Network tools

- Tcpdump
- Traceroute
- Ping

1. Tcpdump

- A packet tracing tool
  - Works on various host platforms
  - Captures packets going through a certain network interface
  - Shows packet header information

From tcpdump Data

- General traffic statistics
  - Traffic volume
  - Burstiness
  - Traffic volume by types
- End-to-end statistics
  - Connection throughput
  - Round trip delay
  - Loss rate

Usage

tcpdump [**-AdDefILnNOpqRStuUvxX**]
[**-i** *interface*][**-c** *count*]
[**-w** *file*] [**-C** *file_size*]
[**-r** *file*]
[**-T** *type*] [**-s** *snaplen*]
[**-m** *module*] [**-E** *algo:secret*] [**-y** datalinktype]
[**-F** *file*] [*expression*]

[-i interface]

- To read packets from a certain network interface

tcpdump –i eth0

[-c count]

- To read up to *count* number of packets

tcpdump –i eth0 –c 5

[-w file]

- To write the output to a file
- Instead of printing to the screen the packet header information

tcpdump –i eth0 –c 5 –w tmp.tr

[-C file_size]

- To output to files up to *file_size* million bytes
- When tmp.tr exceeds *file_size* MB, tmp.tr2 is opened to continue tracing

tcpdump –i eth0 –c 5 –w tmp.tr –C 1

[-r file]

- To read packets from a file
- Generated from [**-w** *file*]

tcpdump –r tmp.tr

[expression]

- To select packets to be read
- Types, directions, protocols
  - [*protocol*][*direction*][*type*]

**tcpdump –i eth0 –c 5 –w tmp.tr –C 100 **
[*expression*]

Expression: Type

- Selecting packets of a particular host, particular network, particular port
- {**host, net, port**} [{*name, number*}]

host mango.csd.uoc.gr
net 147.52.19.0
port 80

Expression: Direction

- Selecting packets of a particular direction, inbound or outbound
- {**src, dst, src or dst, src and dst**}[*type*]

src or dst host nslab.ee.ntu.edu.tw

dst net 140.112.154

dst port 80

Expression: Protocol

- Selecting packets of a particular protocol
- **{ether**, **ip**, **ip6**, **arp**, **rarp**, **tcp**, **udp**, …} {**multicast**, **broadcast**}

ip src or dst host nslab.ee.ntu.edu.tw

arp dst net 140.112.154

tcp dst port 80

Expression: Others

- Selecting packets of particular sizes in bytes
- {**greater, less**}[*size*]
- **len** {**>=**, **<=**}[*size*]

Expression: Operands

- ! or **not**
- && or **and**
- || or **or**

ip host nslab and \(cc.ee.ntu.edu.tw or www.ntu.edu.tw \)

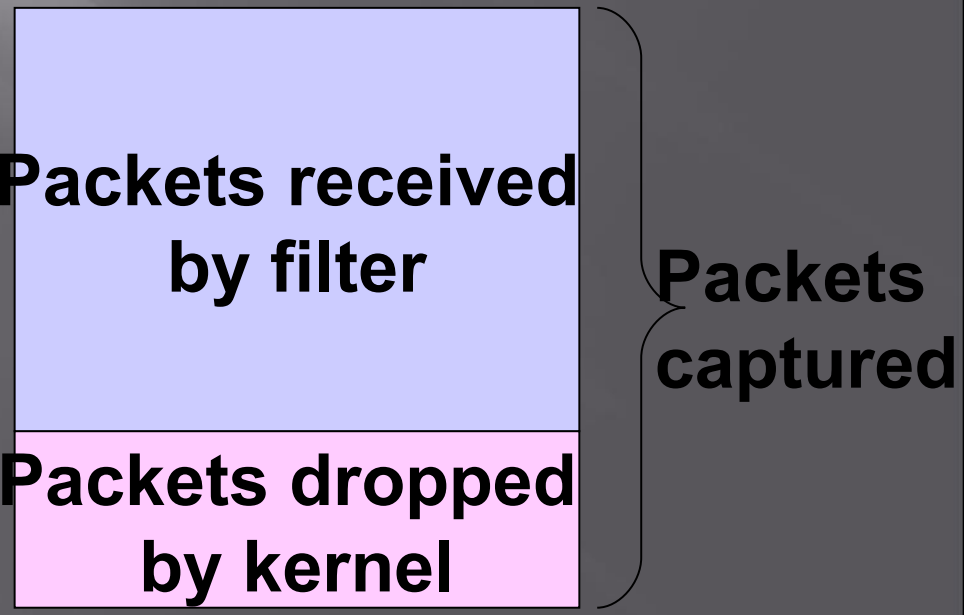
[-F file]

- To load [*expression*] from a file

tcpdump –i eth0 –c 5 –w tmp.tr –C 100 –F test.exp

Final Output

- # packet captured
  - All packets going thru the interface
- # packet received by filter
  - Packets in tcpdump output
- # packet dropped by kernel
  - Packets not in tcpdump output



2. Traceroute

- Shows the path a packet of information takes from your computer to one you specify.
- Lists all the routers it passes through until it reaches its destination, or fails to and is discarded.
- Tells you how long each 'hop' from router to router takes.
- It is widely used
  - Diagnosis of connectivity problems
  - Inferrence of network properties
  - Internet maps

Traceroute example1(www.ntua.gr)

- traceroute to achilles.noc.ntua.gr (147.102.222.210), 64 hops max, 40 byte packets
- 1 dsldevice.lan (192.168.1.254) 62 ms 97 ms 100 ms
- 2 bbras-llu-her-01L0.forthnet.gr (194.219.231.56) 32 ms 32 ms 32 ms
- 3 core-her-01G0-3-0.forthnet.gr (194.219.244.33) 33 ms 32 ms 33 ms
- 4 core-kln-05Gi0-0-2.forthnet.gr (194.219.199.197) 39 ms 40 ms 39 ms
- 5 core-kln-01.forthnet.gr (62.1.37.73) 40 ms 40 ms 40 ms
- 6 core-ath-08G4-0-0.forthnet.gr (212.251.94.5) [MPLS: Label 17760 Exp 0] 40 ms 40 ms 42 ms
- 7 grix.forthnet.gr (194.219.199.38) 39 ms 40 ms 40 ms
- 8 grnet.gr-ix.gr (83.212.8.1) 39 ms 40 ms 40 ms
- 9 athens3-to-eie2.backbone.grnet.gr (195.251.27.45) 42 ms 40 ms 41 ms
- 10 clientRouter.ntua-primary.athens-3.access-link.gr (194.177.209.118) 41 ms 41 ms 40 ms
- 11 achilles.noc.ntua.gr (147.102.222.210) 41 ms 40 ms 41 ms

Traceroute example 2(www.google.com)

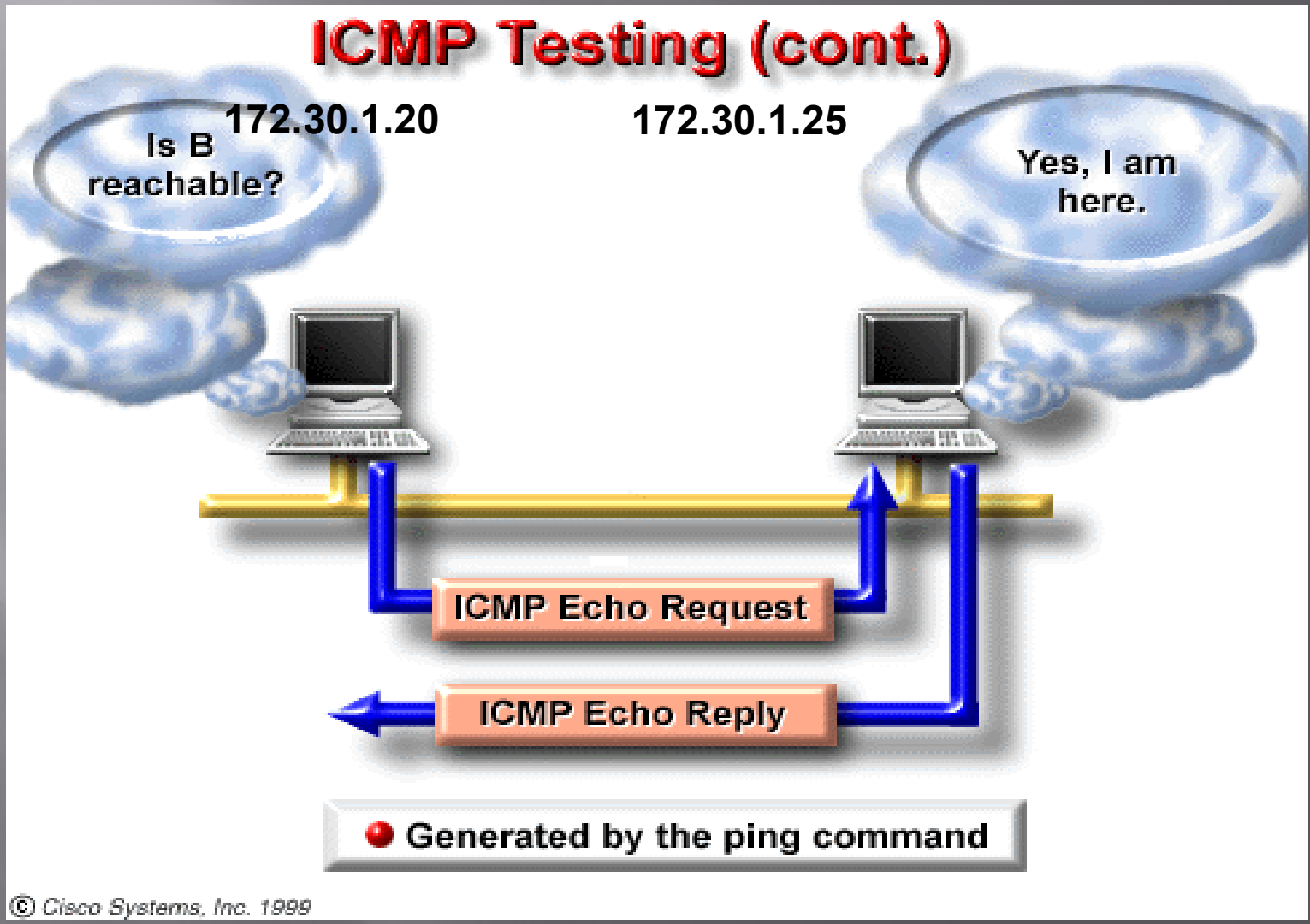
- traceroute to www.l.google.com (209.85.229.104), 64 hops max, 40 byte packets
- 1 dsldevice.lan (192.168.1.254) 87 ms 97 ms 100 ms
- 2 bbras-llu-her-01L0.forthnet.gr (194.219.231.56) 32 ms 32 ms 32 ms
- 3 core-her-01G0-3-0.forthnet.gr (194.219.244.33) 32 ms 33 ms 32 ms
- 4 core-kln-05Gi0-0-2.forthnet.gr (194.219.199.197) 39 ms 41 ms 40 ms
- 5 core-kln-01.forthnet.gr (62.1.37.73) 40 ms 40 ms 39 ms
- 6 core-ath-08G4-0-0.forthnet.gr (212.251.94.5) [MPLS: Label 15778 Exp 0] 40 ms 40 ms 39 ms
- 7 core-ath-03.forthnet.gr (194.219.227.103) 40 ms 40 ms 39 ms
- 8 pal9-forthnet-1.pal.seabone.net (213.144.181.173) 56 ms 56 ms 57 ms
- 9 mil53-mil26-racc2.mil.seabone.net (195.22.205.209) 157 ms 158 ms 158 ms
- 10 72.14.196.141 (72.14.196.141) 105 ms * 108 ms
- 11 * 216.239.47.128 (216.239.47.128) 95 ms (TOS=128!) 209.85.249.54 (209.85.249.54) 115 ms
- 12 209.85.249.234 (209.85.249.234) [MPLS: Label 566960 Exp 4] 88 ms 209.85.251.113 (209.85.251.113) 135 ms 199 ms
- 13 209.85.248.182 (209.85.248.182) [MPLS: Label 342338 Exp 4] 102 ms 209.85.250.140 (209.85.250.140) [MPLS: Label 659408 Exp 4] 138 ms 209.85.248.182 (209.85.248.182) [MPLS: Label 288834 Exp 4] 115 ms
- 14 209.85.255.212 (209.85.255.212) 118 ms 72.14.232.130 (72.14.232.130) 118 ms 118 ms
- 15 216.239.49.45 (216.239.49.45) 118 ms 117 ms 209.85.251.231 (209.85.251.231) 106 ms
- 16 209.85.243.73 (209.85.243.73) 114 ms 209.85.243.77 (209.85.243.77) 106 ms 109 ms
- 17 ww-in-f104.google.com (209.85.229.104) 106 ms (TOS=0!) 104 ms 105 ms

3.Ping

- Used to test the reachability of a host
- Measures the round-trip time for messages sent from the originating host to a destination computer

- The sender of the ping, transmits an ICMP message, “Echo Request”
- The ip address (destination) of the ping, returns the ICMP message, “Echo Reply”

Ping Command



Ping output

```
artpap@artpap-laptop:~$ ping www.csd.uoc.gr
PING ixion.csd.uoc.gr (147.52.16.5) 56(84) bytes of data.
64 bytes from ixion.csd.uoc.gr (147.52.16.5): icmp_seq=1 ttl=53 time=34.7 ms
64 bytes from ixion.csd.uoc.gr (147.52.16.5): icmp_seq=2 ttl=53 time=33.9 ms
64 bytes from ixion.csd.uoc.gr (147.52.16.5): icmp_seq=3 ttl=53 time=33.2 ms
64 bytes from ixion.csd.uoc.gr (147.52.16.5): icmp_seq=4 ttl=53 time=33.7 ms
64 bytes from ixion.csd.uoc.gr (147.52.16.5): icmp_seq=5 ttl=53 time=33.2 ms
^C
--- ixion.csd.uoc.gr ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 33.216/33.790/34.786/0.579 ms
```