CSE 265: System and Network Administration

- Network Architecture
  - Hardware
  - Routing
  - Getting connected
  - Centralization/decentralization
  - Network topology
  - Network debugging tools
Networking hardware

- Ethernet is the core of most networks
  - 10 Mbit 10Base2, 10BaseT
  - 100 Mbit 100BaseTX
  - 1 Gbit 1000BaseT
  - 10 Gbit 10GBase-T
- Many competing LAN technologies
  - ATM, Token Ring, FDDI
- Wireless
  - 802.11b/a/g/n
Connecting ethernets

- **Hub/repeater (physical layer)**
  - Retimes and reconstitutes Ethernet frames to all ports
  - Single collision domain
- **Switch (link layer)**
  - Learns locations of MAC addresses, selectively forwards frames
  - Receives, buffers, and retransmits packets
    - Separate collision domains
    - Required for GbE and 10GbE
- **Router (IP/network layer)**
  - Connects separate ethernet networks
  - Can connect different LAN/WAN technologies
Routing

- Given a packet, on which of multiple network interfaces should it be sent?
- UNIX kernel keeps routing table (netstat -rn)
  - Sample from dual-homed host

<table>
<thead>
<tr>
<th>Kernel IP routing table</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Destination</strong></td>
<td><strong>Gateway</strong></td>
</tr>
<tr>
<td>128.180.98.128</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>192.168.0.0</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>127.0.0.0</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>128.180.98.248</td>
</tr>
</tbody>
</table>
Routing continued

• Routing is static for most systems
  - Established when network card configured

• Additional static routes can be added using the route command

• Dynamic routing can be managed using quagga and xorp (ULSAH if interested)
  - routed and gated are obsolete
Connecting to the Internet

• How can you connect your network to the Internet?
Connecting to the Internet

How can you connect your network to the Internet?

- Dialup
- Wireless (cellular, satellite, point-to-point)
- xDSL
- Cable
- ISDN
- Frame relay
- T1, T3, OC3, etc.
Remote access

- Connecting users to the organization
  - Check email, access data when traveling
  - Work from home
  - Remote facilities (e.g., stationed at customer site) but need access to organization network regularly
- Different needs, different support requirements
  - Establish an SLA
  - Worry about authentication, security, performance, costs
  - Consider centralization of authentication
  - Consider outsourcing changing technologies
Centralization/Decentralization

- Centralization – one focus of control
  - Regardless of the number of servers
- Decentralization – distribute control
  - Among many people/organizations
- Neither is always best

Applies to networks, services, personnel
Centralization

- Improve efficiency with economies of scale (purchasing and personnel)
- New technologies often bring opportunities for centralization
  - e.g., web-based instead of paper forms handling
- Often ideal for commodity services
- Simpler, consistent architecture
- Fewer systems to manage, house, service, etc.
- Consolidate expertise
Decentralization

- Improve speed and flexibility with local control
- On-hand support
- Customization
- Meet customers' needs
- Fault-tolerance
Network Topology

- Network architecture should
  - Be clean and simple
  - Provide for growth (new LAN segments, new remote offices)
  - Ensure reliability through redundancy
- Need to consider both physical and logical topologies
- Typical forms: Star, Ring, Mesh
Network debugging

- Questions to ask
  - Do you have physical connectivity and a link light?
  - Is your interface configured properly?
  - Is DNS configured properly?
  - Do your ARP tables show other hosts?
  - Can you ping the localhost address (127.0.0.1)?
  - Can you ping other local hosts by IP address?
  - Can you ping other local hosts by hostname?
  - Can you ping hosts on another network?
  - Do high-level commands like telnet and ssh work?
Network tools

- ping
- traceroute
- netstat
- arp (saw earlier)
- tcpdump/wireshark
- If ping works, networking between hosts is likely to be working
- It does not test availability of services
- Some firewalls filter ICMP messages

```bash
# ping www.lehigh.edu
PING www.lehigh.edu (128.180.2.14) from 128.180.98.216: 56(84) bytes
64 bytes from ws1.CC.Lehigh.EDU (128.180.2.14): icmp_seq=1 time=0.859 ms
64 bytes from ws1.CC.Lehigh.EDU (128.180.2.14): icmp_seq=2 time=0.685 ms
64 bytes from ws1.CC.Lehigh.EDU (128.180.2.14): icmp_seq=3 time=0.648 ms
64 bytes from ws1.CC.Lehigh.EDU (128.180.2.14): icmp_seq=4 time=0.751 ms
64 bytes from ws1.CC.Lehigh.EDU (128.180.2.14): icmp_seq=5 time=0.667 ms
64 bytes from ws1.CC.Lehigh.EDU (128.180.2.14): icmp_seq=6 time=1.00 ms
64 bytes from ws1.CC.Lehigh.EDU (128.180.2.14): icmp_seq=7 time=0.725 ms
64 bytes from ws1.CC.Lehigh.EDU (128.180.2.14): icmp_seq=8 time=0.655 ms
64 bytes from ws1.CC.Lehigh.EDU (128.180.2.14): icmp_seq=9 time=0.663 ms
64 bytes from ws1.CC.Lehigh.EDU (128.180.2.14): icmp_seq=10 time=0.724 ms

--- www.lehigh.edu ping statistics ---
10 packets transmitted, 10 received, 0% loss, time 9091ms
rtt min/avg/max/mdev = 0.648/0.738/1.006/0.109 ms
```
traceroute

- Finds the sequence of gateways traveled
- Works by increasing the TTL of the packet sent
- traceroute -n skips DNS

ariel% traceroute www.princeton.edu
traceroute to hulk.princeton.edu (128.112.128.15), 30 hops max, 40 byte packets
  1 128.180.123.254 (128.180.123.254)  3.406ms  0.940ms  0.676ms
  2  ewfmB-GBE-A.CC.Lehigh.EDU (128.180.18.4)  0.407ms  0.465ms  0.640ms
  3  ewfmd-ewfmb.CC.Lehigh.EDU (128.180.128.82)  0.952ms  0.649ms  0.830ms
  4  ewfmc-ewfmd.CC.Lehigh.EDU (128.180.128.89)  1.005ms  1.687ms  1.464ms
  5  local.lehigh1.magpi.net (198.32.42.145)  5.148ms  4.810ms  4.721ms
  6  phl-02-08.backbone.magpi.net (198.32.42.197)  4.277ms  4.895ms  4.362ms
  7  remote.princeton.magpi.net (198.32.42.66)  33.474ms 20.958ms 20.399ms
  8  gigagate1.Princeton.EDU (128.112.12.21)  25.451ms  9.580ms  20.908ms
  9  hulk.Princeton.EDU (128.112.128.15)  11.067ms  *  34.043ms
netstat

- Tons o' network statistics

# netstat | more
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address       Foreign Address           State
tcp  0     0 some server:www       td9091978.adsl.ter:1819 ESTABLISHED
tcp  0     0 some server:www       td9091978.adsl.ter:1817 TIME_WAIT
tcp  0     0 some server:www       unknown.servercen:53522 TIME_WAIT
tcp  0     0 some server:www       lj1157.inktomisea:49477 TIME_WAIT
tcp  0     1 some server:1248       218.15.192.166:smtp SYN_SENT
tcp  0     0 some server:www       cable200-75-67-206:3307 FIN_WAIT2
tcp  0     0 some server:1224       mx02.osn.de:smtp ESTABLISHED
tcp  0     0 localhost:x11-ssh-offset localhost:57893 ESTABLISHED
tcp  0     4209 localhost:6023     localhost:34263 FIN_WAIT1

- Can also show
  - interface configurations, routing tables, counter values
Packet sniffers

- Show you what is really on the network
- Not as useful in a switched environment
- Examples: tcpdump, wireshark

```bash
# tcpdump
tcpdump: listening on eth0
19:05:08 220.168.28.55.http > wume1.cse.lehigh.edu.64207: P
1001579411:1001579684(273) ack 3591949882 win 65300 <nop,nop,timestamp
64538628 1686086162> (DF)
19:05:08 wume1.cse.lehigh.edu.36560 > G.ROOT-SERVERS.NET.domain: 7131
19:05:08 G.ROOT-SERVERS.NET.domain > wume1.cse.lehigh.edu.36560: 7131-
% 0/4/2 (164) (DF)
19:05:08 wume1.cse.lehigh.edu.36560 > l.gtld-servers.net.domain: 24184
A? NS1.APNIC.NET. (31) (DF)
19:05:08 wume1.cse.lehigh.edu.36560 > ns.ripe.net.domain: 12092 [1au]
PTR? 55.28.168.220.in-addr.arpa. (55) (DF)
```