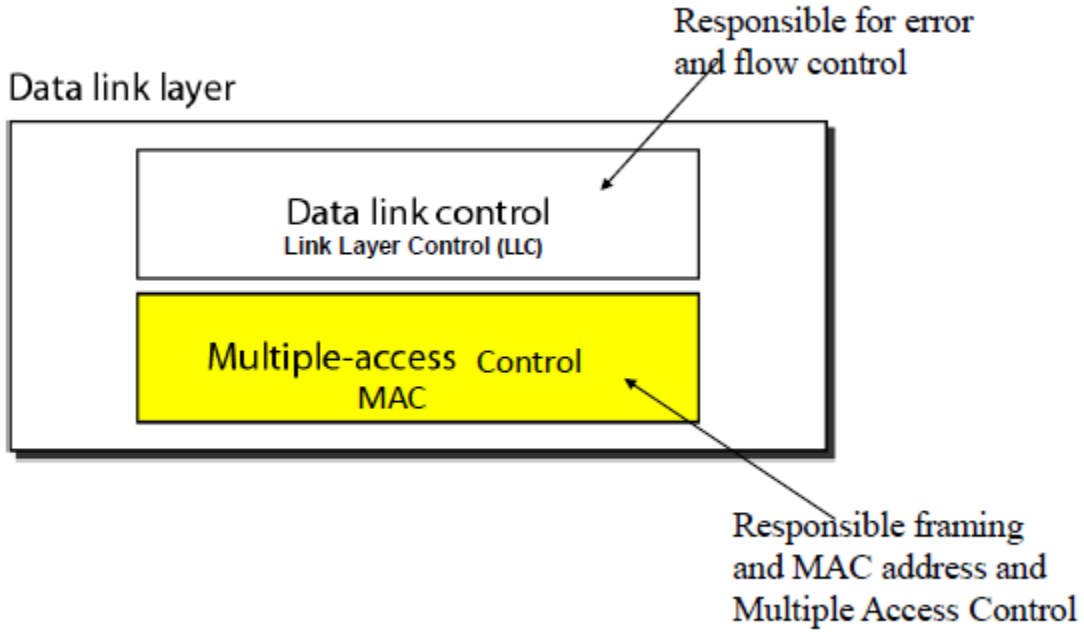
PART IV : DATA LINK LAYER

Data Communication and Computer Network

VER 2025

Data Link Layer Divided Into Two Functionality-oriented Sub-layers



4.1 Error Detection and Correction

Introduction

- Networks must be able to transfer data from one device to another with acceptable accuracy.
- For most applications, a system must guarantee that the data received are identical to the data transmitted.
- Any time data are transmitted from one node to the next, they can become corrupted in passage.

Transmission Errors

- Causes: noises, attenuation, distortion, crosstalk, losing synchronization.
- Error detection
  - Parity checks, cyclic redundancy codes, …
- Error correction
  - send redundant information with data
  - when receiving data incorrectly, the receiver makes “educated guess” about the original data
  - Ex. Hamming code

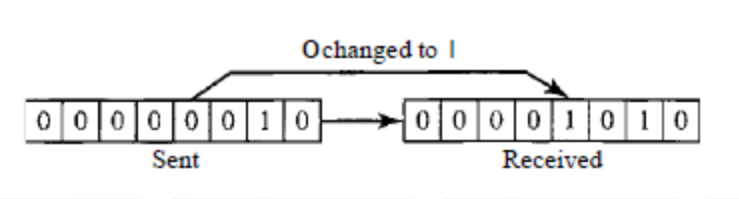
Detection VS Correction

- The correction of errors is more difficult than the detection. In error detection, we are looking only to see if any error has occurred. The answer is a simple yes or no. We are not even interested in the number of errors. A single-bit error is the same for us as a burst error.

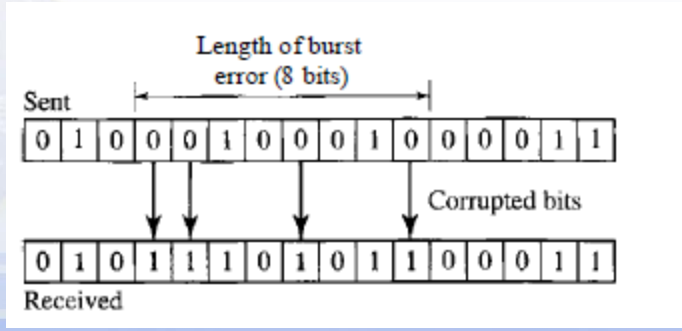
- In error correction, we need to know the exact number of bits that are corrupted and more importantly, their location in the message.
  - The number of the errors and the size of the message are important factors.

Type of Errors

- Single bit error
  - The term *single-bit error means that only 1 bit of a given data unit (such as a byte,* character, or packet) is changed from 1 to 0 or from 0 to 1.



- Burst Error
  - The term *burst error means that 2 or more bits in the data unit have changed from 1 to 0* or from 0 to 1.

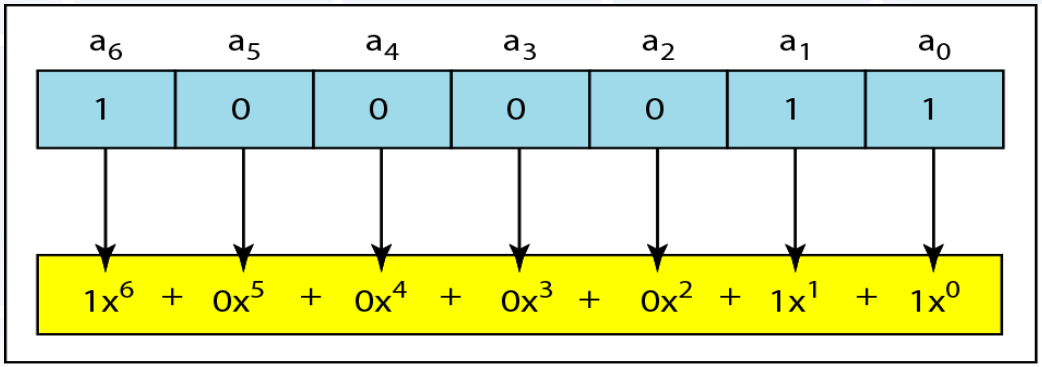


Cyclic Redundancy Check (CRC)

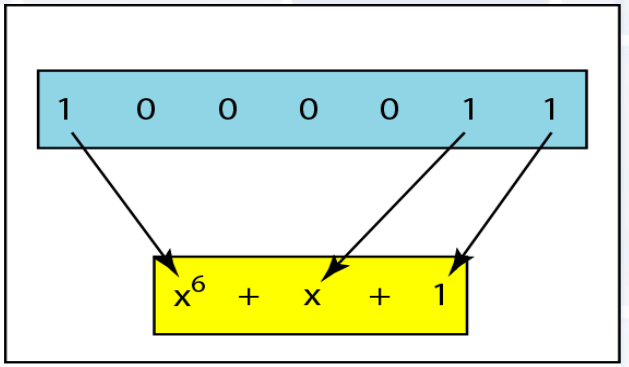
Commonly used polynomials and their binary equivalent for CRC generation

CRC type	Generator Polynomial	Binary Equivalent
CRC-8	$X^8 + x^2+x+1$	10000111
CRC-10	$X^{10}+ X^9 +X^5 +x^4+x+1$	11000110011
CRC-16	$X^{16} + X^{15} +X^2 +1$	1100000000000101
CRC-32	$X^{32} + X^{26} +X^{23} +ssX^{22} + X^{16} +X^{12} +X^{11} + X^{10} +X^8 +X^7 + X^5 +X^4 + X^2 +X +1$	10000010011000001000111010110111

A Polynomial To Represent A Binary Word



a. Binary pattern and polynomial



b. Short form

- Consider a message 10011101 represented by the polynomial $M(x) = x^7 + x^4 + x^3 + x^2 + 1$
- Consider a *generating polynomial* $G(x) = x^3 + x + 1$ (1011).

Solution

- Multiply M(x) by x^3 (highest power in G(x))

  $= (x^7 + x^4 + x^3 + x^2 + 1) * (x^3)$

  $= x^{10} + x7 + x^6 + x^5 + x^3$

  $= 10011101000$

- Divide the result by G(x). The remainder = C(x)

$$= \frac{x^{10} + x7 + x^6 + x^5 + x^3}{x^3 + x + 1}$$

$= x + 1$

$C(x) = x + 1$

Solution

- Data sent /codeword: dataword + reminder

At the sender side : $x^{10} + x7 + x^6 + x^5 + x^3 + x + 1$

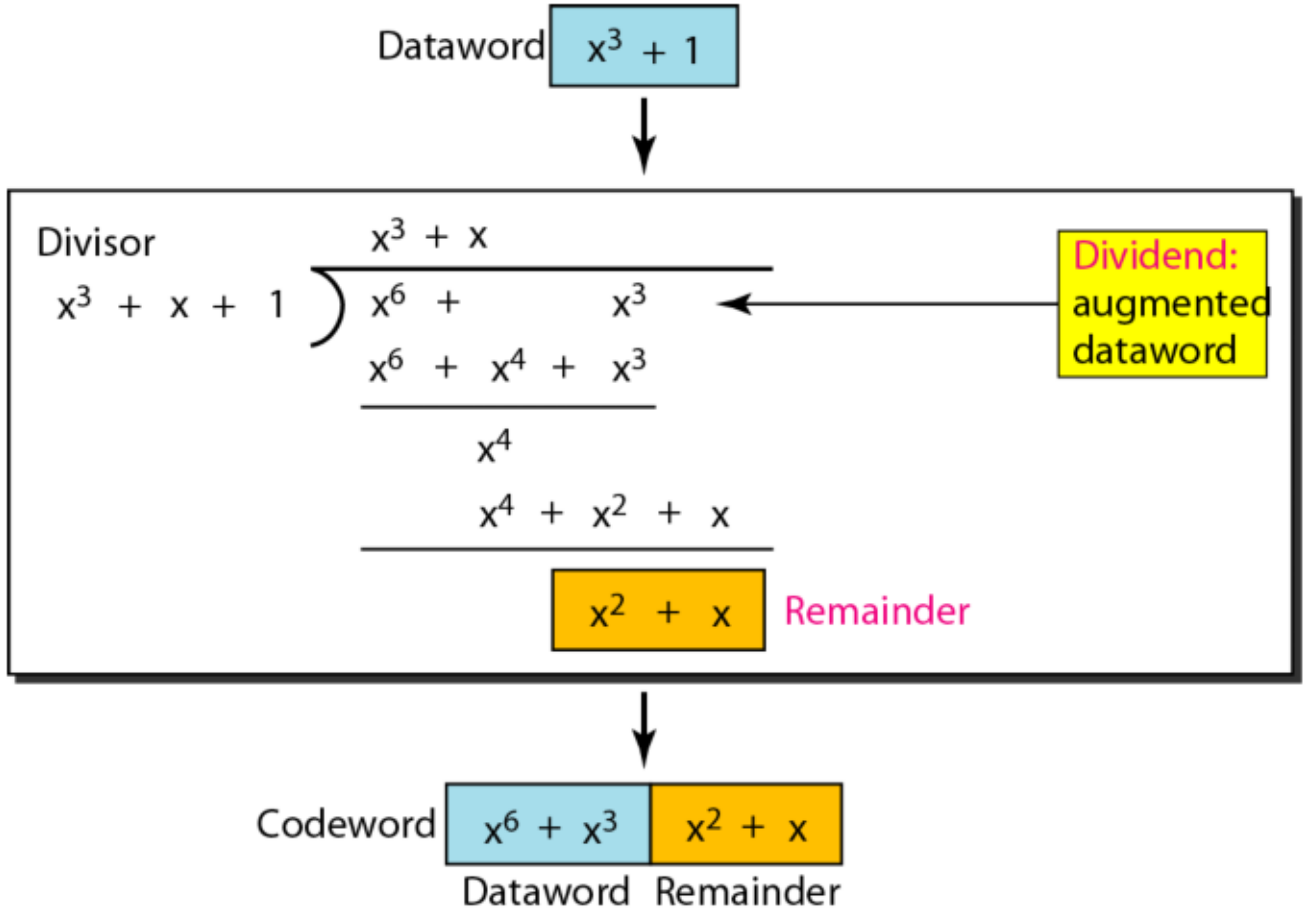
- Sender calculate :

$$= \frac{x^{10} + x7 + x^6 + x^5 + x^3 + x + 1}{x^3 + x + 1}$$

$C(x) = 0$

- Means no error is detected

Another Sample

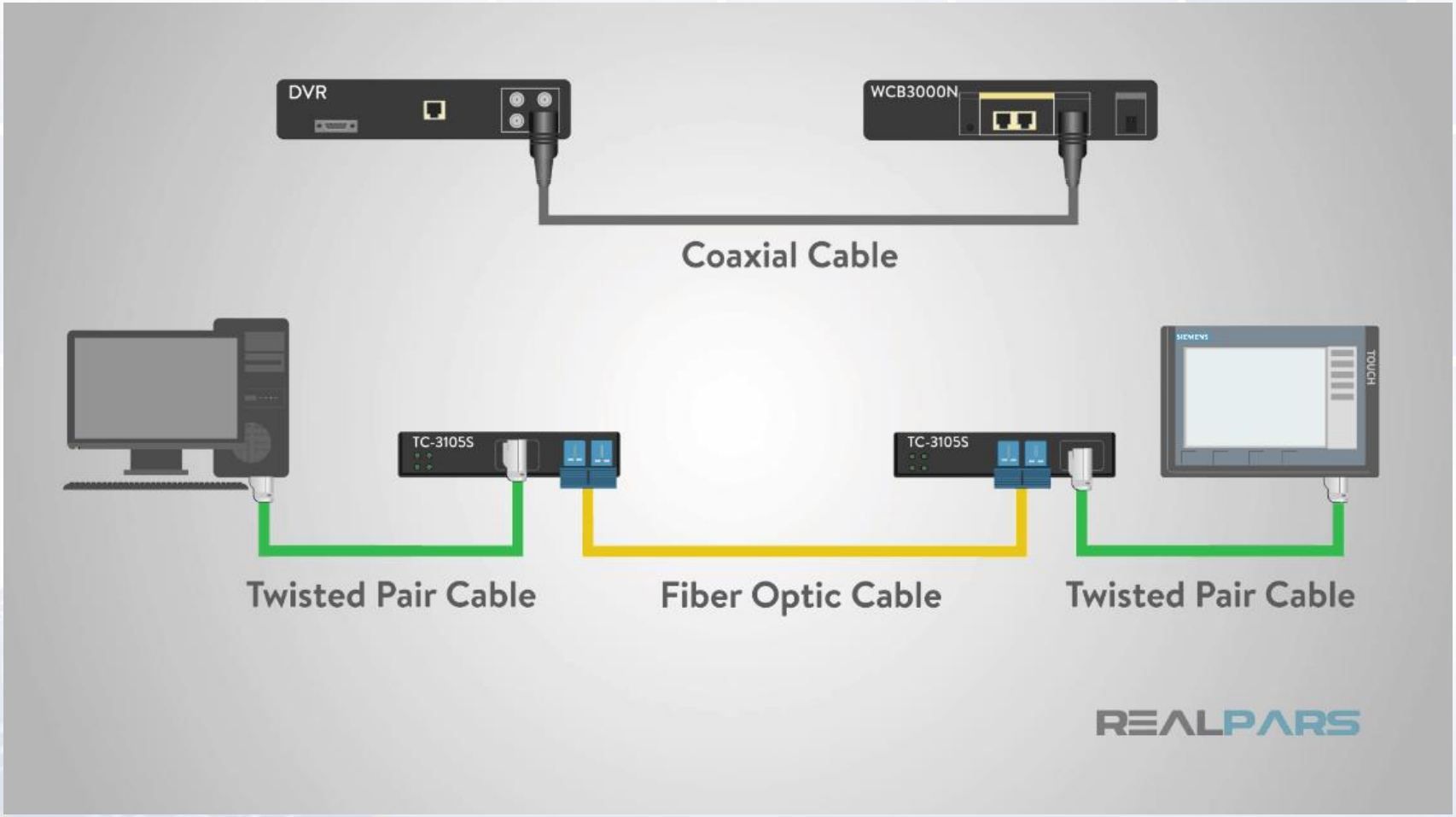


4.2 ETHERNET

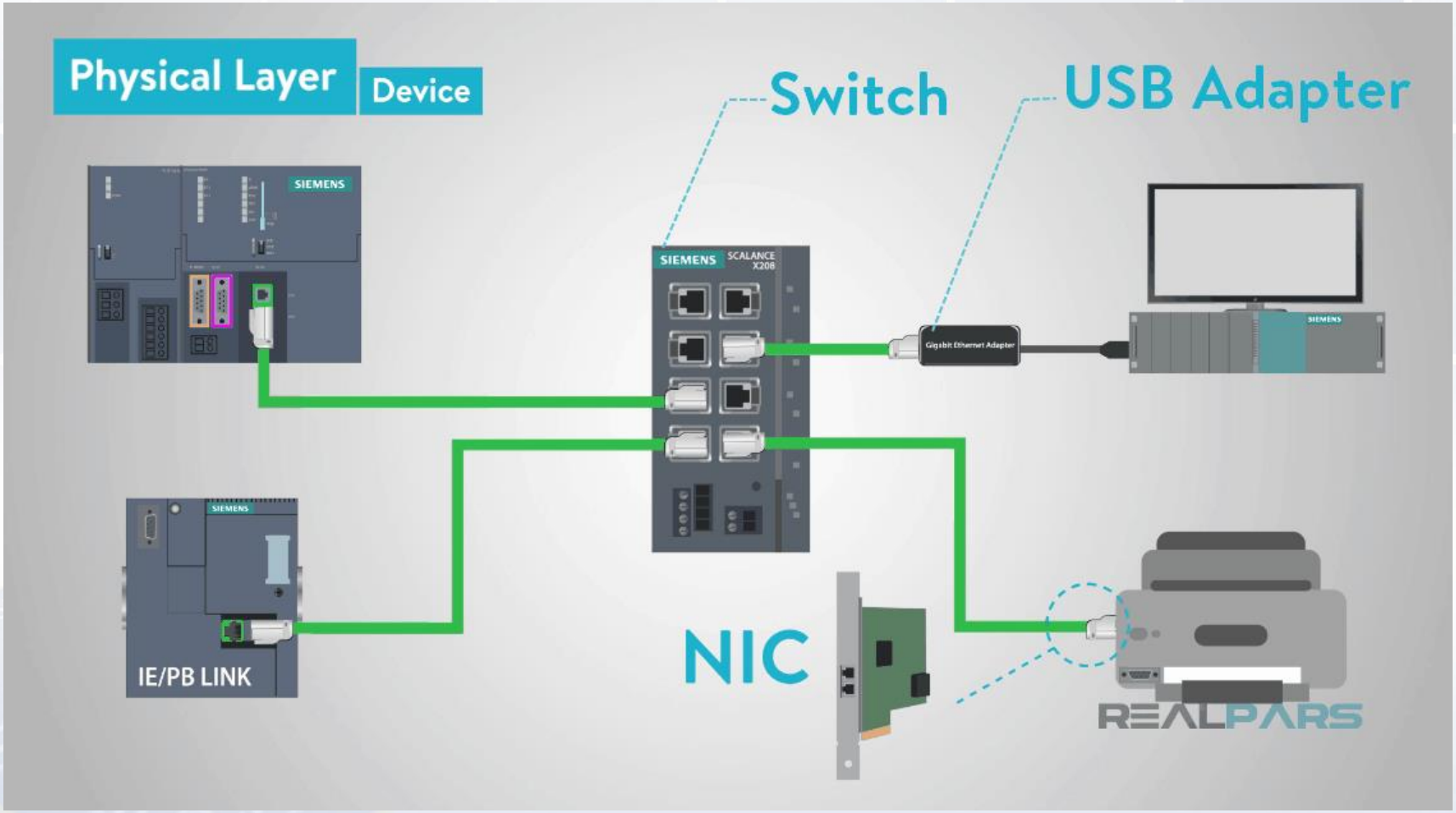
Ethernet

- Ethernet is a communication standard that was developed in the early ’80s to network computers and other devices in a local environment such as a home or a building.
- This local environment is defined as a LAN (Local Area Network) and it connects multiple devices so that they can create, store and share information with others in the location.
- Ethernet is a wired system that started with using coaxial cable and has successfully progressed to now using twisted pair copper wiring and fiber optic wiring.

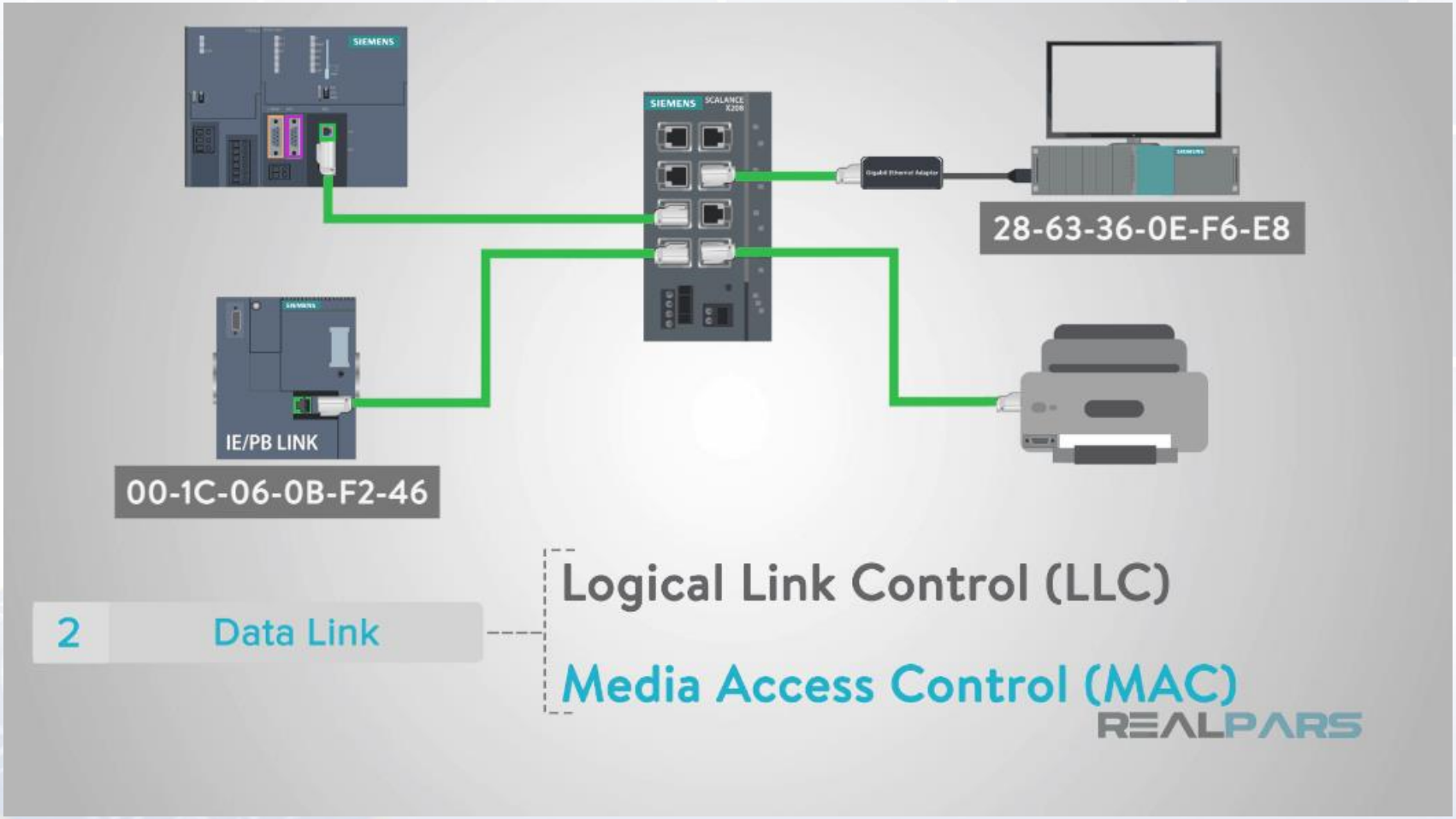
Ethernet Cabel



Ethernet Device



Ethernet Data Link Layer



Ethernet Speed Evolution

- 10 Mbps (Ethernet I, II)
- 100 Mbps (Fast Ethernet)
- 1 Gbps (Gigabit Ethernet)
- 10 Gbps
- 25 Gbps
- 40 Gbps
- 50 Gbps
- 100 Gbps
- 400 Gbps
- 800 Gbps (draft IEEE 802.3df)

IEEE Ethernet Standards & Technologies

- IEEE 802.3bz: 2.5GBASE-T, 5GBASE-T
- IEEE 802.3bq: 25GBASE-T, 40GBASE-T (Cat8)
- IEEE 802.3cd: 50G Ethernet
- IEEE 802.3bs, 802.3cu, 802.3ck: 100G, 400G Ethernet
- IEEE 802.3df (draft): 800G Ethernet

Ethernet Physical Media Evolution

- Twisted Pair UTP: Cat5e, Cat6, Cat6A, Cat7, Cat8
- Fiber Optic: OM3, OM4, OM5 (MMF), SMF
- Direct Attach Copper (DAC)
- Active Optical Cable (AOC)

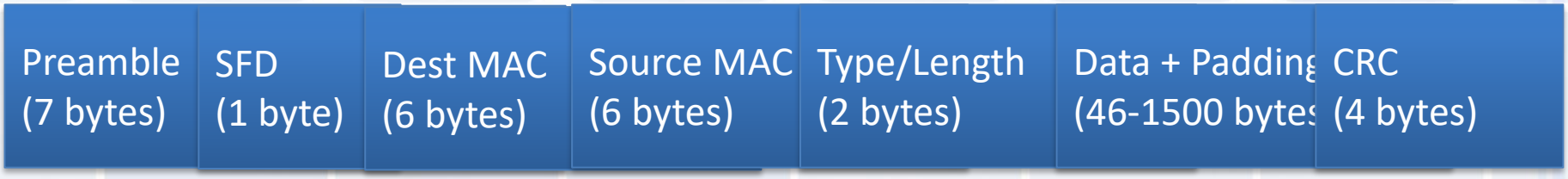
Modern Applications of Ethernet

- Data Center Interconnect
- AI/ML Cluster Networking
- 5G Mobile Backhaul & Fronthaul
- Cloud Computing Fabric (Hyperscale Data Centers)
- Ethernet in IoT & Edge Computing
- High Performance Storage Networks (SAN)

Ethernet Frame Format

- Ethernet II Frame (widely used)
- Still using IEEE 802.3 standard frame format:
  - Preamble (7 bytes)
  - Start Frame Delimiter (1 byte)
  - Destination MAC (6 bytes)
  - Source MAC (6 bytes)
  - Type/Length (2 bytes)
  - Data and Padding (46-1500 bytes)
  - CRC (4 bytes)
- Jumbo Frame support (>1500 bytes) for data center & storage networks

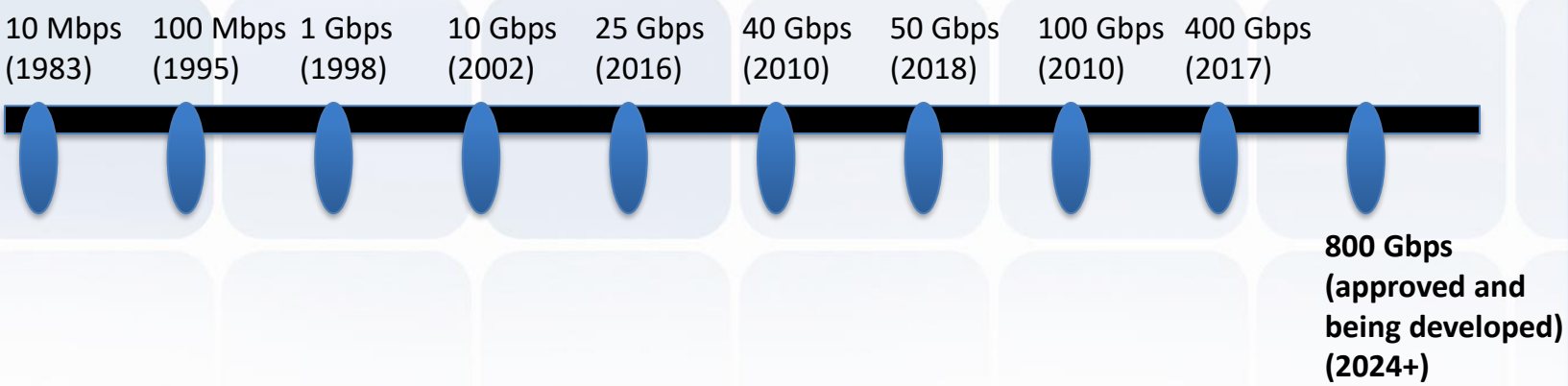
Ethernet Frame Format



Ethernet in Modern Network Architectures

- • Replacing legacy architectures
- • Used in Spine-Leaf data center fabric
- • Supports Virtualization (VXLAN over Ethernet)
- • Replacing InfiniBand in AI/ML workloads (RDMA over Converged Ethernet - RoCE)

Ethernet Speed Evolution Timeline with Years

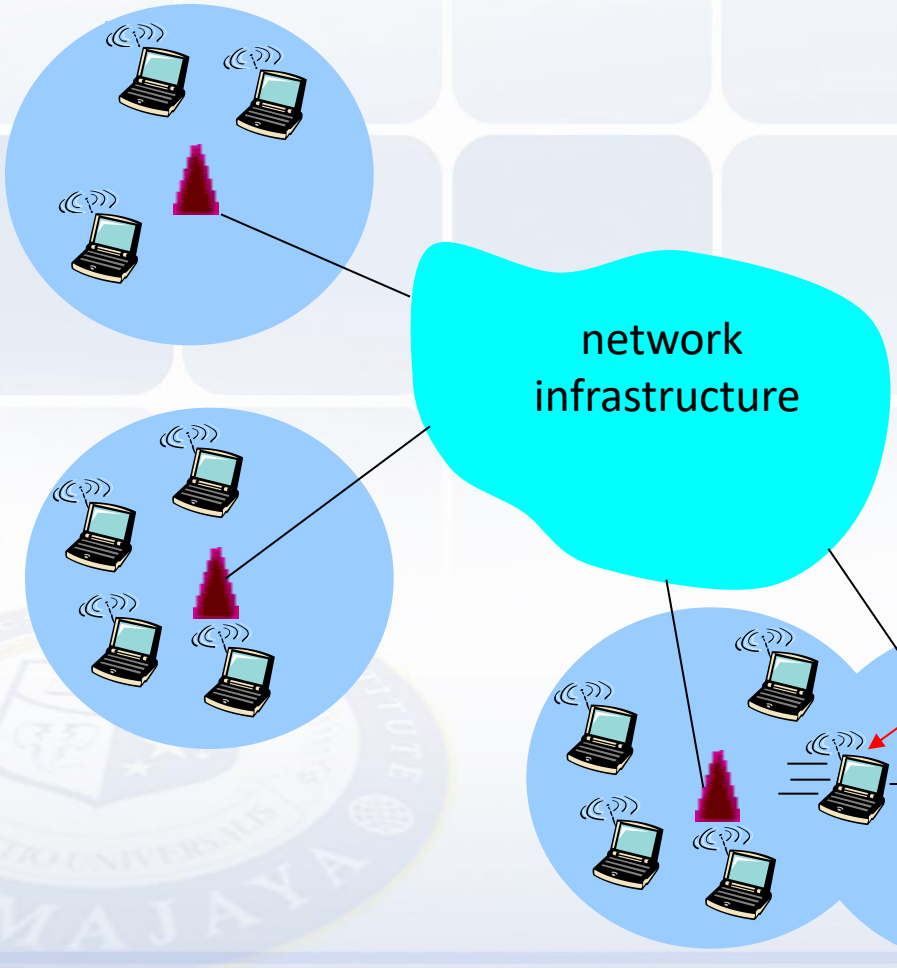


4.3 Wireless LAN

Wireless and Mobile Networks

- wireless (mobile) phone subscribers now exceeds # wired phone subscribers!
- computer nets: laptops, palmtops, PDAs, Internet-enabled phone promise anytime untethered Internet access
- two important (but different) challenges
  - *wireless:* communication over wireless link
  - *mobility:* handling the mobile user who changes point of attachment to network

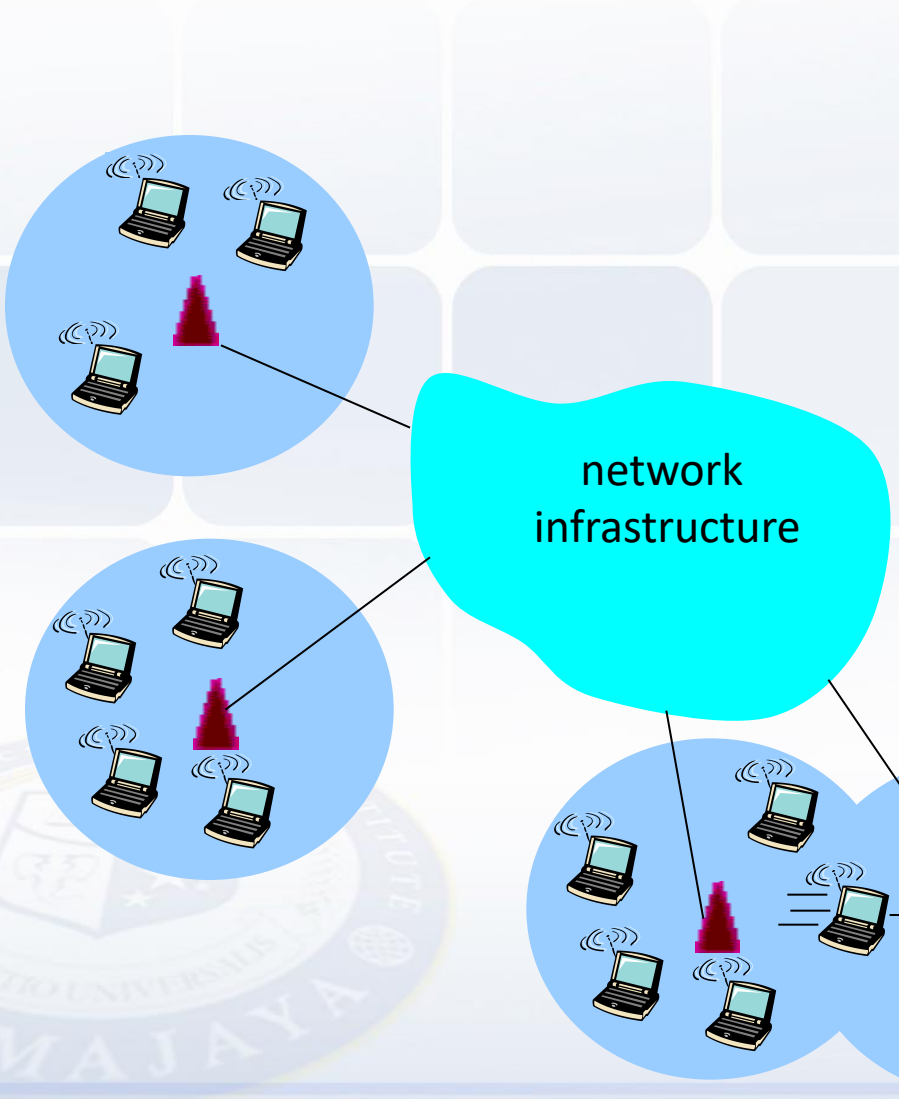
Elements of a wireless network



wireless hosts

- laptop, PDA, IP phone
- run applications
- may be stationary (non-mobile) or mobile
  - wireless does *not* always mean mobility

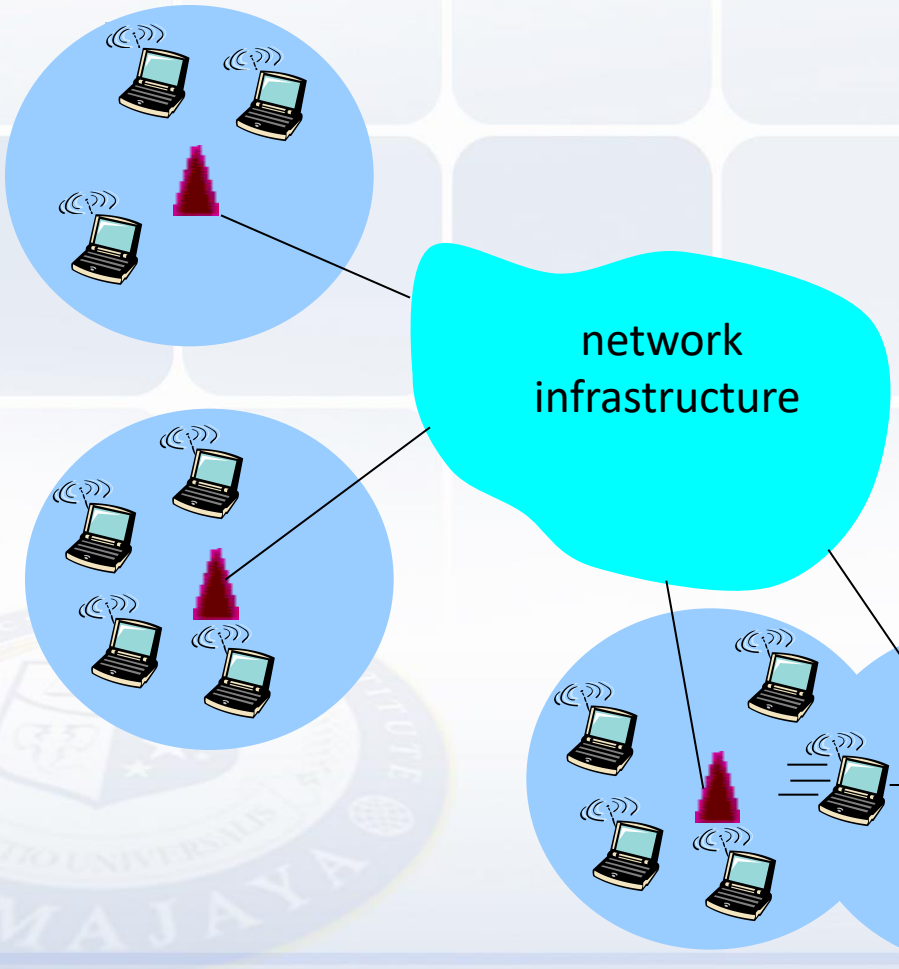
Elements of a wireless network



base station

- typically connected to wired network
- relay - responsible for sending packets between wired network and wireless host(s) in its "area"
  - e.g., cell towers, 802.11 access points

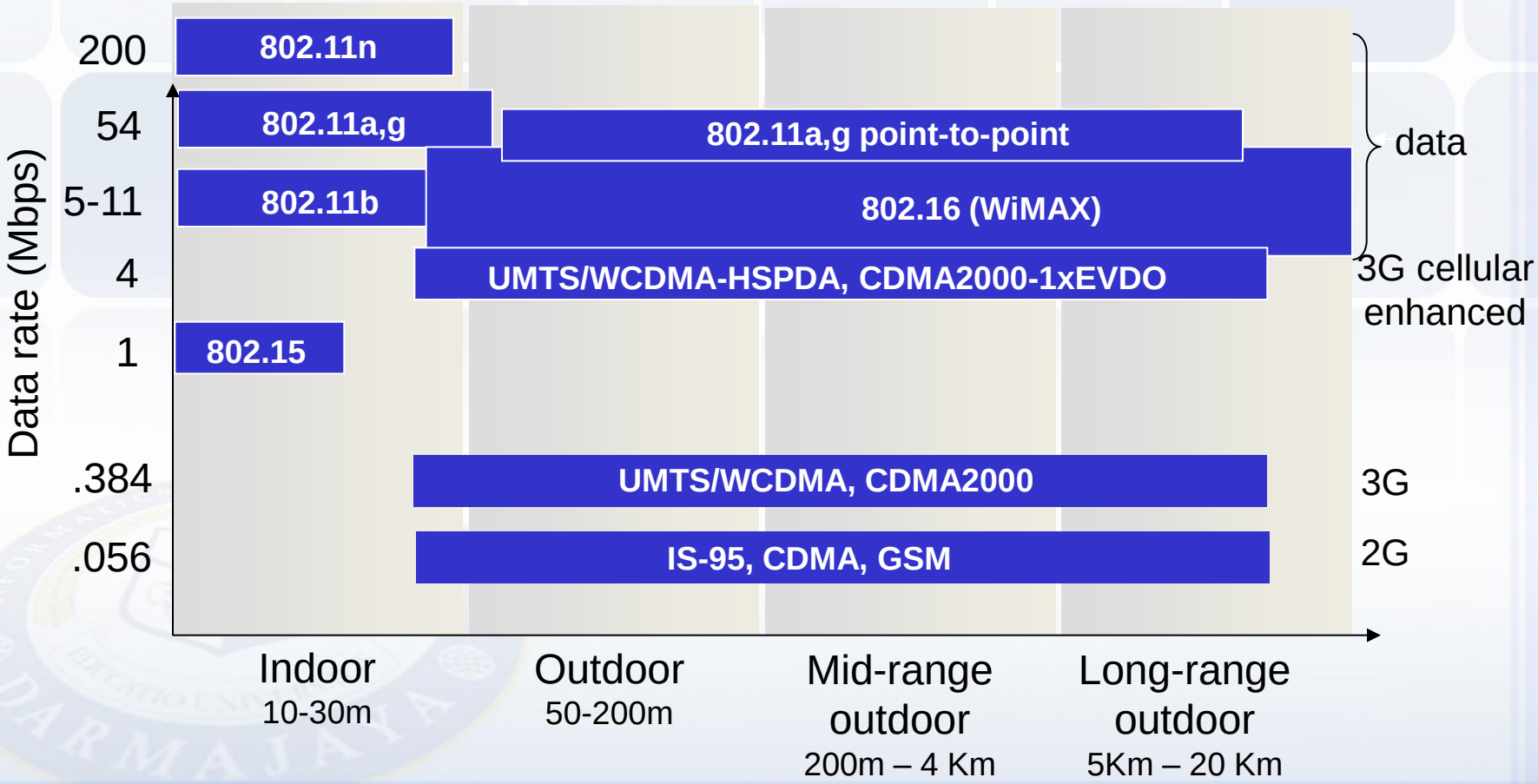
Elements of a wireless network



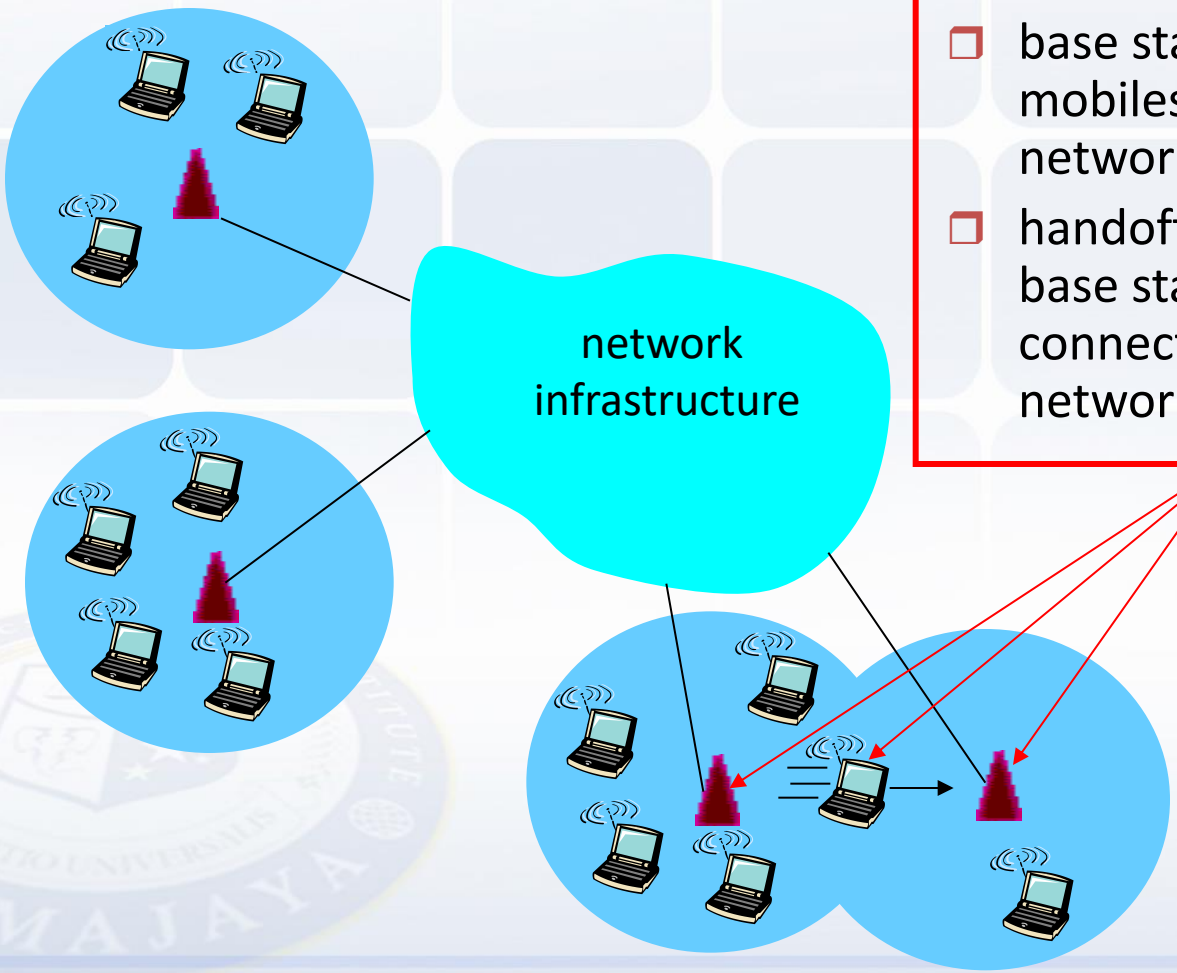
wireless link

- typically used to connect mobile(s) to base station
- also used as backbone link
- multiple access protocol coordinates link access
- various data rates, transmission distance

Characteristics of selected wireless link standards



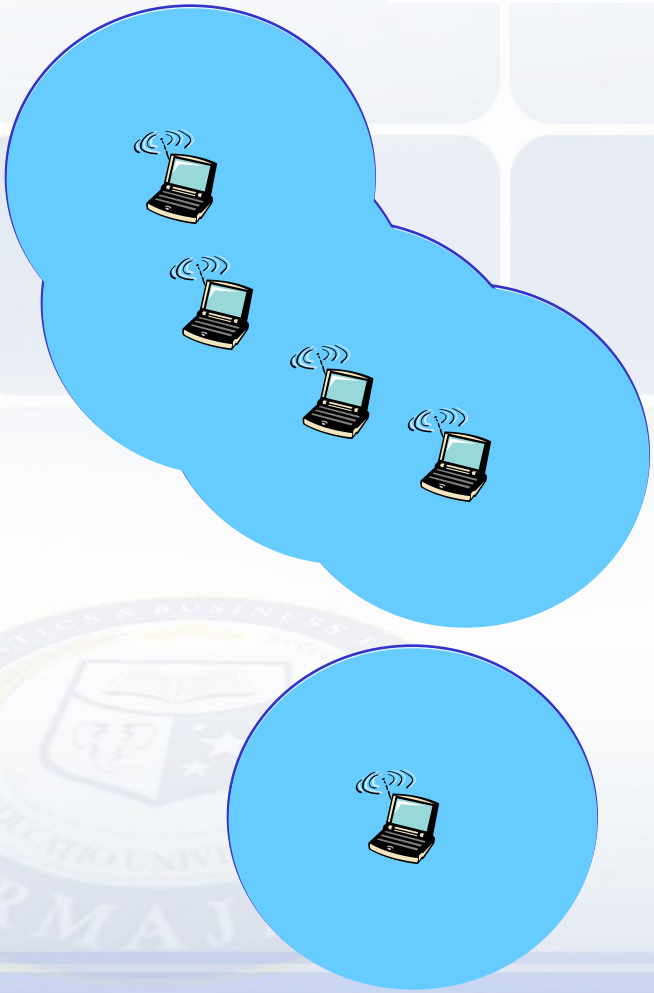
Elements of a wireless network



infrastructure mode

- base station connects mobiles into wired network
- handoff: mobile changes base station providing connection into wired network

Elements of a wireless network



ad hoc mode

- no base stations
- nodes can only transmit to other nodes within link coverage
- nodes organize themselves into a network: route among themselves

Wireless Link Characteristics (1)

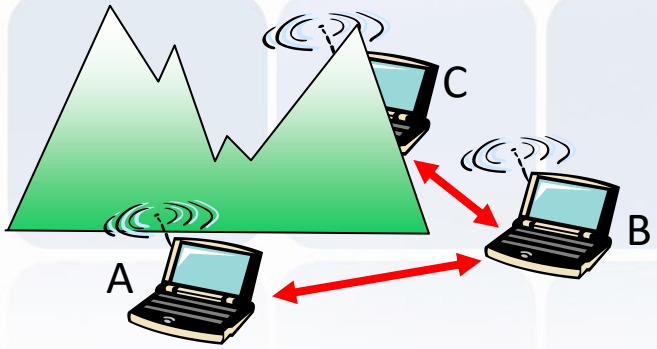
Differences from wired link ….

- decreased signal strength: radio signal attenuates as it propagates through matter (e.g radio signal passing trough a wall) or in free space, the signal strength may decrease as the due to the distance (called path loss)
- interference from other sources: standardized wireless network frequencies (e.g., 2.4 GHz) shared by other devices (e.g., phone); devices (motors) interfere as well
- multipath propagation: radio signal reflects off objects ground, arriving ad destination at slightly different times

…. make communication across (even a point to point) wireless link much more “difficult”

Wireless network characteristics

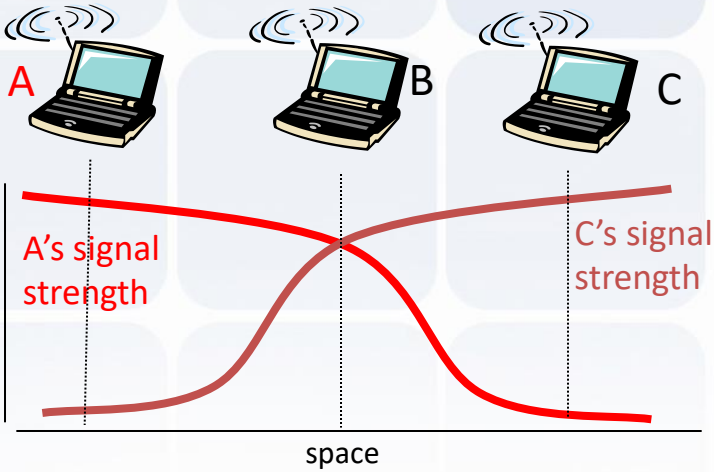
Multiple wireless senders and receivers create additional problems (beyond multiple access):



Hidden terminal problem

- B, A hear each other
- B, C hear each other
- A, C can not hear each other

means A, C unaware of their interference at B



Signal attenuation:

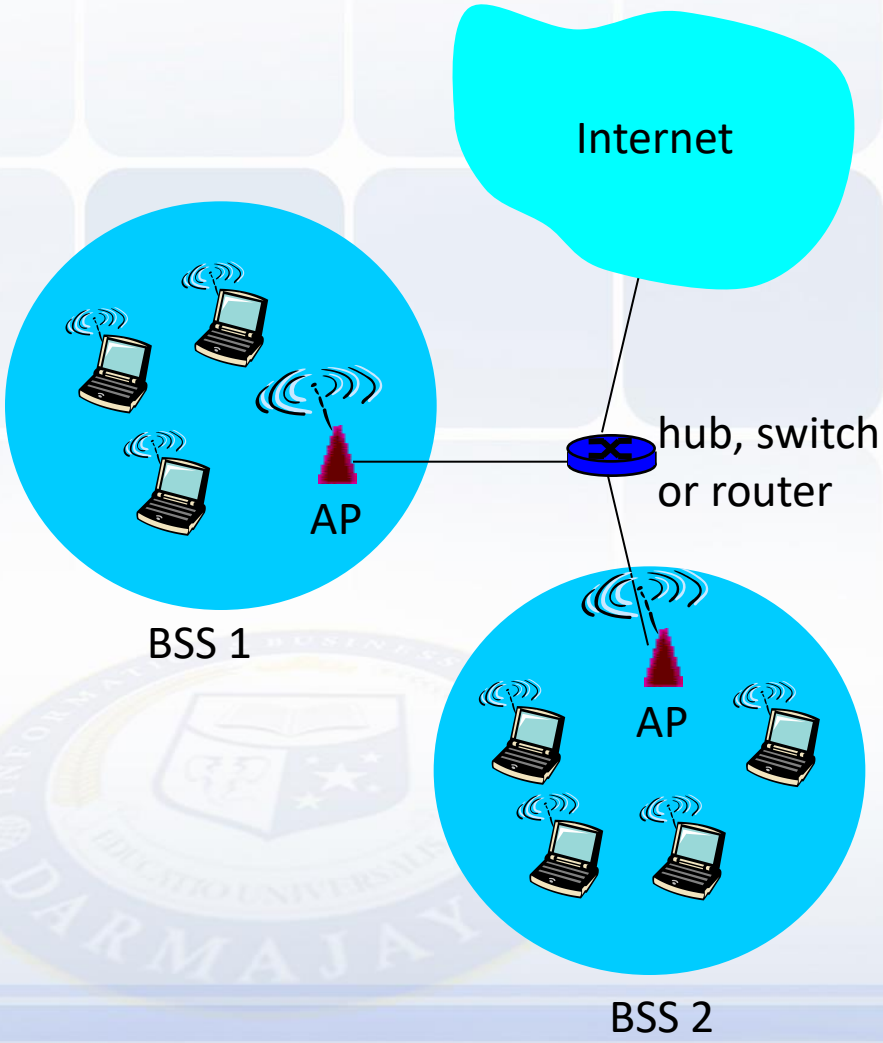
- B, A hear each other
- B, C hear each other
- A, C can not hear each other interfering at B

IEEE 802.11 Wireless LAN

- 802.11b
  - 2.4-5 GHz unlicensed spectrum
  - up to 11 Mbps
  - direct sequence spread spectrum (DSSS) in physical layer
- 802.11a
  - 5-6 GHz range
  - up to 54 Mbps
- 802.11g
  - 2.4-5 GHz range
  - up to 54 Mbps
- 802.11n: multiple antennae
  - 2.4-5 GHz range
  - up to 200 Mbps

- all use CSMA/CA for multiple access
- all have base-station and ad-hoc network versions

802.11 LAN architecture

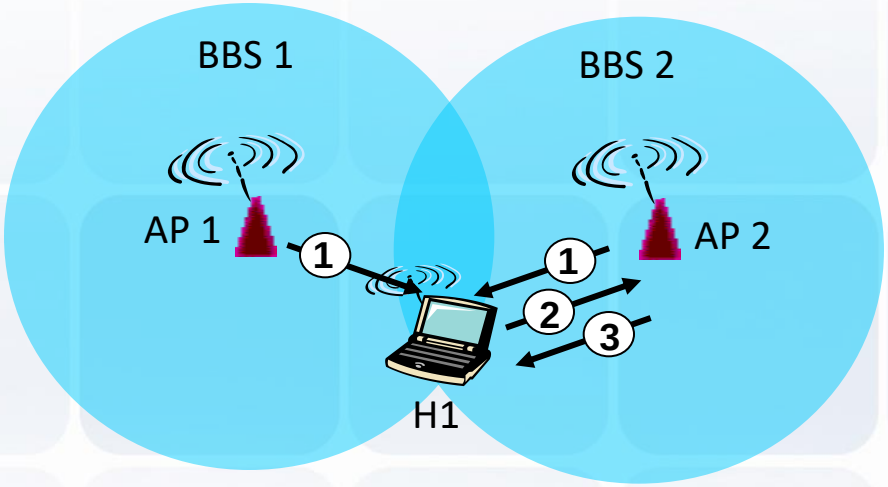


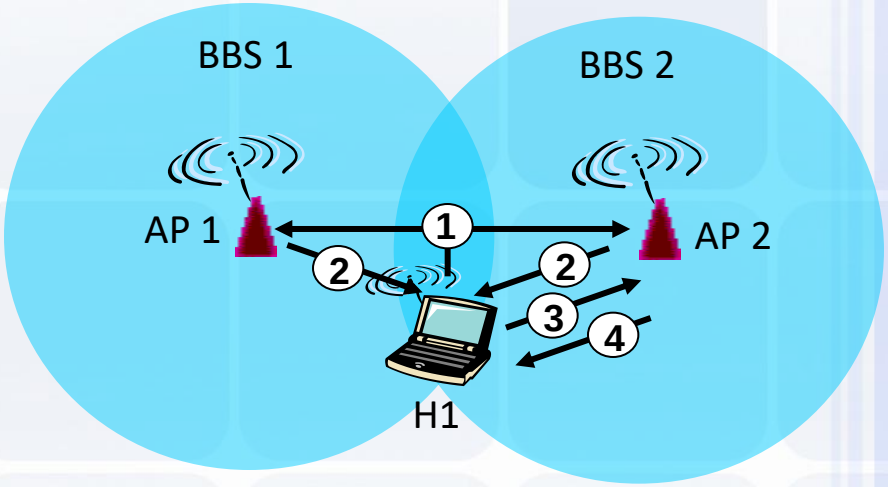
- wireless host communicates with base station
  - base station = access point (AP)
- Basic Service Set (BSS) (aka "cell") in infrastructure mode contains:
  - wireless hosts
  - access point (AP): base station
  - ad hoc mode: hosts only

802.11: Channels, association

- 802.11b: 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies
  - AP admin chooses frequency for AP
  - interference possible: channel can be same as that chosen by neighboring AP.
- host: must *associate* with an AP
  - scans channels, listening for *beacon frames* containing AP's name (SSID) and MAC address
  - selects AP to associate with
  - may perform authentication
  - will typically run DHCP to get IP address in AP's subnet

802.11: Passive/Active Scanning





Passive Scanning:

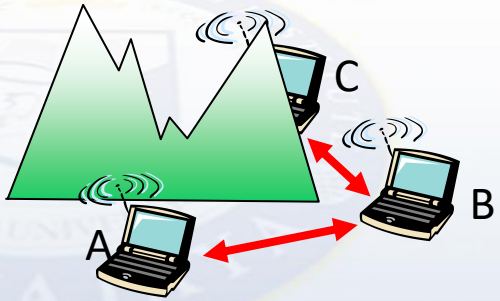
(1) beacon frames sent from APs
(2) association Request frame sent: H1 to selected AP
(3) association Response frame sent: H1 to selected AP

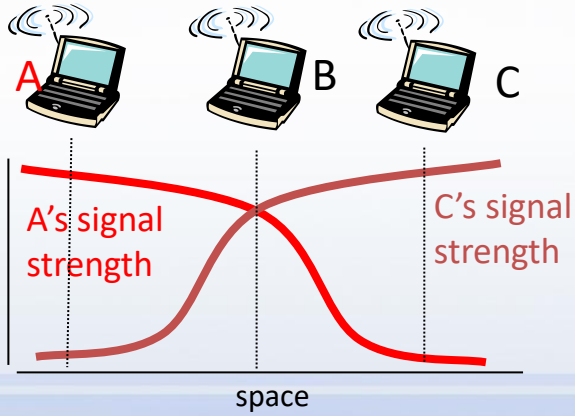
Active Scanning:

(1) Probe Request frame broadcast from H1
(2) Probes response frame sent from APs
(3) Association Request frame sent: H1 to selected AP
(4) Association Response frame sent: H1 to selected AP

IEEE 802.11: multiple access

- avoid collisions: 2^+ nodes transmitting at same time
- 802.11: CSMA - sense before transmitting
  - don't collide with ongoing transmission by other node
- 802.11: *no* collision detection!
  - difficult to receive (sense collisions) when transmitting due to weak received signals (fading)
  - can't sense all collisions in any case: hidden terminal, fading
  - goal: *avoid collisions:* CSMA/C(ollision)A(voidance)





IEEE 802.11 MAC Protocol: CSMA/CA

802.11 sender

1 if sense channel idle for **DIFS** (distributed inter-frame space) then

transmit entire frame (no CD)

2 if sense channel busy then

start random backoff time

timer counts down while channel idle

transmit when timer expires

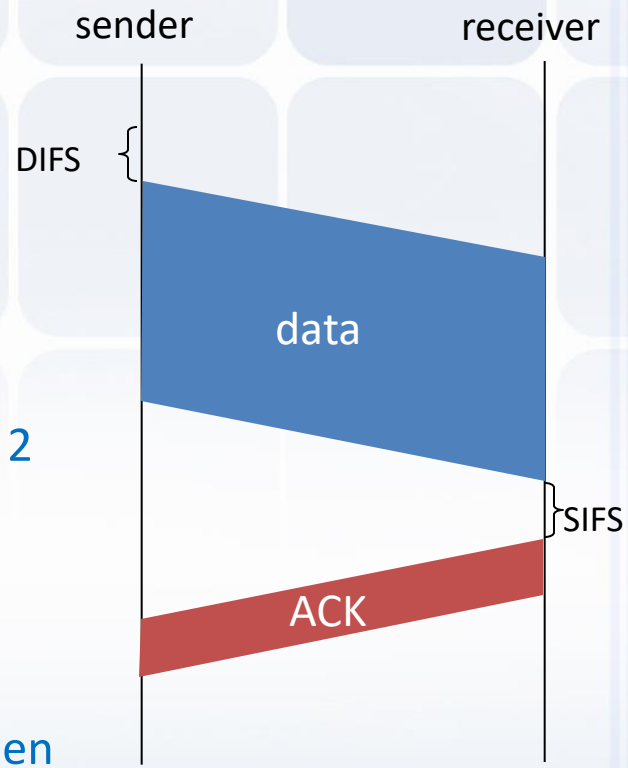
if no ACK, increase random backoff interval, repeat 2

802.11 receiver

- if frame received OK

return ACK after **SIFS (Short Inter-Frame Spacing)**

→**waiting for short period** (ACK needed due to hidden terminal problem)



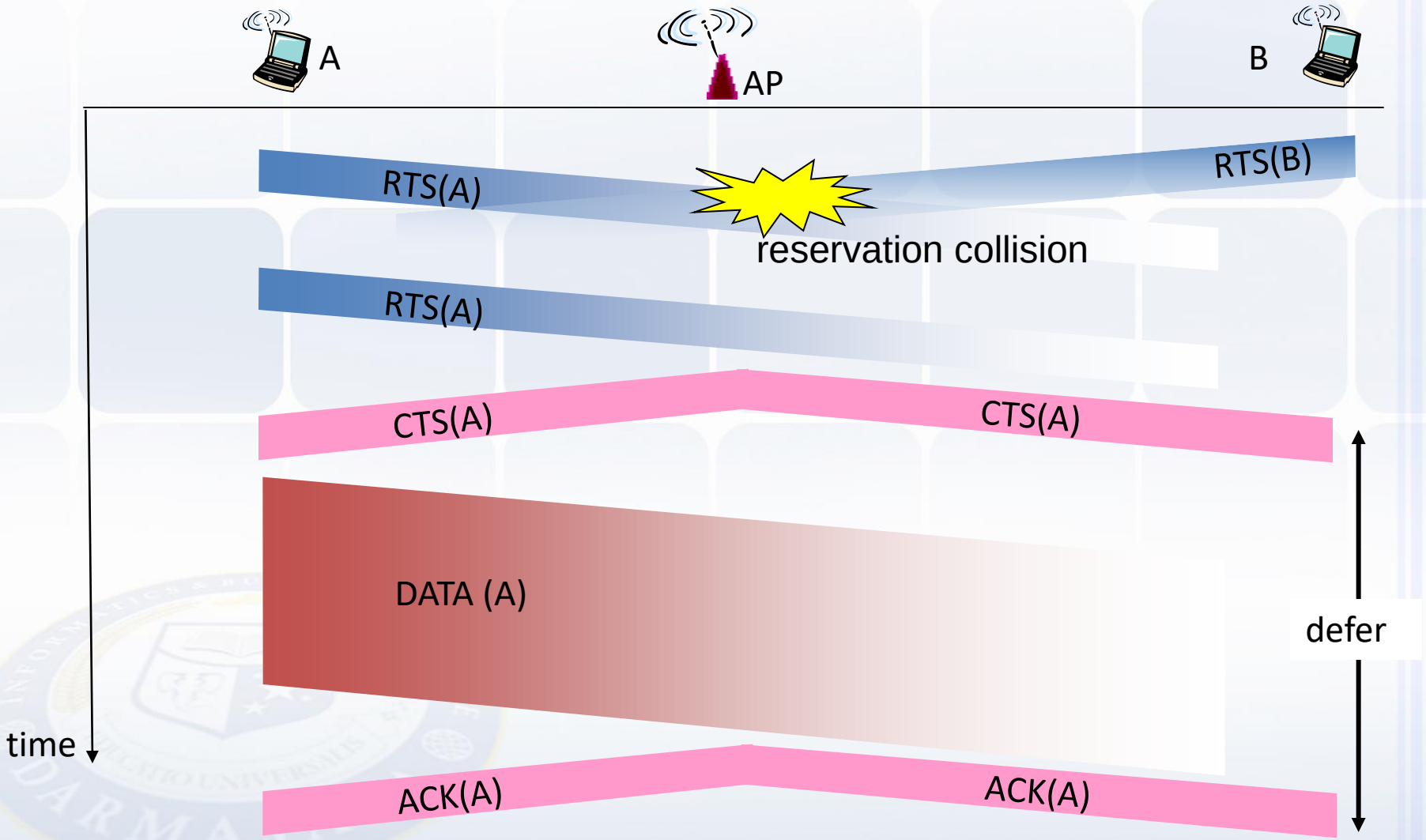
Avoiding collisions (more)

idea: allow sender to "reserve" channel rather than random access of data frames: avoid collisions of long data frames

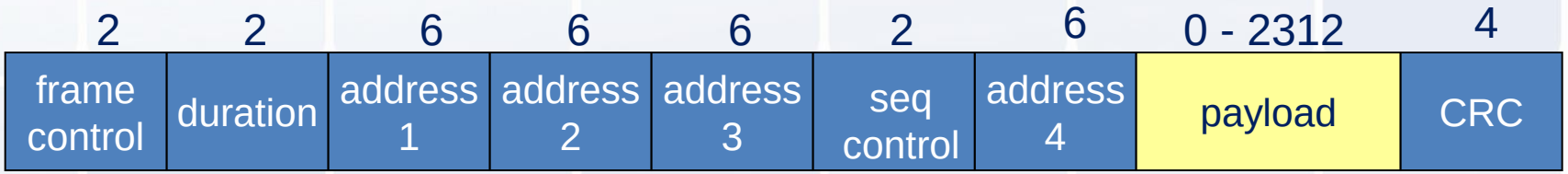
- sender first transmits *small* request-to-send (RTS) packets to BS using CSMA
  - RTSs may still collide with each other (but they're short)
- BS broadcasts clear-to-send CTS in response to RTS
- CTS heard by all nodes
  - sender transmits data frame
  - other stations defer transmissions

avoid data frame collisions completely
using small reservation packets!

Collision Avoidance: RTS-CTS exchange



802.11 frame: addressing



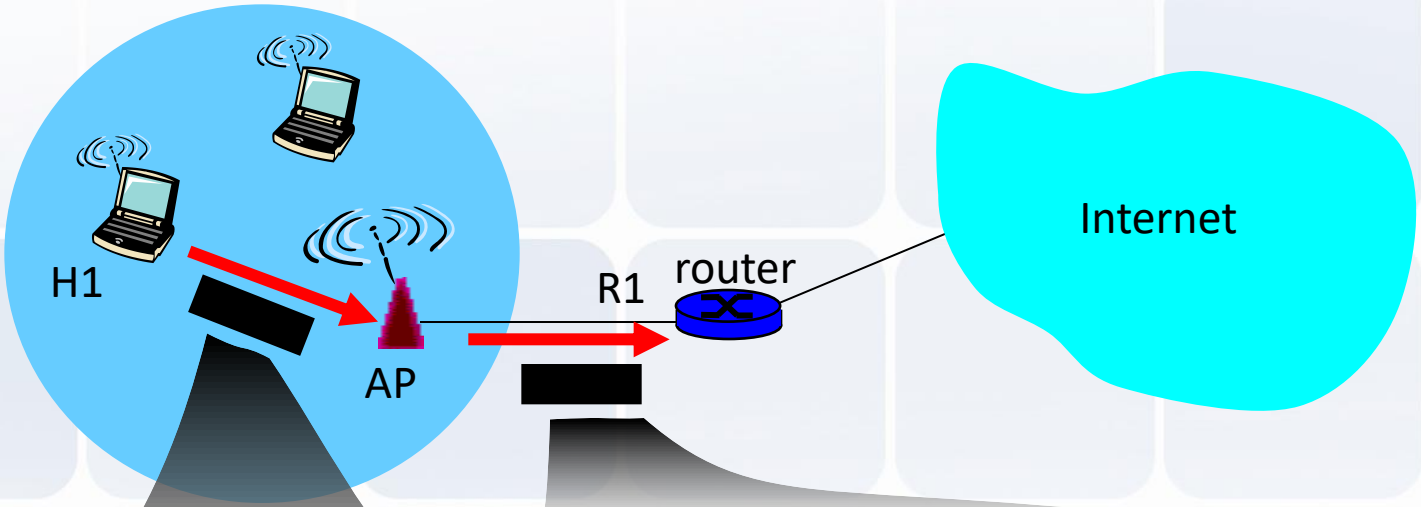
Address 1: MAC address of wireless host or AP to receive this frame

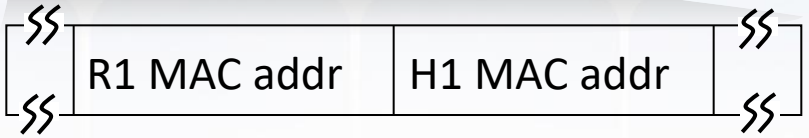
Address 2: MAC address of wireless host or AP transmitting this frame

Address 3: MAC address of router interface to which AP is attached

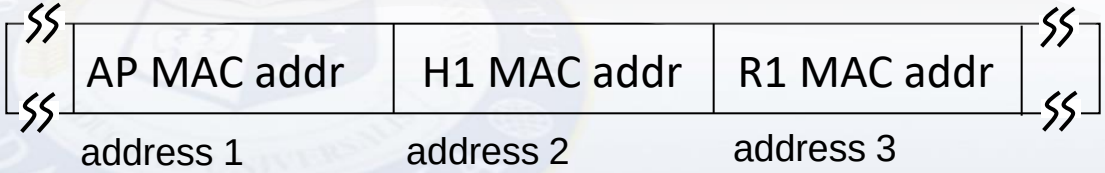
Address 4: used only in ad hoc mode

802.11 Frame: Addressing



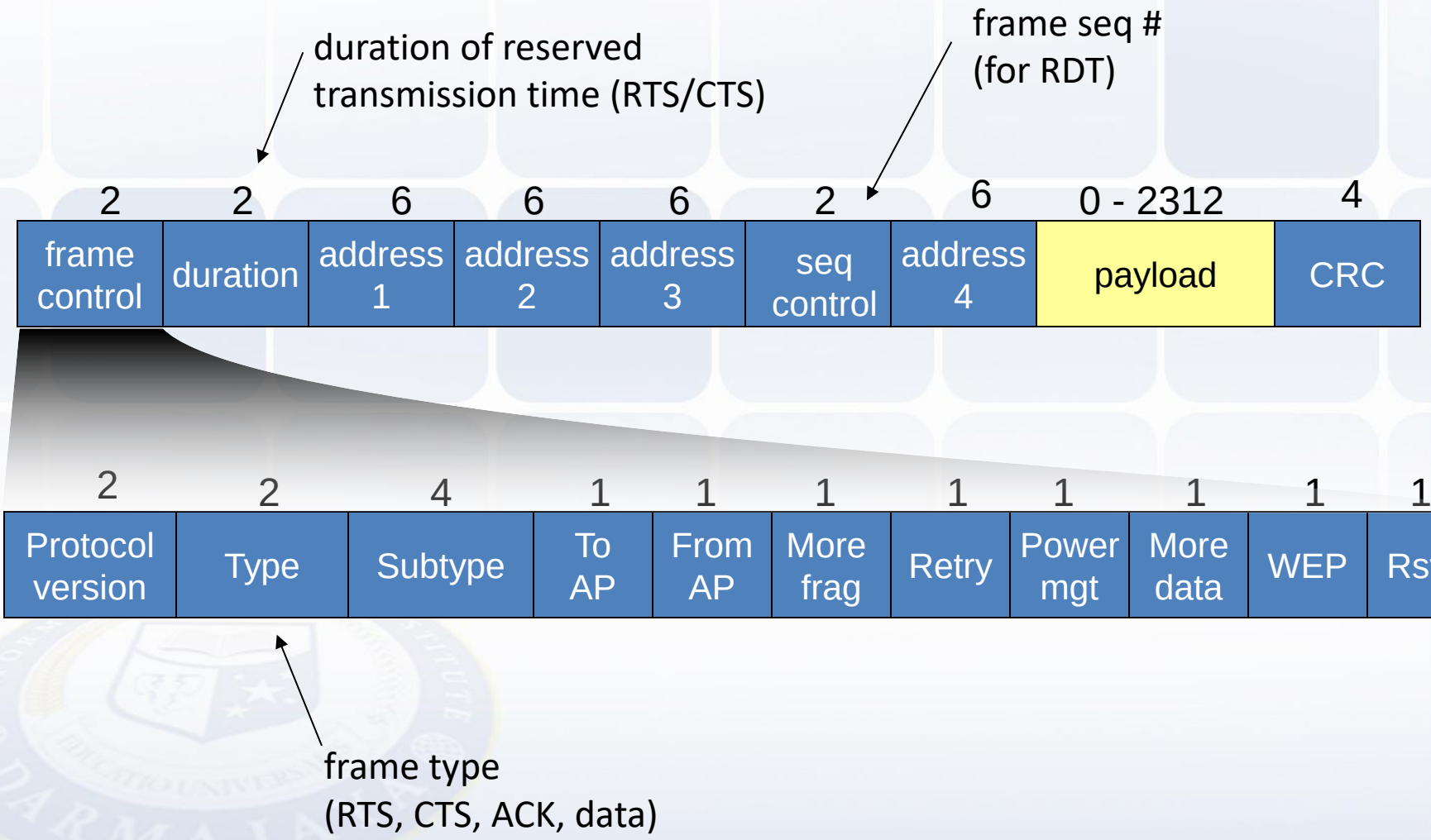


802.**3** frame



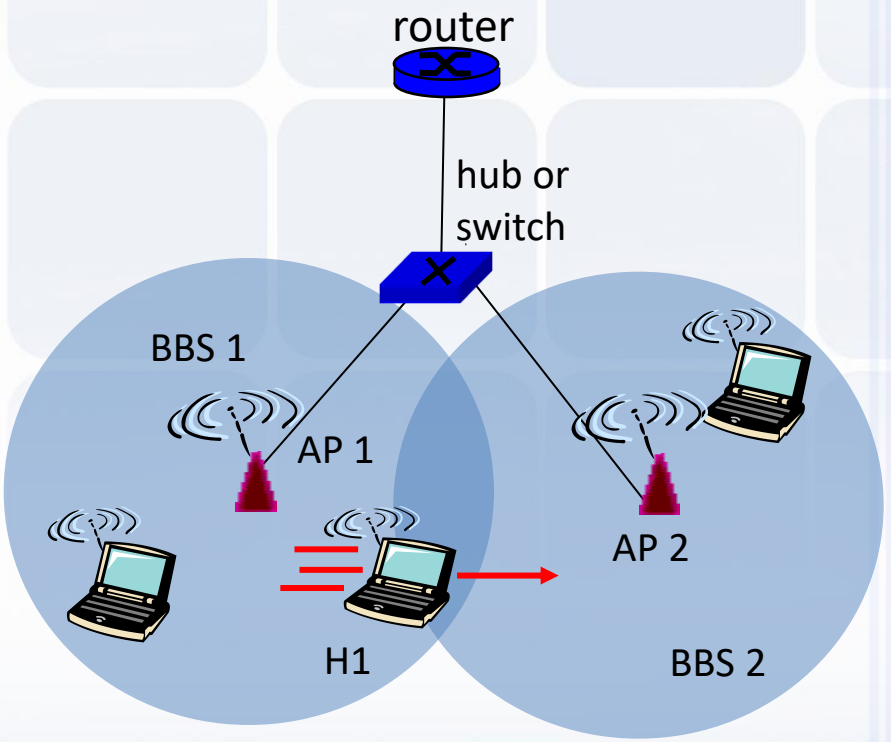
802.**11** frame

802.11 Frame: More



802.11: Mobility within Same Subnet

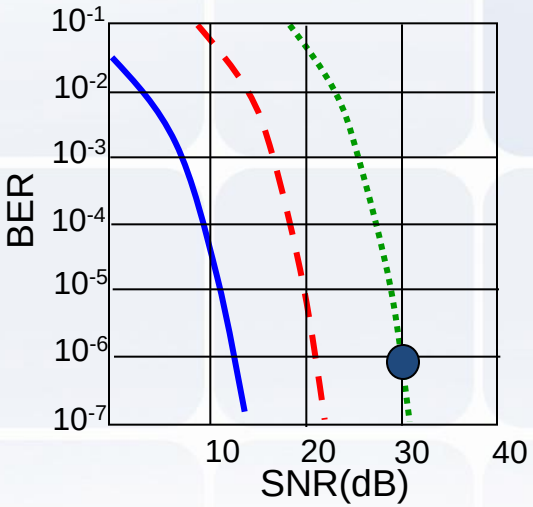
- H1 remains in same IP subnet: IP address can remain same
- switch: which AP is associated with H1?
  - self-learning: switch will see frame from H1 and "remember" which switch port can be used to reach H1



802.11: Advanced Capabilities

Rate Adaptation

- base station, mobile dynamically change transmission rate (physical layer modulation technique) as mobile moves, SNR varies



1. SNR decreases, BER increase as node moves away from base station

2. When BER becomes too high, switch to lower transmission rate but with lower BER

QAM256 (8 Mbps)
QAM16 (4 Mbps)
BPSK (1 Mbps)
operating point

BER : Bit Error Rate

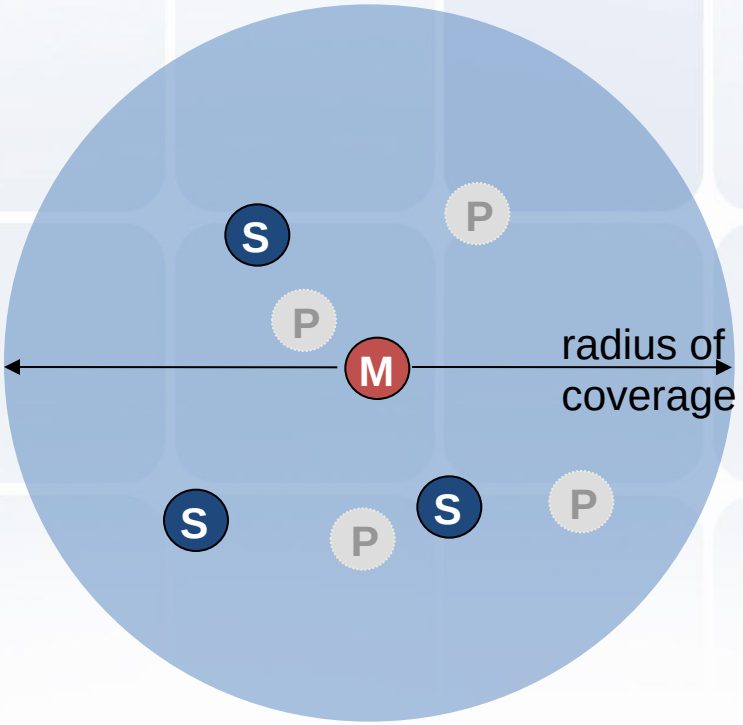
802.11: Advanced Capabilities

Power Management

- node-to-AP: "I am going to sleep until next beacon frame"
  - AP knows not to transmit frames to this node
  - node wakes up before next beacon frame
- beacon frame: contains list of mobiles with AP-to-mobile frames waiting to be sent
  - node will stay awake if AP-to-mobile frames to be sent; otherwise sleep again until next beacon frame

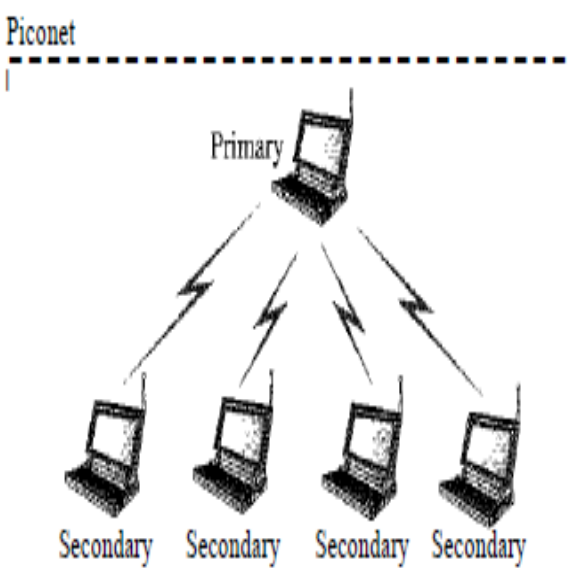
802.15: personal area network

- less than 10 m diameter
- replacement for cables (mouse, keyboard, headphones)
- ad hoc: no infrastructure
- master/slaves:
  - slaves request permission to send (to master)
  - master grants requests
- 802.15: evolved from Bluetooth specification
  - 2.4-2.5 GHz radio band
  - up to 721 kbps

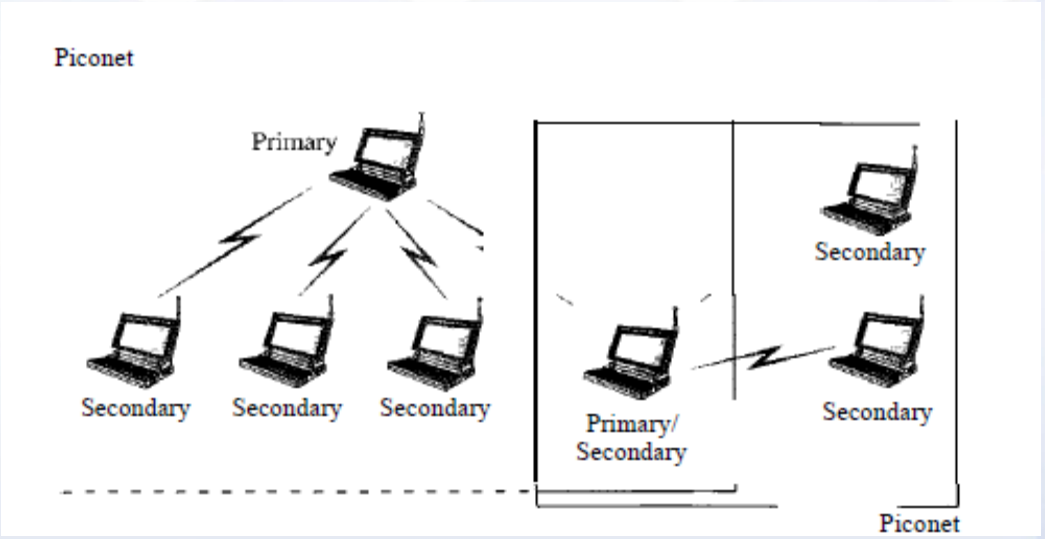


Bluetooth

- Pico net → small net (up to 8 stations)

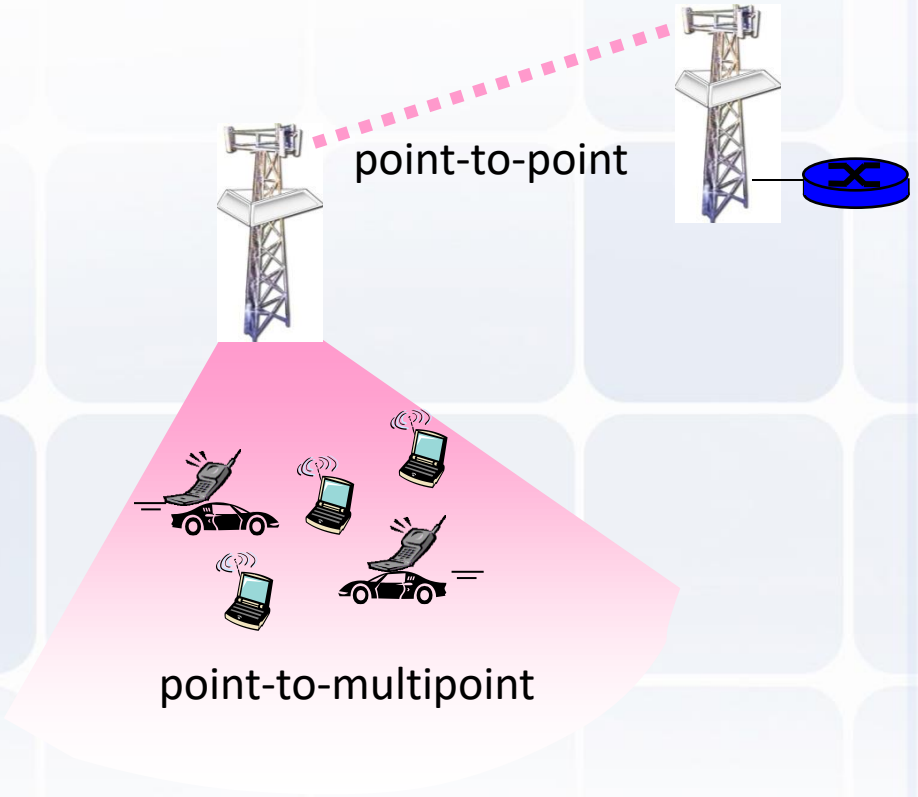


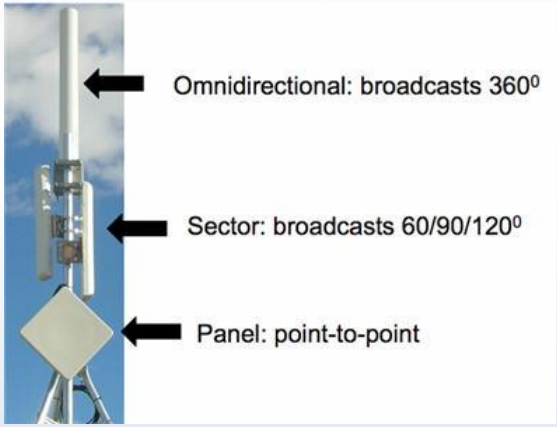
- Piconets can be combined to form what is called scatternet. A secondary station in one piconet can be the primary in another piconet.
- This station can receive messages from the primary in the first piconet (as a secondary) and, acting as a primary, deliver them to secondaries in the second piconet. A station can be a member of two piconets.



802.16: WiMAX

- like 802.11 & cellular: base station model
  - transmissions to/from base station by hosts with omnidirectional antenna
  - base station-to-base station backhaul with point-to-point antenna
- unlike 802.11:
  - range ~ 6 miles ("city rather than coffee shop")
  - ~14 Mbps





4.4 MULTIPLE ACCESS

Multiple Access

- Problem: When two or more nodes transmit at the same time, their frames will collide and the link bandwidth is wasted during collision
  - How to coordinate the access of multiple sending/receiving nodes to the shared link?
- Solution: We need a protocol to coordinate the transmission of the active nodes

Multiple Access

- These protocols are called Medium or Multiple Access Control (MAC) Protocols belong to a sublayer of the data link layer called MAC (Medium Access Control) .
- What is expected from Multiple Access Protocols:
  - Main task is to minimize collisions in order to utilize the bandwidth by:
    - Determining when a station can use the link (medium)
    - what a station should do when the link is busy
    - what the station should do when it is involved in collision

Random Access Protocol

- **Random Access Protocols:**
  - No station is superior to another station and none is assigned the control over another.
  - A station with a frame to be transmitted can use the link directly based on a procedure defined by the protocol to make a decision on whether or not to send.
- ALOHA
- CSMA
- CSMA/CD
- CSMA/CA

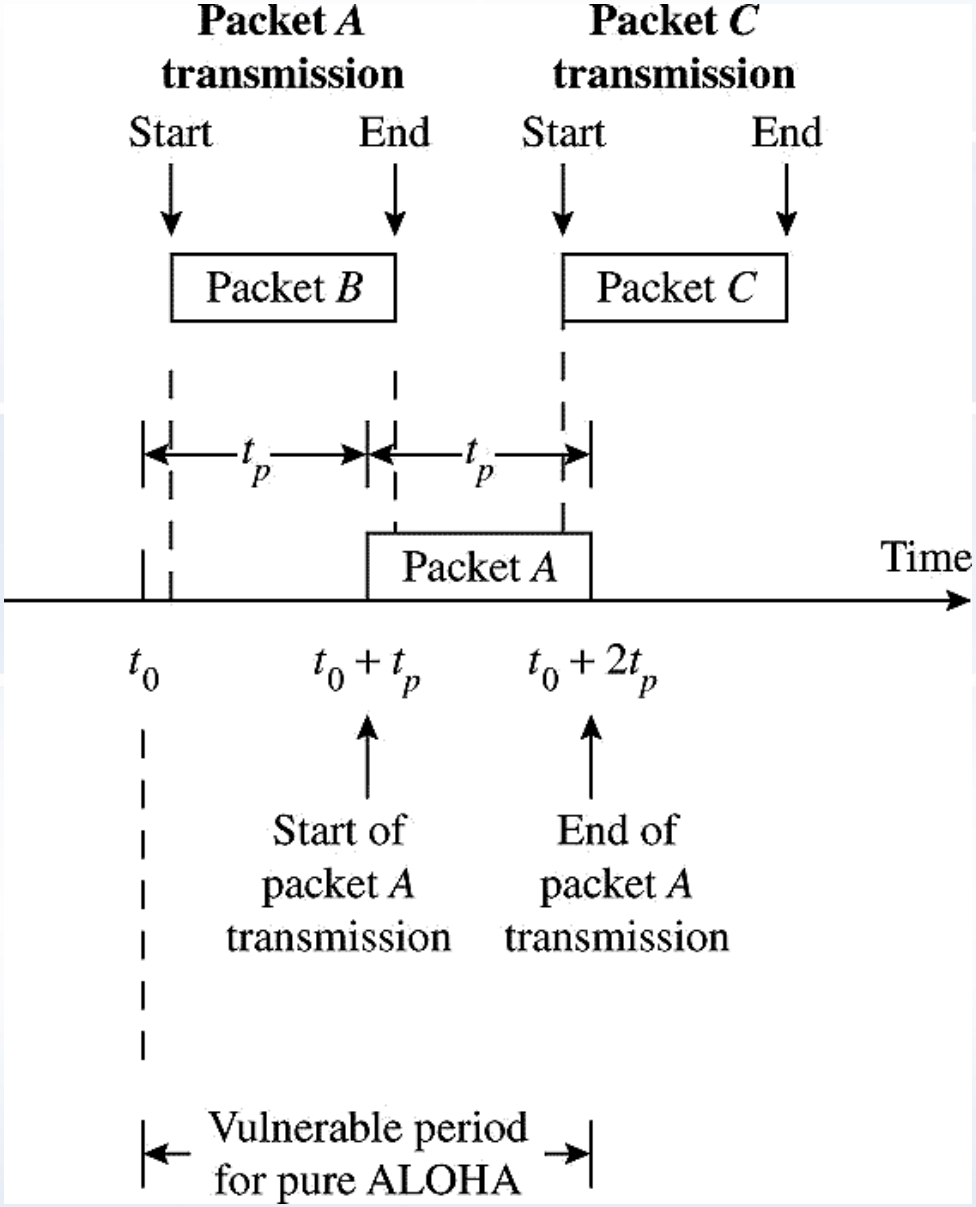
Random Access – PURE ALOHA

- All frames from any station are of fixed length (L bits)
- Stations transmit at equal transmission time (*all stations produce frames with equal frame lengths).*
- A station that has data can transmit at any time
- After transmitting a frame, the sender waits for an acknowledgment for an amount of time (time out) equal to the maximum round-trip propagation

$$delay = 2 \times t_{prop}$$

- If no ACK was received, sender assumes that the frame or ACK has been destroyed and resends that frame after it waits for a *random amount of time*
- If station fails to receive an ACK after repeated transmissions, it gives up
- Channel utilization or efficiency or Throughput is the percentage of the transmitted frames that arrive successfully (without collisions) or the percentage of the channel bandwidth that will be used for transmitting frames without collisions
- ALOHA Maximum channel utilization is 18% (i.e, if the system produces F frames/s, then 0.18 * F frames will arrive successfully on average without the need of retransmission).

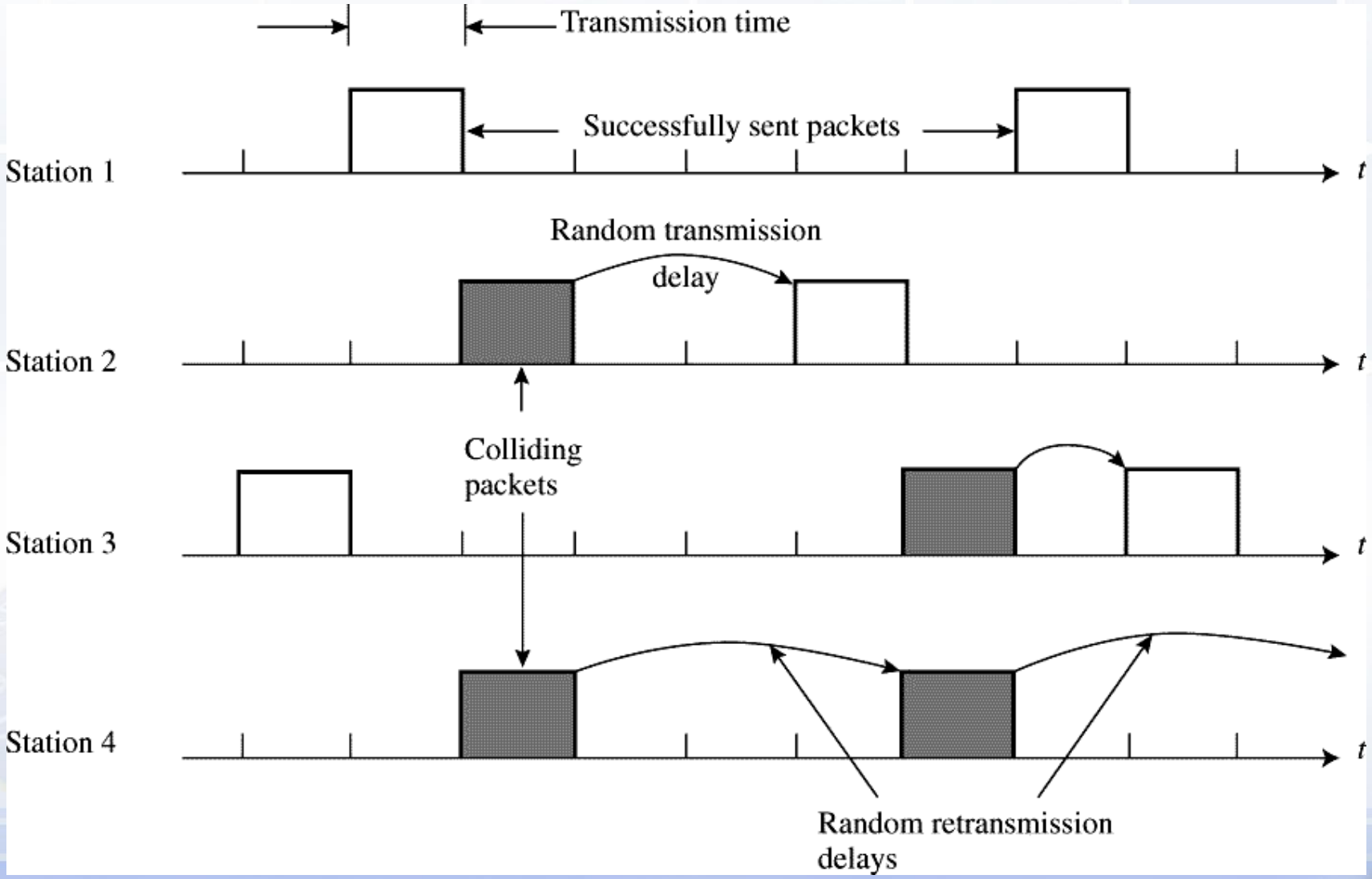
Vulnerable period in the pure ALOHA scheme



Slotted Aloha

- To increase the efficiency of the ALOHA method, the slotted ALOHA scheme was introduced.
- The channel is divided into time slots which are exactly equal to a packet transmission time. All users then are synchronized to these time slots so that whenever a user generates a packet, it must synchronize exactly with the next possible channel slot.

Transmission attempts and random retransmission delays for colliding packets in slotted ALOHA



ALOHA

- Consider an ALOHA radio network that uses a 19.2-kbps channel for sending messages and assume the message packets are 100 bits long. The system therefore is capable of transmitting at(19.2kbps) x (1packet/100bits) = 192 packets per second.
- The maximum throughput for ALOHA then is 192(0.184) ≈ 35 packets per second. For slotted ALOHA the maximum throughput is 192 (0.368) ≈ 70 packets per second.

CSMA

- Since LANs span a limited geographical area, the propagation delay between a sending and a receiving node is small compared to the packet transmission time.
- In this case when a station sends a packet, all the other stations in the network are aware of it within a fraction of the packet transmission time.
- This observation let to the development of the carrier sense multiple access (CSMA) scheme.
- In this scheme a station that wishes to transmit attempts to avoid collisions by first listening to medium to determine of another transmission is in progress.

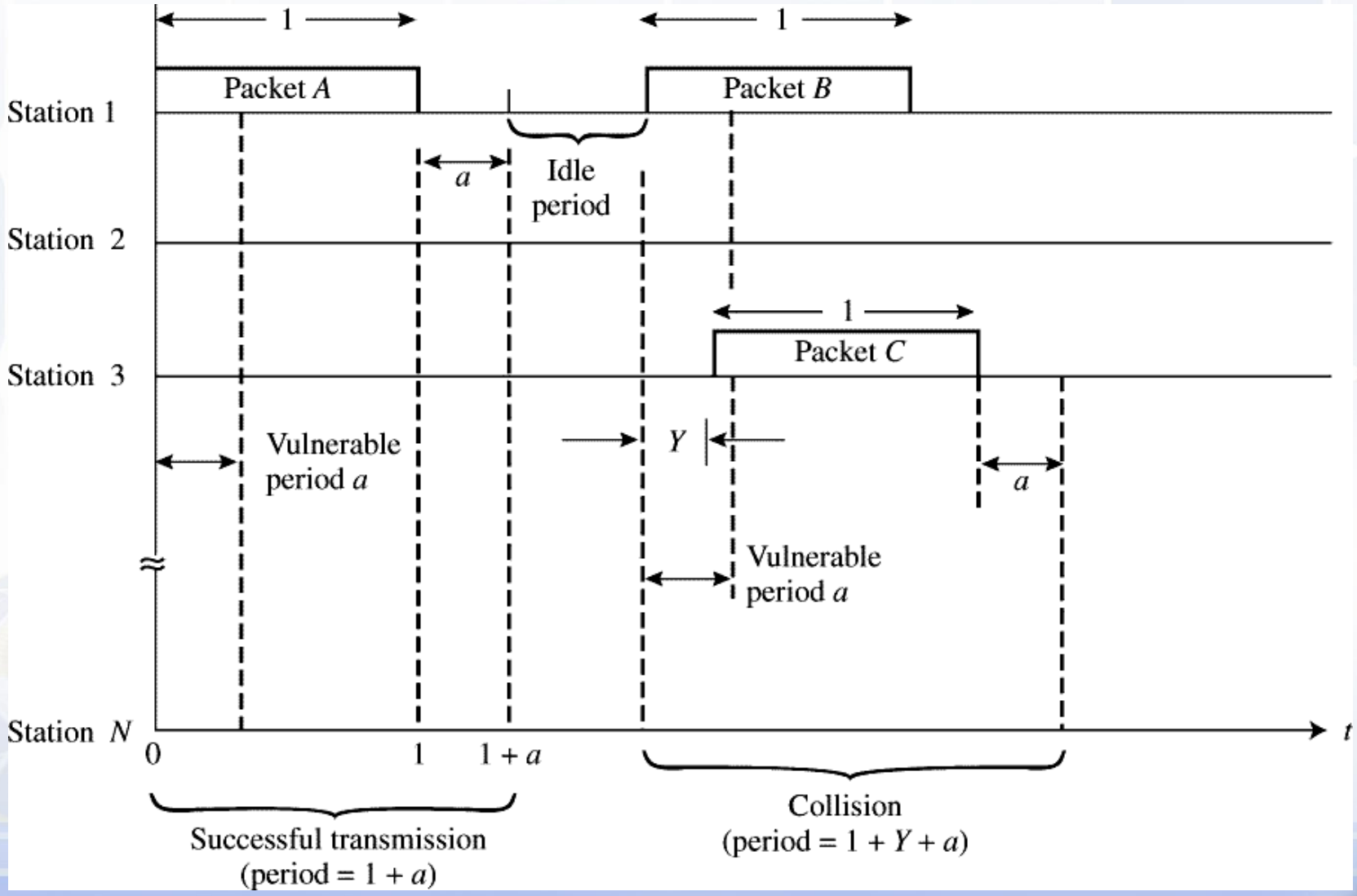
CSMA

- When the channel is sensed to be idle, a station can take one of three different approaches (depending on the network design) to insert to a packet onto the channel.
- These three protocols are known as nonpersitent CSMA , 1-*persistent* CSMA, and *p-persistent* CSMA.
- The 1-persistent protocol is a special case of the *p*-persistent scheme, but we consider it separately here.
- These protocol differ by the action that a station with a packet to transmit takes after sensing the readiness state of the channel.
- When a station notes that transmission was unsuccessful, in each protocol the rescheduling of the packet transmission in the same. In the reschedulings the packet is sent again according to a randomly distributed retransmission delay.

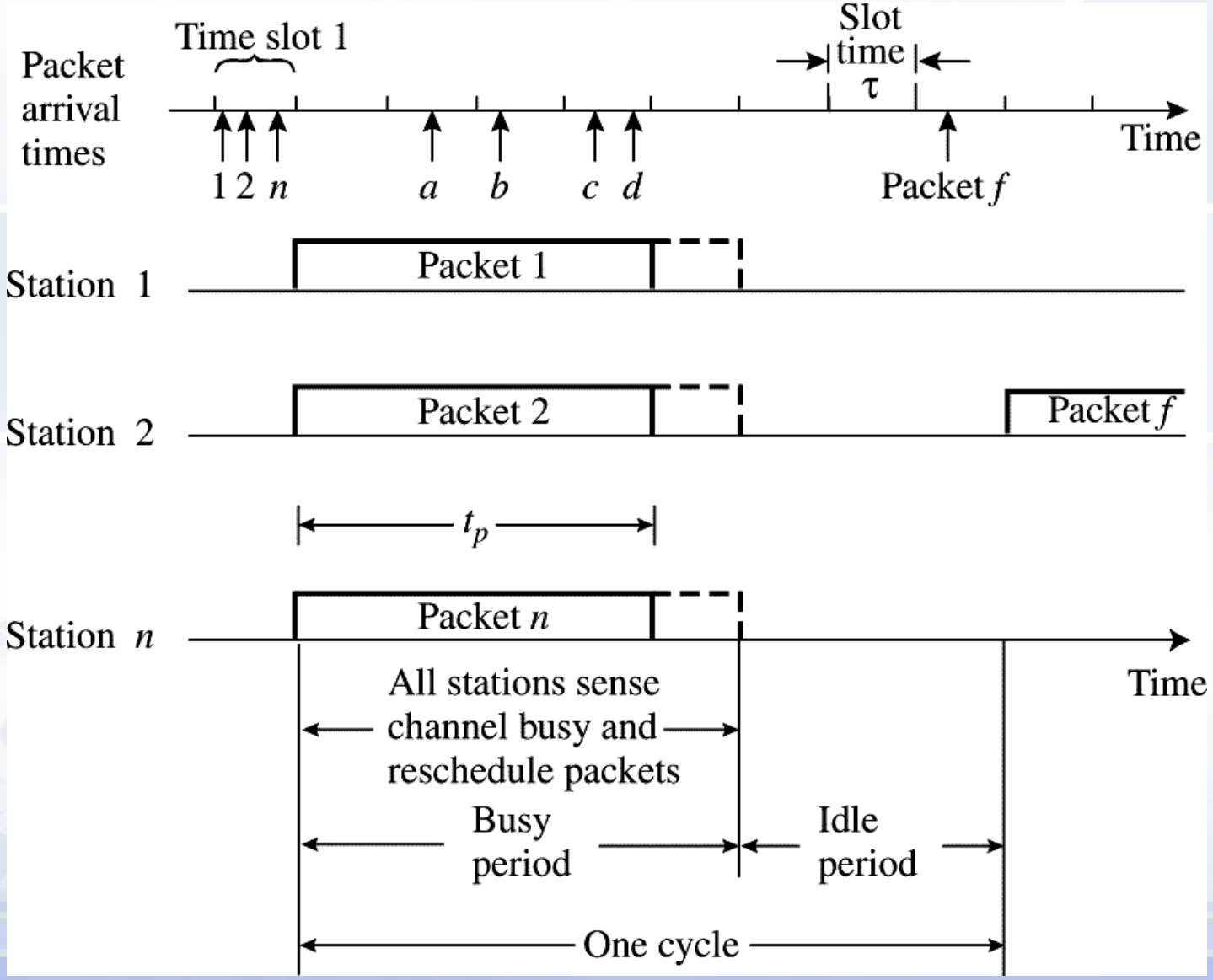
CSMA

CSMA Protocol	Characteristics
Nonpersistent	If medium is idle, transmit. If medium is busy, wait random amount of time and the resense channel.
1-persistent	If medium is idle, transmit. If medium is busy, continue listening until channel is idle ; Than transmit immediately.
P-persistent	If medium is idle, transmit with probability *p*. If medium is busy, continue listening until channel is idle ; Then transmit with probability *p*.

Successful and unsuccessful transmission attempts for nonpersistent CSMA



Packet Arrivals in Slotted Nonpersistent CSMA



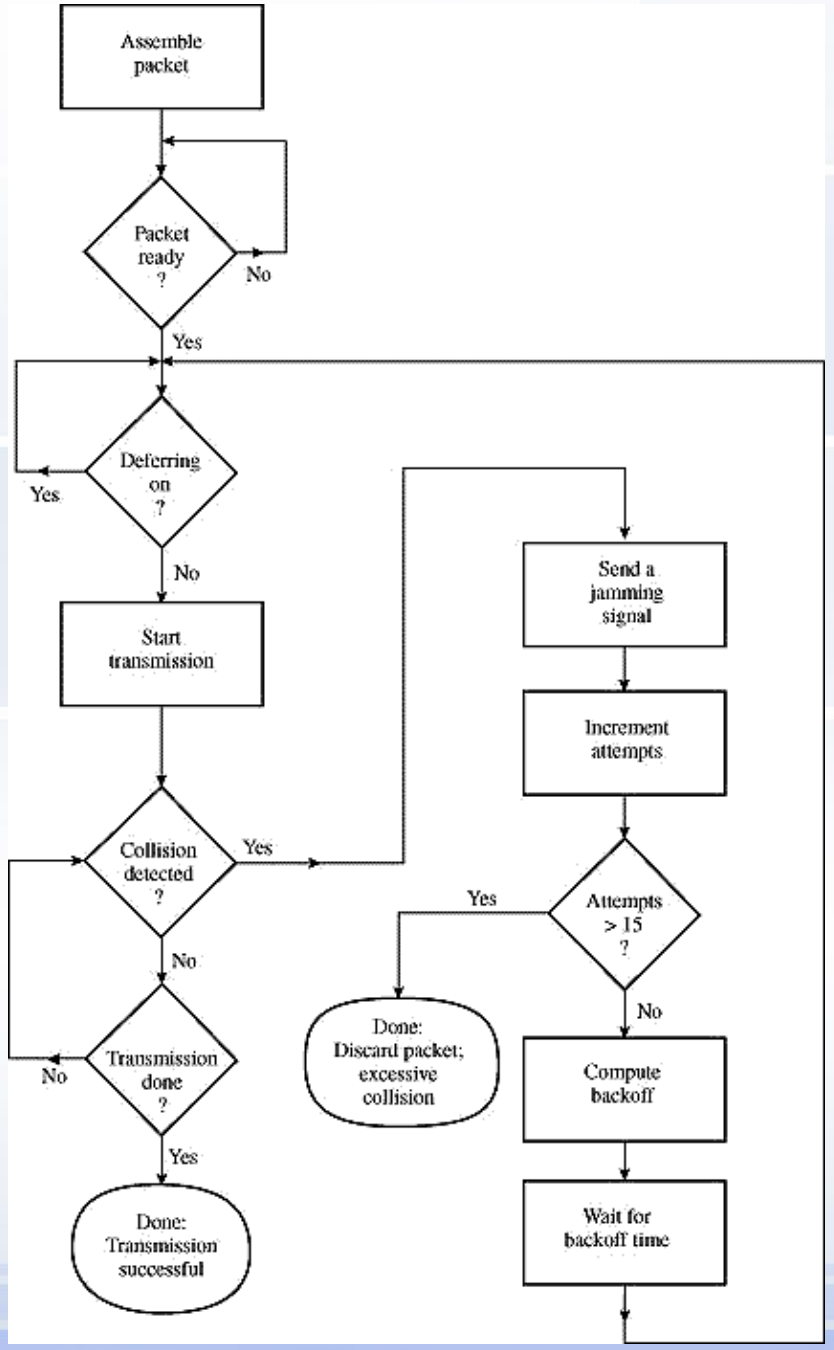
CSMA/CD

- One key feature of the CSMA/CD protocol is a deference mechanism. Even when there is no packet waiting to be transmitted, the CSMA/CD MAC sublayer monitors the physical medium for traffic.
- When the station becomes ready to transmit, the behavior of the deference mechanism depends on which protocol variation is used.
- In particular, if the channel is idle, one of the following actions is taken:
  - The packet transmitted if nonpersistent or 1-persistent CSMA/CD is used
  - For p-persistent CSMA/CD the packet is sent with probability p or is delayed by the propoagation delay with probability (1-p).

CSMA/CD

- If the channel is busy :
  - The packet is backed off and the algorithm is repeated for the nonpersistent case.
  - The station defers transmission until the channel is sensed to be idle and then immediately transmits in the 1-persistent case.
  - For the p-persistent protovol the station defers until the channel is idle and then follow the idle channel procedure.

Flow diagram for the CSMA/CD protocol



THE END