Network Tools and Real Network Traces

Professor Nelson Fonseca

Institute of Computing
State University of Campinas (Unicamp)

1. Objectives
2. Tools
   - Configuration and Information
   - Name to IP Address Resolution (DNS)
   - Making a Connection
   - IP to MAC address resolution (ARP)
   - Performance and Statistics
3. Network Traces
4. Questions?

First Objective

Learn to use basic network tools in a Unix-like system

Why?

- Notion about network parameters in the real world
- Understand the relationship between the protocols
- "See" the network working

Second Objective

Interpret a real network trace

Why?

- Very useful to simulation (input)
- Cheaper and simpler than construct a network
- Useful to analyse experiments later
- "See" the network behaviour during a time interval

UNICAMP

UNICAMP

ifconfig

Function

Configures or displays information about network interfaces (link and network layers)

- Changes IP address, network mask, MTU, etc...
- Even MAC address!
- Shows the configured parameters
- Shows interface statistics: send and received bytes/packets, errors, collisions, etc...

ifconfig output

```
pillars:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:40:F4:5F:4B:5E
          inet addr:10.3.77.11  Bcast:10.3.77.255  Mask:255.255.255.0
          inet6 addr: fe80::240:f4ff:fe5f:4b5e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:7782356 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6378201 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2295837665 (2.1 GiB)  TX bytes:3565175684 (3.3 GiB)
          Interrupt:5 Base address:0xd000
```

route

Function

Configures or displays information about routes

- Changes/Shows the configured routes (IP address and interfaces)
- Mostly used to change the default gateway

```
pillars:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.3.77.0       0.0.0.0         255.255.255.0   U     0      0        0 eth0
0.0.0.0         10.3.77.1       0.0.0.0         UG    0      0        0 eth0
```

netstat

Function

Displays various network parameters (including the same as `ifconfig` and `route`)

- Mostly used to show informations about active connections
- Shows transport protocol, source IP address:port and destination IP address:port to each active connection

```
pillars:~# netstat -anp | grep :80
tcp        0      0 10.3.77.11:34408      72.14.209.99:80       TIME_WAIT -
```

nslookup

Function

Finds out the corresponding IP address of a host name via DNS protocol. It makes the reverse search too

- Shows information about the contacted DNS server
- Shows any number of IP address associated to a host name
- Mostly used to resolve host name to IP address

```
pillars:~# nslookup www.ic.unicamp.br
Server:         143.106.7.31
Address:        143.106.7.31#53

www.ic.unicamp.br       canonical name = solimoes.ic.unicamp.br.
Name:   solimoes.ic.unicamp.br
Address: 143.106.7.13
```

telnet

Function

Connects to a TCP service available at a host via Internet

- Very useful to test if a host is alive at application level
- Works to any service that uses TCP
- It's necessary to know the specific commands of the application layer (HTTP commands $\neq$ SMTP commands $\neq$ IMAP commands, etc...)

telnet output

```
pillars:~# telnet www.unicamp.br 80
Trying 143.106.10.30...
Connected to lvs0.unicamp.br.
Escape character is '^]'.
HEAD / 1.1

HTTP/1.1 200 OK
Date: Wed, 09 May 2007 13:49:43 GMT
Server: Apache/2.0.59 (Unix) mod_ssl/2.0.59 OpenSSL/0.9.8d PHP/5.2.1
Last-Modified: Wed, 09 May 2007 13:45:03 GMT
ETag: "2a847b-7c2c-bdbd95c0"
Accept-Ranges: bytes
Content-Length: 31788
Connection: close
Content-Type: text/html

Connection closed by foreign host.
```

UNICAMP

arp

Function

Manipulates the ARP protocol table and shows the IP and MAC addresses in the ARP cache

- Mostly used to show the ARP table
- Can be used to manual changes

```
pillars:~# arp -v -n
Address                  HWtype  HWaddress           Flags Mask  Iface
10.3.77.1                ether   00:00:B4:74:4C:85   C           eth0
10.3.77.3                ether   00:04:23:B9:25:7D   C           eth0
10.3.77.10               ether   00:02:B3:E9:17:4A   C           eth0
Entries: 3      Skipped: 0      Found: 3
```

ping

Function

Checks connectivity to a host and measures the RTT of sent packets

- Mostly used to test if a host is alive at network level
- Sends ICMP datagrams that contains `ECHO_REQUEST` messages
- The host replies with ICMP datagrams than contains `ECHO_RESPONSE` messages
- The RTT values can be used to check the route integrity

ping output

```
pillars:~# ping 72.14.209.104 -c 5
PING 72.14.209.104 (72.14.209.104) 56(84) bytes of data.
64 bytes from 72.14.209.104: icmp_seq=1 ttl=242 time=128 ms
64 bytes from 72.14.209.104: icmp_seq=2 ttl=242 time=131 ms
64 bytes from 72.14.209.104: icmp_seq=3 ttl=242 time=127 ms
64 bytes from 72.14.209.104: icmp_seq=4 ttl=242 time=130 ms
64 bytes from 72.14.209.104: icmp_seq=5 ttl=242 time=129 ms

--- 72.14.209.104 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 127.370/129.560/131.783/1.538 ms
```

traceroute

Function

Traces the route followed by a IP packet to a host and measures the RTT of sent packets to each hop in the route

- Sends three UDP datagrams with TTL 1. After that, sends three UDP datagrams with TTL 2. After that, sends three UDP datagrams with TTL 3, ... until reach the host
- The hops in the path detect the TTL $==$ 0 and reply with ICMP datagrams that contains a `TIME_EXCEEDED` message

traceroute output

```
pillars:~# traceroute www.unicamp.br
traceroute to lvs0.unicamp.br (143.106.10.30), 30 hops max,
            40 byte packets
 1  medusa (10.3.77.1)  0.255 ms  0.192 ms  0.180 ms
 2  143.106.7.129 (143.106.7.129)  0.437 ms  0.324 ms  0.410 ms
 3  area3-gw.unicamp.br (143.106.1.129)  0.546 ms  0.475 ms  0.362 ms
 4  corp-gw.unicamp.br (143.106.2.55)  0.599 ms  0.399 ms  0.710 ms
 5  lvs0.unicamp.br (143.106.10.30)  0.926 ms  0.608 ms  0.642 ms
```

Real traces

Function

Useful to understand the protocols behaviour and to evaluate simulators with real load

- Traces format aren't standard
- The most used trace format represents a packet by line. Each line has a pair: time, size
- Traces can be collected at routers in the network core or at hosts using appropriated softwares like sniffers

Example – trace collected by wireshark sniffer

No.	Time	Source	Destination	Protocol
18	24.491296	143.106.16.31	143.106.16.144	DNS
19	24.493156	143.106.16.144	143.106.16.31	DNS
20	24.493324	143.106.16.31	143.106.16.144	DNS
21	24.494154	143.106.16.144	143.106.16.31	DNS

???

Questions?