

網路系統總整與實作 Lab #2

Packet Forwarding and DHCP

0716236 劉耀文

Part 1 Complete topology.py

1. After you complete Steps 1-1

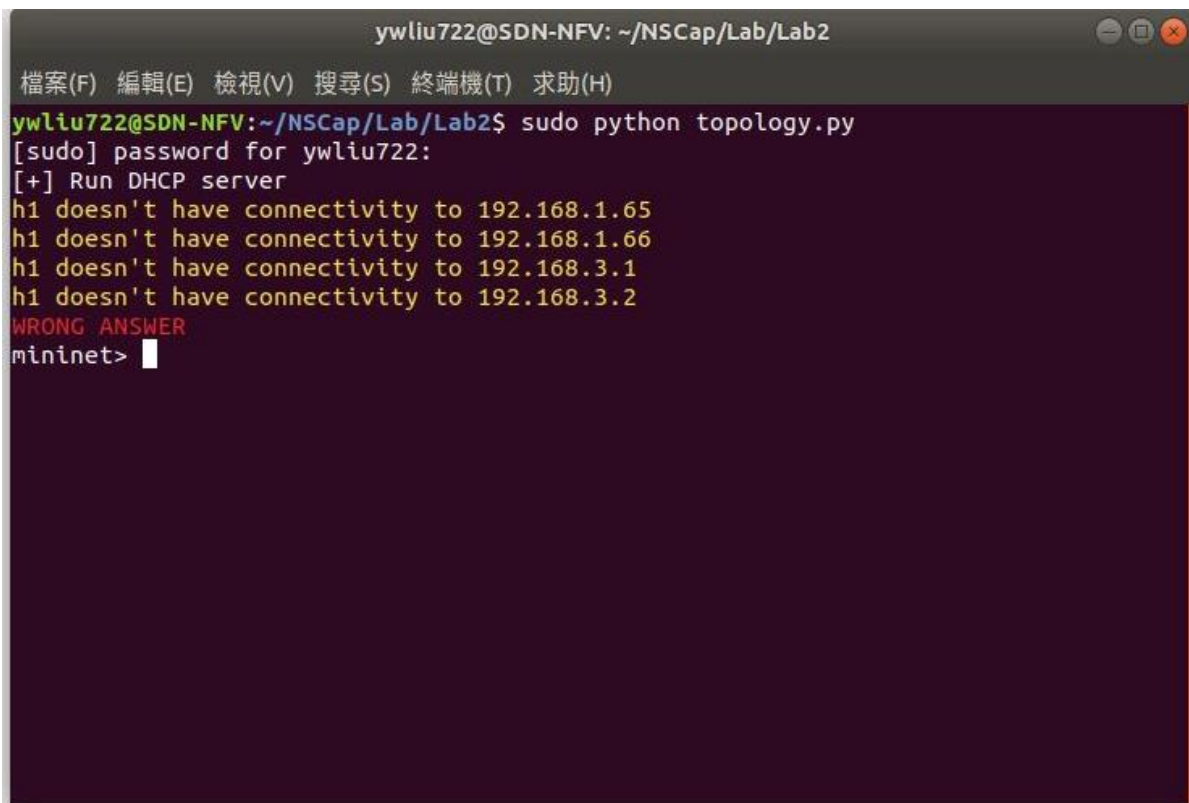
a) Can h2 ping h3? Briefly explain why or why not. (5%)

➔ 可以，因為 h2 和 h3 間只有連接一個 switch，而 switch 的特性為利用 MAC address 傳送資料，且不用額外設定、連接後即可使用，路徑找尋也是利用 ARP 廣播得出，故 h2 及 h3 可以在不用設定 router 的前提下 ping 到對方。

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

➔ 不行，因為 h2 和 h5 之間有 R1、R2、R3、R4 總共四個 router，且在還沒設定 static routing table 以及 host 的 default gateway 前，這中間的線路都是不通的，必須設定完後 router 和 host 才會將封包傳送至對應的線路。

2. Take screenshot to show that your topology configuration is correct. (10%)

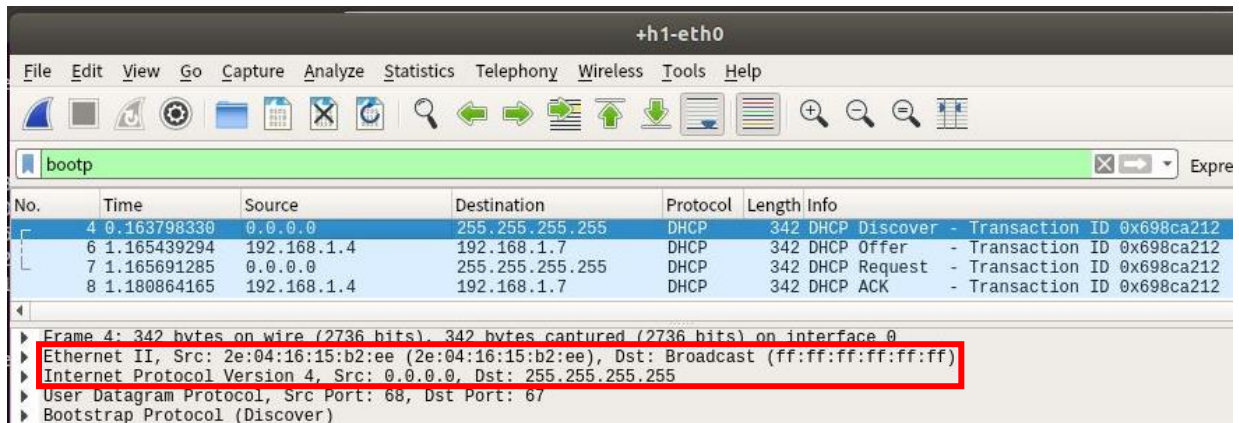


```
ywliu722@SDN-NFV: ~/NSCap/Lab/Lab2
檔案(F) 編輯(E) 檢視(V) 搜尋(S) 終端機(T) 求助(H)
ywliu722@SDN-NFV:~/NSCap/Lab/Lab2$ sudo python topology.py
[sudo] password for ywliu722:
[+] Run DHCP server
h1 doesn't have connectivity to 192.168.1.65
h1 doesn't have connectivity to 192.168.1.66
h1 doesn't have connectivity to 192.168.3.1
h1 doesn't have connectivity to 192.168.3.2
WRONG ANSWER
mininet> 
```

- 執行 python script 後，根據助教的講義，程式會先檢查連線是否正常，由上圖可知除了 h1 還沒透過 DHCP server 取得 IP 以及 default gateway 導致無法連線之外，其他 host 都透過事先設定好的 IP 以及 gateway 來進行連線並且可以傳輸資料給對方。

Part 2 DHCP Server configuration

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

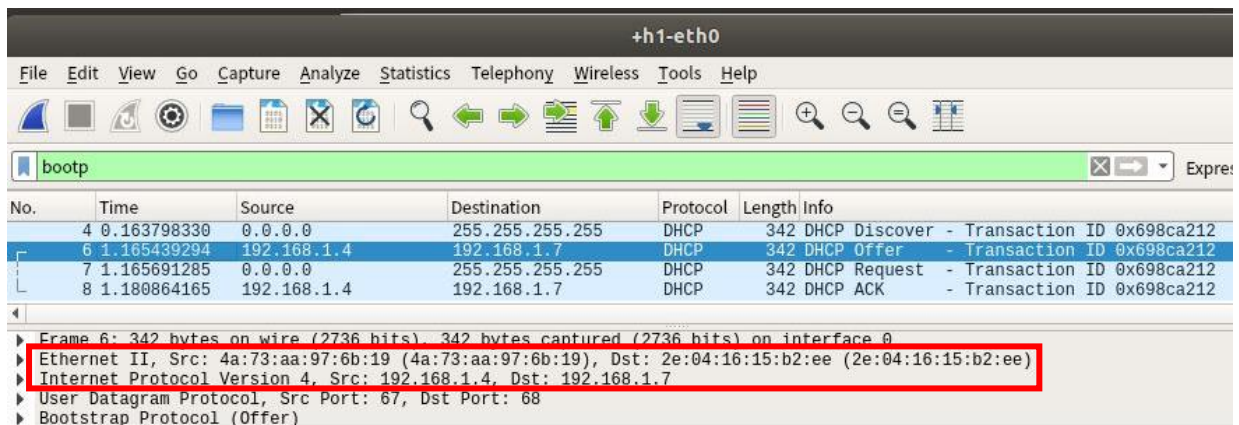


The screenshot shows a Wireshark capture on interface +h1-eth0. The packet list displays four packets: a DHCP Discover (No. 4), a DHCP Offer (No. 6), a DHCP Request (No. 7), and a DHCP ACK (No. 8). The packet details for the selected DHCP Discover packet (No. 4) are shown below the list. The Ethernet II section shows the source MAC as 2e:04:16:15:b2:ee and the destination as Broadcast (ff:ff:ff:ff:ff:ff). The Internet Protocol Version 4 section shows the source IP as 0.0.0.0 and the destination as 255.255.255.255. The User Datagram Protocol section shows the source port as 68 and the destination port as 67. The Bootstrap Protocol section is labeled as Discover.

No.	Time	Source	Destination	Protocol	Length	Info
4	0.163798330	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x698ca212
6	1.165439294	192.168.1.4	192.168.1.7	DHCP	342	DHCP Offer - Transaction ID 0x698ca212
7	1.165691285	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x698ca212
8	1.180864165	192.168.1.4	192.168.1.7	DHCP	342	DHCP ACK - Transaction ID 0x698ca212

Frame 4: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
Ethernet II, Src: 2e:04:16:15:b2:ee (2e:04:16:15:b2:ee), 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
Bootstrap Protocol (Discover)

➤ h1 尚未得到分配之 IP 且不知道 DHCP 伺服器之 IP 及 MAC，故 dst 都為廣播。

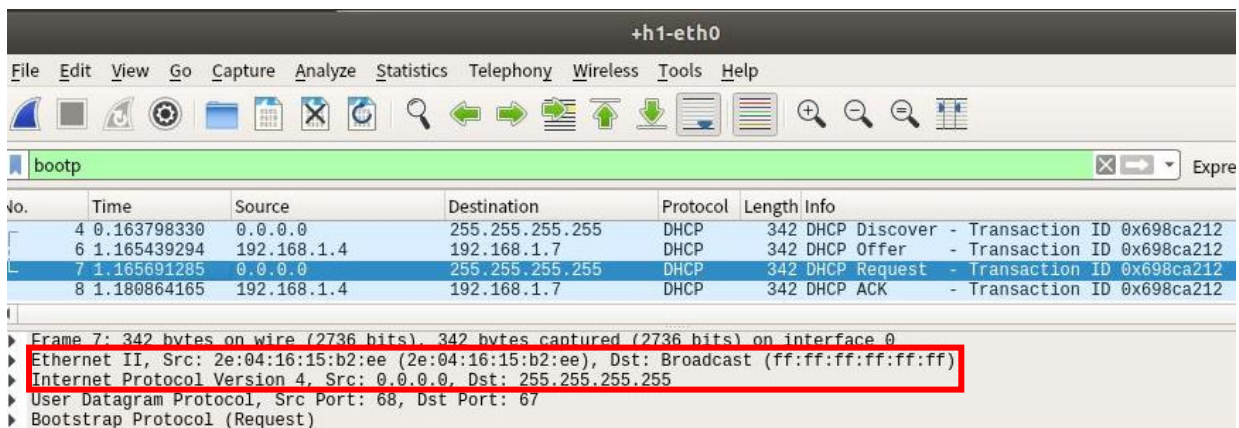


The screenshot shows the same Wireshark capture. The packet details for the selected DHCP Offer packet (No. 6) are shown. The Ethernet II section shows the source MAC as 4a:73:aa:97:6b:19 and the destination as 2e:04:16:15:b2:ee. The Internet Protocol Version 4 section shows the source IP as 192.168.1.4 and the destination as 192.168.1.7. The User Datagram Protocol section shows the source port as 67 and the destination port as 68. The Bootstrap Protocol section is labeled as Offer.

No.	Time	Source	Destination	Protocol	Length	Info
4	0.163798330	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x698ca212
6	1.165439294	192.168.1.4	192.168.1.7	DHCP	342	DHCP Offer - Transaction ID 0x698ca212
7	1.165691285	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x698ca212
8	1.180864165	192.168.1.4	192.168.1.7	DHCP	342	DHCP ACK - Transaction ID 0x698ca212

Frame 6: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
Ethernet II, Src: 4a:73:aa:97:6b:19 (4a:73:aa:97:6b:19), Dst: 2e:04:16:15:b2:ee (2e:04:16:15:b2:ee)
Internet Protocol Version 4, Src: 192.168.1.4, Dst: 192.168.1.7
User Datagram Protocol, Src Port: 67, Dst Port: 68
Bootstrap Protocol (Offer)

➤ DHCP 伺服器接收到請求並以 unicast 方式回傳可用 IP 給 h1。

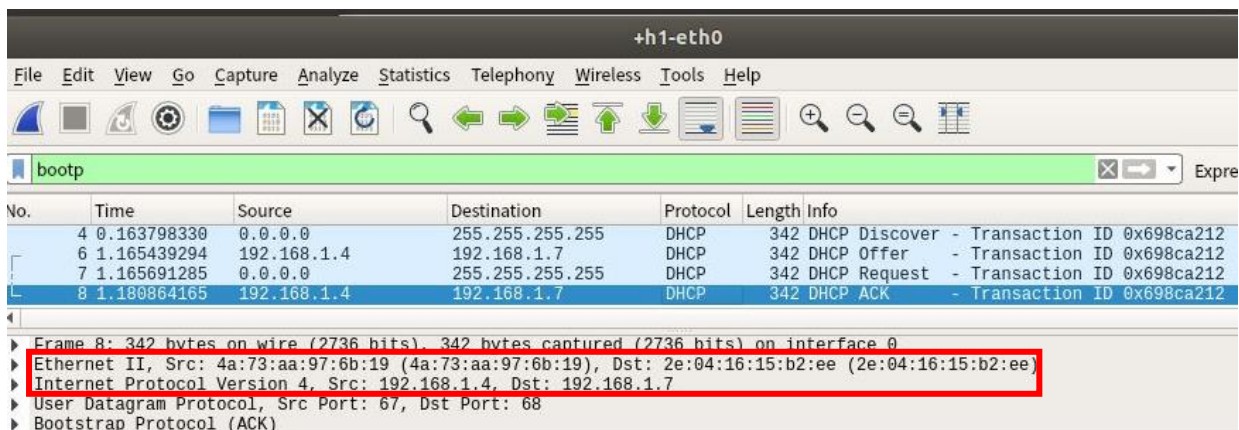


The screenshot shows the same Wireshark capture. The packet details for the selected DHCP Request packet (No. 7) are shown. The Ethernet II section shows the source MAC as 2e:04:16:15:b2:ee and the destination as Broadcast (ff:ff:ff:ff:ff:ff). The Internet Protocol Version 4 section shows the source IP as 0.0.0.0 and the destination as 255.255.255.255. The User Datagram Protocol section shows the source port as 68 and the destination port as 67. The Bootstrap Protocol section is labeled as Request.

No.	Time	Source	Destination	Protocol	Length	Info
4	0.163798330	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x698ca212
6	1.165439294	192.168.1.4	192.168.1.7	DHCP	342	DHCP Offer - Transaction ID 0x698ca212
7	1.165691285	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x698ca212
8	1.180864165	192.168.1.4	192.168.1.7	DHCP	342	DHCP ACK - Transaction ID 0x698ca212

Frame 7: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
Ethernet II, Src: 2e:04:16:15:b2:ee (2e:04:16:15:b2:ee), 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
Bootstrap Protocol (Request)

➤ 由於 h1 仍未正式被分配 IP 以及告知對應 DHCP 伺服器，故 dst 仍都為廣播。



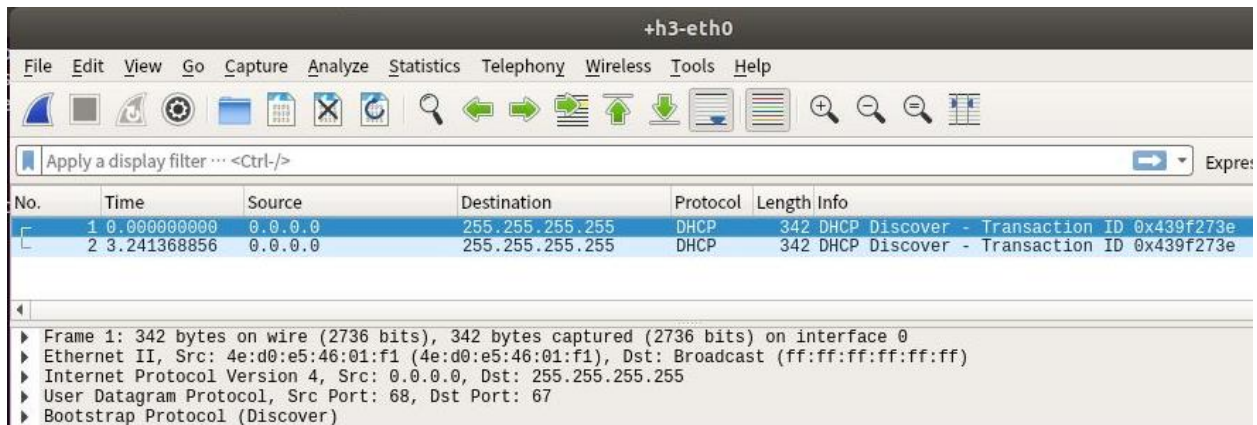
The screenshot shows the same Wireshark capture. The packet details for the selected DHCP ACK packet (No. 8) are shown. The Ethernet II section shows the source MAC as 4a:73:aa:97:6b:19 and the destination as 2e:04:16:15:b2:ee. The Internet Protocol Version 4 section shows the source IP as 192.168.1.4 and the destination as 192.168.1.7. The User Datagram Protocol section shows the source port as 67 and the destination port as 68. The Bootstrap Protocol section is labeled as ACK.

No.	Time	Source	Destination	Protocol	Length	Info
4	0.163798330	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x698ca212
6	1.165439294	192.168.1.4	192.168.1.7	DHCP	342	DHCP Offer - Transaction ID 0x698ca212
7	1.165691285	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x698ca212
8	1.180864165	192.168.1.4	192.168.1.7	DHCP	342	DHCP ACK - Transaction ID 0x698ca212

Frame 8: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
Ethernet II, Src: 4a:73:aa:97:6b:19 (4a:73:aa:97:6b:19), Dst: 2e:04:16:15:b2:ee (2e:04:16:15:b2:ee)
Internet Protocol Version 4, Src: 192.168.1.4, Dst: 192.168.1.7
User Datagram Protocol, Src Port: 67, Dst Port: 68
Bootstrap Protocol (ACK)

➤ DHCP 伺服器正式回覆請求，h1 收到此封包後正式獲得 IP 及 default gateway 分配。

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



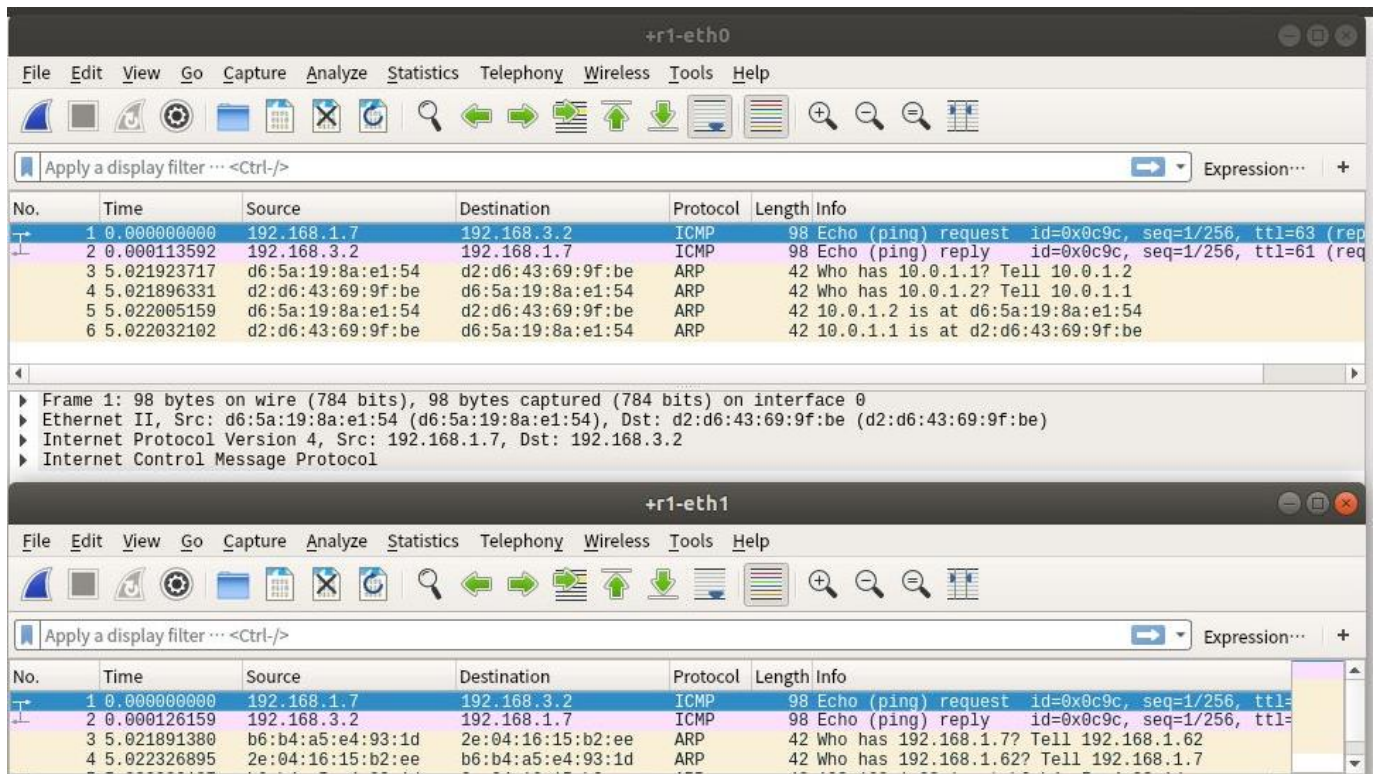
The screenshot shows a Wireshark capture on the h3-eth0 interface. The packet list contains two DHCP Discover packets. The first packet (No. 1) is at time 0.000000000, source 0.0.0.0, destination 255.255.255.255, protocol DHCP, length 342, and info '342 DHCP Discover - Transaction ID 0x439f273e'. The second packet (No. 2) is at time 3.241368856, source 0.0.0.0, destination 255.255.255.255, protocol DHCP, length 342, and info '342 DHCP Discover - Transaction ID 0x439f273e'. The packet details pane shows the structure of the first packet: Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Bootstrap Protocol (Discover).

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x439f273e
2	3.241368856	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x439f273e

- 上圖為在 h3 執行 DHCP 指令後利用 wireshark 所擷取之封包列表。由此圖可以得知除了 h1 之外的 host 無法透過 DHCP server 獲得 IP 位置。由於第一個 discover 步驟還沒有拿到 IP 位置，發出之封包無法穿過 router 到不同內網以要求分配 IP，故所有 host 間只有和 DHCP server 位於同個內網的 h1 可以透過 DHCP server 獲得 IP。並且 DHCP 分配之 default gateway 也不同，故無論如何其他 host 皆無法透過 DHCP 獲得 IP。

Part 3 Answer Questions

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



The screenshot shows two Wireshark captures on the r1 interface. The top capture is on r1-eth0, showing an ICMP Echo (ping) request from 192.168.1.7 to 192.168.3.2, followed by an ICMP Echo (ping) reply from 192.168.3.2 to 192.168.1.7. The bottom capture is on r1-eth1, showing an ICMP Echo (ping) request from 192.168.1.7 to 192.168.3.2, followed by an ICMP Echo (ping) reply from 192.168.3.2 to 192.168.1.7. Both captures also show ARP requests and replies.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.7	192.168.3.2	ICMP	98	Echo (ping) request id=0xc9c, seq=1/256, ttl=63 (req)
2	0.000113592	192.168.3.2	192.168.1.7	ICMP	98	Echo (ping) reply id=0xc9c, seq=1/256, ttl=61 (req)
3	5.021923717	d6:5a:19:8a:e1:54	d2:d6:43:69:9f:be	ARP	42	Who has 10.0.1.1? Tell 10.0.1.2
4	5.021896331	d2:d6:43:69:9f:be	d6:5a:19:8a:e1:54	ARP	42	Who has 10.0.1.2? Tell 10.0.1.1
5	5.022005159	d6:5a:19:8a:e1:54	d2:d6:43:69:9f:be	ARP	42	10.0.1.2 is at d6:5a:19:8a:e1:54
6	5.022032102	d2:d6:43:69:9f:be	d6:5a:19:8a:e1:54	ARP	42	10.0.1.1 is at d2:d6:43:69:9f:be

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.7	192.168.3.2	ICMP	98	Echo (ping) request id=0xc9c, seq=1/256, ttl=
2	0.000126159	192.168.3.2	192.168.1.7	ICMP	98	Echo (ping) reply id=0xc9c, seq=1/256, ttl=
3	5.021891380	b6:b4:a5:e4:93:1d	2e:04:16:15:b2:ee	ARP	42	Who has 192.168.1.7? Tell 192.168.1.62
4	5.022326895	2e:04:16:15:b2:ee	b6:b4:a5:e4:93:1d	ARP	42	Who has 192.168.1.62? Tell 192.168.1.7

- 由上圖兩個 interface 經過之封包可以判斷出 r1 先從 eth-0 接收來自 h1 的 ICMP ping request 封包後，由 eth-1 以 h5 為目的地傳送出去。相反的，來自 h5 的 ICMP ping reply 會先被 r1 的 eth-1 interface 所接收，並以 eth-0 回傳給 h1，以上便完成一次 ping 指令。

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

No.	Time	Source	Destination	Protocol	Length	Info
17	0.000730238	192.168.1.62	192.168.1.7	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
18	0.000774766	192.168.1.62	192.168.1.7	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
19	0.000786803	192.168.1.62	192.168.1.7	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
20	0.000799295	10.0.1.1	192.168.1.7	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
21	0.000809350	10.0.1.1	192.168.1.7	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
22	0.000819424	10.0.1.1	192.168.1.7	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
23	0.000888767	192.168.3.2	192.168.1.7	ICMP	102	Destination unreachable (Port unreachable)
24	0.000896482	192.168.3.2	192.168.1.7	ICMP	102	Destination unreachable (Port unreachable)
25	0.000902560	192.168.3.2	192.168.1.7	ICMP	102	Destination unreachable (Port unreachable)
26	0.000908524	192.168.3.2	192.168.1.7	ICMP	102	Destination unreachable (Port unreachable)
28	0.016329375	192.168.3.2	192.168.1.7	ICMP	102	Destination unreachable (Port unreachable)
30	0.016356640	192.168.3.2	192.168.1.7	ICMP	102	Destination unreachable (Port unreachable)

- 我們從上圖可以得知，h1 僅收到了來自 r1(gateway)、r2 以及 h5 的回應，第三及第四個 hop 的詳細資訊無法被 h1 得知便是因為沒有在 timeout 時間內收到此二節點的回應封包。
- 詳細原因在 bonus 處說明

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%)

No.	Time	Source	Destination	Protocol	Length	Info
17	0.000730238	192.168.1.62	192.168.1.7	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
18	0.000774766	192.168.1.62	192.168.1.7	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
19	0.000786803	192.168.1.62	192.168.1.7	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
20	0.000799295	10.0.1.1	192.168.1.7	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
21	0.000809350	10.0.1.1	192.168.1.7	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
22	0.000819424	10.0.1.1	192.168.1.7	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
23	0.000888767	192.168.3.2	192.168.1.7	ICMP	102	Destination unreachable (Port unreachable)
24	0.000896482	192.168.3.2	192.168.1.7	ICMP	102	Destination unreachable (Port unreachable)
25	0.000902560	192.168.3.2	192.168.1.7	ICMP	102	Destination unreachable (Port unreachable)
26	0.000908524	192.168.3.2	192.168.1.7	ICMP	102	Destination unreachable (Port unreachable)
28	0.016329375	192.168.3.2	192.168.1.7	ICMP	102	Destination unreachable (Port unreachable)
30	0.016356640	192.168.3.2	192.168.1.7	ICMP	102	Destination unreachable (Port unreachable)

- traceroute 是利用 probe 封包 TTL 的增加來尋找路徑的下一步，此機制由 TTL=1 開始、每往下一個 hop 走 TTL-1，直到 TTL 小於 0 後便丟棄該封包並回傳一個 time exceed 的 ICMP type 11 code 0 錯誤回應封包給 h1，所以我們可以在 h1 上最先收到來自 gateway (r1(192.168.1.62))的 ICMP 封包，接著就是來自 r2(10.0.1.1)的 ICMP 封包。

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

No.	Time	Source	Destination	Protocol	Length	Info
17	0.000730238	192.168.1.62	192.168.1.7	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
18	0.000774766	192.168.1.62	192.168.1.7	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
19	0.000786803	192.168.1.62	192.168.1.7	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
20	0.000799295	10.0.1.1	192.168.1.7	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
21	0.000809350	10.0.1.1	192.168.1.7	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
22	0.000810424	10.0.1.1	192.168.1.7	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
23	0.000888767	192.168.3.2	192.168.1.7	ICMP	102	Destination unreachable (Port unreachable)
24	0.000896482	192.168.3.2	192.168.1.7	ICMP	102	Destination unreachable (Port unreachable)
25	0.000902560	192.168.3.2	192.168.1.7	ICMP	102	Destination unreachable (Port unreachable)
26	0.000908524	192.168.3.2	192.168.1.7	ICMP	102	Destination unreachable (Port unreachable)
28	0.016329375	192.168.3.2	192.168.1.7	ICMP	102	Destination unreachable (Port unreachable)
30	0.016356640	192.168.3.2	192.168.1.7	ICMP	102	Destination unreachable (Port unreachable)

- 當 traceroute 傳送之 probe 封包到達目的地之後，因為該 port 並沒有程式在使用，h5(192.168.3.2)會回傳一個 destination port unreachable 的 ICMP type 3 code 3 錯誤回應封包給 h1，h1 得知此之訊後便可以得知已經到達目的地並結束 traceroute 程式。

Bonus (10%)

```
mininet> r1 route -n
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
10.0.0.0         10.0.1.1       255.255.255.0   UG      0      0      0 r1-eth0
10.0.1.0         0.0.0.0        255.255.255.0   U        0      0      0 r1-eth0
10.0.2.0         10.0.1.1       255.255.255.0   UG      0      0      0 r1-eth0
192.168.1.0      0.0.0.0        255.255.255.192 U        0      0      0 r1-eth1
192.168.1.64     0.0.0.0        255.255.255.192 U        0      0      0 r1-eth2
192.168.3.0      10.0.1.1       255.255.255.0   UG      0      0      0 r1-eth0
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) 0.503 ms 0.486 ms 0.496 ms
 2  10.0.1.1 (10.0.1.1) 0.508 ms 0.496 ms 0.499 ms
 3  10.0.0.2 (10.0.0.2) 0.492 ms 0.482 ms 0.474 ms
 4  10.0.2.3 (10.0.2.3) 0.465 ms 0.533 ms 0.354 ms
 5  192.168.3.2 (192.168.3.2) 0.533 ms 0.528 ms 0.498 ms
```

- 在 part 3 執行 traceroute 後執行結果之所以會缺少 hop 3 跟 hop 4 的詳細資訊，表面上來說是因為回覆封包沒有被在 TTL 內被 h1 接收，然而會發生這種狀況的實際原因是因為一開始在設定 static routing 的時候只有考慮到要把 host 所在的子網包含於 routing table 當中，卻沒有注意到 router 間所產生的子網也要考慮進去，以 h1 traceroute h5 為例，在第三次以及第四次 probe 時，r1 會收到來自 h1 要送往 r3 及 r4 的 probe 封包，但此時 r1 的 routing table 並沒有設置 10.0.0.0/24 以及 10.0.2.0/24 這兩個子網的 routing path，故 r3 以及 r4 從頭到尾都沒有接收到 h1 以此二節點為目的地的封包，所以也不會有來自 r3 以及 r4 的 reply 封包產生。