

# Computer Networks

## ICS 651

- Address Resolution Protocol
- Collision Detection and Random Binary Backoff
- Then and now: coaxial to hubs, 3Mb/s to Gigabit and 10G
- Ethernet NIC
- Ethernet Hubs
- Learning Bridges and Ethernet Switches

# ARP Cache

- don't want to send a request for every IP packet
- when I get a reply, I cache the address
- IP is connectionless, so use a timer (15 minutes) to discard old entries
- if ARP cache fills, can do LRU discard
- if I get an ARP request from someone, I will assume:
  - they plan to send me a packet
  - I will eventually send them some reply
- so I add them to my cache

# Ethernet Collision Algorithm

- If there is a collision, it will be detected in the first 512 bits (64 bytes) of the frame
  - 14-byte header, 46-byte minimum payload size, 4-byte CRC
- if a sender detects a collision, it must jam the wire
  - by putting a signal that is not a valid transmission
- receivers and other senders detect jamming, stop listening
- all senders must do binary exponential backoff
- randomization for backoff algorithm comes from my Ethernet address

# Ethernet Evolution and Summary

- Xerox
- 3 Mb/s system with 2- or 6-byte addresses
- 10-Base 5: coaxial 10Mb/s with vampire taps
- 10-Base 2 (thinwire): coaxial 10Mb/s with point-to-point
- 10-Base T: CAT-5 to hubs, no actual shared medium
- 100- and 1000 Mb/s Ethernet(s) over twisted pair or fiber
- Gigabit and 10-Gigabit Ethernet
- Ethernet is usually classified as: Carrier Sense Multiple Access (CSMA) with Collision Detection: CSMA/CD

# Ethernet Network Interface Card

- Analog portion can:
  - read and write bits
  - detect and generate jamming signal
- synchronize to incoming preamble
- Digital receive section can:
  - read destination address and discard unless for us or broadcast
    - unless the interface is in **promiscuous mode**, where it accepts all packets
  - discard if CRC does not match
  - DMA to main memory
- Digital transmit section can:
  - DMA, buffer, and send frame
  - compute and send CRC
  - retransmit in case of collision

# Ethernet Hubs

- A hub interconnects one or more NICs or hubs
- when a hub receives a frame  $F$  from one of its ports
- the hub must immediately forward  $F$  to all its other ports
- if a transmission is in progress on another port, hub must drop both frames and jam all the ports
  - i.e. communicate a collision
- if a frame ends with a jamming signal, we must jam all other ports
- a hub is a layer-1 (physical layer) device
- hub topology must be a spanning tree with no loops

# Learning Bridge

- instead of working on layer 1, a bridge looks at the link layer (MAC) header (layer 2)
- and instead of immediately forwarding the first bits of the frame, the entire frame is stored in memory, then forwarded (store-and-forward, same as most IP routers)
  - this has the advantage of breaking the collision domain: frames can be received on multiple ports at the same time, which increases the possible utilization of the Ethernet
- by default, a learning bridge broadcasts every packet, just like a hub
- however, the learning bridge also looks at the MAC source address:
  - if we get frames from A on port I, remember that
  - any future frames for A (within a limited time) are forwarded only on port I rather than broadcast
  - this reduces the overall amount of traffic, because most traffic is not broadcast
  - for the same reason, this gives some improvement in privacy
- a bridge can interconnect different LAN technologies, by translating headers
  - for example, a Wireless Access Point translates between Ethernet headers and Wifi/802.11 headers
- like a router (and unlike a hub), a learning bridge can be implemented in software
- like hubs, bridges should be interconnected in a tree, with no loops

# Ethernet Switch

- like a learning bridge
- hardware forwarding of frames from one interface to the next
- buffering and queueing of frames for each interface
- these days, hubs are rare, ethernet/wifi switches are common
  - hubs may still be used for network sniffing
  - but configurable ethernet switches can also forward traffic through a special monitoring port

# Ethernet Switches and Spanning Tree

- like hubs, etherswitches must avoid forwarding loops
- to allow redundant links, some etherswitches run the Spanning Tree Protocol (STP)
- STP figures out which links must be used in forwarding, and which must be blocked, by building a spanning tree
- the spanning tree is rooted at the node with the lowest priority (as set by an operator) or the lowest Ethernet address
- the process to determine the spanning tree is automatic
- in case a link or switch goes down, the STP quickly (usually less than a minute for original STP, under 10s for RSTP) starts using previously blocked interfaces
- STP must usually be enabled by an operator

# Names and Layers

- layer 1, physical layer: Hub, forward to all (physical layer)
- layer 2, data link (MAC) layer:
  - Bridge: something interconnecting LANs
  - Learning Bridge: only forwards on interface that reaches the destination
  - Switch: a bridge that uses hardware to forward packets
- layer 3, network (internet) layer:
  - Gateway: old name for router
  - Router: a box that forwards packets among networks
  - IP switch: a router with hardware forwarding
- layer 4, transport layer:
  - Firewall: a forwarding engine that allows or blocks traffic based on port numbers
  - NAT (Network Address Translation): a forwarding engine that looks at and rewrites network layer and transport layer headers