用 Linux 建立 Intranet

Ⅰ. 實驗目的

瞭解要如何來使用 Linux 來架設一個具有 intranet 服務之區域網路並將之連結到 Internet 上面，在這一個實驗中，您將會確實學到如何安裝一台 Linux 的伺服器、架設 MS Network，並將整個 Private Local Network 透過這一台 Linux 伺服器的網路撥接及使用 Private IP address 來連上 Internet。此外我們安排了兩個需要讀者自行研究的實驗—建立堅固的防火牆和製作已設定好服務的開機磁碟片來做爲 Bonus，希望可以透過這一個實驗讓讀者對於網路作業軟體的管理有深入的了解，更在 Bonus 的實驗中訓練對於未來新軟體的管理能力。

此外您也可以練習把一份報告寫得很完整、邏輯很正確、文句很流暢。

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。

Ⅱ. 實驗設備

本實驗需要的硬體可自備，亦可至機房使用專屬實驗機器。不過由於本實驗的實驗時間可能稍長一點，所以使用組員自己的電腦會比較方便一點。由於本實驗是要建立一個 intranet，是故至少需要兩台電腦，一台用來當成 Linux 伺服器，而另一台用來充當這一個 Local Network 中的一台 Client，所以我們至少需要兩台 PC，不過如果情形允許的話，最好是可以有三台至四台的個人電腦來讓我們做實驗。

在 Linux 的 Distribution 方面，我們所選擇的是 RedHat 5.2 加上 CLE 0.7 的套件，其中 CLE 是一套在 Linux 上面的中文整合方案，詳細資料可以至 http://cle.linux.org.tw/CLE/[5]看看。

一、硬體

項目	數量	備註
個人電腦 PC	至少 2	需有剩餘的 ISA 或 PCI 插槽以安裝網路卡

	台	
乙太區域網路環境	1	可使用 Hub 或同軸電纜串接
Linux 和 Win95/98 支援的網路卡 (ISA)	至少 2 片	可以考慮使用 NE2000 相容之網路卡，其相容性最高

二、軟體

項目		數量	備註
Linux	Redhat 5.2 + CLE 中文整合套件	1	
	ipfwadm	1	
	ipchains	1	
Windows 95	Windows 95 之微軟網路環境	1	
	其他使用 TCP/IP 之網路軟體	1	做上網連線測試用

Ⅲ. 背景資料

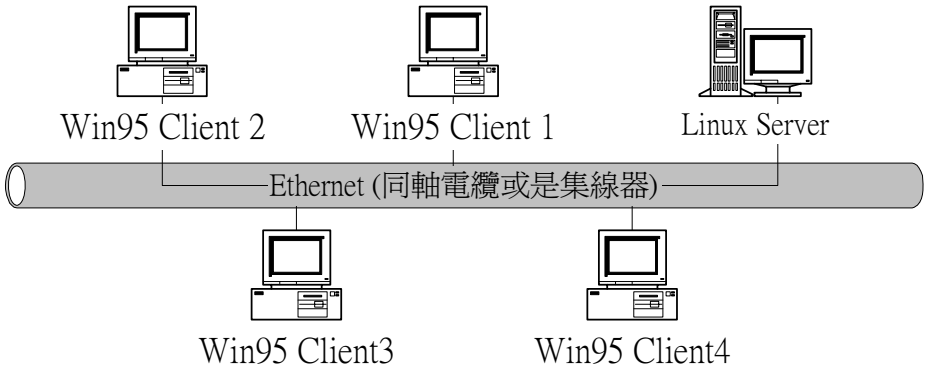
建立一個 intranet 所需要的服務可以略分成網路實體與應用軟體兩個層次。在網路實體方面除了下一章節會提到的網路架構的建立外，還需要讓我們建立起來的區域網路可以連結上 Internet 甚至可以再提供遠端撥接登入的服務，讓公司員工在外出時可以撥接連結公司的網路系統。而在應用層次方面，又可以分成公眾資訊服務(如 WWW 與 FTP 等等)和內部資源共享(如 File & Printer sharing、Database Connection、intranet & Internet Mail、Proxy 等等)。爲了要避免外來不友善人士的惡性破壞及不良員工輸出機密資訊，我們尚需要建立防火牆(Firewall)來隔離 intranet 與 Internet。

由於 intranet 的設計和使用應適環境而異，故在本實驗中，我們儘安排同學們建立一個最基本的 intranet 服務，不過在最困難的基本實體建立起來後，倘若往後欲新增各種服務，相信只需稍微研讀相關文件應可迎刃而解。

在本實驗中，我們假設同學們已會使用 RedHat 套件安裝 Linux 系統，並作 X-Window 的設定，及編譯 Kernel 的能力。如果同學們在這一方面有任何的疑問可以到 [4] 找尋相關的資訊。

首先，您必需建立一個區域網路的實體，也就是利用網路將您的所有電腦

連接起來，如圖 9-1。在這之中，您可以使用集線器(Hub)來串接您的電腦，也可以簡單地用同軸電纜將您的電腦們串起來就可以了。我們假設您對這樣子的網路已有明確的概念，所以這部份就不作贅述。



【圖 9-1】區域網路模型

IV. 實驗方法

一、 建立 Microsoft Network

在上面的網路建構好了之後，其實只要在每一台機器上面跑 TCP/IP(必需設定成使用同一個 Subnet 的 Private IP，我們會在後面詳敘)或是 NetBUEI 網路傳輸協定，就可以建立一個 Microsoft Network 了，也許有人會對 MS Network 這一個名詞覺得有一點點陌生，其實它就是我們在 Window 95/98/NT 中常常會使用到的「網路芳鄰」。

在我們這次實驗中會有幾台跑 Windows 95/98 的電腦充當 Client，而在此時我們可以先將這一些電腦設定起來，而在網路協定上我們只需要使用 TCP/IP 就可以了(因爲 Linux 上面沒有 NetBUEI 協定)。

現在，讓我們來設定一下每一個 Client 應該使用的 IP Address。也由於我們是假設您會在一個企業或是家中用到這樣子的網路環境，也就是您可能沒有太多的 IP 可以供每一個 Client 來使用，這個時候您就可以使用 Private IP 來解決這一個問題。Private IP 是使用了幾組保留的 IP Address，但必須在與

Internet 連接的 server 上轉換，後面提到的 IP Masquerade 就是做這個轉換。對於相關的資訊您可以參考 RFC 1597[1]和 RFC 1918[2]。總之 Internet Assigned Numbers Authority (IANA)保留了以下的 IP 位址空間留給 Private IP 來使用：

10.0.0.0	-	10.255.255.255	(Class A)
172.16.0.0	-	172.31.255.255	(Class B)
192.168.0.0	-	192.168.255.255	(Class C)

由於我們目前實驗中的網路架構並不是十分地大，我們不需要使用到太大的 Class，所以我們可以選擇一個 Class C 的一個 Subnet 即可。將我們的 Client 的 IP Address 從 192.168.1.2 到 192.168.1.249 選出。當您將每一個 Client 選定了一個固定的 IP 並重新開機後，您應該就可以在 Client 的網路芳鄰看到了一個 MS Network，而其內容就是您們那些 Windows 95/98 的電腦。

1. **網路實體的架設：**參考圖 9-1，建立一個乙太區域網路環境。
2. **決定並設定每一個用戶端所使用的 Private IP：**由 IANA 製定的 Private IP 中選定合適者並設定用戶端。
3. **在每一用戶端設定 Microsoft Network 驅動程式：**使得每一用戶端可以透過微軟網路來連結。

二、 加入 Linux-Samba Server

通常在一個網域都要一個 Server 來認證使用者，並提供資源的分享，在一般以 Windows NT Server 建構的網路就是以 NT 來提供這一種角色，而在這兒，我們是使用 Samba 來提供這一些服務，雖然目前 Samba 並沒有提供一部份 NT 所提供的功能，可是對於一般企業及個人使用的資源分享而言，卻已是十分足夠了。

在我們使用的這版 RedHat 套件中，已經幫我們將 Samba Service 給安裝好了，而我們現在最重要的工作就是藉由修改位於/etc/smb.conf 的 Samba 設定檔案，重新設定這一個 Samba Service。

1. **修改/etc/smb.conf，並定義欲分享的資源：**藉由修改 Samba 的設定檔來定義所提供的服務。
2. **重新啓動 Samba Server：**重新啓動 Samba 伺服器使修改過的設定生效。
3. **在每一用戶端使用此 Samba Server 分享出來的資源：**在用戶端測試此一 Samba 伺服器之運作情形。

三、 使用撥接讓 Linux 伺服器上網

在這一部份，我們將透過撥接網路的方式來讓我們的 Linux 伺服器可以連接上網路。

一般頻寬需求較大的公司、企業往往會向當地的 ISP 租用固接專線，而租用的方式不外乎爲時計制或是包月制，而且需要較特別的寬頻 NT (Network Terminal，一般使用 ISDN)來撥接到遠方的 ISP，最後在 IP address 的供給上又可分爲：

1. 給予一組 IP address (一般不會超過一個 class C 的 subnet)，而公司內部機器直接使用這些唯一的 IP address (可以使用傳統的靜態分配或是使用 DHCP 動態分配)。
2. 只給予若干台伺服器固定 IP 使用，而公司內部網路使用 Private IP。
3. 撥接時由 PPP 動態給予一個 IP address (如同一般數據機撥接)，這通常使用於個人使用或是不需要提供公開的服務時。

由於目前個人或是 SOHO 族最常用來撥接網路就是使用數據機來連結了。所以在這邊我們就使用數據機透過電話來連結網路，讓我們的 Linux Server 上網。爲了方便起見，等一下我們的操作是在 X-Window 的環境下，使用 GUI 的工具來連結。

1. **設定 PPP 連接**：設定用來撥接上網的 PPP 介面。
2. **啓動 PPP 連接**：使用 PPP 將 Linux Server 撥接上網。
3. **查看連接成果並上網**：使用 ifconfig 來查看是否連接成功。

四、 讓整個區域網路經由 Linux 伺服器上網

如果只讓 Linux 伺服器上網路的話，似乎有一點點浪費資源，此時爲何不讓整個區域網路都一起上網呢？答案是肯定的，而且技術上也是絕對是可行的。近來這一種需求可以透過 IP Masquerade 來達成，我們只要在 Linux 伺服器上面加上 IP Masquerade 的 Rule 即可以讓我們的 Linux 伺服器擁有這一項能力。

當我們要使用這一項功能時，我們的 Kernel 必需要加入一些設定來將特定的功能 compiled 進 Kernel 的 Image 檔內。總之，由於在我們所安裝的 RedHat 內已將這一些功能 Compile 成 Module 了，所以，也可以正常的使用 IP Masquerade，可是當您要換新版的 Kernel 時就要比較注意了。

接下來我們要如何去設定一個 IP Masquerade 的 Rule 呢？這時我們需要一個可以設定 Forwarding Table 的工具—ipfwadm。

在 Linux 的環境中，只要有您不甚了解的指令，您可以輸入 man command-name 來看看這一個指令的功能列表和參數說明。此外，如果您在實作或是在 Linux 某一方面有困擾時，您可以到/usr/doc/下面可以找到許多的說明文件，尤其是/usr/doc/HOWTO[3]，更是必讀之處，像是/usr/doc/FAQ[3]內就有一些常被人家提出問題的解答。可是要在您的電腦內找到這一些文件的前提是您有安裝 RedHat 的說明文件套件。如果您的電腦內沒有安裝這些文件時，您也可以至 ftp://ftp.nctu.edu.tw/OS/Linux/sunsite/docs 取得。

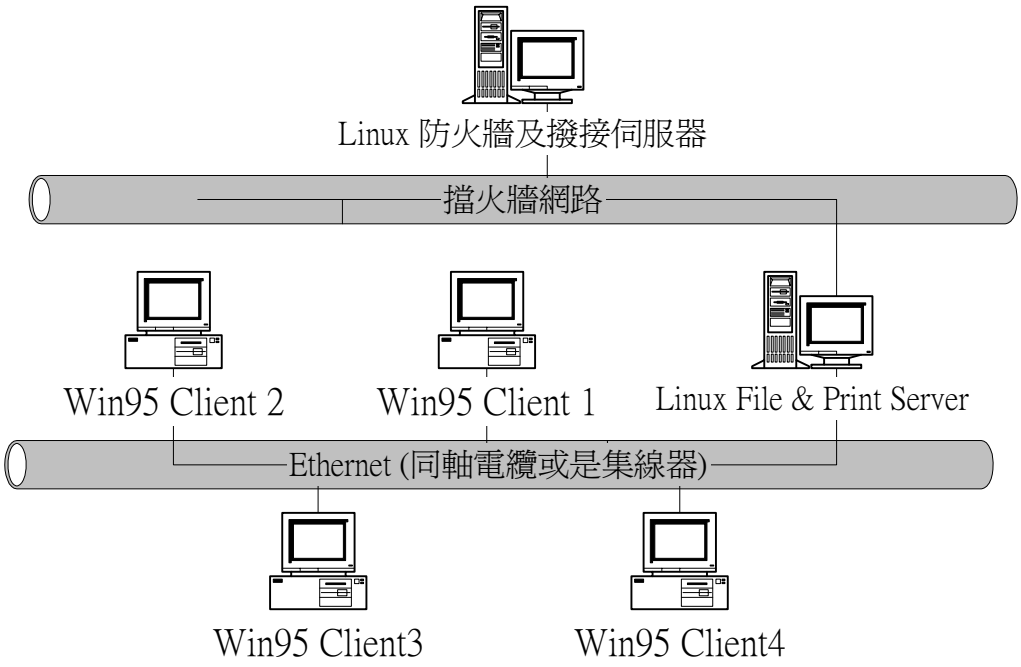
1. **設定 IP Masquerade 的 Rule：**使得 Private IP 可以轉換成 Linux Server 的 IP 並轉送到 Internet 上面。
2. **重新設定用戶端的網路設定：**設定用戶端的網路設定以使用 Linux Server 來轉換 Private IP。
3. **在每一用戶端使用此 Linux 的撥接上網服務：**在用戶端執行使用 TCP/IP 的網路軟體以測試是否可以進入 Internet。

五、 建立堅固的防火牆(Bonus)

在 Linux 上作 Packet Filtering 的防火牆也是要用 ipfwadm 這一個程式來設定的。在設定之前我們先來看看一個標準的防火牆應有的架構圖如圖 9-2。

可是由於我們沒有多出來的 PC 可以專門用來做撥接和防火牆之用，是故我們在這兒是可以把防火牆和我們的之前設定的伺服器設定在同一台電腦(如圖 9-1)，只是如此一來，我們的安全性就會降低不少，做爲防火牆的機器就是要有被 Crack 的準備，是故上面不會跑任何的 Service，也不會有和網路或是公司相關的資料存在。

在這個部份的實驗中，您可以選擇如圖 9-2 的標準做法，也可以選擇上述的簡易方式(如圖 9-1)。然後將您的設定步驟和結果寫成實驗手冊之步驟。(您可以參考/usr/doc/HOWTO/Firewall-HOWTO)



【圖 9-2】標準的防火牆架構圖

六、 製作已設定好服務的開機磁碟片(Bonus)

有時爲了要可以讓整個區域網路可以上網，您可能要花費大把的鈔票去買一些硬體的裝置，如路由器。可是如果可以使用一台便宜的電腦的話，這將是一件十分划算的事，由於一般我們在公司或是家庭使用的網路撥接的傳輸速率並不會很快，使用到 ISDN 並擴充成 T1 的速率已是十分少見了，一般是使用 64Kbps 的固接網路，在我們這個實驗中是使用數據機撥接。以目前最快的 56Kbps 速率而言，一台已退休的 486 又可以拿出來用了。(其實 386 也可以，只是可能很難找到了。)

由於我們將只使用一張開機磁碟片來啓動所有已設定好的服務，所以使用的電腦是不需要有硬碟的，所以之前的 Samba 伺服器就可以不用裝上了，就算裝上了也沒有什麼多大的用處(因爲沒有硬碟)，而這一台機器就可以單純做爲撥接和防火牆伺服器，您可以考慮將整個架構做成如圖 9-2 的樣子，配合另一台 Linux 伺服器來建立一個完整的網域，最重要的是，將您的設定步驟和結果寫成實驗手冊之步驟。

V. 實驗步驟

1. 建立 Microsoft Network

1.1 網路實體的架設

1.1.1 準備至少二台電腦(一爲 Linux，另一爲 Win95 用戶端)。

1.1.2 決定使用集線器或是同軸電纜來連接所有的電腦。(設定方法可以參考實驗手冊七:區域網路的規劃與建立)記錄您的網路實體建構方式【記錄 1】。

1.2 決定並設定每一個用戶端所使用的 Private IP

1.2.1 在 Linux 伺服器端我們使用 192.168.1.254 並使用 Console-Panel 內的網路設定對話框來設定 eth0 的位址，Network Mask 爲 255.255.255.0；注意：在 eth0 的 Gateway 設定中留白。執行 ifconfig 查詢您的網路介面並將結果記錄下來【記錄 2】。

1.2.2 在 Win95 用戶端我們使用 192.168.1.2(如有其他電腦以遞增方式設定，但請使用 2~249 的 IP 位址)並使用「設定」→「控制台」內的網路設定對話框來設定此一網路卡的位址，Network Mask 爲 255.255.255.0；注意：在 Gateway 設定中留白。截取您程式執行或是設定的畫面，並編輯此圖檔以標示出該輸入的欄位以及程式內的控制元件所代表的意義和使用方式【記錄 3】。

1.3 在每一用戶端設定 Microsoft Network 驅動程式

1.3.1 在 Win95 用戶端使用「設定」→「控制台」內的網路設定對話框並選擇「新增」→「服務」→「File and printer sharing for Microsoft Networks」。此外再選擇「檔案及列印分享」並在「別人也可以存取我的檔案」和「別人也可以使用我的印表機」打勾。截取您程式執行或是設定的畫面，並編輯此圖檔以標示出該輸入的欄位以及程式內的控制元件所代表的意義和使用方式 【記錄 4】。

2 加入 Linux-Samba Server

2.1 修改/etc/smb.conf，並定義欲分享的資源。

2.1.1 在 [global] 區間內，我們需要更改：

```
# workgroup = NT-Domain-Name or Workgroup-Name
workgroup = SPEED

# server string is the equivalent of the NT Description field
server string = Linux EXP Samba Server
```

2.1.2 如果您希望除了在這 Linux 上面有帳號的人也可以存取的話，您要將

“; security = user”這一行 remark 起來(remark 就是使之成註解，也就是不要執行的意思，可以用「#」或是「;」來達到這一個目的)。

2.1.3 定義要共享的資源：

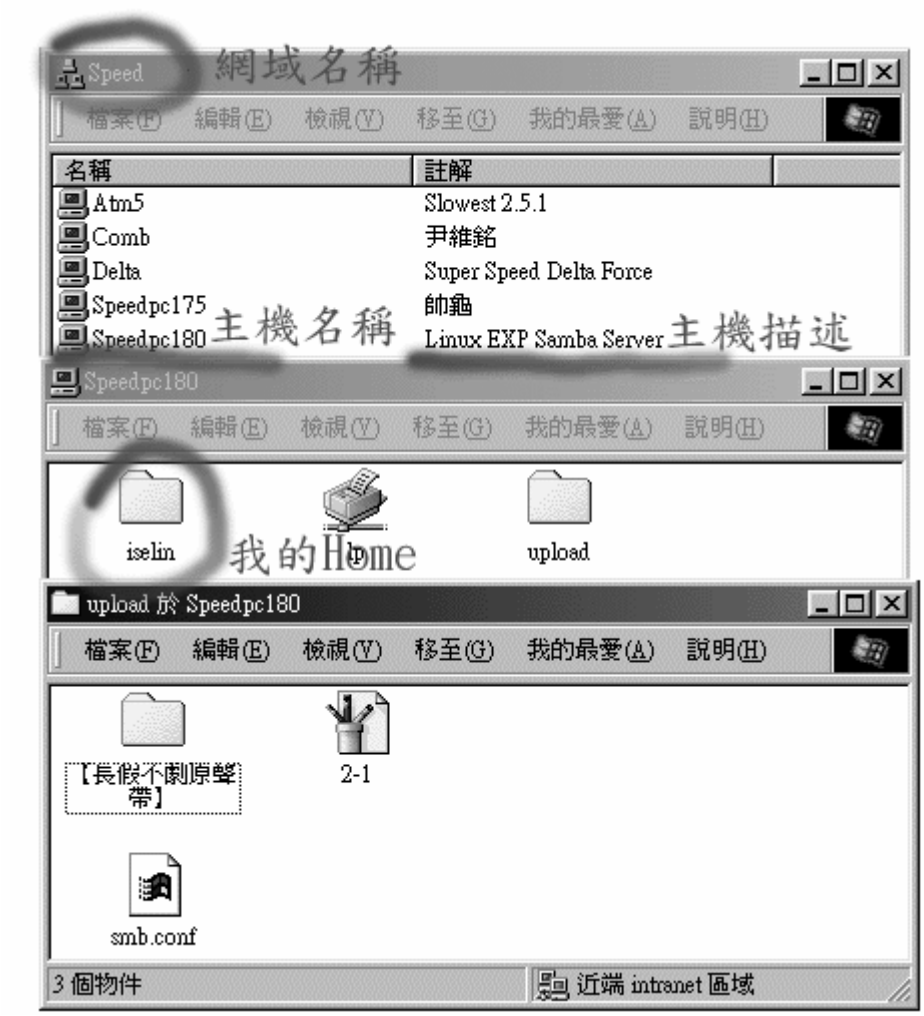
```
#============== Share Definitions ==============
```

[homes]　　#可以讓每一個 user 看到他們自己的目錄
comment = Home Directories
browseable = no
writable = yes

[upload]
comment = Home Directories
path = /home/samba/upload　　#實際的目錄位置
public = yes　　#是否對無帳號者開放
writable = yes　　#可否更動檔案

2.1.3.1 在這兒要注意的是不但要設定 Samba 的設定，更要去設定實際的目錄權限，如上例中，/home/samba/upload 就要設定 chmod 777。

2.1.3.2 如此一來，我們就可以在 Window 95/98 的電腦上面看到經由 Samba 分享出來的資源如圖 9-3。重新設定並開放一個資源的分享，將您的設定記錄下來，並截取在您用戶端「網路芳鄰」執行的畫面，並編輯此圖檔以標示出該輸入的欄位以及程式內的控制元件所代表的意義和使用方式(可以參考圖 9-3) 【記錄 5】。



【圖 9-3】經由 Samba 分享出來的資源

2.2 重新啓動 Samba Server

2.2.1 執行 /etc/rc.d/init.d/smb restart 來重新啓動 Samba Server。記錄 /etc/rc.d/init.d/smb 可以使用的參數，及執行之後的結果【記錄 6】。

2.3 在每一用戶端使用此 Samba Server 分享出來的資源

2.3.1 在 Win95 用戶端使用「設定」→「控制台」內的網路設定對話框並選擇「識別資料」這一頁並在「工作群組」內填上"SPEED"。截取您程式執行或是設定的畫面，並編輯此圖檔以標示出該輸入的欄位以及程式內的控制元件所代表的意義和使用方式【記錄 7】。

2.3.2 將這一台用戶端電腦重新開機後並打開「網路上的芳鄰」即可以看到這一台 Linux 伺服器。

3 使用撥接讓 Linux 伺服器上網

3.1 設定 PPP 連接

3.1.1 先進入 X-Window，再來啓始 Control-Panel，並選擇最下方的數據機設定，其後會出現一個通訊埠對話窗。在選擇了您數據機連結的

COM Port 後，選擇 OK 並 Save 設定值。截取您程式執行或是設定的畫面，並編輯此圖檔以標示出該輸入的欄位以及程式內的控制元件所代表的意義和使用方式【記錄 8】。

3.1.2 選擇位於數據機設定盒上方的網路設定鈕，在切換到 Interface 的那一頁後，選擇 ADD 的按鈕來新增一個 Interface，這時會出現一個 Interface 選擇對話框，由於我們要使用數據機撥接交大的撥接專線，所以我們選擇新增一個 PPP 的 Interface。在確認之後會帶出另一個 PPP 撥接伺服器的相關資料對話框，這個對話框最主要是用來讓我們填寫一些關於 PPP 撥接伺服器的資料；在這兒，提供一個在數據機撥號時常常會用到的指令，就是在電話號碼上面打上「,」這是代表了要暫停撥號三秒，如果您的電話是一個分機或是您要打到一個需要鍵入分機號碼的地方，您一家會需要它。其次是，目前我們交大已經採用了 PAP 的認證方式，所以您也要一併輸入您的帳號和密碼。如此一來就完成了 PPP 的設定。截取您程式執行或是設定的畫面，並編輯此圖檔以標示出該輸入的欄位以及程式內的控制元件所代表的意義和使用方式【記錄 9】。

3.2 啓動 PPP 連接

3.2.1 打開數據機電源和接上電話線之後，這時我們再回到網路設定對話框，在選擇了 ppp0 這一個 Interface 後，按下 Activate 這一個按鈕，此時數據機就會開始撥號了，在數據機的 Handshake 完成之後，即完成了 PPP 的連線。截取您程式執行或是設定的畫面，並編輯此圖檔以標示出該輸入的欄位以及程式內的控制元件所代表的意義和使用方式【記錄 10】。

3.3 查看連接成果並上網

3.3.1 在 Terminal 中打入 ifconfig，我們可以發現多了一個 ppp0 這一個裝置，而且此時我們的 Linux 也可以連線到其他的網站了。記錄這一個 ppp0 裝置的資訊【記錄 11】

3.3.2 只要按下網路設定對話框的 Deactivate 就可以結束這一個撥接的連線了，此時我們再打入 ifconfig，可以發現原先多出來的 ppp0 的 Device 已經不見了。

4 讓整個區域網路經由 Linux 伺服器上網

4.1 設定 IP Masquerade 的 Rule

4.1.1 執行 ipfwadm -F -f 清除所有的 forwarding rules。

4.1.2 執行 ipfwadm -F -a masquerade -S 192.168.1.0/24 -D 0.0.0.0/0 -W ppp0 新增一個 IP Masquerade rule 到 forwarding table 內，內容是充許我們將 Subnet 內 Source IP Address 是 192.168.1.*的封包經由 IP

Masquerade 的方式經由 ppp0 這一個 Network Device forward 到各個地方去。

4.2 重新設定用戶端的網路設定

4.2.1 在 Win95 用戶端，使用「設定」→「控制台」內的網路設定對話框來設定此一網路卡的位址，在 Gateway 設定 192.168.1.254。截取您程式執行或是設定的畫面，並編輯此圖檔以標示出該輸入的欄位以及程式內的控制元件所代表的意義和使用方式【記錄 12】。

4.3 在每一用戶端使用此 Linux 的撥接上網

4.3.1 使用 ping140.113.23.3 這個工具測試和用戶端到交大資料 BBS 是否可以連線。記錄使用 ping 所得到的時間資訊，並請重複執行以取得 10 次的結果並算出平均值和變異數【記錄 13】。

VI. 實驗記錄

請完成在實驗步驟內指定的十三項記錄。

記錄	內容
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	

VII. 問題與討論

注意：請針對問題中每一項目回答，並避免引述「太」多資料。

1.使用過大的 Private IP Space 會有壞處嗎？

2.IP Masquerade 在將某一個封包由 intranet 送至 Internet 時，如何轉換 private IP address？而在該封包的反向封包(如 ACK 或是遠端 server 的反應)由 Internet 送至此 intranet 時如何將 destination IP address 轉換成正確的 private IP，使該台 client 可以收到？

3.爲什麼用戶端 IP 最好使用 2～249？

4.爲什麼使用 Win98 連接我們的 Samba 伺服器會一直說密碼錯誤，可是使用 Win95 卻不會有問題？

5.在設定完 PPP 後，也可以正常運作，但是除了 root 外一般使用者卻不行撥接上網，要如何解決？此外要如何在 Console 模式（非 X-Window 環境）下啓動撥接上網？

6.要如何讓 Linux 一開機就自動撥接上網呢？

7.在每次開機之後，IP Forwarding Table 內的 Rule 都會被清掉，我們可以將指令加在何處，使以後在開機後會自動載入？

8.在這個實驗中，Kernel 在編譯時需要打開那一些功能才可以順利完成這一些實驗。

9.在最近新版的 Kernel 中對於網路結構做了變動，在 IP Masquerade 方面需要使用 IP Chains 來設定，請詳述 IP Chains 的使用方法？（您可以參考在 HOWTO 下面的文章）

10. 自問自答。(可以是您在操作所遇到的問題並解決的方法，或是新的啓示和想法)

Ⅷ. 參考文獻

[1] Y. Rekhter, B. Moskowitz, D. Karrenberg & G. de Groot, "*Address Allocation for Private Internets*", RFC 1597, March 1994.

[2] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot & E. Lear, "*Address Allocation for Private Internets*", RFC1918, February 1996.

[3] Linux HOWTO & FAQ Documents
[4] Linux.org 中文網站，”http://www.linux.org.tw/”
[5] 中文 Linux 延伸安裝套件網站，”http://cle.linux.org.tw/CLE/”