1. After you complete Steps 1-1

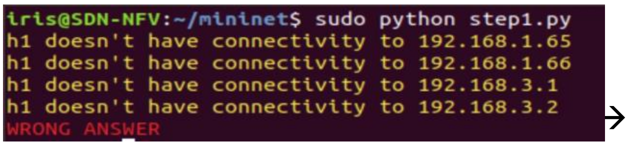
(a) Can h2 ping h3? Briefly explain why or why not. (5%)

Yes. Since they are in the same LAN.

(b) Can h2 ping h4? Briefly explain why or why not. (5%)

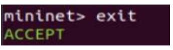
No. Since they are in the different LANs.

2. Complete topology.py so that all hosts, except h1, can ping one another. Take screenshot to show that your topology configuration is correct. (10%)



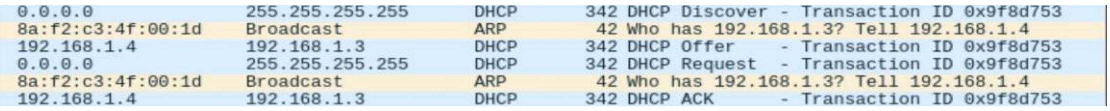
```
iris@SDN-NFV:~/mininet$ sudo python step1.py
h1 doesn't have connectivity to 192.168.1.65
h1 doesn't have connectivity to 192.168.1.66
h1 doesn't have connectivity to 192.168.3.1
h1 doesn't have connectivity to 192.168.3.2
WRONG ANSWER
```

→after enabling DHCP→

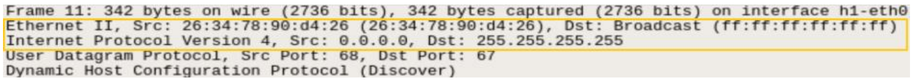
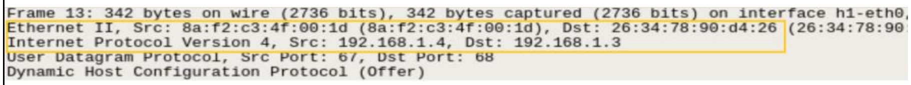
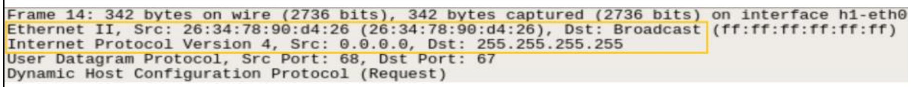
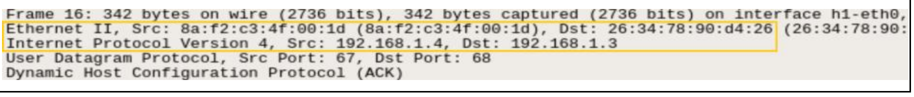


```
mininet> exit
ACCEPT
```

3. Capture DHCP messages and show the IPs and MACs (10%)



```
0.0.0.0              255.255.255.255      DHCP       342 DHCP Discover - Transaction ID 0x9f8d753
8a:f2:c3:4f:00:1d    Broadcast            ARP         42 Who has 192.168.1.3? Tell 192.168.1.4
192.168.1.4          192.168.1.3          DHCP       342 DHCP Offer    - Transaction ID 0x9f8d753
0.0.0.0              255.255.255.255      DHCP       342 DHCP Request  - Transaction ID 0x9f8d753
8a:f2:c3:4f:00:1d    Broadcast            ARP         42 Who has 192.168.1.3? Tell 192.168.1.4
192.168.1.4          192.168.1.3          DHCP       342 DHCP ACK      - Transaction ID 0x9f8d753
```

<table>
<tr><th></th><th>Src IP</th><th>Dst IP</th><th>Src MAC</th><th>Dst MAC</th></tr>
<tr><td rowspan="2">DHCP Discover</td><td>0.0.0.0</td><td>255.255.255.255</td><td><MAC of h1></td><td>ff : ff : ff : ff : ff : ff</td></tr>
<tr><td colspan="4">
Frame 11: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface h1-eth0
Ethernet II, Src: 26:34:78:90:d4:26 (26:34:78:90:d4:26), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Discover)</td></tr>
<tr><td rowspan="2">DHCP Offer</td><td>192.168.1.4</td><td>192.168.1.3</td><td><MAC of server></td><td><MAC of h1></td></tr>
<tr><td colspan="4">
Frame 13: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface h1-eth0,
Ethernet II, Src: 8a:f2:c3:4f:00:1d (8a:f2:c3:4f:00:1d), Dst: 26:34:78:90:d4:26 (26:34:78:90
Internet Protocol Version 4, Src: 192.168.1.4, Dst: 192.168.1.3
User Datagram Protocol, Src Port: 67, Dst Port: 68
Dynamic Host Configuration Protocol (Offer)</td></tr>
<tr><td rowspan="2">DHCP Request</td><td>0.0.0.0</td><td>255.255.255.255</td><td><MAC of h1></td><td>ff : ff : ff : ff : ff : ff</td></tr>
<tr><td colspan="4">
Frame 14: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface h1-eth0
Ethernet II, Src: 26:34:78:90:d4:26 (26:34:78:90:d4:26), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Request)</td></tr>
<tr><td rowspan="2">DHCP Ack</td><td>192.168.1.4</td><td>192.168.1.3</td><td><MAC of server></td><td><MAC of h1></td></tr>
<tr><td colspan="4">
Frame 16: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface h1-eth0,
Ethernet II, Src: 8a:f2:c3:4f:00:1d (8a:f2:c3:4f:00:1d), Dst: 26:34:78:90:d4:26 (26:34:78:90:
Internet Protocol Version 4, Src: 192.168.1.4, Dst: 192.168.1.3
User Datagram Protocol, Src Port: 67, Dst Port: 68
Dynamic Host Configuration Protocol (ACK)</td></tr>
</table>

4. Can hosts other than h1 acquire IP addresses from DHCP server? Briefly explain your answer. (5%)

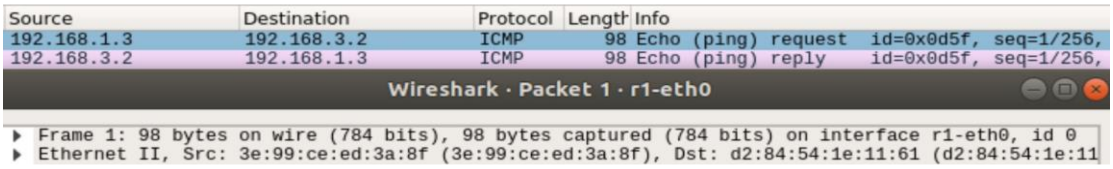
No, since they are not in the same LAN with DHCP server.

(The mechanism relies on broadcast, so the client can’t get IP from DHCP server if the server is not at the same LAN with the client unless using DHCP Relay/IP Helper.)

5. What does r1 do on the packets from h1 to h5, and h5 to h1, respectively? Capture packets to explain your answers. (5%)

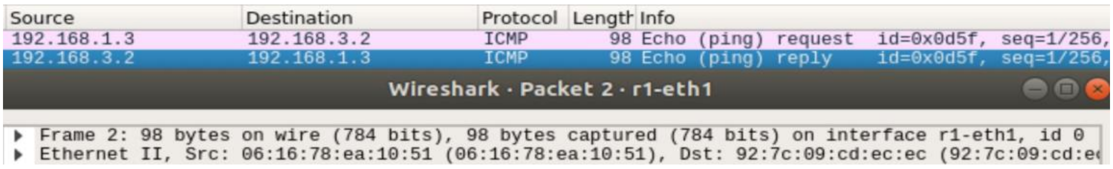
After checking routing table, r1 will forward the packets.

h1 to h5 : R1 pass the packet received from eth1 to eth0 and then forward it from eth0 to the next hop -- r2-eth1.



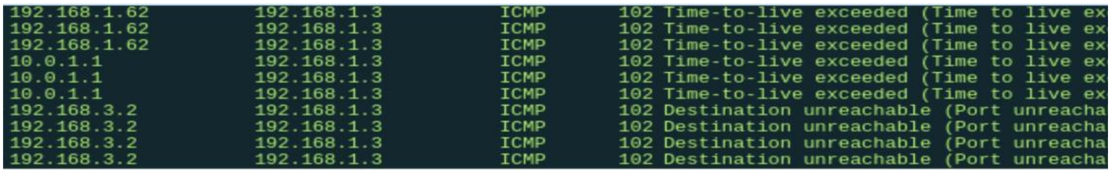
```
Source            Destination       Protocol Lengtł Info
192.168.1.3       192.168.3.2       ICMP         98 Echo (ping) request  id=0x0d5f, seq=1/256,
192.168.3.2       192.168.1.3       ICMP         98 Echo (ping) reply    id=0x0d5f, seq=1/256,
                         Wireshark · Packet 1 · r1-eth0
▸ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface r1-eth0, id 0
▸ Ethernet II, Src: 3e:99:ce:ed:3a:8f (3e:99:ce:ed:3a:8f), Dst: d2:84:54:1e:11:61 (d2:84:54:1e:11
```

h5 to h1 : R1 pass the packet received from eth0 to eth1 then forward it from eth1 to the next hop -- h1.



```
Source            Destination       Protocol Lengtł Info
192.168.1.3       192.168.3.2       ICMP         98 Echo (ping) request  id=0x0d5f, seq=1/256,
192.168.3.2       192.168.1.3       ICMP         98 Echo (ping) reply    id=0x0d5f, seq=1/256,
                         Wireshark · Packet 2 · r1-eth1
▸ Frame 2: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface r1-eth1, id 0
▸ Ethernet II, Src: 06:16:78:ea:10:51 (06:16:78:ea:10:51), Dst: 92:7c:09:cd:ec:ec (92:7c:09:cd:e
```

6. Capture all ICMP messages received by h1 and explain why h1 can only derive only 1st, 2nd, and 5th hops details. (10%)



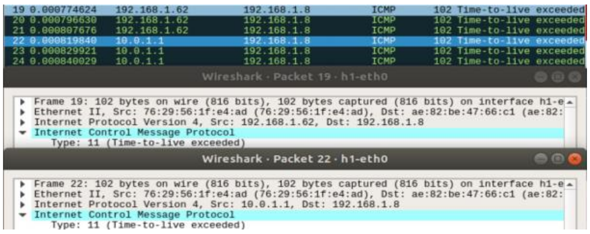
```
192.168.1.62      192.168.1.3       ICMP      102 Time-to-live exceeded (Time to live ex
192.168.1.62      192.168.1.3       ICMP      102 Time-to-live exceeded (Time to live ex
192.168.1.62      192.168.1.3       ICMP      102 Time-to-live exceeded (Time to live ex
10.0.1.1          192.168.1.3       ICMP      102 Time-to-live exceeded (Time to live ex
10.0.1.1          192.168.1.3       ICMP      102 Time-to-live exceeded (Time to live ex
10.0.1.1          192.168.1.3       ICMP      102 Time-to-live exceeded (Time to live ex
192.168.3.2       192.168.1.3       ICMP      102 Destination unreachable (Port unreacha
192.168.3.2       192.168.1.3       ICMP      102 Destination unreachable (Port unreacha
192.168.3.2       192.168.1.3       ICMP      102 Destination unreachable (Port unreacha
192.168.3.2       192.168.1.3       ICMP      102 Destination unreachable (Port unreacha
```

It means that h1 didn't get the respond of the 3rd and 4th hop.

It might because that the router didn't send back the ICMP time-exceeded messages or the ICMP time-exceeded messages are blocked.

However, when the 5th probe reaches the intended destination, it responds with an ICMP echo reply; since the echo replies aren't blocked, the last hop shows up in the traceroute.

7. h1 uses some ICMP messages to derive 1st and 2nd hop details. What are the type(s) and sender(s) of the ICMP messages? (5%)

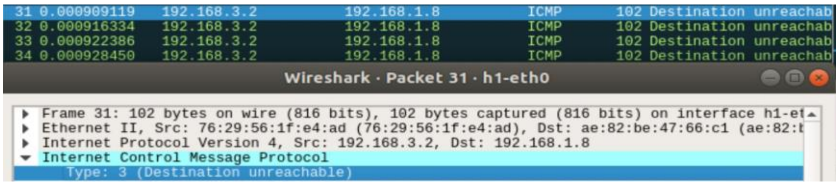


```
19 0.000774624   192.168.1.62     192.168.1.8      ICMP    102 Time-to-live exceeded
20 0.000796630   192.168.1.62     192.168.1.8      ICMP    102 Time-to-live exceeded
21 0.000807676   192.168.1.62     192.168.1.8      ICMP    102 Time-to-live exceeded
22 0.000819840   10.0.1.1         192.168.1.8      ICMP    102 Time-to-live exceeded
23 0.000829921   10.0.1.1         192.168.1.8      ICMP    102 Time-to-live exceeded
24 0.000840029   10.0.1.1         192.168.1.8      ICMP    102 Time-to-live exceeded
                    Wireshark · Packet 19 · h1-eth0
▸ Frame 19: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface h1-e
▸ Ethernet II, Src: 76:29:56:1f:e4:ad (76:29:56:1f:e4:ad), Dst: ae:82:be:47:66:c1 (ae:82:
▸ Internet Protocol Version 4, Src: 192.168.1.62, Dst: 192.168.1.8
▾ Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
                    Wireshark · Packet 22 · h1-eth0
▸ Frame 22: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface h1-e
▸ Ethernet II, Src: 76:29:56:1f:e4:ad (76:29:56:1f:e4:ad), Dst: ae:82:be:47:66:c1 (ae:82:
▸ Internet Protocol Version 4, Src: 10.0.1.1, Dst: 192.168.1.8
▾ Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
```

Type : 11 (Time to live exceeded in transit)

Sender : 1st is r1 (192.168.6--r1-eth1); 2nd is r2 (10.0.1.1--r2-eth1).

8. h1 uses some ICMP messages to derive 5th hop details. What are the type(s) and sender(s) of the ICMP messages? (5%)



```
31 0.000909119   192.168.3.2        192.168.1.8        ICMP      102 Destination unreachab
32 0.000916334   192.168.3.2        192.168.1.8        ICMP      102 Destination unreachab
33 0.000922386   192.168.3.2        192.168.1.8        ICMP      102 Destination unreachab
34 0.000928450   192.168.3.2        192.168.1.8        ICMP      102 Destination unreachab
```

Wireshark · Packet 31 · h1-eth0

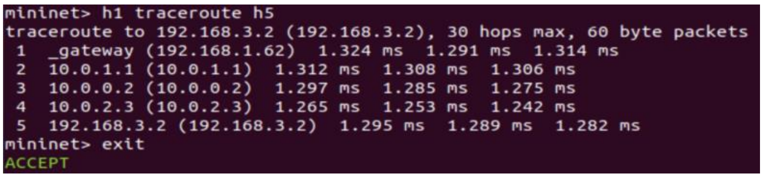
```
▸ Frame 31: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface h1-et
▸ Ethernet II, Src: 76:29:56:1f:e4:ad (76:29:56:1f:e4:ad), Dst: ae:82:be:47:66:c1 (ae:82:t
▸ Internet Protocol Version 4, Src: 192.168.3.2, Dst: 192.168.1.8
▾ Internet Control Message Protocol
     Type: 3 (Destination unreachable)
```

Type : 3 (Destination unreachable)

Sender : 192.168.3.2(h5)

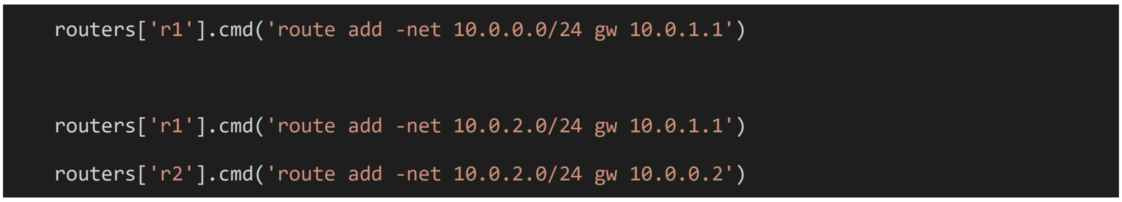
Bonus :

截圖如下。



```
mininet> h1 traceroute h5
traceroute to 192.168.3.2 (192.168.3.2), 30 hops max, 60 byte packets
 1  _gateway (192.168.1.62)  1.324 ms  1.291 ms  1.314 ms
 2  10.0.1.1 (10.0.1.1)  1.312 ms  1.308 ms  1.306 ms
 3  10.0.0.2 (10.0.0.2)  1.297 ms  1.285 ms  1.275 ms
 4  10.0.2.3 (10.0.2.3)  1.265 ms  1.253 ms  1.242 ms
 5  192.168.3.2 (192.168.3.2)  1.295 ms  1.289 ms  1.282 ms
mininet> exit
ACCEPT
```

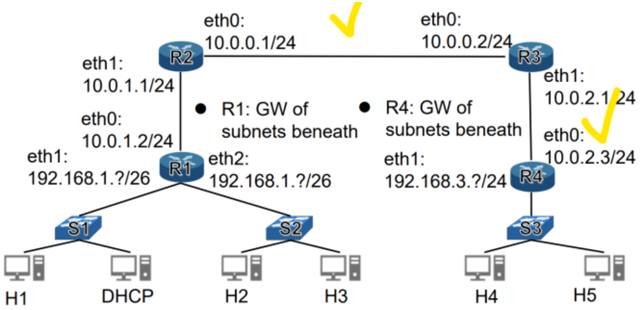
實作方法是加上送至打勾兩段網域的 routing rule。



```
    routers['r1'].cmd('route add -net 10.0.0.0/24 gw 10.0.1.1')


    routers['r1'].cmd('route add -net 10.0.2.0/24 gw 10.0.1.1')

    routers['r2'].cmd('route add -net 10.0.2.0/24 gw 10.0.0.2')
```



eth0:
10.0.0.1/24
eth0:
10.0.0.2/24
R2
R3
eth1:
10.0.1.1/24
eth1:
10.0.2.1/24
R1: GW of subnets beneath
R4: GW of subnets beneath
eth0:
10.0.1.2/24
eth0:
10.0.2.3/24
eth1:
192.168.1.?/26
R1
eth2:
192.168.1.?/26
eth1:
192.168.3.?/24
R4
S1
S2
S3
H1
DHCP
H2
H3
H4
H5