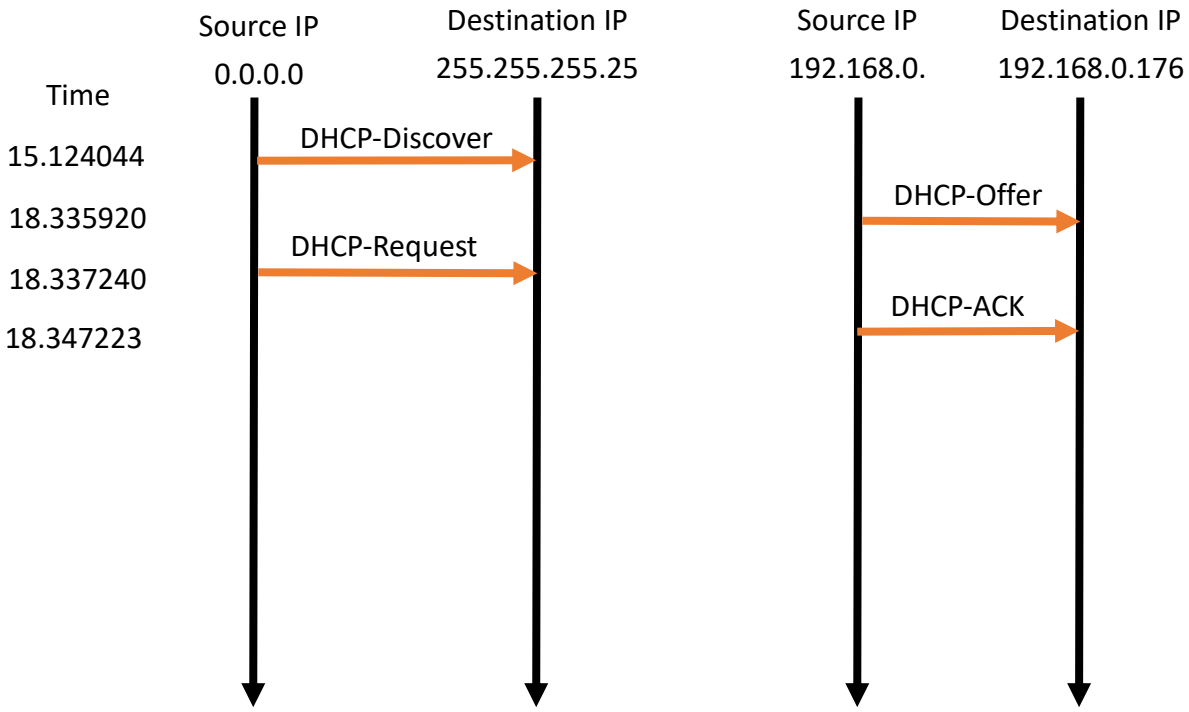
DHCP 作業(使用 Wireshark)

S0954052 范家豪

1. UDP

2. It used 67 and 68 for port numbers.



3. 00:f4:8d:9f:ac:e5

4. 在 DHCP Request 裡 Option 比較多。無論是 Discover 或是 Request 在 Message Type 有不同的值。

DHCP Discover

```
Option: (53) DHCP Message Type (Discover)
    Length: 1
    DHCP: Discover (1)
Option: (61) Client identifier
Option: (50) Requested IP Address (192.168.0.176)
Option: (12) Host Name
Option: (60) Vendor class identifier
Option: (55) Parameter Request List
Option: (255) End
```

DHCP Request

```
Option: (53) DHCP Message Type (Request)
    Length: 1
    DHCP: Request (3)
Option: (61) Client identifier
Option: (50) Requested IP Address (192.168.0.176)
Option: (54) DHCP Server Identifier (192.168.0.1)
Option: (12) Host Name
Option: (81) Client Fully Qualified Domain Name
Option: (60) Vendor class identifier
Option: (55) Parameter Request List
Option: (255) End
```

5.

The first Transaction ID : 0xf24a877
The second Transaction ID : 0xca62af39
Purpose : Allow host to differentiate which requests is being asked by user.

```
344 DHCP Discover - Transaction ID 0xf24a877
342 DHCP Offer    - Transaction ID 0xf24a877
370 DHCP Request  - Transaction ID 0xf24a877
354 DHCP ACK      - Transaction ID 0xf24a877
358 DHCP Request  - Transaction ID 0xca62af39
354 DHCP ACK      - Transaction ID 0xca62af39
```

6.

Discover(0.0.0.0/255.255.255.255)
Offerr(192.168.0.1/192.168.0.176)
Request(0.0.0.0/255.255.255.255)
ACK(192.168.0.1/192.168.0.176)

1025	50.841014	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover
1059	53.965528	192.168.0.1	192.168.0.176	DHCP	342	DHCP Offer
1060	53.966368	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request
1061	53.992912	192.168.0.1	192.168.0.176	DHCP	354	DHCP ACK

7.

192.168.0.1

```
Option: (54) DHCP Server Identifier (192.168.0.1)
    Length: 4
    DHCP Server Identifier: 192.168.0.1
```

8.

192.168.0.176

```
> Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 192.168.0.176
  Next server IP address: 192.168.0.1
  Relay agent IP address: 0.0.0.0
```

9.

Yes, and IP address is 0.0.0.0

```
> Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 0.0.0.0
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
```

10.

在 DHCP message 裡，router 告訴 client 哪個路由器是來傳遞訊息的，而 subnet mask 告訴 client 應該用哪一種 subnet mask。

11.

Option(50):192.168.0.176

```
v Option: (50) Requested IP Address (192.168.0.176)
      Length: 4
      Requested IP Address: 192.168.0.176
```

1059	53.965528	192.168.0.1	192.168.0.176	DHCP	342	DHCP Offer
1060	53.966368	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request
1061	53.992912	192.168.0.1	192.168.0.176	DHCP	354	DHCP ACK

12.

The amount of time the DHCP server assigns an IP address to the client.

```
v Option: (51) IP Address Lease Time
      Length: 4
      IP Address Lease Time: (86400s) 1 day
```

13.

The DHCP release message tells the DHCP server that you want to cancel the IP address offered. The DHCP server will not issue an ACK of the client's DHCP request. If the release message is lost then the DHCP server retains the IP address until the lease time expires.

14.

The purpose of those ARP packets are to track IP addresses back to a physical server in a local area network.

50	1.387589	D-LinkIn_5f:e1:37	Broadcast	ARP	42	Who has 192.168.0.133? Tell 192.168.0.1
77	2.412220	D-LinkIn_5f:e1:37	Broadcast	ARP	42	Who has 192.168.0.133? Tell 192.168.0.1
93	2.789989	LiteonTe_9f:ac:e5	Broadcast	ARP	42	Who has 169.254.102.142? (ARP Probe)
97	3.436221	D-LinkIn_5f:e1:37	Broadcast	ARP	42	Who has 192.168.0.133? Tell 192.168.0.1
100	3.790043	LiteonTe_9f:ac:e5	Broadcast	ARP	42	Who has 169.254.102.142? (ARP Probe)
106	4.790381	LiteonTe_9f:ac:e5	Broadcast	ARP	42	Who has 169.254.102.142? (ARP Probe)
114	5.790418	LiteonTe_9f:ac:e5	Broadcast	ARP	42	ARP Announcement for 169.254.102.142
133	6.200436	D-LinkIn_5f:e1:37	Broadcast	ARP	42	Who has 192.168.0.137? Tell 192.168.0.1
206	18.376310	LiteonTe_9f:ac:e5	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.176
207	18.380138	D-LinkIn_5f:e1:37	LiteonTe_9f:ac:e5	ARP	42	192.168.0.1 is at f0:b4:d2:5f:e1:37
229	18.636036	LiteonTe_9f:ac:e5	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.176
230	18.638352	D-LinkIn_5f:e1:37	LiteonTe_9f:ac:e5	ARP	42	192.168.0.1 is at f0:b4:d2:5f:e1:37
237	18.788474	LiteonTe_9f:ac:e5	Broadcast	ARP	42	Who has 192.168.0.176? (ARP Probe)