

路由器操作設定

I. 實驗目的

本實驗的目的是希望學生藉由使用模擬程式練習操作設定路由器(router)，利用路由器連通不同的子網路以建立簡單的網路雛型，並在實驗中了解路由協定(routing protocol)以及存取控制表列(Access Control List)在網路內所扮演的角色，以更深一層了解 OSI 協定層次架構的意義。

實驗報告的內容應包含：實驗題目、參與人員及單位、目的、設備、方法、記錄、問題討論、心得。報告內容應是經討論、整理、濃縮後，重新詮釋而寫出，切勿全部剪下、照單全貼。

所列實驗方法為參考用，若有更好的方法請在報告問題討論裡的「自問自答題目」裡詳述步驟，會有額外的加分。

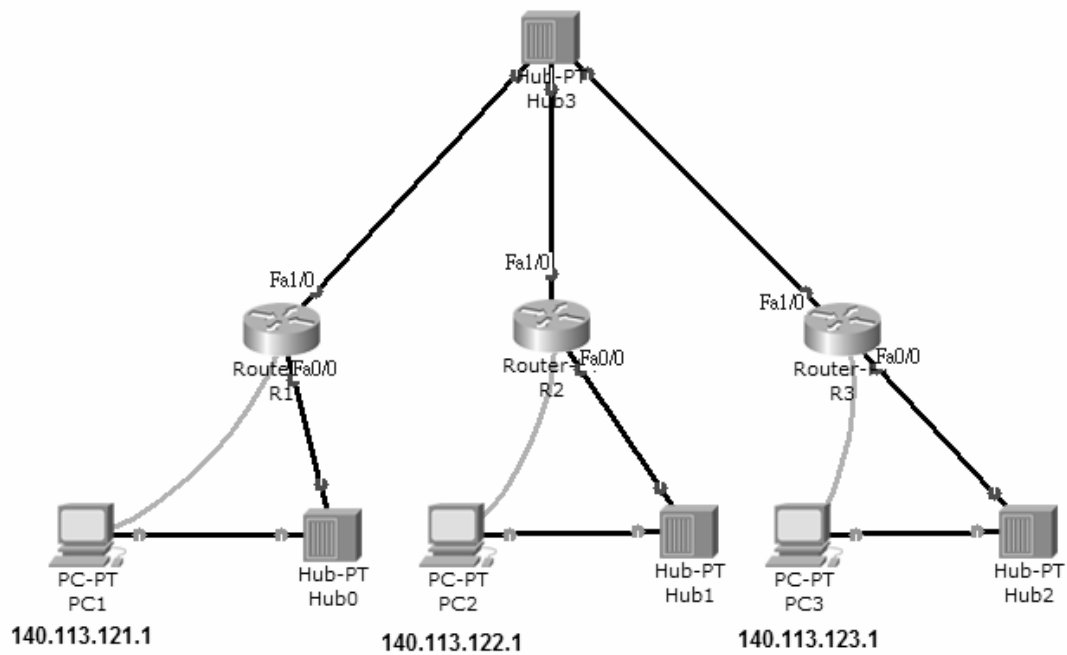
II. 實驗設備

一、軟體

項目	數量	備註
Packet Tracer 4.0	1	由各組向助教索取。

實驗的架構如【圖 11-1】，其中 s 表 serial interface，e 表 Ethernet interface 即 AUI¹；實驗一開始請使用 packet tracer 佈置出如圖所示之環境，並使用軟體所提供之設定畫面，確實設定好各 pc 之 ip 及 netmask。另外，雖然軟體也有提供方便的選定畫面，讓使用者不需透過 CLI 來設定 router，但不建議各位使用該功能。畢竟在實際的操作時，並不會有這項功能。請依照實驗步驟的說明，由連到各 router 之 pc 作 telnet 登入動作，來設定 router，才能確實達到練習 router 設定之目的。

¹ AUI (Attachment Unit Interface)為 10 Mb/s Ethernet 使用之介面。



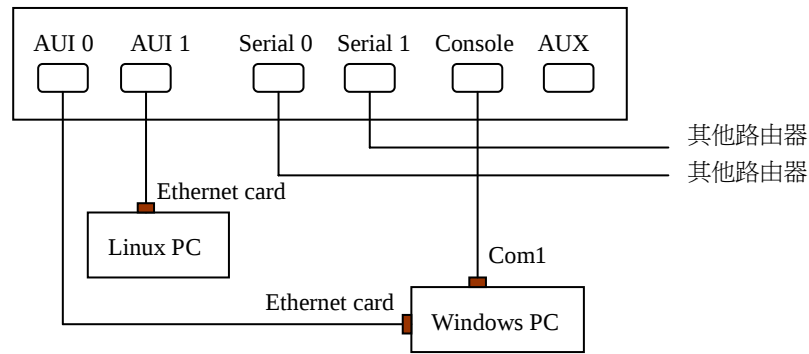
【圖 11-1】IP 分配環境初始設定圖。

IP 分配	R1.e0: 140.113.121.254	R1.e1: 140.113.120.1
	R1.s0: 140.113.1.1	R1.s1: 140.113.2.254
	R2.e0: 140.113.122.254	R2.e1: 140.113.120.2
	R2.s0: 140.113.2.1	R2.s1: 140.113.3.254
	R3.e0: 140.113.123.254	R3.e1: 140.113.120.3
	R3.s0: 140.113.3.1	R3.s1: 140.113.1.254

III. 背景資料

本節首先介紹實驗中所使用的路由器 Cisco 2514 的規格 [1]，以了解其各介面的作用；其次介紹路由協定以及 Cisco 2514 所支援的一些路由協定，以了解路由協定對路由表(routing table)的影響；最後介紹存取控制表列，以了解路由器如何利用過濾功能以保護網路安全。

一、Cisco 2514 介面規格



【圖 11-2】Cisco 2514 router interface

【圖 11-2】是一台 Cisco 2514 router 的介面，包括了兩個 AUI (Attachment Unit Interface)、兩個 serial ports、一個 console 及一個 AUX (AUXiliary port)。其中 AUI 是 router 與 Ethernet Transceiver 的連接介面；而 serial port 則是 router 與 WAN (廣域網路) 的連接介面，簡單的說它是用來做 router 互相連接的介面；另外 console 則是用來與主機(可以是一台 PC)連接的介面，如此可透過主機直接對 router 做設定修改；最後的 AUX 則是用來連接數據機的（此實驗中不會用到）。

由上圖可知利用單一台 router 使其兩個 AUI 介面各連接一台 PC，且其中一台 PC 可再利用其 COM1 介面與 router 的 console 介面連接當 router 主機，透過對 router 做適當的環境設定，則可以做出兩個最難型的子網路。

二、路由協定

我們可以將 routing protocol 分為二大類：靜態(static)與動態(dynamic)。當靜態的 routing table 無法正確反應網路狀況時，則以動態協定所建立的 routing table 來修補。但是當網路大到某種程度時，table 不可能詳盡的記錄到所有的網路節點，此時需要有個 default router，當在 routing table 中找不到對應記錄時封包將送往此 default router，由其負責繞路。一個網路系統（可能是一個企業的系統，包含一個 default router）稱為一個 AS (autonomous system)，適用於一個系統內的 routing protocol 稱為 Interior Routing Protocol，適用於系統之間的 routing protocol 則為 Exterior Routing Protocol。

動態 Routing protocol 則可再分為二大類[2]：distance vector routing 以及 link state routing。其中 distance vector routing 的運作是靠每個 router 與相鄰 router 交換 distance vector(即由該 router 到所有其他 router 的距離)，每個 router 根據這些 local 交換的 vector 來更動自己的 vector，即更動 routing table，如 RIP [3]。而為維護此 routing table，相鄰 routers 需定期互送訊息以確定表格所記錄的資料沒有過期。而 link state routing 中，每個 router 將自己連接的 link

的狀態廣播給其他 router，每一個 router 再根據這些 global 資訊計算路徑，如 OSPF [4]。

以下簡單介紹三種本實驗所涉及的 routing protocol，注意這些協定皆屬於 Interior Routing Protocol。

1. Static Routing

由系統管理者自行設定到某目的 IP 位址或目的子網路的路徑（routing table），好處是比較有安全控制以及可減少流量。

2. RIP (Routing Information Protocol) [3]

RIP 屬於 distance vector routing，記錄 hop count 以決定最佳路徑，其最大可允許的 hop count 為 15，預設每 30 秒就與鄰近的 router 互送訊息。當網路有斷線情況時會有 count-to-infinity 的問題，故適用於較小的 AS。

3. IGRP (Interior Gateway Routing Protocol) [5]

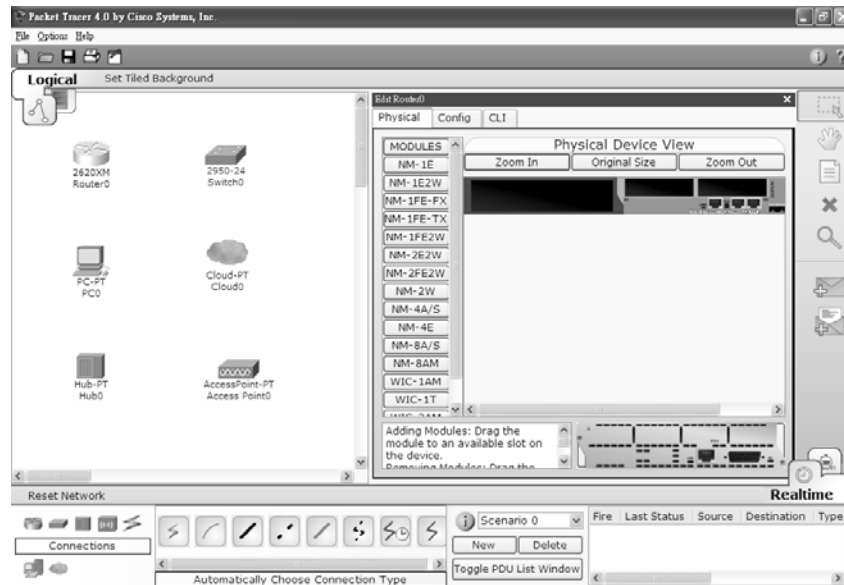
此處的 IGRP 是 Cisco 公司自己發展的一個 distance vector routing protocol，使用一組參數來決定最佳路徑，此組參數包括了頻寬(Bandwidth)、延遲(Delay)、網路負載量(Load)、可靠度(Reliability)以及最大傳送單位(Maximum transmission unit)。

三、路由器模擬程式(Packet Tracer)

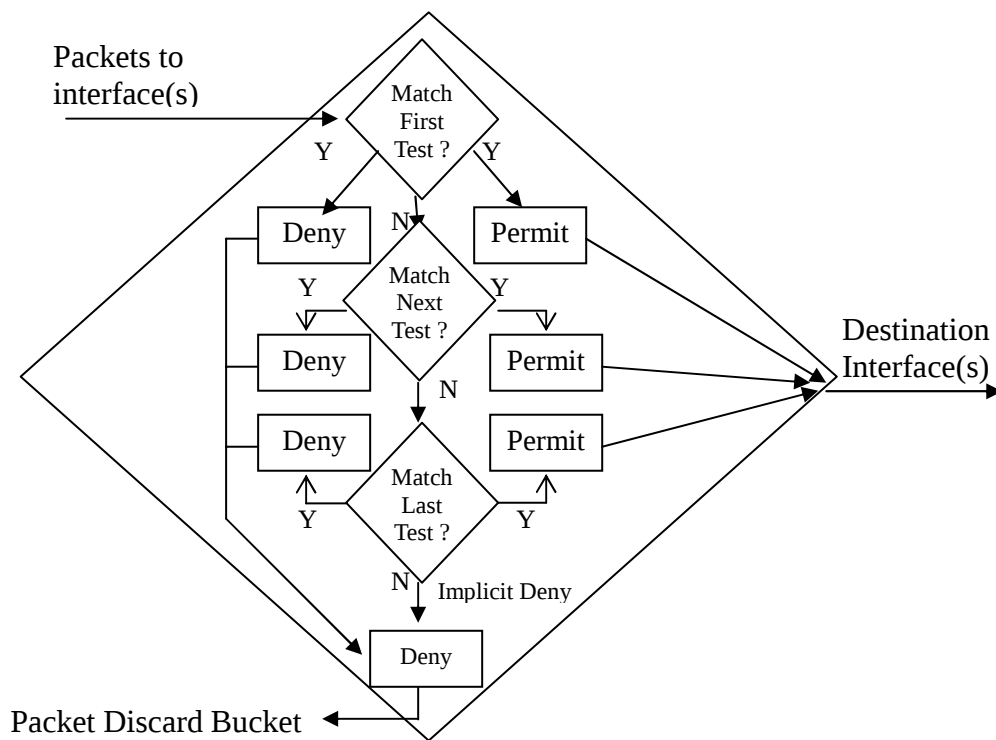
Packet Tracer 是一套由 Cisco 所設計的路由器模擬程式。由於路由器的取得較為不易，尤其以本實驗而言，需要三部路由器、三部個人電腦，以及三個集線器才能夠架設好實驗平台。而 Packet Tracer 提供了一個方便的模擬方式，只要在程式內的平面圖上，佈上實驗所需之設備(如圖一)，即可以在個人的電腦上，作模擬的網路配置，使用者亦可以在各種設備的圖示上作模擬的操作；如 pc 設備可以提供遠端登入畫面，讓使用者登入此 pc 使用 rs232 埠連接之 router。遠端登入設定該 router 之功能，幾乎和使用一般設備相同，相同方便。

四、存取控制表列(Access Control List)

存取控制表列 [6] 的功能就是可以拒絕某些你不想要的 packet，例如某個 IP 位址的 packet 或是某種 traffic type(如：FTP, TCP, ICMP...)的 packet，進而維護網路安全。【圖 11-4】是其檢驗流程，其中已有三個存取控制表列，有如三個 filters。



【圖 11-3】Packet Tracer 軟體畫面



【圖 11-4】存取控制表列運作流程圖。

IV. 實驗方法與步驟（以第二台Router為例）

安裝好 Packet Tracer 這套軟體之後，可以使用畫面顯示各元件，來配置出如圖一所示之網路環境。需注意的一點就是，各元件之間的連線所使用的線材設備是有所區別的，例如 pc 與 router 之間的連接、使用 rs232 埠連接到 router 之 console 埠之連接，以及 pc 與 hub 之間、hub 與 router 之間需透過網路線來連接。由於每台 router 的 console 介面是與 PC 的 COM1 連接，所以各組必須透過 PC 來操作實驗。實驗流程大致可分四大步驟：第一步驟為初始化，即開啓軟體中 Windows 的應用程式 Hyper Terminal 做為操作 router 的介面。第二步驟為分別設定 router 四個介面 (e0, e1, s0, s1) 的 IP 位址，若設定無誤，則此 router 已透過(e0, e1)連通兩個子網路了。第三步驟目的為測試 routing protocol，學習如何在 static routing table 中加入 routing entry，如何取消或重新啓動 RIP、IGRP routing protocol，在使用不同 routing protocol 的狀況下觀察 routing table 有何不同；在此步驟中將利用 serial cable 串接所有的 router，使得路由得以多方向進行。第四步驟則為測試存取控制表列的功能；由於資料封包在每段連線中是可雙向流動的，所以在此步驟中將利用存取控制表列的功能把連接 router 的兩段 serial cables 改為單向流通，即對某台 router 而言，屬於某 IP 位址的資料封包只能出不能進，進而達到保護的功能。

0. 準備開始

- 0.1 在下指令的過程中，任何時刻都可以打 “?” 尋求線上支援。
- 0.2 使用 ctrl-c 可中斷正在執行的指令。
- 0.3 在 ‘[]’ 中為預設值，若要接受預設值則直接按 enter。
- 0.4 Cisco 的機器要 disable 某項功能時，其指令格式通常為: “**no command parameter**”，其中若不加 “no” 則表要 enable 此功能。
- 0.5 常用指令(在回答問題的時候你可能需要用到這些指令)
 - 0.5.1 ping xxx.xxx.xxx.xxx (檢測與某 IP 位址是否連通)
 - 0.5.2 show ip route (觀看 routing table)
 - 0.5.3 show ip protocols (觀看目前此 router 有那些 routing protocol 是 enabled)
 - 0.5.4 traceroute xxx.xxx.xxx.xxx (觀看到某 IP 位址的 routing path)
 - 0.5.5 show access-lists (觀看目前有那些已設定的 access-lists)

1. 初始化（**黑體字**部份為由 keyboard 所做的輸入）

- 1.1 點選畫面中 PC2 電腦圖示
- 1.2 進入右邊出現之視窗，點選 Desktop 標籤，點選 terminal 選項，會出現 Terminal Configuration 畫面。
- 1.3 “Bit Per Second” 選項選擇 “9600”，即設定與 console 連接的速度，
- 1.4 “Flow control” 選擇 “Hardware”，
- 1.5 其它設定則使用預設值，按 “OK”。

- 1.6 R2> **enable** (“R2>”為 command prompt，所下指令為進入 enable mode)
- 1.7 通常 router 會詢問密碼，由於我們使用的是模擬器，不會詢問密碼
- 1.8 R2#**write erase** (清除 Nonvolatile Random Access Memory 內已有的設定)，按 y 確定

- 1.9 此時 initial interface 應如下(四個 interface 都沒設定)：

Any interface listed with OK? value "NO" does not have a valid configuration

Interface	IP-Address	OK? Method	Status	Protocol
Ethernet0	unassigned	NO unset	up	up
Ethernet1	unassigned	NO unset	up	up
Serial0	unassigned	NO unset	up	up
Serial1	unassigned	NO unset	up	up

2. 設定 router 的 hostname 及四個 interface 的 IP 位址

- 2.1 R2#**configure terminal** 進入設定模式
- 2.2 R2(configure) # **hostname R2** 更改 router hostname 為 r2
- 2.3 Configuring interface FastEthernet0/0:
R2(config)#**interface fastethernet0/0**
R2(config-if)#**ip address 140.113.122.253 255.255.255.0**
- 2.4 Configuring interface FastEthernet1/0:
R2(config)#**interface fastethernet1/0**
R2(config-if)#**ip address 140.113.120.2 255.255.255.0**
- 2.5 Configuring interface Serial2/0:
R2(config)#**interface Serial2/0**
R2(config-if)#**ip address 140.113.120.2 255.255.255.0**
Configuring interface Serial3/0:
R2(config)#**interface Serial3/0**
R2(config-if)#**ip address 140.113.120.2 255.255.255.0**

Note: 一開始連線到 router 的時候是在 normal mode；在 normal mode 下使用 enable 指令並輸入正確密碼之後就可進入 enabled mode。

Note:此時 RIP 是 enabled，需另下指令才能 disable 掉。

【記錄 1】觀看目前的 routing table，記錄各 interface 連線狀況，並解釋。

【記錄 2】ping 自己 subnet 及其它 subnet 上的 IP 位址，記錄哪幾台是可連通的。

3. 設定 static routing table and routing protocols

在此步驟中，將先測驗 static routing 的功能，在 disable RIP 和 IGRP 後再測試可以接通那些子網路，註此時的 route 都仍是透過 Ethernet。

接著我們將利用 serial cable 來串接三台 router，增加 routing 的方向，enable RIP 和 IGRP，測試這兩種協定的功能。

3.1 新增 static routing table entry

3.1.1 R2>**enable** (進入 enabled mode)

3.1.2 R2#**configure** (“R2#” 為 enabled mode 的 command prompt，下 configure 指令才能修改環境設定)

Configuring from terminal, memory, or network [terminal]?

Enter configuration commands, one per line. End with CNTL/Z.

3.1.3 R2(config)#**ip route 140.113.121.0 255.255.255.0 140.113.120.1**

Note: ip route 為新增一筆資料到 static routing table 的指令，其後所接的參數意義為將往 140.113.121.x (140.113.121.x 與 255.255.255.0 netmask 的結果)的 packet 都 forward 至 140.113.120.1 (在 2.15 步驟中設定了子網路部份的 bit 數目為 8，所以到 140.113.120.1 的封包會透過 120.113.120.2，即 e1 介面送出)。

3.1.4 R2(config)#**ip route 140.113.123.0 255.255.255.0 140.113.120.3**

Note:要往 140.113.123.0 子網路的 packet 都 forward 到 140.113.120.3

【記錄 3】記錄可 ping 其它子網路的 IP 位址。

3.2 Disable routing protocols

3.2.1 R2#**configure**

Configuring from terminal, memory, or network [terminal]?

Enter configuration commands, one per line. End with CNTL/Z

3.2.2 R2(config)#**no router rip** (disable rip)

3.2.3 R2(config)#**^Z** (Ctrl+z)

3.2.4 R2#

【記錄 4】記錄目前有那些 routing protocol 是 enable 的。

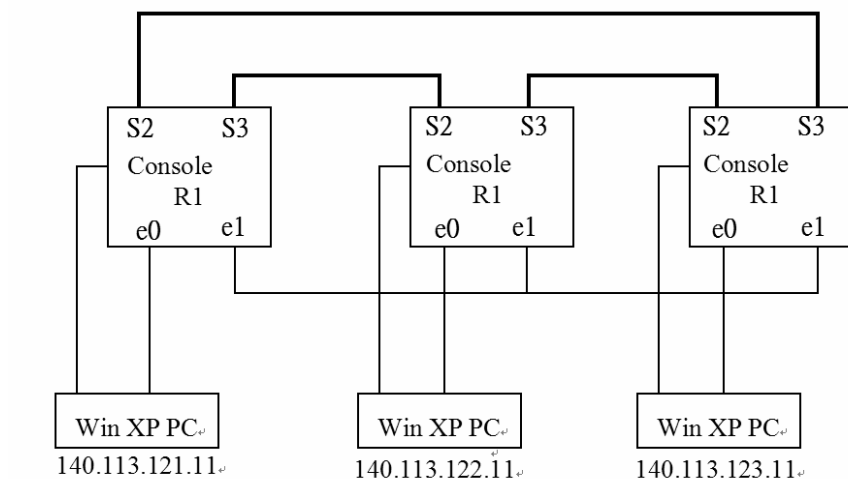
【記錄 5】觀看目前的 routing table，記錄各 interface 連線狀況並解釋。

【記錄 6】將 e1 的線拔掉，是否可 ping 到其它子網路的 IP 位址？

3.3 連接 routers 之間的 serial interface 並設定 clock rate。

3.3.1 用 serial cable 串接 serial interface，其線路請參照【圖 11-5】粗線部份。

3.3.2 由連接 serial cable DCE (Data Communications Equipment)端的機器設定 serial cable 的 clock rate，此例假設連接第二台 Router serial 2 的 serial cable 是 DCE 端，所以只有設定 interface serial 2，在操作時請考慮實際狀況。



【圖 11-5】加上 serial cable 後的網路環境

3.3.3 R2#configure

Configuring from terminal, memory, or network [terminal]?

Enter configuration commands, one per line. End with CNTL/Z.

3.3.4 R2(config)#interface serial 2/0 (設定 serial 0)

3.3.5 R2(config-if)#clock rate ? (在下指令的過程中可隨輸入 “?”, 系統會顯示有那些參數可以選擇, 如下所示)

```
Speed (bits per second
1200
2400
4800
9600
19200
38400
56000
64000
72000
125000
128000
148000
250000
500000
800000
1000000
1300000
2000000
4000000
<300-4000000> Choose clockrate from list above
R2(config-if)#clock ra
```

3.3.6 R2(config-if)#clock rate 1000000

3.3.7 R2(config-if)#exit

3.3.8 R2(config)#exit

【記錄 7】觀看目前的 routing table, 記錄各 interface 連線狀況並解釋。

Note:一條 serial cable 的兩端各為 DTE(Data Terminal Equipment)端或 DCE 端，並分別有標籤標示，例如：V.35 DCE REV. DO ...。而只能藉由 DCE 端才能設定 clock rate，實驗時每條 serial cable 都需由其 DCE 端設定 clock rate。

3.4 Enable 及 configure RIP

3.4.1 R2#configure

Configuring from terminal, memory, or network [terminal]?

Enter configuration commands, one per line. End with CNTL/Z.

3.4.2 R2(config)#router rip (enable rip)

3.4.3 R2(config-router)#network 140.113.0.0 (設定需為 140.113.x.x 的網路建立 RIP 的的 routing table)

3.4.4 R2(config-router)#exit

3.4.5 R2(config)#exit

【記錄 8】 觀看目前的 routing table，記錄各 interface 連線狀況，並解釋。

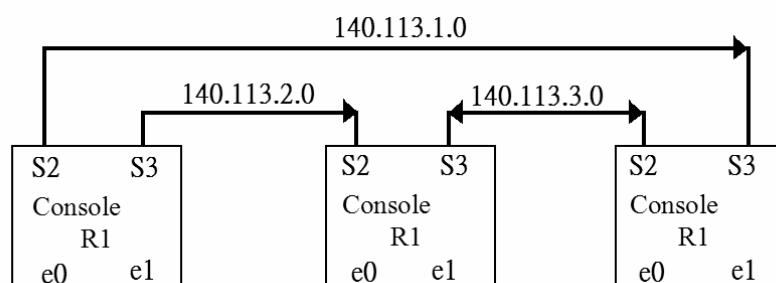
【記錄 9】 只拔掉一條 serial cable，觀看是否能否即時建立新的 routing table 以反應網路狀況，是否出現 count-to-infinity 的問題，並請解釋為什麼有或是沒有出現此問題。

【記錄 10】 觀看目前的 routing table，記錄各 interface 連線狀況並解釋。

【記錄 11】 將 Q9 中拔掉的 serial cable 接回，觀看是否能否即時建立新的 routing table 以反應網路狀況。再將剛接回的線拔掉，看是否出現 count-to-infinity 的問題。

4. Access Control List 的設定

所有的連線一開始都是雙向連通的，在此部份我們要利用 access control list 的過濾功能將屬於 140.113.122.X 的資料封包流動方向改為如【圖 11-6】，因此請確定各 router 所設定的方向是正確的。



【圖 11-6】 屬於 140.113.122.X 的 packets 流向圖。

4.1 R2#configure

Configuring from terminal, memory, or network [terminal]?

Enter configuration commands, one per line. End with CNTL/Z.

4.2 R2(config)#access-list ? (看有那些參數可以選擇)

<1-99> IP standard access list ... 未完

Note:在下指令的過程中隨時可以打 `?`，善用 on-line help

4.3 R2(config)#access-list 1 deny 140.113.122.0 0.0.0.255

(IP standard access list 第一條：拒絕所有 IP 位址是 140.113.122.x 的 packets)

4.4 R2(config)#interface serial 2/0

4.5 R2(config-if)#ip access-group 1 out

(限制 140.113.122.x 的 packets 不能從 serial 0 出去)

Note:此例仍是以 R2 為範例；在此步驟中若最後一個參數是 in，則表不能從 serial0 進入。若步驟 4.4 的參數是 serial 1，則是對 serial 1 的方向做限制。

4.6 R2(config-if)#exit

4.7 R2(config)#exit

【記錄 12】觀看目前已設定那些 access-lists 了。

【記錄 13】開啓 PC 圖示，進入 terminal，由此下 ping 的指令，並記錄是否能 ping 到 140.113.122.x 的機器。若 access-list 的功能生效，在 terminal 下 ping 的指令，會看到什麼訊息？

4.8 取消 access-lists

4.8.1 Router-C#configure

Configuring from terminal, memory, or network [terminal]?

Enter configuration commands, one per line. End with CNTL/Z.

4.8.2 Router-C(config)#no access-list 1

4.8.3 Router-C(config)#exit

5. 請先了解第六節中所列舉的討論問題，若須動手實驗才能找到解答的項目，請先在此實驗之。

V. 實驗記錄

所記錄的 router 是 (R1, R2, R3) ?_____

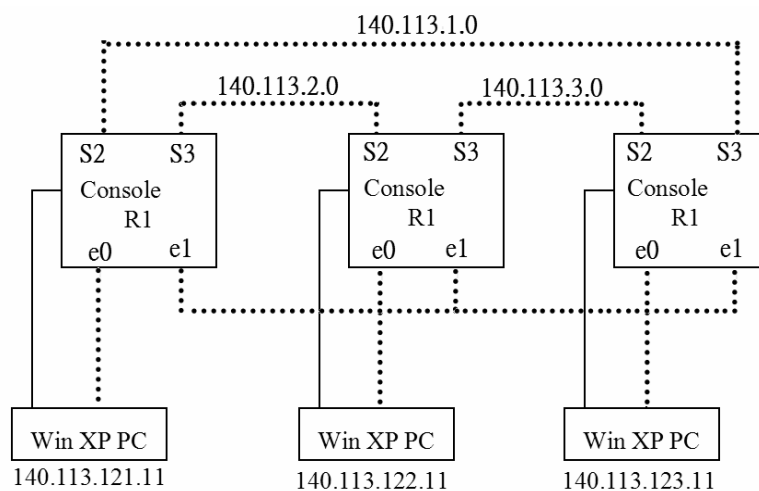
【記錄 1】以你所記錄的 router 為主，一共連接了___個 subnets?

請在下【圖 11-7】將連通的部份由虛線改爲實線，並於實線旁標明連通訊息代號，另外條

列訊息代號及其訊息內容，並註解訊息之意義。

ex: 1: C 140.113.122.0 is directly connected, Ethernet 0

註解:.....



【圖 11-7】網路連通圖(1)。

【記錄 2】請填寫下列表格，並打勾以標示那些 subnet 是屬於此 router 的。

Subnet	可 ping 到的 IP 位址
140.113.1.0	
140.113.2.0	
140.113.3.0	
140.113.120.0	
140.113.121.0	
140.113.122.0	
140.113.123.0	

【表 11-1】網路連通表(1)。

【記錄 3】記錄可 ping 其它子網路的 IP 位址。

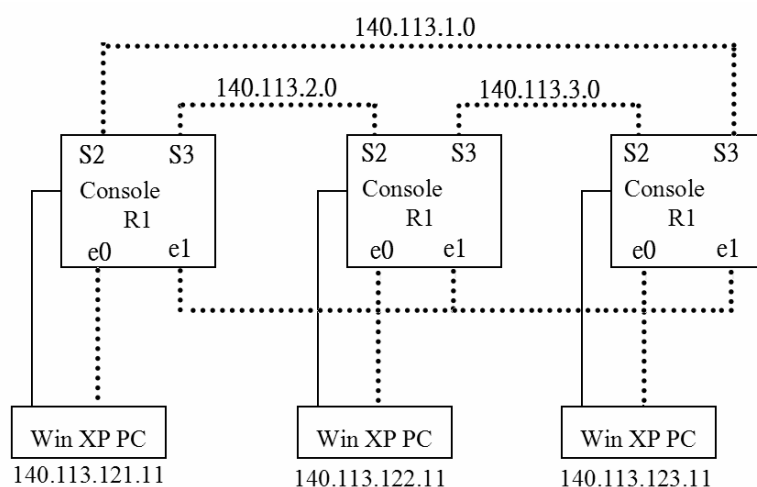
Subnet	可 ping 到的 IP 位址
140.113.1.0	
140.113.2.0	
140.113.3.0	
140.113.120.0	
140.113.121.0	
140.113.122.0	
140.113.123.0	

【表 11-2】網路連通表(2)。

【記錄 4】記錄目前有那些 routing protocol 是 enable 的。

【記錄 5】以你所記錄的 router 為主，一共連接了___個 subnets?

請在下【圖 11-8】將連通的部份由虛線改為實線，並於實線旁標明連通訊息代號，另外條列訊息代號及其訊息內容，並註解訊息之意義。



【圖 11-8】網路連通圖(2)

【記錄 6】記錄可 ping 其它子網路的 IP 位址。

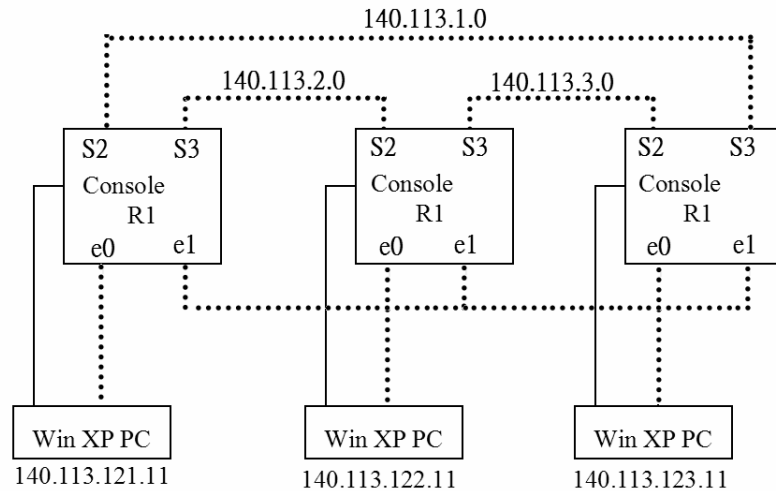
Subnet	可 ping 到的 IP 位址
140.113.1.0	
140.113.2.0	
140.113.3.0	
140.113.120.0	
140.113.121.0	
140.113.122.0	
140.113.123.0	

【表 11-3】網路連通表(3)

【記錄 7】以你所記錄的 router 為主，一共連接了___個 subnets?

請在下【圖 11-9】將連通的部份由虛線改為實線，並於實線旁標明連通訊息代號，另外條

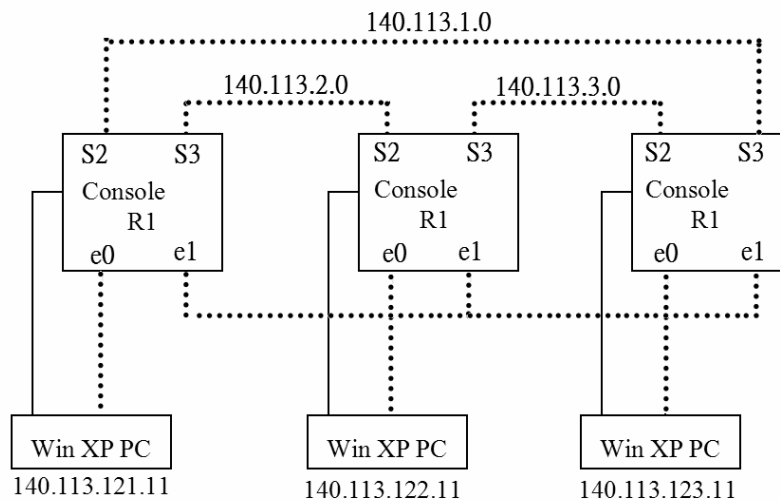
列訊息代號及其訊息內容，並註解訊息之意義。



【圖 11-9】網路連通圖(3)

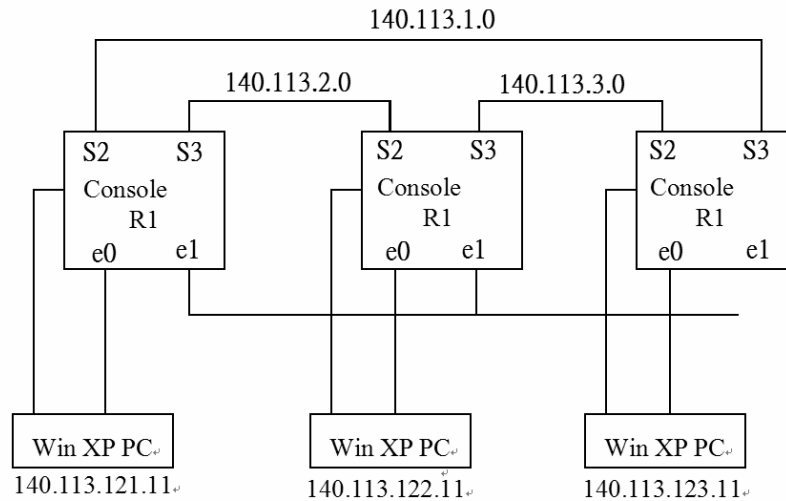
【記錄 8】以你所記錄的 router 為主，一共連接了__個 subnets?

請在下【圖 11-10】將連通的部份由虛線改為實線，並於實線旁標明連通訊息代號，另外條列訊息代號及其訊息內容，並註解訊息之意義。



【圖 11-10】網路連通圖(4)。

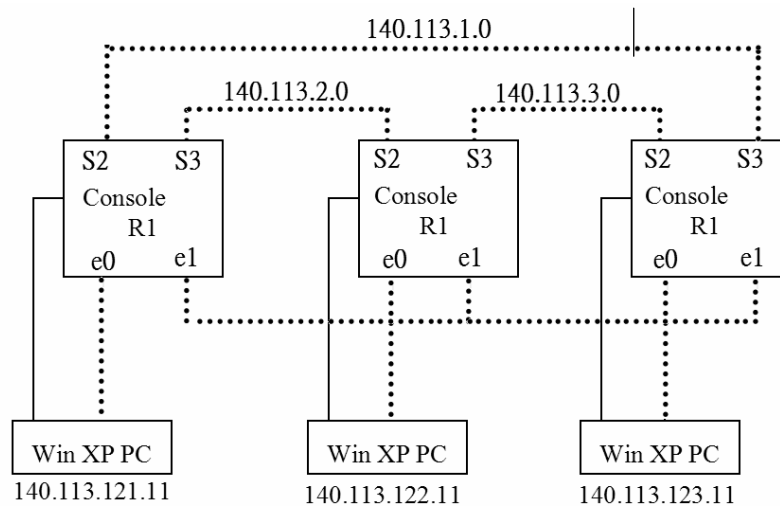
【記錄 9】是否出現 count-to-infinity 的問題，並請解釋為什麼有或是沒有出現此問題，並請於下【圖 11-11】標明是拔掉那條線。



【圖 11-11】網路連通圖(5)。

【記錄 10】以你所記錄的 router 為主，一共連接了___個 subnets?

請在下【圖 11-12】將連通的部份由虛線改為實線，並於實線旁標明連通訊息代號，另外條列訊息代號及其訊息內容，並註解訊息之意義。



【圖 11-12】網路連通圖(6)。

【記錄 11】將 Q9 中拔掉 serial cable 接回，觀看是否能否即時建立新的 routing table 以反應網路狀況。再將線拔掉，看是否出現 count-to-infinity 的問題。

【記錄 12】觀看目前已設定那些 access-lists 了，並說明你下了哪些指令。

【記錄 13】開啓 MS-DOS 模式視窗，由此下 ping 的指令，並記錄是否能 ping 到 140.113.122.x 的機器。若 access-list 的功能生效，在 MS-DOS 下 ping 的指令，會看到什麼訊息？

VI. 問題討論（請善用Cisco的線上支援：輸入’?’）

1. 描述正常及完整的 router 設定程序。
2. 若三台 routers 設定使用不同的 routing protocol，會不會產生問題，請解釋原因。
3. 若 3 個 LAN 的 IP subnet 設成一樣，會產生什麼樣的問題？
4. 如何在一個 subnet 上限制及禁止使用某一種 application？

Hint: access-lists extended lists (100-199) can test conditions of

- (a) Source and destination addresses
- (b) Specific TCP/IP-suite protocols
- (c) Destination ports

5. 如何將一個 subnet 切割成兩個分開的 subnet？

例如將一個 140.113.121.X 分成 140.113.121.0X 及 140.113.121.1X。

Hint: 在 configure router interfaces 的時候，number of bits in subnet field 不一定要設 8

6. RIP 的 count-to-infinity 問題是如何產生的？畫圖舉例說明要在什麼樣的網路環境下才能看出此問題的存在。
7. 自問自答，即自行提出問題並尋找解答。

VII. 參考文獻

- [1] Cisco 2500 Series Router Installation and Configuration Guide, http://www.cisco.com/univercd/cc/td/doc/product/access/acs_fix/cis2500/2514/index.htm.
- [2] Andrew Tanenbaum, “*Computer Networks*”, Prentice Hall, 3rd edition, 1996.
- [3] G. Malkin, “*RIP Version 2*”, RFC 2453, November 1998.
- [4] J. Moy, “*OSPF Version 2*”, RFC 2328, April 1998.
- [5] An introduction to IGRP, <http://www.cisco.com/warp/public/459/2.html>.
- [6] Access Control List: Overview and Guildlines, http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/secur_c/scprt3/scacsls.htm.