Introduction to Computer Networks

COSC 4377

Lecture 19

Spring 2012

April 2, 2012

Announcements

- HW9 due this week
- HW10 out
- HW11 and HW12 coming soon!
- Student presentations

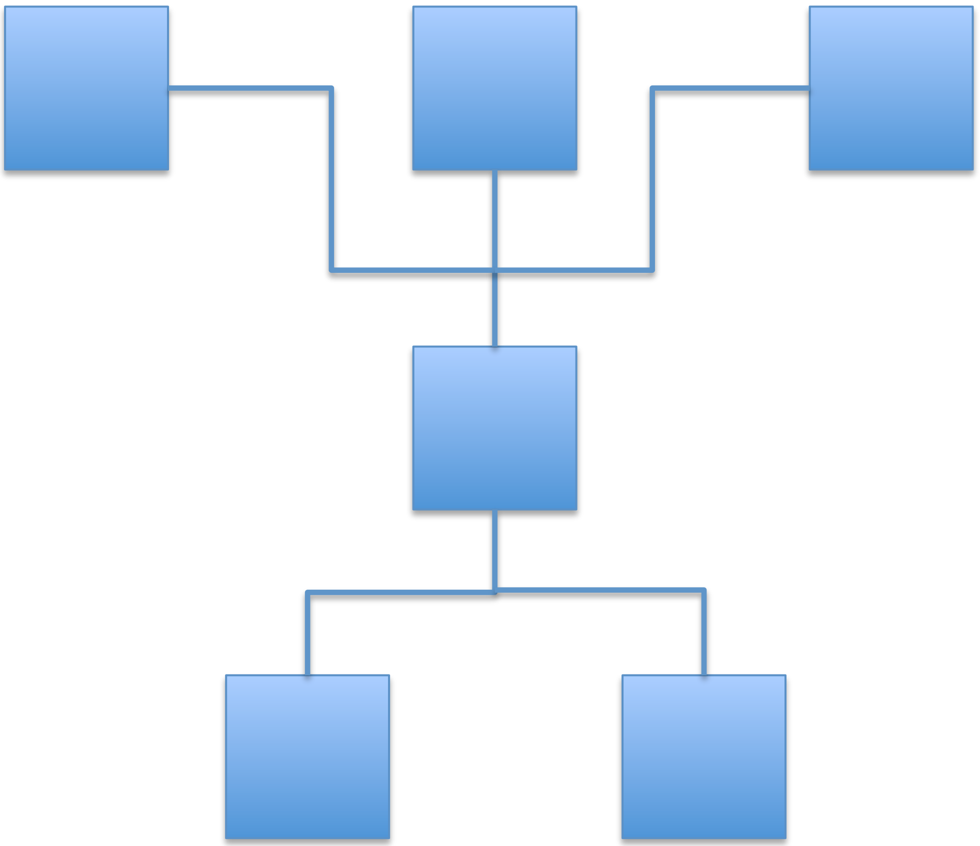
HW9

- Capture packets using Wireshark
- Plot CDF

Today’s Topics

- Link Layer
  - Media Access
  - Switching

Wired Media Access



Link Layer

- Single-hop addressing
- Media Access
- Single-hop reliability

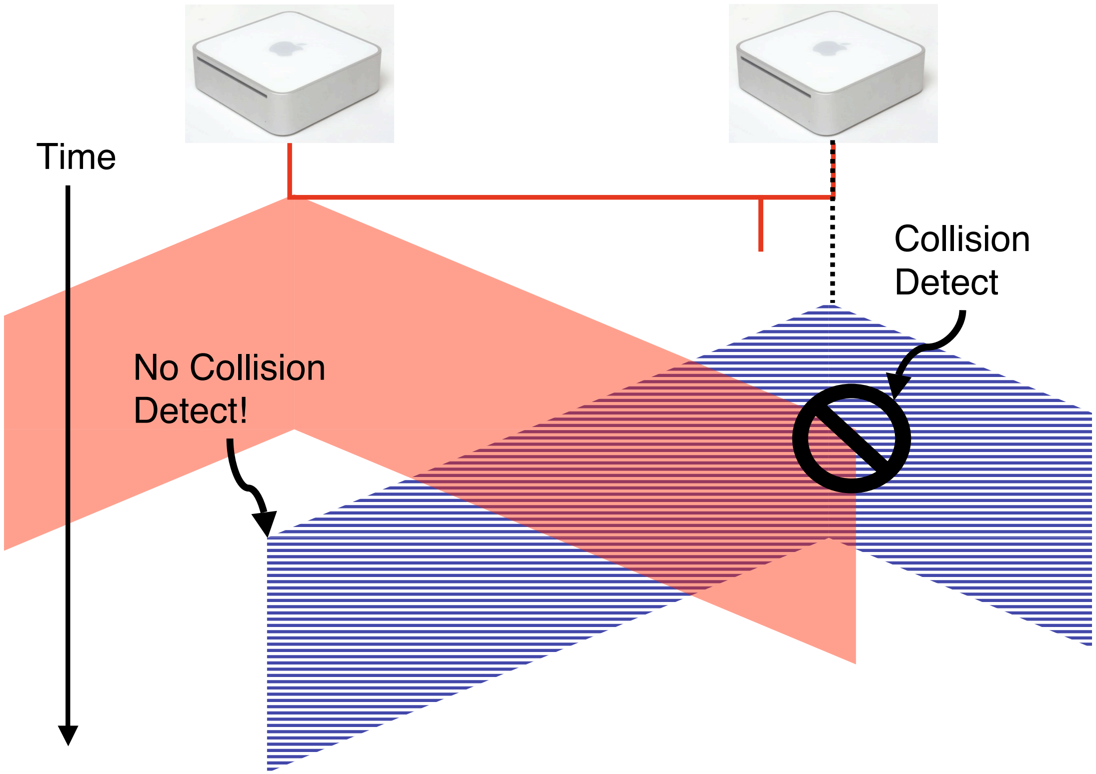
Media Access Control

- Control access to shared physical medium
  - E.g., who can talk when?
  - If everyone talks at once, no one hears anything
  - Job of the Link Layer
- Two conflicting goals
  - Maximize utilization when one node sending
  - Approach 1/N allocation when N nodes sending

Different Approaches

- Partitioned Access
  - Time Division Multiple Access (TDMA)
  - Frequency Division Multiple Access (FDMA)
  - Code Division Multiple Access (CDMA)
- Random Access
  - ALOHA/ Slotted ALOHA
  - Carrier Sense Multiple Access / Collision Detection (CSMA/CD)
  - Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA)
  - RTS/CTS (Request to Send/Clear to Send)
  - Token-based

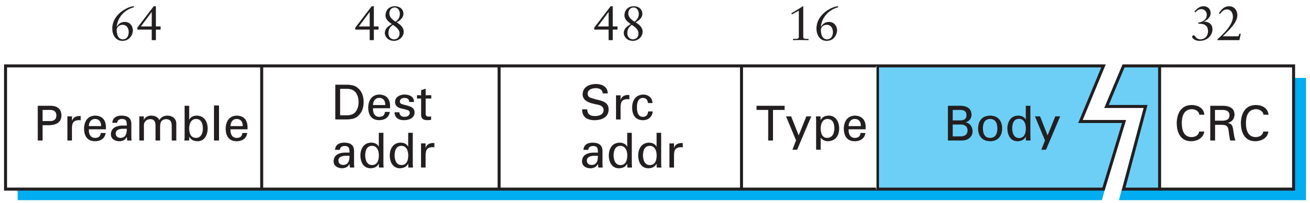
Collision Detection



- Without minimum frame length, might not detect collision

Case Study: Ethernet (802.3)

- Dominant wired LAN technology
- Both Physical and Link Layer specification
- CSMA/CD
  - Carrier Sense / Multiple Access / Collision Detection
- Frame Format (Manchester Encoding):



Ethernet MAC

- Problem: shared medium
  - 10Mbps: 2500m, with 4 repeaters at 500m
- Transmit algorithm
  - If line is idle, transmit immediately
  - Upper bound message size of 1500 bytes
  - Must wait 9.6μs between back to back frames
  - If line is busy: wait until idle and transmit immediately

Handling Collisions

- Collision detection (10Base2 Ethernet)
  - Uses Manchester encoding
  - Constant average voltage unless multiple transmitters
- If collision
  - Jam for 32 bits, then stop transmitting frame
- Collision detection constrains protocol
  - Imposes min. packet size (64 bytes or 512 bits)
  - Imposes maximum network diameter (2500m)
  - Ensure transmission time ≥ 2x propagation delay (why?)

When to transmit again?

- Delay and try again: exponential backoff
- *n*th time: $k \times 51.2\mu s$, for $k = U\{0..2^{\min(n,10)}-1\}$
  - 1^{st} time: 0 or 51.2μs
  - 2^{nd} time: 0, 51.2, 102.4, or 153.6μs
- Give up after several times (usually 16)

Capture Effect

- Exponential backoff leads to self-adaptive use of channel
- A and B are trying to transmit, and collide
- Both will back off either 0 or 51.2μs
- Say A wins.
- Next time, collide again.
  - A will wait between 0 or 1 slots
  - B will wait between 0, 1, 2, or 3 slots
- …

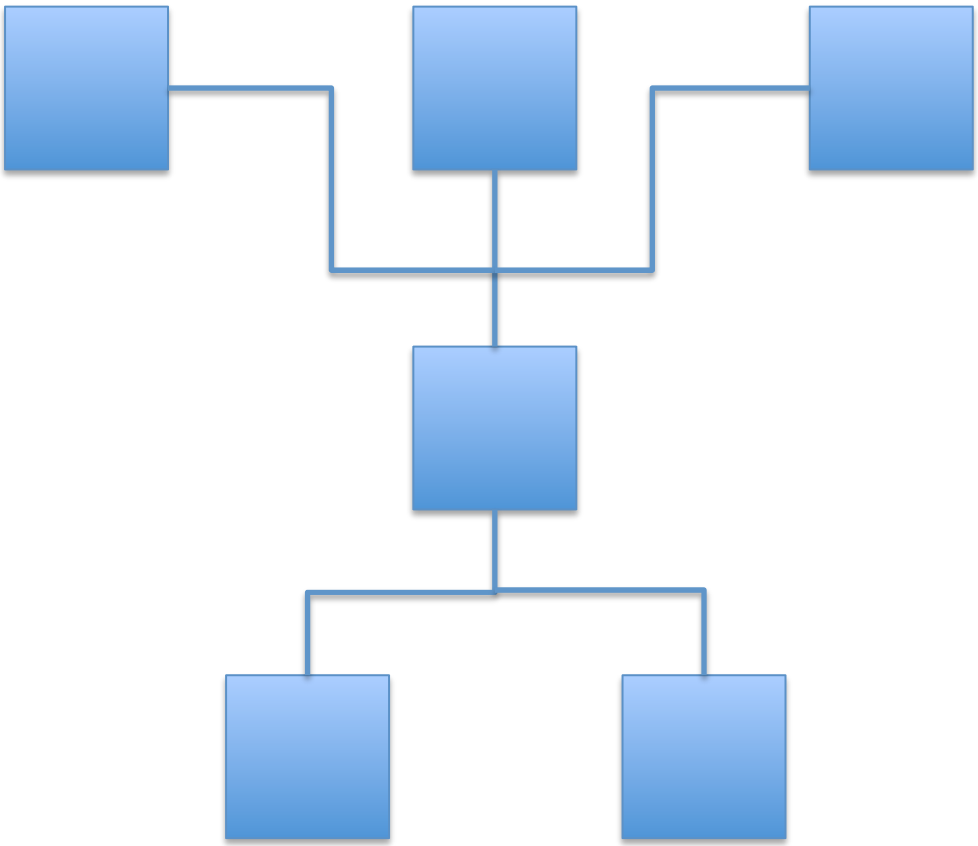
Ethernet Addressing

- Globally unique, 48-bit unicast address per adapter
  - Example: 00:1c:43:00:3d:09 (Samsung adapter)
  - 24 msb: organization
  - http://standards.ieee.org/develop/regauth/oui/oui.txt
- Broadcast address: all 1s
- Multicast address: first bit 1
- Adapter can work in *promiscuous* mode

Ethernet Efficiency

- Efficiency = $\dfrac{1}{1 + \dfrac{5d_{prop}}{d_{trans}}}$

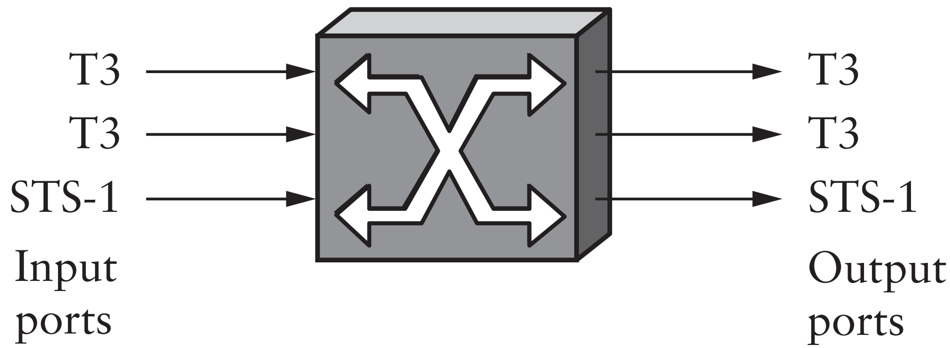
Wired Media Access



Scaling the Network

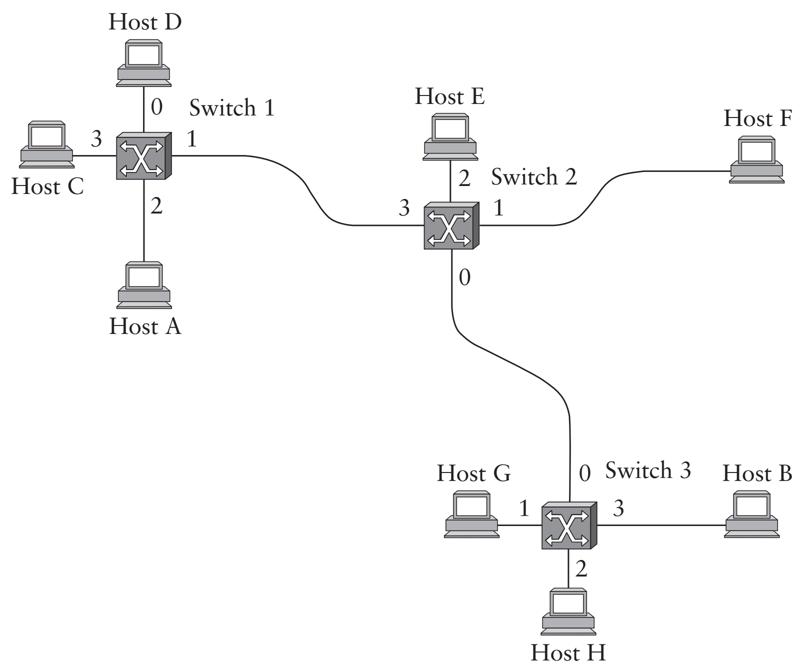
- Problem: all the nodes on the same wire
  - Collision
  - Capacity
- Solution
  - Group the nodes into separate networks connected by hubs or switches
  - Consequences?
- Very little Ethernet today is shared

Switching



- Switches must be able to, given a packet, determine the outgoing port
- 3 ways to do this:
  - Datagram Switching
  - Virtual Circuit Switching
  - Source Routing

Datagram Switching



Switch 2

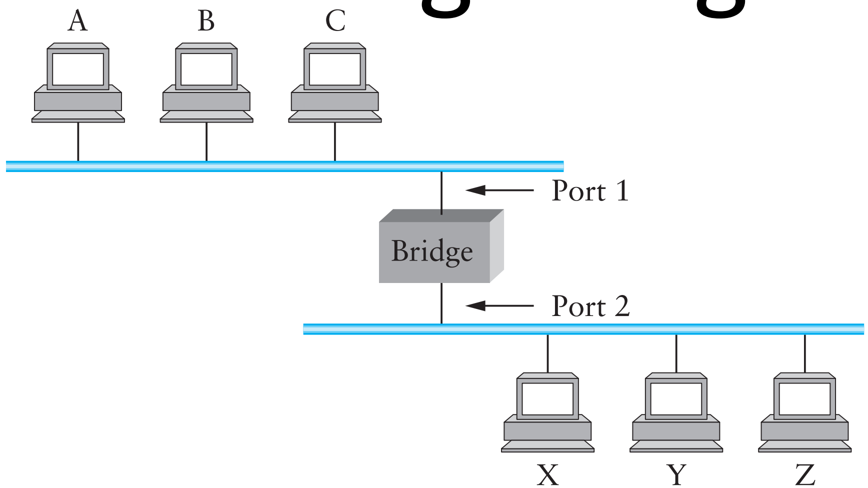
Addr	Port
A	3
B	0
C	3
D	3
E	2
F	1
G	0
H	0

- Each packet carries destination address
- Switches maintain address-based tables
  - Maps [destination address]:[out-port]
- Also called *connectionless* model

Datagram Switching

- No delay for connection setup
- Source can't know if network can deliver a packet
- Possible to route around failures
- Higher overhead per-packet
- Potentially larger tables at switches

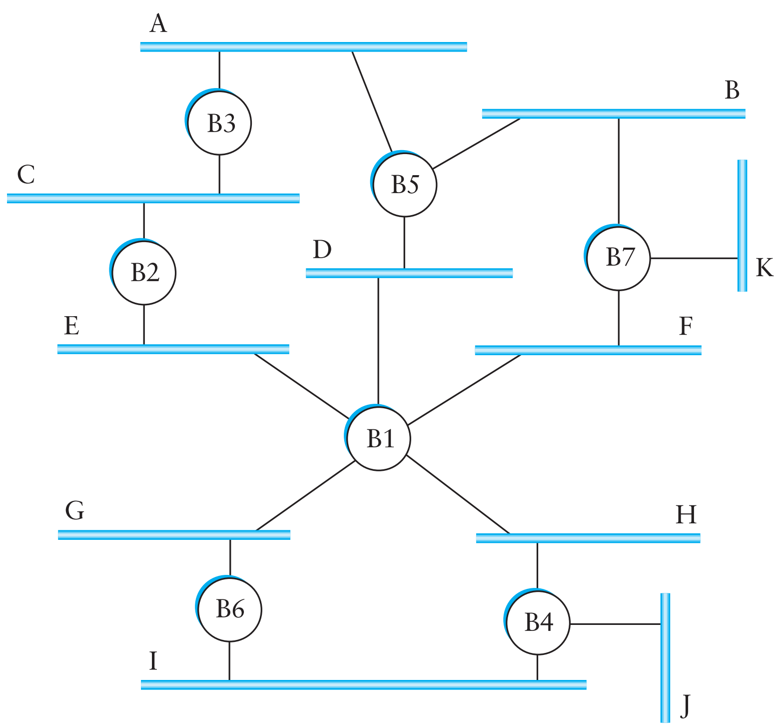
Learning Bridges



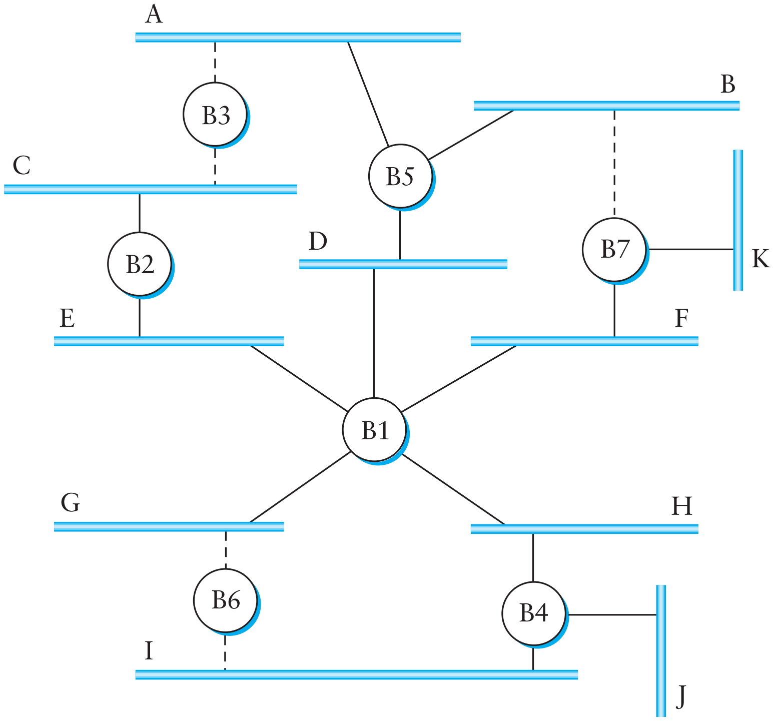
- Idea: don't forward a packet where it isn't needed
  - If you know recipient is not on that port
- Learn hosts' locations based on source addresses
  - Build a table as you receive packets
- Table says when *not* to forward a packet
  - Doesn't need to be complete for *correctness*

Dealing with Loops

- Problem: people may create loops in LAN!
  - Accidentally, or to provide redundancy
  - Don't want to forward packets indefinitely



Spanning Tree



- Need to disable ports, so that no loops in network
- Like creating a spanning tree in a graph
  - View switches and networks as nodes, ports as edges