ECE461 Lab Report

Lab1 & Lab2

Mingqi Hou 99976767613
Xiaoyang Guo 999578513

Lab 1

EXERCISE 5

Question 1

Which files must be edited to change the name of a Linux PC?

· Edit the “HOSTNAME” field in /etc/sysconfig/network

Question 2

Which files include information that determines whether a Linux PC performs IP forwarding?

· “FORWARD_IPV4” field in /etc/sysconfig/network determines whether a Linux PC performs IP forwarding.

Question 3

Attach the content of the file /etc/sysconfig/network-scripts/ifcfg-eth0 to your lab report

```
DEVICE=eth0
BOOTPROTO=static
BROADCAST=10.0.1.255
IPADDR=10.0.1.11
NETMASK=255.255.255.0
NETWORK=10.0.1.0
ONBOOT=yes
METRIC=5
MII_NOT_SUPPORTED=no
USERCTL=yes
LINK_DETECTION_DELAY=6
IPV6INIT=no
IPV6TO4INIT=no
```

EXERCISE 6

Question 1

Include the output you saved in this exercise.

```
[root@PC1 root]# ping -c 5 10.0.1.12
PING 10.0.1.12 (10.0.1.12) 56(84) bytes of data.
64 bytes from 10.0.1.12: icmp_seq=1 ttl=64 time=0.113 ms
64 bytes from 10.0.1.12: icmp_seq=2 ttl=64 time=0.084 ms
64 bytes from 10.0.1.12: icmp_seq=3 ttl=64 time=0.082 ms
64 bytes from 10.0.1.12: icmp_seq=4 ttl=64 time=0.083 ms
64 bytes from 10.0.1.12: icmp_seq=5 ttl=64 time=0.080 ms
```

```
--- 10.0.1.12 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.080/0.088/0.113/0.014 ms

[root@PC2 root]# ping -c 5 10.0.1.11
PING 10.0.1.11 (10.0.1.11) 56(84) bytes of data.
64 bytes from 10.0.1.11: icmp_seq=1 ttl=64 time=0.109 ms
64 bytes from 10.0.1.11: icmp_seq=2 ttl=64 time=0.081 ms
64 bytes from 10.0.1.11: icmp_seq=3 ttl=64 time=0.078 ms
64 bytes from 10.0.1.11: icmp_seq=4 ttl=64 time=0.083 ms
64 bytes from 10.0.1.11: icmp_seq=5 ttl=64 time=0.079 ms
--- 10.0.1.11 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3997ms
rtt min/avg/max/mdev = 0.078/0.086/0.109/0.011 ms

[root@PC2 root]# ping -c 5 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.035 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.024 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.028 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.027 ms
64 bytes from 127.0.0.1: icmp_seq=5 ttl=64 time=0.027 ms
--- 127.0.0.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3998ms
rtt min/avg/max/mdev = 0.024/0.028/0.035/0.005 ms
```

Question 2

Explain the difference between pinging the local Ethernet interface and the loop-back interface. Specifically, on PC1, what is the difference between typing ping 10.0.1.11 and ping 127.0.0.1?

- Loopback interface is a virtual interface used by a computer to communicate with itself. Ethernet interface is physical interface. If the physical network is not connected to PC1, pinging 10.0.1.11 will fail, while pinging 127.0.0.1 will be successful.

EXERCISE 7A

Question 1

Include the saved output in your lab report. Explain the meaning of each field in the captured data.

```
[root@PC1 root]# tcpdump -n host 10.0.1.12
tcpdump: verbose output suppressed, use -v or -vv for full protocol
decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
15:54:28.951670 arp who-has 10.0.1.12 tell 10.0.1.11
15:54:28.951738 arp reply 10.0.1.12 is-at 00:04:5a:7a:c8:ca
15:54:28.951751 IP 10.0.1.11 > 10.0.1.12: ICMP echo request, id 19269,
seq 1, length 64
```

```
15:54:28.951820 IP 10.0.1.12 > 10.0.1.11: ICMP echo reply, id 19269,
seq 1, length 64
15:54:33.954590 arp who-has 10.0.1.11 tell 10.0.1.12
15:54:33.954609 arp reply 10.0.1.11 is-at 00:04:5a:7a:c8:25

6 packets captured
6 packets received by filter
0 packets dropped by kernel
```

- Each line starts with a timestamp, followed by a protocol.
  If it is an ARP request, the next field is the target's IP address. And after that is the sender's IP address. For ARP reply, it is sender's IP address followed by the target's MAC address.
  If it is an IP packet, the first field is the source and destination IP addresses. The field next is the protocol for which the data is using. The following field is for identification number. Packets of the same datagram share s the same identification number. After that is the TCP sequence number indicating the order of the packet in the datagram. And the last field indicates the size of the packet.

EXERCISE 7B

Question 1

Include the saved output in your lab report and interpret the results. How many of the Linux PCs responded to the broadcast ping?

```
[root@PC1 root]# ping -c 1 111.111.111.111
connect: Network is unreachable
[root@PC1 root]# ping -c 2 -b 10.0.1.255
WARNING: pinging broadcast address
PING 10.0.1.255 (10.0.1.255) 56(84) bytes of data.
64 bytes from 10.0.1.11: icmp_seq=1 ttl=64 time=0.043 ms
64 bytes from 10.0.1.13: icmp_seq=1 ttl=64 time=3.85 ms (DUP!)
64 bytes from 10.0.1.12: icmp_seq=1 ttl=64 time=4.41 ms (DUP!)
64 bytes from 10.0.1.14: icmp_seq=1 ttl=64 time=5.97 ms (DUP!)
64 bytes from 10.0.1.11: icmp_seq=2 ttl=64 time=0.027 ms
--- 10.0.1.255 ping statistics ---
2 packets transmitted, 2 received, +3 duplicates, 0% packet loss, time
1003ms
rtt min/avg/max/mdev = 0.027/2.863/5.975/2.412 ms

[root@PC1 root]# tcpdump -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol
decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
15:57:30.347242 IP 10.0.1.11 > 10.0.1.255: ICMP echo request, id
20293, seq 1, length 64
```

```
15:57:30.350971 arp who-has 10.0.1.11 tell 10.0.1.13
15:57:30.351000 arp reply 10.0.1.11 is-at 00:04:5a:7a:c8:25
15:57:30.351048 IP 10.0.1.13 > 10.0.1.11: ICMP echo reply, id 20293,
seq 1, length 64
15:57:30.351535 arp who-has 10.0.1.11 tell 10.0.1.12
15:57:30.351565 arp reply 10.0.1.11 is-at 00:04:5a:7a:c8:25
15:57:30.351611 IP 10.0.1.12 > 10.0.1.11: ICMP echo reply, id 20293,
seq 1, length 64
15:57:30.353081 arp who-has 10.0.1.11 tell 10.0.1.14
15:57:30.353121 arp reply 10.0.1.11 is-at 00:04:5a:7a:c8:25
15:57:30.353168 IP 10.0.1.14 > 10.0.1.11: ICMP echo reply, id 20293,
seq 1, length 64
15:57:31.350301 IP 10.0.1.11 > 10.0.1.255: ICMP echo request, id
20293, seq 2, length 64
15:57:31.350366 IP 10.0.1.13 > 10.0.1.11: ICMP echo reply, id 20293,
seq 2, length 64
15:57:31.350378 IP 10.0.1.14 > 10.0.1.11: ICMP echo reply, id 20293,
seq 2, length 64
15:57:31.350389 IP 10.0.1.12 > 10.0.1.11: ICMP echo reply, id 20293,
seq 2, length 64

14 packets captured
14 packets received by filter
0 packets dropped by kernel
```

- 3 PCs responded to the broadcast ping.

EXERCISE 8

Questions 1

Include the file with the captured data in your lab report. Describe the differences between the files saved by tcpdump (in Part 7) and by etherreal (in this part).

```
No. Time Source Destination Protocol Info
1 0.000000 00:04:5a:7a:c8:25 ff:ff:ff:ff:ff:ff ARP Who has 10.0.1.13?
Tell 10.0.1.11

Frame 1 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25), Dst:
ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

No. Time Source Destination Protocol Info
2 0.000074 00:04:5a:7a:c6:64 00:04:5a:7a:c8:25 ARP 10.0.1.13 is at
00:04:5a:7a:c6:64

Frame 2 (60 bytes on wire, 60 bytes captured)
```

```
Ethernet II, Src: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64), Dst:
00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25)
Address Resolution Protocol (reply)

No. Time Source Destination Protocol Info
3 0.000087 10.0.1.11 10.0.1.13 ICMP Echo (ping) request

Frame 3 (98 bytes on wire, 98 bytes captured)
Ethernet II, Src: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25), Dst:
00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)
Internet Protocol, Src: 10.0.1.11 (10.0.1.11), Dst: 10.0.1.13
(10.0.1.13)
Internet Control Message Protocol

No. Time Source Destination Protocol Info
4 0.000152 10.0.1.13 10.0.1.11 ICMP Echo (ping) reply

Frame 4 (98 bytes on wire, 98 bytes captured)
Ethernet II, Src: 00:04:5a:7a:c6:64 (00:04:5a:7a:c
No. Time Source Destination Protocol Info
5 0.999855 10.0.1.11 10.0.1.13 ICMP Echo (ping) request

Frame 5 (98 bytes on wire, 98 bytes captured)
Ethernet II, Src: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25), Dst:
00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)
Internet Protocol, Src: 10.0.1.11 (10.0.1.11), Dst: 10.0.1.13
(10.0.1.13)
Internet Control Message Protocol

No. Time Source Destination Protocol Info
6 0.999927 10.0.1.13 10.0.1.11 ICMP Echo (ping) reply

Frame 6 (98 bytes on wire, 98 bytes captured)
Ethernet II, Src: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64), Dst:
00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25)
Internet Protocol, Src: 10.0.1.13 (10.0.1.13), Dst: 10.0.1.11
(10.0.1.11)
Internet Control Message Protocol

No. Time Source Destination Protocol Info
7 4.995848 00:04:5a:7a:c6:64 00:04:5a:7a:c8:25 ARP Who has 10.0.1.11?
Tell 10.0.1.13

Frame 7 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64), Dst:
00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25)
Address Resolution Protocol (request)

No. Time Source Destination Protocol Info
```

8 4.995866 00:04:5a:7a:c8:25 00:04:5a:7a:c6:64 ARP 10.0.1.11 is at 00:04:5a:7a:c8:25

Frame 8 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25), Dst: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)
Address Resolution Protocol (reply)6:64), Dst: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25)
Internet Protocol, Src: 10.0.1.13 (10.0.1.13), Dst: 10.0.1.11 (10.0.1.11)
Internet Control Message Protocol

No. Time Source Destination Protocol Info
5 0.999855 10.0.1.11 10.0.1.13 ICMP Echo (ping) request

Frame 5 (98 bytes on wire, 98 bytes captured)
Ethernet II, Src: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25), Dst: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)
Internet Protocol, Src: 10.0.1.11 (10.0.1.11), Dst: 10.0.1.13 (10.0.1.13)
Internet Control Message Protocol

No. Time Source Destination Protocol Info
6 0.999927 10.0.1.13 10.0.1.11 ICMP Echo (ping) reply

Frame 6 (98 bytes on wire, 98 bytes captured)
Ethernet II, Src: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64), Dst: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25)
Internet Protocol, Src: 10.0.1.13 (10.0.1.13), Dst: 10.0.1.11 (10.0.1.11)
Internet Control Message Protocol

No. Time Source Destination Protocol Info
7 4.995848 00:04:5a:7a:c6:64 00:04:5a:7a:c8:25 ARP Who has 10.0.1.11? Tell 10.0.1.13

Frame 7 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64), Dst: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25)
Address Resolution Protocol (request)

No. Time Source Destination Protocol Info
8 4.995866 00:04:5a:7a:c8:25 00:04:5a:7a:c6:64 ARP 10.0.1.11 is at 00:04:5a:7a:c8:25

Frame 8 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25), Dst: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)
Address Resolution Protocol (reply)

- The operation results were the same. However, the Wireshark output contained the data in much more detail. The Wireshark output provided the information regarding the content of the datagram

Lab 2

EXERCISE 1

Include the saved data in your lab report.

```
16:17:49.417709 arp who-has 10.0.1.12 tell 10.0.1.11
16:17:49.417789 arp reply 10.0.1.12 is-at 00:04:5a:7a:c8:ca
16:17:49.417802 IP 10.0.1.11 > 10.0.1.12: ICMP echo request, id 8520,
seq 1, length 64
16:17:49.417870 IP 10.0.1.12 > 10.0.1.11: ICMP echo reply, id 8520,
seq 1, length 64
16:17:50.413581 IP 10.0.1.11 > 10.0.1.12: ICMP echo request, id 8520,
seq 2, length 64
16:17:50.413654 IP 10.0.1.12 > 10.0.1.11: ICMP echo reply, id 8520,
seq 2, length 64
16:17:51.413416 IP 10.0.1.11 > 10.0.1.12: ICMP echo request, id 8520,
seq 3, length 64
16:17:51.413488 IP 10.0.1.12 > 10.0.1.11: ICMP echo reply, id 8520,
seq 3, length 64
16:17:52.413256 IP 10.0.1.11 > 10.0.1.12: ICMP echo request, id 8520,
seq 4, length 64
16:17:52.413328 IP 10.0.1.12 > 10.0.1.11: ICMP echo reply, id 8520,
seq 4, length 64
16:17:53.413132 IP 10.0.1.11 > 10.0.1.12: ICMP echo request, id 8520,
seq 5, length 64
16:17:53.413203 IP 10.0.1.12 > 10.0.1.11: ICMP echo reply, id 8520,
seq 5, length 64
16:17:54.420025 arp who-has 10.0.1.11 tell 10.0.1.12
16:17:54.420048 arp reply 10.0.1.11 is-at 00:04:5a:7a:c8:25

16:25:33.940252 IP 10.0.1.11 > 10.0.1.12: ICMP echo request, id 14152,
seq 1, length 64
16:25:33.940343 IP 10.0.1.12 > 10.0.1.11: ICMP echo reply, id 14152,
seq 1, length 64
16:25:34.939245 IP 10.0.1.11 > 10.0.1.12: ICMP echo request, id 14152,
seq 2, length 64
16:25:34.939319 IP 10.0.1.12 > 10.0.1.11: ICMP echo reply, id 14152,
seq 2, length 64
16:25:35.938462 IP 10.0.1.11 > 10.0.1.12: ICMP echo request, id 14152,
seq 3, length 64
```

```
16:25:35.938538 IP 10.0.1.12 > 10.0.1.11: ICMP echo reply, id 14152,
seq 3, length 64
16:25:36.938301 IP 10.0.1.11 > 10.0.1.12: ICMP echo request, id 14152,
seq 4, length 64
16:25:36.938373 IP 10.0.1.12 > 10.0.1.11: ICMP echo reply, id 14152,
seq 4, length 64
16:25:37.938144 IP 10.0.1.11 > 10.0.1.12: ICMP echo request, id 14152,
seq 5, length 64
16:25:37.938218 IP 10.0.1.12 > 10.0.1.11: ICMP echo reply, id 14152,
seq 5, length 64
```

EXERCISE 3A

Question 1

What is the destination MAC address of an ARP Request packet?

- The destination MAC address of an ARP Request packet is the MAC address of the destination IP address

Question 2

What are the different values of the Type field in the Ethernet headers that you observed?

- The type fields are IP for ICMP packets and ARP.

Question 3

Use the captured data to discuss the process in which ARP acquires the MAC address for IP address 10.0.1.12.

- The first line IP 10.0.1.11 (PC1) sends out an ARP request, asking the MAC address of IP 10.0.1.12 to be sent back to PC1. Then IP 10.0.1.12 (PC2) replies with its own MAC address to PC1. After that PC1 will cache the MAC address of PC2 for further use.

EXERCISE 3B

Question 1

Include the completed Table2.2 in you lab report.

Linux PC	IP Address of Ethernet Interface *eth0*	MAC Address of Ethernet Interface eth0
PC1	10.0.1.11/24	00:04:5a:7a:c8:ca
PC2	10.0.1.12/24	00:04:5a:7a:c6:64

PC3	10.0.1.13/24	00:04:5a:7a:c8:25
PC4	10.0.1.14/24	00:04:5a:7b:3d:83

EXERCISE 3C

Question 1

Using the saved output, describe the time interval between each ARP Request issued by PC1. Describe the method used by ARP to determine the time between retransmissions of an unsuccessful ARP request. Include relevant data to support your answer.

No.	Time
1	0.000000
2	0.999795
3	1.999633
4	5.935041
5	7.934566

- The time interval between first 3 ARP requests was 1 seconds. After 3 failed attempts, the time interval was adjusted to 4 seconds.

Question 2

Why are ARP request packets not transmitted like IP packets? Explain your answer.

- IP packets are encapsulated with specific destinations, but ARP request packets are not necessarily sent to specific MAC address. And ARP request packets are not encapsulated.

EXERCISE 6

Question 1

Explain why the Telnet session was established to one of the hosts with the duplicate address and not the other. Explain why the Telnet session was established at all and did not result in an error message. Use the ARP cache and the captured packets to support your explanation.

- The first responder to the ARP request can establish telnet session with the ARP request sender. PC3 will update its ARP cache. Any responder after the first one will be rejected since PC3 has already resolved the MAC address. In our experiment, PC3 picked up MAC address 00:04:5a:7b:3d:83 as 10.0.1.11 and ignored MAC address 00:04:5a:7a:c8:25.
- Captured data:

```
No.     Time        Source                Destination
Protocol Info
1 0.000000    00:04:5a:7a:c6:64     ff:ff:ff:ff:ff:ff     ARP      Who
has 10.0.1.11?  Tell 10.0.1.13

Frame 1 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64), Dst:
ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

No.     Time        Source                Destination
Protocol Info
     2 0.000039    00:04:5a:7b:3d:83     00:04:5a:7a:c6:64     ARP
10.0.1.11 is at 00:04:5a:7b:3d:83

Frame 2 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: 00:04:5a:7b:3d:83 (00:04:5a:7b:3d:83), Dst:
00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)
Address Resolution Protocol (reply)

No.     Time        Source                Destination
Protocol Info
     3 0.000050    10.0.1.13             10.0.1.11             TCP
53369 > 23 [SYN] Seq=0 Len=0 MSS=1460 TSV=1282731 TSER=0

Frame 3 (70 bytes on wire, 70 bytes captured)
Ethernet II, Src: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64), Dst:
00:04:5a:7b:3d:83 (00:04:5a:7b:3d:83)
Internet Protocol, Src: 10.0.1.13 (10.0.1.13), Dst: 10.0.1.11
(10.0.1.11)
Transmission Control Protocol, Src Port: 53369 (53369), Dst Port: 23
(23), Seq: 0, Len: 0

No.     Time        Source                Destination
Protocol Info
     4 0.000063    00:04:5a:7a:c8:25     00:04:5a:7a:c6:64     ARP
10.0.1.11 is at 00:04:5a:7a:c8:25

Frame 4 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25), Dst:
00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)
Address Resolution Protocol (reply)

No.     Time        Source                Destination
Protocol Info
     5 0.000120    10.0.1.11             10.0.1.13             TCP
23 > 53369 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 TSV=1237056
TSER=1282731
```

EXERCISE 7

Question 1

Use your output data and ping results to explain what happened in each of the ping commands. Which ping operations were successful and which were unsuccessful? Why?

· PC1% ping -c 1 10.0.1.120

This ping operation was successful. PC1 (10.0.1.100/24) and PC3 (10.0.1.120/24) are on the same network.

· PC1% ping -c 1 10.0.1.101

This ping operation was successful. The IP addresses PC1 (10.0.1.100/24) and PC2 (10.0.1.101/28) match on the first 24 bits. As a result, PC2 is on the same network from PC1's point of view. In addition, the IP addresses match on the first 28 bits, indicating PC1 is on the same network from PC2's point of view. As a result, PC1 and PC2 were able to communicate with each other.

· PC1% ping -c 1 10.0.1.121

This ping operation was able to successfully transmit packets from PC1 to PC4. However, no response packet was received from PC4 to PC1. The IP addresses PC1 (10.0.1.100/24) and PC4 (10.0.1.121/28) match on the first 24 bits. As a result, PC4 is on the same network from PC1's point of view. Thus the packets were successfully transmitted to PC4. However, the IP addresses does not match for the first 28 bits, indicating PC1 is on not the same network from PC4's point of view. Thus no no response packet was delivered.

· PC4% ping -c 1 10.0.1.100

This ping operation failed. The IP addresses PC4 (10.0.1.121/28) and PC1 (10.0.1.100/24) does not match for the first 28 bits. As a result, PC4 was not able to see PC1 on its network.

· PC2% ping -c 1 10.0.1.121

This ping operation failed. The IP addresses PC4 (10.0.1.121/28) and PC2 (10.0.1.101/28) does not match for the first 28 bits. As a result, PC2 was not able to see PC4 on its network.

· PC2% ping -c 1 10.0.1.120

This ping operation failed. The IP addresses PC2 (10.0.1.101/28) and PC3 (10.0.1.120/24) does not match for the first 28 bits. As a result, PC2 was not able to see PC3 on its network.

EXERCISE 8

Question 1

Explain why a static mapping of names and IP addresses is impractical when the number of hosts is large.

· Static mapping can only be done manually, it is too time consuming to map IP and names statically for a large number of hosts.

Question 2

What will be the result of the host name resolution when multiple IP addresses are associated with the same host name in the /etc/hosts file?

- Only the first IP address in /etc/hosts will respond.

EXERCISE 9A

Question 1

Using the saved output, identify the port numbers of the FTP client and the FTP server.

- Answer: The port number for FTP client is Port 21. The port number for the FTP server is Port 41858.
- Captured data

```
No.     Time        Source                Destination           Protocol
Info
     1 0.000000    10.0.1.11             10.0.1.12             TCP
41858 > 21 [SYN] Seq=0 Len=0 MSS=1460 TSV=1938456 TSER=0

Frame 1 (70 bytes on wire, 70 bytes captured)
   Arrival Time: Sep 26, 2016 17:22:07.102649000
   [Time delta from previous packet: 0.000000000 seconds]
   [Time since reference or first frame: 0.000000000 seconds]
   Frame Number: 1
   Packet Length: 70 bytes
   Capture Length: 70 bytes
   [Frame is marked: False]
   [Protocols in frame: eth:ip:tcp]
   [Coloring Rule Name: TCP SYN/FIN]
   [Coloring Rule String: tcp.flags & 0x02 || tcp.flags.fin == 1]
Ethernet II, Src: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25), Dst:
00:04:5a:7a:c8:ca (00:04:5a:7a:c8:ca)
   Destination: 00:04:5a:7a:c8:ca (00:04:5a:7a:c8:ca)
   Source: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25)
   Type: IP (0x0800)
Internet Protocol, Src: 10.0.1.11 (10.0.1.11), Dst: 10.0.1.12 (10.0.1.12)
   Version: 4
   Header length: 20 bytes
   Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
   Total Length: 56
   Identification: 0xb0ac (45228)
   Flags: 0x04 (Don't Fragment)
   Fragment offset: 0
   Time to live: 64
   Protocol: TCP (0x06)
   Header checksum: 0x73fd [correct]
   Source: 10.0.1.11 (10.0.1.11)
   Destination: 10.0.1.12 (10.0.1.12)
Transmission Control Protocol, Src Port: 41858 (41858), Dst Port: 21 (21),
Seq: 0, Len: 0
```

Question 2

Identify the login name and the password, shown in plain text in the payload of the packets that you captured.

- Username: root; Password: rootroot

EXERCISE 9B

Question 1

Does the Telnet have the same security flaws as FTP? Support your answer using the saved output.

- Yes, the Telnet has the same security flaws as FTP. Instead of sending the unencrypted username and passwords in 2 packets consecutively, FTP sends the unencrypted username and password character by character in many packets. By tracking these consecutive packets, one can still easily obtain the username and password as they are not encrypted.

EXERCISE 9C

Question 1

Attach the saved output to your report. Explain why three packets are sent in a Telnet session for each character typed on the terminal.

```
No.     Time         Source            Destination           Protocol
Info
   1 0.000000  10.0.1.11         10.0.1.12         TELNET   Telnet Data
...

Frame 1 (67 bytes on wire, 67 bytes captured)
   Arrival Time: Sep 26, 2016 17:39:30.179113000
   [Time delta from previous packet: 0.000000000 seconds]
   [Time since reference or first frame: 0.000000000 seconds]
   Frame Number: 1
   Packet Length: 67 bytes
   Capture Length: 67 bytes
   [Frame is marked: False]
   [Protocols in frame: eth:ip:tcp:telnet]
Ethernet II, Src: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25), Dst:
00:04:5a:7a:c8:ca (00:04:5a:7a:c8:ca)
   Destination: 00:04:5a:7a:c8:ca (00:04:5a:7a:c8:ca)
         Source: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25)
         Address: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25)
   Type: IP (0x0800)
Internet Protocol, Src: 10.0.1.11 (10.0.1.11), Dst: 10.0.1.12 (10.0.1.12)
   Version: 4
   Header length: 20 bytes
```

```
    Differentiated Services Field: 0x10 (DSCP 0x04: Unknown DSCP; ECN:
0x00)
   Total Length: 53
    Identification: 0xef87 (61319)
   Flags: 0x04 (Don't Fragment)
   Fragment offset: 0
   Time to live: 64
   Protocol: TCP (0x06)
   Header checksum: 0x3515 [correct]
   Source: 10.0.1.11 (10.0.1.11)
   Destination: 10.0.1.12 (10.0.1.12)
Transmission Control Protocol, Src Port: 51009 (51009), Dst Port: 23 (23),
Seq: 0, Ack: 0, Len: 1
Telnet
   Data: j

No.     Time         Source             Destination       Protocol Info
   2 0.000081  10.0.1.12         10.0.1.11         TELNET   Telnet Data
...

Frame 2 (155 bytes on wire, 155 bytes captured)
   Arrival Time: Sep 26, 2016 17:39:30.179194000
   [Time delta from previous packet: 0.000081000 seconds]
   [Time since reference or first frame: 0.000081000 seconds]
   Frame Number: 2
   Packet Length: 155 bytes
   Capture Length: 155 bytes
   [Frame is marked: False]
   [Protocols in frame: eth:ip:tcp:telnet]
Ethernet II, Src: 00:04:5a:7a:c8:ca (00:04:5a:7a:c8:ca), Dst:
00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25)
   Destination: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25)
         Address: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25)
   Source: 00:04:5a:7a:c8:ca (00:04:5a:7a:c8:ca)
         Address: 00:04:5a:7a:c8:ca (00:04:5a:7a:c8:ca)
   Type: IP (0x0800)
Internet Protocol, Src: 10.0.1.12 (10.0.1.12), Dst: 10.0.1.11 (10.0.1.11)
   Version: 4
   Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
   Total Length: 141
    Identification: 0x7ce4 (31972)
   Flags: 0x04 (Don't Fragment)
   Fragment offset: 0
   Time to live: 64
   Protocol: TCP (0x06)
   Header checksum: 0xa770 [correct]
   Source: 10.0.1.12 (10.0.1.12)
   Destination: 10.0.1.11 (10.0.1.11)
Transmission Control Protocol, Src Port: 23 (23), Dst Port: 51009 (51009),
Seq: 0, Ack: 1, Len: 89
```

```
Telnet
   Data: \r\000
   Data: \033[01;31m[root@PC2 ~]#\033[00m j\r\000
   Data: \033[01;31m[root@PC2 ~]#\033[00m \r\000
   Data: \033[01;31m[root@PC2 ~]#\033[00m j

No.     Time         Source            Destination       Protocol Info
   3 0.000085  10.0.1.11         10.0.1.12         TCP   51009 > 23
[ACK] Seq=1 Ack=89 Win=21440 Len=0 TSV=2199259 TSER=2191941

Frame 3 (66 bytes on wire, 66 bytes captured)
   Arrival Time: Sep 26, 2016 17:39:30.179198000
   [Time delta from previous packet: 0.000085000 seconds]
   [Time since reference or first frame: 0.000085000 seconds]
   Frame Number: 3
   Packet Length: 66 bytes
   Capture Length: 66 bytes
   [Frame is marked: False]
   [Protocols in frame: eth:ip:tcp]
   [Coloring Rule Name: TCP]
   [Coloring Rule String: tcp]
Ethernet II, Src: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25), Dst:
00:04:5a:7a:c8:ca (00:04:5a:7a:c8:ca)
   Destination: 00:04:5a:7a:c8:ca (00:04:5a:7a:c8:ca)
   Source: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25)
   Type: IP (0x0800)
Internet Protocol, Src: 10.0.1.11 (10.0.1.11), Dst: 10.0.1.12 (10.0.1.12)
   Version: 4
   Header length: 20 bytes
    Differentiated Services Field: 0x10 (DSCP 0x04: Unknown DSCP; ECN:
0x00)
   Total Length: 52
    Identification: 0xef88 (61320)
   Flags: 0x04 (Don't Fragment)
   Fragment offset: 0
   Time to live: 64
   Protocol: TCP (0x06)
   Header checksum: 0x3515 [correct]
   Source: 10.0.1.11 (10.0.1.11)
   Destination: 10.0.1.12 (10.0.1.12)
Transmission Control Protocol, Src Port: 51009 (51009), Dst Port: 23 (23),
Seq: 1, Ack: 89, Len: 0
```

- The first packet was sent from client to server, delivering the single character that was typed. The second packet was sent from server to client, containing the information to be displayed in the client console. The third packet is the ACK packet sent from client to server.