ICS 351: Today's plan

- Quiz, on overall Internet function, linux and IOS commands, network monitoring, protocols
- IPv4 addresses: network part and host part
- address masks
- IP interface configuration
- IPv6 addresses
- ARP protocol
- `arp` command
IPv4 addresses

- 32 bits, usually written in dotted-decimal notation: 128.241.5.17
- each address is split into a network part and a host number
- the network part of the address identifies the network
- for example, www.cmu.edu is 128.2.10.162
- the first 16 bits of the address, 128.2/16, identify the network
- the entire IP address, 128.2.10.162, identifies the host
- every network number should be unique
- host numbers should be unique within a network
IPv4 address details

- an IP address actually identifies an interface rather than a host -- a host or router with multiple interfaces has multiple IP addresses

- 1. packets within the network are routed by using ARP to find the MAC address of the destination, and then sent using the LAN protocol

- 2. packets outside the network are routed to the network number, ignoring the host part
IPv4 subnetting

- different addresses have different numbers of bits assigned to the network part of the address
- one network can be split into subnetworks. For example, the network 128.2/16 could be split into 4 networks, 128.2.0/18, 128.2.64/18, 128.2.128/18, and 128.2.192/18
- outside the network, packets are routed to 128.2/16
- within the 128.2/16 network, packets are routed to one of the four subnetworks
- within the subnetworks, packets are delivered using Ethernet
IPv4 network masks

- except for routes to an individual network, a routing table must hold (a) the destination address, and (b) the number of bits which make up the network number
- this is done by storing a network mask together with the destination address
- to find out if a destination address (in an IP packet) matches a route (in the routing table), both addresses are ANDed with the network mask, and if the result is equal, the route is a match
- the outcome of this is that the length of the network part of an address is determined only by the accompanying network mask
- this is known as Classless InterDomain Routing (CIDR)
IPv4 network mask examples

• 128.2.128.162 matches 128.2.0.0/16
• 128.2.128.162 does not match 128.2.0.0/18
• 128.2.128.162 matches 128.2.128.0/18
• the network mask is also written in dotted-decimal notation, e.g. 255.255.0.0 for a 16-bit mask, or 255.255.192.0 for an 18-bit mask
IP interface configuration

- `ifconfig` on Unix systems, `ipconfig` on Windows
- some IP interface configuration can be done automatically, e.g. using DHCP
- but DHCP requires someone to decide which IP addresses get assigned to which interfaces
- this can be done automatically in some cases, but usually not when assigning static IP addresses
- when setting up an interface for IP, must specify:
  - the IP address
  - the network mask
IPv6 addresses

- IPv6 addresses (128 bits) are also split into network and host parts
- this split is not determined by a netmask, but by the first few bits of the address
- using the first few bits determine the class of the address was first developed for IPv4
  - but abandoned as inefficient when IPv4 addresses started to become scarce
- an address beginning with 80 zero bits followed by 16 1 bits is an "IPv4-mapped IPv6 address", and is valid as long as the interface's valid IPv4 address is used as the last 32 bits (80+16+32 = 128)
IPv6 addresses: no netmasks

- IPv6 addresses (128 bits) are split into network and host parts
- "normal" IPv6 addresses have a global routing prefix (essentially a network number) and a subnet ID in the first 64 bits, followed by 64 bits of interface ID
- such an interface ID could, for example, be taken from the globally unique 48-bit Ethernet address associated with the Ethernet hardware
- RFC 4291 (http://tools.ietf.org/html/rfc4291) has many more details
ARP protocol

- when communicating over the local network, the routing table only records the IP address of the next interface
- one advantage of this is that the next hop (e.g. a router) can be replaced relatively easily
- an ARP request (ARP who-has) is broadcast whenever the MAC address is needed for an IP address on a local net
- the ARP reply is unicast back to the sender, and carries both IPs and both Ethernet addresses
- the ARP reply could be sent by an ARP proxy if the intended destination does not support ARP
- ARP packets are not IP packets (ping packets are IP packets)
arp command

- always use "-n" in the lab for all these commands, to request numerical output rather than domain name resolution
- `arp -a -n`: print all the entries in the ARP table
- `arp -d address`: remove the table entry corresponding to the given IP address
- `arp -s address MAC`: add a table entry mapping the given IP address to the given MAC address (use `temp` at the end of the command to install a normal temporary translation)