ICS 351: Today's plan

- 802.11 security: WEP, 802.11i, WPA, WPA2.
- networking security
- wireless ad-hoc and mesh networks
802.11 Security

- tapping a wired network requires physical access to the wires
- tapping a wireless network requires being in range of the signal
- originally, cryptographic Wired Equivalent Privacy (WEP) was introduced to hide the contents of the messages
- the original design for WEP was not widely published -- unfortunately, this lead to a lack of serious examination of the protocol (security by obscurity often does not work)
- unfortunately, WEP is sufficiently weak that it can be cracked by listening to a few minutes of busy traffic
- 802.11i introduced:
  - WiFi Protected Access (WPA), a simple but much stronger encryption protocol, and
  - WPA2, stronger than WPA and requiring more resources for implementation (including, in some cases, newer equipment)
networking security

- "in the clear" protocol can be easily broken when information is snooped: telnet, ftp, http, many email protocols
- encrypted protocol are secure against many attacks, including someone examining the data: ssh/scp, https, secure POP/IMAP, PGP
- most protocols are not secure against traffic analysis
- some general principles:
  - o it is usually better to have more security than less security
  - o security that inconveniences users is more likely to be resisted or circumvented
  - o security can inadvertently lock out people who should have access
  - o data requiring security should not be sent unencrypted over the Internet (because some of the links may be accessible to adversaries)
  - o data requiring security is still often sent unencrypted over the Internet (but data with monetary value is usually protected these days)
- host security is more concerned with installing applications, running foreign code, firewalls/NATs, etc
wireless ad-hoc and mesh networks

- using the ad-hoc mode of 802.11, any machine ("node") may directly talk to any other node
- if nodes agree to forward data for each other, they can form a wireless ad-hoc network
- machines may move or go to sleep, so routing can be challenging
- also, the notion of a "link" is different for wired and wireless networks: successful wireless protocols take advantage of broadcasting
- generally machines should discover each other and automatically send data to the destination

- a wireless mesh network consists of static wireless nodes
- possibly with some wired nodes coordinating to provide Internet access
- mobile nodes may obtain Internet access from nodes in a mesh network
ICS 351: Today's plan

- IPv6 addresses
- IPv6 packets
- IPv6 over Ethernet
IPv4 vs. IPv6

- IPv4 does not have enough addresses:
  - CIDR (netmasks) developed to deal with a shortage of IPv4 addresses
  - NAT developed to deal with a shortage of IPv4 addresses

- what if we had a very large number of IP addresses?
- what if we could assign these addresses automatically without using DHCP?
IPv6 addresses

- IPv6 uses 128-bit addresses instead of the 32-bit IPv4 addresses
- these are written as 8 groups of 4 hex digits separated by colons: 
  1234:5678:0000:0000:0000:0008:9ABC:DEF0
- leading zeros may be omitted: 1234:5678:0:0:0:8:9ABC:DEF0
- a single sequence of all-zero groups can be omitted: 1234:5678::8:9ABC:DEF0
- networks are followed by a slash to indicate the number of bits in the network number: 
  1234:5678/32
- the loopback address is ::1
- an interface with a MAC address automatically has a non-routable IPv6 address: 
  fe80::48 bits of MAC address+16 inserted bits
- for example, with a hardware address of 00:01:03:a0:31:51, my non-routable IPv6 address will be fe80::201:3ff:fe00:3151 -- note the "u" bit is set to one to indicate universal scope
- globally routable unicast addresses have a network and subnetwork number in the most significant 64 bits
- ffff::/8 addresses are multicast addresses
* the IPv6 header is twice as big as the (minimal) IPv4 header, but simpler (from RFC 2460):
IPv6 details

- instead of IP header options, there may be extension headers
- fragmentation is only done by the sender, and path MTU discovery is required
- upper layer is now required to checksum.
- IPv6 routing is essentially the same as IPv4 routing (perhaps minus netmasks)
- when sent over Ethernet, the Ethertype field is 0x86DD instead of 0x800. (RFC 2464)
- Neighbor Discovery Protocol (NDP, RFC 2461) replaces both ARP and DHCP, uses IPv6 packets