Networking 3

TCP/IP Review

IP Addr

Uniform namespace for all computers
e.g. 171.64.64.250

IP Datagram

The standard packet format used for IP communication
Header uses IP addresses for from / to information

IP Routing

IP routers forward the IP datagram one hop closer to the ultimate destination
IP routers carry on
IP provides a "best effort" service to send one datagram from the source, across the IP internet, to the destination

On top of LAN

TCP / IP does not replace the LAN
TCP / IP is built on top of the LAN

TCP

Builds an end-to-end reliable "connection oriented" service on top of IP
Provides the illusion of a read / write stream of bytes that may be larger than a single packet
Does packetizing, error checking, re-sending, packet re-assembly, etc. to provide the illusion of a error-free stream of bytes
Most Internet software uses TCP

Misc TCP/IP Issues

IP Port Numbers

Each IP addr is logically divided into logical port numbers in the range 1-65535.
Traffic is addressed to a specific port number at the IP -- this allows a computer with one IP to be in multiple conversations at once. As we'll see, specific port numbers are reserved for specific purposes -- e.g. port 80 is used for HTTP traffic.

Each end of a connection has a source and destination port number as well as IP addr.

Broadcast

It's possible to send a packet on the LAN specifically marked as "broadcast", so everyone reads it. You may be able to see a broadcast packet on your hub if all your "receive" lights blink at once.

TCP/IP also has a "broadcast" notion for sending information to an entire subnet.

IP to LAN Translation

How does the router know the right LAN addr to use to contact another machine on its LAN?

i.e. given an IP addr, what is the LAN addr of that machine?

ARP -- address resolution protocol

- Broadcast "who has IP addr 171.64.64.250" on local LAN
- The owner answers back with it's LAN addr (e.g. its ethernet addr if ethernet is the LAN)

Reverse ARP -- aka RARP

- At boot time, a machine broadcasts its ethernet addr. A RARP server notices the broadcast, and replies with an IP addr to use. DHCP has pretty much replaced RARP.

Ping

ping -- sends a little IP query packet to see if a host responds at all -- see if it is up and reachable.

```
elaine0:~> ping www.whitehouse.gov
PING EM-AKAMAI.Stanford.EDU (171.66.255.140): 56 data bytes
64 bytes from EM-AKAMAI.Stanford.EDU (171.66.255.140): seq=0 ttl=252 time=2.41 ms.
64 bytes from EM-AKAMAI.Stanford.EDU (171.66.255.140): seq=1 ttl=252 time=3.45 ms.
64 bytes from EM-AKAMAI.Stanford.EDU (171.66.255.140): seq=2 ttl=252 time=4.12 ms.
^C
---- EM-AKAMAI.Stanford.EDU (171.66.255.140) PING Statistics ----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (ms) min/avg/max = 2.41/3.33/4.12 (std = 0.706)
```

Time To Live -- TTL

Neat bit of design -- every IP packet has a max -hops counter, so it cannot get stuck in a loop -- a robust design, even in the face of router errors. When the packet hits its hop limit, a polite router will send back a "failure" notification, which will identify the IP addr of the router.

Traceroute

Send out packets with TTL values 1, 2, 3, 4,to probe the path to somewhere.

With firewalls and whatnot attempting to "hide" internal networks, sometimes traceroute won't work and the path appears to go on endlessly.

The times listed are round-trip times in milliseconds

```
elaine40:/usr/class/cs193i/WWW> traceroute www.sjsu.edu
traceroute to rhea.sjsu.edu (130.65.3.13), 30 hops max, 40 byte packets
 1  leland-gateway (171.64.15.97)  1.277 ms  1.371 ms  0.973 ms
```

```
 2  Core2-gateway (171.64.1.233)  0.530 ms  0.624 ms  0.513 ms
 3  Core4-gateway-2 (171.64.3.18)  0.897 ms  0.785 ms  0.926 ms
 4  i2-gateway (171.64.1.225)  1.180 ms  0.770 ms  0.777 ms
 5  STAN.POS.calren2.NET (171.64.1.213)  1.125 ms  0.784 ms  1.084 ms
 6  SUNV--STAN.POS.calren2.net (198.32.249.73)  1.562 ms  1.119 ms  1.438 ms
 7  QSV-QSV-C2-GSR-ATM.CSU.net (137.145.203.209)  1.791 ms  2.051 ms  2.078 ms
 8  SJSU-QSV-ATM.CSU.net (137.145.203.106)  286.774 ms  149.992 ms  150.181 ms
 9  firewall.sjsu.edu (130.65.11.6)  138.667 ms  137.488 ms  147.755 ms
10  cc1omnicore.sjsu.edu (130.65.11.2)  134.991 ms  134.259 ms  111.274 ms
11  cc1omni-a.sjsu.edu (130.65.5.252)  313.109 ms  142.407 ms  146.947 ms
12  rhea.sjsu.edu (130.65.3.13)  137.231 ms *  134.619 ms
```

Host Configuration

Things that need to be set for a computer to use TCP/IP...

1. IP addr -- need to know what IP addr to use
2. Subnet mask -- this number encodes what the local set up is for which part of the IP is subnet vs. which part is host addr.
3. Router -- the IP addr of the local router to forward traffic to
4. DNS server addr -- the IP addr of the DNS server(s) to use.

DHCP

Dynamic Host Configuration Protocol

Allows a host, at boot time or whatever, to broadcast a query to a local DHCP server. The DHCP server can reply with all of the above configuration values. The DHCP may give out an arbitrary IP addr from its supply, or it may use a specific setup based on the LAN addr of the sender.

This is much more convenient way to do configuration for the end user -- just set the use-DHCP checkbox and you're done.

Standard, Collective, Cooperative

TCP/IP is just a standard -- an agreed format and protocol for things

It's a free, public, open standard

Vendors voluntarily implement TCP/IP

TCP/IP allows each vendor's equipment to, in one step, interoperate with all the other computers which is irresistible

Compare this to the "balkanized" picture where each vendor only works with their own equipment.