Cover Page

Student name: Wei Lin (999595193)

Student name: Shenglin Meng (1000695517)

Lab1 Report

Exercise 5

1. Which files must be edited to change the name of a Linux PC, e.g., from `PC1' to `machine1'?

Ans:

2. Edit the file /etc/sysconfig/network", change "HOSTNAME=PC1" to "HOSTNAME=machine1"

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

Ans:

In the file "/etc/sysctl.conf" that has "net.ipv4.ip_forward = $boolean".

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

Ans:

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

1. Include the output you saved in this exercise.

Ans:

6.1

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=4.60 ms

64 bytes from 10.0.1.12: icmp_seq=2 ttl=64 time=0.101 ms

64 bytes from 10.0.1.12: icmp_seq=3 ttl=64 time=0.103 ms

64 bytes from 10.0.1.12: icmp_seq=4 ttl=64 time=0.098 ms

64 bytes from 10.0.1.12: icmp_seq=5 ttl=64 time=0.105 ms

--- 10.0.1.12 ping statistics ---

5 packets transmitted, 5 received, 0% packet loss, time 4000ms

rtt min/avg/max/mdev = 0.098/1.002/4.606/1.802 ms

6.2

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=0.112 ms

64 bytes from 10.0.1.11: icmp_seq=2 ttl=64 time=0.099 ms

64 bytes from 10.0.1.11: icmp_seq=3 ttl=64 time=0.101 ms

64 bytes from 10.0.1.11: icmp_seq=4 ttl=64 time=0.101 ms

64 bytes from 10.0.1.11: icmp_seq=5 ttl=64 time=0.108 ms

--- 10.0.1.11 ping statistics ---

5 packets transmitted, 5 received, 0% packet loss, time 3997ms

rtt min/avg/max/mdev = 0.099/0.104/0.112/0.008 ms

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=0.033 ms

64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.025 ms

64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.025 ms

64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.021 ms

64 bytes from 127.0.0.1: icmp_seq=5 ttl=64 time=0.024 ms

--- 127.0.0.1 ping statistics ---

5 packets transmitted, 5 received, 0% packet loss, time 3998ms

rtt min/avg/max/mdev = 0.021/0.025/0.033/0.006 ms

2. Explain the difference between pinging the local Ethernet interface and the loopback interface. Specifically, on PC1, what is the difference between typing "ping 10.0.1.11" and "ping 127.0.0.1". (This is a conceptual question on the role of the loopback interface. The response to the ping command does not provide you with the answer to this question.)

Ans:

127.0.0.1 is a local loopback address, an virtual address, that the host uses to communicate with itself while 10.0.1.11 is an ip address assigned to the physical ethernet interface. Therefore, if the ethernet interface is not connected, ping 10.0.1.11 will fail while ping 127.0.0.1 will succeed.

3. (To be completed after the lab). Find a host connected to the Internet. Send ping messages to a number of web servers on the Internet and collect statistics on the maximum round-trip delay of the ICMP Echo Request/Echo Reply. Try to find a host with a very long round-trip time. To avoid overloading the destination, do not send more than 3 ping packets to any destination machine. Save the output data and include it in your lab report.

Ans:

Pinging www.mingwangdao.com [211.149.206.190] with 32 bytes of data:

Reply from 211.149.206.190: bytes=32 time=266ms TTL=46

Reply from 211.149.206.190: bytes=32 time=265ms TTL=46

Reply from 211.149.206.190: bytes=32 time=265ms TTL=46

Ping statistics for 211.149.206.190:

Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 265ms, Maximum = 266ms, Average = 265ms

Exercise 7

7-a.

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

Ans:

04:25:00.330294 IP 10.0.1.11 > 10.0.1.12: ICMP echo request, id 54368, seq 1, length 64

04:25:00.336191 arp who-has 10.0.1.11 tell 10.0.1.12

04:25:00.336213 arp reply 10.0.1.11 is-at 00:04:5a:7a:c8:25

04:25:00.336279 IP 10.0.1.12 > 10.0.1.11: ICMP echo reply, id 54368, seq 1, length 64

Meaning:

Each line standards for a packet contains the ip address: 10.0.1.12. Each line starts with the time that packet is observed followed by the protocol type and information inside the packet.

The 1st line means host 10.0.1.11 sends an ICMP request to host 10.0.1.12. It also prints out the id, sequence number and length of the packet.

The 2nd line means host 10.0.1.11 sends an ARP request for the MAC address of host 10.0.1.12.

The 3rd line means host 10.0.1.11 gets an ARP reply that containing the host 10.0.1.12's MAC address: 00:04:5a:7a:c8:25.

The 4th line means host 10.0.1.11 receives an ICMP reply from host 10.0.1.12. It also prints out the id, sequence number and length of the packet.

7-b.

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

Ans:

When ping -c 1 111.111.111.111, the output is:

connect: Network is unreachable

When ping -c 2 -b 10.0.1.255, the output is:

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=0.041 ms

64 bytes from 10.0.1.11: icmp_seq=2 ttl=64 time=0.029 ms

--- 10.0.1.255 ping statistics ---

2 packets transmitted, 2 received, 0% packet loss, time 1003ms

rtt min/avg/max/mdev = 0.029/0.035/0.041/0.006 ms

tcpdump output is:

04:30:04.807672 IP 10.0.1.11 > 10.0.1.255: ICMP echo request, id 7777, seq 1, length 64

04:30:04.807778 IP 10.0.1.12 > 10.0.1.11: ICMP echo reply, id 7777, seq 1, length 64

04:30:04.810936 arp who-has 10.0.1.11 tell 10.0.1.13

04:30:04.810964 arp reply 10.0.1.11 is-at 00:04:5a:7a:c8:25

04:30:04.811030 IP 10.0.1.13 > 10.0.1.11: ICMP echo reply, id 7777, seq 1, length 64

04:30:04.814185 arp who-has 10.0.1.11 tell 10.0.1.14

04:30:04.814211 arp reply 10.0.1.11 is-at 00:04:5a:7a:c8:25

04:30:04.814276 IP 10.0.1.14 > 10.0.1.11: ICMP echo reply, id 7777, seq 1, length 64

04:30:05.807187 IP 10.0.1.11 > 10.0.1.255: ICMP echo request, id 7777, seq 2, length 64

04:30:05.807274 IP 10.0.1.13 > 10.0.1.11: ICMP echo reply, id 7777, seq 2, length 64

04:30:05.807287 IP 10.0.1.12 > 10.0.1.11: ICMP echo reply, id 7777, seq 2, length 64

04:30:05.807291 IP 10.0.1.14 > 10.0.1.11: ICMP echo reply, id 7777, seq 2, length 64

04:30:09.809004 arp who-has 10.0.1.11 tell 10.0.1.12

04:30:09.809034 arp reply 10.0.1.11 is-at 00:04:5a:7a:c8:25

Interpretation:

ping output:

The 111.111.111.111 is not in the network, so PC1 cannot send ICMP message to the IP address and prompted the warning: "Network is unreachable".

The 10.0.1.255 is the broadcast address of PC1, so PC1 sends ICMP request to all the PCs in the network, and as a result, PC1 receives 4 ICMP reply from all the PCs in the network, including PC1 (itself), PC2, PC3 and PC4.

tcpdmup output: each short paragraph below explains meaning of each line in above tcpdump output

host 10.0.1.11 sends an ICMP request to broadcast address 10.0.1.255. Packet id is 7777, sequence number is 1 and length is 64 bytes.

host 10.0.1.11 receives an ICMP reply from host 10.0.1.12. Packet id is 7777, sequence number is 1 and length is 64 bytes.

host 10.0.1.11 receives ARP request for the MAC address of host 10.0.1.11 from host 10.0.1.13.

host 10.0.1.11 sends an ARP reply that containing the host 10.0.1.11’s MAC address: 00:04:5a:7a:c8:25.

host 10.0.1.11 receives an ICMP reply from host 10.0.1.13. Packet id is 7777, sequence number is 1 and length is 64 bytes.

host 10.0.1.11 receives an ARP request for the MAC address of host 10.0.1.11 from host 10.0.1.14.

host 10.0.1.11 sends an ARP reply that containing the host 10.0.1.11's MAC address: 00:04:5a:7a:c8:25.

host 10.0.1.11 receives an ICMP reply from host 10.0.1.14. Packet id is 7777, sequence number is 1 and length is 64 bytes

host 10.0.1.11 sends an 2nd ICMP request to broadcast address 10.0.1.255. Packet id is 7777, sequence number is 2 and length is 64 bytes.

host 10.0.1.11 receives an ICMP reply from host 10.0.1.13. Packet id is 7777, sequence number is 2 and length is 64 bytes.

host 10.0.1.11 receives an ICMP reply from host 10.0.1.12. Packet id is 7777, sequence number is 2 and length is 64 bytes.

host 10.0.1.11 receives an ICMP reply from host 10.0.1.14. Packet id is 7777, sequence number is 2 and length is 64 bytes.

All 4 PCs response to the broadcast ping, which is 10.0.1.11, 10.0.1.12, 10.0.1.13 and 10.0.1.14, because they are all in same network.

Exercise 8

Include the file with the captured data in your lab report. Save the details of the captured traffic, using the "Print detail" option in the Print window . Describe the differences between the files saved by tcpdump (in Part 7) and by wireshark (in this part).

Ans:

Differences:

Wireshark contains much more information about the network traffic while tcpdump only provides simple description about the packet content.

In Wireshark, all the header is shown, such as IP header, ARP header and Ethernet header, etc. In addition, information inside the header is also exhibited in Wireshark.

For example, we can see the version, header length, differentiated Services Field, Total Length, Identification, Flags, Fragment offset, Time to live, Protocol, Header checksum, Source and Destination in the IP header; the MAC address of source and destination in the Ethernet header.

Below is the output:

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)

Arrival Time: Jun 7, 2007 04:34:46.936353000

[Time delta from previous packet: 0.000000000 seconds]

[Time since reference or first frame: 0.000000000 seconds]

Frame Number: 1

Packet Length: 42 bytes

Capture Length: 42 bytes

[Frame is marked: False]

[Protocols in frame: eth:arp]

[Coloring Rule Name: ARP]

[Coloring Rule String: arp]

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)

Destination: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)

Address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)

....1 .... = IG bit: Group address (multicast/broadcast)

.... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)

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)

....0 .... = IG bit: Individual address (unicast)

.... ..0. .... = LG bit: Globally unique address (factory default)

Type: ARP (0x0806)

Address Resolution Protocol (request)

Hardware type: Ethernet (0x0001)

Protocol type: IP (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: request (0x0001)

Sender MAC address: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25)

Sender IP address: 10.0.1.11 (10.0.1.11)

Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)

Target IP address: 10.0.1.13 (10.0.1.13)

No. Time Source Destination Protocol Info

2 0.000082 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)

Arrival Time: Jun 7, 2007 04:34:46.936435000

[Time delta from previous packet: 0.000082000 seconds]

[Time since reference or first frame: 0.000082000 seconds]

Frame Number: 2

Packet Length: 60 bytes

Capture Length: 60 bytes

[Frame is marked: False]

[Protocols in frame: eth:arp]

[Coloring Rule Name: ARP]

[Coloring Rule String: arp]

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)

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)

....0 .... = IG bit: Individual address (unicast)

.... ..0. .... = LG bit: Globally unique address (factory default)

Source: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)

Address: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)

....0 .... = IG bit: Individual address (unicast)

.... ..0. .... = LG bit: Globally unique address (factory default)

Type: ARP (0x0806)

Trailer: 000000000000000000000000000000000000

Address Resolution Protocol (reply)

Hardware type: Ethernet (0x0001)

Protocol type: IP (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: reply (0x0002)

Sender MAC address: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)

Sender IP address: 10.0.1.13 (10.0.1.13)

Target MAC address: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25)

Target IP address: 10.0.1.11 (10.0.1.11)

No.	Time	Source	Destination	Protocol	Info
3	0.000095	10.0.1.11	10.0.1.13	ICMP	Echo (ping) request

Frame 3 (98 bytes on wire, 98 bytes captured)

Arrival Time: Jun 7, 2007 04:34:46.936448000

[Time delta from previous packet: 0.000013000 seconds]

[Time since reference or first frame: 0.000095000 seconds]

Frame Number: 3

Packet Length: 98 bytes

Capture Length: 98 bytes

[Frame is marked: False]

[Protocols in frame: eth:ip:icmp:data]

[Coloring Rule Name: ICMP]

[Coloring Rule String: icmp]

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)

Destination: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)

Address: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)

....0 .... = IG bit: Individual address (unicast)

.... ..0. .... = LG bit: Globally unique address (factory default)

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)

....0 .... = IG bit: Individual address (unicast)

.... ..0. .... = LG bit: Globally unique address (factory default)

Type: IP (0x0800)

Internet Protocol, Src: 10.0.1.11 (10.0.1.11), Dst: 10.0.1.13 (10.0.1.13)

Version: 4

```
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 84
    Identification: 0x0000 (0)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (0x01)
    Header checksum: 0x2492 [correct]
        [Good: True]
        [Bad : False]
    Source: 10.0.1.11 (10.0.1.11)
    Destination: 10.0.1.13 (10.0.1.13)
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xe640 [correct]
    Identifier: 0x2461
    Sequence number: 1 (0x0001)
    Data (56 bytes)

0000  36 d1 67 46 56 42 0e 00 08 09 0a 0b 0c 0d 0e 0f   6.gFVB.........
0010  10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f   ................
0020  20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f    !"#$%&'()*+,-./
0030  30 31 32 33 34 35 36 37                          01234567
```

No.	Time	Source	Destination	Protocol	Info
4	0.000176	10.0.1.13	10.0.1.11	ICMP	Echo (ping) reply

Frame 4 (98 bytes on wire, 98 bytes captured)

Arrival Time: Jun 7, 2007 04:34:46.936529000

[Time delta from previous packet: 0.000081000 seconds]

[Time since reference or first frame: 0.000176000 seconds]

Frame Number: 4

Packet Length: 98 bytes

Capture Length: 98 bytes

[Frame is marked: False]

[Protocols in frame: eth:ip:icmp:data]

[Coloring Rule Name: ICMP]

[Coloring Rule String: icmp]

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)

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)

....0 .... = IG bit: Individual address (unicast)

.... ..0. .... = LG bit: Globally unique address (factory default)

Source: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)

Address: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)

....0 .... = IG bit: Individual address (unicast)

.... ..0. .... = LG bit: Globally unique address (factory default)

Type: IP (0x0800)

Internet Protocol, Src: 10.0.1.13 (10.0.1.13), Dst: 10.0.1.11 (10.0.1.11)

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)

0000 00.. = Differentiated Services Codepoint: Default (0x00)

.... ..0. = ECN-Capable Transport (ECT): 0

```
        .... ...0 = ECN-CE: 0
    Total Length: 84
    Identification: 0x1a4a (6730)
    Flags: 0x00
        0... = Reserved bit: Not set
        .0.. = Don't fragment: Not set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (0x01)
    Header checksum: 0x4a48 [correct]
        [Good: True]
        [Bad : False]
    Source: 10.0.1.13 (10.0.1.13)
    Destination: 10.0.1.11 (10.0.1.11)
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xee40 [correct]
    Identifier: 0x2461
    Sequence number: 1 (0x0001)
    Data (56 bytes)

0000  36 d1 67 46 56 42 0e 00 08 09 0a 0b 0c 0d 0e 0f   6.gFVB.....
0010  10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f   .....
0020  20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f    !"#$%&'()*+,-./
0030  30 31 32 33 34 35 36 37                          01234567

No.     Time        Source              Destination         Protocol Info
      5 0.997150    10.0.1.11           10.0.1.13           ICMP     Echo (ping) request
```

Frame 5 (98 bytes on wire, 98 bytes captured)

Arrival Time: Jun 7, 2007 04:34:47.933503000

[Time delta from previous packet: 0.996974000 seconds]

[Time since reference or first frame: 0.997150000 seconds]

Frame Number: 5

Packet Length: 98 bytes

Capture Length: 98 bytes

[Frame is marked: False]

[Protocols in frame: eth:ip:icmp:data]

[Coloring Rule Name: ICMP]

[Coloring Rule String: icmp]

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)

Destination: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)

Address: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)

....0 .... = IG bit: Individual address (unicast)

.... ..0. .... = LG bit: Globally unique address (factory default)

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)

....0 .... = IG bit: Individual address (unicast)

.... ..0. .... = LG bit: Globally unique address (factory default)

Type: IP (0x0800)

Internet Protocol, Src: 10.0.1.11 (10.0.1.11), Dst: 10.0.1.13 (10.0.1.13)

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)

0000 00.. = Differentiated Services Codepoint: Default (0x00)

.... ..0. = ECN-Capable Transport (ECT): 0

....0 = ECN-CE: 0

Total Length: 84

Identification: 0x0000 (0)

Flags: 0x04 (Don't Fragment)

0... = Reserved bit: Not set

.1.. = Don't fragment: Set

..0. = More fragments: Not set

Fragment offset: 0

Time to live: 64

Protocol: ICMP (0x01)

Header checksum: 0x2492 [correct]

[Good: True]

[Bad : False]

Source: 10.0.1.11 (10.0.1.11)

Destination: 10.0.1.13 (10.0.1.13)

Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0

Checksum: 0xcb43 [correct]

Identifier: 0x2461

Sequence number: 2 (0x0002)

Data (56 bytes)

```
0000  37 d1 67 46 70 3e 0e 00 08 09 0a 0b 0c 0d 0e 0f   7.gFp>.....
0010  10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f   .....
0020  20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f    !"#$%&'()*+,-./
0030  30 31 32 33 34 35 36 37                          01234567
```

No.	Time	Source	Destination	Protocol	Info
6	0.997235	10.0.1.13	10.0.1.11	ICMP	Echo (ping) reply

Frame 6 (98 bytes on wire, 98 bytes captured)

Arrival Time: Jun 7, 2007 04:34:47.933588000

[Time delta from previous packet: 0.000085000 seconds]

[Time since reference or first frame: 0.997235000 seconds]

Frame Number: 6

Packet Length: 98 bytes

Capture Length: 98 bytes

[Frame is marked: False]

[Protocols in frame: eth:ip:icmp:data]

[Coloring Rule Name: ICMP]

[Coloring Rule String: icmp]

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)

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)

....0 .... = IG bit: Individual address (unicast)

.... ..0. .... = LG bit: Globally unique address (factory default)

Source: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)

Address: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)

....0 .... = IG bit: Individual address (unicast)

.... ..0. .... = LG bit: Globally unique address (factory default)

Type: IP (0x0800)

Internet Protocol, Src: 10.0.1.13 (10.0.1.13), Dst: 10.0.1.11 (10.0.1.11)

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)

0000 00.. = Differentiated Services Codepoint: Default (0x00)

.... ..0. = ECN-Capable Transport (ECT): 0

....0 = ECN-CE: 0

Total Length: 84

Identification: 0x1a4b (6731)

Flags: 0x00

0... = Reserved bit: Not set

.0.. = Don't fragment: Not set

..0. = More fragments: Not set

Fragment offset: 0

Time to live: 64

Protocol: ICMP (0x01)

Header checksum: 0x4a47 [correct]

[Good: True]

[Bad : False]

Source: 10.0.1.13 (10.0.1.13)

Destination: 10.0.1.11 (10.0.1.11)

Internet Control Message Protocol

Type: 0 (Echo (ping) reply)

Code: 0

Checksum: 0xd343 [correct]

Identifier: 0x2461

Sequence number: 2 (0x0002)

Data (56 bytes)

0000 37 d1 67 46 70 3e 0e 00 08 09 0a 0b 0c 0d 0e 0f 7.gFp>.....

0010 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f .....

0020 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f !"#$%&'()*+,-./

0030 30 31 32 33 34 35 36 37 01234567

No. Time Source Destination Protocol Info

7 5.000016 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)

Arrival Time: Jun 7, 2007 04:34:51.936369000

[Time delta from previous packet: 4.002781000 seconds]

[Time since reference or first frame: 5.000016000 seconds]

Frame Number: 7

Packet Length: 60 bytes

Capture Length: 60 bytes

[Frame is marked: False]

[Protocols in frame: eth:arp]

[Coloring Rule Name: ARP]

[Coloring Rule String: arp]

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)

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)

....0 .... = IG bit: Individual address (unicast)

.... ..0. .... = LG bit: Globally unique address (factory default)

Source: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)

Address: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)

....0 .... = IG bit: Individual address (unicast)

.... ..0. .... = LG bit: Globally unique address (factory default)

Type: ARP (0x0806)

Trailer: 000000000000000000000000000000000000

Address Resolution Protocol (request)

Hardware type: Ethernet (0x0001)

Protocol type: IP (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: request (0x0001)

Sender MAC address: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)

Sender IP address: 10.0.1.13 (10.0.1.13)

Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)

Target IP address: 10.0.1.11 (10.0.1.11)

No. Time Source Destination Protocol Info

8 5.000034 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)

Arrival Time: Jun 7, 2007 04:34:51.936387000

[Time delta from previous packet: 0.000018000 seconds]

[Time since reference or first frame: 5.000034000 seconds]

Frame Number: 8

Packet Length: 42 bytes

Capture Length: 42 bytes

[Frame is marked: False]

[Protocols in frame: eth:arp]

[Coloring Rule Name: ARP]

[Coloring Rule String: arp]

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)

Destination: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)

Address: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)

....0 .... = IG bit: Individual address (unicast)

.... ..0. .... = LG bit: Globally unique address (factory default)

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)

....0 .... = IG bit: Individual address (unicast)

.... ..0. .... = LG bit: Globally unique address (factory default)

Type: ARP (0x0806)

Address Resolution Protocol (reply)

Hardware type: Ethernet (0x0001)

Protocol type: IP (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: reply (0x0002)

Sender MAC address: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25)

Sender IP address: 10.0.1.11 (10.0.1.11)

Target MAC address: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)

Target IP address: 10.0.1.13 (10.0.1.13)

Lab2 Report

[Exercise 1]
Include the saved data in your lab report .

Ans:
05:54:49.601457 arp who-has 10.0.1.12 tell 10.0.1.11
05:54:49.601547 arp reply 10.0.1.12 is-at 00:04:5a:7a:c8:ca
05:54:49.601560 IP 10.0.1.11 > 10.0.1.12: ICMP echo request, id 8516, seq 1, length 64
05:54:49.601649 IP 10.0.1.12 > 10.0.1.11: ICMP echo reply, id 8516, seq 1, length 64
05:54:50.601335 IP 10.0.1.11 > 10.0.1.12: ICMP echo request, id 8516, seq 2, length 64
05:54:50.601427 IP 10.0.1.12 > 10.0.1.11: ICMP echo reply, id 8516, seq 2, length 64
05:54:51.601200 IP 10.0.1.11 > 10.0.1.12: ICMP echo request, id 8516, seq 3, length 64
05:54:51.601290 IP 10.0.1.12 > 10.0.1.11: ICMP echo reply, id 8516, seq 3, length 64
05:54:52.601062 IP 10.0.1.11 > 10.0.1.12: ICMP echo request, id 8516, seq 4, length 64
05:54:52.601153 IP 10.0.1.12 > 10.0.1.11: ICMP echo reply, id 8516, seq 4, length 64
05:54:53.600926 IP 10.0.1.11 > 10.0.1.12: ICMP echo request, id 8516, seq 5, length 64
05:54:53.601014 IP 10.0.1.12 > 10.0.1.11: ICMP echo reply, id 8516, seq 5, length 64
05:54:54.599346 arp who-has 10.0.1.11 tell 10.0.1.12
05:54:54.599365 arp reply 10.0.1.11 is-at 00:04:5a:7a:c8:25

06:09:10.967501 IP 10.0.1.11 > 10.0.1.12: ICMP echo request, id 19524, seq 1, length 64
06:09:10.967590 IP 10.0.1.12 > 10.0.1.11: ICMP echo reply, id 19524, seq 1, length 64
06:09:11.963288 IP 10.0.1.11 > 10.0.1.12: ICMP echo request, id 19524, seq 2, length 64
06:09:11.963381 IP 10.0.1.12 > 10.0.1.11: ICMP echo reply, id 19524, seq 2, length 64
06:09:12.963153 IP 10.0.1.11 > 10.0.1.12: ICMP echo request, id 19524, seq 3, length 64
06:09:12.963242 IP 10.0.1.12 > 10.0.1.11: ICMP echo reply, id 19524, seq 3, length 64
06:09:13.963016 IP 10.0.1.11 > 10.0.1.12: ICMP echo request, id 19524, seq 4, length 64
06:09:13.963108 IP 10.0.1.12 > 10.0.1.11: ICMP echo reply, id 19524, seq 4, length 64
06:09:14.962878 IP 10.0.1.11 > 10.0.1.12: ICMP echo request, id 19524, seq 5, length 64
06:09:14.962968 IP 10.0.1.12 > 10.0.1.11: ICMP echo reply, id 19524, seq 5, length 64

[Exercise 3A]

1. What is the destination Mac address of an ARP request packet?

Ans:
The destination MAC address is ff:ff:ff:ff:ff:ff:ff:ff, since PC1 broadcast an ARP request packet to the network asking who has the MAC address of IP address: 10.0.1.12.

Data:
No. Time Source Destination Protocol Info
1 0.000000 00:04:5a:7a:c8:25 **ff:ff:ff:ff:ff:ff ARP Who has 10.0.1.12? Tell 10.0.1.11**

Frame 1 (42 bytes on wire, 42 bytes captured)
Arrival Time: Jun 7, 2007 07:09:06.610649000

[Time delta from previous packet: 0.000000000 seconds]
[Time since reference or first frame: 0.000000000 seconds]
Frame Number: 1
Packet Length: 42 bytes
Capture Length: 42 bytes
[Frame is marked: False]
[Protocols in frame: eth:arp]
[Coloring Rule Name: ARP]
[Coloring Rule String: arp]
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)
Destination: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
Address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)

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: ARP (0x0806)
Address Resolution Protocol (request)
Hardware type: Ethernet (0x0001)
Protocol type: IP (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (0x0001)
Sender MAC address: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25)
Sender IP address: 10.0.1.11 (10.0.1.11)
Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
Target IP address: 10.0.1.12 (10.0.1.12)

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

Ans:
It was "ARP (0x0806)" for all of the ARP packets. It was "IP (0x0800)" for all of the ICMP packets.

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

Ans:
First , PC1 (10.0.1.11) broadcast an ARP request to the network asking who has the MAC address of PC2(10.0.1.12). After PC2 received the ARP request, it will send an ARP reply to PC1 with its MAC address. PC1 received the ARP reply containing PC2's MAC address, and cache the MAC address in ARP table for future use.

[Exercise 3B]
Include the completed Table 2.2 in your 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:C8:25
PC2	10.0.1.12/24	00:04:5A:7A:C8:CA
PC3	10.0.1.13/24	00:04:5A:7A:C6:64
PC4	10.0.1.14/24	00:04:5A:7B:3D:83

[Exercise 3C]

1.Using the saved output, describe the time interval between each ARP Request packet 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.

ARP request:

No.	Time Stamp
1	0.0000000
2	0.999831
3	1.999693
4	36.362985
5	37.362843

As the data shown above , PC1 send the ARP request at time 0.0000000 but didn't get the ARP reply; then, it resent a 2nd ARP request at 0.999831 but didn't get the ARP reply again; lastly, it resent a 3rd ARP request at 1.999693 but still failed to receive the ARP reply. After failing to send ARP request 3 times, PC1 stops sending ARP request. The time interval between 2 ARP packets is about 1 second. It is determined by measuring the time between the previous captured frame and the displayed frame.

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

Because ARP request and IP packets are handled differently by the protocol. IP packets are sent across networks, therefore they are handled by the network layer protocol.Whereas ARP is only within a single network , hence only handled by link layer protocol.

[Exercise 6]

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

Output 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)
Arrival Time: Jun 7, 2007 06:07:47.163046000
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)
Destination: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
Address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
Source: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)
Address: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)
Type: ARP (0x0806)
Address Resolution Protocol (request)
Hardware type: Ethernet (0x0001)
Protocol type: IP (0x0800)

No. Time Source Destination Protocol Info
2 0.000056 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 2 (60 bytes on wire, 60 bytes captured)
Arrival Time: Jun 7, 2007 06:07:47.163102000
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)
Destination: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)
Address: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)
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: ARP (0x0806)
Trailer: 000000000000000000000000000000000000
Address Resolution Protocol (reply)
Hardware type: Ethernet (0x0001)
Protocol type: IP (0x0800)

No. Time Source Destination Protocol Info
3 0.000070 10.0.1.13 10.0.1.11 TCP 57680 > 23 [SYN] Seq=0 Len=0 MSS=1460 TSV=4922142 TSER=0

Frame 3 (70 bytes on wire, 70 bytes captured)
Arrival Time: Jun 7, 2007 06:07:47.163116000
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)
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:c6:64 (00:04:5a:7a:c6:64)
Address: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)

Type: IP (0x0800)
Internet Protocol, Src: 10.0.1.13 (10.0.1.13), Dst: 10.0.1.11 (10.0.1.11)

No. Time Source Destination Protocol Info
4 0.000058 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 4 (60 bytes on wire, 60 bytes captured)
Arrival Time: Jun 7, 2007 06:07:47.163104000
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)
Destination: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)
Address: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)
Source: 00:04:5a:7b:3d:83 (00:04:5a:7b:3d:83)
Address: 00:04:5a:7b:3d:83 (00:04:5a:7b:3d:83)
Type: ARP (0x0806)
Trailer: 000000000000000000000000000000000000
Address Resolution Protocol (reply)
Hardware type: Ethernet (0x0001)
Protocol type: IP (0x0800)

No. Time Source Destination Protocol Info
5 0.000154 10.0.1.11 10.0.1.13 TCP 23 > 57680 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 TSV=3161556 TSER=4922142

Ans:
From the data captured above , after an ARP request is sent , the first PC responds to the request will build up ARP cache. Any other responders will be ignored / rejected. In the experiment PC3 is the first PC respond to the request and the resolved MAC address is 00:04:5a:7a:c8:25 and ignored MAC address is 00:04:5a:7b:3d:83.

[Exercise 7]
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?

Ans:

When PCA send packet to PCB, we will determine if the IP address of PCA and PCB are in the same network by using the subnet mask of PCA.

Therefore, if PCA ping PCB, the IP address of PCA and PCB in ICMP request will be masked by the subnet mask of PCA while the IP address in ICMP reply will be masked by the subnet mask of PCB.

Following answers will be based on the explanation above.

a. From PC1 to PC3: PC1% ping –c 1 10.0.1.120
Both ICMP request and reply succeeded. The ICMP request succeeded, because based on the subnet mask of PC1, the ip address of PC1 and PC3 are in the same network. The ICMP reply

succeeded, because based on the subnet mask of PC3, the ip address of PC1 and PC3 are in the same network.

b. From PC1 to PC2: PC1% ping –c 1 10.0.1.101
Both ICMP request and reply succeeded. The ICMP request succeeded, because based on the subnet mask of PC1, the ip address of PC1 and PC2 are in the same network. The ICMP reply succeeded, because based on the subnet mask of PC2, the ip address of PC1 and PC2 are in the same network.

c. From PC1 to PC4: PC1% ping –c 1 10.0.1.121

The ICMP request succeed but the ICMP reply failed. The ICMP request succeeded, because based on the subnet mask of PC1, the ip address of PC1 and PC3 are in the same network. The ICMP reply failed, because based on the subnet mask of PC4, the ip address of PC1 and PC4 are not in the same network.

d. From PC4 to PC1: PC4% ping –c 1 10.0.1.100
The network is unreachable, which means ICMP request failed, because based on the subnet mask of PC4, the ip address of PC1 and PC4 are not in the same network.

e. From PC2 to PC4: PC2% ping –c 1 10.0.1.121
The network is unreachable, which means ICMP request failed, because based on the subnet mask of PC2, the ip address of PC2 and PC4 are not in the same network.

f. From PC2 to PC3: PC2% ping –c 1 10.0.1.120
The network is unreachable, which means ICMP request failed, because based on the subnet mask of PC2, the ip address of PC3 and PC4 are not in the same network.

[Exercise 8]

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

Ans: Since static mapping can only be done manually , when the number of names and IP to be mapped is too large , it is easy to make mistype and too time consuming.

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

Ans: Since only one IP address can be associated with the same hostname , and it is based on " first come first serve " rule .Therefore only the first IP address in the file will respond.

[Exercise 9A]

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

Data:

No.	Time	Source	Destination	Protocol Info
1	0.000000	10.0.1.11	10.0.1.12	**TCP 38829 > 21 [SYN] Seq=0 Len=0 MSS=1460 TSV=2768723 TSER=0**

Frame 1 (70 bytes on wire, 70 bytes captured)
Arrival Time: Jun 7, 2007 07:54:40.229371000
[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)
Address: 00:04:5a:7a:c8:ca (00:04:5a:7a:c8:ca)
....0 .... = IG bit: Individual address (unicast)
.... ..0. .... = LG bit: Globally unique address (factory default)
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)
....0 .... = IG bit: Individual address (unicast)
.... ..0. .... = LG bit: Globally unique address (factory default)
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)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..0. = ECN-Capable Transport (ECT): 0
....0 = ECN-CE: 0
Total Length: 56
Identification: 0x090e (2318)
Flags: 0x04 (Don't Fragment)
0... = Reserved bit: Not set
.1.. = Don't fragment: Set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 64
Protocol: TCP (0x06)
Header checksum: 0x1b9c [correct]
[Good: True]
[Bad : False]
Source: 10.0.1.11 (10.0.1.11)
Destination: 10.0.1.12 (10.0.1.12)
Transmission Control Protocol, **Src Port: 38829 (38829), Dst Port: 21 (21), Seq: 0, Len: 0**
Source port: 38829 (38829)

Ans: As the data shown above the port number of the FTP client is port 21 , and the port number for the server is 38829.

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

Data:

No. Time Source Destination **Protocol Info**
10 2.418502 10.0.1.11 10.0.1.12 **FTP Request: USER root**

Frame 10 (77 bytes on wire, 77 bytes captured)
Arrival Time: Jun 7, 2007 07:54:42.647873000
[Time delta from previous packet: 2.367874000 seconds]
[Time since reference or first frame: 2.418502000 seconds]
Frame Number: 10
Packet Length: 77 bytes
Capture Length: 77 bytes
[Frame is marked: False]
[Protocols in frame: eth:ip:tcp:ftp]
[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)

No. Time Source Destination **Protocol Info**
13 4.930049 10.0.1.11 10.0.1.12 **FTP Request: PASS rootroot**

Frame 13 (81 bytes on wire, 81 bytes captured)
Arrival Time: Jun 7, 2007 07:54:45.159420000
[Time delta from previous packet: 2.511014000 seconds]
[Time since reference or first frame: 4.930049000 seconds]
Frame Number: 13
Packet Length: 81 bytes
Capture Length: 81 bytes
[Frame is marked: False]
[Protocols in frame: eth:ip:tcp:ftp]
[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)
Address: 00:04:5a:7a:c8:ca (00:04:5a:7a:c8:ca)
....0 .... = IG bit: Individual address (unicast)
.... ..0. .... = LG bit: Globally unique address (factory default)
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)
....0 .... = IG bit: Individual address (unicast)
.... ..0. .... = LG bit: Globally unique address (factory default)
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)

0001 00.. = Differentiated Services Codepoint: Unknown (0x04)

Ans: As the data shown above (look at the boldface text in the output data), under the Protocol Info: FTP Request: USER root, which means the username is root , and under the 2nd Protocol Info: FTP Request: PASS rootroot, which means the password is rootroot.

[Exercise 9B]

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

Ans: Yes the Telnet does have the same security flaws as FTP. The user name and password were sent with no encryption. Same as TCP, the information is under the Protocol Info field. From the output data, If I go over and highlight the packets with "telnet data..." under the protocol info, the username and password are displayed gradually in the telnet data section of the middle window. Although it is safer than sending two packets that contains password and username by dividing the content by characters , it is still very hackable by catching those encrypted consecutive packets to acquire the login information.

Data:

No. Time Source Destination Protocol Info
17 1.020796 10.0.1.11 10.0.1.12 TELNET Telnet Data ...

Frame 17 (69 bytes on wire, 69 bytes captured)
Arrival Time: Jun 7, 2007 08:04:28.629215000
[Time delta from previous packet: 0.000049000 seconds]
[Time since reference or first frame: 1.020796000 seconds]
Frame Number: 17
Packet Length: 69 bytes
Capture Length: 69 bytes
[Frame is marked: False]
[Protocols in frame: eth:ip:tcp:telnet]
[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)
Address: 00:04:5a:7a:c8:ca (00:04:5a:7a:c8:ca)
....0 .... = IG bit: Individual address (unicast)
.... ..0. .... = LG bit: Globally unique address (factory default)
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)
....0 .... = IG bit: Individual address (unicast)
.... ..0. .... = LG bit: Globally unique address (factory default)
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)
0001 00.. = Differentiated Services Codepoint: Unknown (0x04)
.... ..0. = ECN-Capable Transport (ECT): 0
....0 = ECN-CE: 0

Total Length: 55
Identification: 0x8e53 (36435)
Flags: 0x04 (Don't Fragment)
0... = Reserved bit: Not set
.1.. = Don't fragment: Set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 64
Protocol: TCP (0x06)
Header checksum: 0x9647 [correct]
[Good: True]
[Bad : False]
Source: 10.0.1.11 (10.0.1.11)
Destination: 10.0.1.12 (10.0.1.12)

Transmission Control Protocol, Src Port: 47649 (47649), Dst Port: 23 (23), Seq: 123, Ack: 93, Len: 3

Source port: 47649 (47649)
Destination port: 23 (23)
Sequence number: 123 (relative sequence number)
[Next sequence number: 126 (relative sequence number)]
Acknowledgement number: 93 (relative ack number)
Header length: 32 bytes
Flags: 0x18 (PSH, ACK)
0... .... = Congestion Window Reduced (CWR): Not set
.0.. .... = ECN-Echo: Not set
..0. .... = Urgent: Not set
...1 .... = Acknowledgment: Set
.... 1... = Push: Set
.... .0.. = Reset: Not set
.... ..0. = Syn: Not set
....0 = Fin: Not set
Window size: 5840
Checksum: 0x23c7 [correct]
[Good Checksum: True]
[Bad Checksum: False]
Options: (12 bytes)
NOP
NOP
Timestamps: TSval 2915843, TSecr 3846261
[SEQ/ACK analysis]
[This is an ACK to the segment in frame: 16]
[The RTT to ACK the segment was: 0.000049000 seconds]

Telnet

Command: Do Echo

No.	Time	Source	Destination	Protocol	Info
18	1.020873	10.0.1.12	10.0.1.11	TELNET	Telnet Data ...

Frame 18 (73 bytes on wire, 73 bytes captured)

Arrival Time: Jun 7, 2007 08:04:28.629292000
[Time delta from previous packet: 0.000077000 seconds]

[Time since reference or first frame: 1.020873000 seconds]
Frame Number: 18
Packet Length: 73 bytes
Capture Length: 73 bytes
[Frame is marked: False]
[Protocols in frame: eth:ip:tcp:telnet]
[Coloring Rule Name: TCP]
[Coloring Rule String: tcp]
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)
....0 .... = IG bit: Individual address (unicast)
.... ..0. .... = LG bit: Globally unique address (factory default)
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)
....0 .... = IG bit: Individual address (unicast)
.... ..0. .... = LG bit: Globally unique address (factory default)
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)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..0. = ECN-Capable Transport (ECT): 0
....0 = ECN-CE: 0
Total Length: 59
Identification: 0xae3f (44607)
Flags: 0x04 (Don't Fragment)
0... = Reserved bit: Not set
.1.. = Don't fragment: Set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 64
Protocol: TCP (0x06)
Header checksum: 0x7667 [correct]
[Good: True]
[Bad : False]
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: 47649 (47649), Seq: 93, Ack: 126, Len: 7
Source port: 23 (23)
Destination port: 47649 (47649)
Sequence number: 93 (relative sequence number)
[Next sequence number: 100 (relative sequence number)]
Acknowledgement number: 126 (relative ack number)
Header length: 32 bytes
Flags: 0x18 (PSH, ACK)
0... .... = Congestion Window Reduced (CWR): Not set
.0.. .... = ECN-Echo: Not set
..0. .... = Urgent: Not set

...1 .... = Acknowledgment: Set
.... 1... = Push: Set
.... .0.. = Reset: Not set
.... ..0. = Syn: Not set
....0 = Fin: Not set
Window size: 5792
Checksum: 0xc2da [correct]
[Good Checksum: True]
[Bad Checksum: False]
Options: (12 bytes)
NOP
NOP
Timestamps: TSval 3846261, TSecr 2915843
[SEQ/ACK analysis]
[This is an ACK to the segment in frame: 17]
[The RTT to ACK the segment was: 0.000077000 seconds]
Telnet
Data: login:

No. Time Source Destination Protocol Info
19 1.058947 10.0.1.11 10.0.1.12 TCP 47649 > 23 [ACK] Seq=126 Ack=100 Win=5840 Len=0 TSV=2915853 TSER=3846261

Frame 19 (66 bytes on wire, 66 bytes captured)
Arrival Time: Jun 7, 2007 08:04:28.667366000
[Time delta from previous packet: 0.038074000 seconds]
[Time since reference or first frame: 1.058947000 seconds]
Frame Number: 19
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)
Address: 00:04:5a:7a:c8:ca (00:04:5a:7a:c8:ca)
....0 .... = IG bit: Individual address (unicast)
.... ..0. .... = LG bit: Globally unique address (factory default)
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)
....0 .... = IG bit: Individual address (unicast)
.... ..0. .... = LG bit: Globally unique address (factory default)
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)
0001 00.. = Differentiated Services Codepoint: Unknown (0x04)
.... ..0. = ECN-Capable Transport (ECT): 0
....0 = ECN-CE: 0

Total Length: 52
Identification: 0x8e54 (36436)
Flags: 0x04 (Don't Fragment)
0... = Reserved bit: Not set
.1.. = Don't fragment: Set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 64
Protocol: TCP (0x06)
Header checksum: 0x9649 [correct]
[Good: True]
[Bad : False]
Source: 10.0.1.11 (10.0.1.11)
Destination: 10.0.1.12 (10.0.1.12)

[Exercise 9C]

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

Ans: As the highlighted data shown, three packets are required to transmit a single character in Telnet session, since the first packet was sent from the client to the server , containing the character delivered. The second packet is sent from the server back to the client , that request the client's confirmation of the content received. The last packet is an ACK packet from the client that confirm the transmission is completed .

Output Data:

No.	Time	Source	Destination	Protocol	Info
17	**1.020796**	**10.0.1.11**	**10.0.1.12**	**TELNET**	**Telnet Data ...**

Frame 17 (69 bytes on wire, 69 bytes captured)
Arrival Time: Jun 7, 2007 08:04:28.629215000
[Time delta from previous packet: 0.000049000 seconds]
[Time since reference or first frame: 1.020796000 seconds]
Frame Number: 17
Packet Length: 69 bytes
Capture Length: 69 bytes
[Frame is marked: False]
[Protocols in frame: eth:ip:tcp:telnet]
[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)
Address: 00:04:5a:7a:c8:ca (00:04:5a:7a:c8:ca)
....0 .... = IG bit: Individual address (unicast)
.... ..0. .... = LG bit: Globally unique address (factory default)
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)
....0 .... = IG bit: Individual address (unicast)
.... ..0. .... = LG bit: Globally unique address (factory default)
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)
    0001 00.. = Differentiated Services Codepoint: Unknown (0x04)
    .... ..0. = ECN-Capable Transport (ECT): 0
    ....0 = ECN-CE: 0
    Total Length: 55
    Identification: 0x8e53 (36435)
    Flags: 0x04 (Don't Fragment)
    0... = Reserved bit: Not set
    .1.. = Don't fragment: Set
    ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x9647 [correct]
    [Good: True]
    [Bad : False]
    Source: 10.0.1.11 (10.0.1.11)
    Destination: 10.0.1.12 (10.0.1.12)
Transmission Control Protocol, Src Port: 47649 (47649), Dst Port: 23 (23), Seq: 123, Ack: 93, Len: 3
    Source port: 47649 (47649)
    Destination port: 23 (23)
    Sequence number: 123 (relative sequence number)
    [Next sequence number: 126 (relative sequence number)]
    Acknowledgement number: 93 (relative ack number)
    Header length: 32 bytes
    Flags: 0x18 (PSH, ACK)
    0... .... = Congestion Window Reduced (CWR): Not set
    .0.. .... = ECN-Echo: Not set
    ..0. .... = Urgent: Not set
    ...1 .... = Acknowledgment: Set
    .... 1... = Push: Set
    .... .0.. = Reset: Not set
    .... ..0. = Syn: Not set
    ....0 = Fin: Not set
    Window size: 5840
    Checksum: 0x23c7 [correct]
    [Good Checksum: True]
    [Bad Checksum: False]
    Options: (12 bytes)
    NOP
    NOP
    Timestamps: TSval 2915843, TSecr 3846261
    [SEQ/ACK analysis]
    [This is an ACK to the segment in frame: 16]
    [The RTT to ACK the segment was: 0.000049000 seconds]
Telnet
    Command: Do Echo

No. Time Source Destination Protocol Info
18 1.020873 10.0.1.12 10.0.1.11 TELNET Telnet Data ...

Frame 18 (73 bytes on wire, 73 bytes captured)
Arrival Time: Jun 7, 2007 08:04:28.629292000
[Time delta from previous packet: 0.000077000 seconds]
[Time since reference or first frame: 1.020873000 seconds]
Frame Number: 18
Packet Length: 73 bytes
Capture Length: 73 bytes
[Frame is marked: False]
[Protocols in frame: eth:ip:tcp:telnet]
[Coloring Rule Name: TCP]
[Coloring Rule String: tcp]
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)
....0 .... = IG bit: Individual address (unicast)
.... ..0. .... = LG bit: Globally unique address (factory default)
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)
....0 .... = IG bit: Individual address (unicast)
.... ..0. .... = LG bit: Globally unique address (factory default)
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)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..0. = ECN-Capable Transport (ECT): 0
....0 = ECN-CE: 0
Total Length: 59
Identification: 0xae3f (44607)
Flags: 0x04 (Don't Fragment)
0... = Reserved bit: Not set
.1.. = Don't fragment: Set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 64
Protocol: TCP (0x06)
Header checksum: 0x7667 [correct]
[Good: True]
[Bad : False]
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: 47649 (47649), Seq: 93, Ack: 126, Len: 7
Source port: 23 (23)
Destination port: 47649 (47649)
Sequence number: 93 (relative sequence number)

[Next sequence number: 100 (relative sequence number)]
Acknowledgement number: 126 (relative ack number)
Header length: 32 bytes
Flags: 0x18 (PSH, ACK)
0... .... = Congestion Window Reduced (CWR): Not set
.0.. .... = ECN-Echo: Not set
..0. .... = Urgent: Not set
...1 .... = Acknowledgment: Set
.... 1... = Push: Set
.... .0.. = Reset: Not set
.... ..0. = Syn: Not set
....0 = Fin: Not set
Window size: 5792
Checksum: 0xc2da [correct]
[Good Checksum: True]
[Bad Checksum: False]
Options: (12 bytes)
NOP
NOP
Timestamps: TSval 3846261, TSecr 2915843
[SEQ/ACK analysis]
[This is an ACK to the segment in frame: 17]
[The RTT to ACK the segment was: 0.000077000 seconds]

Telnet

Data: login:

No. Time Source Destination Protocol Info

19 1.058947 10.0.1.11 10.0.1.12 TCP 47649 > 23 [ACK] Seq=126 Ack=100 Win=5840 Len=0 TSV=2915853 TSER=3846261

Frame 19 (66 bytes on wire, 66 bytes captured)
Arrival Time: Jun 7, 2007 08:04:28.667366000
[Time delta from previous packet: 0.038074000 seconds]
[Time since reference or first frame: 1.058947000 seconds]
Frame Number: 19
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)
Address: 00:04:5a:7a:c8:ca (00:04:5a:7a:c8:ca)
....0 .... = IG bit: Individual address (unicast)
.... ..0. .... = LG bit: Globally unique address (factory default)
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)
....0 .... = IG bit: Individual address (unicast)
.... ..0. .... = LG bit: Globally unique address (factory default)
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)
    0001 00.. = Differentiated Services Codepoint: Unknown (0x04)
    .... ..0. = ECN-Capable Transport (ECT): 0
    ....0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x8e54 (36436)
    Flags: 0x04 (Don't Fragment)
    0... = Reserved bit: Not set
    .1.. = Don't fragment: Set
    ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x9649 [correct]
    [Good: True]
    [Bad : False]
    Source: 10.0.1.11 (10.0.1.11)
    Destination: 10.0.1.12 (10.0.1.12)