Precept 3

Host Configuration

Peng Sun

What TCP conn. running?

- Commands
  - `netstat [-n] [-p] [-c]` (Linux)
  - `lsof -i -P` (Mac)
  - `ss` (newer version of netstat)
- Demo
  - `iperf`: TCP-based throughput test tool

Demo

- `node0:~>` `netstat -npc`
- `node1:~>` `netstat -npc`
- `node0:~>` `netstat -npc`
- `node1:~>` `netstat -npc`
- `node0:~>` `iperf -c 10.1.1.3`
- `node1:~>` `iperf -s`

Play with IP Layer

- `ifconfig`
  - Show all the network interfaces
  - Configure IP
  - Configure MAC (!)
- `route`
  - Show local IP routing table
  - Set routes: add/del

Demo

- `node0:~>` `ping 10.1.2.2`
- `node0:~>` `route add -net 10.1.2.0 netmask 255.255.255.0 gw 10.1.1.3`
- `node2:~>` `route add -net 10.1.1.0 netmask 255.255.255.0 gw 10.1.2.3`

traceroute

- Why we need `traceroute`?
  - No global information
  - Want to know the forwarding path
- Based on ICMP
  - Internet Control Message Protocol
  - Used to signal error
- Adjust Time-To-Live for each hop
  - When timeout, ICMP returns the IP where TTL expires.
**traceroute**

```
    Server       Router 2       Router 1       User
    ---------------------------------------------
  ICMP TTL=1   Timeout at Rt. 1
  ICMP TTL=2   Timeout at Rt. 2
  ICMP TTL=3   Reply from Server
```

**ARP**

- ARP table (cache)
  1. Look up local ARP table
  2. If not, broadcast to ask
  3. LAN switch caches ARP to port

**ARP Spoofing**

- No protection from ARP itself
- Rely on other mechanism
  - Static ARP entry (perfect security. High cost of maintenance)
  - Spoofing detection software
- Legitimate usage
  - Hotel
  - Redundancy of service (takeover of bad server)

**Wireshark**

- [http://www.wireshark.org/](http://www.wireshark.org/)
- Packet Capture & Analysis
  - Live capture
  - Critical for Debug in Assign. 2
- Filter
  - e.g., ip / (not) arp / tcp / etc.