Chapter 5: Link Layer and LAN

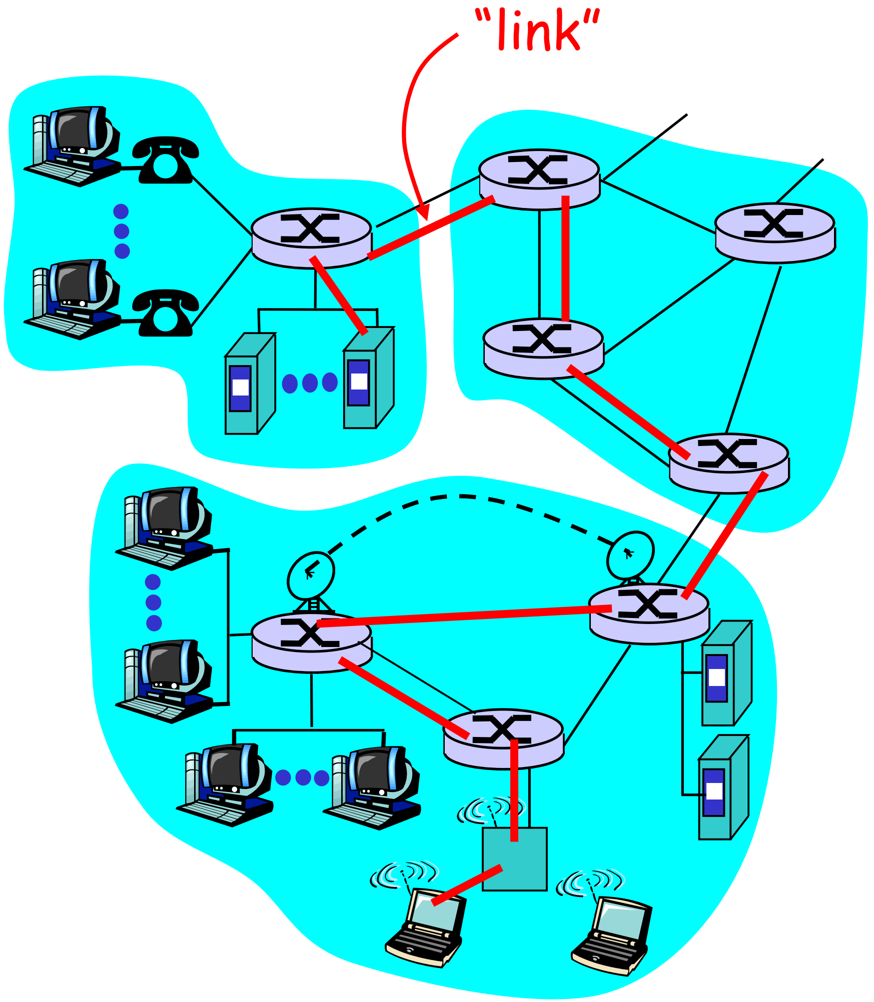
Part_1: MAC Protocol

Instructor: HOU, Fen

2025

The Link Layer

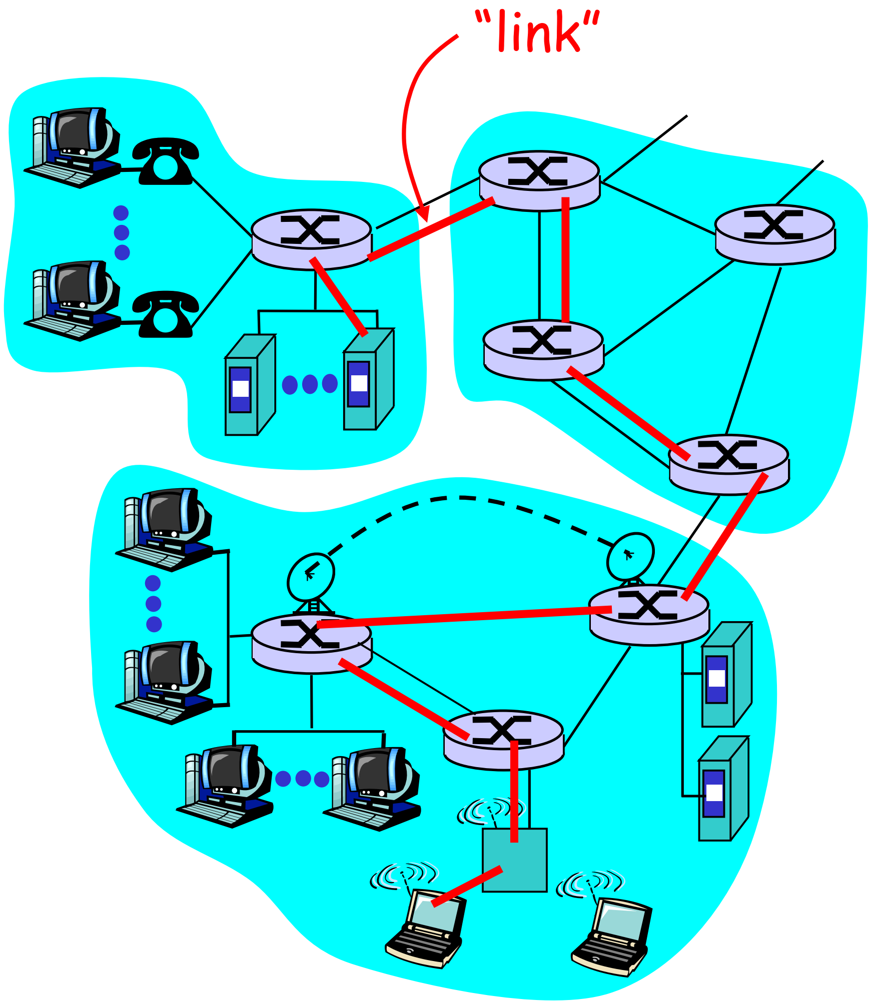
- Network layer provides logical communication between two hosts.
- The communication path between two hosts consists of multiple individual links.
- Link layer is responsible for transferring network layer datagrams from one node to adjacent node over a link.



Link Layer Service

Some terminologies:

- Nodes: hosts and routers are **nodes**
- Links: communication channels that connect adjacent nodes along communication path are **links**
  - wired links
  - wireless links
- Frames: Link-layer packet is called as **frame**. It is the unit of data exchanged by a link-layer protocol. Each link layer frame typically encapsulates a network layer datagram.



How are frames sent across the individual links?

Our Goals

- understand the principles behind data link layer services:
  - sharing a broadcast channel: multiple access
  - link layer addressing
  - error detection, correction
- Description and implementation of various link layer technologies

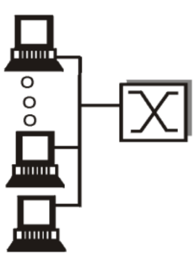
Sharing a Broadcast Channel: Multiple Access

Multiple Access Links and Protocols

Two types of "links/channels/media":

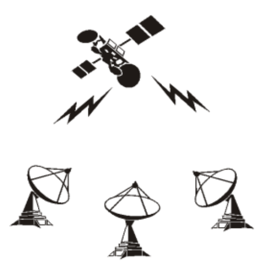
- point-to-point link
  - A single node at one end of the link and a single node at other end of the link.
- broadcast (shared wire or medium) link
  - Multiple nodes share a same, single link (wireless link or wireless link).
  - Examples
    - Ethernet
    - 802.11 wireless LAN

Multiple access problem: how to coordinate the access of multiple nodes to a broadcast link.



shared wire
(e.g. Ethernet)

shared wireless
(e.g. Wavelan)



satellite

cocktail party

Multiple Access Control (MAC) Protocols

- A human analogy: A classroom
  - Teacher(s) and student(s) share the same, single, broadcast channel
- The problem: who gets to talk? i.e., how to arrange the usage of the broadcast channel.
  - Collision occurs if multiple persons talk at the same time. Nobody can hear clearly.
- A mechanism or protocol is needed to control(or to organize or to schedule) the usage of broadcast channel among multiple persons------ Multiple Access Control (MAC) protocol
- Basic principles for sharing the broadcast channel
  - Raise your hand if you have a question
  - Don't interrupt when someone is speaking
  - Pay attention when someone else is talking
  - Given everyone a chance to speak

Multiple Access Control Protocol

- MAC protocol: it is designed to coordinate the transmission from different nodes in order to minimize/avoid collision.
- MAC protocol is to solve
  - WHO is going to use the link?
  - WHEN the link is going to be used?
  - HOW long the link is used?
- Goal: efficient, fair, simple, decentralized
  - Efficient and fair
    - When one node wants to transmit, it can send at rate R, where R is the rate of broadcast link.
    - When N nodes want to transmit, each can send at average rate R/N
  - Simple
    - Simple and easy to implement
  - decentralized
    - no special node to coordinate transmissions
    - no synchronization among all nodes (in terms of clocks, slots)

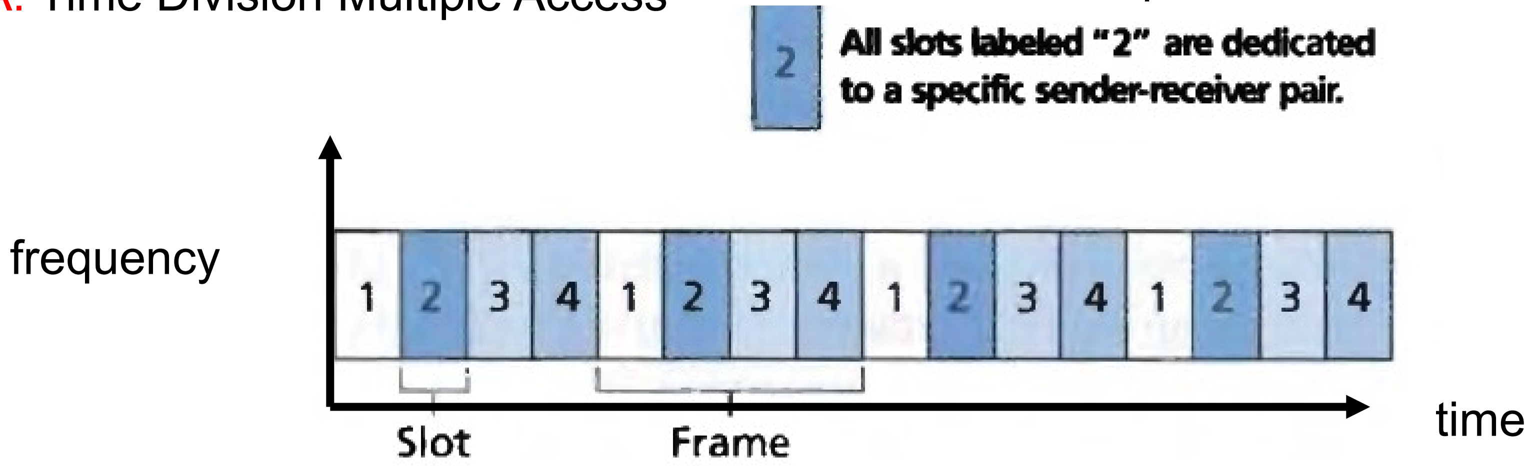
Multiple Access Control (MAC)Protoco

- Three categories of MAC protocols
  - Channel Partitioning protocols
    - divide link into smaller "pieces" (TDMA (Time Division Multiple Access) , FDMA, etc.) – TDM, and FDM are introduced in chapter 1
    - allocate piece to each node for the exclusive use
  - Random Access protocols
    - don't divide this link. A transmitting node always transmits at the full rate of the link;
    - exist collisions
    - "recover" from collisions
  - "Taking turns" protocols
    - Nodes take turns to access the link.
    - No collision, but each node may take a long time to wait for its turn when there are many nodes.

Channel Partitioning Protocols: TDMA (Time Division Multiple Access)

TDMA: Time Division Multiple Access

Example: 4 nodes



- Main principles of TDMA
  - Time is divided into time frames and each frame is further divided into N time slots.
  - Each time slot is assigned to one of the N nodes.
  - Whenever a node has a packet to send, it transmits the packets during its assigned time slots at the rate of this link.
  - Different nodes are separated in the time domain

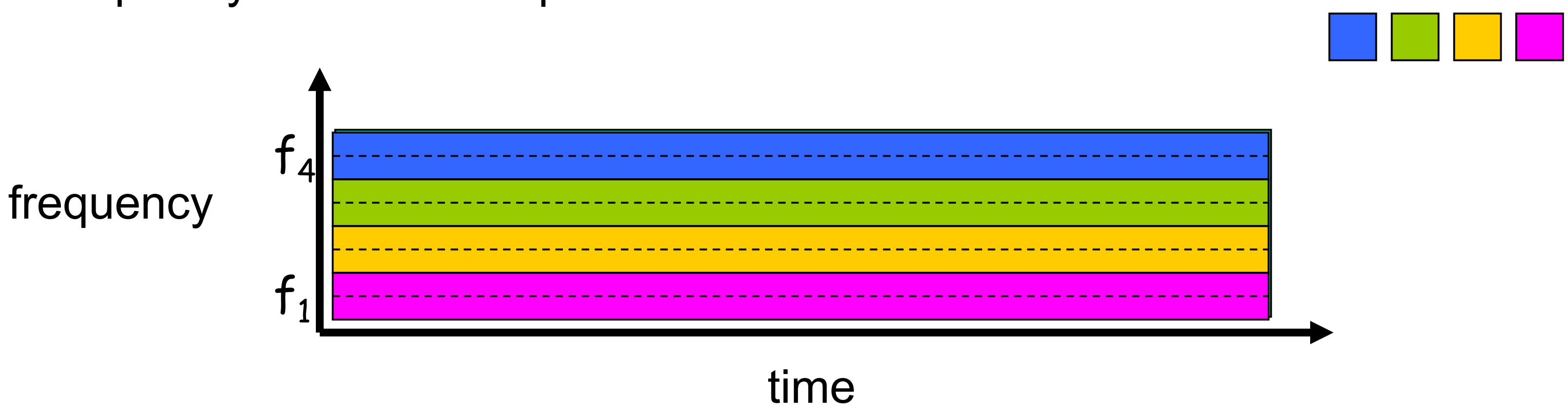
Channel Partitioning Protocols: TDMA (Time Division Multiple Access)

- Advantages
  - Simple
  - Eliminate collision
  - Provide fair allocation
- Drawbacks
  - Limit the average rate to R/N
  - Resource waste due to the inactive nodes

Channel Partitioning Protocols: FDMA (Frequency Division Multiple Access)

FDMA: Frequency Division Multiple Access

Example: 4 nodes



- Main principles of FDMA
  - Frequency band is divided into different parts, and each has a bandwidth of R/N.
  - Each frequency part is assigned to one of the N nodes.
  - Each user transmits with no limitation in time, but using only a portion of the whole available bandwidth.
  - Different users are separated in the frequency domain.

Channel Partitioning Protocols: FDMA (Frequency Division Multiple Access)

- Advantages
  - Simple
  - Eliminate collision
  - Provide fair allocation
- Drawbacks
  - Limit the average rate to R/N
  - Resource waste due to the inactive nodes

Random Access Protocols

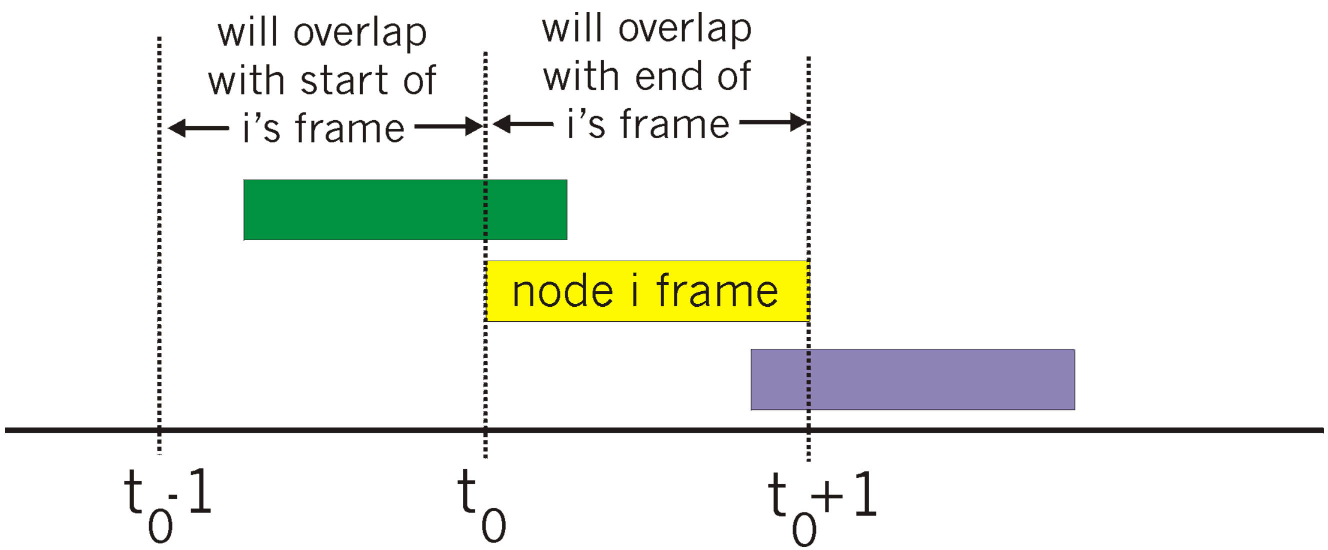
- Main principles of random access protocols
  - When node has packet to send, it transmits **at random** (i.e., no a priori coordination among nodes) and **at full link data rate R.**
- When there are two or more transmitting nodes ➜ "collision",
- Random Access MAC protocol specifies:
  - how to detect collisions
  - how to recover from collisions (e.g., via delayed retransmissions)
- Examples of random access MAC protocols:
  - Pure ALOHA
  - Slotted ALOHA
  - CSMA, CSMA/CD, CSMA/CA

ALOHA

- In 1970's, Norman Abramson and his colleagues at the University of Hawaii devised a new and elegant method to solve the channel allocation problem and this method is known as ALOHA SYSTEM.
- The basic idea is applicable to any system in which uncoordinated users are competing for the use of a single shared link.
- There are two versions of Aloha system which differ with respect to whether or not time is divided up into discrete slots into which all frames must fit.
  - Pure ALOHA
  - Slotted ALOHA

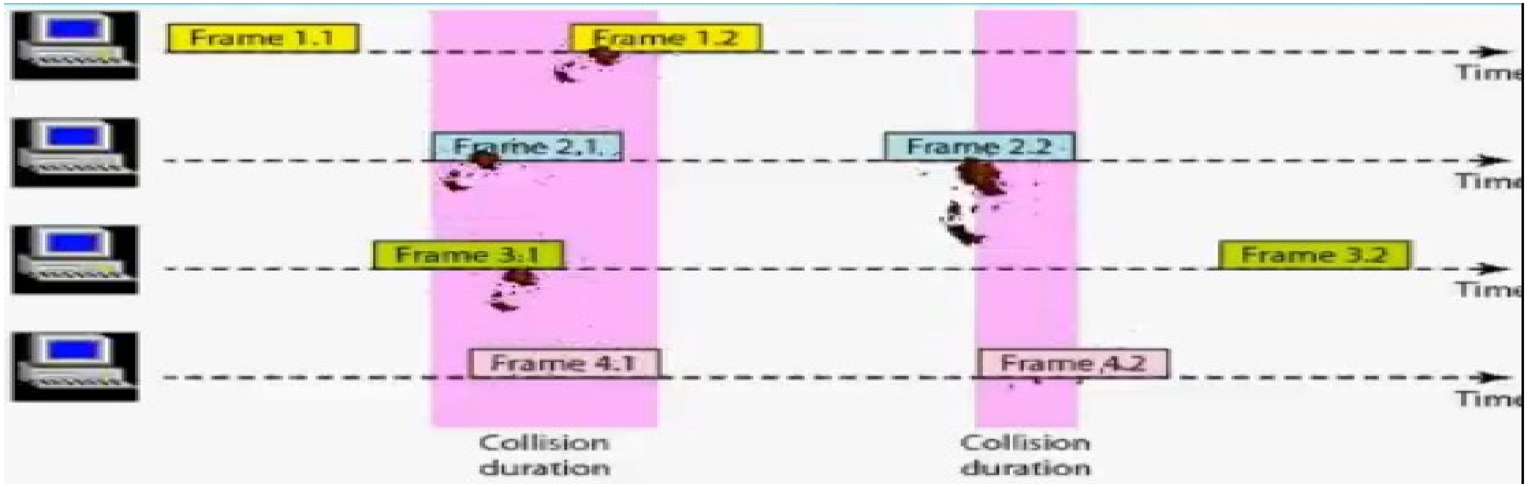
Pure ALOHA

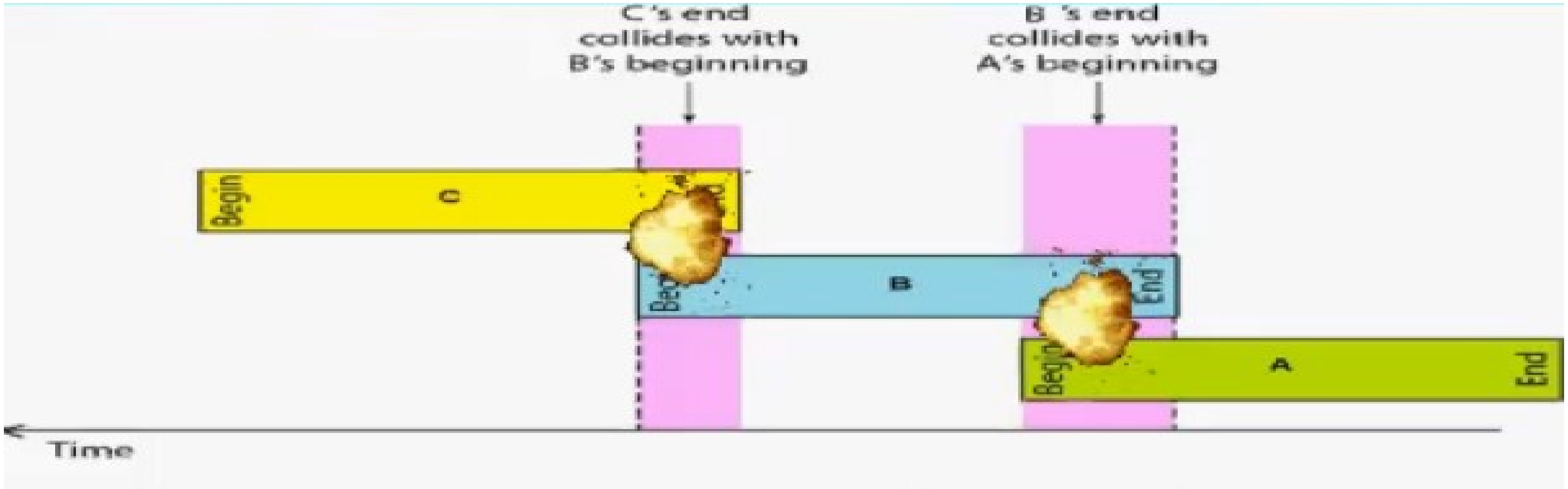
- Let nodes transmit whenever they have data to be sent
- No synchronization among nodes
  - If collision, retransmit after a random delay
- collision probability increases:
  - frame sent at t_0 collides with other frames sent in $[t_0-1, t_0+1]$



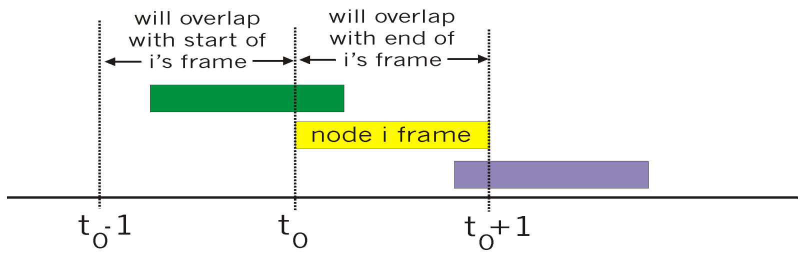
Pure ALOHA

- Collision in pure Aloha





Efficiency of Pure Aloha



P(success by a given node) = P(the node transmits) ·

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

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

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

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

Since there are N nodes, the probability that an arbitrary node has a successful transmission is $NP(1-p)^{2(N-1)}$

choosing optimum $p^*=1/(2N-1)$, let $E=NP^*(1-p^*)^{2(N-1)} = N/(2N-1)*(1-1/(2N-1))^{2(N-1)}$

N	1	2	5	10	20	100
E	1	0.296	0.216	0.199	0.191	0.185

In 1987, Robert publish a method called Slotted Aloha which doubled the efficiency of Pure Aloha

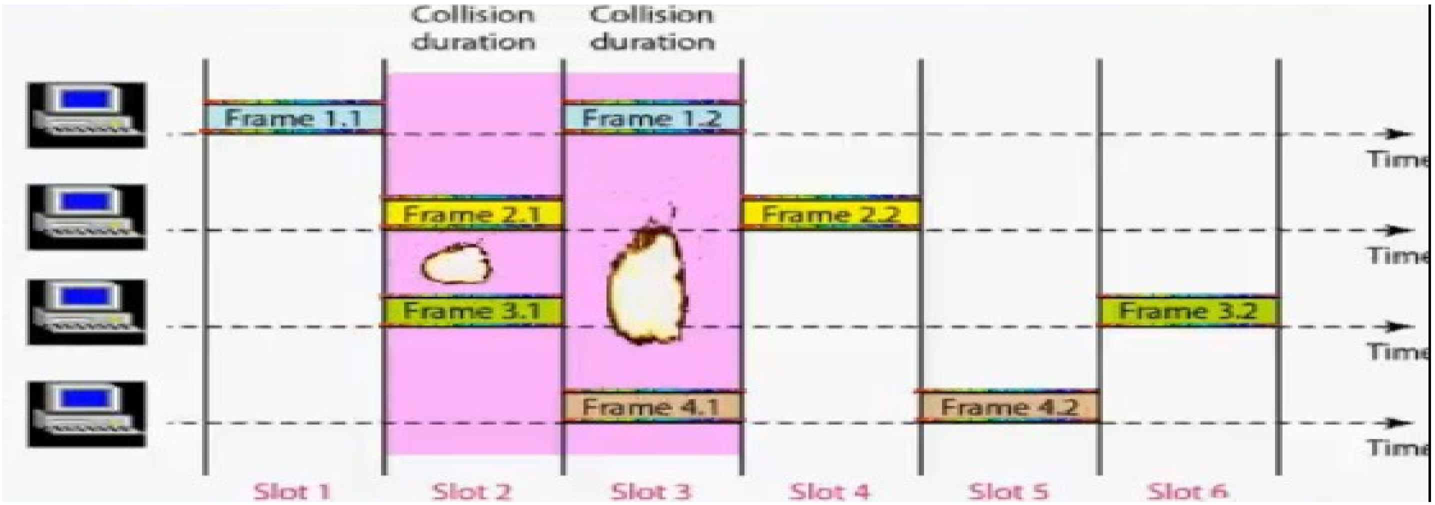
Slotted ALOHA

- In 1987, Robert published a method called slotted aloha which doubled the efficiency of pure aloha
- Main principles of slotted Aloha
  - All frames consist of exactly fixed-size bits (e.g., L bits)
  - Slotted Aloha divides time into equal size time slots, each time slot equals the time to transmit one frame.
  - The nodes start to transmit data at the beginning of each time slots only.
  - When a node has a new frame, it waits until the beginning of the next slot and **transmits the entire frame in the slot.**
  - If there is no collision, the node has successfully transmitted this frame. Then the node can prepare a new frame for transmission if it has one.
  - If 2 or more nodes transmit in this slot, a collision occurs. All nodes detect the collision before the end of the slot. In this case, each transmitting node retransmits its frame in each subsequent slot **with probability *p*** until success

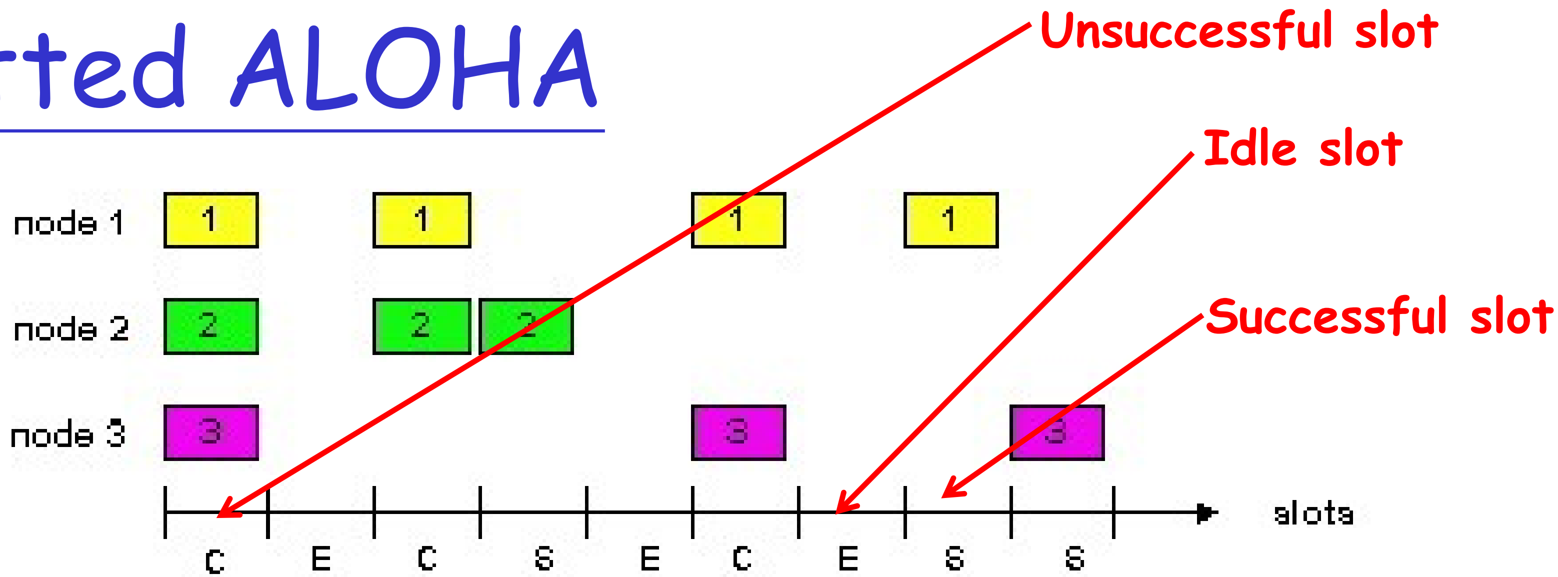
Slotted ALOHA

Synchronization in slotted Aloha

- Nodes are synchronized so that each node knows when the slots begin.
- When a node has a new frame, it waits until the beginning of the next slot and **transmits the entire frame in the slot.**
- If frames collide they will **overlap completely instead of partially.**
- The time that nodes take to detect a collision may be less than that used to transmit a frame.



Slotted ALOHA



Pr(a slot is occupied by the success transmission of the node 2) = Pr(node 2 transmits) · Pr(no other node transmits in this time slot)

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

The efficiency of Slotted ALOHA: The probability that an arbitrary slot is used for a successful transmission is $NP(1-p)^{(N-1)}$

choosing optimum $p^*=1/N$, let $E=NP^*(1-p^*)^{(N-1)}=(1-1/N)^{(N-1)}$

N	1	2	5	10	20	100
E	1	0.5	0.41	0.387	0.377	0.370

Exercise

Consider the following multiple access scheme that combines TDMA and slotted ALOHA. There are 30 users, separated into two groups, one of 4 users and the other of 26 users. Even time slots (i.e., 0, 2, 4, ...) are reserved for the 4-user group. Odd time slots (i.e., 1, 3, 5, ...) are reserved for the 26-user group. Contention within each group is resolved by the slotted ALOHA protocol (e.g., when a user in the 26-user group wants to send, it waits for an odd slot and then transmits with a probability p).

Question: Please derive the successful transmission rate (in packets/slot) of the system, assuming that every user always has data to send and in each group the users use the optimal probability. (Note that your answer can be in terms of fractions)

Solution:

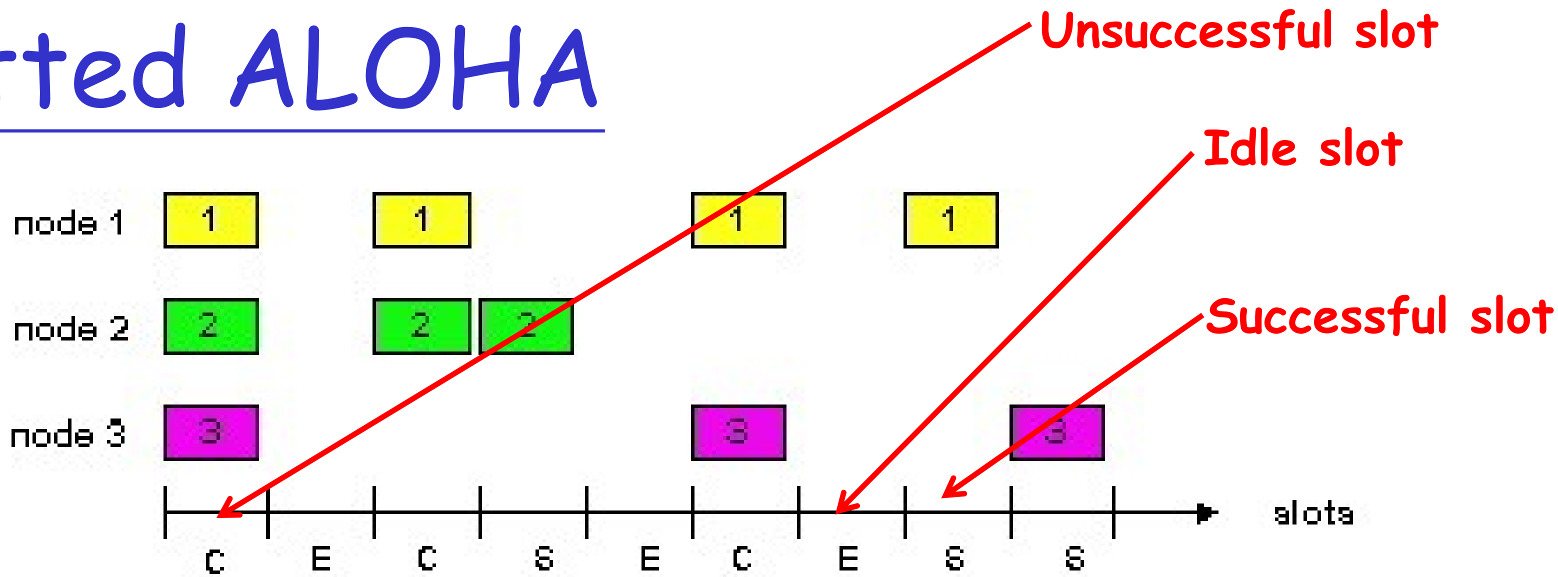
For slotted-ALOHA of N nodes, the throughput is $Np[(1-p)^{N-1}]$, where p is the transmission probability. The optimal p is $1/N$, resulting in throughput of $(1-p)^{N-1}$.

The 4-user group and even slots form a 4-node slotted-ALOHA system. Thus its max throughput is achieved when $p = 1/4$, and equals $1-(1/4))^3$, which equals $(3/4)^3$, which equals $27/64$.

The 26-user group and odd slots form a 26-node slotted-ALOHA system. Thus its max throughput is achieved when $p = (1/26)$, and equals $(1-(1/26))^{25}$,

Thus the overall throughput is $(1/2)[(27/64) + (1-(1/26))^{25}$

Slotted ALOHA



Advnantages

- simple
- highly decentralized:
  - nodes detect collision independently.
  - Node decides when to retransmit independently.
- single active node can continuously transmit at full rate of link

Disadvantages

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

Carrier Sense Multiple Access (CSMA)

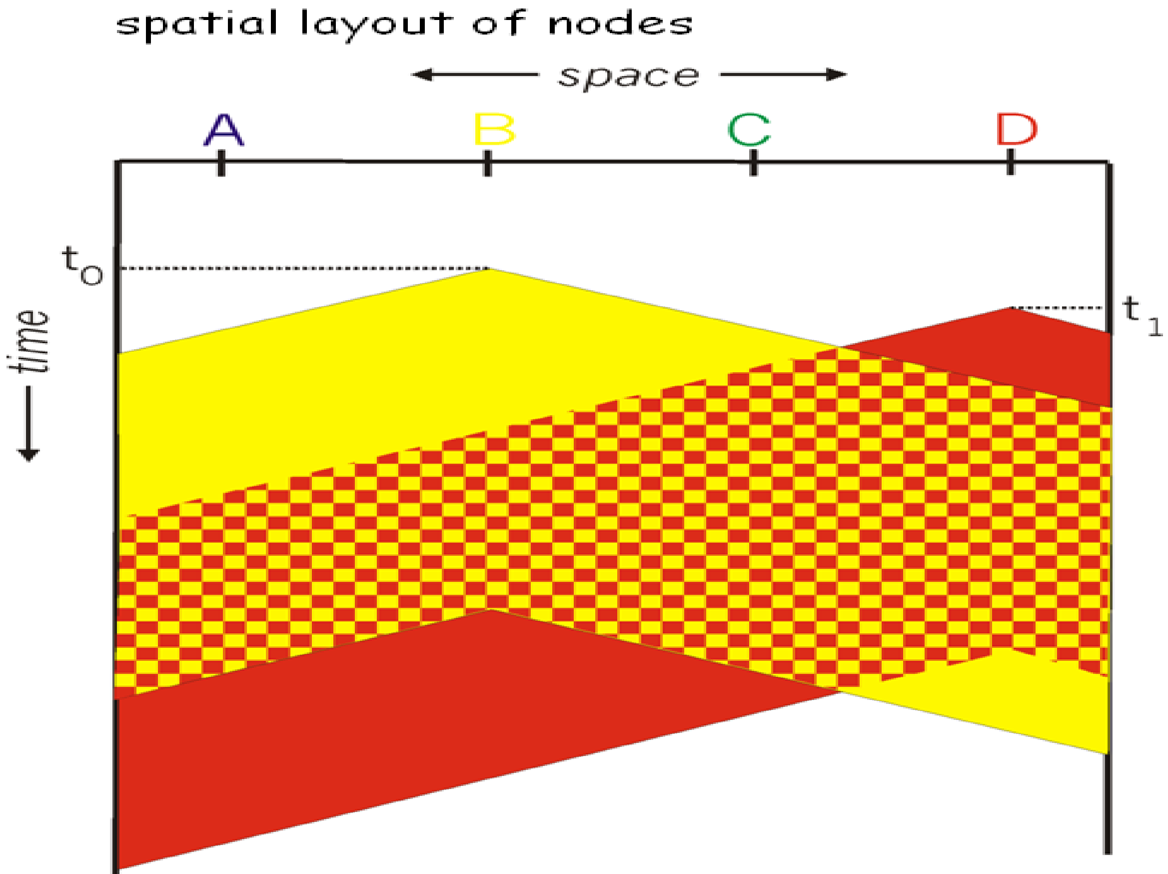
- Slotted Aloha: when a node has a new frame, it waits until the beginning of the next slot and transmits the entire frame in the slot.
- In slotted Aloha, a node's decision about the transmission is made independently of the activity of the other nodes
  - A node neither pays attention to whether another node happens to do transmission when it starts to transmit, nor stops transmission if another node begins to interfere with its transmission.-----→leads to a large amount of collision time
- In order to reduce the amount of collision time, we introduce CSMA and CSMA/CD:
  - Listen before speaking ----**Carrier sensing**
  - If someone else begins talking at the same time, stop talking----- **Collision detection**

Carrier Sense Multiple Access (CSMA)

- CSMA: listen before doing transmission. If channel is sensed busy, the ready node defers transmission; do transmission only if channel is sensed to be idle.

- Collisions still exist or Not?
  - Yes. Collisions still exist
    - Two or more nodes may sense the channel idle at the same time
    - Two or more nodes may not be aware of other transmission even after the channel is sensed idle due to signal propagation delay

The effect of propagation delay on CSMA



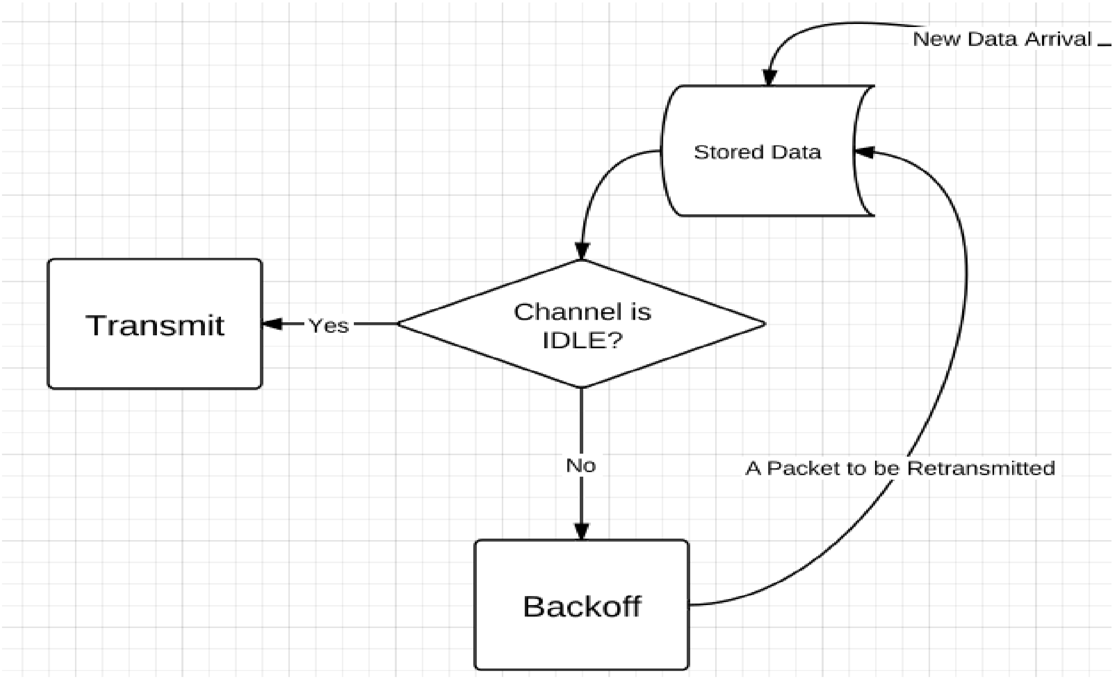
The effect of propagation delay on CSMA

- For effective carrier sensing, the propagation delay plays a crucial role in determining the performance. The longer the propagation delay, the larger the chance of the collision. Therefore, the propagation delay should be small.

- For example, Satellite system: long propagation delay (i.e., 270 msec) . In this case, taking 270 msec to sense the channel is a really long time. Carrier sense makes no sense.

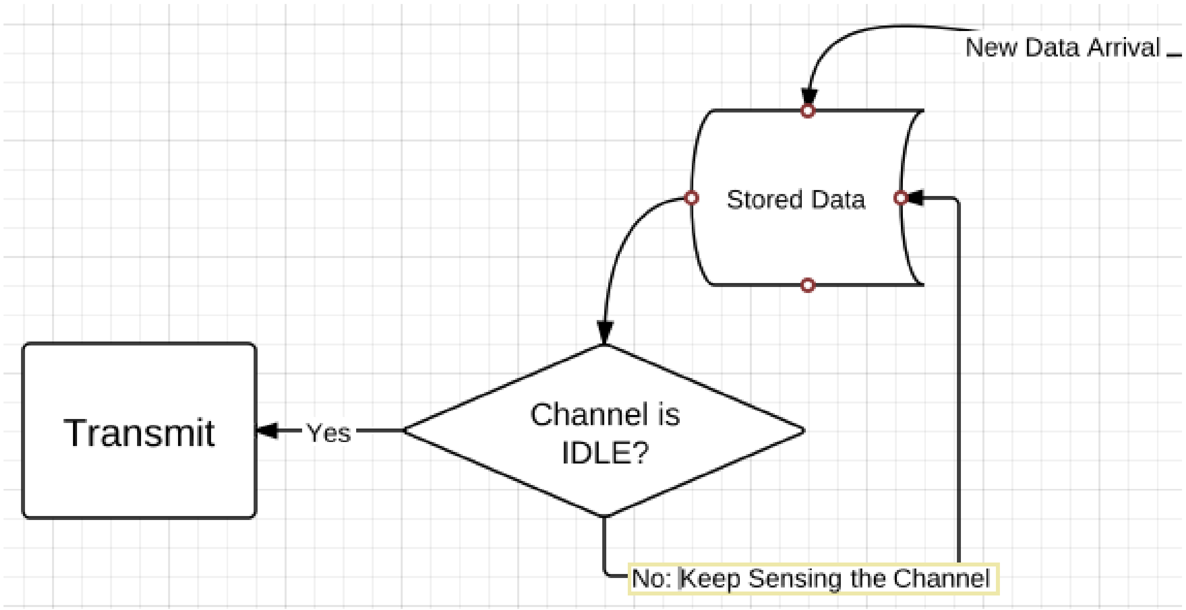
Carrier Sense Multiple Access (CSMA)

- Non persistent CSMA:
  - If channel is sensed idle then transmit packet
  - If channel is busy, use backoff algorithm to delay transmission, i.e. retry after random time.



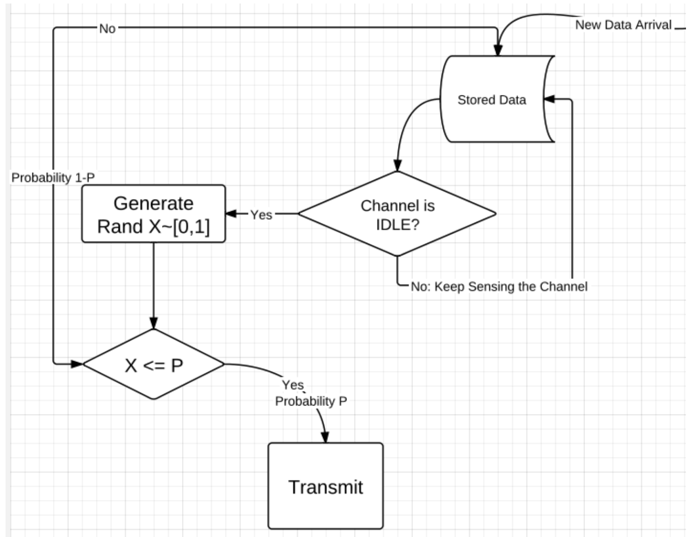
Carrier Sense Multiple Access (CSMA)

- 1-Persistent CSMA
  - If channel is sensed idle then transmit packet
  - If the channel is busy, a ready node will keep sensing until the channel becomes idle. The node starts to transmit immediately when channel becomes idle. That is, with probability 1.



Carrier Sense Multiple Access (CSMA)

- p-persistent CSMA
  - If channel is sensed idle then transmit packet
  - If the channel is busy, a ready node will persist in sensing until the channel becomes idle. As soon as the channel becomes idle, with probability p, the node starts to transmit, or with probability (1-p), the node waits for a predefined time period before sensing the channel again. Then, the same process is repeated.



CSMA/CD (Collision Detection)

- **Collision Detection(CD):** A transmitting node listens to the channel while it is transmitting. If it detects that another node is transmitting at the same time, it stops transmitting and uses some protocol to determine when it should do next attempt to transmit.

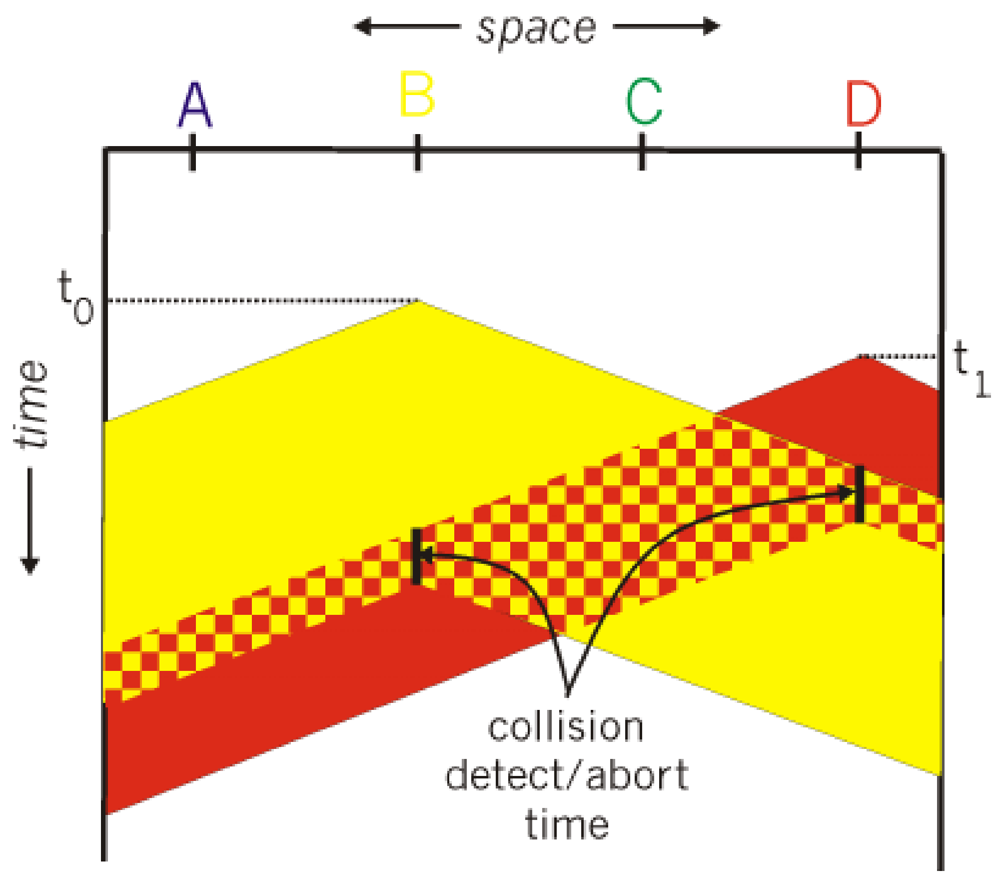
CSMA/CD (Collision Detection)

- Sense the channel before transmission
  - If idle, transmit immediately
  - If busy, wait or keep sensing until the channel becomes idle
- Collision detection: Listen while transmitting
  - Abort a transmission immediately if a collision is detected.
  - Try again later after waiting a random time.

CSMA/CD (Collision Detection)

- Sense the channel
  - Reduce the number of collision
- Collision detection
  - Why is collection detection necessary?
    - Reduce the impacts of collisions, making the channel ready to use sooner
    - Stopping the damaged frame at early time is to reduce the channel wastage
  - How?
    - The sender detects the collision by measuring signal strengths, compare transmitted, received signals
    - Collisions are detected within short time

CSMA/CD (Collision Detection)



CSMA/CD (Collision Detection)

- To ensure that the sender knows that a packet is transmitted without a collision, the sender must be able to detect a collision before it finishes transmission.

- The minimum frame size L should satisfy the following condition:

  Transmission time >= Round-trip prorogation time

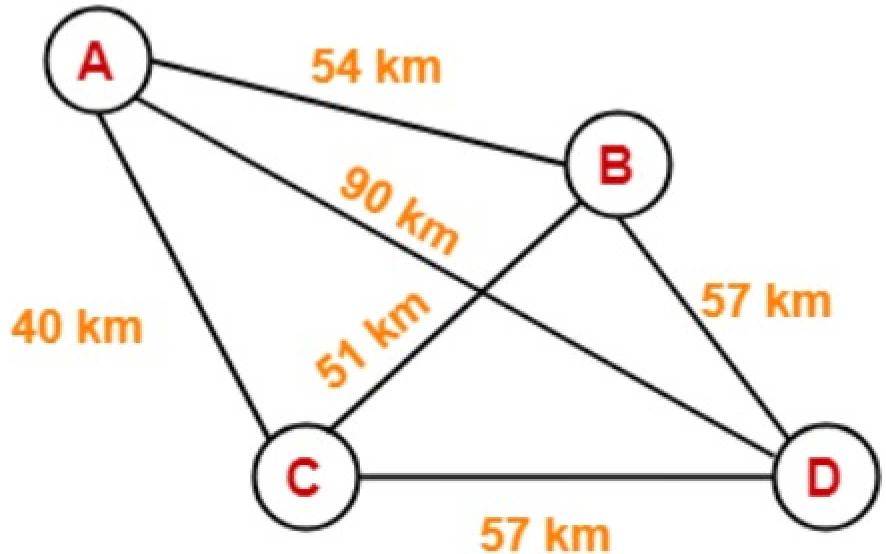
- Example: In a CSMA / CD network running at 1 Gbps over 1 km cable with no repeaters, the signal speed over the cable is $2 * 10^5$ km/sec. Please calculate the minimum frame size.
  - Minimum frame size is 10000 bits

CSMA/CD (Collision Detection)

- Example: A 2 km long broadcast LAN has 10^7bps transmission rate and uses CSMA / CD. The signal travels along the wire at 2×10^8 m/sec. What is the minimum packet size that can be used on this network?
  - A. 50 bits
  - B. 100 bits
  - C. 200 bits
  - D. None of the above
- Answer: C

CSMA/CD (Collision Detection)

- Example: The network consists of 4 hosts distributed as shown below. Assume this network uses CSMA / CD and signal travels with a speed of 3 x 10^5 km/sec. If sender sends at 1 Mbps, please calculate the minimum size of the frame.
  - A. 600 bits
  - B. 400 bits
  - C. 6000 bits
  - D. 1500 bits
- Answer: A



Two Desirable Properties of MAC protocols

- **Full rate**: when only one node is active, it can have the full rate of the link.
- **Fairness and efficiency**: when M nodes are active, each active node has a throughput of nearly R/M.

TDMA/FDMA MAC protocols----have the second property
- share channel efficiently and fairly at high load
- inefficient at low load: delay in channel access, 1/N bandwidth allocated even if only 1 active node!

Random access MAC protocols—have the first property
- efficient at low traffic load: single node can fully utilize channe
- high load: collision overhead

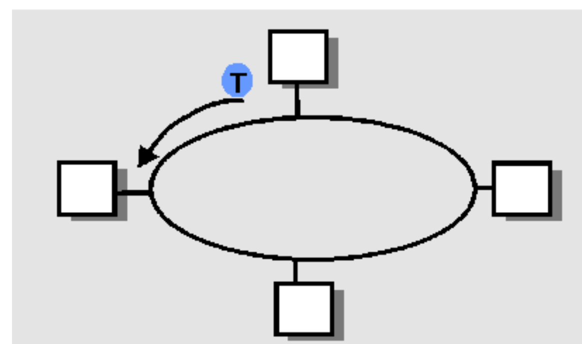
"Taking turns" protocols---have both properties
- Look for best of both aspects
- MAC protocols achieve both fairness and full rate, at the expense of some extra overhead

Two Kinds of "Taking Turns" MAC Protocols

- Polling protocol
  - A node is designated as a master node.
  - Master node polls each of nodes in a round-robin fashion and to "invites" them to transmit in turn.
- Advantages
  - Eliminate the collision and empty slots
- Drawbacks:
  - single point of failure (master node)
  - polling overhead
  - latency

Two Kinds of “Taking Turns” MAC Protocols

- Token passing protocol
  - Token: it is a small, special-purpose frame.
  - Token is exchanged among nodes in a fixed order.
  - When a node receives the token, the node immediately forwards the token to the next node if it has no frames to send; otherwise, it holds the token and send frames at the full rate of link for a period of time, then passes the token to the next node.
  - control token passed from one node to next sequentially.
- Advantages
  - Decentralized and highly efficient.
  - Eliminate the collision and empty slots
- Disadvantages:
  - single point of failure (token)
  - token overhead
  - latency



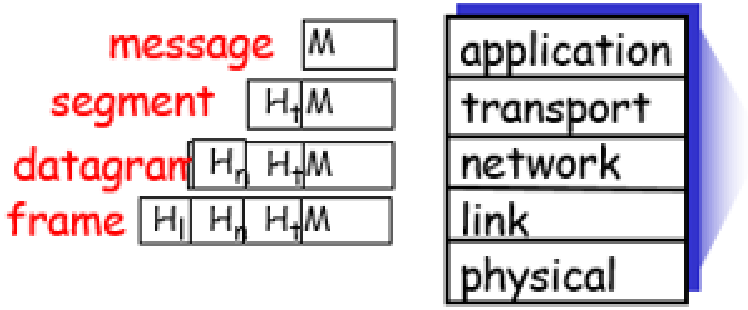
MAC protocols

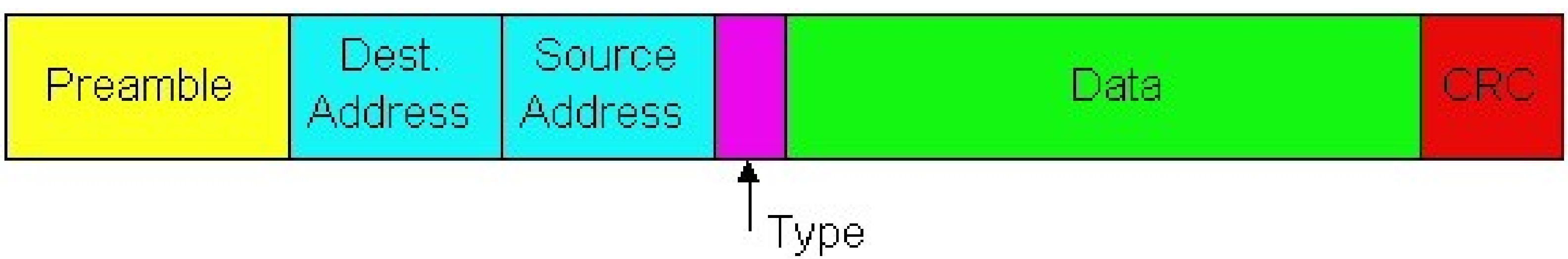
- MAC protocol: mechanism to control the access of multiple nodes to shared media.
  - Contention-free:
    - Channel Partitioning: TDMA, FDMA, CDMA
    - Taking-turns: polling protocol, token passing
  - Contention-based
    - Pure-ALOHA, S-ALOHA, CSMA, CSMA/CD

Ethernet Frame Structure and MAC Address

Ethernet Frame Structure

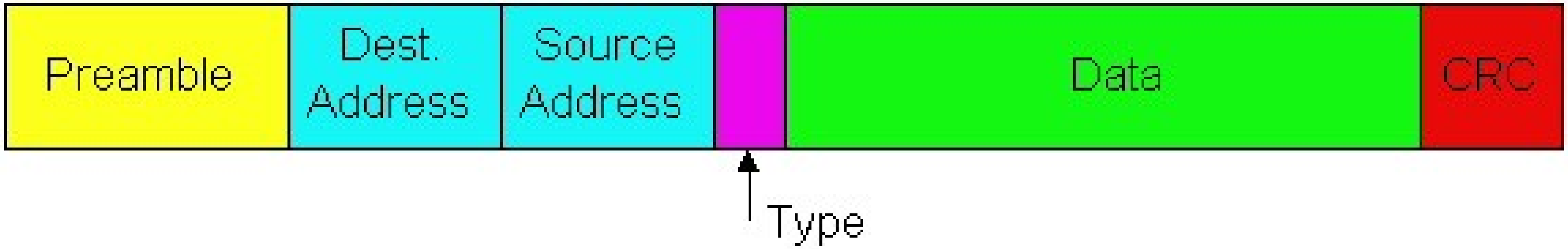
- Frame and MAC Address: 6 byte MAC address





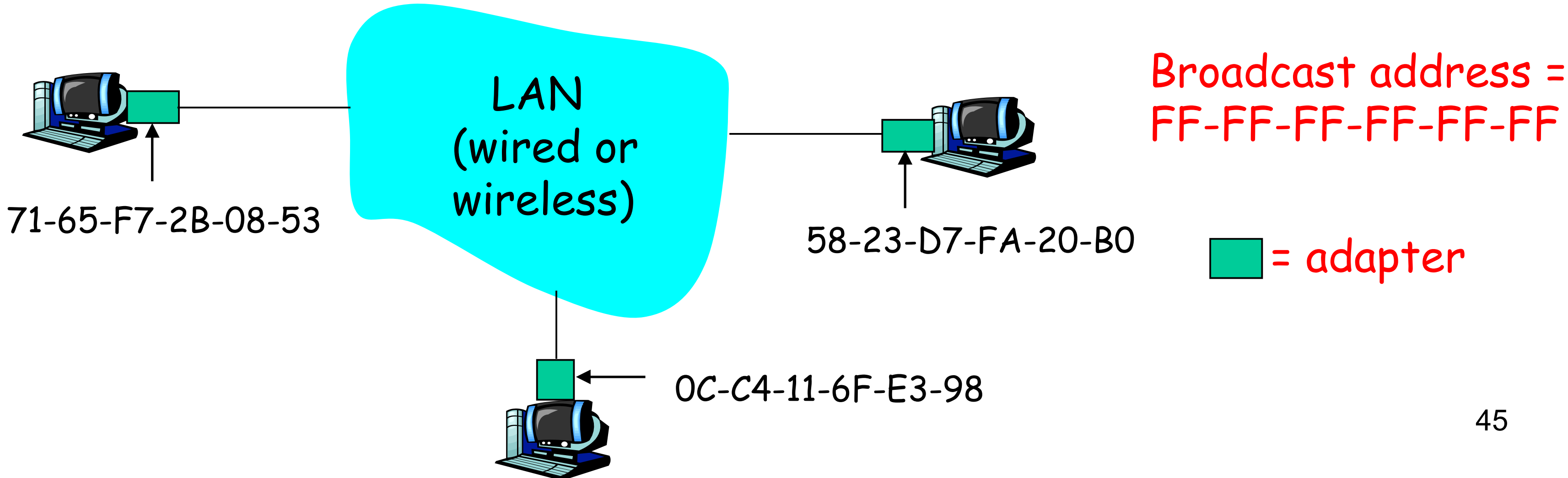
Ethernet Frame Structure

- **Preamble:**
  - 7 bytes with pattern 10101010 followed by one byte with pattern 10101011 to synchronize receiver, sender clock rates
- **Addresses:** 6 bytes
  - if adapter receives frame with matching destination address, or with broadcast address, it passes data in frame to network layer protocol
  - otherwise, adapter discards frame
- **Type:** indicates the higher layer protocol
- **CRC:** checked at receiver, if error is detected, the frame is simply dropped



Link-layer Addresses

- Each host/end system has a 32-bit network layer address (or IP address):
  - 4-byte IP addresses are typically expressed in decimal notation and hierarchical structure, with each period separating one of the bytes expressed in decimal notation from 0 to 255.
- Each adapter on a host has a unique 48-bit link-layer (or MAC, or LAN, or physical or Ethernet) address:
  - 6-byte MAC addresses are typically expressed in hexadecimal notation, with each byte of the address expressed as a pair of hexadecimal numbers.



MAC Addresses

- 32-bit IP address:
  - *network-layer* address
  - Hierarchical name structure of 32 bits (subnet and host)
  - Like a postal mailing address
  - used at router to direct datagram to destination IP subnet
  - DNS(Domain Name System) provides the transformation from hostname to IP address
- 48-bit MAC (LAN, physical or Ethernet) address:
  - Link-layer address
  - Flat name structure of 48 bits (eg. 00-0E-9B-32-96-69)
  - Like an ID number. It is burned in the adapter ROM. It is permanent.
  - used to drive frame from one LAN adapter card to the another node's LAN adapter card on the same LAN (i.e., both adapters are physically-connected)
  - ARP(address resolution protocol) provides the service of getting the MAC address for a specified IP address.