

Problem 1

Ping another IP address.

Commands:

Open wireshark using `sudo wireshark`

List arp cache using `arp -n`

Clear cach using `arp -d IPADDRESS`

Open sniffer using ping IPADDRESS

The image shows two windows. The top window is Wireshark 1.6.7, displaying a packet capture on the eth0 interface. The packet list shows ICMP Echo (ping) requests and replies between 10.30.56.200 and 10.30.56.101. The packet details pane shows the structure of an ICMP Echo request, including the type, code, identifier, and sequence number. The packet bytes pane shows the raw data in hexadecimal and ASCII.

The bottom window is a terminal running on a system named 'reshma@zn-HP-Compaq-Pro-6300-MT-1-S'. It shows the output of the `arp -n` command, which lists the ARP table. The table has columns for Address, HWtype, HWaddress, Flags Mask, and Iface. The entries show the local interface eth0 and the IP address 10.30.56.101.

```

reshma@zn-HP-Compaq-Pro-6300-MT-1-S$ arp -n
Address HWtype HWaddress Flags Mask Iface
10.30.56.1 ether 00:1f:9d:f2:bcc9 C eth0
10.30.56.120 ether 6c:3b:e5:3d:90:63 C eth0
10.30.56.101 ether 88:51:fb:42:80:72 C eth0

reshma@zn-HP-Compaq-Pro-6300-MT-1-S$ ping 10.30.56.101
PING 10.30.56.101 (10.30.56.101) 56(84) bytes of data:
64 bytes from 10.30.56.101: icmp_req=1 ttl=64 time=0.507 ms
64 bytes from 10.30.56.101: icmp_req=2 ttl=64 time=0.525 ms
64 bytes from 10.30.56.101: icmp_req=3 ttl=64 time=0.528 ms
64 bytes from 10.30.56.101: icmp_req=4 ttl=64 time=0.513 ms
64 bytes from 10.30.56.101: icmp_req=5 ttl=64 time=0.527 ms
64 bytes from 10.30.56.101: icmp_req=6 ttl=64 time=0.747 ms
64 bytes from 10.30.56.101: icmp_req=7 ttl=64 time=0.523 ms
64 bytes from 10.30.56.101: icmp_req=8 ttl=64 time=0.613 ms
64 bytes from 10.30.56.101: icmp_req=9 ttl=64 time=0.579 ms
64 bytes from 10.30.56.101: icmp_req=10 ttl=64 time=0.494 ms
64 bytes from 10.30.56.101: icmp_req=11 ttl=64 time=0.547 ms
64 bytes from 10.30.56.101: icmp_req=12 ttl=64 time=0.519 ms
64 bytes from 10.30.56.101: icmp_req=13 ttl=64 time=0.514 ms
64 bytes from 10.30.56.101: icmp_req=14 ttl=64 time=0.698 ms
64 bytes from 10.30.56.101: icmp_req=15 ttl=64 time=0.510 ms
64 bytes from 10.30.56.101: icmp_req=16 ttl=64 time=0.513 ms
64 bytes from 10.30.56.101: icmp_req=17 ttl=64 time=0.551 ms
64 bytes from 10.30.56.101: icmp_req=18 ttl=64 time=0.501 ms
64 bytes from 10.30.56.101: icmp_req=19 ttl=64 time=0.804 ms
64 bytes from 10.30.56.101: icmp_req=20 ttl=64 time=0.655 ms
64 bytes from 10.30.56.101: icmp_req=21 ttl=64 time=0.509 ms
64 bytes from 10.30.56.101: icmp_req=22 ttl=64 time=0.567 ms
64 bytes from 10.30.56.101: icmp_req=23 ttl=64 time=0.492 ms
64 bytes from 10.30.56.101: icmp_req=24 ttl=64 time=0.662 ms
64 bytes from 10.30.56.101: icmp_req=25 ttl=64 time=0.558 ms
64 bytes from 10.30.56.101: icmp_req=26 ttl=64 time=0.745 ms
64 bytes from 10.30.56.101: icmp_req=27 ttl=64 time=0.559 ms
64 bytes from 10.30.56.101: icmp_req=28 ttl=64 time=0.528 ms

```

Problem 2

ping www.google.com

Commands:

Open wireshark using `sudo wireshark`

Open sniffer using `ping www.google.com`

The screenshot displays two windows from a Linux environment. The top window is Wireshark 1.6.7, capturing traffic on the eth0 interface. The packet list shows various protocols including Spanning-tree, ICMP, and DNS. The packet details pane shows the selected packet's structure. The bottom window is a terminal showing the execution of network commands. It starts with an ARP table listing the IP 10.30.56.120 and its MAC address. Then, it runs a series of ping commands to 74.125.236.114, showing the sequence number, bytes, and time for each request and reply.

Wireshark Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
10	0.000000	Cisco 7f:1b:2e	Spanning-tree-(for-br)	STP	60	Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x802e
20	0.255528	10.30.56.200	74.125.236.114	ICMP	98	Echo (ping) request id=0x8cdc, seq=5/1280, ttl=64
30	0.318776	74.125.236.114	10.30.56.200	ICMP	98	Echo (ping) reply id=0x8cdc, seq=5/1280, ttl=56
40	0.319028	10.30.56.200	8.8.8.8	DNS	87	Standard query PTR 114.236.125.74.in-addr.arpa
50	0.405558	8.8.8.8	10.30.56.200	DNS	126	Standard query response PTR bom03s01-in-f18.1e100.net
60	0.256601	10.30.56.200	74.125.236.114	ICMP	98	Echo (ping) request id=0x8cdc, seq=6/1536, ttl=64
70	0.1464059	10.30.56.200	8.8.8.8	DNS	76	Standard query A daisy.ubuntu.com
80	0.1561294	8.8.8.8	10.30.56.200	DNS	108	Standard query response A 91.189.95.54 A 91.189.95.55
90	0.000371	Cisco 7f:1b:2e	Spanning-tree-(for-br)	STP	60	Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x802e
100	0.255617	10.30.56.200	74.125.236.114	ICMP	98	Echo (ping) request id=0x8cdc, seq=7/1792, ttl=64
110	0.310070	74.125.236.114	10.30.56.200	ICMP	98	Echo (ping) reply id=0x8cdc, seq=7/1792, ttl=56
120	0.310310	10.30.56.200	8.8.8.8	DNS	87	Standard query PTR 114.236.125.74.in-addr.arpa
130	0.405899	8.8.8.8	10.30.56.200	DNS	126	Standard query response PTR bom03s01-in-f18.1e100.net
140	0.246622	10.30.56.200	8.8.8.8	DNS	76	Standard query A daisy.ubuntu.com
150	0.555340	8.8.8.8	10.30.56.200	DNS	108	Standard query response A 91.189.95.54 A 91.189.95.55
160	0.3256978	10.30.56.200	74.125.236.114	ICMP	98	Echo (ping) request id=0x8cdc, seq=8/2048, ttl=64
170	0.354137	74.125.236.114	10.30.56.200	ICMP	98	Echo (ping) reply id=0x8cdc, seq=8/2048, ttl=56
180	0.354394	10.30.56.200	8.8.8.8	DNS	87	Standard query PTR 114.236.125.74.in-addr.arpa
190	0.408036	8.8.8.8	10.30.56.200	DNS	126	Standard query response PTR bom03s01-in-f18.1e100.net
200	0.000062	Cisco 7f:1b:2e	Spanning-tree-(for-br)	STP	60	Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x802e
210	0.258046	10.30.56.200	74.125.236.114	ICMP	98	Echo (ping) request id=0x8cdc, seq=9/2304, ttl=64
220	0.352602	74.125.236.114	10.30.56.200	ICMP	98	Echo (ping) reply id=0x8cdc, seq=9/2304, ttl=56
230	0.352815	10.30.56.200	8.8.8.8	DNS	87	Standard query PTR 114.236.125.74.in-addr.arpa
240	0.491070	8.8.8.8	10.30.56.200	DNS	126	Standard query response PTR bom03s01-in-f18.1e100.net
250	0.526834	10.30.56.200	74.125.236.114	ICMP	98	Echo (ping) request id=0x8cdc, seq=10/2560, ttl=64
260	0.705502	10.30.56.122	224.0.0.251	IGMP	129	Standard query SRV amajithesystem-of-a-down.presence.tcp.local, "QV" question A

Terminal Output:

```
reshma@zn-HP-Compaq-Pro-6300-MT:~$ arp -n
Address HWtype HWaddress Flags Mask Iface
10.30.56.1 ether 08:1f:9d:f2:bc:c9 C eth0
10.30.56.120 ether 6c:3b:e5:3d:90:63 C eth0
reshma@zn-HP-Compaq-Pro-6300-MT:~$ ping www.google.com
PING www.google.com (74.125.236.114): 56(84) bytes of data:
64 bytes from bom03s01-in-f18.1e100.net (74.125.236.114): icmp_req=1 ttl=56 time=72.9 ms
64 bytes from bom03s01-in-f18.1e100.net (74.125.236.114): icmp_req=2 ttl=56 time=63.6 ms
64 bytes from bom03s01-in-f18.1e100.net (74.125.236.114): icmp_req=3 ttl=56 time=56.6 ms
64 bytes from bom03s01-in-f18.1e100.net (74.125.236.114): icmp_req=4 ttl=56 time=55.1 ms
64 bytes from bom03s01-in-f18.1e100.net (74.125.236.114): icmp_req=5 ttl=56 time=53.2 ms
64 bytes from bom03s01-in-f18.1e100.net (74.125.236.114): icmp_req=7 ttl=56 time=54.4 ms
64 bytes from bom03s01-in-f18.1e100.net (74.125.236.114): icmp_req=8 ttl=56 time=57.1 ms
64 bytes from bom03s01-in-f18.1e100.net (74.125.236.114): icmp_req=9 ttl=56 time=94.5 ms
64 bytes from bom03s01-in-f18.1e100.net (74.125.236.114): icmp_req=11 ttl=56 time=68.2 ms
64 bytes from bom03s01-in-f18.1e100.net (74.125.236.114): icmp_req=12 ttl=56 time=63.7 ms
64 bytes from bom03s01-in-f18.1e100.net (74.125.236.114): icmp_req=13 ttl=56 time=217 ms
64 bytes from bom03s01-in-f18.1e100.net (74.125.236.114): icmp_req=14 ttl=56 time=134 ms
64 bytes from bom03s01-in-f18.1e100.net (74.125.236.114): icmp_req=15 ttl=56 time=176 ms
64 bytes from bom03s01-in-f18.1e100.net (74.125.236.114): icmp_req=16 ttl=56 time=120 ms
64 bytes from bom03s01-in-f18.1e100.net (74.125.236.114): icmp_req=18 ttl=56 time=180 ms
64 bytes from bom03s01-in-f18.1e100.net (74.125.236.114): icmp_req=20 ttl=56 time=162 ms
64 bytes from bom03s01-in-f18.1e100.net (74.125.236.114): icmp_req=21 ttl=56 time=100 ms
64 bytes from bom03s01-in-f18.1e100.net (74.125.236.114): icmp_req=22 ttl=56 time=...
```