Netzwerktechnik und IT-Netze

Chapter 5: Link Layer

Vorlesung im WS 2016/2017

Bachelor Informatik

(3. Semester)

Prof. Dr. rer. nat. Andreas Berl

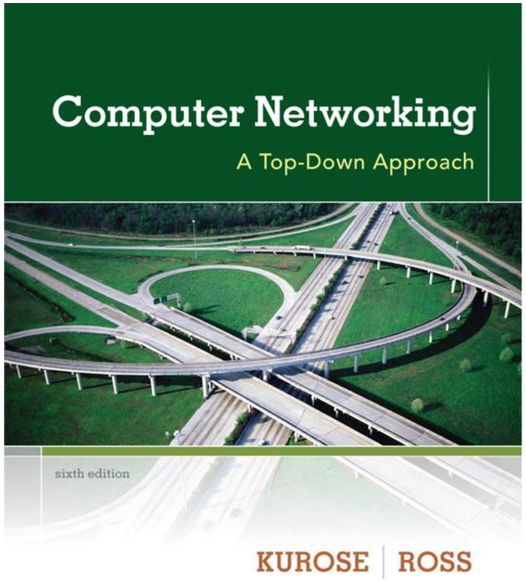
Fakultät für Elektrotechnik, Medientechnik und Informatik

Overview

- Introduction
- Computer Networks and the Internet
- Application Layer
  - WWW, Email, DNS, and more
  - Socket programming
  - Web service
- Transport Layer
- Network Layer
- Link Layer

Introduction

- A note on the use of these power point slides:
  -
  -



Computer Networking: A Top Down Approach
6th edition
Jim Kurose, Keith Ross
Addison-Wesley
March 2012

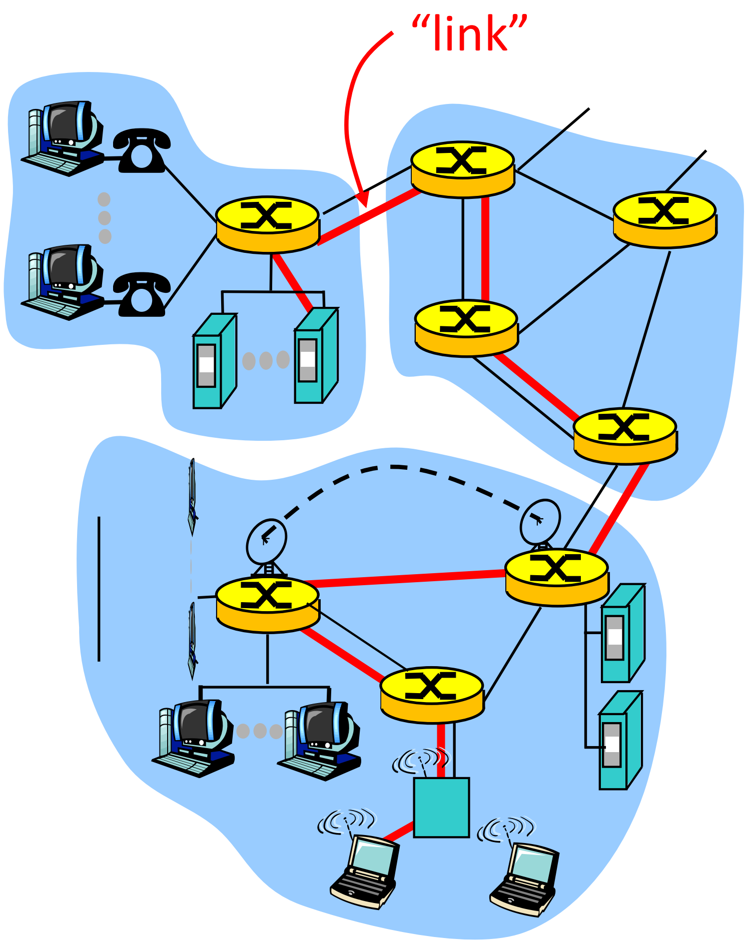
Link layer, LANs: outline

- Introduction and services
- Multiple access protocols
- LANs
  - Addressing, ARP
  - Ethernet
  - Switches

Link Layer: Introduction

Some terminology:

- Hosts and routers are **nodes**
- Communication channels that connect adjacent nodes along communication path are **links**
  - Wired links
  - Wireless links
  - LANs
- Layer-2 packet is a **frame**, encapsulates datagram



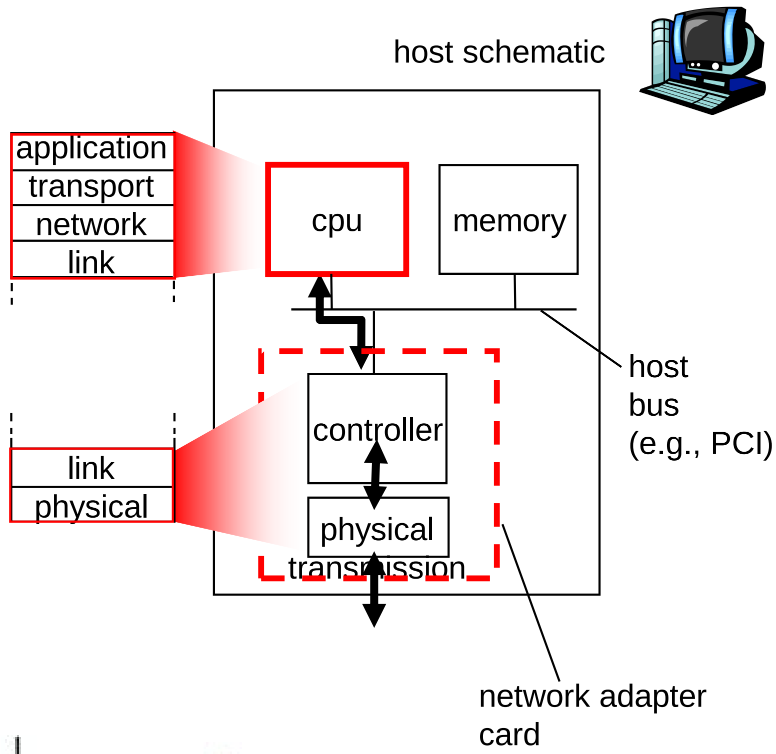
Data-link layer has responsibility of transferring datagram from one node to adjacent node over a link

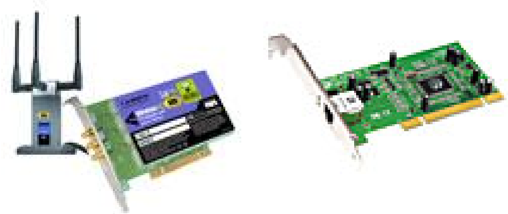
Link Layer Services (more)

- Flow Control:
  - Pacing between adjacent sending and receiving nodes
- Error Detection:
  - Errors caused by signal attenuation, noise.
  - Receiver detects presence of errors:
    - signals sender for retransmission or drops frame
- Error Correction:
  - Receiver identifies *and corrects* bit error(s) without resorting to retransmission
- Half-duplex and full-duplex
  - With half duplex, nodes at both ends of link can transmit, but not at same time

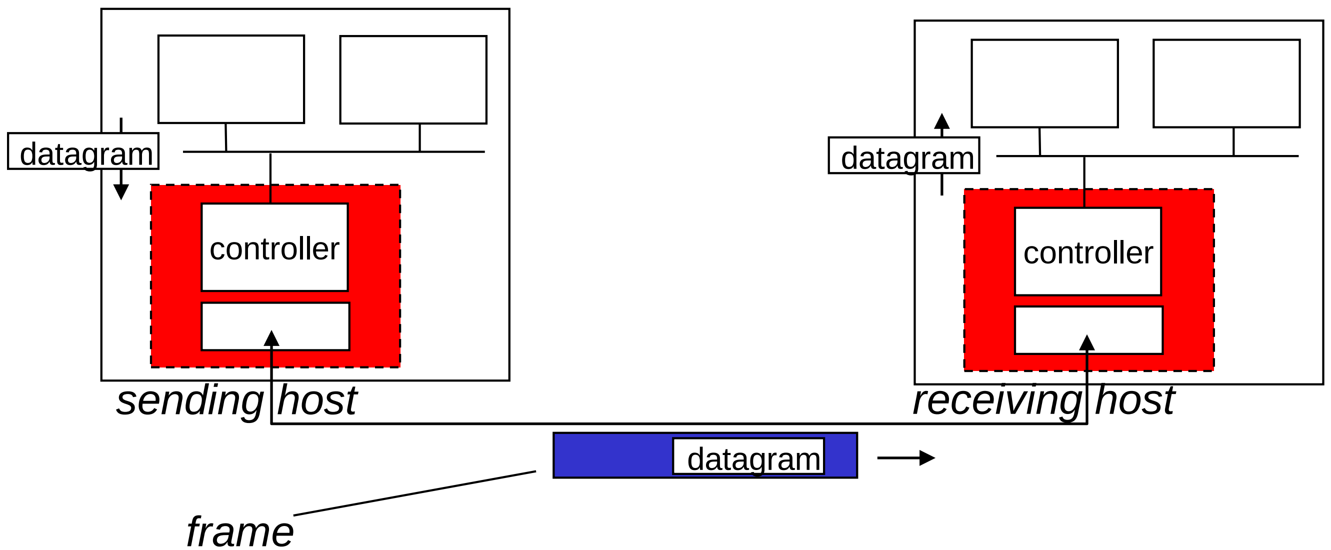
Where is the link layer implemented?

- In each and every host
- Link layer implemented in “adaptor” (a.k.a network interface card NIC)
  - Ethernet card, PCMCI card, 802.11 card
  - Implements link, physical layer
- Attaches into host’s system buses
- Combination of hardware, software, firmware





Adaptors Communicating



- Sending side:
  - Encapsulates datagram in a frame
  - Adds error checking bits, rdt, flow control, etc.
- receiving side
  - Looks for errors, rdt, flow control, etc.
  - Extracts datagram, passes to upper layer at receiving side

Link layer, LANs: outline

- Introduction and services
- Multiple access protocols
- LANs
  - Addressing, ARP
  - Ethernet
  - Switches

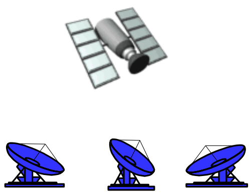
Multiple Access Links, Protocols

Two types of “links”:

- Point-to-Point
  - PPP for dial-up access
  - Point-to-Point link between Ethernet switch and host
- Broadcast (shared wire or medium)
  - Old-fashioned Ethernet
  - 802.11 wireless LAN

shared wire (e.g., cabled Ethernet)

shared RF (e.g., 802.11 WiFi)



shared RF (satellite)

humans at a cocktail party (shared air, acoustical)

Multiple Access protocols

- Single shared broadcast channel
- Two or more simultaneous transmissions by nodes: interference
  - Collision if node receives two or more signals at the same time

Multiple access protocol

- Distributed algorithm that determines how nodes share channel, i.e., Determine when node can transmit
- Communication about channel sharing must use channel itself!
  - No out-of-band channel for coordination

An Ideal Multiple Access Protocol

- Given: Broadcast channel of rate R bps
- Desiderata:

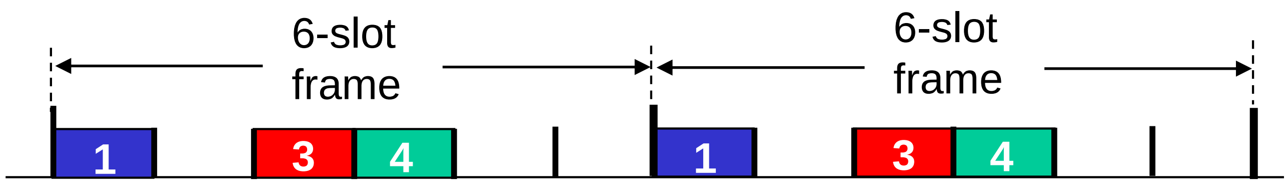
1. When one node wants to transmit, it can send at rate R.
2. When M nodes want to transmit, each can send at average rate R/M
3. Fully decentralized:
   - No special node to coordinate transmissions
   - No synchronization of clocks, slots
4. Simple

MAC Protocols: Taxonomy

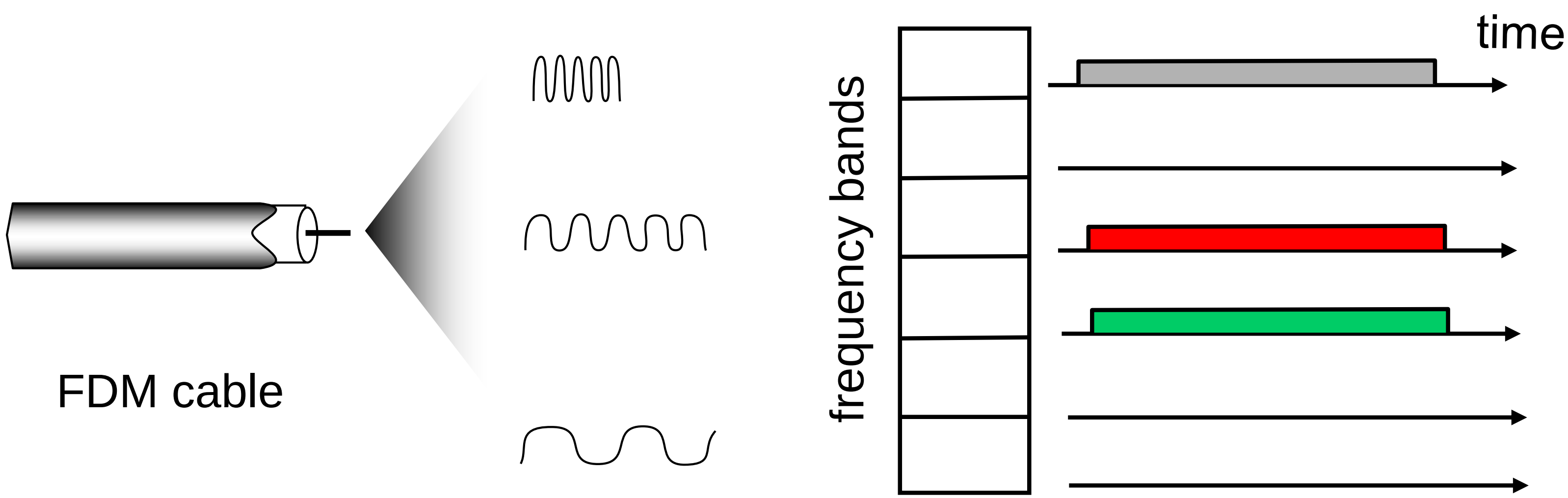
- Three broad classes:
  - Channel Partitioning
    - Divide channel into smaller “pieces” (time slots, frequency, code)
    - Allocate piece to node for exclusive use
  - Random access
    - Channel not divided, allow collisions
    - “Recover” from collisions
  - “Taking turns”
    - Nodes take turns, but nodes with more to send can take longer turns

Channel Partitioning MAC protocols: TDMA/FDMA

- TDMA: frequency division multiple access



- FDMA: frequency division multiple access



Random Access Protocols

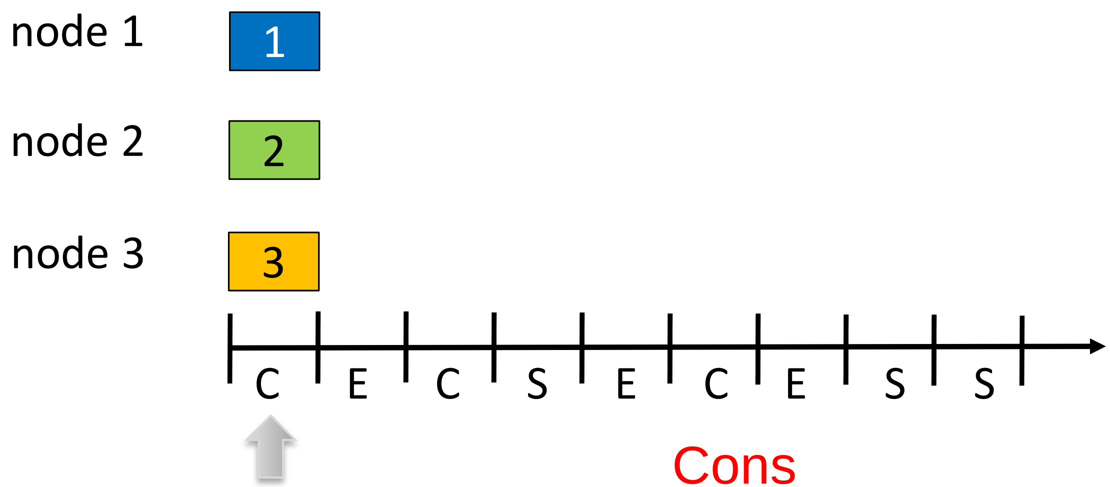
- When node has packet to send
  - Transmit at full channel data rate R.
  - No *a priori* coordination among nodes
- Two or more transmitting nodes ➜ “collision”,
- Random access MAC protocol specifies:
  - How to detect collisions
  - How to recover from collisions (e.g., via delayed retransmissions)
- Examples of random access MAC protocols:
  - Slotted ALOHA
  - ALOHA
  - CSMA, CSMA/CD, CSMA/CA

Slotted ALOHA

- Assumptions
  - All frames same size
  - Time is divided into equal size slots (time to transmit 1 frame)
  - Nodes start to transmit frames only beginning
  - Nodes are synchronized
  - If 2 or more nodes transmit in slot, all nodes detect collision

- Operation
  - When node obtains fresh frame, it transmits in next slot
    - If no collision, node can send new frame in next slot
    - If collision: node retransmits frame in each subsequent slot with probability p until success

Slotted ALOHA



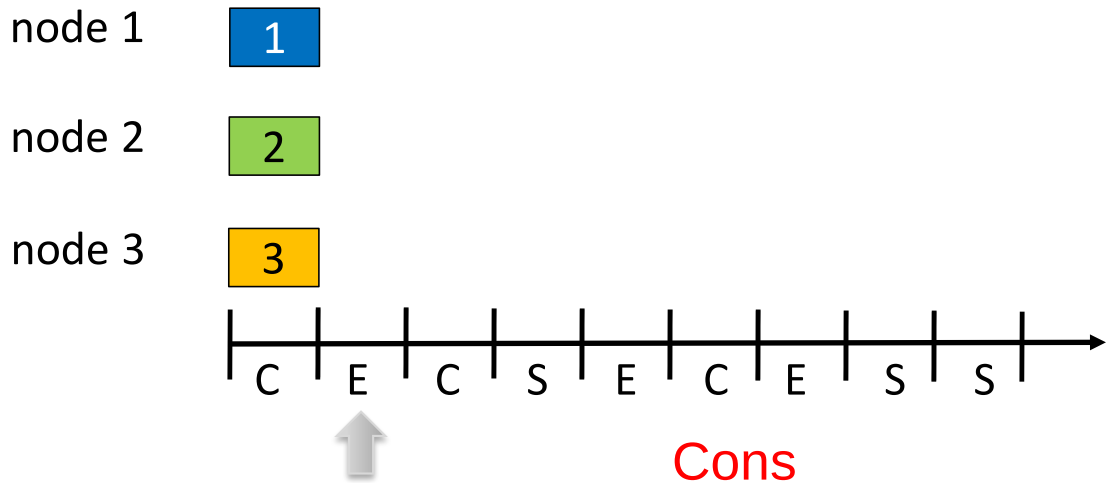
Pros

- Single active node can continuously transmit at full rate of channel
- Highly decentralized: only slots in nodes need to be in sync
- Simple

Cons

- Collisions, wasting slots
- Idle slots are also wasted
- Nodes may be able to detect collision in less than time to transmit packet
- Clock synchronization

Slotted ALOHA



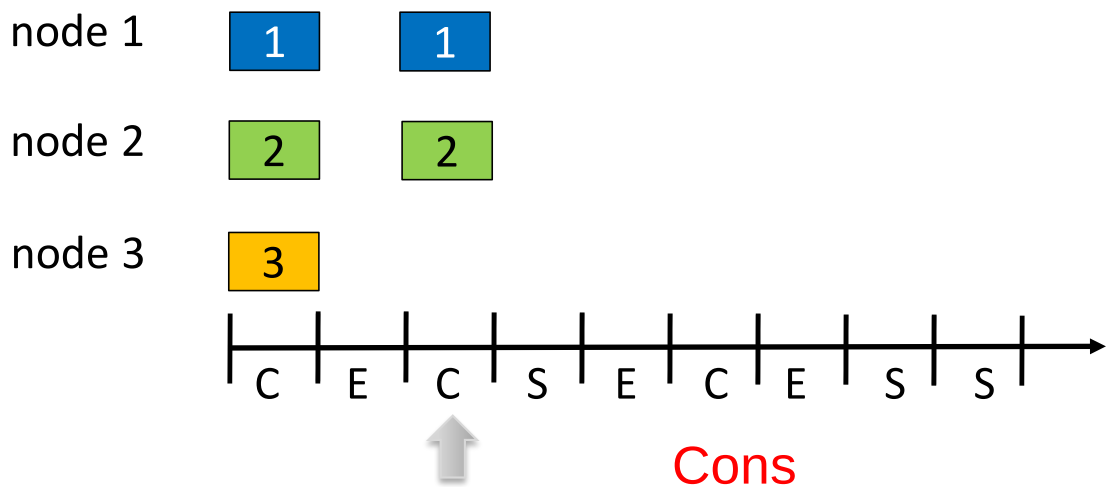
Pros

- Single active node can continuously transmit at full rate of channel
- Highly decentralized: only slots in nodes need to be in sync
- Simple

Cons

- Collisions, wasting slots
- Idle slots are also wasted
- Nodes may be able to detect collision in less than time to transmit packet
- Clock synchronization

Slotted ALOHA



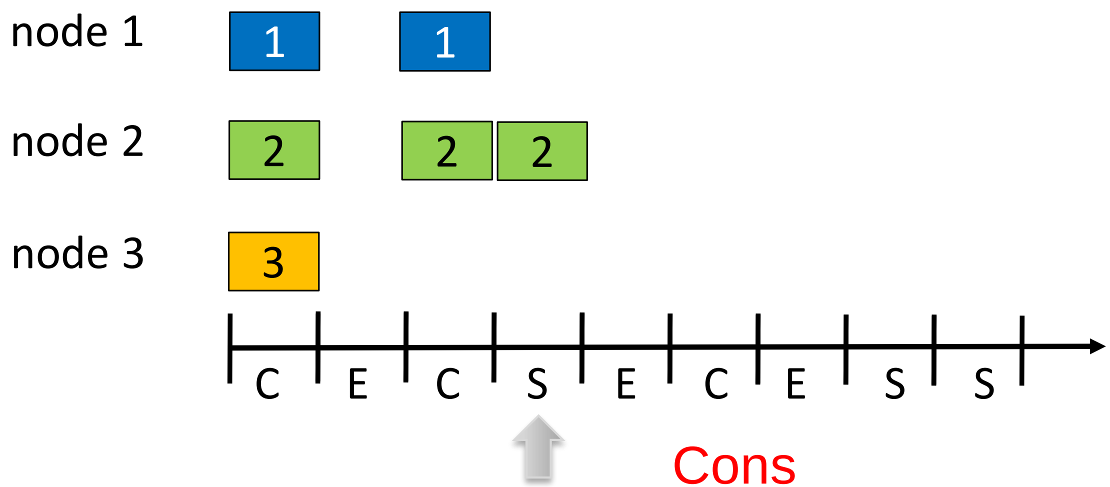
Pros

- Single active node can continuously transmit at full rate of channel
- Highly decentralized: only slots in nodes need to be in sync
- Simple

Cons

- Collisions, wasting slots
- Idle slots are also wasted
- Nodes may be able to detect collision in less than time to transmit packet
- Clock synchronization

Slotted ALOHA



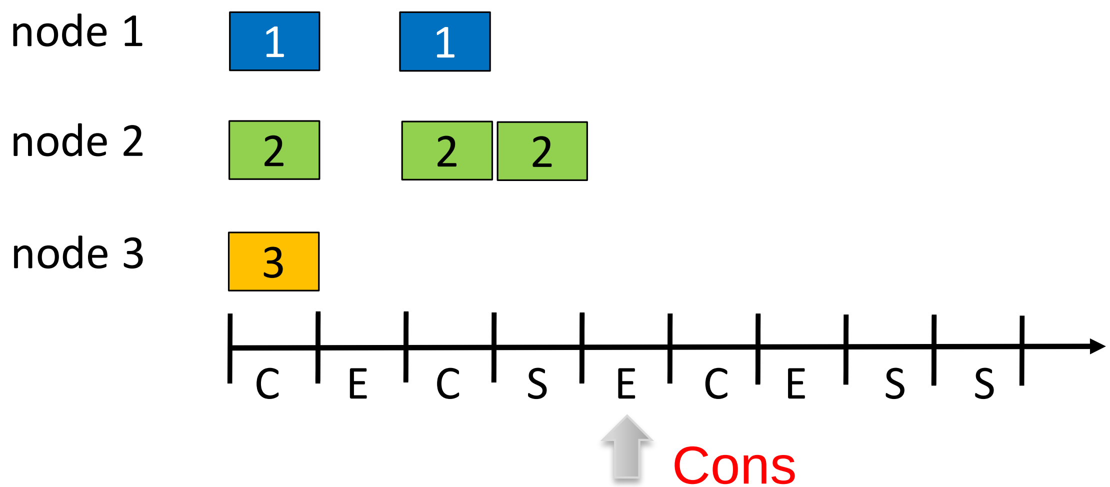
Pros

- Single active node can continuously transmit at full rate of channel
- Highly decentralized: only slots in nodes need to be in sync
- Simple

Cons

- Collisions, wasting slots
- Idle slots are also wasted
- Nodes may be able to detect collision in less than time to transmit packet
- Clock synchronization

Slotted ALOHA



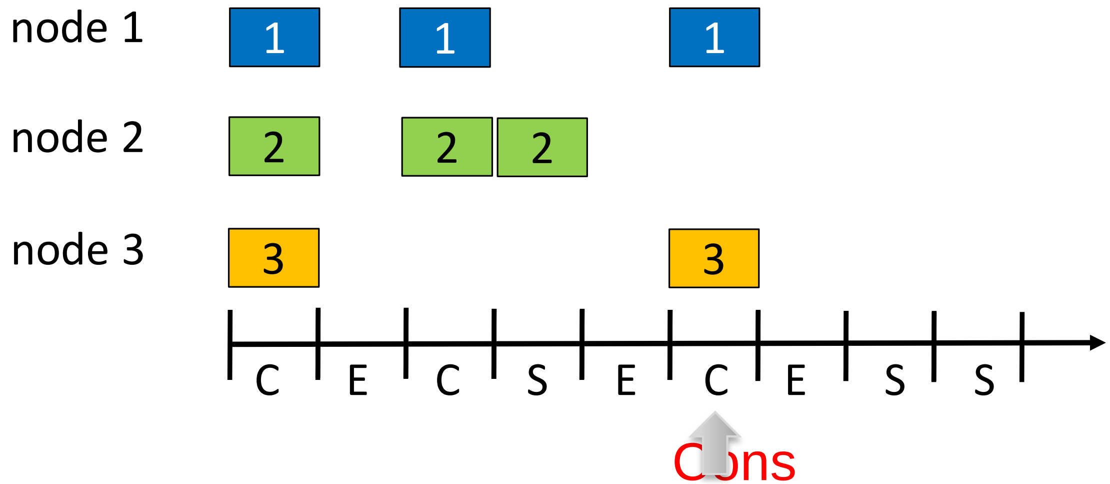
<u>Pros</u>

- Single active node can continuously transmit at full rate of channel
- Highly decentralized: only slots in nodes need to be in sync
- Simple

<u>Cons</u>

- Collisions, wasting slots
- Idle slots are also wasted
- Nodes may be able to detect collision in less than time to transmit packet
- Clock synchronization

Slotted ALOHA



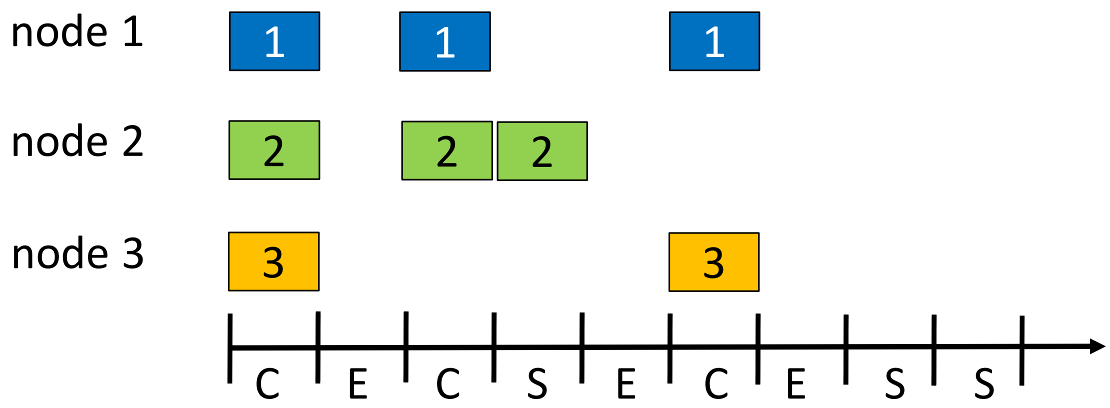
Pros

- Single active node can continuously transmit at full rate of channel
- Highly decentralized: only slots in nodes need to be in sync
- Simple

Cons

- Collisions, wasting slots
- Idle slots are also wasted
- Nodes may be able to detect collision in less than time to transmit packet
- Clock synchronization

Slotted ALOHA



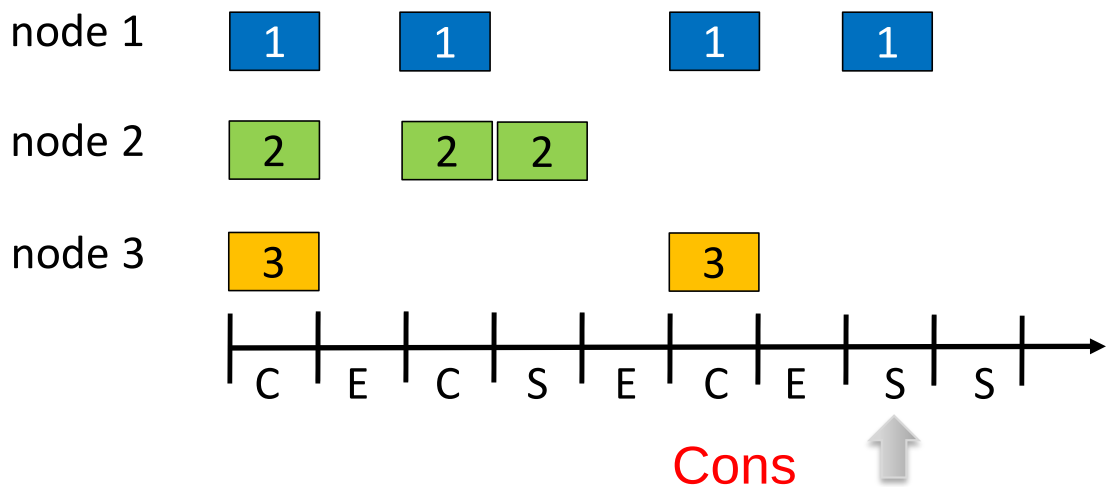
Pros

- Single active node can continuously transmit at full rate of channel
- Highly decentralized: only slots in nodes need to be in sync
- Simple

Cons

- Collisions, wasting slots
- Idle slots are also wasted
- Nodes may be able to detect collision in less than time to transmit packet
- Clock synchronization

Slotted ALOHA



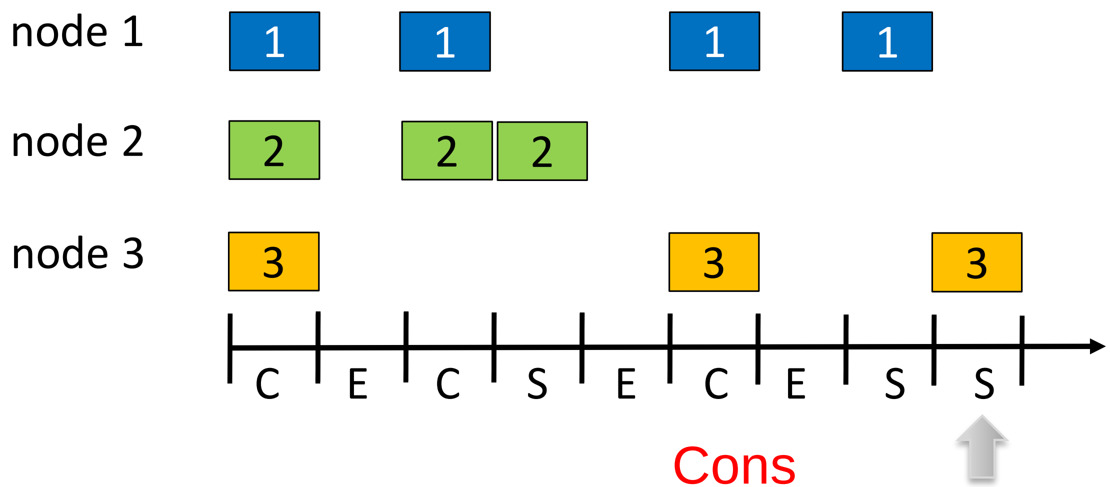
<u>Pros</u>

- Single active node can continuously transmit at full rate of channel
- Highly decentralized: only slots in nodes need to be in sync
- Simple

<u>Cons</u>

- Collisions, wasting slots
- Idle slots are also wasted
- Nodes may be able to detect collision in less than time to transmit packet
- Clock synchronization

Slotted ALOHA



Pros

- Single active node can continuously transmit at full rate of channel
- Highly decentralized: only slots in nodes need to be in sync
- Simple

Cons

- Collisions, wasting slots
- Idle slots are also wasted
- Nodes may be able to detect collision in less than time to transmit packet
- Clock synchronization

Slotted Aloha efficiency

Efficiency : Long-run fraction of successful slots (many nodes, each with many frames to send)

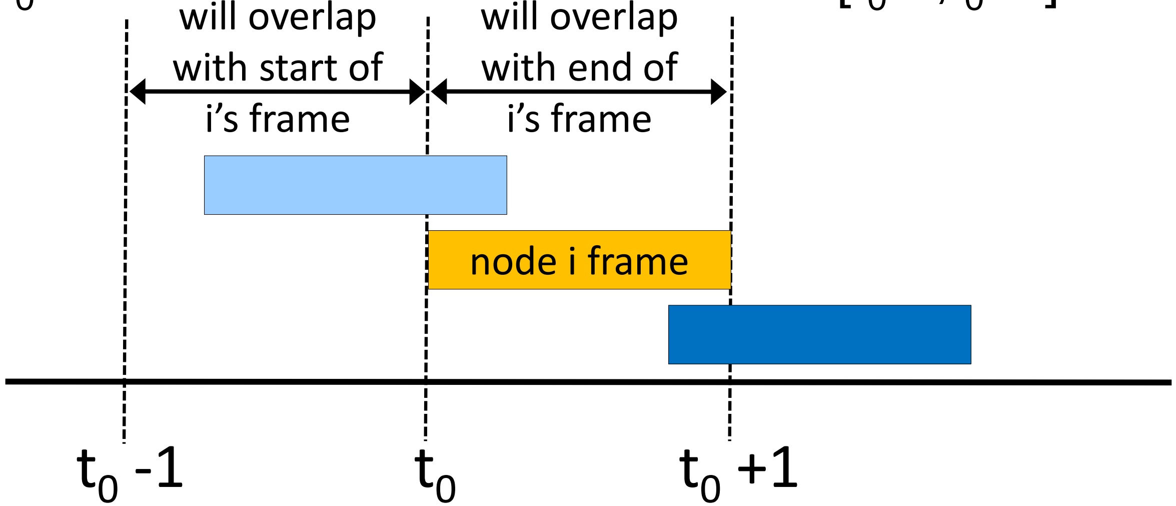
- Suppose N nodes with many frames to send, each transmits in slot with probability *p*
- Prob that node 1 has success in a slot = $p(1-p)^{N-1}$
- Prob that any node has a success = $Np(1-p)^{N-1}$

- For max efficiency with N nodes, find p* that maximizes $Np(1-p)^{N-1}$
- For many nodes, take limit of $Np^*(1-p^*)^{N-1}$ as N goes to infinity, gives 1/e = 0.37

At best: channel used for useful transmissions 37% of time!

Pure (unslotted) ALOHA

- Unslotted Aloha: simpler, no synchronization
- When frame first arrives
  - Transmit immediately
- Collision probability increases:
  - Frame sent at t_0 collides with other frames sent in $[t_0-1, t_0+1]$



Pure Aloha efficiency

P(success by given node) = P(node transmits) $\cdot$

P(no other node transmits in $[t_0\text{-}1,t_0]$ $\cdot$

P(no other node transmits in $[t_0\text{-}1,t_0]$

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

$= p \,.\, (1\text{-}p)^{2}(N\text{-}1)$

… Choosing optimum p and then letting n → ∞

= 1/(2e) = 0.18

Even worse than slotted Aloha!

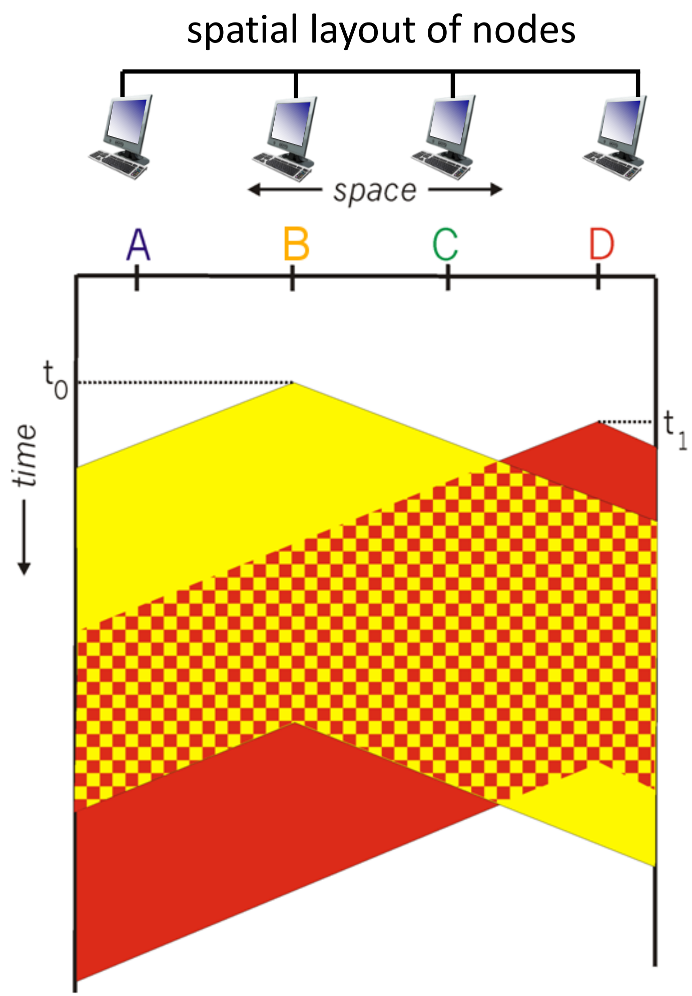
Prof. Dr. rer. nat. Andreas Berl – www.andreas-berl.de

CSMA
(Carrier Sense Multiple Access)

- CSMA: Listen before transmit:
  - If channel sensed idle: Transmit entire frame
  - If channel sensed busy: defer transmission
  - Human analogy: don’t interrupt others!

CSMA Collisions

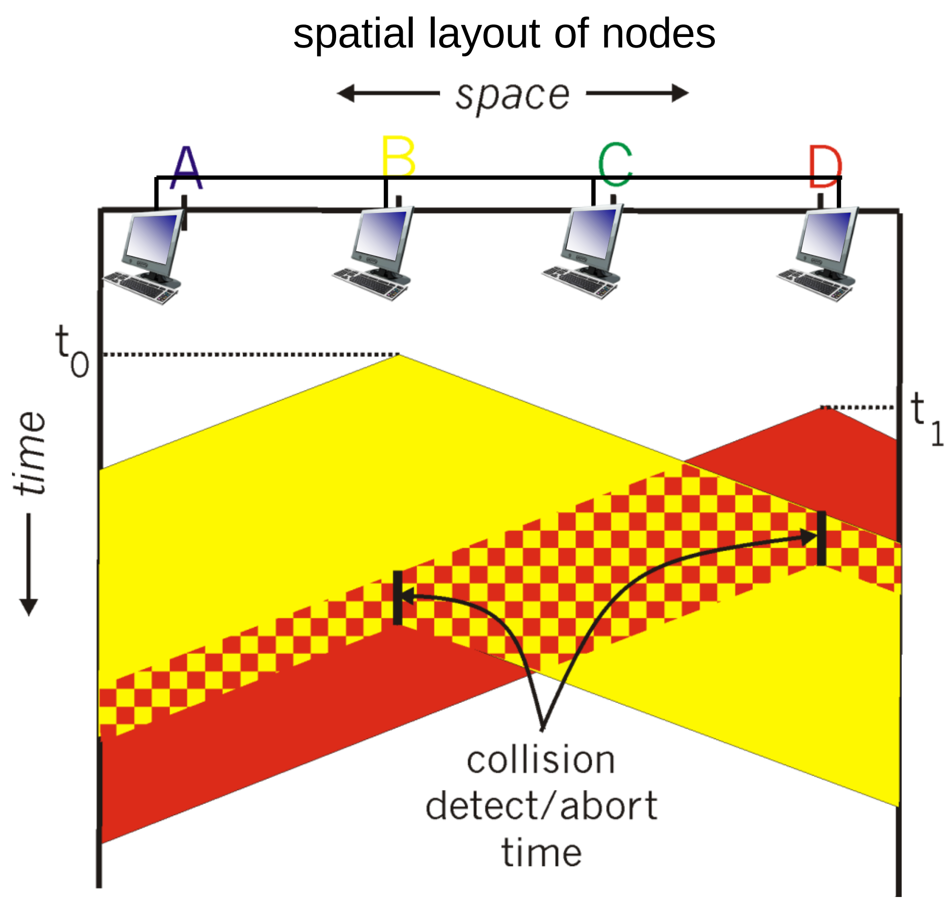
- Collisions can still occur
  - Propagation delay means two nodes may not hear each other’s transmission
- Collision
  - Entire packet transmission time wasted
    - Distance & propagation delay play role in in determining collision probability



CSMA/CD (Collision Detection)

- CSMA/CD: carrier sensing, deferral as in CSMA
  - Collisions *detected* within short time
  - Colliding transmissions aborted, reducing channel wastage
- Collision detection:
  - Easy in wired LANs: Measure signal strengths, compare transmitted, received signals
  - Difficult in wireless LANs: Received signal strength overwhelmed by local transmission strength
- Human analogy: The polite conversationalist

CSMA/CD collision detection



Prof. Dr. rer. nat. Andreas Berl – www.andreas-berl.de

Ethernet CSMA/CD algorithm

1. NIC receives datagram from network layer, creates frame
2. If NIC senses channel idle, starts frame transmission. If NIC senses channel busy, waits until channel idle, then transmits.
3. If NIC transmits entire frame without detecting another transmission, NIC is done with frame !

4) If NIC detects another transmission while transmitting, aborts and sends **jam signal**

5) After aborting, NIC enters binary (exponential) backoff:
   - After m^{th} collision, NIC chooses K at random from {0,1,2, ..., 2^m-1}. NIC waits K·512 bit times, returns to step 2
   - Longer backoff interval with more collisions

CSMA/CD efficiency

- t_{prop} = Max prop delay between 2 nodes in LAN
- t_{trans} = Time to transmit max-size frame

$$efficiency = \frac{1}{1 + 5t_{prop}/t_{trans}}$$

- Efficiency goes to 1
  - As t_{prop} goes to 0
  - As t_{trans} goes to infinity
- Better performance than ALOHA: and simple, cheap, decentralized!

“Taking Turns” MAC protocols

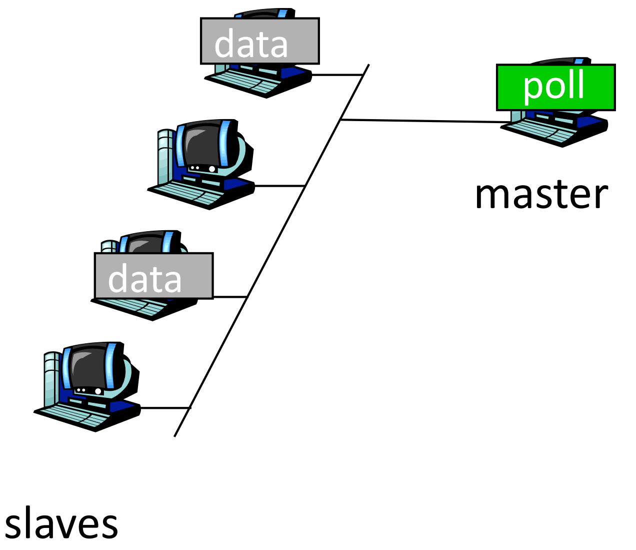
- Channel partitioning MAC protocols:
  - Share channel efficiently and fairly at high load
  - Inefficient at low load: delay in channel access, 1/N bandwidth allocated even if only 1 active node!
- Random access MAC protocols
  - Efficient at low load: single node can fully utilize channel
  - High load: collision overhead
- “taking turns” protocols
  - Look for best of both worlds!

Prof. Dr. rer. nat. Andreas Berl – www.andreas-berl.de

"Taking Turns" MAC protocols

Polling:

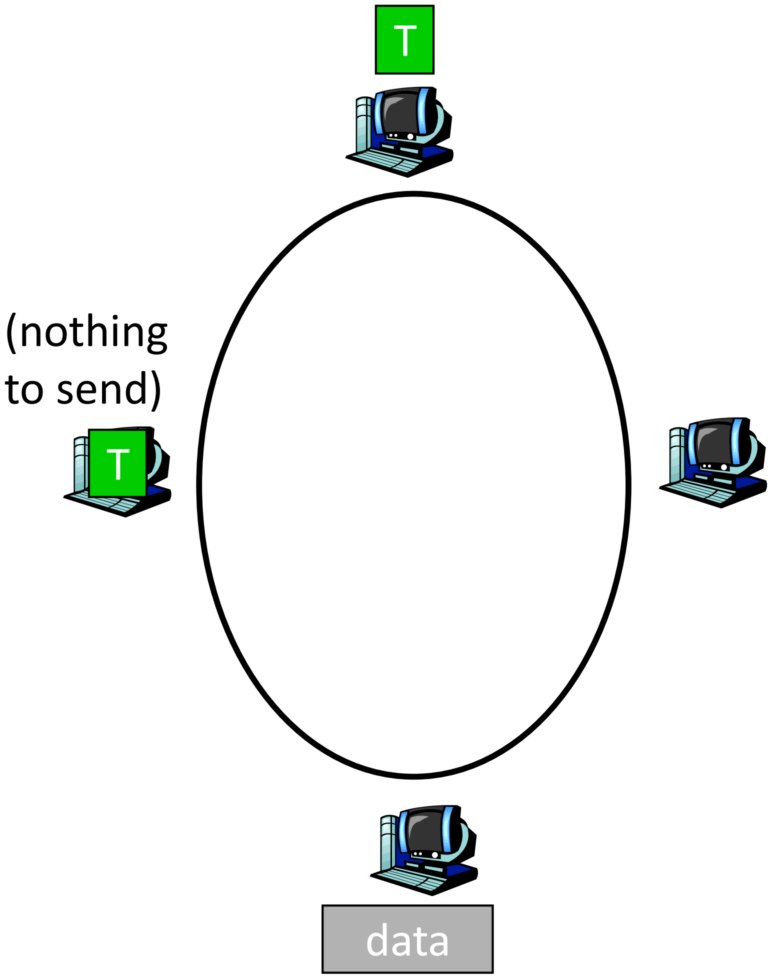
- Master node "invites" slave nodes to transmit in turn
- Typically used with "dumb" slave devices
- Concerns:
  - Polling overhead
  - Latency
  - Single point of failure (master)



"Taking Turns" MAC protocols

Token passing:

- Control token passed from one node to next sequentially.
- Token message
- Concerns:
  - Token overhead
  - Latency
  - Single point of failure (token)



Link layer, LANs: outline

- Introduction and services
- Error detection and correction
- Multiple access protocols
- LANs
  - Addressing, ARP
  - Ethernet
  - Switches

Prof. Dr. rer. nat. Andreas Berl – www.andreas-berl.de

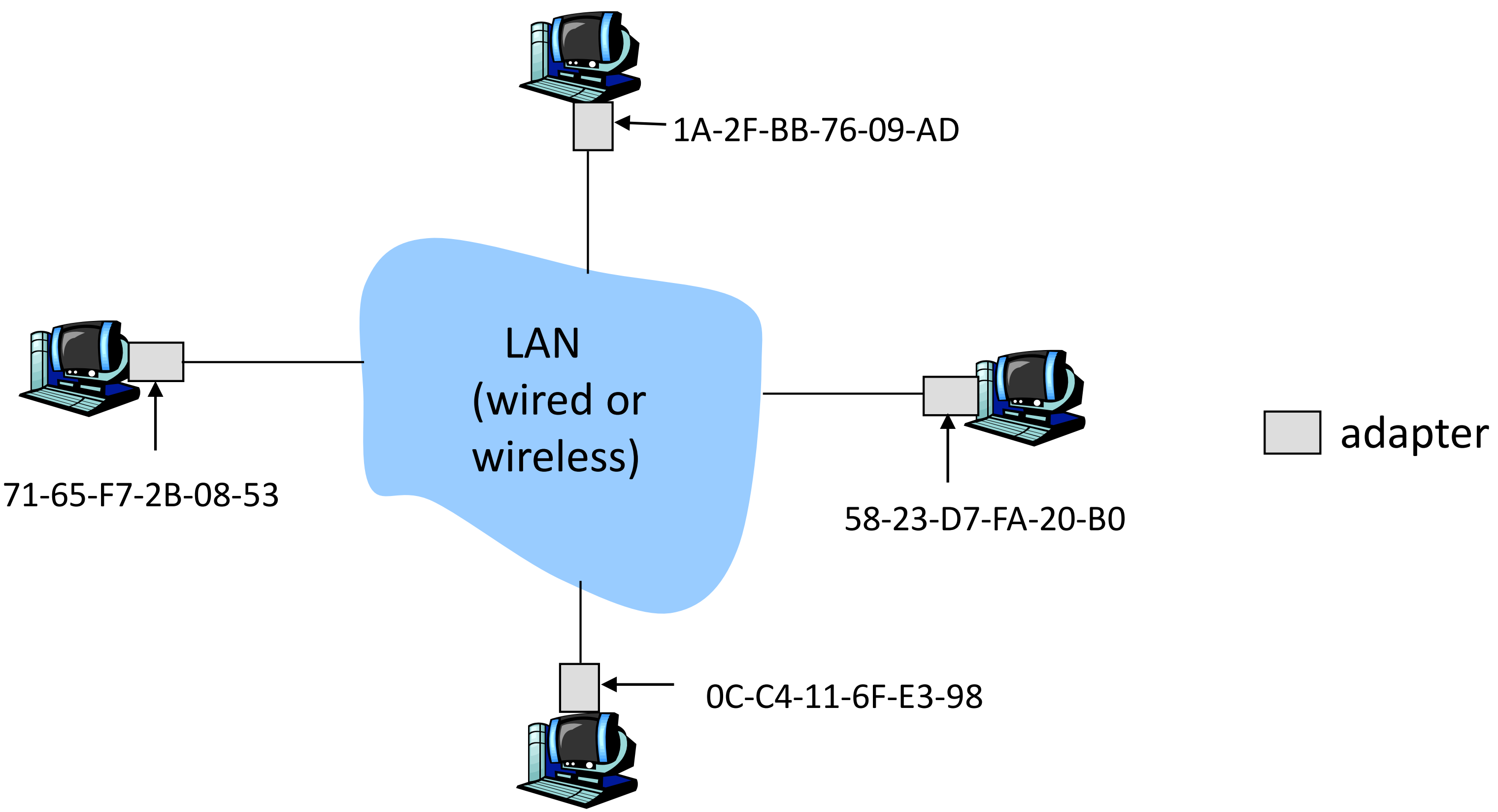
MAC Addresses and ARP

- 32-bit IP address:
  - Network-layer address
  - Used for layer 3 (network layer) forwarding
- MAC (or LAN or physical or Ethernet) address:
  - Function: Used 'locally" to get frame from one interface to another physically-connected interface (same network, in IP-addressing sense)
  - 48 bit MAC address (for most LANs) burned in NIC ROM, also sometimes software settable
  - e.g.: 1A-2F-BB-76-09-AD

Hexadecimal (base 16) notation
(each "number" represents 4 bits)

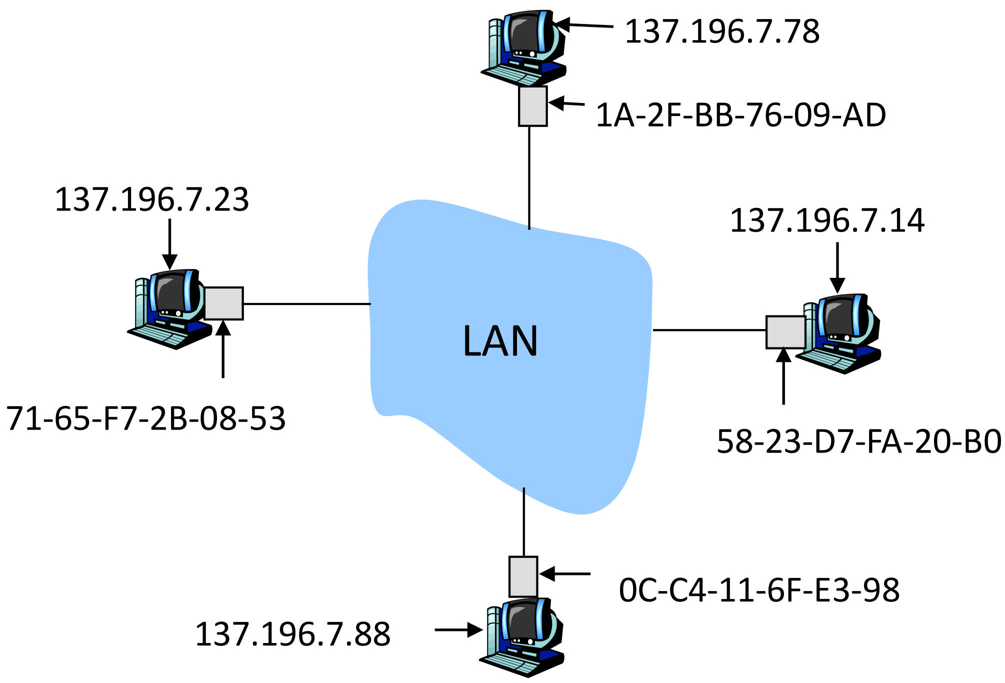
LAN Addresses and ARP

Each adapter on LAN has unique LAN address



ARP: Address Resolution Protocol

Question: How to determine MAC address of B knowing B's IP address?



- Each IP node (Host, Router) on LAN has ARP table
- ARP Table: IP/MAC address mappings for some LAN nodes

  < IP address; MAC address; TTL>

  - TTL (Time To Live): time after which address mapping will be forgotten (typically 20 min)

ARP protocol: Same LAN

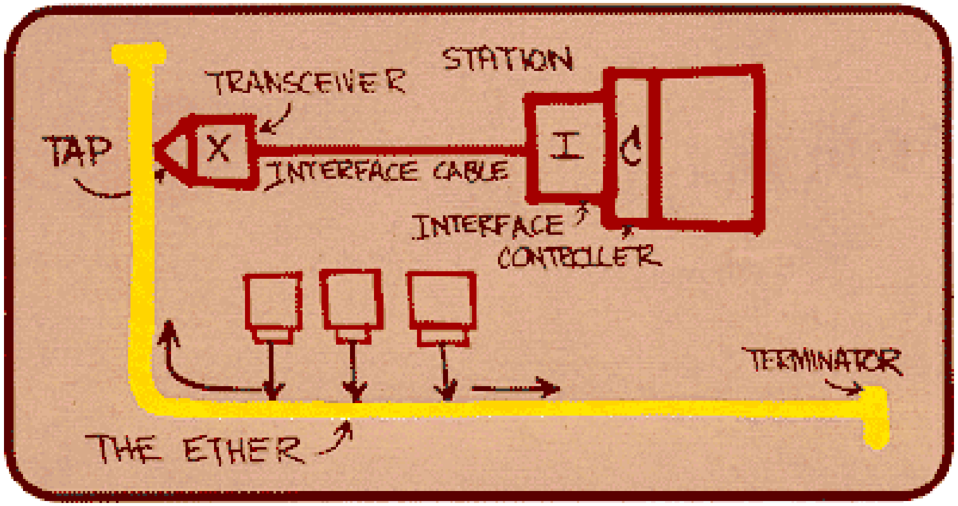
- A wants to send datagram to B, and B’s MAC address not in A’s ARP table.
- A broadcasts ARP query packet, containing B's IP address
  - Dest MAC address = FF-FF-FF-FF-FF-FF
  - All machines on LAN receive ARP query
- B receives ARP packet, replies to A with its (B's) MAC address
  - Frame sent to A’s MAC address (unicast)
- A caches (saves) IP-to-MAC address pair in its ARP table until information becomes old (times out)
  - Soft state: Information that times out (goes away) unless refreshed
- ARP is “plug-and-play”:
  - Nodes create their ARP tables without intervention from net administrator

Link layer, LANs: outline

- Introduction and services
- Error detection and correction
- Multiple access protocols
- LANs
  - Addressing, ARP
  - Ethernet
  - Switches

Ethernet

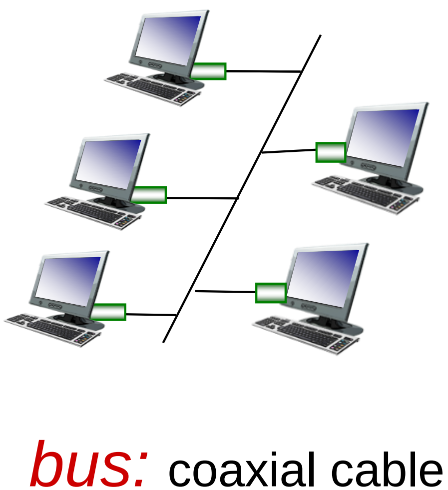
- “Dominant” wired LAN technology:
  - Cheap $20 for NIC
  - First widely used LAN technology
  - Simpler, cheaper than token LANs and ATM
  - Kept up with speed race: 10 Mbps – 10 Gbps

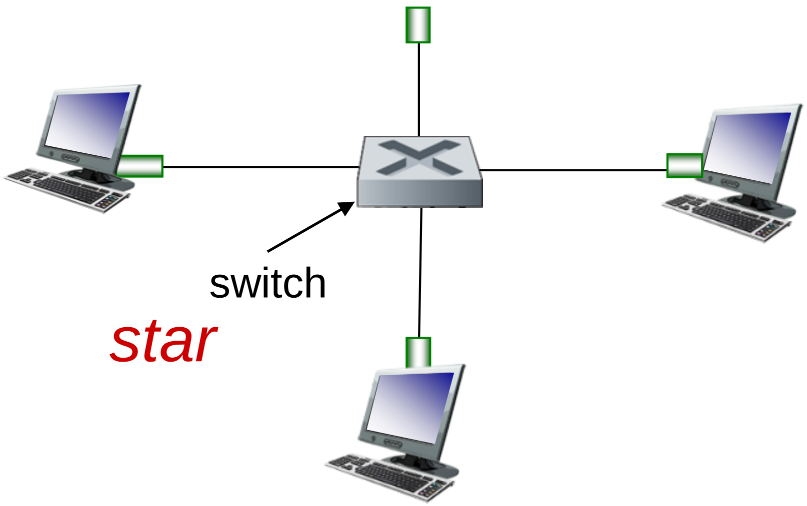


Metcalfe’s Ethernet sketch

Star topology

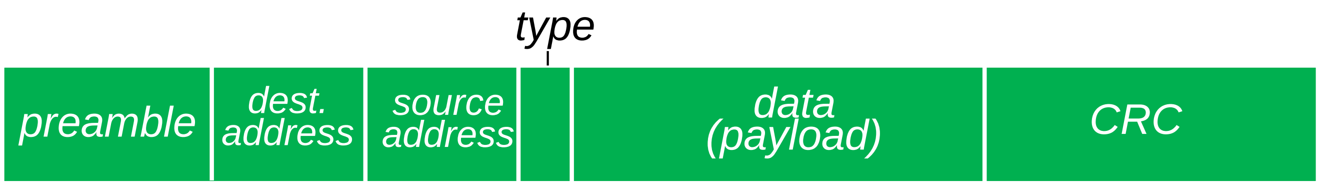
- Bus topology popular through mid 90s
  - All nodes in same collision domain (can collide with each other)
- Today: star topology prevails
  - Active *switch* in center
  - Each "spoke" runs a (separate) Ethernet protocol (nodes do not collide with each other)





Ethernet Frame Structure

- Sending adapter encapsulates IP datagram (or other network layer protocol packet) in Ethernet frame



- preamble
  - 7 bytes with pattern 10101010 followed by one byte with pattern 10101011
  - Used to synchronize receiver, sender clock rates

Prof. Dr. rer. nat. Andreas Berl – www.andreas-berl.de

Ethernet Frame Structure (more)

- Addresses: 6 byte source, destination MAC adresses
  - If adapter receives frame with matching destination address, or with broadcast address (e.g. ARP packet), it passes data in frame to net-layer protocol
  - Otherwise, adapter discards frame
- Type: indicates the higher layer protocol (mostly IP but others may be supported such as Novell IPX and AppleTalk)
- CRC: Cyclic redundancy checked at receiver
  - Error is detected, the frame is dropped

Ethernet:
Unreliable, connectionless

- Connectionless: No handshaking between sending and receiving NICs
- Unreliable: Receiving NIC doesn't send ACKs or NACKs to sending NIC
  - Data in dropped frames recovered only if initial sender uses higher layer rdt (e.g., TCP), otherwise dropped data lost
- Ethernet's MAC protocol: unslotted CSMA/CD with binary backoff

Chapter 5: Summary

- Principles behind data link layer services:
  - Error detection, correction
  - Sharing a broadcast channel: multiple access
  - Link layer addressing
- Instantiation and implementation of various link layer technologies
  - Ethernet