CSCI 251
Systems and Networks

Medium Access Control Sublayer

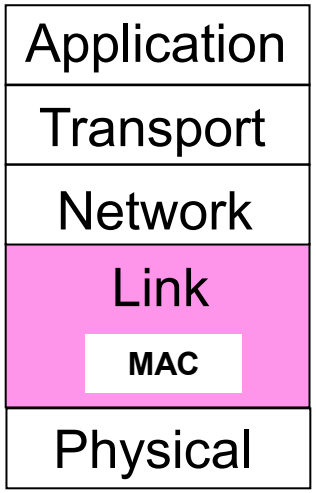
Humayun Kabir
Professor, CS, Vancouver Island University, BC, Canada

Outline

- Channel Allocation Problem
- Multiple Access Protocols
  - Pure and Slotted ALOHA
  - Carrier Sense Multiple Access (CSMA)
  - CSMA with Collision Detection (CSMA/CD)
  - Binary Exponential Backoff Algorithm
- Ethernet
- Wireless
  - CSMA with Collision Avoidance (CSMA/CA)
  - WiFi(IEEE 801.11)

The MAC Sublayer

- Multiple Access Control (MAC) sublayer is part of Data Link Layer
- It is responsible for deciding who sends next on a multi-access link



Channel Allocation Problem

For constant traffic from a fixed number (N) of users

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

This static allocation performs poorly for traffic that comes at burst

- Allocation to a user will sometimes go unused

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

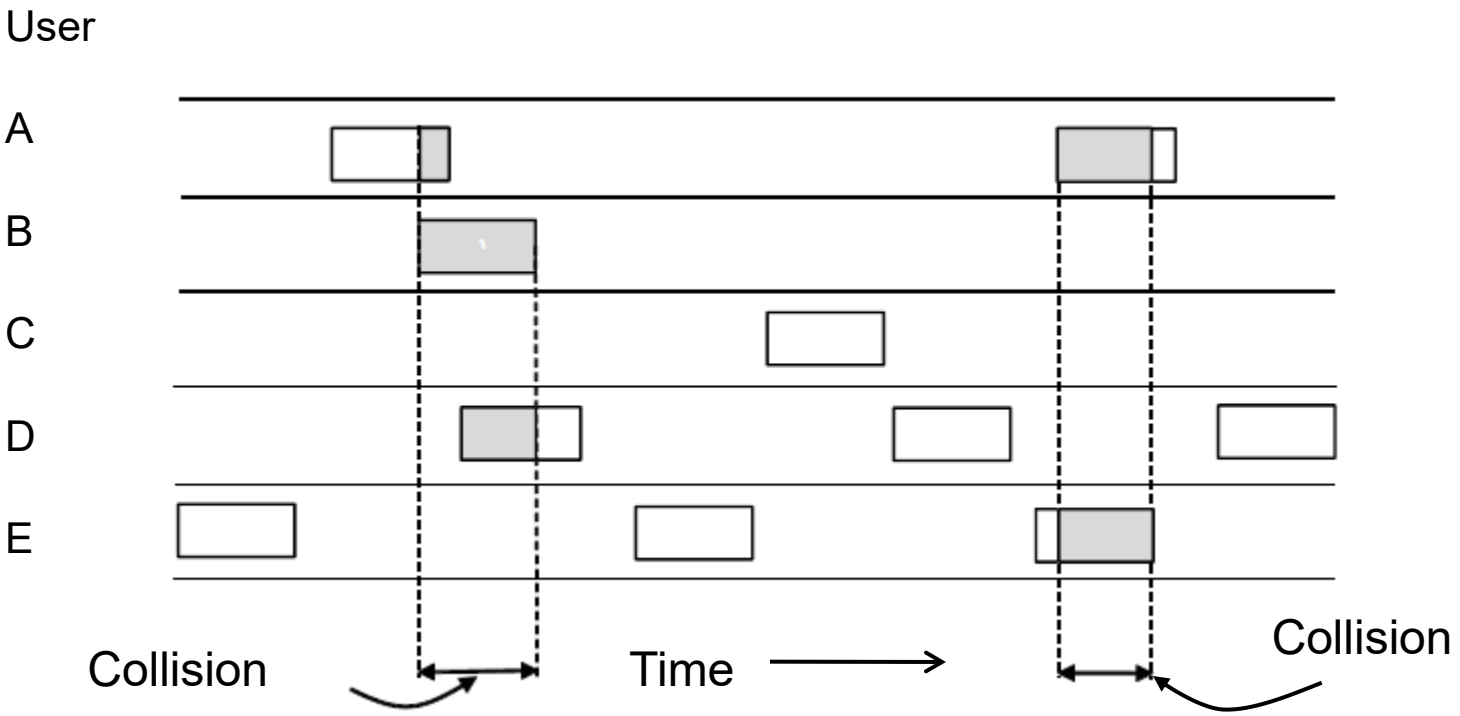
Multiple Access Protocols

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

ALOHA

In pure ALOHA, users transmit frames whenever they have data; users retry after a random time if collision occurs

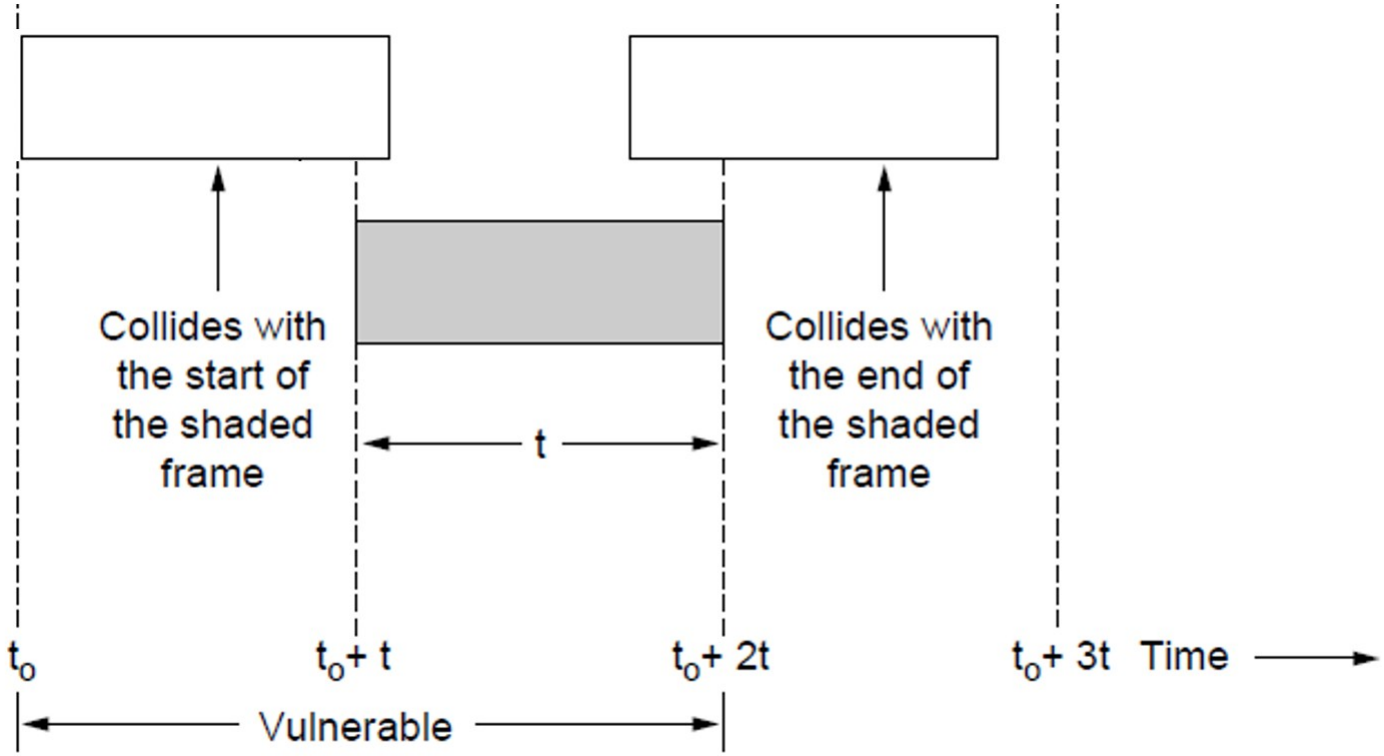
- Efficient and low-delay under low load



ALOHA

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

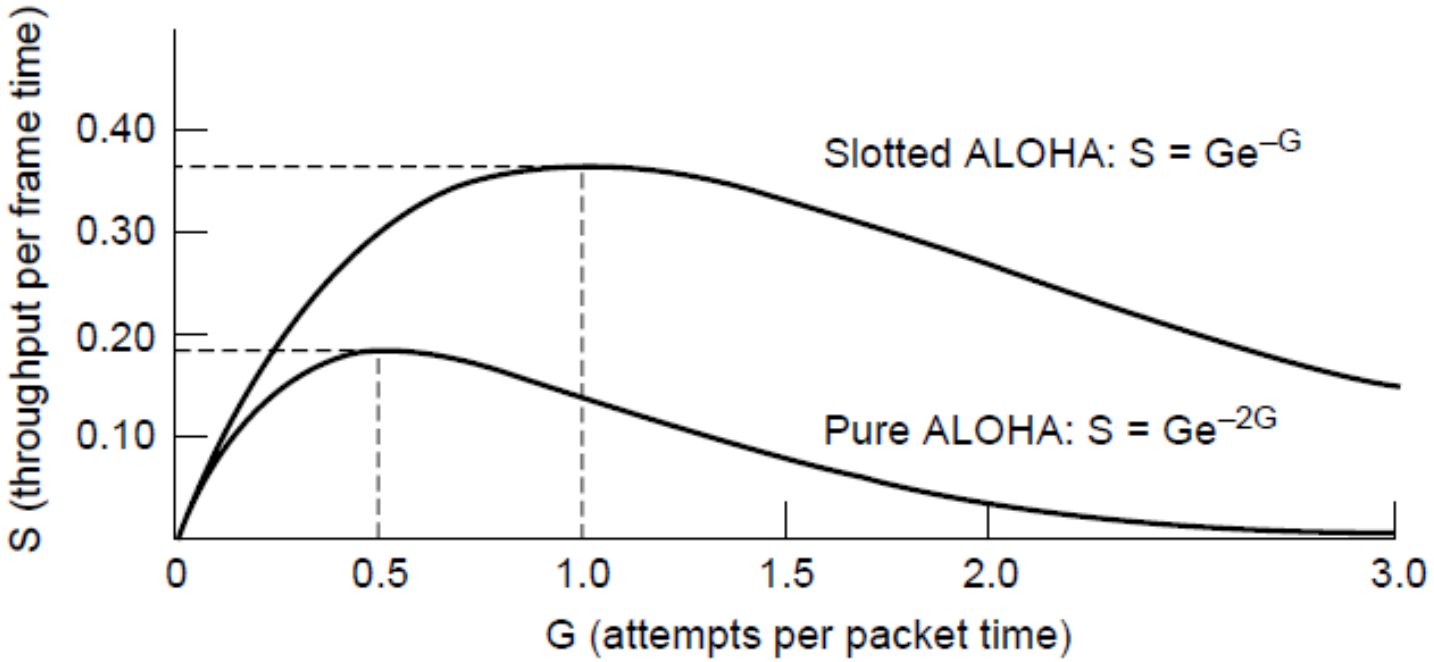
- Synchronizing senders to slots can reduce collisions



ALOHA

Slotted ALOHA is twice as efficient as pure ALOHA

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



CSMA

CSMA improves on ALOHA by sensing the channel!

- User doesn't send if it senses someone else

Variations on what to do if the channel is busy:

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

1-persistent CSMA

- When a station has data to send it persistently senses the channel and transmits the frame as soon as it gets the channel idle.
- Waits for a random time if collision occurs and starts sensing again.
- If two stations are sensing while a third station is transmitting both will seize the idle channel at the same time and collide.

Non-persistent CSMA

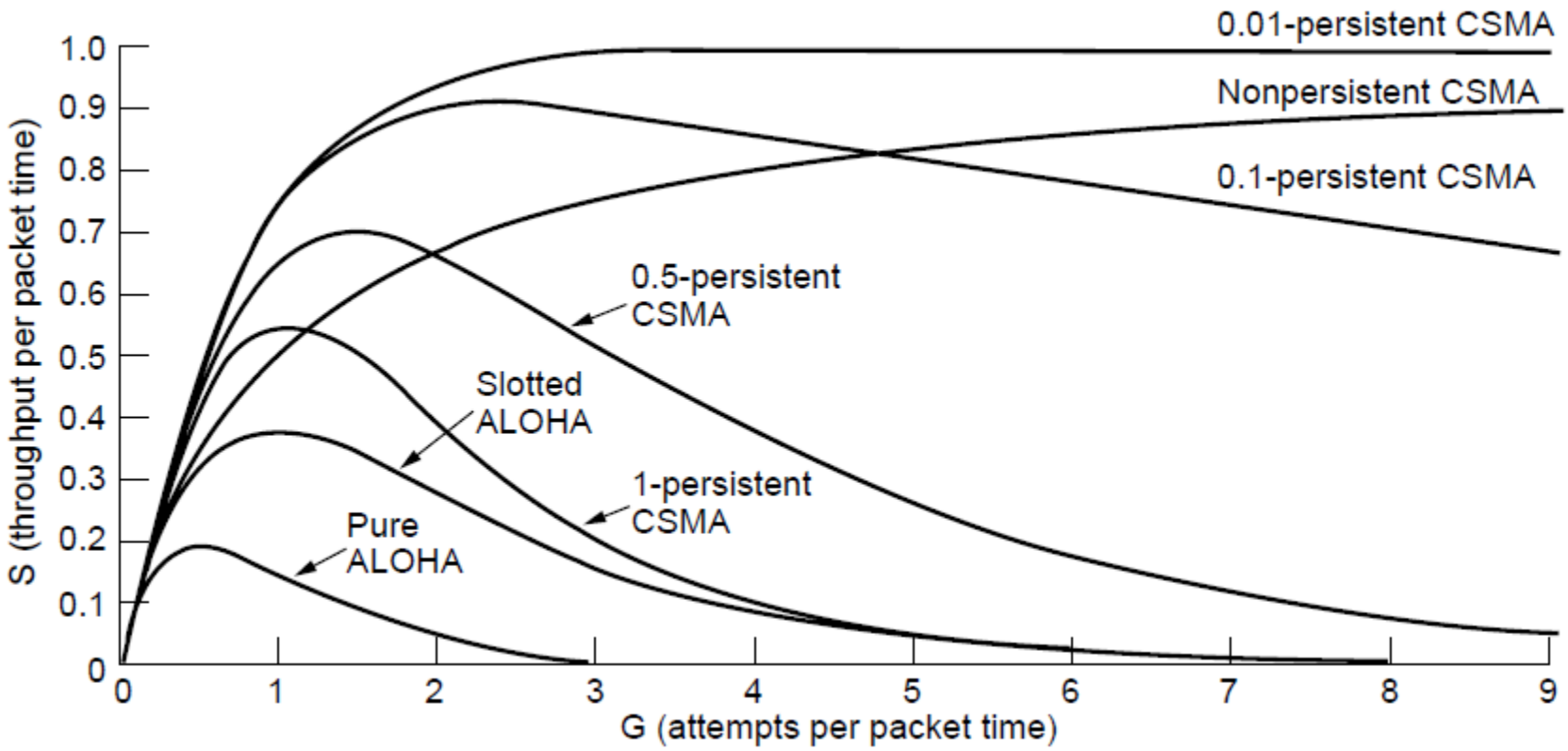
- When a station has data to send it senses the channel as before and transmits the frame if the channel is idle.
- Does not continue sensing if the channel is busy. Waits for a random time and starts over again.
- If collision occurs, waits for random time and starts sensing again.
- If two stations are sensing while a third station is transmitting both will not come back at the same time to seize the idle channel, i.e., less collision.

P-persistent CSMA

- Uses **slotted** channel.
- When a station has data to send it senses the channel as before.
- If the channel is busy, it waits until the beginning of the next slot for sensing.
- If the channel is idle it transmits the frame with probability ***p*** or defers until the next slot with probability ***q*** = 1- ***p***.
- If the channel is idle in the next slot it transmits the frame with probability ***p*** or defers until the next slot with the probability ***q*** again.
- If the channel is busy in the next slot or a collision occurs it waits for a random time to start over again

CSMA– Persistence

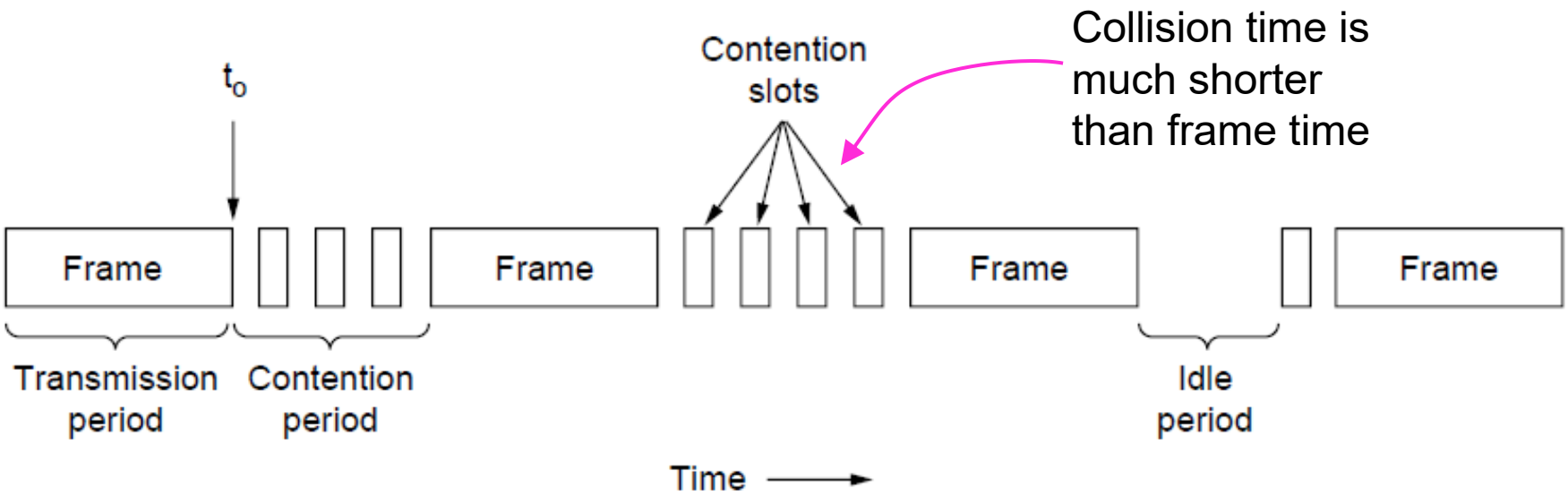
CSMA outperforms ALOHA, and being less persistent is better under high load



CSMA – Collision Detection

CSMA/CD improvement is to **detect collisions** and **abort transmissions** immediately after the detection.

- Without CD contention times are equal to frame transmission times
- With CD contention times are much shorter, i.e., improve performance



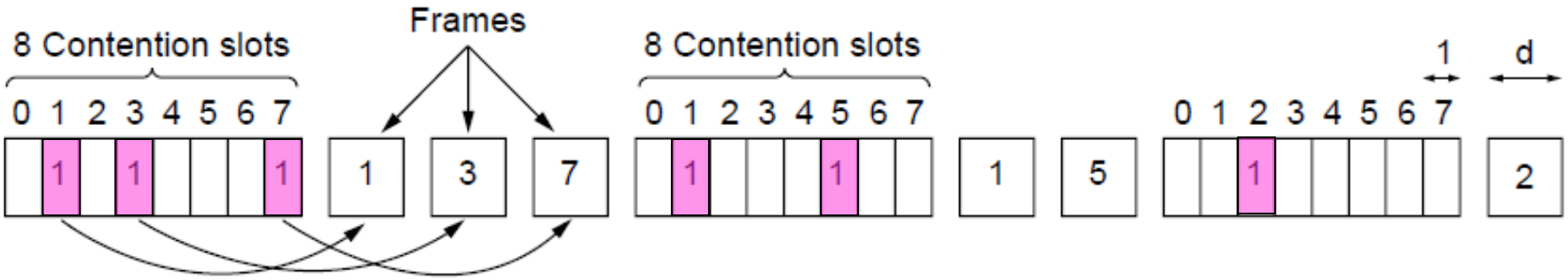
Collision-Free – Bitmap

Collision-free protocols avoid collisions entirely

- Senders must know when it is their turn to send

The basic bit-map protocol:

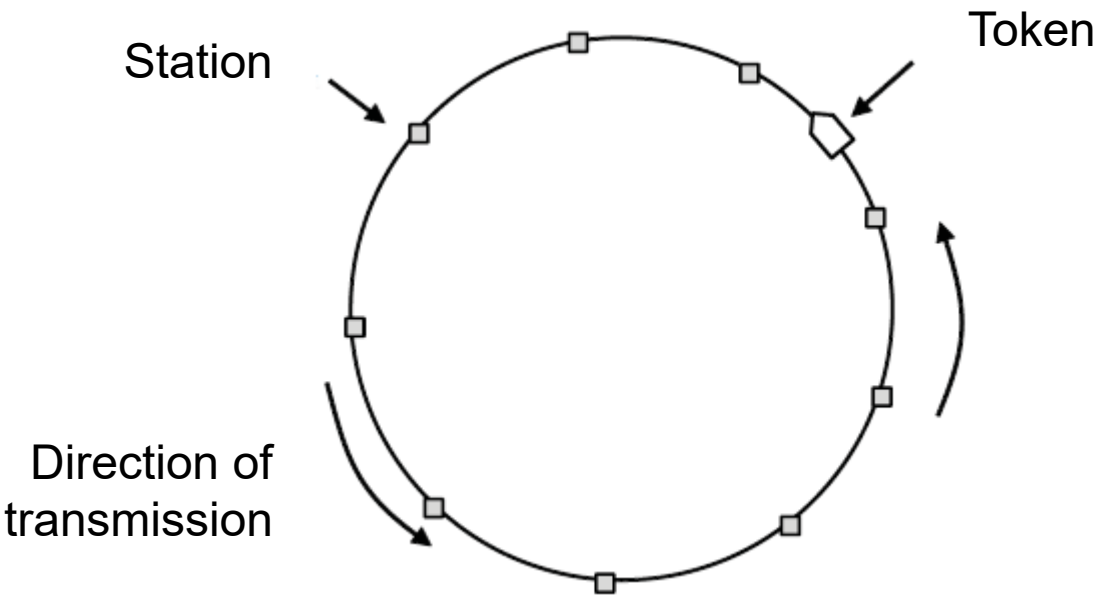
- Sender set a bit in contention slot if they have data
- Senders send in turn; everyone knows who has data



Collision-Free – Token Ring

Token sent round ring defines the sending order

- Station without data passes the token.
- Station with data seizes the token and sends a frame.
- Station with token passes the token after completing its frame transmission.
- Idea can be used without ring too, e.g., token bus



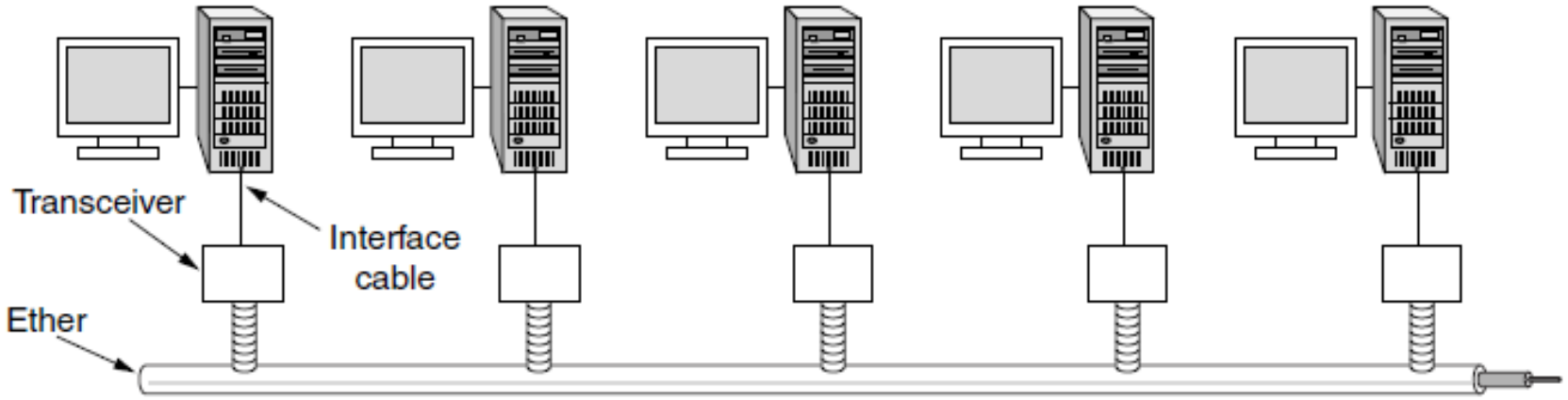
Ethernet

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

Classic Ethernet – Physical Layer

One shared coaxial cable to which all hosts attached

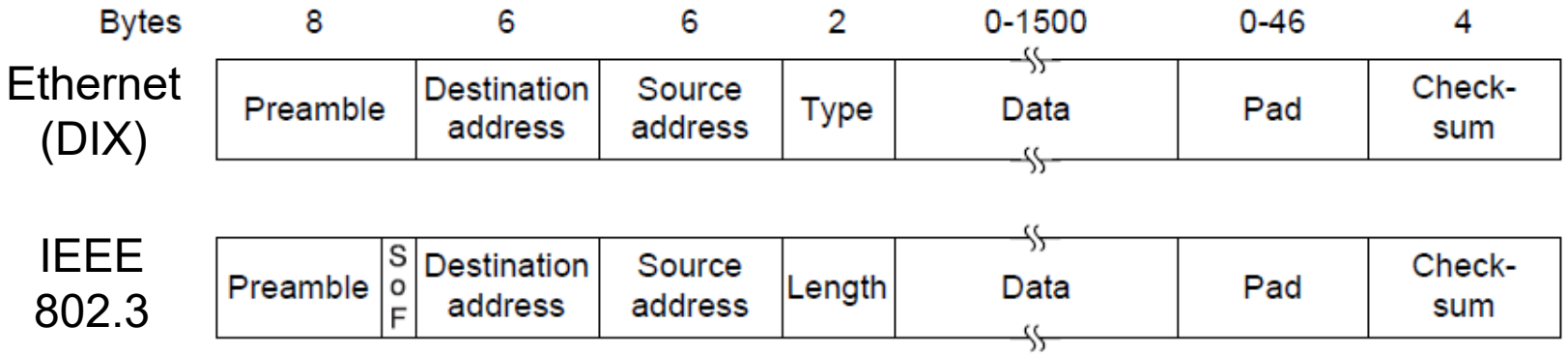
- Up to 10 Mbps, with Manchester encoding
- Hosts ran the classic Ethernet protocol for access



Classic Ethernet – MAC

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

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



Classic Ethernet – MAC

8 Byte Preamble

10101010	10101010	10101010	10101010	10101010	10101010	10101010	10101011
							SoF

6 Byte Destination Address

Unicast address	0xxxxxxx	xxxxxxxx	xxxxxxxx	xxxxxxxx	xxxxxxxx	xxxxxxxx
Multicast address	1xxxxxxx	xxxxxxxx	xxxxxxxx	xxxxxxxx	xxxxxxxx	xxxxxxxx
Broadcast address	11111111	11111111	11111111	11111111	11111111	11111111

6 Byte Source Address (world wide unique)

xxxxxxxx	xxxxxxxx	xxxxxxxx	xxxxxxxx	xxxxxxxx	xxxxxxxx
Organizationally Unique Identifier			Manufacturer Assigned Number		

Classic Ethernet – MAC

2 Byte **Type** or **Length**

xxxxxxxx	**xxxxxxxx**

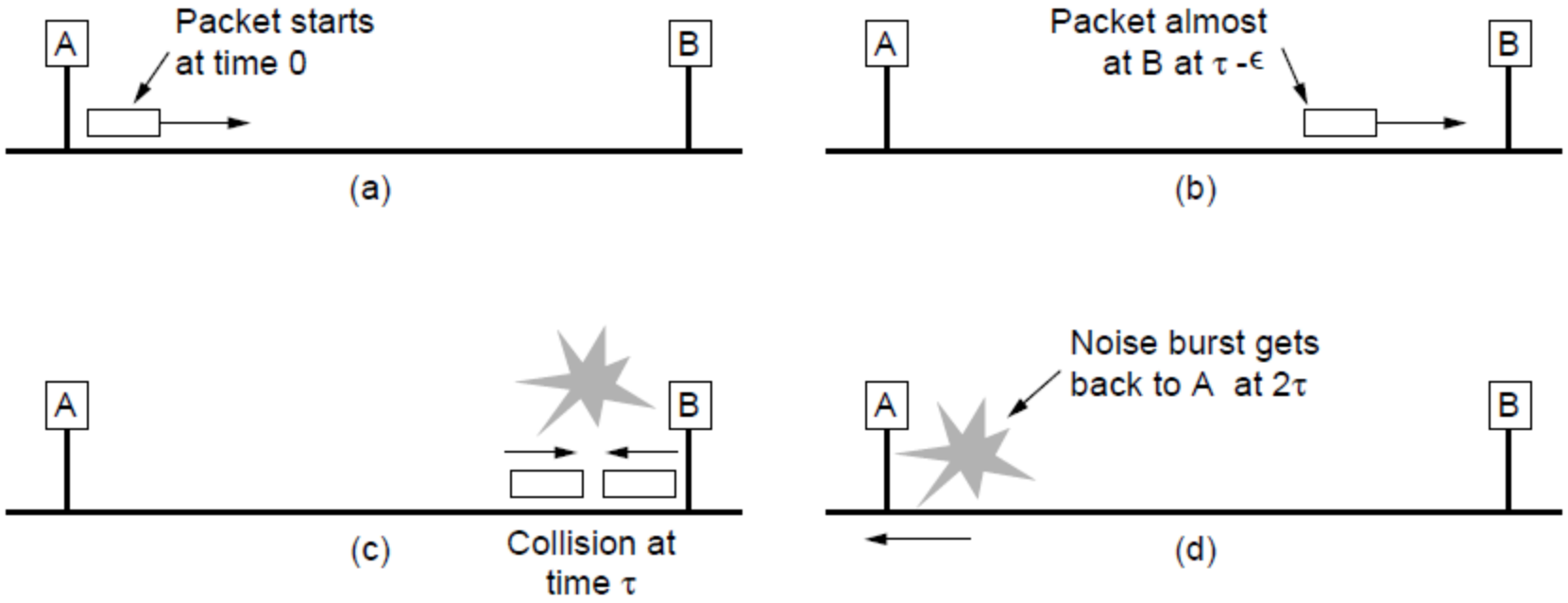
- Indicates the type of the upper layer protocol, e.g., value 0x0800 indicates IPv4
- Value less than or equal to **0x600** or 1536 is treated as **Length** of the Ethernet frame. In this case, 2 byte **Type** field in Logical Link Control (**LLC**) layer will determine the type of the upper layer protocol

Maximum Length of an **Ethernet** frame is chosen **1500 bytes** to ensure 1500 bytes RAM in the network card will be sufficient.

Classic Ethernet – MAC

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

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



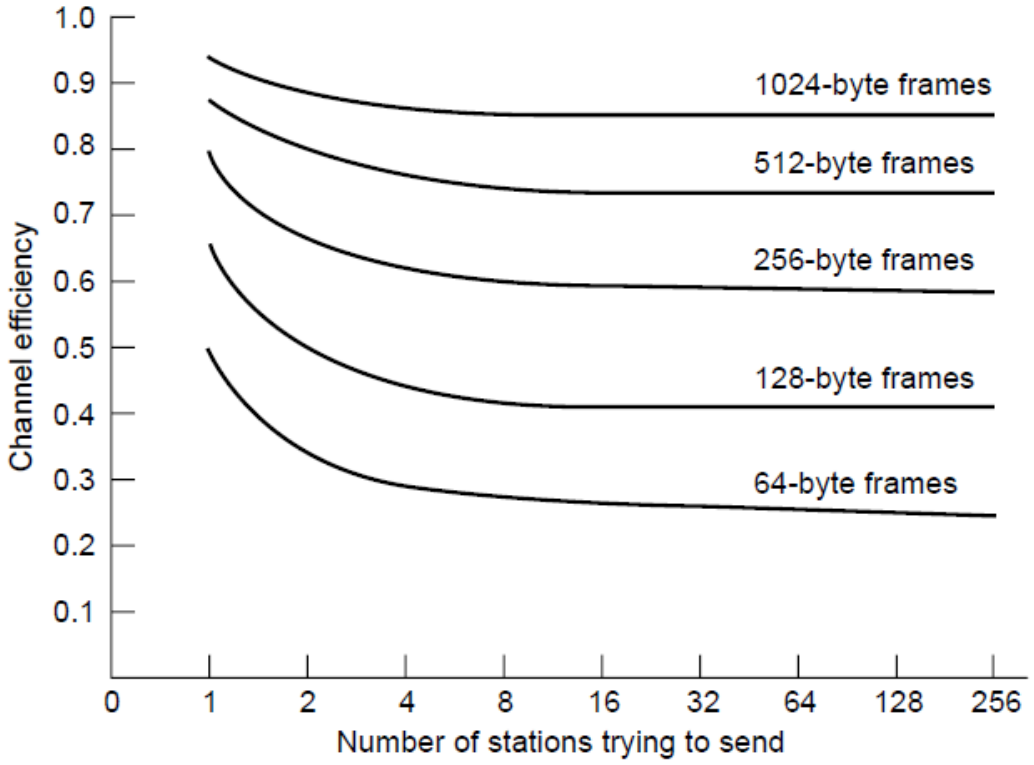
Classic Ethernet – MAC

- **Minimum Length** of an Ethernet frame is chosen **64 bytes** considering 2500 meters long and 10Mbps link (worst case round-trip propagation time is 50 micro seconds)
- 0 to 46 (64-18) bytes **padding** is required to ensure 64 bytes minimum length.
- 2 bytes **Checksum** is CRC computed on Ethernet frame using a 32-bit generator polynomial.

Classic Ethernet – Performance

Efficient for large frames, even with many senders

- Degrades for small frames (and long LANs)



10 Mbps Ethernet,
64 byte min. frame

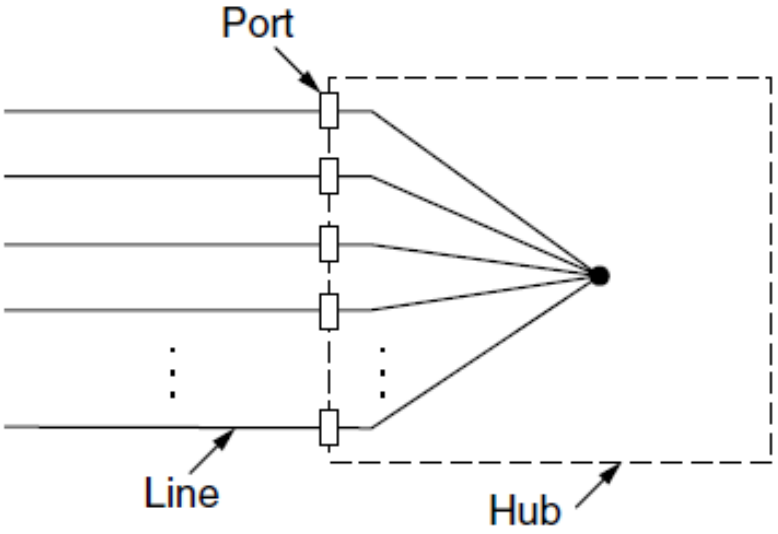
Classic Ethernet – MAC

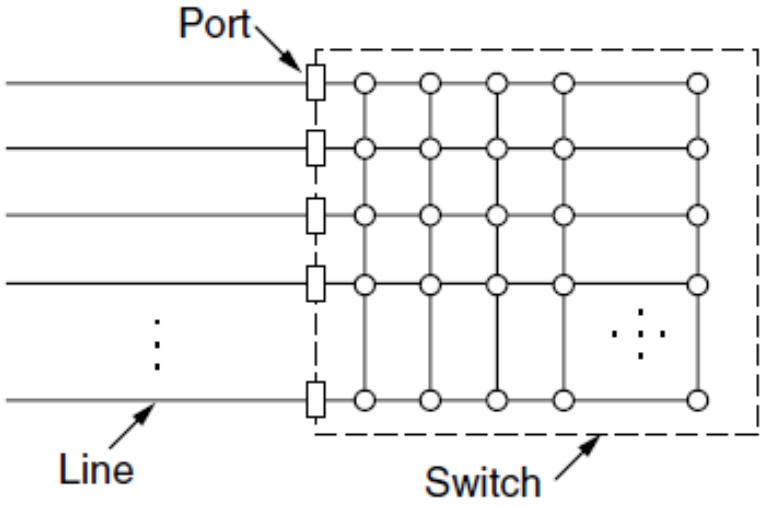
Binary Exponential Backoff for random waiting after each collision

- Time is divided into 51.2 micro second slots.
- After 1st collision station waits either 0 or 1 time slot.
- After 2nd collision station waits either 0,1,2, or 3 time slots in random.
- After 3rd collision station waits either 0,1,2,3,4,5,6, or 7 time slots in random.
- After n^{th} collision station waits either 0,1,2,3, …….$(2^n - 1)$ time slots in random.
- After 10th collision the randomization interval is frozen at a maximum of 1023 slots.
- After 16th collision station gives up.

Switched/Fast Ethernet

- Hubs wire all lines into a single CSMA/CD domain
- Switches isolate each port to a separate domain
  - Much greater throughput for multiple ports
  - No need for CSMA/CD with full-duplex lines

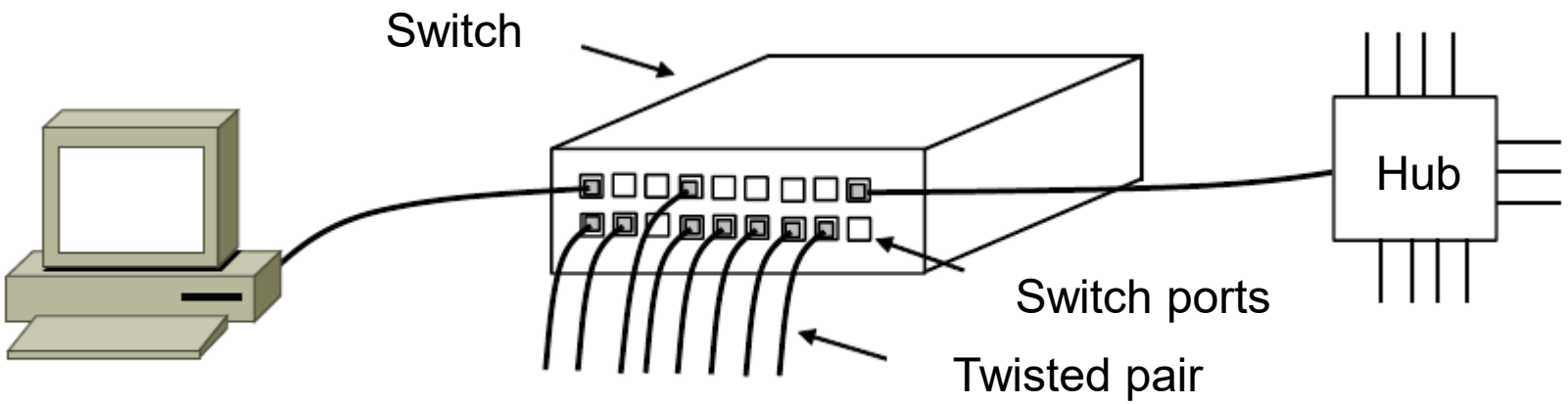




Switched/Fast Ethernet

Switches can be wired to computers, hubs and switches

- Hubs concentrate traffic from computers
- Switch does not concentrate frames but switches frames from source to destination.
- How to switch frames?



Switched/Fast Ethernet

Fast Ethernet extended Ethernet from 10 to 100 Mbps

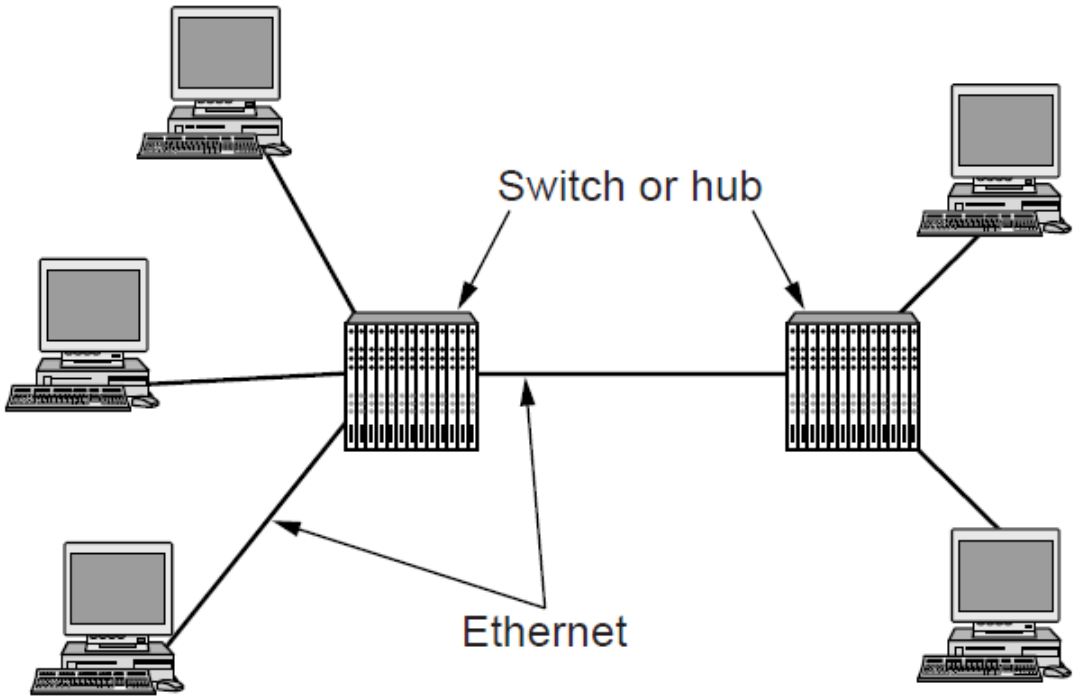
- Twisted pair (with Cat 5) dominated the market

Name	Cable	Max. segment	Advantages
100Base-T4	Twisted pair	100 m	Uses category 3 UTP
100Base-TX	Twisted pair	100 m	Full duplex at 100 Mbps (Cat 5 UTP)
100Base-FX	Fiber optics	2000 m	Full duplex at 100 Mbps; long runs

1 Gigabit / 10 Gigabit Ethernet

Switched Gigabit Ethernet is now the garden variety

- With full-duplex lines between computers/switches



1Gigabit / 10 Gigabit Ethernet

- 1 Gigabit Ethernet is commonly run over twisted pair

Name	Cable	Max. segment	Advantages
1000Base-SX	Fiber optics	550 m	Multimode fiber (50, 62.5 microns)
1000Base-LX	Fiber optics	5000 m	Single (10 μ) or multimode (50, 62.5 μ)
1000Base-CX	2 Pairs of STP	25 m	Shielded twisted pair
1000Base-T	4 Pairs of UTP	100 m	Standard category 5 UTP

- 10 Gigabit Ethernet is being deployed where needed

Name	Cable	Max. segment	Advantages
10GBase-SR	Fiber optics	Up to 300 m	Multimode fiber (0.85μ)
10GBase-LR	Fiber optics	10 km	Single-mode fiber (1.3μ)
10GBase-ER	Fiber optics	40 km	Single-mode fiber (1.5μ)
10GBase-CX4	4 Pairs of twinax	15 m	Twinaxial copper
10GBase-T	4 Pairs of UTP	100 m	Category 6a UTP

- 40/100 Gigabit Ethernet is under development

Wireless LAN Protocols

Wireless has complications compared to wired.

Nodes may have different coverage regions

- Leads to hidden and exposed terminals

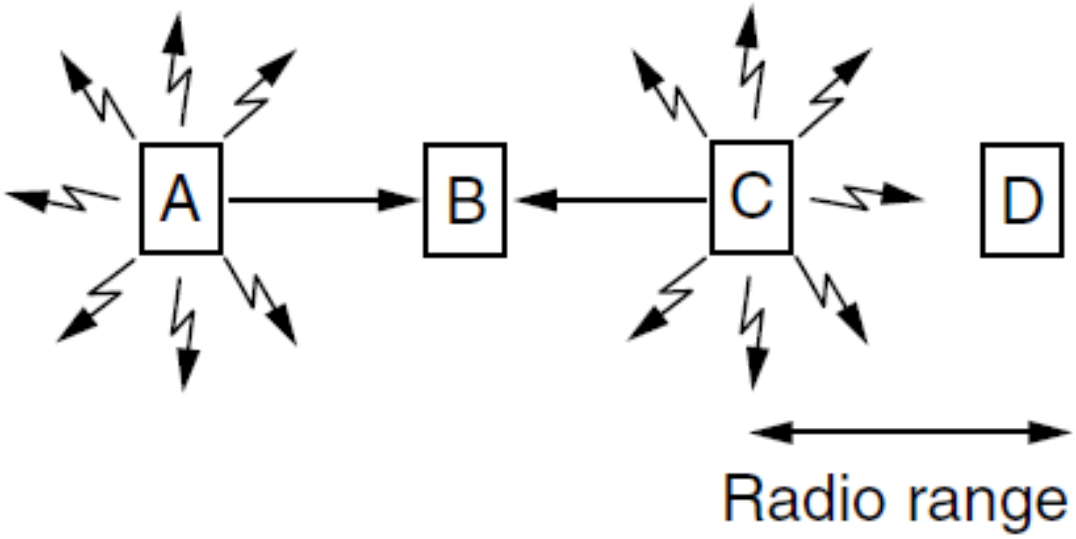
Nodes can't sense while sending, i.e., no collision detection

- Makes collisions expensive that must be avoided
- Does not transmit frames right away after getting the channel idle
- Uses backoff slots to avoid collisions.

Wireless LANs – Hidden terminals

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

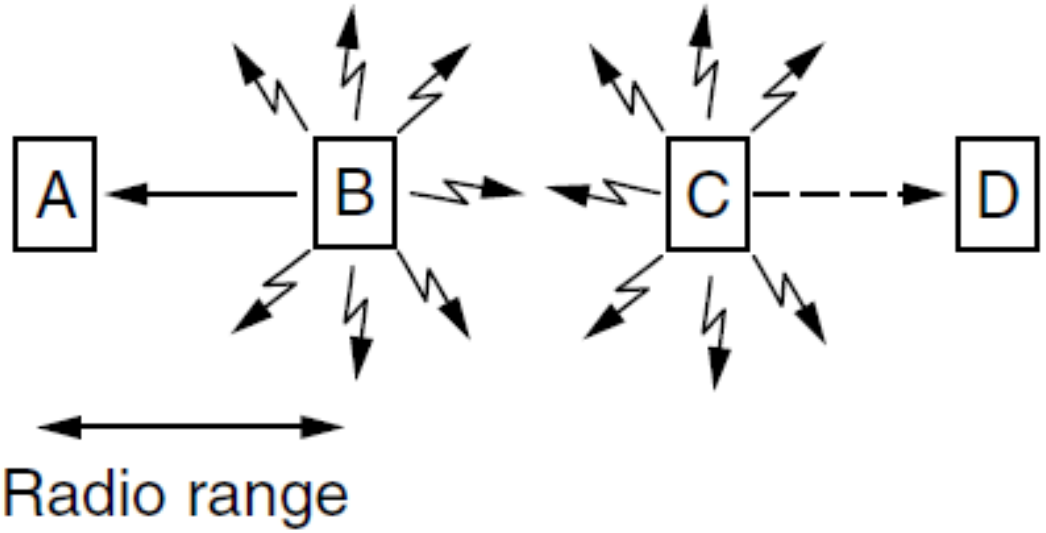
- Want to prevent; loss of efficiency
- A and C are hidden terminals to each other when sending to B



Wireless LANs – Exposed terminals

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

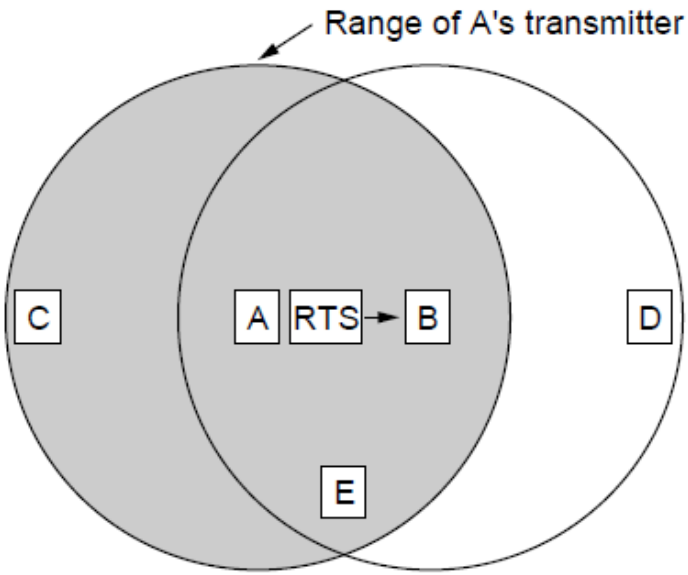
- Desirably concurrency; improves performance
- B and C are exposed terminals that prevents B → A and C → D transmissions

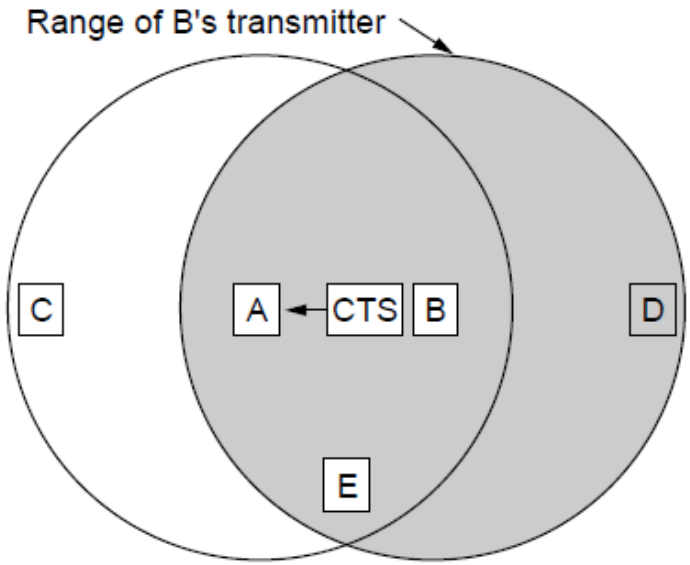


Wireless LANs – MACA

MACA protocol grants access for A to send to B:

- A sends RTS to B; C and E hear and defer for CTS
- B replies with CTS; D and E hear and defer for data
- A sends data to B hearing CTS from it





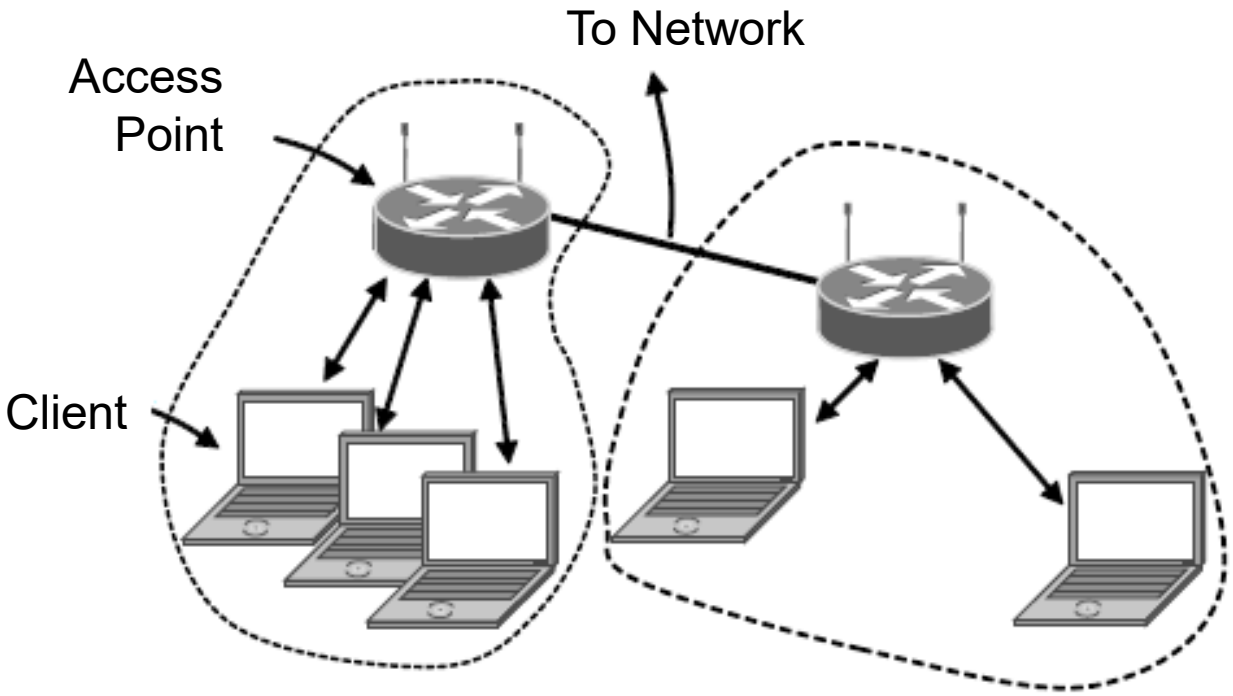
Wireless LANs

- 802.11 architecture/protocol stack »
- 802.11 physical layer »
- 802.11 MAC »
- 802.11 frames »

802.11 Architecture/Protocol Stack

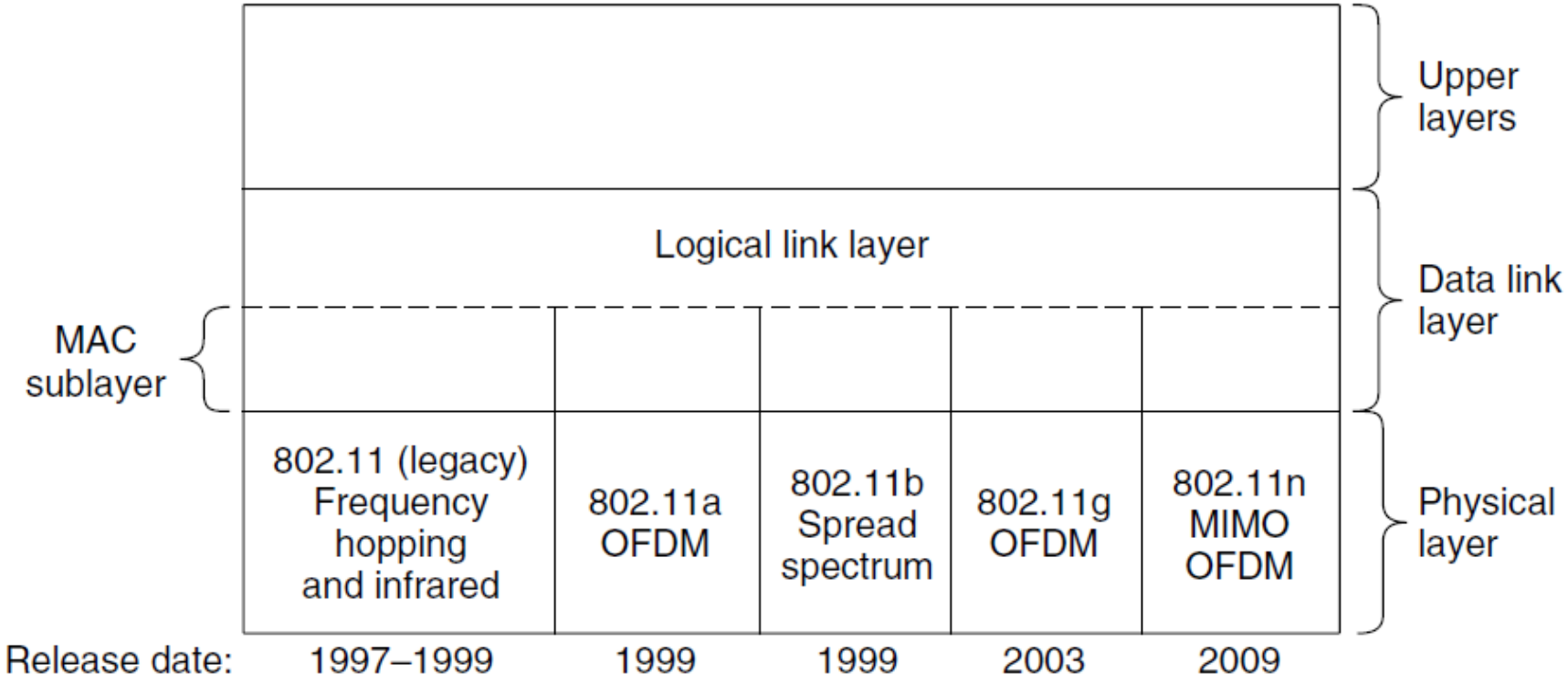
Wireless clients associate to a wired AP (Access Point)

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



802.11 Architecture/Protocol Stack

MAC is used across different physical layers



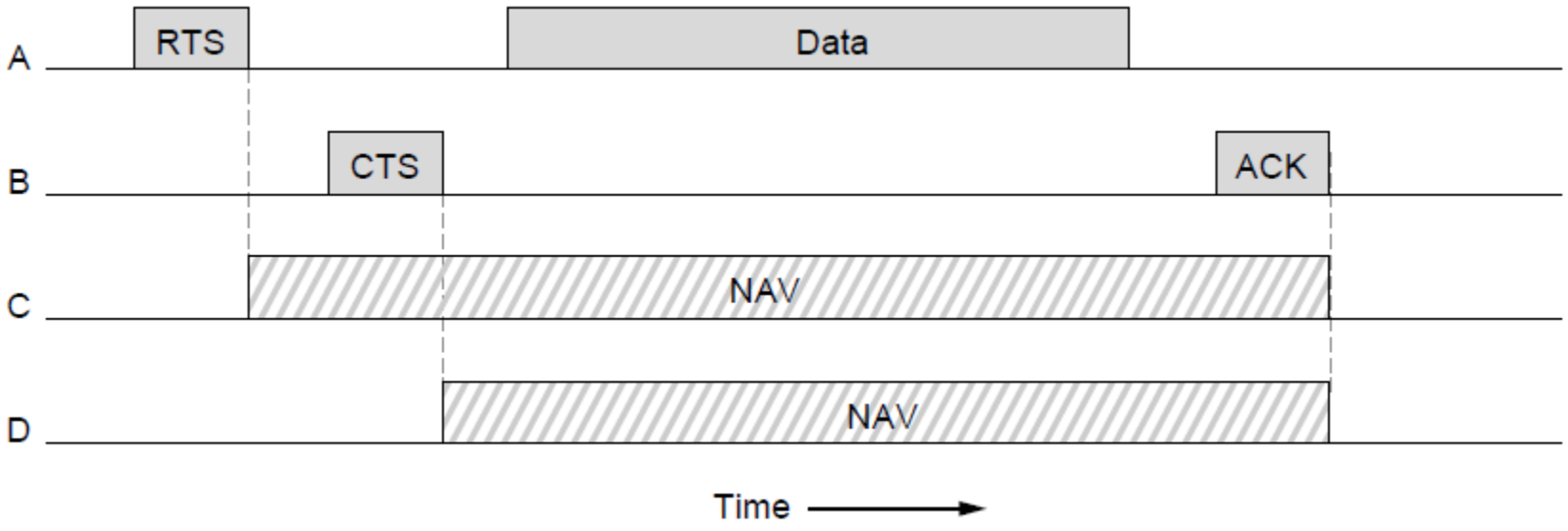
802.11 physical layer

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

Name	Technique	Max. Bit Rate
802.11b	Spread spectrum, 2.4 GHz	11 Mbps
802.11g	OFDM, 2.4 GHz	54 Mbps
802.11a	OFDM, 5 GHz	54 Mbps
802.11n	OFDM with MIMO, 2.4/5 GHz	600 Mbps

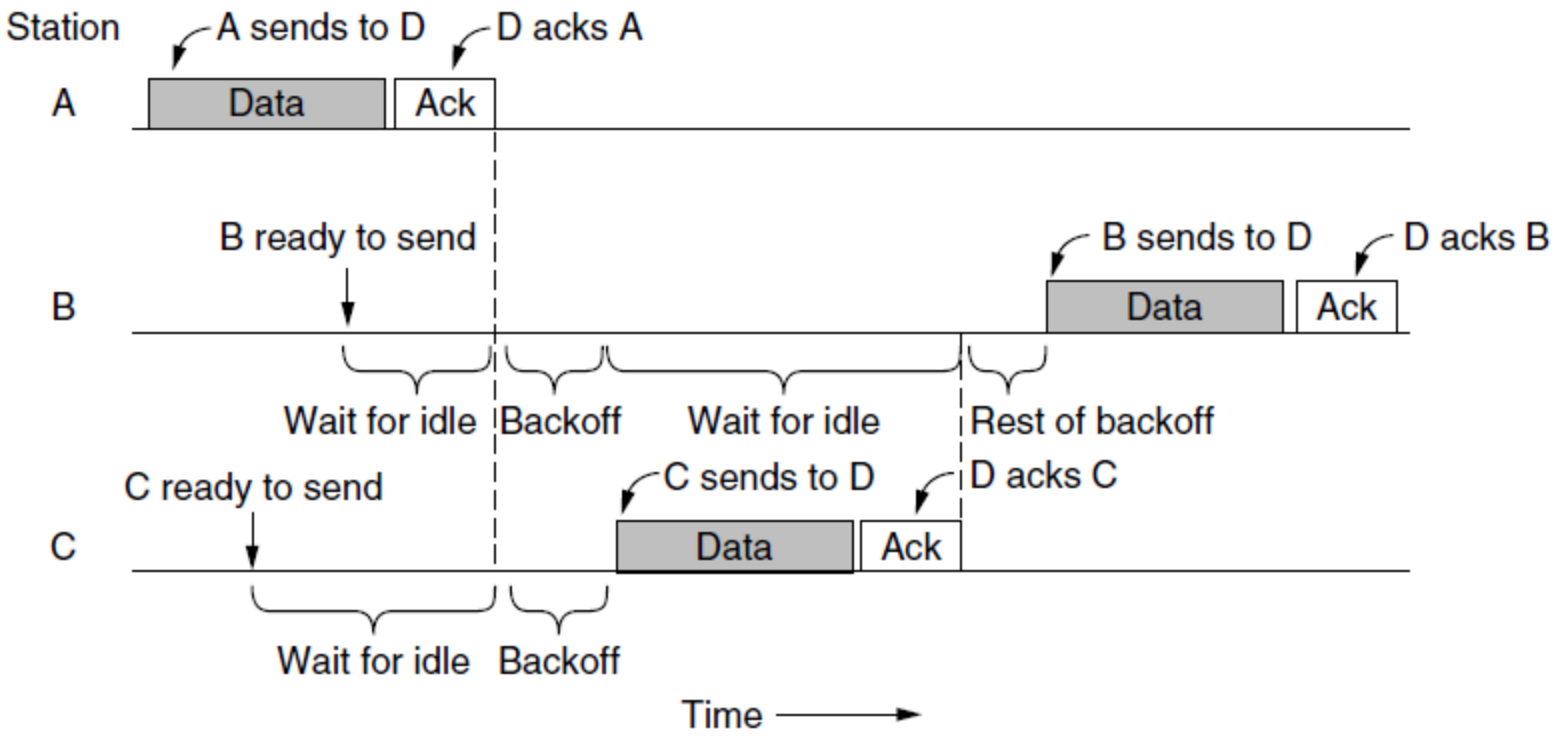
802.11 MAC

- Uses **ACKs/retransmissions** to recover from wireless errors
- Uses **stop-and-wait** for flow control
- Uses **Distributed Coordination Function** (DCF) for access control
- Virtual channel sensing with the **Network Allocation Vector** (NAV) and optional RTS/CTS avoids hidden terminals



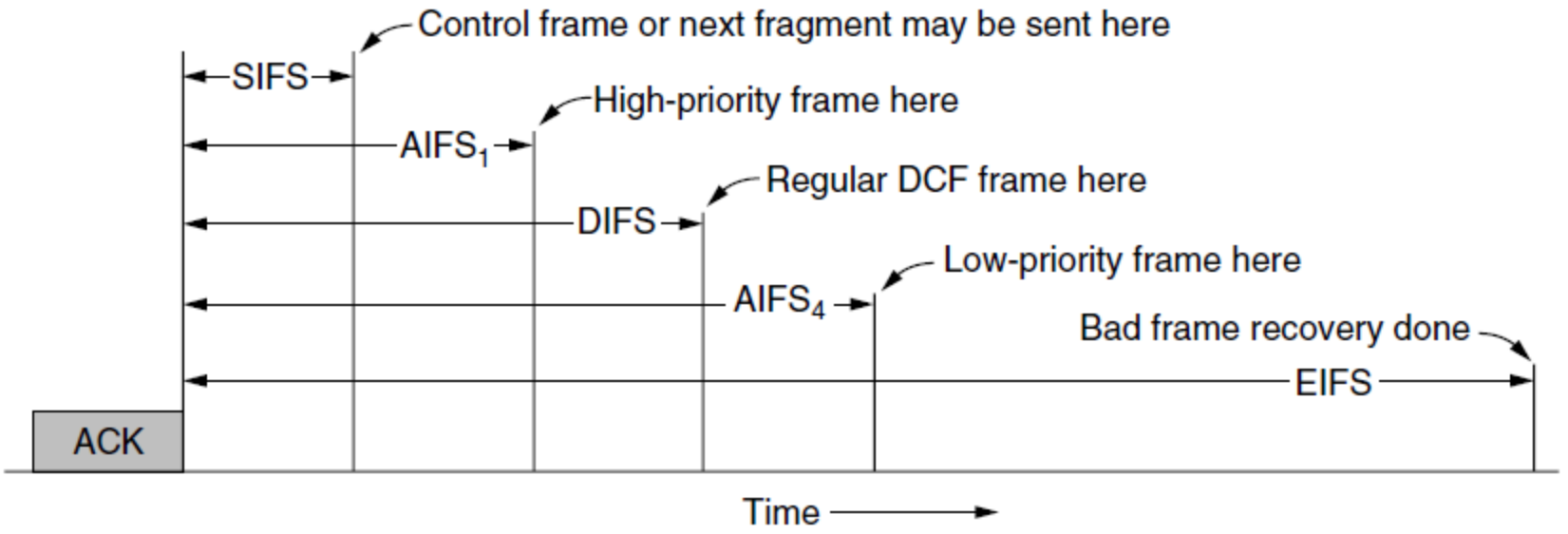
802.11 MAC

- Stations use different types of backoff slots for different types of frames to avoid collisions



802.11 MAC

- Different backoff slot times add quality of service
  - Short intervals give preferred access, e.g., control, VoIP



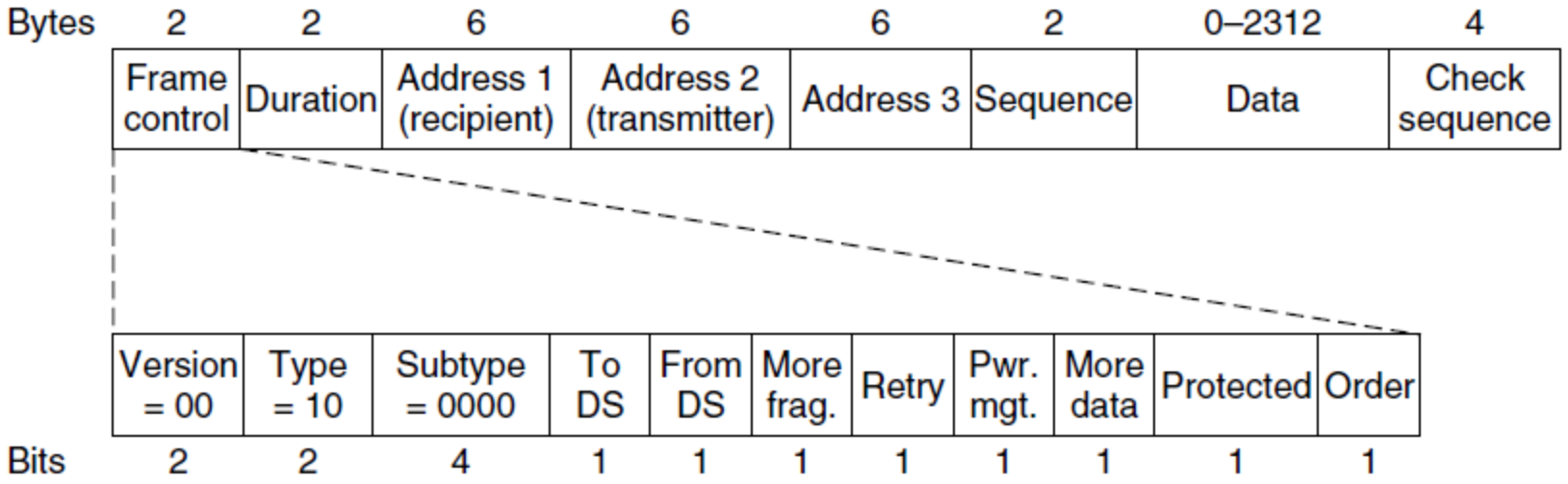
802.11 MAC

- **SIFS** (Short InterFrame Spacing): Backoff interval for control frames, e,g., ACK, RTS, CTS etc.
- **AIFS1** (Arbitration IterFrame Spacing 1): Backoff interval for high priority frames, e.g., VoIP
- **DIFS** (DCF InterFrame Spacing): Backoff interval between regular data frames.
- **AIFS4** (Arbitration IterFrame Spacing 4): Backoff interval for background traffic that can be deferred.
- **EIFS** (Extended InterFrame Spacing): Backoff interval for reporting problem, e.g., reception of bad or unknown frames.

- MAC has other mechanisms too, e.g., **power save mode**

802.11 Frame Structure

- Frames vary depending on their type (Frame control)
- Data frames have 3 addresses to pass via APs

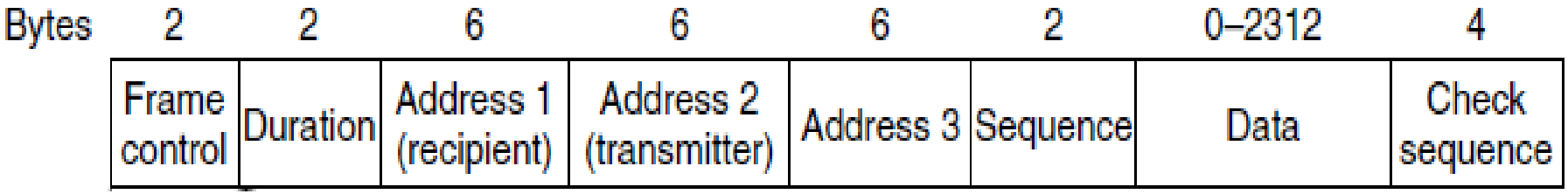


802.11 Frame Control

	Version = 00	Type = 10	Subtype = 0000	To DS	From DS	More frag.	Retry	Pwr. mgt.	More data	Protected	Order
Bits	2	2	4	1	1	1	1	1	1	1	1

- **Type**: Data, Control, Management
- **Subtype**: RTS or CTS
- **To DS**: Frame to AP (Distribution System)
- **From DS**: Frame from AP (Distribution System)
- **More fragments**: More fragments will follow
- **Retry**: Retransmitted
- **Power Management**: Sender entering power-save mode.
- **More data**: Sender has more frames for the receiver
- **Protected**: Frame is encrypted
- **Order**: Receiver must deliver the frames in-order to its higher layer

802.11 Data Frame



- **Duration**: Length of data and acknowledgement in microseconds, used by the stations to implement NAV
- **Address1**: Destination Address (Endpoint/DS)
- **Address2**: Source Address (Endpoint/DS)
- **Address3**: Endpoint Address
- **Sequence**: Detects the duplicate
- **Data**: Payload
- **Check sequence**: 32-bit CRC

Summary

- Channel Allocation Problem
- Multiple Access Protocols
  - Pure and Slotted ALOHA
  - Carrier Sense Multiple Access (CSMA)
  - CSMA with Collision Detection (CSMA/CD)
  - Binary Exponential Backoff Algorithm
- Ethernet
- Wireless
  - CSMA with Collision Avoidance (CSMA/CA)
  - WiFi(IEEE 801.11)

Next: Network Layer

- Store and Forward Packet Switching
- Datagrams
- Routers
- Routing Algorithms
  - Shortest Path Routing
  - Distance Vector Routing
  - Link State Routing
- Internet Protocol (IP)
  - IP Packet
  - IP Address
  - Routing Information Protocol (RIP)
  - Open Shortest Path First Protocol (OSPF)
  - Address Resolution Protocol (ARP)
  - Dynamic Host Configuration Protocol (DHCP)
  - Network Address Translation (NAT)
  - Internet Control Message Protocol (ICMP)