

Computer Networks I

Data Link Layer – Local Area Network (LAN)

Prof. Dr.-Ing. **Lars Wolf**

IBR, TU Braunschweig
Mühlenpfordtstr. 23, D-38106 Braunschweig, Germany,
Email: wolf@ibr.cs.tu-bs.de

Scope

Complementary Courses					
	Applications	Transitions, Address.	Email	Web	⋮
L5	Application Layer				
L4	Transport Layer		Internet: (TCP, UDP, ...)		
L3	Network Layer		Internet: (IP, ...)		
L2	Data Link Layer		LAN, ..., WAN: (ETH, ...)		
L1	Physical Layer		Other lectures of ET/IT, ...		
Introduction					

Overview

- 1 What are Local Area Networks (LANs)?
- 2 Medium Access Control (MAC)
- 3 Dynamic Channel Allocation: Contention Free
- 4 Dynamic Channel Allocation: with Contention
- 5 Reference Model and Logical Link Control
- 6 Link Layer Addressing
- 7 IEEE 802.3: CSMA / CD
- 8 IEEE 802.5: Token Ring
- 9 Faster IEEE 802.3 Variants
- 10 IEEE 802.11 Wireless LANs

1 What are Local Area Networks (LANs)?

Processor Distance	CPUs are in a common ..	Example
...
10 m	room	LAN
100 m	building	
1 km	campus	
...

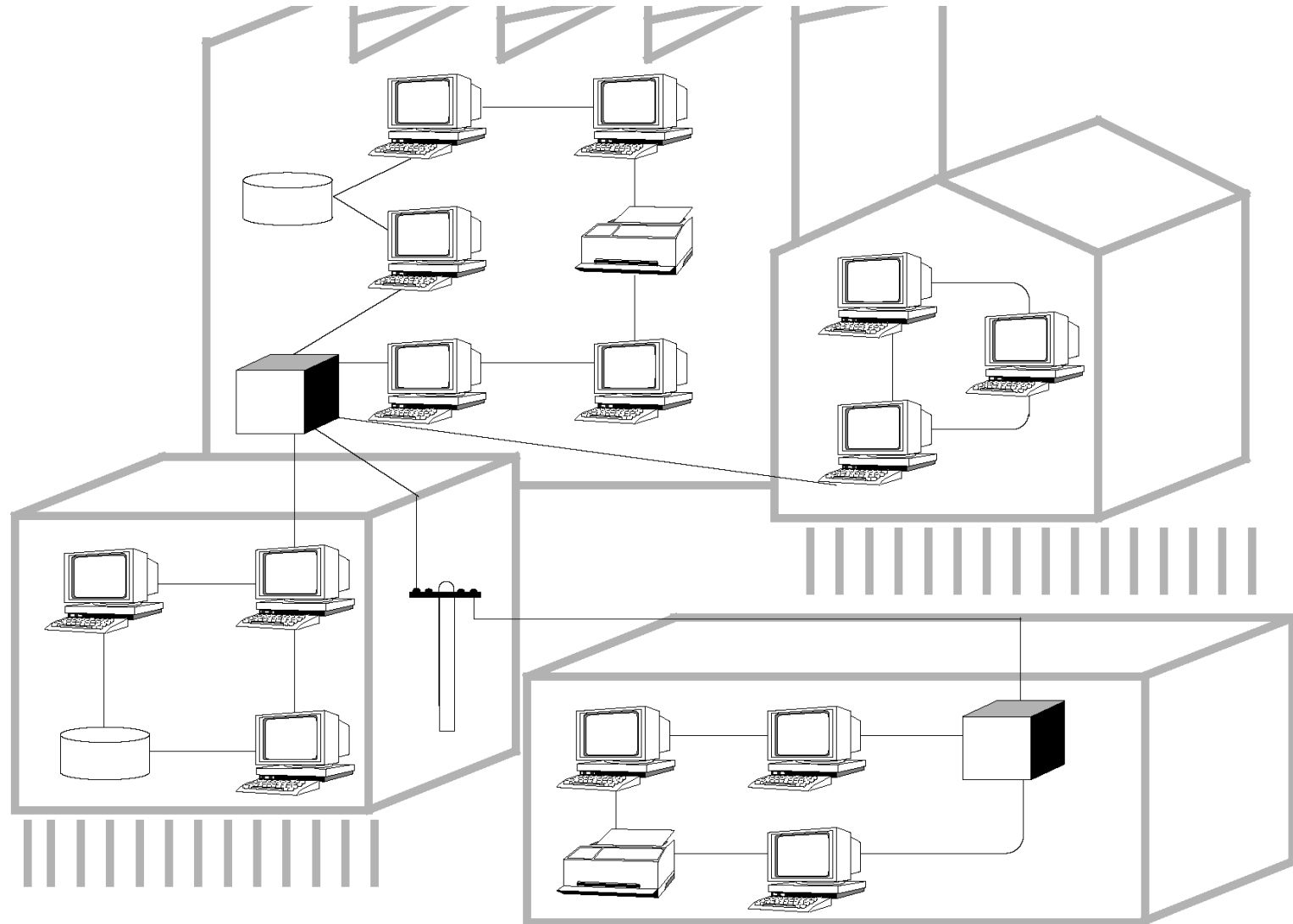
A LAN (Local Area Network) is

- a network for the bit-serial transmission of information between components that are
 - independent and
 - connected to each other
- legally it is controlled by the user
- its range is usually limited to the area within the property boundaries

Source: ISO TC 97

(International Standardization Organization - Technical Committee 97)

What are Local Area Networks (LANs)?



Features of Local Area Networks

- relatively high speed
- easy / reasonably priced connection
- no telecommunication regulations
- distance limited to a few kilometers
- transmission of varying types of information
 - texts, general data
 - images, animated images
 - audio, video
- connecting different devices
 - computers
 - terminals / printers
 - storage units
 - ...

(Classical) common aspect of LANs:

- several senders/sources share a channel/medium

➔ **MEDIUM ACCESS CONTROL**

2 Medium Access Control (MAC)

Reasons for the need of MAC

- if
several persons (senders/sources) share a channel/medium
- then
it is very likely that two or more will start communicating at the same time

➔ schemes needed to avoid chaos

Important sublayer of L2

- especially for LANs
- technically lower part of L2

Channel Allocation Problem

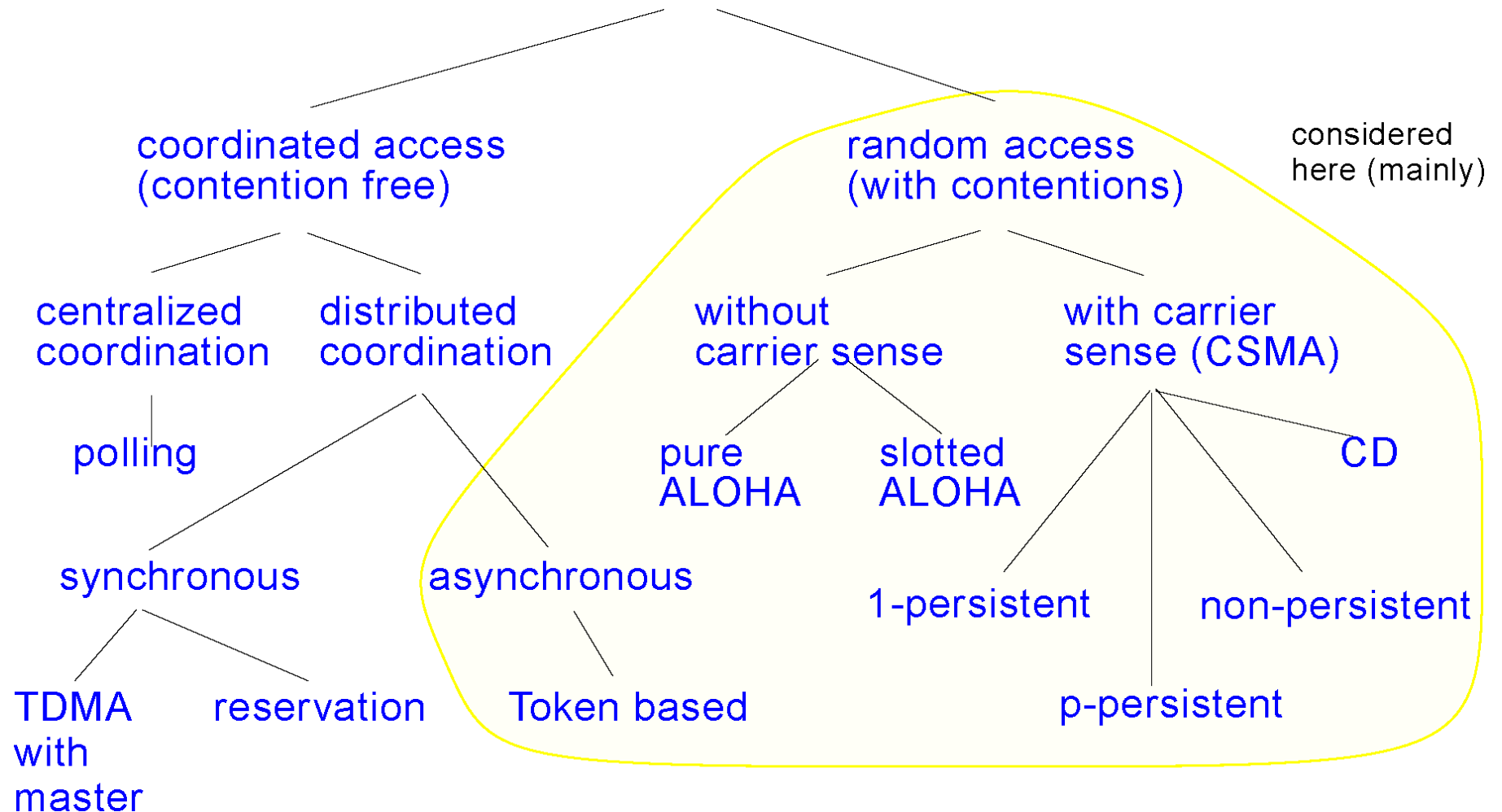
Static Channel Allocation

- using multiplexing schemes such as FDM or TDM
- simple
- does not work well with bursty traffic
 - inefficient and with poor performance

➔ Dynamic Channel Allocation needed

Dynamic Channel Allocation Schemes

Access Control Procedures



Dynamic Channel Allocation – Terms / Assumptions

1. Station Model

- N independent stations (computers, ...) generating frames for transmission
- station blocks until frame has been successfully transmitted

2. Single Channel Assumption

- single channel for all communication (all can send / receive)

3. Collision Assumption

- 2 frames transmitted simultaneously overlap → signal is garbled → collision
- stations can detect collisions

4. (a) Continuous Time

- frame transmission can begin at any instant; no master clock

(b) Slotted Time

- time is divided into discrete intervals (slots)
- frame transmission always begins at start of slot
- slot may contain 0, 1, 2, ... frames (idle, successful transmission, collision)

5. (a) Carrier Sense

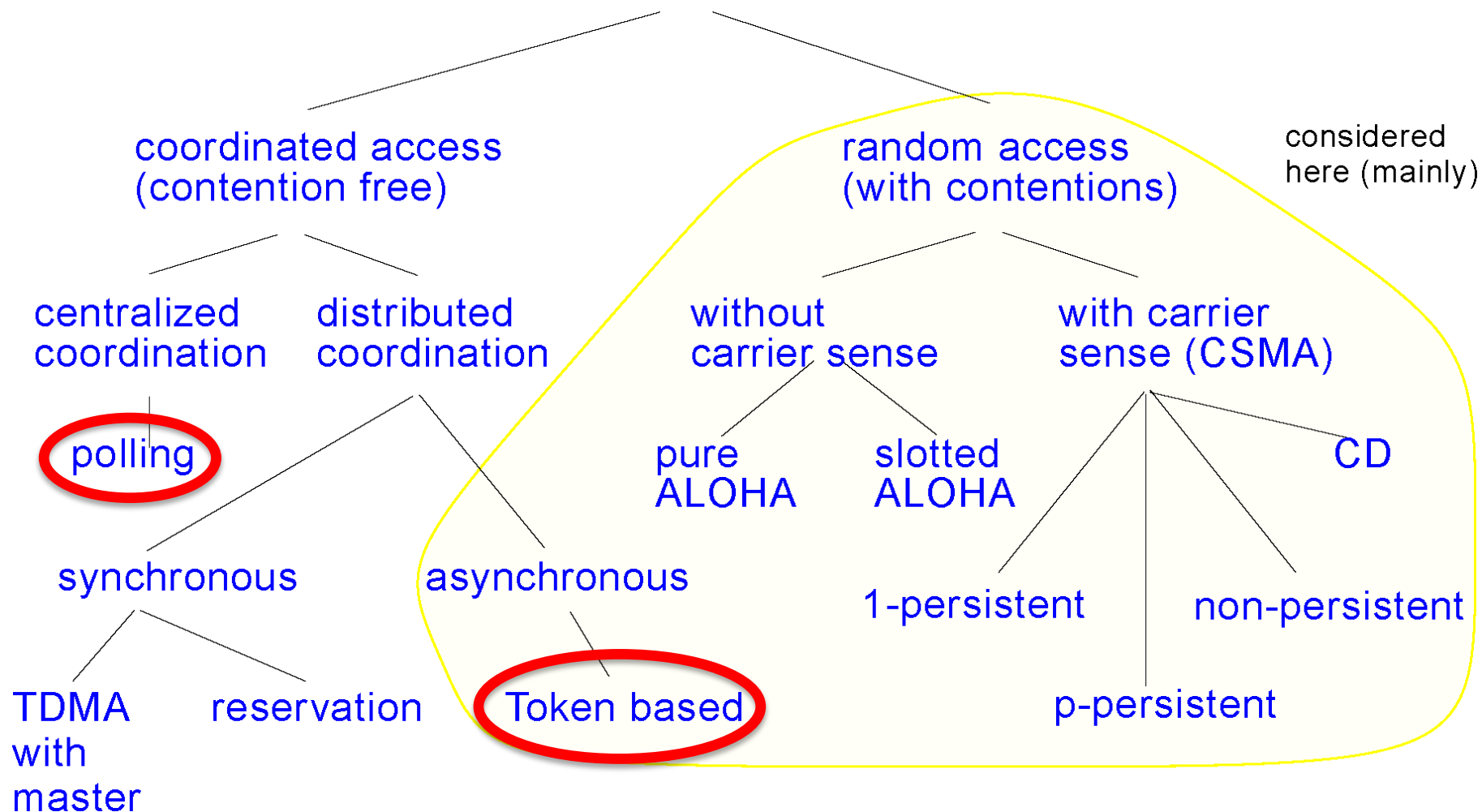
- stations know whether channel is in use or not before trying to use it
- if channel sensed as busy, no station will attempt to transmit until it goes idle

(b) No Carrier Sense

- stations cannot sense channel before trying to use it

3 Dynamic Channel Allocation: Contention Free

Access Control Procedures



3.1 Polling

Control Station

```
LOOP
  FOR i = 1 TO N      /* for all N Stations */
    DO
      POLL Station i;
      /* Request Data / Give Permission To Send */

      WAIT for EOT from Station i;
      /* End of Transmission*/
    END;
```

Follow-up Station X

```
LOOP
  Wait for Poll for Station X;
  IF Data available to be send
    THEN Send Data;
  EOT to Control Station;
END;
```

Characteristics:

- simple and controlled but ...
 - Control Station failure leads to complete outage
 - wasted capacity (polling unnecessary) if no data has to be send

3.2 Token-based

- stations form a physical or a virtual ring
- token (authorization to send) circulates on this ring
- station can send, if it has token

Station X

LOOP

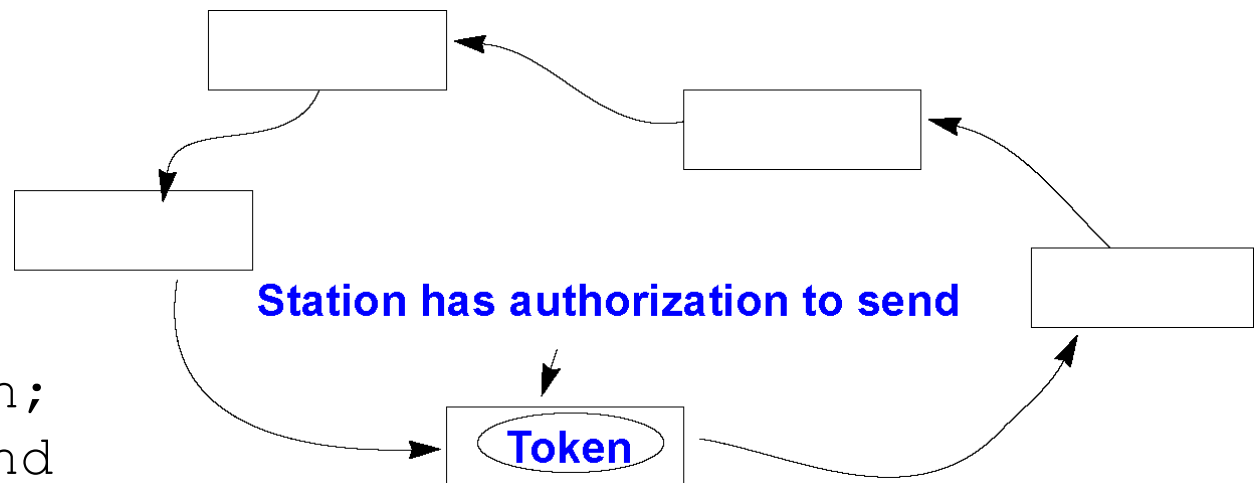
wait for Token;

IF Data to Send

THEN Send Message;

Transmit Token to the Next Station;

END;

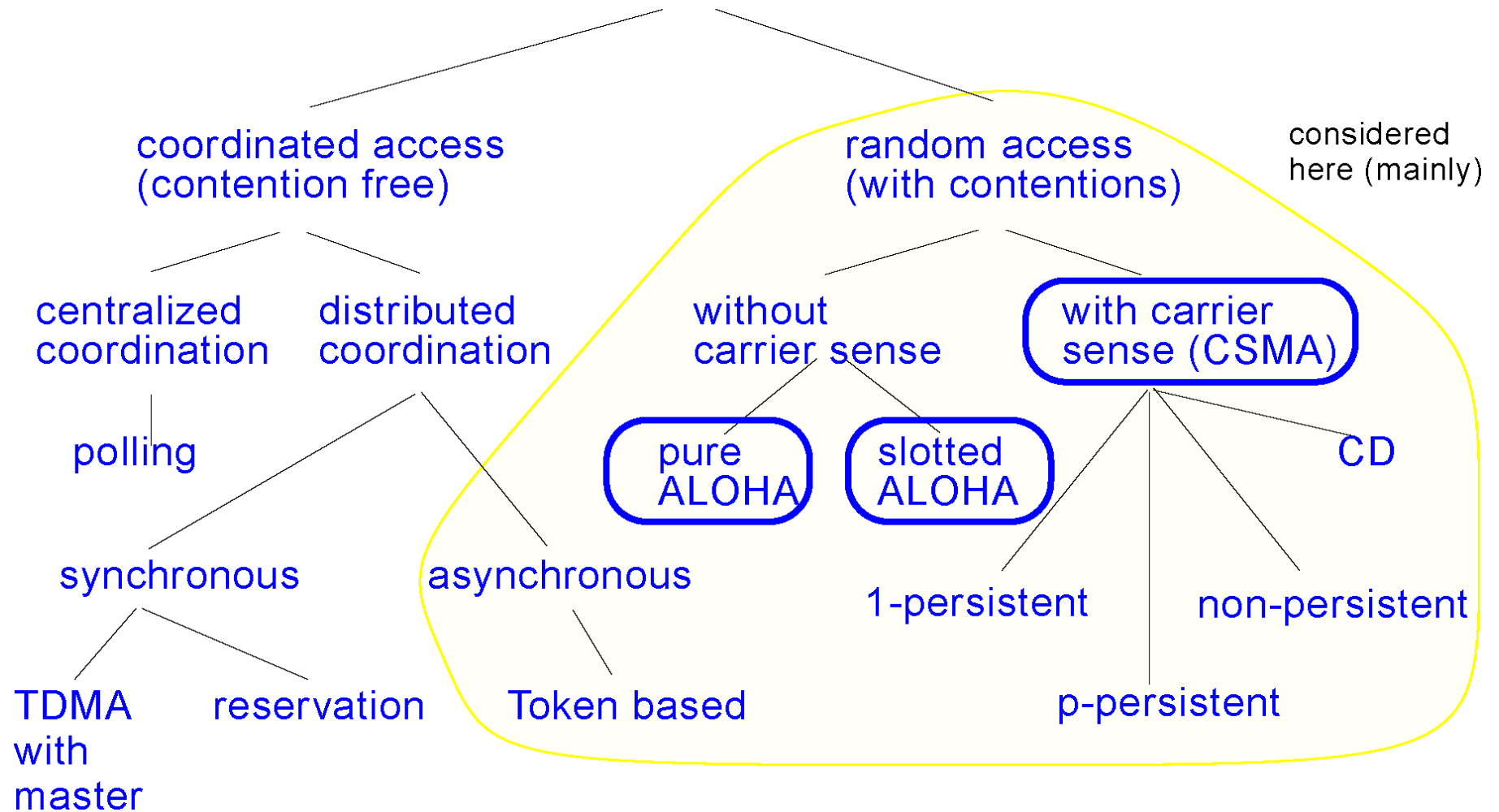


Characteristics:

- **Waiting time (for Token)**
- **Deterministic scheme (fair)**

4 Dynamic Channel Allocation: with Contention

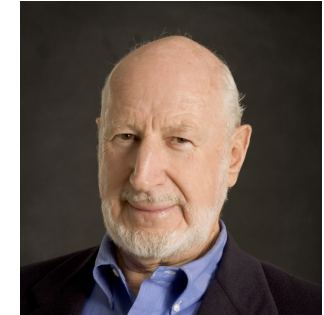
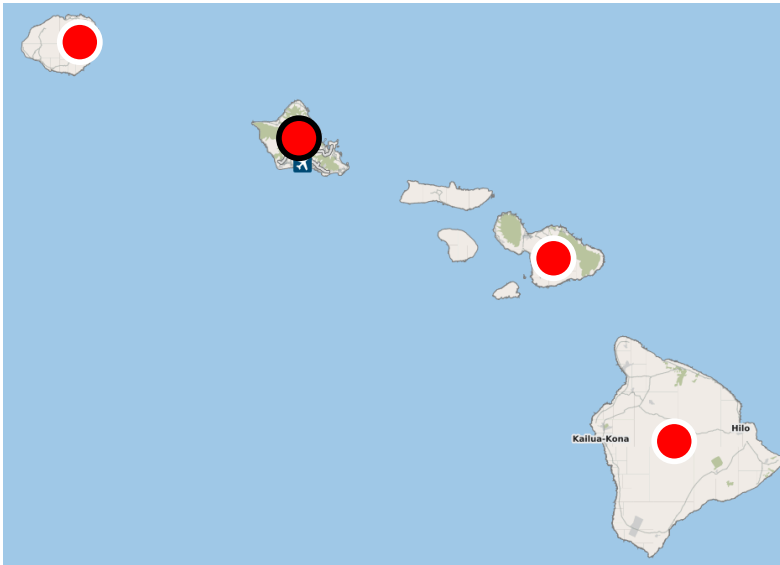
Access Control Procedures



4.1 (Pure) ALOHA

History

- University of Hawaii, 1970 (Norm Abramson et al.)



- Seven campuses on four islands:
 - Oahu, Kauai, Maui, and Hawaii
- One mainframe at main campus on the island of Oahu
- Terminals on other islands
- Linking sites via dial-up telephone lines was very expensive

(Pure) ALOHA

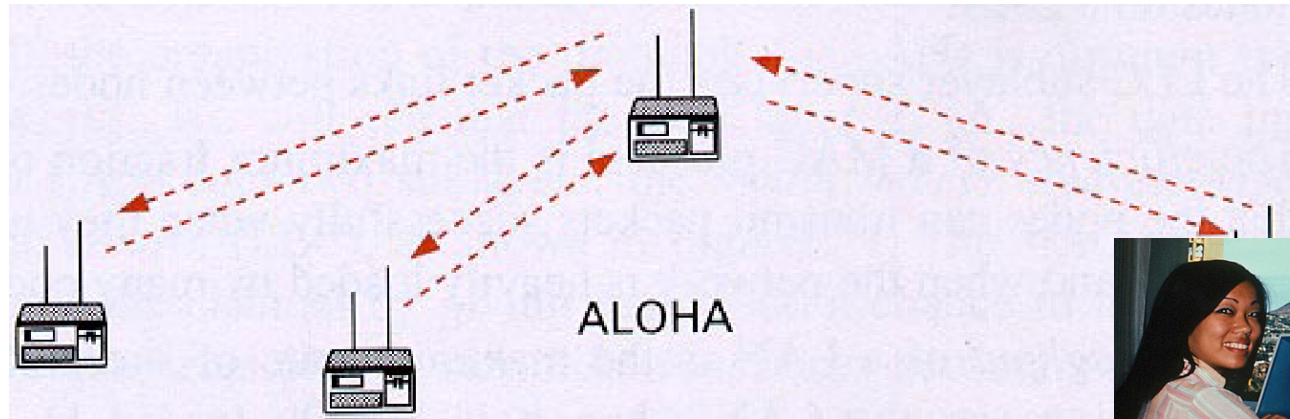


Photo: Norm Abramson/University of Hawai'i at Mānoa

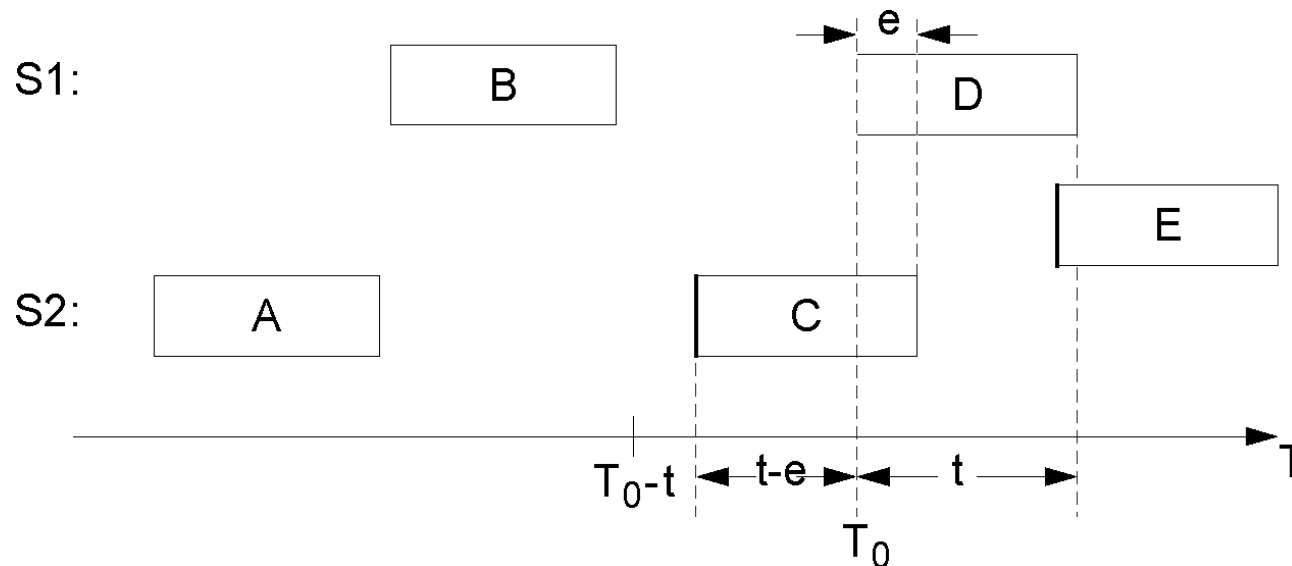
Approach

- use radio communication instead of wired lines
- originally via radio station with 9.600 bps
- two channels
 - 413 MHz: centralized host (to everybody) on ground
 - 407 MHz: all stations to host

Principle:

- sending without any coordination whatsoever
- sender listens at the (return-)channel (after sending)
 - host sends ACKs if data received successfully
- in case of collision
 - retransmit after a random time interval

ALOHA: Example of a Collision



t : time for sending a frame

Collision

- considering frame D, a collision occurs if
 - another frame has been generated between $T_0 - t$ and T_0 or between T_0 and $T_0 + t$
 - collision window: $\lim_{\epsilon \rightarrow 0} 2t - \epsilon = 2t$

Characteristics:

- potentially large number of collisions \rightarrow disadvantage

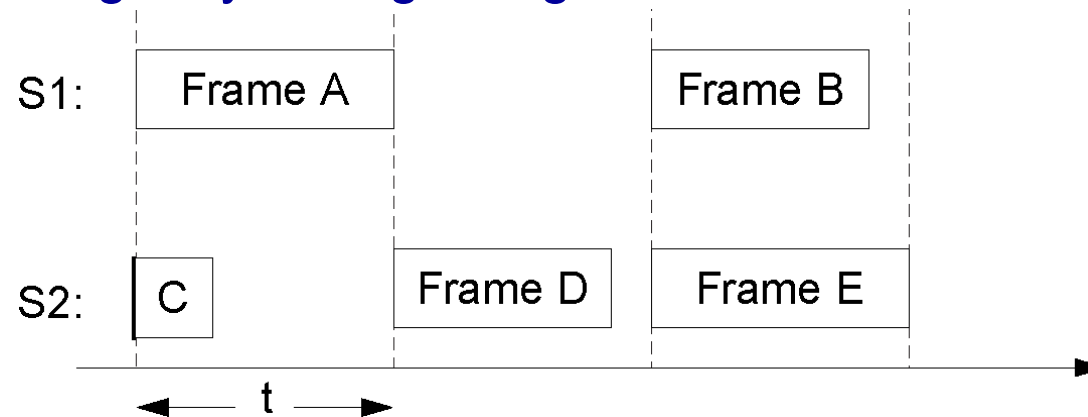
Slotted ALOHA

History

- University of Hawaii, 1972

Principle like Unslotted ALOHA, but discrete approach:

- time divided into slots
- start sending only at beginning of a slot



- collision
 - if the beginning of a frame is between T_0 and T_0+t , i. e. it cannot start at T_0-t and last into T_0+t
 - the time pattern reduces the collision window by half ($= t$)
- requires centralized synchronization

Characteristics

- still many collisions, but less than with Unslotted ALOHA

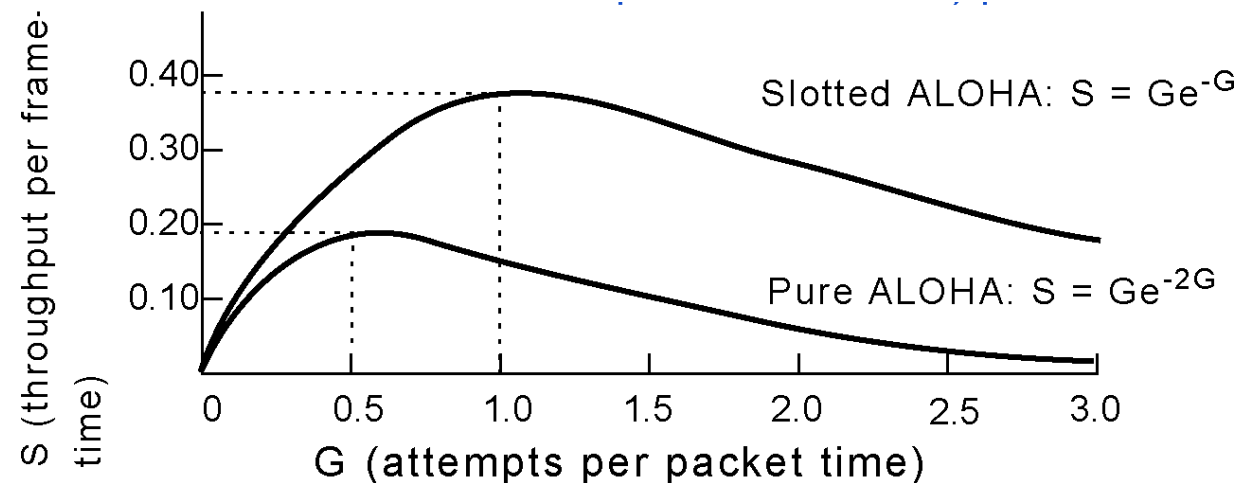
ALOHA: Throughput

Assumptions here: a multitude of stations

- t : time for sending a frame
- S : AMOUNT OF NEW requests to send per frame sending time t
Poisson's distribution
 - $S > 1$ more channel capacity required than available,
i. e. almost always collision
 - $0 < S < 1$ more sensible ...
- G : ALL requests to send
 - (retransmissions added to new requests to send S) per frame time

Maximum channel usage

- Unslotted ALOHA: $1/2e \approx 0.184$
- Slotted ALOHA: $1/e \approx 0.368$



4.2 CSMA (Carrier Sense Multiple Access)

ALOHA and Slotted ALOHA:

- station sends (if request to send exists) and realizes only **AFTERWARDS**, if it was actually able to send

ALOHA inspired Bob Metcalfe to invent Ethernet with CSMA

CSMA Principle

check the channel **BEFORE** sending

channel status

- busy:
 - do not send but wait
 - keep checking continuously until channel is available
 - **OR** wait some time and re-check channel
- idle:
 - transmit frame
 - possibility for collision still exists!
- collision:
 - wait for a random time then start again with channel checking

Several variants

CSMA Variant 1-Persistent

Principle

- Request to send → check channel
- channel status
 - busy:
 - continuous re-checking until channel becomes idle
 - idle:
 - send
 - i. e. **send with probability 1**
 - collision:
 - wait random time, then re-check channel

Properties

- if channel is idle: send with probability 1 (thus 1-persistent)
- **MINIMIZING THE DELAY OF OWN STATION**
- but many collisions during higher load
 - low throughput

CSMA Variant Non-Persistent

Principle

- Request to send → check channel
- channel status
 - busy:
 - wait random time without checking the channel continuously,
 - channel RE-CHECK ONLY AFTER A RANDOM TIME INTERVAL
 - idle:
 - send
 - collision:
 - wait for a random time, then re-check channel

Properties

- assumption that other stations want to send also,
 - therefore it is better to have the intervals for the re-checks randomly determined
- improved overall channel utilization (efficiency)
- but longer delays for single stations

CSMA Variant P-Persistent

Applied with "slotted" channels

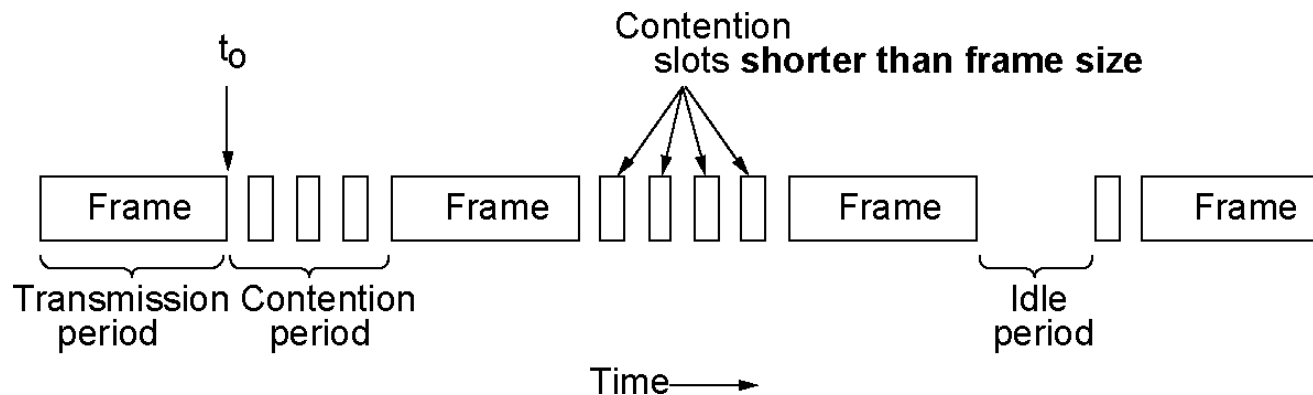
Principle

- Request to send → check channel
- channel status
 - busy:
 - wait for the next slot, re-check (continuously)
 - idle:
 - Send with Probability p ,
 - wait with probability $1-p$ for the next slot,
 - check next slot
 - busy: wait random time, re-check channel
 - idle: send with probability p , wait for next slot with probability $1-p$, ...etc.
 - collision: ..etc
- collision:
 - wait random time, re-check channel

Properties

- compromise between delay and throughput
- defined by parameter p

CSMA Variant CD



Carrier Sense Multiple Access with Collision Detection

- CSMA 1-persistent with CD

Principle:

- sending stations abort transmissions as soon as they detect a collision
 - saves time and bandwidth
 - frequently used (802.3, Ethernet)
 - algorithm
 - while sending a frame: station must detect collision (comparing received with transmitted signal: signal encoding must allow collisions to be detection)

Contention period:

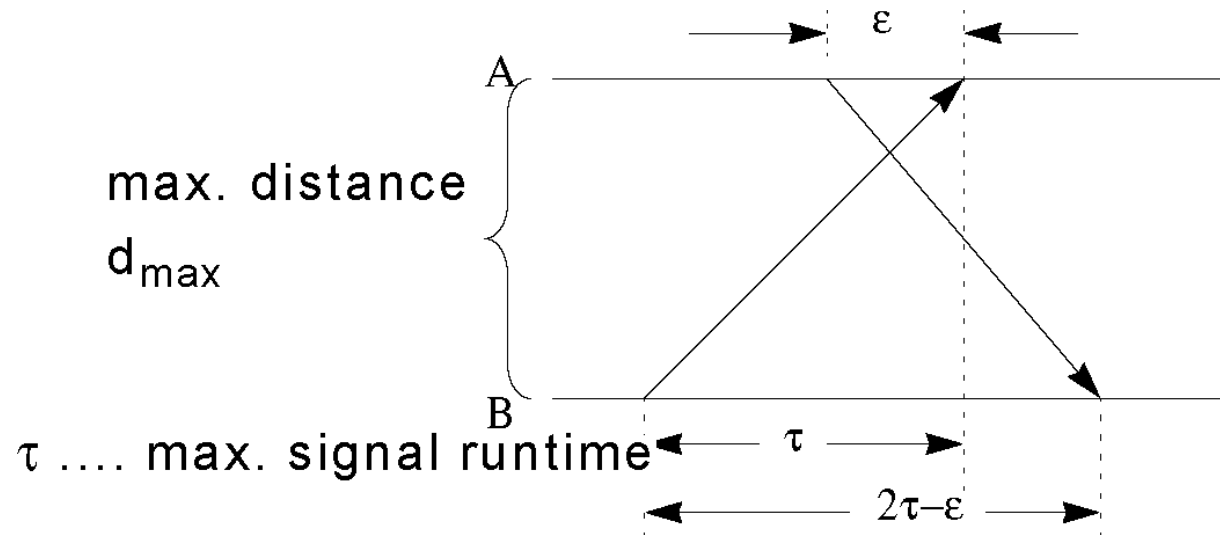
- Extreme case: short frame, maximum distance between stations

CSMA Variant CD: Contention Period

Extreme Case:

- short frame, maximum distance between stations

collision window



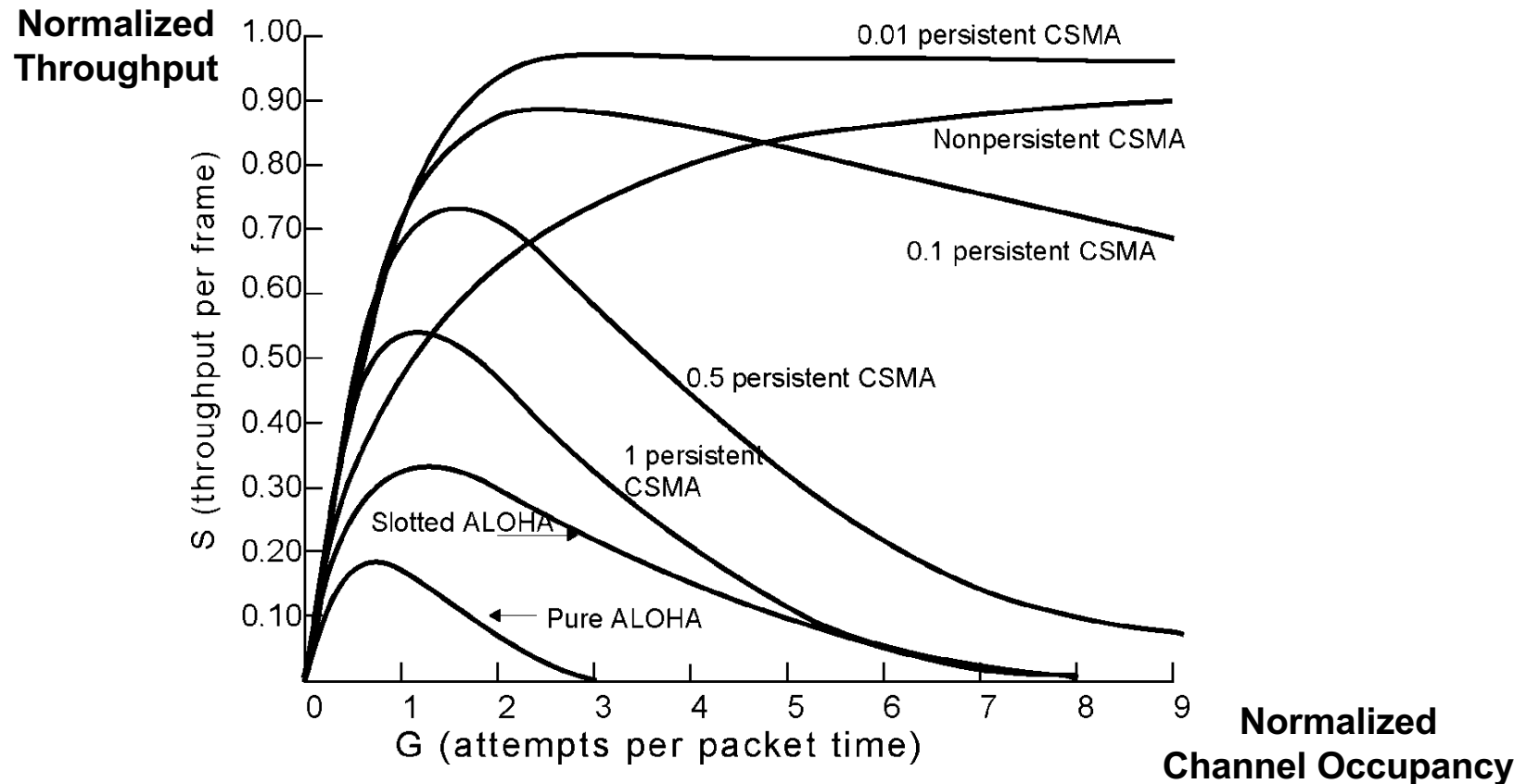
station can be certain only after 2τ

- that it has occupied the channel with no collision
- (1 km coax cable: $\tau \approx 5 \mu\text{s}$)

4.3 Comparing ALOHA, CSMA., CSMA CD

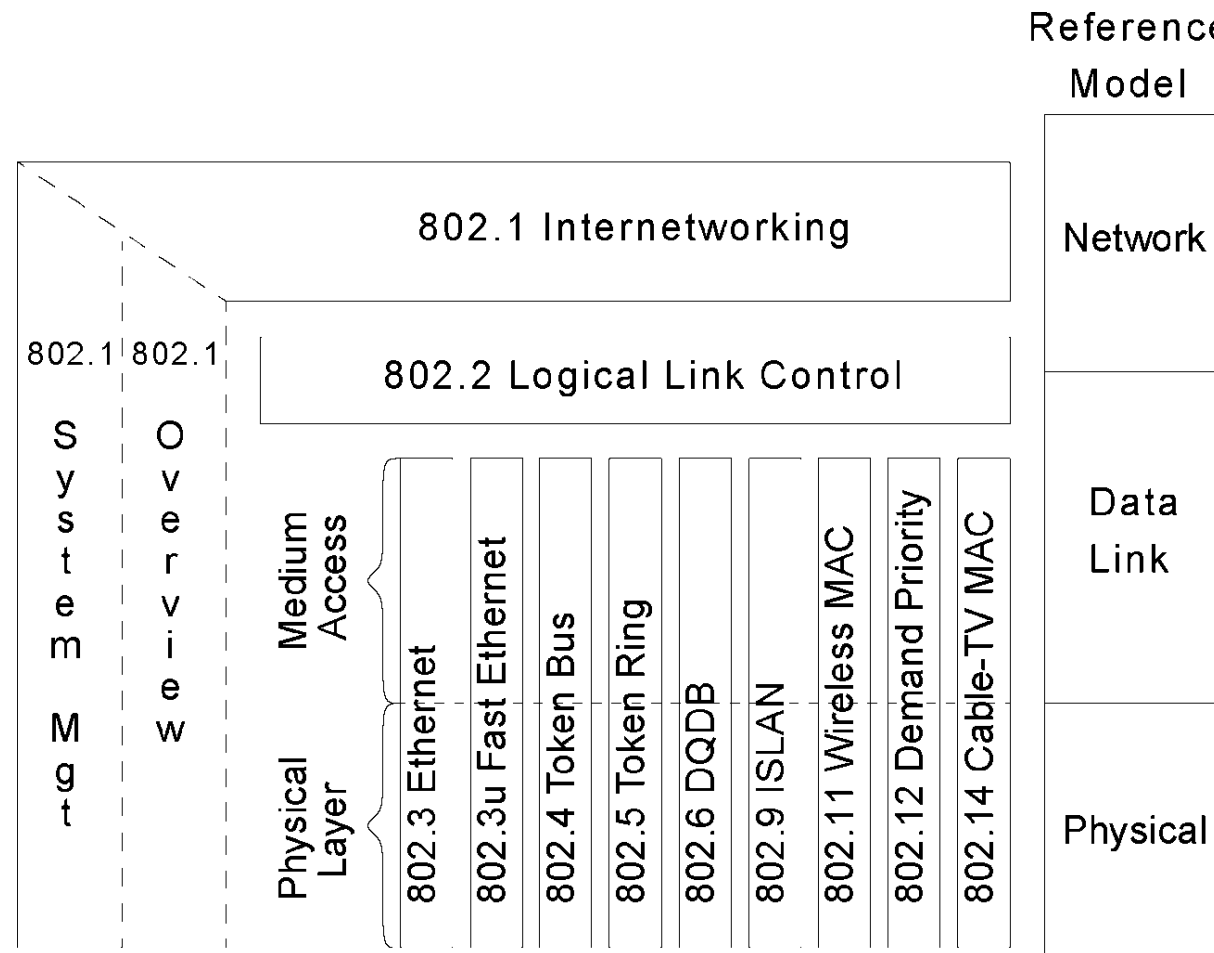
		channel is checked (regarding decision to send, not with regard to collision)			behavior in case of desire to send and if one of the following states has been determined			Time slot
		before	during	after	busy	idle	collision	
ALOHA	pure			X	sender does not know these conditions		re-transmit after random time interval	
	slotted			X				X
CSMA	nonpersist	X		(X)	re-check channel only after random time interval	sends immediately	wait random time interval then re-check channel and send (if possible) (depending on algorithm "idle/busy")	
	1 persist.	X		(X)	continuous wait until channel is idle			
	p persist.	X		(X)	initially: continuous wait until chnl/slot idle	sends with probability p, waits with probability 1-p (for next slot, then re-checks status)		X
CSMA/CD		X	X		depending on procedure, (see above) 1-persistent is e.g. Ethernet		Terminates sending immediately, waits random time	

Comparing Performance: CSMA, ALOHA



- S channel usage / throughput per frame
- i. e. new requests to send, per frame sending time t
 - note: possibly long delay
- G load (attempts per frame-time)
- i.e. all requests to send per frame time
 - re-transmissions added to new requests to send S

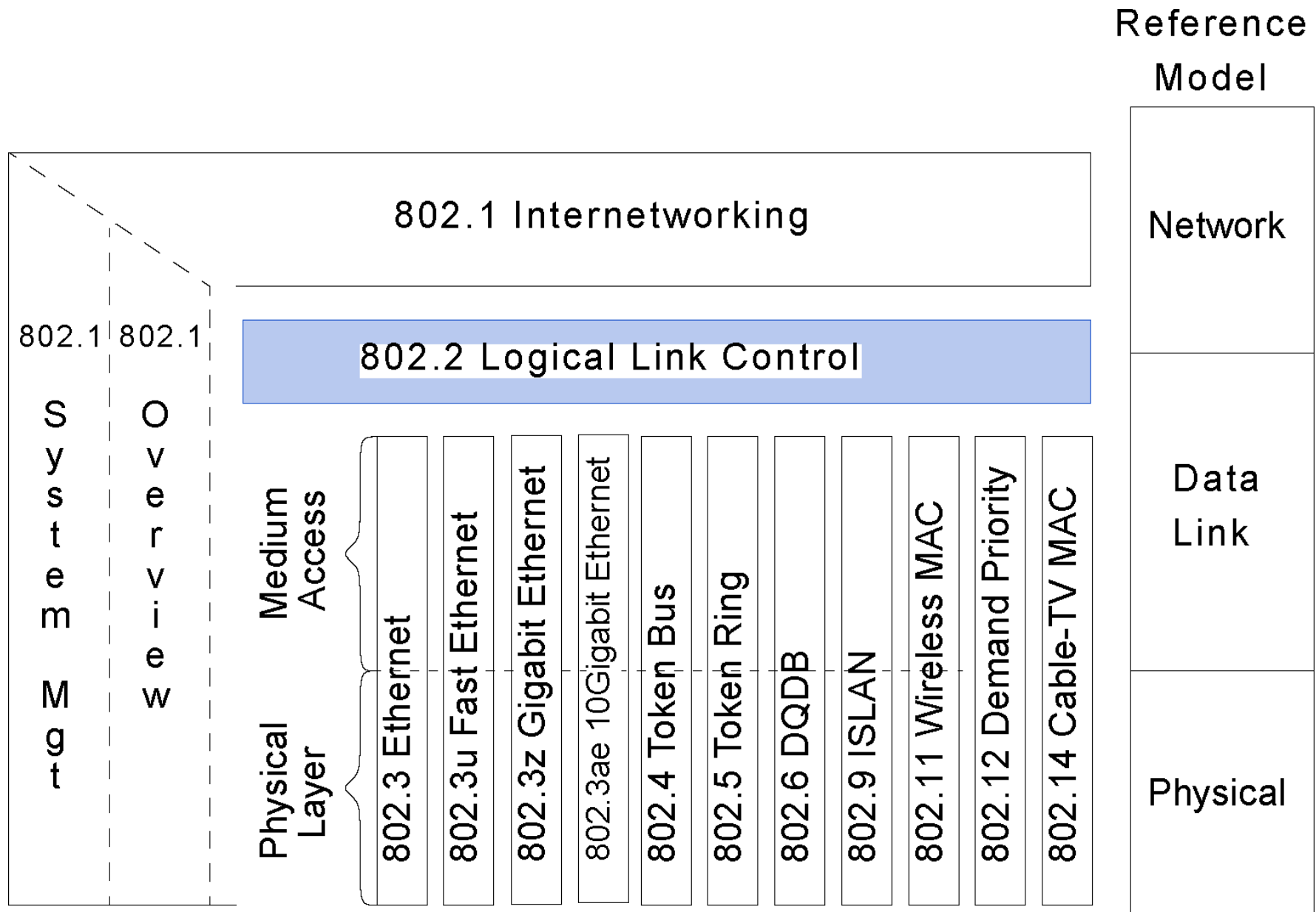
5 Reference Model and Logical Link Control



e. g.

- IEEE 802.3 Ethernet (10 Mbit/s)
- IEEE 802.3u Fast Ethernet (100 Mbit/s)
- IEEE 802.3z / 802.3ab Gigabit Ethernet over fiber / twisted pair
- IEEE 802.3ae 10 Gigabit Ethernet
- IEEE 802.3.....

802.2: Logical Link Control



802.2: Logical Link Control (LLC)

Function

- subset of HDLC
 - High Level Data Link Control HDLC
- common interface
 - to L3 for all underlying LAN/MAN/WAN components

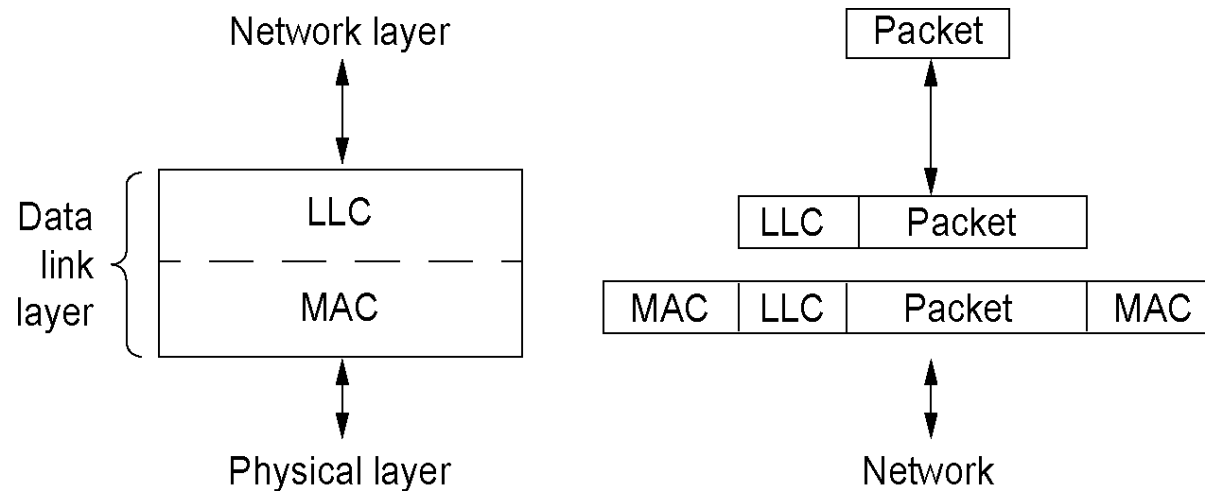
Services

- unacknowledged connection-less (unreliable datagram)
 - upper layers ensure
 - that sequence is maintained, error correction, flow control
- acknowledged connection-less (acknowledged datagram)
 - each datagram is followed by exactly one acknowledgement
- connection-oriented
 - connect and disconnect
 - data transmission incl. acknowledgement, guaranteed delivery to receiver
 - maintaining the sequence
 - flow control

LLC Frame

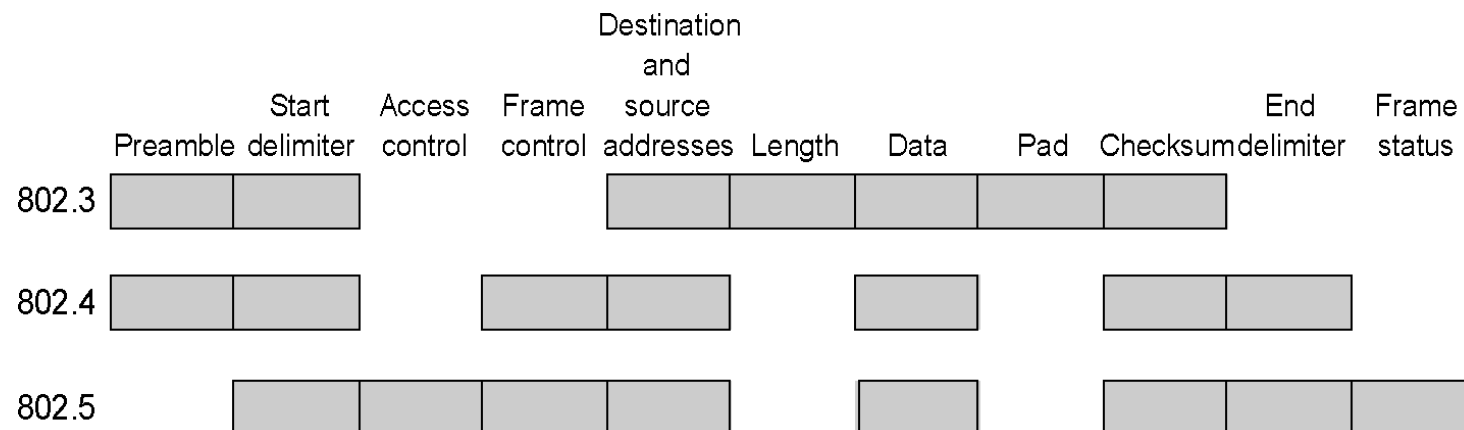
Format

- includes LLC Service Access Points SAPs for source and destination



Varying AC frames:

- formats

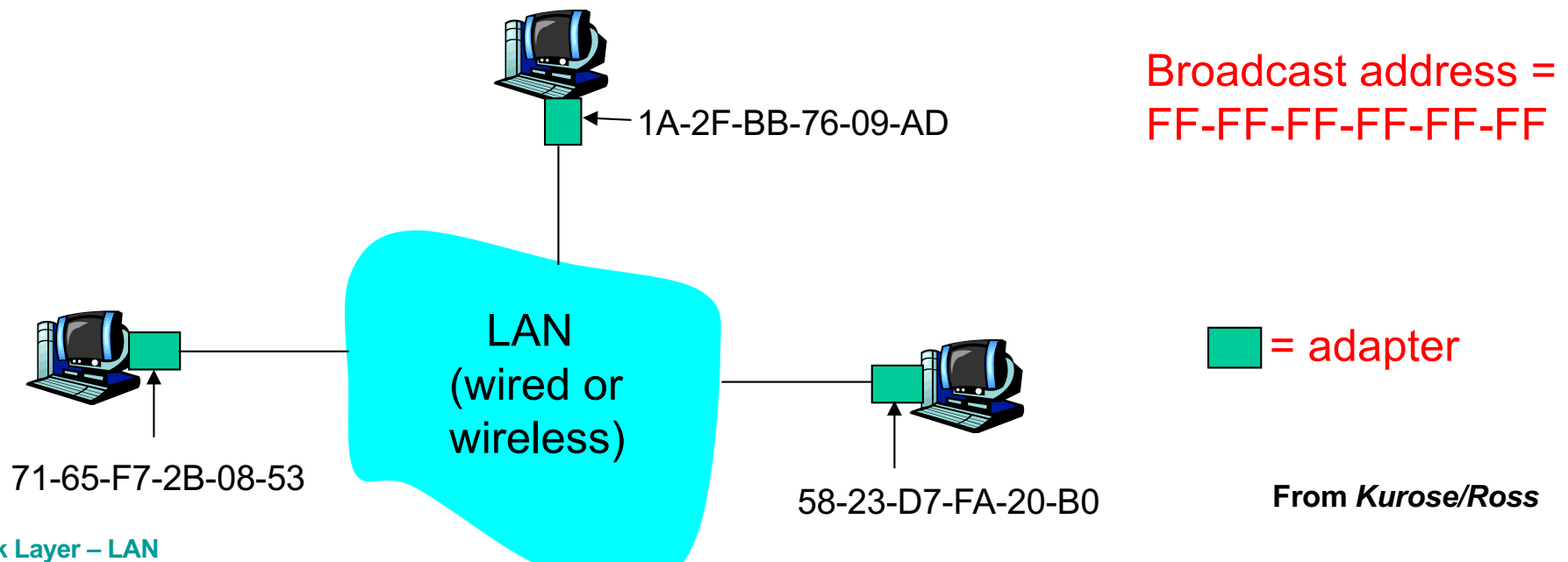


6 Link Layer Addressing

MAC (or LAN or physical or Ethernet) address:

- function: *get frame from one interface to another physically-connected interface (same network)*
- 48 bit MAC address (for most LANs)
 - burned in NIC ROM, also sometimes software settable

Each adapter on LAN has unique LAN address

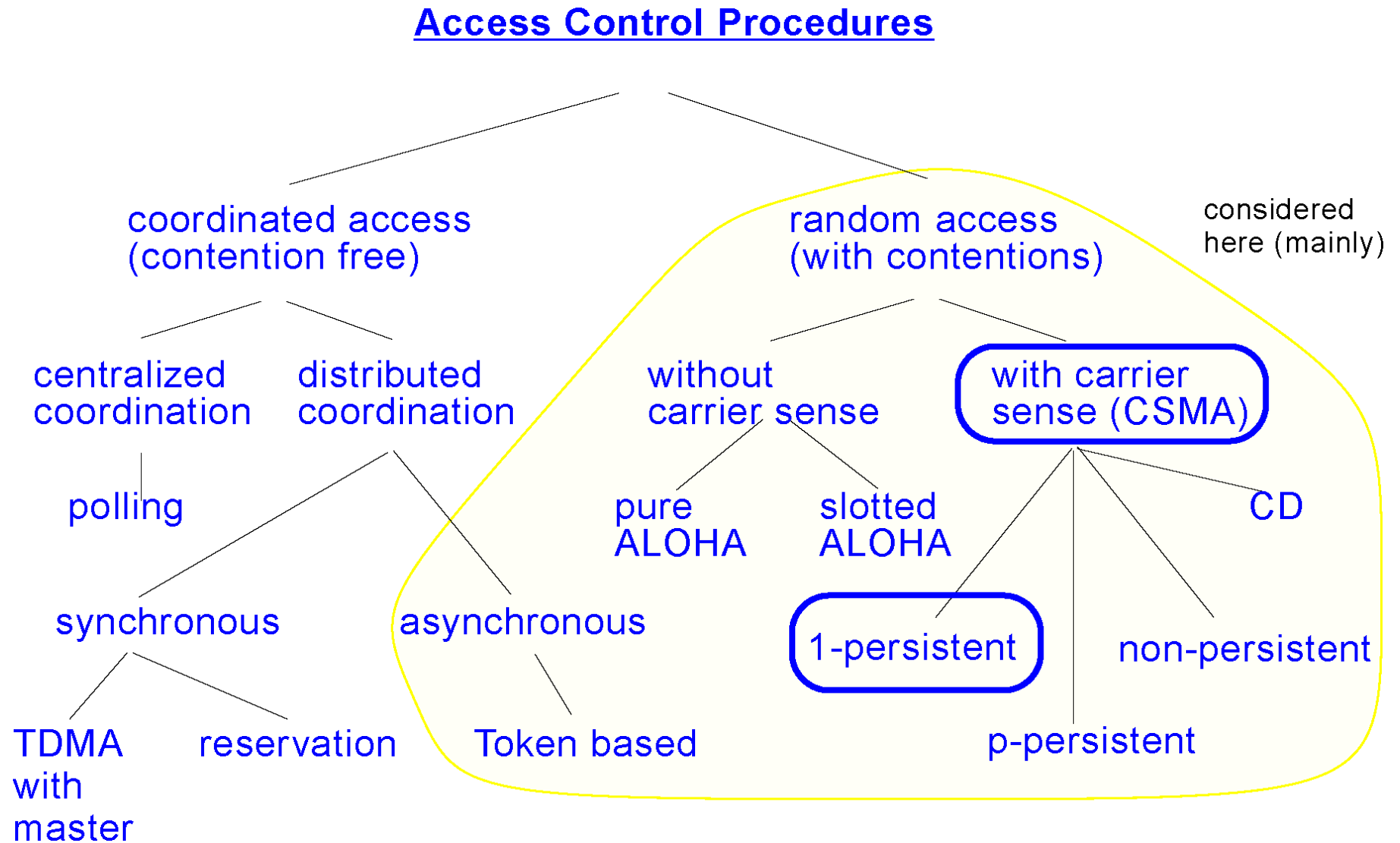


MAC / LAN Address

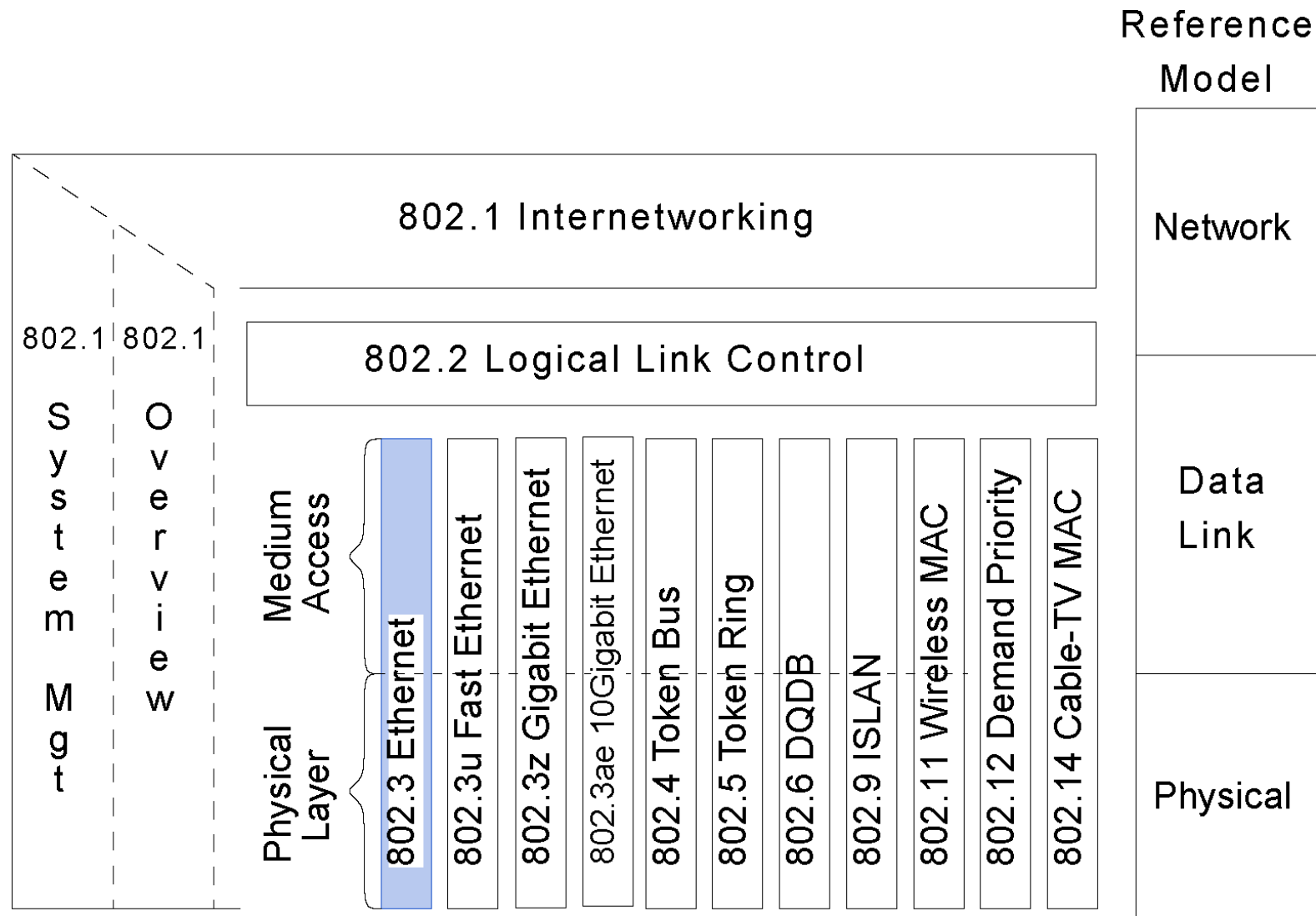
MAC address allocation administered by IEEE

- manufacturer buys portion of MAC address space (to assure uniqueness)
- analogy:
 - (a) MAC address: like Social Security Number
 - (b) IP address: like postal address
- MAC address: flat → portability
 - can move LAN card from one LAN to another
- IP address: hierarchical → NOT portable
 - address depends on IP subnet to which node is attached

7 IEEE 802.3: CSMA / CD



IEEE 802.3: CSMA / CD



IEEE 802.3: CSMA / CD

History

- 1976
 - Ethernet by Xerox, Robert Metcalf (2,94 Mbps)
- 1980
 - Ethernet industrial standard by Xerox, Digital Equipment (today part of HP) and Intel (10 Mbps)
- 1985
 - IEEE 802.3 based on Ethernet

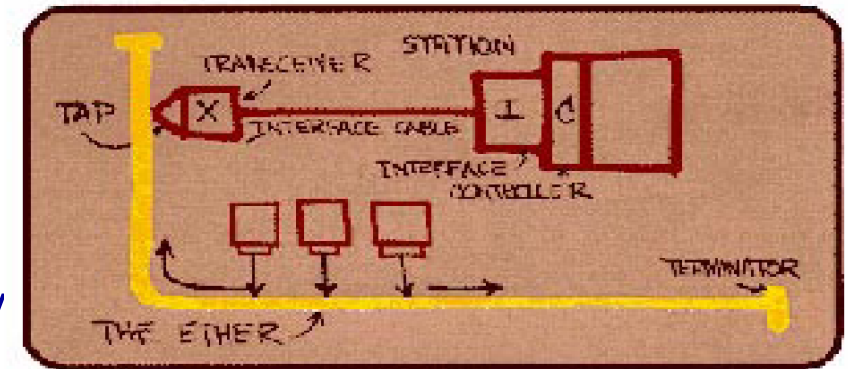


Figure 1. Robert Metcalf's drawing of the first Ethernet design.

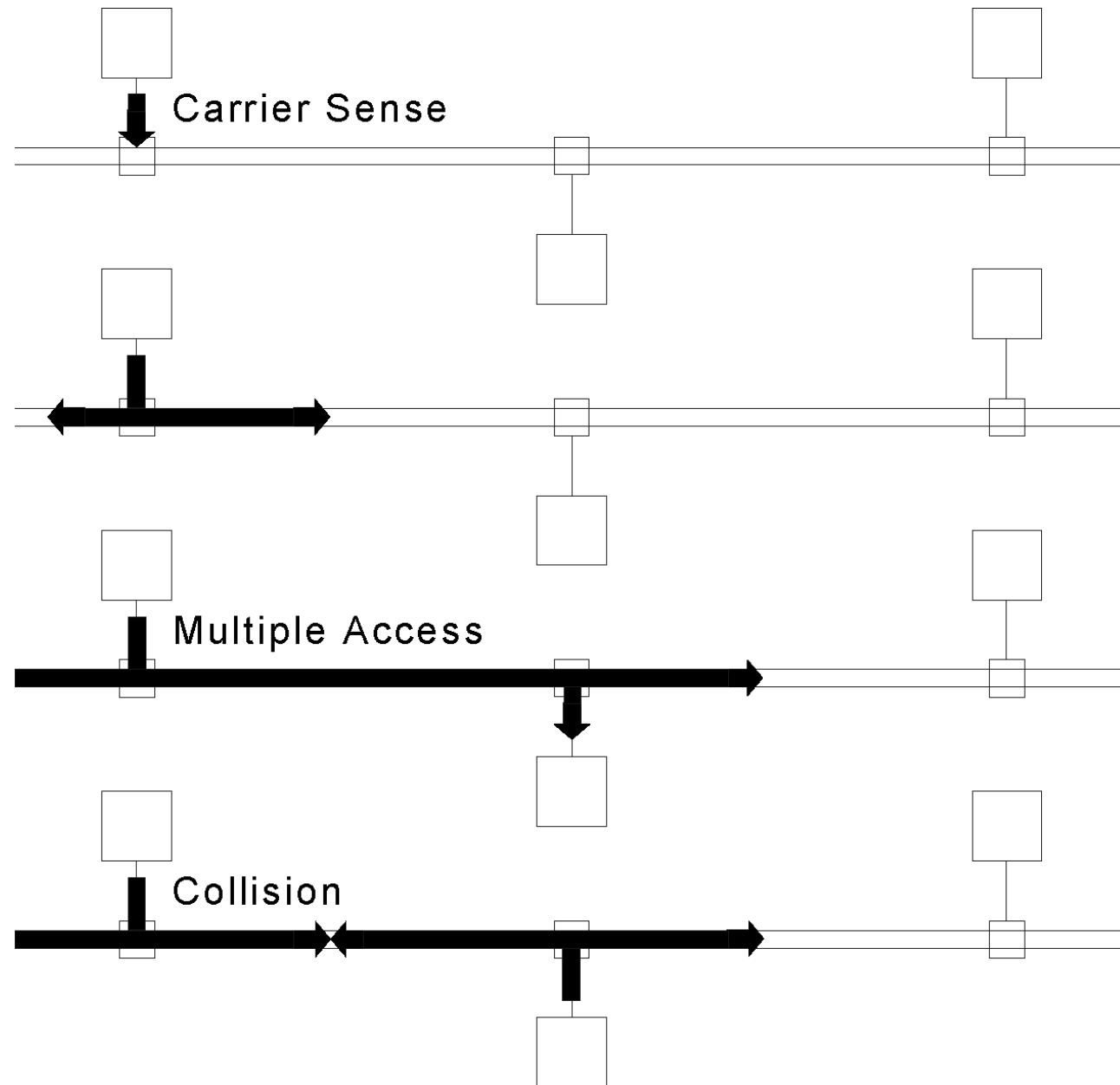
IEEE 802.3

- specifies a family based on the 1-persistent CSMA/CD systems
- (1 -) 10, 100 Mbps, 1, 10, 100, ... Gbps on different media
- Ethernet is a protocol of this family

1-persistent CSMA / CD

- L1:
 - Manchester Encoding
 - (on all cables except for 10BROAD36 broadband, here DPSK)

IEEE 802.3: CSMA / CD

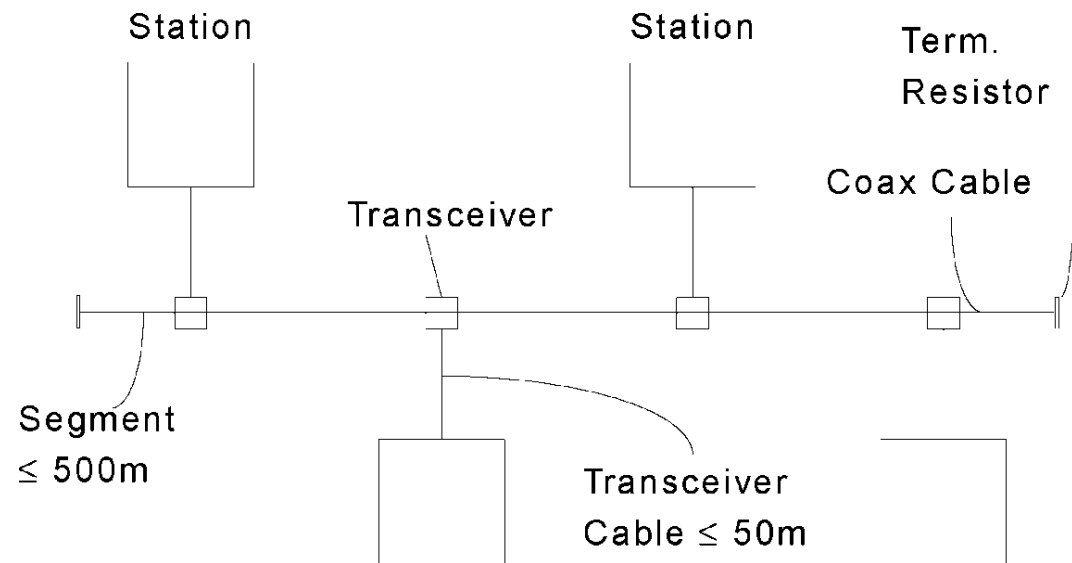


7.1 802.3: Configurations & Components

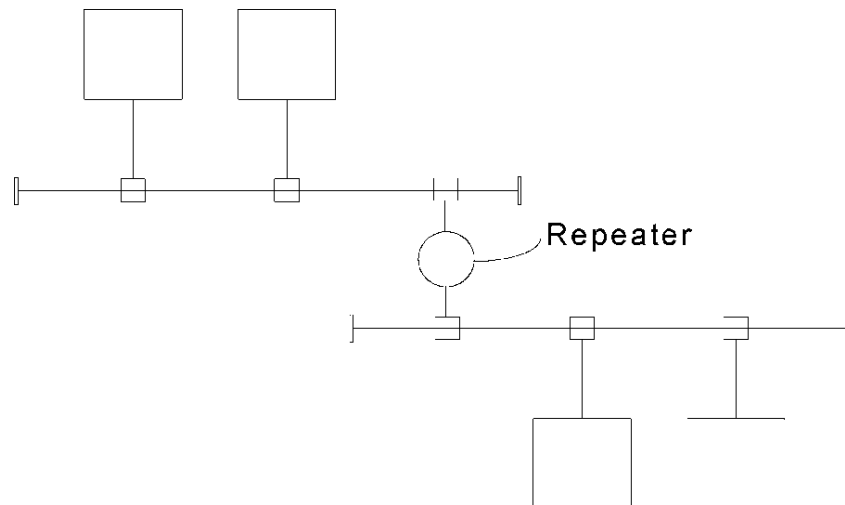
Rule (in general)

- Always **EXACTLY ONE WAY** between 2 stations in the Ethernet

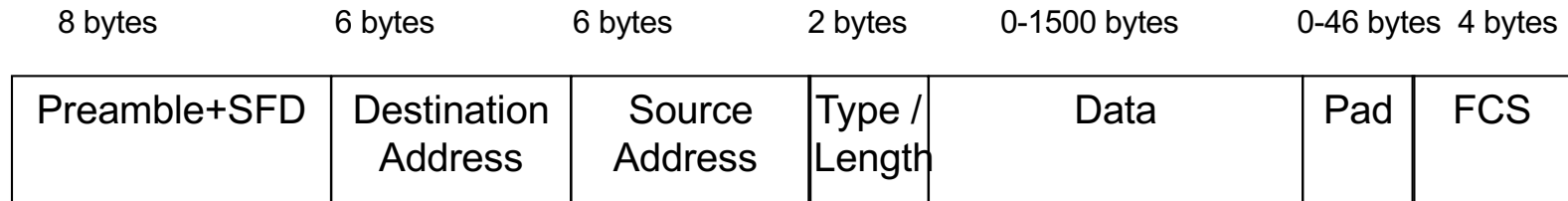
Small configuration
(classical)



Medium configuration



7.2 802.3: Frame Format



Preamble:

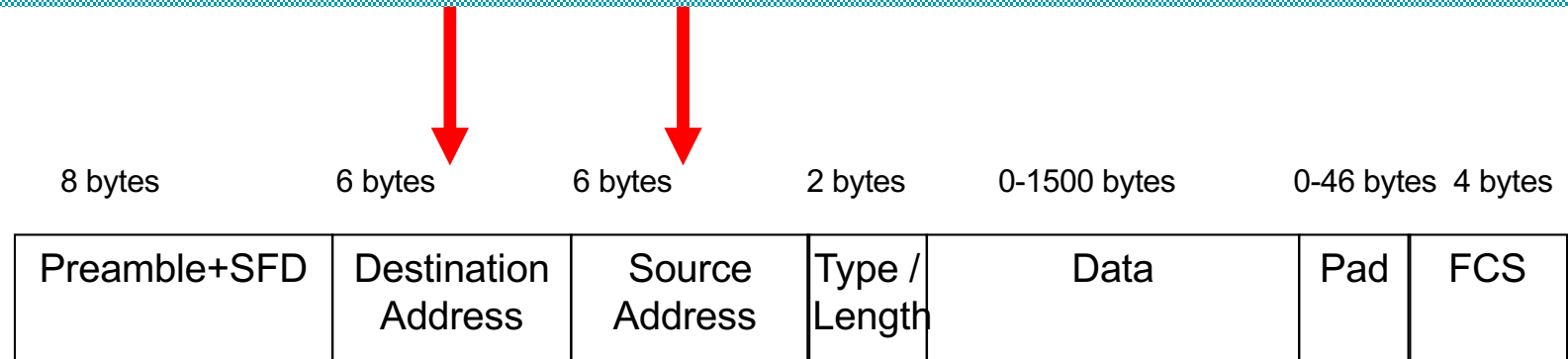
- 7 bytes with bit pattern 10101010

Start Frame Delimiter:

- beginning of the frame (10101011)

allows synchronization of the receiver's clock with sender's clock

802.3: Frame Format

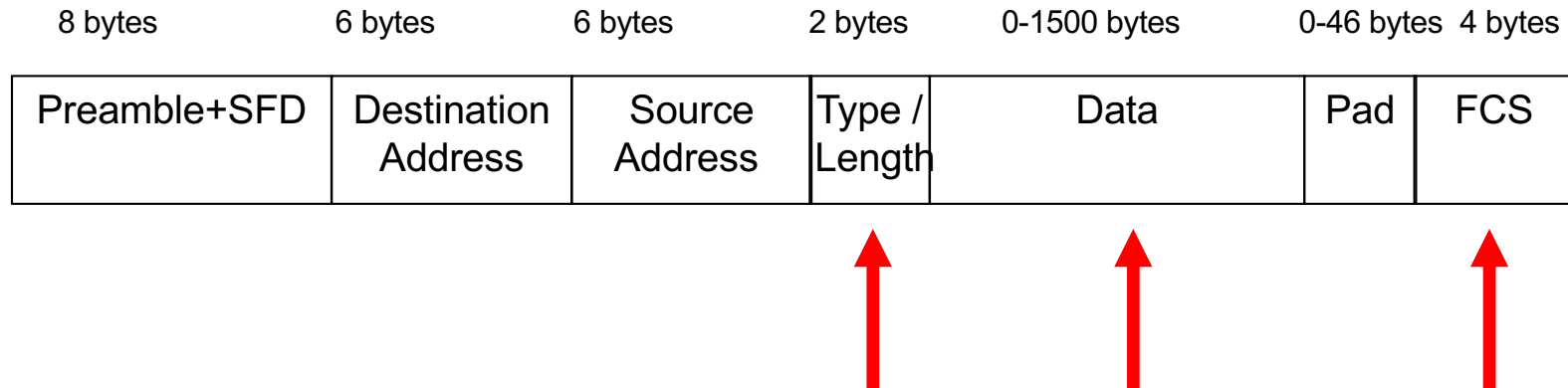


Destination Address and Source Address:

- MAC address (as discussed above)
 - local address assignment
 - can be done on site by authorized entity
 - global address assignment
 - IEEE assigns worldwide unique 46 bit addresses (7.03×10^{13} potential addresses)
 - L3 (network layer) has to locate address
- individual, group, all:
 - unicast → individual address
 - multicast → group address
 - broadcast → all address bits = "1"

I/G	U/L	46-Bit Address
I/G = 0		Individual Address
I/G = 1		Group Address
	U/L = 0	Globally Administered Address
	U/L = 1	Locally Administered Address

802.3: Frame Format



Type / Length:

- In old version: length of data field (number of bytes)
- Now: type, indicates protocol of next upper layer (IP, IPX, ...)
 - 0x0800 IP Internet Protocol, Version 4 (IPv4)
 - 0x0806 Address Resolution Protocol (ARP)
 - ...
 - Only values above 1536 (0x600) are used (above max. data length)

LLC Data:

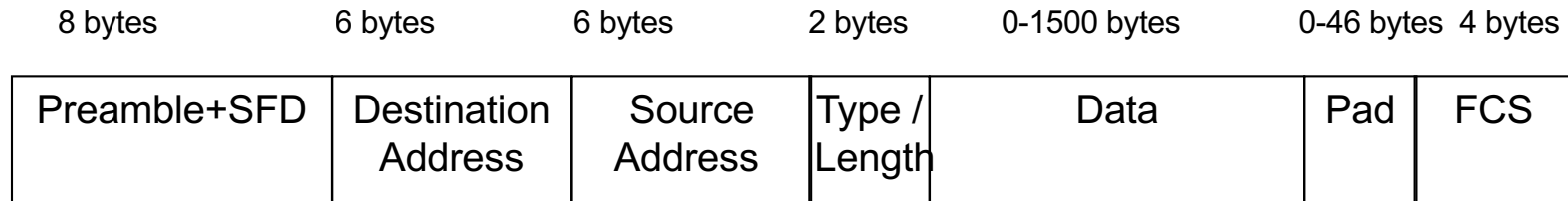
- 0 - 1 500 bytes actual data

Frame Check Sum

- 32-bit CRC to detect errors (in that case receiver drops frame)
- Calculated without preamble+SFD

802.3: Frame Format

Pad:



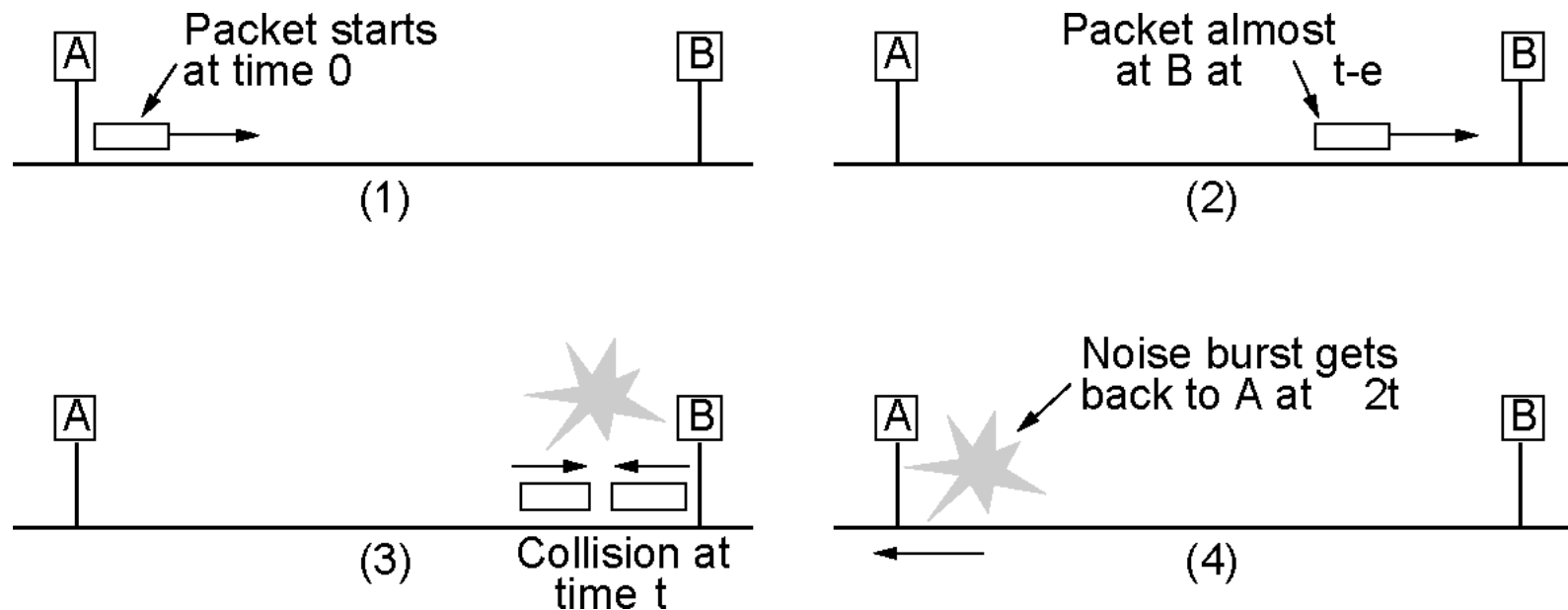
- min. frame length = 64 bytes (=6+6+2+46+4)
 - for collision detection (see below)
- shorter frame length → invalid frame

➔ potentially padding bytes to achieve the minimum frame length

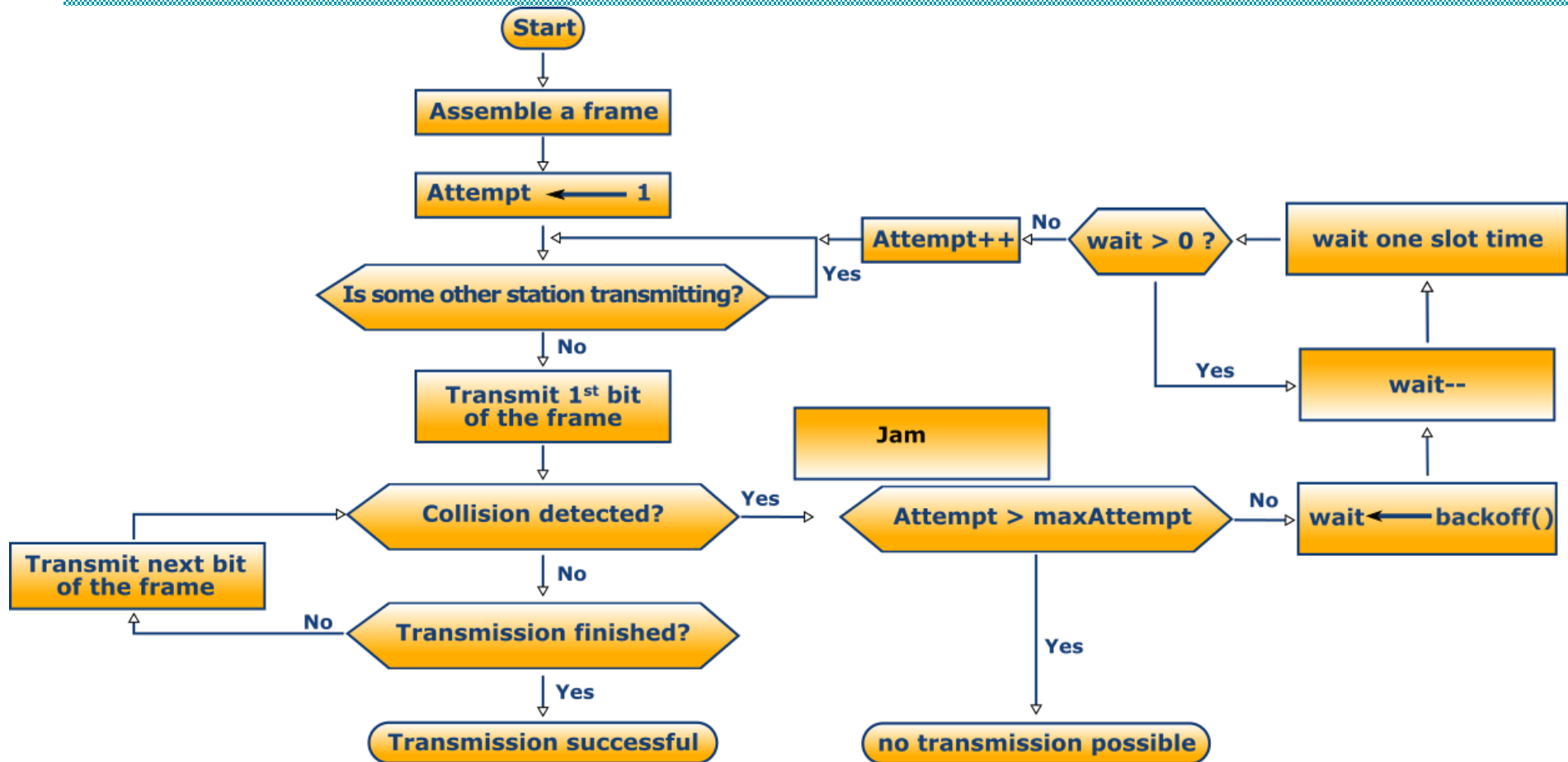
802.3: Frame Format – Details on Minimum Length

Reason (for minimum length):

- transceiver aborts frame transmission during collision
 - i. e. short invalid frames appear
- algorithm
 - station should recognize **during** frame transmission whether a collision occurred
 - extreme case:
 - short frame & stations at maximum distance



7.3 802.3: Control Flow



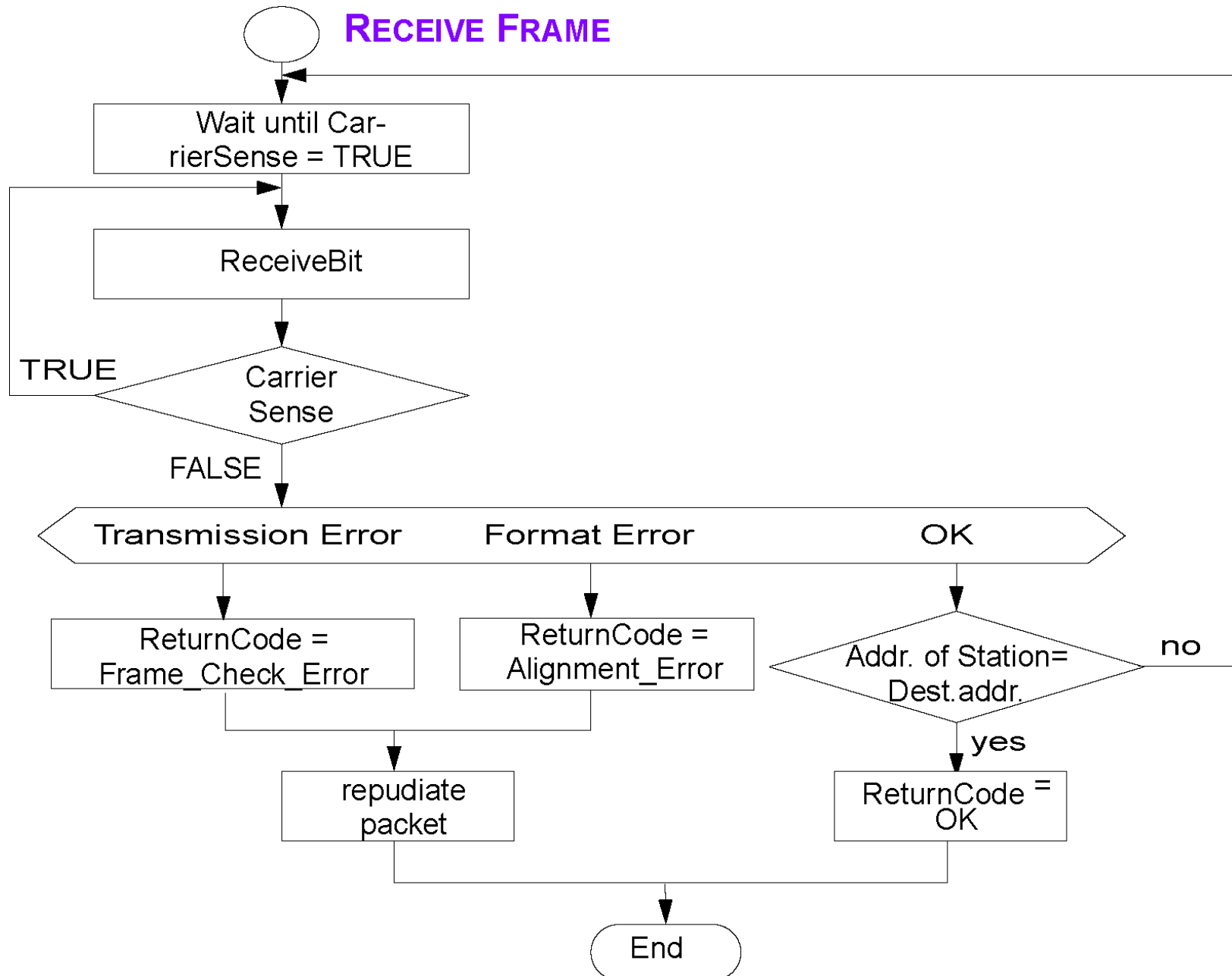
Adapted from
<https://upload.wikimedia.org/wikipedia/commons/3/37/CSMACD-Algorithm.svg>

$\text{backoff} = r \cdot \Delta t$ with $\Delta t = \text{send time for 512 Bits (51,2 } \mu\text{s)}$

$0 \leq r < 2^k$ with $k = \min(n, 10)$

$n = \text{number of unsuccessful attempts to send (1 } \leq n \leq 16)$

802.3: Control Flow



7.4 802.3: Collision Treatment

Time is divided into discrete slots

- slot length equal to worst case round-trip propagation time ($2t$)

Binary Exponential Backoff Algorithm

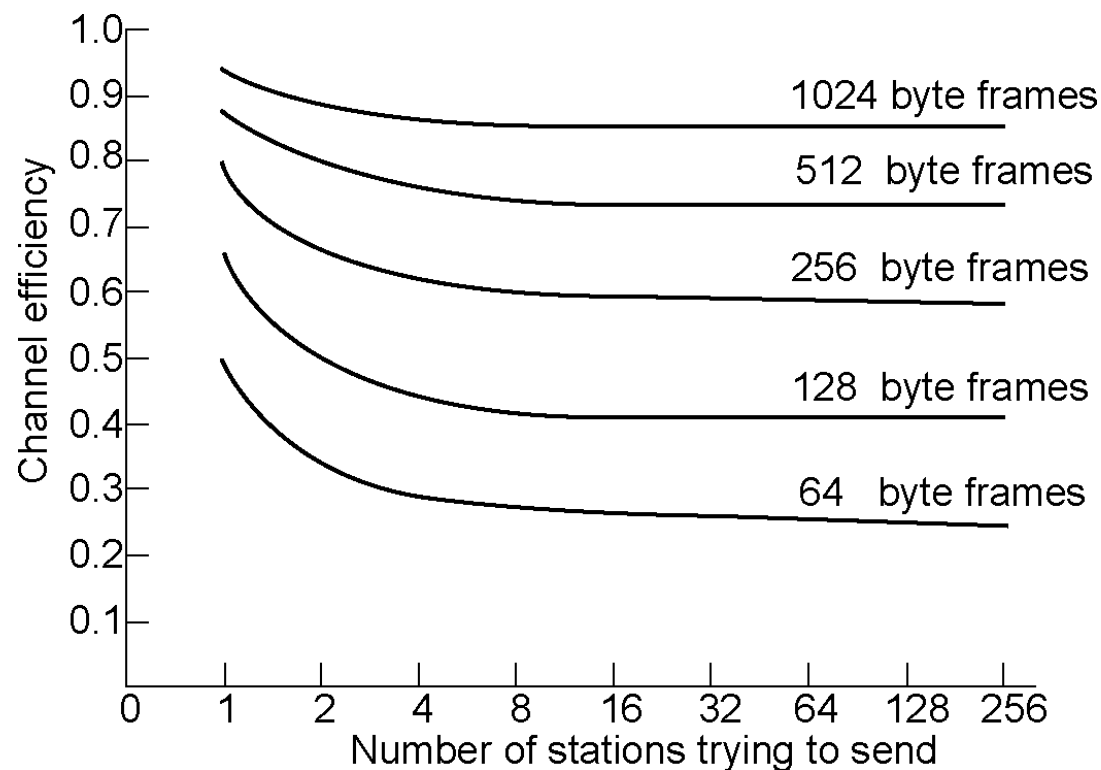
... collision after first request to send	next attempt after a waiting ... frames
1st	0 or 1
2nd	0, 1, 2 or 3
3rd	0, 1, 2, 3, 4, 5, 6 or 7
...	
nth	$0, \dots, 2^k - 1$ $k = \min(n, 10)$
16th	error message to L3

Effects, behavior...

802.3: Behavior

Behavior

- during increasing load
 - if more stations
 - if longer frames
- longer waiting periods
lower utilization
higher utilization



7.5 Switched 802.3 LANs

Problems with hubs (repeaters)

- all stations within one collision domain

collision domain

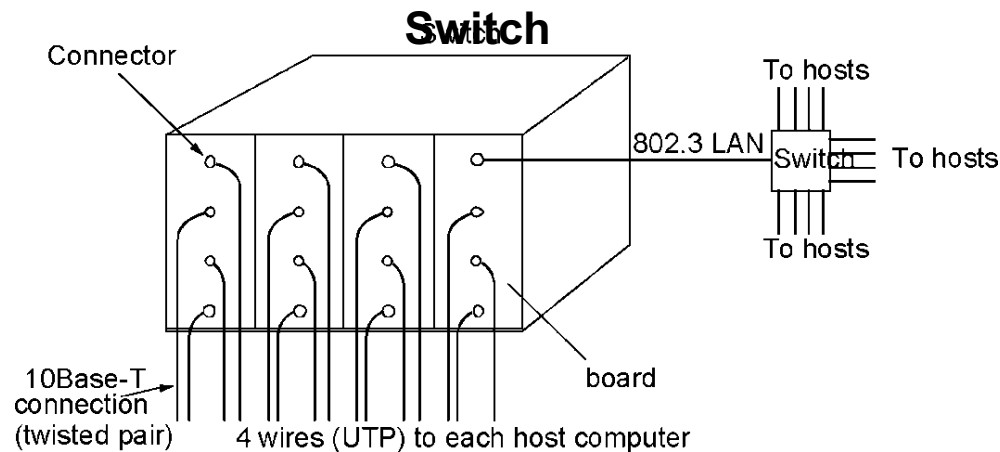
- collisions possible internally,
- but no collisions with other domains

to avoid collisions

- introduce switching functions

Switched 802.3 LANs

SWITCH (instead of **HUBs**) as relaying center

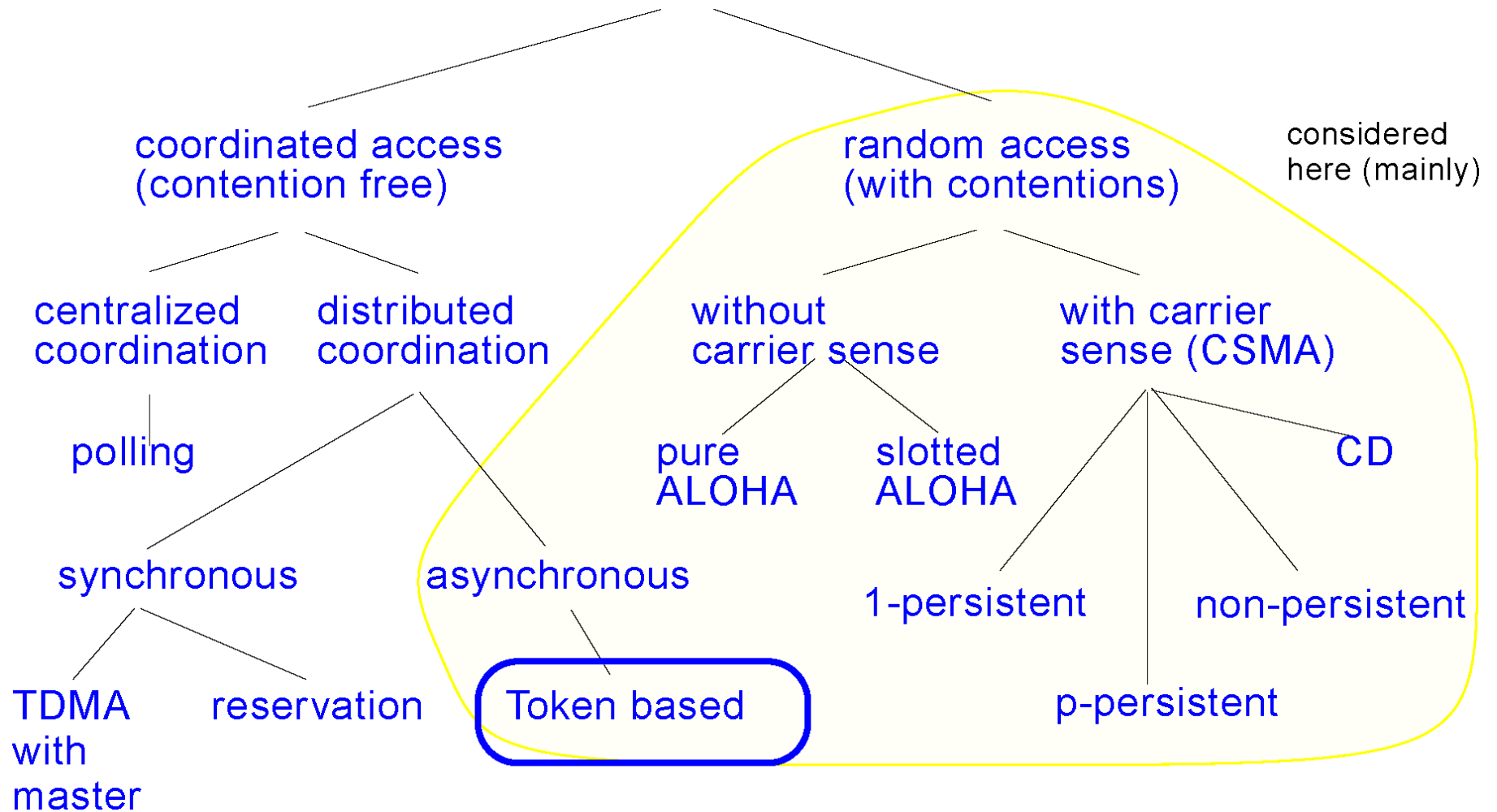


- station sends frame
- switch tries to locate
 - first: the receiver within the "board"
 - and only if not located: at a different location
 - but (typically) does not broadcast frame on all lines (tries to avoid this)

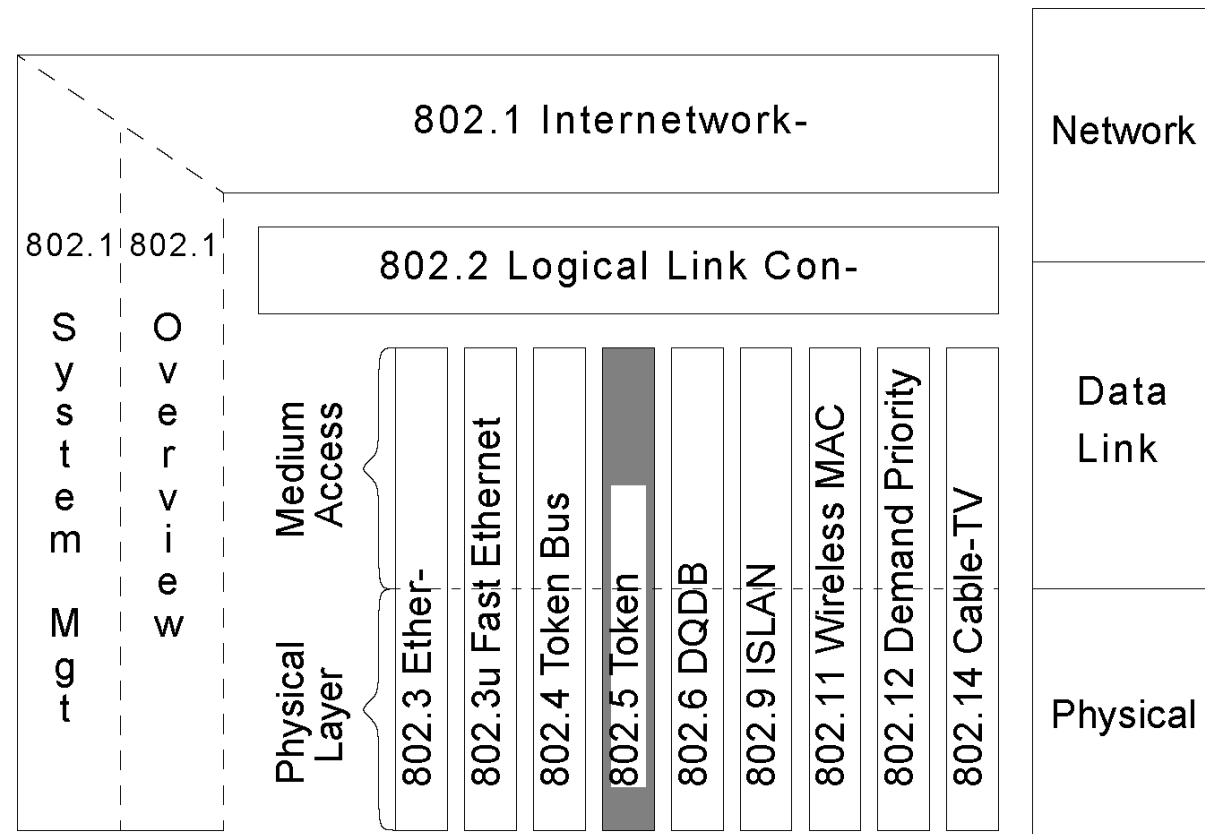
➔ hence: reduced collision domain

8 IEEE 802.5: Token Ring

Access Control Procedures



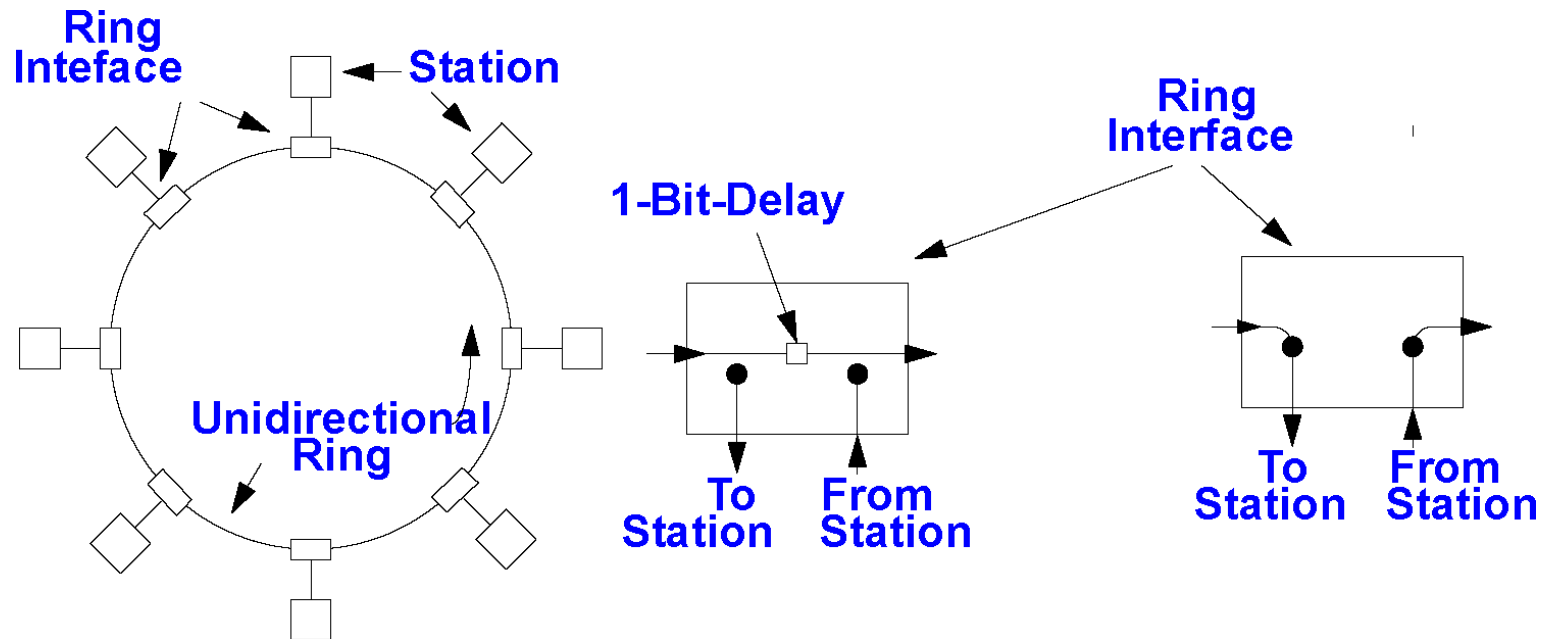
IEEE 802.5: Token Ring



History

- Z-Ring: prototype of a Token Ring (IBM Zurich)
- IBM chooses Token Ring as the inhouse LAN standard
 - 1985: IEEE 802.5
 - 1986: IBM Token Ring product
- Reasonably widespread use in 1980's and 1990's
- Basically out of operation since many years

802.5: Ring Topology

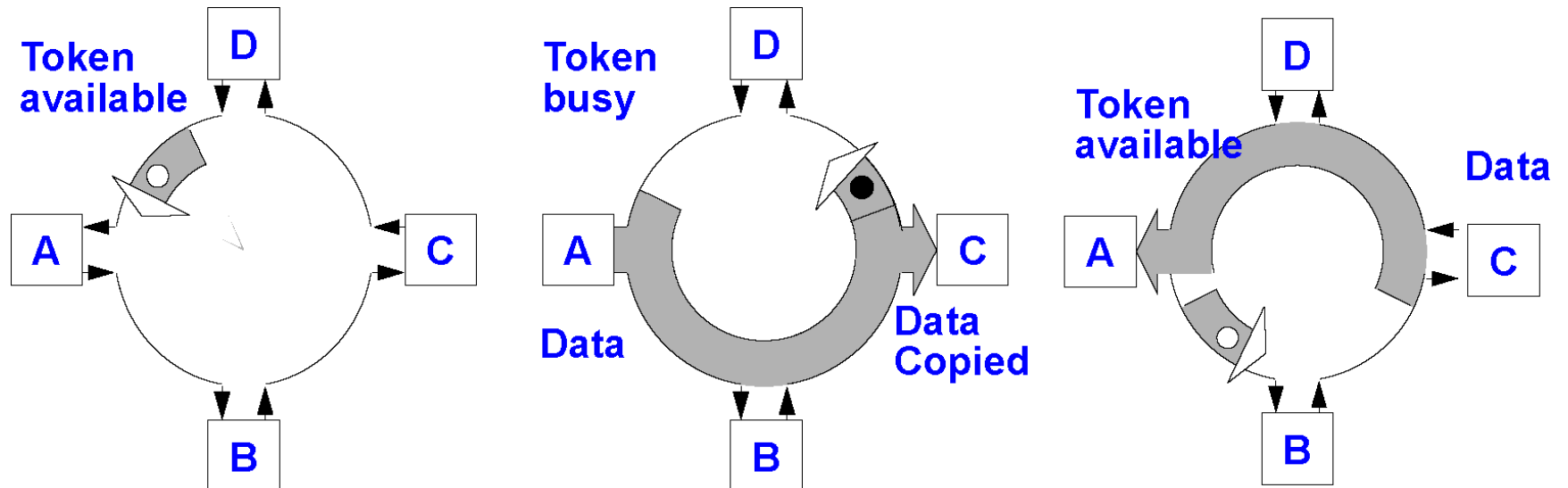


Ring

- not really a broadcast medium, but
 - a concatenation of point-to-point lines
- station copies information bit by bit from one line to the next (active station)

802.5: MAC Protocol

Token Protocol



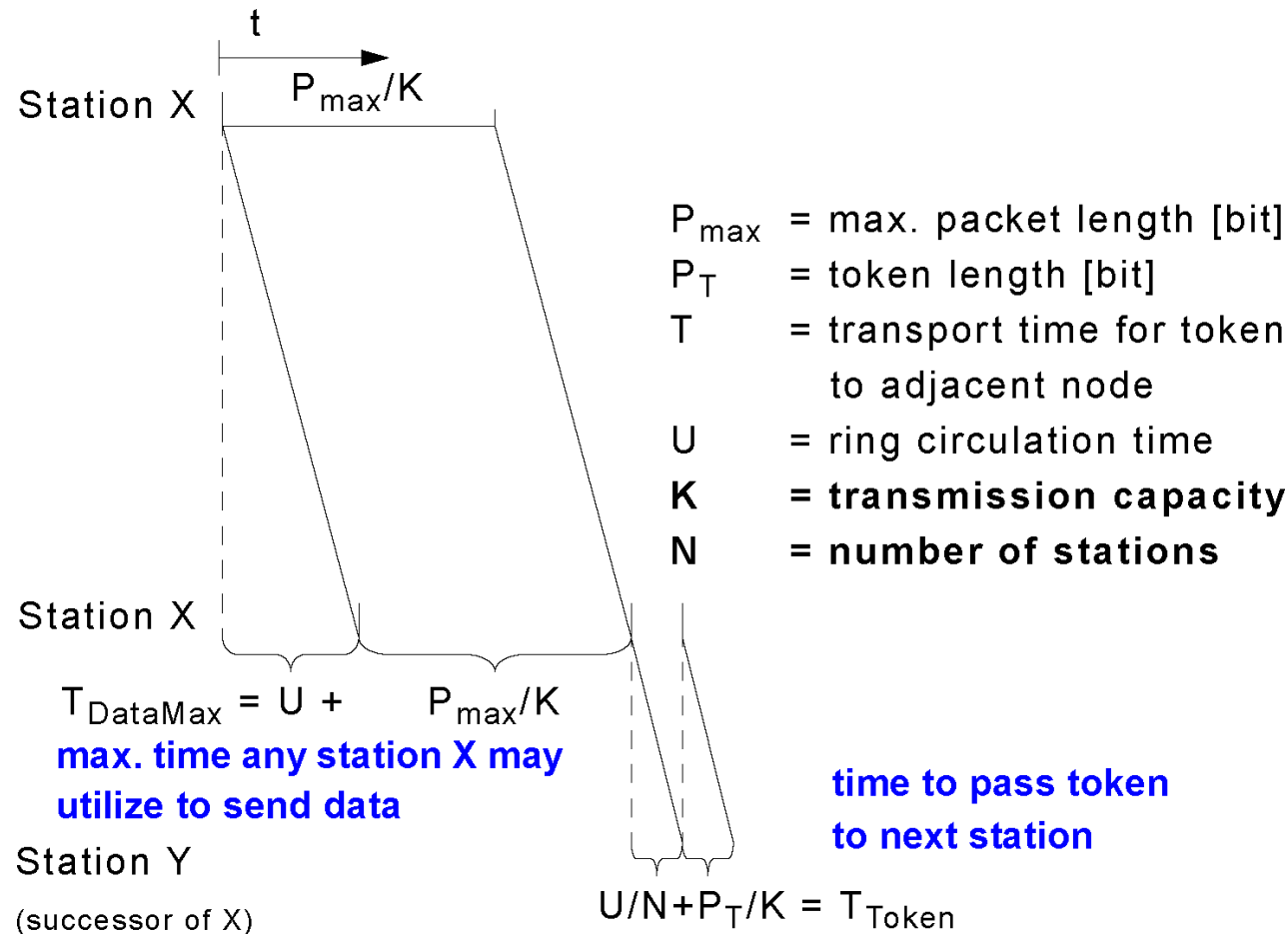
Principle

- token
 - frame with special bit pattern
- one token circulates on the ring
 1. before station is permitted to send
 - it must own and remove the token from the ring
 2. station may keep the token for a pre-defined time and may send several frames
 3. after sending
 - the station generates a new token

802.5: Maximum Waiting Period

What is the maximum waiting period for a station before it receives permission to send again?

- i.e. all stations want to send with the max. amount of allowed time



802.5: Maximum Waiting Period

What is the maximum waiting period for a station before it receives permission to send again?

W = maximum waiting period:

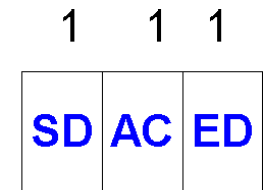
$$\begin{aligned} W &= \text{all others are sending} + \text{token rotates } x\text{-times} \\ &= (N-1) (P_{\max}/K + U) + N(P_T/K + U/N) \\ &= (N-1) (P_{\max}/K + U) + NP_T/K + U \\ &= (N-1) (P_{\max}/K + U) + U \end{aligned}$$

Note: $NP_T/K = 0$ for $P_T \ll P_{\max}$

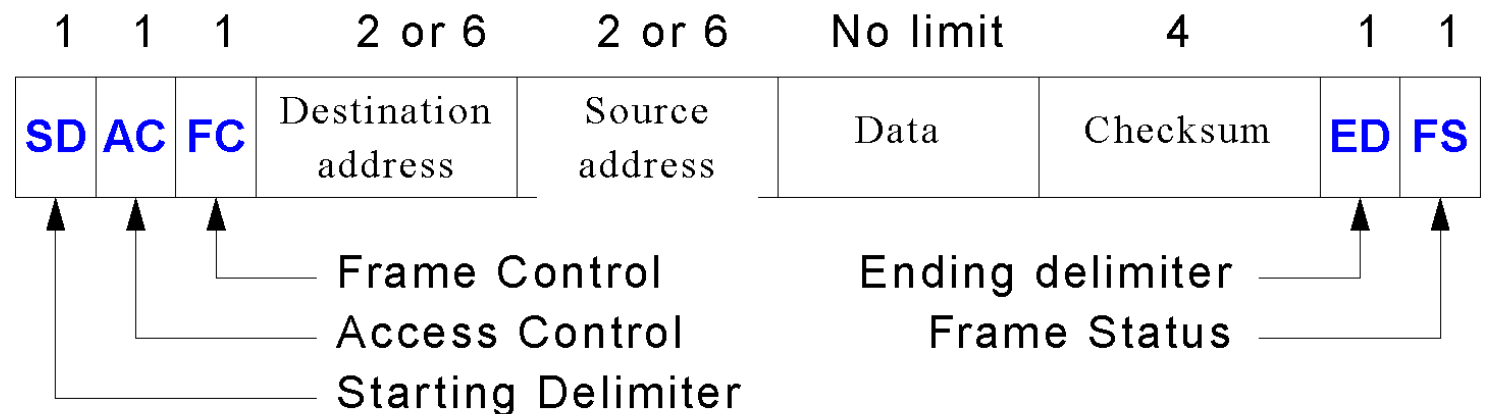
802.5: Token and Frames

Token

- 3 byte length



Frame



AC contains **TOKENBIT T**

SD AC mit T = 1: "Start of Frame"-Sequence

T = 0: Token

T = 1: Data

- "Remove Token from Ring": T := 1

AC provides for priorities & reservations

9 Higher-Speed LANs, WANs and MANs

LAN development

- towards
 - more speed
 - shared bandwidth
- from conventional data towards
 - integrated data (conventional & audio/video)
- sometimes also increasing extension (100 km)
- i.e. High-Speed LAN also as MAN

WAN development

- towards
 - more speed
 - bandwidth per connection
- from audio (video) towards
 - integrated services (conventional & audio/video)
- also decreasing extension (down to Desk Area range)
- i. e. WAN also as MAN (and LAN)

LAN, (MANs) and IEEE

- 802.1 Overview Document Containing the Reference Model, Tutorial, and Glossary
 - 802.1 p Specification for LAN Traffic Prioritization
 - 802.1 q Virtual Bridged LANs
- 802.2 Logical Link Control
- 802.3 Contention Bus Standard 10 base 5 (Thick Net)
 - 802.3a Contention Bus Standard 10base 2 (Thin Net)
 - 802.3b Broadband Contention Bus Standard 10 broad 36
 - 802.3d Fiber-Optic InterRepeater Link (FOIRL)
 - 802.3e Contention Bus Standard 1 base 5 (Starlan)
 - 802.3i Twisted-Pair Standard 10base T
 - 802.3j Contention Bus Standard for Fiber Optics 10base F
 - ➔ • 802.3u 100-Mb/s Contention Bus Standard 100base T
 - 802.3x Full-Duplex Ethernet
 - ➔ • 802.3z Gigabit Ethernet
 - 802.3ab Gigabit Ethernet over Category 5 UTP

9.1 IEEE 802.3u: Fast Ethernet

History

- High-Speed LAN COMPATIBLE to existing Ethernet
- 1992:
 - IEEE sets objective to improve existing systems
- 1995:
 - 802.3u passed as an addendum to 802.3
 - (alternative solution containing new technology in 802.12)

Principle

- retain all procedures, format, protocols
- bit duration
 - reduced from 100 ns to 10 ns

IEEE 802.3u: Fast Ethernet: Properties

Properties: CSMA/CD at 100 Mbps

cost efficient extension of 802.3

very limited network extension

- sender has to be able to recognize collision while it is sending
 - network extension must not exceed the size of the minimum frame
 - frame at least 64 byte, i.e. 5 μ s at 100 Mbps per bit
- i.e. extension only a few 100 meters
"collision domain diameter" = 412 m
(instead of 3000m)

many collisions (lower utilization)

9.2 IEEE 802.3z: Gigabit Ethernet

History

- IF POSSIBLE,
 - High-Speed LAN compatible with existing Ethernet
- 1998: 802.3z passed as an Addendum to 802.3

Desirable principle

- if 100% compatible
 - retain all procedures, formats, protocols
 - bit duration reduced from 100 ns over 10 ns to 1 ns
- but, then
 - maximum extension would also be
 - 1/100 of the 10 Mbit/s Ethernet,
 - i. e. (depending on the type of cable) approx. 30 m

IEEE 802.3z: Gigabit Ethernet

Principle for

- A. point-to-point links
 - full duplex mode
 - no change of packet size
 - interconnected by switch function
 - with 1 Gbps in both directions
- B. shared broadcast mode
 - half duplex mode
 - CSMA/CD
 - interconnected by hub function
 - tradeoff between distance and efficiency
- i.e. see the following details

IEEE 802.3z: Gigabit Ethernet: Shared Broadcast Mode

Principle:

- maintain (as far as possible)
 - CSMA/CD with 64 byte minimum length

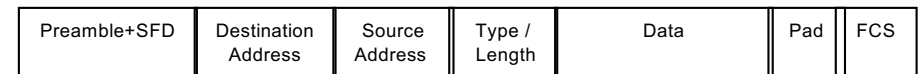
→ introducing two features

- **carrier extension**
- **frame bursting**

IEEE 802.3z: Gigabit Ethernet: Shared Broadcast Mode

Principle:

- maintain (as far as possible)
 - CSMA/CD with 64 byte minimum length
- introducing two features
 - **carrier extension**
 - frame bursting



Carrier extension

- from 512 bit (64 byte) length, previously
- to 512 byte length
- i. e. by attaching a new extension field
 - following the FCS field (Frame Check Sum)
 - to achieve the length of 512 byte
- Approach:
 - added by sending hardware and
 - removed by receiving hardware
 - software doesn't notice this
- low efficiency
 - transmit 46 byte user data using 512 byte: 9%

IEEE 802.3z: Gigabit Ethernet: Shared Broadcast Mode

Principle:

- maintain (as far as possible)
 - CSMA/CD with 64 byte minimum length
- introducing two features
 - carrier extension
 - **frame bursting**

Frame bursting

- allow sender to transmit **CONCATENATED SEQUENCE OF MULTIPLE FRAMES** in single transmission
 - needs frames waiting for transmission
 - better efficiency



IEEE 802.3z: Gigabit Ethernet: Shared Broadcast Mode

Maximum extension of a segment (i.e. of a Collision Domain)

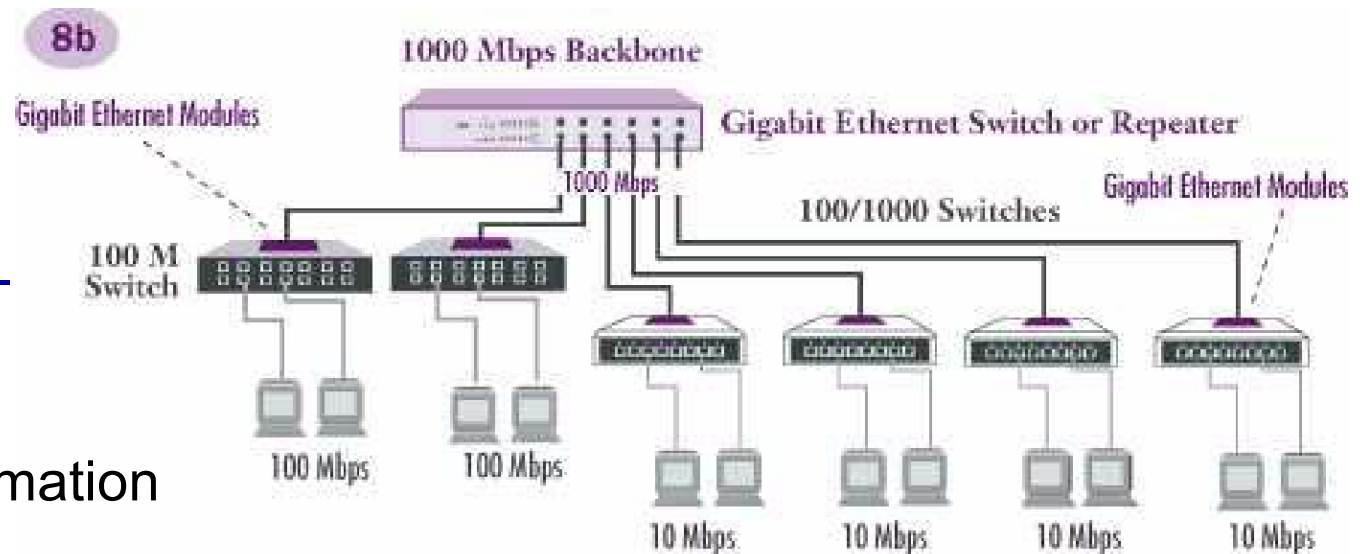
- 5 UTP 100 m
- coax 25 m
- multimode fiber 550 m
- single mode fiber 5 km

Possible uses

- preferably in the "Backbone-Network"

Sources of information

- IEEE
 - <http://grouper.ieee.org/groups/802/3/z/index.html>
- Gigabit Ethernet Alliance
 - <http://www.gigabit-ethernet.org>



9.3 IEEE 802.3ae: 10Gbit Ethernet

History:

- 1999: IEEE 802.3ae task force founded
- 2002: approval as a standard

Objectives

- to preserve 802.3 frame format
 - incl. minimal and maximal frame sizes
- to support full duplex operation only
- ➔ no CSMA/CD required

Type of media used

- works over optical fiber only
- (now also variants IEEE 802.3ak and IEEE 802.3an for copper cables)

Sources of information

- **IEEE:** <http://grouper.ieee.org/groups/802/3/ae/index.html>
- further
 - 10 Gigabit Ethernet Alliance (10GEA) and others
 - <http://www.10gea.org>
 - <http://www.10gigabit-ethernet.com/>

9.4 40 Gbit and 100 Gbit Ethernet

History:

- 2006: formation of High Speed Study Group (HSSG)
- Then first standard defined by the IEEE 802.3ba-**2010**
- Later standards 802.3bg-**2011**, 802.3bj-**2014**, and 802.3bm-**2015**

Objectives

- to preserve 802.3 frame format
 - incl. minimal and maximal frame sizes
- to support full duplex operation only

Definition of numerous port types with different optical and electrical interfaces and different numbers of optical fiber strands per port

Short distances over *twina*xial cable are supported

40GBASE-T uses twisted pair cabling for 40 Gbit/s over up to 30 m

Further information, e.g.,

- **IEEE:** <http://grouper.ieee.org/groups/802/3/ba>

10 Wireless LANs

Can we use media access methods from wired networks?

- e.g., CSMA/CD?

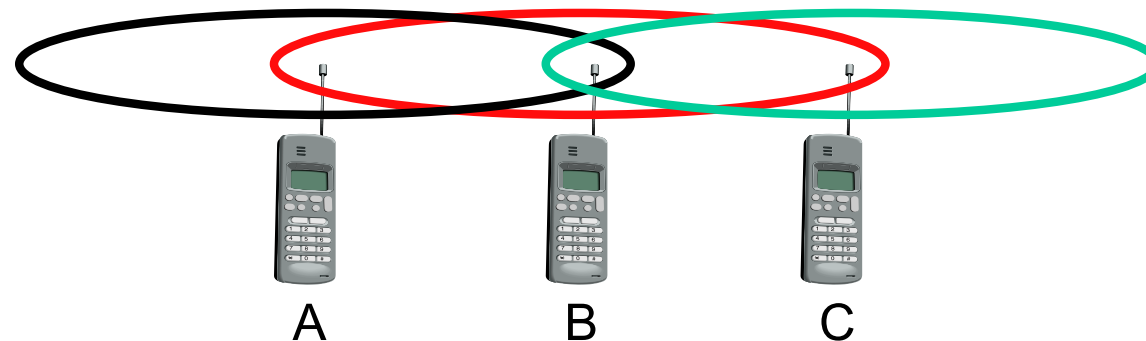
Several problems in wireless networks

- signal strength decreases proportional to square of the distance
- sender applies CS and CD, but collisions happen at receiver
- sender might not “hear” the collision, i.e., CD does not work
- furthermore, CS might not work if, e.g., a terminal is “hidden”

Hidden and Exposed Terminals

Hidden terminals

- A sends to B, C cannot receive A
- C wants to send to B, C senses a “free” medium (CS fails)
- collision at B, A cannot receive the collision (CD fails)
- A is “hidden” for C



Exposed terminals

- B sends to A, C wants to send to another terminal (not A or B)
- C has to wait, CS signals a medium in use
- but A is outside radio range of C, thus, waiting is not necessary
- C is “exposed” to B

MACA - collision avoidance

MACA (Multiple Access with Collision Avoidance) uses short signaling packets for collision avoidance

- RTS (request to send): a sender request the right to send from a receiver with a short RTS packet before it sends a data packet
- CTS (clear to send): the receiver grants the right to send as soon as it is ready to receive

Signaling packets contain

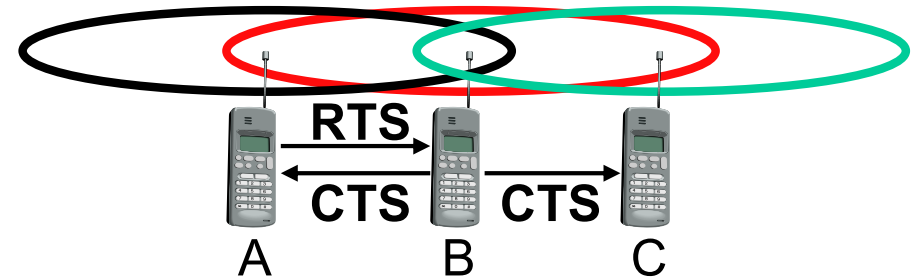
- sender address
- receiver address
- packet size

Variants of this method can be found in IEEE802.11 as DFWMAC (Distributed Foundation Wireless MAC)

MACA examples

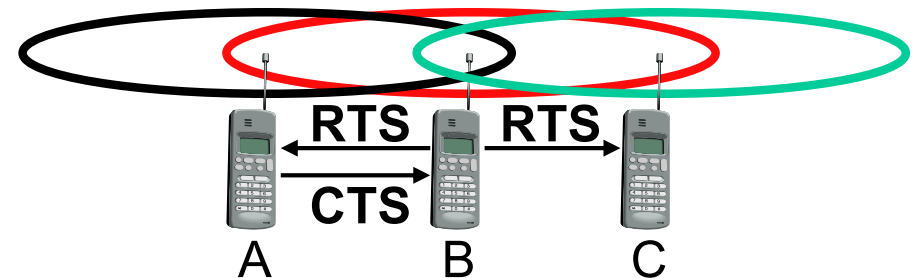
MACA avoids the problem of hidden terminals

- A and C want to send to B
- A sends RTS first
- C waits after receiving CTS from B



MACA avoids the problem of exposed terminals

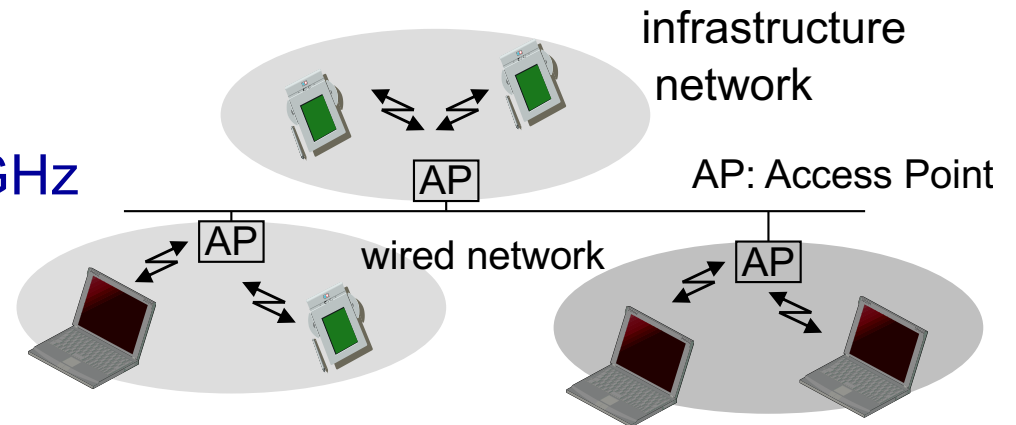
- B wants to send to A, C to another terminal
- now C does not have to wait for it cannot receive CTS from A



IEEE 802.11: Wireless LANs -- WiFi

Starting in the 1990s

- e.g., easy setup of LANs
- uses ISM bands, e.g., 2.4GHz
- many variants
- very dynamic development
- very common



CSMA/CA for Medium Access

- Use random small gaps (Inter-Frame Spaces) to avoid collisions
- Station picking shorter gap wins

