CS244A Review Session
Routing and DNS

January 18, 2008
Peter Pawlowski

Slides derived from:
Justin Pettit (2007)
Matt Falkenhagen (2006)
Yashar Ganjali (2005)
Guido Appenzeller (2002)

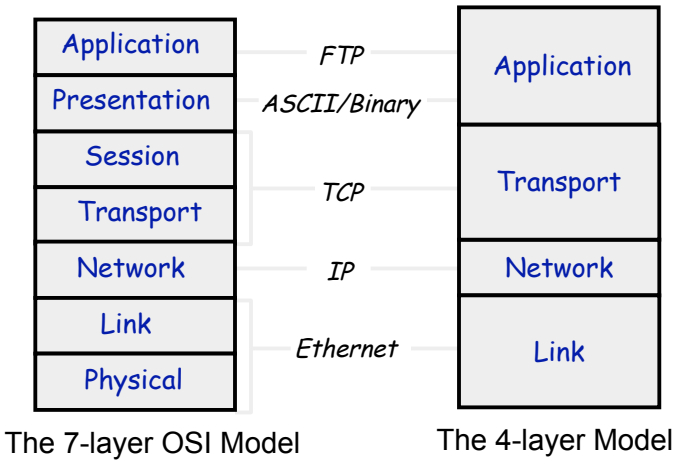
Announcements

- PA #1 was due at noon
- Problem submitting? Send to TA.
- PS #1 due Tuesday at noon
- PA #2 live tonight at 11:59PM

What's Covered Today

- The three most important things learned so far:
  - The Layer Model
  - IP and Routing Basics
  - The Domain Name System (DNS)
- Some useful Network Tools
  - Netstat and ifconfig
  - Traceroute
  - Tcpdump/Wireshark
  - Host

The Layer Model



The 7-layer OSI Model

The 4-layer Model

- What abstraction(s) does each layer expose?

Useful tools #1a: netstat

Tells you about current network status

- Current TCP sessions on the system
  - netstat -t
- Current TCP listeners on the system
  - netstat -ltn
- Current routing table
  - netstat –r
  - netstat -rn (to display IP addresses instead of domain names)
- Current interfaces
  - netstat –i

Useful tools #1b: ifconfig

Tells you about current network interfaces

- Displays all interfaces, including their MTU, netmask, and IP addresses.
  - ifconfig –a
- Must have root privileges to modify the network interfaces but anyone may view the current state

```
[user@myth8 ~] ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:0F:1F:84:75:2E
          inet addr:171.64.15.186  Bcast:171.64.255.255  Mask:255.255.0.0
          inet6 addr: fe80::20f:1fff:fe84:752e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2393901 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1958553 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1108847978 (1.0 GiB)  TX bytes:1208671699 (1.1 GiB)
          Base address:0xdcc0 Memory:dfee0000-dff00000
```

Layer Trivia

- Which layers are the following protocols:

IP	Network Layer
TCP	Transport Layer
HTTP	Application Layer, on top of TCP
FTP	Application Layer, on top of TCP
Wi-Fi/802.11	Link Layer
Bluetooth	Link Layer plus some Application
DHCP	Between Link and Network

Protocol Quiz

- Q: How does a computer decide whether an incoming IP packet is UDP or TCP?
- A: Look at the protocol field.

- Q: How does a computer decide whether an incoming IP packet is HTTP or FTP?
- A: Look at the port number. But it doesn't care, it just sends it to the application bound to that port.

- Q: You just fragged your friend with the AK-47 on Counter-Strike. What protocols did you use?
- A: Application layer protocol over UDP.

Useful tools #2a: tcpdump

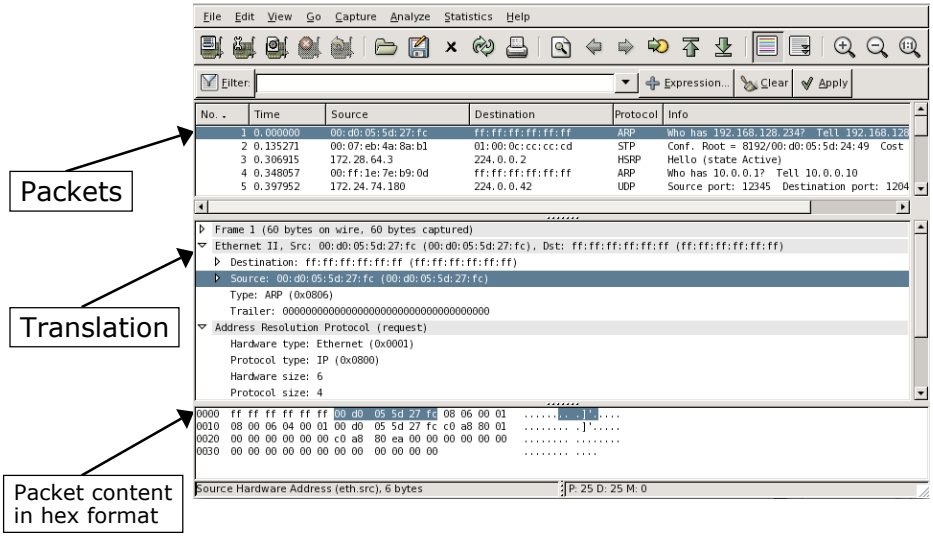
- Tool to capture and display network traffic on the local area network
- Runs on Unix and Windows
- On Unix only the root user may listen on the interface

```
[root@colorado user]# tcpdump -n -i eth0 -x -X -vvv -c 1 -s 200
tcpdump: listening on eth0
11:17:47.738282 171.64.74.34.22 > 64.175.39.85.1221: P [tcp sum ok]
     2168458766:2168458810(44) a
ck 1258905391 win 5840 (DF) [tos 0x10]  (ttl 64, id 50841, len 84)
0x0000   4510 0054 c699 4000 4006 1694 ab40 4a22  E..T..@.@....@J"
0x0010   40af 2755 0016 04c5 8140 0e0e 4b09 5f2f  @.'U.....@..K._/
```

Useful tools #2b: wireshark

- GUI tool similar to tcpdump. Lets you view packets and translates a lot of the fields for you
- Formally called ethereal
- Runs on Unix or Windows
- On Unix only the root user may listen on the interface
- Both wireshark and tcpdump are available for the Myth systems in /usr/class/cs244a/bin
- No man page but has lots of documentation, including a user manual at http://www.wireshark.org

View of wireshark



IP Fragmentation Quiz

- Q: What happens if a packet arrives that is too long for the link layer?
- A: It is split into several pieces.

- Q: Where in the network are packets fragmented?
- A: Can happen at any router or host!

- Q: Where are they re-assembled?
- A: Only at the destination!

- Q: What percentage of packets in the internet are fragmented?
- A: Almost none

Useful tools #3: traceroute

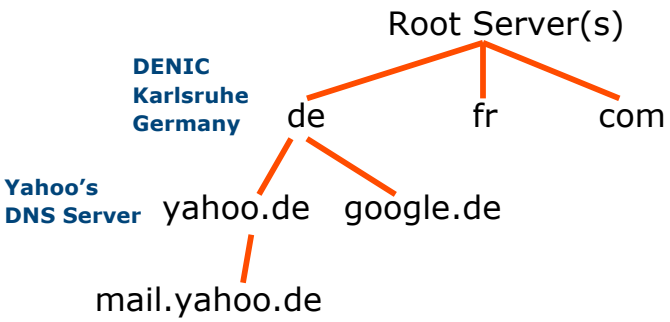
- Traces how a packet gets from the local machine to the destination
  - Sets TTL to n = 1...32
  - Collects "timeout" ICMP messages from hosts along the way
- Good for finding out what is happening if the network is down
- Also good for finding what the MTU on a path is or if packets get fragmented
  - traceroute -F <host> <fragment size>

Domain Name Service (DNS)

- Maps domain names (e.g. cs.stanford.edu) to IP addresses (e.g. 171.64.64.64)
- Top level name servers handle top level domains (e.g. ".edu", ".de" etc.)
- Each domain has a DNS server that is responsible for the domain (e.g. DENIC for the ".de" domain)
- Each subdomains (e.g. google.de) has a DNS server that is responsible for the subdomain

Domain Name Service (DNS)

- To find a mapping I work my way downwards



- In reality all this is done for me by my local DNS server

Useful tools #4: host

Tells you anything (almost) about DNS records

- Map a DNS name to an IP address
  host www.google.com
- Map an IP address to a DNS name
  host 171.64.64.64
- Which DNS servers are responsible for a domain
  host –t NS stanford.edu
- Which hosts accept mail for a domain
  host –t MX stanford.edu

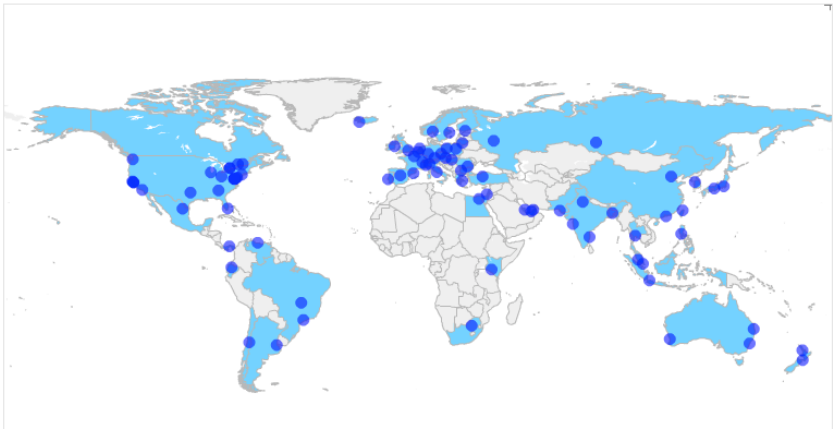
Root Name Servers (The Old Way)

There are 13 root name servers
[Herndon, VA, USA] A.ROOT-SERVERS.NET (Verisign)
[Marina del Rey, CA, USA] B.ROOT-SERVERS.NET (ISI)
[Herndon, VA, USA] C.ROOT-SERVERS.NET (Cogent)
[College Park, MD, USA] D.ROOT-SERVERS.NET (UM)
[Mt View, CA, USA] E.ROOT-SERVERS.NET (NASA)
[Palo Alto, CA, USA] F.ROOT-SERVERS.NET (ISC)
[Columbus, OH, USA] G.ROOT-SERVERS.NET (DoD)
[Aberdeen, MD, USA] H.ROOT-SERVERS.NET (US Army)
[Stockholm, Sweden] I.ROOT-SERVERS.NET (Autonomica)
[Dulles, VA, USA] J.ROOT-SERVERS.NET (Verisign)
[London, UK] K.ROOT-SERVERS.NET (Reseaux)
[Los Angeles, CA, USA] L.ROOT-SERVERS.NET (ICANN)
[Tokyo, Japan] M.ROOT-SERVERS.NET (WIDE)

Root Name Servers (The Old Way)

Source: ICANN

Root Name Servers (Today)



Source: ICANN