ICS 351: Today's plan

- review of packet forwarding: switching and Internet routing

packets

- data is divided into units of finite size, called packets or: frames, datagrams, PDUs, etc.
  - finite size limits the delay when multiplexing data from different sources
- to accommodate packets, longer data must be split up into smaller units: fragmentation (IP), segmentation (TCP)
- each packet has one or more nested headers, and possibly one or more trailers

network structure

- networks include point-to-point links or physical broadcast media
  - most of today's internet, including the lab, is made up of point-to-point connections
  - wireless is physically broadcast, ethernet was physically broadcast until about 1990
- networks are interconnected by a variety of switching technologies: hub, ethernet bridg or switch, router (or IP switch), NAT, WAP
- "switch" implies hardware forwarding

Ethernet switching

- packets on an Ethernet have Ethernet headers
- a hub works on the physical layer, and rebroadcasts the packet without regard to the header
- an Ethernet switch works on the data-link layer
- data-link forwarding does not scale to large networks, since it requires broadcasting at least some of the time
- special provisions (e.g. STP) are needed to prevent forwarding loops in Ethernet networks

Ethernet switching details

- an Ethernet switch rebroadcasts every packet *unless it has better information*:
  - a learning switch that has seen this **destination address** as the *source address* of previous packets, only forwards on the interface the prior packet came from
  - a switch that implements the Spanning Tree Protocol (STP), only forwards on interfaces that are part of the spanning tree
    - root or forwarding port

Internet addresses

- for scaling, it is important that network addresses be **assigned** based on their point of connection to the Internet
  - MAC addresses are encoded in hardware
- IP has **network** and **host parts** of the address
  - all hosts on the same network should have the same network part of the address
- IP addresses and netmasks must be configured for every interface on the Internet!
  - perhaps automatically, via DHCP or NDP

Netmasks

- the netmask determines the number of bits in the IP address that are in the network part of the address
  - the netmask has a 1 bit corresponding to every bit of the address that is in the network part
  - every 1 bit comes before every 0 bit
- different netmasks can be used in different parts of a network, allowing for subnetting

Internet Routing

- where there is broadcasting, it is limited, e.g. to routers within an OSPF network
- each router processes the **routing data** it receives, updates its routing table accordingly
- routers can maintain multiple, alternative routes for both redundancy and load balancing

Internet Routing: Distance Vector

- Distance-Vector (RIP): the **routing data** is essentially the neighbor's routing table
  - better routes (and worse routes from the next hop) are added to the routing table
  - otherwise, worse routes are ignored
  - routes that are not refreshed, time out
- Path-Vector (BGP) is similar, but the entire path (the list of each AS in the path) is distributed, rather than just the cost

Internet Routing: Link State

- Link-State (OSPF): the **routing data** is the router's neighborhood information
  - these link states are broadcast
  - each router combines the received link states into a graph representation of the network
  - Dijkstra's shortest path algorithm gives the actual routes

What happens when an IP packet is received over Ethernet? (part 1)

- hardware error checking (CRC) and destination address verification
- interrupt and dispatch to the IP module
  - CPU starts executing interrupt code
  - interrupt code executes IP code
- variety of checks, including IP version, header length, and header checksum

What happens when an IP packet is received over Ethernet? (part 2)

- IP destination address lookup:
  - is it for local delivery? If so, check protocol, port number(s)
    - if match an existing socket, deliver to the application
  - otherwise, check routing table (and cache) to obtain *interface* and *next hop*
    - next hop is gateway or destination
- decrement TTL

What happens when an IP packet is received over Ethernet? (part 3)

- if necessary, queue for transmission on the selected interface
- if outgoing interface is Ethernet or WiFi, check ARP table for translation
  - if not available, broadcast ARP request for next hop IP address, wait for response
- create an Ethernet frame using the MAC address given by ARP, and give to NIC (Network Interface Card) for transmission
- recycle buffer space