實驗五
網路探測：路徑、延遲與流量統計

Ⅰ. 實驗目的

本實驗的目的是希望同學能了解網路量測工具的種類及運作原理，利用工具探測網路連線之路徑、延遲及阻塞的瓶頸，並且上網站蒐集一些網路流量統計資料。

實驗報告應該包括下列項目：實驗名稱、組員與系級（撰寫報告者列於首位）、實驗目的、實驗設備、實驗背景知識、實驗方法與步驟、觀察與記錄、問題與討論、心得及參考資料。

Ⅱ. 實驗設備

本實驗所使用的作業平台不拘，只要探測軟體能夠適用即可。由於網路探測工具眾多，且漸漸趨向整合性和圖形化，所以功能常常彼此重疊。下面將網路探測工具大致分爲六大類，分別列出數種代表性的工具以供參考。本實驗以路徑探測與網路效能分析爲主，同學可自行採用表 5-1～5-7 或以外的適當工具來實驗。

一、硬體

項目	數量	備註
個人電腦 PC	1	
網路卡	1	其他撥接工具（如 Modem）亦可

二、軟體

IP Domain/Address 查詢工具		
軟體名稱	**功能簡介**	**作業平台**
DNS workshop [1]	轉換 IP 位址及 Domain name 的工具。	Windows
DynIP [2]	自動追蹤到目前撥接上 Internet 的 IP 位址。	Windows/UNIX

【表 5-1】IP Domain/Address 查詢工具

遠端主機狀態查詢工具		
軟體名稱	功能簡介	作業平台
Ping	確認遠端主機是否 alive 的工具。	Windows/UNIX
Mping [3]	Multicast ping 數個主機以確認它們是否在上線。	Windows
Pingplus [4]	增強版的 ping，含 ping, tracert 等。	Windows
Tjping Pro [5]	Ping Client 及 trace 路徑。	Windows

【表 5-2】遠端主機查詢工具

路徑查詢工具		
軟體名稱	功能簡介	作業平台
Traceroute	可查詢本地主機至任意站台間的路徑及延遲。	Unix
Tracert	可查詢本地主機至任意站台間的路徑及延遲。	Windows
Visual route [6]	圖形化的介面，主要功能與 traceroute 相近，但可自動分析網路問題癥結，另外也有增強新的功能。	Windows/UNIX

【表 5-3】路徑查詢工具

傳輸效能分析工具		
軟體名稱	功能簡介	作業平台
Ttcp [7]	可產生 TCP 或 UDP 的 traffic，觀察網路傳輸的情形。	Windows/UNIX
TracePlus [8]	分析通訊協定 TCP/IP 等資料傳遞情況與 WINSOCK 運作狀況程式。	Windows
NetMedic [9]	診斷網路塞車的原因是電腦本身、ISP、或是遠端機器。	Windows

【表 5-4】傳輸效能分析工具

網路監聽工具		
軟體名稱	功能簡介	作業平台
Ethereal	可截取並分析 LAN 上的封包，提供 GUI 的操作。	Unix/Windows
Tcpdump	可截取封包，分析網路傳輸速度等資料。	Unix
NetXRay	可截取及產生封包，分析監聽到的封包內容。	Windows

【表 5-5】網路監聽工具

其它分析工具		
軟體名稱	功能簡介	作業平台

Modem monitor graph [10]	以圖形顯示出數據機撥接上 Internet 後封包資料的接收傳遞以及 CPU 使用狀況等的數據。	Windows
Web Trends Log Analyzer [11]	極富盛名的 Web Server 流量與使用量分析工具，將詳盡的分析結果以 HTML 方式呈現。	Windows
Yonc [12]	檢查上線的 ISP 線路是否忙碌，保持在網際網路的活動，以免因閒置過久而斷線。監視 Email 帳號，上線時間，上網花費，網路頻寬等等。	Windows

【表 5-6】其它分析工具

整合套裝工具		
軟體名稱	**功能簡介**	**作業平台**
AckNak [13]	取代原來的 WSPING32，功能增加包括 Ping、Traceroute、 DNS Lookup、 Finger、 Whois 等工具。	Windows
NetInfo [14]	包括 Local Info、Ping、Trace、Look Up、Finger、Whois、Scanner 的 Services.	Windows
Idyle GimmIP [15]	監視 Internet 連結，並將連結與否的結果在工具列上以不同顏色顯示。附有 Finger、Ping、Nameserver Lookup、Internet Sensor 與 Trace Route 等網路連結資訊的相關功能。	Windows

【表 5-7】整合套裝工具

Ⅲ. 背景資料

由於網路探測工具種類繁多，難以一一盡述，所以僅以功能爲路徑探測爲主的 Visual Route 爲例，說明一般探測工具的運作原理。

Visual Route 和 Traceroute 性質十分類似，都是探測路徑的工具。只需指定目的地的位址，Visual Route 就會將路徑中的每一個 hop 的延遲情形回報給使用者，所以利用這種量測工具來得知網路狀況是十分方便的。我們要更進一步來了解這些工具的運作原理。

首先，Visual Route 先利用 DNS（Domain Name System）將一般的 host name 轉換成 IP 位址 。接著，Visual Route 開始向目的地發出 UDP 封包。在 IP 封包其中有一個欄位 TTL（Time To Live），它是爲了防止封包在網路中漫無止境地傳送而設，與路徑的選擇無關。當封包從 source 端發出時，它的 TTL 欄位就填入一個正整數，此後每經過一個 router，這個數字就被減 1 ;如果 TTL 欄位已經被減至零，這個封包就會被視爲過時的資訊而被 router 丟棄。發生這種情況時，封包

不能傳遞至目的地，而由丟棄它的 router 回傳一個 ICMP（Internet Control Message Protocol）的封包告訴 source 端" time exceeded "訊息。Visual Route 就可以藉由這個回傳的封包得知 router 的 IP 位址。由此可知，Visual Route 只要依序送出 TTL 由 1 開始遞增的封包，就可以靠著這個網路機制，依序得到沿路 router 的位址，並經由計算送出封包時間至收到 ICMP 封包時間差的一半，很容易估計出路徑中任何一個 router 與 source 之間的延遲。當然，TTL 的上限是 255，所以 source 到 destination 之間不能超過 255 級 hop，否則封包是永遠傳送不到的。

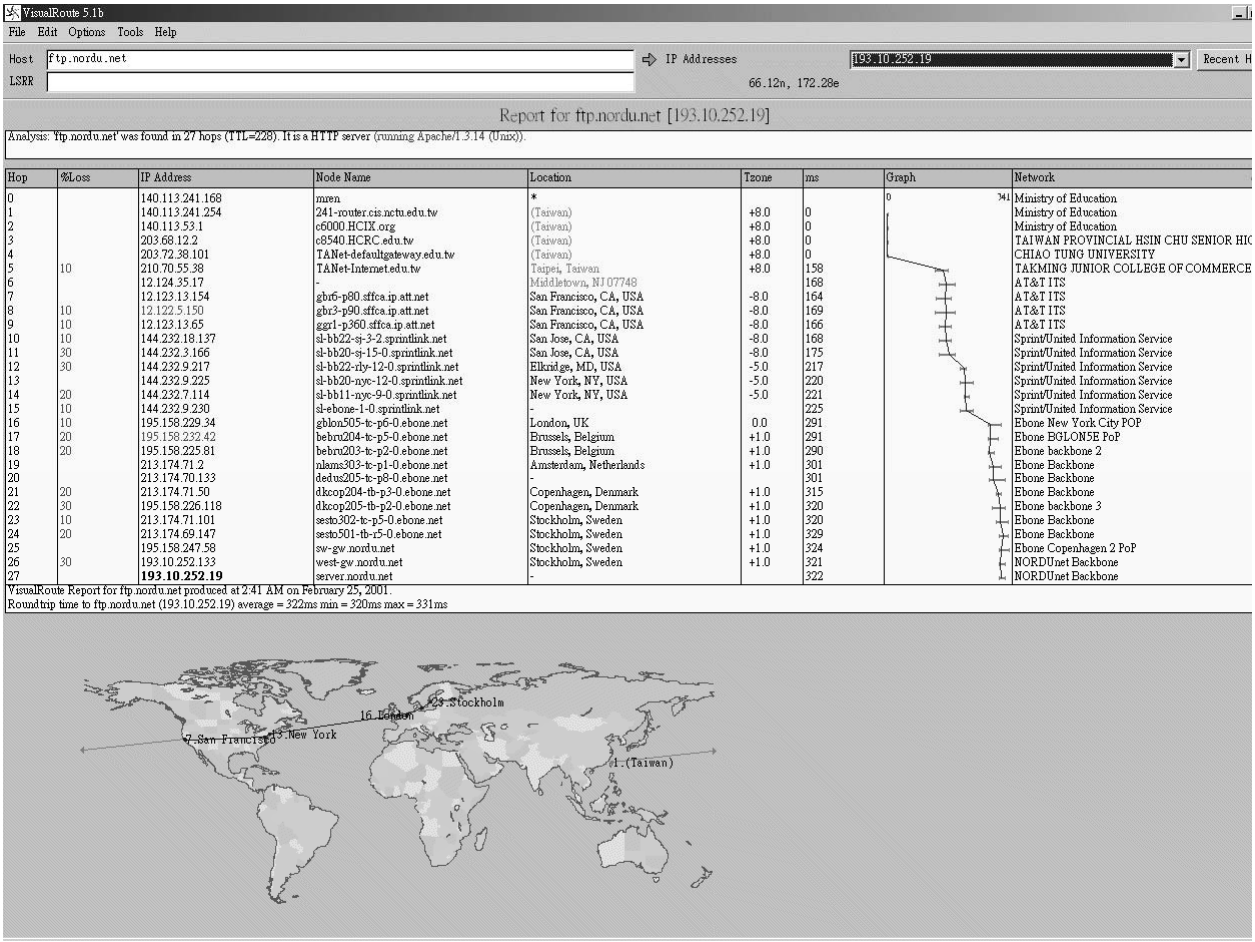
封包傳送失敗有很多種原因，通常是 destination host 本身有問題，或是網路根本就不通。Visual Route 中有一個功能叫做 Scan Network，它可以告訴使用者無法連接到目的地的原因是上述原因中的何者。其運作方式十分地簡單，就是對欲查詢機器所在的 LAN 上所有可能的 IP 位址發出 ping 的封包。若有任何回應從該網域傳來，表示問題不是出在傳遞封包的過程，很可能是該機器沒有正常運作。Scan Network 利用目前 IP 位址的分配採用 subnet 原則，以及 LAN 有 broadcast 的特性，所以才能藉著 LAN 上其他機器的回應來斷定路徑是否暢通。不過使用 Scan Network 時要小心，有些受到較高度安全保護的 LAN 會以爲它自己受到了惡意攻擊，所以往後這個 source host 傳出的封包再也無法進入該網域了。

IP (Internet Protocol)有 LSRR（Loose Source and Record Route）的 option，它可以指定路徑中途必須經過的節點，也就是我們可以替封包決定路徑，而 Visual Route 有支援這個功能。一般而言，我們使用網路時並不關心封包如何從 Internet backbone 傳到目的地，但是在進行除錯時，路徑卻是很重要的資訊。舉例來說，以往僅能獲得本身所處的 A 點至遠端 B 點之間的路徑資料；現在藉著 LSRR，讓封包從 A 點出發後先經過指定的 C 點再繞到 B 點，如此一來，在 A 點不但可以直接得到 AB 和 AC 間的路徑，也間接得到了 CB 間的路徑；這種探測遠端兩點間路徑的方法稱爲 Remote Trace Route。另外，假如我們把 source 和 destination 都設在同一點 A，用 LSRR 指定封包必須通過 B 點，則可以得到 AB 和 BA 的路徑。這樣的探測路徑稱爲 Round Trip Trace Route。在本實驗中，將要借助這兩種 trace route 的方法來探測四個不同站址間的路徑，詳細內容請看實驗方法及實驗步驟。

圖 5-1 是 Visual Route 的主畫面。左邊最上方的 edit box 是用來輸入欲觀察的目的地，它可以是 URL、host name 或是 IP 位址。它的正下方有一個 LSRR 欄位，它是用來指定路徑所必須經過之處，雖然它只有一個欄位，但是可以填入多個位址，要記得將位址間用空白隔開；若不想啓動 LSRR 功能，只要將此欄位空白即可。右上方是 Visual Route 將 host name 轉成 IP 位址之後的列表，由於可能有數個 IP 位址共用一個 host name，所以 Visual Route 會優先觀察排在首位的站址，若要切換到其他的站址，只要拉下列表的選單即可。最右邊是最近觀察過的站址列表，按下按鈕就可以看到。當然也可以從此處直接選擇站址來觀察路徑。

下方的三個欄位是路徑分析後的結果，分別是 Visual Route Analysis、Trace Route Table 以及 Trace Route Map。Visual Route Analysis 是分析封包不能抵達目的地的原因。Trace Route Table 是最主要的資訊來源，它會將路徑上所有的 host 的位址、最大延遲及平均延遲等資訊列出。Trace Route Map 是將路徑用視覺化的方式在世界地圖中展現出來，這樣可更明顯看出實際的連接情形。

Visual Route 還有一些次要功能在這裡尚未提及，請自行至 Visual Route 網站[6]瀏覽查詢，將可得到更詳實的資料。



【圖 5-1】Visual Route 分析路徑畫面

IV. 實驗方法

本實驗著重於對網路探測工具的了解、故首先對於探測工具的使用務須熟稔，不限制使用的工具種類。

觀察三個以上的網站與你的機器彼此的路徑，至少要記錄路徑中每一個 hop 的 IP 位址、location（位於哪個國家境內）、delay，並記錄此路徑的瓶頸在哪兩個 hop 之間。接著，利用工具監視任意一台機器所處的區域網路狀況。最後，在 TWNIC 的網站[16] 中，查出交通大學與 Internet 間的流量佔全部 TANET 與 Internet 間流量的百分比;並查出佔交通大學流量比例最高的前三種 application。此外最好能找到外國網路流量統計資料，擇要記錄在後，亦可獲得額外分數。流量統計的年月份不限制，但是要記得註明來源。

[選擇性實驗]

利用路徑查詢工具或是遠端主機查詢工具，畫出交大或他校或 TAnet 的網路架構圖。

到網路上找尋任一種網路工具的原始程式，將它 trace 一遍並說明它的運作原理。

V. 實驗步驟

由於本實驗所使用的軟體可自由選擇，所以實際上操作的時候可能與此處的說明不盡相同。同學應該說明、記錄自己使用的軟體操作步驟。以下以 Visual Route 作四點間路徑與延遲探測爲例，說明實驗步驟的大致情形。

實驗軟體：Visual Route

測試位址：

（1）	140.113.xxx.xxx	NCTU, Taiwan（local host）
（2）	204.147.129.146	Los Angeles, USA
（3）	205.207.128.190	Montreal, Canada
（4）	166.48.217.254	Seattle, USA

1. 選擇主選單中的「Options」→「Preferences…」。
2. 將「Display/Mapping options」中的「Advanced GUI」欄位打勾，這樣便啓動了 Loose Source Route 功能。
3. 在「Host」欄位填入自己機器的位址。
4. 在「LSRR」欄位分別填入上述三個位於洛杉磯、蒙特婁、西雅圖的機器位址。這麼一來，封包從自己的機器出發後，必須依序經過上述三個位址，最後又回到自己的機器。
5. 按下 enter，開始觀察路徑。
6. 利用主選單中的「File」 →「Print」或「Edit」 →「Snap table as text…」將分析結果記錄下來。

7. 重複步驟 3、4，把「LSRR」欄位中的三個位址順序對調，觀察路徑與原先有何不同。

[註] 同學們可選擇別的網站查詢。但是網路上有很多機器都尚未支援 LSRR，要找到適合觀察的網站可能不容易。這時你可以選擇最接近目的地而又支援 LSRR 的機器作爲新的觀察對象。例如 hop12 回報說它不支援 LSRR，可見 hop11 是支援 LSRR 而又最接近 destination，於是便可採用 hop11 來觀察路徑，以此類推。

[選擇性實驗]

畫出校園網路或 TAnet 架構圖：

1. 先用 ping 或其他工具盡量找出校園內的所有 subnet，由於 router 的 IP 位址多半是 xxx.xxx.xxx.254，所以大部份的 subnet 應該都能找到。
2. 用 traceroute 之類的工具，查詢各 subnet 之間的連接通路，由這些節點的連接情形，推測網路佈線狀況。
3. 若想製作 TAnet 網路架構圖，建議先至 TWNIC 網站查詢，內有部份資料可供參考。
4. 將所推想的架構圖畫出，並附於報告之中。

VI. 實驗記錄

本實驗的記錄包括下列三個部分：

追蹤四點間路徑實驗（以下爲範例）【記錄 1】

Source	140.113.251.1	NCTU, Taiwan
Destination	140.113.251.1	NCTU, Taiwan
LSRR host 1	205.207.128.190	Montreal, Canada
LSRR host 2	204.147.129.146	Los Angeles, USA
LSRR host 3	166.48.217.254	Seattle, USA
LSRR host 4	N/A	

Hop	Host name	IP address	Location	Delay（ms）
1	cc-251-fddi.nctu.edu.tw	140.113.251.1	Taiwan	6
2				
3				

偵測網路狀況實驗【記錄 2】

監視網域 ：140.113.xxx. x				
起始監視時間：		終止監視時間：		
封包總數（packets）	傳輸量（bytes）	Collision 次數	最大傳輸速率（bps）	平均傳輸速率（bps）

記錄台灣學術網路與 Internet 的流量統計資料【記錄 3】

資料出處：												
日期（年/月/日）：												
Member	FTP	Telnet	Domain	News	Mail	Gopher	IRC	WWW	MUD	Others	Total(%)	Total KB
交通大學												
清華大學												
台灣大學												
電算中心												
資策會												

Ⅶ. 問題與討論

1. 請比較本手冊提到的各種網路探測軟體工具，說明它們各適合於哪些用途？

2. 能否再找一些網路探測工具（公用或商用軟體），並說明用途？

3. 用 Round Trip Trace Route 方式探測任意 AB 兩點間的路徑，請問 AB 的路徑必然與 BA 的路徑呈對稱關係嗎？

4. 請用 web 瀏覽器瀏覽剛剛用探測工具測量過的網站（不使用 proxy），此網站的反應速度和探測工具測出的最大延遲時間大約相符嗎?若不符，可能是由哪些原因所造成的？

5. 請解釋爲何一條路徑上的延遲未必呈絕對遞增（即較遠的 hop 之延遲有時反而較小）？

6. 請找出有支援 LSRR 的節點（國內國外各兩個）。

7. 請自行發掘問題，並自行找到解答。

Ⅷ. 參考文獻

[1] Info Evolution Ltd. homepage, http://www.evolve.co.uk/dns/.

[2] Canweb Internet Services Ltd. homepage, http://www.dynip.com/.

[3] Microsoft Research, http://www.research.microsoft.com/barc/mbone/mping.htm.

[4] Available at http://home.kimo.com.tw/bxdc/p1/n4.htm.

[5] Top Jimmy's Web Site, http://www.topjimmy.net/.

[6] Visual Route homepage, http://www.visualroute.com/.

[7] Mentor Technologies homepage, http://www.mentortech.com/learn/tools/tools.shtml.

[8] Systems Software Technology homepage, http://www.sstinc.com/.

[9] International Network Services Software homepage, http://www.vitalsigns.com/netmedic/.

[10] Available at http://www.geocities.com/ashoka_kumar_2000/akprog.htm.

[11] WebTrends Corporation homepage, http://www.webtrends.com/.

[12] EmTec Innovation Software, http://www.emtec.com/yonc/.

[13] Available at http://www.allfile.com/index5/705535.htm.

[14] Netinfo homepage, http://www.netinfo.co.il/.

[15] Idyle Software homepage, http://www.idyle.com/gimmip/.

[16] TaiWan Network Information Center homepage, "http://www.twnic.net/twnet/traffic/"