Medium Access Protocols
Summary of MAC protocols

• What do you do with a shared media?
  – Channel Partitioning, by time, frequency or code
    • Time Division, Code Division, Frequency Division
  – Random partitioning (dynamic),
    • ALOHA, S-ALOHA, CSMA, CSMA/CD
    • carrier sensing: easy in some technologies (wire), hard in others (wireless)
    • CSMA/CD used in Ethernet
  – Taking Turns
    • polling from a central cite, token passing
LAN technologies

Data link layer so far:
- services, error detection/correction, multiple access

Next: LAN technologies
- addressing
- Ethernet
- hubs, bridges, switches
- 802.11
- PPP
- ATM
LAN Addresses and ARP

32-bit IP address:

- *network-layer* address
- used to get datagram to destination network

LAN (or MAC or physical) address:

- used to get datagram from one interface to another physically-connected interface (same network)
- 48 bit MAC address (for most LANs) burned in the adapter ROM
LAN Addresses and ARP

Each adapter on LAN has unique LAN address
LAN Address (more)

- MAC address allocation administered by IEEE
- manufacturer buys portion of MAC address space (to assure uniqueness)
- Analogy:
  (a) MAC address: like Social Security Number
  (b) IP address: like postal address
- MAC flat address => portability
  - can move LAN card from one LAN to another
- IP hierarchical address NOT portable
  - depends on network to which one attaches
Address Resolution Protocol (ARP)

- Maps IP addresses to Ethernet Addresses
- ARP responses are cached
ARP protocol

- A knows B's IP address, wants to learn physical address of B
- A broadcasts ARP query pkt, containing B's IP address
  - all machines on LAN receive ARP query
- B receives ARP packet, replies to A with its (B's) physical layer address
- A caches (saves) IP-to-physical address pairs until information becomes old (times out)
  - soft state: information that times out (goes away) unless refreshed
Ethernet

“dominant” LAN technology:
• cheap $20 for 100Mbs!
• first widely used LAN technology
• Simpler, cheaper than token ring LANs and ATM
• Kept up with speed race: 10, 100, 1000 Mbps

Metcalfe’s Ethernet sketch
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
Ethernet Frame Structure (more)

- **Addresses**: 6 bytes, frame is received by all adapters on a LAN and dropped if address does not match.
- **Type/length**: indicates the higher layer protocol, mostly IP but others may be supported such as Novell IPX and AppleTalk.
- **CRC**: checked at receiver, if error is detected, the frame is simply dropped.

![Ethernet Frame Structure Diagram]
Ethernet: uses CSMA/CD

A: sense channel, if idle
   then {
      transmit and monitor the channel;
      If detect another transmission
      then {
         abort and send jam signal;
         update # collisions;
         delay as required by exponential backoff algorithm;
         goto A
      }
      else {done with the frame; set collisions to zero}
   }
else {wait until ongoing transmission is over and goto A}
Ethernet’s CSMA/CD (more)

**Jam Signal:** make sure all other transmitters are aware of collision; 48 bits;

**Exponential Backoff:**
- **Goal:** adapt retransmission attempts to estimated current load
  - heavy load: random wait will be longer
- first collision: choose K from \{0,1\}; delay is \(K \times 512\) bit transmission times
- after second collision: choose K from \{0,1,2,3\}…
- after ten or more collisions, choose K from \{0,1,2,3,4,…,1023\}
Ethernet Technologies: 10Base2

- **10**: 10Mbps; **2**: under 200 meters max cable length
- thin coaxial cable in a bus topology

- repeaters used to connect up to multiple segments
- repeater repeats bits it hears on one interface to its other interfaces: physical layer device only!
10BaseT and 100BaseT

- 10/100 Mbps rate; latter called “fast ethernet”
- T stands for Twisted Pair
- Hub to which nodes are connected by twisted pair, thus “star topology”
- CSMA/CD implemented at hub
10BaseT and 100BaseT (more)

- Max distance from node to Hub is 100 meters
- Hub can disconnect “jabbering adapter
- Hub can gather monitoring information, statistics for display to LAN administrators
Gbit Ethernet

• use standard Ethernet frame format
• allows for point-to-point links and shared broadcast channels
• in shared mode, CSMA/CD is used; short distances between nodes to be efficient
• uses hubs, called “Buffered Distributors”
• Full-Duplex at 1 Gbps for point-to-point links
Token Passing: IEEE802.5 standard

- 4 Mbps
- max token holding time: 10 ms, limiting frame length

<table>
<thead>
<tr>
<th>SD</th>
<th>AC</th>
<th>FC</th>
</tr>
</thead>
<tbody>
<tr>
<td>SD</td>
<td>AC</td>
<td>FC</td>
</tr>
</tbody>
</table>

- **SD, ED** mark start, end of packet
- **AC**: access control byte:
  - **token bit**: value 0 means token can be seized, value 1 means data follows FC
  - **priority bits**: priority of packet
  - **reservation bits**: station can write these bits to prevent stations with lower priority packet from seizing token after token becomes free
Token Passing: IEEE802.5 standard

- **FC**: frame control used for monitoring and maintenance
- **source, destination address**: 48 bit physical address, as in Ethernet
- **data**: packet from network layer
- **checksum**: CRC
- **FS**: frame status: set by dest., read by sender
  - set to indicate destination up, frame copied OK from ring
  - DLC-level ACKing
Interconnecting LANs

Q: Why not just one big LAN?
• Limited amount of supportable traffic: on single LAN, all stations must share bandwidth
• Limited length: 802.3 specifies maximum cable length
• Large “collision domain” (can collide with many stations)
• Limited number of stations: 802.5 have token passing delays at each station
Hubs

- Physical Layer devices: essentially repeaters operating at bit levels: repeat received bits on one interface to all other interfaces
- Hubs can be arranged in a hierarchy (or multi-tier design), with backbone hub at its top
Hubs (more)

- Each connected LAN referred to as LAN **segment**
- Hubs **do not isolate** collision domains: node may collide with any node residing at any segment in LAN
- Hub Advantages:
  - simple, inexpensive device
  - Multi-tier provides graceful degradation: portions of the LAN continue to operate if one hub malfunctions
  - extends maximum distance between node pairs (100m per Hub)
Hub limitations

• single collision domain results in no increase in max throughput
  – multi-tier throughput same as single segment throughput
• individual LAN restrictions pose limits on number of nodes in same collision domain and on total allowed geographical coverage
• cannot connect different Ethernet types (e.g., 10BaseT and 100baseT)
Bridges

- **Link Layer devices**: operate on Ethernet frames, examining frame header and selectively forwarding frame based on its destination.
- Bridge **isolates collision** domains since it buffers frames.
- When frame is to be forwarded on segment, bridge uses CSMA/CD to access segment and transmit.
Bridges (more)

• Bridge advantages:
  – Isolates collision domains resulting in higher total max throughput, and does not limit the number of nodes nor geographical coverage

  – Can connect different type Ethernet since it is a store and forward device

  – Transparent: no need for any change to hosts LAN adapters
Bridges: frame filtering, forwarding

• bridges filter packets
  – same-LAN -segment frames not forwarded onto other LAN segments

• forwarding:
  – how to know which LAN segment on which to forward frame?
  – looks like a routing problem (more shortly!)
Backbone Bridge
Interconnection Without Backbone

- Not recommended for two reasons:
  - single point of failure at Computer Science hub
  - all traffic between EE and SE must path over CS segment
Bridge Filtering

• bridges *learn* which hosts can be reached through which interfaces: maintain filtering tables
  – when frame received, bridge “learns” location of sender: incoming LAN segment
  – records sender location in filtering table

• filtering table entry:
  – (Node LAN Address, Bridge Interface, Time Stamp)
  – stale entries in Filtering Table dropped (TTL can be 60 minutes)
Bridge Filtering

- filtering procedure:
  \[
  \textbf{if} \ \text{destination is on LAN on which frame was received}
  \]
  \[
  \textbf{then} \ \text{drop the frame}
  \]
  \[
  \textbf{else} \ \{ \ \text{lookup filtering table}
  \]
  \[
  \textbf{if} \ \text{entry found for destination}
  \]
  \[
  \textbf{then} \ \text{forward the frame on interface indicated;}
  \]
  \[
  \textbf{else} \ \text{flood;} \quad /* \text{forward on all but the interface on which the frame arrived}*/
  \]
  \[
  \}
Bridge Learning: example

Suppose C sends frame to D and D replies back with frame to C

- C sends frame, bridge has no info about D, so floods to both LANs
  - bridge notes that C is on port 1
  - frame ignored on upper LAN
  - frame received by D
Bridge Learning: example

- D generates reply to C, sends
  - bridge sees frame from D
  - bridge notes that D is on interface 2
  - bridge knows C on interface 1, so **selectively** forwards frame out via interface 1
Spanning Tree

- The learning bridge fails when the network topology has a loop.
  - Why?

- Loops are not necessarily bad. They provide redundancy that can be used to recover from failures

- To handle loops, bridges implement the spanning tree algorithm.
  - The spanning tree algorithm imposes a logical tree over the physical topology
  - Data is only transferred along links that belong to the spanning tree
Spanning Tree Algorithm

- Each bridge has unique id (e.g., B1, B2, B3)
- Select bridge with smallest id as root
- Select bridge on each LAN closest to root as designated bridge (use id to break ties)
- Each bridge forwards frames over each LAN for which it is the designated bridge
Spanning Tree Algorithm (contd.)

• Bridges exchange configuration messages called CBPDU’s (Configuration Bridge Protocol Data Unit)
  – id for bridge sending the message
  – id for what the sending bridge believes to be root bridge
  – distance (hops) from sending bridge to root bridge

• Each bridge records the current best configuration message for each port

• Initially, each bridge believes it is the root
Spanning Tree Algorithm (contd.)

• When a bridge learns that it is not the root it stops generating configuration messages
  – in steady state, only root generates configuration messages

• When the bridge learns that it is not the designated bridge, it stops forwarding configuration messages
  – in steady state, only designated bridges forward config messages

• Root continues to periodically send config messages

• If any bridge does not receive successive config messages, it starts generating config messages claiming to be the root
  – This is used to recover from root failure
Limitations of Bridges

• Do not scale
  – spanning tree algorithm does not scale
  – single large broadcast domains do not scale

• Do not accommodate heterogeneity
  – Bridges support ethernet to ethernet, ethernet to 802.5 and 802.5 to 802.5.

• Caution: beware of transparency
  – Applications that assume that they are executing on a single LAN will fail.
  – Latency increases in large LANs, so does jitter
WWF Bridges vs. Routers

- both store-and-forward devices
  - routers: network layer devices (examine network layer headers)
  - bridges are Link Layer devices
- routers maintain routing tables, implement routing algorithms
- bridges maintain filtering tables, implement filtering, learning and spanning tree algorithms
Bridges + and -

+ Bridge operation is simpler requiring less processing bandwidth

- Topologies are restricted with bridges: a spanning tree must be built to avoid cycles

- Bridges do not offer protection from broadcast storms (endless broadcasting by a host will be forwarded by a bridge)
Routers vs. Bridges

**Routers + and -**

+ arbitrary topologies can be supported, cycling is limited by TTL counters (and good routing protocols)
+ provide firewall protection against broadcast storms
- require IP address configuration (not plug and play)
- require higher processing bandwidth

• bridges do well in small (few hundred hosts) while routers used in large networks (thousands of hosts)