Medium Access Control Sublayer

Thomas Schwarz, SJ

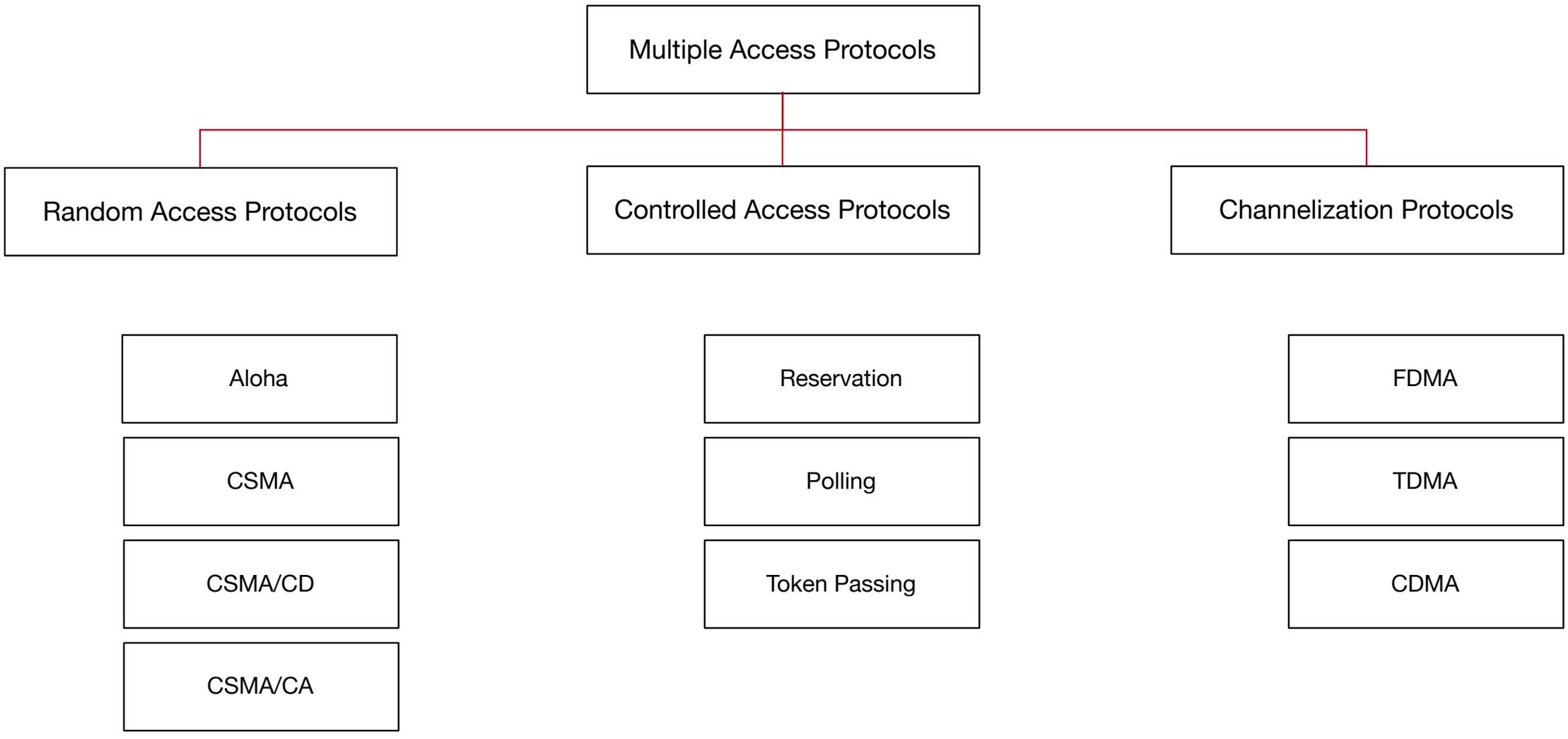
Media Access Control

- Problem:
  - Several entities use the same physical channel
  - Need to allow fair access:
    - No starvation
    - No conflicts

Media Access Control Protocols

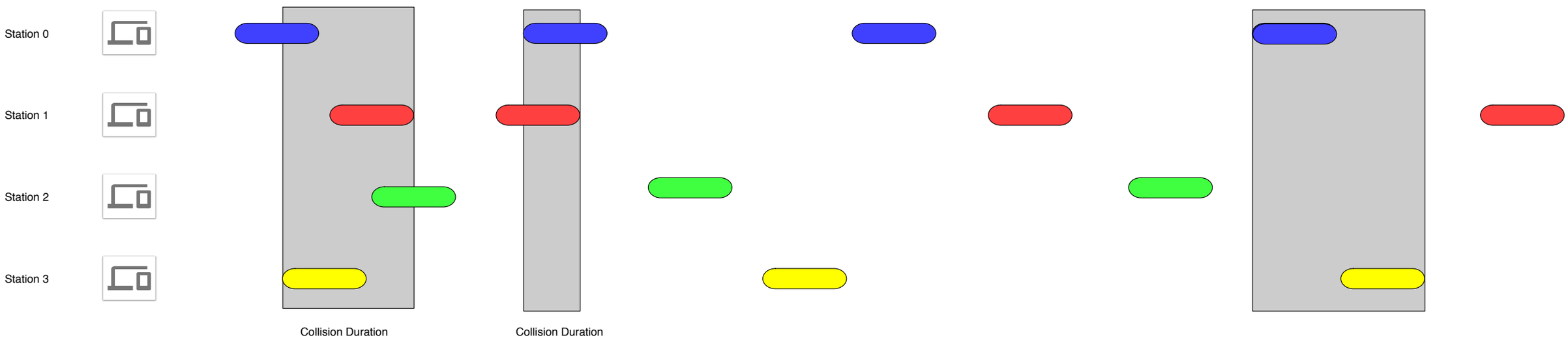
- Random Access / Contention Protocols
  - No coordination
  - Nodes decide according to protocol when to send
  - Possibility of frame collision
- Controlled Access
  - Nodes coordinate to provide one node with the right to send packages
- Channelization
  - Available bandwidth divided into channels
  - Each channel owned by one node

Media Access Control Protocols



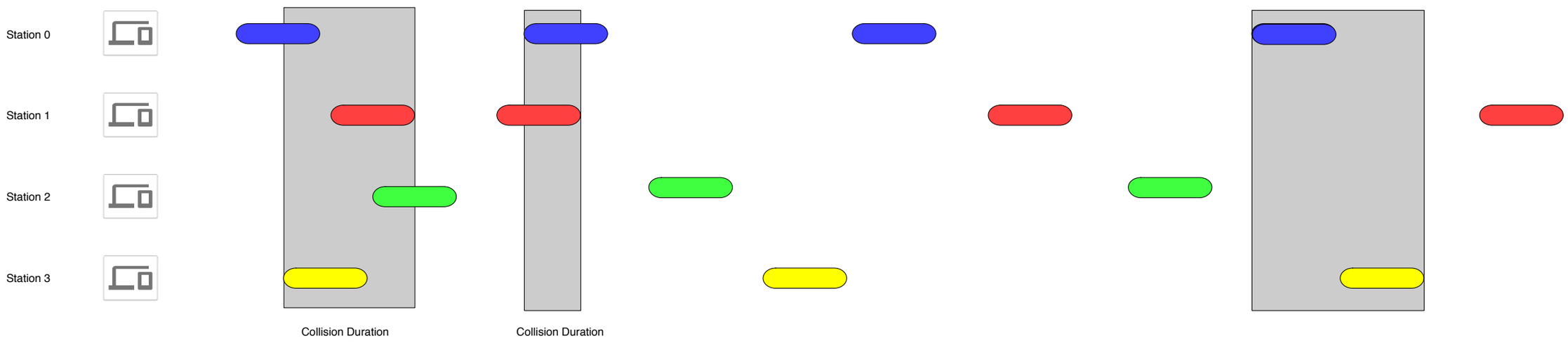
Aloha

- Developed at University of Hawaii to allow multiple campus share the same mainframe by Abramson (1970)
  - Each station sends a frame whenever some frame is ready
  - Frames can collide
  - Frames that make it through are acknowledged

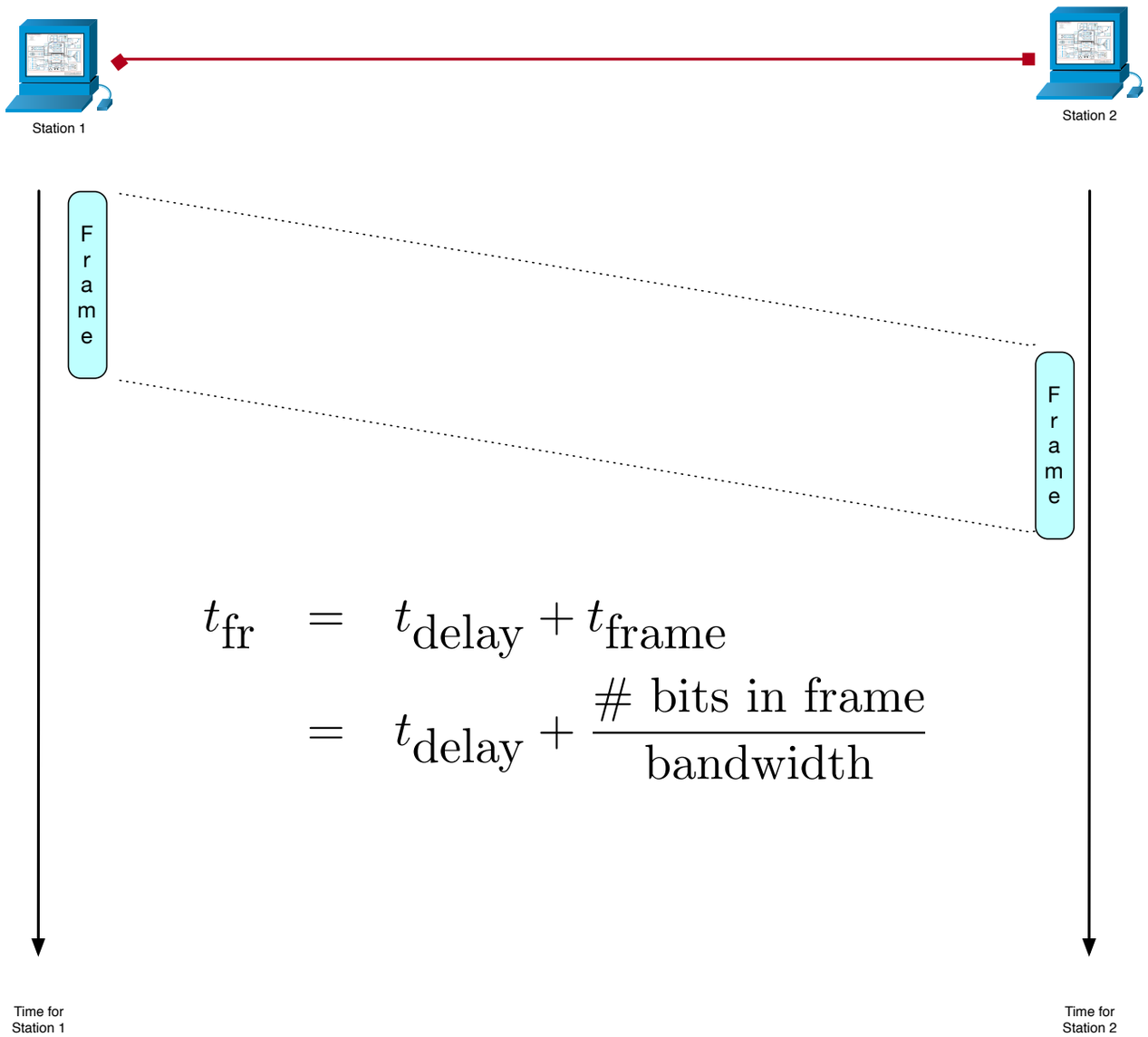


Aloha Collisions

- Collision:
  - Two frames that overlap even in a single bit collide



Aloha Vulnerable Time

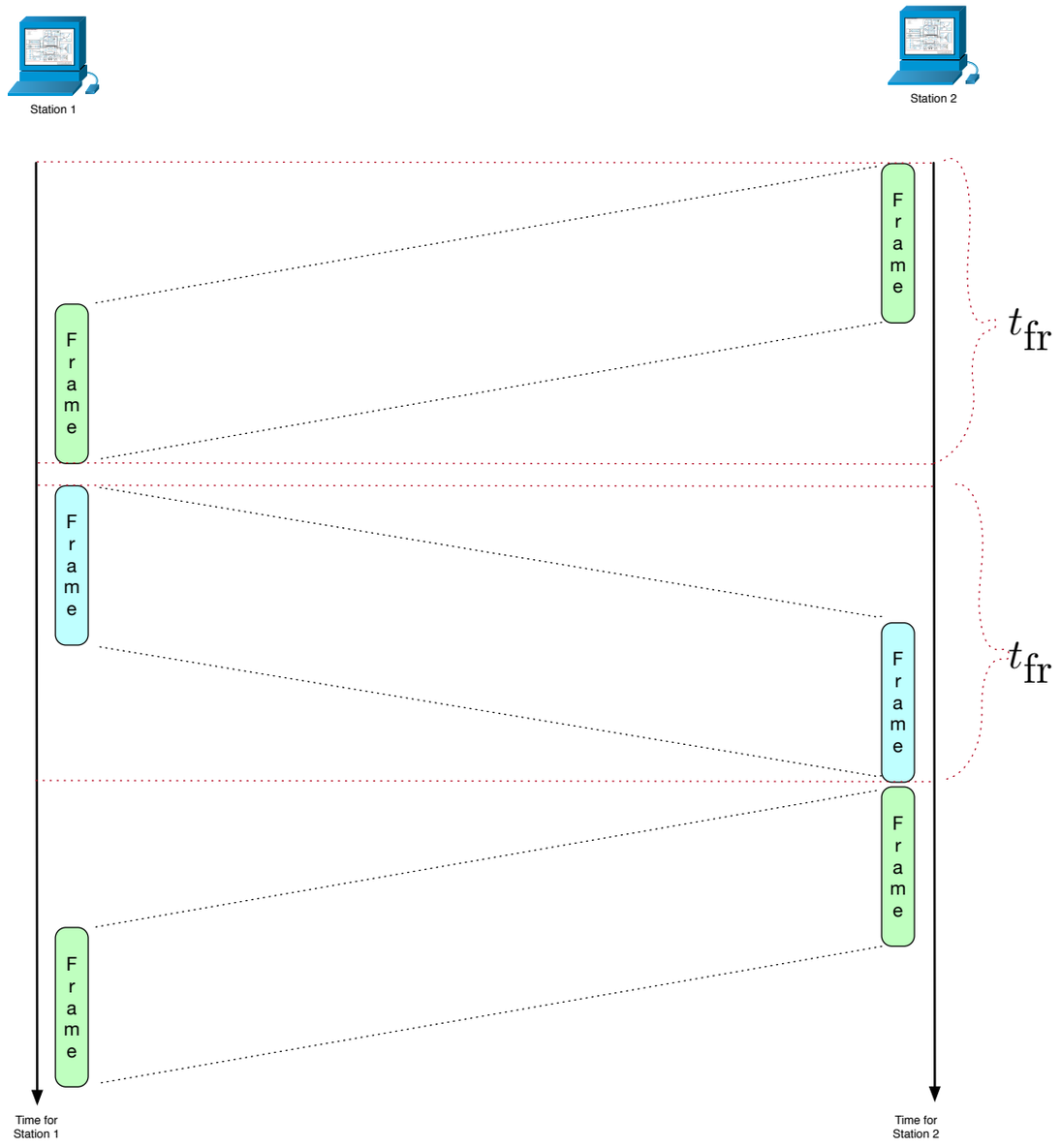


$$
\begin{aligned}
t_{\text{fr}} &= t_{\text{delay}} + t_{\text{frame}} \\
&= t_{\text{delay}} + \frac{\#\text{ bits in frame}}{\text{bandwidth}}
\end{aligned}
$$

Frame transmission time is composed of delay and the time to send out the frame

Aloha Vulnerable Time

- Station 1's frame suffers no collision
  - If no-one sends t_{fr} seconds before
  - AND
  - If no-one sends t_{fr} seconds after beginning of transmission time
- **Vulnerable time is $2t_{fr}$**



Aloha Backoff

- If two Aloha stations discover a collision
  - They should not both resend the frame immediately
    - Because that creates another collision for sure
  - Classic Aloha:
    - Both stations wait a random time, the **back-off time**
- Improved Aloha:
  - If a maximum number of trials has not succeeded, give up (and try a few seconds later)
  - If there is a collision, use a back-off time calculated from the number *k* of tries
  - Back-off time is typically a random integer *r* times 2^k-1

Exercises

- Stations on a wireless Aloha network are a maximum of 372 miles apart. Assume that speed of light is 3×10^8 m/s. What is the maximum delay?
- Assume that the channel has a 200kbps bandwidth and frames are 200b long, what is the time to transmit a frame?
- What is the vulnerable time under Aloha?

Answer

- 372 miles is approximately 600 km
- Signal propagation:
  - $\text{speed} = \dfrac{\text{distance}}{\text{time}} \Rightarrow \text{time} = \dfrac{\text{distance}}{\text{speed}}$
- Maximum delay is
  - $t_{\text{delay}} = \dfrac{600}{3000000} \dfrac{\text{km}}{\dfrac{\text{km}}{\text{sec}}} = 2 \times 10^{-3} \text{sec} = 2 \text{msec}$

Answer

- Time to place frame on ether:
  - $\frac{200\text{b}}{200 \times 10^3\text{bps}} = 10^{-3}\text{sec} = 1\text{msec}$

Answer

- Transmission time is the delay plus the frame time
  - 3 msec

Answer

- Vulnerable time under Aloha is twice that:
  - 6 msec

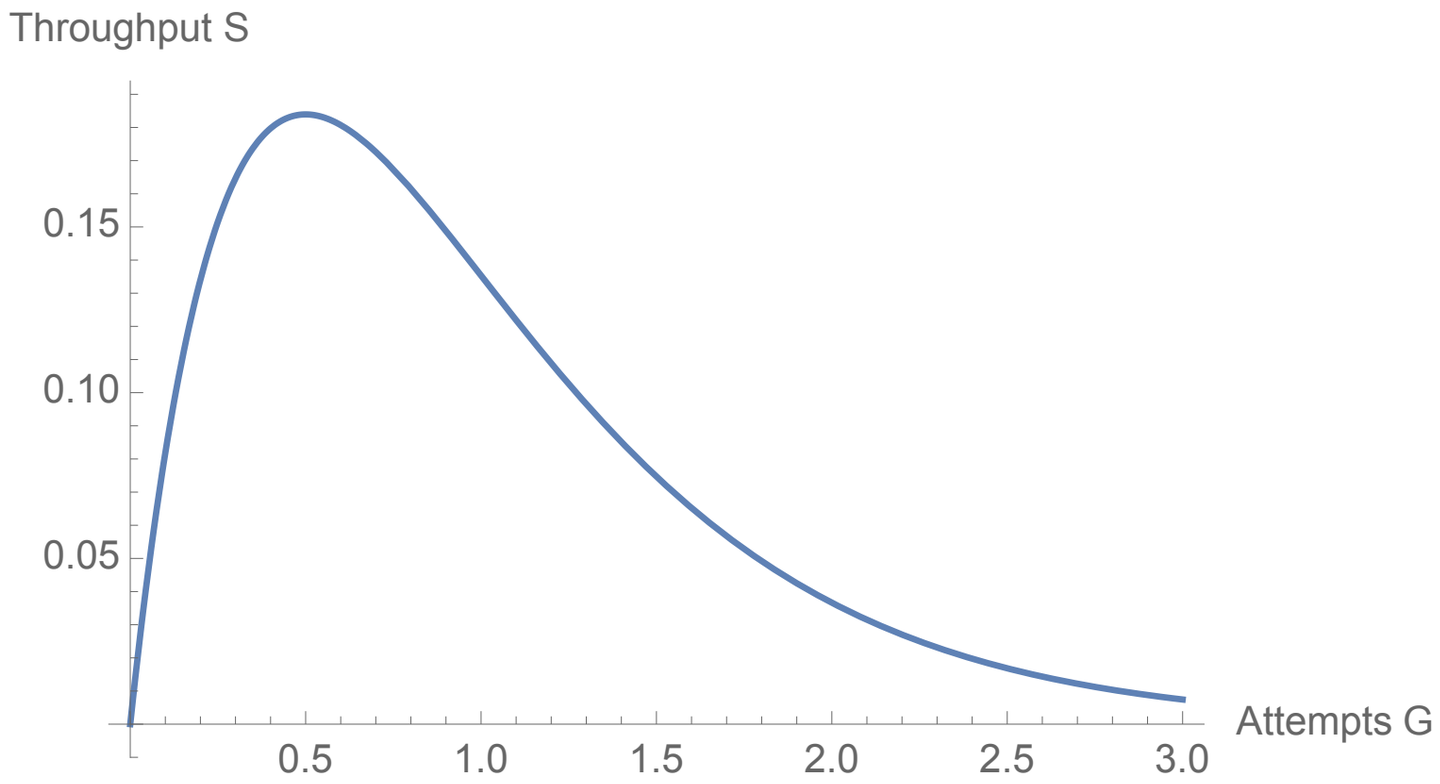
Aloha Performance

- Assume that there are *G* frames per frame time generated in an Aloha system (with many different stations)
- Assume that the probability of sending a packet during a frame time is independent of previous history.
  - This means Poisson distribution
- Probability of *k* frames during frame time is

$$\text{Prob}(k) = \frac{G^k e^{-G}}{k!}$$

- Frame goes through with probability e^{-2G}
- Throughput is $S = Ge^{-2G}$

Aloha Throughput

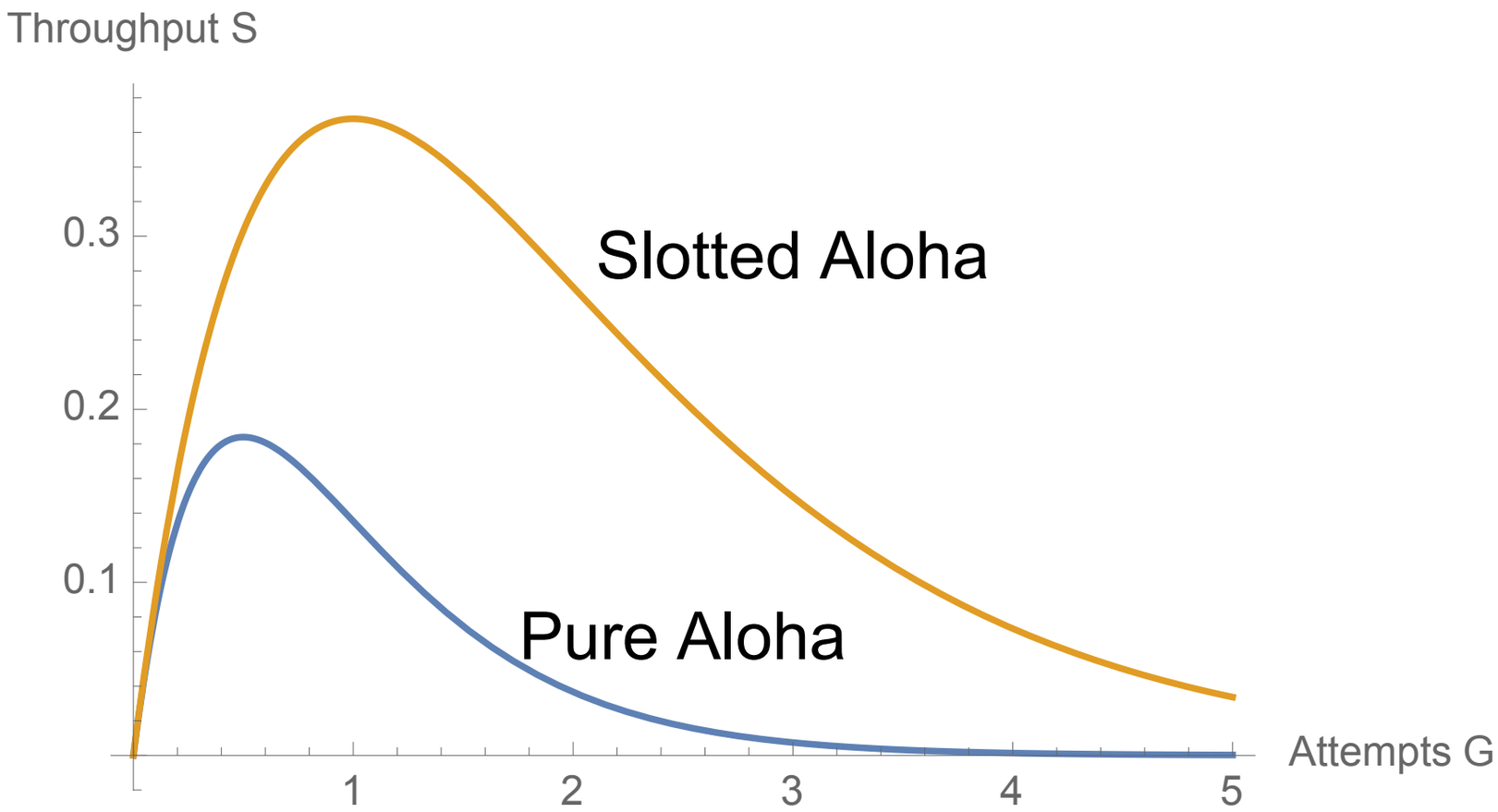


- Maximum Throughput 1/2e = 0.184 at G=1/2

Slotted Aloha

- Roberts (1972) improves Aloha by:
  - Frames are initiated only at the beginning of slots of length frame time
  - Vulnerability period is now only the frame time
  - Same calculation yields throughput is $S = Ge^{-G}$

Slotted Aloha

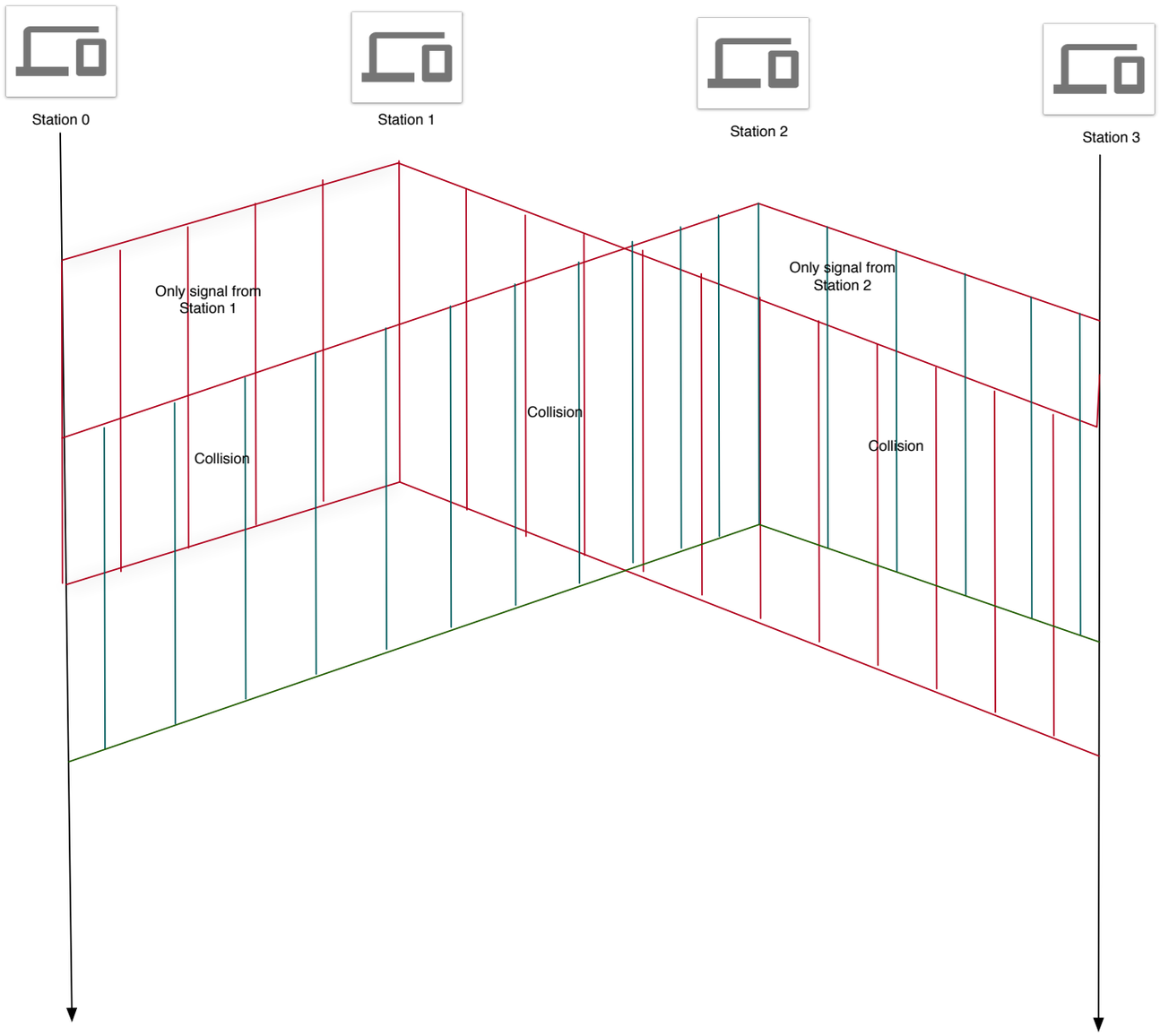


- Maximum throughput is 0.368 at G =1.
- Probability of empty slot is 37%, of slot with one frame is 37% and of slot with collision is 26%.

Carrier Sense Multiple Access

- We can reduce the number of collisions by
  - Checking whether the medium is busy before sending
  - Extension: Back-off if we detect a competing frame
    - Difficult because power of sent and received signal differs by order of magnitude in wireless communication
- Does not avoid all collisions because of non-zero propagation delay

Carrier Sense Multiple Access



Station 1 senses no frame and starts sending to Station 3

Station 2 senses no frame and starts sending to Station 2

Collision detectable at Station 0 when frame from Station 2 arrives

Collision detectable at Station 3 when frame from Station 1 arrives

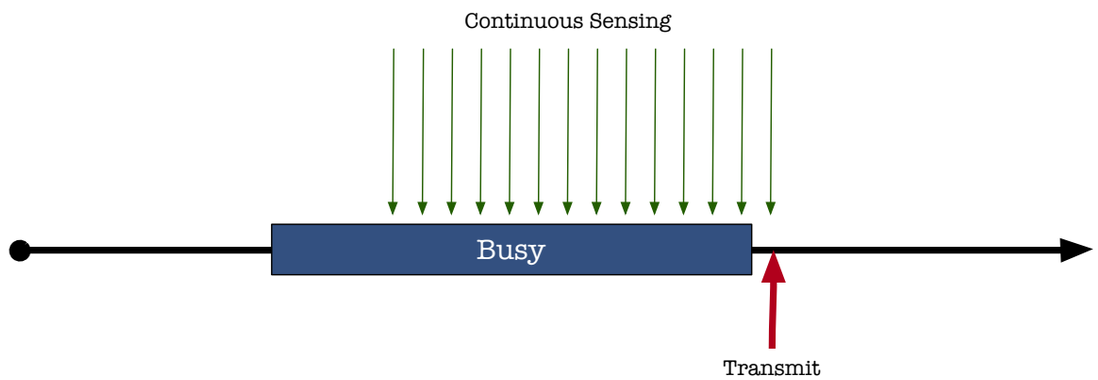
Vulnerable time is the ***propagation delay***

CSMA Persistence

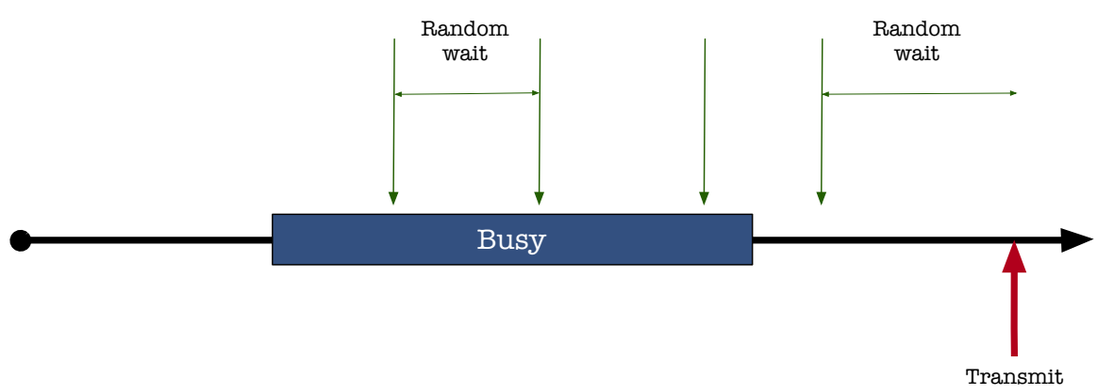
- Persistence describes what a station should do when a channel is idle
  - 1-Persistent:
    - When station finds channel idle, always sends a frame
      - Has lowest delay, but also highest chances of collision
  - Non-persistent:
    - When line is not idle:
      - Wait a random amount of time and then check line again
        - Often does not use medium if there are frames to send
  - *p*-Persistent:
    - Time is divided into slots
    - Station checks line only at the beginning of slot times
    - If slot is free, send frame with probability *p*
    - Otherwise, check again at the next slot time

CSMA Persistence

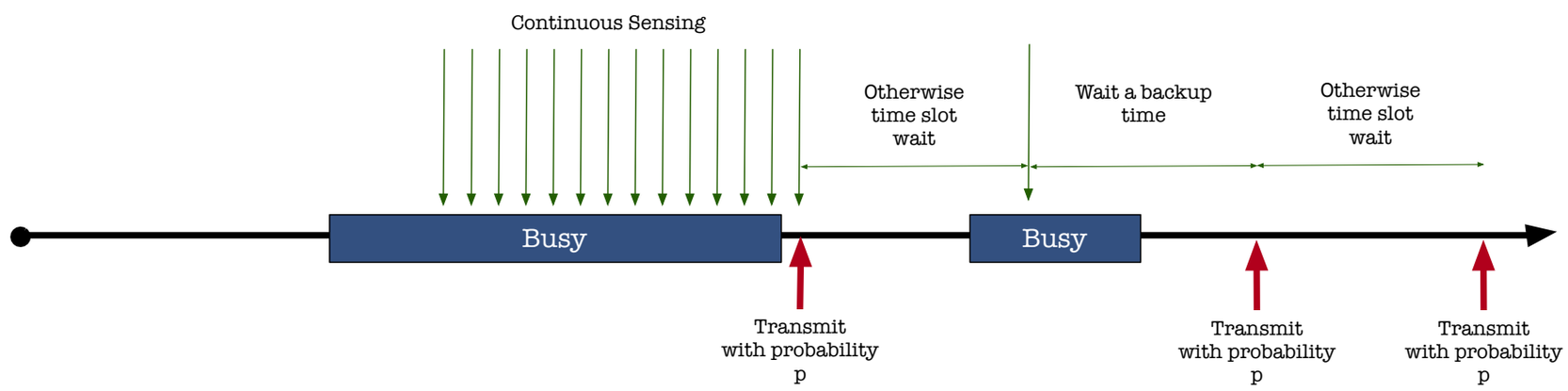
1 Persistent



Non-Persistent



***p*-Persistent**

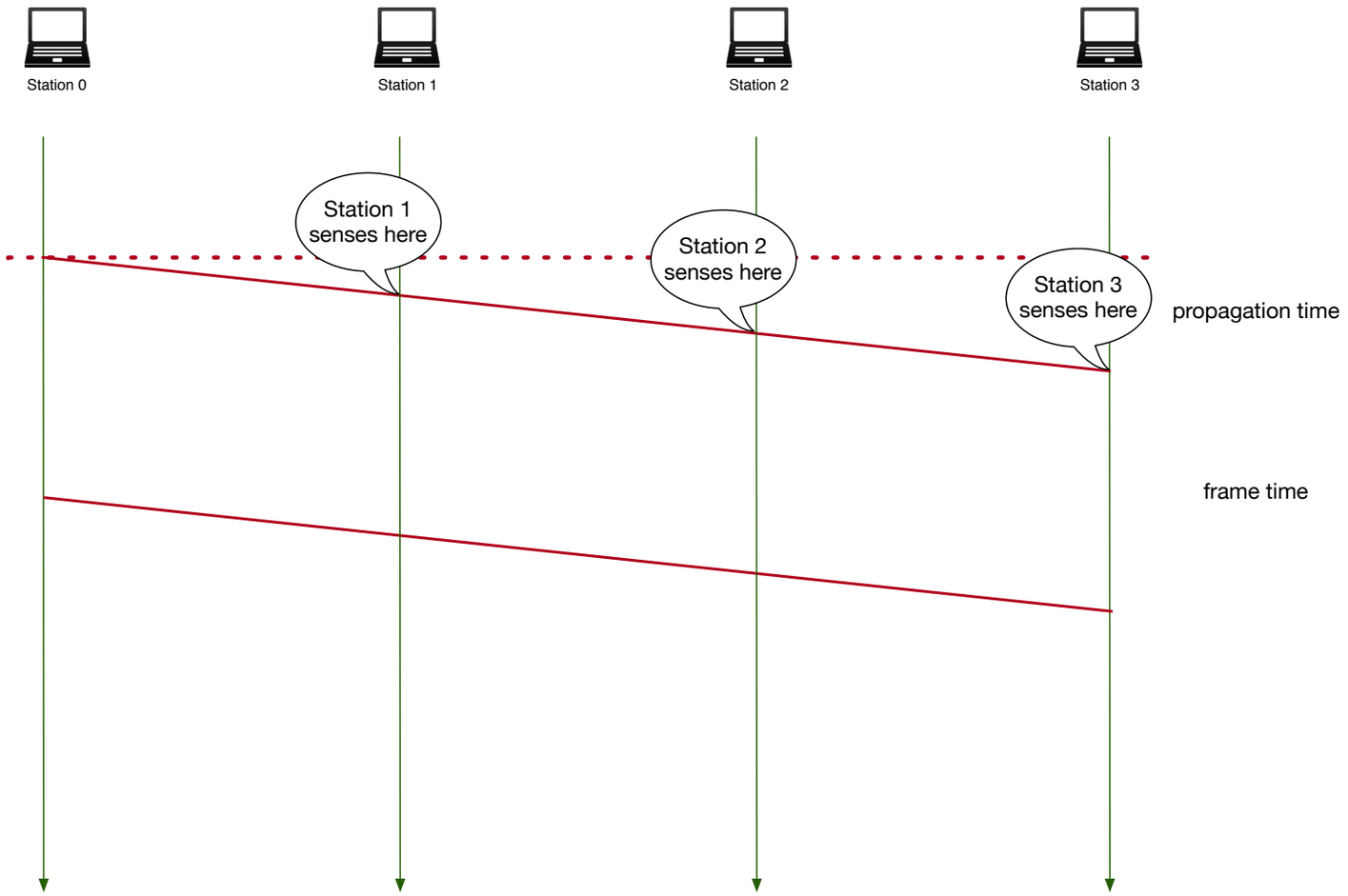


CSMA with collision detection

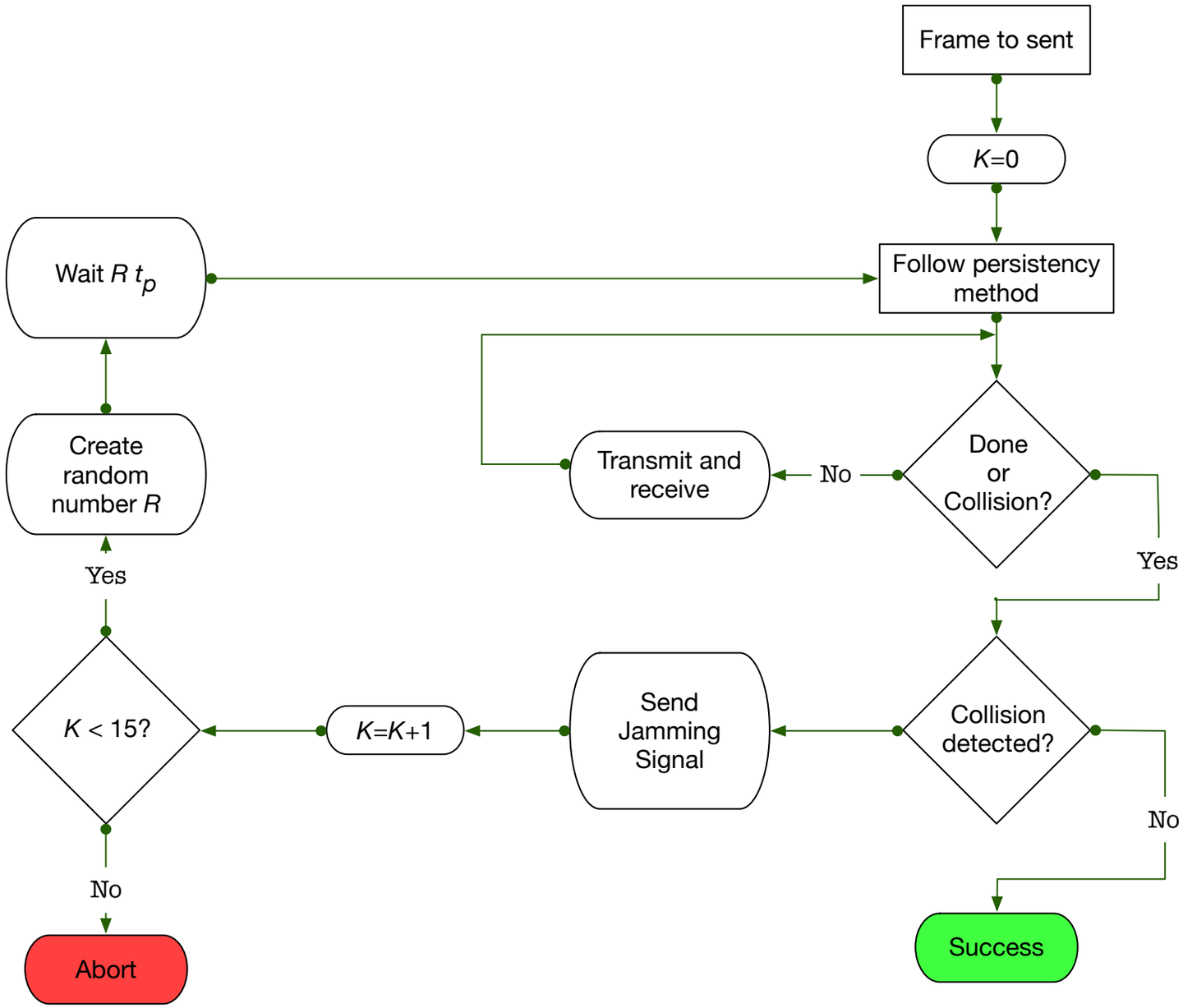
- Stations monitor for collisions
  - When a collision is detected,
    - station stops transmitting
    - creates jamming signal so that everyone knows that there is a collision
    - retries later
      - Using *p*-persistency

CSMA CD

- Stations do not retain frames and cannot resend
- All collisions need to be detected by sending stations
- Need to insist on minimum frame length



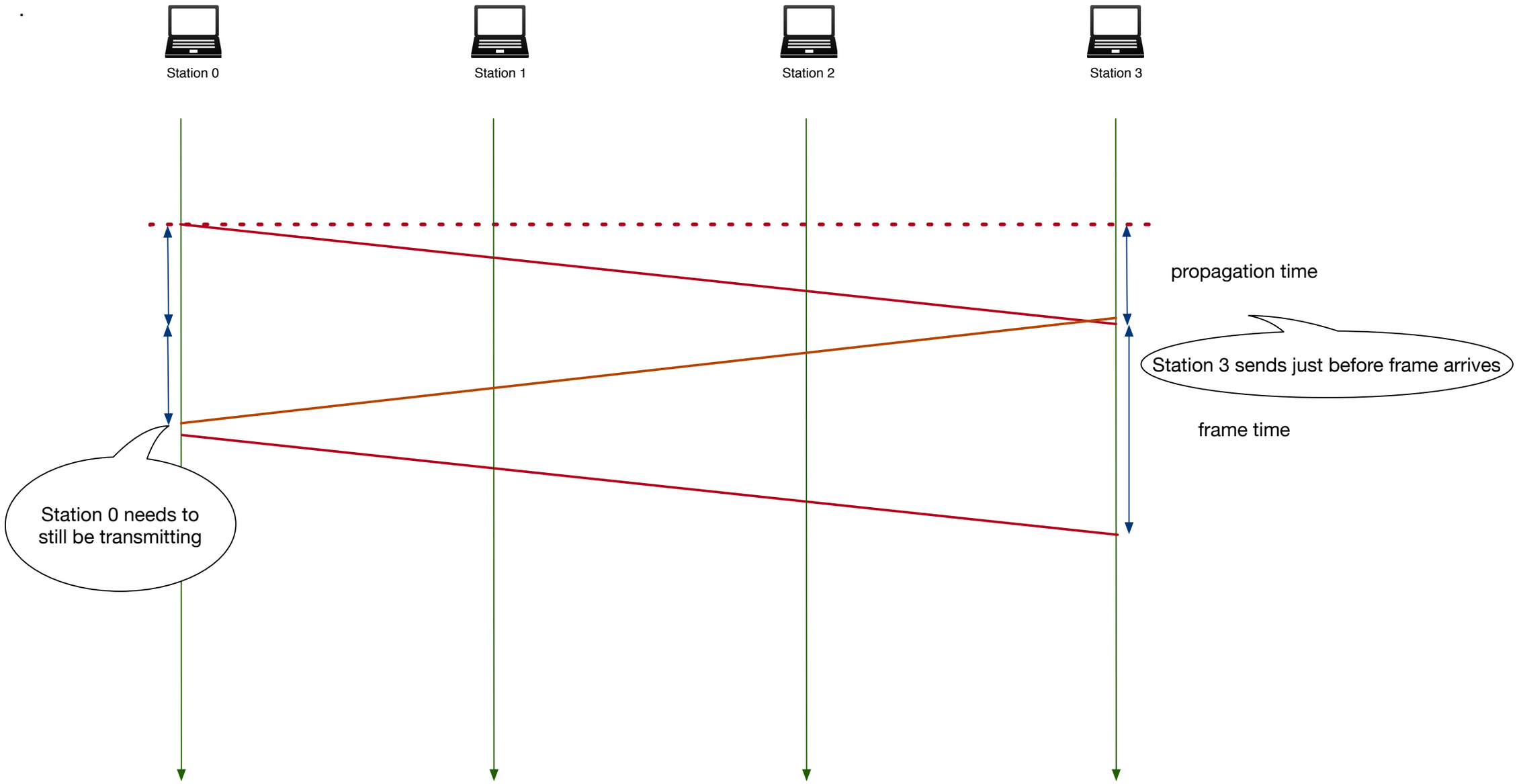
CSMA / CD


Frame to sent
K=0
Follow persistency method
Wait R t_p
Create random number R
Transmit and receive
No
Done or Collision?
Yes
Yes
K < 15?
K=K+1
Send Jamming Signal
Collision detected?
No
No
Abort
Success

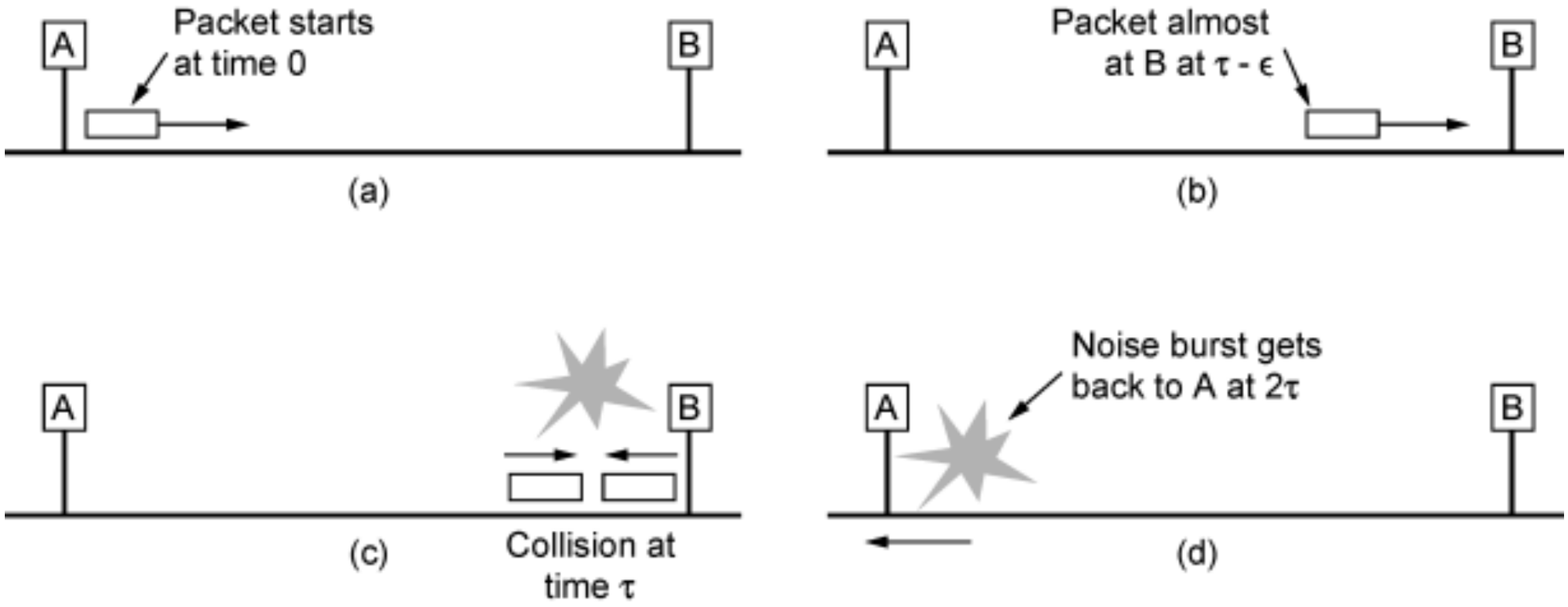
CSMA CD

Collision Detection in Ethernet

CSMA CD


Station 0
Station 1
Station 2
Station 3
propagation time
Station 3 sends just before frame arrives
frame time
Station 0 needs to
still be transmitting

Collision Detection

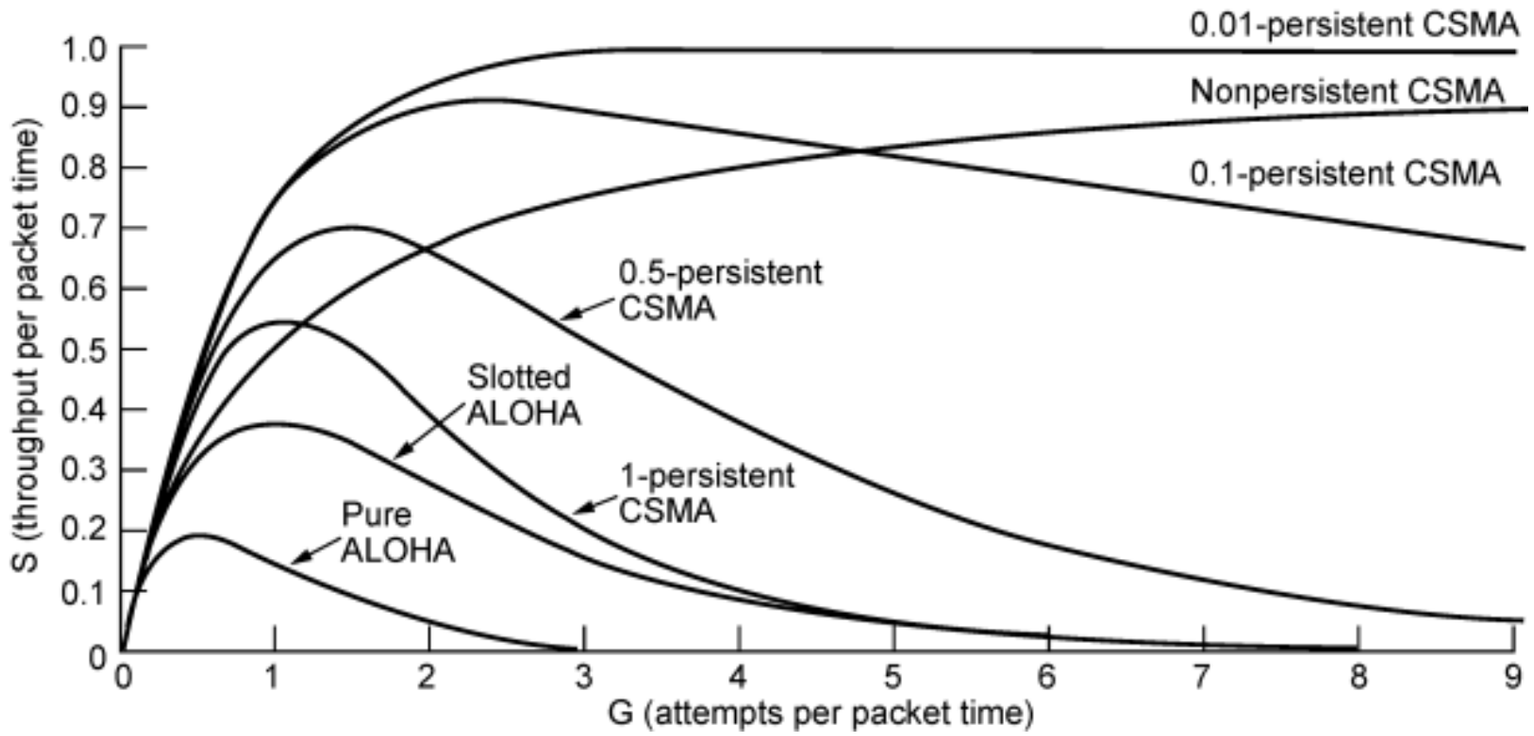


Collision detection can take as long as 2τ

CSMA CD

- Minimal frame length needs to be twice as large in order to detect collisions of frames just sent.

CSMA-CD

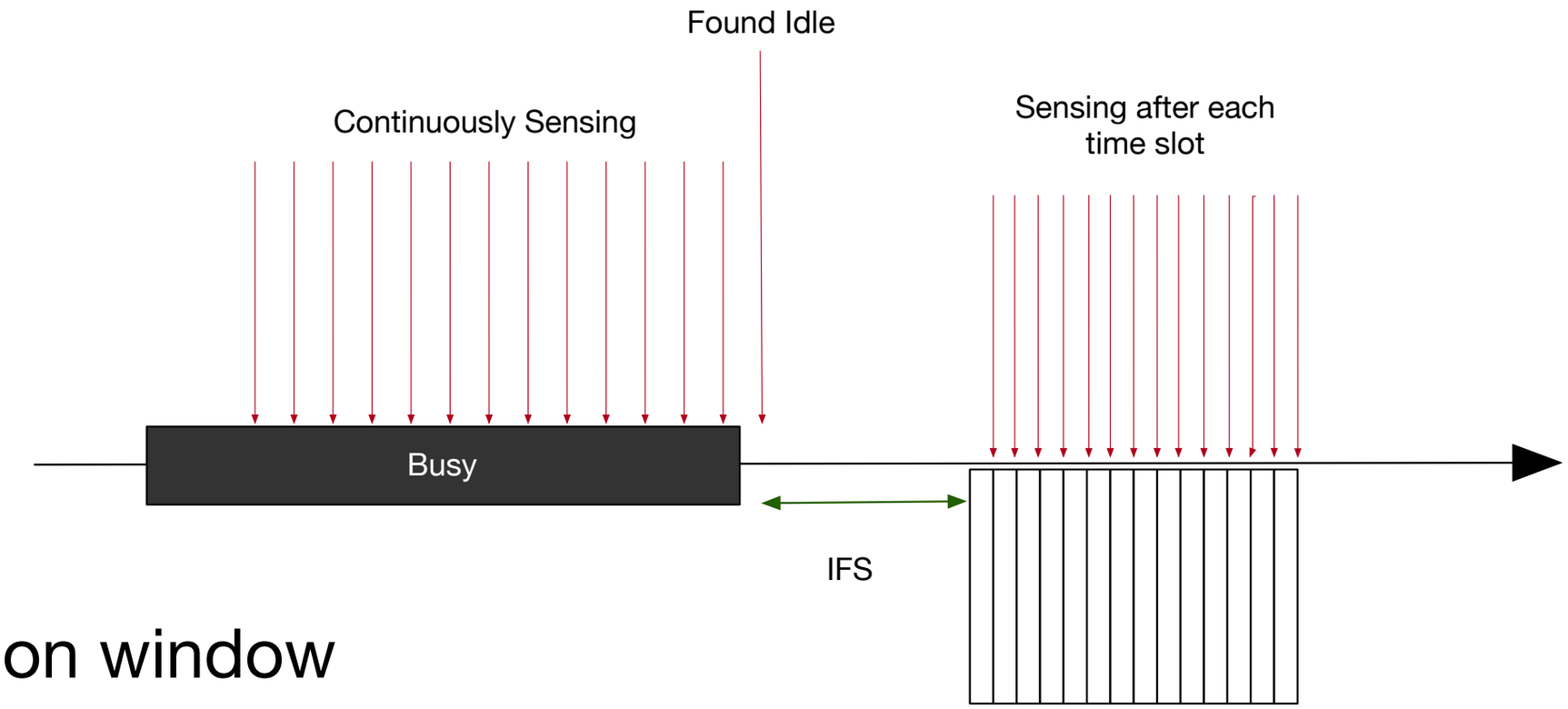


Comparison of the channel utilization versus load for various random access protocols.

CSMA / Collision Avoidance

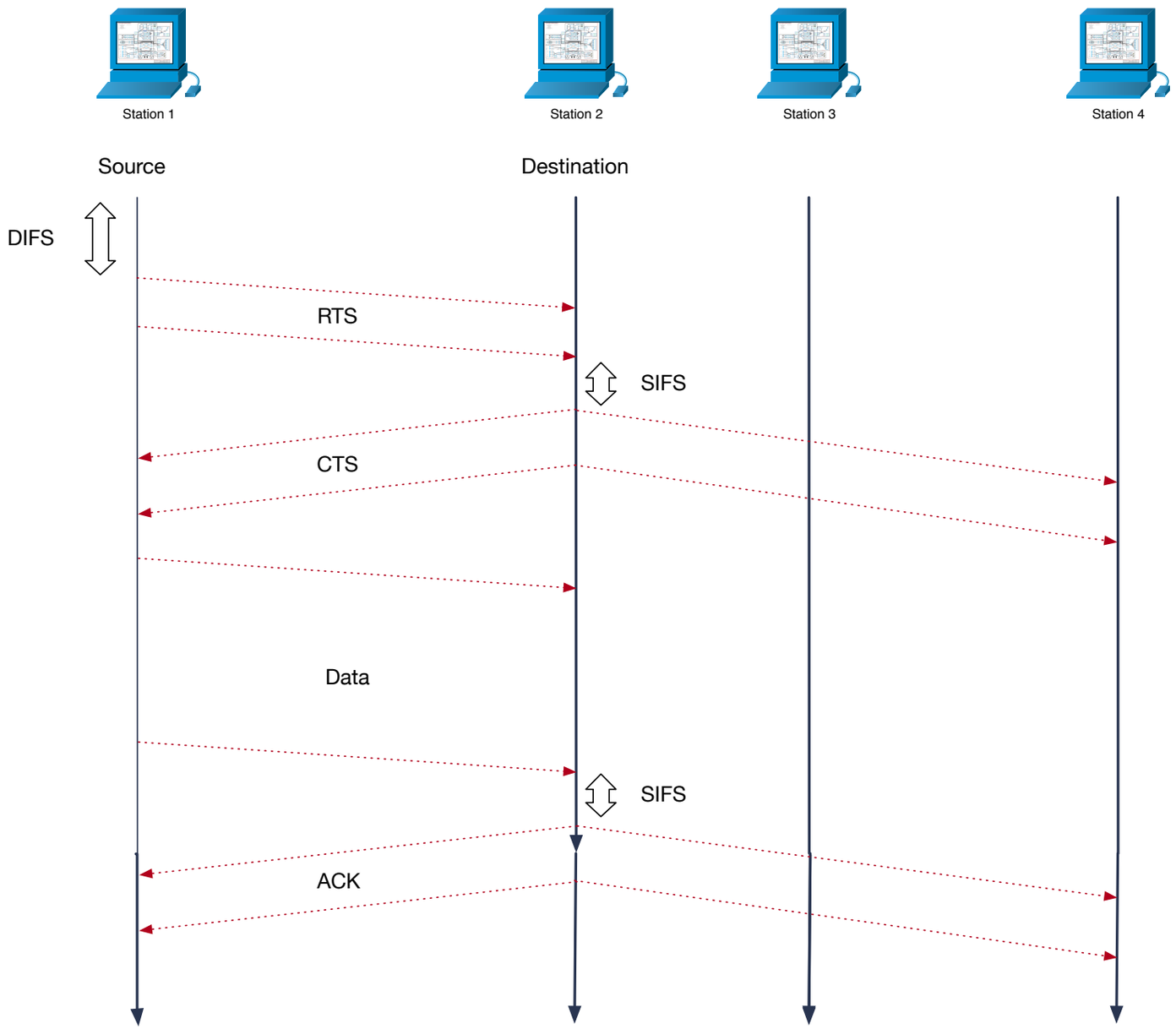
- Invented for wireless networks
  - Three strategies
    1. Inter-Frame Space (IFS)
       - When an idle channel is found, wait for IFS
         - Because a distant station might already have started sending
    2. Contention window
       - Additional time to wait divided into slots
       - Number of slots is power of 2
       - Incremented whenever channel becomes busy
    3. Acknowledgments
       - Use positive acks and time-outs to ensure that frames are received

CSMA / Collision Avoidance



- Contention window
  - Starts out with one slot
  - Number of slots doubled after each failure to require channel

CSMA / CA



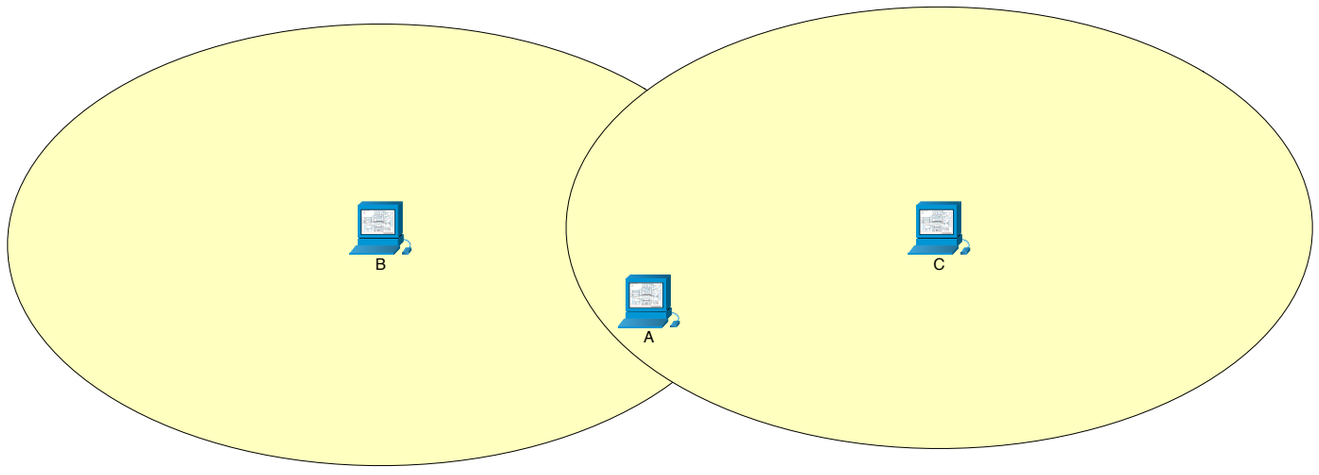
1. Channel idle, then source waits for time DCF Inter Frame Space (DIFS)
2. Sends control frame Request To Send
3. Destination waits for short interframe space (STFS)
4. Sends Clear To Send (CTS) frame
5. Source sends data after waiting STFS
6. Destination waits STFS
7. Sends Ack

CSMA / CA

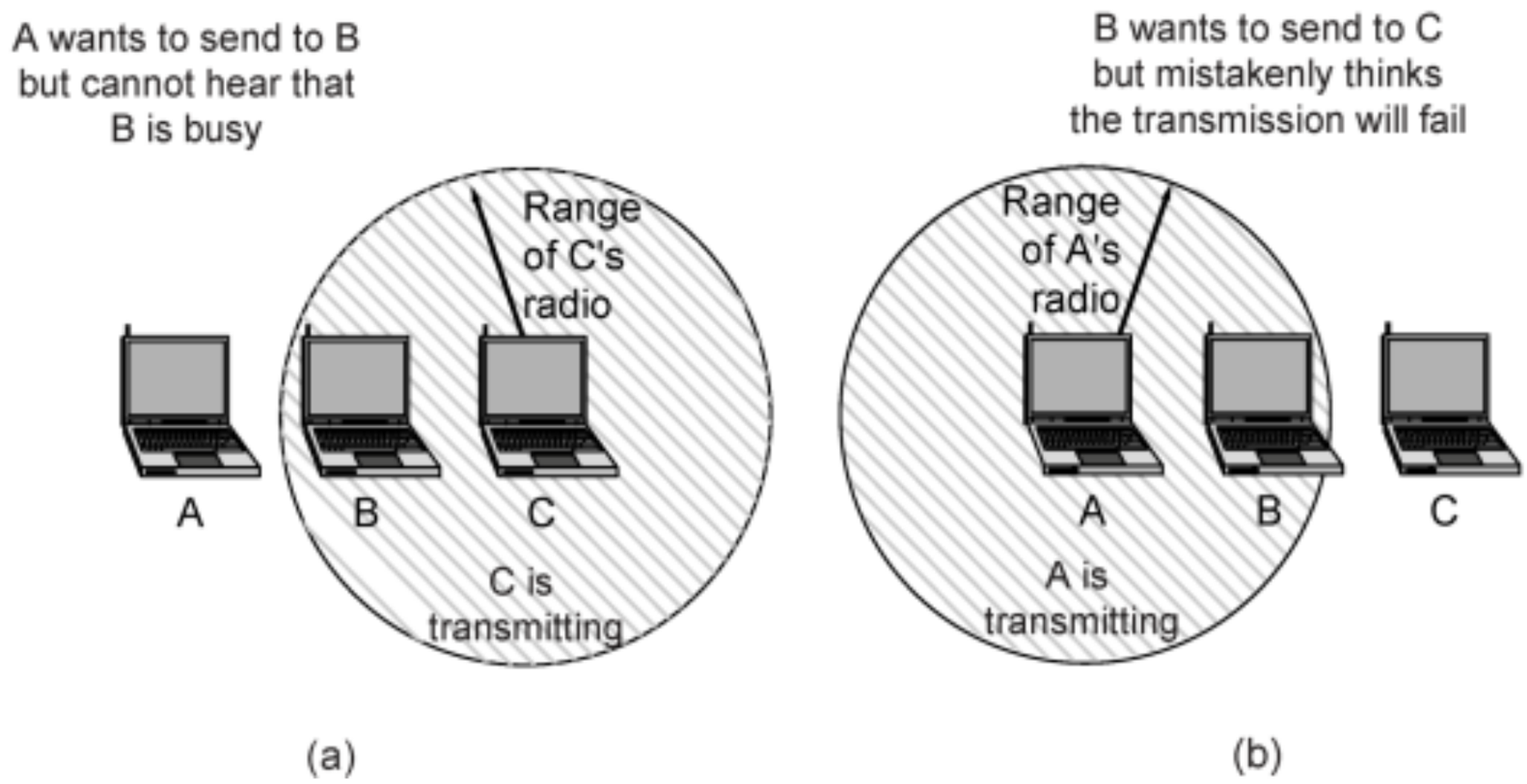
- How to avoid collisions?
  - When a station sends an RTS, it includes duration of time needed to send
    - All other stations create an entry in the **Network Allocation Vector**
      - Do not check for channel idle until all times are down
- Collisions are possible during exchange of RTS and CTS
  - Sender backs off if it does not receive an CTS

CSMA / CA

- Hidden station problem
  - Station B can disrupt traffic sent by Station C to Station A
  - even though Station C cannot see Station B

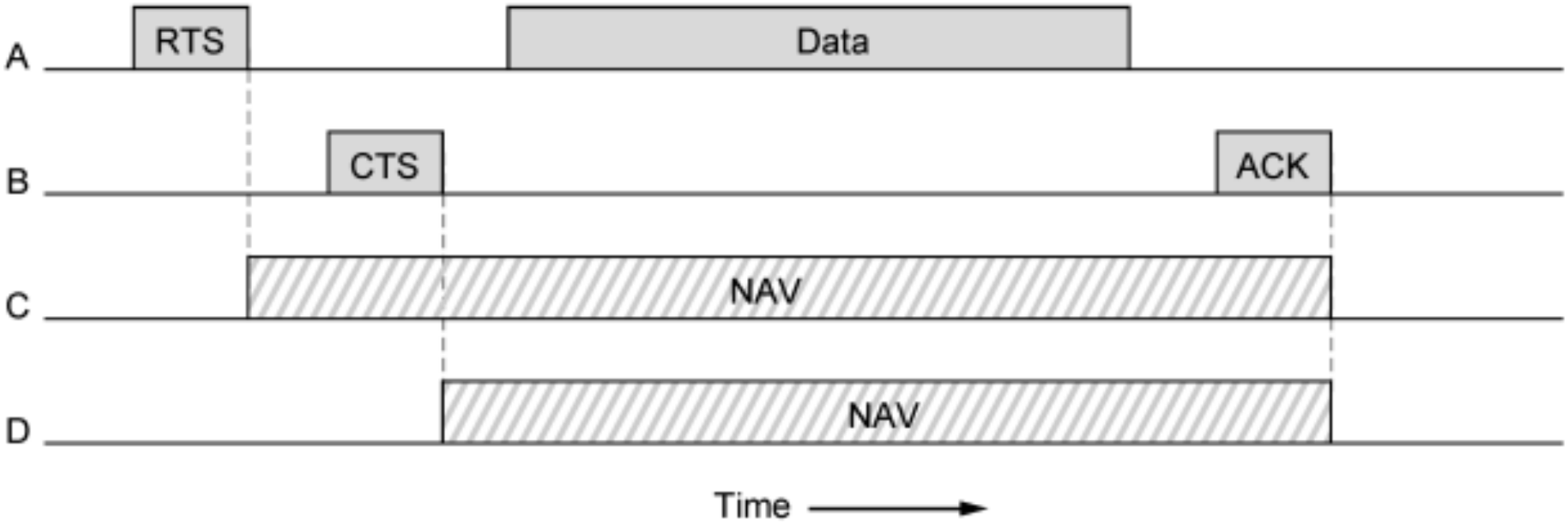


CSMA / CA



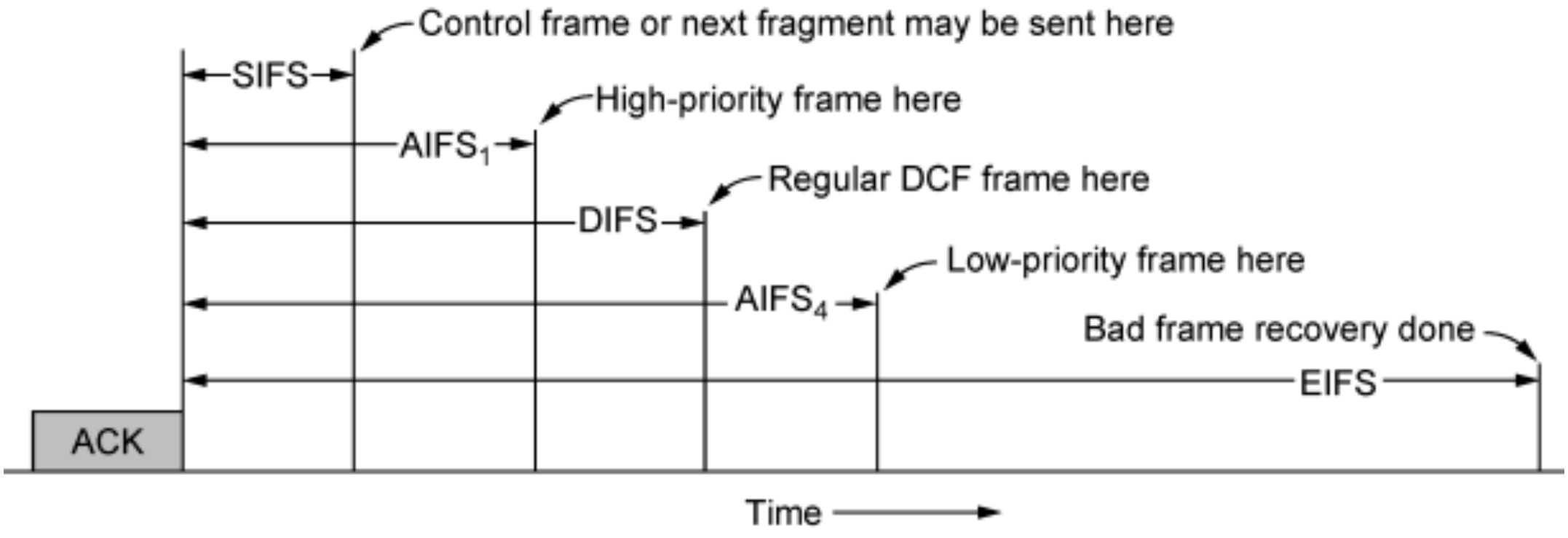
(a) The hidden terminal problem. (b) The exposed terminal problem.

CSMA - CA



Virtual channel sensing using CSMA/CA.

802-11



Interframe spacing in 802.11.

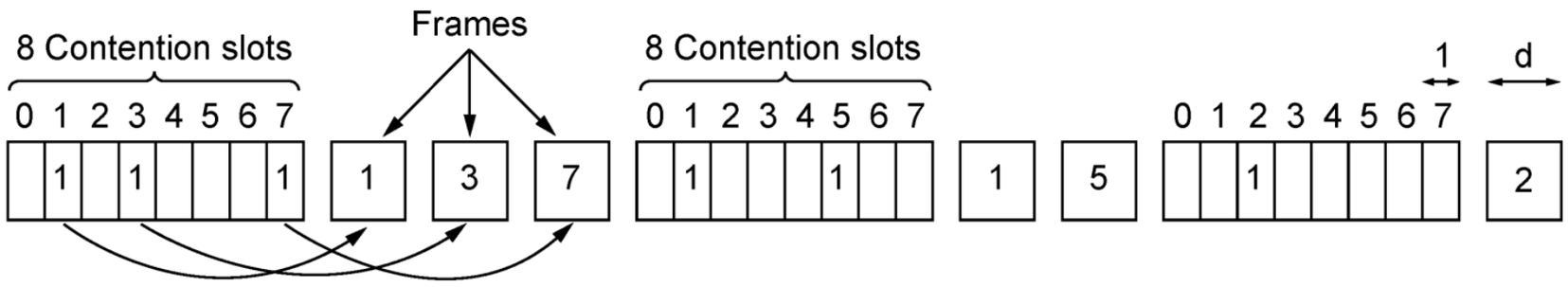
Collision Free Protocols

- Not currently used
- Idea:
  - Stations reserve the right to send during a slot

Basic Bit-Map Protocol

- All *n* stations on the cable are given a number
- A contention frame is sent at the beginning of a period
  - Consists of *n* slots
  - Station *i* with a frame to send inserts a 1 into its slot
  - After contention frames have been received by all stations, every station knows who wants to send a data frame
  - The data frames are then send in order

Basic Bit-Map Protocol

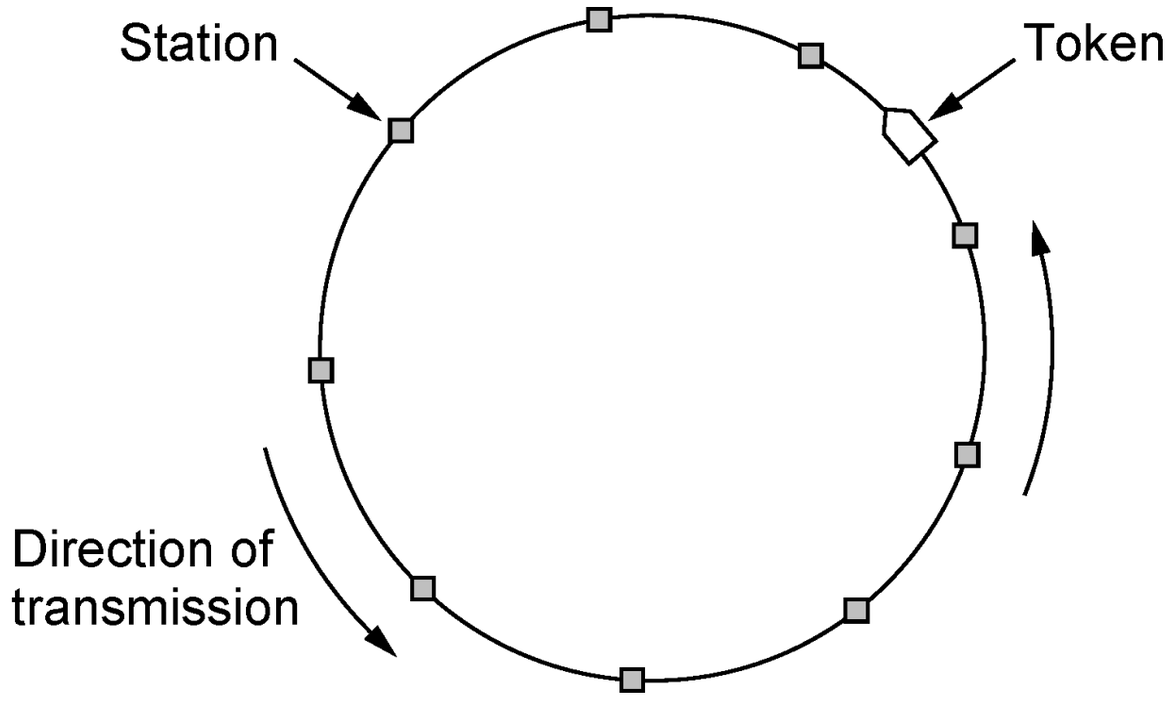


The basic bit-map protocol.

Token Ring Protocol

- Stations organized in a logical ring
- Token circulates through the ring
    - If a station receives a token
        - If it wants to send a frame, the frame is being sent, then token passed on
        - If there is no frame to send, token is passed on

Token Ring

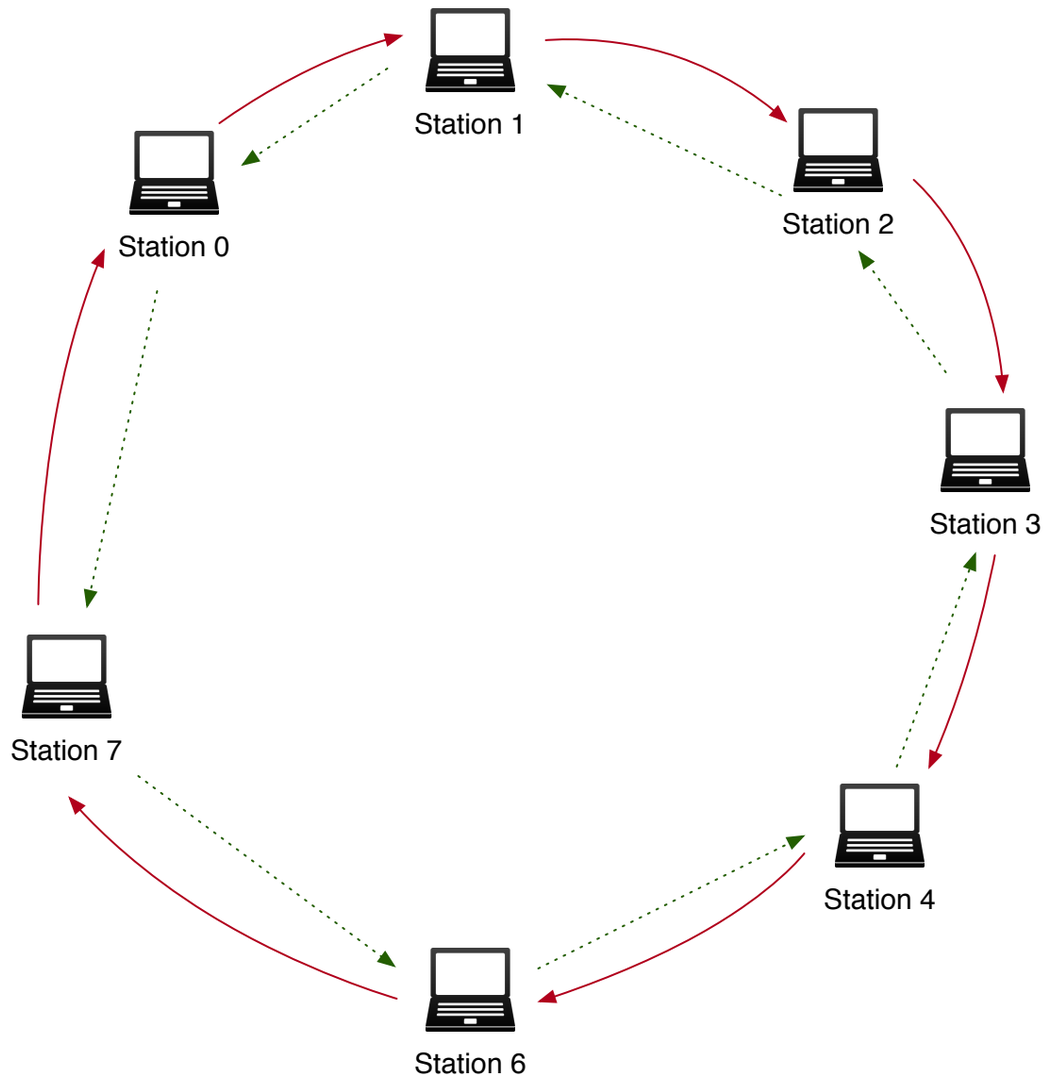


Token ring.

Token Ring

- Dual Ring Topology
  - Physical ring topology
  - Dual ring topology in reverse order
    - Each station needs to have two transmitter ports and two receiver ports
  - If one link fails, there is still a ring left
- High Speed Token Ring networks that use dual ring topology:
  - FDDI - Fiber Distributed Data Interface
  - CDDI - Copper Distributed Data Interface

Double Ring Topology

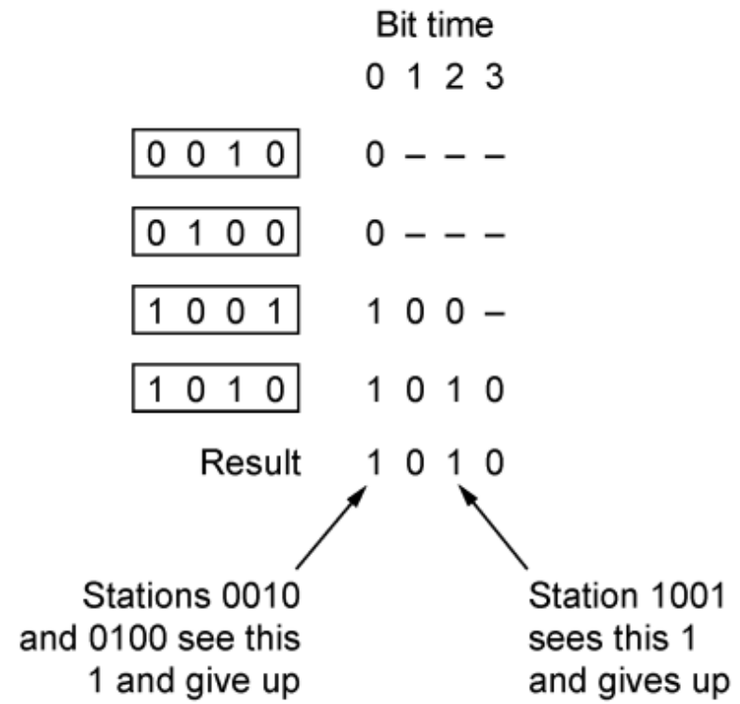


Binary Countdown

- To scale to thousands of stations in a network with little delay, use binary countdown
  - All stations have a unique id
  - Binary number of given length
  - Every station that wants to send a frame, asserts its number during the contention slot
  - The number that everyone sees is the logical-or
  - Stations that see a zero where there number has a bit one drop out of contention

Binary Countdown Example

- Assume that stations 0010, 0100, 1001, and 1010 are competing for the channel
- All assert the first bit
  - 0010 and 0100 drop out
- Nobody asserts the second bit, 1001 and 1010 still stay
- 1010 asserts the third bit and 1001 drops out
- Nobody asserts the last bit, and 1010 is the only contender left.
- 1010 sends its frame



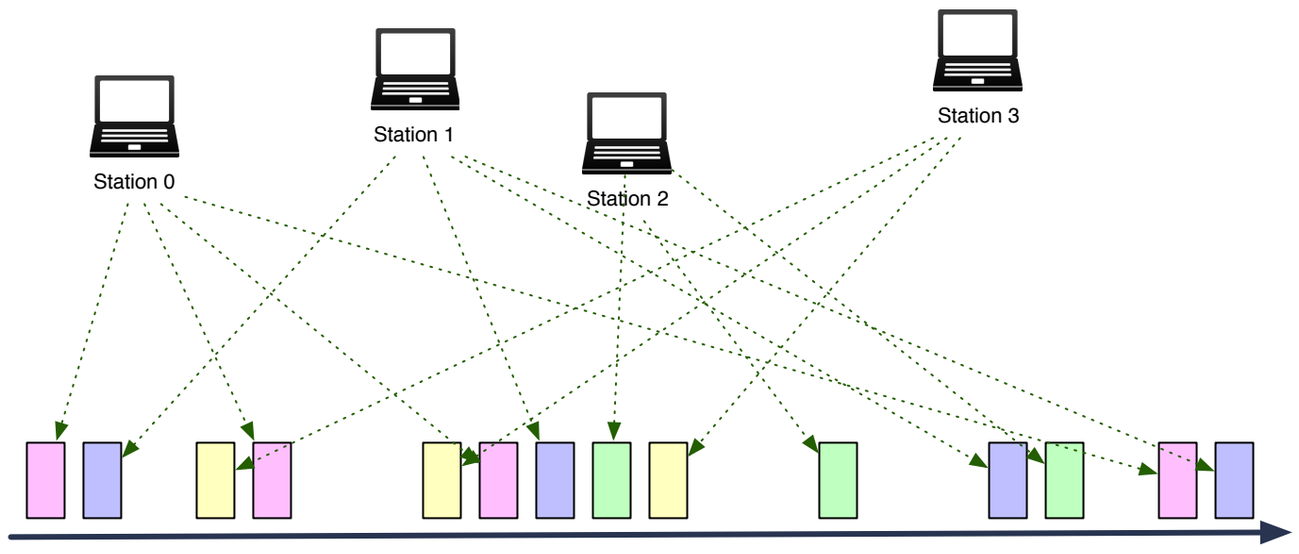
The binary countdown protocol. A dash indicates silence.

Channelization

- Frequency Division Multiple Access (FDMA)
  - Each station is assigned a frequency band
  - Uses a bandpass filter to filter out transmission on other frequencies
  - Receive transmissions from everything else

Channelization

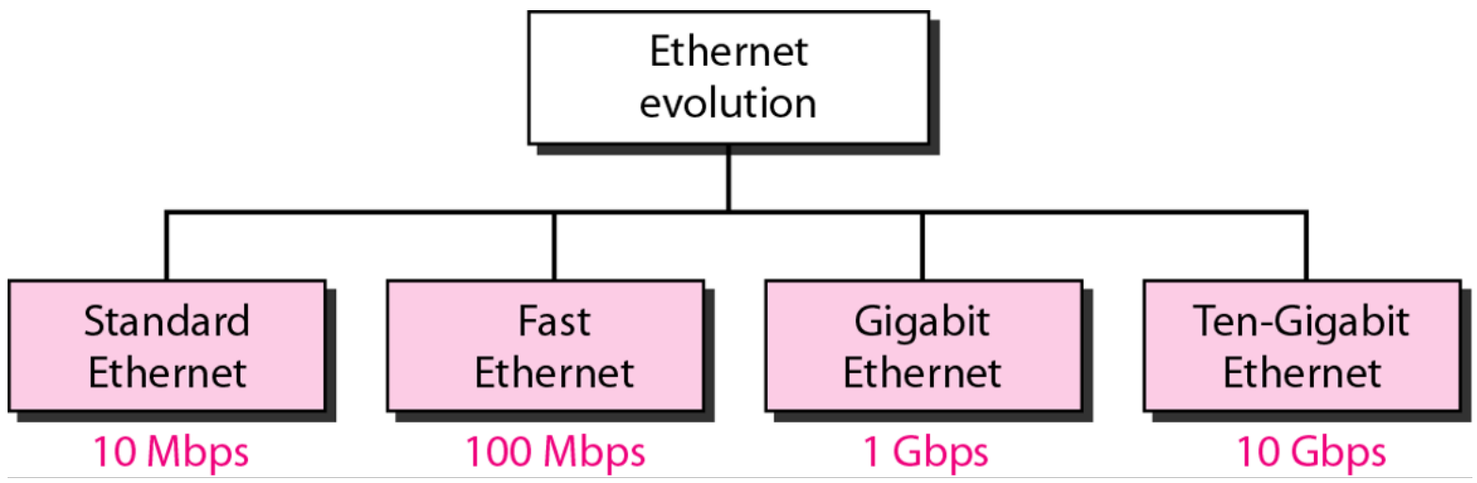
- Time Division Multiple Access
  - Each station is allocated a time slot
  - Because of propagation delays, all time slots are separated by small guard bands



Protocols

Ethernet

- Classic Ethernet
- Switched / Fast Ethernet
- Gigabit Ethernet
- 10 Gigabit Ethernet

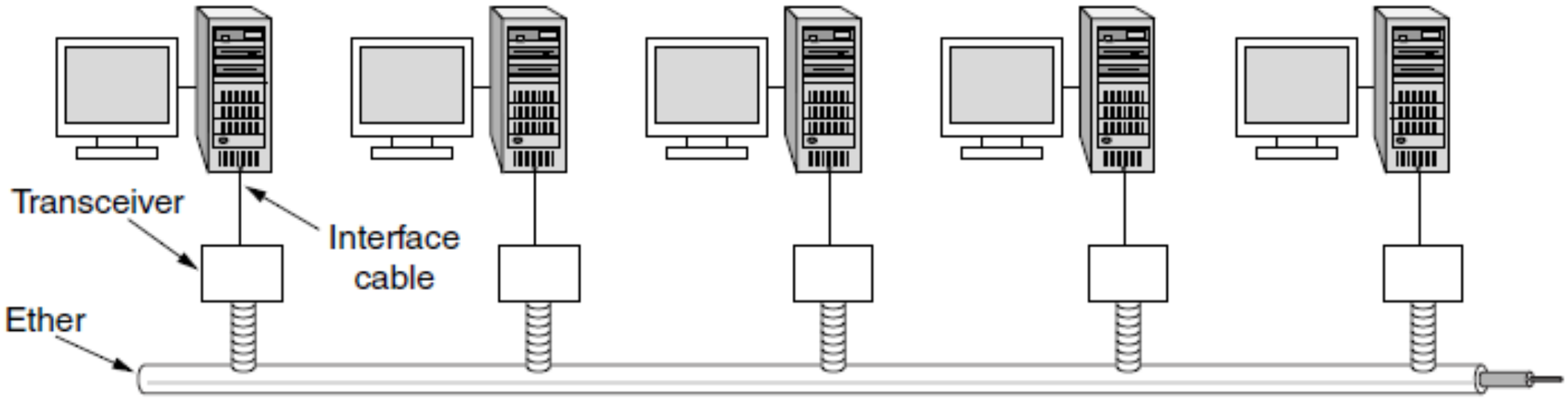


Ethernet

- 1985: IEEE project 802
- Divided into
  - Logical Link Control
    - Framing, flow control, error control
  - Media Access Control

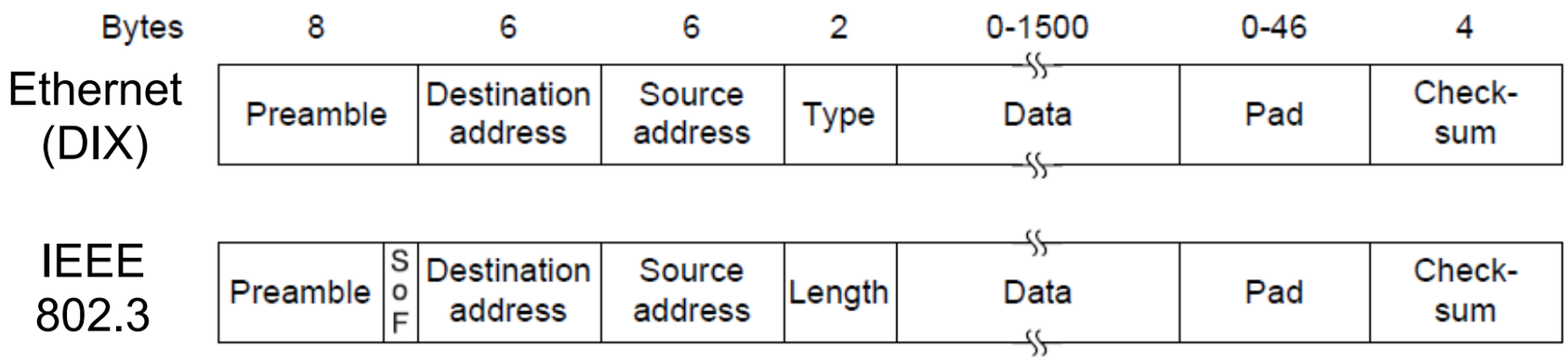
Classic Ethernet Physical Layer

- One shared coaxial cable to which all hosts are attached
  - Up to 10 Mbps with Manchester encoding
  - Hosts ran the classic Ethernet protocol for access



Classic Ethernet MAC

- MAC protocol is 1-persistent CSMA/CD
  - Random delay after collision is computed with Binary Exponential Backoff
- Frame format is still used with modern ethernet



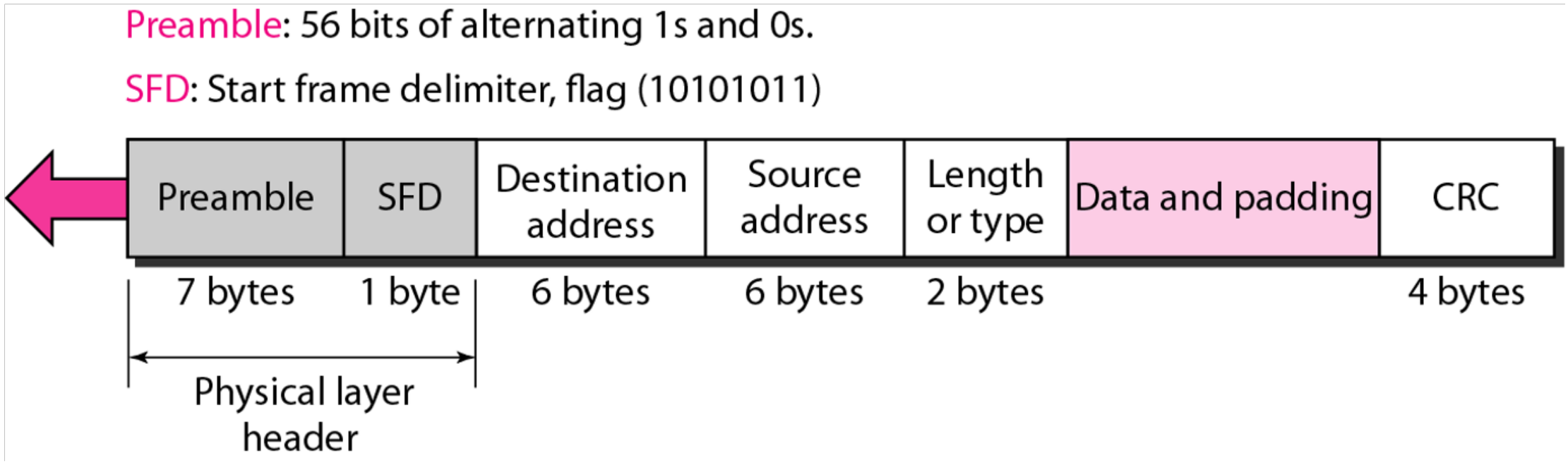
Classic Ethernet Frame Format

- Preamble: 7 bytes of 10101010, 1 byte 10101011 (frame delimiter)
- 6B destination and source address
    - First bit distinguishes between ordinary (0) and group (1) addresses
    - All ones for broadcasting
    - Station addresses are unique
        - First three bytes assigned as Organizationally Unique Identifiers by IEEE
        - Manufacturers assign the last 3 bytes
        - Each station address is programmed into NIC
- Type / Length field of 2B
    - Ethernet uses type to tell receiver what to do with the frame
        - E.g. 0x0800 —> IPv4
    - IEEE 802.3 contains length — which necessitates another header for Logical Link Control
    - Both are used. Types are bigger than 0x600 (=1536), which is bigger than the maximal data length
- <= 1500B data field
- Padding (to make sure that packages are at least 64B long
- 32b CRC checksum

Classic Format

Preamble: 56 bits of alternating 1s and 0s.

SFD: Start frame delimiter, flag (10101011)



Classic Format

- Frame Length:
  - Minimum length needed for correct operation of CSMA/CD
    - 512 bits (64B)
  - Maximum length 1518 B

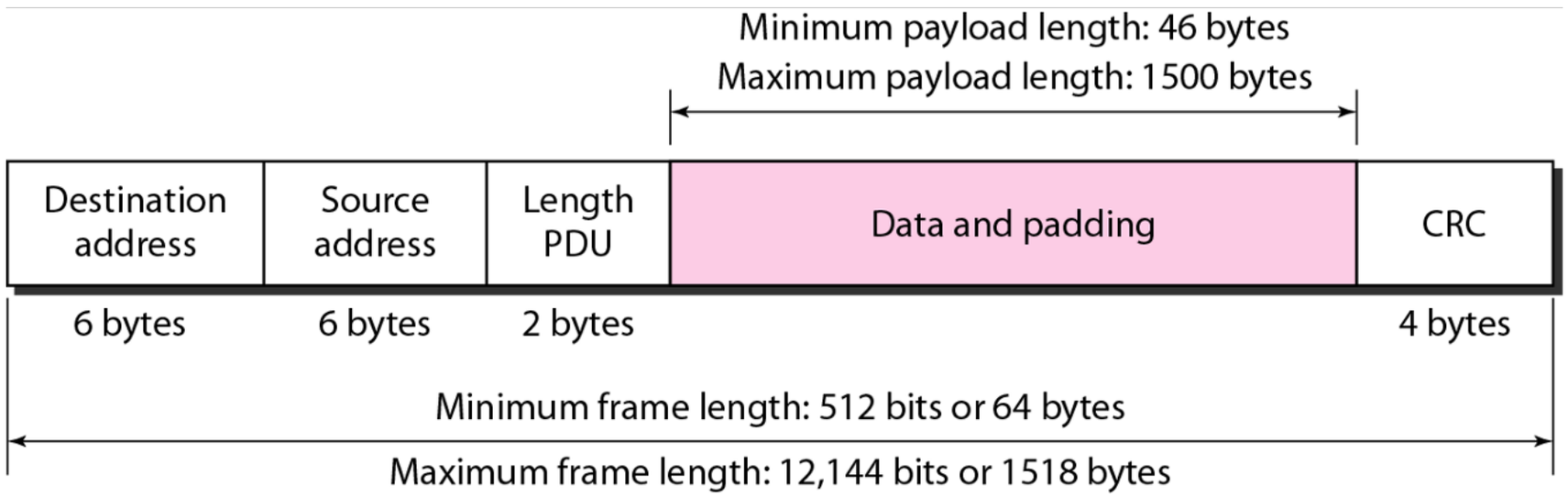
Quiz:

- How much user data does an ethernet frame need?

Answer

- There are 6+6+2+4 B = 18B overhead
- Minimal length is 64B
- Payload needs to have 64B-18B = 46B
- If payload is smaller, need to use padding

Answer


Minimum payload length: 46 bytes
Maximum payload length: 1500 bytes
Destination address
Source address
Length PDU
Data and padding
CRC
6 bytes
6 bytes
2 bytes
4 bytes
Minimum frame length: 512 bits or 64 bytes
Maximum frame length: 12,144 bits or 1518 bytes

Ethernet

- Each ethernet network has its own **Network Interface Card**
  - Provides link-layer address
  - 6 Bytes, written in hexadecimal notation

Ethernet

- Address is sent left to right: Byte for Byte
- Each byte is sent right to left
- Example:

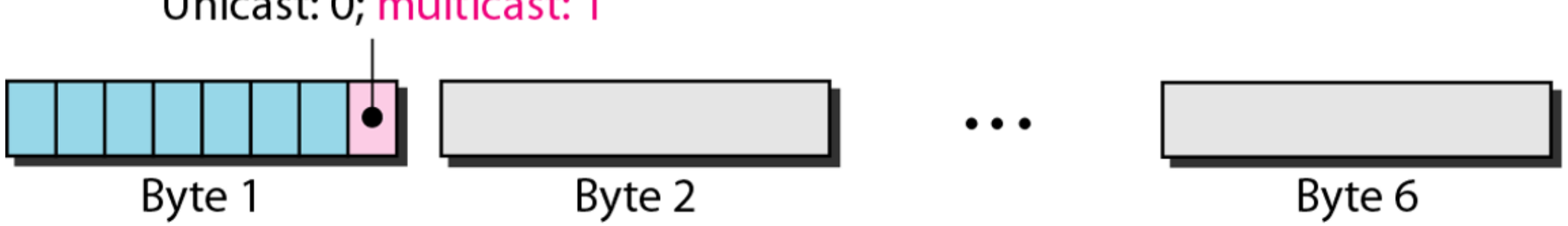
06:01:A3:5C:6B:F3

0000 0110	0000 0001	1010 0011	0101 1100	0100 1011	1111 0011

0110 0000	1000 0000	1100 0101	0011 1010	1101 0010	1100 1111

Ethernet

- One bit distinguishes uni-cast and multi-cast address



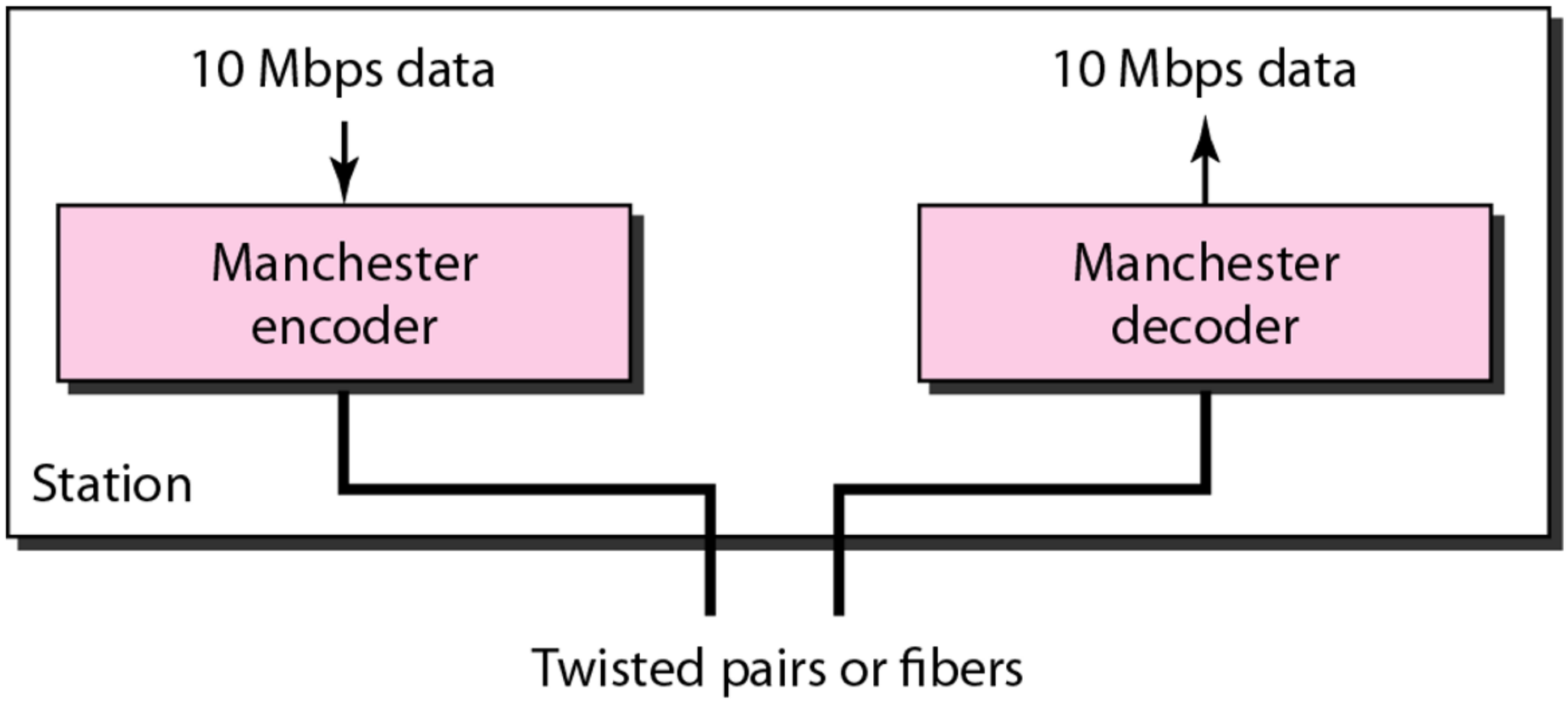
Ethernet

- Quiz:
  - How is 47:20:1B:2E:08:EE sent out?

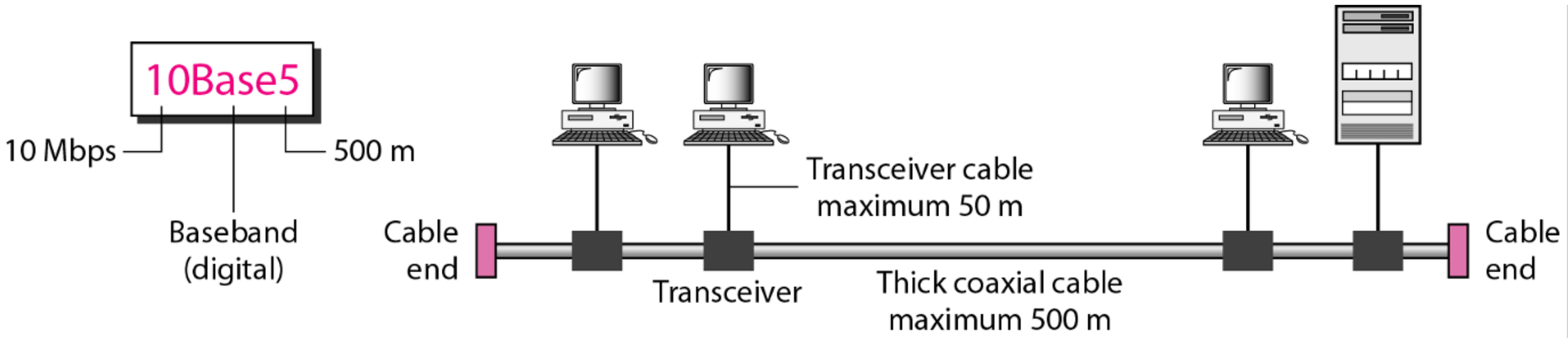
Ethernet

- Answer:

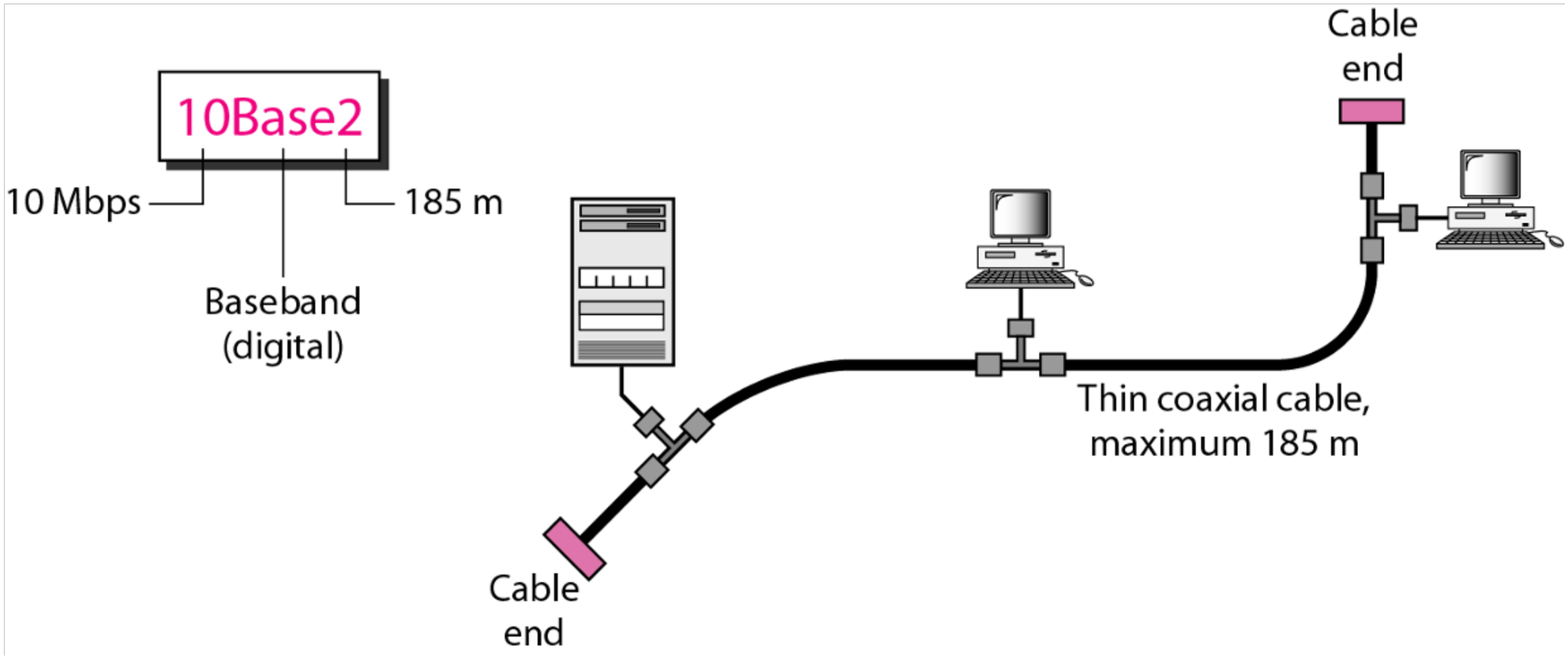
Classic Ethernet Performance



Classic Ethernet Performance



Classic Ethernet Performance



Classic Ethernet Performance

- When we use a common cable, Ethernet uses 1-persistent CSMA/CD
  - Sense the medium when they have a frame to send
  - If medium is free, immediately send
  - Monitor channel for collisions
  - If there is a collision, use a short jam signal
  - Try to resend after a short interval
    - Divide time into slots of length = worst time roundtrip propagation delay

Quiz

- What is the worst time roundtrip delay for a 500 m copper cable?

Answer

- Velocity is distance divided by time, so time equals distance divided by velocity
  - Copper conducts at about 2/3 of speed of light
  - An approximation, see tables of velocity factors
- Single trip: $\frac{500 \text{ m}}{2 \times 10^8 \frac{\text{m}}{\text{sec}}} = 2.5 \times 10^{-6} \text{ sec} = 2.5 \ \mu\text{sec}$
- Round trip: $5 \ \mu\text{sec}$

Classic Ethernet Performance

- Each station randomly selects 0 or 1 slots to wait
- If there is another collision:
  - Select randomly 0, 1, 2, or 3 slots to wait
- After *i* collisions:
  - Select randomly 0, 1, … , $2^i - 1$ slots to wait, with a maximum of 1023 slots
- Exponential back-off

Classic Ethernet Performance

- Rigorous analysis of behavior is difficult
- Assume constant retransmission probability per slot
  - If there are Q stations constantly queued to send packets
  - They try to acquire the ether with probability 1/Q
    - Known to be the optimum decision rule
    - Approximated by load-estimating retransmission control algorithm
- Probability of one station trying to send (and therefore successfully send) is $A = Q \times \frac{1}{Q} \times (1 - \frac{1}{Q})^{Q-1}$

Classic Ethernet Performance

- Probability for sending at slot 0 is A
- Probability for sending at slot 1 is $A(1-A)$
- Probability for sending at slot 2 is $A(1-A)^2$
- …

- Average waiting time is $A + 2A(1-A) + 3A(1-A)^2 + \ldots$
- Mean is $W = (1-A)/A$

Classic Ethernet Performance

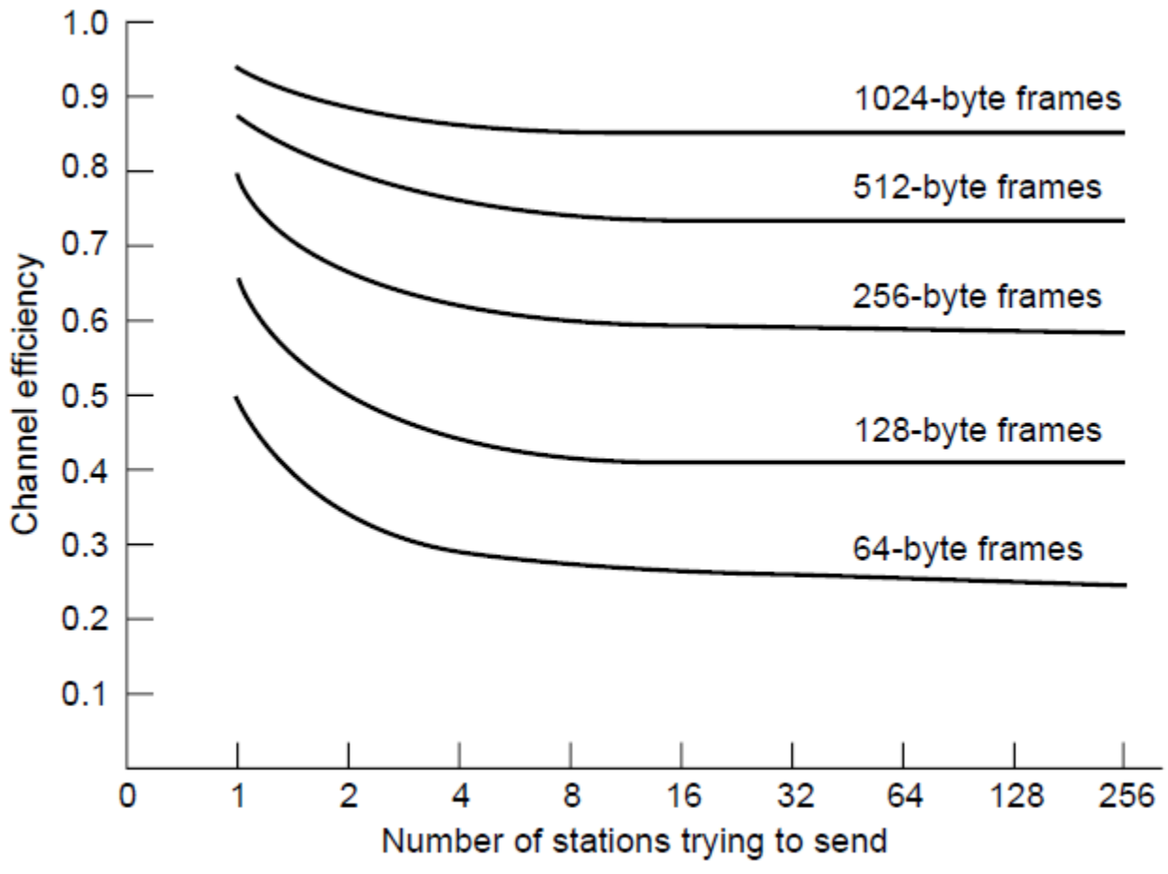
- Efficiency is the time that packages are actually sent over total time
- Packet transmission takes $L = \frac{\text{package size}}{\text{bandwidth}} + \tau$
- Time to acquisition is $M = W \times 2\tau = 2\frac{1-A}{A}\tau$
- Efficiency is $\frac{L}{L+M}$

Classic Ethernet Performance

- A more precise formula for efficiency
  - F Frame length
  - B band width
  - L cable length
  - c propagation speed
  - Assume optimal contention slots:
- Efficiency = $\dfrac{1}{1 + \dfrac{2BLe}{cF}}$

Classic Ethernet Performance

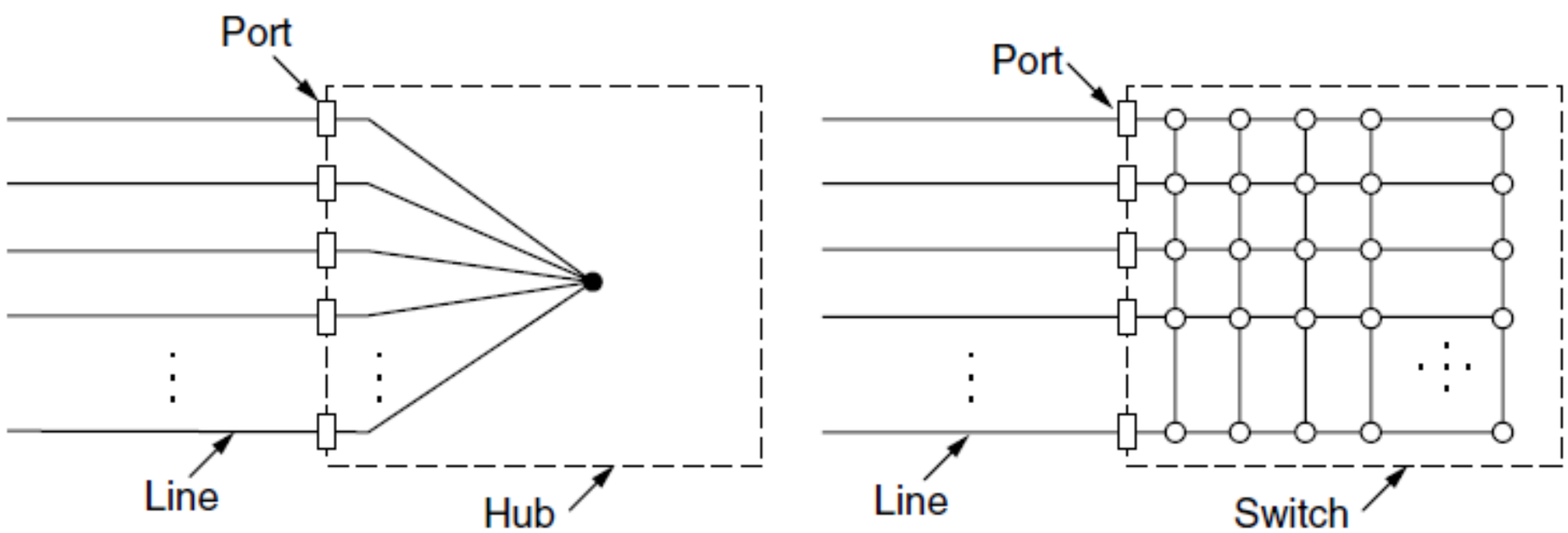
- Efficient for large frames
- Degraded performance for small frames and long LANs



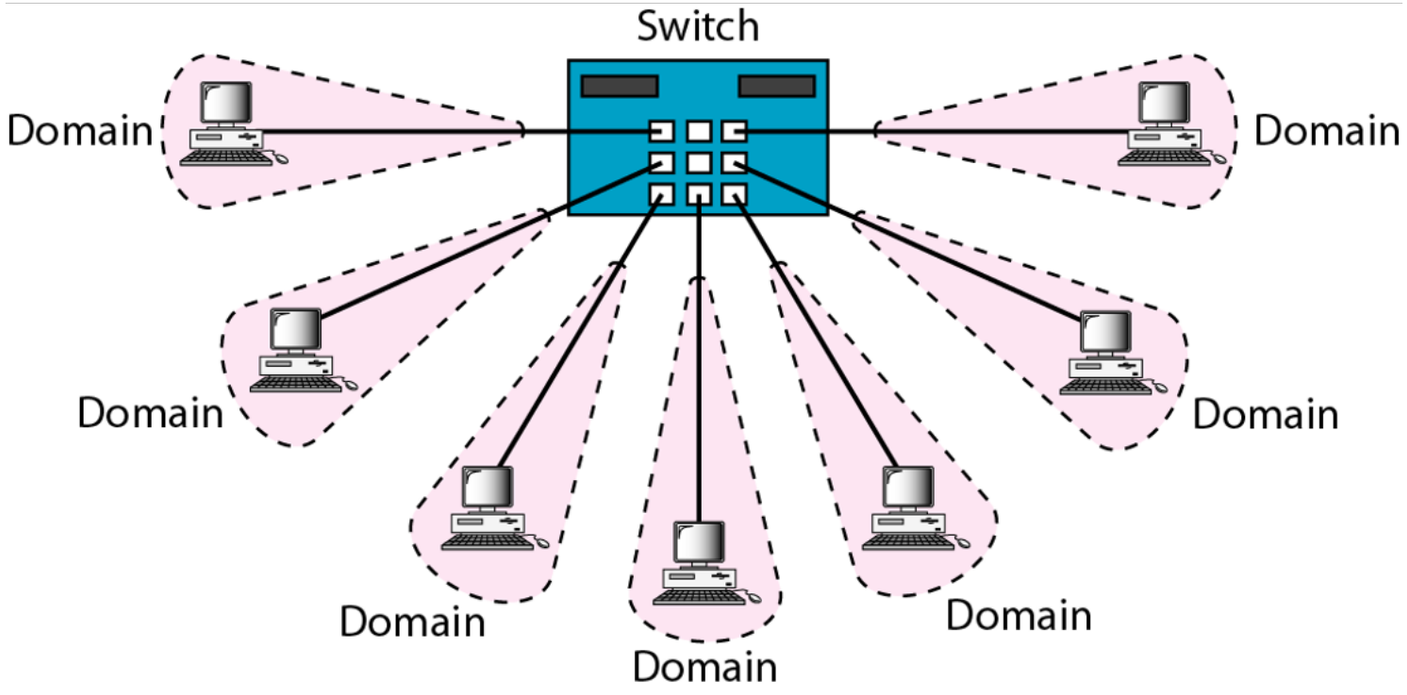
10 Mbps Ethernet,
64 byte min. frame

Switched / Fast Ethernet

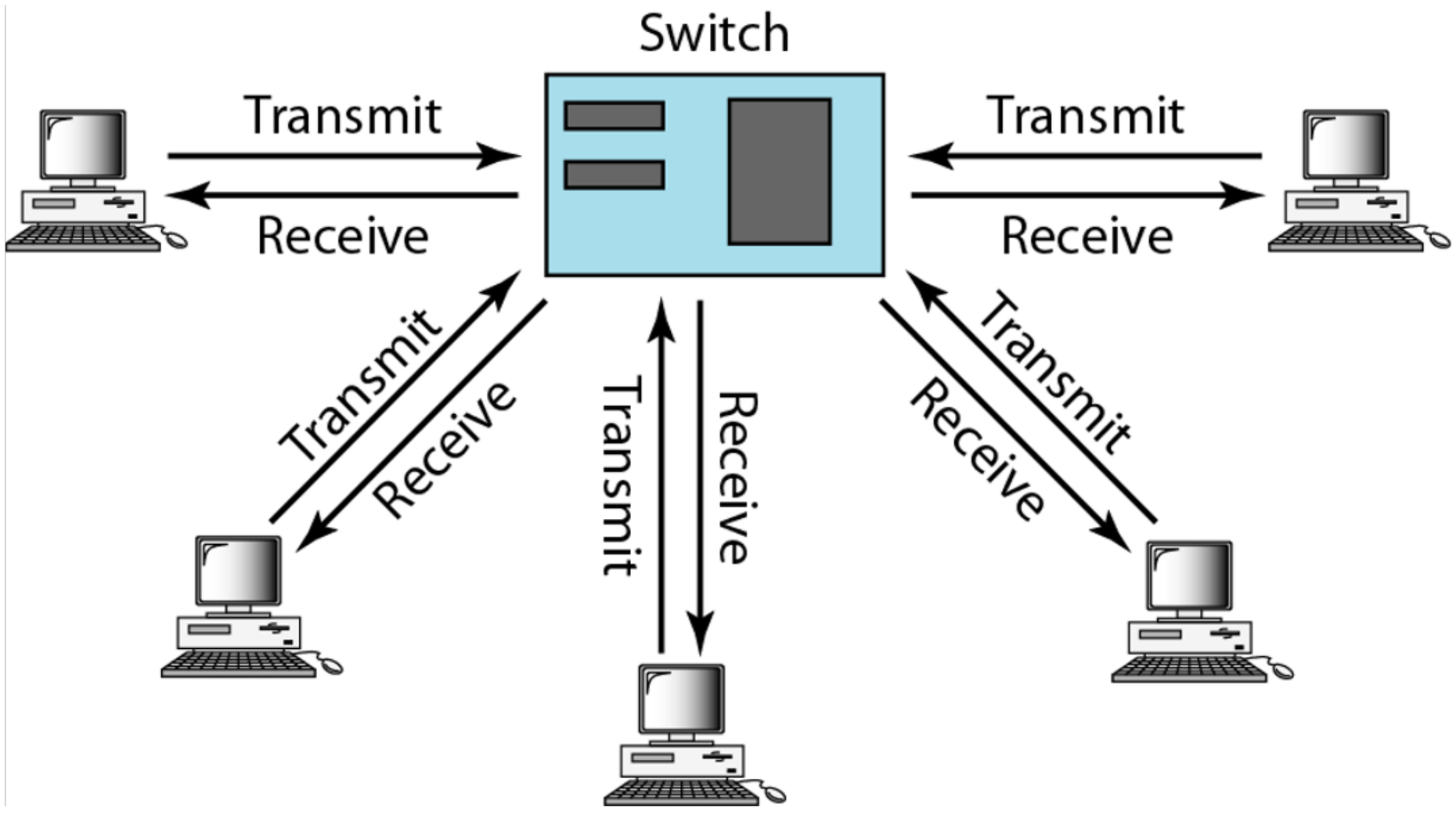
- Hubs wire all lines into a single CSMA/CD domain
- Switches isolate each port to a separate domain
  - Much greater throughput for multiple ports
  - No need for CSMA/CD with full-duplex lines



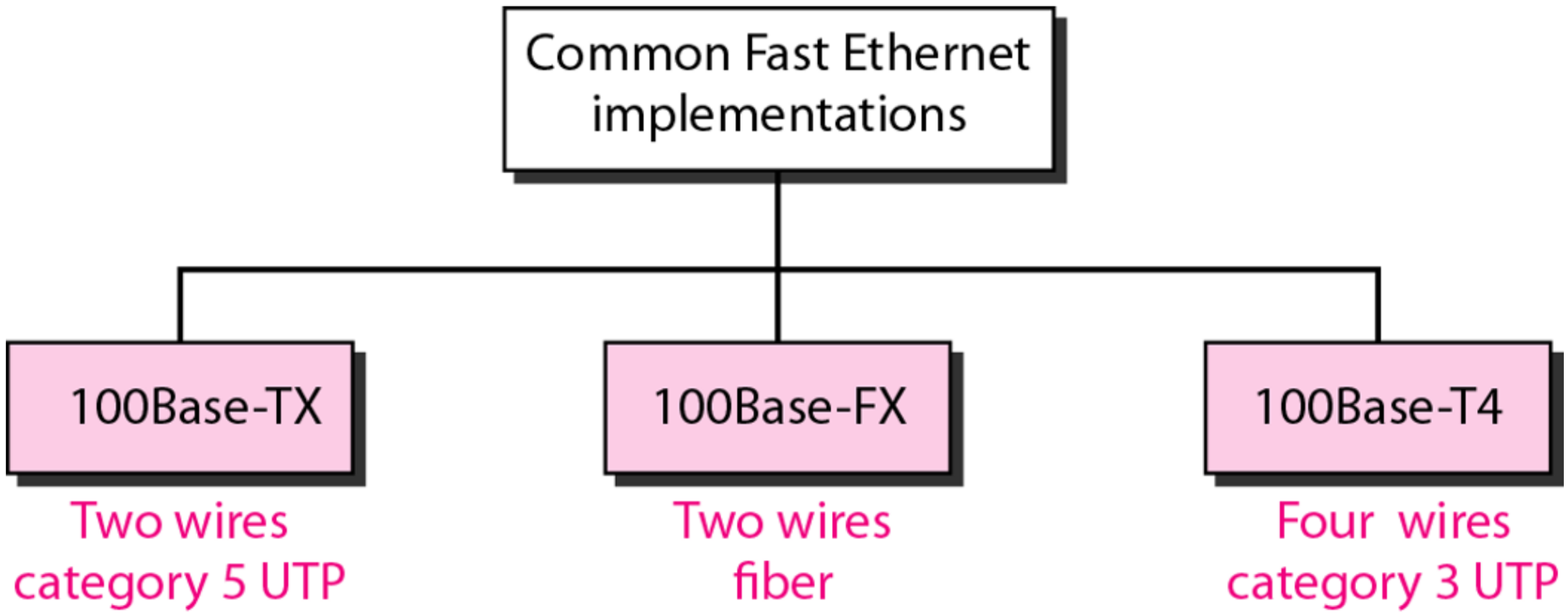
Switched / Fast Ethernet



Switched / Fast Ethernet



Switched / Fast Ethernet



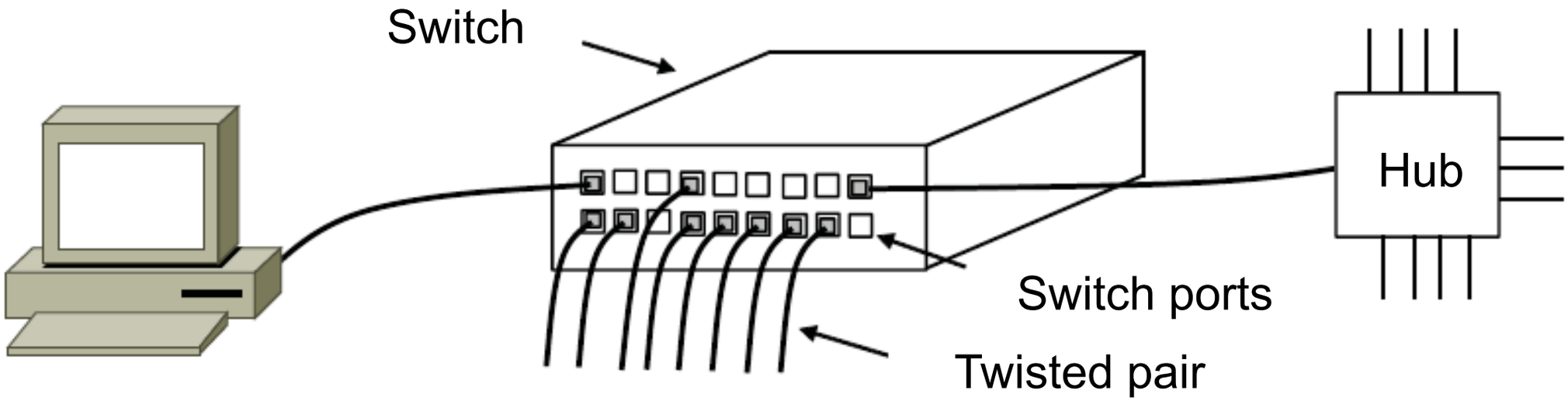
Switched / Fast Ethernet

- Two possibilities in 1992:
  - Keep protocol, but make it faster (won)
    - 802.3u
  - Keep name, but change everything
    - lost —> IEEE 802.12 standard

Switched / Fast Ethernet

- Needed to decide on cabling:
  - Category 3 twisted wire
    - Used in telephone cabling
    - Limits maximum distance to 10 m, therefore not used
  - 100Base-T4 (Cat 4 UTP)
    - or four Cat3 twisted pairs, standard for telephone cables
    - obsolete
- 100Base-TX
  - Two Category 5 UTP wires
- 100Base-FX
  - Two Fiber Optics cable
  - max distance is 2000m

Switched / Fast Ethernet



Switched / Fast Ethernet

- Hubs broadcast all packets received to all other ports
- Switches only forward packets received to one port
- Use a Mac-table (with aging)
- Addressing can be:
  - done by administration only (inflexible but most secure)
  - Automatic setup
    - When a package arrives, add the sender address to the MAC table
    - If unknown sender address: flood to all
      - Return packet will give the missing entry

Fast Ethernet

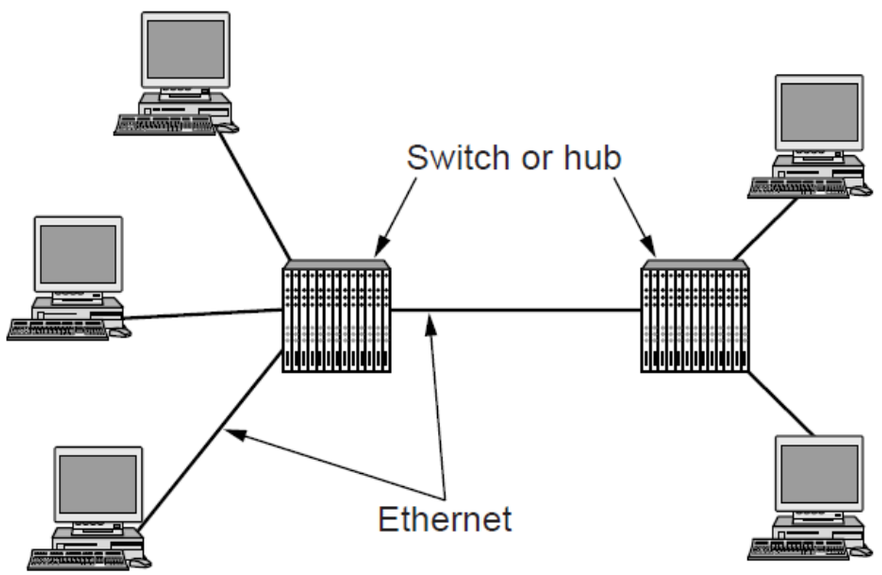
- Fast ethernet from 10 to 100 Mbps
- Twisted pair with CAT 5 dominated the market

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

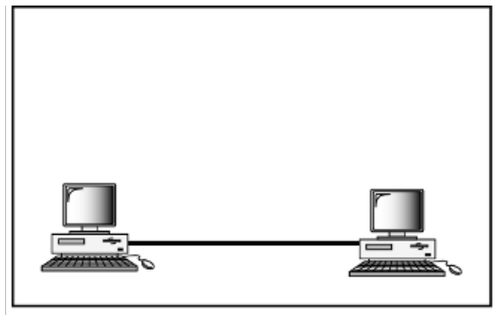
- Fast ethernet keeps all frame formats
- Reduce bit time from 100 nsec to 10 nsec
- Use hubs/switches instead of vampire taps / BNC connectors
- Cabling
  - Update 3 UTP in pairs or use better cabling

Gigabit Ethernet

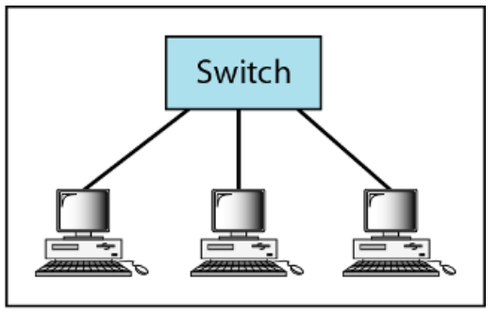
- Switched Gigabit Ethernet is now standard
  - Full duple lines between computers / switches
    - No contention possible when using switches
    - When using hubs (obsolete)
      - Use CSMA/CD with larger minimum frame size of 512B
      - Allows frame bursts (several frames sent together)



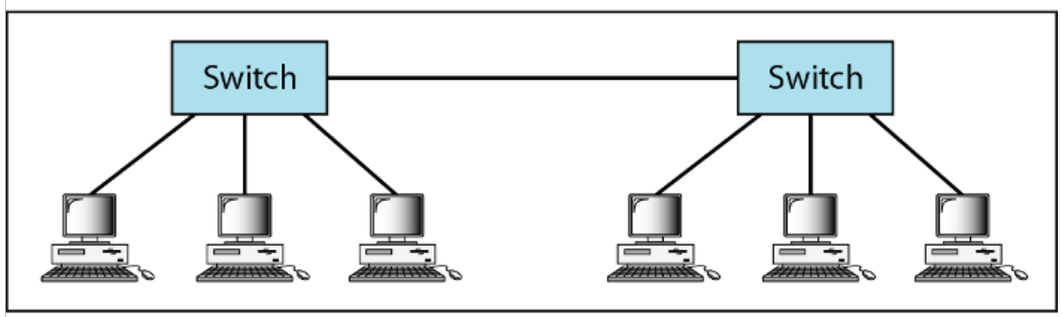
Gigabit Ethernet



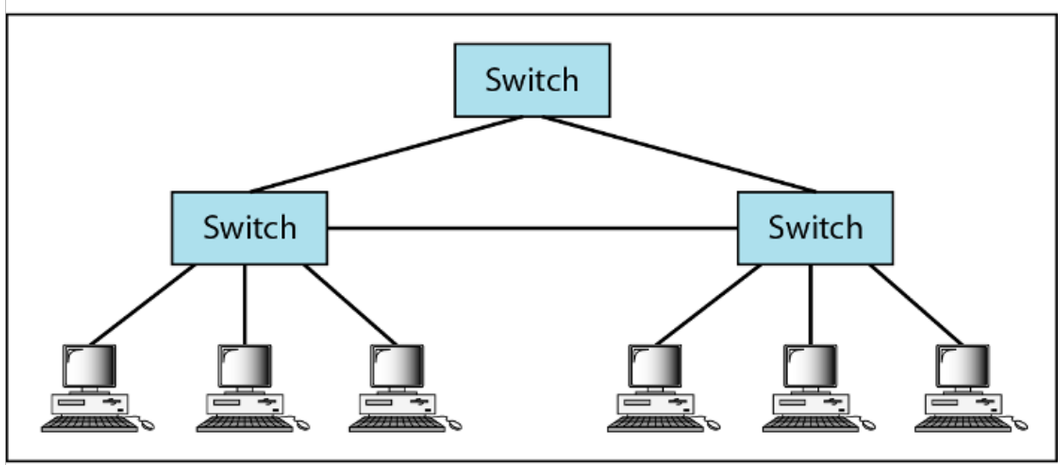
a. Point-to-point



b. Star

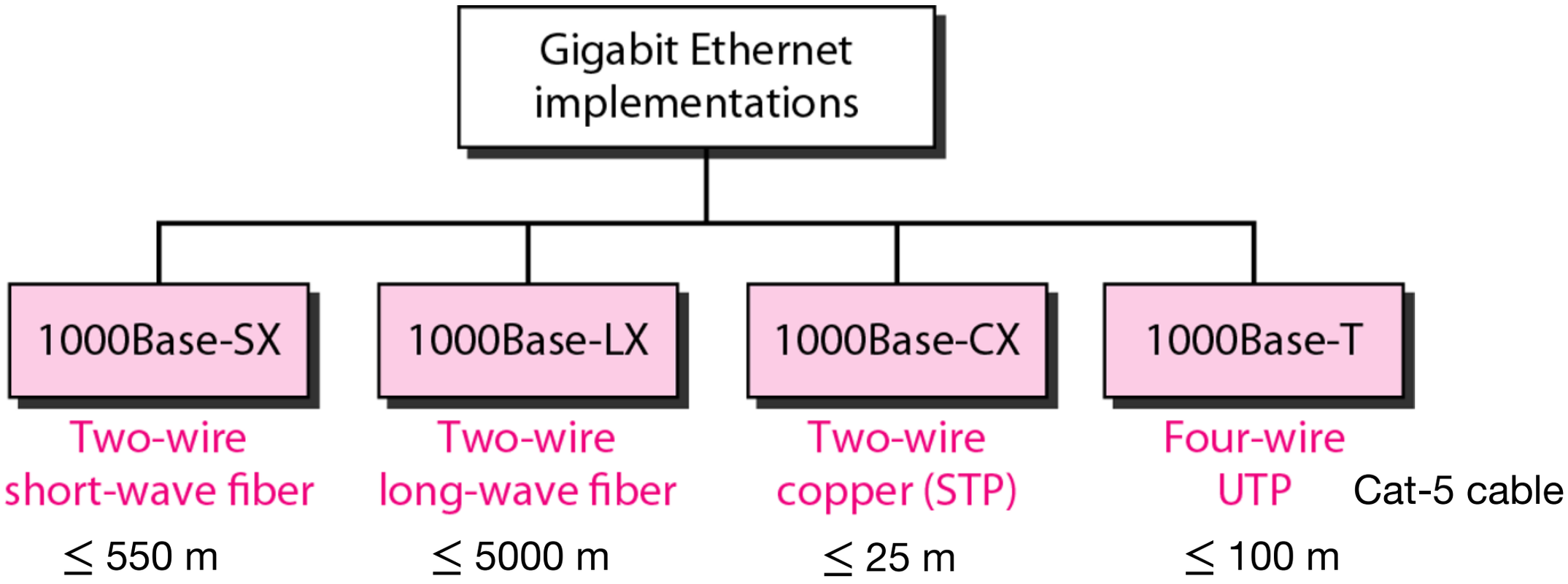


c. Two stars



d. Hierarchy of stars

Gigabit Ethernet

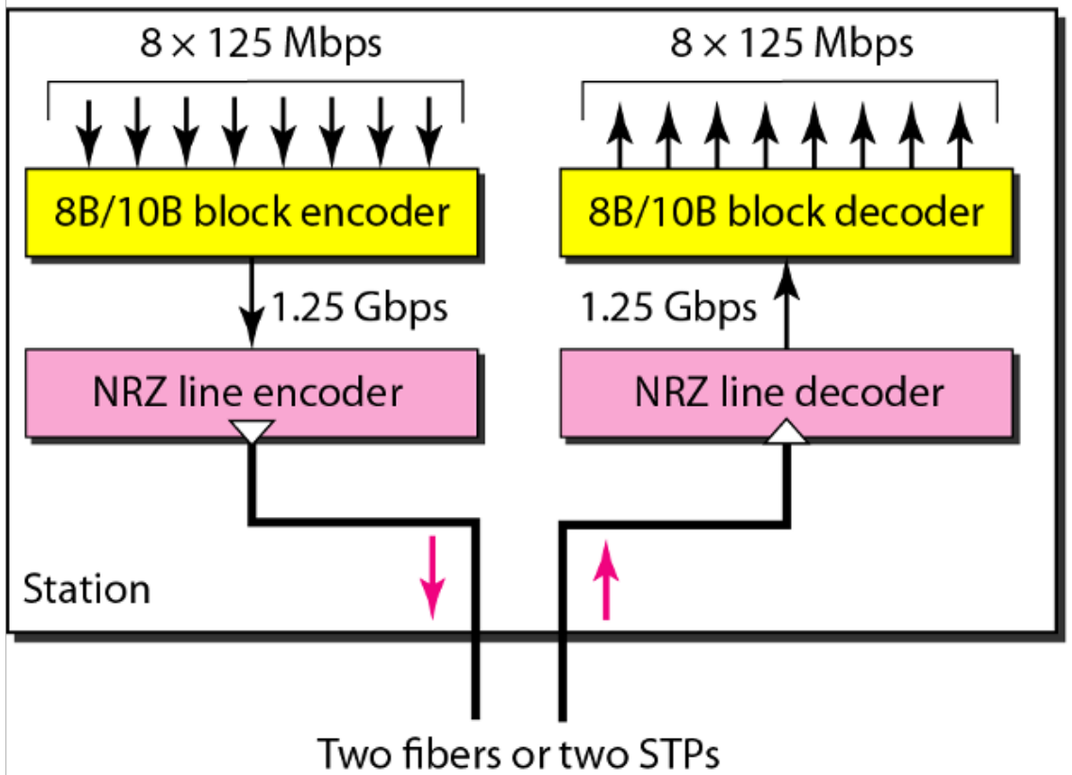


STP: Shielded Twisted Pair
UTP: Unshielded Twisted Pair

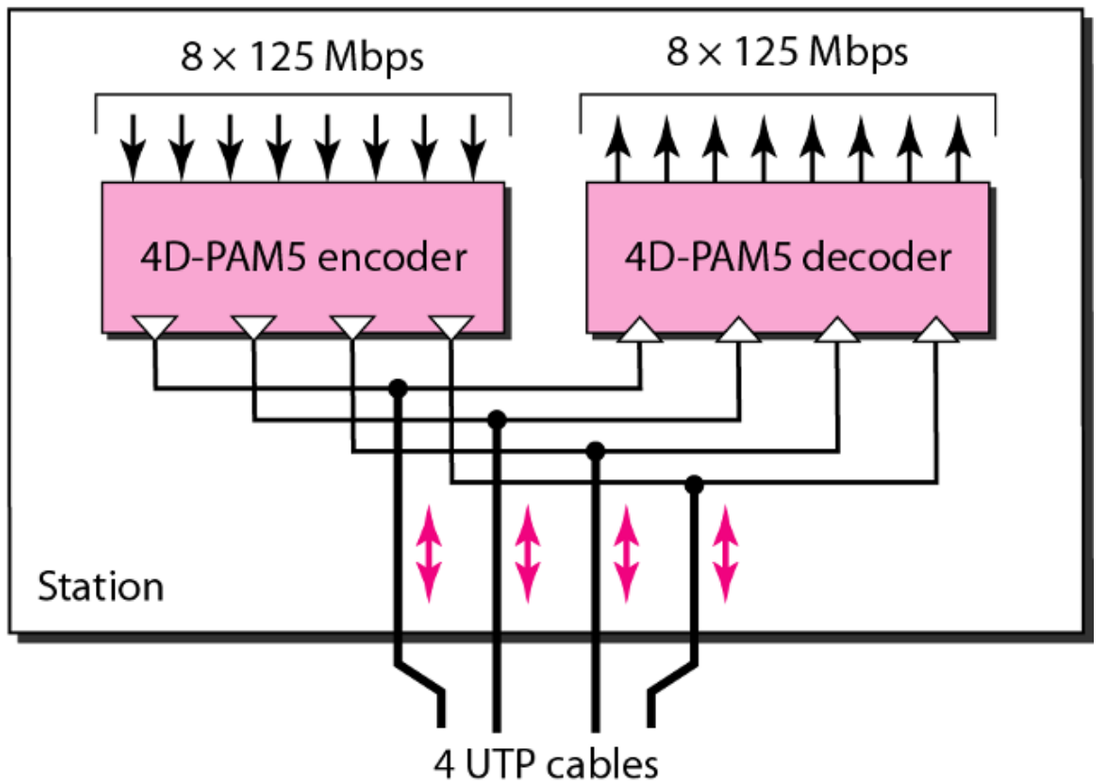
Gigabit Ethernet

- Physical level:
  - two wire implementation: fiber-optic cable
  - four wire implementation: Cat 5 twisted pair cable

1000Base-SX, 1000Base-LX, and 1000Base-CX



1000Base-T



Gigabit Ethernet

- To accommodate long lines and CSMA/CD:
  - Carrier extension: Hardware makes frames longer
  - Frame bursting: Sender concatenates frames
- Only needed for backward extension
  - Even then, most companies would just replace hubs and switches

Gigabit Ethernet

- To achieve throughput over copper wire:
  - Use short, shielded copper wire
  - Change encoding, using 8B/10B encoding and NRZ
- For Cat 5 wires:
  - Use all four twisted pairs with five voltage levels
    - signaling at 125 Msymbols/sec

Gigabit Ethernet

- Introduce flow control:
  - PAUSE command to stop sender from sending
- Jumbo frames up to 9KB
  - proprietary feature
  - allows fewer frames to be processed

Gigabit Ethernet

Characteristics	*1000Base-SX*	*1000Base-LX*	*1000Base-CX*	*1000Base-T*
Media	Fiber short-wave	Fiber long-wave	STP	Cat 5 UTP
Number of wires	2	2	2	4
Maximum length	550 m	5000 m	25 m	100 m
Block encoding	8B/10B	8B/10B	8B/10B	
Line encoding	NRZ	NRZ	NRZ	4D-PAM5

Gigabit Ethernet

Gigabit Ethernet is commonly run over twisted pair

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

10 Gigabit Ethernet is being deployed where needed

Name	Cable	Max. segment	Advantages
10GBase-SR	Fiber optics	Up to 300 m	Multimode fiber (0.85μ)
10GBase-LR	Fiber optics	10 km	Single-mode fiber (1.3μ)
10GBase-ER	Fiber optics	40 km	Single-mode fiber (1.5μ)
10GBase-CX4	4 Pairs of twinax	15 m	Twinaxial copper
10GBase-T	4 Pairs of UTP	100 m	Category 6a UTP

40/100 Gigabit Ethernet is under development

10 Gigabit Ethernet

- Needed in data centers
  - No more CSMA/CD
  - Only full duplex operations
  - Use a 64/66 code

10 Gb Ethernet

Characteristics	*10GBase-S*	*10GBase-L*	*10GBase-E*
Media	Short-wave 850-nm multimode	Long-wave 1310-nm single mode	Extended 1550-mm single mode
Maximum length	300 m	10 km	40 km

- Needs to use fiber-optical
- Operates only in full duplex mode

10 Gigabit Ethernet

- Over copper:
  - 10GBase-CX4
    - four pairs of twinaxial copper wires with maximum distance of 15m
  - 10GBase-T:
    - four pairs of UTP (Cat 6A) with maximum distance of 100m

Ethernet

- IEEE 802.3bs
  - 400 Gb/sec over fiber
- IEEE 802.3cd
  - 200 Gb/sec over twin-axial cables up to 3m
- IEEE 802.3cn
  - 400 Gb/s over 8 pairs of MMF up to 100 m

Wireless

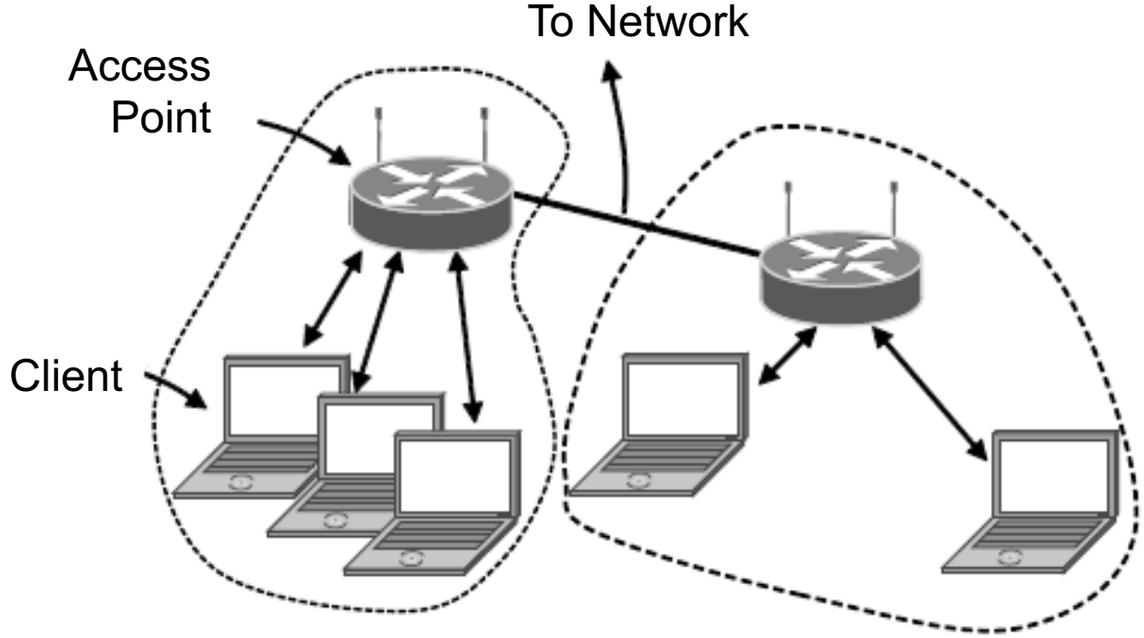
IEEE 802.11

802.11: Wireless Local Area Network (WLAN)

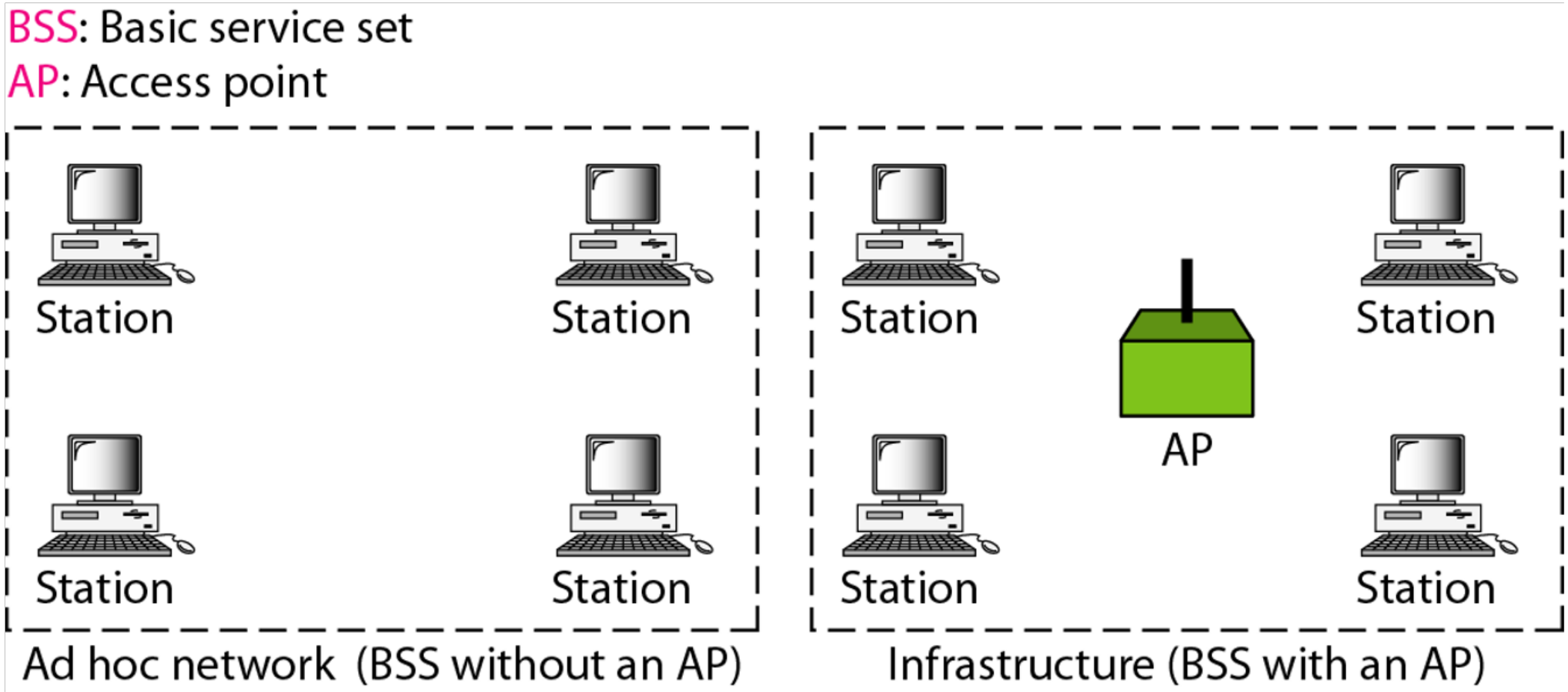
- IEEE has defined the specifications for wireless LAN
  - Covers physical and data link layers
- Can be used as "ad hoc" networks
- Can be used as an infrastructure network
  - With one or more access points

Wireless LAN Architecture

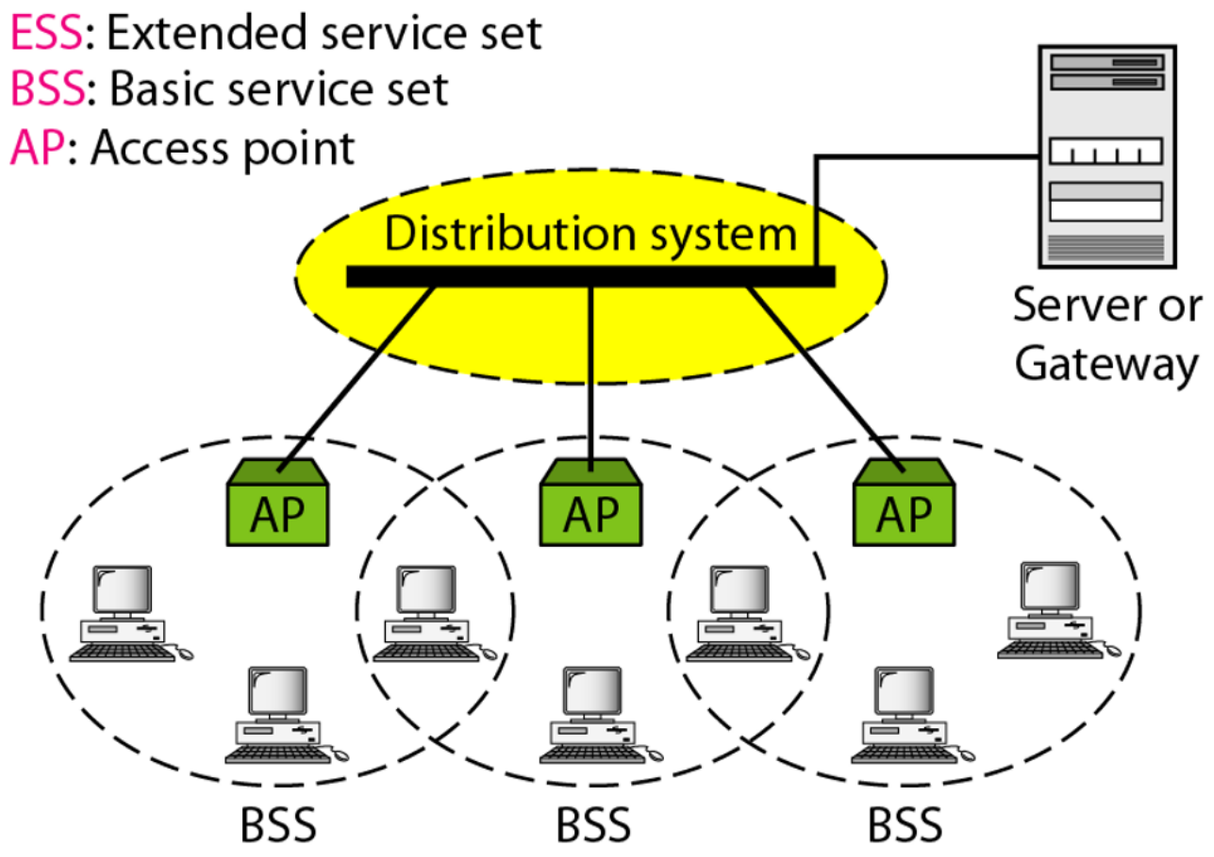
- Wireless clients associate in general to a wired Access Point (infrastructure mode)



WLAN


BSS: Basic service set
AP: Access point
Station
Station
Station
Station
Station
Station
Station
Station
Station
AP
Ad hoc network (BSS without an AP)
Infrastructure (BSS with an AP)

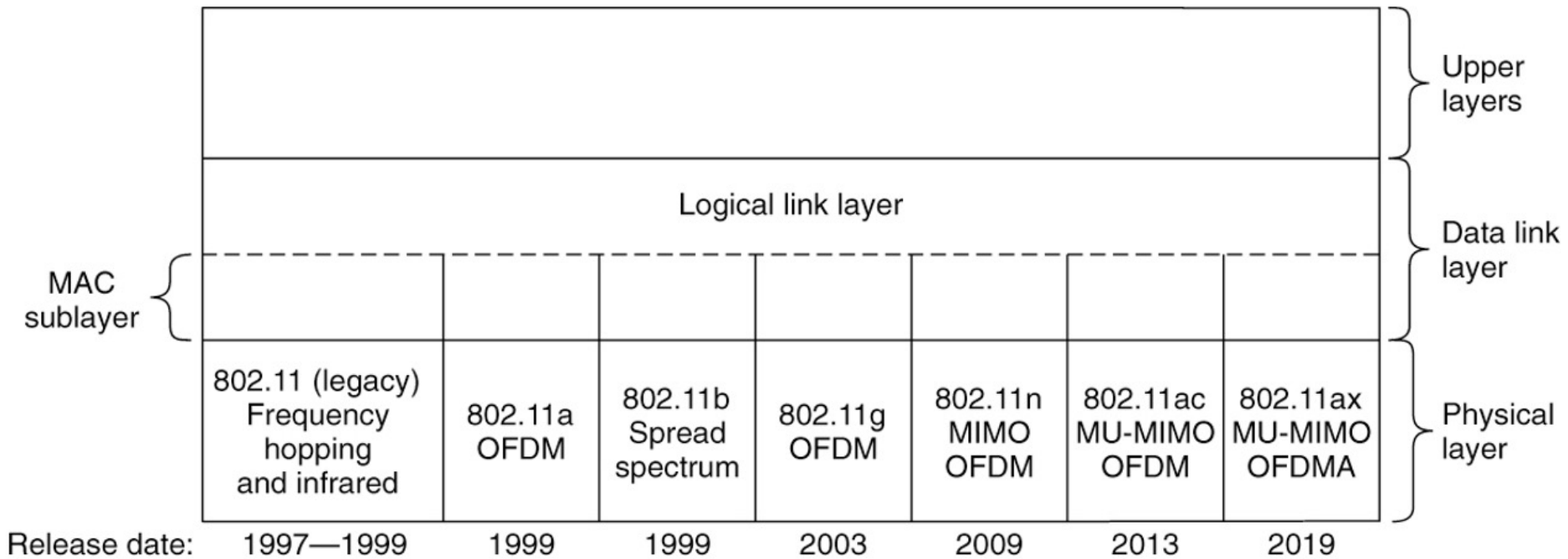
WLAN



Extended Service Sets

802.11 Architecture

- Uses different physical layer technologies over the years



802.11

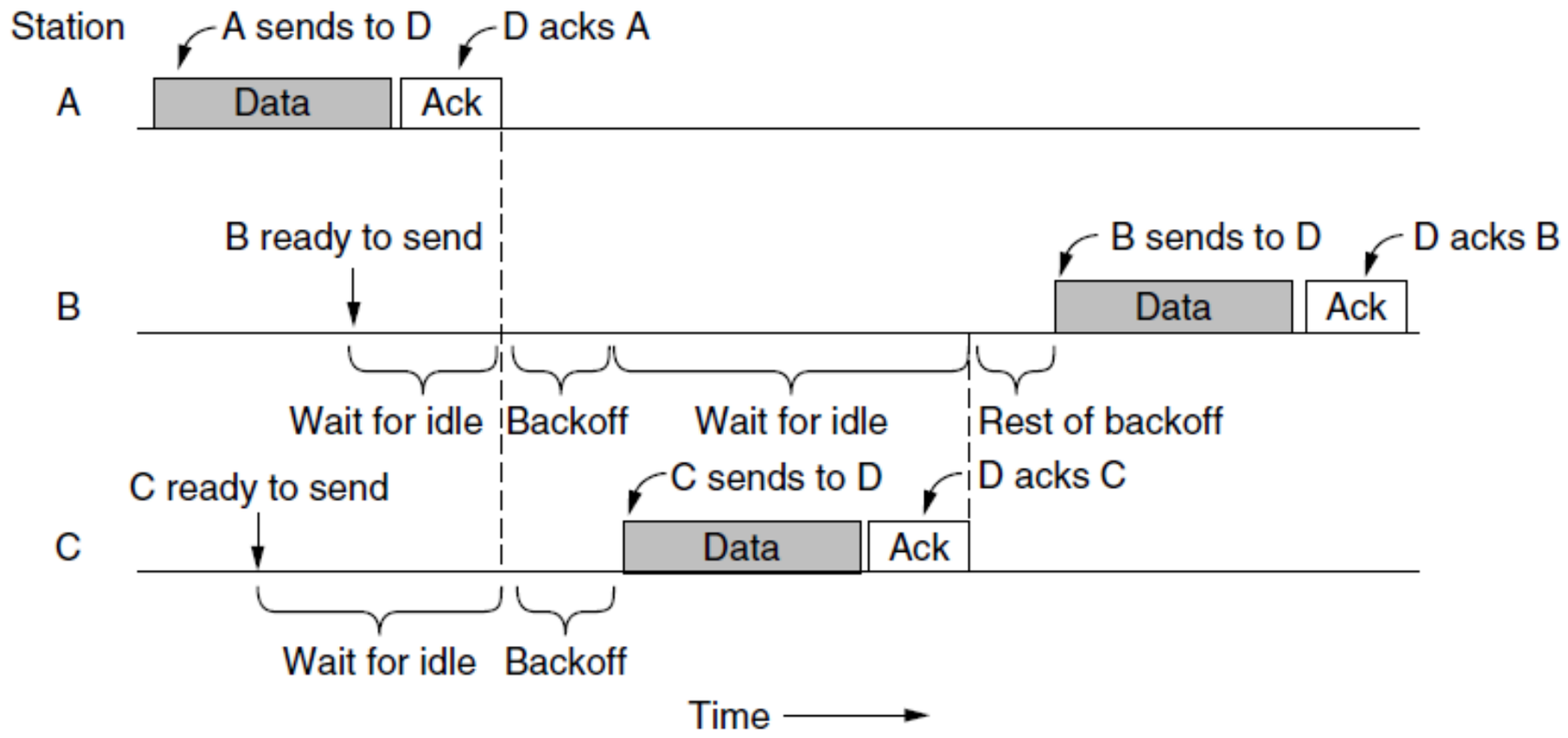
- 802.11b spread-spectrum using Barker sequence / Complementary Code Keying
- 802.11a uses Orthogonal Frequency Division Multiplexing
  - Uses 52 subcarriers
  - Shorter range but higher data flow than 802.11b
- 802.11g also uses OFDM but operates in a different band
- 802.11n doubles channels and reduces frame overhead, up to four antennas for four different streams
  - Throughput of 100 Mbps
- 802.11ad: "WiGig" Triband, speeds up to 7Gbps, distance then only 11 ft

802.11 Physical Layer

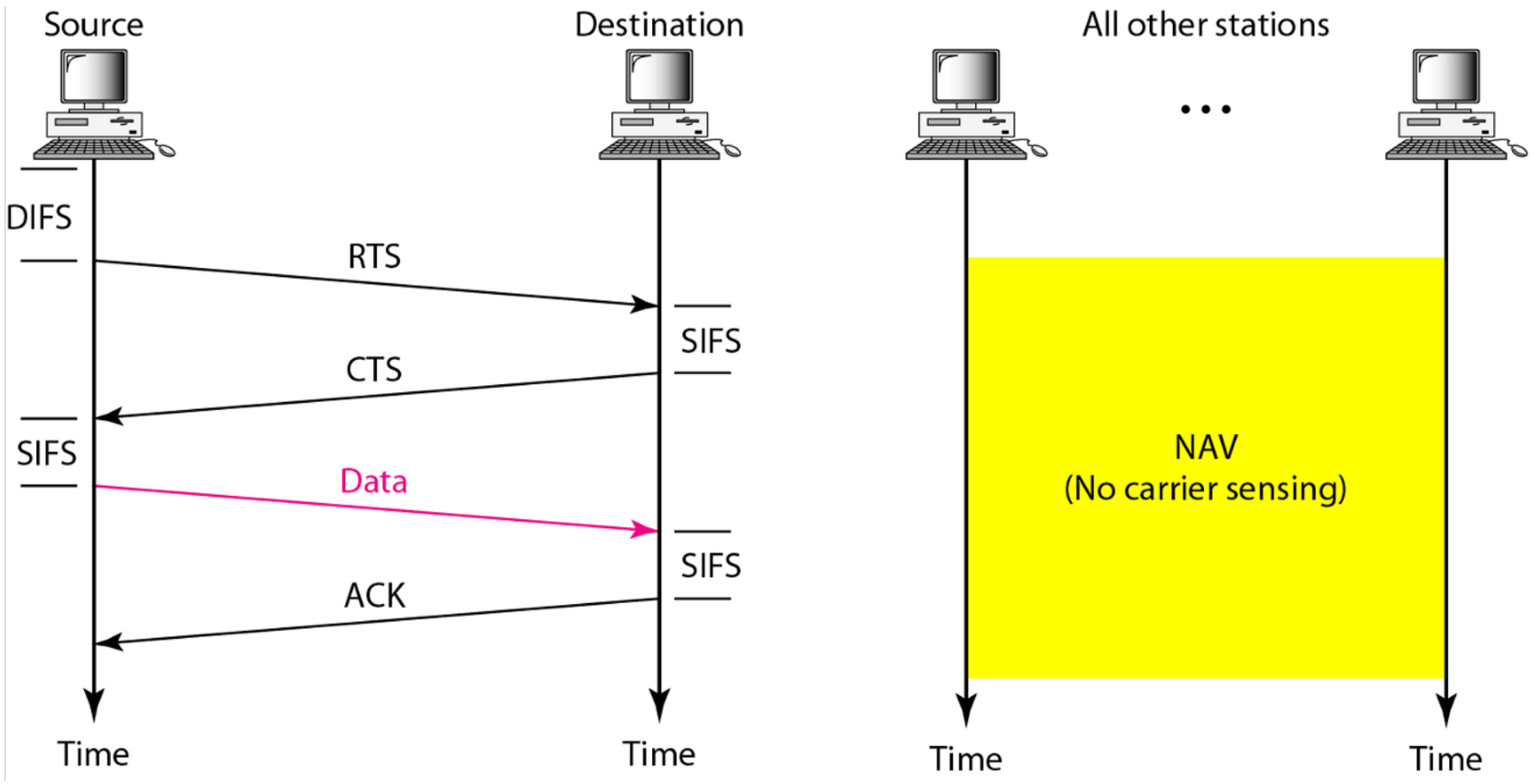
Name	Technique	Max. Bit Rate
802.11b	Spread spectrum, 2.4 GHz	11 Mbps
802.11g	OFDM, 2.4 GHz	54 Mbps
802.11a	OFDM, 5 GHz	54 Mbps
802.11n	OFDM with MIMO, 2.4/5 GHz	600 Mbps

802.11 MAC

- Uses CSMA / Collision Avoidance with Acks



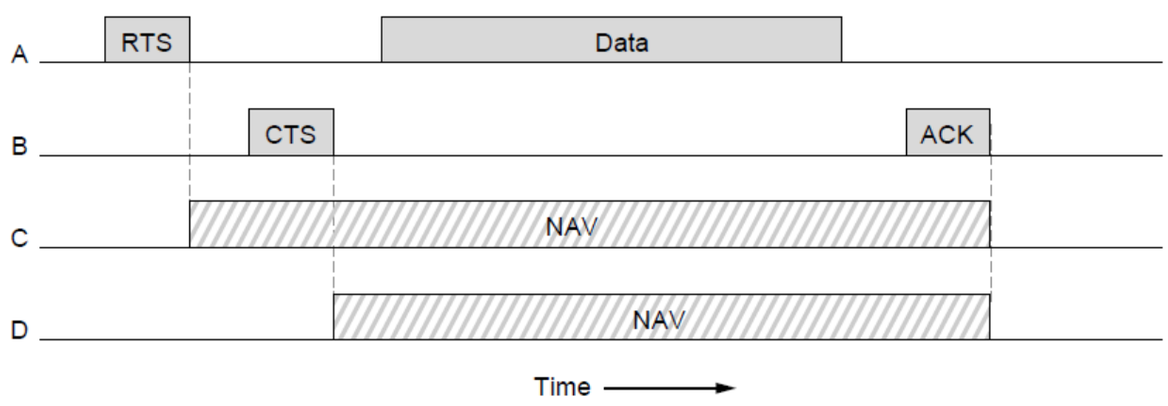
802.11 MAC



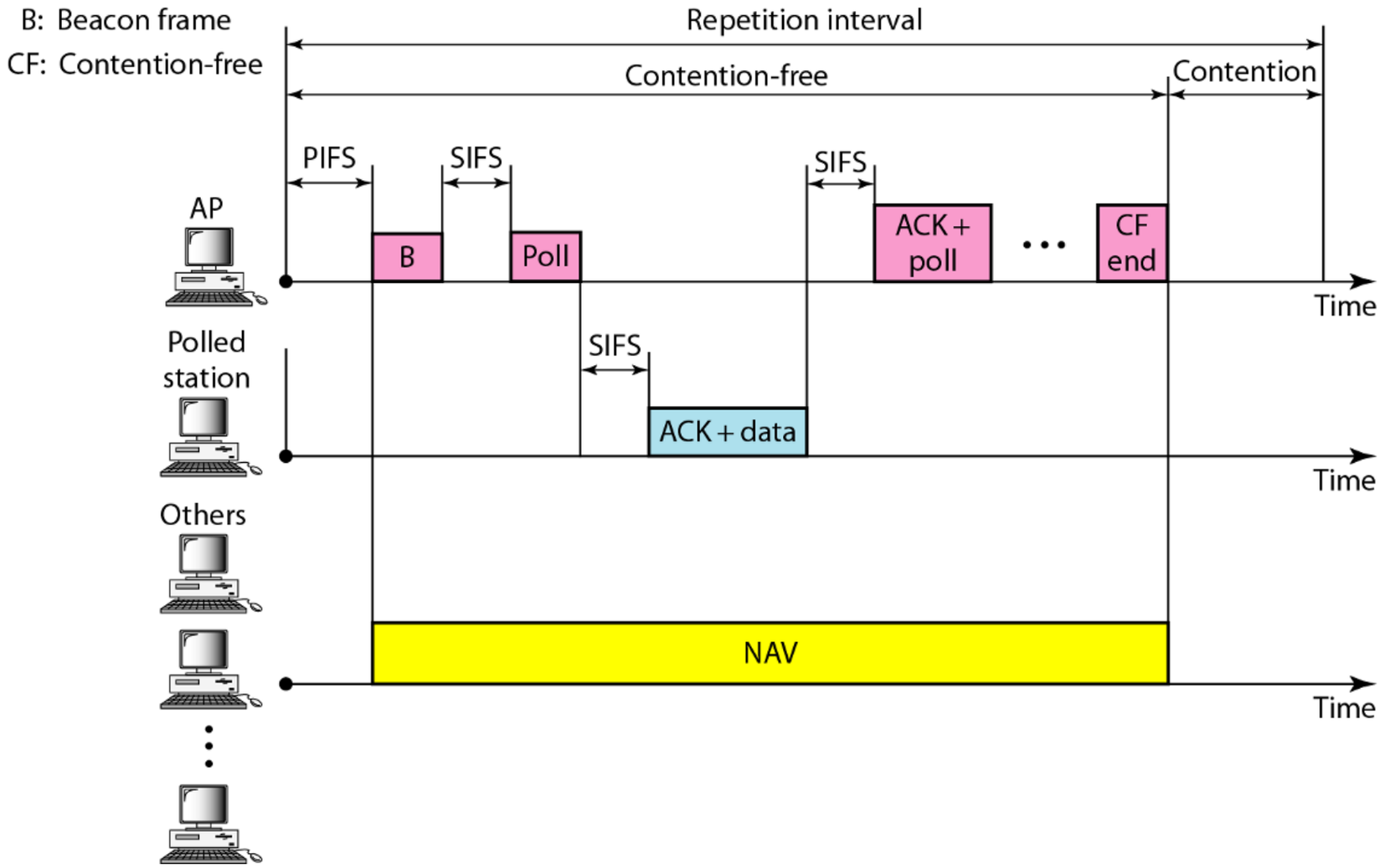
Optional RTS/CTS protocol

802.11 MAC

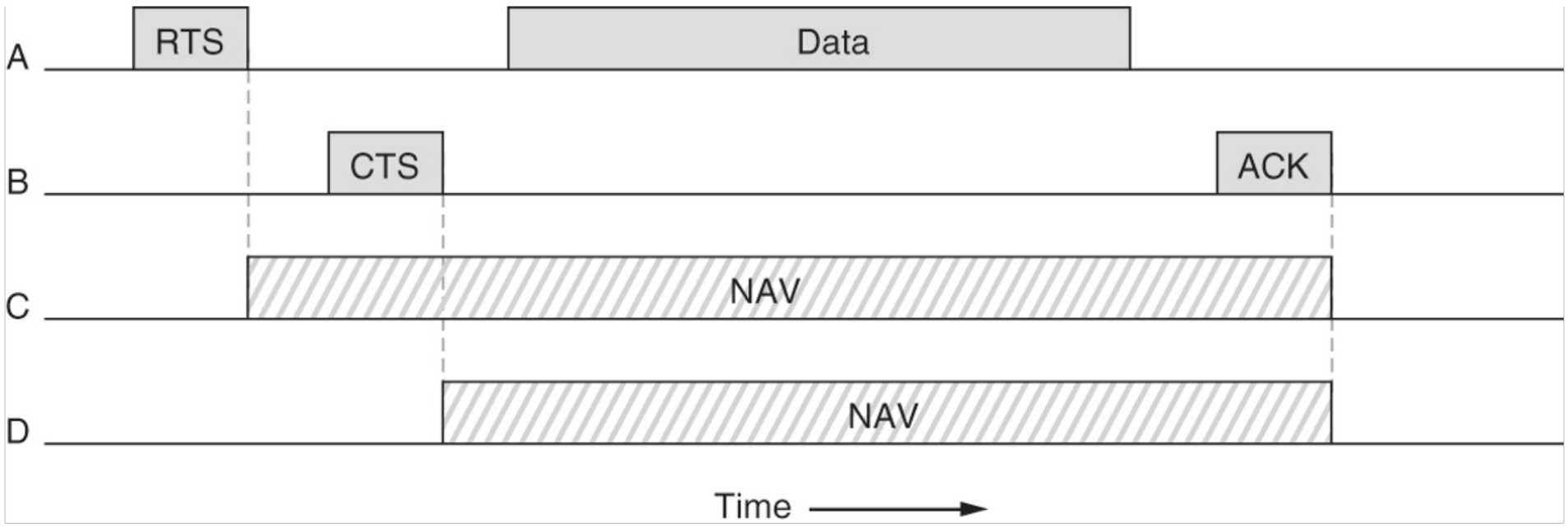
- Uses physical and virtual sensing
  - Physical sensing:
    - Is there a valid signal on the medium
  - Virtual sensing:
    - Track use by other stations
- Network Allocation Vector:
  - Each frame carries an NAV field that gives the time that the station will use the medium



802.11 MAC

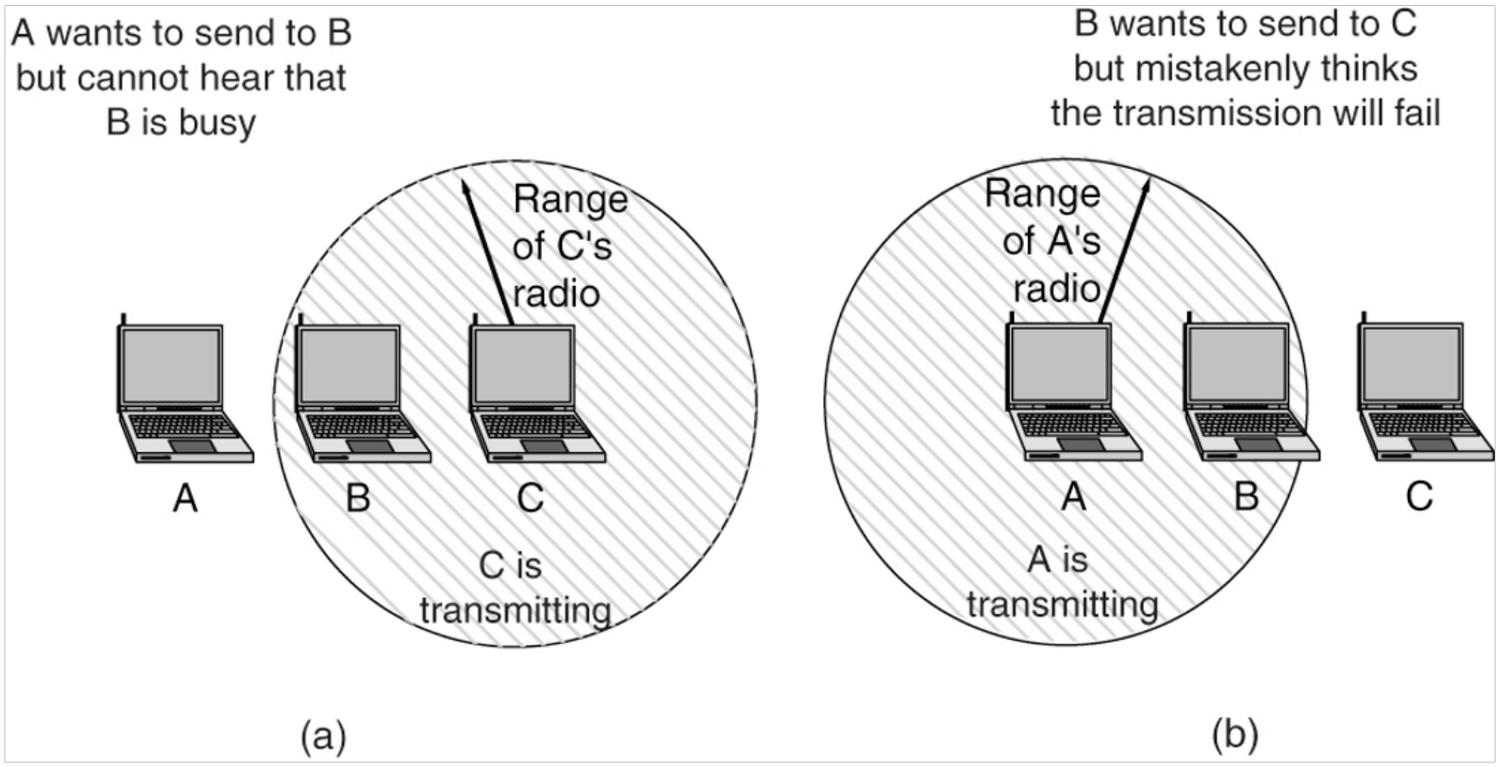

B: Beacon frame
CF: Contention-free
Repetition interval
Contention-free
Contention
PIFS
SIFS
SIFS
AP
B
Poll
ACK + poll
CF end
Time
Polled station
SIFS
ACK + data
Time
Others
NAV
Time

802.11 MAC



Virtual channel sensing using CSMA/CA

802.11



(a) The hidden terminal problem. (b) The exposed terminal problem.

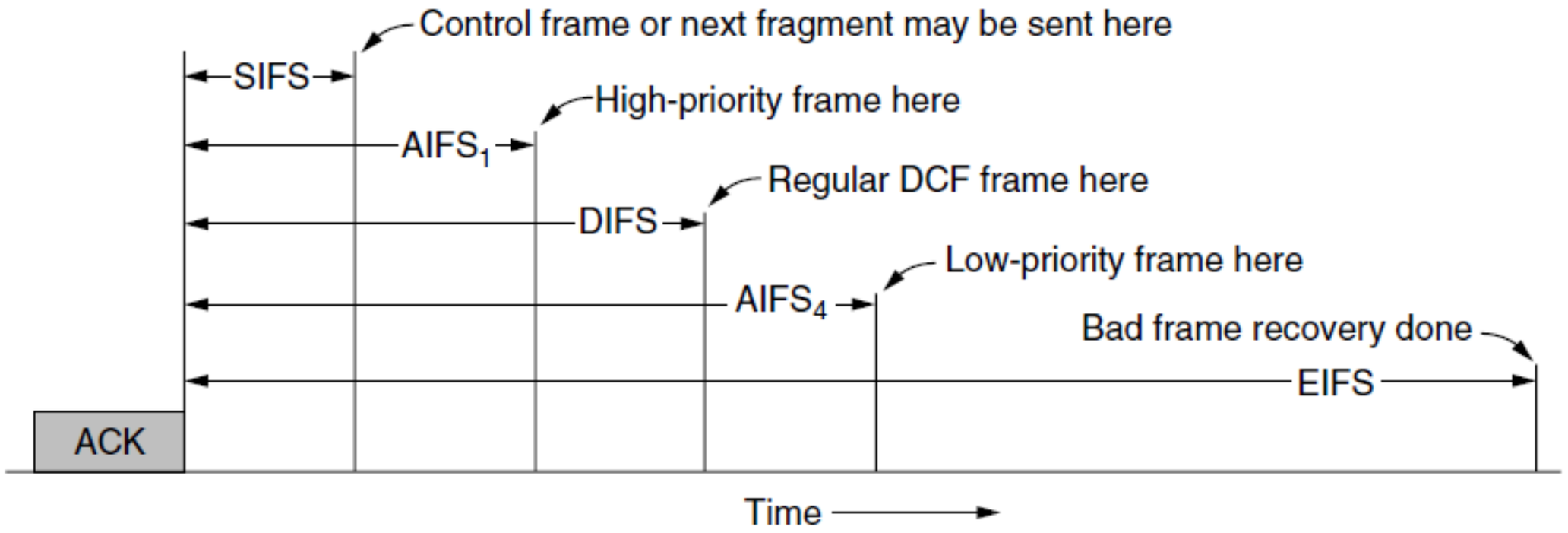
802.11

- RTS/CTS: not of great value
  - only helps with hidden terminals, but these are unlikely
  - does not help with short frames
  - not necessary since each frame carries a NAV field

802.11 Issues

- Reliability
  - Use slower transmission rates
  - Use shorter frames (including fragmentation)
- Saving power
  - Use beacon frames by which access points advertise their presence
  - Clients can enter power-safe mode
    - AP will buffer traffic for them
  - Automatic Power Save Delivery (APSD)
    - AP sends frames only after interchange with station
    - So station can go to sleep
- Quality of service
  - Extend CSMA/CA with carefully defined intervals between frames

802.11e Interframe Spacing

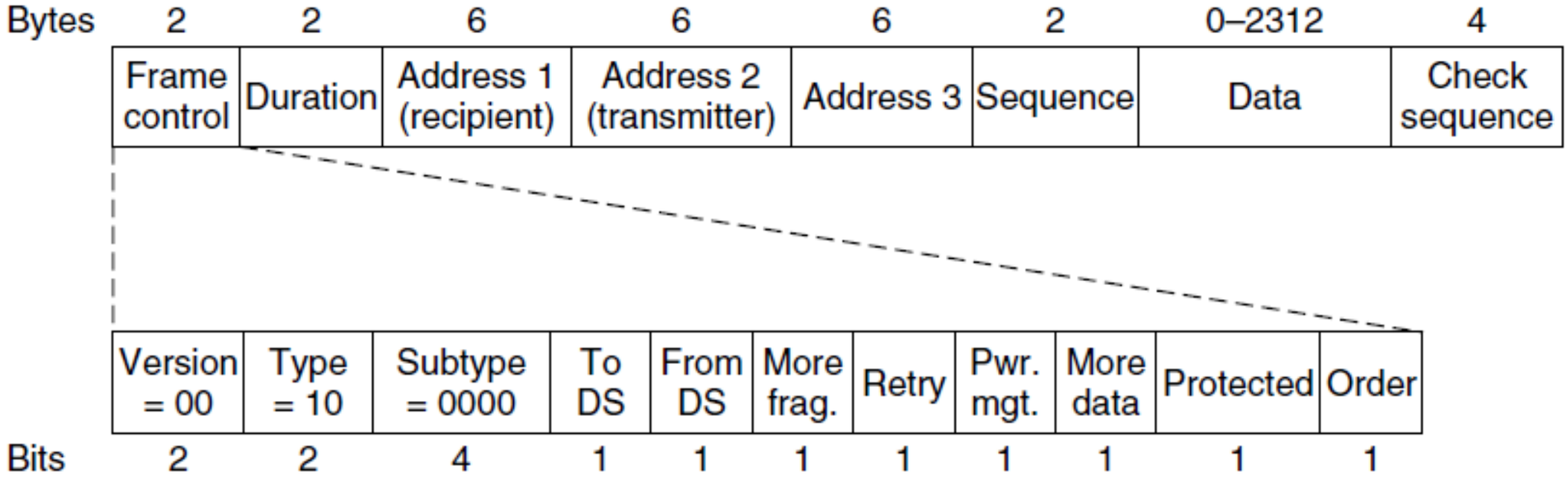


802.11

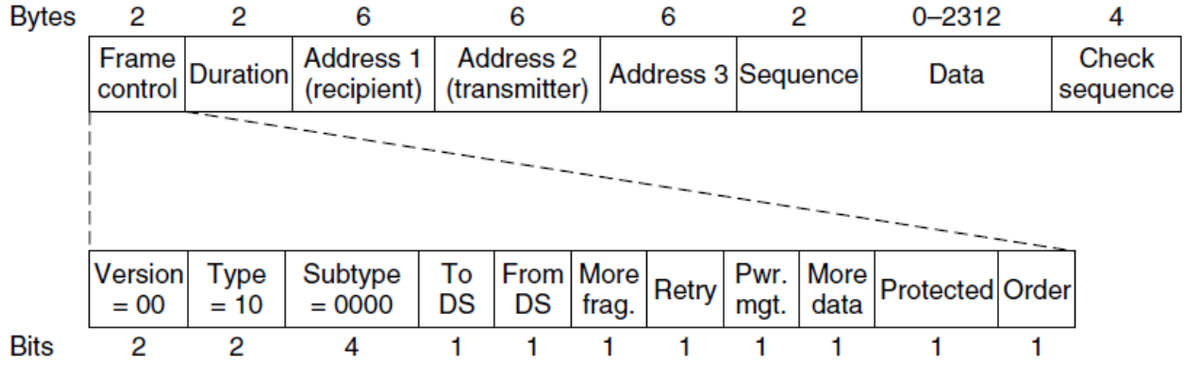
- Frames:
  - Data, control, and management frames

802.11 Frames

- Frames vary depending on their type (frame control bytes)
- Data frames have three addresses to select Access Point



802.11 Frames



Field	*Explanation*
Version	Current version is 0
Type	Type of information: management (00), control (01), or data (10)
Subtype	Subtype of each type (see Table 14.2)
To DS	Defined later
From DS	Defined later
More flag	When set to 1, means more fragments
Retry	When set to 1, means retransmitted frame
Pwr mgt	When set to 1, means station is in power management mode
More data	When set to 1, means station has more data to send
WEP	Wired equivalent privacy (encryption implemented)
Rsvd	Reserved

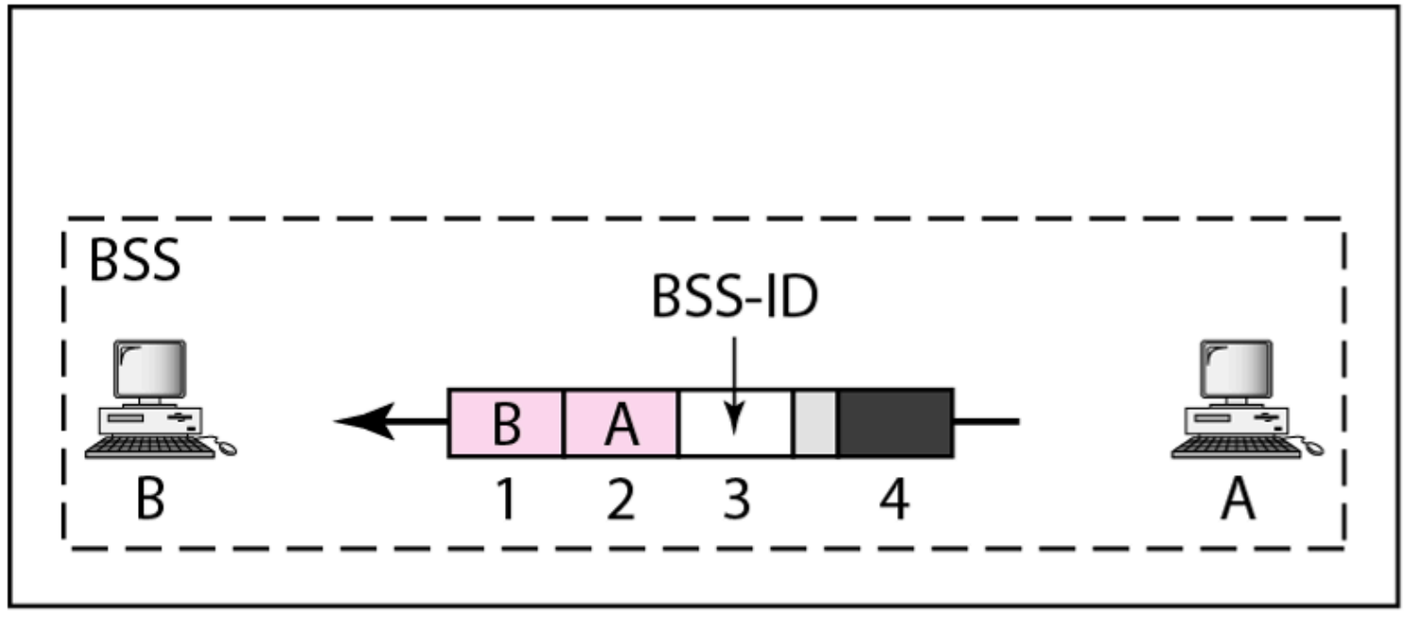
802.11 Addressing

- FC field specifies four addressing cases

To DS	*From DS*	*Address 1*	*Address 2*	*Address 3*	*Address 4*
0	0	Destination	Source	BSS ID	N/A
0	1	Destination	Sending AP	Source	N/A
1	0	Receiving AP	Source	Destination	N/A
1	1	Receiving AP	Sending AP	Destination	Source

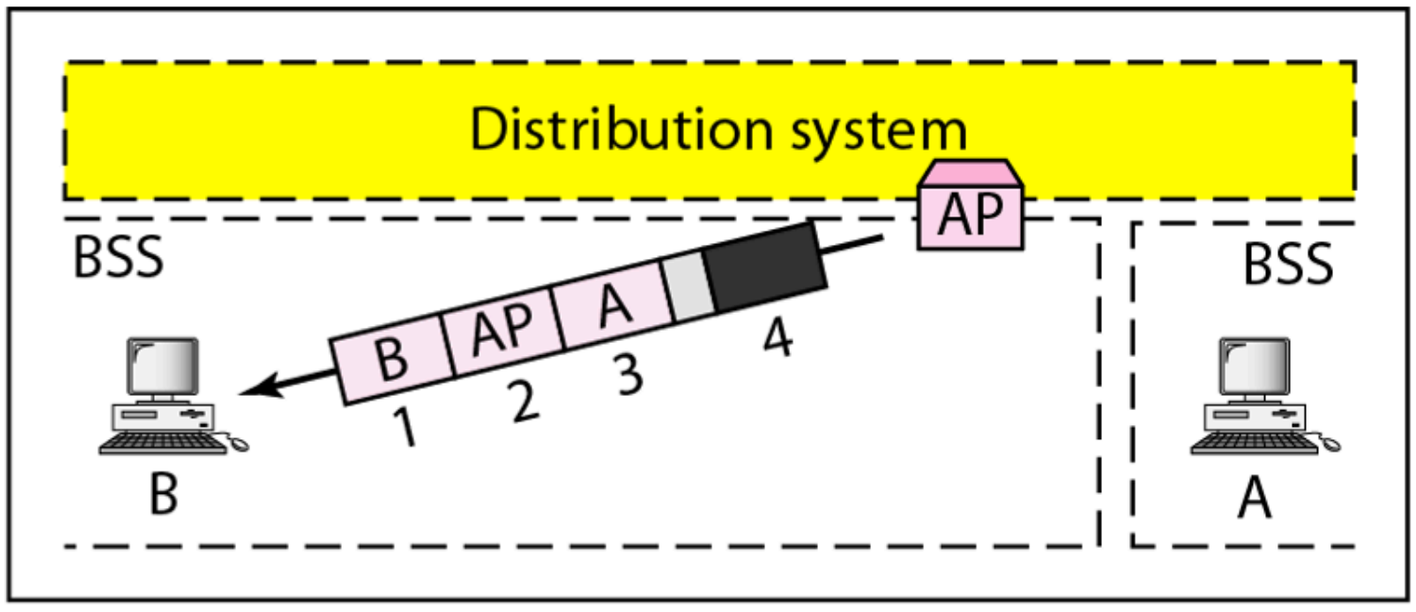
802.11 Frames

- Case 1: ToDS = 0, From DS=0
  - The frame travels inside a Basic Service Set (BSS)
    - Address 1 is Destination
    - Address 2 is Source
    - Address 3 is BSS Id



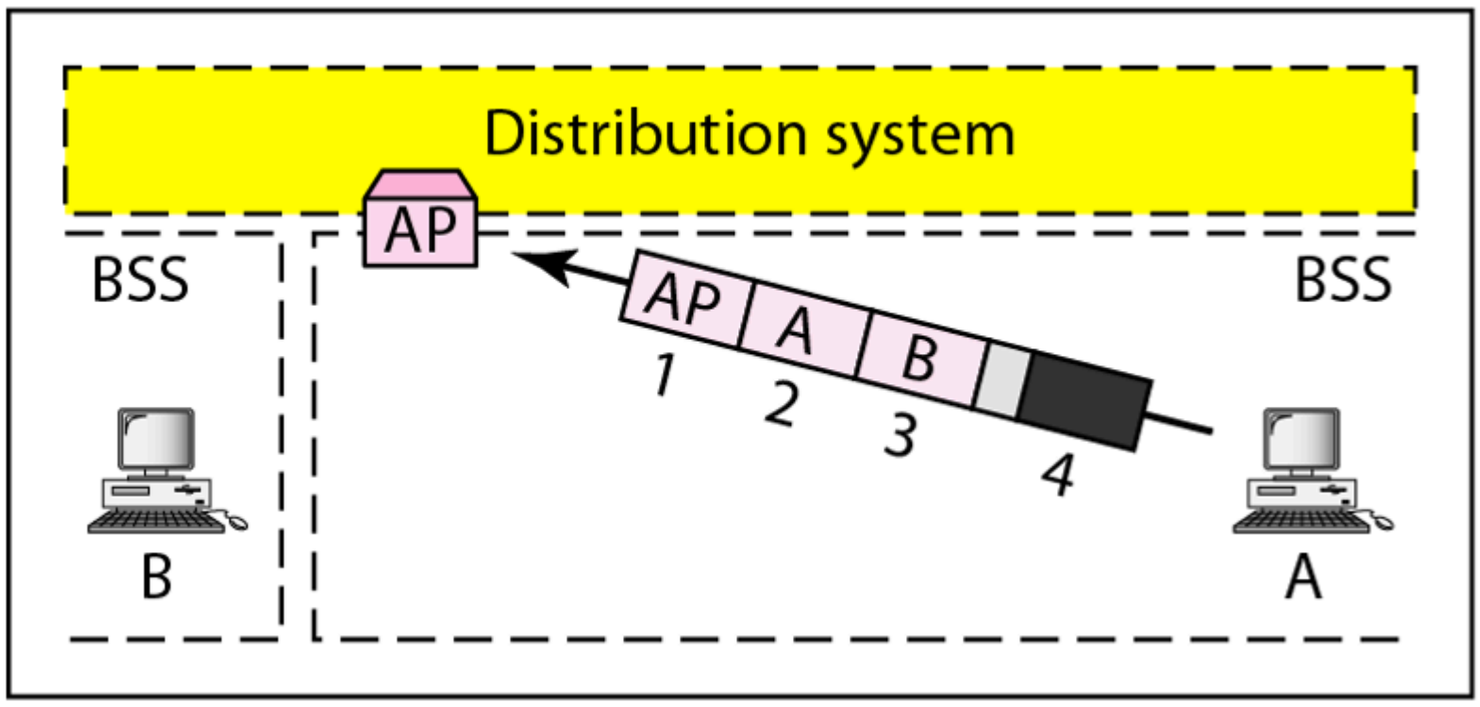
802.11 Addressing

- Case 2: ToDS = 0, FromDS = 1
  - Frame is coming from a distribution system and goes to a wireless station
  - Address 1 is wireless station
  - Address 2 is the Access Point (AP)
  - Address 3 is the original sender outside the BSS



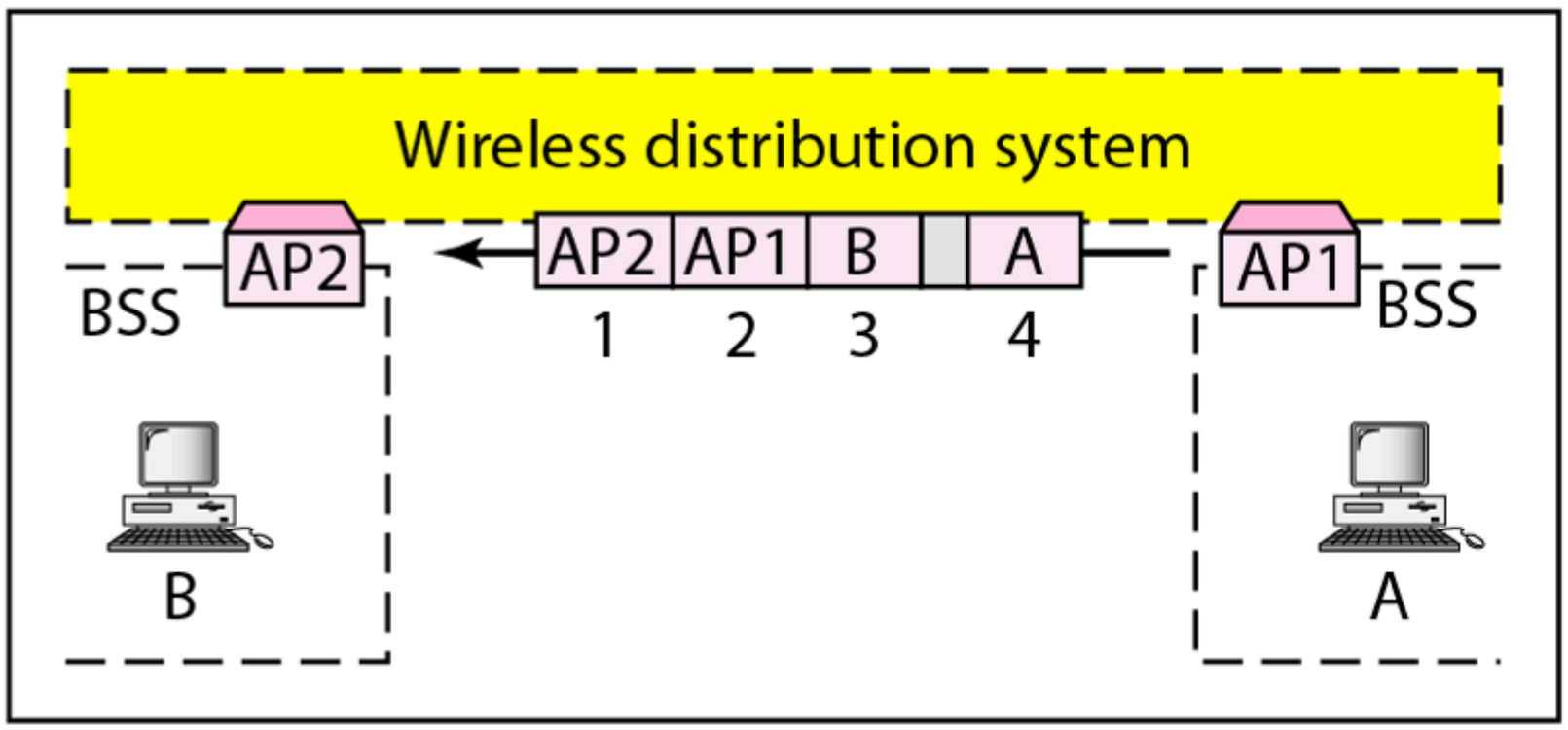
802.11 Addressing

- Case 3: ToDS = 1 and FromDS = 0
  - Frame is going to a distribution system from inside the BSS
  - Address 1: Address of access point
  - Address 2: Sender in the BSS
  - Address 3: Address of final destination



802.11 Addressing

- Case 4: ToDS=1 FromDS=1
  - Distribution system is also wireless and frame goes from one AP to another AP
  - Need four addresses: original sender, AP sender, original destination, AP destination



802.11 Services

- Association service:
  - Mobile station connects to Access Points
  - After learning from beacon frame or directly asking AP
- Reassociation:
  - Allows station to change to preferred AP
- Authentication:
  - Depends on choice of security credentials
    - WPA2 — Wifi protected access 2
    - Replacing WEP: Wired equivalency privacy

802.11 Services

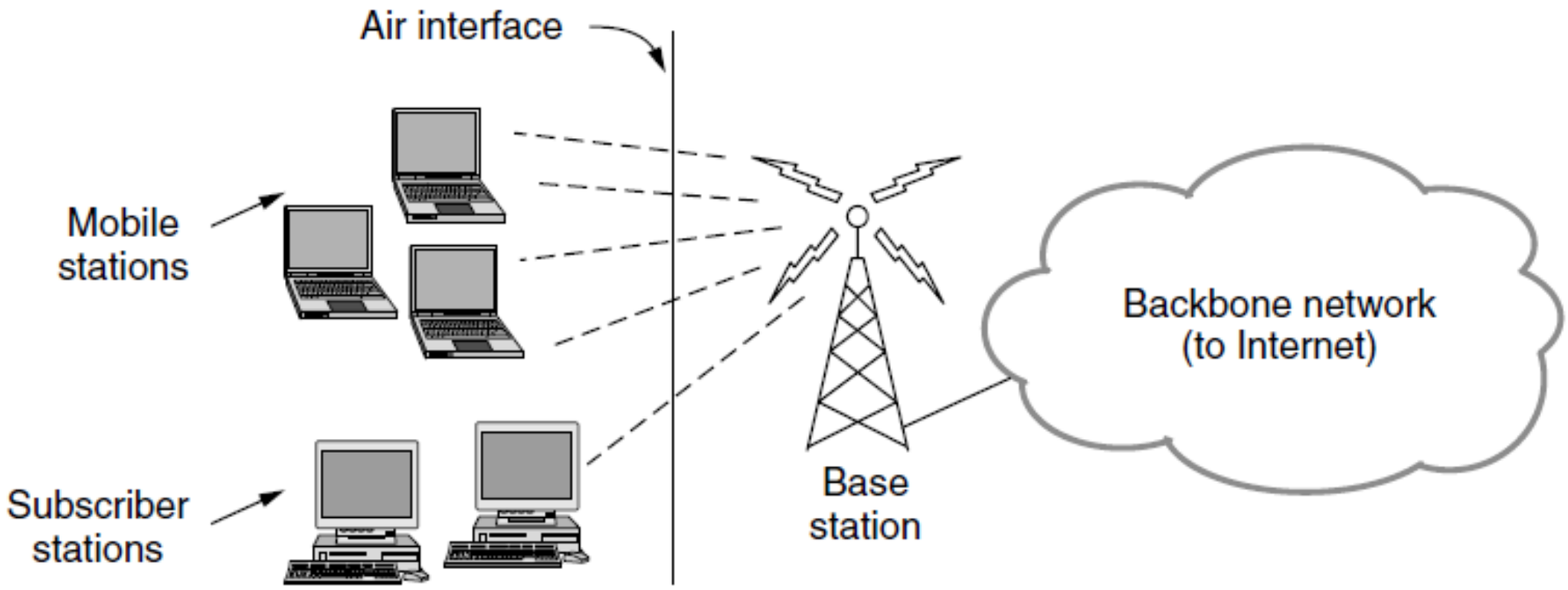
- Data delivery:
  - Not guaranteed (like in Ethernet)
- Security:
  - Use AES
  - Quality of Service Scheduling
  - Transmit power control: for regulatory compliance
  - Dynamic frequency selection: to avoid using frequencies in the 5-Ghz band that are used for radar in the proximity

WiMax

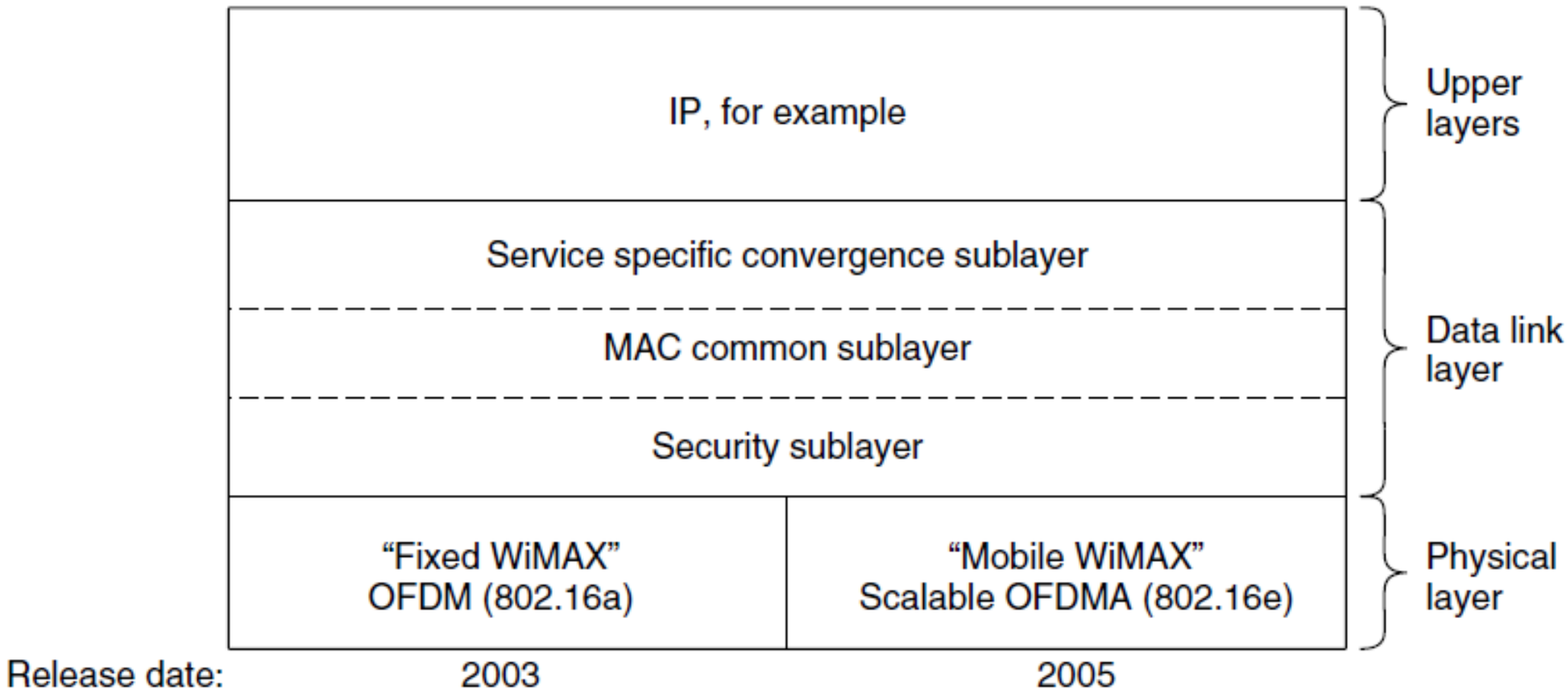
802.16 WiMAX

- Broadband wireless
  - A.k.a. Worldwide Interoperability for Microwave Access
- Works in licensed frequency space
  - Combines aspects of 4G and 802.11

802.16 Architecture

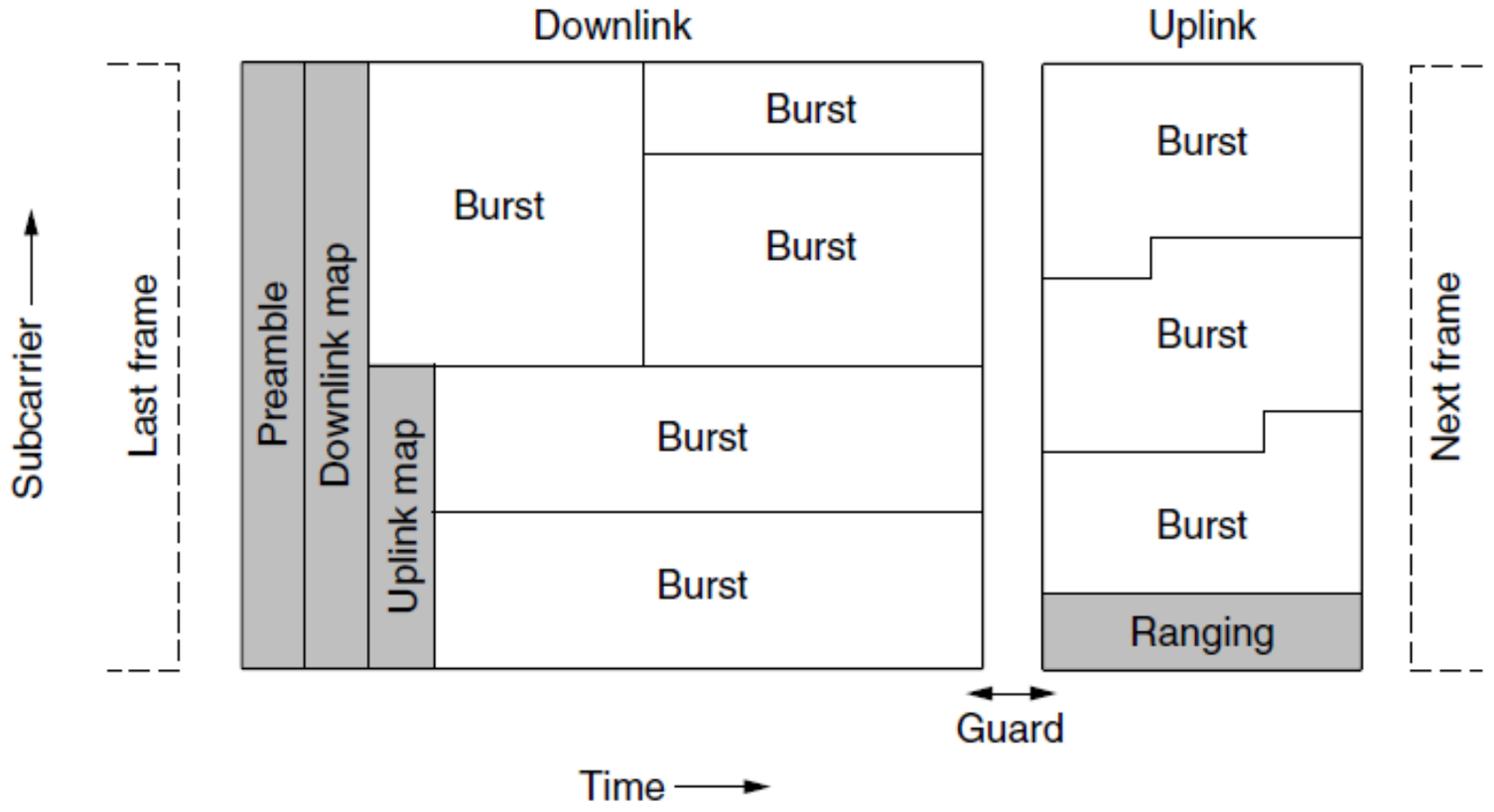


802.16 Protocol Stack



802.16 Physical Layer

- Uses OFDM
- Base stations give mobiles bursts for uplink and downlink
  - Bursts are for different stations
  - Layout in the preamble

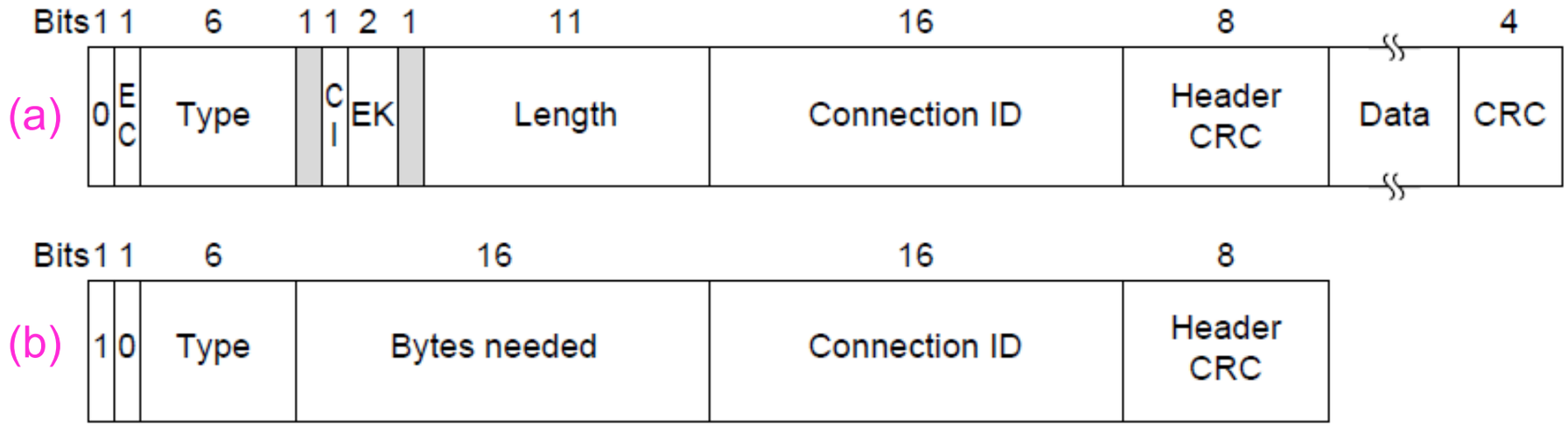


802.16 MAC

- Connection oriented service controlled by base station
  - Clients request the bandwidth they need
  - Clients request kind of service:
    - Constant bit rate, e.g., uncompressed voice
    - Real-time variable bit rate, e.g., video, Web
    - Non-real-time variable bit rate, e.g., file download
    - Best-effort for everything else

802.16 Frame Structure

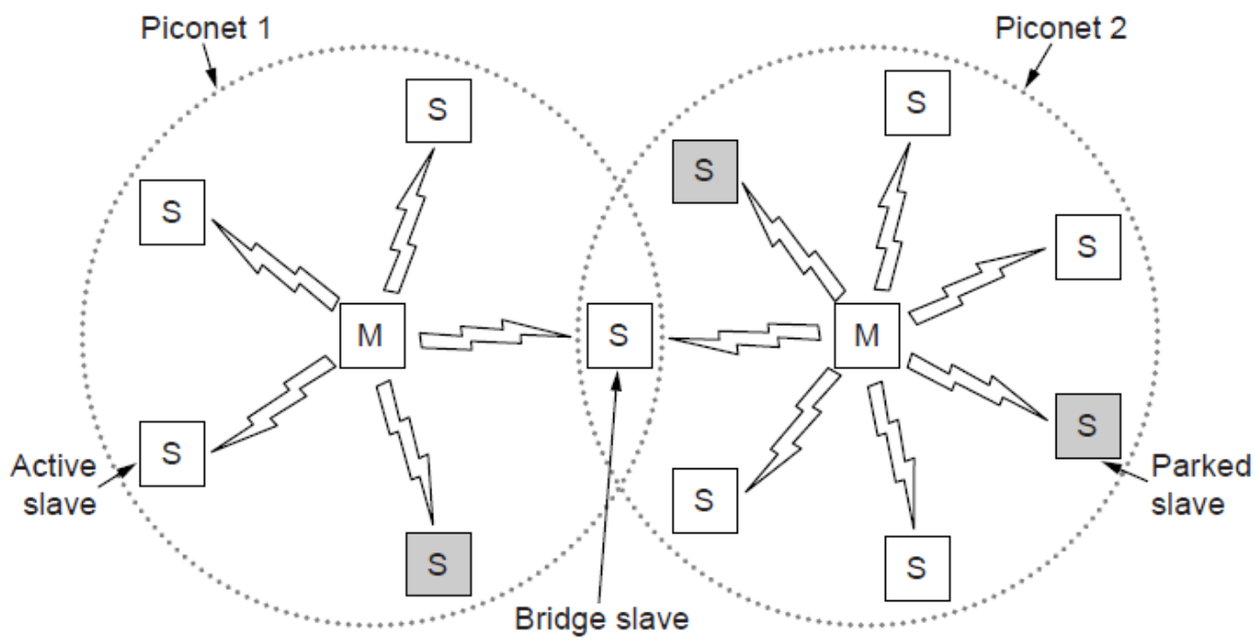
- Many different frame formats



(a) A generic frame. (b) A bandwidth request frame

Bluetooth

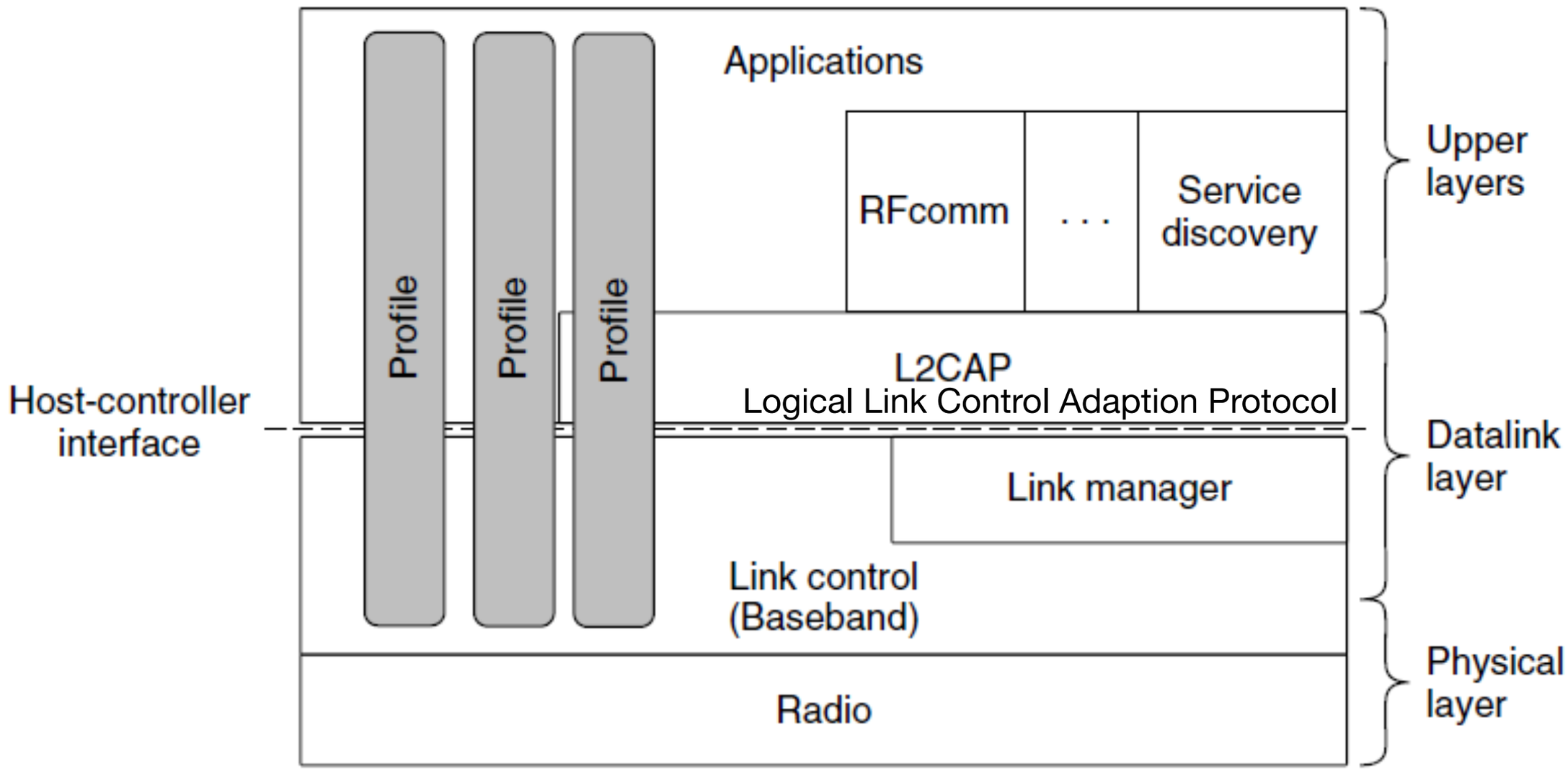
- 1994 Ericsson wants to connect cell phones to laptops without cables
  - Devices find and connect to each other (**pairing**)
  - Establish master-slave relationships
  - Basic unit is a piconet that forms a scatternet via bridges



Bluetooth

- Bluetooth SIG defines 25 different applications
  - Called profiles
    - E.g.: Intercom (two phones used as walkie-talkies), headset, hands-free (while driving a car), streaming audio/video, camera - computer/phone, remote TV control, …
- Protocol stack does NOT use OSI, TCP/IP, 802 model

Bluetooth Protocol Stack



Bluetooth Protocol

- Physical layer — (same as for OSI)
  - Radio transmission and modulation
  - Uses adaptive frequency hopping in the 2.4 GHz band
    - Learns if wifi uses frequencies and avoids them
- Link Layer
  - TDM with 625 µsec time slots for master and slaves
    - E.g.: Used alternatively by master and by one of the slaves
  - Frames can be 1, 3, or 5 slots long
  - Each frame has an overhead of 126b (access code & header)
  - Needs settling time of 250 - 260 µsec between hops
  - Link manager protocol sets up *links* between devices

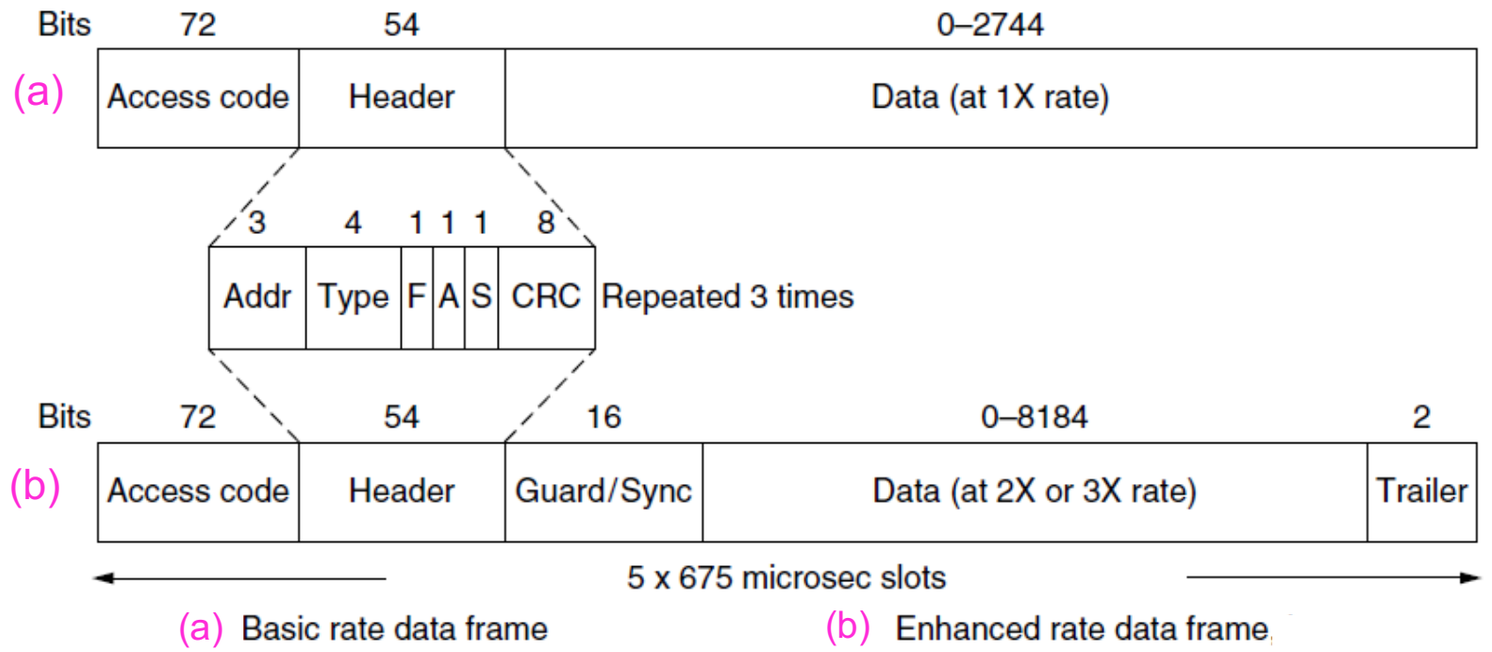
Bluetooth Protocol

- Bluetooth pairing
  - Old pairing: both devices configured with the same PIN
  - **Secure Simple Pairing**:
    - Both devices are using the same passkey
    - Observe passkey on one device and enter it on the other

Bluetooth Link Manager

- After pairing
  - Link manager sets up links
    - Synchronous Connection Oriented (SCO) link
      - Allocates a fixed slot in each direction
      - A slave can have up to three SCO links with its master
      - SCO link can transmit one 64Kb PCM audio channel
      - Frames are never retransmitted
    - Asynchronous ConnectionLess (ACL) link
      - for packet-switched data
      - Uses L2CAP layer:
        - Takes packets of <= 64KB from upper layer and breaks them into frames
        - Handles multiplexing and demultiplexing multiple packet sources
        - Handles error control and retransmission
        - Enforces quality of service

Bluetooth Frames



(a) Basic rate data frame (b) Enhanced rate data frame

- Addresses are only 3 bits
- Type is the frame type (ACL, SCO, poll, null), error correction, and the number of slots
- Flow bit: set if a slave can not receive any more data
- Acknowledgement bit to piggyback acks into frame
- Sequence bits to number frames to detect retransmissions

Bluetooth Capacity

- Slave uses odd slots: 800 slots per second
- 80b payload —> 64Kbps: enough for a PCM voice channel
- Raw bandwidth is 1Mbps
  - 13% efficiency
  - 41% is settling time
  - 20% on headers
  - 26% on repetition coding

Bluetooth 5

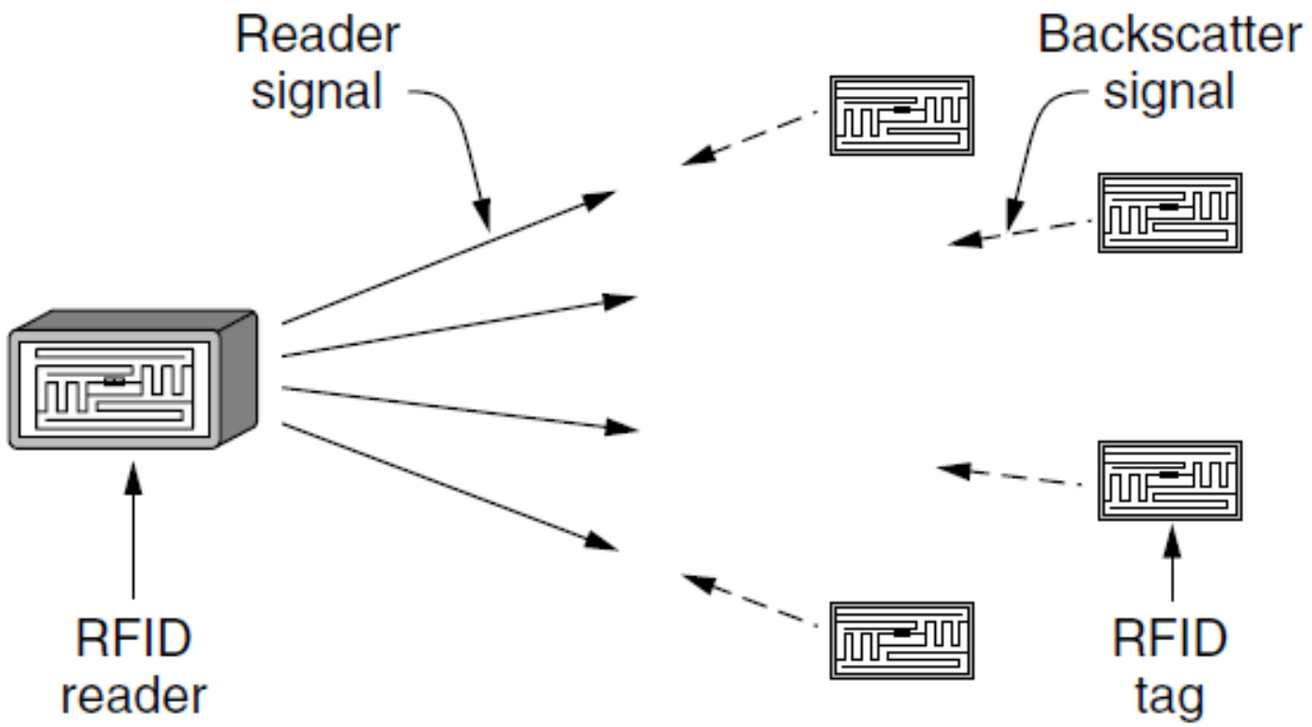
- Support of Internet of Things
- Speed increases from 1Mbps to 2Mbps
- Message size is now 255B
- Indoor range is now 40m
- Power requirements are slightly reduced
- Range of beacons has gone up slightly
- Slightly better security

RFID

Radio Frequency IDentification

- Developed for Electronic Product Code (MIT 1999)
  - Replacement for a barcode
    - Readable from 10m
  - EPCglobal (2003) commercialized RFID technology
  - Now in second generation EPC Gen 2

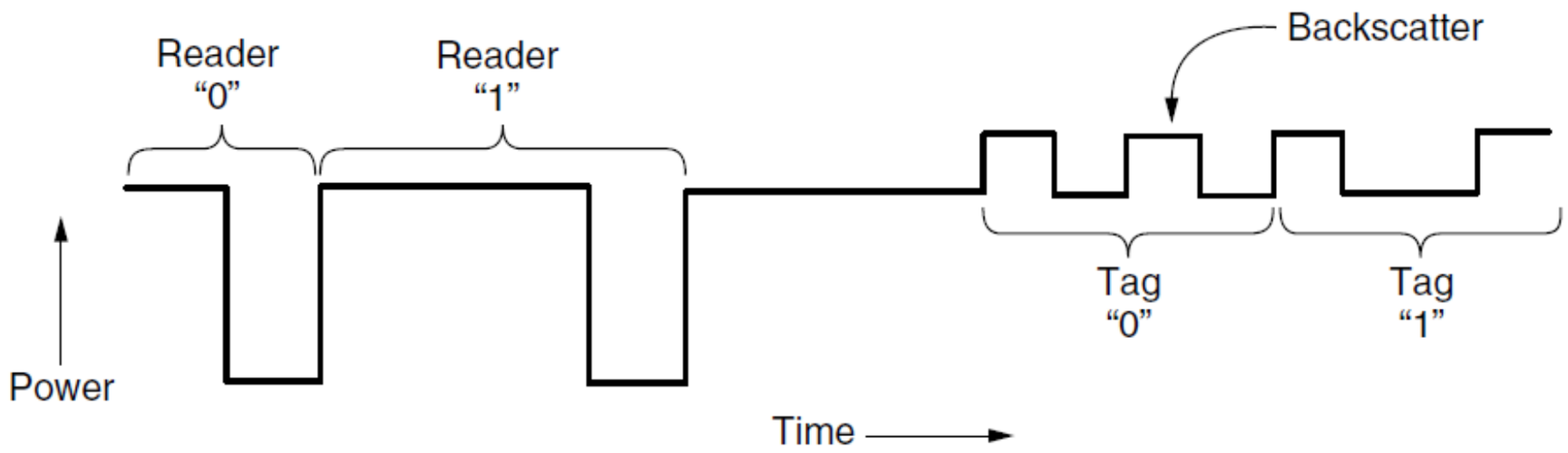
RFID EPCGen2 Architecture



RFID EPC Gen2

- Reader is always transmitting a signal
  - Tags do not have power and use the reader signal to power them
  - If reader is transmitting a fixed carrier signal, then tags can send data: **Backscatter**
  - Reader needs to filter out the outgoing signal
  - Modulation is very simple, 0 and 1 have different timings

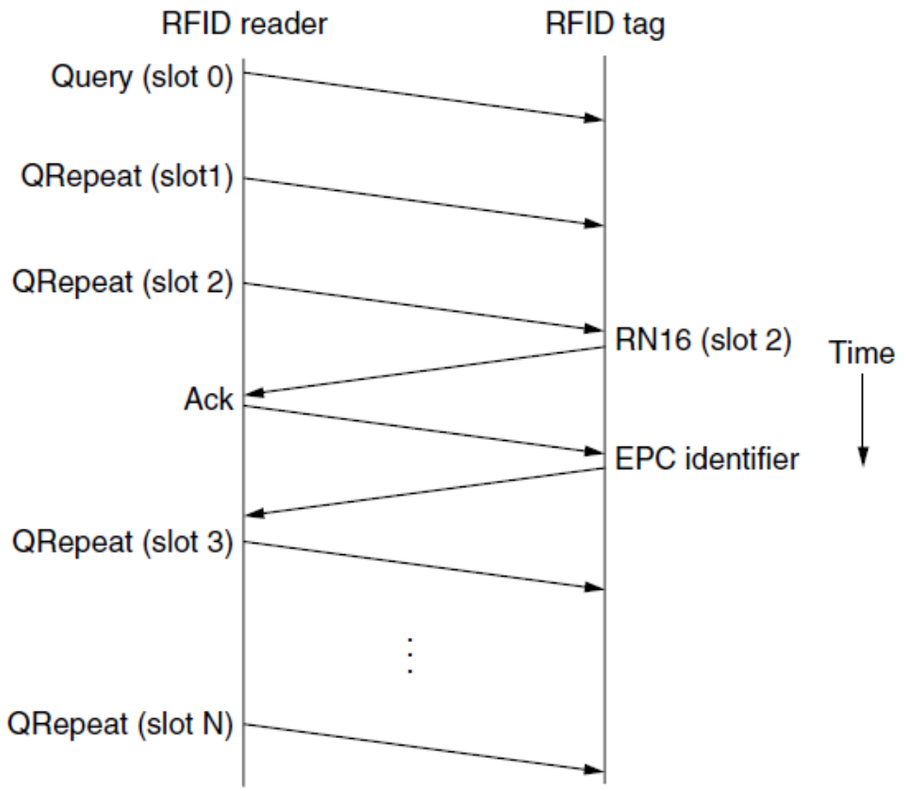
RFID reader and backscatter signal



RFID Gen 2
Tag Identification Layer

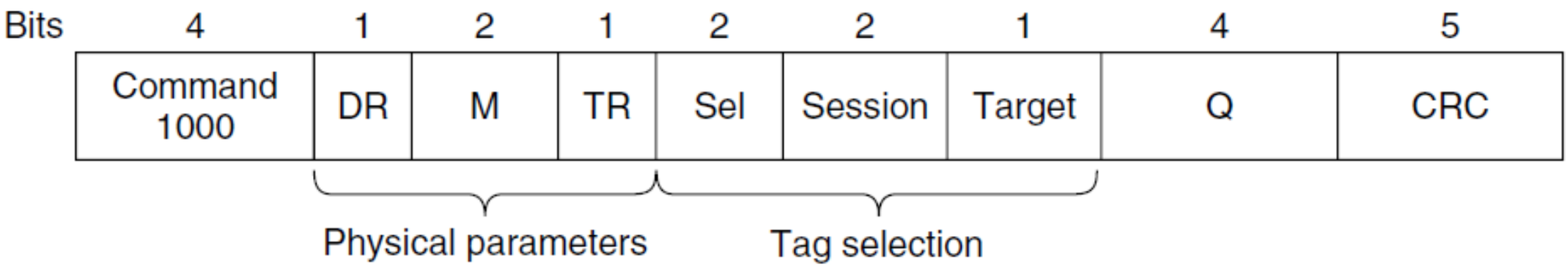
- Tags do not know each other
- Tags use slotted Aloha to communicate

- Reader sends query and sets slot structure
- Tags reply in a random slot with a random 16b number
- If there is no collision, reader sends an ACK message
- Tag sends its EPC identifier
- Tag then stops to queries for a while to give other tags a chance
- Reader uses binary exponential to set number of slots in a QAdjust message



RFID

- Readers can perform other operations on tags
- Messages need to be compact as downlink rates are 27kbps / 128 kbps
- Q defines the range of slots 0 — 2^Q-1
- (Tag to reader messages are more simple)

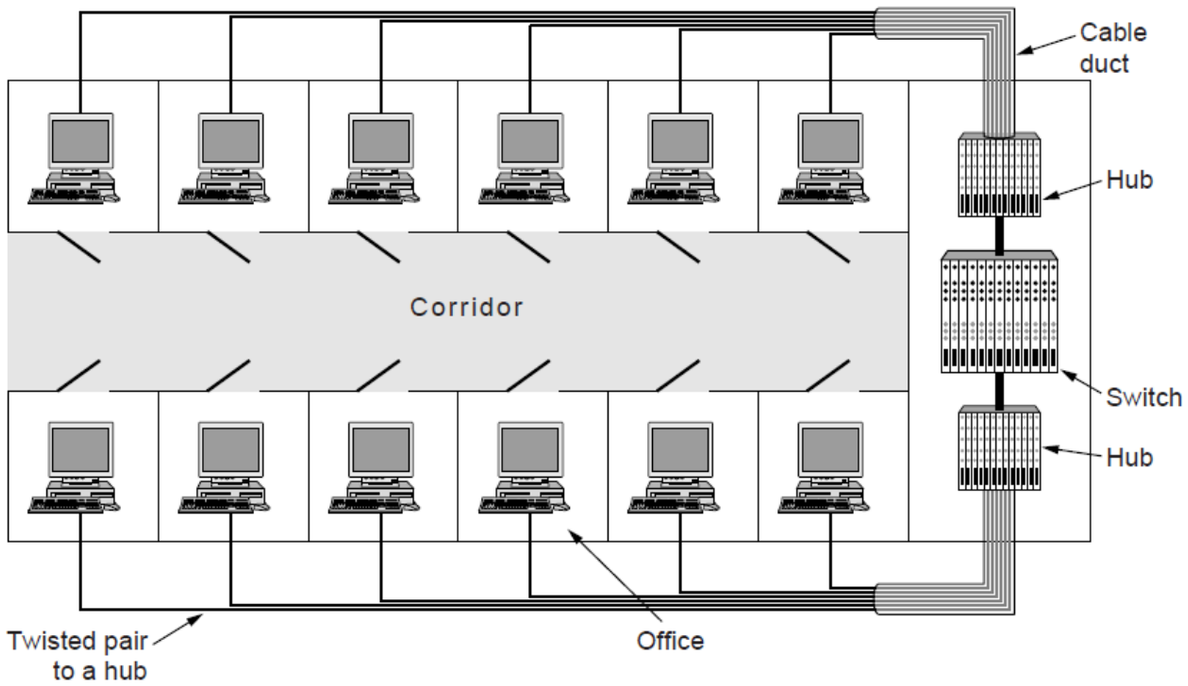


Data Link Layer Switching

Bridges

- How to make bigger LANs
  - Bridges (= Ethernet switches) run at data link layer
    - Use MAC addresses
  - Routers run at network layer
    - Use IP addresses
- Bridges can be used
  - to combine physical LANs into a single logical LAN
  - to separate the same physical LAN into multiple logical LANs (VLANs)

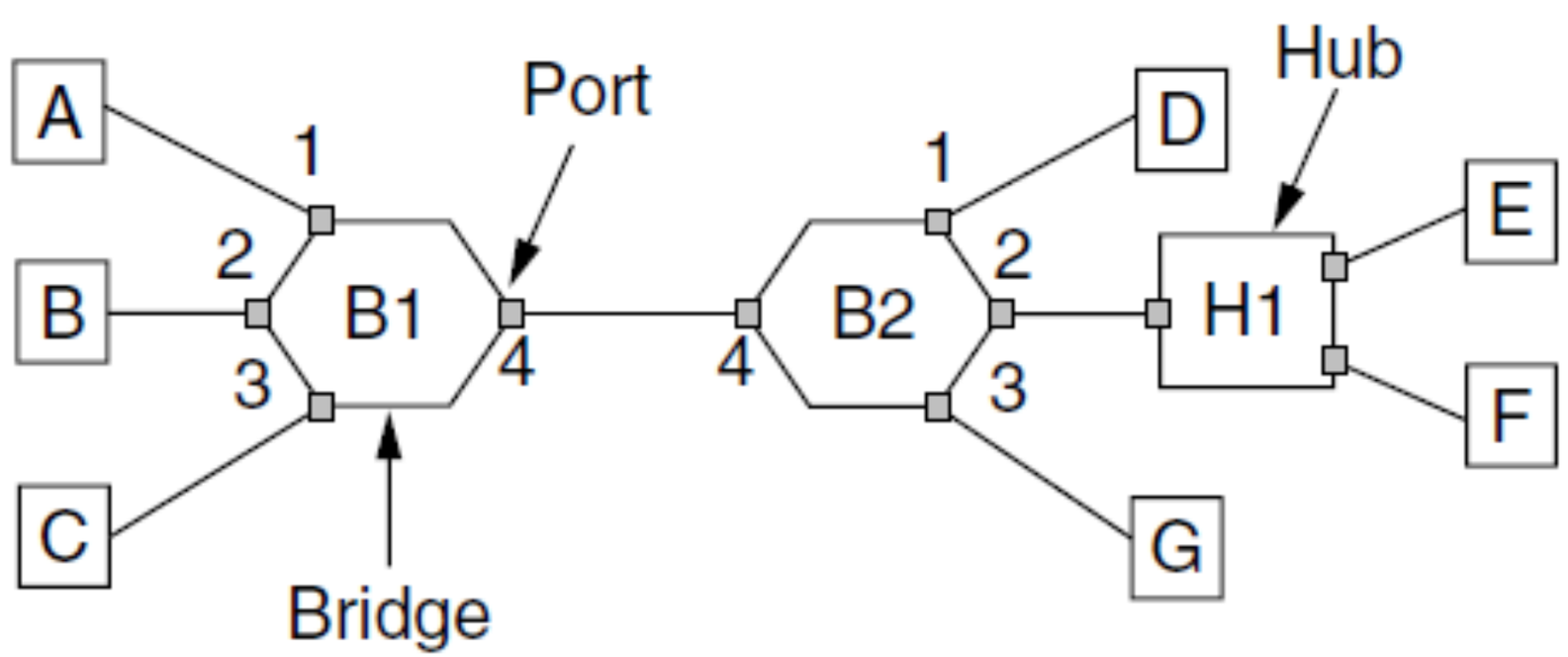
Bridges



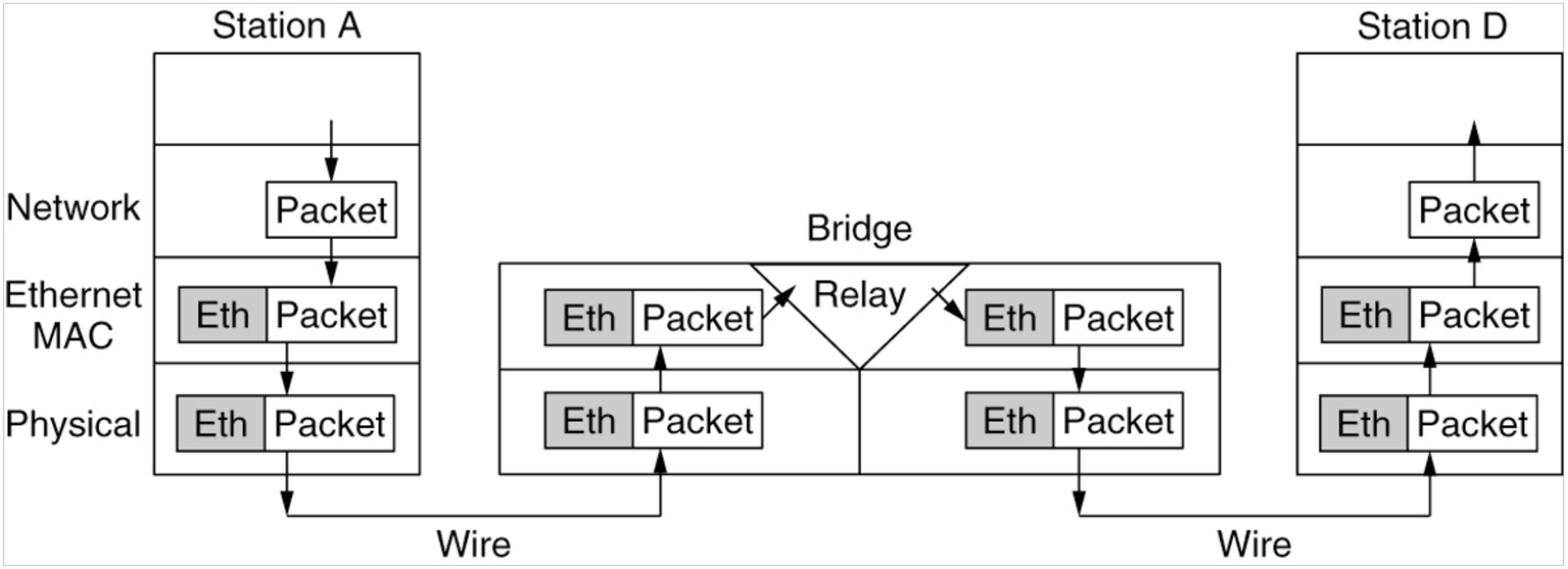
Bridges allow to generate a single LAN over a larger geographical area with many more nodes than a single LAN can handle

Bridges

- Computers, bridges, and hubs connects to the ports of a bridge



Bridges



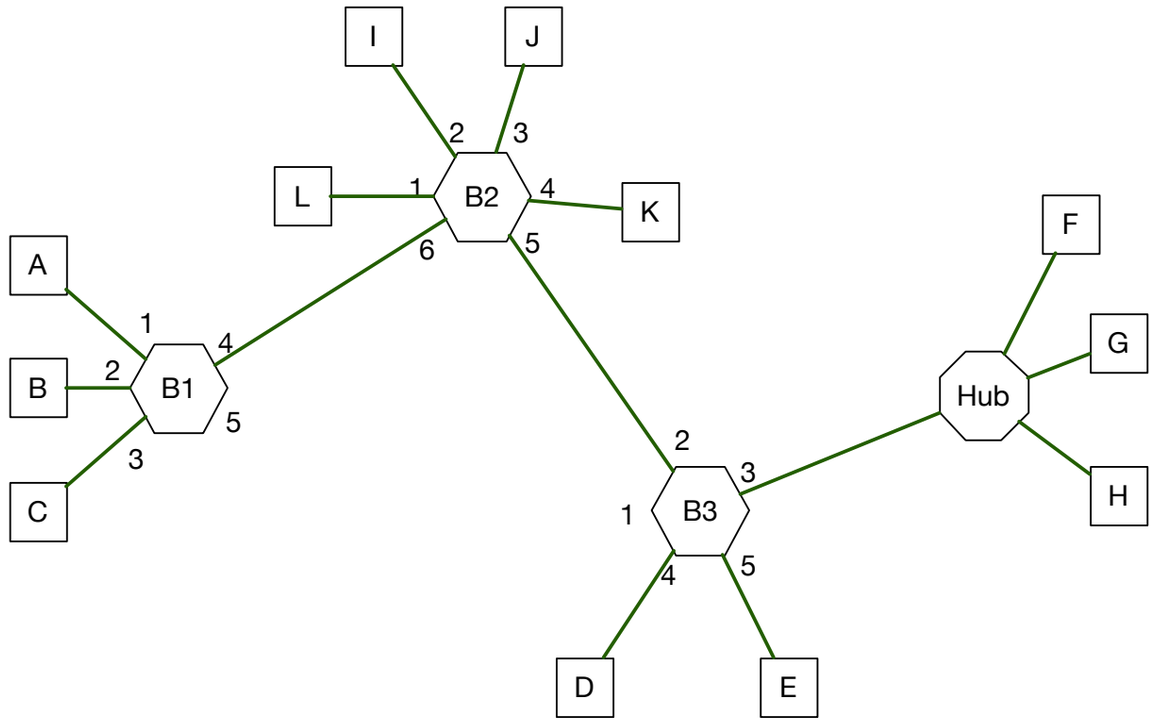
Protocol processing at a bridge

Bridges

- Bridges can be transparent to the user
  - Backward learning algorithm to stop unneeded traffic
  - Spanning tree algorithm to break loops

Bridges

- Backward learning bridges
  - Bridges operate in promiscuous mode
    - Accept all frames that they see
    - Use destination address to forward to selected ports
      - Using a big hash table for the look-up
  - Originally, all bridges use flooding
    - Send frames to all ports
  - Use source addresses in order to determine which ports lead to given addresses
  - To accomodate dynamism:
    - Purge old hash table entries.



- A to K:
    - B1 sends out to ports 2, 3, 4, 5; sets entry A<—>1
    - B2 sends out to ports 1, 2, 3, 4, 5; sets entry A <—>6
    - B3 sends out to ports 3, 4, 5; sets entry A <—>1
- K responds to A
    - B2 sends to port 6; sets entry K <—>4
    - B1 sends to port 1; sets entry K<—>4

Bridges

Forwarding rules for bridges

If the port for the destination address is the same as the source port, discard the frame.

(Can happen with hubs that forward to all their ports)

Else: look up the hash table.

If entry is found:

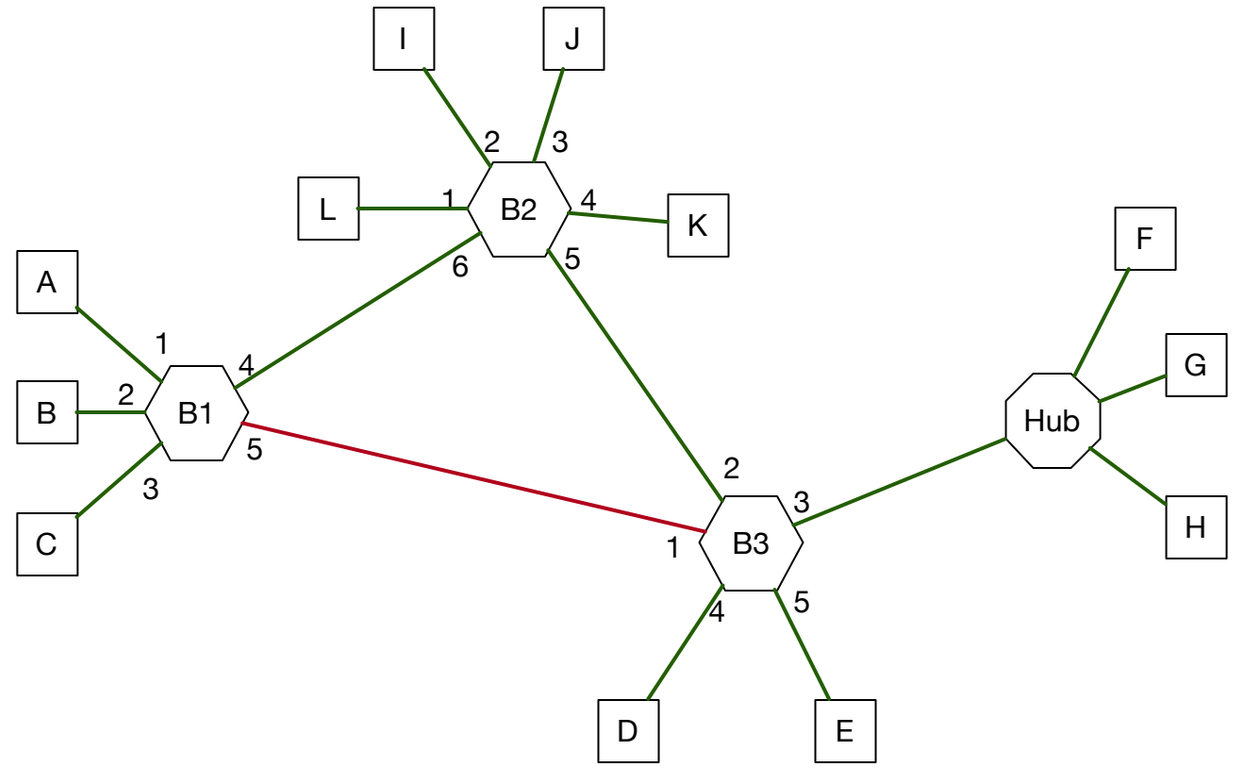
Forward on that port

Else:

Forward to all ports

Bridges

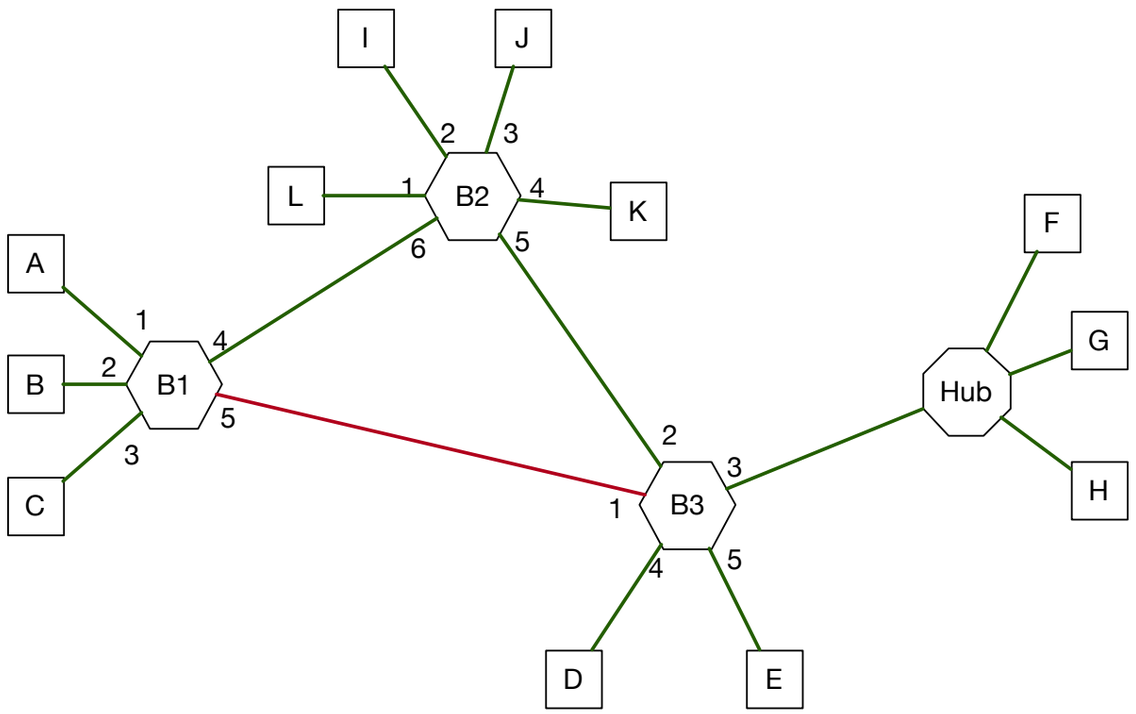
- Why are loops bad?



What happens if A sends to K?

Bridges

- Answer:
  - B3 receives the same frame from B1 and B2
  - Forwards the same frame to B2 and B1
  - Receives the frame again and forwards them again, …



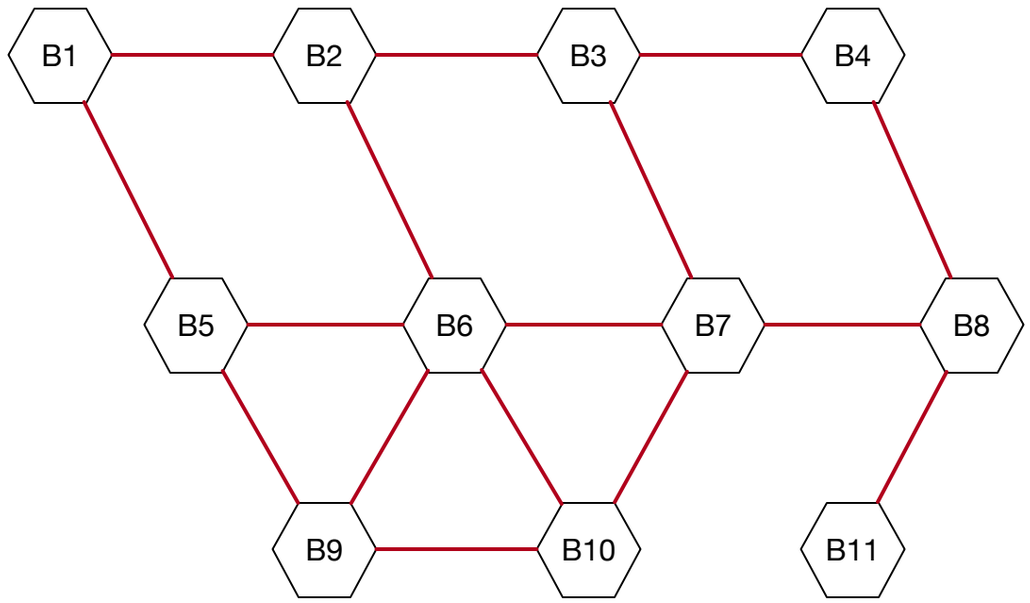
Bridges

- Redundant links are good for reliability, but cause havoc with flooding
  - Use an overlay network: A spanning tree
    - All bridges are part of the spanning tree
    - There is only one path between bridges

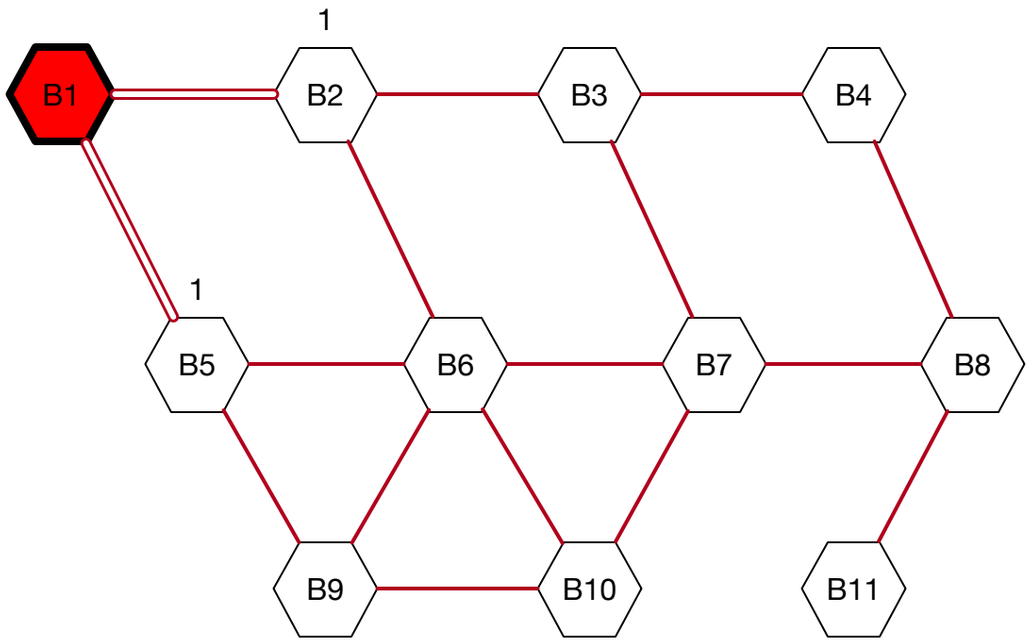
Bridges

- Distributed spanning tree algorithm:
  - All bridges have an id
    - The one with the lowest id becomes the root of the tree
      - How do you figure out that you are the root:
        - Everybody floods with ID message announcement
- Construct a tree of shortest distances
  - Break ties by using lowest outgoing ID

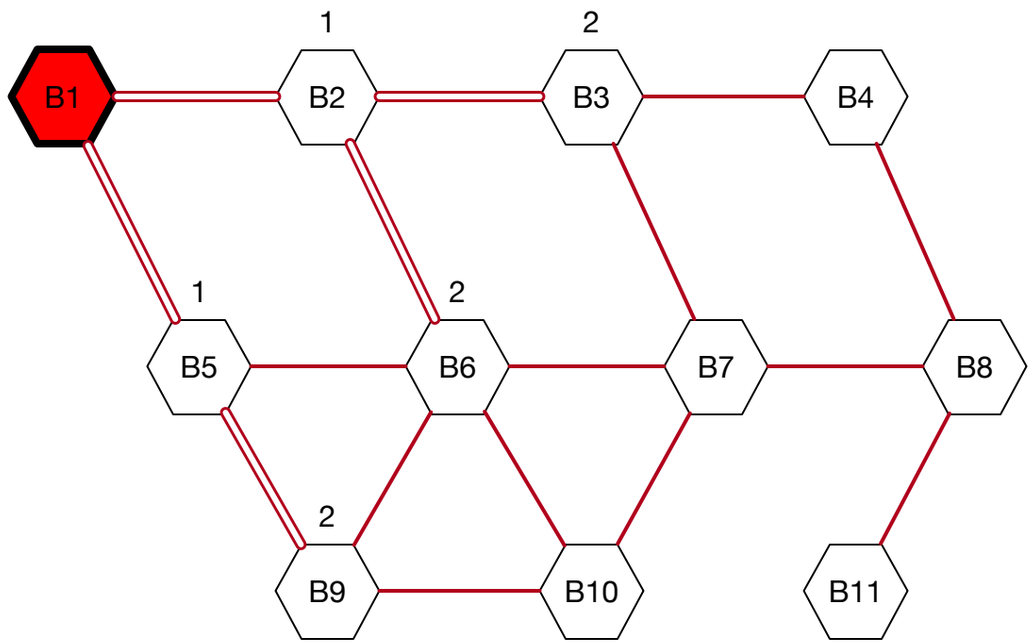
Bridges



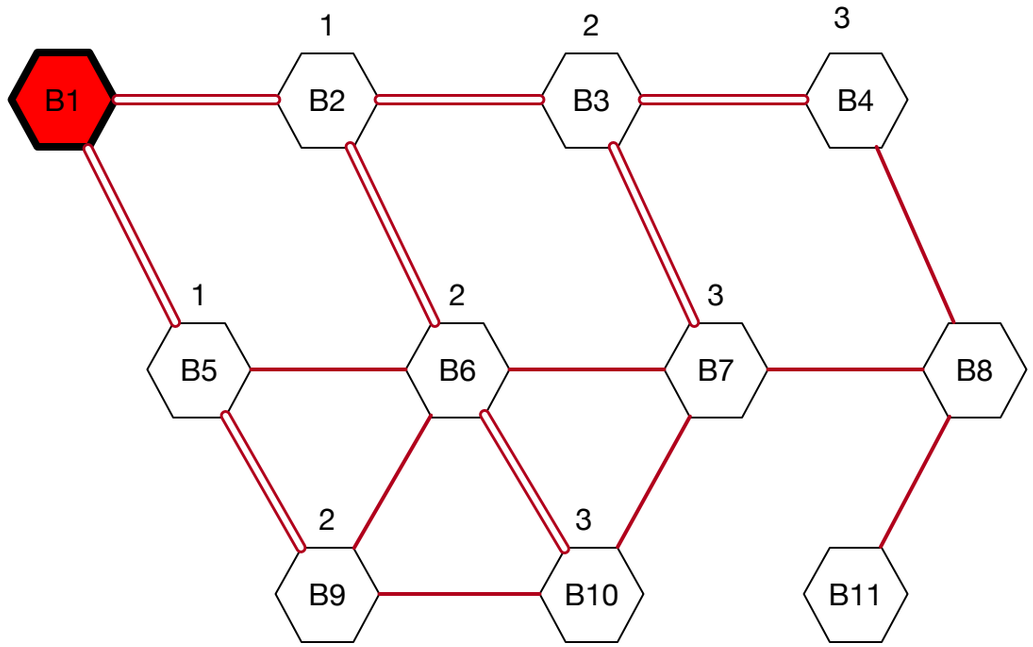
Bridges



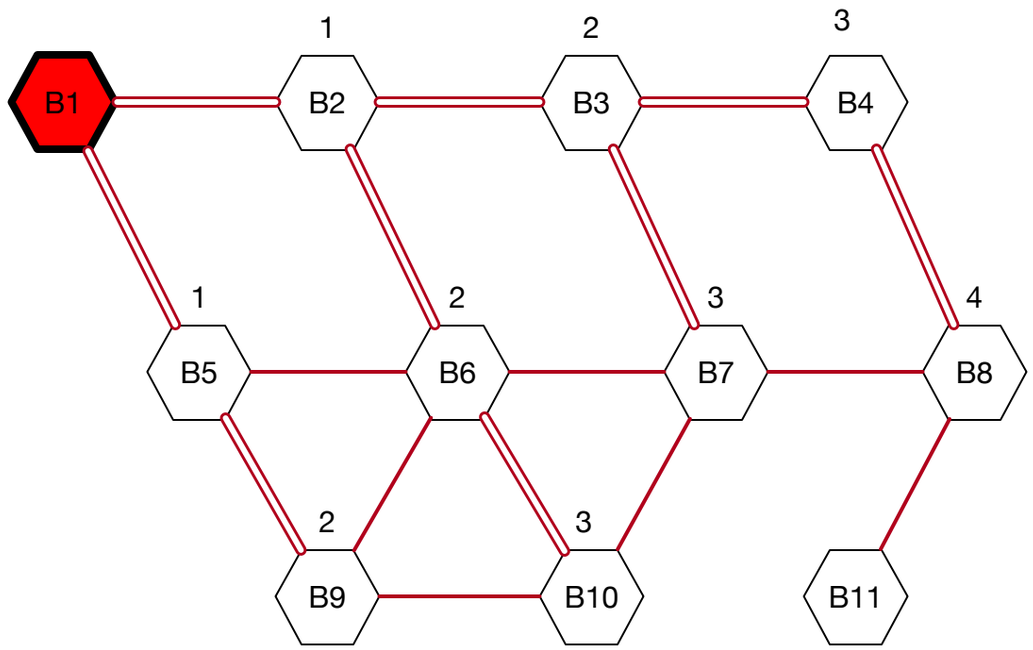
Bridges



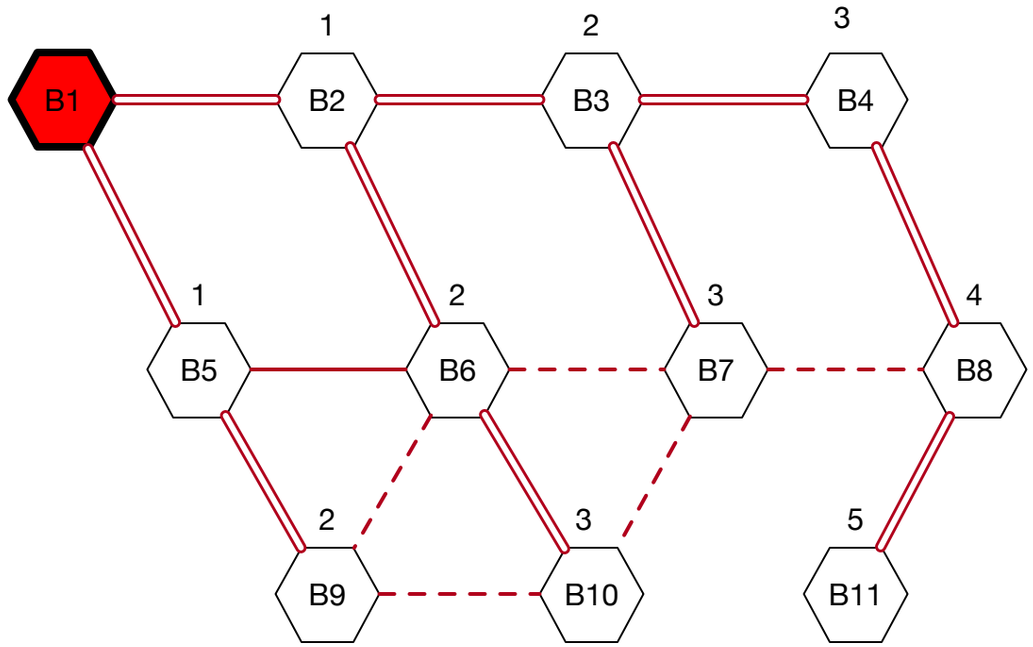
Bridges



Bridges



Bridges



Bridges

- Rule:
  - Root sends out a configure message
    - Those that receive it become the nodes at distance 1
      - Attach themselves to the root
  - Then they send out configure messages themselves
  - Those that receive these messages:
    - Become nodes at distance 2
    - Attach themselves through the node with the smallest ID

Bridges

- In order to be dynamic:
  - Trees rerun algorithm periodically
  - Standardized as IEEE 802.1D
  - Updated in 2001 to find a new spanning tree more quickly after a change in topology

I think that I shall never see

A graph more lovely than a tree.

A tree whose crucial property

Is loop-free connectivity.

A tree which must be sure to span.

So packets can reach every LAN.

First the Root must be selected

By ID it is elected.

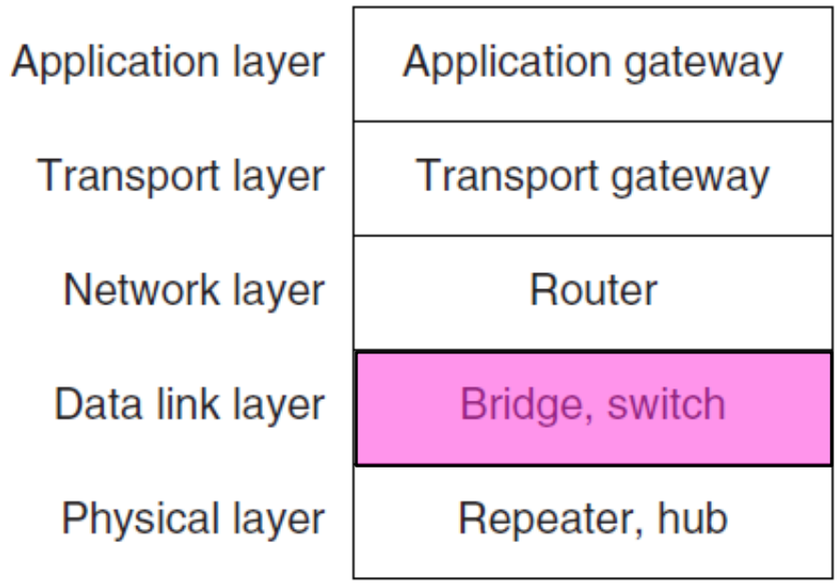
Least-cost paths from Root are traced

In the tree these paths are placed.

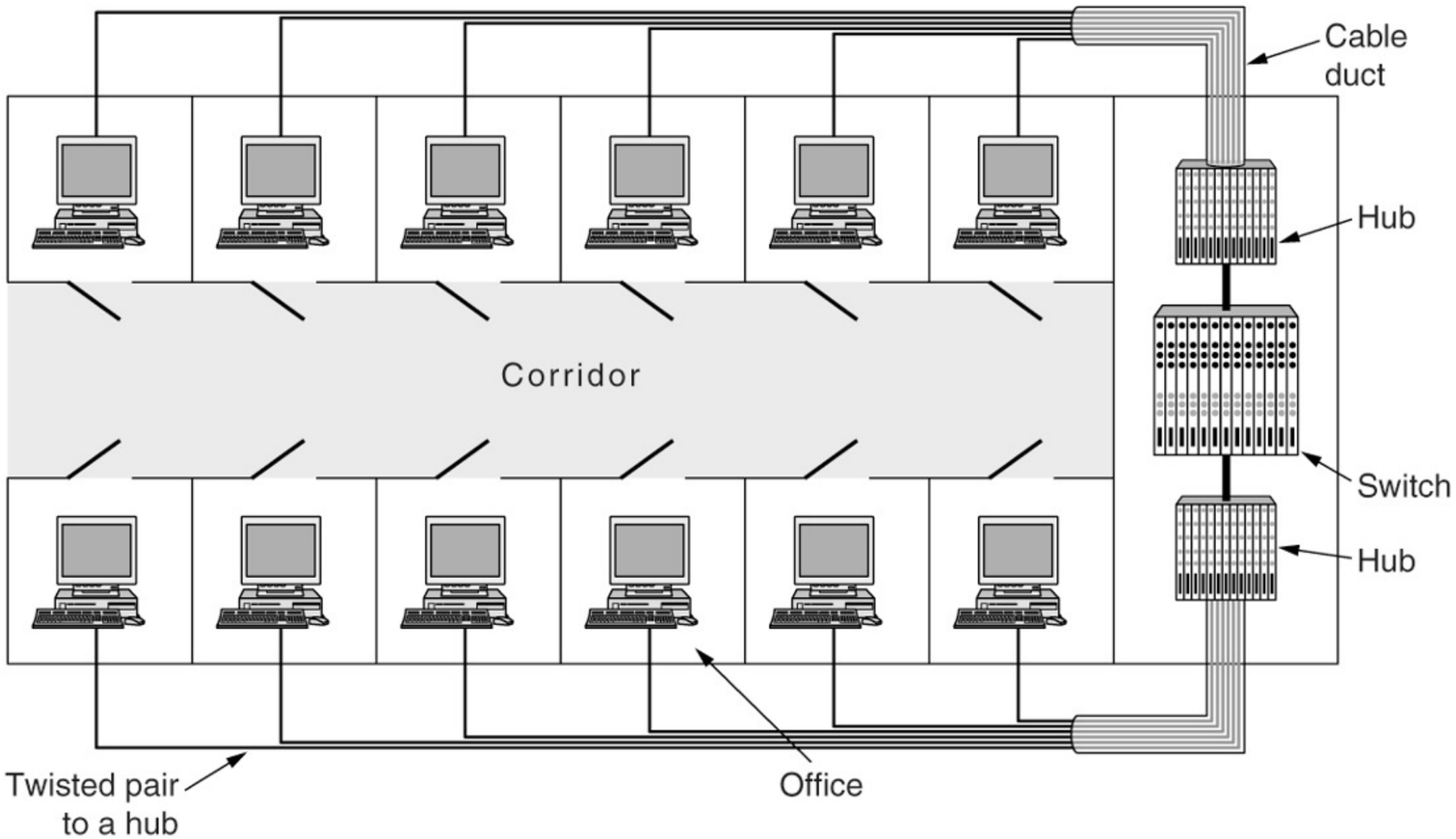
A mesh is made by folks like me

Then bridges find a spanning tree.

Repeaters, Hubs, Switches, Bridges, Routers, & Gateways

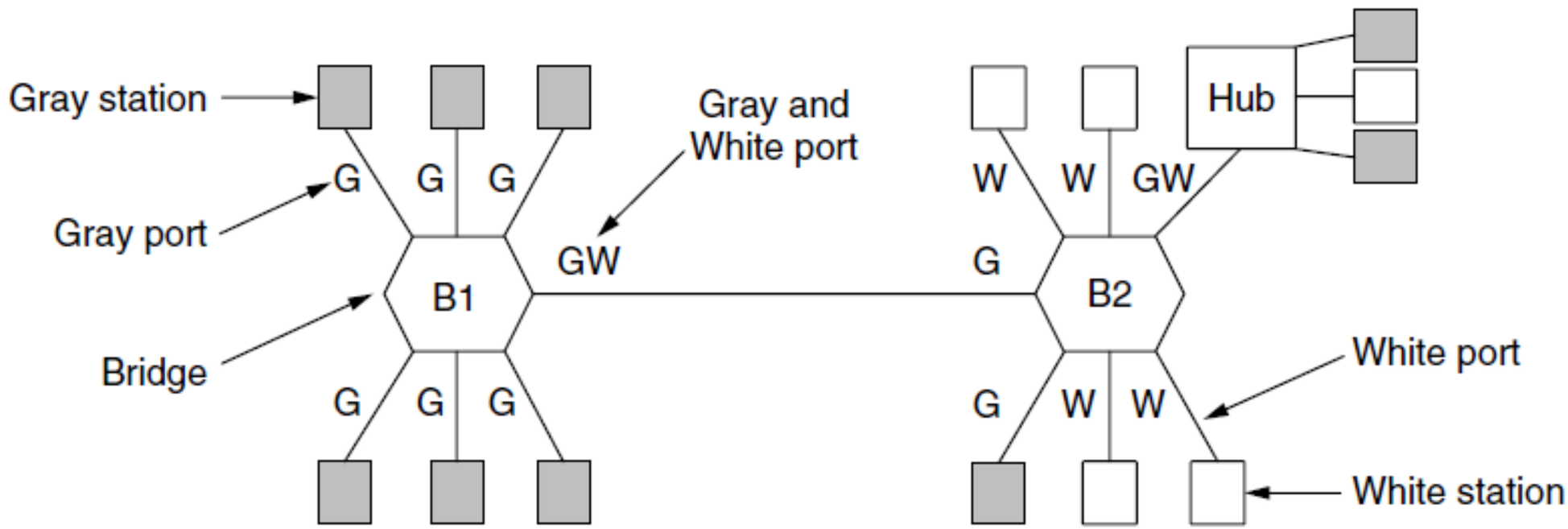


Virtual LAN


Cable duct
Hub
Corridor
Switch
Hub
Twisted pair to a hub
Office

Virtual LANs

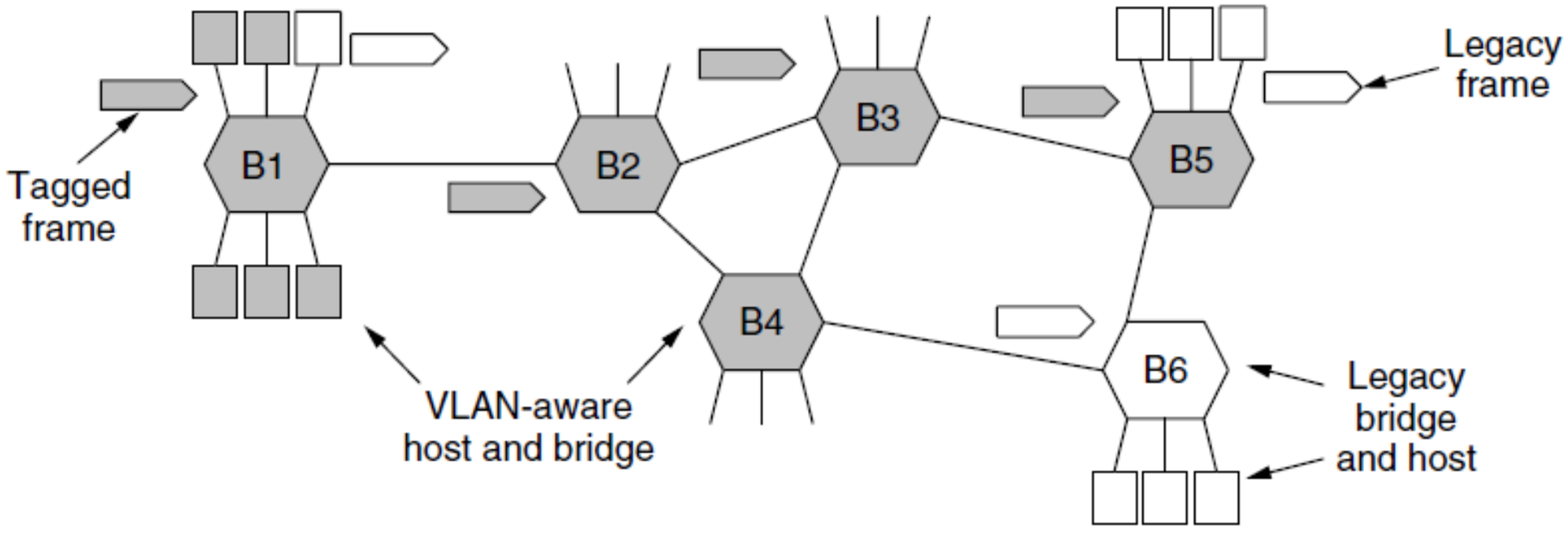
- Can be used to split one physical LAN into multiple logical LANs
  - Color ports according to VLAN



Two VLANs, gray and white, on a bridged LAN

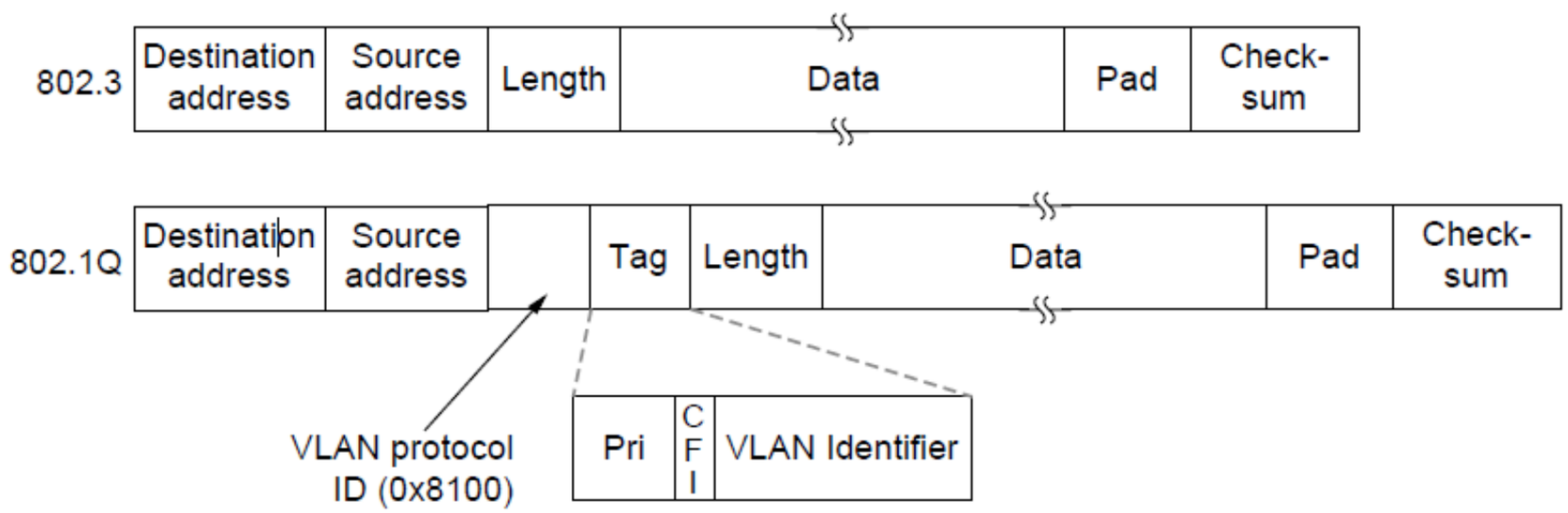
Virtual LANs

- IEEE 802.1Q
  - Make bridges aware of VLANs
  - Frames are tagged with their color
  - Legacy switches with no tags are supported

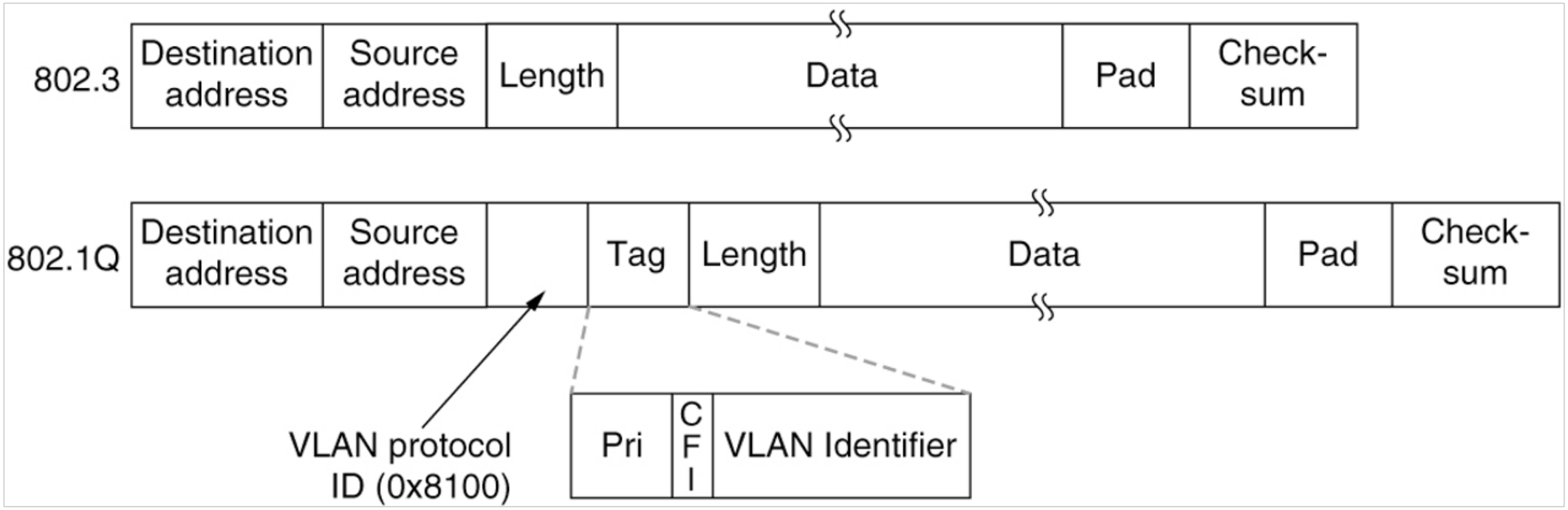


Virtual LANs

- 802.1Q frames carry a color tag (the VLAN identifier)
  - Length/Type value is 0x8100 for VLAN protocol



VLANs



The 802.3 (legacy) and 802.1Q Ethernet frame formats