Medium Access Control Sublayer

Chapter 4

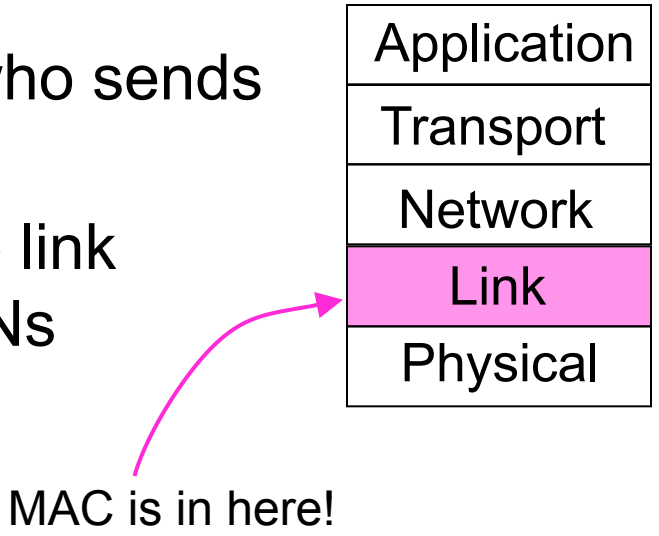
- Channel Allocation Problem
- Multiple Access Protocols
- Ethernet
- Wireless LANs
- Broadband Wireless
- Bluetooth
- RFID
- Data Link Layer Switching

Revised: August 2011

The MAC Sublayer

Responsible for deciding who sends next on a multi-access link

- An important part of the link layer, especially for LANs



Channel Allocation Problem (1)

For fixed channel and traffic from N users

- Divide up bandwidth using FTM, TDM, CDMA, etc.
- This is a static allocation, e.g., FM radio

This static allocation performs poorly for bursty traffic

- Allocation to a user will sometimes go unused

Channel Allocation Problem (2)

Dynamic allocation gives the channel to a user when they need it. Potentially N times as efficient for N users.

Schemes vary with assumptions:

Assumption	**Implication**
Independent traffic	Often not a good model, but permits analysis
Single channel	No external way to coordinate senders
Observable collisions	Needed for reliability; mechanisms vary
Continuous or slotted time	Slotting may improve performance
Carrier sense	Can improve performance if available

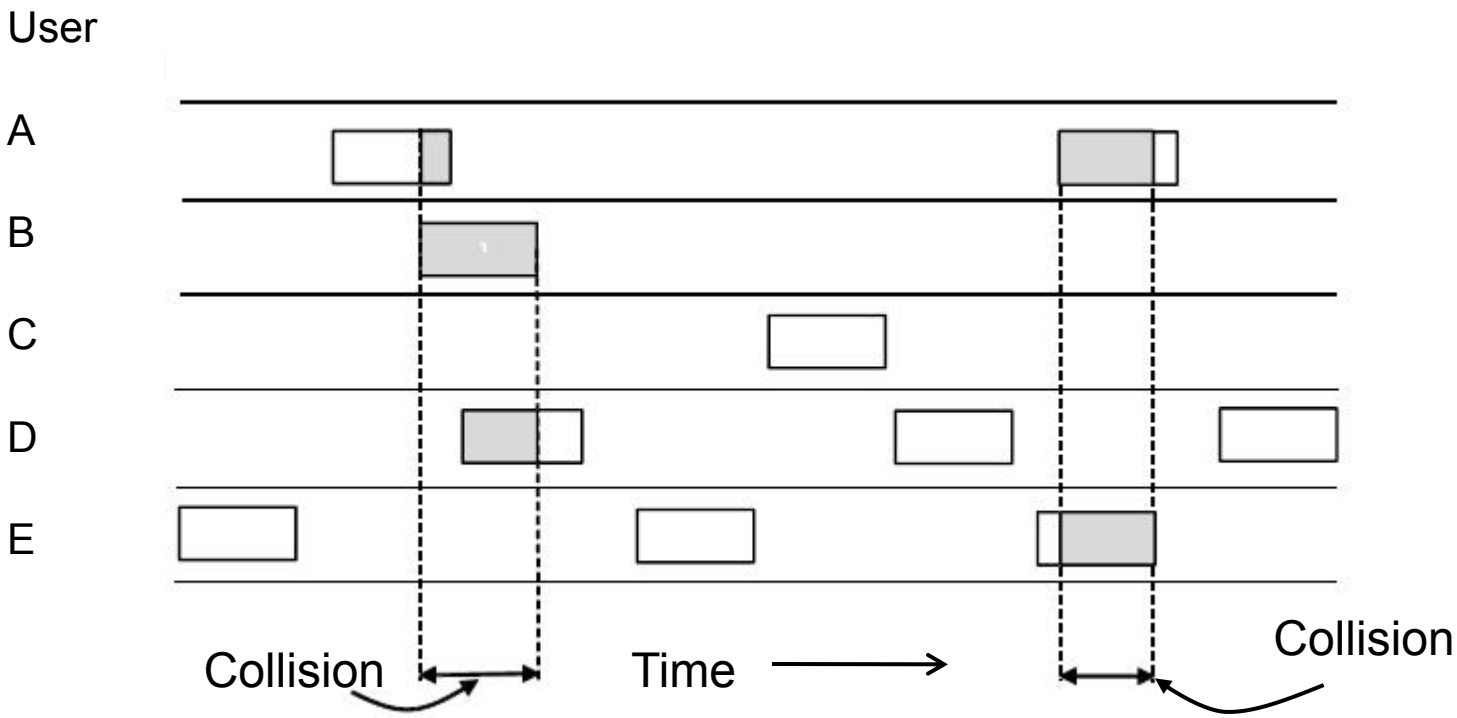
Multiple Access Protocols

- ALOHA »
- CSMA (Carrier Sense Multiple Access) »
- Collision-free protocols »
- Limited-contention protocols »
- Wireless LAN protocols »

ALOHA (1)

In pure ALOHA, users transmit frames whenever they have data; users retry after a random time for collisions

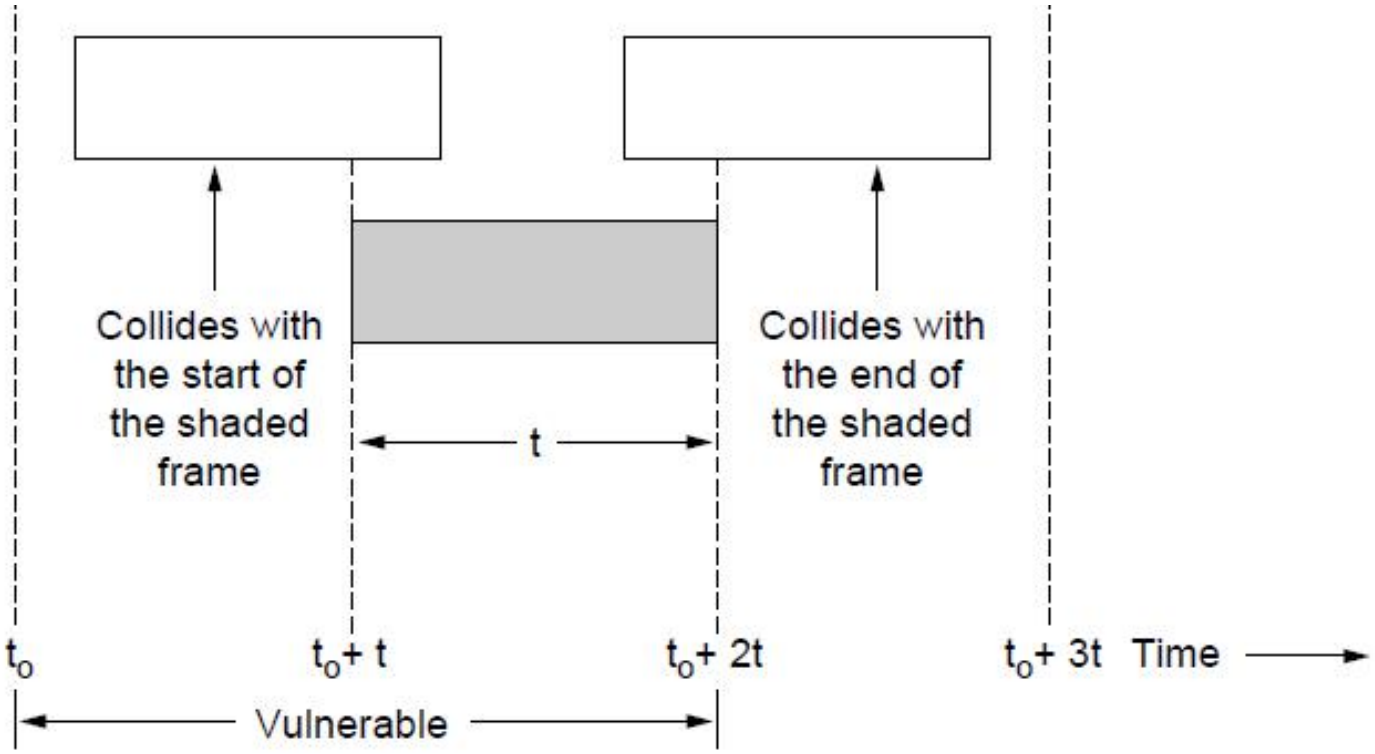
- Efficient and low-delay under low load



ALOHA (2)

Collisions happen when other users transmit during a vulnerable period that is twice the frame time

- Synchronizing senders to slots can reduce collisions



ALOHA (3)

- Efficiency of ALOHA
- frametime – time needed to transmit standard sized frame
- N – New frames per frame time by poison distribution
- If N>1, nearly every frame will suffer a collision. 0<N<1 expected for reasonable throughput
- G – mean number of frames/frametime including retransmissions. Clearly, G ≥ N.
- At low load (i.e.,N~ 0), there will be few collisions, hence few retransmissions, so G≈N
- At high load G>N
- Throughput S is G x probability P_0 of successful transmission
- $S = G P_0$

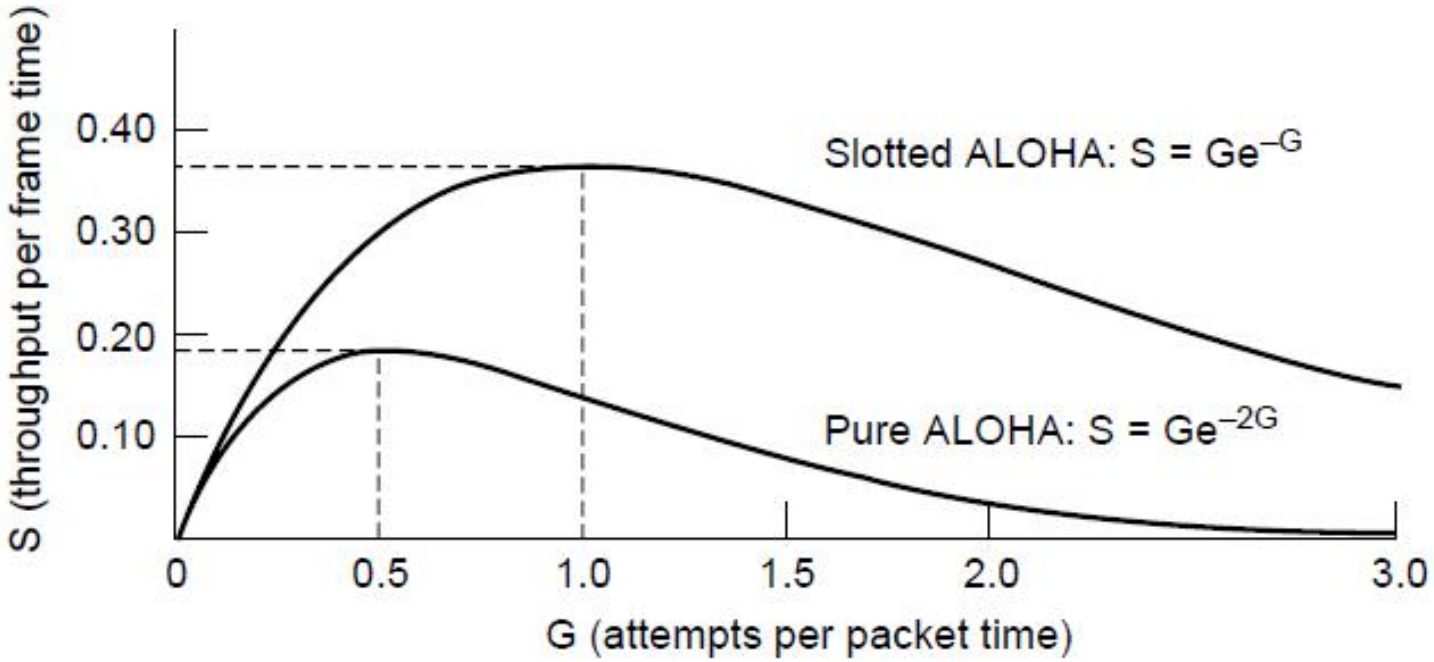
ALOHA (4)

- The probability that k frames are generated during a given frame time in which G frame were expected, is given by the Poisson distribution $\Pr[k] = \frac{G^k e^{-G}}{k!}$
- So probability of no frame is e^{-G}
- In an interval two frame times long, the mean number of frames generated is 2G. The probability of no frames being initiated during the entire vulnerable period is thus given by $P_0=e^{-2G}$. Using $S=GP_0$, we get $S=Ge^{-2G}$
- The maximum throughput occurs at G=0.5, with S=1/2e, which is about 0.184

ALOHA (5)

Slotted ALOHA is twice as efficient as pure ALOHA

- Low load wastes slots, high loads causes collisions
- Efficiency up to 1/e (37%) for random traffic models



CSMA (1)

CSMA improves on ALOHA by sensing the channel!

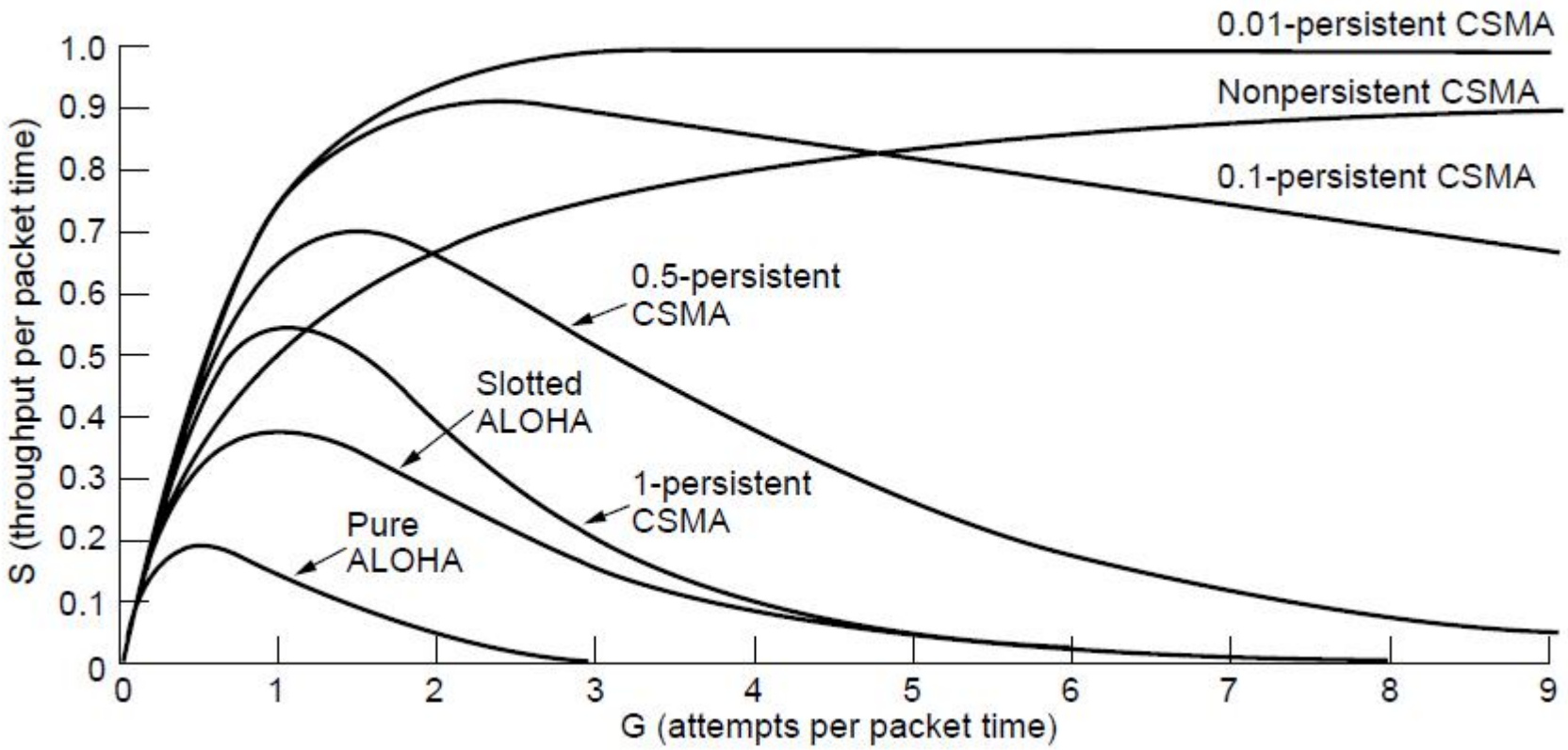
- User doesn't send if it senses someone else

Variations on what to do if the channel is busy:

- 1-persistent (greedy) sends as soon as idle
- Nonpersistent waits a random time then tries again
- p-persistent sends with probability p when idle

CSMA (2) – Persistence

CSMA outperforms ALOHA, and being less persistent is better under high load

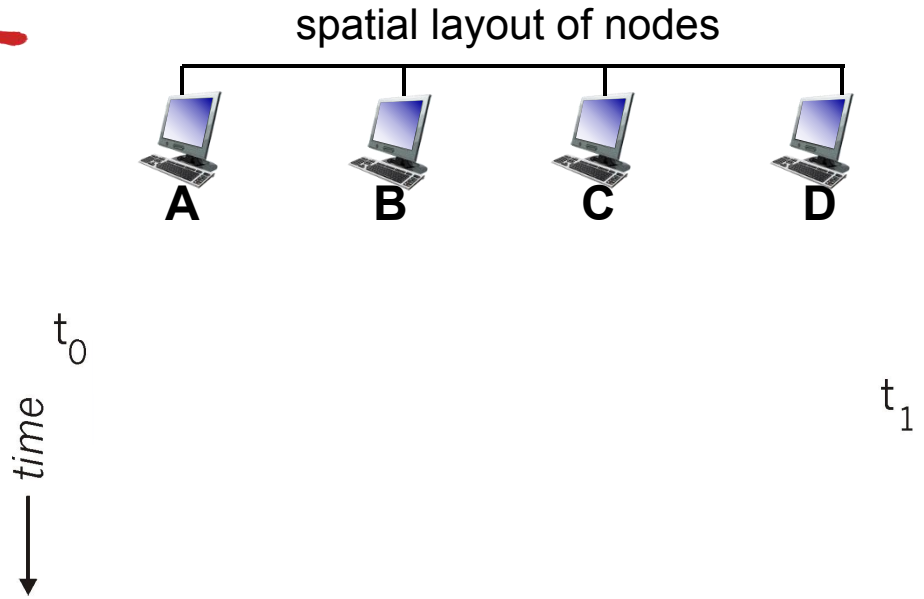


CSMA collisions

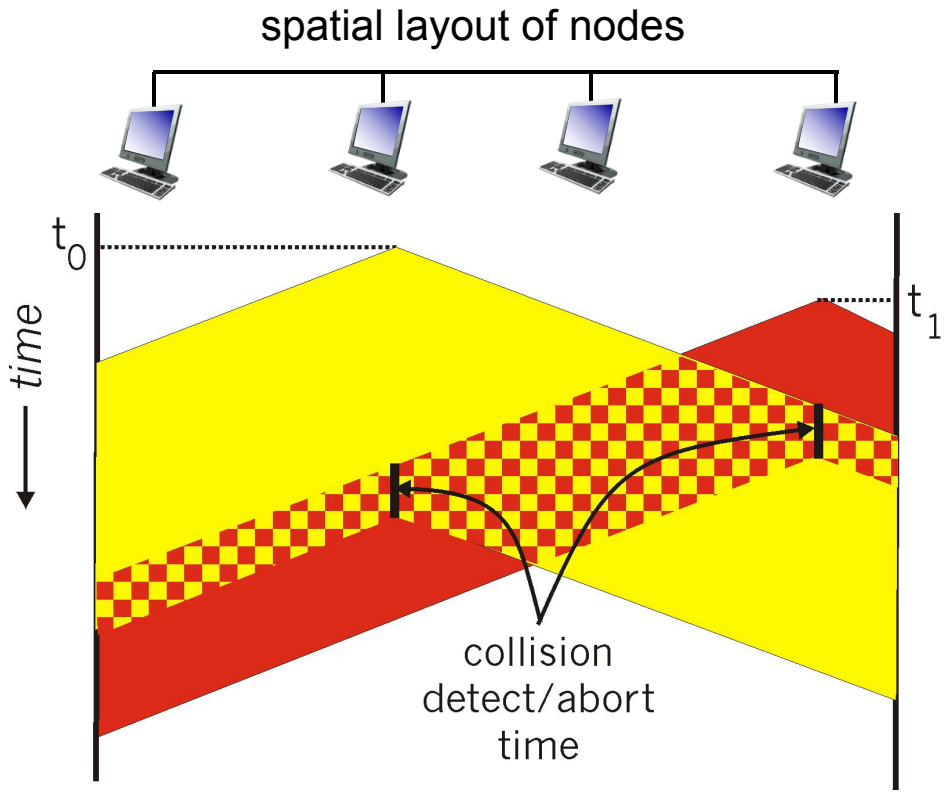
collisions *can* still occur: propagation delay means two nodes may not hear each other's transmission

collision: entire packet transmission time wasted

- distance & propagation delay play role in in determining collision probability



CSMA/CD (collision detection)



Carrier Sense Multiple Access (CSMA)

In some shorter distance networks, it is possible to listen to the channel before transmitting

In radio networks, this is called “ sensing the carrier”

The CSMA protocol works just like Aloha except: If the channel is sensed busy, then the user waits to transmit its packet, and a collision is avoided

This really improves the performance in short distance networks!

Carrier Sense Multiple Access (CSMA)

How long does a blocked user wait before trying again to transmit its packet? Three basic variants:

1-persistent: Blocked user continuously senses channel until its idle, then transmits

0-persistent: Blocked user waits a randomly chosen amount of time before sensing channel again

Carrier Sense Multiple Access (CSMA)

P-persistent: Let τ = end-to-end propagation delay

- If channel is idle then transmit packet
- If channel busy then toss coin *[with P(heads) = P]*
- Heads: Transmit at first idle
- Tails: wait until first idle plus T, sense, repeat

Human analogy: Don't interrupt others

CSMA/CD (collision detection)

CSMA/CD: carrier sensing, as in CSMA

- collisions *detected* within short time
- colliding transmissions aborted, reducing channel wastage

❖Collision detection:

- easy in wired LANs: measure signal strengths, compare transmitted, received signals
- difficult in wireless LANs: received signal strength overwhelmed by local transmission strength

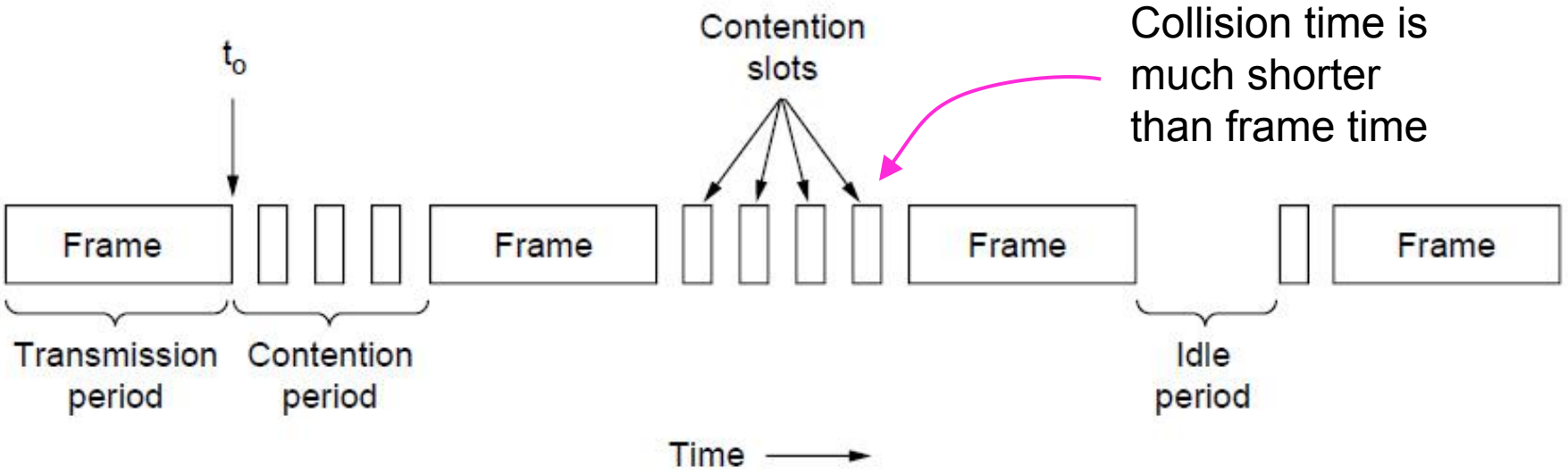
CSMA/CD (collision detection)

- The minimum time to detect the collision is just the time it takes the signal to propagate from one station to the other
- A station that has not heard a collision for a time equal to the full cable propagation time after starting its transmission can be sure it has seized the cable
- Let the propagation time between the two farthest stations be τ.
- At t0, one station begins transmitting. At $t0+\tau-\varepsilon$, an instant before the signal arrives at the most distant station, that station also begins transmitting.
- Second station immediately detects collision and aborts transmission
- The little noise burst caused by the collision does not get back to the original station until time $2\tau-\varepsilon$

CSMA (3) – Collision Detection

CSMA/CD improvement is to detect/abort collisions

- Reduced contention times improve performance



CSMA – Collision Detection

- Can we think of CSMA/CD contention as a slotted ALOHA system with a slot width of 2τ
- The difference for CSMA/CD compared to slotted ALOHA is that slots in which only one station transmits (i.e., in which the channel is seized) are followed by the rest of a frame.
- This difference will greatly improve performance if the frame time is much longer than the propagation time

Collision-Free Protocols

- Collisions adversely affect the system performance
- In protocols to follow, we assume that there are exactly N stations, each programmed with a unique address from 0 to N−1.
- Propagation delay is negligible

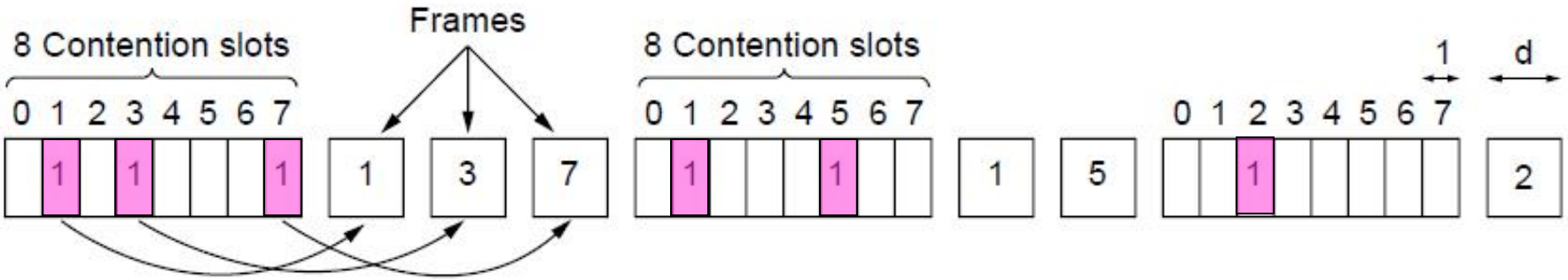
Collision-Free – Bitmap

Collision-free protocols avoid collisions entirely

- Senders must know when it is their turn to send

The basic bit-map protocol:

- Sender set a bit in contention slot if they have data
- Senders send in turn; everyone knows who has data



Collision-Free – Bitmap

Performance

- measure time in units of the contention bit slot, with data frames consisting of d time units
- Under conditions of low load
  - A lower numbered station has to wait N+N/2 slots
  - Higher numbered station has to wait for N/2 slots
  - The mean dealy for all station is N slot
  - Channel efficiency: The overhead per frame is N bits and the amount of data is d bits, for an efficiency of d/(d+N).
- Under conditions of high load
  - The mean delay for a frame is (N−1)d+N
  - Channel efficiency: The overhead per frame is 1 bits for an efficiency of d/(d+1).

Bit Map Protocol

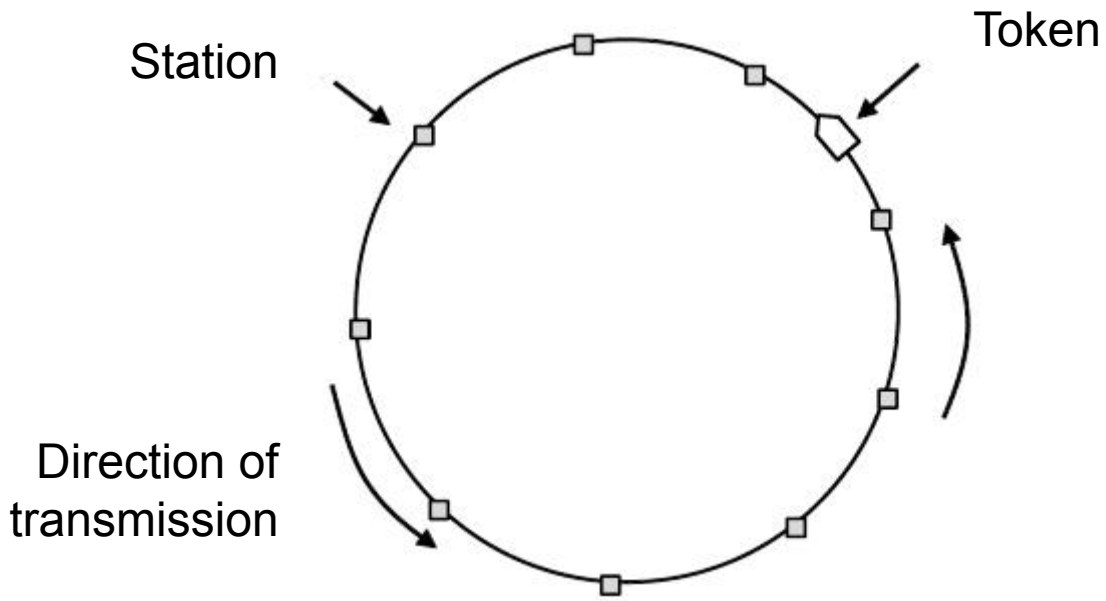
Issues

- Stations' access to the network is unfair: That is, if station *i* and station *j* both want to transmit, and *i* < *j*, then station *i* always first to transmit.
- low numbered stations have to wait longer than high numbered stations for the reservation to complete.
- Efficiency: at low load, the protocol efficiency is low.

Collision-Free – Token Ring

Token sent round ring defines the sending order

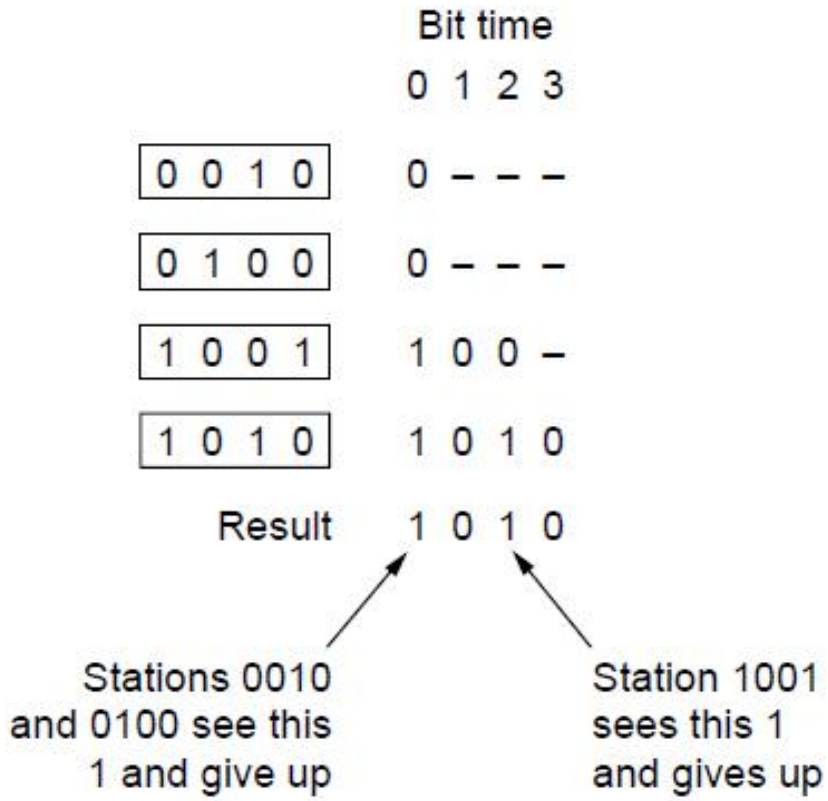
- Station with token may send a frame before passing
- Idea can be used without ring too, e.g., token bus



Collision-Free – Countdown

Binary countdown improves on the bitmap protocol

- Stations send their address in contention slot (log N bits instead of N bits)
- Medium ORs bits; stations give up when they send a "0" but see a "1"
- Station that sees its full address is next to send



Collision-Free – Countdown

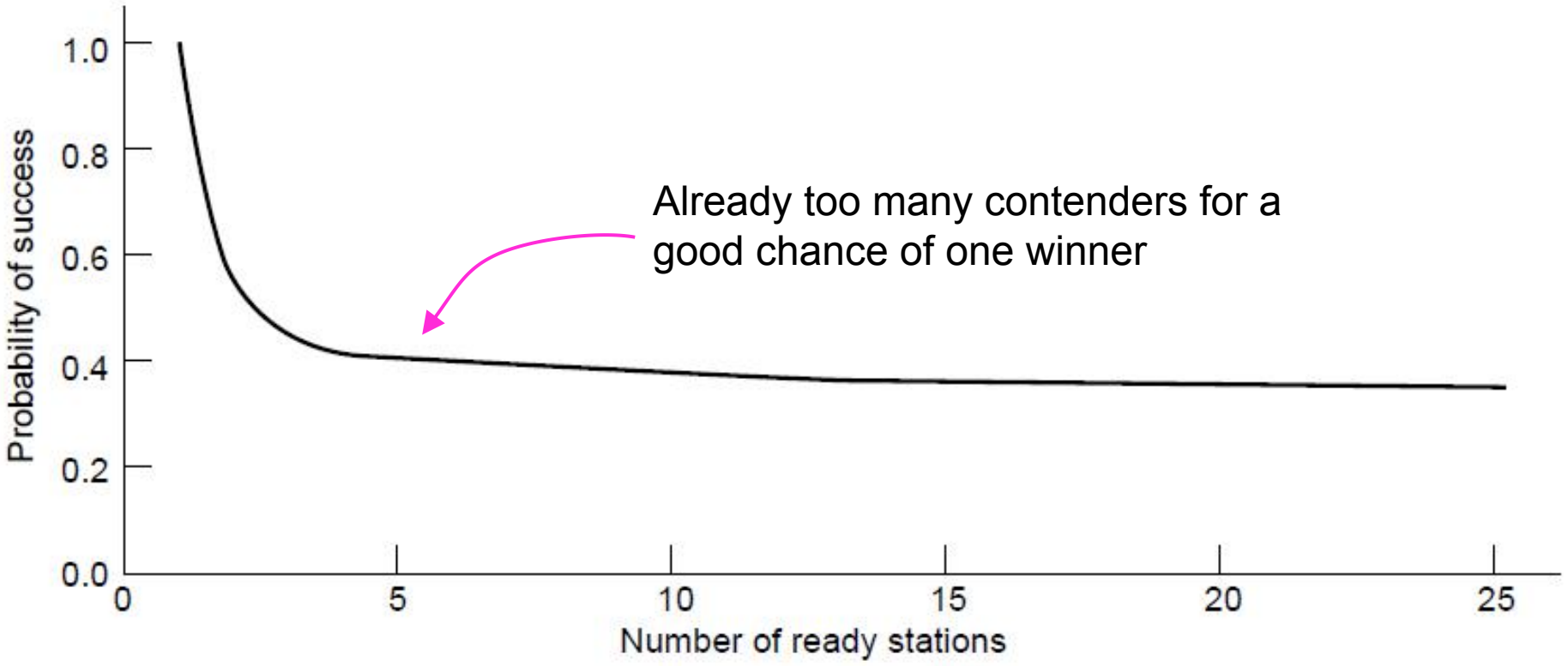
- Performance
- The channel efficiency is $d/(d+\log_2 N)$

Summary

It is concluded that contention based systems performs better at lower load and reservation based protocols performs better when at higher load.

Is it possible to design an adaptive solution which works like contention system at lower load and like reservation system when load increases ?

Limited-Contention Protocols



Limited-Contention Protocols

Idea is to divide stations into groups within which only a very small number are likely to want to send

Avoids wastage due to idle periods and collisions

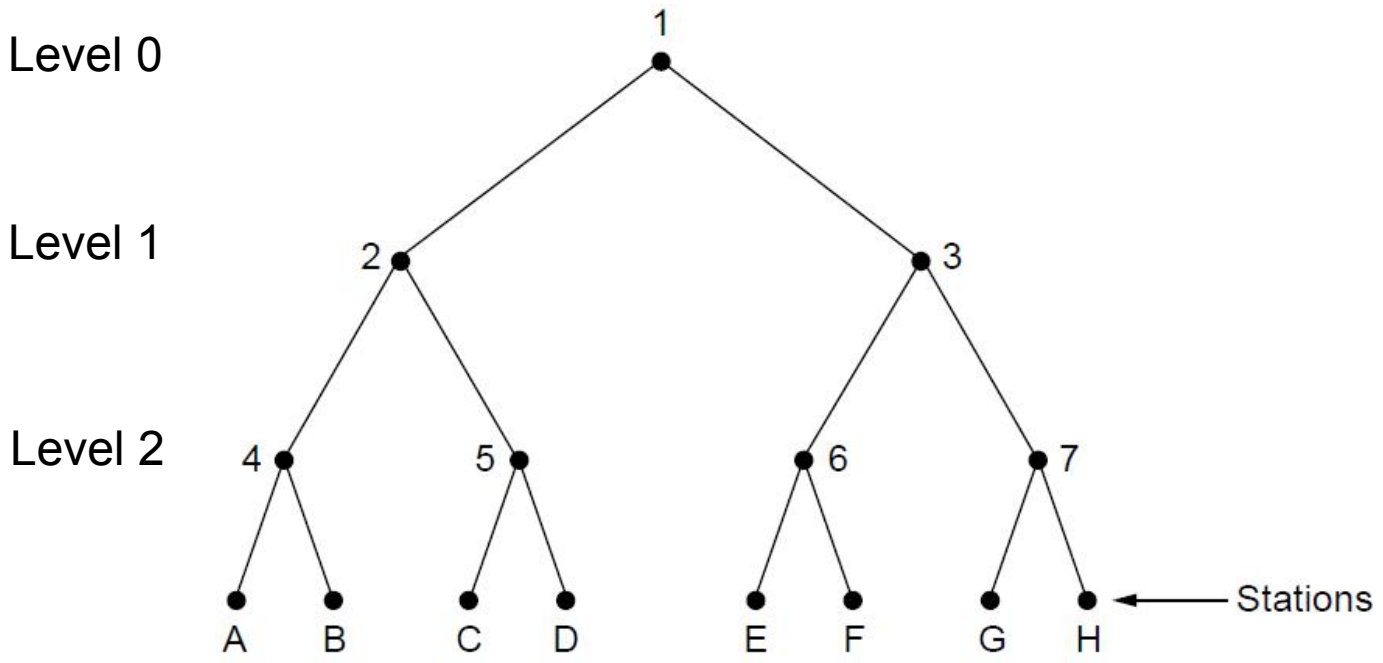
- k station with probability p of transmitting in a slot
- Probability of success = $kp\,(1-p)^{k-1}$
- To find optimal value of p, differentiate wrt p, set it 0 and solve for p
- p =1/k, substituting gives

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

Limited Contention –Adaptive Tree Walk

Tree divides stations into groups (nodes) to poll

- Depth first search under nodes with poll collisions
- Start search at lower levels if >1 station expected



Limited Contention –Adaptive Tree Walk

Tree divides stations into groups (nodes) to poll

- Depth first search under nodes with poll collisions
- Start search at lower levels if >1 station expected
- Which is ideal level to start with ?
- Assume each station has estimate of ready stations q
- Each node at level i has a fraction 2^{-i} of the station below it
- If q ready stations are uniformly distributed, expected number of ready stations under a node at level i is 2^{-i} q
- Ideally it should be 1 means $i=\log_2 q$

Example Networks

Ethernet

Wireless LAN

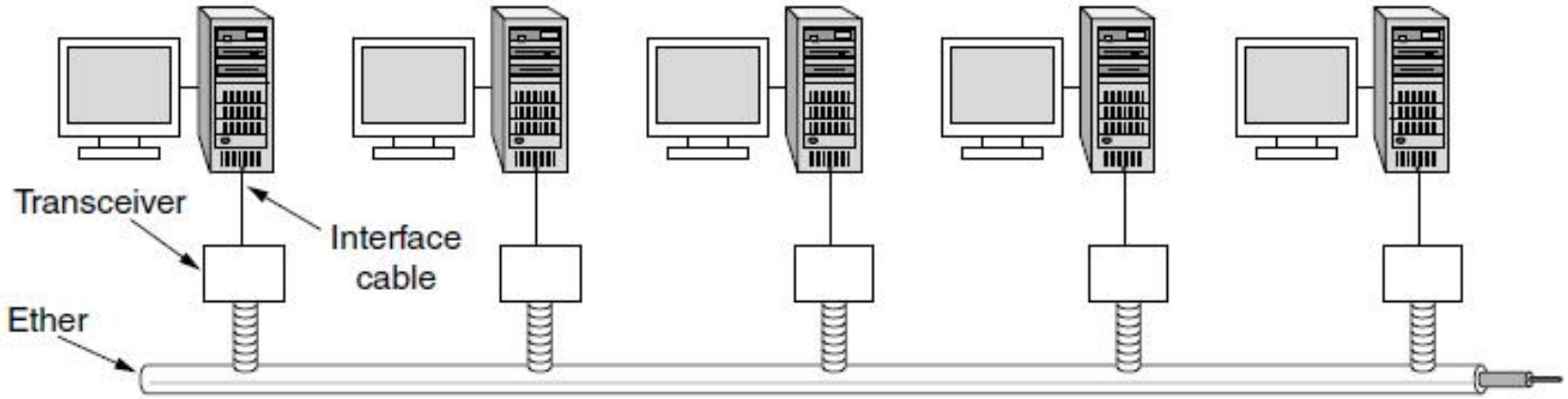
Ethernet

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

Classic Ethernet – Physical Layer

One shared coaxial cable to which all hosts attached

- 3 to 10 Mbps, with Manchester encoding
- Hosts ran the classic Ethernet protocol for access



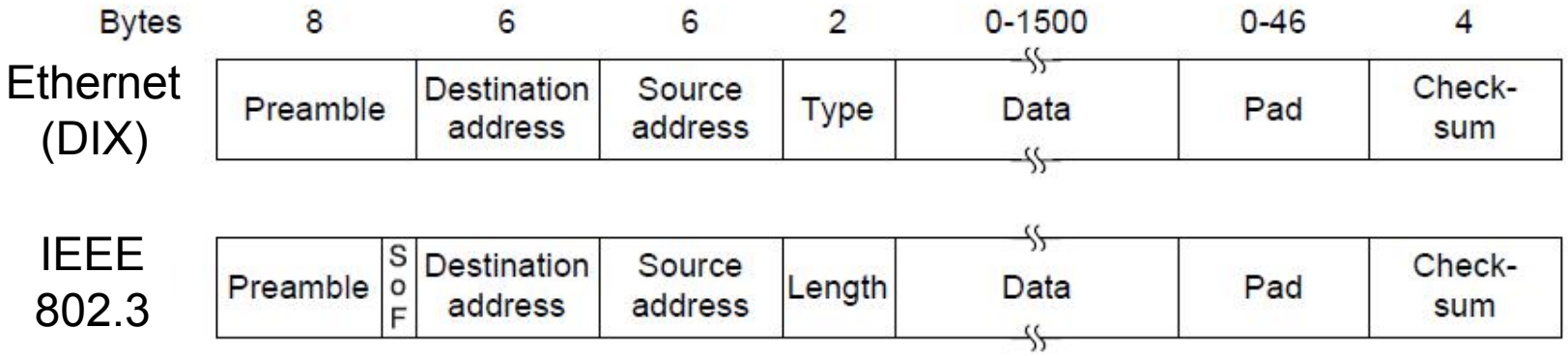
Classic Ethernet – Physical Layer

- Thick Ethernet - Thick coaxial cable with segment length of 500 m with each segment can have 100 PCs
- Thin Ethernet - Thin and flexible coaxial cable with segment length of 185 m with each segment can have 30 PCs
- Repeaters can be used to extend the length of Ethernet beyond the max segment length

Classic Ethernet – MAC

MAC protocol is 1-persistent CSMA/CD (earlier)

- Random delay (backoff) after collision is computed with BEB (Binary Exponential Backoff)
- Frame format is still used with modern Ethernet.



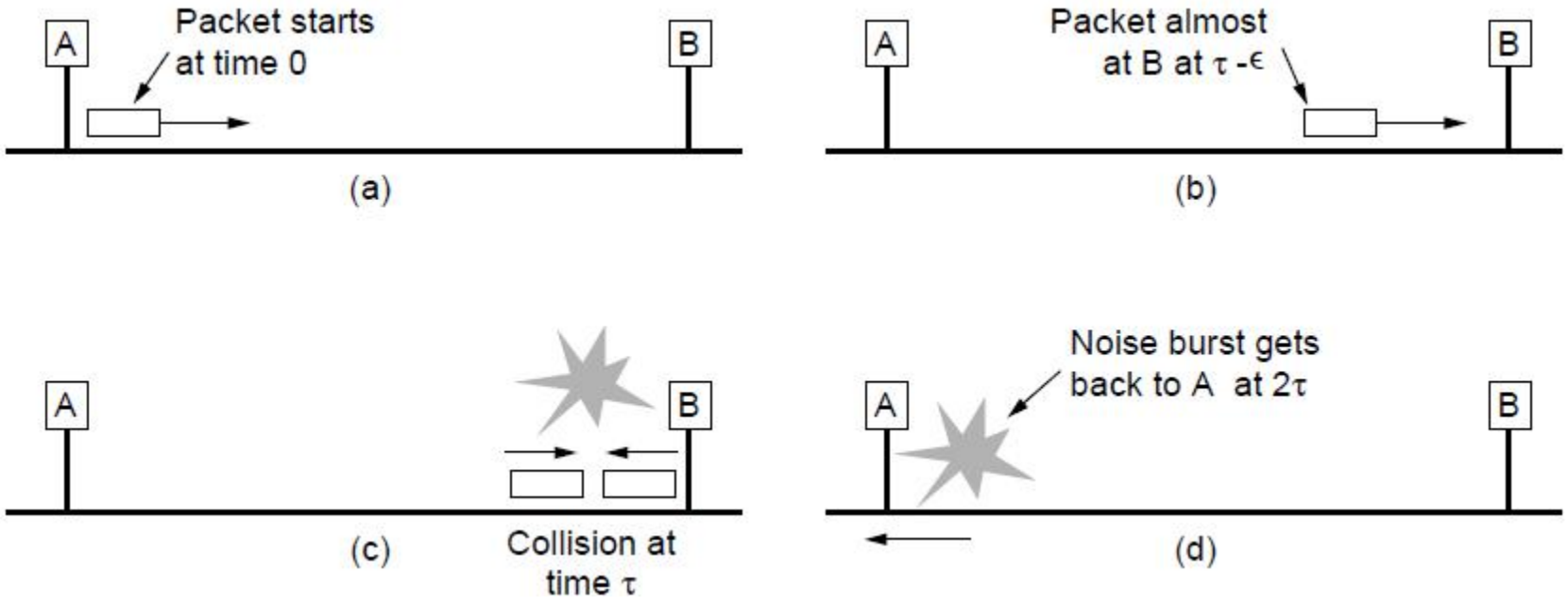
Classic Ethernet – MAC

- Preamble is 101010... pattern. The last 2 bits are set to 11. Manchestor encoding of this pattern produces a square wave which is used for synchronization
- Address - beginning with 0 is normal address while address commencing with 1 is multicast or braodcast address
- MAC addresses are globally unique
- Type/Length - type indicates the kind of contents carried by the frame like 0x0800 means IPv4. If the number is less than 0x600 (1536), it is intepreted as length else as type to ensure compatibility between both versions
- Data - Maximum 1500

Classic Ethernet – MAC

Collisions can occur and take as long as 2τ to detect

- τ is the time it takes to propagate over the Ethernet
- Leads to minimum packet size for reliable detection



Ethernet CSMA/CD algorithm

1. NIC receives datagram from network layer, creates frame
2. If NIC senses channel idle, starts frame transmission. If NIC senses channel busy, waits until channel idle, then transmits.
3. If NIC transmits entire frame without detecting another transmission, NIC is done with frame !

4. If NIC detects another transmission (*collision*) while transmitting, it aborts and sends jam signal

5. After aborting, NIC enters *binary (exponential) backoff:*

- after m^{th} collision, NIC chooses K at random from $\{0,1,2, \ldots, 2^m-1\}$. NIC waits K·512 bit times, returns to Step 2
- longer backoff interval with more collision

Classic Ethernet – Performance

Try to find mean duration of contention interval

Or

mean number of contention slots in a contention interval

Assume k node is contending in contention period

Assume each node transmits with a fixed probability *p* in any slot

What is the probability ('A') that some station acquires the channel in a slot (for successful transmission)?

$A = p(1-p)^{k-1} + p(1-p)^{k-1} + \ldots$ k times

$= k\,p(1-p)^{k-1}$

A is maximized when p =1/k, with **A => 1/e** as k tends to infinity.

Classic Ethernet – Performance

The probability (P_j) that a contention interval has exactly j slots?

- (after the collision, the least size of back-off interval chosen by some node is j slots or, what is the probability that some station transmits only at j^{th} slot and not in previous j-1 slots?)
- p(Not transmitting in 1^{st} slot)= (1-A)
- p(Not transmitting in 1^{st} slot and 2^{nd} slot)= (1-A)(1-A)

$P_j = A(1-A)^{j-1}$ ----------(1)

Over a long period of time, the mean number of slots per contention interval is given by

$$\sum_{j=0}^{\infty} (j * A(1-A)^{j-1})$$

Assuming optimal p, the mean number of contention slots is never more than 1/A or e

Classic Ethernet – Performance

Since each slot is $2*T_{prop}$,

Mean length of contention interval is

$$T_{contention} = 2* T_{prop} /A$$

Now if T_{trans} is time needed for transmitting mean packet size then

Channel efficiency (w) is = time required to transmit in absence of collision/ time required to transmit in presence of collision

$$w= T_{trans} / (T_{trans} + 2* T_{prop} /A)$$

So longer the propagation time T_{prop}(cable length!), the longer the contention interval.

The longer the contention interval, the lesser the efficiency / throughput

Classic Ethernet – Performance

Assume the frame length is F, the network bandwidth, B, the cable length, L, and the speed of signal propagation, c

$T_{trans} = F / B$

$T_{prop} = L / c$

$$w = \frac{T_{trans}}{(T_{trans} + {2 * T_{prop}}/{A})}$$

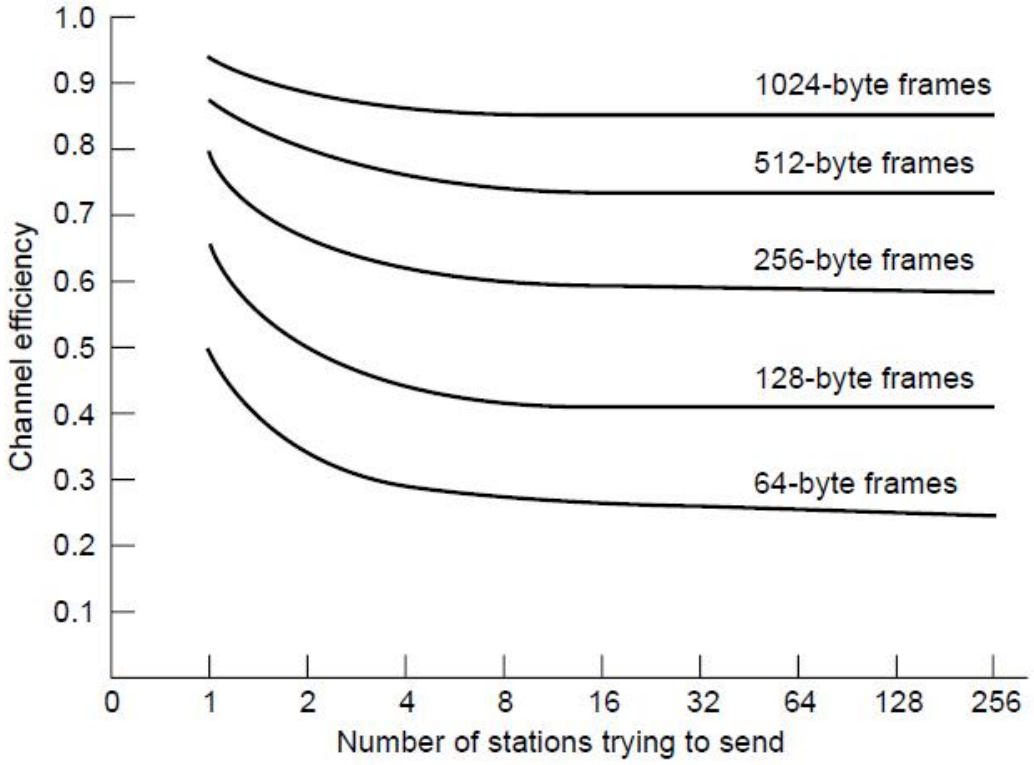
$$w = \frac{{F}/{B}}{({F}/{B} + {2\ eL}/{c})}$$

$$w = \frac{1}{(1 + {2\ BLe}/{cF})}$$

Classic Ethernet – Performance

Efficient for large frames, even with many senders

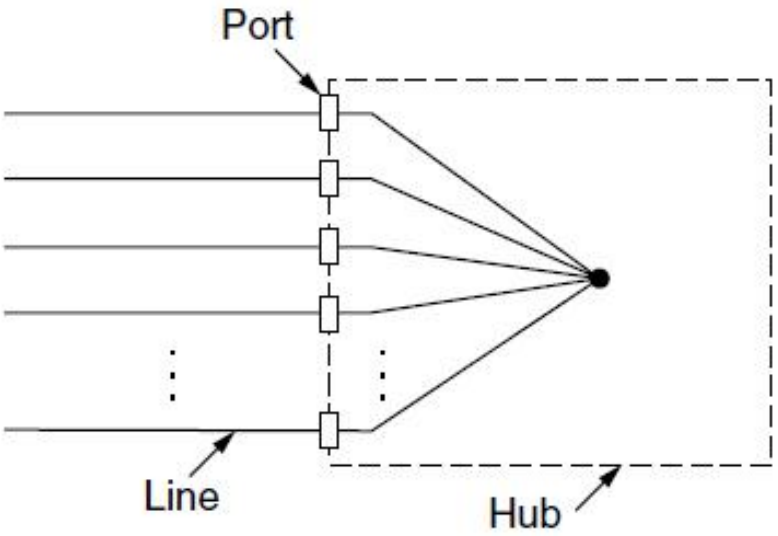
- Degrades for small frames (and long LANs)

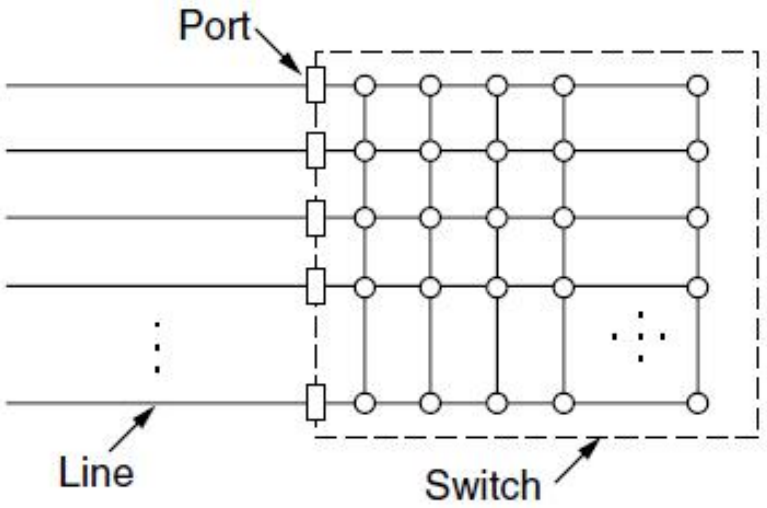


10 Mbps Ethernet,
64 byte min. frame

Switched/Fast Ethernet (1)

- 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

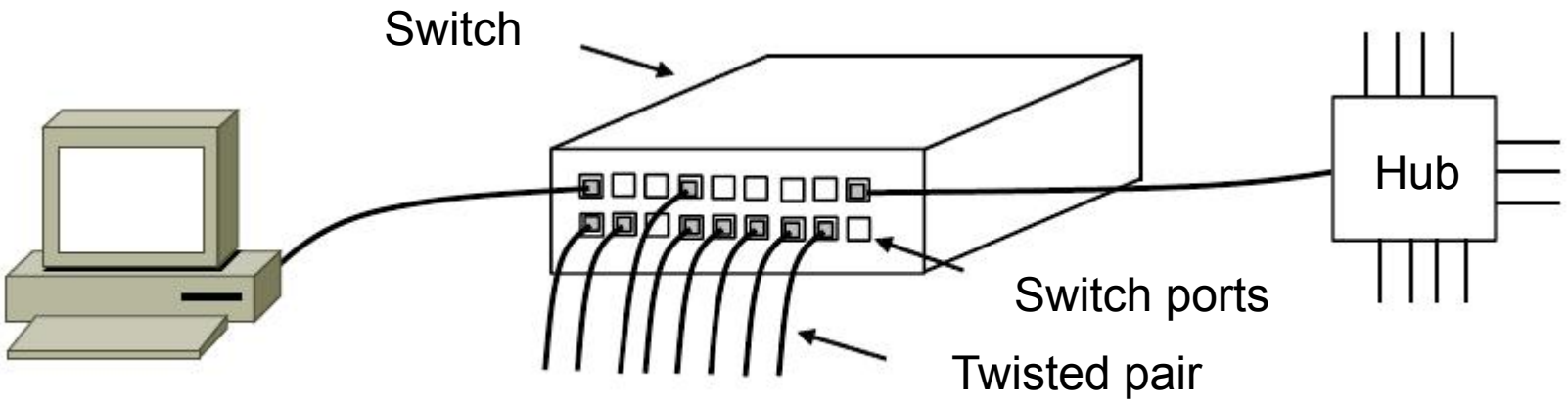




Switched/Fast Ethernet (2)

Switches can be wired to computers, hubs and switches

- Hubs concentrate traffic from computers
- More on how to switch frames the in 4.8



Switched/Fast Ethernet (3)

Fast Ethernet extended Ethernet from 10 to 100 Mbps

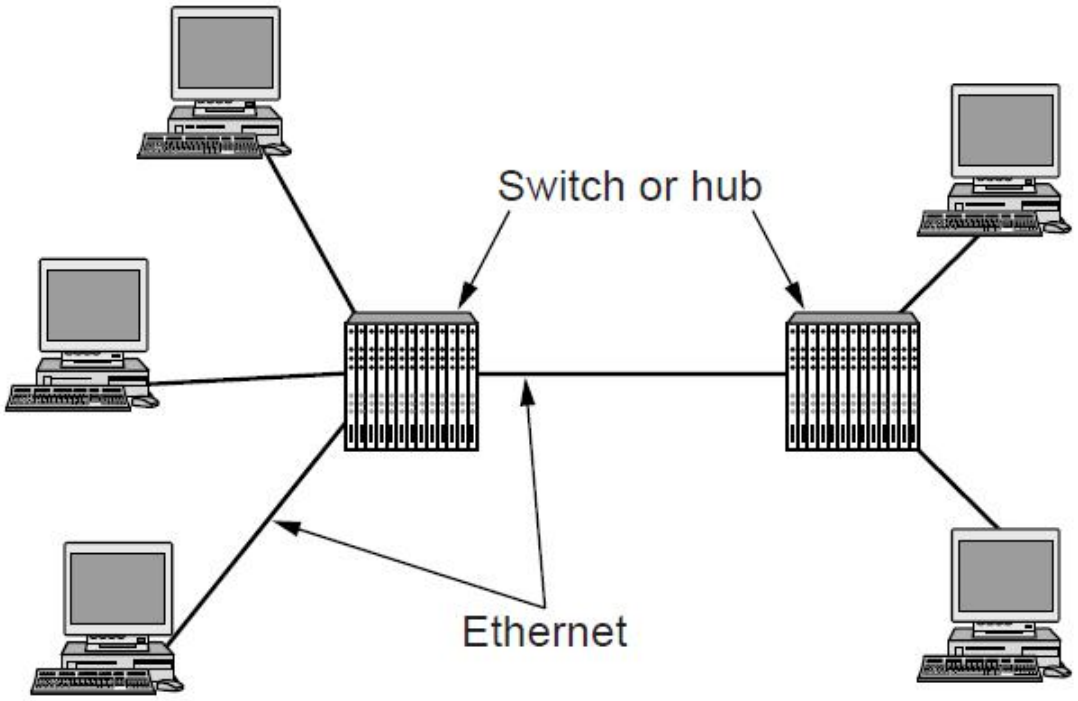
- Twisted pair (with Cat 5) dominated the market

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

Gigabit / 10 Gigabit Ethernet (1)

Switched Gigabit Ethernet is now the garden variety

- With full-duplex lines between computers/switches



Gigabit / 10 Gigabit Ethernet (1)

- 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

Wireless LAN Protocols (1)

Wireless has complications compared to wired.

Nodes may have different coverage regions

- Leads to hidden and exposed terminals

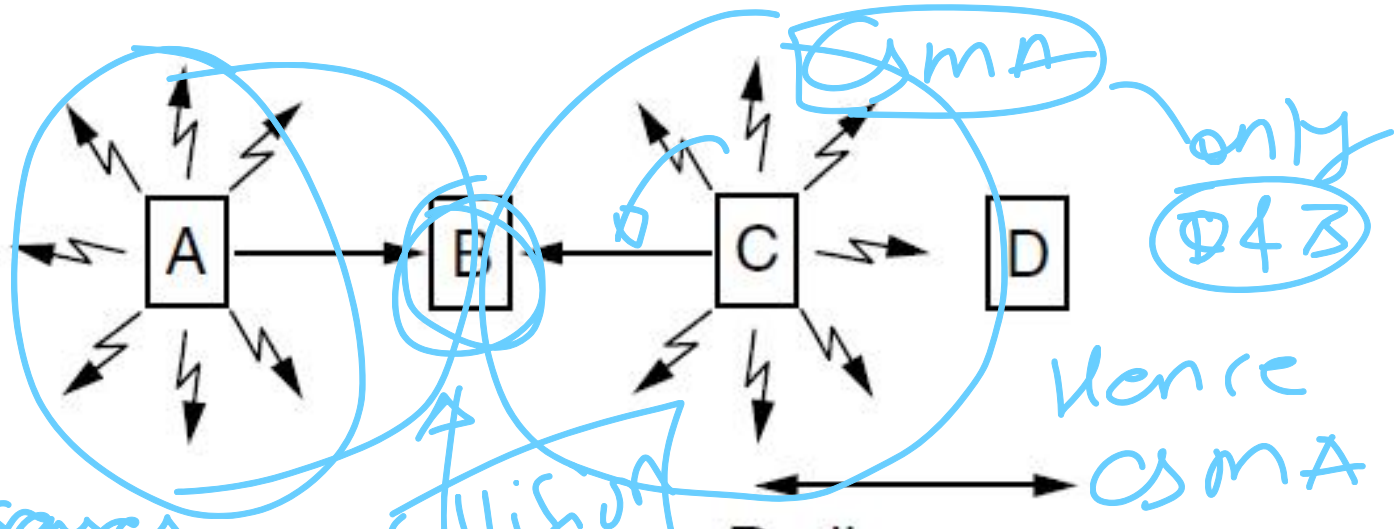
Nodes can't detect collisions, i.e., sense while sending

- Makes collisions expensive and to be avoided

Wireless LANs (2) – Hidden terminals

Hidden terminals are senders that cannot sense each other but nonetheless collide at intended receiver

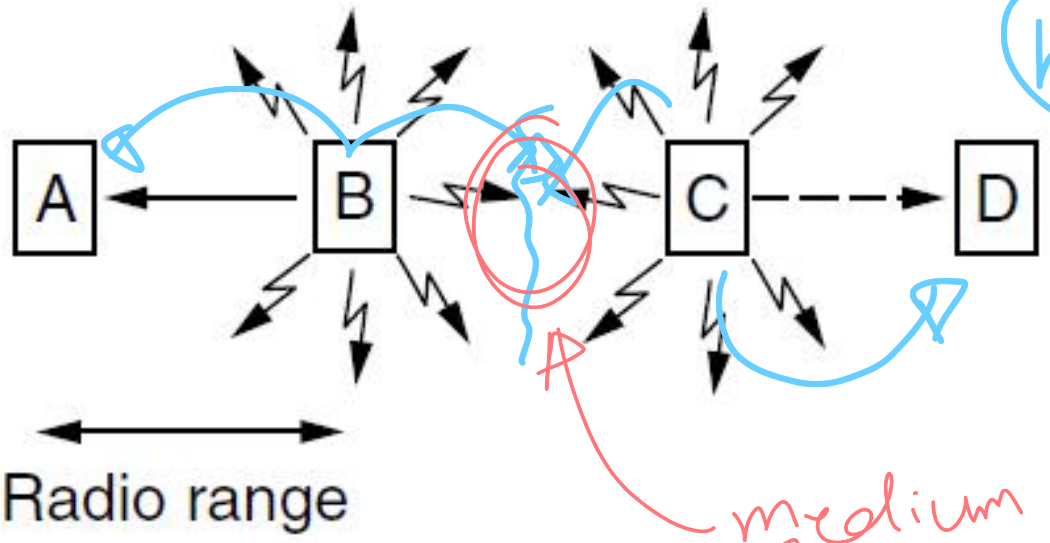
- Want to prevent; loss of efficiency
- A and C are hidden terminals when sending to B



Wireless LANs (3) – Exposed terminals

Exposed terminals are senders who can sense each other but still transmit safely (to different receivers)

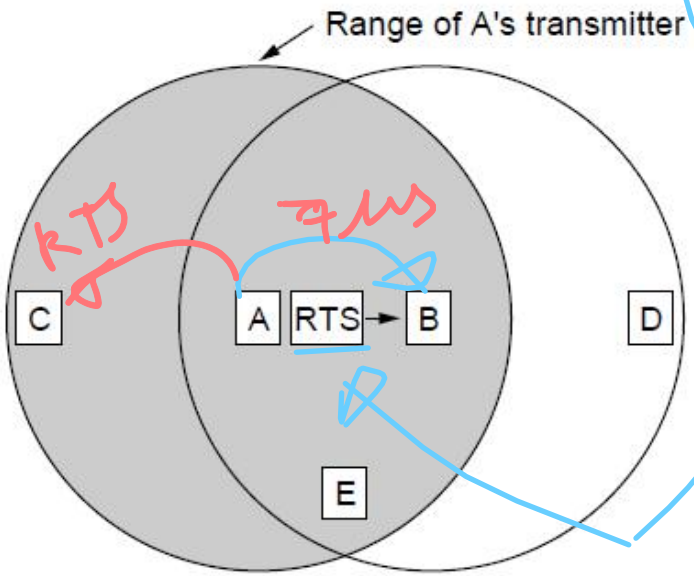
- Desirably concurrency; improves performance
- B → A and C → D are exposed terminals



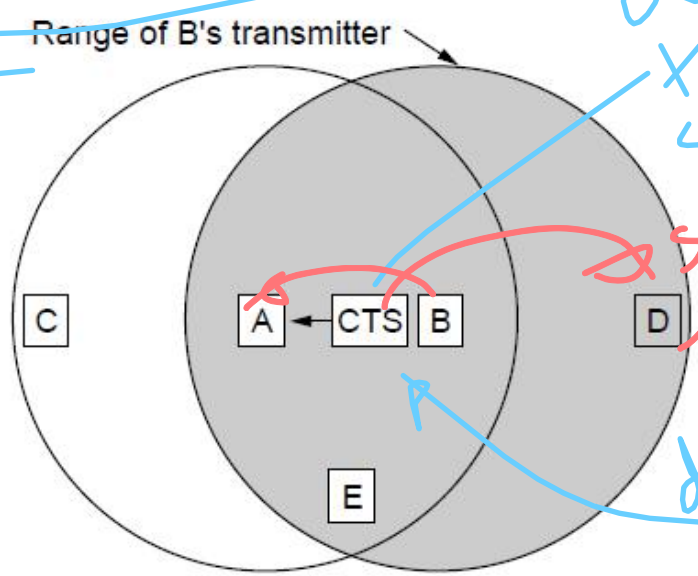
Wireless LANs (4) – MACA

MACA protocol grants access for A to send to B:

- A sends RTS to B [left]; B replies with CTS [right]
- A can send with exposed but no hidden terminals



A sends RTS to B; C and E hear and defer for CTS



B replies with CTS; D and E hear and defer for data

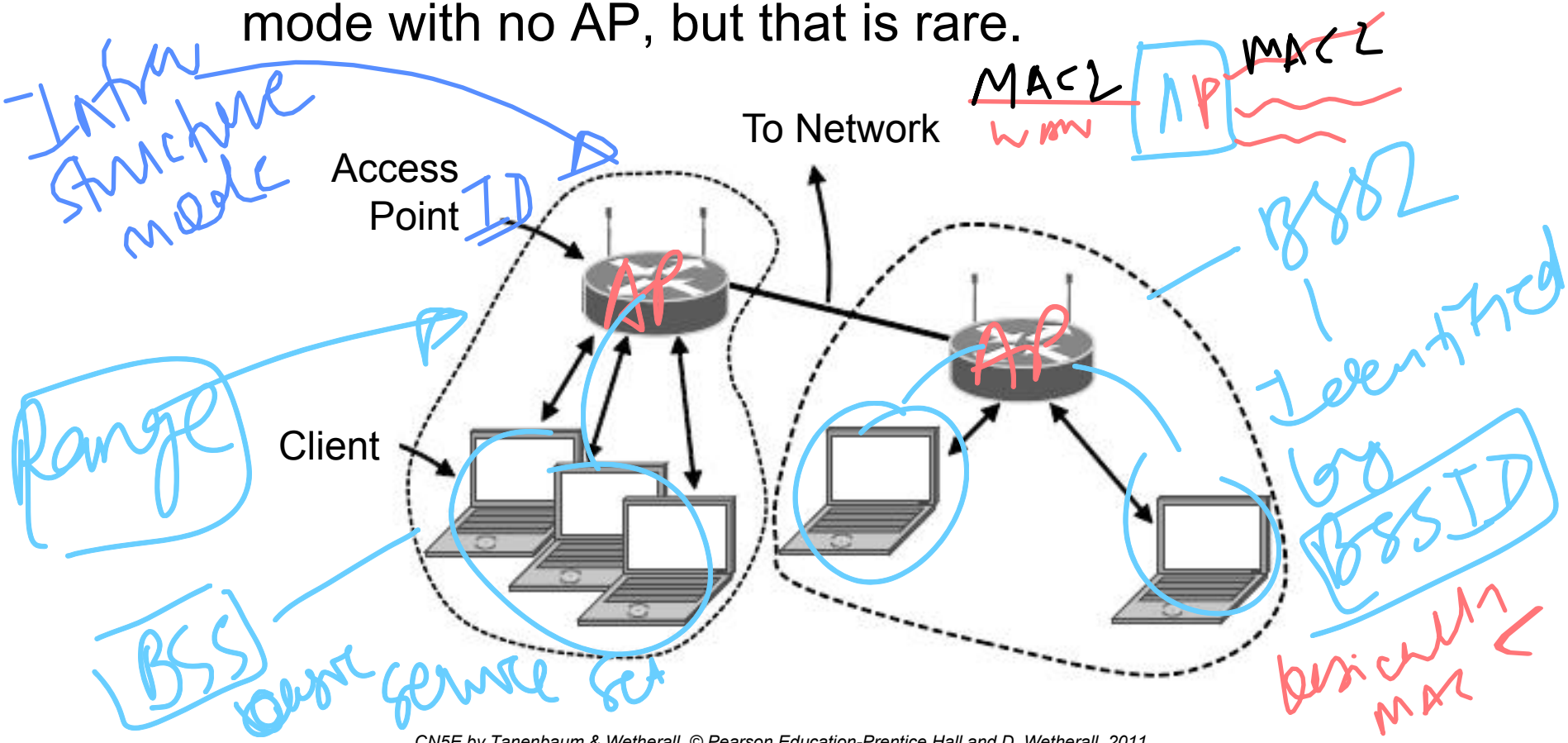
Wireless LANs

- 802.11 architecture/protocol stack »
- 802.11 physical layer »
- 802.11 MAC » details of
- 802.11 frames » frameformat of wifi

802.11 Architecture/Protocol Stack (1)

Wireless clients associate to a wired AP (Access Point)

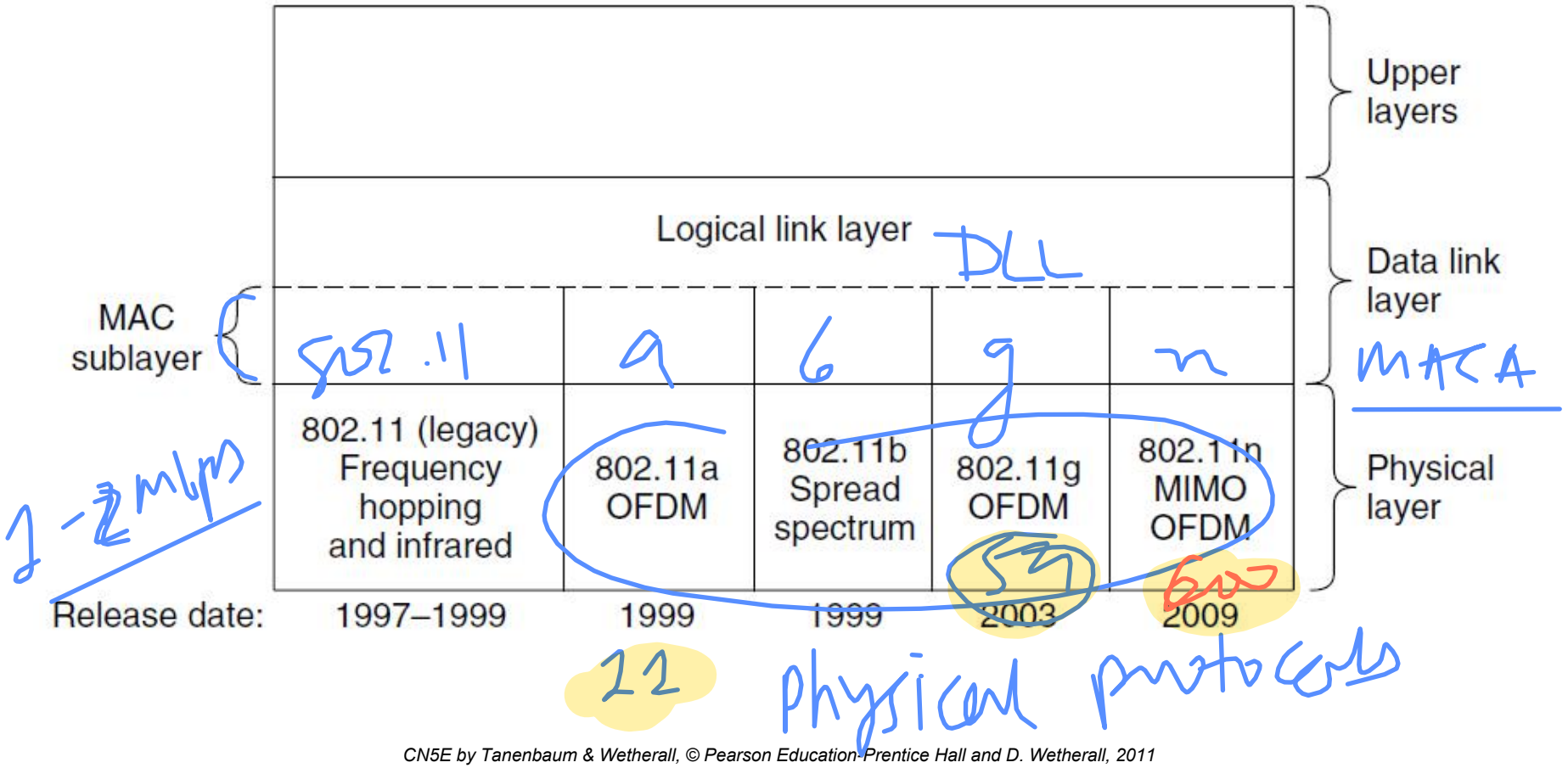
- Called infrastructure mode; there is also ad-hoc mode with no AP, but that is rare.



802.11 Architecture/Protocol Stack (2)

SSID = Service set IDentifier

MAC is used across different physical layers



802.11 physical layer

- NICs are compatible with multiple physical layers
  - E.g., 802.11 a/b/g

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 layer I - DFWMAC

Traffic services

- Asynchronous Data Service (mandatory)
  - exchange of data packets based on “best-effort”
  - support of broadcast and multicast
- Time-Bounded Service (optional)
  - implemented using PCF (Point Coordination Function)

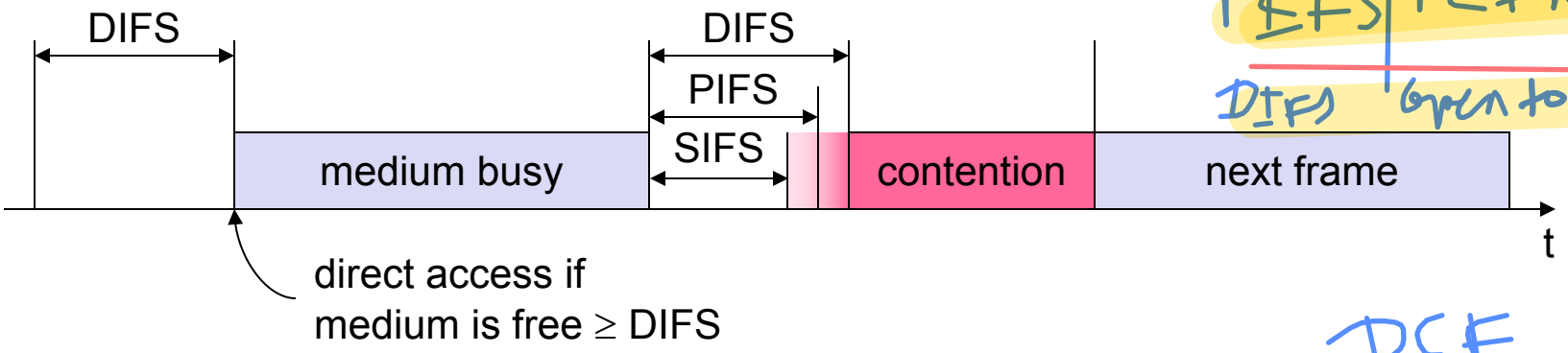
Access methods

- DFWMAC-DCF CSMA/CA (mandatory)
  - collision avoidance via randomized „back-off“ mechanism
  - minimum distance between consecutive packets
  - ACK packet for acknowledgements (not for broadcasts)
- DFWMAC-DCF w/ RTS/CTS (optional)
  - Distributed Foundation Wireless MAC
  - avoids hidden terminal problem
- DFWMAC- PCF (optional)

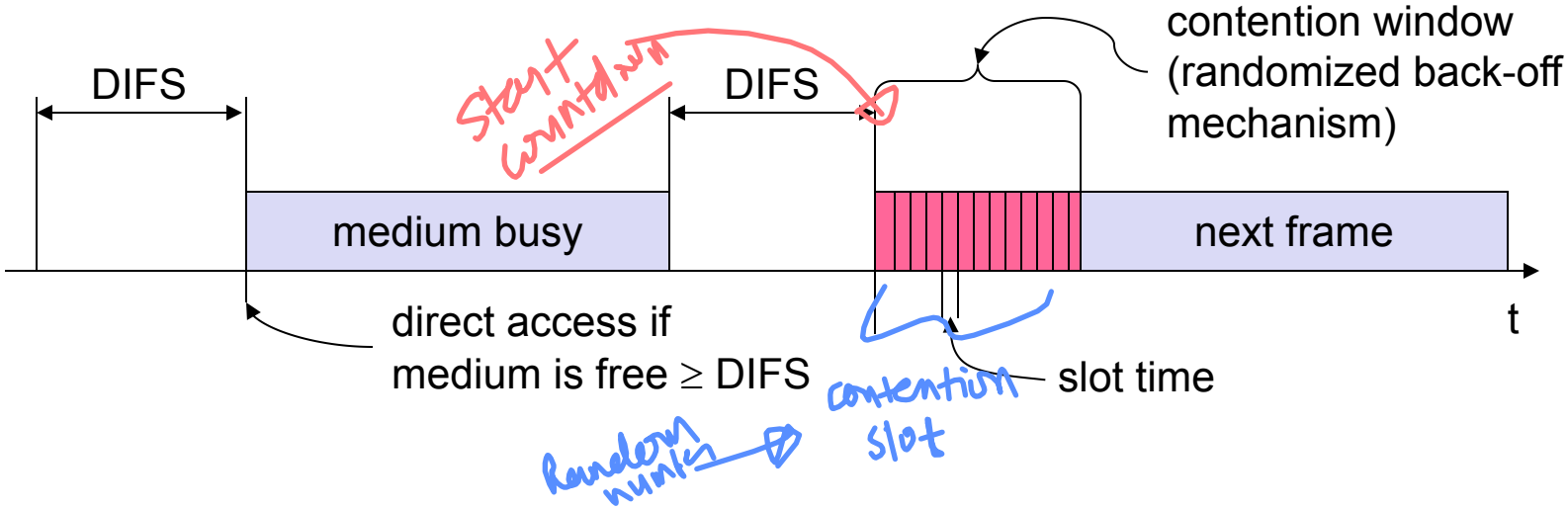
802.11 - MAC layer II

Priorities

- defined through different inter frame spaces
- no guaranteed, hard priorities
- SIFS (Short Inter Frame Spacing)
  - highest priority, for ACK, CTS, polling response
- PIFS (PCF IFS)
  - medium priority, for time-bounded service using PCF
- DIFS (DCF, Distributed Coordination Function IFS)
  - lowest priority, for asynchronous data service

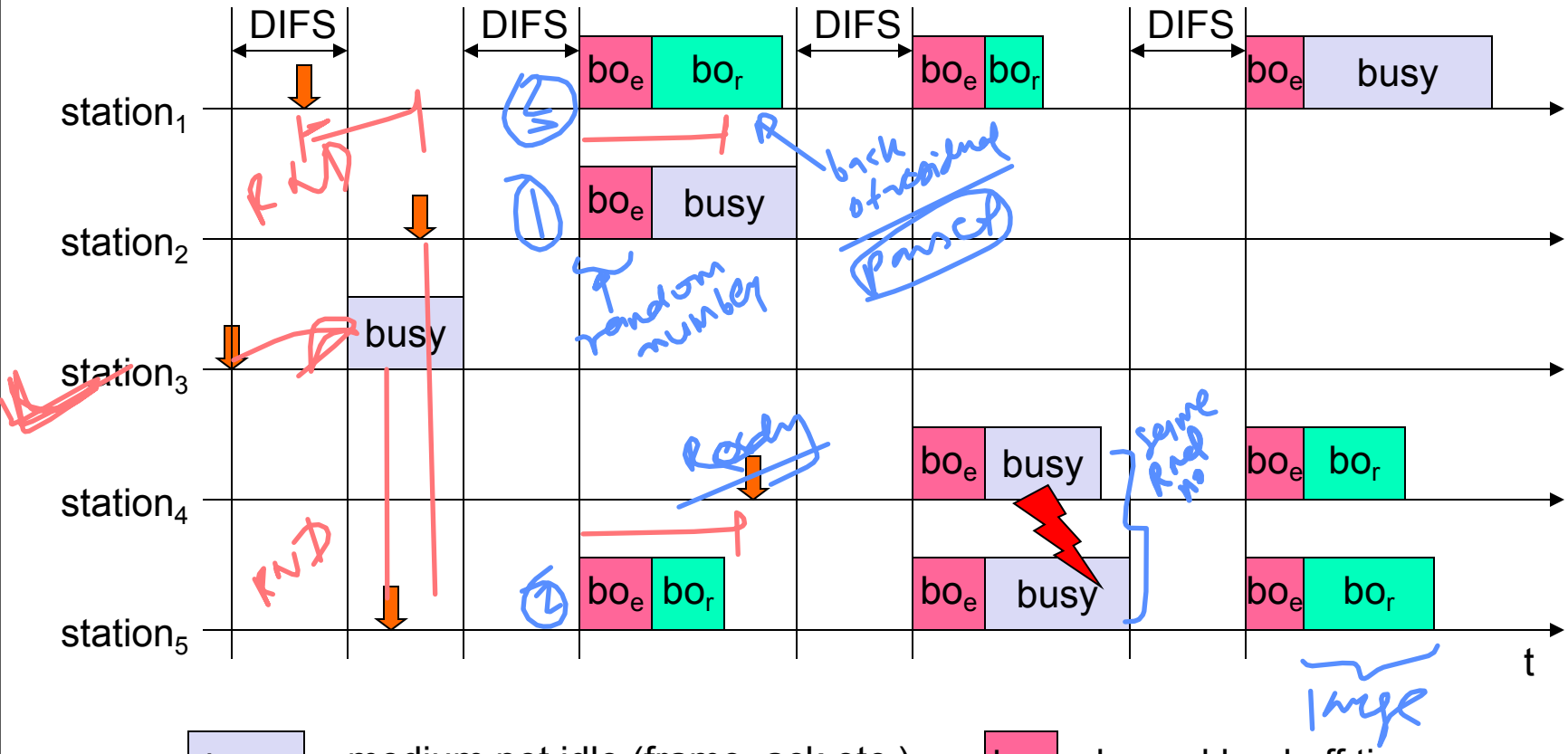


802.11 - CSMA/CA access method I



- station ready to send starts sensing the medium (Carrier Sense based on CCA, Clear Channel Assessment)
- if the medium is free for the duration of an Inter-Frame Space (IFS), the station can start sending (IFS depends on service type)
- if the medium is busy, the station has to wait for a free IFS, then the station must additionally wait a random back-off time (collision avoidance, multiple of slot-time)
- if another station occupies the medium during the back-off time of the station, the back-off timer stops (fairness)

802.11 - competing stations - simple version



busy — medium not idle (frame, ack etc.)

bo_e — elapsed backoff time

packet arrival at MAC

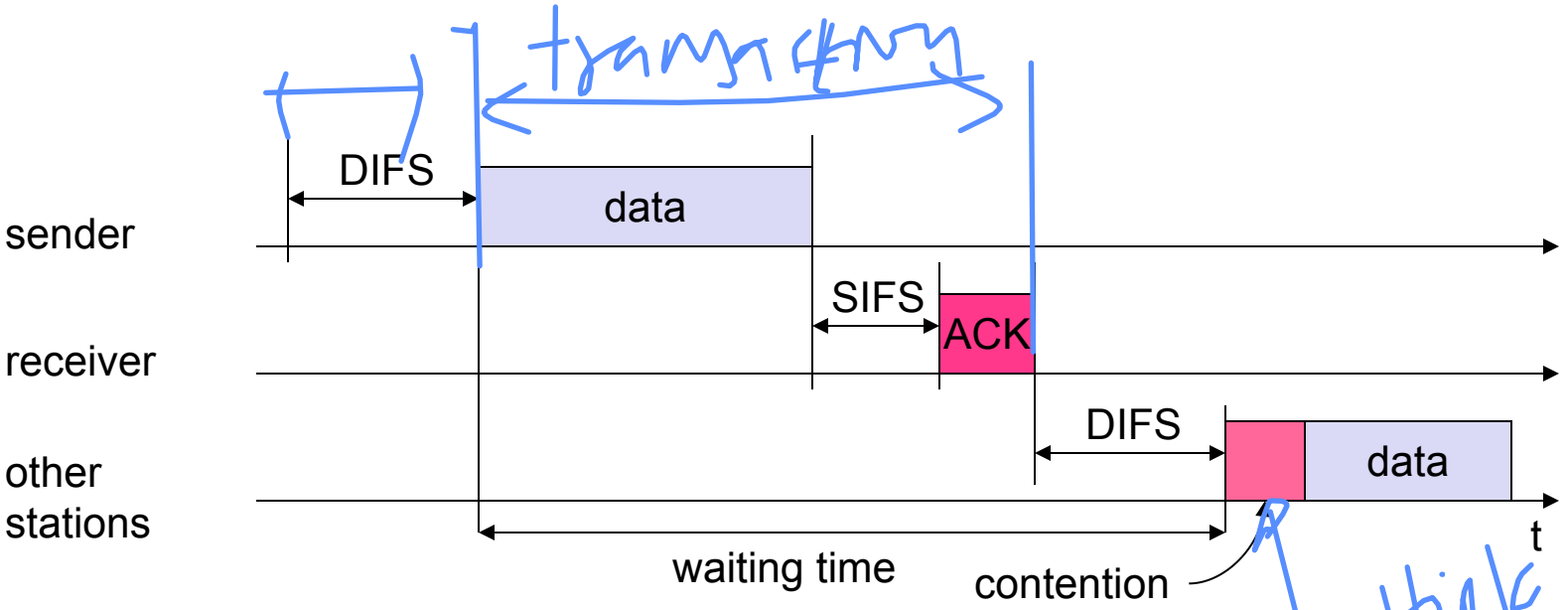
bo_r — residual backoff time

as medium was free for DIFS
3 started transmission
rightaway

802.11 - CSMA/CA access method II

Sending unicast packets

- station has to wait for DIFS before sending data
- receivers acknowledge at once (after waiting for SIFS) if the packet was received correctly (CRC)
- automatic retransmission of data packets in case of transmission errors

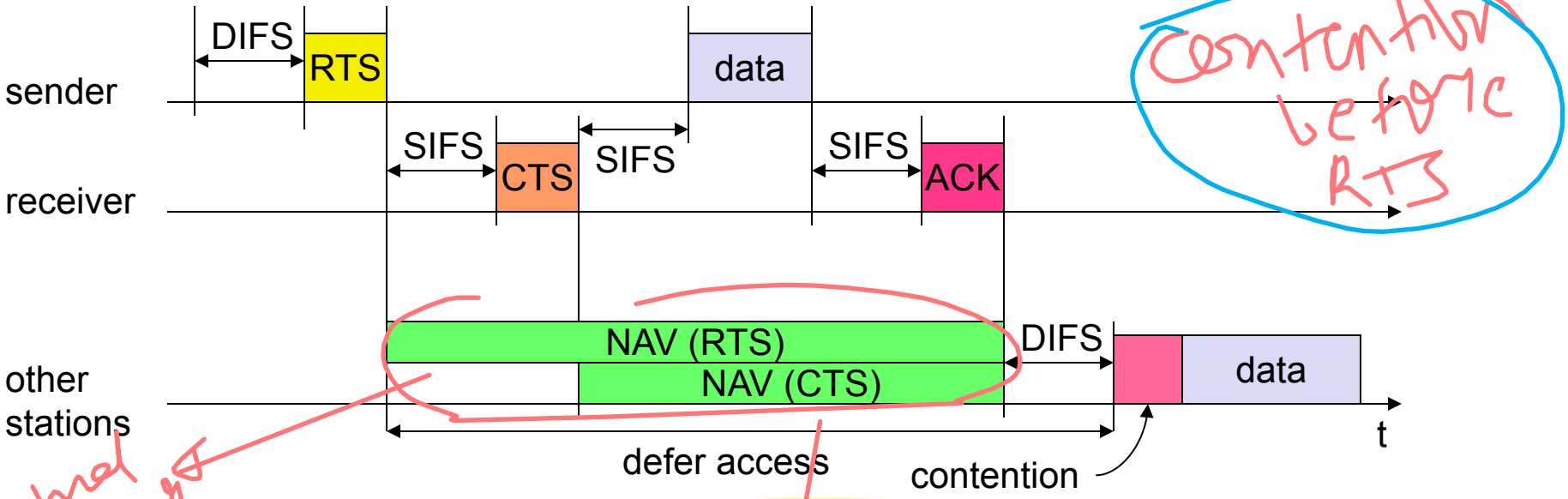


802.11 - DFWMAC

Sending unicast packets

RTS - for hidden node problem

- station can send RTS with reservation parameter after waiting for DIFS (reservation determines amount of time the data packet needs the medium)
- acknowledgement via CTS after SIFS by receiver (if ready to receive)
- sender can now send data at once, acknowledgement via ACK
- other stations store medium reservations distributed via RTS **and** CTS



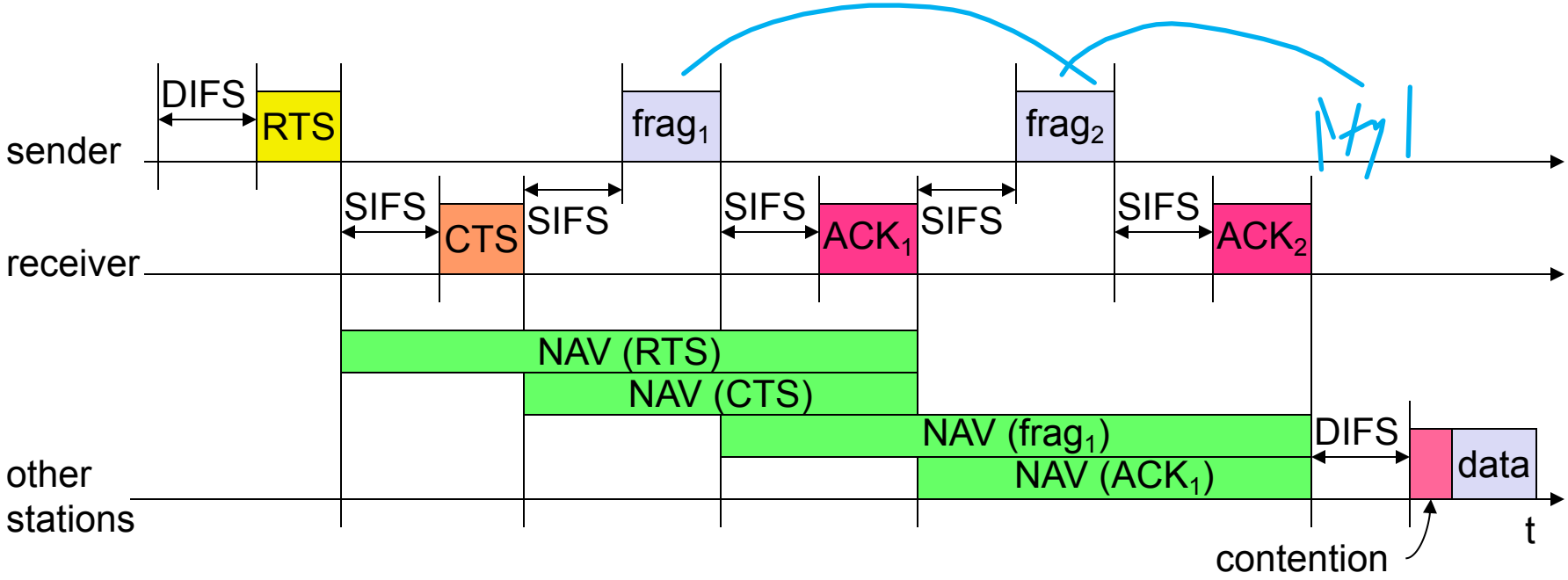
contention before RTS

Virtual carrier sensing

RTS = 3*SIFS + CTS + Ack + data

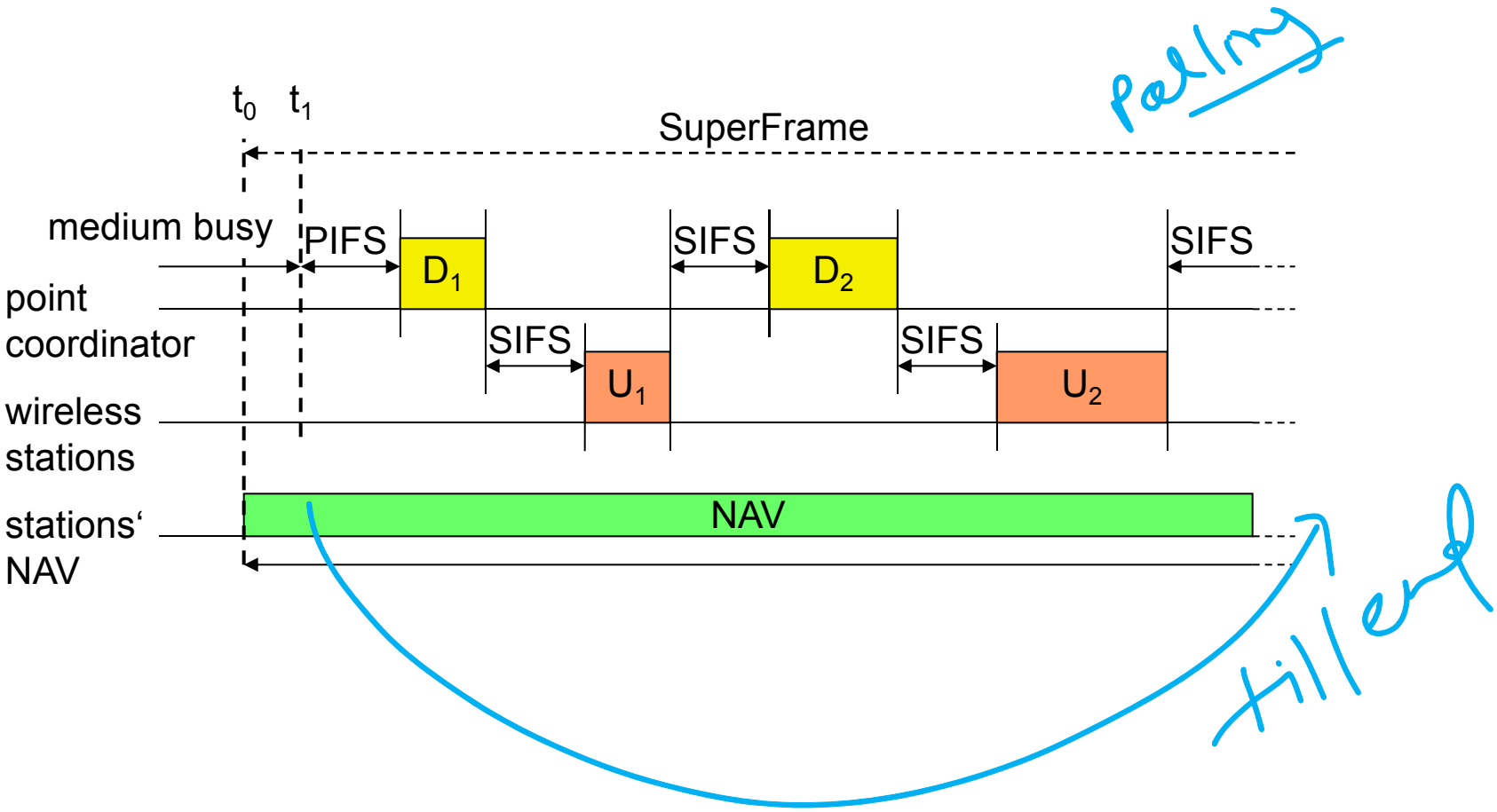
Able to sense

Fragmentation

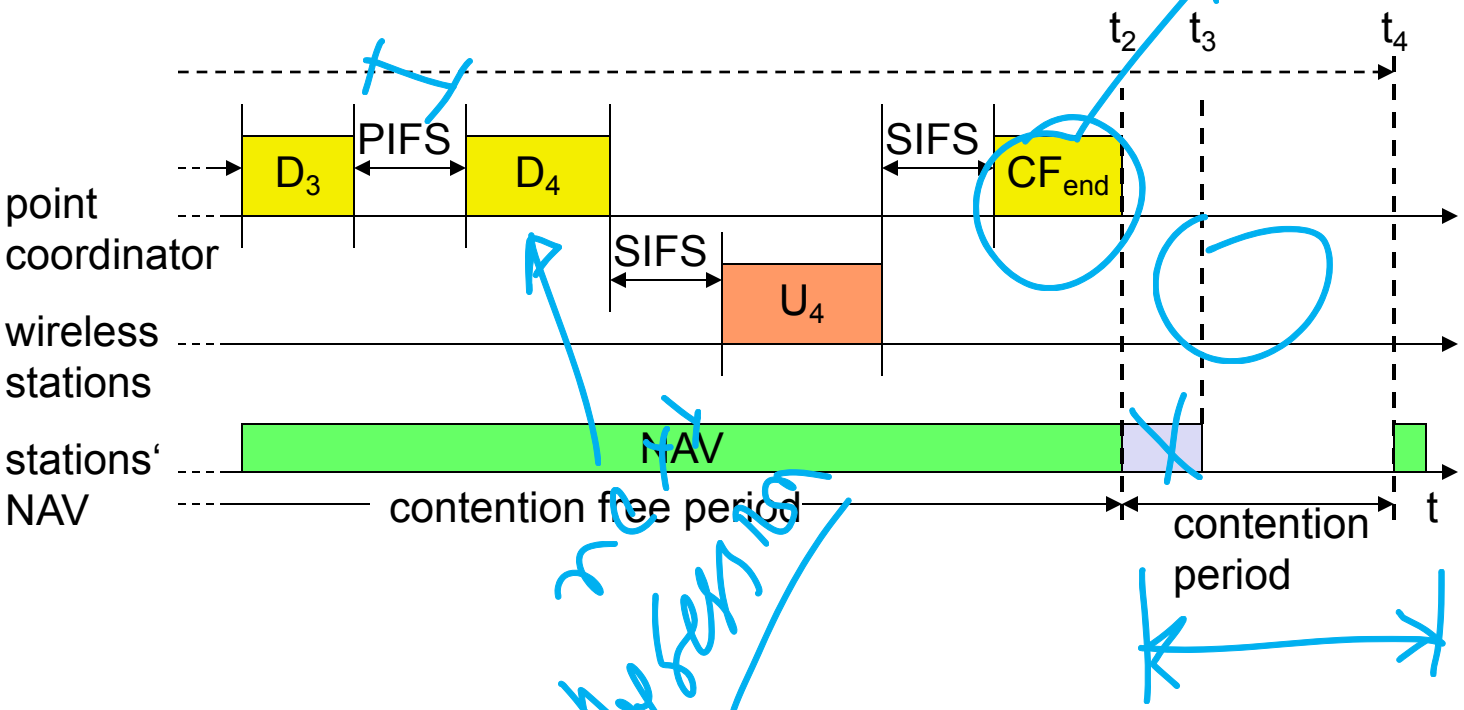


all fragements are sent in same contention → Frag2 extends the contention

DFWMAC-PCF I


t0
t1
SuperFrame
medium busy
PIFS
D1
SIFS
D2
SIFS
point coordinator
SIFS
U1
SIFS
U2
wireless stations
stations' NAV
NAV
polling
till end

DFWMAC-PCF II



802.11 - Frame format

Types

- control frames, management frames, data frames

Sequence numbers

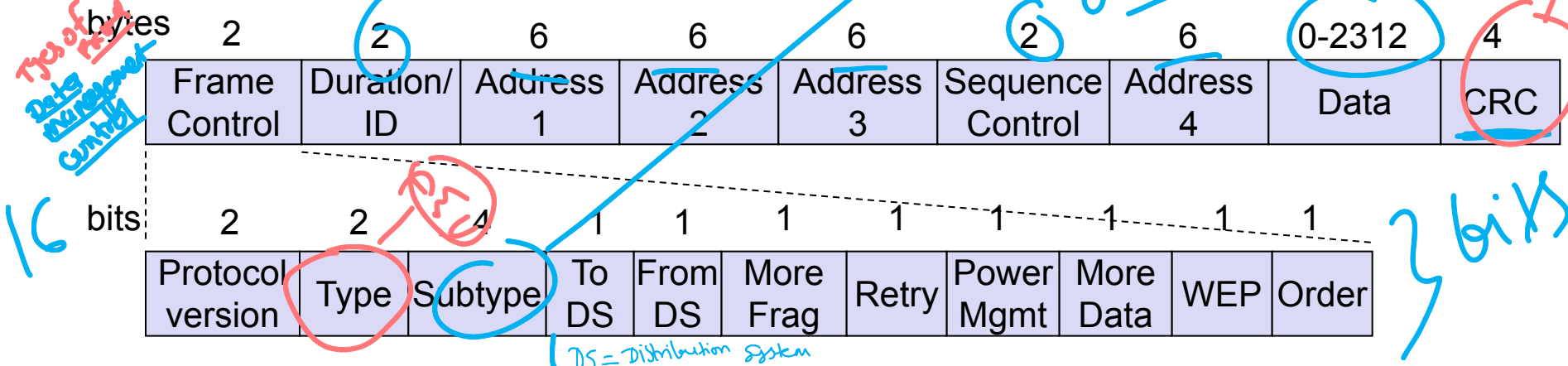
- important against duplicated frames due to lost ACKs

Addresses

- receiver, transmitter (physical), BSS identifier, sender (logical)

Miscellaneous

- sending time, checksum, frame control, data



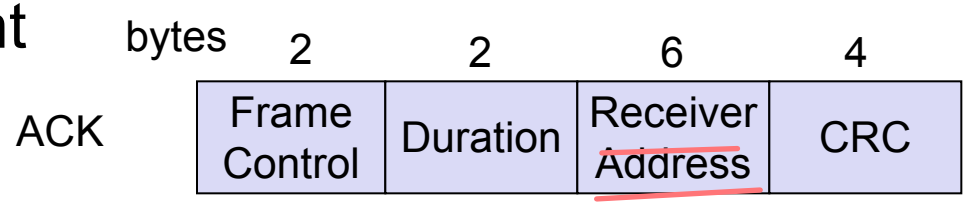
MAC address format

scenario	to DS	from DS	address 1	address 2	address 3	address 4
ad-hoc network	0	0	DA	SA	BSSID	-
infrastructure network, from AP	0	1	DA	BSSID	SA	-
infrastructure network, to AP	1	0	BSSID	SA	DA	-
infrastructure network, within DS	1	1	RA	TA	DA	SA

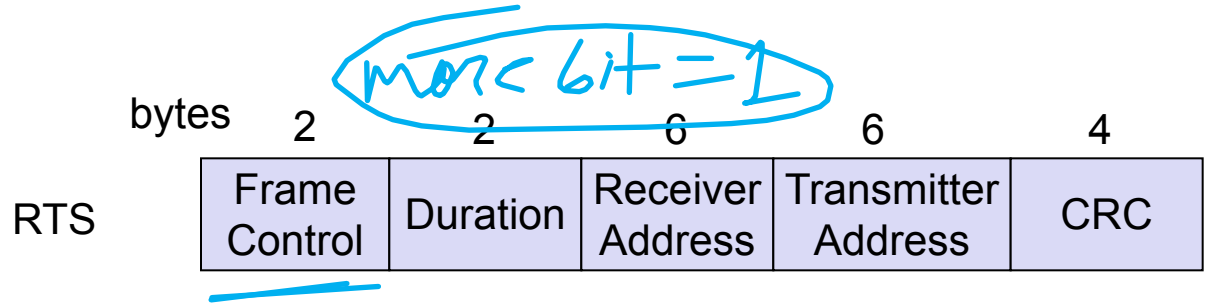
DS: Distribution System
AP: Access Point
DA: Destination Address
SA: Source Address
BSSID: Basic Service Set Identifier
RA: Receiver Address
TA: Transmitter Address

Special Frames: ACK, RTS, CTS

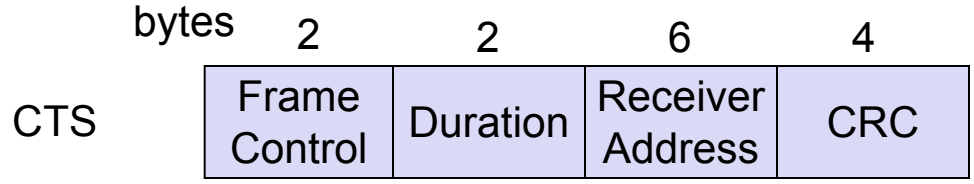
Acknowledgement



Request To Send



Clear To Send



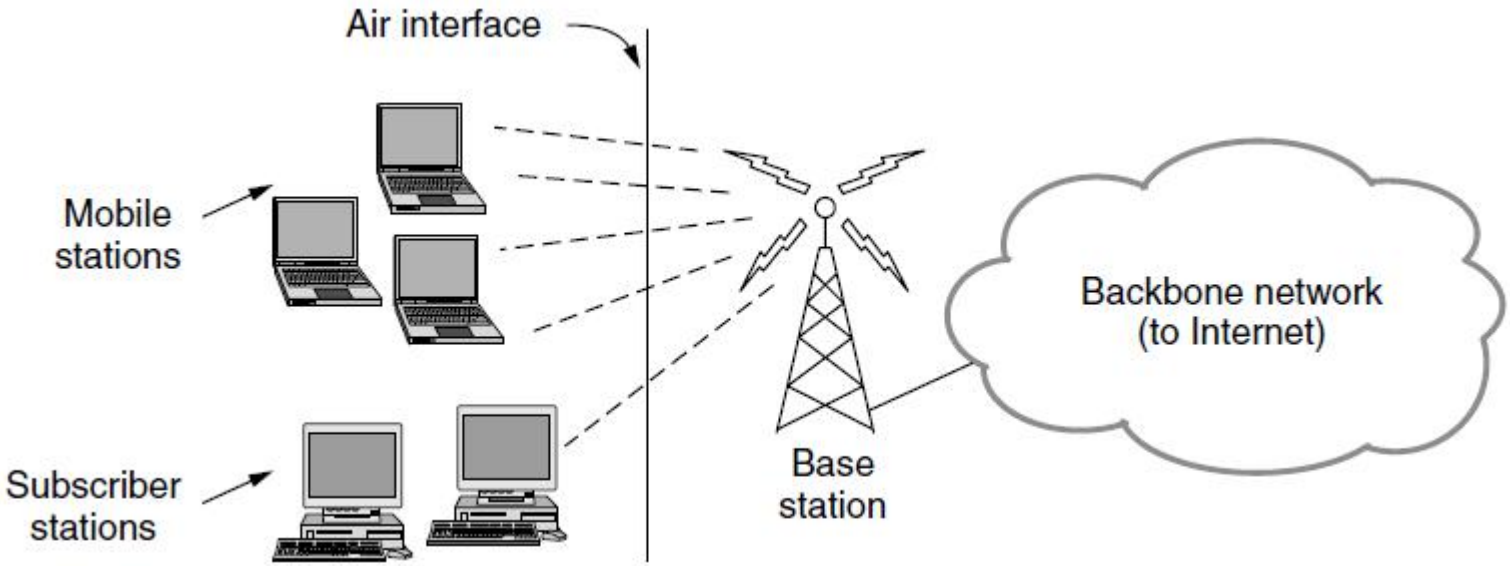
power saver asks the router to keep it in buffer

Broadband Wireless

- 802.16 Architecture / Protocol Stack »
- 802.16 Physical Layer »
- 802.16 MAC »
- 802.16 Frames »

802.16 Architecture/Protocol Stack (1)

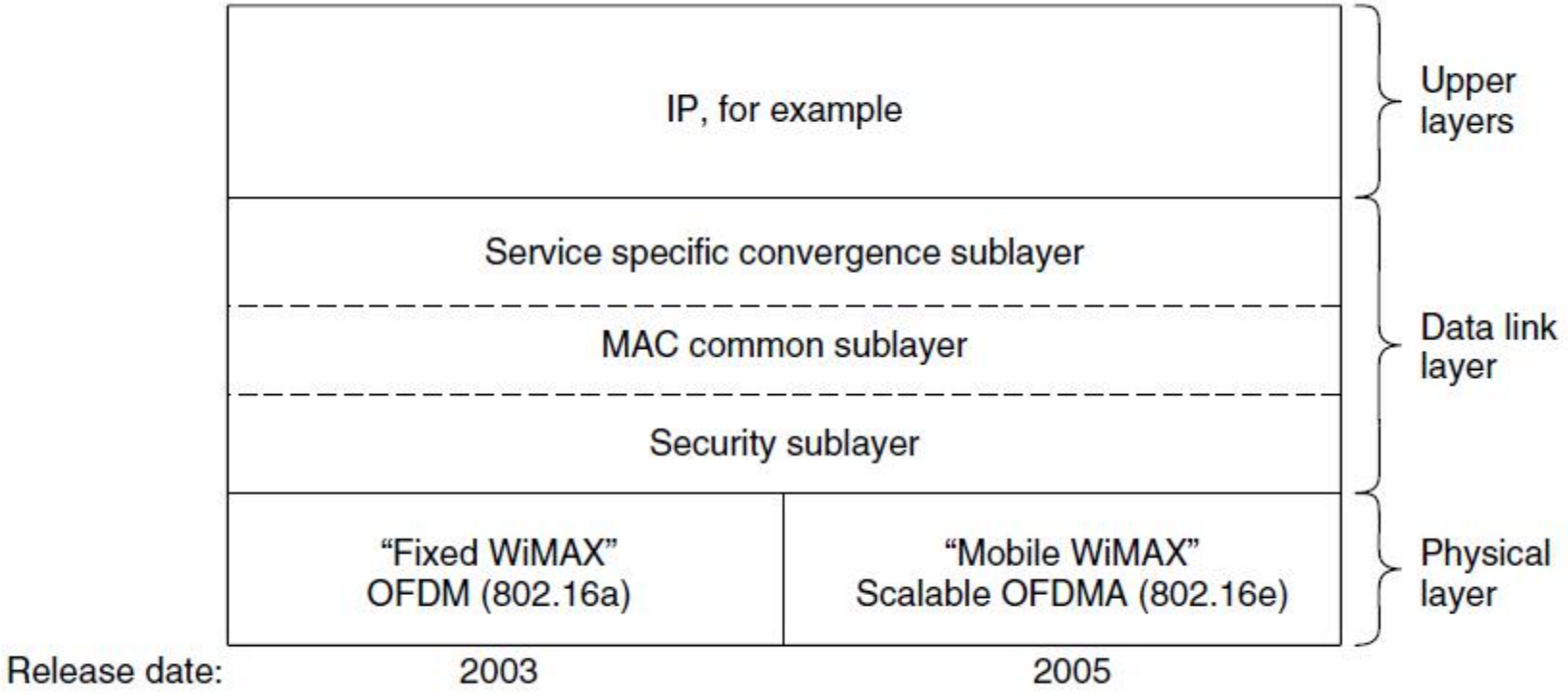
Wireless clients connect to a wired basestation (like 3G)



802.16 Architecture/Protocol Stack (2)

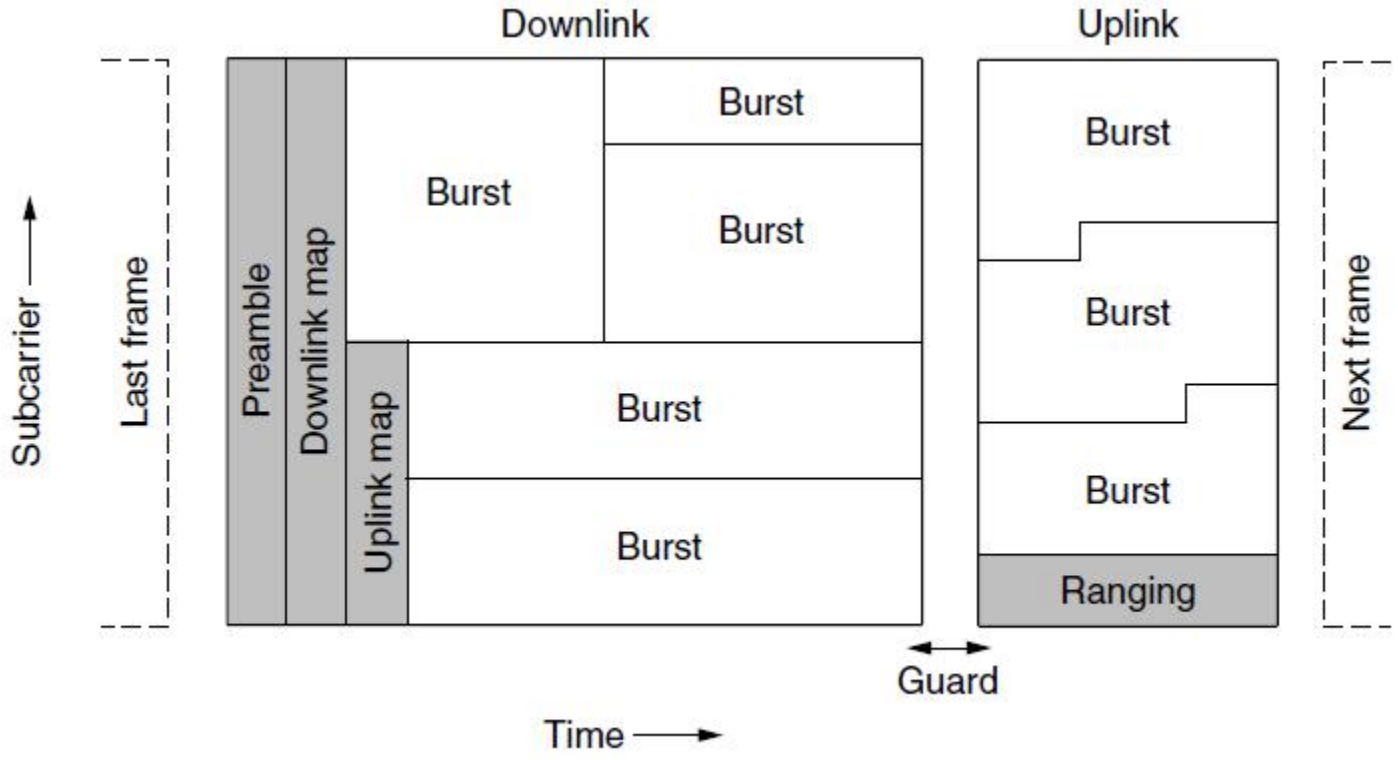
MAC is connection-oriented; IP is connectionless

- Convergence sublayer maps between the two



802.16 Physical Layer

Based on OFDM; base station gives mobiles bursts (subcarrier/time frame slots) for uplink and downlink



802.16 MAC

Connection-oriented with base station in control

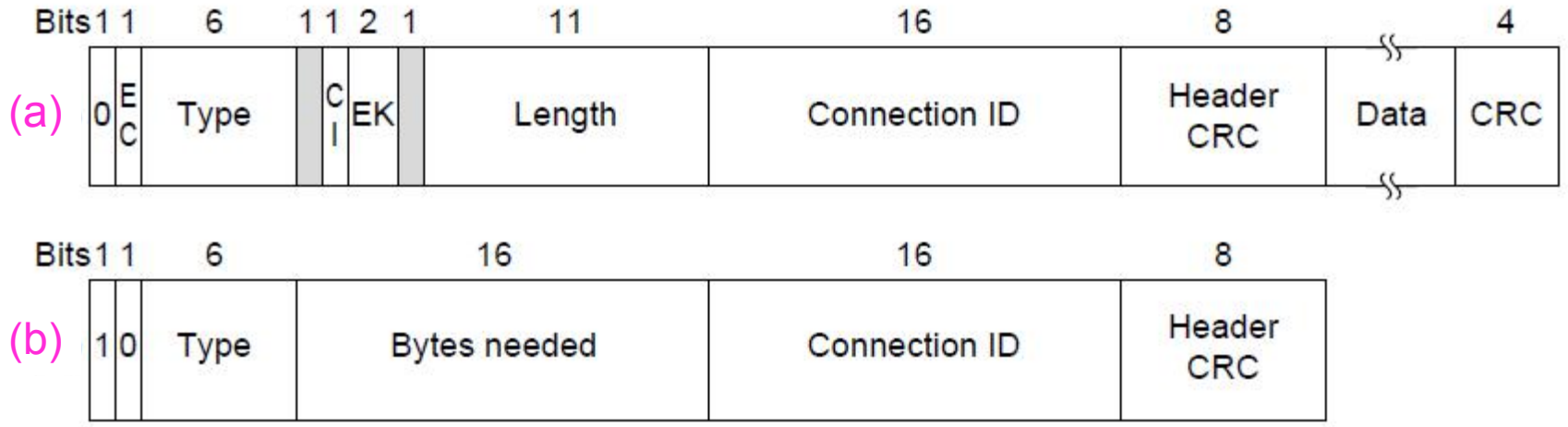
- Clients request the bandwidth they need

Different kinds of service can be requested:

- 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 Frames

- Frames vary depending on their type
- Connection ID instead of source/dest addresses



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

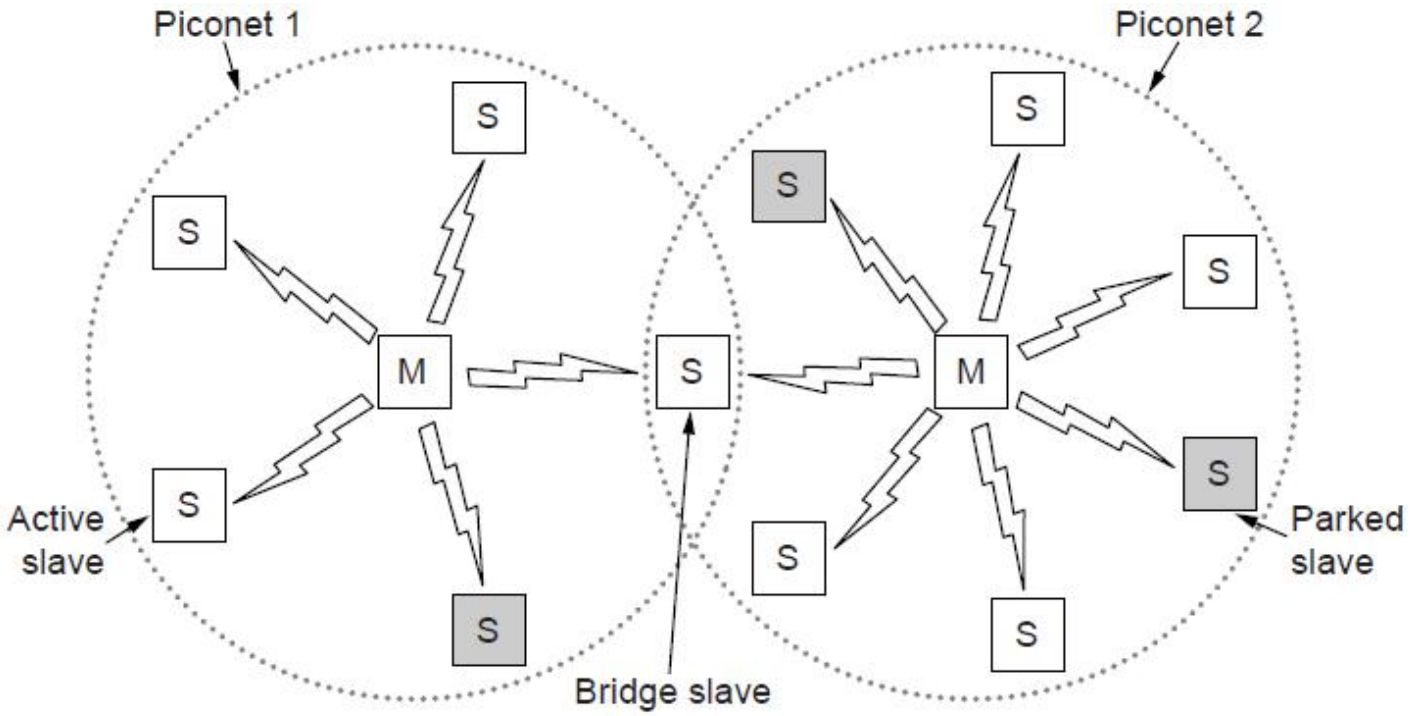
Bluetooth

- Bluetooth Architecture »
- Bluetooth Applications / Protocol »
- Bluetooth Radio / Link Layers »
- Bluetooth Frames »

Bluetooth Architecture

Piconet master is connected to slave wireless devices

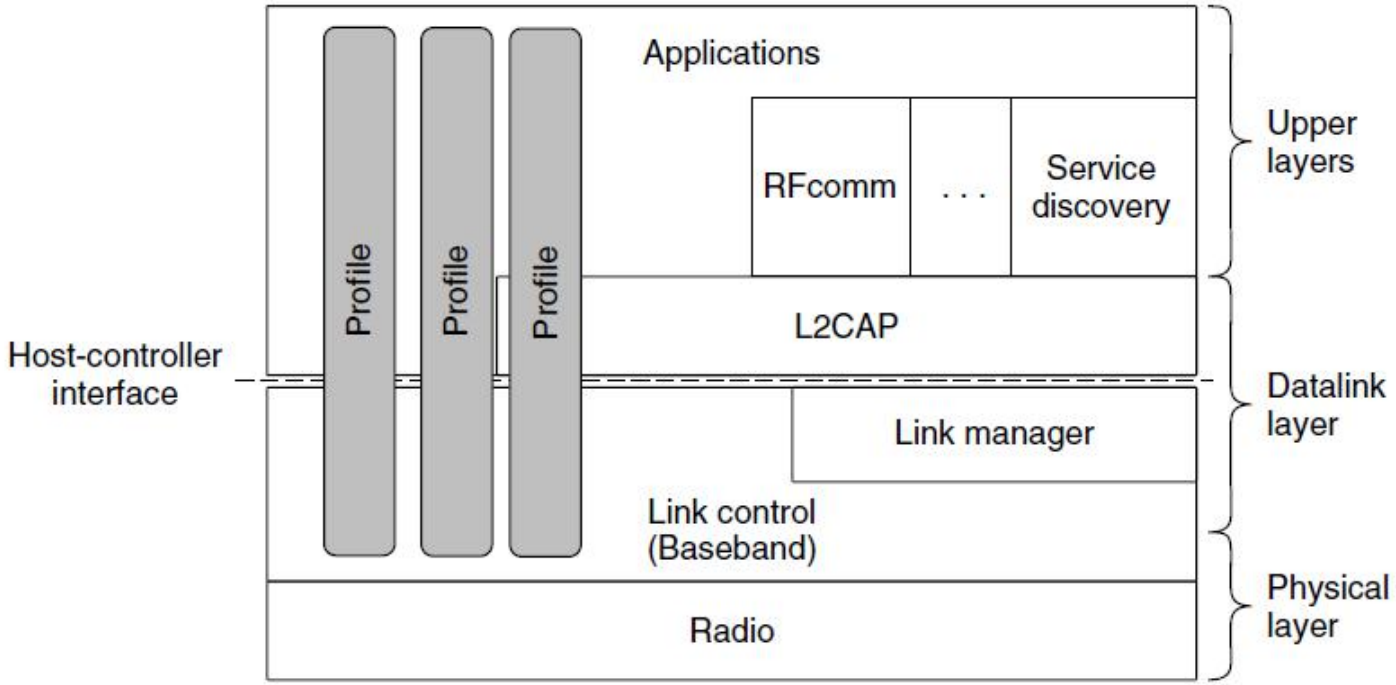
- Slaves may be asleep (parked) to save power
- Two piconets can be bridged into a scatternet



Bluetooth Applications / Protocol Stack

Profiles give the set of protocols for a given application

- 25 profiles, including headset, intercom, streaming audio, remote control, personal area network, …



Bluetooth Radio / Link Layers

Radio layer

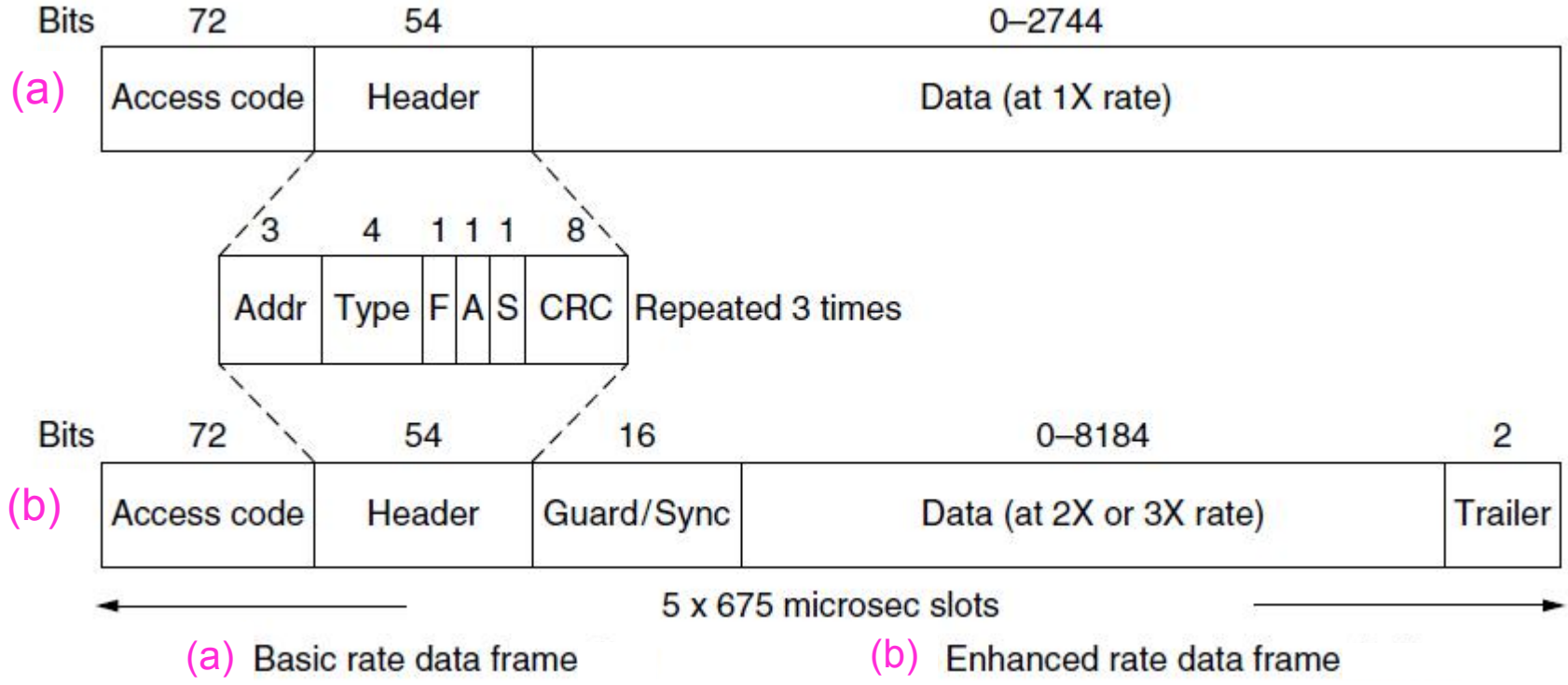
- Uses adaptive frequency hopping in 2.4 GHz band

Link layer

- TDM with timeslots for master and slaves
- Synchronous CO for periodic slots in each direction
- Asynchronous CL for packet-switched data
- Links undergo pairing (user confirms passkey/PIN) to authorize them before use

Bluetooth Frames

Time is slotted; enhanced data rates send faster but for the same time; addresses are only 3 bits for 8 devices

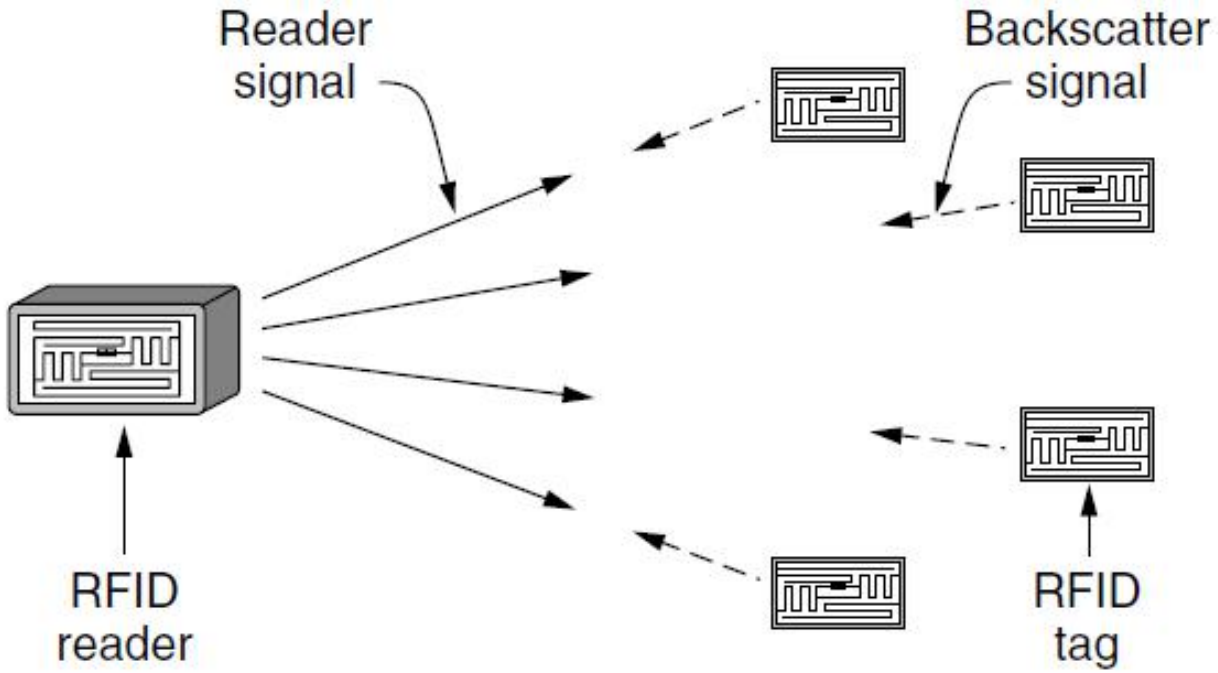


RFID

- Gen 2 Architecture »
- Gen 2 Physical Layer »
- Gen 2 Tag Identification Layer »
- Gen 2 Frames »

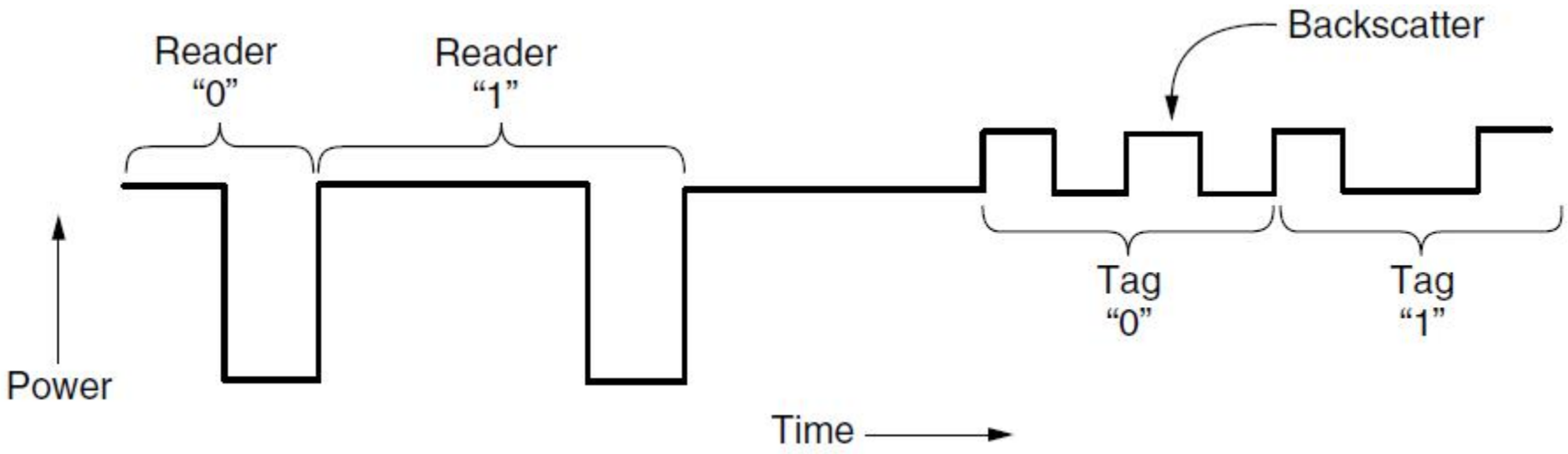
Gen 2 Architecture

Reader signal powers tags; tags reply with backscatter



Gen 2 Physical Layer

- Reader uses duration of on period to send 0/1
- Tag backscatters reader signal in pulses to send 0/1



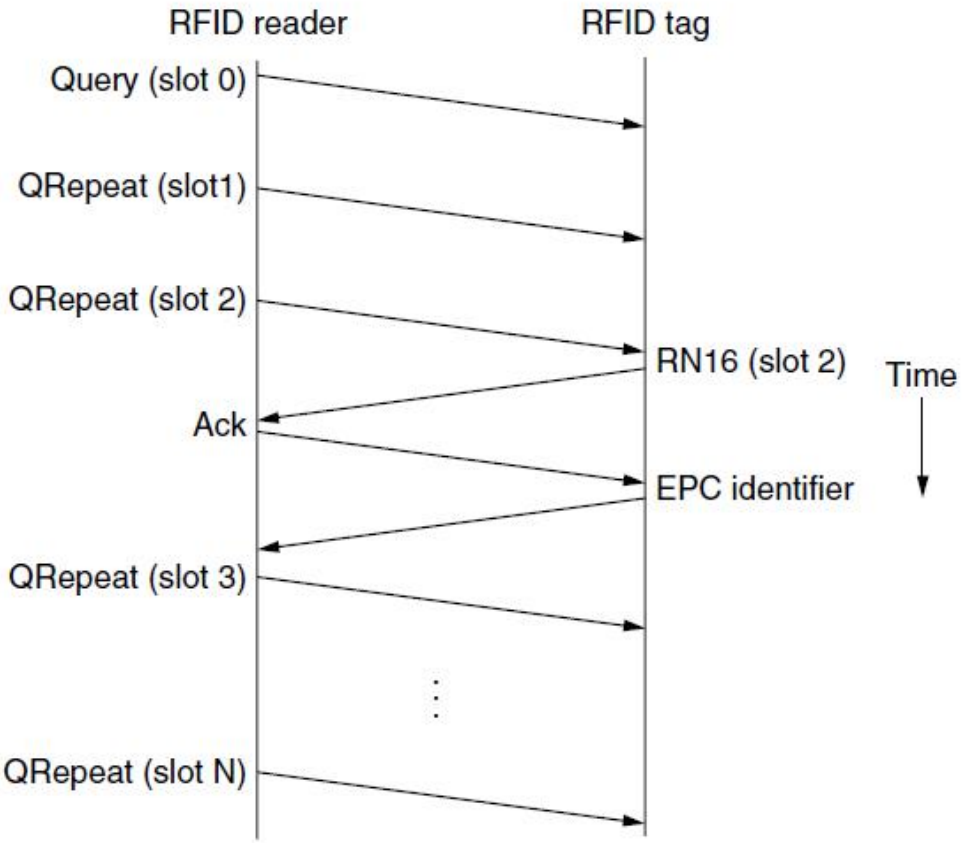
Gen 2 Tag Identification Layer

Reader sends query and sets slot structure

Tags reply (RN16) in a random slot; may collide

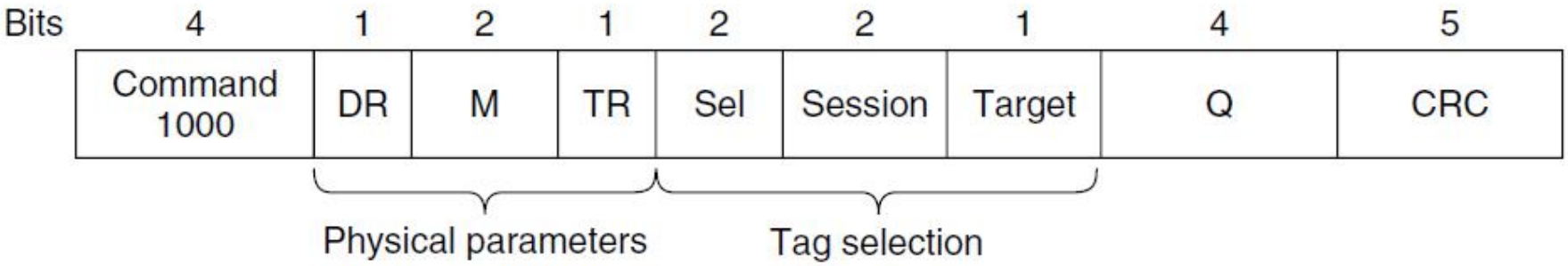
Reader asks one tag for its identifier (ACK)

Process continues until no tags are left



Gen 2 Frames

- Reader frames vary depending on type (Command)
  - Query shown below, has parameters and error detection
- Tag responses are simply data
  - Reader sets timing and knows the expected format



Query message

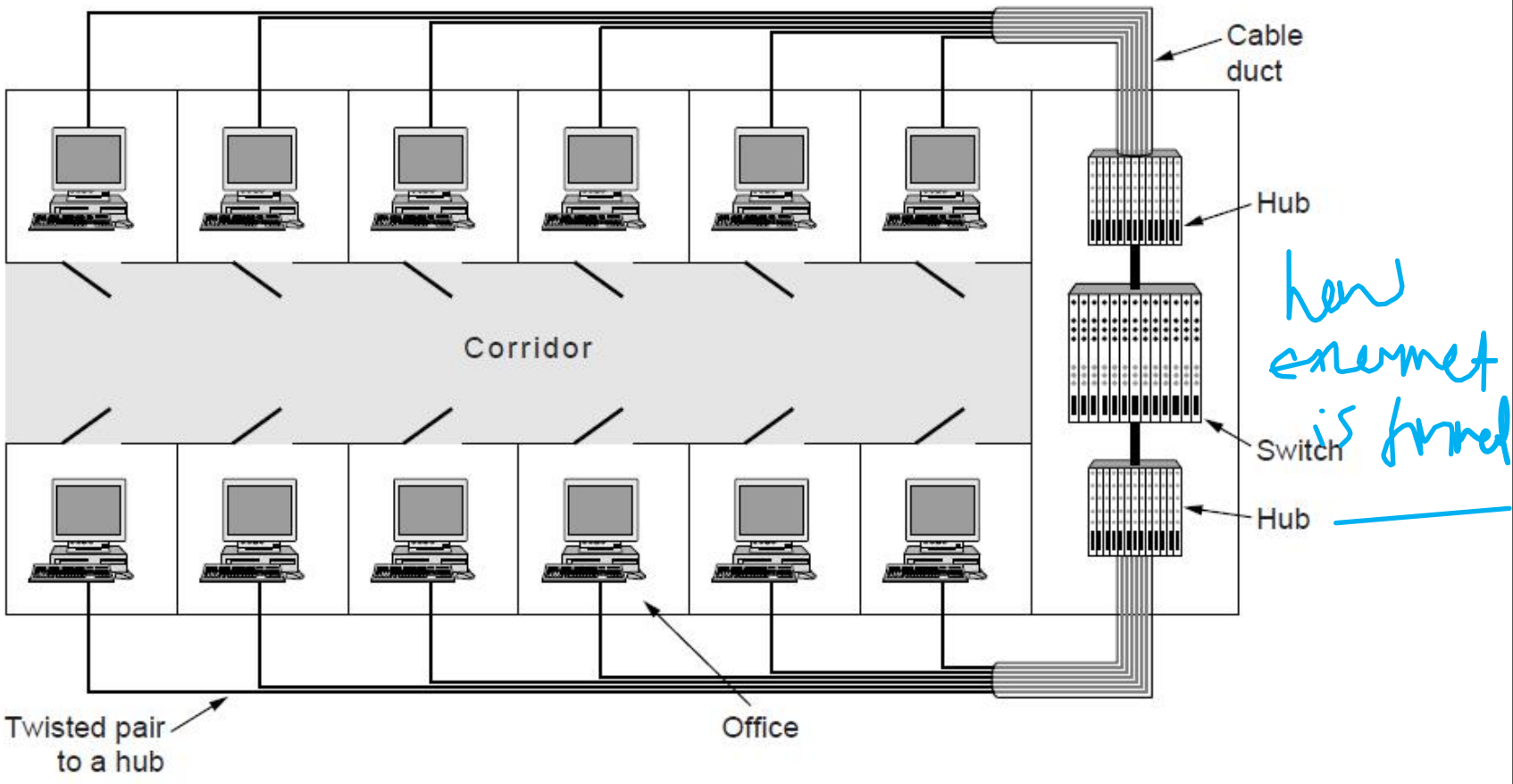
Data Link Layer Switching

- Uses of Bridges »
- Learning Bridges »
- Spanning Tree »
- Repeaters, hubs, bridges, .., routers, gateways »
- Virtual LANs »

Uses of Bridges

Common setup is a building with centralized wiring

- Bridges (switches) are placed in or near wiring closets



Learning Bridges (1)

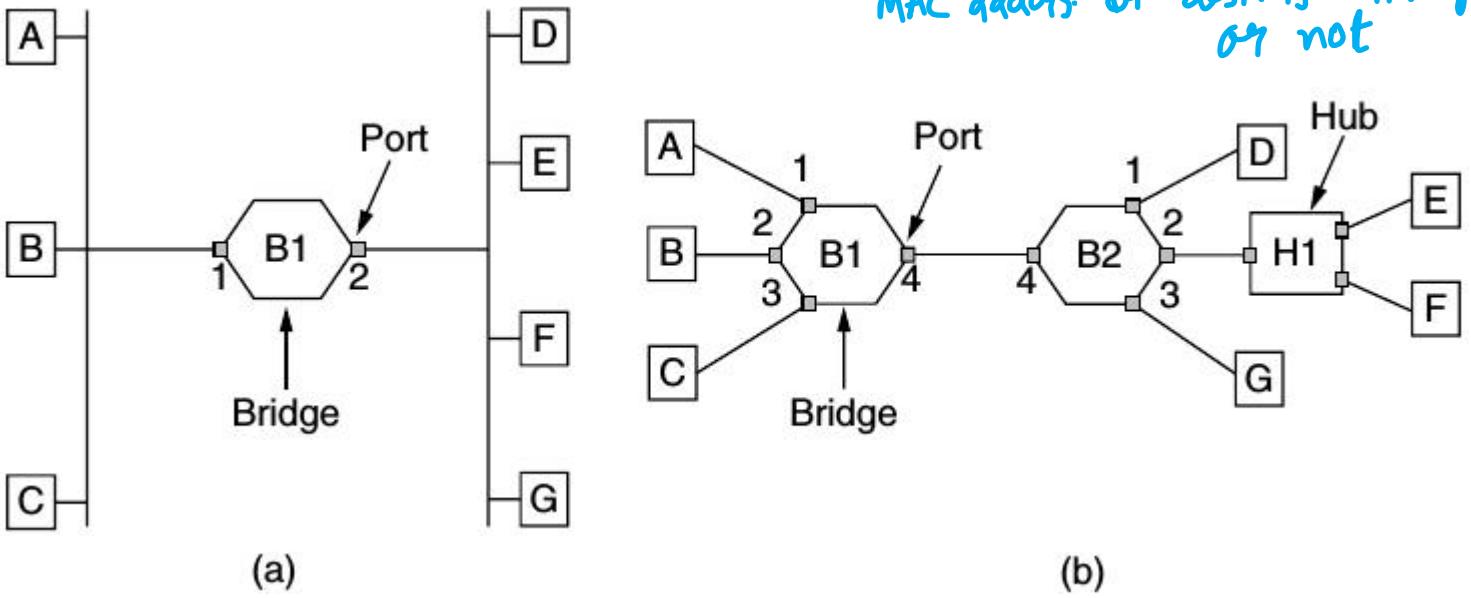
As hub doesn't have table it always broadcasts the packet

Switch maintains a table whereas hub doesn't

A bridge operates as a switched LAN (not a hub)

- Computers, bridges, and hubs connect to its ports
- Bridges operate in promiscus mode

↳ Accepts the packet whether or not MAC addrs of dest. is matching or not



Learning Bridges (2)

when switch learning about MAC address on itself

Backward learning algorithm picks the output port:

- Associates source address on frame with input port
- Frame with destination address sent to learned port
- Unlearned destinations are sent to all other ports

Needs no configuration

- Forget unused addresses to allow changes
- Bandwidth efficient for two-way traffic

Forwrding procedure

1. If the port for the destination address is the same as the source port, discard the frame. SRC=DST | discard
2. If the port for the destination address and the source port are different, forward the frame on to the destination port. S → D
3. If the destination port is unknown, use flooding and send the frame on all ports except the source port. S → all except SRC

This algorithm needs to be applied for each frame, hence it is implemented in special-purpose VLSI chips

flooding is Routing alg

Bridge forwarding types

Slower

- A store-and-forward switch stores each incoming frame in its entirety, then examines it and forwards it.
- A cut-through switch starts to forward incoming frames before they have arrived completely. As soon as the destination address is in, the forwarding can begin.
- Store-and-forward switches store entire frames before forwarding them. After a frame comes in, the checksum can be verified. If the frame is damaged, it is discarded immediately.

Faster

- With cut-through, damaged frames cannot be discarded by the switch because by the time the error is detected, the frame is already gone.

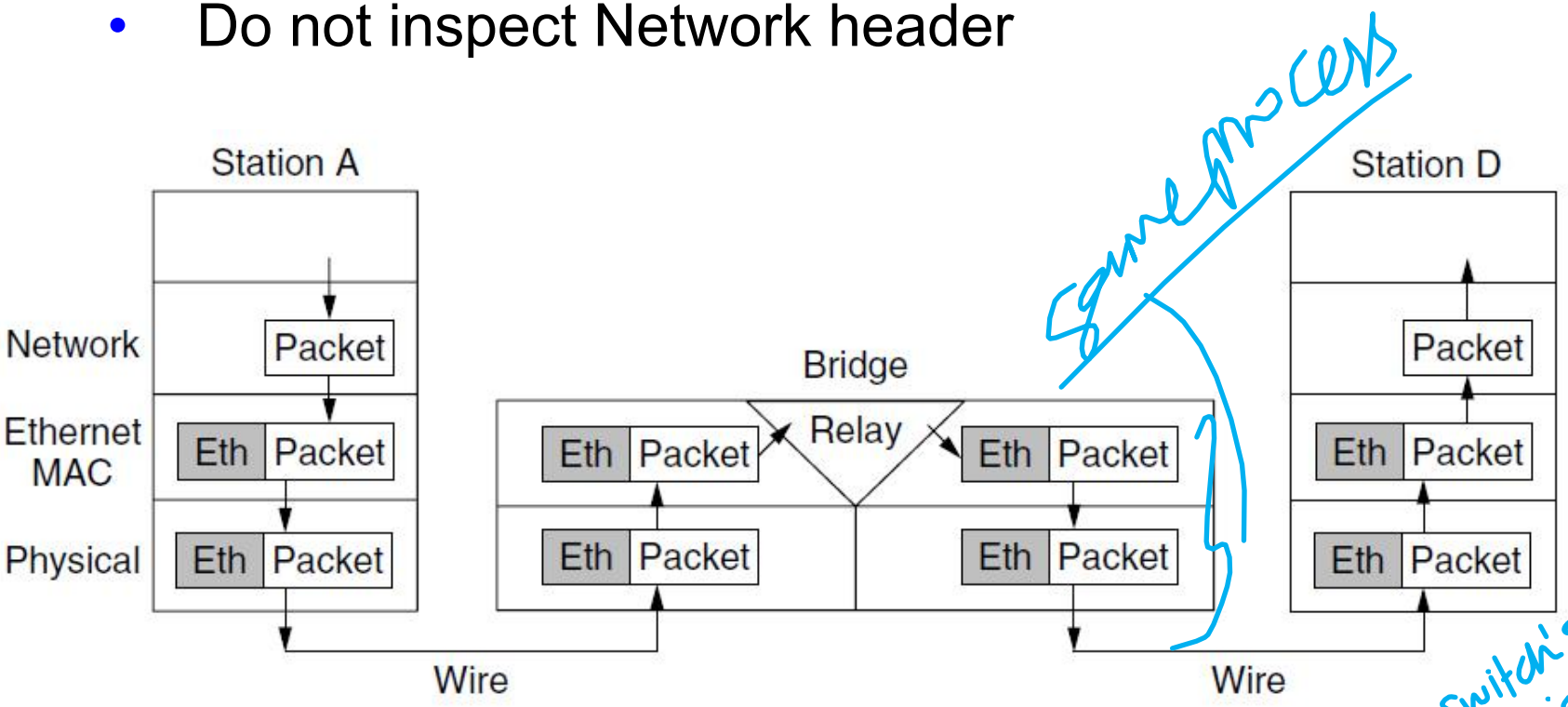
byte-by-byte

not validated in cut through

Learning Bridges (3)

Bridges extend the Link layer:

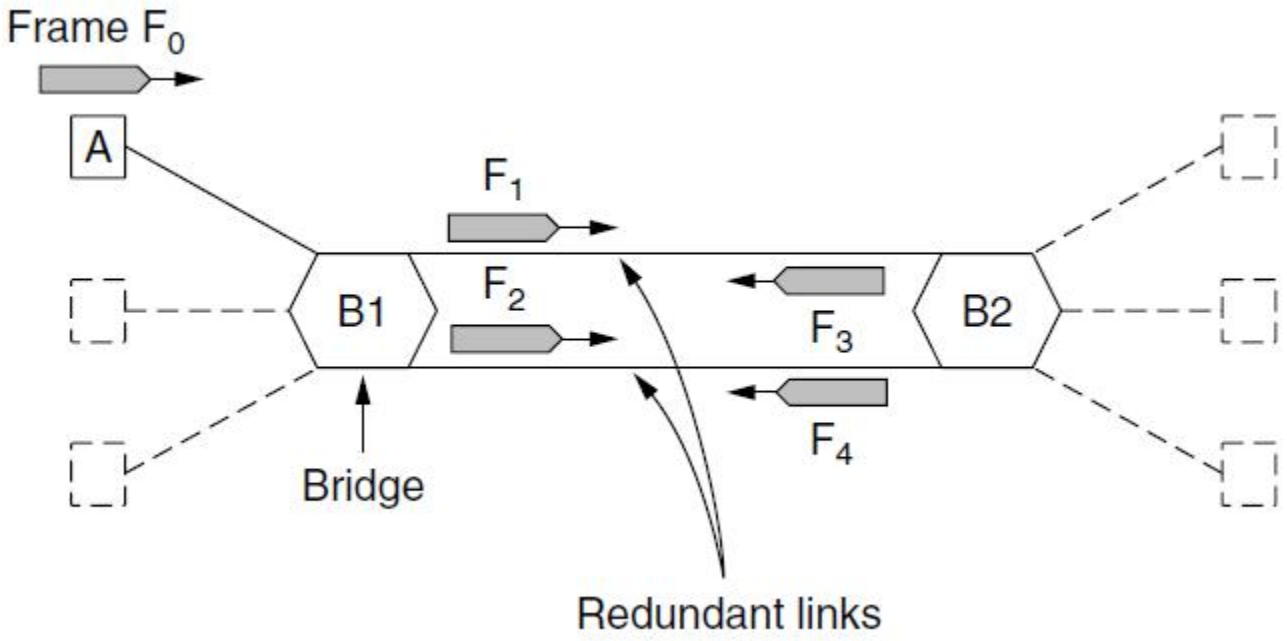
- Use but don't remove Ethernet header/addresses
- Do not inspect Network header



Spanning Tree (1) – Problem

Bridge topologies with loops and only backward learning will cause frames to circulate for ever

- Need spanning tree support to solve problem



Spanning Tree (2) – Algorithm

- Subset of forwarding ports are used to avoid loops
- Selected with the spanning tree distributed algorithm by Perlman

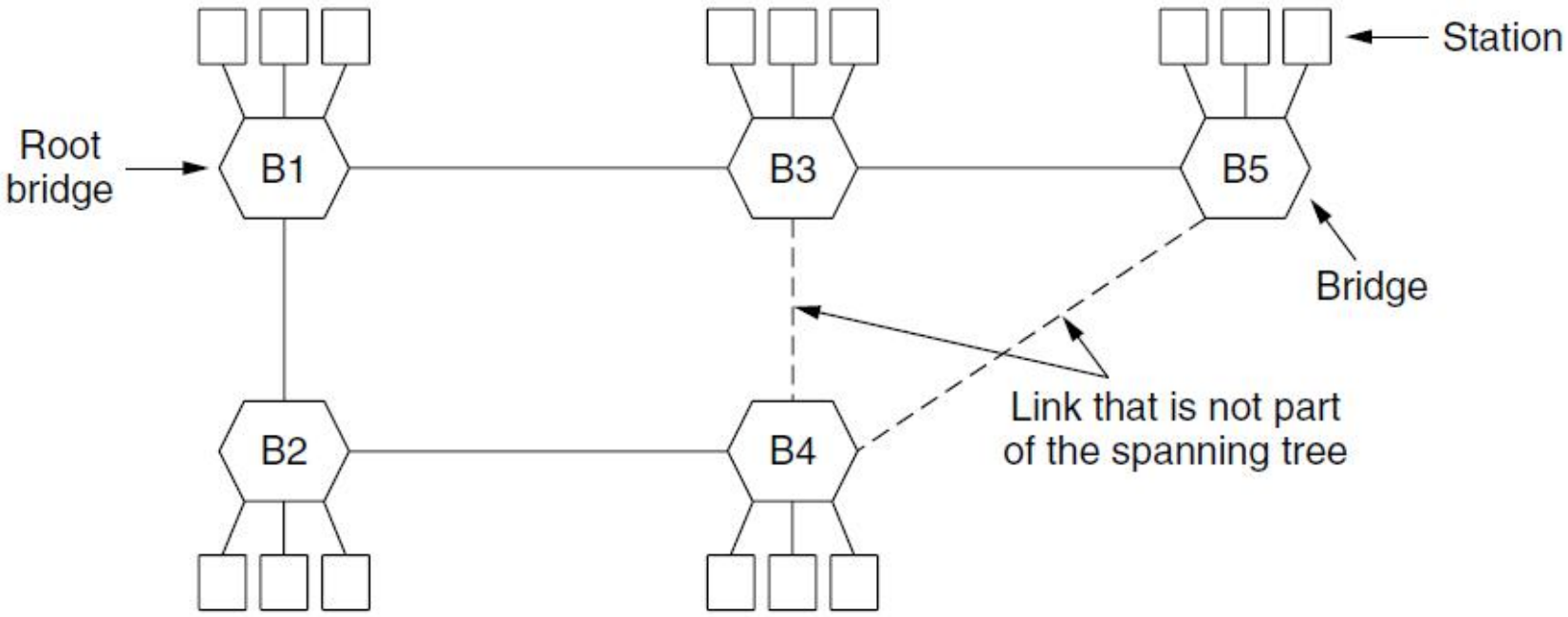
I think that I shall never see
A graph more lovely than a tree.
A tree whose crucial property
Is loop-free connectivity.
A tree which must be sure to span.
So packets can reach every LAN.
First the Root must be selected
By ID it is elected.
Least cost paths from Root are traced
In the tree these paths are placed.
A mesh is made by folks like me
Then bridges find a spanning tree.

– Radia Perlman, 1985.

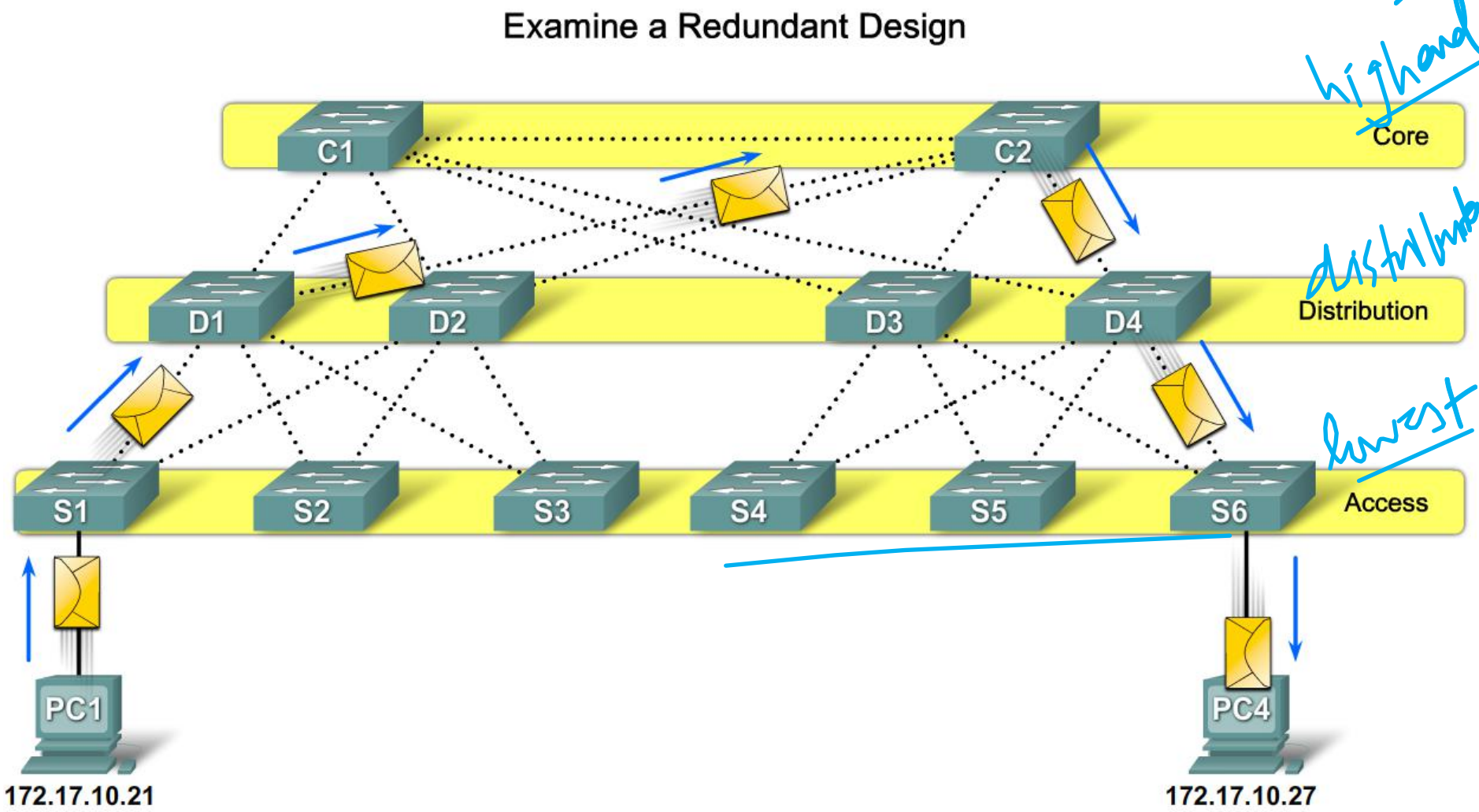
Spanning Tree (3) – Example

After the algorithm runs:

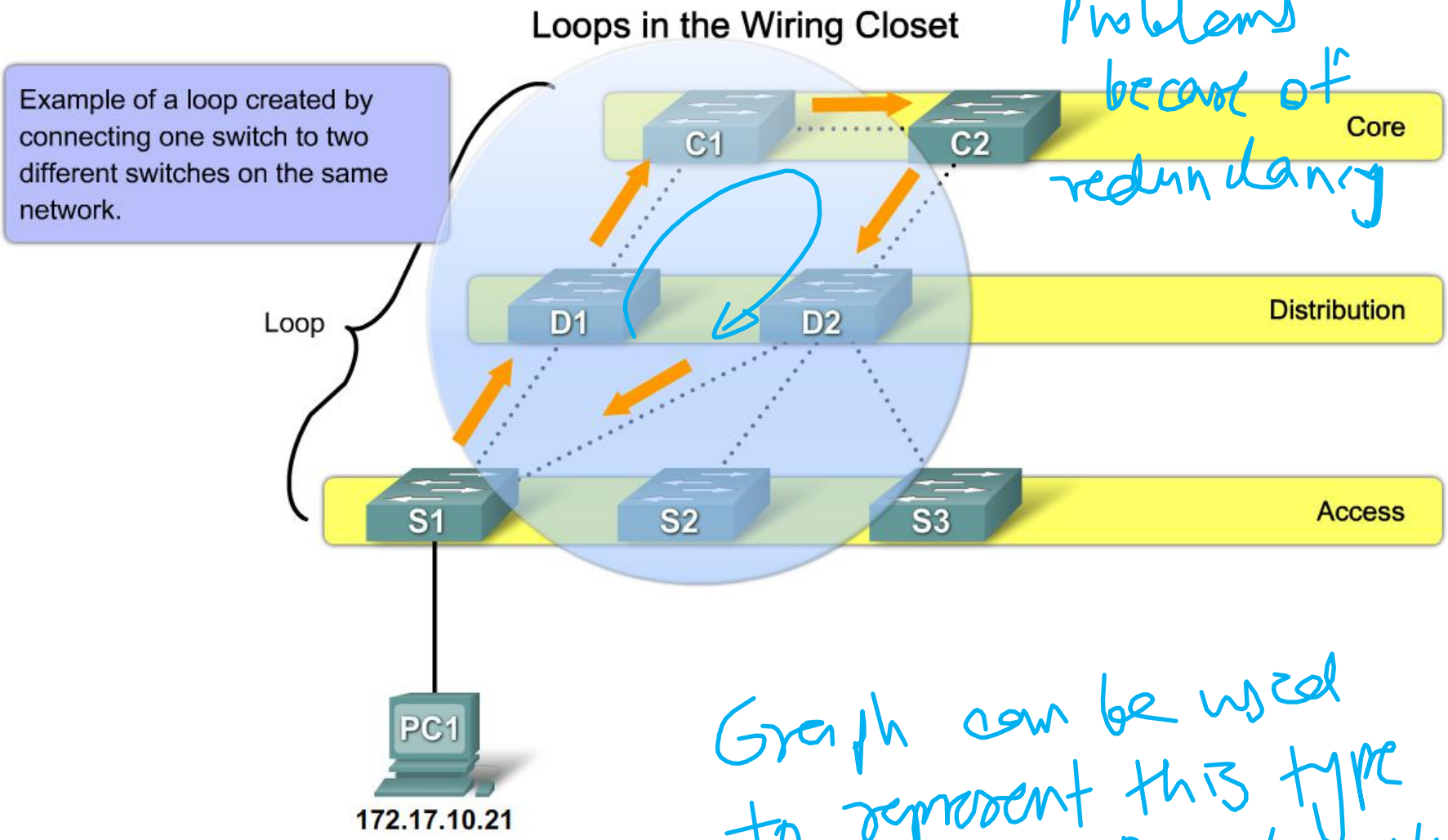
- B1 is the root, two dashed links are turned off
- B4 uses link to B2 (lower than B3 also at distance 1)
- B5 uses B3 (distance 1 versus B4 at distance 2)



Role of Redundancy in Network



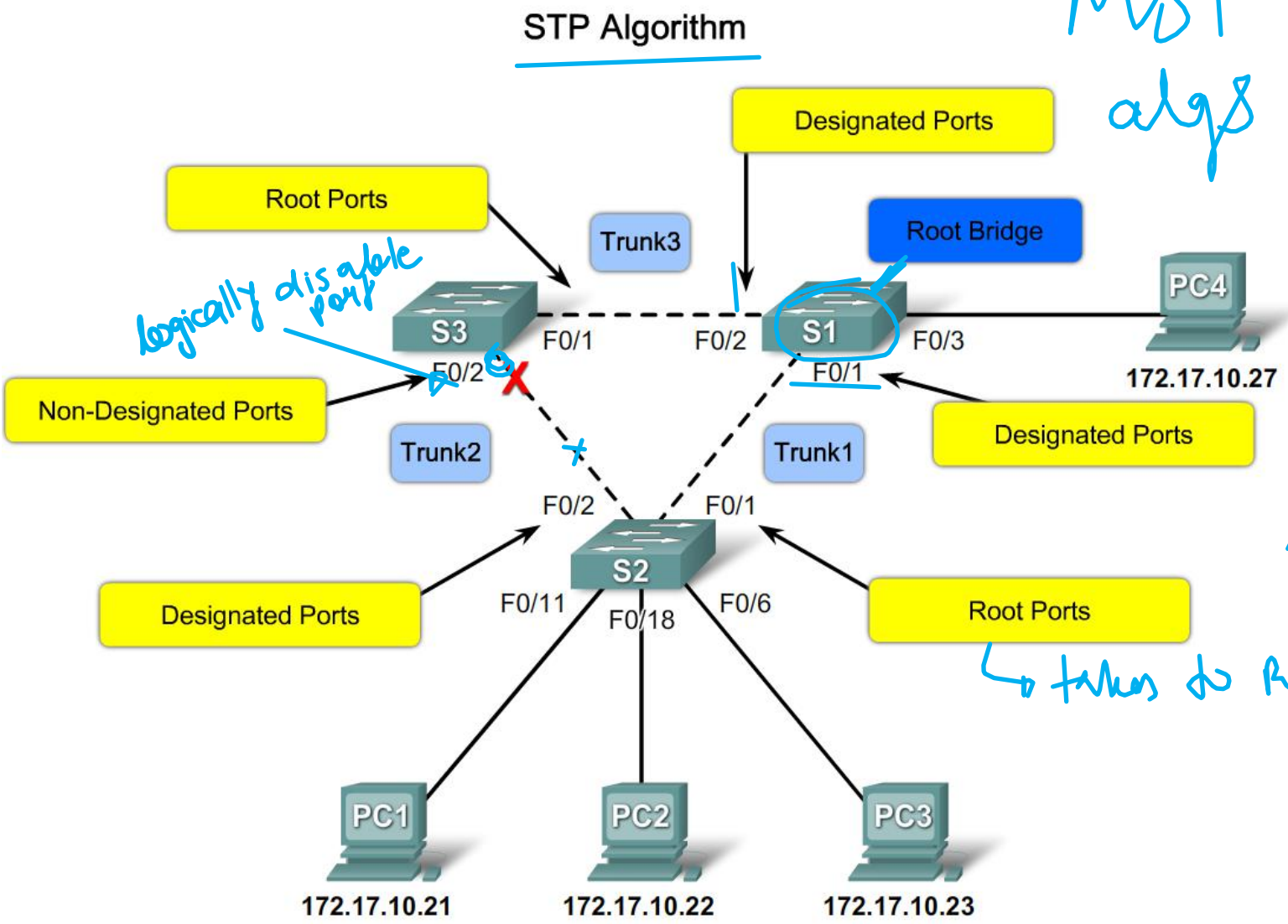
Role of Redundancy in Network



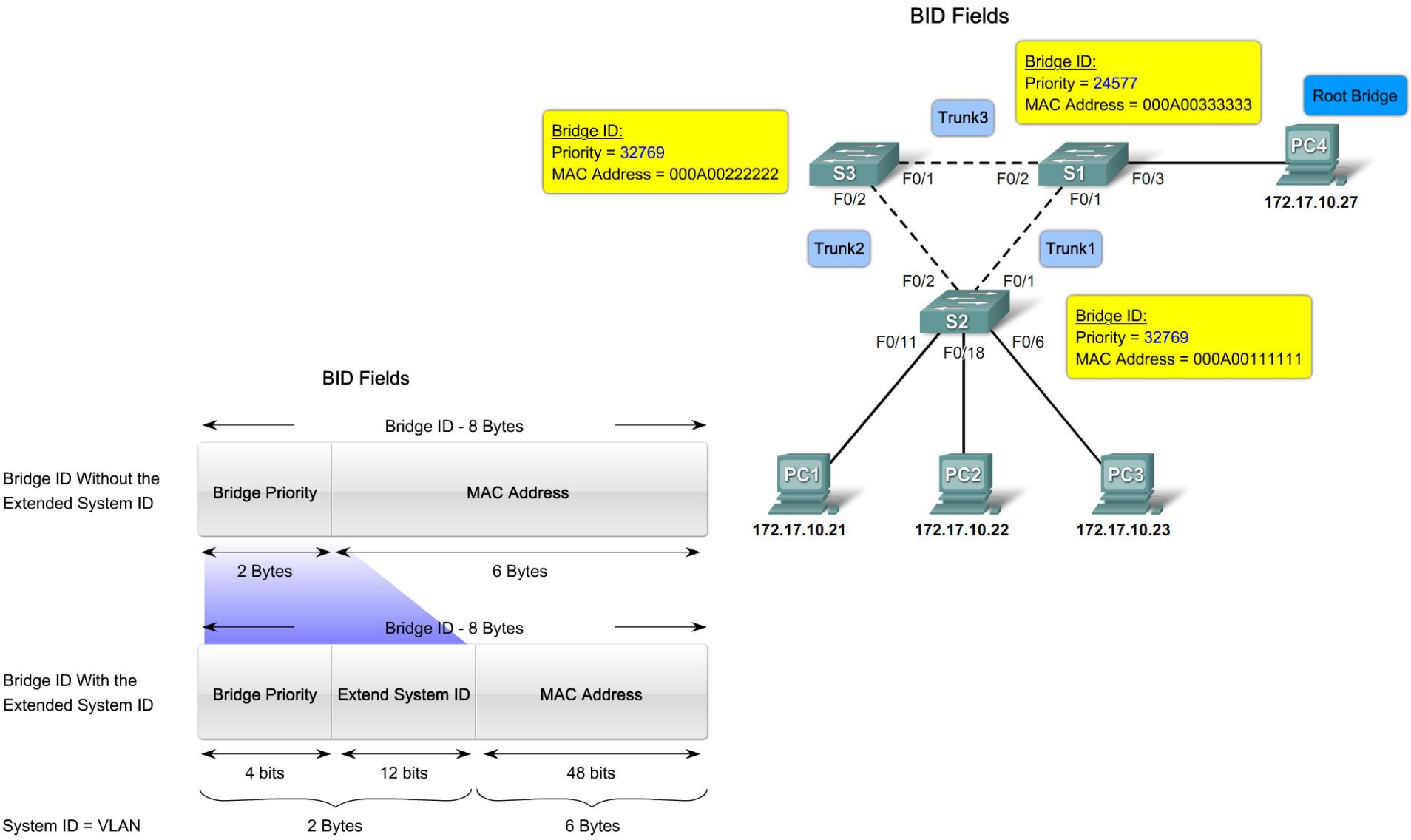
Problems because of redundancy

Graph can be used to represent this type of network

Eliminate Layer 2 Loops in Network



Eliminate Layer 2 Loops in Network



STP Algorithm – Step 1

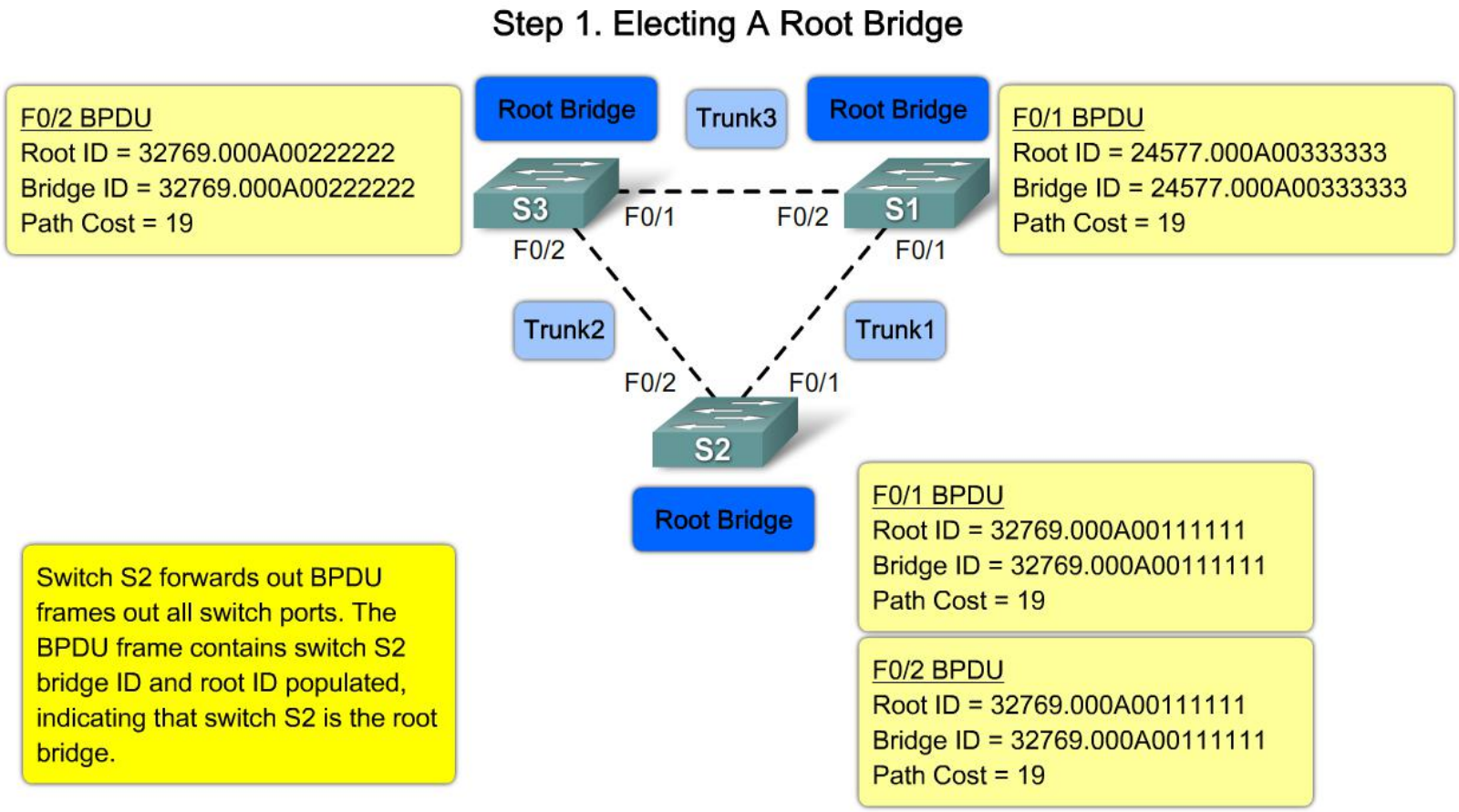
The bridge with the lowest Bridge ID (BID) becomes the root bridge.

BPDUs containing BID is exchanged between the switches to elect a root bridge

All ports on the root bridge are set as designated and thus are always set to a forwarding state.

STP Algorithm – Step 1

STP decision sequence is used to elect a root bridge for a network



STP Algorithm – Step 2

Elect Root Port

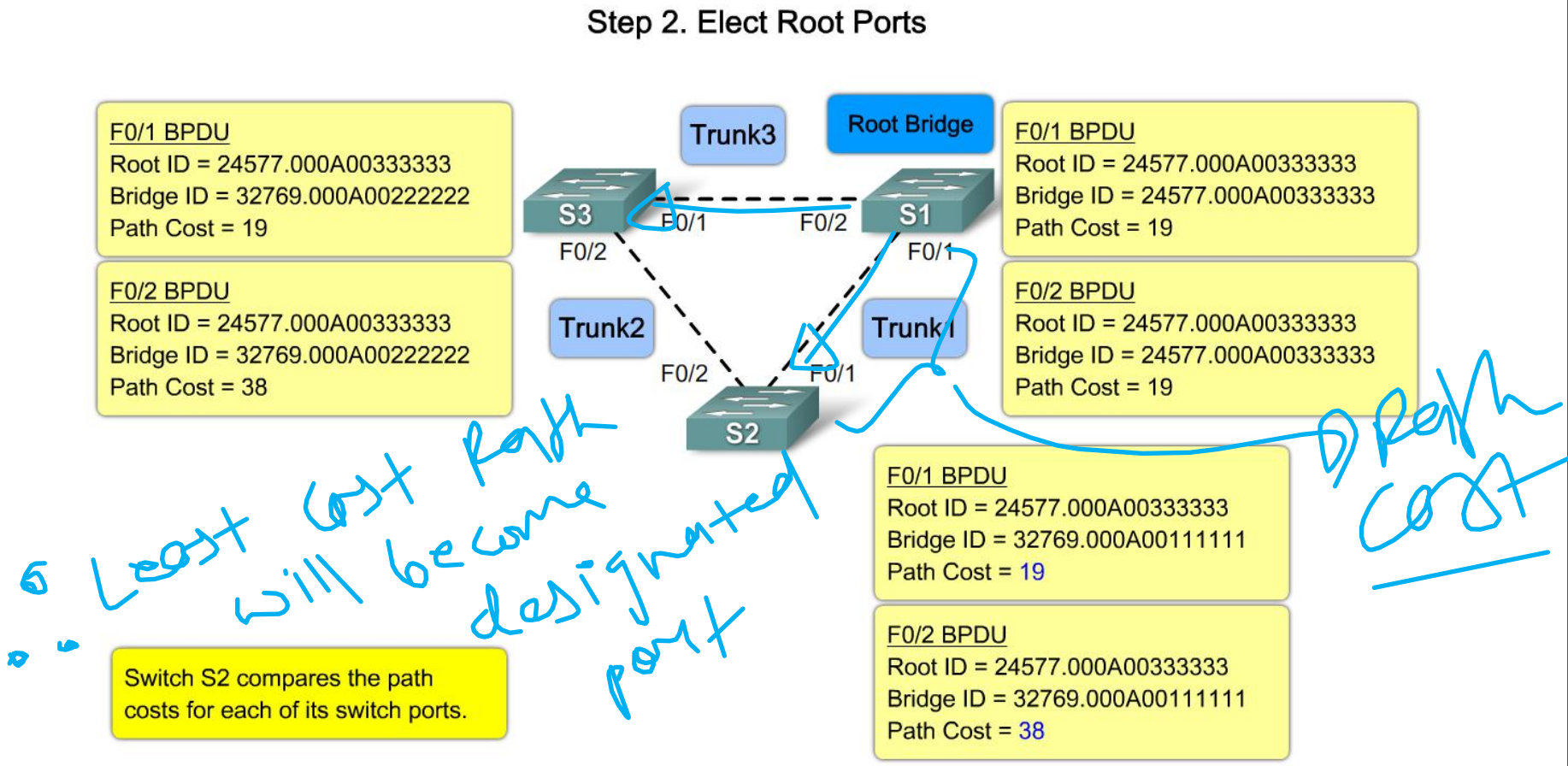
For non-root bridges there will be only one root port. The root port will be the port with the lowest path cost to the root bridge. The root port will also be set to forwarding state.

Link Speed	STP cost
4 Mbps	250
10 Mbps	100
16 Mbps	62
100 Mbps	19
1 Gbps	4
10 Gbps	2

Cost of the path can be c[illegible]ning-tree cost N command

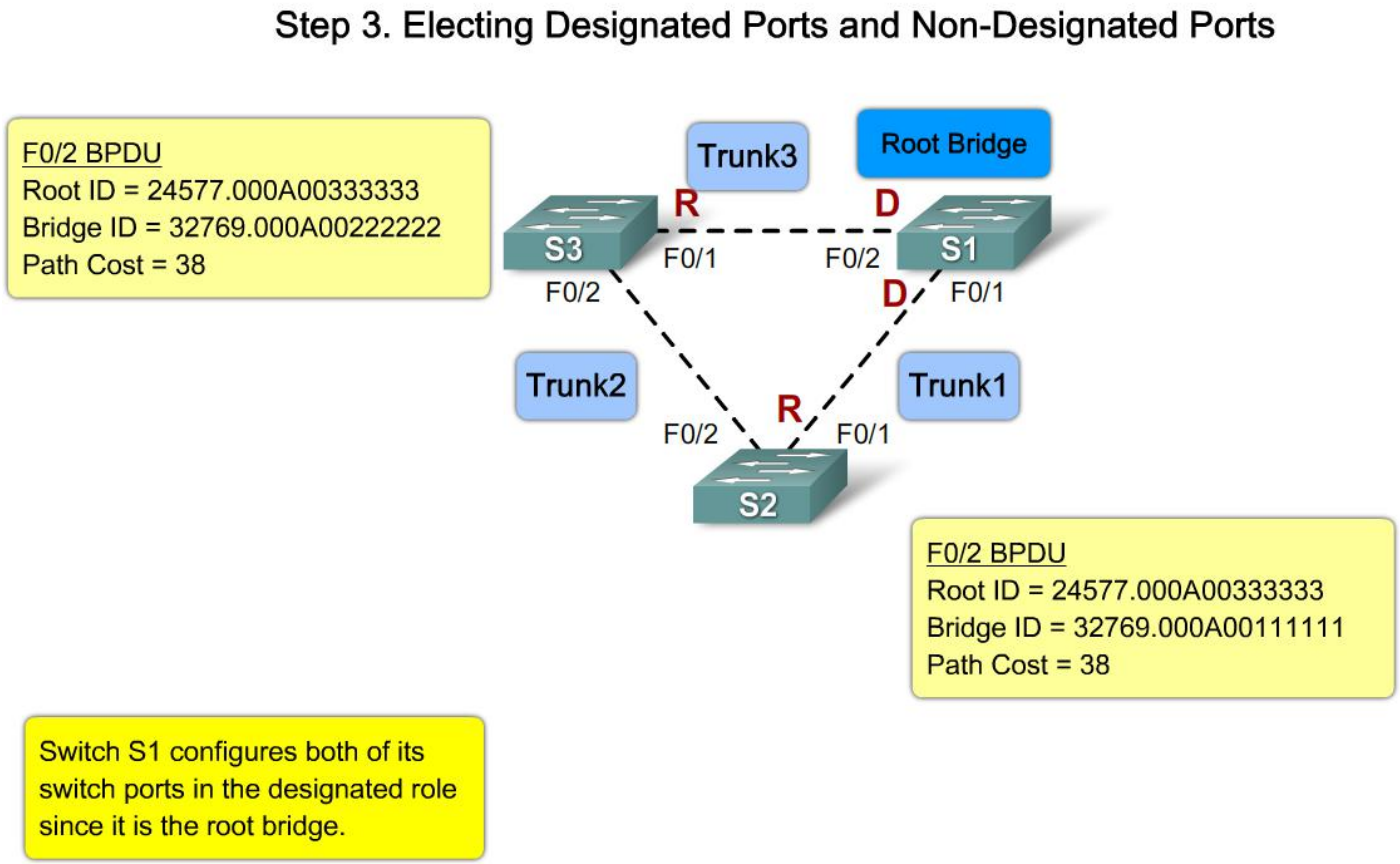
STP Algorithm – Step 2

Electing a root port on a switch



STP Algorithm – Step 3

Electing designated ports and non-designated ports on a switch



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

Devices are named according to the layer they process

- A bridge or LAN switch operates in the Link layer

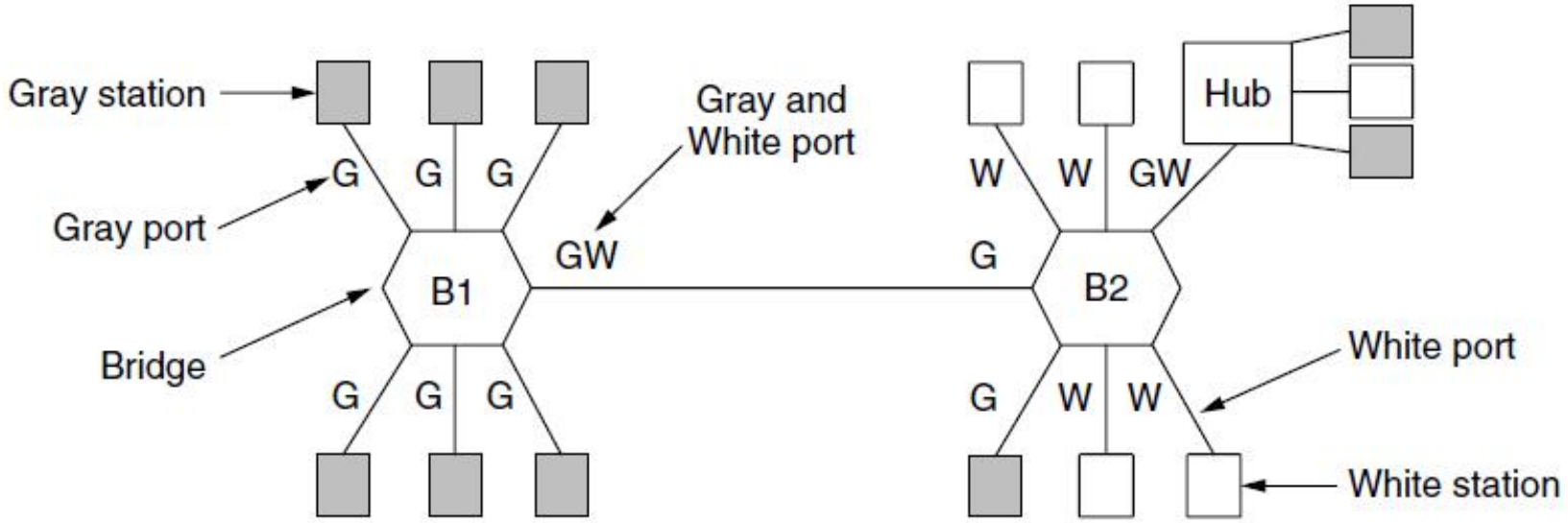
Application layer	Application gateway
Transport layer	Transport gateway
Network layer	Router
Data link layer	Bridge, switch
Physical layer	Repeater, hub

Virtual LANs - IEEE 802.1Q

↳ Divide single LAN into 2 parts

VLANs (Virtual LANs) splits one physical LAN into multiple logical LANs to ease management tasks

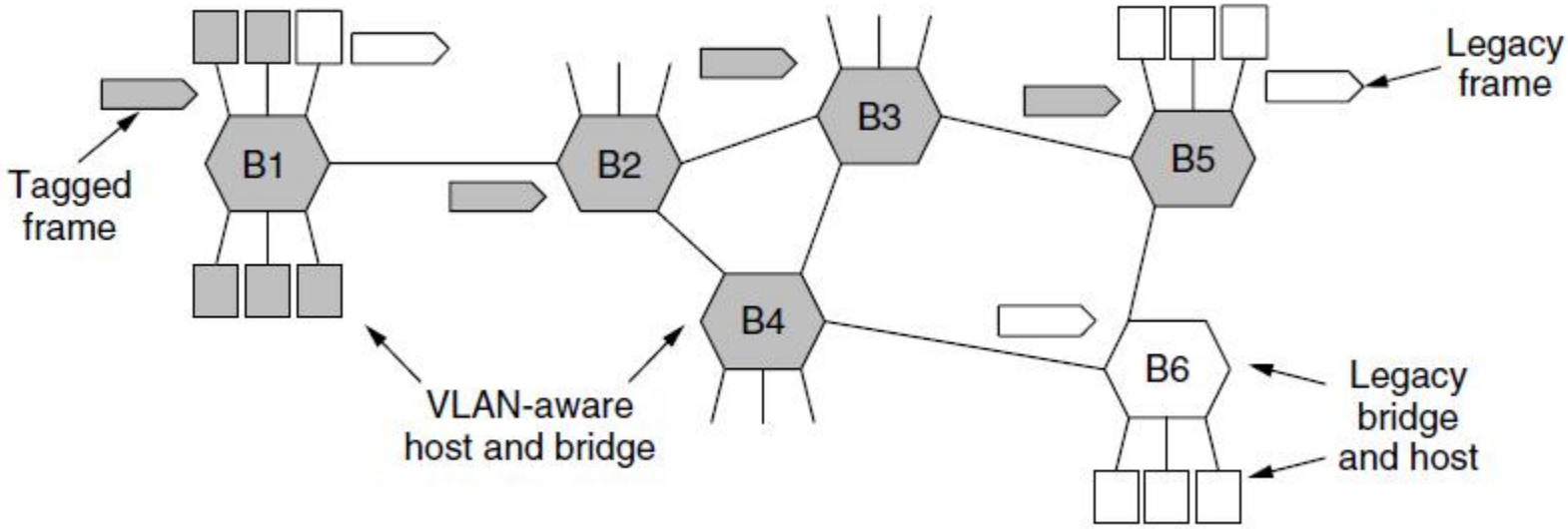
- Ports are “colored” according to their VLAN



Virtual LANs – IEEE 802.1Q

Bridges need to be aware of VLANs to support them

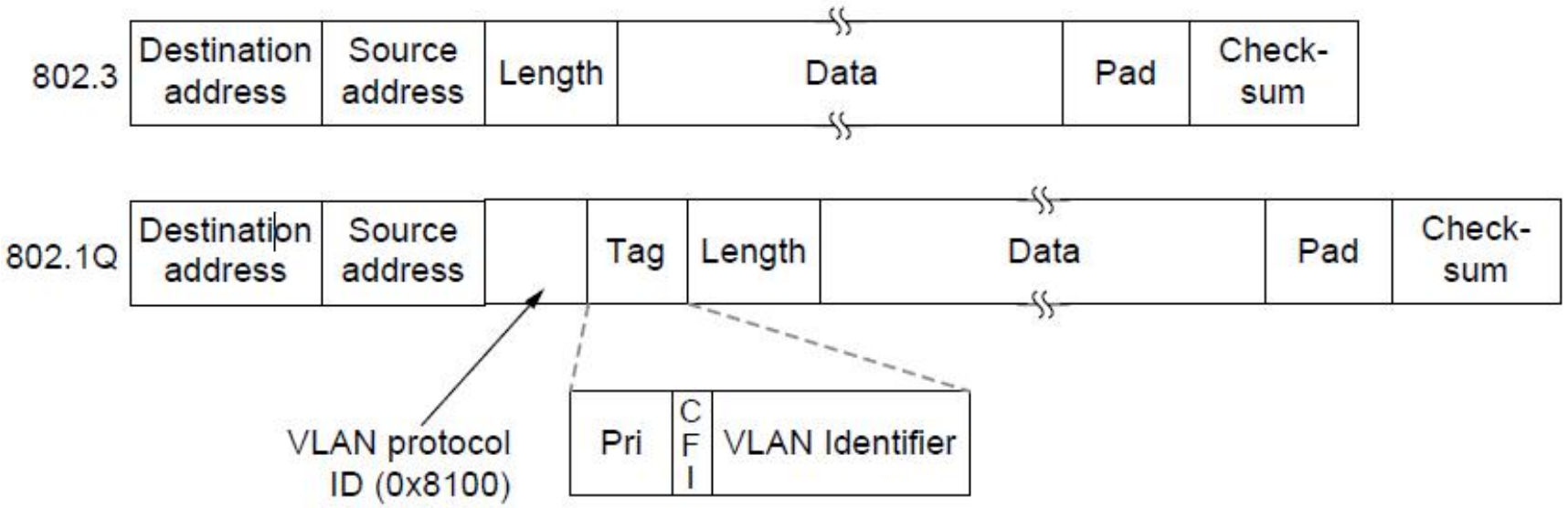
- In 802.1Q, frames are tagged with their "color"
- Legacy switches with no tags are supported



Virtual LANs – IEEE 802.1Q

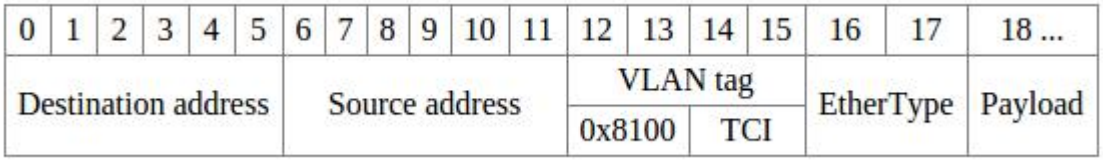
802.1Q frames carry a color tag (VLAN identifier)

- Length/Type value is 0x8100 for VLAN protocol



VLAN - Tagging

- It is placed between the source MAC and the EtherType fields



- The first two bytes of the tag contain the TPID (tag protocol identifier), which is defined to be equal to 0x8100
- The remaining two bytes contain the TCI (tag control information), of which 12 bits correspond to the VID and 4 bits contain metadata used for quality of service management.

VLAN - Numbering

- Each 802.1Q VLAN is identified by a 12-bit integer called a VID (VLAN Identifier) in the range 1 to 4094 inclusive.
- The values 0 and 4095 are reserved and should not be used.
- The first VLAN, with a VID of 1, is the default VLAN to which ports are presumed to belong

VLAN - Ports

- There are two ways in which a machine can be connected to a switch carrying 802.1Q VLAN traffic:
  - via an access port, where VLAN support is handled by the switch (so the machine sees ordinary, untagged Ethernet frames); or
  - via a trunk port, where VLAN support is handled by the attached machine (which sees 802.1Q-tagged Ethernet frames).
- It is also possible to operate a switch port in a hybrid mode, where it acts as an access port for one VLAN and a trunk port for others (so the attached Ethernet segment carries a mixture of tagged and untagged frames)

End

Chapter 4