Week 4 - MAC Sub-Layer

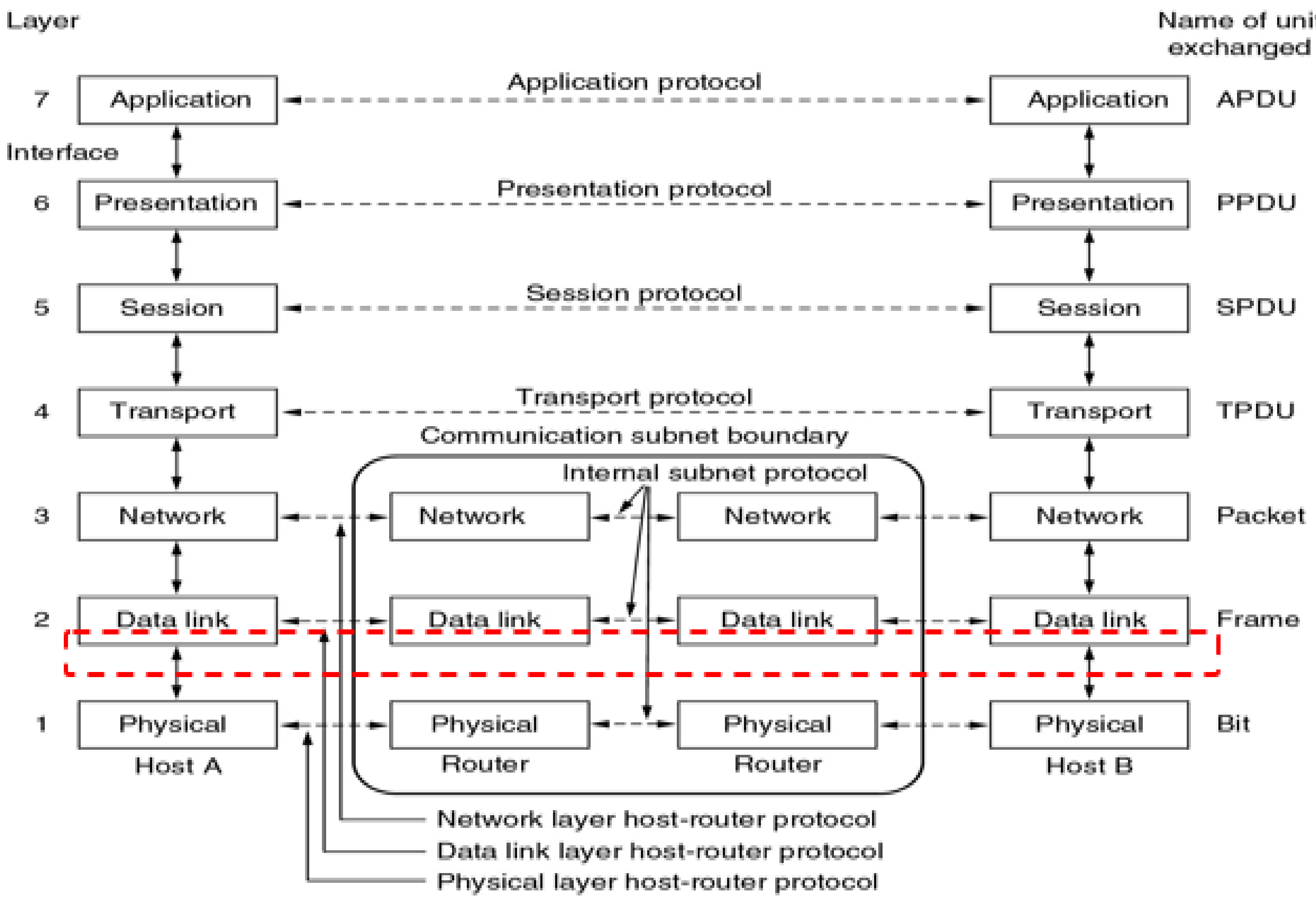
COMP90007

Internet Technologies

Introduction

- On **point to point networks**, there are only singular sender and receiver pairs, eliminating transmission contention
- On **broadcast networks**, determining right to transmit is a complex problem
- **Medium Access Control (MAC)** sub-layer is used to assist in resolving transmission conflicts

MAC Sub-layer



Types of Channel Allocation Mechanisms

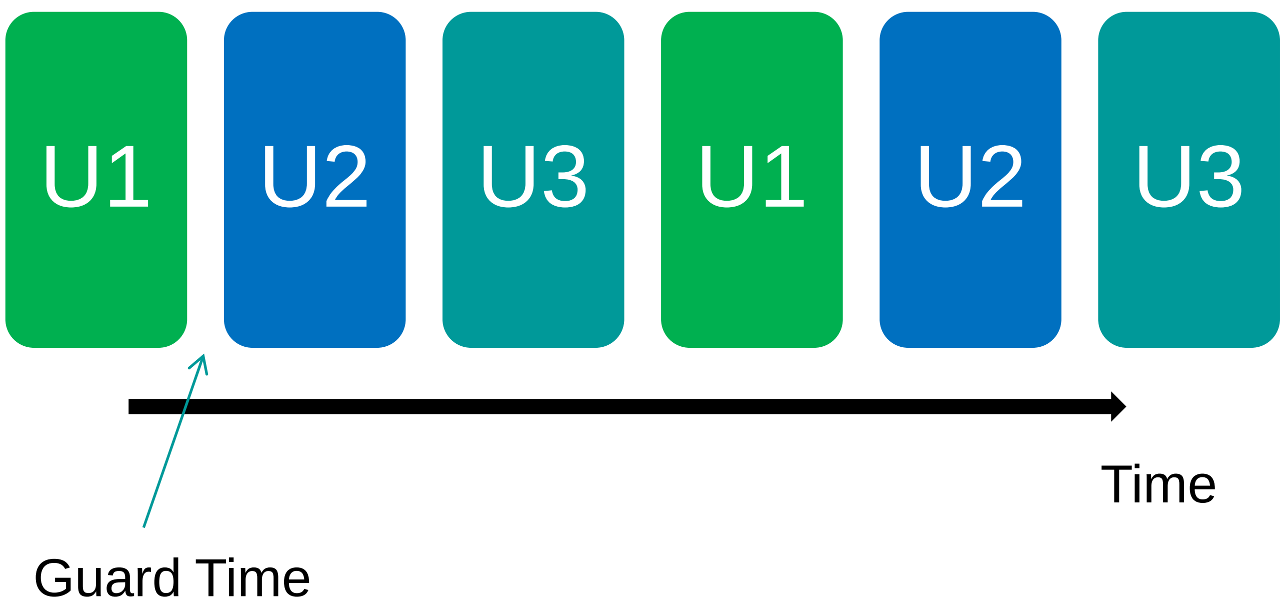
- Various methods exist for allocating a single broadcast channel amongst competing users
  - **<u>Static Channel Allocation</u>**
  - **<u>Dynamic Channel Allocation</u>**

Static Channel Allocation (1)

- Arbitrary division of a channel into segments and each user allocated a dedicated segment for transmission
- Time Division Multiplexing (TDM) and Frequency Division Multiplexing (FDM)
- Where are they used?
  - TV and Radio use FDM
  - 2G uses TDM

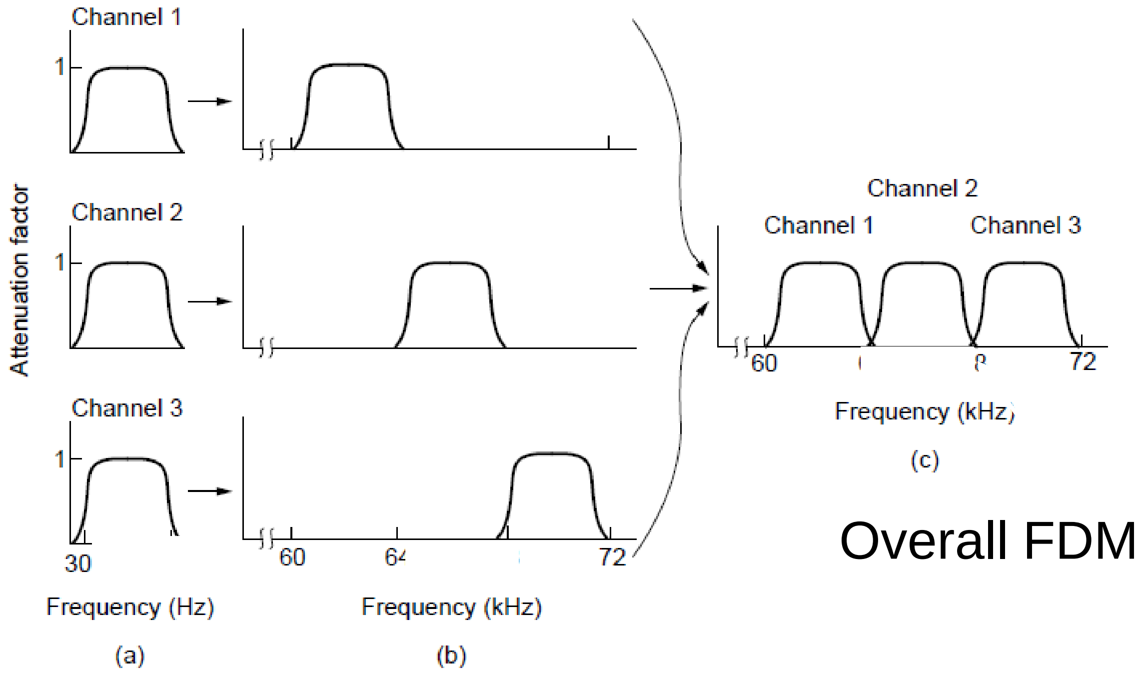
Time Division Multiplexing

- Users take turns on a fixed schedule



Frequency Division Multiplexing

- FDM (Frequency Division Multiplexing) shares the channel by placing users on different frequencies:



Overall FDM channel

Static Channel Allocation (2)

- Usually good for fixed number of users
- Significant inefficiencies arise when:
  - Number of senders > allocated segments
  - Number of senders is not static
  - Network Traffic is bursty: static methods TDM and FDM try to give consistent access to the network

Dynamic Channel Allocation (1)

- Channel segmentation is dynamic, segment allocation is dynamic
- Assumptions for dynamic channel allocation:

1) Independent transmission stations
2) Single channel for all communication
3) Simultaneous transmission results in damaged frames (collision)

Dynamic Channel Allocation (2)

4) Time

- Continuous: Transmission can begin at any time
- Slotted: Transmission can begin only within discrete intervals

5) Carrier Sense

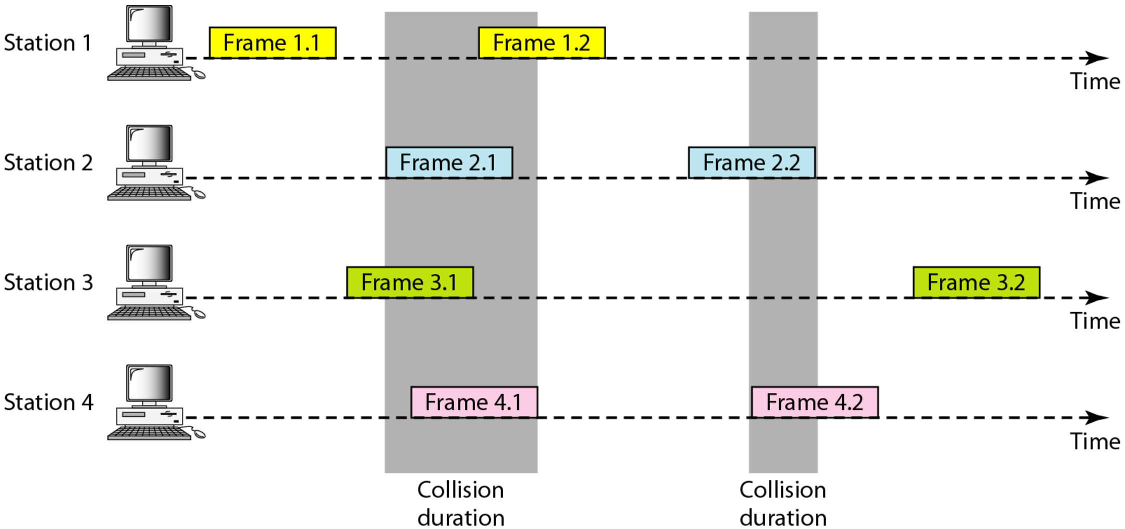
- Carrier Sense: Detection of channel use prior to transmission
- No Carrier Sense: No detection of channel use prior to transmission

Multiple Access Protocols

- Contention
  - ALOHA
  - Carrier Sense Multiple Access
- Collision Free
- Limited Contention
- MACA/MACAW (for Wireless LANs)

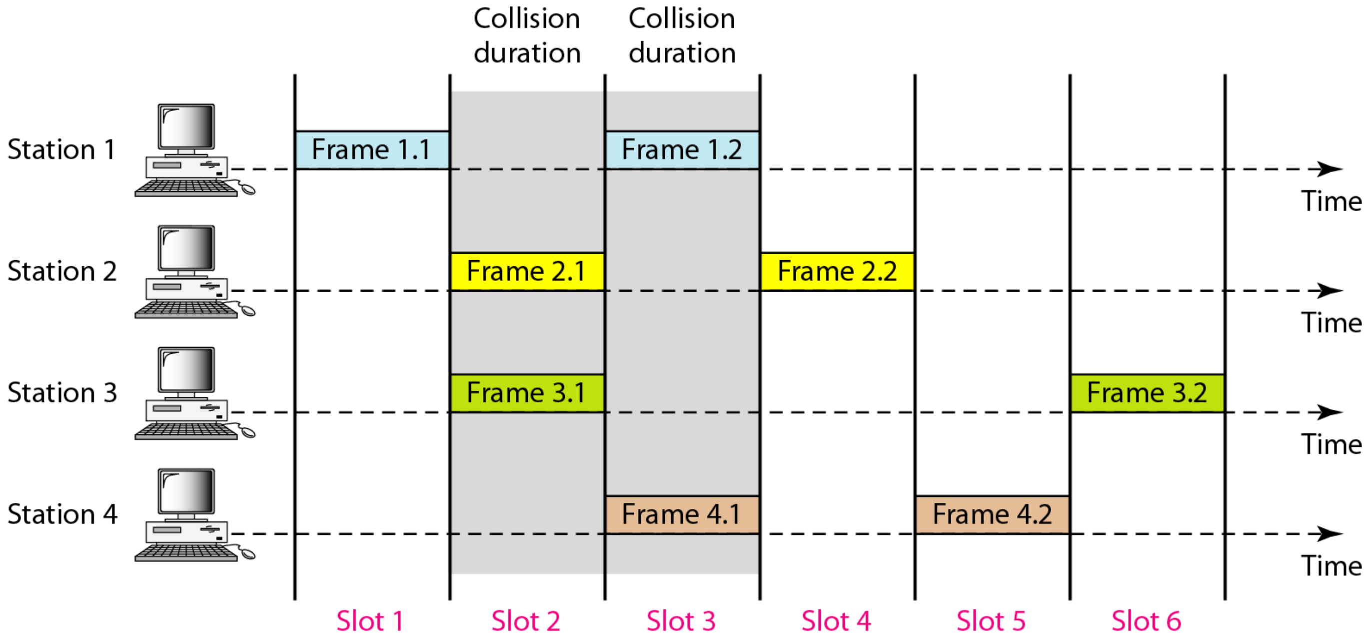
ALOHA

- Users **transmit frames whenever they have data**; users **retry after a random time if there are collisions** (or no Ack is arrived)
- Requires **no central control mechanism**
- **Efficient under low load** but inefficient under high traffic loads



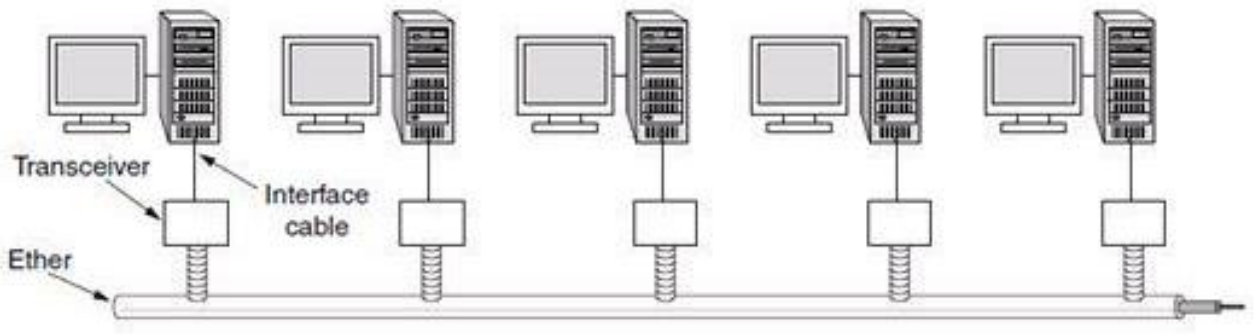
Slotted ALOHA

- **<u>Slotted ALOHA</u>**: Allows the users to start sending only at the beginning of defined slots.
- Increase efficiency of pure ALOHA by reducing possibility of collisions



Carrier Sense Multiple Access (CSMA)

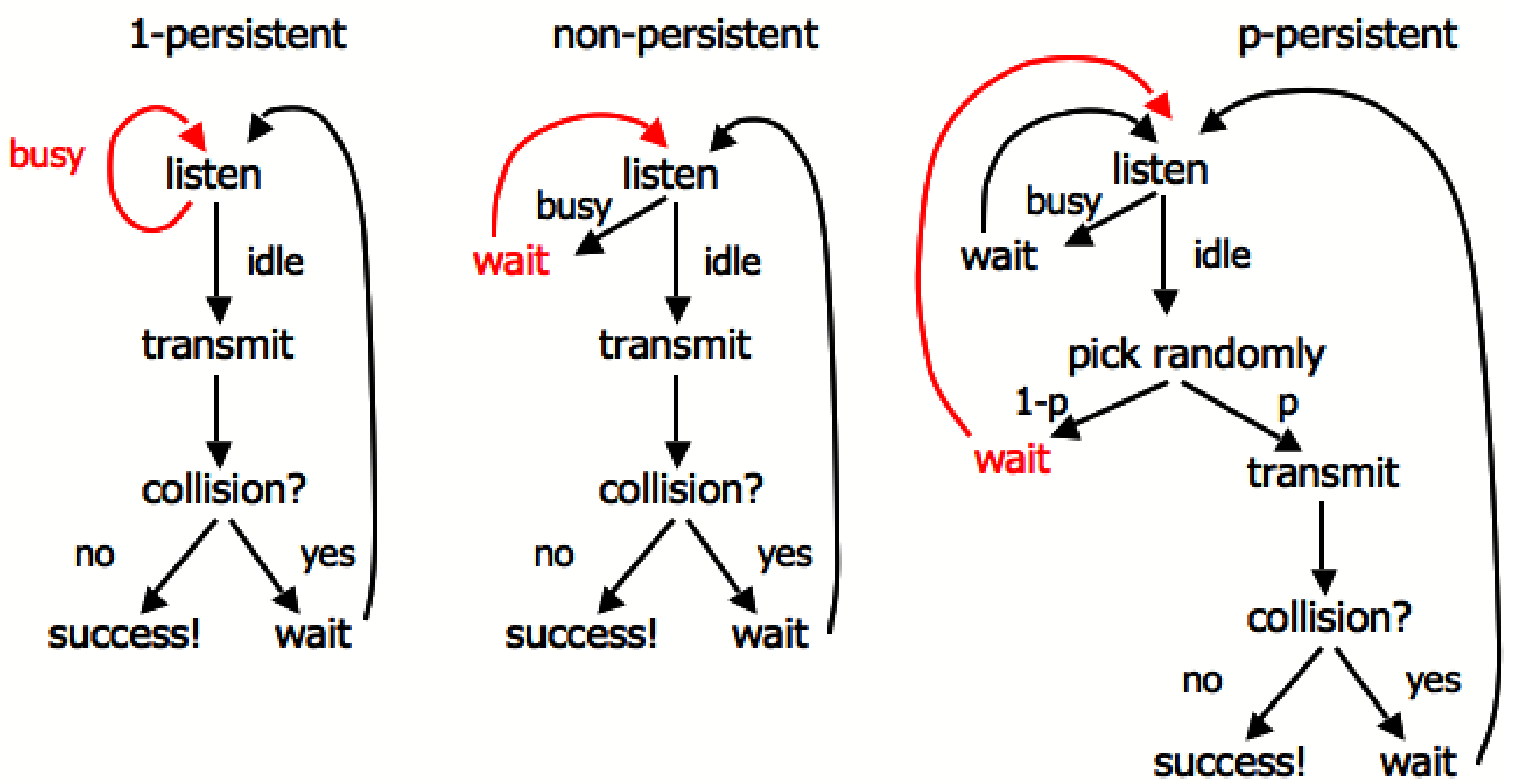
- In networks which **<u>require transmission state detection</u>** to determine transmission rights dynamically, there are specific protocols which are used
  - Persistent and Non-Persistent CSMA
  - CSMA with Collision Detection



Persistent and Non-Persistent CSMA (1)

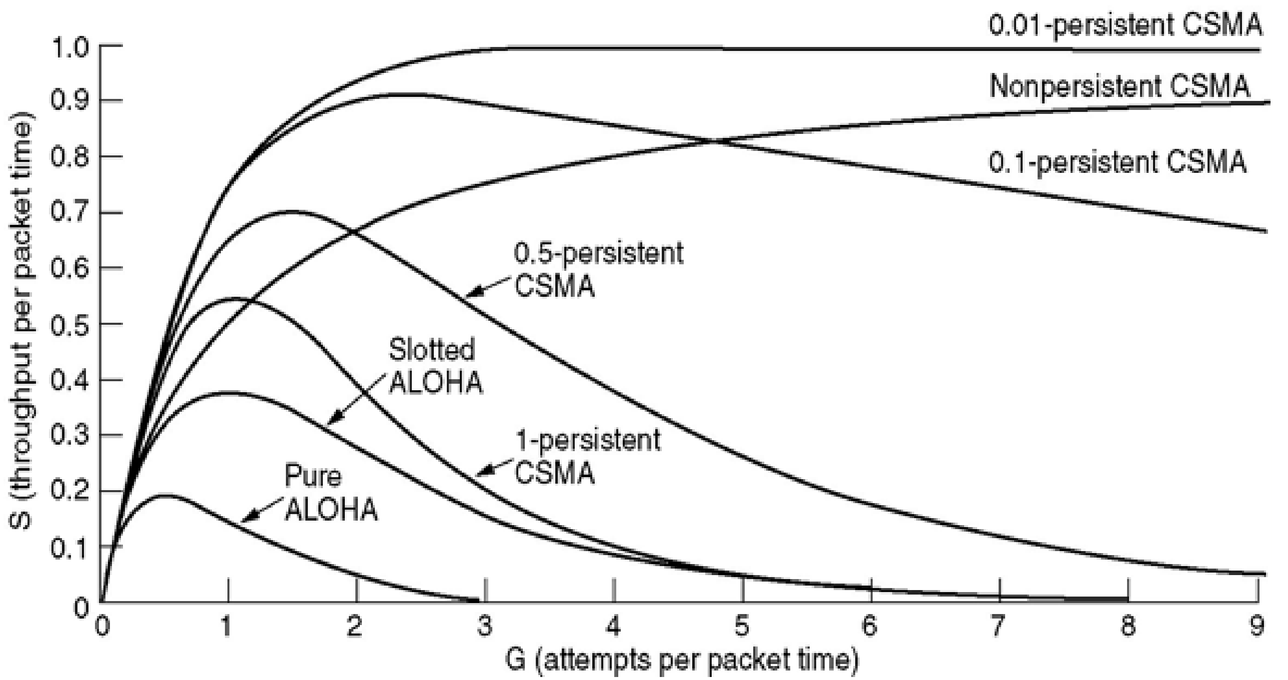
- When a sender has data to transmit, first check channel to **detect other active transmission**
- **1-persistent CSMA**
  - **Continuously check, and wait until channel idle; transmit one frame and check collisions**; if collision, wait for a random time and repeat
- **Non-persistent CSMA**
  - **If channel busy, wait random period and check again**; if idle, start transmitting
- **p-persistent CSMA**
  - **If channel idle, transmit with probability p, or wait with probability (1-p)** and check again

Persistent and Non-Persistent CSMA (2)



CSMA Variants

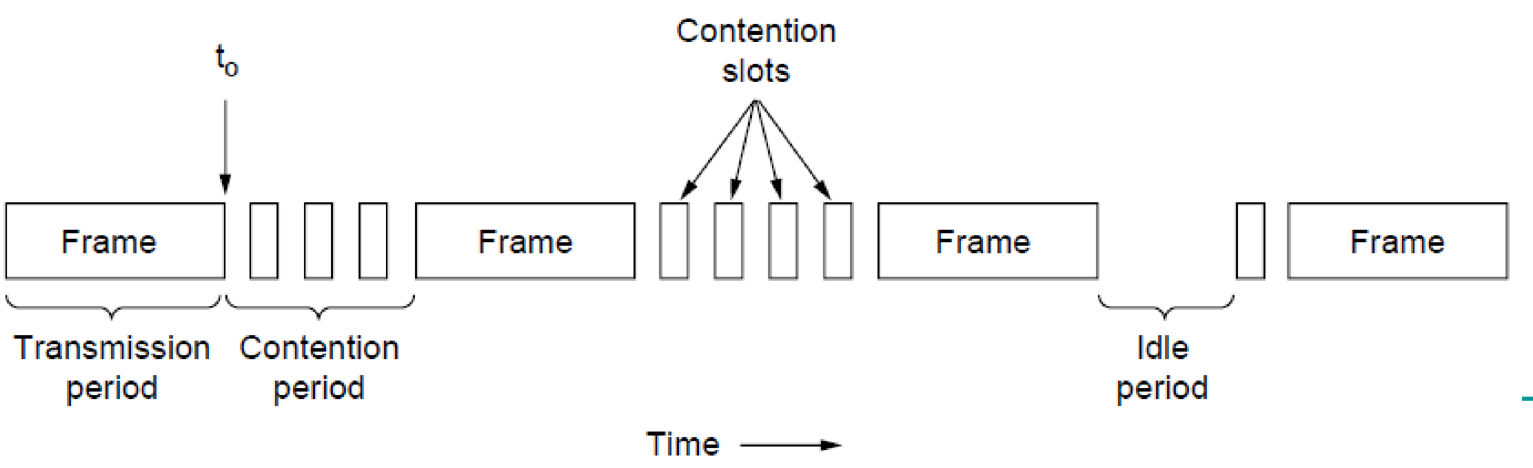
- Comparison of the efficiencies (channel utilisations) for various protocols



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

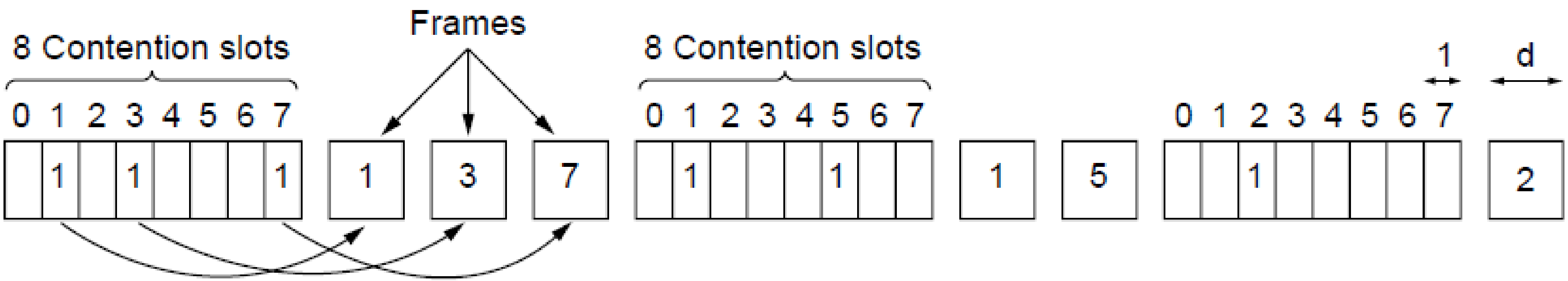
CSMA with Collision Detection

- Principle: transmission aborted when collision detected
- Process: After collision detected, abort, wait random period, try again
- Channel must be continually monitored
- Used in half-duplex system (e.g., with hub or repeater)
- Reduced contention times improve performance



Collision Free Protocols (1)

- Bit Map Protocol
  - Reservation-based protocol
  - 1 bit per station overhead
  - Division of transmission right, and transmission event - no collisions as this is a reservation based protocol

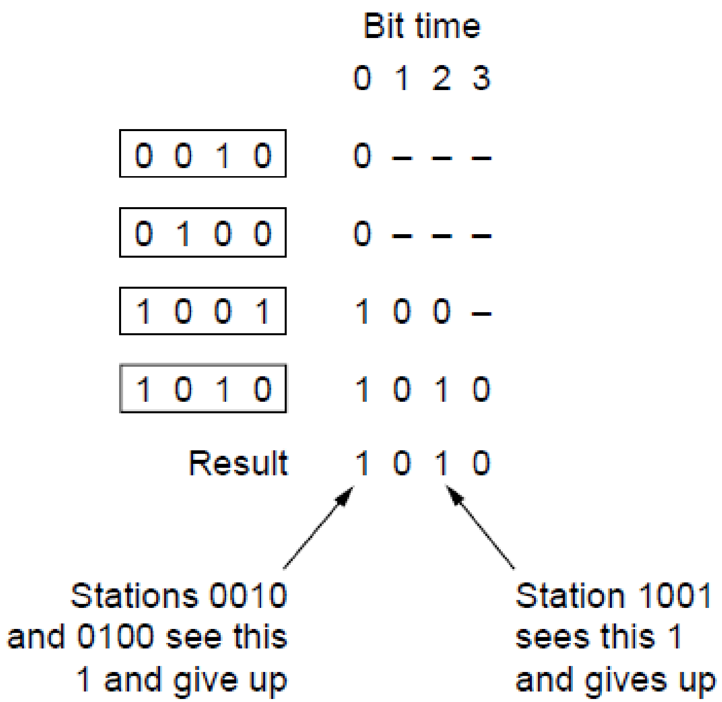


Collision Free Protocols (2)

- Binary Countdown Protocol
  - Avoid the 1 bit per station scalability problem by using binary station addressing
  - No collisions as higher-order bit positions are used to arbitrate between stations wanting to transmit
  - Higher numbered stations have a higher priority

Collision Free Protocols (3)

- Binary Countdown Protocol
  - Stations send their address in contention slot ($\log_2$ N bits instead of N bits)
  - Channel medium ORs bits; stations give up when they send a "0" but see a "1"
  - Station that sees its full address is next to send

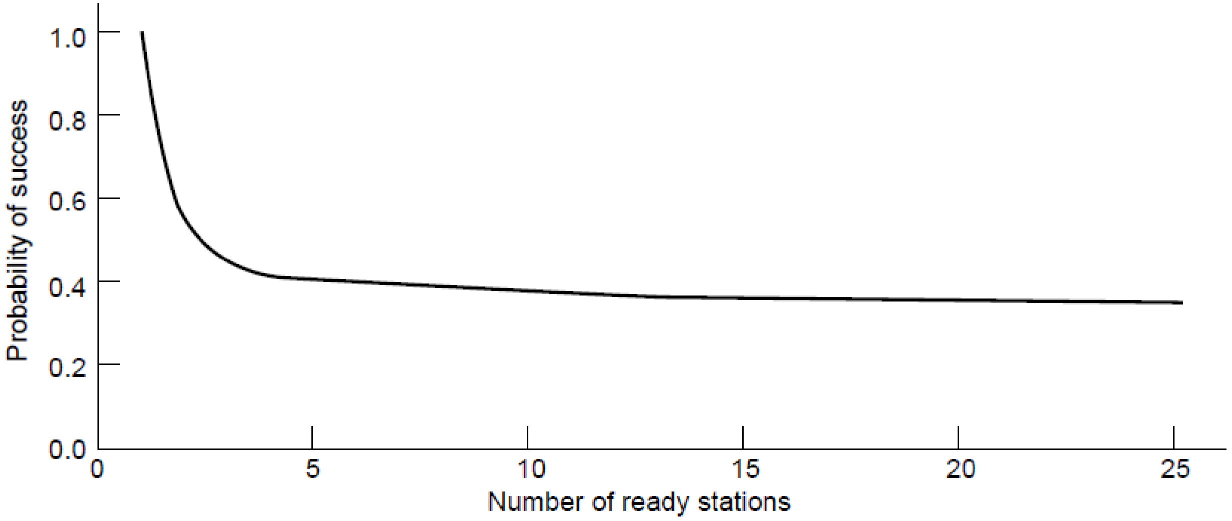


Contention vs. Collision Free

- 2 strategies - **contention** and **collision free** - both become inefficient at different points
- Under **low loads**, collision free is less attractive because of a higher delay between transmissions
- Under **higher loads**, contention is less attractive because overhead associated with channel arbitration becomes greater

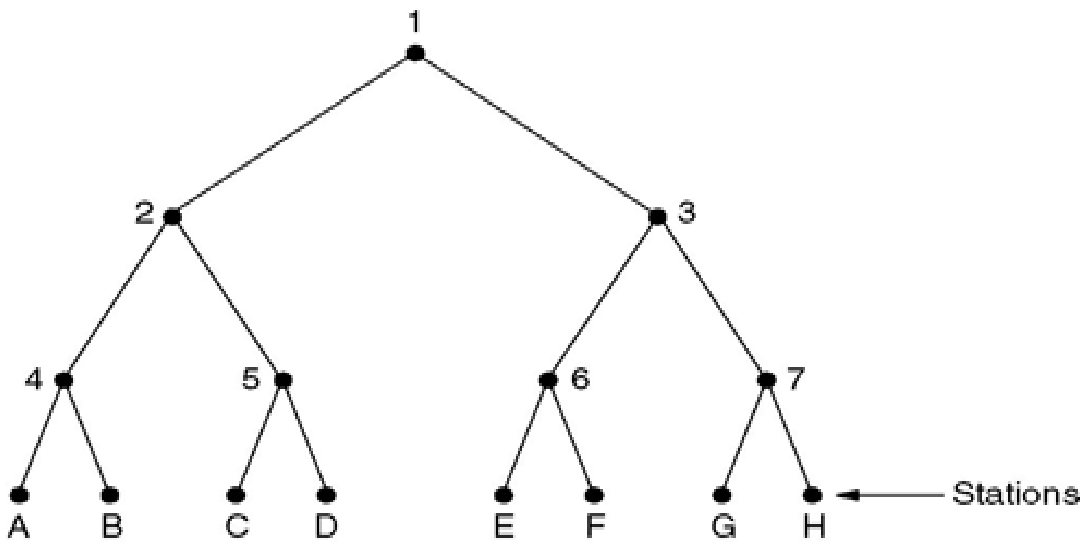
Limited Contention Protocols

- Idea: divide stations into groups within which only a very small number are likely to transmit data.
- Increase the probability of stations acquiring transmission rights by dividing stations and using a binary algorithm to determine rights allocation
- Avoid wastage due to idle periods and collisions



Adaptive Tree Walk Protocol

- All stations compete for right to transmit, if a collision occurs, binary division is used to resolve contention
- Tree divides stations into groups (nodes) to poll
  - Depth first search under nodes with poll collisions
  - Start search at lower levels if >1 station expected



Example 1: D G
Slot 1 → D, G – collision
Slot 2 → D
Slot 3 → G

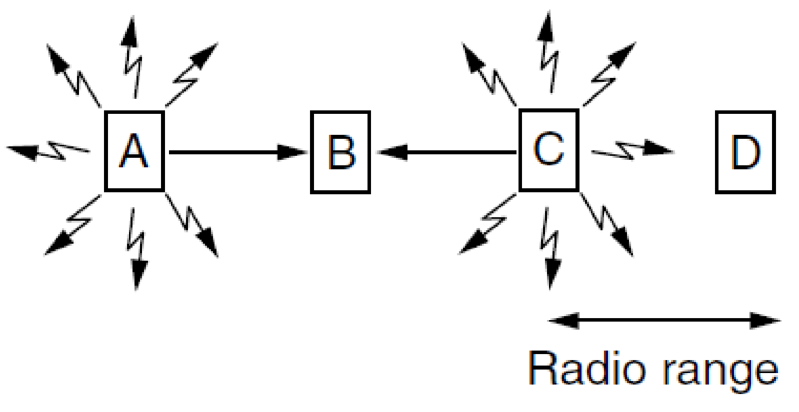
Example 2: B D G
Slot 1 → B, D, G – collision
Slot 2 → B, D - collision
Slot 3 → B
Slot 4 → D
Slot 5 → G

Wireless LAN Protocols

- Wireless Complications: when a station is in the range of two transmitters or relays, interference affects signal reception.
- Stations have coverage regions, which leads to **hidden** and **exposed terminal** problems.
- Require **detection of transmissions to receiver, not just carrier sensing.**
- Transmission Protocols for Wireless LANs (802.11)
  - Multiple Access with Collision Avoidance for Wireless (MACAW)

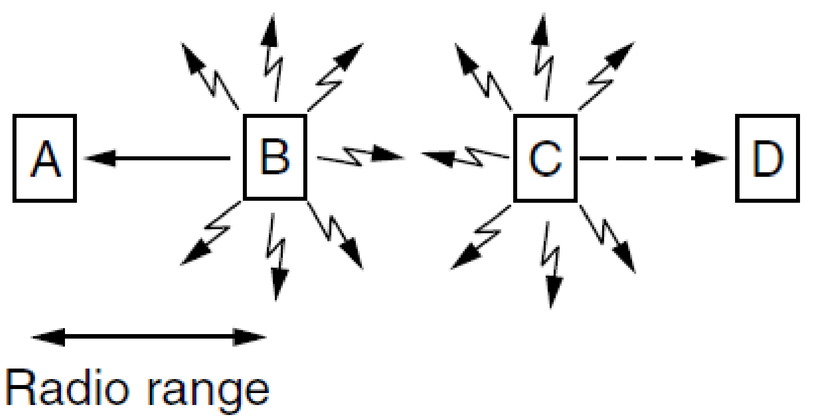
Hidden and Exposed Terminals (1)

- **<u>Hidden terminals</u>** are senders that cannot sense each other but nonetheless collide at intended receiver
  - A and C are hidden terminals when sending to B
  - Want to prevent; loss of efficiency



Hidden and Exposed Terminals (2)

- **<u>Exposed terminals</u>** are senders who can sense each other but still transmit safely (to different receivers)
  - B → A and C → D are exposed terminals
  - Desirably concurrency; improves performance



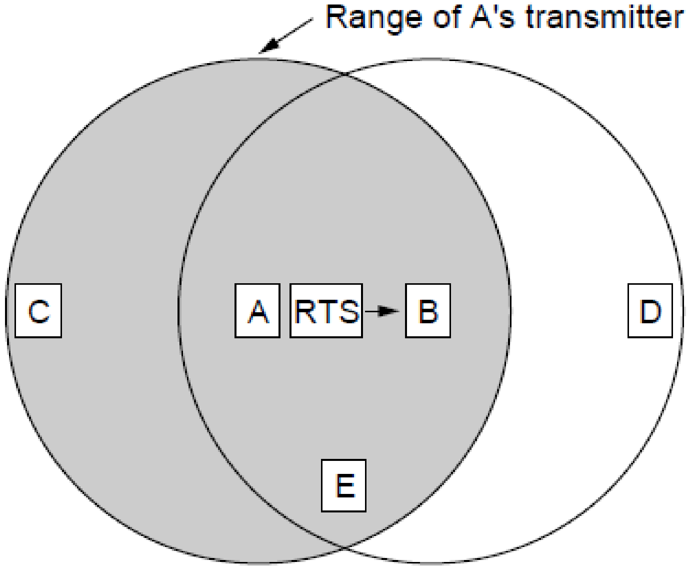
MACA (1)

- MACA: Multiple Access with Collision Avoidance
- Sender asks receiver to transmit short control frame
- Stations near receiver hear control frame
- Sender can then transmit data to receiver

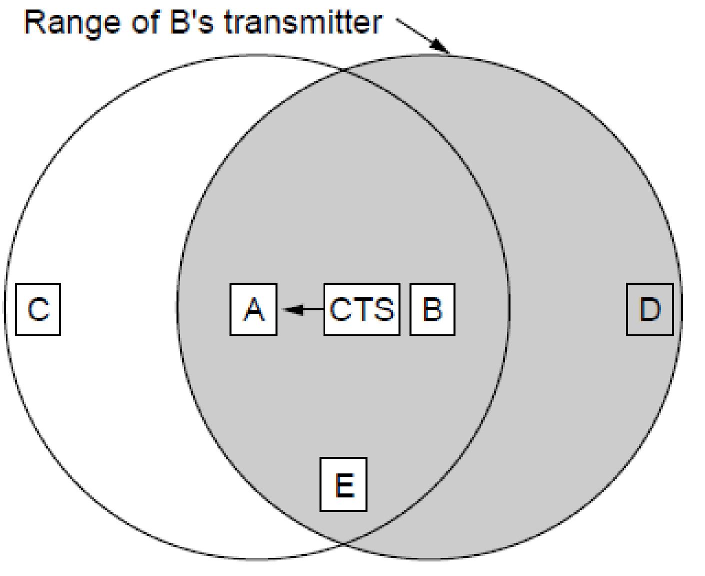
MACA (2)

MACA protocol grants access for A to send to B:

- A sends RTS to B [left]; B replies with CTS [right]
- A can send with exposed but no hidden terminals



A sends RTS to B; C and E hear and defer for CTS



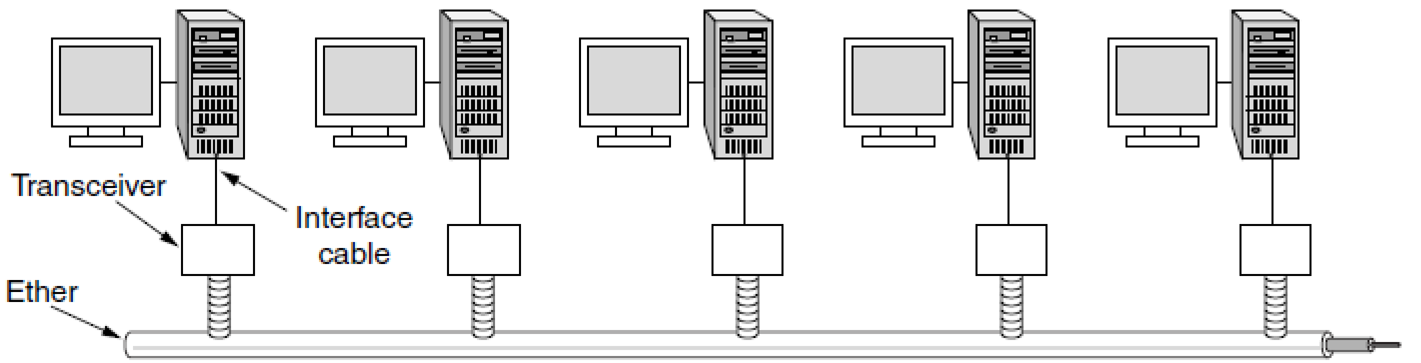
B replies with CTS; D and E hear and defer for data

Ethernet

- A Famous MAC Sub-Layer Case Study
  - Classic Ethernet
  - Switched Ethernet

Classic Ethernet

- Each type of Ethernet has a maximum cable length per segment.
- Multiple cable lengths can be connected by repeaters - a physical device which receives, amplifies and retransmits signals in both directions.



Ethernet Frame Format

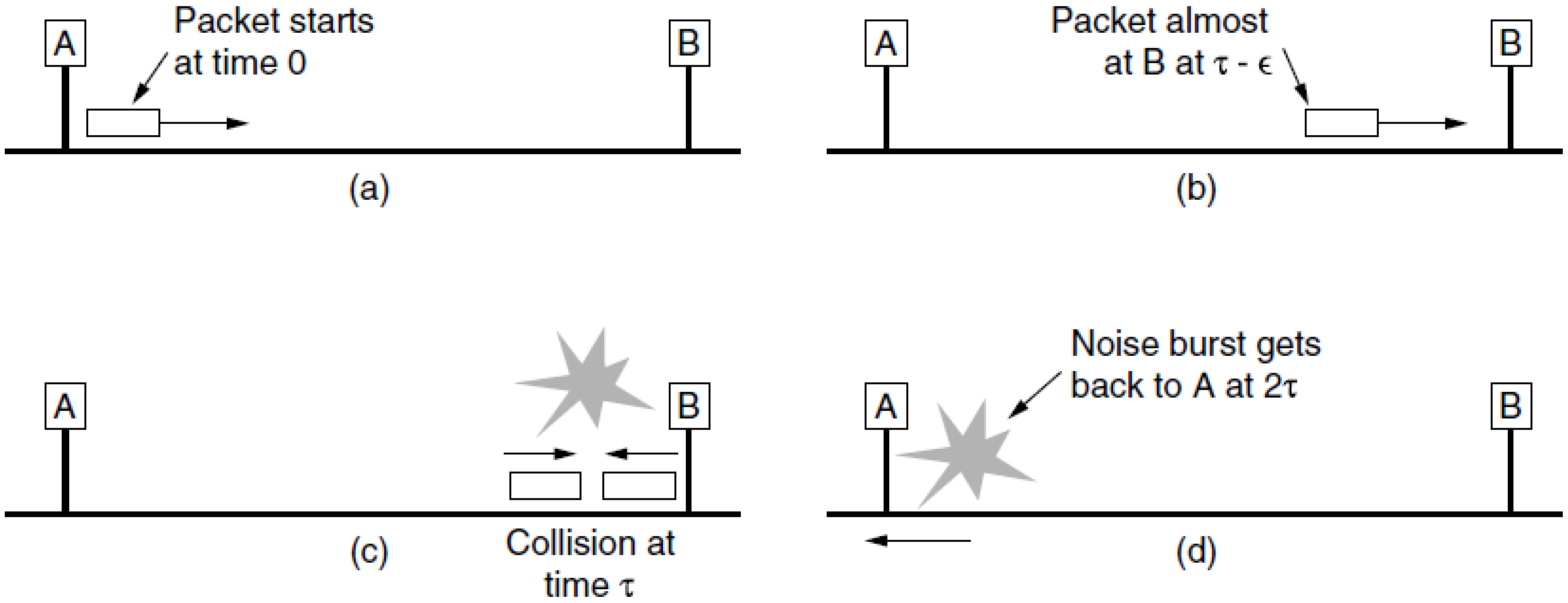
- MAC protocol is 1-persistent CSMA/CD
  - Random delay (backoff) after collision is computed with BEB (Binary Exponential Backoff, i.e., random number 0 to $2^i - 1$)
- Frame format is still used with modern Ethernet

IEEE 802.3	Preamble	SOF	Destination address	Source address	Length	Data	Pad	Check-sum

Preamble (7B) – synchronisation between sender and receiver
Start of Frame (1B) – FLAG bytes
Dest. & Source addresses (6B + 6B) – to identify sender and receiver
Type & Length (2B) – specifies which process to give the frame to (0x0800 means data contains IPv4)
Data (0~1500B)
Pad(0~46B) – minimum size of the message of the Ethernet – 64 Bytes
CRC (4B) – 32 bits checksum

Classic Ethernet Minimum Packet Size

- 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



MAC Addressing

- Source and Destination Addressing can be done at a local or global levels
- The **MAC Address** provides the unique identifier for a physical interface
- MAC Address is a 48-bit number encoded in the frame, written in hexadecimal notation

  e.g. 00:02:2D:66:7C:2C

Ethernet Performance

$$\textbf{Channel Efficiency} = \frac{1}{1 + (2BLe)/(cF)}$$

- F: frame length
- B: bandwidth
- L: cable length
- c: speed of signal propagation; e: constant ≈ 2.71828
- Optimal case: e contention slots per frame

- When cF is large, the channel efficiency will be high.
- Increasing network bandwidth or distance (BL) reduces the efficiency for a given frame size.

Switched 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