

Part1:

1. Flush all switch tables and take screenshots to show the switch tables of all switches.

port	VLAN	MAC	Age
------	------	-----	-----

2. How does h4 knows h1's MAC address? Take screenshot on Wireshark to verify your answers.

h1會發送ARP request尋找h4，而封包中的資訊會包含h1的MAC位址(源硬體位址)，h4即可對封包的此段訊息做解析與紀錄取得MAC位址。

25	140.991304308	56:4a:fc:26:8f:37	Broadcast	ARP	42	Who has 10.0.0.4? Tell 10.0.0.1
26	140.991589856	ea:93:b5:a0:a4:8c	56:4a:fc:26:8f:37	ARP	42	10.0.0.4 is at ea:93:b5:a0:a4:8c
27	140.991595269	10.0.0.1	10.0.0.4	ICMP	98	Echo (ping) request id=0x094c, seq=1/256, ttl=64 (r
28	140.991681652	10.0.0.4	10.0.0.1	ICMP	98	Echo (ping) reply id=0x094c, seq=1/256, ttl=64 (r
29	142.015750223	10.0.0.1	10.0.0.4	ICMP	98	Echo (ping) request id=0x094c, seq=2/512, ttl=64 (r
30	142.015782179	10.0.0.4	10.0.0.1	ICMP	98	Echo (ping) reply id=0x094c, seq=2/512, ttl=64 (r
31	143.039536579	10.0.0.1	10.0.0.4	ICMP	98	Echo (ping) request id=0x094c, seq=3/768, ttl=64 (r
32	143.039565394	10.0.0.4	10.0.0.1	ICMP	98	Echo (ping) reply id=0x094c, seq=3/768, ttl=64 (r
33	144.063779154	10.0.0.1	10.0.0.4	ICMP	98	Echo (ping) request id=0x094c, seq=4/1024, ttl=64 (r
34	144.063806627	10.0.0.4	10.0.0.1	ICMP	98	Echo (ping) reply id=0x094c, seq=4/1024, ttl=64 (r
35	145.087512458	10.0.0.1	10.0.0.4	ICMP	98	Echo (ping) request id=0x094c, seq=5/1280, ttl=64 (r
36	145.087541662	10.0.0.4	10.0.0.1	ICMP	98	Echo (ping) reply id=0x094c, seq=5/1280, ttl=64 (r

Frame 25: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
Ethernet II, Src: 56:4a:fc:26:8f:37 (56:4a:fc:26:8f:37), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: 56:4a:fc:26:8f:37 (56:4a:fc:26:8f:37)
Sender IP address: 10.0.0.1
Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
Target IP address: 10.0.0.4

3. How does h1 knows h4's MAC address? Take screenshot on Wireshark to verify your answers.

因為在s1的ARP快取表中尚未有h4的IP位址對應MAC位址資訊，所以會透過廣播方式傳送ARP request尋找h4，而接受到廣播的h4會對h1做出回應，所以h1可以取得h4的MAC位址。

25	140.991304308	56:4a:fc:26:8f:37	Broadcast	ARP	42	Who has 10.0.0.4? Tell 10.0.0.1
26	140.991589856	ea:93:b5:a0:a4:8c	56:4a:fc:26:8f:37	ARP	42	10.0.0.4 is at ea:93:b5:a0:a4:8c
27	140.991595269	10.0.0.1	10.0.0.4	ICMP	98	Echo (ping) request id=0x094c, seq=1/256, ttl=64 (r
28	140.991681652	10.0.0.4	10.0.0.1	ICMP	98	Echo (ping) reply id=0x094c, seq=1/256, ttl=64 (r
29	142.015750223	10.0.0.1	10.0.0.4	ICMP	98	Echo (ping) request id=0x094c, seq=2/512, ttl=64 (r
30	142.015782179	10.0.0.4	10.0.0.1	ICMP	98	Echo (ping) reply id=0x094c, seq=2/512, ttl=64 (r
31	143.039536579	10.0.0.1	10.0.0.4	ICMP	98	Echo (ping) request id=0x094c, seq=3/768, ttl=64 (r
32	143.039565394	10.0.0.4	10.0.0.1	ICMP	98	Echo (ping) reply id=0x094c, seq=3/768, ttl=64 (r
33	144.063779154	10.0.0.1	10.0.0.4	ICMP	98	Echo (ping) request id=0x094c, seq=4/1024, ttl=64 (r
34	144.063806627	10.0.0.4	10.0.0.1	ICMP	98	Echo (ping) reply id=0x094c, seq=4/1024, ttl=64 (r
35	145.087512458	10.0.0.1	10.0.0.4	ICMP	98	Echo (ping) request id=0x094c, seq=5/1280, ttl=64 (r
36	145.087541662	10.0.0.4	10.0.0.1	ICMP	98	Echo (ping) reply id=0x094c, seq=5/1280, ttl=64 (r

Frame 26: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
Ethernet II, Src: ea:93:b5:a0:a4:8c (ea:93:b5:a0:a4:8c), Dst: 56:4a:fc:26:8f:37 (56:4a:fc:26:8f:37)
Address Resolution Protocol (reply)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: reply (2)
Sender MAC address: ea:93:b5:a0:a4:8c (ea:93:b5:a0:a4:8c)
Sender IP address: 10.0.0.4
Target MAC address: 56:4a:fc:26:8f:37 (56:4a:fc:26:8f:37)
Target IP address: 10.0.0.1

0000 56 4a fc 26 8f 37 ea 93 b5 a0 a4 8c 08 06 00 01 VJ&7
0010 08 00 06 04 00 02 ea 93 b5 a0 a4 8c 0a 0a 00 04

4. Why does the first ping have a longer delay?

因為first ping的封包通常會被擱置，讓ARP broadcast先發送，尋找目標的MAC位址，得到回應之後才會再發送first ping的封包，導致delay較長甚至遺失

封包。

5. Show the switch tables and identify the entries that constitute the path of Ping.

```
kaorip@kaorip-VirtualBox:~$ sudo ovs-appctl fdb/show s1
```

port	VLAN	MAC	Age
1	0	56:4a:fc:26:8f:37	105
3	0	ea:93:b5:a0:a4:8c	105

```
kaorip@kaorip-VirtualBox:~$ sudo ovs-appctl fdb/show s2
```

port	VLAN	MAC	Age
1	0	56:4a:fc:26:8f:37	150
2	0	ea:93:b5:a0:a4:8c	150

```
kaorip@kaorip-VirtualBox:~$ sudo ovs-appctl fdb/show s3
```

port	VLAN	MAC	Age
3	0	56:4a:fc:26:8f:37	166
2	0	ea:93:b5:a0:a4:8c	166

h1 >> port1|s1|port3 >> port1|s2|port2 >> port2|s3|port3 >> h4

Part2:

1. Can h1 ping h4 successfully before enabling STP?

不行，封包會在網路中形成迴圈。

2. Can h1 ping h4 successfully after STP enabled?

可以，STP 會確保 switch 之間的封包傳遞沒有迴圈產生。

3. Show s1 MAC tables before and after enables STP and explain the differences.

Before:

```
kaorip@kaorip-VirtualBox:~$ sudo ovs-appctl fdb/show s1
```

port	VLAN	MAC	Age
4	0	c6:69:f0:d9:bd:27	0
4	0	22:82:ab:5e:84:cd	0
3	0	52:15:f6:a1:31:5f	0
4	0	b2:ce:e7:f9:3c:47	0
4	0	ca:1b:4d:a0:0c:3b	0
3	0	4a:2f:08:04:1f:6b	0
3	0	be:73:13:01:2a:97	0
3	0	06:01:e6:bd:b5:42	0
4	0	be:d7:02:d1:56:56	0
3	0	56:01:3a:b2:dd:c4	0
4	0	5a:1f:c2:1b:17:de	0
3	0	4a:b4:5c:1e:49:ab	0

After:

```
kaorip@kaorip-VirtualBox:~$ sudo ovs-appctl fdb/show s1
```

port	VLAN	MAC	Age
------	------	-----	-----

在 STP 開啟之前，一旦發送廣播就會在 switch 之間形成迴圈，導致封包不斷在 switch 之間傳遞，而不斷改變 MAC table；STP 開啟之後，則會刪去無效的冗贅路徑。

4. What have you observed and learned from this lab?

觀察到 MAC address table learning 情形，以及在 switch 有形成迴圈的情況下，會遇到廣播封包不斷傳遞，導致 MAC address table 不斷被改變而無法連線

到目標位址，而此種情形可以透過 STP 來解決。