ICS 351: Networking Protocols

- IP packet forwarding
- application layer: DNS, HTTP
- transport layer: TCP and UDP
- network layer: IP, ICMP, ARP
- data-link layer: Ethernet, WiFi

Networking concepts

- each protocol provides some functionality to the protocol above it, uses some functionality from the protocol below it
- interfaces can be in promiscuous mode, where they listen to all incoming data, and programs can be run on those interfaces to read the data
- the way the Internet works to provide communication among computers is captured by a collection of protocols, particularly IP, TCP, DNS, and HTTP

Networking issues

- there are many potential issues on the Internet, with many ways that data might be discarded, computers disconnected, and traffic slow
- security is important to users, but requires careful implementation
- servers are programs, not machines
  - "server" may also designate a machine on which the server runs

Lessons learned in the lab (1/2)

- don't use the upload port unless you need to!
- mis-configuration is often a source of problems (sometimes rebooting helps, other times it doesn't)
- familiarity with tools: ping, traceroute, telnet, wireshark/tcpdump, and many more
- familiarity with Cisco IOS, Linux
- routers are computers that (a) run a routing protocol, and (b) forward packets from one interface to another

Lessons learned in the lab (2/2)

- switches/bridges are computers that forward packets from one interface to another
- NAT/firewalls are computers that forward selected packets from one interface to another by changing the IP and TCP/UDP/ICMP headers
- all routing protocols are designed to automatically build routing tables
- all forwarding of IP packets is based on the routing table

Networking Protocols: DNS

- a hierarchical naming system
- with delegation of authority for subtrees
- and a distributed read-only cacheable database
- a zone is the contiguous part of a subtree which has its own name servers and is administered independently
- caching is used throughout, the TTL specifies how long information may be cached
- DNS queries usually use UDP, but other DNS functions may use TCP

Networking Protocols: DNS queries

- a client (resolver) sends a query to a server, which may:
  - respond to it, from its own or cached data,
  - respond negatively, but provide the address of another server closer to the destination (iterative query), or
  - recursively query another server closer to the destination and return the answer to the client

Networking Protocols: HTTP

- a client (browser) sends a query to a server over a TCP connection, the server responds
- the headers are printable ASCII (until HTTP/2)
- Host: gives the domain name part of the URL
- Content-Type: many different content types
- Accept: specifies which content types are acceptable
- connections are usually closed by the server, immediately or after a given time (e.g. 5min)

Networking Protocols: TCP

- TCP provides reliable end-to-end communication
  - IP provides end-to-end communication
  - TCP sends streams of bytes (not blocks)
  - a stream is an ordered sequence of bytes
- port numbers select among different applications running on the same machine
  - but really, remote and local port numbers identify a socket on the local machine

Networking Protocols: TCP reliable transmission

- sequence numbers and acknowledgements, and retransmissions when there is a timeout, are used to make the transmission reliable
- flow control window is used to let the receiver slow down the sender
- congestion control "window" is used by the sender to slow down when the network is congested

Networking Protocols: UDP

- the User Datagram Protocol encapsulates the user data with port numbers, a checksum and length for correctness, and an IP header
- UDP is not reliable
- UDP is connectionless
- UDP is datagram (block) oriented rather than byte-stream oriented
- UDP provides the same kind of ports as TCP

Networking Protocols: IP

- the Internet Protocol
  - allows communication among networks
- end-to-end connectionless data transmission
- IP header has source and destination IP address, support for fragmentation, and TTL
- routing is based only on the destination address
- packets may be lost, reordered, duplicated, delayed
  - due to routing errors, congestion, or mis-configuration

Networking Protocols: IPv6

- the next generation Internet Protocol
- essentially the same as IP, except for the addresses: 128 bits, built-in structure
- ::1 is the loopback address
- no need for ARP or DHCP (replaced by NDP), less need for NAT
- everything else should work almost the same on top of IPv6 as over IPv4

Networking Protocols: ICMP

- ICMP Echo: for testing whether IP is being delivered end-to-end
- ICMP Destination Unreachable: to report a packet being dropped due to routing problems
- ICMP Destination Unreachable because Fragmentation needed: to report a packet being dropped due to exceeding local MTU
- ICMP Redirect: to report a better first-hop router
- ICMP time exceeded in transit: TTL reached 0

Networking Protocols: ARP

- the routing table provides the IP address of the next hop
- the routing table does not provide the Ethernet address (hardware address) of the next hop
- so, broadcast an ARP request with the IP address of the next hop as well as of the sender
- the next hop (or a proxy) replies giving its hardware address, temporarily saved in the ARP cache

Networking Protocols: Ethernet

- source and destination addresses
- broadcast is the default mode of transmission
- broadcast doesn't work if there are loops
    - use STP to restricts the broadcast
- broadcast is inefficient and less secure
    - smart switches learn where different hosts are by remembering the source address
    - a learning switch need not broadcast if it knows the segment for a destination

Networking Protocols: WiFi/802.11

- much in common with Ethernet, including broadcasting
- no wires needed
- easy to intercept, so security protocols: WEP (useless against a serious attacker), WPA, WPA2
- usually used in managed mode with a single Wireless Access Point (WAP)
  - can be used in ad-hoc mode