Cover Page

ECE461 Lab3 Report

Name: Wei Lin (#999595193)
Name: Shenglin Meng (#1000695517)

[Exercise 1]

1(a). What is the output on PC1 when the ping commands are issued?

Ans:
PC1% ping –c 5 10.0.1.21
Output:
PING 10.0.1.21 (10.0.1.21) 56(84) bytes of data.
64 bytes from 10.0.1.21: icmp_seq=1 ttl=64 time=4.10 ms
64 bytes from 10.0.1.21: icmp_seq=2 ttl=64 time=0.111 ms
64 bytes from 10.0.1.21: icmp_seq=3 ttl=64 time=0.108 ms
64 bytes from 10.0.1.21: icmp_seq=4 ttl=64 time=0.111 ms
64 bytes from 10.0.1.21: icmp_seq=5 ttl=64 time=0.106 ms

--- 10.0.1.21 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4003ms
rtt min/avg/max/mdev = 0.106/0.907/4.103/1.598 ms

PC1% ping –c 5 10.0.2.1
Output:
connect: Network is unreachable

PC1% ping –c 5 10.0.3.41
Output:
connect: Network is unreachable

Which packets, if any, are captured by ethereal?

Ans:
ARP and ICMP packets are captured when ping –c 5 10.0.1.21. No packet is captured when ping –c 5 10.0.2.1 and ping –c 5 10.0.3.41.

Do you observe any ARP or ICMP packets? If so, what do they indicate?

Ans:
Yes, ARP and ICMP packets are observed when ping -c 5 10.0.1.21. The ARP packets indicate that PC1 and PC2 are trying to resolve the MAC address of each other: PC1 sends ARP request while PC2 sends ARP reply. The ICMP request sends from PC1 and ICMP reply sends from PC2 indicate that the ping command is successful, and PC1 and PC2 are able to communicate with each other.

Which destinations are not reachable? Explain.

Ans:
The destinations that are unreachable are 10.0.2.1 (router1) and 10.0.3.41 (PC4).
Reason: These 2 IP address are not in the same network as PC1; the IP forwarding function was not enabled in PC2; the routing table in router1, PC1, PC2 and PC4 haven't been setup yet; therefore, PC1 cannot communicate with hosts that are not in the same network.

1(c). Include the saved output of the routing table. Explain the entries in the routing table and discuss the values of the fields for each entry.

Ans:
The output data is the routing table of PC1:
Kernel IP routing table

Destination	Gateway	Genmask	Flags	MSS	Window	irtt	Iface
10.0.1.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
10.0.2.0	10.0.1.21	255.255.255.0	UG	0	0	0	eth0
10.0.3.0	10.0.1.21	255.255.255.0	UG	0	0	0	eth0
169.254.0.0	0.0.0.0	255.255.0.0	U	0	0	0	eth0
127.0.0.0	0.0.0.0	255.0.0.0	U	0	0	0	lo

The 10.0.1.0 with mask 255.255.255.0 indicates the local network address. The gateway for this address is default gateway: 0.0.0.0. The flags U means "Route Usable". The Iface eth0 means the output interface is eth0. The information above indicates that packets sends to same network as PC1 will go to the default gateway on eth0 interface.

The 10.0.2.0 with mask 255.255.255.0 indicates network address of PC2. The gateway for this address is 10.0.1.21. The flags UG means the "Route Usable" and "Destination requires forwarding by intermediary". The Iface eth0 means the output interface is eth0. The information above indicates that packets sends to network 10.0.2.0 will be routed to the gateway 10.0.1.21 on eth0 interface.

The 10.0.3.0 with mask 255.255.255.0 indicates the network address of PC4. The gateway for this address is 10.0.1.21. The flags UG means the "Route Usable" and "Destination requires forwarding by intermediary". The Iface eth0 means the output interface is eth0. The information above indicates that packets sends to network 10.0.3.0 will be routed to the gateway 10.0.1.21 on eth0 interface.

The 169.254.0.0 with mask 255.255.0.0 indicates the link-local address. The gateway for this address is default gateway: 0.0.0.0. The flags U means “Route Usable”. The Iface eth0 means the output interface is eth0.

The 127.0.0.0 with mask 255.0.0.0 indicates the local loopback address. The gateway for this address is default gateway: 0.0.0.0. The flags U means “Route Usable”. The Iface eth0 means the output interface is lo.

All MSS, Window and irtt is 0. It means MSS is the default “maximum segment size”, Window is the default “window size” and irtt is the default “initial road trip time” for TCP connection over this route.

[Exercise 3]

3.b Use the ethereal output and the previously saved routing table to explain the operation of traceroute.

Ans:

Traceroute is used to display the route information and transit delays of packets across IP network. Ethereal captured data from command: PC1% traceroute 10.0.3.41. From the data, the operation of traceroute from PC1 to PC4 is:

1. PC1(10.0.1.11) sends a UDP traceroute packet with TTL(time to live) = 1 to PC2(10.0.1.21) based on the routing table
2. PC2 receives the traceroute packet and decrements the TTL value to 0. As a result, PC2 will drop the packet and send an ICMP error message to PC1 indicates that Time-to-live exceeded.
3. PC1 receives the ICMP error message and tries to the UDP traceroute packet with same TTL=1 again. After 3 attempts, PC1 sends a traceroute packet with increment TTL =2.
4. After increment the TTL to 2, the traceroute packet successfully passes the PC2 but it is dropped in the router 1(10.0.2.1), and router 1 send back an ICMP Time-to-live exceeded message to PC1.
5. After another 3 attempts of sending traceroute packet with TTL=2, PC1 starts sending a traceroute packet with TTL=3.
6. With TTL=3, the traceroute packet is able to reach PC4 (10.0.3.41). Then, PC 4 will send back an ICMP: Destination unreachable (Port unreachable) message to PC1.
7. After 3 attempts with TTL=3, PC1 receives 3 times ICMP: Destination unreachable (Port unreachable) message.
8. The traceroute command completes.

Output Segments Support: It is not the complete output, so the data below is not continuous (NO. are not continuous). We want to show the TTL value in IP headers is changing and the ICMP error message, so we only include the required sections. The TTL and ICMP error is highlighted in the following data:

No. Time Source Destination Protocol Info
1 0.000000 10.0.1.11 10.0.3.41 UDP Source port: 51762 Destination port: 33435

Frame 1 (52 bytes on wire, 52 bytes captured)
……..
Internet Protocol, Src: 10.0.1.11 (10.0.1.11), Dst: 10.0.3.41 (10.0.3.41)
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: 38
Identification: 0xca33 (51763)
Flags: 0x00
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 1

No. Time Source Destination Protocol Info
2 0.000059 10.0.1.21 10.0.1.11 **ICMP Time-to-live exceeded** (Time to live exceeded in transit)
……..

No. Time Source Destination Protocol Info
7 0.011249 10.0.1.11 10.0.3.41 UDP Source port: 51762 Destination port: 33438
……..
Internet Protocol, Src: 10.0.1.11 (10.0.1.11), Dst: 10.0.3.41 (10.0.3.41)
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: 38
Identification: 0xca36 (51766)
Flags: 0x00
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 2

No. Time Source Destination Protocol Info
13 0.013509 10.0.1.11 10.0.3.41 UDP Source port: 51762 Destination port: 33441

…….
Internet Protocol, Src: 10.0.1.11 (10.0.1.11), Dst: 10.0.3.41 (10.0.3.41)
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: 38
Identification: 0xca39 (51769)
Flags: 0x00
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 3

……

No. Time Source Destination Protocol Info
14 0.013762 10.0.3.41 10.0.1.11 **ICMP Destination unreachable (Port unreachable)**

…….

[Exercise 6]

Are the two ICMP packets that you saved identical? If not, what is different? Include the packet data in your lab report to substantiate your claims.

Ans:

No, they are different. They had different "NO." value, different "Time" value, and different "Time to live" values. Since the time-to-live values are different, the checksums are different as well.

Output:

```
No.     Time        Source                Destination           Protocol Info
    1  21.637399   10.0.4.10             10.0.1.10             ICMP     Echo (ping) request
Frame 10 (98 bytes on wire, 98 bytes captured)
    Arrival Time: Jun 27, 2007 20:59:56.687829000
    [Time delta from previous packet: 0.000019000 seconds]
    [Time since reference or first frame: 21.637399000 seconds]
    Frame Number: 10
    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:80:93:f3 (00:04:5a:80:93:f3), Dst: 00:1c:58:6a:23:28
(00:1c:58:6a:23:28)
    Destination: 00:1c:58:6a:23:28 (00:1c:58:6a:23:28)
        Address: 00:1c:58:6a:23:28 (00:1c:58:6a:23:28)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    Source: 00:04:5a:80:93:f3 (00:04:5a:80:93:f3)
        Address: 00:04:5a:80:93:f3 (00:04:5a:80:93:f3)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    Type: IP (0x0800)
Internet Protocol, Src: 10.0.4.10 (10.0.4.10), Dst: 10.0.1.10 (10.0.1.10)
    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
……….....

No.     Time        Source              Destination         Protocol Info
     2  21.660085   10.0.4.10           10.0.1.10           ICMP     Echo (ping) request

Frame 10 (98 bytes on wire, 98 bytes captured)
    Arrival Time: Jun 27, 2007 20:59:56.687829000
    [Time delta from previous packet: 0.000019000 seconds]
    [Time since reference or first frame: 21.637399000 seconds]
    Frame Number: 10
    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:80:93:f3 (00:04:5a:80:93:f3), Dst: 00:1c:58:6a:23:28
(00:1c:58:6a:23:28)
    Destination: 00:1c:58:6a:23:28 (00:1c:58:6a:23:28)
        Address: 00:1c:58:6a:23:28 (00:1c:58:6a:23:28)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    Source: 00:04:5a:80:93:f3 (00:04:5a:80:93:f3)
        Address: 00:04:5a:80:93:f3 (00:04:5a:80:93:f3)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    Type: IP (0x0800)
Internet Protocol, Src: 10.0.4.10 (10.0.4.10), Dst: 10.0.1.10 (10.0.1.10)
    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: 61
……...

Why does the ICMP Echo Request packet not loop forever in the network?

Ans:

The ICMP request packet has a TTL (time-to-live) value. When the packet passes through a router, the TTL value will be decremented by 1. After the TTL value decremented to 0, the packet will be dropped and an ICMP error message: Time-to-live exceeded will be sent back. Therefore, the packet will not looped forever.