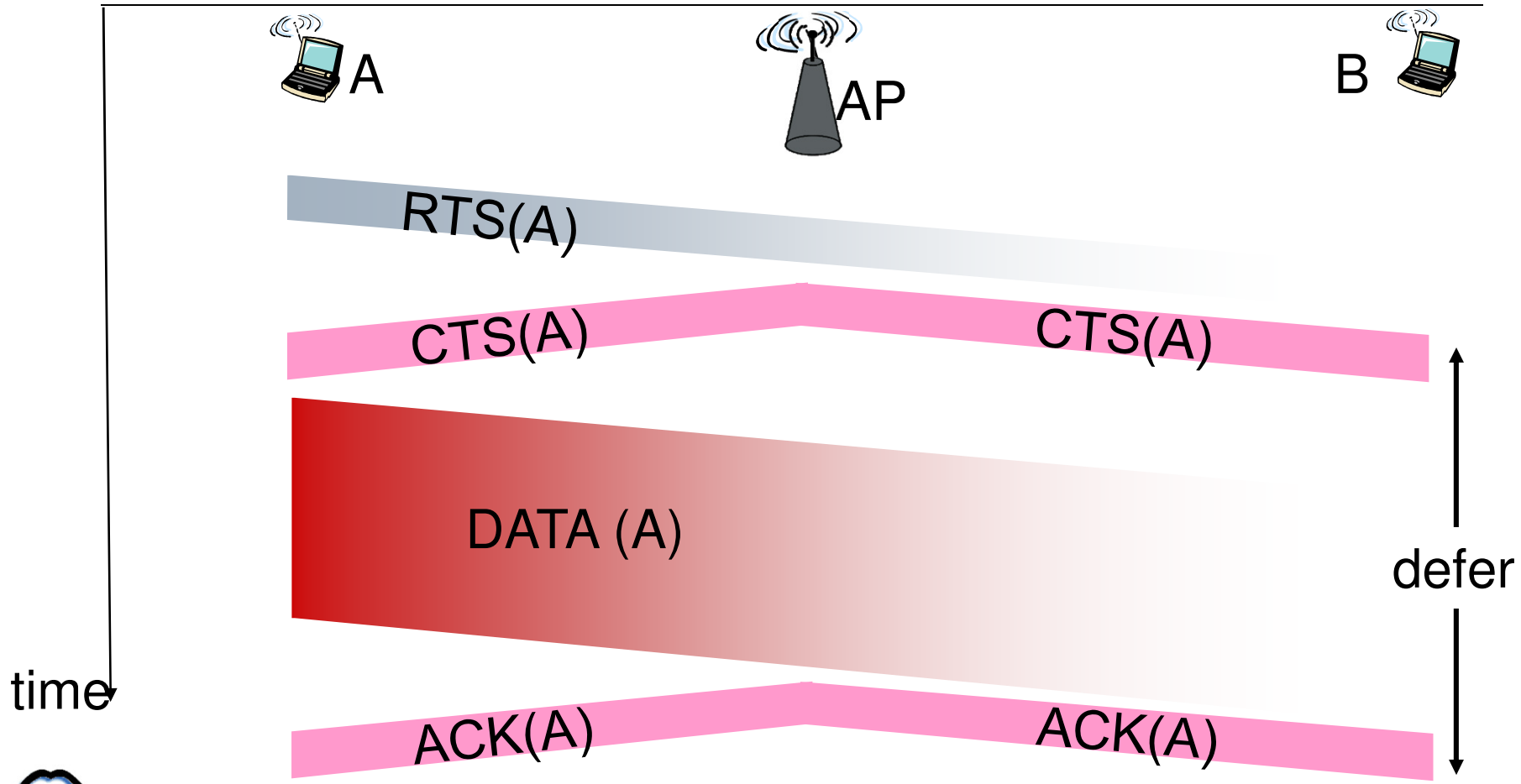
802.11 MAC: CSMA/CA



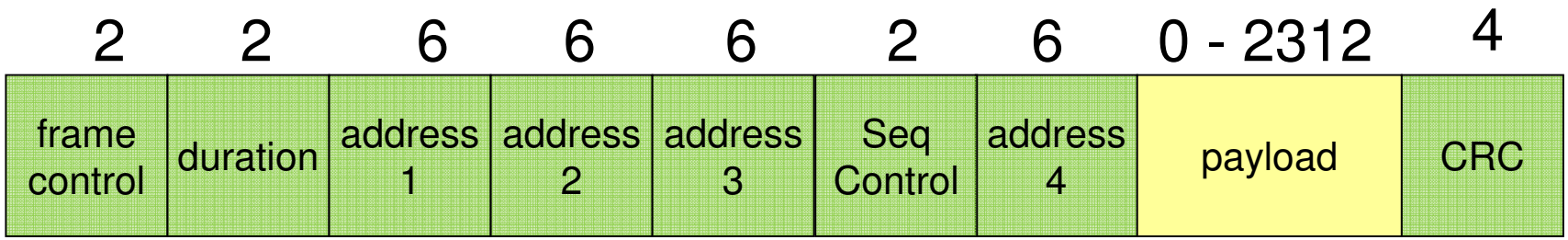
The use of virtual channel sensing using CSMA/CA.

C can hear A (RTS) and D can hear B (CTS)

Collision Avoidance: RTS-CTS exchange



802.11 frame: addressing



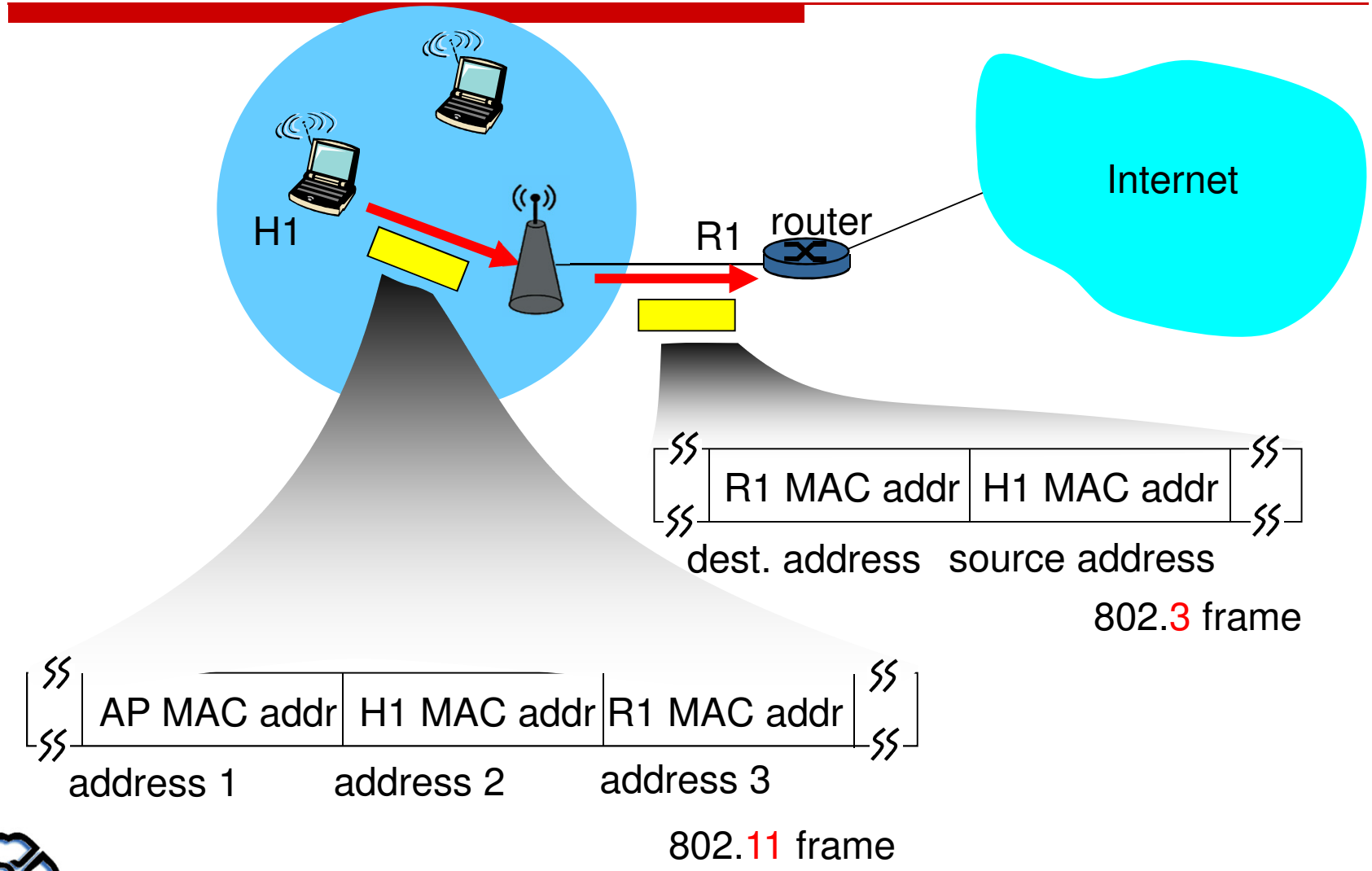
Address 1: MAC address of wireless host or AP to receive this frame

Address 2: MAC address of wireless host or AP transmitting this frame

Address 3: MAC address of router interface to which AP is attached

Address 4: used only in ad hoc mode

802.11 frame: addressing



802.11 MAC (fragmentation)

- Wireless environments very noisy!
- Probability of frame to be transmitted successfully inversely proportional to the frame length

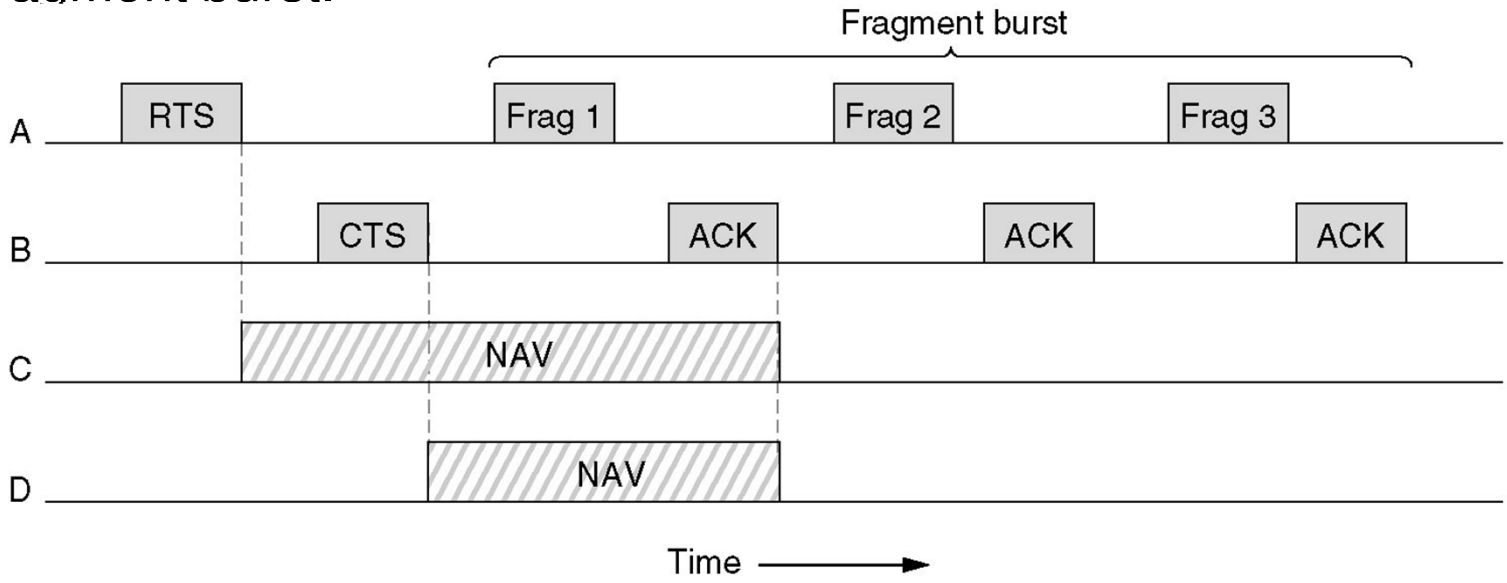
Frame length

- If bit error ρ then successful frame transmission $(1-\rho)^n$
  - for $\rho=10^{-4}$ and frame size of 1000 bytes, almost 55% of frames are damaged.
- Damaged frames have to be retransmitted

- Solution:
- Each frame fragmented with fragments having their own FCS
- The fragments are ACKn'd using Stop-and-Wait protocol

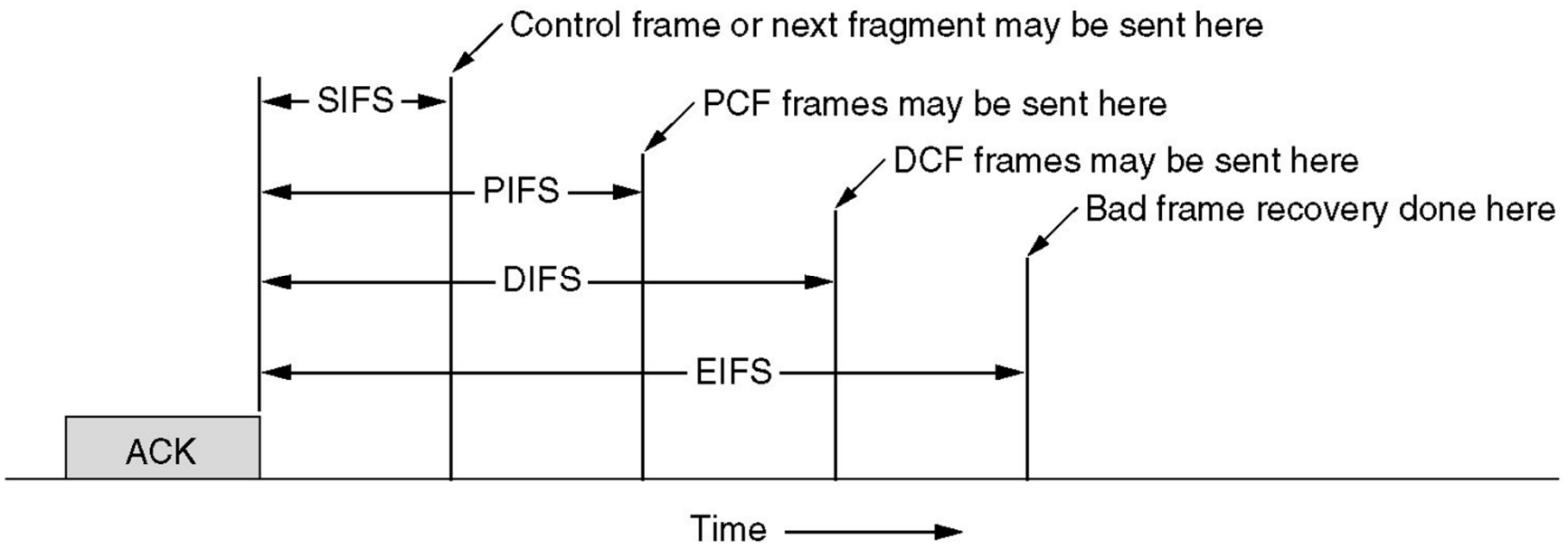
CSMA/CA with frame fragmentation

- A fragment burst.



- Only damaged fragments retransmitted -throughput increased
- NAV keeps the other station quiet only until the next ACK
- How to transmit whole frame without interference? (using SIFS)

Interframe spacing in 802.11



SIFS: Short Inter-Frame Space (28 microseconds)

PIFS: PCF Inter-Frame Space (78 microseconds)

DIFS: Distributed Inter-Frame Space (128 microseconds)

EIFS: Extended Inter-Frame Space


Questions