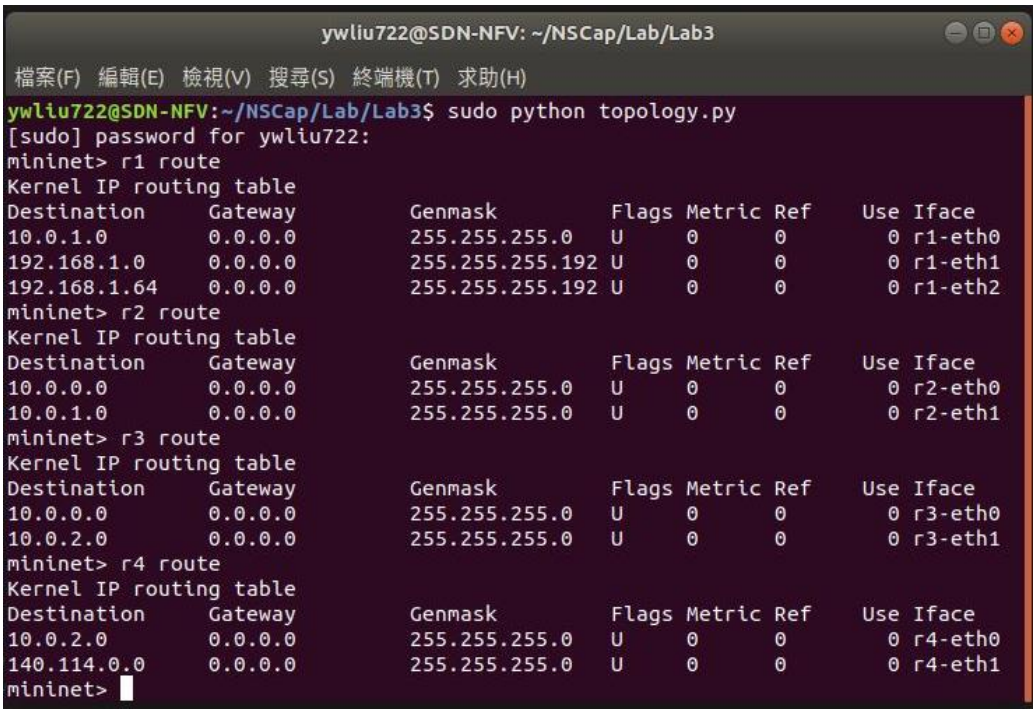
網路系統總整與實作 Lab #3

Dynamic Routing and Network Address Translation

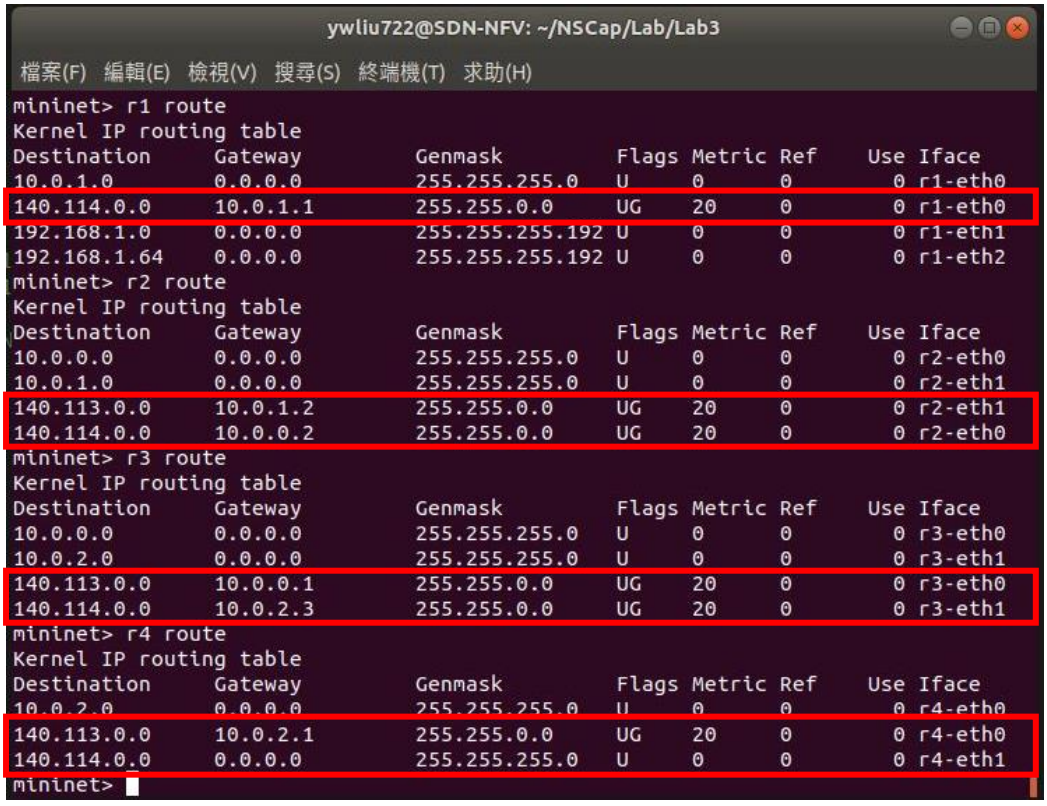
0716236 劉耀文

Part 1 BGP and Zebra configuration

1. Take routing tables screenshot before/after on [r1-r4] (10%)

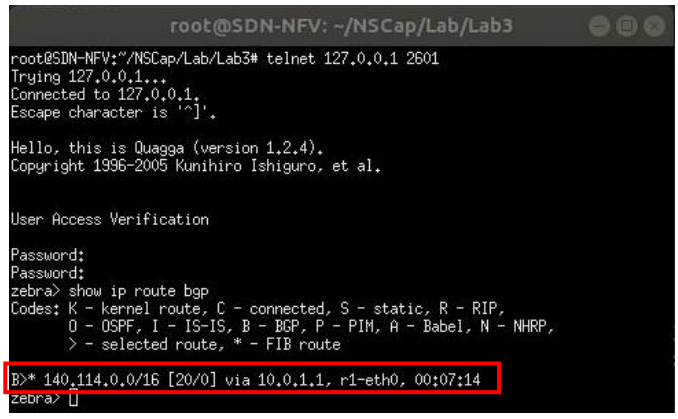


➔ 一開始尚未載入 BGP 的 routing table，除了有連接到的子網之外沒有其他項目。

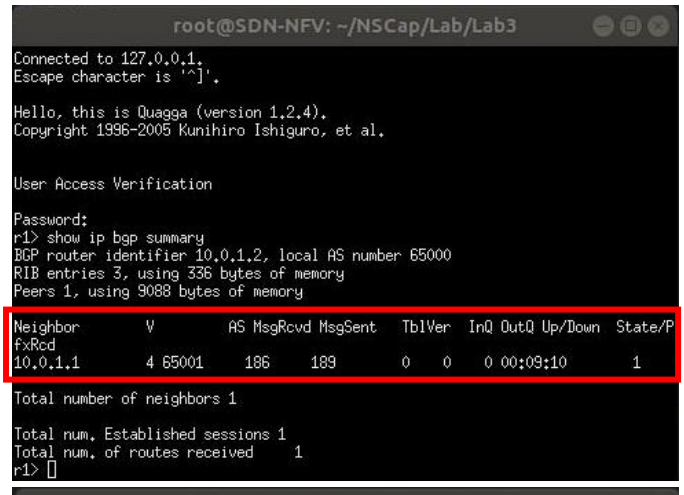


➔ 逐一載入 zebra 以及 BGP 設定檔並完成路由探索之後的結果，由於在 r2 以及 r3 的 BGP 設定檔中並沒有設定所屬子網域 IP，故只會增加 r1 以及 r4 連接之子網域 IP。

2. Telnet zebra and bgpd daemons of [r1-r4] and take screenshots of routes in zebra and bgpd daemons. (10%)

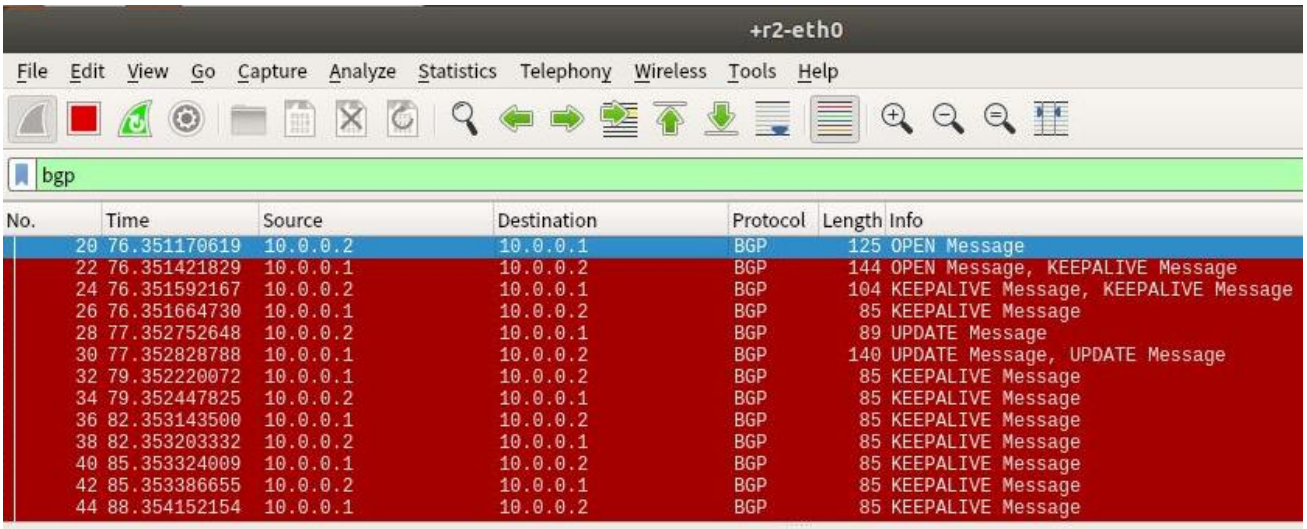


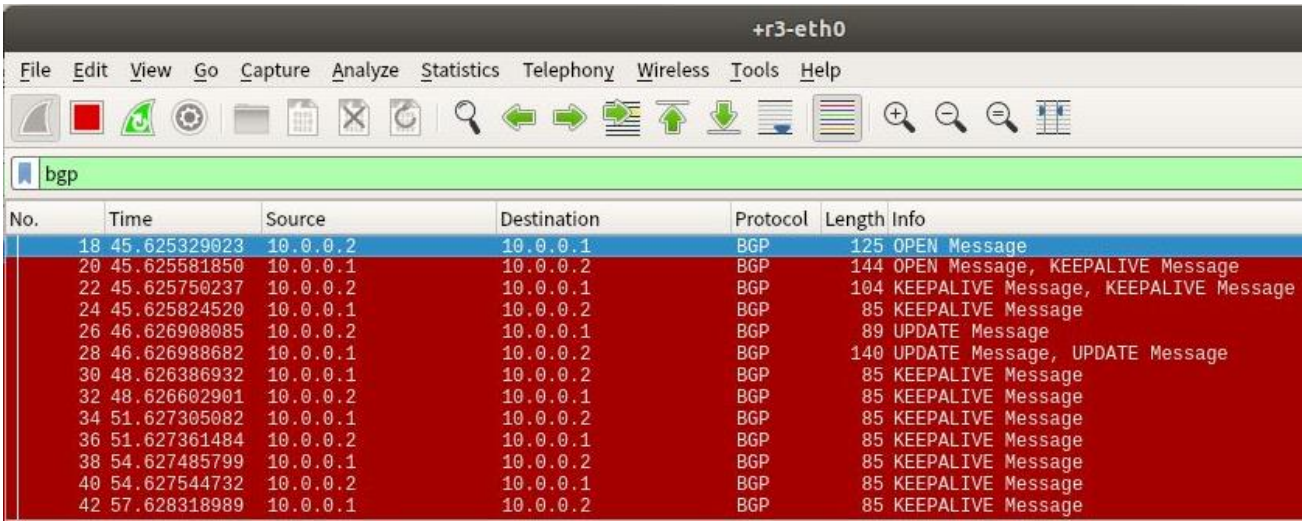
➔ Zebra daemon 顯示除了自己所在子網之外的 routing table entries。左上 r1、右上 r2、左下 r3、右下 r4。

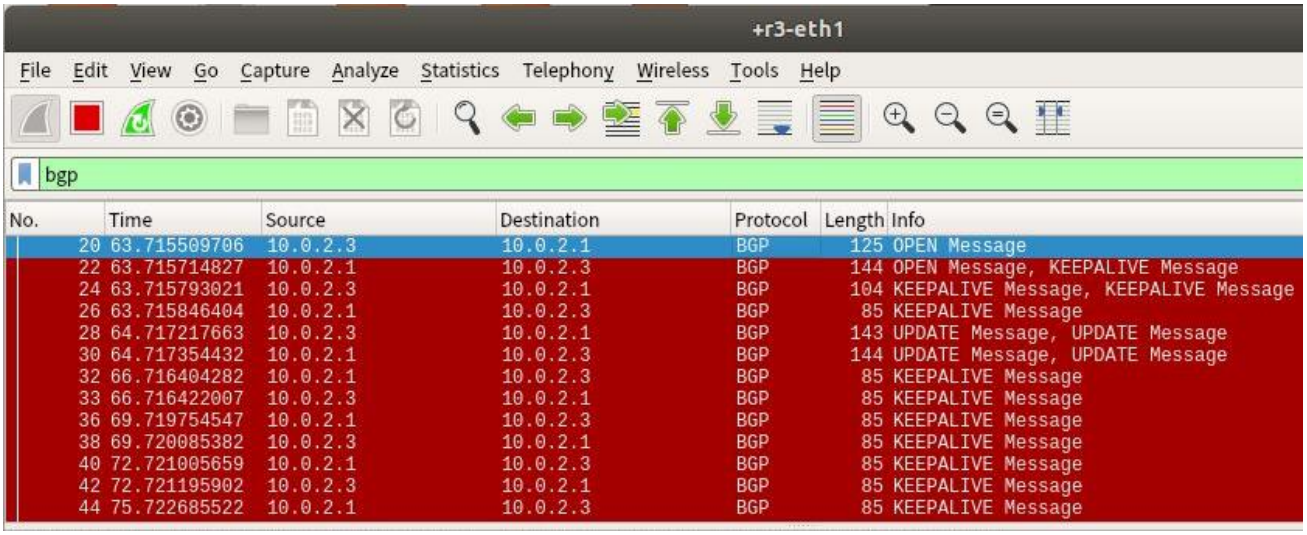


➔ BGPD daemon 顯示了此 router 連接之其他 router 以及其所在之 AS。左上 r1、右上 r2、左下 r3、右下 r4。

3. Capture BGP packets from wireshark and take screenshot to verify your answer for the following questions (20%)
   3-1 Show BGP packets (OPEN, UPDATE, KEEP ALIVE) exchanged by r2 and r3

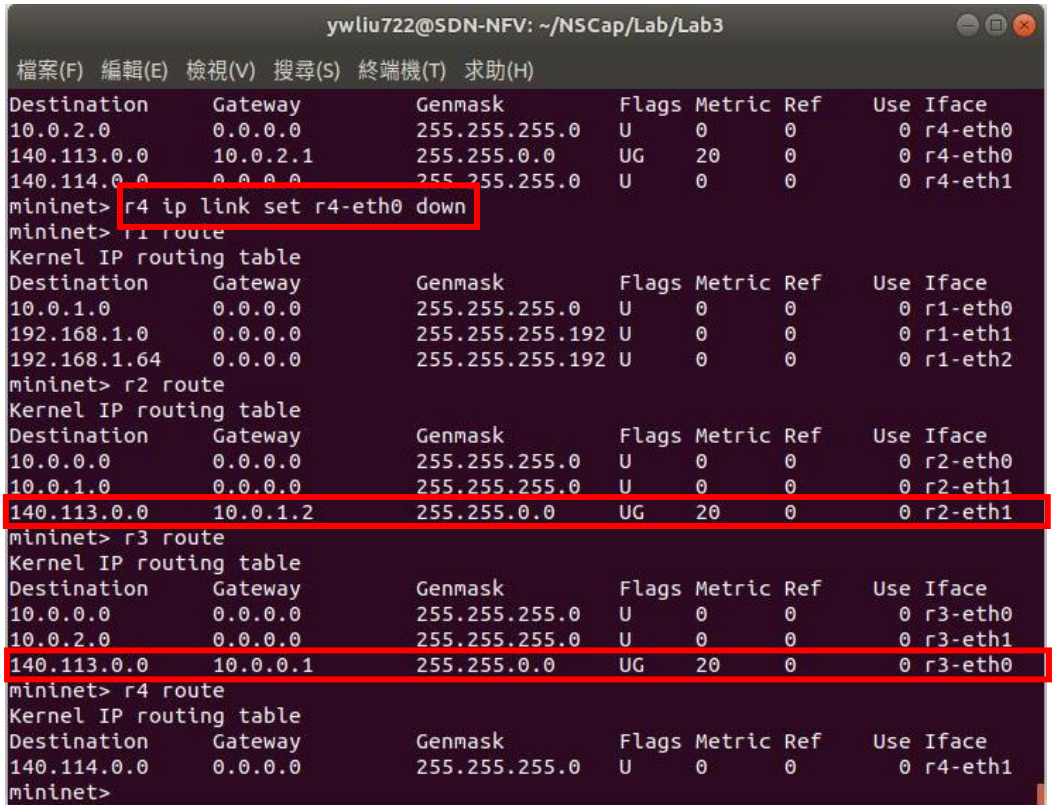






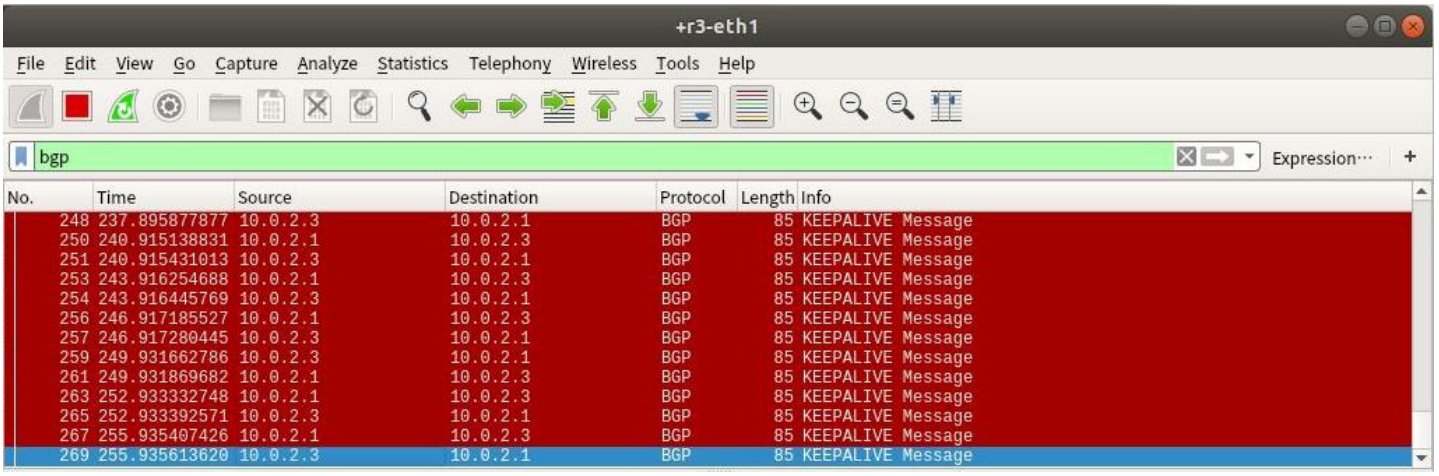
➔ r2-eth0 以及 r3-eth0 可以列出 r2 以及 r3 兩個 router 之間的交換訊息封包、r3-eth1 可以列出 r3 以及 r4 兩個 router 之間的交換訊息封包。

3-2 What will happen to the routing table if you set r4-eth0 down?



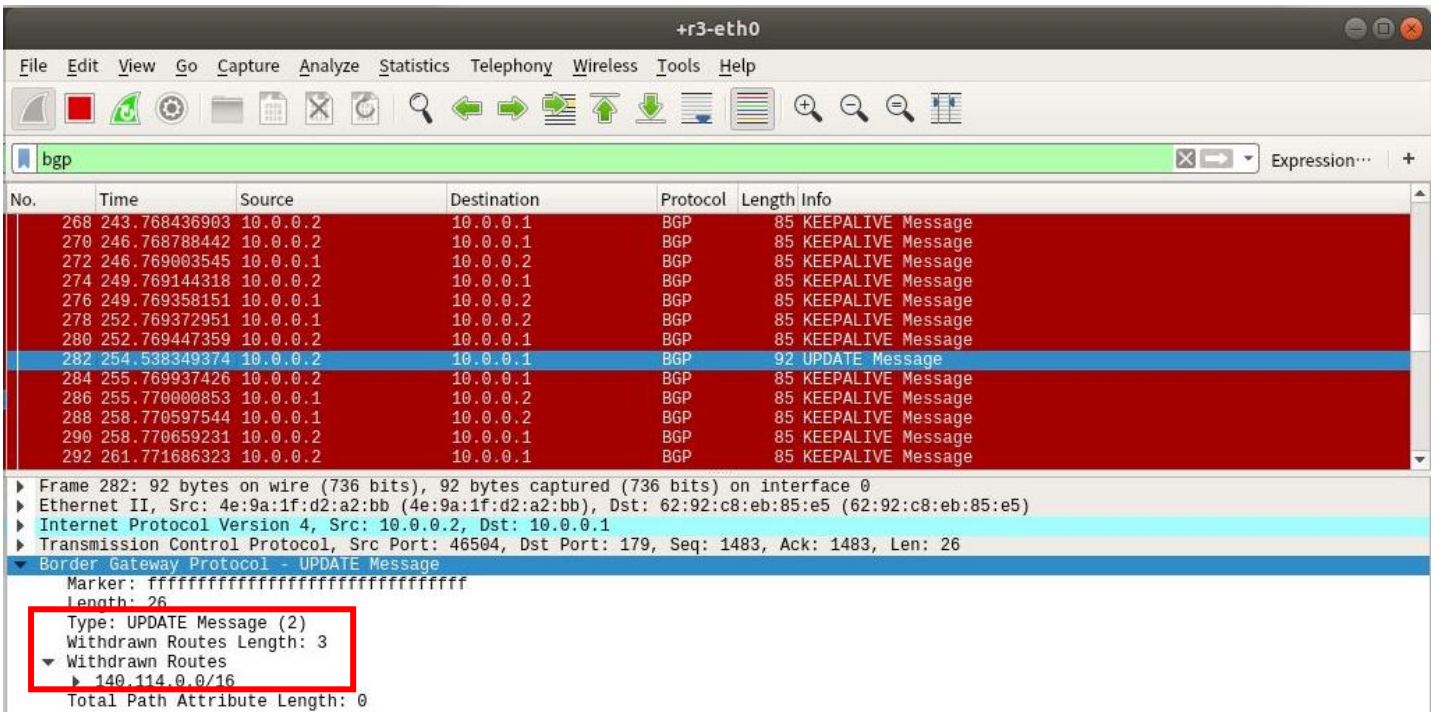
➔ 此圖爲執行指令後的 routing table。將 r4 的 eth0 介面關閉後，r4 便無法和外部交換 BGP keep alive 封包，故其他 router 會認爲 r4 已經關閉，便將 r4 所在之子網域從 routing table 移除。

3-3 How does r3 know r4 is unreachable? Explain how



➔ 此圖爲 r3-eth1 所經過之 BGP 封包。如上題所述，r4 的 eth0 介面關閉後 r3 的 eth1 便無法與之聯繫，BGP keep alive 封包的持續傳輸也隨之停止，r3 也因此得知 r4 目前爲 unreachable 的狀態。

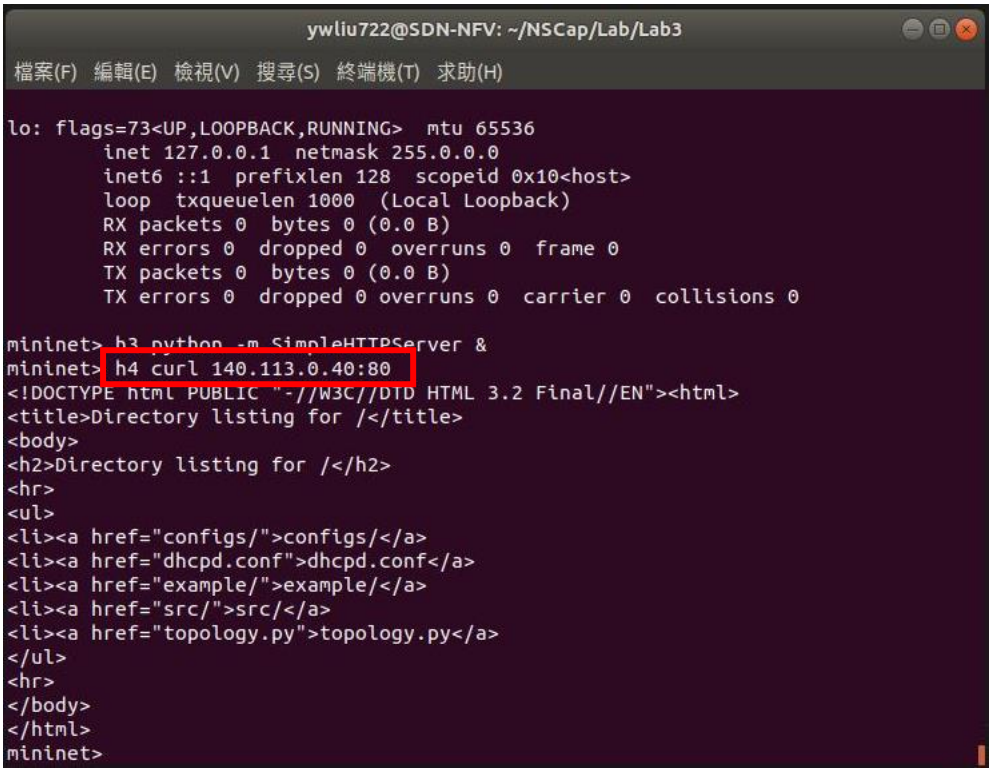
3-4 How does r2 know r4 is unreachable? Explain how



➔ 此圖爲 r3-eth0 所經過之 BGP 封包。由於 r3 已經得知 r4 爲 unreachable 的狀態，所以會傳送 BGP update 封包(withdraw routes)給所有連接的 router(目前只剩下 r2)，告訴所有 router 之前存在的 r4 現在已經離線，所以要更新會經過該點的路由或是 r4 所在的子網域路由，因此 r2 便能知道 r4 目前爲 unreachable 狀態。

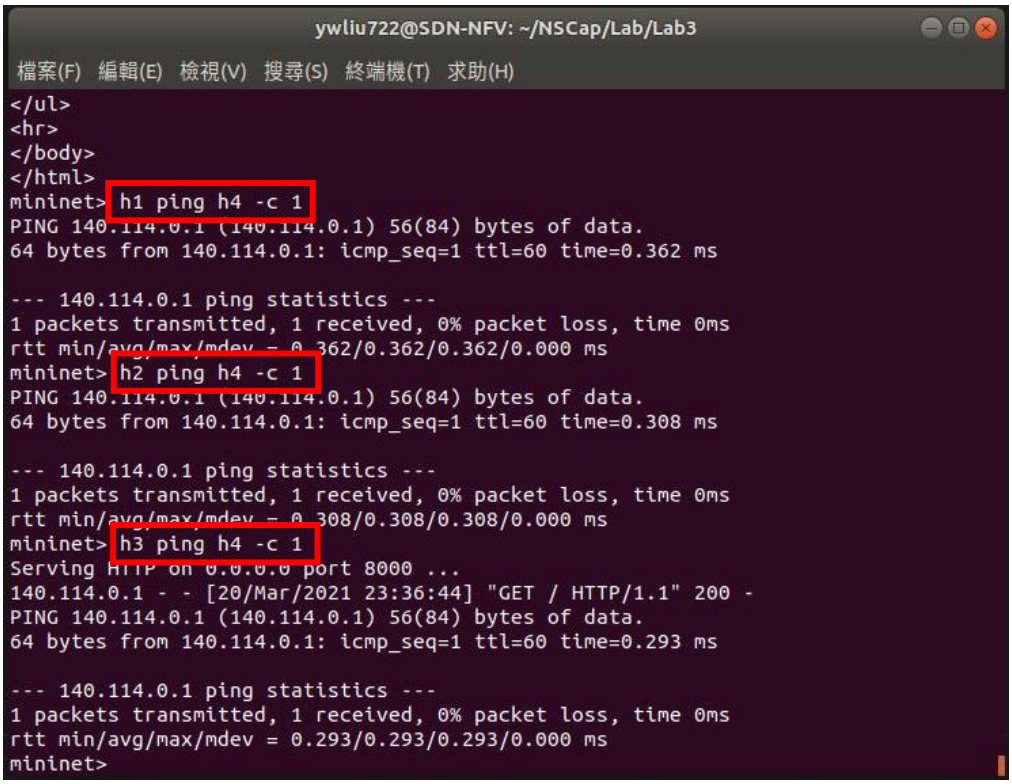
Part 2 Source NAT and Destination NAT

1. Take screenshot of curl result (10%)



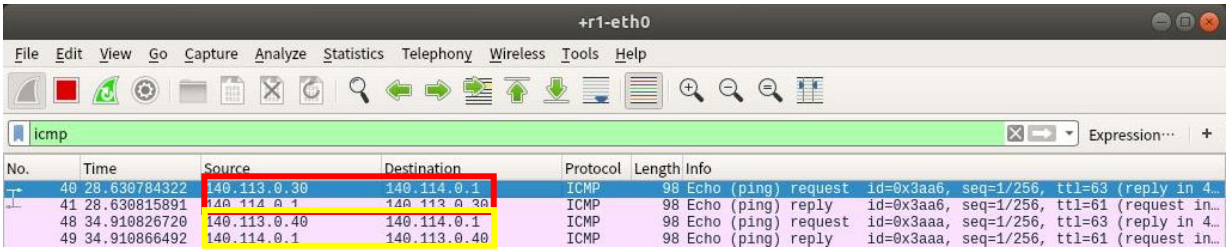
➔ 此爲 h4 透過 curl 這個程式來聯繫位於 h3 上的 HTTP server 所得到之回傳訊息。由於我們有在 iptables 設定 DNAT，故外部的 h4 可以與子網域內的 h3 聯繫。

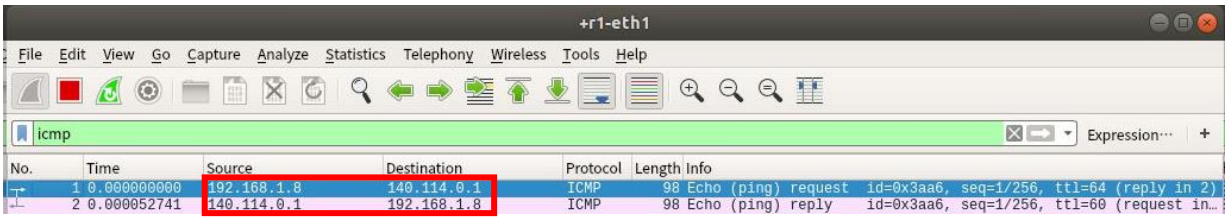
2. Check reachability and take screenshot (10%)

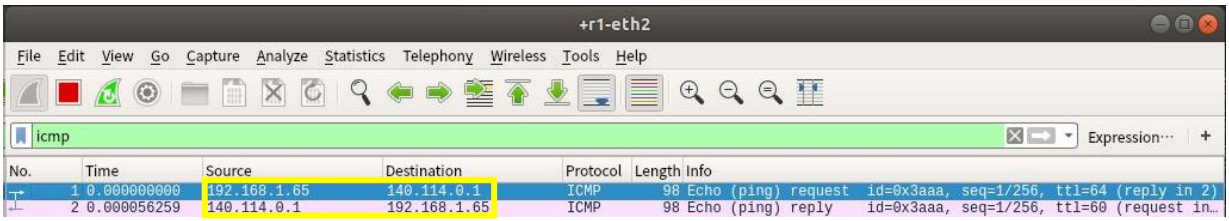


➔ 此圖爲 h1、h2、h3 對 h4 執行 ping 指令的結果。由於我們有在 iptables 設定 SNAT，故可以將封包於傳出 r1 之前改變 source IP，r1 在收到來自 h4 的回應封包之後，也可以透過 SNAT 所轉換的結果將封包回傳給對應的 host，所以 h1、h2、h3 之間是可以連通的(h1 有先透過 DHCP 取得 IP(from Lab2)，故也可以和 h4 連通)。

3. Run wireshark on r1 to take screenshot of input/output packet (10%)
   Explain the difference of packet headers







➔ 根據 SNAT 的設定，192.168.0.0/26 的 IP 會轉換爲 140.113.0.30、192.168.0.64/26 的 IP 會轉換爲 140.113.0.40，可以從上圖觀察出 r1 在 eth1 以及 eth2 接收到的封包，會根據所在之子網對 source IP 進行轉換，使外部網路所看到之 source IP 皆來自 140.113.0.0/16，而非子網內的 192.168.0.0/24，收到回應封包後也會根據 SNAT 轉換規則將 destination IP 改爲子網內的 IP。