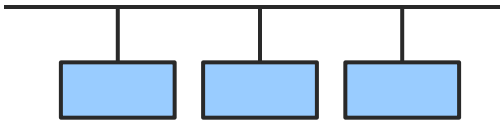
Multiple Access Media

Reading: Peterson and Davie, Chapter 2

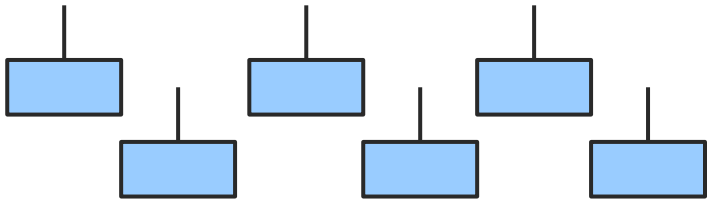
Multiple Access Media

- Multiple senders on some media
  - Buses (Ethernet)
  - Radio, Satellite
  - Token Ring
- Need methods to mediate access
  - Fair arbitration
  - Good performance



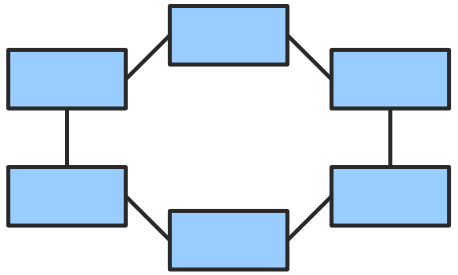
Bus Topology: Shared

Ethernet, Token Bus



Wireless: Shared

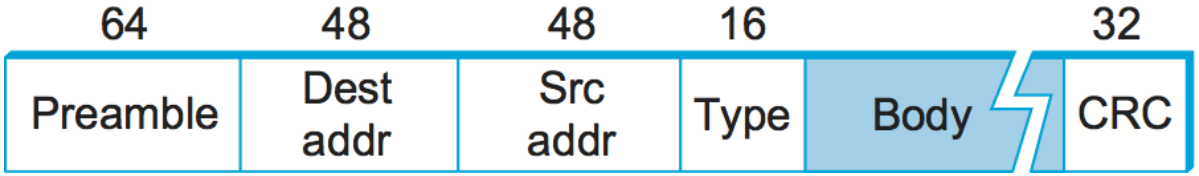
IEEE 802.11



Ring Topology: Multihop

FDDI, IEEE 802.5

Ethernet Frame Format



- 64 bit preamble: allows the receiver to synchronize with the signal
- Source, Destination: 48-bit address (6 bytes)
- Type: demultiplexing key, it identifies which higher-level protocols this frame should be delivered
- Data: 46 bytes, up to 1500 bytes
  - Minimum length to ensure detection of collision
  - Upper bound of time a sender can occupy

MAC addresses

- Every Ethernet device has unique address.
- Ethernet addresses are typically printed as a sequence of six numbers separated by colons
  - For example, 8:0:2b:e4:b1:2 ➔ 00001000 00000000 00101011 11100100 10110001 00000010
- Each manufacturer of Ethernet devices is allocated a different prefix that must be prepended to the address on every adaptor they build.
  - For example, Advanced Micro Devices has been assigned the 24-bit prefix 080020 (or 8:0:20).
- A given manufacturer then makes sure the address suffixes it produces are unique.

Receiver Algorithm

- Ethernet adaptor receives *ALL* frames but accepts only the following:
  - Frames addressed to its own address
  - Frames addressed to the broadcast address (Ethernet address consisting of all 1s)
  - Frames addressed to a multicast address (address that has the first bit set to 1 but is not the broadcast address), if it has been instructed to listen to that address
  - All frames, if it has been placed in promiscuous mode
- It passes to the host only the frames that it accepts.

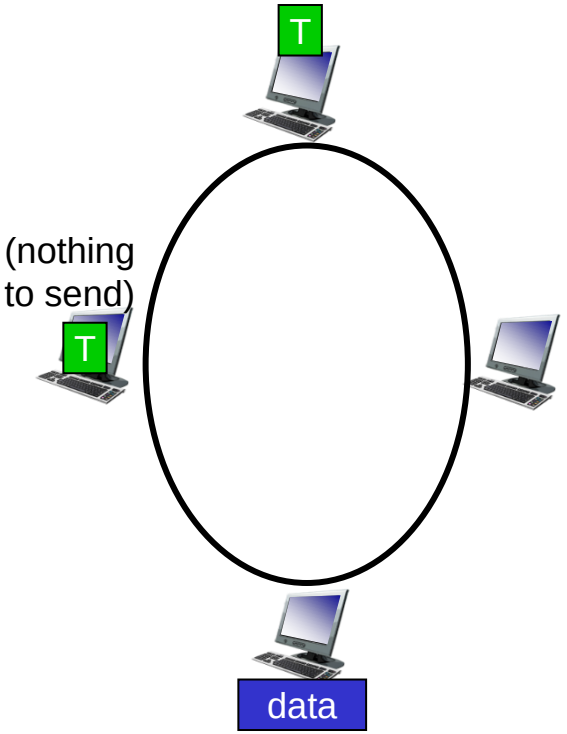
Transmitter algorithm (Multiple Access Media)

- Problem: demands can conflict, e.g., two hosts send simultaneously
  - STDM does not address this problem fully
  - Solution is a **Media Access Control (MAC)** algorithm
- Two solutions (of many)
  - Carrier sense multiple access with collision detection (CSMA/CD)
    - Send only if medium is idle
    - Stop sending immediately if collision detected
  - Token ring/Fiber Distributed Data Interface (FDDI) pass a token around a ring; only token holder sends

“Token Pass” MAC protocols

token passing:

- control *token* message explicitly passed from one node to next, sequentially
  - transmit while holding token
- concerns:
  - token overhead
  - latency
  - single point of failure (token)



Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

- Used by Ethernet
  - Xerox and IEEE 802.3 (10Mbps standards)
  - IEEE 802.3u (Fast Ethernet, 100Mbps standard)
  - Also applies to 1-Gbps, 10-Gbps, 40-Gbps, and 100-Gbps versions
- Goal
  - Distributed algorithm that provides fair efficient access to a shared medium

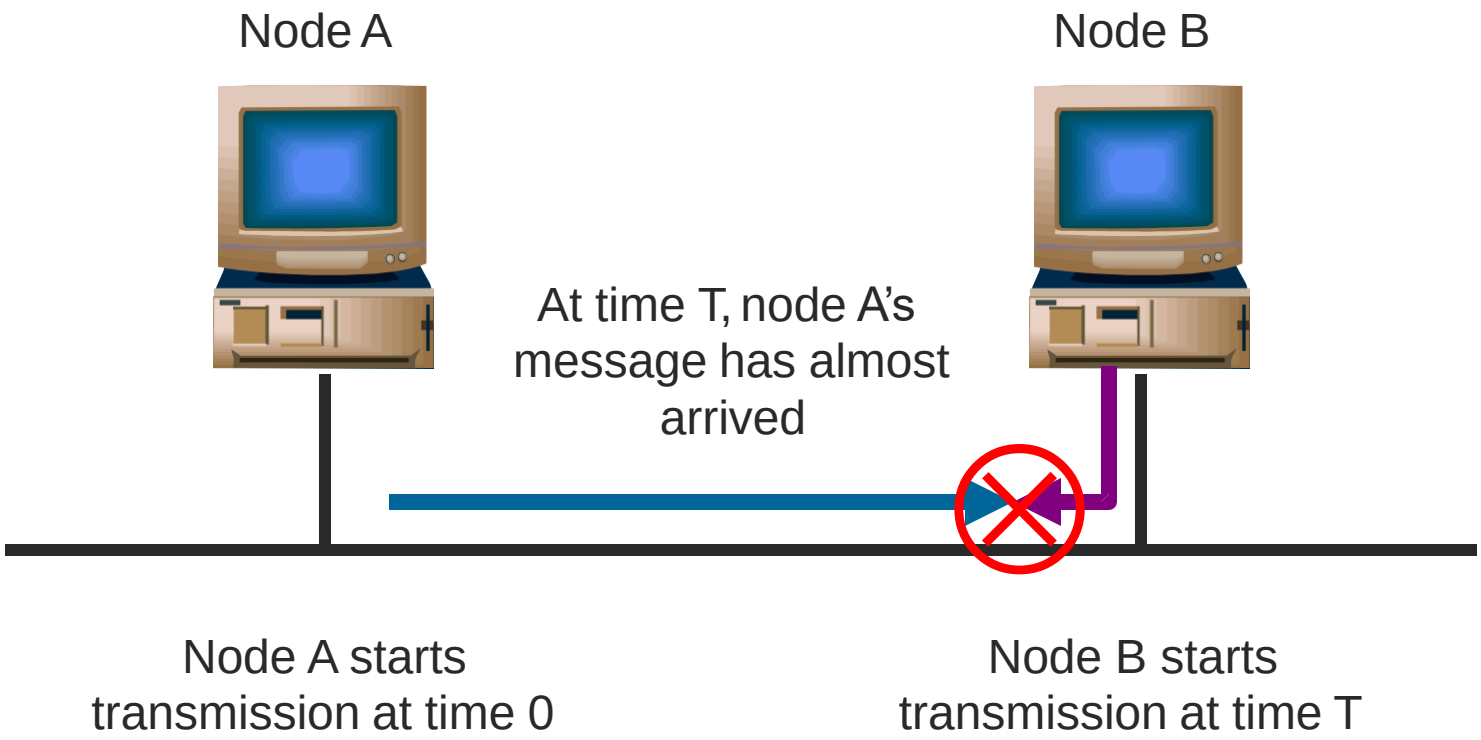
Ethernet MAC Algorithm

- Sender/Transmitter
  - If line is idle
    - Send immediately
    - Send maximum of 1500B data (Ensure the upper bound of time a sender can occupy the line)
    - Wait 9.6 μs (10^{-6} second) before sending again
  - If line is busy
    - Wait until line becomes idle
    - Send immediately (1-persistent)
  - If collision detected
    - Stop sending and jam signal (32 bit jam signal+64 bit preamble) ➔ *"Runt frame"*
    - Try again later

Why? -- Explanations

- Because there is no centralized control
- possible for two (or more) adaptors to begin transmitting at the same time (collide)
  - either because both found the line to be idle
  - or because both had been waiting for a busy line to become idle
- Ethernet supports collision detection

Ethernet MAC Algorithm

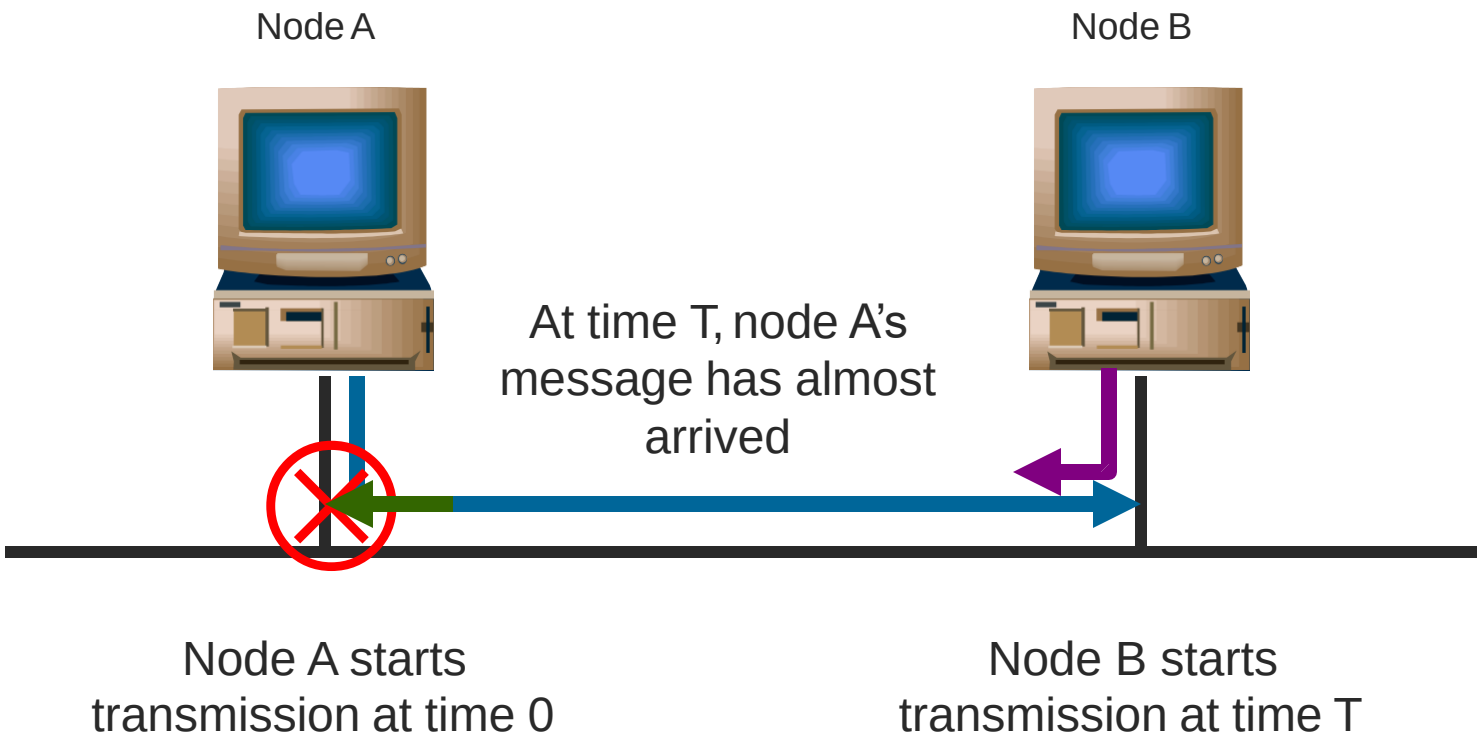


How can we ensure that A knows about the collision? (Sender "Smart")

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 (assume: 2500m Ethernet)
  - At 10Mbps 51.2μs = 512b or 64B
  - Packet length ≥ 64B = 512b
  - Details: 14 bytes of header (6B source addr, 6B dest addr, 2B type) plus 46 bytes of data plus 4 bytes of CRC., total 64 bytes

Ethernet MAC Algorithm



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

Jamming after Collision

- Ensures that all hosts notice the collision
- Jam signal is 32-bit, how does it notify the collision to other hosts?
  - Stop transmitting the current frame
  - Start transmitting the jam signal ≠ CRC
  - CRC check fails at other hosts → collision
  - Discard the frame due to CRC error

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
      - N=1; 0 or 51.2 μs, selected at random.
      - N=2; it then waits 0, 51.2, 102.4, or 153.6 μs (selected randomly) before trying again
      - N=3; it waits $k \times 51.2$ μs for k= 0. . .2^3−1, again selected at random
    - 2^N discrete possibilities from 0 to maximum = 2^N -1

Wireless

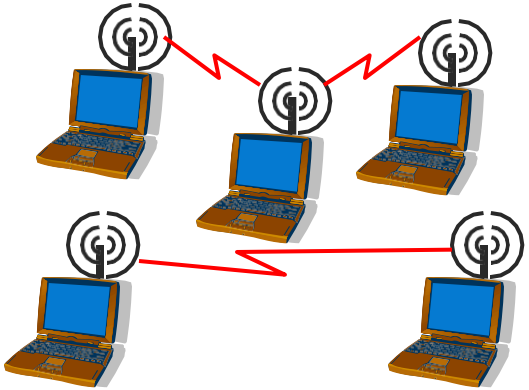
- IEEE 802.11 (Wi-Fi)
  - A physical and multiple access layer standard for wireless local area networks (WLAN)

Wireless Technologies

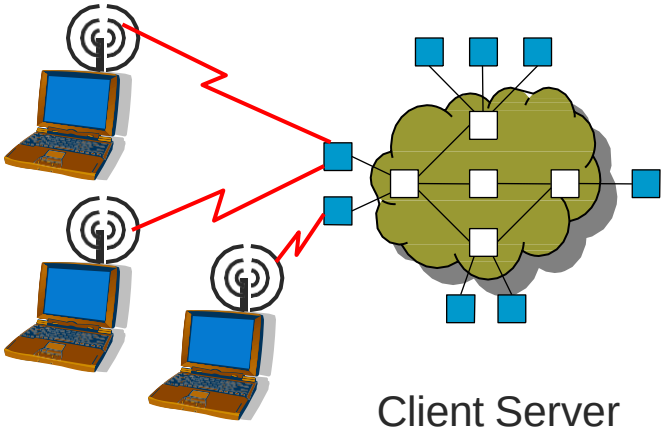
	Bluetooth (802.15.1)	Wi-Fi (802.11)	4G Cellular
Typical link length	10 m	100 m	Tens of kilometers
Typical data rate	2 Mbps (shared)	150-450 Mbps	1-5 Mbps
Typical use	Link a peripheral to a computer	Link a computer to a wired base	Link mobile phone to a wired tower
Wired technology analogy	USB	Ethernet	PON

Wireless

- IEEE 802.11 (Wi-Fi)
  - A physical and multiple access layer standard for wireless local area networks (WLAN)



Ad Hoc Network: no servers or access points



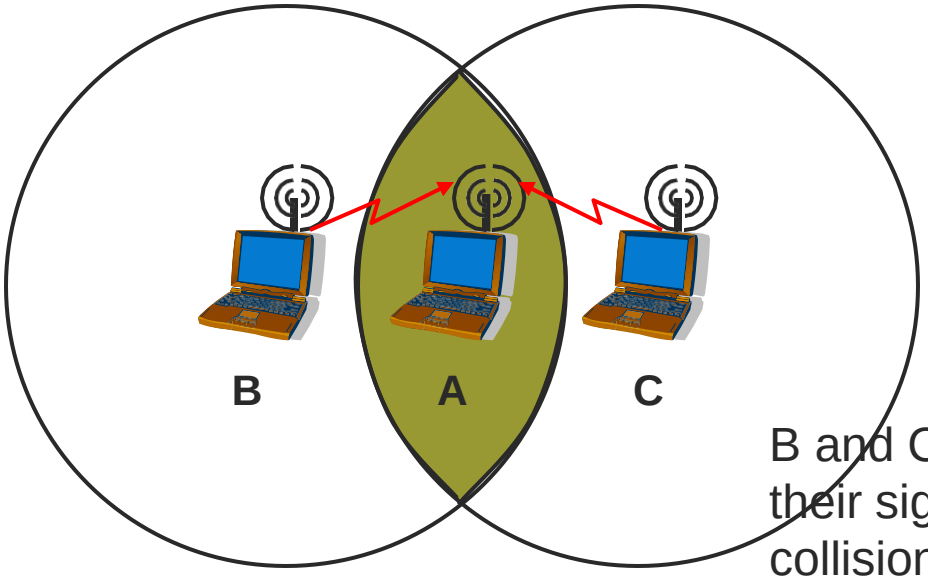
Client Server Network

Differences from Ethernet

- wireless nodes cannot usually transmit and receive at the same time (on the same frequency)
  - power generated by the transmitter is much higher than any received signal is likely to be and so swamps the receiving circuitry
- a node may not receive transmissions from another node
  - Too far, or blocked by obstacle
- =>Collision detection is not feasible
  - Wireless transceivers can't send and receive on the same channel at the same time
  - To be more precise: whenever collision detected , the signals cannot be sent to the sender device that the collision has been occured

IEEE 802.11 MAC Layer Standard

- Similar to Ethernet
- But consider the following:

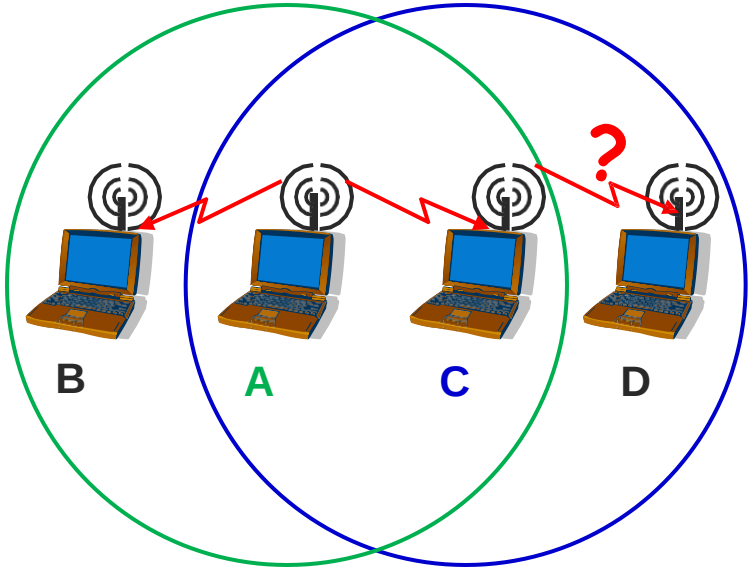


Hidden Terminal Problem

B and C are unaware of each other since their signals do not carry that far.=> collision at A, but neither B nor C is aware of this collision. (hidden nodes)

IEEE 802.11 MAC Layer Standard

- Another problem



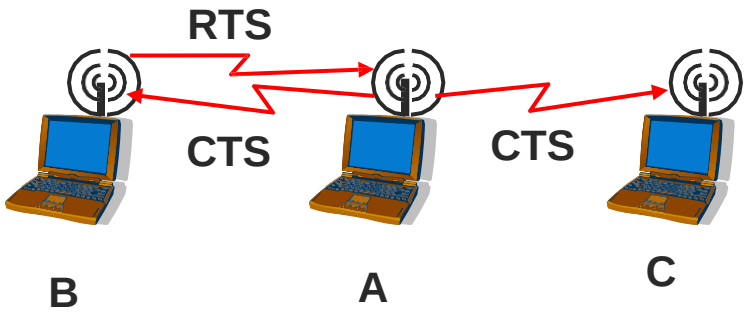
Exposed Terminal Problem

Mistake: for C to conclude that it cannot transmit to anyone just because it can hear A's transmission.
C can transmit to node D. This is not a problem since C's transmission to D will not interfere with B's ability to receive from A (but will interfere when B is transmitting to A)

IEEE 802.11 MAC Layer Standard – CSMA/CA

- Solution to the Hidden Terminal Problem
  - Request/Ready to Send (RTS)
  - Clear to Send (CTS)

The RTS (from B) may not be heard by a hidden terminal (C), the CTS probably will be. This **CTS** (from A) effectively tells the nodes (e.g. C) within range of the receiver that they should not send anything for a while (including the RTS and CTS packets.)



IEEE 802.11 MAC Layer Standard

- Solution to the Exposed Terminal Problem
  - Request to Send (RTS)
  - Clear to Send (CTS)