Lecture 10: From Links to Networks to Internets

10.0 Main Points

Broadcast networks
Switched networks
Internets

10.1 Broadcast Networks

Broadcast networks: shared communication medium.

For example, shared medium can be a wire -- all hosts listen to wire. Inside a computer, this is called a "bus" -- a shared set of wires between the CPU and the memory modules

Ethernet is an example broadcast network (10 Mbits/sec)
Another example: cellular phones (100Kb - 1Mbit/sec).

Problem #1: Delivery
When you broadcast a packet, how does receiver know who it is for?

Put header on front of packet:
Destination | Packet

For example, header would contain unique machine # (network address) of target. Everyone gets packet, discards if not the target. In Ethernet, this check is done in hardware; no interrupt if not for you.

This is an example of layering: we're going to build up complex network protocols by layering more and more stuff on top of the packet.

Problem #2: Arbitration
How do machines arbitrate for use of shared medium?
Very simple approach: assign each host a timeslot in which to transmit (static multiplexing). Sometimes called TDM (time division multiplexing) or FDM (frequency division multiplexing) or WDM (wave division multiplexing).

OK if everyone always has stuff to send, but what if traffic is very bursty? Wastes bandwidth to allocate slots to hosts without anything to send!

Aloha network (70's) -- packet radio between Hawaiian islands

Arbitration
(i) carrier sense -- don't start sending if can hear someone else already transmitting.
(ii) receiver discards if collision

What if two try tostart sending at the same time?

What happens as more hosts want to send -- load increases?

Ethernet -- early 80's, first practical local area network (Xerox PARC). 10 Mb/s. Most common LAN for UNIX environments, becoming more common in PC's. What we have in the department.

Key advance was in a new way to do arbitration. Three pieces:

1. carrier sense -- don't send unless idle

2. collision detect -- sender checks if packet is trampled. If so, abort, wait, and retry.
Requires maximum Ethernet link distance (2.5 km), max latency (24.6 microseconds), and minimum Ethernet frame size (64 bytes).
3. Adaptive randomized waiting strategy -- if try to send, and get collision, means there are a number of people trying to send, so pick bigger mean wait time. If collide again, pick even bigger wait (up to some limit) -- exponential backoff.

Token rings (IBM Token Ring, FDDI).

Address fairness, increase bandwidth over Ethernet by connecting hosts in a ring, rather than as a bus. Ring uses point to point links between hosts (easier to go fast).

Ring is still broadcast -- only one host can send at a time, by grabbing right to send (token). For example, everyone gets to send one packet, before giving up token and passing it around.

Technology adoption question: lots of competing broadcast network standards. Why did Ethernet win, and token rings lose?

10.2 Switched Networks

What if you need more machines than will fit on a single Ethernet?

What if you need network to extend farther (in distance) than a single Ethernet?

What if you need more bandwidth than a single Ethernet?

Solution: switching -- connect hosts together with a mesh of point to point links and switches. Switches copy packets from one link to another to get packets closer to host.

Switched networks have a number of (potential) advantages:

1. Higher link performance by using point to point links

2. Much greater aggregate bandwidth

3. Incremental scaling

4. Improved fault tolerance through redundant paths
Examples of switched networks: ATM, switched Ethernet, Internet

Delivery -- how do we get packets from source to destination through a switched network?

Some definitions:

name (user known) -- Mom, cs.washington.edu

address (globally unique ID) -- phone #, IP address

route -- how do you get from here to there

Internet is a switched network of networks -- can combine ATM, Ethernet, FDDI, etc.

IP provides single address space -- globally unique ID for every host (packet has IP address in addition to Ethernet/FDDI/ATM network address

DNS name service translates user machine names to IP addresses

Routing protocols set up tables in switches to determine how packets are routed to destination address

A few more definitions:
1. repeater -- straddles two networks, puts all packets from one onto the other

2. bridge -- selectively repeats packets from one network to hosts on another (e.g., between two or more Ethernet segments)

3. router -- forwards packets across multiple potentially heterogeneous networks (e.g., Internet)

4. gateway -- router at the edge of an administrative domain, connecting domain to the rest of the world

5. firewall -- gateway that checks packets going in/out for security (e.g., every incoming packet must have a source address from outside, to help prevent IP spoofing)

6. switch -- forwards packets to destination within a single network (e.g., ATM)

But nothing set in concrete -- see products crossing these boundaries all the time. Bridges that do routing across many Ethernet segments. Firewalls that double as gateway routers. Etc.

Many of the same functions throughout this space. For now, focus on how switch/router knows where to send incoming packet.

Several options:

1. source routing (Myrinet)

2. table of global addresses (Internet)

3. table of virtual circuits (ATM)