ECE 461 Lab3 report

Xiaoyang Guo 999578513

Mingqi Hou 999767676

Exercise 1 (A)

1. **What is the output on PC1 when *ping* commands are issued?**

```
[root@PC1 root]# ping -c 5 10.0.1.21
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=2.99 ms
64 bytes from 10.0.1.21: icmp_seq=2 ttl=64 time=0.110 ms
64 bytes from 10.0.1.21: icmp_seq=3 ttl=64 time=0.110 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=0.110 ms

--- 10.0.1.21 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 0.110/0.687/2.994/1.153 ms

[root@PC1 root]# ping -c 5 10.0.2.1
connect: Network is unreachable

[root@PC1 root]# ping -c 5 10.0.3.41
connect: Network is unreachable
```

2. **Which packets, if any, are captured by *Ethernal*?**

ARP and ICMP packets are captured on Ethereal when command *ping -c 5 10.0.1.21* is issued. No packet is captured when commands *ping -c 5 10.0.2.1* and *ping -c 5 10.0.3.41* are issued.

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

Yes. APR and ICMP packets are captured when command *ping -c 5 10.0.1.21* is issued. The ARP packet indicates PC1 and PC2 eth0 are resolving each other's MAC address. PC1 sends out ICMP echo request packets once the MAC address of PC2 eth0 is available. The ICMP echo reply packets sent by PC2 eth0 are received by PC1. The ARP and ICMP echo packets indicate PC1 and PC2 eth0 are able to communicate between each other.

4. **Which destinations are unreachable? Explain.**

PC4 and Router1 F0/0 are unreachable. PC4 eth0 has IP address 10.0.3.41/24. Router1 F0/0 has IP address 10.0.2.1/24. They are not in the same network as PC1 eth0 (10.0.1.11/24). In addition, routing table and IP forwarding are not configured to enable PC1 to communicate with hosts outside its network.

Exercise 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.

```
[root@PC1 root]# netstat -rn
```

```
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    lo
```

- 10.0.1.0/24 is the local network of PC1. This entry corresponds to the packets delivered to the local network of PC1. The gateway 0.0.0.0 indiactes local network. Flag U indicates the router is up. The packet will be sent to interface eth0 as indicated in Iface field.
- The entry 10.0.2.0/24 corresponds to the packets delivered to the network of PC2 eth1. To successfully deliver packets to PC2 eth1, PC1 must route the packets to gateway 10.0.1.21, which is PC2 eth0. Flag UG indicates the router is up and gateway is used. The packet will be sent to interface eth0 as indicated in Iface field.
- The entry 10.0.3.0/24 is used by packets delivered to the network of PC4. To successfully deliver packets to PC4, PC1 must route the packets to gateway 10.0.1.21, which is PC2 eth0. Flag UG indicates the router is up and gateway is used. The packet will be sent to interface eth0 as indicated in Iface field.
- Entry 127.0.0.0/8 is the loopback interace. Flag U indicates the router is up. The packet will be sent to interface eth0 as indicated in Iface field.
- Entry 169.254.0.0/16 is the link-local address. Flag U indicates the router is up. The packet will be sent to location interface as indicated in Iface field.
- Fields MSS, Window, and irtt have the same value 0 for all entries. MSS is the default maximum segment size for TCP connections over this route. Window is the default window size for TCP connections over this route. Irtt is the initial round trip time.

Exercise 2(C)

Include the output from Step 3 in your lab report.

```
Router1#show interface
FastEthernet0/0 is up, line protocol is up
  Hardware is MV96340 Ethernet, address is 001c.5845.33c0 (bia
001c.5845.33c0)
  Internet address is 10.0.2.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:01:06, output 00:00:06, output hang never
  Last clearing of "show interface" counters never
```

```
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output
drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     13 packets input, 970 bytes
     Received 7 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     236 packets output, 14278 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
FastEthernet0/1 is up, line protocol is down
  Hardware is MV96340 Ethernet, address is 001c.5845.33c1 (bia
001c.5845.33c1)
  Internet address is 10.0.3.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto Speed, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:03, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output
drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     235 packets output, 14168 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Serial0/0/0 is administratively down, line protocol is down
  Hardware is GT96K Serial
```

```
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output
drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 3 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=down  DSR=down  DTR=down  RTS=down  CTS=down
Serial0/0/1 is administratively down, line protocol is down
  Hardware is GT96K Serial
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output
drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 3 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=down  DSR=down  DTR=down  RTS=down  CTS=down
```

```
Router1#show running-config
Building configuration...
Current configuration : 887 bytes
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname Router1
boot-start-marker
boot-end-marker
enable secret 5 $1$uWfK$x520n9KfNRI/uOr74ptQj1
no aaa new-model
resource policy
ip subnet-zero
ip cef
no ip domain lookup
interface FastEthernet0/0
 ip address 10.0.2.1 255.255.255.0
 duplex auto
 speed auto
 no cdp enable
interface FastEthernet0/1
 ip address 10.0.3.1 255.255.255.0
 duplex auto
 speed auto
 no cdp enable
interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
ip classless
ip http server
no cdp run
control-plane
line con 0
 privilege level 15
line aux 0
line vty 0 4
 privilege level 15
 no login
line vty 5
```

```
 login
scheduler allocate 20000 1000
End
```

Exercise 2(D)

Include the saved output of the routing table from Step 1 and 2. Explain the field of the routing table entries of the Cisco router. Explain how the routing table has changed from Step 1 to Step 3.

```
Router1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
level-2
ia - IS-IS inter area, * - candidate default, U - per-user static
route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set
     10.0.0.0/24 is subnetted, 3 subnets
C       10.0.2.0 is directly connected, FastEthernet0/0
C       10.0.3.0 is directly connected, FastEthernet0/1
S       10.0.1.0 [1/0] via 10.0.2.0
```

- The entry 10.0.2.0 is the network directly connected to interafce F0/0.
- The entry 10.0.3.0 is the network directly connected to interafce F0/1.
- The entry 10.0.1.0 indicates all packets going to that netork should be routed through interafce F0/0 (10.0.2.0).
- Compared to the routing table from Step 1, a new entry, 10.0.1.0, is added.

Exercise 3(B)

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

The command *traceroute 10.0.3.41* is issued on PC1 and traffic is captured by *ethereal*. According to the routing tables, the path of the packets from PC1 to PC4 is to go through PC2, which receives packets on eth0 and forward them to eth1, then router1, which receives the packets on F0/0 and sends them out on F0/1, and finally to PC4, the destination host. Traceroute is a tool for displaying the route (path) and measuring transit delays of packets across an IP network. Traceroute works by sending packets with gradually increasing TTL value, starting with TTL value of one. Once command *traceroute 10.0.3.41* is issued on PC1,

it sends UDP packets to PC4 with incrementing TTL values. For example, the following is the first UDP packet sent by PC1, which has a TTL value of 1.

```
No. Time      Source    Destination  Protocol Info
1   0.000000  10.0.1.11 10.0.3.41    UDP      Source port: 53528
Destination port: 33435
```

The first hop in the route, which is PC2, receives the packet and decrements the TTL value. In this case, the TTL value is decremented to zero. As a result, the packet is dropped and an ICMP Time-to-live exceeded exception is sent to PC1 by PC2.

```
No. Time      Source    Destination  Protocol Info
2   0.000064  10.0.1.21 10.0.1.11    ICMP     Time-to-live
exceeded (Time to live exceeded in transit)
```

Traceroute sends the same UDP packets with the same TTL 3 times for each hop. The average round trip time can be calculated by averaging the delivery time for the 3 attempts. In addition, the port numbers of the UDP requests increments starting from 33435. This allows *traceroute* to keep track of which outgoing packet corresponds to the returning packet by checking if the port numbers match. After the first 3 attempts, the TTL value is incremented to 2. The new packets go through PC2 but is dropped at the second hop, Router1.

```
No. Time      Source    Destination  Protocol Info
7   0.003046  10.0.1.11 10.0.3.41    UDP      Source port: 53528
Destination port: 33438
No. Time      Source    Destination  Protocol Info
8   0.003673  10.0.2.1  10.0.1.11    ICMP     Time-to-live
exceeded (Time to live exceeded in transit)
```

Traceroute uses the returned ICMP time exceeded messages to build a list of routers that packets traverse, until the destination is reached and returns an ICMP Destination unreachable message.

```
No. Time      Source    Destination  Protocol Info
13  0.005394  10.0.1.11 10.0.3.41    UDP      Source port: 53528
Destination port: 33441
No. Time      Source    Destination  Protocol Info
14  0.005664  10.0.3.41 10.0.1.11    ICMP     Destination
unreachable (Port unreachable)
```

Complete traffic captured by *ethereal*

```
No. Time      Source    Destination  Protocol Info
1   0.000000  10.0.1.11 10.0.3.41    UDP      Source port: 53528
Destination port: 33435
Frame 1 (52 bytes on wire, 52 bytes captured)
Ethernet II, Src: LinksysG_7b:4d:1d (00:04:5a:7b:4d:1d), Dst:
LinksysG_7a:c8:94 (00:04:5a:7a:c8:94)
Internet Protocol, Src: 10.0.1.11 (10.0.1.11), Dst: 10.0.3.41
(10.0.3.41)
User Datagram Protocol, Src Port: 53528 (53528), Dst Port: 33435
(33435)
```

```
Data (10 bytes)
0000  01 01 46 bb ff 57 46 7a 00 00                     ..F..WFz..

No. Time      Source    Destination  Protocol Info
2   0.000064  10.0.1.21 10.0.1.11    ICMP     Time-to-live
exceeded (Time to live exceeded in transit)
Frame 2 (80 bytes on wire, 80 bytes captured)
Ethernet II, Src: LinksysG_7a:c8:94 (00:04:5a:7a:c8:94), Dst:
LinksysG_7b:4d:1d (00:04:5a:7b:4d:1d)
Internet Protocol, Src: 10.0.1.21 (10.0.1.21), Dst: 10.0.1.11
(10.0.1.11)
Internet Control Message Protocol

No. Time      Source    Destination  Protocol Info
3   0.002340  10.0.1.11 10.0.3.41    UDP      Source port: 53528
Destination port: 33436
Frame 3 (52 bytes on wire, 52 bytes captured)
Ethernet II, Src: LinksysG_7b:4d:1d (00:04:5a:7b:4d:1d), Dst:
LinksysG_7a:c8:94 (00:04:5a:7a:c8:94)
Internet Protocol, Src: 10.0.1.11 (10.0.1.11), Dst: 10.0.3.41
(10.0.3.41)
User Datagram Protocol, Src Port: 53528 (53528), Dst Port: 33436
(33436)
Data (10 bytes)
0000  02 01 46 bb ff 57 94 83 00 00                     ..F..W....

No. Time      Source    Destination  Protocol Info
4   0.002406  10.0.1.21 10.0.1.11    ICMP     Time-to-live
exceeded (Time to live exceeded in transit)
Frame 4 (80 bytes on wire, 80 bytes captured)
Ethernet II, Src: LinksysG_7a:c8:94 (00:04:5a:7a:c8:94), Dst:
LinksysG_7b:4d:1d (00:04:5a:7b:4d:1d)
Internet Protocol, Src: 10.0.1.21 (10.0.1.21), Dst: 10.0.1.11
(10.0.1.11)
Internet Control Message Protocol

No. Time      Source    Destination  Protocol Info
5   0.002599  10.0.1.11 10.0.3.41    UDP      Source port: 53528
Destination port: 33437
Frame 5 (52 bytes on wire, 52 bytes captured)
Ethernet II, Src: LinksysG_7b:4d:1d (00:04:5a:7b:4d:1d), Dst:
LinksysG_7a:c8:94 (00:04:5a:7a:c8:94)
Internet Protocol, Src: 10.0.1.11 (10.0.1.11), Dst: 10.0.3.41
(10.0.3.41)
User Datagram Protocol, Src Port: 53528 (53528), Dst Port: 33437
(33437)
```

```
Data (10 bytes)
0000  03 01 46 bb ff 57 9a 84 00 00                     ..F..W....

No. Time      Source    Destination  Protocol Info
6   0.002662  10.0.1.21 10.0.1.11    ICMP     Time-to-live
exceeded (Time to live exceeded in transit)
Frame 6 (80 bytes on wire, 80 bytes captured)
Ethernet II, Src: LinksysG_7a:c8:94 (00:04:5a:7a:c8:94), Dst:
LinksysG_7b:4d:1d (00:04:5a:7b:4d:1d)
Internet Protocol, Src: 10.0.1.21 (10.0.1.21), Dst: 10.0.1.11
(10.0.1.11)
Internet Control Message Protocol

No. Time      Source    Destination  Protocol Info
7   0.003046  10.0.1.11 10.0.3.41    UDP      Source port: 53528
Destination port: 33438
Frame 7 (52 bytes on wire, 52 bytes captured)
Ethernet II, Src: LinksysG_7b:4d:1d (00:04:5a:7b:4d:1d), Dst:
LinksysG_7a:c8:94 (00:04:5a:7a:c8:94)
Internet Protocol, Src: 10.0.1.11 (10.0.1.11), Dst: 10.0.3.41
(10.0.3.41)
User Datagram Protocol, Src Port: 53528 (53528), Dst Port: 33438
(33438)
Data (10 bytes)
0000  04 02 46 bb ff 57 57 86 00 00                     ..F..WW...

No. Time      Source    Destination  Protocol Info
8   0.003673  10.0.2.1  10.0.1.11    ICMP     Time-to-live
exceeded (Time to live exceeded in transit)
Frame 8 (70 bytes on wire, 70 bytes captured)
Ethernet II, Src: LinksysG_7a:c8:94 (00:04:5a:7a:c8:94), Dst:
LinksysG_7b:4d:1d (00:04:5a:7b:4d:1d)
Internet Protocol, Src: 10.0.2.1 (10.0.2.1), Dst: 10.0.1.11
(10.0.1.11)
Internet Control Message Protocol

No. Time      Source    Destination  Protocol Info
9   0.004075  10.0.1.11 10.0.3.41    UDP      Source port: 53528
Destination port: 33439
Frame 9 (52 bytes on wire, 52 bytes captured)
Ethernet II, Src: LinksysG_7b:4d:1d (00:04:5a:7b:4d:1d), Dst:
LinksysG_7a:c8:94 (00:04:5a:7a:c8:94)
Internet Protocol, Src: 10.0.1.11 (10.0.1.11), Dst: 10.0.3.41
(10.0.3.41)
User Datagram Protocol, Src Port: 53528 (53528), Dst Port: 33439
(33439)
```

```
Data (10 bytes)
0000  05 02 46 bb ff 57 5d 8a 00 00                     ..F..W]...

No. Time      Source    Destination  Protocol Info
10  0.004550  10.0.2.1  10.0.1.11    ICMP     Time-to-live
exceeded (Time to live exceeded in transit)
Frame 10 (70 bytes on wire, 70 bytes captured)
Ethernet II, Src: LinksysG_7a:c8:94 (00:04:5a:7a:c8:94), Dst:
LinksysG_7b:4d:1d (00:04:5a:7b:4d:1d)
Internet Protocol, Src: 10.0.2.1 (10.0.2.1), Dst: 10.0.1.11
(10.0.1.11)
Internet Control Message Protocol

No. Time      Source    Destination  Protocol Info
11  0.004723  10.0.1.11 10.0.3.41    UDP      Source port: 53528
Destination port: 33440
Frame 11 (52 bytes on wire, 52 bytes captured)
Ethernet II, Src: LinksysG_7b:4d:1d (00:04:5a:7b:4d:1d), Dst:
LinksysG_7a:c8:94 (00:04:5a:7a:c8:94)
Internet Protocol, Src: 10.0.1.11 (10.0.1.11), Dst: 10.0.3.41
(10.0.3.41)
User Datagram Protocol, Src Port: 53528 (53528), Dst Port: 33440
(33440)
Data (10 bytes)
0000  06 02 46 bb ff 57 e9 8c 00 00                     ..F..W....

No. Time      Source    Destination  Protocol Info
12  0.005218  10.0.2.1  10.0.1.11    ICMP     Time-to-live
exceeded (Time to live exceeded in transit)
Frame 12 (70 bytes on wire, 70 bytes captured)
Ethernet II, Src: LinksysG_7a:c8:94 (00:04:5a:7a:c8:94), Dst:
LinksysG_7b:4d:1d (00:04:5a:7b:4d:1d)
Internet Protocol, Src: 10.0.2.1 (10.0.2.1), Dst: 10.0.1.11
(10.0.1.11)
Internet Control Message Protocol

No. Time      Source    Destination  Protocol Info
13  0.005394  10.0.1.11 10.0.3.41    UDP      Source port: 53528
Destination port: 33441
Frame 13 (52 bytes on wire, 52 bytes captured)
Ethernet II, Src: LinksysG_7b:4d:1d (00:04:5a:7b:4d:1d), Dst:
LinksysG_7a:c8:94 (00:04:5a:7a:c8:94)
Internet Protocol, Src: 10.0.1.11 (10.0.1.11), Dst: 10.0.3.41
(10.0.3.41)
User Datagram Protocol, Src Port: 53528 (53528), Dst Port: 33441
(33441)
```

```
Data (10 bytes)
0000  07 03 46 bb ff 57 88 8f 00 00                     ..F..W....

No. Time      Source    Destination  Protocol Info
14  0.005664  10.0.3.41 10.0.1.11    ICMP     Destination
unreachable (Port unreachable)
Frame 14 (80 bytes on wire, 80 bytes captured)
Ethernet II, Src: LinksysG_7a:c8:94 (00:04:5a:7a:c8:94), Dst:
LinksysG_7b:4d:1d (00:04:5a:7b:4d:1d)
Internet Protocol, Src: 10.0.3.41 (10.0.3.41), Dst: 10.0.1.11
(10.0.1.11)
Internet Control Message Protocol

No. Time      Source    Destination  Protocol Info
15  0.006090  10.0.1.11 10.0.3.41    UDP      Source port: 53528
Destination port: 33442
Frame 15 (52 bytes on wire, 52 bytes captured)
Ethernet II, Src: LinksysG_7b:4d:1d (00:04:5a:7b:4d:1d), Dst:
LinksysG_7a:c8:94 (00:04:5a:7a:c8:94)
Internet Protocol, Src: 10.0.1.11 (10.0.1.11), Dst: 10.0.3.41
(10.0.3.41)
User Datagram Protocol, Src Port: 53528 (53528), Dst Port: 33442
(33442)
Data (10 bytes)
0000  08 03 46 bb ff 57 3c 92 00 00                     ..F..W<...

No. Time      Source    Destination  Protocol Info
16  0.006272  10.0.3.41 10.0.1.11    ICMP     Destination
unreachable (Port unreachable)
Frame 16 (80 bytes on wire, 80 bytes captured)
Ethernet II, Src: LinksysG_7a:c8:94 (00:04:5a:7a:c8:94), Dst:
LinksysG_7b:4d:1d (00:04:5a:7b:4d:1d)
Internet Protocol, Src: 10.0.3.41 (10.0.3.41), Dst: 10.0.1.11
(10.0.1.11)
Internet Control Message Protocol

No. Time      Source    Destination  Protocol Info
17  0.006447  10.0.1.11 10.0.3.41    UDP      Source port: 53528
Destination port: 33443
Frame 17 (52 bytes on wire, 52 bytes captured)
Ethernet II, Src: LinksysG_7b:4d:1d (00:04:5a:7b:4d:1d), Dst:
LinksysG_7a:c8:94 (00:04:5a:7a:c8:94)
Internet Protocol, Src: 10.0.1.11 (10.0.1.11), Dst: 10.0.3.41
(10.0.3.41)
User Datagram Protocol, Src Port: 53528 (53528), Dst Port: 33443
(33443)
```

```
Data (10 bytes)
0000  09 03 46 bb ff 57 a4 93 00 00                    ..F..W....

No. Time      Source    Destination  Protocol Info
18  0.006623  10.0.3.41 10.0.1.11    ICMP     Destination
unreachable (Port unreachable)
Frame 18 (80 bytes on wire, 80 bytes captured)
Ethernet II, Src: LinksysG_7a:c8:94 (00:04:5a:7a:c8:94), Dst:
LinksysG_7b:4d:1d (00:04:5a:7b:4d:1d)
Internet Protocol, Src: 10.0.3.41 (10.0.3.41), Dst: 10.0.1.11
(10.0.1.11)
Internet Control Message Protocol
```

Routing table

```
[root@PC1 root]# netstat -rn
Kernel IP routing table
Destination  Gateway    Genmask         Flags MSS Window irtt Iface
10.0.2.22    10.0.1.21  255.255.255.255 UGH   0   0      0   eth0
10.0.2.1     10.0.1.21  255.255.255.255 UGH   0   0      0   eth0
10.0.3.41    10.0.1.21  255.255.255.255 UGH   0   0      0   eth0
10.0.3.1     10.0.1.21  255.255.255.255 UGH   0   0      0   eth0
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

[root@PC2 root]# netstat -rn
Kernel IP routing table
Destination  Gateway    Genmask         Flags MSS Window irtt Iface
10.0.3.41    10.0.2.1   255.255.255.255 UGH   0   0      0   eth0
10.0.3.1     10.0.2.1   255.255.255.255 UGH   0   0      0   eth0
10.0.1.0     0.0.0.0    255.255.255.0   U     0   0      0   eth0
10.0.2.0     0.0.0.0    255.255.255.0   U     0   0      0   eth0
10.0.3.0     10.0.2.1   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

[root@PC4 root]# netstat -rn
Kernel IP routing table
Destination  Gateway    Genmask         Flags MSS Window irtt Iface
10.0.2.22    10.0.3.1   255.255.255.255 UGH   0   0      0    eth0
10.0.1.11    10.0.3.1   255.255.255.255 UGH   0   0      0    eth0
10.0.1.21    10.0.2.1   255.255.255.255 UGH   0   0      0    eth0
10.0.1.0     10.0.2.1   255.255.255.0   UG    0   0      0    eth0
10.0.2.0     10.0.2.1   255.255.255.0   UG    0   0      0    eth0
```

```
10.0.3.0     0.0.0.0    255.255.255.0   U     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
Router1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1
- OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
level-2
ia - IS-IS inter area, * - candidate default, U - per-user static
route
o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
     10.0.0.0/24 is subnetted, 3 subnets
C       10.0.2.0 is directly connected, FastEthernet0/0
C       10.0.3.0 is directly connected, FastEthernet0/1
S       10.0.1.0 [1/0] via 10.0.2.0
```

Exercise 3(C)

1. **Determine the destination and source addresses in the Ethernet and IP headers for the ICMP Echo Request message at PC1.**

The following is the ICMP Echo Request messages captured at PC1.

```
No. Time      Source    Destination  Protocol Info
3   0.000100  10.0.1.11 10.0.3.41    ICMP     Echo (ping) request
Frame 3 (98 bytes on wire, 98 bytes captured)
Ethernet II, Src: LinksysG_7b:4d:1d (00:04:5a:7b:4d:1d), Dst:
LinksysG_7a:c8:94 (00:04:5a:7a:c8:94)
Internet Protocol, Src: 10.0.1.11 (10.0.1.11), Dst: 10.0.3.41
(10.0.3.41)
Internet Control Message Protocol

No. Time      Source    Destination  Protocol Info
5   0.999851  10.0.1.11 10.0.3.41    ICMP     Echo (ping) request
Frame 5 (98 bytes on wire, 98 bytes captured)
Ethernet II, Src: LinksysG_7b:4d:1d (00:04:5a:7b:4d:1d), Dst:
LinksysG_7a:c8:94 (00:04:5a:7a:c8:94)
Internet Protocol, Src: 10.0.1.11 (10.0.1.11), Dst: 10.0.3.41
(10.0.3.41)
Internet Control Message Protocol

No. Time      Source    Destination  Protocol Info
7   1.999690  10.0.1.11 10.0.3.41    ICMP     Echo (ping) request
Frame 7 (98 bytes on wire, 98 bytes captured)
```

```
Ethernet II, Src: LinksysG_7b:4d:1d (00:04:5a:7b:4d:1d), Dst:
LinksysG_7a:c8:94 (00:04:5a:7a:c8:94)
Internet Protocol, Src: 10.0.1.11 (10.0.1.11), Dst: 10.0.3.41
(10.0.3.41)
Internet Control Message Protocol

No. Time      Source    Destination  Protocol Info
9   2.999528  10.0.1.11 10.0.3.41    ICMP     Echo (ping) request
Frame 9 (98 bytes on wire, 98 bytes captured)
Ethernet II, Src: LinksysG_7b:4d:1d (00:04:5a:7b:4d:1d), Dst:
LinksysG_7a:c8:94 (00:04:5a:7a:c8:94)
Internet Protocol, Src: 10.0.1.11 (10.0.1.11), Dst: 10.0.3.41
(10.0.3.41)
Internet Control Message Protocol

No. Time      Source    Destination  Protocol Info
11  3.999368  10.0.1.11 10.0.3.41    ICMP     Echo (ping) request
Frame 11 (98 bytes on wire, 98 bytes captured)
Ethernet II, Src: LinksysG_7b:4d:1d (00:04:5a:7b:4d:1d), Dst:
LinksysG_7a:c8:94 (00:04:5a:7a:c8:94)
Internet Protocol, Src: 10.0.1.11 (10.0.1.11), Dst: 10.0.3.41
(10.0.3.41)
Internet Control Message Protocol
```

The source address in the Ethernet header is LinksysG_7b:4d:1d(00:04:5a:7b:4d:1d).
The destination address in the Ethernet header is LinksysG_7a:c8:94 (00:04:5a:7a:c8:94)
The source address in the IP header is 10.0.1.11
The destination address in the IP header is 10.0.3.41

2. **Determine the destination and source addresses in the Ethernet and IP headers for the ICMP Echo Request message at PC4.**

The following is the ICMP Echo Request messages captured at PC4.

```
No. Time      Source    Destination  Protocol Info
1   0.000000  10.0.1.11 10.0.3.41    ICMP     Echo (ping) request
Frame 1 (98 bytes on wire, 98 bytes captured)
Ethernet II, Src: 00:1c:58:45:33:c1 (00:1c:58:45:33:c1), Dst:
LinksysG_80:93:f3 (00:04:5a:80:93:f3)
Internet Protocol, Src: 10.0.1.11 (10.0.1.11), Dst: 10.0.3.41
(10.0.3.41)
Internet Control Message Protocol

No. Time      Source    Destination  Protocol Info
3   0.994994  10.0.1.11 10.0.3.41    ICMP     Echo (ping) request
Frame 3 (98 bytes on wire, 98 bytes captured)
Ethernet II, Src: 00:1c:58:45:33:c1 (00:1c:58:45:33:c1), Dst:
LinksysG_80:93:f3 (00:04:5a:80:93:f3)
```

```
Internet Protocol, Src: 10.0.1.11 (10.0.1.11), Dst: 10.0.3.41
(10.0.3.41)
Internet Control Message Protocol

No. Time      Source    Destination  Protocol Info
5   1.994840  10.0.1.11 10.0.3.41    ICMP     Echo (ping) request
Frame 5 (98 bytes on wire, 98 bytes captured)
Ethernet II, Src: 00:1c:58:45:33:c1 (00:1c:58:45:33:c1), Dst:
LinksysG_80:93:f3 (00:04:5a:80:93:f3)
Internet Protocol, Src: 10.0.1.11 (10.0.1.11), Dst: 10.0.3.41
(10.0.3.41)
Internet Control Message Protocol

No. Time      Source    Destination  Protocol Info
7   2.994671  10.0.1.11 10.0.3.41    ICMP     Echo (ping) request
Frame 7 (98 bytes on wire, 98 bytes captured)
Ethernet II, Src: 00:1c:58:45:33:c1 (00:1c:58:45:33:c1), Dst:
LinksysG_80:93:f3 (00:04:5a:80:93:f3)
Internet Protocol, Src: 10.0.1.11 (10.0.1.11), Dst: 10.0.3.41
(10.0.3.41)
Internet Control Message Protocol

No. Time      Source    Destination  Protocol Info
9   3.994504  10.0.1.11 10.0.3.41    ICMP     Echo (ping) request
Frame 9 (98 bytes on wire, 98 bytes captured)
Ethernet II, Src: 00:1c:58:45:33:c1 (00:1c:58:45:33:c1), Dst:
LinksysG_80:93:f3 (00:04:5a:80:93:f3)
Internet Protocol, Src: 10.0.1.11 (10.0.1.11), Dst: 10.0.3.41
(10.0.3.41)
Internet Control Message Protocol
```

The source address in the Ethernet header is 00:1c:58:45:33:c1.
The destination address in the Ethernet header is 00:04:5a:80:93:f3
The source address in the IP header is 10.0.1.11
The destination address in the IP header is 10.0.3.41

3. **Explain how the source and destination addresses are changed when a datagram is forwarded by a router.**

IP address for source and destination will remain the same throughout the process of forwarding. The ethernet addresses are changing each time the packet passes a hop, because ethernet addresses only indicate the current hop and the next hop.

Exercise 3(D)

Use the saved output to indicate the number of matches for each of the preceding IP addresses. Explain how PC1 resolve multiple matches on the routing table. Include only relevant output data in your report to support your analysis of the data.

According to the routing table, multiple matches can be found for addresses 10.0.3.9, 10.0.3.14. In addition, one match is found for address 10.0.4.1

Routing table matches for 10.0.3.9

- 10.0.3.9/32, Gatway 10.0.1.81
- 10.0.3.0/24, Gatway 10.0.1.21
- 10.0.0.0/16, Gatway 10.0.1.71

Routing table matches for 10.0.3.14

- 10.0.3.0/24, Gatway 10.0.1.21
- 10.0.0.0/16, Gatway 10.0.1.71

Routing table matches for 10.0.4.1

- 10.0.0.0/16, Gatway 10.0.1.71

The following is the traffic captured by ethereal when command *ping -c 1 10.0.3.9* is issued on PC1.

```
No. Time      Source             Destination  Protocol Info
1   0.000000  LinksysG_7b:4d:1d  Broadcast    ARP      Who has
10.0.1.81?  Tell 10.0.1.11
No. Time      Source             Destination  Protocol Info
2   0.999915  LinksysG_7b:4d:1d  Broadcast    ARP      Who has
10.0.1.81?  Tell 10.0.1.11
No. Time      Source             Destination  Protocol Info
3   1.999828  LinksysG_7b:4d:1d  Broadcast    ARP      Who has
10.0.1.81?  Tell 10.0.1.11
```

The ARP request is repeated 3 times as the address 10.0.1.81 does not exist. There is also multiple match for address 10.0.3.9 in routing table. PC1 sends ARP packets following the route for entry 10.0.3.9/32, whcih is the longest match. Similarly, when command *ping -c 1 10.0.3.14* is issued on PC1, the packets follow the route specified in entry 10.0.3.0/24, which is the longest match.

```
No. Time      Source             Destination  Protocol Info
4   45.860024 LinksysG_7b:4d:1d  Broadcast    ARP      Who has
10.0.1.21?  Tell 10.0.1.11
```

The captured data clearly shows that the longest match is preferred if multiple entries match in the routing table.

Data captured: PC1 routing table

```
[root@PC1 root]# netstat -rn
Kernel IP routing table
Destination  Gateway    Genmask        Flags MSS Window irtt Iface
```

```
10.0.3.9     10.0.1.81  255.255.255.255 UGH   0   0      0    eth0
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
10.0.0.0     10.0.1.71  255.255.0.0     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
```

Data captured: *ethereal*

```
No. Time      Source             Destination  Protocol Info
1   0.000000  LinksysG_7b:4d:1d  Broadcast    ARP      Who has
10.0.1.81?  Tell 10.0.1.11
Frame 1 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: LinksysG_7b:4d:1d (00:04:5a:7b:4d:1d), Dst:
Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

No. Time      Source             Destination  Protocol Info
2   0.999915  LinksysG_7b:4d:1d  Broadcast    ARP      Who has
10.0.1.81?  Tell 10.0.1.11
Frame 2 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: LinksysG_7b:4d:1d (00:04:5a:7b:4d:1d), Dst:
Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

No. Time      Source             Destination  Protocol Info
3   1.999828  LinksysG_7b:4d:1d  Broadcast    ARP      Who has
10.0.1.81?  Tell 10.0.1.11
Frame 3 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: LinksysG_7b:4d:1d (00:04:5a:7b:4d:1d), Dst:
Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

No. Time      Source             Destination  Protocol Info
4   45.860024 LinksysG_7b:4d:1d  Broadcast    ARP      Who has
10.0.1.21?  Tell 10.0.1.11
Frame 4 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: LinksysG_7b:4d:1d (00:04:5a:7b:4d:1d), Dst:
Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

No. Time      Source             Destination  Protocol Info
5   45.860109 LinksysG_7a:c8:94 LinksysG_7b:4d:1d ARP 10.0.1.21 is
at 00:04:5a:7a:c8:94
Frame 5 (60 bytes on wire, 60 bytes captured)
```

```
Ethernet II, Src: LinksysG_7a:c8:94 (00:04:5a:7a:c8:94), Dst:
LinksysG_7b:4d:1d (00:04:5a:7b:4d:1d)
Address Resolution Protocol (reply)

No. Time      Source     Destination  Protocol Info
6 45.860123   10.0.1.11  10.0.3.14    ICMP     Echo (ping) request
Frame 6 (98 bytes on wire, 98 bytes captured)
Ethernet II, Src: LinksysG_7b:4d:1d (00:04:5a:7b:4d:1d), Dst:
LinksysG_7a:c8:94 (00:04:5a:7a:c8:94)
Internet Protocol, Src: 10.0.1.11 (10.0.1.11), Dst: 10.0.3.14
(10.0.3.14)
Internet Control Message Protocol

No. Time      Source             Destination  Protocol Info
7   81.288948 LinksysG_7b:4d:1d  Broadcast    ARP      Who has
10.0.1.71?  Tell 10.0.1.11
Frame 7 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: LinksysG_7b:4d:1d (00:04:5a:7b:4d:1d), Dst:
Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

No. Time      Source             Destination  Protocol Info
8   82.288863 LinksysG_7b:4d:1d  Broadcast    ARP      Who has
10.0.1.71?  Tell 10.0.1.11
Frame 8 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: LinksysG_7b:4d:1d (00:04:5a:7b:4d:1d), Dst:
Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

No. Time      Source             Destination  Protocol Info
9   83.288776 LinksysG_7b:4d:1d  Broadcast    ARP      Who has
10.0.1.71?  Tell 10.0.1.11
Frame 9 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: LinksysG_7b:4d:1d (00:04:5a:7b:4d:1d), Dst:
Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
```

Exercise 3(E)

1. What is the output on PC1 when ping command is issued?

```
[root@PC1 root]# ping -c 5 10.0.10.110
PING 10.0.10.110 (10.0.10.110) 56(84) bytes of data.
From 10.0.2.1 icmp_seq=1 Destination Host Unreachable
From 10.0.2.1 icmp_seq=2 Destination Host Unreachable
From 10.0.2.1 icmp_seq=3 Destination Host Unreachable
From 10.0.2.1 icmp_seq=4 Destination Host Unreachable
```

```
From 10.0.2.1 icmp_seq=5 Destination Host Unreachable

--- 10.0.10.110 ping statistics ---
5 packets transmitted, 0 received, +5 errors, 100% packet loss,
time 4012ms
```

2. Determine how for the ICMP Echo Request message travel?

According to the traffic captured by ethereal, the ICMP request travels as far as Router 1. Once the command *ping -c 5 10.0.10.110* is issued on PC1, the packets are sent to the default gateway, PC2, as there is no entry for 10.0.10.110 in PC1's routing table. Similarly, the the packets are forwarded to the default gateway, Router1, once they arrive at PC2. The router is unable to resolve the next hop for packets going to 10.0.10.110. As a result, a ICMP destination unreachable message is sent by Router1.

The following is a ICMP echo request packet sent by PC1, captured on PC1

```
No. Time      Source    Destination  Protocol Info
3   0.000110  10.0.1.11 10.0.10.110  ICMP     Echo (ping) request
Frame 3 (98 bytes on wire, 98 bytes captured)
Ethernet II, Src: LinksysG_7b:4d:1d (00:04:5a:7b:4d:1d), Dst:
LinksysG_7a:c8:94 (00:04:5a:7a:c8:94)
Internet Protocol, Src: 10.0.1.11 (10.0.1.11), Dst: 10.0.10.110
(10.0.10.110)
Internet Control Message Protocol
```

According to the Ethernet header, the next hop of this packet is 00:04:5a:7a:c8:94, which is PC2. The same request is forwarded by PC2, as captured on PC2 by ethereal

```
No. Time      Source    Destination  Protocol Info
8   11.608334 10.0.1.11 10.0.10.110  ICMP     Echo (ping) request
Frame 8 (100 bytes on wire, 100 bytes captured)
Linux cooked capture
Internet Protocol, Src: 10.0.1.11 (10.0.1.11), Dst: 10.0.10.110
(10.0.10.110)
Internet Control Message Protocol
```

An ICMP destination unreachable error is return to PC2 by Router1, indicating Router1 is the last hop of the ICMP echo request

```
No. Time      Source    Destination  Protocol Info
9   11.609024 10.0.2.1  10.0.1.11    ICMP     Destination
unreachable (Host unreachable)
Frame 9 (72 bytes on wire, 72 bytes captured)
Linux cooked capture
Internet Protocol, Src: 10.0.2.1 (10.0.2.1), Dst: 10.0.1.11
(10.0.1.11)
Internet Control Message Protocol
```

3. Which, if any, ICMP Echo Reply message returns to PC1?

There is no ICMP Echo Reply message returned to PC1. However, an ICMP destination unreachable packet is returned to PC1 for each ICMP echo request sent.

```
No. Time      Source    Destination  Protocol Info
```

```
10  3.000663  10.0.2.1  10.0.1.11    ICMP     Destination
unreachable (Host unreachable)
Frame 10 (70 bytes on wire, 70 bytes captured)
Ethernet II, Src: LinksysG_7a:c8:94 (00:04:5a:7a:c8:94), Dst:
LinksysG_7b:4d:1d (00:04:5a:7b:4d:1d)
Internet Protocol, Src: 10.0.2.1 (10.0.2.1), Dst: 10.0.1.11
(10.0.1.11)
Internet Control Message Protocol
```

Exercise 4

Use the captured data to explain the outcome of the exercise. Use the data to explain how Proxy ARP allowed PC4 to communicate with PC1. Include only relevant data from your saved output.

PC1 (10.0..1.11/24) is not in the routing table or the ARP table of PC4 (10.0.3.41/8). However, PC4 believes that it is on the same network work (10.0.0.0) with PC1. Thus, an ARP request is sent out when the command *ping -c 2 10.0.1.11* is issued on PC4. Router1, whose Proxy ARP is enabled, receives the ARP request. According to its routing table, there is a path to deliver packets between Router1 and PC1. As a result, Router1 responds to the ARP request for PC1 with its own MAC address. This mechanism makes PC4 to believe that it is directly communicating with PC1 while the packets are actually routed to Router1, as shown in PC4's MAC table.

```
Address    HWtype  HWaddress           Flags Mask     Iface
10.0.1.11  ether   00:1C:58:45:33:C1   C              eth0
```

The traffic is captured by *ethereal* on PC4.

```
No. Time      Source            Destination  Protocol Info
1   0.000000  LinksysG_80:93:f3 Broadcast    ARP      Who has
10.0.1.11?  Tell 10.0.3.41
Frame 1 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: LinksysG_80:93:f3 (00:04:5a:80:93:f3), Dst:
Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
No. Time    Source            Destination  Protocol Info
2 0.000564  00:1c:58:45:33:c1 LinksysG_80:93:f3 ARP 10.0.1.11 is
at 00:1c:58:45:33:c1
Frame 2 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: 00:1c:58:45:33:c1 (00:1c:58:45:33:c1), Dst:
LinksysG_80:93:f3 (00:04:5a:80:93:f3)
Address Resolution Protocol (reply)
```

The ICMP echo requests from PC4 are routed through Router1 and PC2 in realistic. From PC4's point of view, the packets are directly delivered to PC1.The following is an ICMP echo request captured by *ethereal* on PC4. Note the Ethernet destination address matches the MAC address of PC1 in MAC table.

```
No. Time     Source     Destination  Protocol Info
```

```
3   0.000586 10.0.3.41  10.0.1.11    ICMP     Echo (ping) request
Frame 3 (98 bytes on wire, 98 bytes captured)
Ethernet II, Src: LinksysG_80:93:f3 (00:04:5a:80:93:f3), Dst:
00:1c:58:45:33:c1 (00:1c:58:45:33:c1)
Internet Protocol, Src: 10.0.3.41 (10.0.3.41), Dst: 10.0.1.11
(10.0.1.11)
Internet Control Message Protocol
```

The ICMP echo request packet is routed from Router1 to PC2, and is captured by *ethereal* on PC2.

```
No. Time      Source     Destination  Protocol Info
4   20.587249 10.0.3.41  10.0.1.11    ICMP     Echo (ping) request
Frame 4 (98 bytes on wire, 98 bytes captured)
Ethernet II, Src: 00:1c:58:45:33:c0 (00:1c:58:45:33:c0), Dst:
LinksysG_80:2a:d0 (00:04:5a:80:2a:d0)
Internet Protocol, Src: 10.0.3.41 (10.0.3.41), Dst: 10.0.1.11
(10.0.1.11)
Internet Control Message Protocol
```

PC2 forwards the packet to its final and real destination, PC1. The packet is captured by *ethereal* on PC1.

```
No. Time      Source     Destination  Protocol Info
1   0.000000  10.0.3.41  10.0.1.11    ICMP     Echo (ping) request
Frame 1 (98 bytes on wire, 98 bytes captured)
Ethernet II, Src: LinksysG_7a:c8:94 (00:04:5a:7a:c8:94), Dst:
LinksysG_7b:4d:1d (00:04:5a:7b:4d:1d)
Internet Protocol, Src: 10.0.3.41 (10.0.3.41), Dst: 10.0.1.11
(10.0.1.11)
Internet Control Message Protocol
```

To send an ICMP echo reply packet back to PC4, PC1 checks its routing table and realizes that the packets need to be routed through PC2 eth0. The destination MAC address is PC2 eth0 in the Ethernet header of the ICMP echo reply packets captured by *ethereal* on PC1.

```
No. Time      Source     Destination  Protocol Info
4   0.001187  10.0.1.11  10.0.3.41    ICMP     Echo (ping) reply
Frame 4 (98 bytes on wire, 98 bytes captured)
Ethernet II, Src: LinksysG_7b:4d:1d (00:04:5a:7b:4d:1d), Dst:
LinksysG_7a:c8:94 (00:04:5a:7a:c8:94)
Internet Protocol, Src: 10.0.1.11 (10.0.1.11), Dst: 10.0.3.41
(10.0.3.41)
Internet Control Message Protocol
```

When the ICMP echo reply packets arrive at PC2, they are forwarded to Router1 F0/0 according to PC2's routing table. This is demonstrated by traffic captured by *ethereal* on PC2.

```
No. Time      Source     Destination  Protocol Info
5   20.588621 10.0.1.11  10.0.3.41    ICMP     Echo (ping) reply
Frame 5 (98 bytes on wire, 98 bytes captured)
```

```
Ethernet II, Src: LinksysG_80:2a:d0 (00:04:5a:80:2a:d0), Dst:
00:1c:58:45:33:c0 (00:1c:58:45:33:c0)
Internet Protocol, Src: 10.0.1.11 (10.0.1.11), Dst: 10.0.3.41
(10.0.3.41)
Internet Control Message Protocol
```

The ICMP echo reply packet is finally routed through Router1 to arrive at PC4.

```
No. Time      Source     Destination  Protocol Info
4   0.002325  10.0.1.11  10.0.3.41    ICMP     Echo (ping) reply
Frame 4 (98 bytes on wire, 98 bytes captured)
Ethernet II, Src: 00:1c:58:45:33:c1 (00:1c:58:45:33:c1), Dst:
LinksysG_80:93:f3 (00:04:5a:80:93:f3)
Internet Protocol, Src: 10.0.1.11 (10.0.1.11), Dst: 10.0.3.41
(10.0.3.41)
Internet Control Message Protocol
```

If the Proxy ARP is disabled on Router1, PC4 will not be able to resolve the MAC address of PC1. PC4 believes it is on the same network with PC1. It sends ARP request broadcast within its network. However, the broadcast will never reach PC1.

Exercise 5

1. **Is there a difference between the contents of the routing table and the routing cache immediately after the ICMP route redirect message?**

The content of the routing table remains the same. The content of the routing cache is changed after the ICMP route redirect message. The following entry is added.

```
Source     Destination  Gateway    Flags Metric Ref  Use Iface
10.0.2.10  10.0.3.10    10.0.2.2           0      0    1  eth0
```

2. **When you viewed the cache a few minutes later, what did you observe?**

The new entry introduced by the ICMP redirect message is removed.

3. **Describe how the ICMP route redirect works using the output you saved. Include only relevant data from your saved output to support your explanations.**

An intermediate router would inform the source router if a better path exists for sending the packet from the source to destination. As the captured data shows, when PC2 sends a packet to PC3 through Router1 while there is a better path(Router2), Router1 directs the packet to Router2 while sending back to PC2 an ICMP redirect message. The following is the traffic captured on *ethereal*

```
No. Time      Source             Destination       Protocol Info
1   0.000000  00:04:5a:7a:c6:6f  ff:ff:ff:ff:ff:ff ARP      Who
has 10.0.2.1?  Tell 10.0.2.10
Frame 1 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: 00:04:5a:7a:c6:6f (00:04:5a:7a:c6:6f), Dst:
ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

No. Time      Source             Destination       Protocol Info
```

```
2   0.000542  00:1c:58:7e:03:c1  00:04:5a:7a:c6:6f ARP
0.0.2.1 is at 00:1c:58:7e:03:c1
Frame 2 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: 00:1c:58:7e:03:c1 (00:1c:58:7e:03:c1), Dst:
00:04:5a:7a:c6:6f (00:04:5a:7a:c6:6f)
Address Resolution Protocol (reply)

No. Time      Source     Destination  Protocol Info
3   0.000563  10.0.2.10  10.0.3.10    ICMP     Echo (ping) request
Frame 3 (98 bytes on wire, 98 bytes captured)
Ethernet II, Src: 00:04:5a:7a:c6:6f (00:04:5a:7a:c6:6f), Dst:
00:1c:58:7e:03:c1 (00:1c:58:7e:03:c1)
Internet Protocol, Src: 10.0.2.10 (10.0.2.10), Dst: 10.0.3.10
(10.0.3.10)
Internet Control Message Protocol

No. Time     Source   Destination Protocol Info
4   0.001136 10.0.2.1 10.0.2.10   ICMP     Redirect (Redirect for
host)
Frame 4 (70 bytes on wire, 70 bytes captured)
Ethernet II, Src: 00:1c:58:7e:03:c1 (00:1c:58:7e:03:c1), Dst:
00:04:5a:7a:c6:6f (00:04:5a:7a:c6:6f)
Internet Protocol, Src: 10.0.2.1 (10.0.2.1), Dst: 10.0.2.10
(10.0.2.10)
Internet Control Message Protocol

No. Time      Source     Destination  Protocol Info
5   0.003391  10.0.3.10  10.0.2.10    ICMP     Echo (ping) reply
```

After receiving the ICMP redirect message, PC2 update its routing cache. The following ICMP echo request packets are routed to Router2 instead of Router1. The following is the traffic captured on *ethereal*

```
No. Time      Source            Destination       Protocol Info
6   0.004002  00:04:5a:7a:c6:6f ff:ff:ff:ff:ff:ff ARP      Who has
10.0.2.2?  Tell 10.0.2.10
Frame 6 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: 00:04:5a:7a:c6:6f (00:04:5a:7a:c6:6f), Dst:
ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

No. Time      Source            Destination       Protocol Info
7   0.004390  00:1c:58:68:eb:89 00:04:5a:7a:c6:6f ARP     10.0.2.2
is at 00:1c:58:68:eb:89
Frame 7 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: 00:1c:58:68:eb:89 (00:1c:58:68:eb:89), Dst:
00:04:5a:7a:c6:6f (00:04:5a:7a:c6:6f)
Address Resolution Protocol (reply)
```

```
No. Time      Source     Destination  Protocol Info
8   0.995847  10.0.2.10  10.0.3.10    ICMP     Echo (ping) request
Frame 8 (98 bytes on wire, 98 bytes captured)
Ethernet II, Src: 00:04:5a:7a:c6:6f (00:04:5a:7a:c6:6f), Dst:
00:1c:58:7e:03:c1 (00:1c:58:7e:03:c1)
Internet Protocol, Src: 10.0.2.10 (10.0.2.10), Dst: 10.0.3.10
(10.0.3.10)
Internet Control Message Protocol

No. Time      Source     Destination  Protocol Info
9   0.996186  10.0.3.10  10.0.2.10    ICMP     Echo (ping) reply
Frame 9 (98 bytes on wire, 98 bytes captured)
Ethernet II, Src: 00:1c:58:68:eb:89 (00:1c:58:68:eb:89), Dst:
00:04:5a:7a:c6:6f (00:04:5a:7a:c6:6f)
Internet Protocol, Src: 10.0.3.10 (10.0.3.10), Dst: 10.0.2.10
(10.0.2.10)
Internet Control Message Protocol
```

4. **Explain how Router1, in the previous example, knows that datagrams destined to network 10.0.3.10 should be forwarded to 10.0.2.2?**

A static routing entry was built on Router1 indicates packets going to 10.0.3.0/24 should be routed to 10.0.2.2, which is Router2 F0/1. The ICMP echo request comes from host 10.0.2.10, which is in the same network of 10.0.2.2 and 10.0.2.1. The destination host of the packet is 10.0.3.10, which is in the network of 10.0.3.0. As a result, Router1 decides that all packets from PC2 to OC3 should be forwards to Router2. Since PC2 and Router2 are on the same network, Router1 sends out the ICMP redirect message to advise PC2 that it can directly deliver the packets to Router2.

Exercise 6

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

No, they have different TTL value. For example, the first ICMP packet has ‘ Time to live: 64’ and the second ICMP packet has ‘ Time to live: 61’. Since they have different TTL value, the header checksum is also different. The following are the 2 ICMP echo request packets captured by *ethereal*.

```
No. Time      Source     Destination  Protocol Info
1   0.000000  10.0.4.10  10.0.1.10    ICMP     Echo (ping) request
Frame 1 (98 bytes on wire, 98 bytes captured)
Ethernet II, Src: 00:04:5a:7b:21:cc (00:04:5a:7b:21:cc), Dst:
00:1c:58:45:33:18 (00:1c:58:45:33:18)
Internet Protocol version 4, Src: 10.0.4.10 (10.0.4.10), Dst:
10.0.1.10 (10.0.1.10)
     Version: 4
```

```
      Header Length: 20 bytes
      ......
      Fragment offset: 0
      Time to live: 64
      Protocol: ICMP (0x01)
Internet Control Message Protocol
      Type: 8 (Echo (ping) request)
      Code: 0
      ......
No. Time      Source     Destination  Protocol Info
2   0.002739  10.0.4.10  10.0.1.10    ICMP     Echo (ping) request
Frame 2 (98 bytes on wire, 98 bytes captured)
Ethernet II, Src: 00:04:5a:7b:21:cc (00:04:5a:7b:21:cc), Dst:
00:1c:58:45:33:18 (00:1c:58:45:33:18)
Internet Protocol version 4, Src: 10.0.4.10 (10.0.4.10), Dst:
10.0.1.10 (10.0.1.10)
      Version: 4
      Header Length: 20 bytes
      ......
      Fragment offset: 0
      Time to live: 61
      Protocol: ICMP (0x01)
Internet Control Message Protocol
      Type: 8 (Echo (ping) request)
      Code: 0
      ......
```

2. Why does the ICMP Echo message not loop forever in the network?

There is a TTL value defined for every ICMP echo request packet. The TTL value decrements by 1 when the packet is delivered to the next hop. The packet is dropped and the ICMP Time-to-live exceeded exception is sent when a packet arrives the next hop with a TTL value of 1. As a result, the ICMP echo message will not loop forever.