Outline

- A preliminary overview
- Propagation characteristics
- ISO-OSI Model
- Physical layer: modulation
- **MAC layer:**
  - Fixed resource assignment
  - **Random access**
    - Ethernet (CSMA/CD)
    - WiFi (CSMA/CA)
- Personal Area Networks
  - Bluetooth
  - Zigbee
- Cellular network dimensioning
- Cellular networks
  - From GSM (2G) to UMTS (3G)
  - LTE (4G)

Multiple Access protocols

- Single shared broadcast channel
- Two or more simultaneous transmissions by nodes: interference
  - Collision if node receives two or more signals at the same time

Multiple Access Protocol

- Distributed algorithm that determines how nodes share channel, i.e., determine when node can transmit
- Communication about channel sharing must use channel itself!
  - No out-of-band channel for coordination

Channel Partitioning

- Frequency Division Multiplexing
  - Each node has a frequency band
- Time Division Multiplexing
  - Each node has a series of fixed time slots
- What networks are these good for?

Computer Network Characteristics

- Transmission needs vary
  - Between different nodes
  - Over time
- Network is not fully utilized

Ideal Multiple Access Protocol

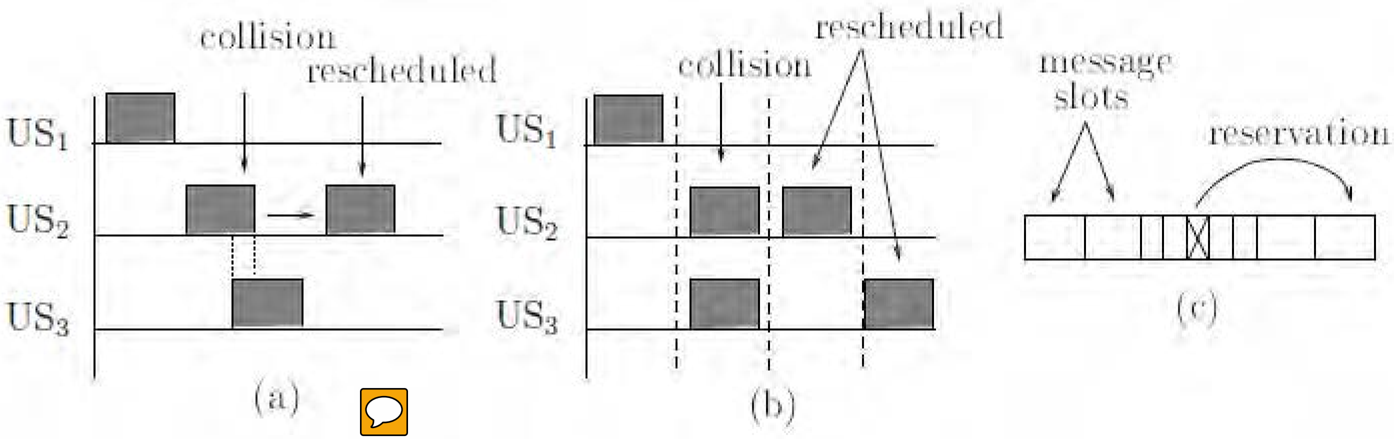
<u>Broadcast channel of rate R bps</u>

1. When one node wants to transmit, it can send at rate R.
2. When M nodes want to transmit, each can send at average rate R/M
3. Fully decentralized:
   - no special node to coordinate transmissions
   - no synchronization of clocks, slots
4. Simple

Random Access Protocols

- When node has packet to send
  - transmit at full channel data rate R.
  - no *a priori* coordination among nodes
- two or more transmitting nodes ➜ “collision”,
- random access MAC protocol specifies:
  - how to detect collisions
  - how to recover from collisions (e.g., via delayed retransmissions)
- Examples of random access MAC protocols:
  - slotted ALOHA
  - ALOHA
  - CSMA, CSMA/CD, CSMA/CA

Aloha: the idea



(a) Pure Aloha;

(b) slotted Aloha;

(c) reservation Aloha.

- Created at the University of Hawaii in 1970 under the leadership of Norman Abramson.
- The idea was to use shared radio to create a computer network linking the far-flung campuses of the University.
- Two distinct frequencies in a star configuration were used, one for downlink channel and one for the uplink channel.

Slotted Aloha

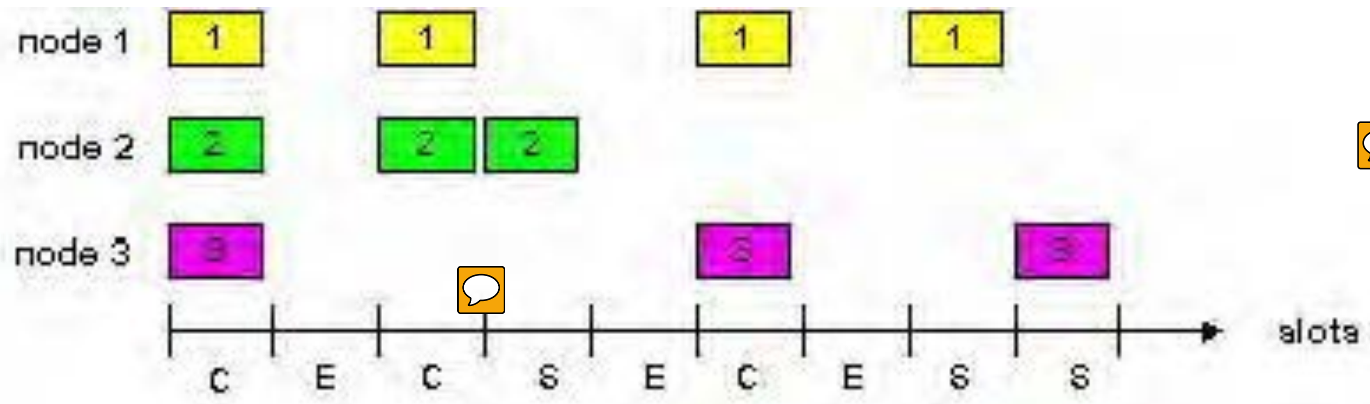
Assumptions

- all frames same size
- time is divided into equal size slots, time to transmit 1 frame
- nodes start to transmit frames only at beginning of slots
- nodes are synchronized
- if 2 or more nodes transmit in slot, all nodes detect collision

Operation

- when node obtains fresh frame, it transmits in next slot
- no collision, node can send new frame in next slot
- if collision, node retransmits frame in each subsequent slot with prob. p until success

Slotted Aloha



Pros

- single active node can continuously transmit at full rate of channel
- highly decentralized: only slots in nodes need to be in sync
- simple

Cons

- collisions, wasting slots
- idle slots
- nodes may be able to detect collision in less than time to transmit packet
- clock synchronization

Slotted Aloha efficiency

- **Efficiency** is the long-run fraction of successful slots when there are many nodes, each with many frames to send
- Suppose N nodes with many frames to send, each transmits in slot with probability *p*
- prob that node 1 has success in a slot = $p(1-p)^{N-1}$
- prob that any node has a success = $Np(1-p)^{N-1}$

Optimal choice of p

- For max efficiency with N nodes, find p* that maximizes
  $Np(1-p)^{N-1}$
- For many nodes, take limit of $Np^*(1-p^*)^{N-1}$ as N goes to infinity, gives 1/e = .37
- Efficiency is 37%, even with optimal p

Throughput of the Slotted Aloha Protocol

- It can be easily proved (Reti B) that the throughput is twice that of the pure Aloha:

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

- A maximum can be identified as

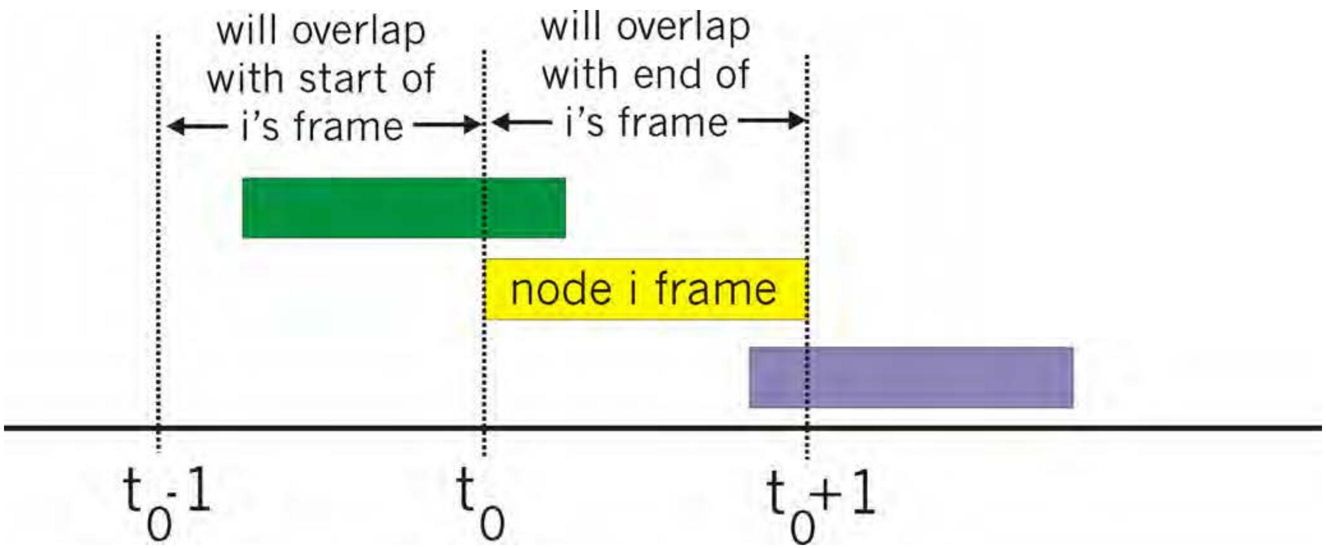
$$S' = e^{-G} - Ge^{-G} = e^{-G}(1 - G)$$

obtaining

$$S' = 0 \Longrightarrow S_{\max} = e^{-1} = 0.36.$$

Pure (unslotted) Aloha

- unslotted Aloha: simpler, no synchronization
- when frame first arrives
  - transmit immediately
- collision probability increases:
  - frame sent at t_0 collides with other frames sent in $[t_0-1,t_0+1]$



Pure Aloha efficiency

P(success by given node) = P(node transmits) $\cdot$

P(no other node transmits in $[t_0\text{-}1,t_0]$ $\cdot$

P(no other node transmits in $[t_0,t_0+1]$

$= p \cdot (1\text{-}p)^{N\text{-}1} \cdot (1\text{-}p)^{N\text{-}1}$

$= p \cdot (1\text{-}p)^{2(N\text{-}1)}$

… choosing optimum p and then letting n -> ∞ ...

Even worse !

Efficiency = 1/(2e) = .18

Throughput of the Pure Aloha Protocol

- It can be easily prove~~d~~N (Reti B) that

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

where G is the offered load.

- A maximum can be identified by deriving:

$$S' = e^{-2G} - 2Ge^{-2G} = e^{-2G}(1 - 2G)$$

and setting the derivative to zero:

$$S' = 0 \Longrightarrow S_{\max} = \frac{1}{2}e^{-1} = 0.18.$$

- If $\lambda = 1$ Mb/s, then $\lambda S_{\max} = 180$ Kb/s.
- In TDMA-based systems, instead, $\lambda S_{\max} = 1$ Mb/s, since the maximum throughput of 1 can be achieved without any synchronization error.

Carrier Sense Multiple Access

<u>CSMA</u>: listen before transmit:

If channel sensed idle: transmit entire frame

- If channel sensed busy, defer transmission

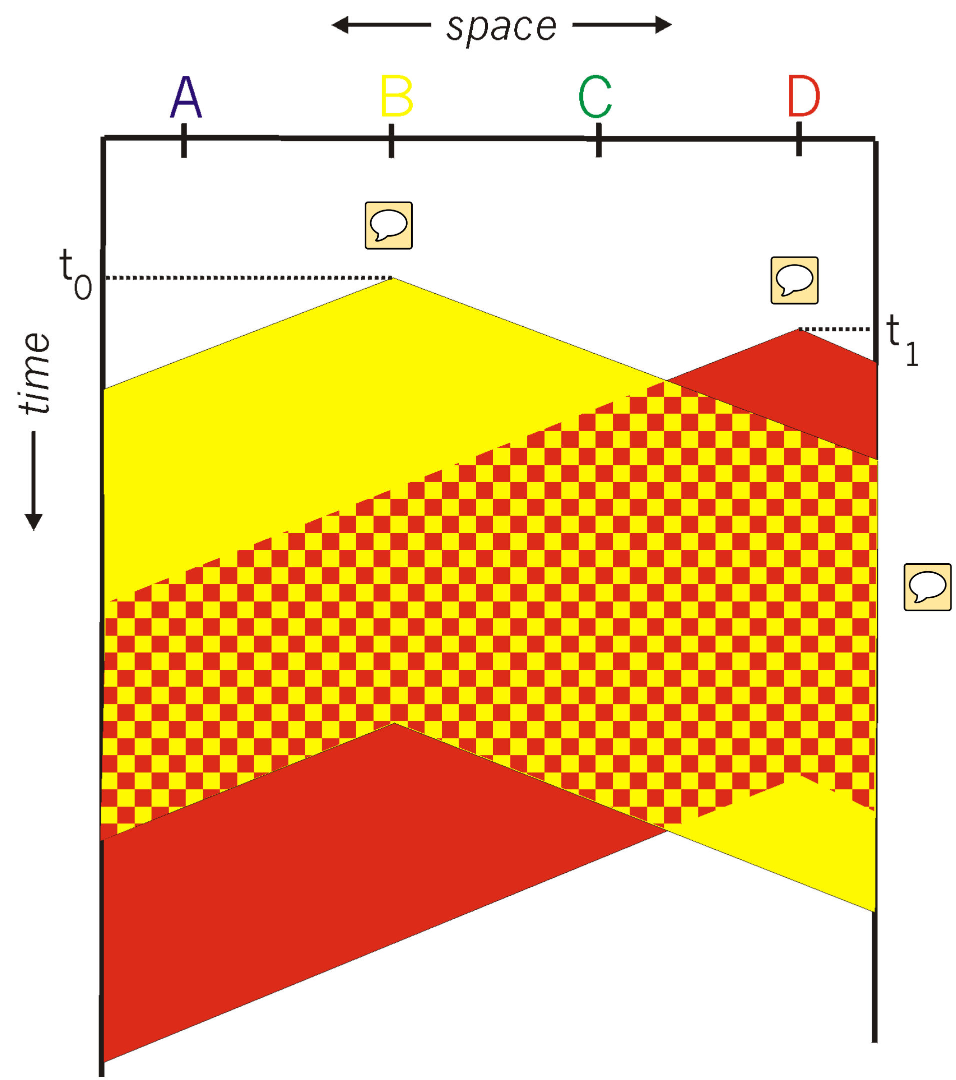
- Human analogy: don't interrupt others!

CSMA collisions

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

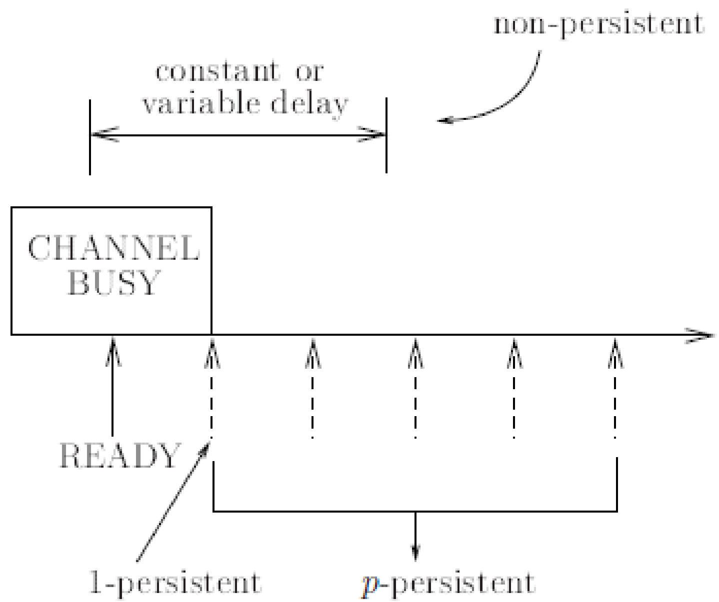
collision:
entire packet transmission time wasted

note:
role of distance & propagation delay in determining collision probability

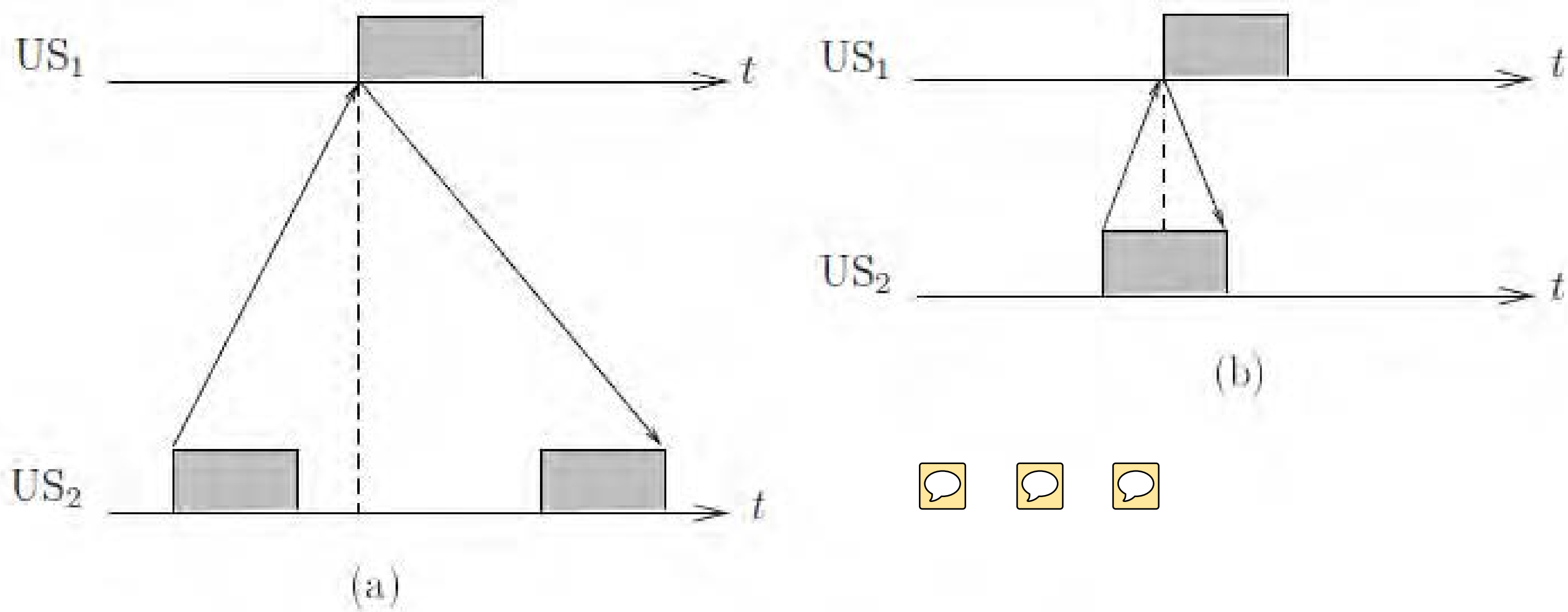


Retransmission strategies

- Non-persistent: if an user senses the channel busy, the transmission is deferred by a constant or pseudo-random delay.
- 1-persistent: if the medium becomes idle, the sender transmits with probability *p*, and so on.
- *p*-persistent: the sender waits a random period of time, checks the channel, and if it is idle, transmits with a probability *p*, and so on.



Vulnerable interval



$$\text{vulnerable interval} = \min\{t_\mathrm{p}, 2\tau\}$$

where t_p is the packet time and τ is the propagation delay (i.e., 2τ is round trip delay).

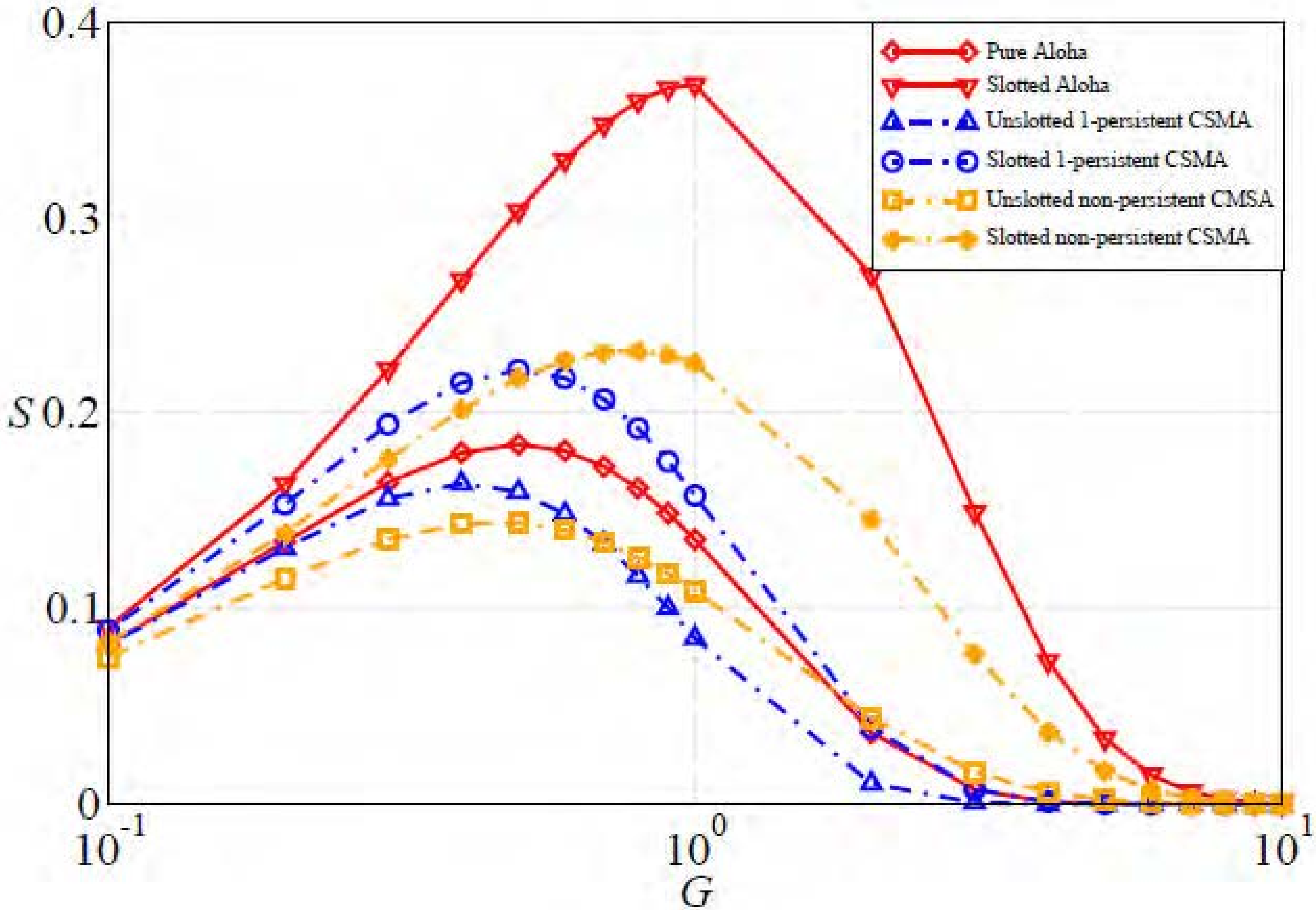
A Few Formulas

Protocol	Throughput (S)
Aloha	Ge^{-2G}
Slotted Aloha	Ge^{-G}
Unslotted 1-persistent CSMA	$\frac{G[1+G+aG(1+G+aG/2)]e^{-G(1+2a)}}{G(1+2a)-(1-e^{-aG})+(1+aG)e^{-G(1+a)}}$
Slotted 1-persistent CSMA	$\frac{G(1+a-e^{-aG})e^{-G(1+a)}}{(1+a)(1-e^{-aG})+ae^{-G(1+a)}}$
Unslotted nonpersistent CSMA	$\frac{Ge^{-aG}}{G(1+2a)+e^{-aG}}$
Slotted nonpersistent CSMA	$\frac{aGe^{-aG}}{1-e^{-aG}+a}$

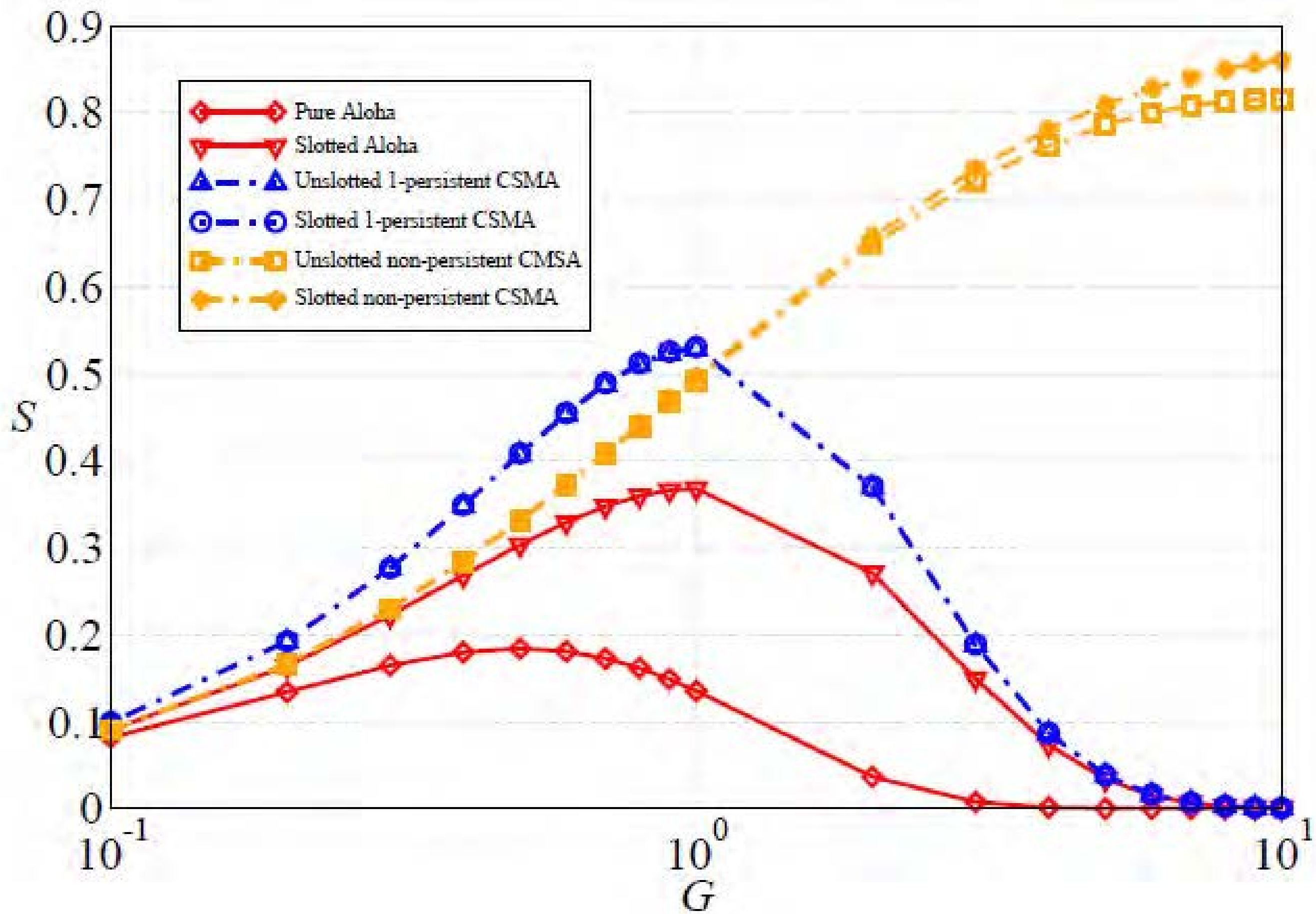
where

- $a \triangleq \frac{\tau}{T_{\text{pck}}}$ (normalized propagation delay);
- S is the average number of successful transmissions in T_{pck};
- G is the average number of packets generated (network-wide) in T_{pck}

Throughput Comparison (CSMA with $a = 1$)



Throughput Comparison (CSMA with $a = 0.01$)



Outline

- A preliminary overview
- Propagation characteristics
- ISO-OSI Model
- Physical layer: modulation
- MAC layer:
  - Fixed resource assignment
  - Random access
    - **Ethernet (CSMA/CD)**
    - WiFi (CSMA/CA)
- Personal Area Networks
  - Bluetooth
  - Zigbee
- Cellular network dimensioning
- Cellular networks
  - From GSM (2G) to UMTS (3G)
  - LTE (4G)

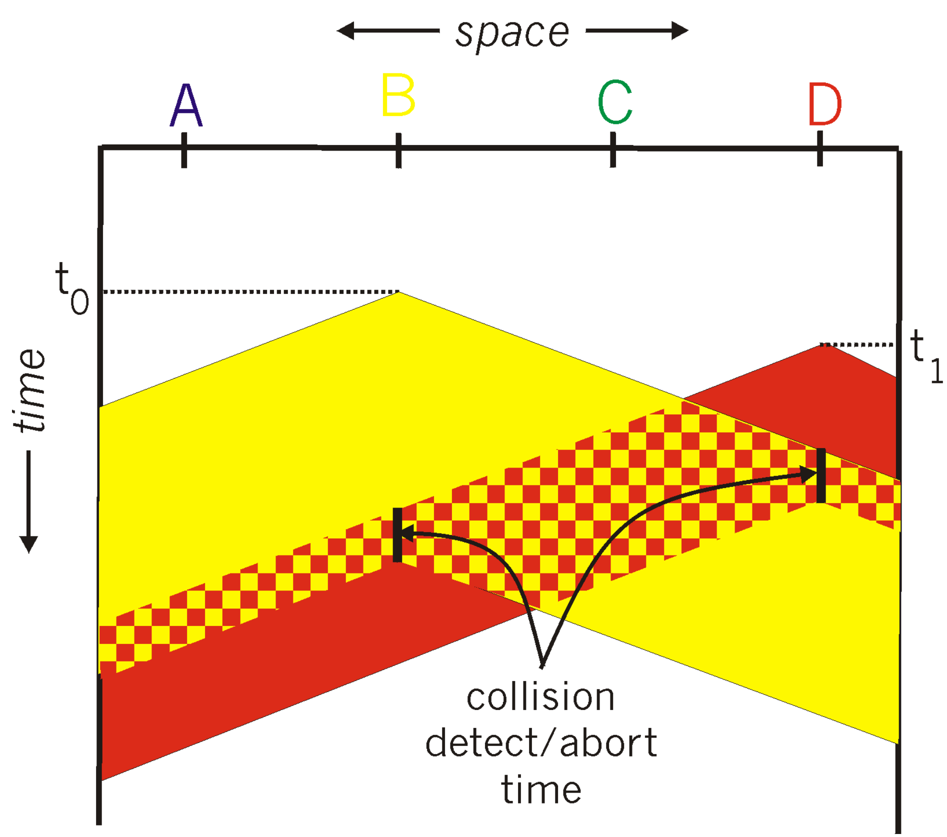
CSMA/CD (Collision Detection)

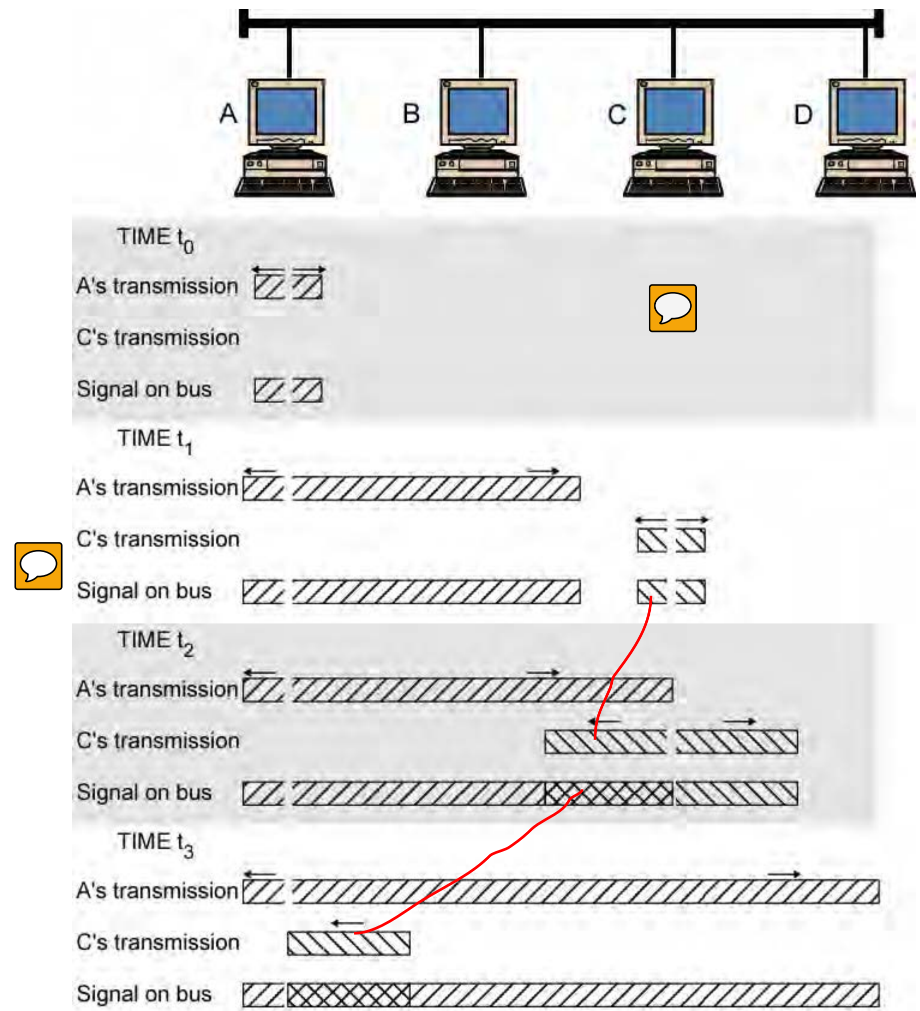
CSMA/CD: carrier sensing, deferral as in CSMA

- 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: receiver shut off while transmitting
- human analogy: the polite conversationalist

CSMA/CD collision detection

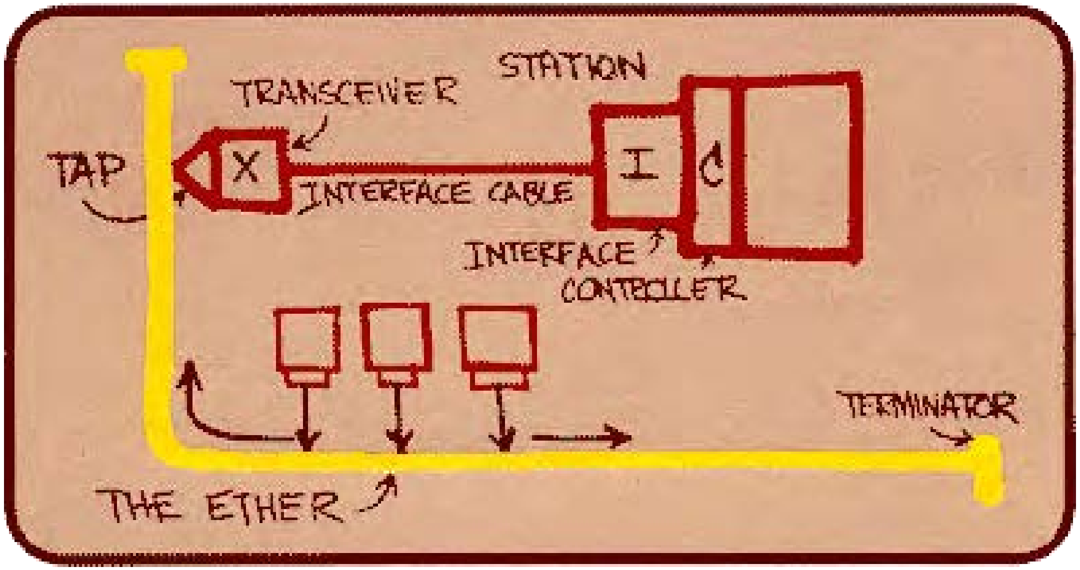




Ethernet

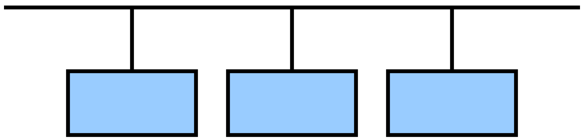
dominant wired LAN technology:

- cheap $20 for 100Mbs!
- first widely used LAN technology
- Simpler, cheaper than token LANs and ATM
- Kept up with speed race: 10 Mbps – 10 Gbps



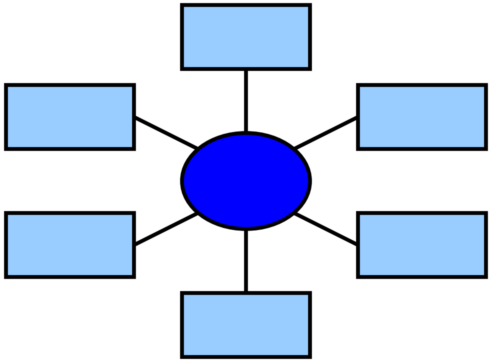
Metcalfe's Ethernet sketch

Ethernet Topologies



Bus Topology: Shared

All nodes connected to a wire



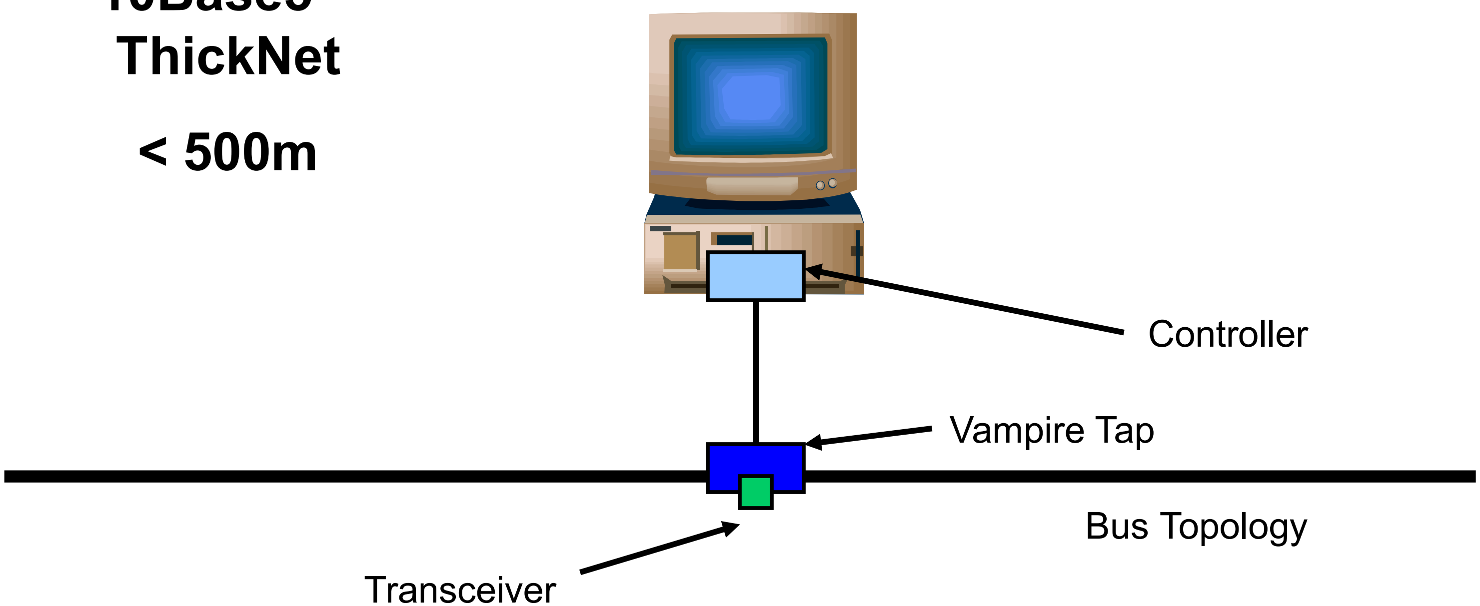
Star Topology:

All nodes connected to a central repeater

Ethernet Connectivity

10Base5 – ThickNet

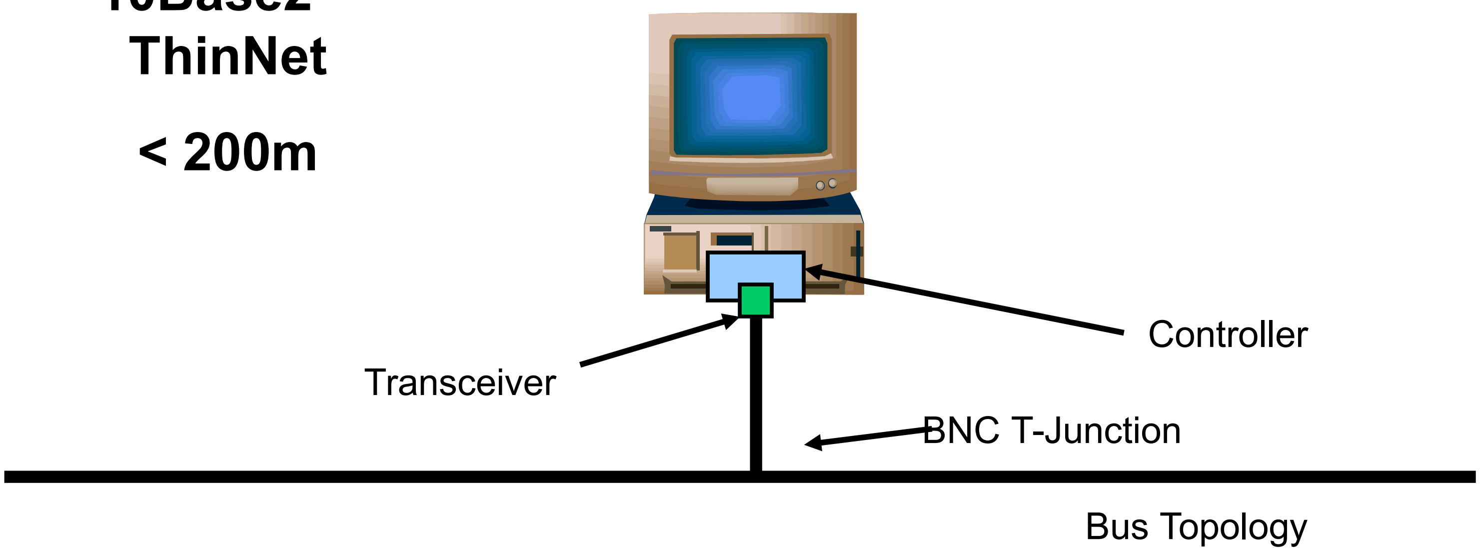
< 500m



Ethernet Connectivity

10Base2 – ThinNet

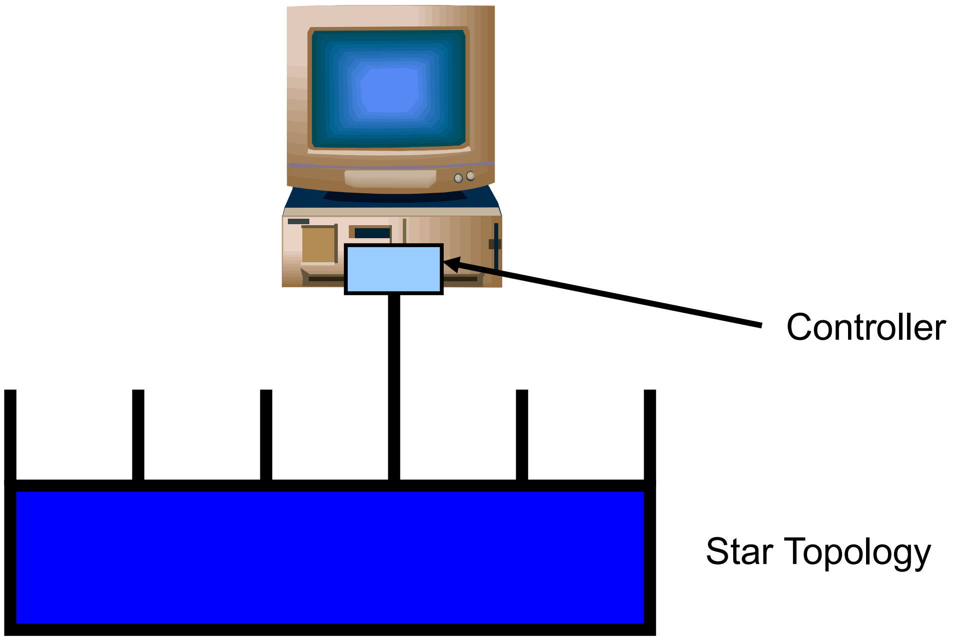
< 200m



Ethernet Connectivity

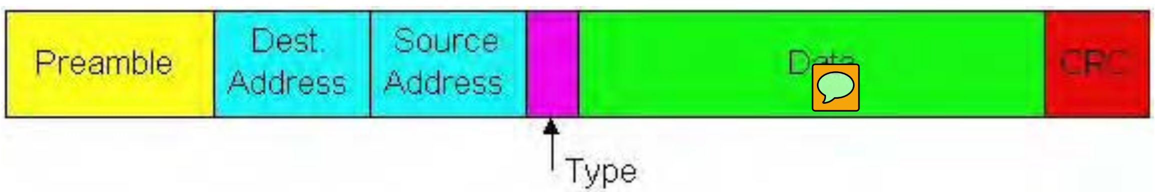
10BaseT

< 100m



Ethernet Frame Structure

Sending adapter encapsulates IP datagram (or other network layer protocol packet) in Ethernet frame

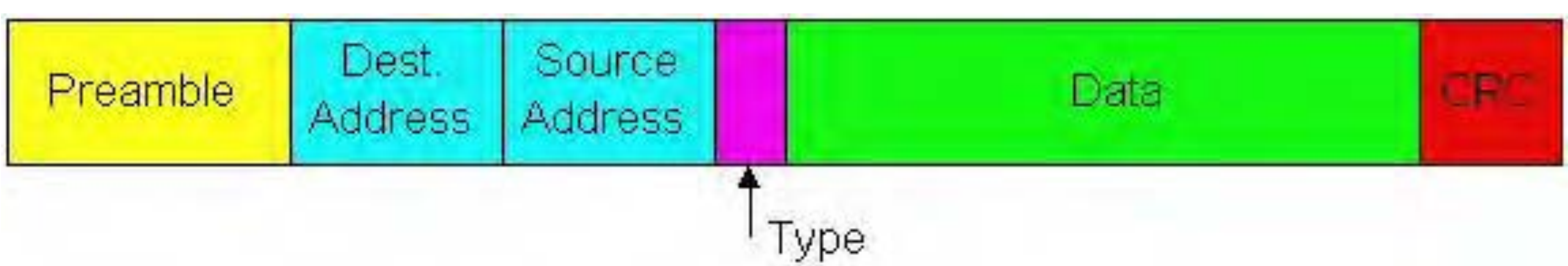


Preamble:

- 7 bytes with pattern 10101010 followed by one byte with pattern 10101011
- Used to synchronize receiver, sender clock rates (Manchester encoding)

Ethernet Frame Structure (ctd)

- Addresses: 6 bytes
  - if adapter receives frame with matching destination address, or with broadcast address (eg ARP packet), it passes data in frame to net-layer protocol
  - otherwise, adapter discards frame
- Type: indicates the higher layer protocol (mostly IP but others may be supported such as Novell IPX and AppleTalk)
- CRC: checked at receiver, if error is detected, the frame is simply dropped



Ethernet Specifications

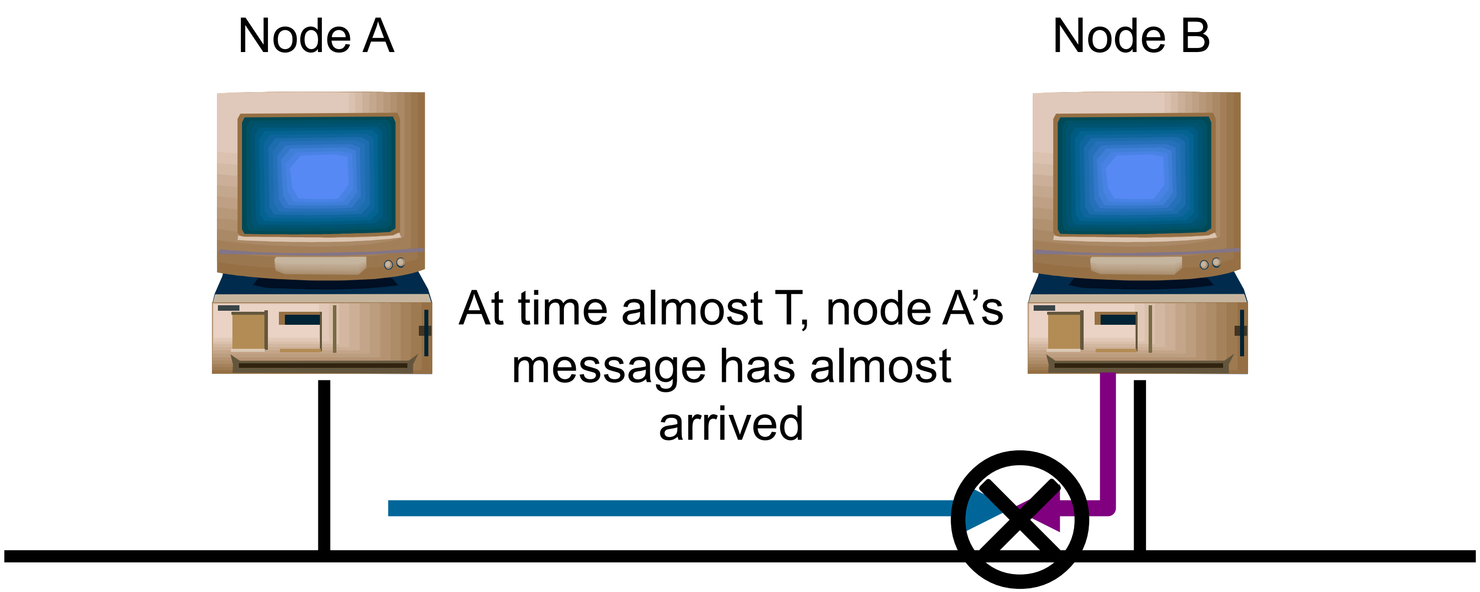
- Coaxial Cable
  - Up to 500m
- Taps
  - > 2.5m apart
- Transceiver
  - Idle detection
  - Sends/Receives signal
- Repeater
  - Joins multiple Ethernet segments
  - < 5 repeaters between any two hosts
- < 1024 hosts

Ethernet MAC Algorithm

- Sender/Transmitter
  - If line is idle (NO carrier sensed)
    - Send immediately
    - Send maximum of 1500B data (1527B total)
    - Wait 9.6 μs before sending again
  - If line is busy (~~no~~ carrier sense)
    - Wait until line becomes idle
    - Send immediately
  - If collision detected
    - Stop sending and jam signal
    - Try again later

YUMMY

Ethernet MAC Algorithm



Node A starts transmission at time 0

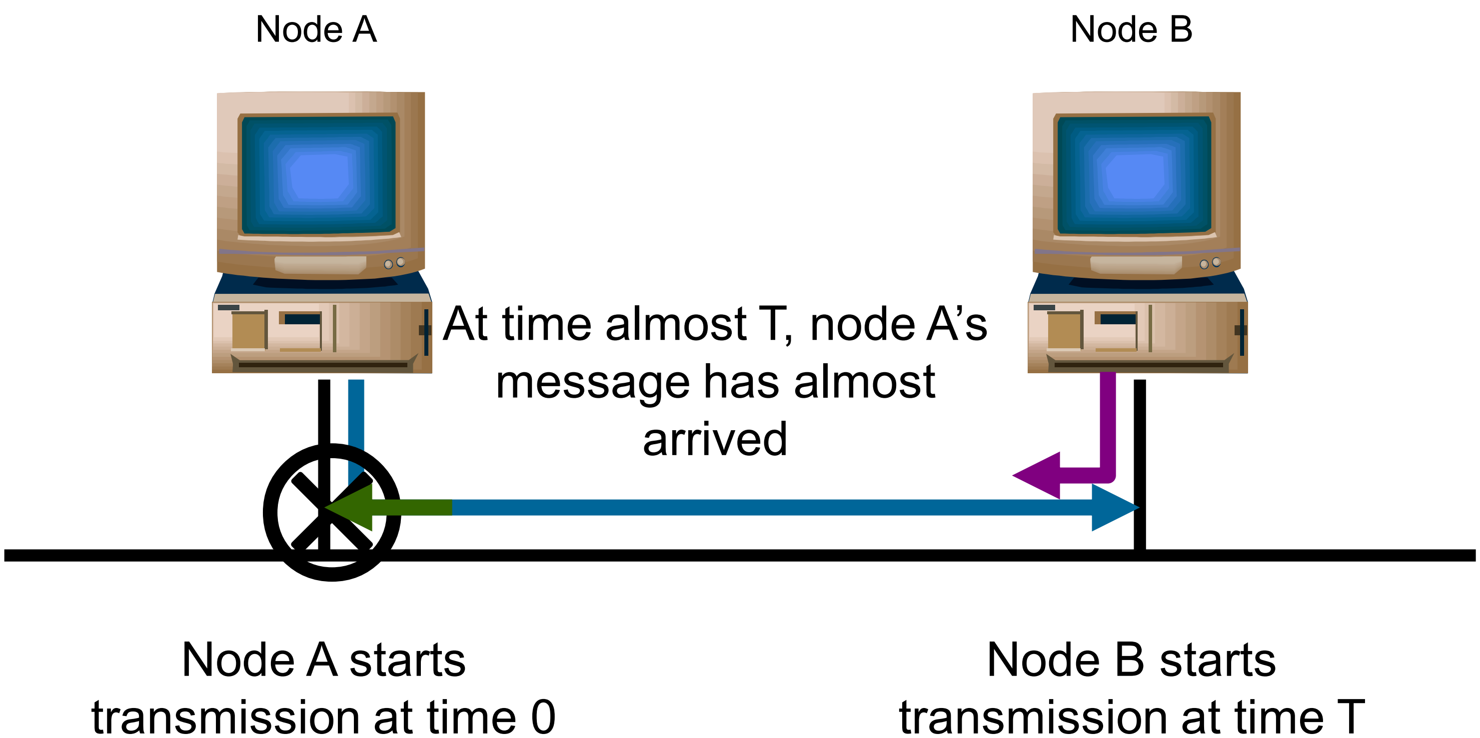
Node B starts transmission at time T

How can we ensure that A knows about the collision?

Collision Detection

- Example
  - Node A's message reaches node B at time T
  - Node B's message reaches node A at time 2T
  - For node A to detect a collision, node A must still be transmitting at time 2T
- 802.3
  - 2T is bounded to 51.2μs
  - At 10Mbps 51.2μs = 512b or 64B
  - Packet length $\geq$ 64B
- Jam after collision
  - Ensures that all hosts notice the collision

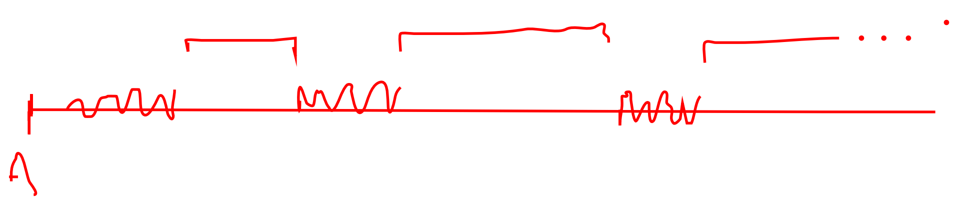
Ethernet MAC Algorithm



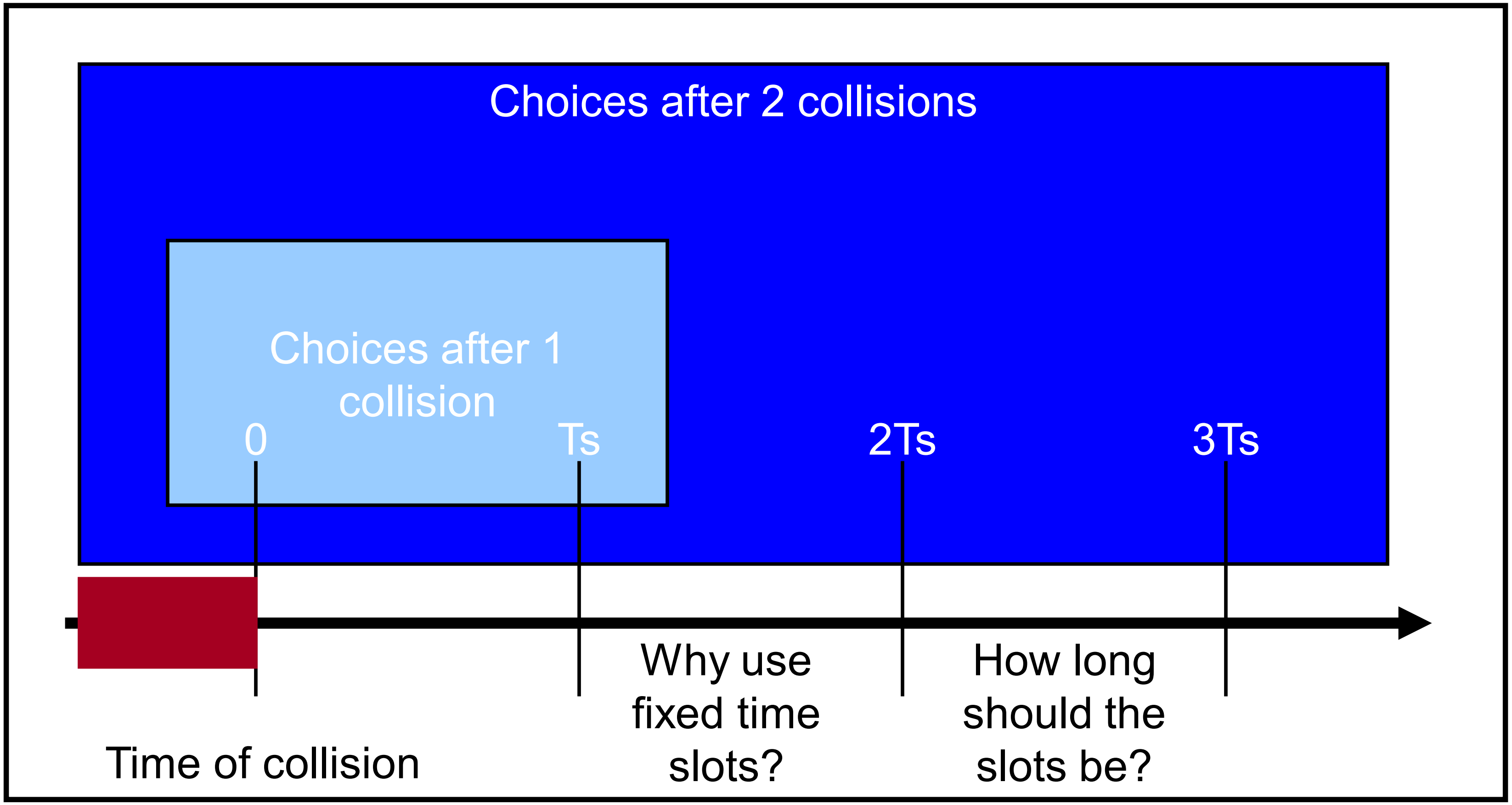
At time 2T, A is still transmitting and notices a collision

Retransmission

- How long should a host wait to retry after a collision?
  - Binary exponential backoff
    - Maximum backoff doubles with each failure
    - After N failures, pick an N-bit number
    - 2^N discrete possibilities from 0 to maximum



Binary Exponential Backoff



Binary Exponential Backoff

- For 802.3, T = 51.2 μs
- Consider the following
  - k hosts collide
  - Each picks a random number from 0 to $2^{(N-1)}$
  - If the minimum value is unique
    - All other hosts see a busy line
    - Note: Ethernet RTT < 51.2 μs
  - if the minimum value is not unique
    - Hosts with minimum value slot collide again!
    - Next slot is idle
    - Consider the next smallest backoff value

CSMA/CD efficiency

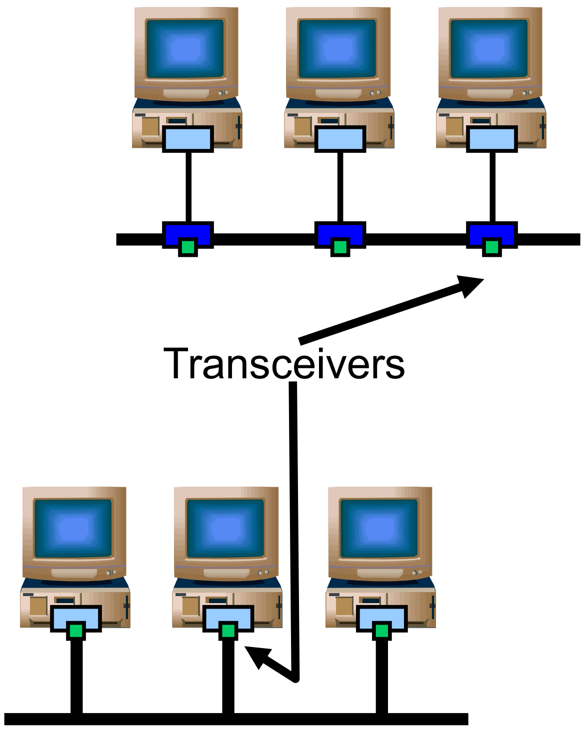
- t_{prop} = max prop between 2 nodes in LAN
- t_{trans} = time to transmit max-size frame
  - Efficiency = $1/(1+5 * t_{prop} / t_{trans})$
  - For 10 Mbit Ethernet, t_{prop} = 51.2 us, t_{trans} = 1.2 ms
  - Efficiency is 82.6%!
- Much better than ALOHA, but still decentralized, simple, and cheap
- Efficiency goes to 1 as t_{prop} goes to 0
- Goes to 1 as t_{trans} goes to infinity

Frame Reception

- Sender handles all access control
- Receiver simply pulls the frame from the network
- Ethernet controller/card
  - Sees all frames
  - Selectively passes frames to host processor
- Acceptable frames
  - Addressed to host
  - Addressed to broadcast
  - Addressed to multicast address to which host belongs
  - Anything (if in promiscuous mode)
    - Need this for packet sniffers/TCPDump

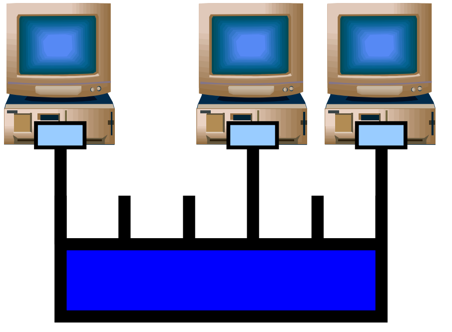
Collision Detection Techniques: Bus Topology

- Transceiver handles
  - Carrier detection
  - Collision detection
  - Jamming after collision
- Transceiver sees sum of voltages
  - Outgoing signal
  - Incoming signal
- Transceiver looks for
  - Voltages that are impossible for only outgoing



Collision Detection Techniques: Hub Topology

- Controller/Card handles
  - Carrier detection
- Hub handles
  - Collision detection
  - Jamming after collision
- Need to detect activity on all lines
  - If more than one line is active
    - Assert collision to all lines
    - Continue until no lines are active



10Mbps Ethernet Media

Name	Cable	Advantages	Max. Segment Length	Max Nodes on Segment
10Base5	Thick Coaxial (10mm)	Good for backbones	500m	100
10Base2	Thin Coaxial (5mm)	Cheapest system	200m	30
10BaseT	Twisted Pair (0.5mm)	Easy Maintenance	100m	1 (to hub)
10BaseFP	Fiber (0.1mm)	Best between buildings	500m	33
Extended segments may have up to 4 repeaters (total of 2.5km)				

100Mbps Ethernet Media

Name	Cable	Max. Segment Length	Advantages
100BaseT4	4 Twisted Pair	100m	Cat 3, 4 or 5 UTP
100BaseTX	Twisted Pair	100m	Full duplex on Cat 5 UTP
100BaseFX	Fiber Pair	100m	Full duplex, long runs
All hub based. Other types not allowed. Hubs can be shared or switched			

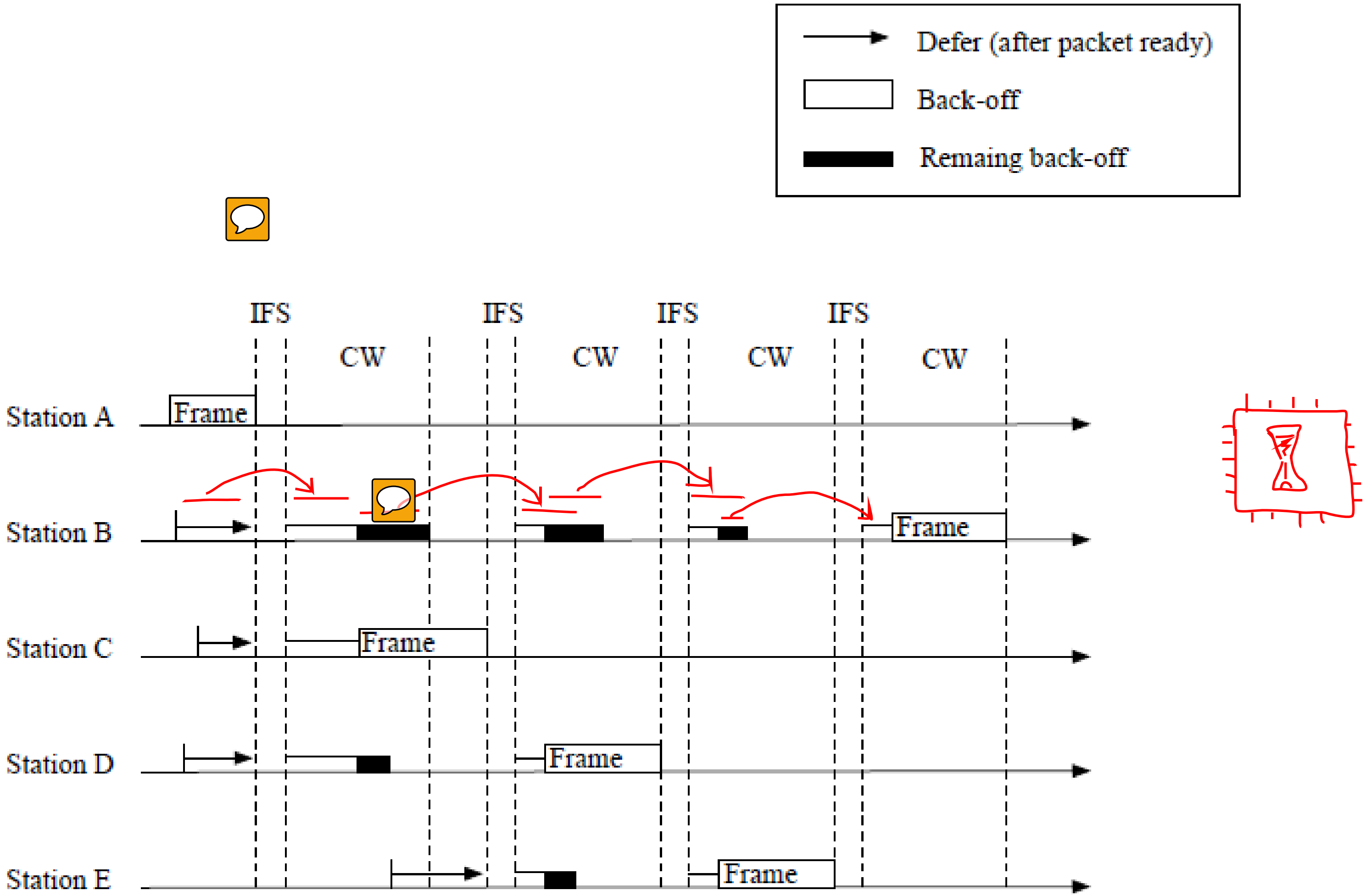
Ethernet in Practice

- Number of hosts
  - Limited to 200 in practice, standard allows 1024
- Range
  - Typically much shorter than 2.5km limit in standard
- Round Trip Time
  - Typically 5 or 10 μs, not 50
- Flow Control
  - Higher level flow control limits load (e.g. TCP)
- Topology
  - Star easier to administer than bus

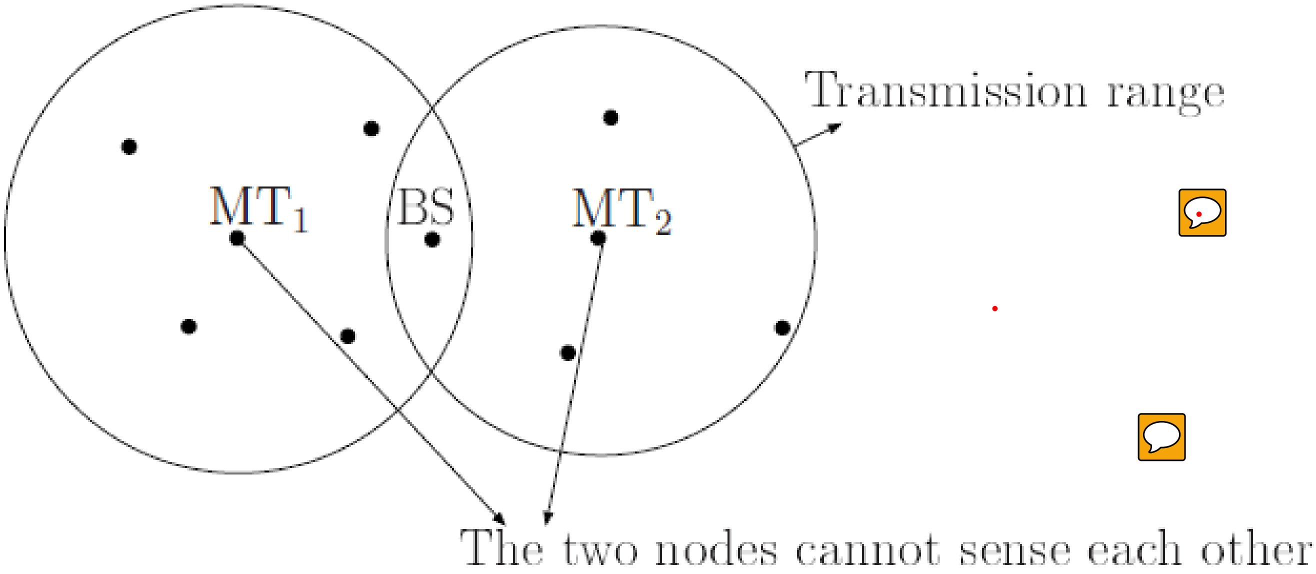
Outline

- A preliminary overview
- Propagation characteristics
- ISO-OSI Model
- Physical layer: modulation
- MAC layer:
  - Fixed resource assignment
  - Random access
    - Ethernet (CSMA/CD)
    - **WiFi (CSMA/CA)**
- Personal Area Networks
  - Bluetooth
  - Zigbee
- Cellular network dimensioning
- Cellular networks
  - From GSM (2G) to UMTS (3G)
  - LTE (4G)

CSMA/CA in IEEE 802.11 Networks



Hidden and Exposed Terminal Problems



- Busy Tone Multiple Access (BTMA): bandwidth is divided into a message channel (for data) and a busy-tone channel (for requests).
- Request-To-Send/Clear-To-Send (RTS/CTS): this couple of messages is handshaked between neighbor stations to detect on-going transmissions.

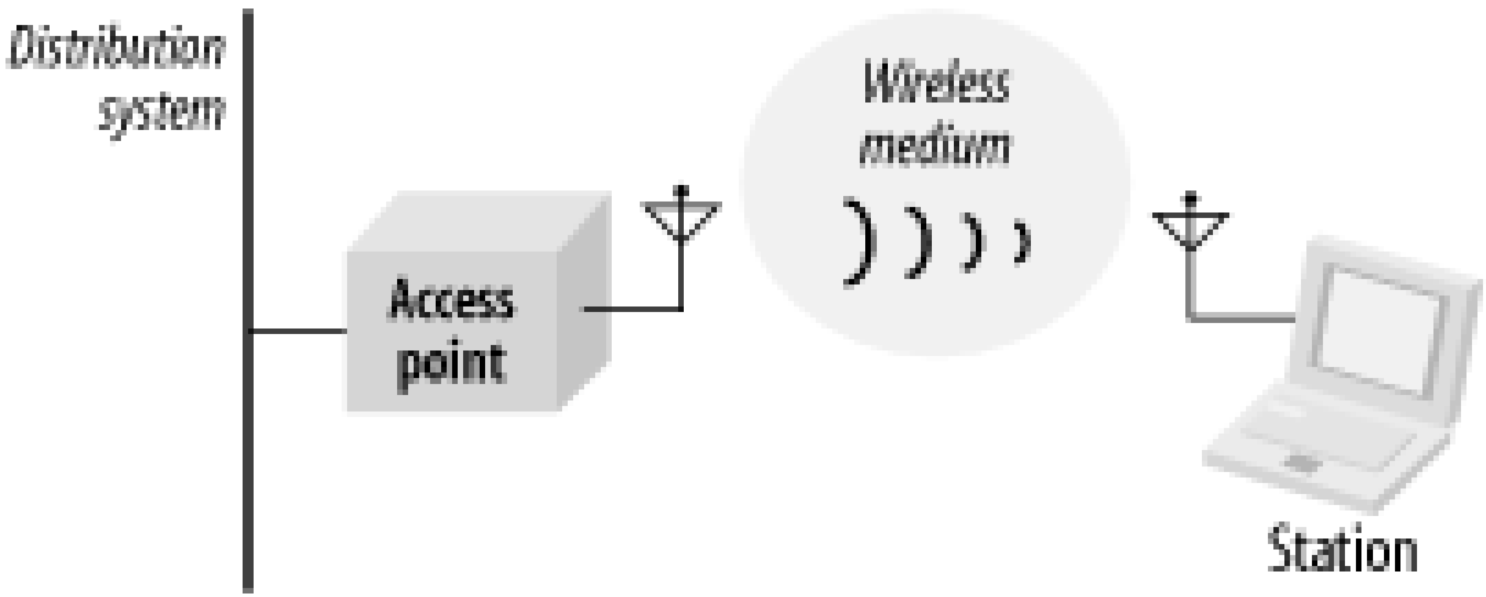
What is Wi-Fi?

- Short for ***wireless fidelity.***
- IEEE (Institute of Electrical and Electronics Engineers) established the 802.11 Group in 1990. Specifications for standard ratified in 1997.
- Initial speeds were 1 and 2 Mbps.
- IEEE modified the standard in 1999 to include:
  - 802.11b
  - 802.11a
  - 802.11g was added in 2003.
- IEEE Created standard, but Wi-Fi Alliance certifies products

Wi-Fi Alliance

- Non-profit standards organization.
- Global organization that created the Wi-Fi brand name.
- Formerly the Wireless Ethernet Compatibility Alliance.
- The Wi-Fi CERTIFIED logo from the Wi-Fi Alliance.
  - Rigorous interoperability testing requirements.
  - Certifies the interoperability of 802.11 products from the many different vendors.

Wireless LAN Networks

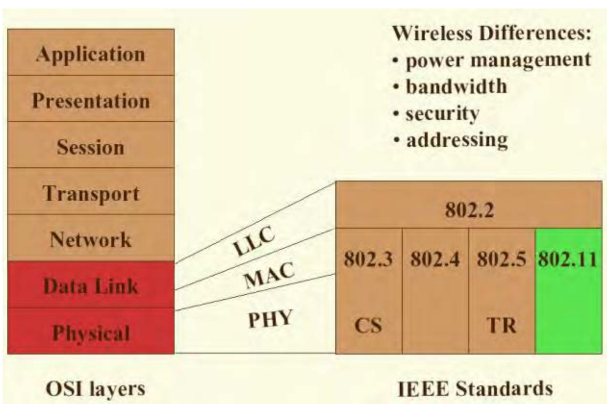


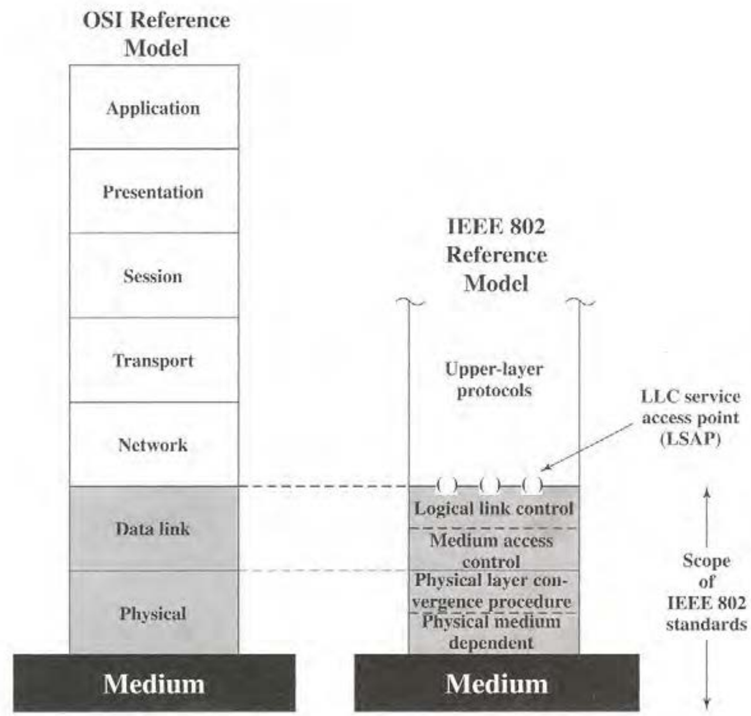
Advantages/Disadvantages

- Advantages
  - Freedom – You can work from any location that you can get a signal.
  - Setup Cost – No cabling required.
  - Flexibility – Quick and easy to setup in temp or permanent space.
  - Scaleable – Can be expanded with growth.
  - Mobile Access – Can access the network on the move.
- Disadvantages
  - Speed – Slower than cable.
  - Range – Affected by various medium.
  - Travels best through open space.
  - Reduced by walls, glass, water, etc
  - Security – Greater exposure to risks.
  - Unauthorized access.
  - Compromising data.
  - Denial of service.

802.11 Standard

- 802.11 is primarily concerned with the lower layers of the OSI model.
- Data Link Layer
  - Logical Link Control (LLC).
  - Medium Access Control (MAC).
- Physical Layer
  - Physical Layer Convergence Procedure (PLCP).
  - Physical Medium Dependent (PMD).





IEEE 802 Protocol Layers Compared to OSI Model

802.11 sub-standards (amendments)

- 802.11 MAC (Media Access Control) ratified 1999
- 802.11b PHY 2.4 GHz (max 11 Mbps) ratified 1999
- 802.11a PHY 5.0 GHz (max 54 Mbps) ratified 1999
- 802.11g PHY 2.0 GHz (max 54 Mbps) ratified 2003
- 802.11i Security draft number XXX
- 802.11e QoS, Multimedia draft number XXX
- 802.11h European regulations for 5GHz draft number XXX
- 802.11h Japan regulations for 5GHz draft number XXX

802.11b Standard

- Well-supported, stable, and cost effective, but runs in the **2.4 GHz range** that makes it prone to interference from other devices (microwave ovens, cordless phones, etc) and also has security disadvantages.

- Limits the number of **access points in range of each other** to **three**.

- Has 11 channels, with 3 non-overlapping, and supports rates from 1 to 11 Mbps, but realistically about **4-5 Mbps max**.

- Uses **direct-sequence spread-spectrum** technology.

802.11g Standard

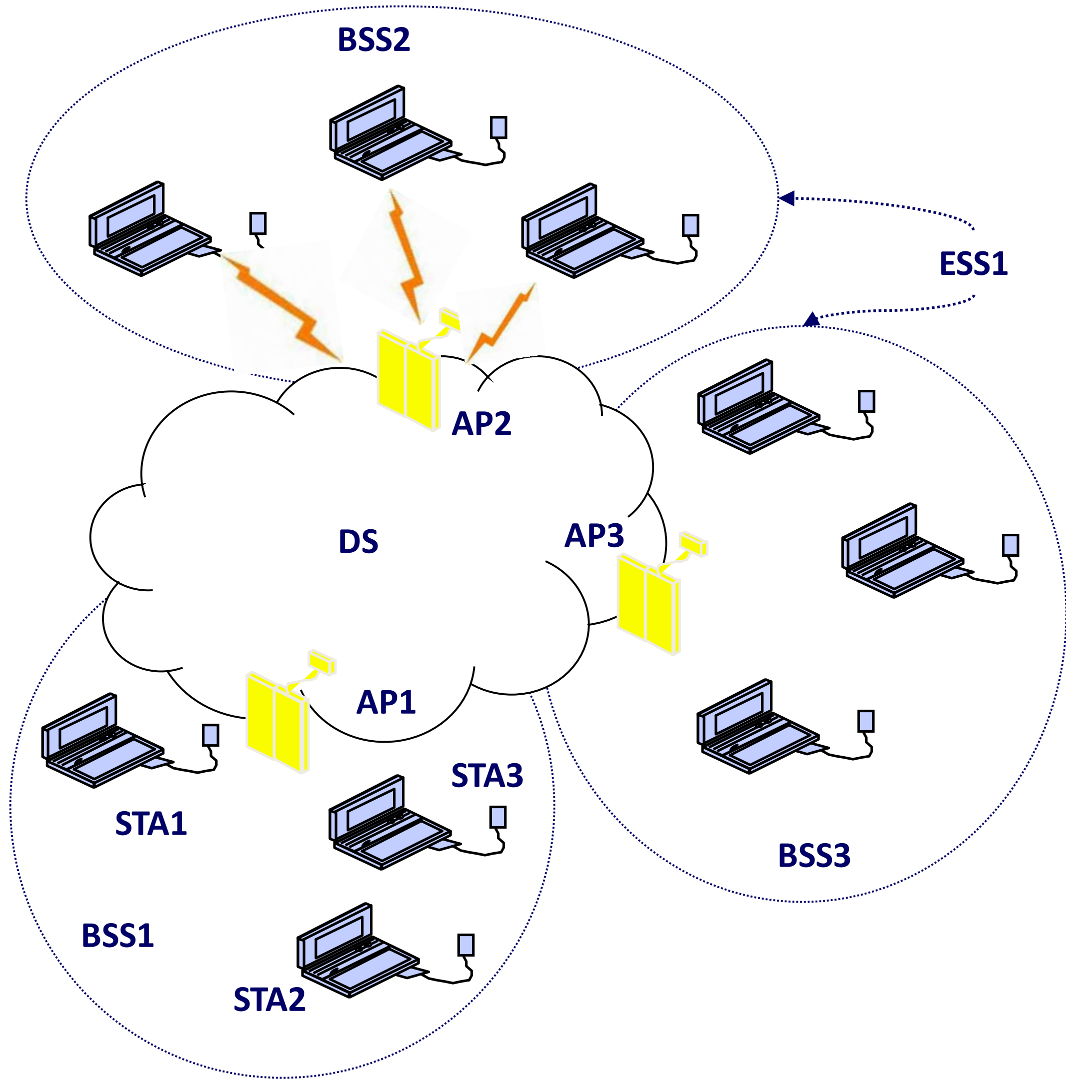
- Extension of 802.11b (still in **2.4 GHz band**), with the same disadvantages (security and interference).
- Has a **shorter range than 802.11b**.
- Is backwards compatible with 802.11b so it allows or a smooth transition from 11b to 11g.
- Flexible because multiple channels can be combined for faster throughput, but **limited to one access point**.
- Runs at 54 Mbps, but realistically about **20-25 Mbps** and about 14 Mbps when b associated
- Uses **frequency division multiplexing**

802.11a Standard

- Completely different from 11b and 11g.
- Flexible because **multiple channels can be combined** for higher throughput and **more access points can be co-located**.
- **Shorter range** than 11b and 11g.
- Runs in the **5 GHz range**, so **less interference** from other devices.
- Has **12 channels**, 8 non-overlapping, and supports rates from 6 to 54 Mbps, but realistically about **27 Mbps max**
- Uses **frequency division multiplexing**

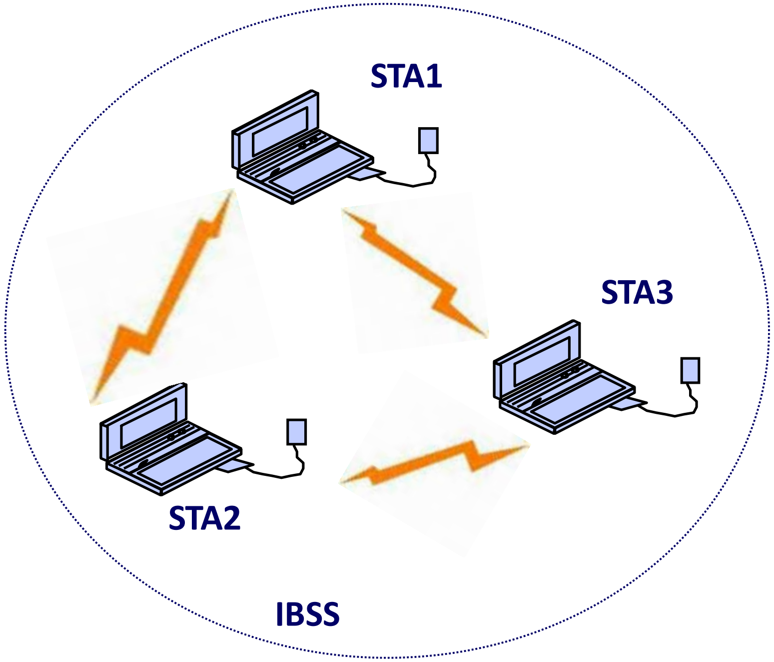
Infrastructure Mode (most common)

- Stations (STA)
  – any wireless device
- Access Point (AP)
  – connects BSS to DS
  – controls access by STA's
- Basic Service Set (BSS)
  – a region controlled by an AP
  – mobility is supported within a single BSS
- Extended Service Set (ESS)
  – a set of BSS's forming a virtual BSS
  – mobility is supported between BSS's in an ESS
- Distribution Service (DS)
  – connection between BSS's



Ad-hoc Mode

- Stations (STA)
  - any wireless device
  - act as distributed AP
- Independent Basic Service Set (IBSS)
  - BSS forming a self contained network
  - no AP and no connection to the DS



Security

- **WEP** (wired equivalent privacy) 64/128 bits

  Using RC4 algorithm, almost permanent key, very week security, able to crack by collecting statistic

  ~~Current security level for 99.9% products on the market.~~ NOoo

- **TKIP** (temporal key integrity protocol)

  Used RC4 algorithm with with a 128-bit "temporal key"

  but changes temporal keys every 10,000 packets and key dependes on address and sequence number.

  Will be required to obtain WiFi certification from 09/01/03

- **AES** (Advanced Encryption Standard)

  New, much more stronger encryption, protect against hacker frames in insertion. Need hardware accelerator. Optional feature.