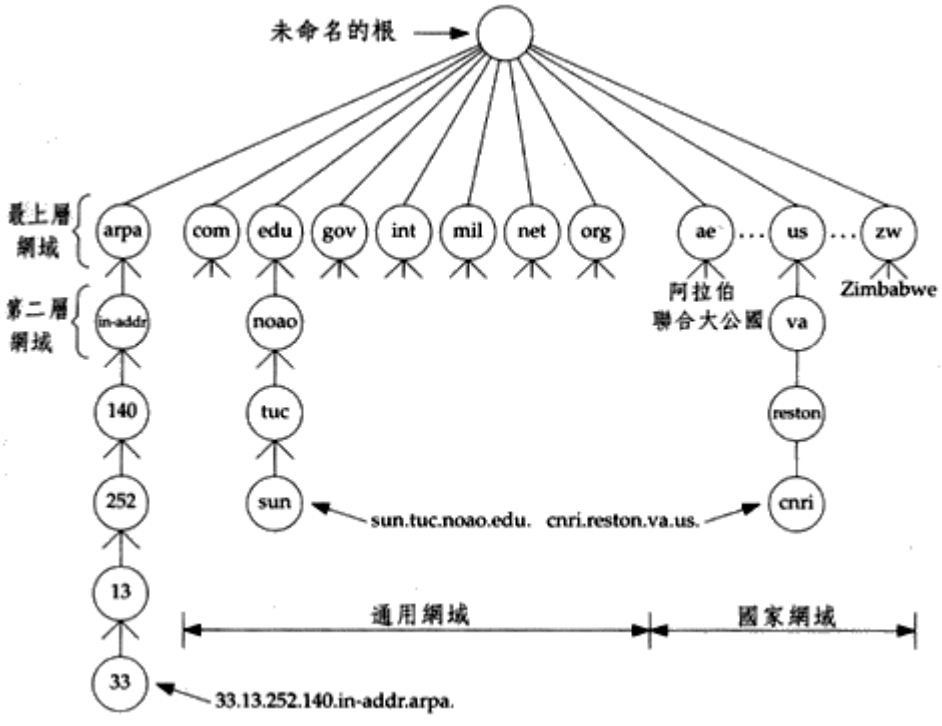
網路名稱系統

作者:李忠憲 2002/10/15 修訂

DNS 階層架構



根伺服器：由固定幾台主機提供全球資源定址服務（URL），主機清單隨著效能的需求成長，需定期從 interNIC 更新。

最上層網域：例如：tw. ，由國家或地區成立的 NIC 分支機構負責維運管理，提供服務的主機需註冊於根伺服器中，以建立階層結構關係。

第二層網域：由各地區 NIC 組織授權給各相關領域機構負責管理，例如：授權教育部負責管理 edu.tw. 領域。提供服務的主機必須註冊於上層網域的伺服器上，以建立階層結構關係。

運作機制

重要紀錄類型

1. 主機（ A ）紀錄：紀錄網址名稱對應成 IP
2. 指標（PTR）紀錄：紀錄 IP 對應成網址名稱
3. 名稱伺服器（NS）紀錄：紀錄管理該網域的伺服器 IP
4. 授權（SOA）紀錄：

   origin = dns.spps.tp.edu.tw
   mail addr = shane.mail.spps.tp.edu.tw
   serial = 2000091401
   refresh = 86400 (1 day)
   retry = 1800 (30 mins)
   expire = 1728000 (20 days)
   minimum ttl = 259200 (3 days)

   紀錄該網域的管理主機、管理員信箱、目前的版本序號、正副 DNS 更新頻率、更新失敗時重試頻率、過期期限、授權期限（最後這個設定是給其他 DNS 用來規範快取記憶體的）。

正反解析（UDP或TCP）

1. 工作站向 local DNS 伺服器提出解析（正解或反解）要求。
2. local DNS 從快取記憶體中搜尋該網址名稱或 IP 是否有對應紀錄，如果找到則 檢查授權期限（TTL），超過期限視同找不到紀錄，若資料未過期，則回覆給工作站。
3. 找不到紀錄的處理方式：去除頭碼後，從快取記憶體中搜尋 NS 紀錄，假設有搜尋到 NS 紀錄，則向該網域 DNS 伺服器提出解析要求 ，若找不到則再去除頭碼並進行搜尋，依此方法反覆進行到只剩下 .（根）。
4. 由於根伺服器已預先儲存在快取記憶體中，所以可以成功找到，並將解析要求送往該伺服器。
5. 根伺服器送回下一層 NS 紀錄，要求連往該網域伺服器查詢。
6. local DNS 伺服器紀錄該 NS 的 IP 與 DN 的對應關係，並寫入快取記憶體中，並向該網域伺服器提出解析要求。
7. 該網域伺服器代為查詢出結果，並送回 A 紀錄
8. local DNS 伺服器紀錄該主機的 IP 與 DN 的對應關係，並寫入快取記憶體中，並將結果送回給工作站。

遞迴（recursive）、重複（interative）查詢

1. 當 local DNS 收到其他 DNS 所提出的解析要求，並且從快取記憶體中查不到答案時，則可以代為查詢，或拒絕代查（需在啟動 DNS 前預先設定運作模式）。
2. 若拒絕代查，則 local DNS 會回應最接近答案的 NS 紀錄給對方，以方便對方繼續查詢。

領域傳送（TCP）

1. 次要 DNS 伺服器向主 DNS 伺服器詢問版次。
2. 次要 DNS 比較 SOA 紀錄中的版次大小，決定是否要向主 DNS 提出 zone transfer 要求。
3. 主 DNS 伺服器使用 TCP 通訊協定傳送完整領域紀錄給次要 DNS。

輪詢

1. 當多個 DN 對應到同一個 IP 時，主要的 DN 可以設定為 A 紀錄，其餘 DN 設為 CNAME 紀錄，則 DNS 回應解析要求時，不會進行輪詢，而會固定送回 A 紀錄。這會對 mail 主機的運作造成一些問題，當一台 mail 主機在 DNS 上所註冊的 A 紀錄與郵寄地址不同時，會使得 mail 程式在進行運算時，無法通過 DNS 查核，而導致信件無法遞送。因此對於提供 mail 服務的主機來說，在 DNS 上註冊之 A 紀錄，必須與郵寄地址相符。
2. 當多個 IP 對應到同一個 DN 時，DNS 會以 round robin 演算法來進行輪詢。這個機制可以被運用在負載平衡上。

NAT 架構下的雙 DNS 設定

NAT 就是虛擬網址對應機制，是為了解決 IP 不足而發展的。由於使用 NAT 機制，可以讓多台工作站偽裝成同一個 IP 上網，從外部網路並無法得知是哪些工作站連線，間接的也保護了工作站的安全，因此 NAT 機制也被視為是防火牆產品所必須提供的基本功能 。

完整的 NAT 機制應提供以下功能：

- IP 偽裝（多對一 、多對多對應：多個虛擬 IP 對應成 1 個或多個真實 IP）
- 伺服主機對應（一對一 對應： 1 個虛擬 IP 對應成 1 個真實 IP）
- Port 轉送（將某一通訊協定固定轉往一台內部伺服主機）

以上三種功能，都必須對 IP 封包來加以改寫才能完成，因此只有支援 Layer 3 以上的網路設備，才能提供 NAT 機制（或在 PC 上安裝防火牆軟體來提供）。

在 NAT 虛擬網域內，所有的工作站都只有虛擬 IP，而提供對外服務之伺服器，則同時具備一個真實 IP 和一個虛擬 IP。這就會造成 DNS 建置上的困擾，因為對外部的網域而言，並無法得知虛擬 IP 的存在，因此必須將伺服器的 DN 對應到真實 IP，才能從外部網路連通。對於內部網域而言，必須要能夠以虛擬 IP 直接連通該伺服器，而不應使用真實 IP。問題是 DNS 並無法同時提供虛擬 IP 和真實 IP 對應到同一個 DN，這就是為何 NAT 架構下需要兩台 DNS 的原因。

由於 DNS 階層是由上而下的（上層需註冊下層的紀錄，下層則可以不用理會上層），因此對於上層 DNS 而言，只要知道對應到真實 IP 的 DNS 伺服器就行了；對應到虛擬 IP 的 DNS 伺服器並不須要註冊於上層，也可以正常運作。

假設在 NAT 虛擬網域內，只使用一台對外 DNS 伺服器，將會耗用加倍的網路頻寬，尤其是會佔用防火牆資源，容易造成網路效能降低，原因如下：

> 當虛擬網域內之工作站想要連上本地端伺服器時（假設是 Web 伺服器），首先會送出名稱解析要求給 DNS 伺服器，然後會得到 Web 伺

服器的真實 IP ，由於真實 IP 並非本地端 IP ，因此會將封包往外送到防火牆，再由防火牆進行 IP 轉換，轉換結果得到 Web 伺服器之虛擬 IP ，這時封包再送給 Web 伺服器處理，因此封包並非直接由工作站送往 Web 伺服器，而是會先經過防火牆，造成內部封包排擠外部封包的效應，使得連通外部網路的頻寬打對折。

DNS 偵錯

當家長反應學校網站無法瀏覽時，有時並非 DNS 的問題，我們可以採取以下的處理流程來釐清問題成因：

1. 請對方取消瀏覽器的 Proxy 設定，試試看能不能連通，藉以確認是否為 Proxy 不通。
2. 請對方直接打 IP ，試試看能不能連通，藉以確定是否為 DNS 無法正常解析。
3. 在校內工作站上 ping 網站 URL 看看是否有回應，以便確認是否為校內 DNS 之問題。
4. 請對方告知他們所使用的 DNS 的 IP（使用 ipconfig /all 指令），以 nslookup 檢測對方使用的 DNS，是否能正常解析學校網站的網址。

特別要注意的是，即使是確定 DNS 有問題，有時候問題並非出在校內自己的 DNS 上，其他的可能性包括：上層 DNS 委派子網域時發生錯誤、對方 DNS 故障、對方快取記憶未及時更新.....等原因。而這些原因則需要使用 nslookup 來進行檢測。

我們可以使用 nslookup 來偵測DNS名稱解析是否正確，這是 Linux 上常用的指令，你要注意的是，在 Windows系統中只有NT系列有提供這個指令，所以請不要在 98上面做這項偵錯。

我們來看以下的偵錯過程：

C:\>nslookup

預設伺服器： dns.spps.tp.edu.tw <--我的網路組態以它當第一台DNS
Address: 192.57.1.3 <--因為是使用內部 DNS ，所以對應到虛擬 IP

> www.spps.tp.edu.tw <--先測試該Server管理的正解紀錄是否存在

伺服器： dns.spps.tp.edu.tw
Address: 192.57.1.3

名稱： www.spps.tp.edu.tw <--OK沒問題
Address: 192.57.1.2

> 192.57.1.2 <--再測試該Server管理的反解紀錄是否存在

伺服器： dns.spps.tp.edu.tw
Address: 192.57.1.3

名稱： www.spps.tp.edu.tw <--OK也沒問題
Address: 192.57.1.2

> set q=any <--改變查詢的選項為任何型態紀錄
> tp.edu.tw <--查詢我們上一層的網域內容

伺服器： dns.spps.tp.edu.tw
Address: 192.57.1.3

tp.edu.tw internet address = 163.21.236.5
tp.edu.tw nameserver = dns.tp.edu.tw
tp.edu.tw nameserver = ns.tp.edu.tw
tp.edu.tw primary name server = dns.tp.edu.tw
responsible mail addr = mail.tp.edu.tw
serial = 199911173
refresh = 21600 (6 hours)
retry = 7200 (2 hours)
expire = 3600000 (41 days 16 hours)
default TTL = 172800 (2 days)

tp.edu.tw nameserver = dns.tp.edu.tw <--上一層的DNS主機
tp.edu.tw nameserver = ns.tp.edu.tw
dns.tp.edu.tw internet address = 163.21.236.5
ns.tp.edu.tw internet address = 163.21.236.7

> lserver 163.21.236.5 <--將上一層的DNS主機設定為查詢對象

預設伺服器： dns.tp.edu.tw
Address: 163.21.236.5

> spps.tp.edu.tw <--查詢本地網域在上一層的設定內容

伺服器： dns.tp.edu.tw
Address: 163.21.236.5

spps.tp.edu.tw nameserver = dns.spps.tp.edu.tw <--與我們呈報上去的設定一致沒有設錯
dns.spps.tp.edu.tw internet address = 163.21.166.2 <--指到對應真實 IP 的外部 DNS

> exit <--離開nslookup工具

這一段偵錯過程是在追蹤DNS為何不工作，通常我們是由下往上查，而不是由上往下查，因為越往上層其管理會越嚴謹，出錯機率相對不高，除非是我們給上層錯誤的資料，否則不致於會有問題。

偵測過程中，先偵測自己Server管轄內的機器是否能正確的正反解，如果不能解出正確結果，那麼就是我們自己的Server設定錯誤（通常是語法錯誤），如果根本不能查詢，而且出現錯誤訊息，那就是Server掛掉了，請將它修復後重新開機。

如果偵測沒有問題，但是在瀏覽器中還是不能看到自己的網頁，這時候我們懷疑上一層資料與我們不Match，我們就必須進行記錄比對。

假如不知道上層DNS的位址，可以先在自己的Server上查詢一下，查出結果後，再

將該Server設成本地端預設DNS，這樣做的目的是讓以下的查詢可以真正讀取到該Server管轄的記錄內容。

查詢有關本地網域它所知道的任何訊息，Server應該會回應所有有關的紀錄，核對看看是不是與我們通報上去的資料一致。假如是因為我們這邊做了修改，但是沒有通知上一層的管理員，那發生錯誤就是天經地義的了！

任何已登錄的DNS，要修改IP或網域名稱，一定要經過正常行政程序通知上一層管理員，請上一層管理員幫你修改紀錄，這樣改變才是有效的！

微軟 DNS 特殊機制

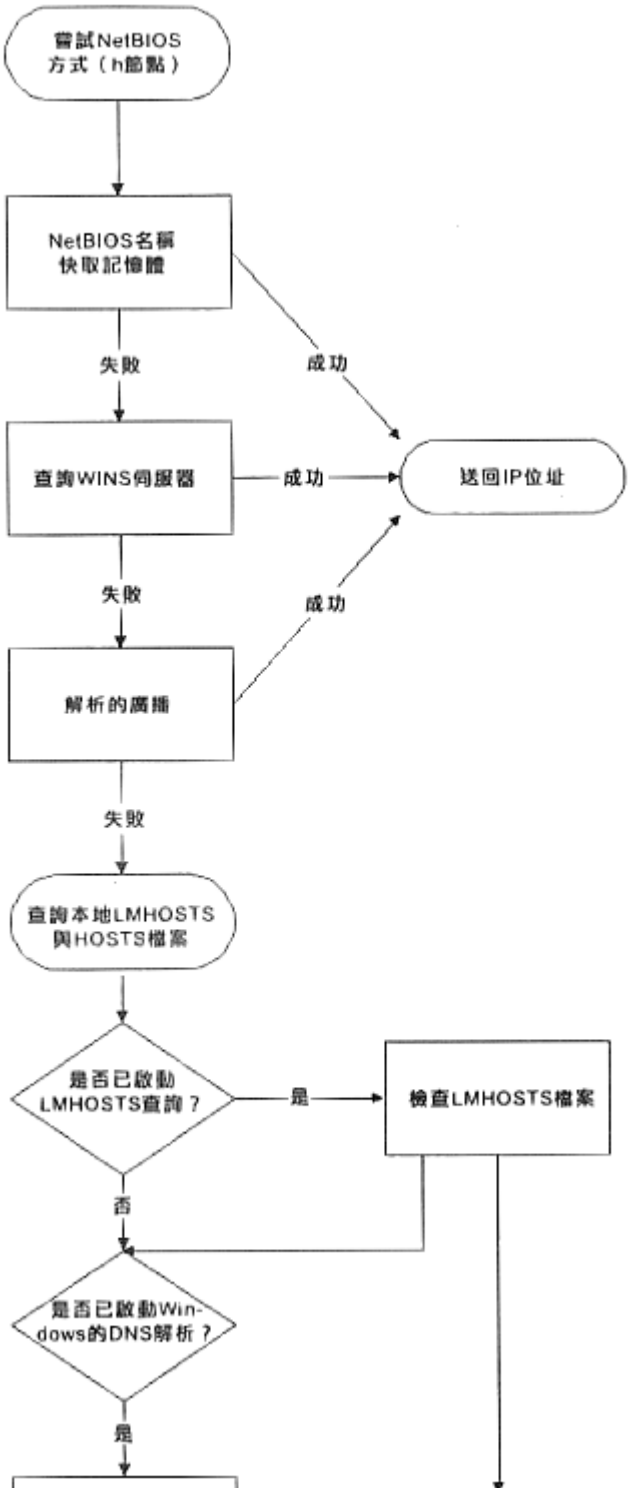
與 Netbios 解析的合作

windows 網路是使用 Netbios 名稱來進行主機的辨識，有關 Netbios 名稱解析的詳細內容，在下個小節介紹，這裡主要是要討論微軟的用戶端解析工具，如何融合 Netbios 和 DNS 查詢。

當我們從命令列輸入

Ping www

由於 Ping 指令需要 IP 才能運作，因此會先啟動用戶端名稱解析工具，以便將 www 解析為 IP 位址。首先會判斷名稱內是否含有 . 如果有則送往 DNS 要求解析，若否則以 Netbios 機制來解析，解析流程如右圖所示。



我們從圖上可以了解，當 www 名稱無法使用 Netbios 解析（詢問 WINS 伺服器或 Netbios 廣播），則會比對 LMHOSTS 和 HOSTS 檔案，如果還是找不到，則會加上網域尾碼，來進行 DNS 查詢，於是要解析的名稱就從 www 變成是 www.spps.tp.edu.tw。

此項功能可以從我的電

腦->控制台->網路組態設
定開啟。

有趣的是如果 local DNS 伺服器是使用 win NT /2000 ，那麼當 DNS 找不到 www.spps.tp.edu.tw 的 A 紀錄時，會將網域尾碼去除變成 www 然後再交給 WINS 伺服器解析。

換句話說，當某台主機其 Netbios 名稱為 web ，但網址名稱為 www.spps.tp.edu.tw 時，以下指令都可以查到正確結果：

Ping web（使用 Netbios 解析成功）

Ping www（使用 Netbios 解析失敗後，轉送 DNS 解析成功）

Ping www.spps.tp.edu.tw（使用 DNS 解析成功）

Ping web.spps.tp.edu.tw（使用 DNS 解析失敗後，轉送 WINS 解析成功）

第四種情形，可以讓未登錄於 DNS 的主機，也能成功解析 URL，看起來就像是有一台動態 DNS （DDNS）提供服務一樣，只不過這種動態是模擬的 ，而且網域內必須安裝 WINS 伺服器才行。

與 AD 的合作

Win 2000 所提供的 LDAP 服務，被命名為 Active Directory（簡稱AD），這個服務用來取代 NT 的帳號管理，配合這項轉變，win 2000 上的帳號認證，也改用 Linux 流行多年的 kerbros 認證機制。另由於 Netbios 名稱解析存在許多的缺點，所以在 win 2000 上面改提供 DNS 來作為 windows 網路的標準名稱系統。這兩項新的標準，最後結合在一起，成為真正的 DDNS（還是與 Linux 上標準的 DDNS 有所不同）

當我們將 windows DNS 設定為與 AD 結合時，原本由 DNS 所管理的網域名稱資料庫，會轉移到 AD 資料庫內，由 AD 來進行動態維護，也就是說，當該網域內的 win98 工作站開機登入網域後，AD 便根據該工作站 Netbios 名稱（加上網域尾碼），以及該工作站的 IP （無論固定 IP 或得自 DHCP 的動態 IP），自動建立 DNS 紀錄；如果該工作站係由 DHCP 取得 IP，則因為每次開機都會登入網域並自動更新 DNS 紀錄，所以該工作站可以被 DNS 查到。

網芳運作原理

Netbios 原本是一組 DOS 環境下所使用的網路應用程式介面（API），後來由於被 windows 網路採用作為電腦名稱機制，所以不但沒有被淘汰，反而還大行其道。由於早期的 windows 網路使用 Netbeui 通訊協定，所以 Netbios 封包也被封裝成 Netbeui，當 TCP/IP 盛行後，Netbios 封包又被改用 TCP/IP 來封裝，並命名為 NBT（Netbios over TCP/IP）通訊協定（修改自 Unix 系統的 SMB）。總之 Netbios 並不是 Netbeui。

Netbios 服務被 windows 網路採用的功能有下列三項：

1. 名稱服務（Name service，TCP 137）：具有專屬名稱與群組名稱兩種不同名

稱空間，兩台主機之間可藉由 Netbios 廣播或透過 WINS 伺服器，來查詢對方是否存在。
2. 連線服務（Session service，TCP 138）：提供兩台主機之間使用 Netbios 名稱來進行身分認證，並建立連線。
3. 資料傳送服務（Datagram service，UDP 139）：用來在兩台主機之間交換大量資料。

Netbios名稱服務是透過廣播的方式來查詢主要名稱瀏覽器（Master Browser）來獲得電腦名單，主要名稱瀏覽器通常是網路上第一台開機的電腦，如果網域裡面有作業系統版本較高的主機被開機，則會在開機後自動進行「選舉」，並成為新的主要名稱瀏覽器，原有的主要名稱瀏覽器則被降級為備份名稱瀏覽器。

主要名稱瀏覽器會每隔十五分鐘檢查一次備份名稱瀏覽器是否還開機，若否則會選擇一台新的機器當備份名稱瀏覽器（Backup Browser），備份清單上的資料。

網域內的工作站會每隔12秒廣播自己的電腦名稱，以及存在的分享資源，主要名稱瀏覽器收到後，就會整理清單。網域內如果電腦數太多會造成廣播封包急速增加，而佔用頻寬，規劃上可以使用橋接器或 Layer 2 的 Switch 管制廣播封包的流向，減輕網路負荷，有許多網路系統就是因為規劃不當而造成廣播風暴，致使網路效能不彰。

由於 NetBT 廣播封包無法跨越網段，如果 同一個 windows 網域的工作站，分布在不同網段上，想要穿越路由器 （或是橋接器、交換器、防火牆）互相溝通，就只能透過 WINS 伺服器來擔任媒人。同時因為 WINS 伺服器的架設，原本會定期廣播的機制，會轉變成固定向 WINS 查詢，可以有效減輕網路負擔，一台專職的 WINS 伺服器，其效能足以提供給五個網域內一千台以上的工作站使用。如果路由器後方有防火牆，必須將 TCP137~139、UDP138~139 放行，才能通過防火牆的攔堵；通常只有在多個網域互相連接時，才需要考慮這個問題。這裡再強調一次，如果區域網路電腦數量太多，或者已經用橋接器或交換器或路由器來連接各個子網域，一定要安裝一台專職 WINS 伺服器（選擇NT的WINS或UNIX的SAMBA都可以），這樣透過網路工作才會輕鬆宜人。

舉實例來說明：當我們打開網路上的芳鄰時，工作站就會透過 Netbios 名稱服務取得電腦清單，這時候我們可以看到一大堆電腦小圖示，接著我們在目標電腦的小圖示上按一下，工作站就透過 Netbios 名稱服務取得該台電腦的分享資源名稱，這時候我們可以看到該台電腦分享出來得資料夾。接著我們打開其中一個資料夾，工作站就會透過 Netbios 連線服務與對方建立連線，當我們以拖拉方式將資料夾內的檔案拖到桌面上，則工作站會透過 Netbios 資料傳送服務取得該檔案的內容，並複製到我們的電腦上。

WINS 伺服器

當工作站已設定 WINS 時，開機啟動後會嘗試直接與 WINS 伺服器聯繫，而非以廣播方式來宣告主機存活，這樣就可以有效減少廣播封包的產生。WINS 伺服器在接到工作站的名稱登記要求時，會傳回 TTL （Time to Live）值，當 TTL 值到期時，工作站會再與 WINS 伺服器聯繫，以便刷新已經登錄的名稱。工作方式與不設定 WINS 時完全相同，差別只在於一個使用廣播，另一個不使用。

當工作站關閉時，會送出名稱解除請求給 WINS 伺服器，WINS 伺服器收到請求後，會將該電腦名稱從資料庫刪除。

雖然工作站已經設定了 WINS 伺服器，但開啟網芳時，一樣是透過主要名稱瀏覽器來取得電腦清單，只不過原本用廣播來找尋主要名稱瀏覽器，現在則改成問 WINS。前面已經描述過主要名稱瀏覽器必然是網域內作業系統版本最高的電腦，這就有可能使得主要名稱瀏覽器與 WINS 伺服器不在同一台主機上，因此會導致網芳上面所看到的電腦名稱清單，並不是正確的。

當你發現某台主機從網芳看不到，但是可以 Ping 得到，無法從網芳存取分享檔案，但是可以用遠端連線磁碟機來存取時，便是發生了 WINS 與主要名稱瀏覽器不一致的情形。

為了避免發生這種現象，必須把 WINS 伺服器安裝在作業系統版本最高的機器上。

WINS 伺服器由於使用 TCP/IP 來封裝 Netbios 封包（NBT），所以可以跨越路由器。當同一個群組的電腦位於路由器的兩端時，它們雖然可以共用同一台 WINS 伺服器，但是卻需要兩台主要名稱瀏覽器來維護電腦名稱清單，這樣就會經常造成清單的不一致。

因此就算是使用 WINS 伺服器，您還是不應該將同一群組的電腦跨越在不同的網段上。這就是我們先前所提過的 Netbios 的重大缺陷，也就是 win 2000 捨棄 Netbios 的原因。

Samba 伺服器

由於 Linux 系統並不使用 Netbios 來作為電腦名稱，所以在 windows 的網芳看不到 Linux 主機是一種正常現象。但是如果我們在 Linux 上面安裝 Samba 伺服器，使用其提供的 NMB 和 SMB 服務，那就可以輕易將 windows 和 Linux 整合在同一個群組內。

Samba 所提供的 NMB 和 SMB 服務，其實也就是 WINS 伺服器所提供的 NBT 服務，事實上 Samba 不但可以當成 WINS 伺服器來使用，甚至還可以取代 NT 網域主控站，當成 PDC 來使用。Samba 的功能實在遠非 WINS 伺服器可比，況且它還是免費的。

關於 Samba 的三種應用，分別討論如下：

當作 WINS 用戶端

這是 Samba 伺服器最基礎的用途。Samba 當作 WINS 用戶端來使用時，能向 WINS 伺服器提出名稱登記、名稱解除以及名稱解析要求，讓 Linux 主機也可以從遠端存取 windows 工作站所分享出來的資料夾或檔案（使用 smbclient 以及 smbmount 工具），或是提供共享資源（包含檔案、資料夾和印表機）給 windows 工作站。

當作 WINS 伺服器

以 Samba 當作 WINS 伺服器效能並不好，而且經常會造成 Linux 主機的負載過重，而無法正常提供檔案分享服務。我們並不建議這樣用。

當作 PDC

Samba 套件具有 DES（MD4）編密工具，能夠管理和維護 Windows 帳號密碼，因此可以扮演 PDC 的角色，windows 使用者可以直接登入 Samba 主機，甚至是變更 windows 密碼。但是要具備這些功能，必須先在 Samba 主機上使用 smbpasswd 工具，一筆一筆將 windows 帳號建立起來。

除了完全取代 NT PDC 外，另外還有一種較為迂迴的做法，就是把 Samba 當成 PDC 的 proxy，這種做法有點像 windows 的 BDC，但是 Samba 本身並不備份和維護 windows 帳號，而是在使用者登入時，代為向 NT PDC 提出登入要求。

Netbios 名稱偵錯

使用 ipconfig /all 來檢查 Netbios 設定

C:\>ipconfig /all

Host Name . . . . . : spps130.spps.tp.edu.tw
DNS Servers . . . . . : 192.57.1.3
163.21.236.5
163.21.236.7
Node Type . . . . . : Hybrid
NetBIOS Scope ID. . . . . :
IP Routing Enabled. . . . : No
WINS Proxy Enabled. . . . : No
NetBIOS Resolution Uses DNS : Yes

0 Ethernet adapter :

Description . . . . . : Fast Ethernet PCI Adapter
Physical Address. . . . . : 00-80-C8-F7-ED-29
DHCP Enabled. . . . . : No
IP Address. . . . . : 192.57.1.130
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.57.1.253
Primary WINS Server . . . . :192.57.1.10
Secondary WINS Server . . . :
Lease Obtained. . . . . :
Lease Expires . . . . . :

上面各種組態中 Netbios 名稱服務以紅色標示，分別敘述如下：

Node Type . . . . . : Broadcast 表示本機以廣播方式從主要名稱瀏覽器取得 Netbios 名稱表列。Hybrid 表示透過 WINS 伺服器解析 Netbios 名稱，若找不到才使用 Broadcast 廣播。

NetBIOS Scope ID. . . . . : 表示 Netbios 轄區號碼，轄區號碼是用來定義 Netbios 群組，以便在同一子網域中分隔電腦共享資源成不同的表列。

WINS Proxy Enabled. . . . : No 表示不要成為WINS在本地網域代理者（如果設成 Yes，可以讓本機成為遠端WINS的本地端代理器，可以有效降低頻寬用量）

NetBIOS Resolution Uses DNS : Yes 表示要使用DNS來做Netbios名稱解析

使用 nbtstat 檢查 Netbios 狀態

-a 將 Netbios 名稱解析為 IP

-A 將 IP 解析為 Netbios 名稱

-n 列出本機提供共享的資源名稱

-s 用來顯示目前本機透過 Netbios 名稱服務取用資源的情形。

C:\>nbtstat -s

NetBIOS Connection Table

Local Name State In/Out Remote Host Input Output

SHANE <00> Connected Out WWW <20> 426KB 629KB
SHANE <03> Listening
SHANE Listening
ROOT <03> Listening

使用 net view 查看電腦清單

當網芳無法使用時，可以利用以下指令來查詢共享資源的名稱。

net view /Domain:群組名稱 列出該群組的電腦清單

net view \\電腦名稱 列出遠端電腦提供共享的資源名稱

使用 \\電腦名稱 或 \\IP 來存取分享資源

由於網路上的芳鄰所顯示的電腦清單是由主要名稱瀏覽器來維護，當主要名稱瀏覽器進行選舉時，會使用廣播封包，而廣播封包是無法跨越網段的，因此會造成跨越網段的 windows 網域其電腦清單不完整的現象，有時候因為主要名稱瀏覽器與備份名稱瀏覽器剛好同時被關機，也會造成電腦清單流失，在以上這些情況下，雖然打開網芳會看不到某台網域內的電腦，但在網址列直接輸入 \\電腦名稱還是可以連線成功，這表示 Netbios 名稱服務是正常的。當使用電腦名稱也無法連線，而必須在網址列直接輸入 \\IP 才能連通，這就表示工作站上的 Netbios 名稱解析機制無法正常工作。如果無法透過以上任一種方式連線，多半是作業系統失敗需要修復。

使用 smbclient 來找尋主要名稱瀏覽器

smbclient 是 Samba 所提供的工具，只能在 Linux 上使用，但是卻可以獲得比 windows 偵錯工具更多的重要訊息。可以用來剖析各個群組現用的主要名稱瀏覽器是哪一台，如果在多台電腦上查到的結果不一致，則可以斷定是 WINS 與主要名稱瀏覽器不在同一台電腦或跨越路由器造成的錯誤。

```
[root@mail shane]# smbclient -L cc1
Password:

Sharename Type Comment          -> cc1 所提供的共享資源
--------- ---- -------

Server Comment                  ->同一群組已經連線的電腦
--------- -------
CC1
OLDWEB

Workgroup       Master          ->網域內各個群組的主要名稱瀏覽器
---------       -------
CLASS           NBTEST
SPPS            SPPSPDC
SPPSCC          CC1
STU             SERVER
TEACHER         MAIL
WORKGROUP       WWW
```

DHCP 運作原理

「動態主機組態通訊協定」（Dynamic Host Configuration Protocol，DHCP）是用於將 TCP/IP 設定值自動指派至用戶端。工作站在啟動時，會從 DHCP 伺服器請求 IP 位址及其
他資訊（例如：DNS、預設閘道或 WINS 伺服器位址）。IP 位址來自定義於 DHCP 伺服器稱為轄區的資料庫中的「集中區」（pool）。伺服器會提供稱為「租期」（lease）的指定期間的 IP 位址。

這表示使用者不再需要從管理者處獲得 IP 資訊，或是必須為這些設定值而以人工方式設定電腦，這樣可以避免使用重複 IP 位址、設定值輸入錯誤而導致不能連線的問題發生。

DHCP 的運作方式如下：

1. 用戶端會送出 DHCP 請求封包，來源地址為 0.0.0.0（因為還沒有 IP），目的地為 255.255.255.255（因為還不知道 DHCP 是哪一台，因此使用廣播）這個階段稱為「IP租期請求階段」（IP lease request phase）
2. 所有（一部或一部以上）收到請求的 DHCP 伺服器會廣播答案。此廣播包含了請求者的MAC 位址、提供給請求者的 IP 位址和子網路遮罩、租期的長度以及提供的伺服器 IP 位址。這個階段稱為「IP租期提供階段」（IP lease offer phase）
3. 用戶端會接受最先到達的提議，然後廣播其已接受該項提議。這會讓提供的伺服器知道要「結束交易」，並讓其他的 DHCP 伺服器知道要取消它們的提議。這個階段稱為「IP租期選擇階段」（IP lease selection phase）
4. 已被接受提議的 DHCP 伺服器會廣播認可用戶端。如果伺服器是設定為提供訊息，則此訊息包含了有效的 IP 位址及其他的組態資訊。這個階段就是「IP租期認可階段」(IP lease acknowledgment phase)

在第四個階段以後，由於工作站已取得合法 IP ，並能以點對點方式與 DHCP 溝

通，而不需要再透過廣播。當工作站在到達 IP 租期一半的時間點時，會要求 DHCP 更新租期，當 IP 仍然有效時，DHCP 會回應認可訊息，或是任何更新設定值（當 IP 組態設定變更時），與前述第三和第四步驟類似。當 IP 無效而導致更新要求無法送達 DHCP 伺服器，則仍沿用舊設定值，直到租約到期後，再依前述四個步驟取得新的 IP。

DHCP 的功能

保留 IP：能保留一個或一組連續 IP不提供租用。

IP 租約期限：預設值為三天，可視需要自行修改。

領域組態設定：可以預先設定組態給一組 IP ，當這組 IP 中的某一個 IP 出租時，會傳送該組態給租用端。可設定的組態常用的有：預設閘道、子網路遮罩、DNS、WINS.....等。

衝突調解：當租出去的 IP ，發現與現有電腦發生衝突時，能取消租期，使工作站於租約到期後，租用另一個有效的 IP。

MAC 靜態對應：能配發某個固定 IP 給固定的用戶端。

DDNS：若使用 DHCP 4.0 以後的版本，則能傳送 DNS 登錄或刪除請求給 DDNS 伺服器，以達到動態對應網址的目的。

最後要注意的是，由於 DHCP 使用廣播封包，因此無法跨越交換器，除非交換器有提供 DHCP 支援功能。

DHCP偵錯

作業系統版本差異

使用前版 Win98，當工作站提出 IP 租期請求，因為網路塞車或因為 DHCP 忙碌中無法回應訊息，而未獲得任何回應的情況下，作業系統會自動沿用上次所取得的 IP ，而不去理會租約是否到期，這種情形下經常會造成 IP 衝突，必須手動更新 IP 才能解決。

新版的作業系統已經修正此問題，在同樣情況發生時，作業系統會自動指派 169.254 開頭的虛擬 IP，而不會佔用租約到期的 IP。

使用 ipconfig 來查看租期

C:\>ipconfig /all

Host Name . . . . . : spps130.spps.tp.edu.tw
DNS Servers . . . . . : 192.57.1.3
163.21.236.5
163.21.236.7
Node Type . . . . . : Hybrid
NetBIOS Scope ID. . . . . :
IP Routing Enabled. . . . . : No

WINS Proxy Enabled. . . . . : No
NetBIOS Resolution Uses DNS : Yes

0 Ethernet adapter :

Description . . . . . : Fast Ethernet PCI Adapter
Physical Address. . . . . : 00-80-C8-F7-ED-29
DHCP Enabled. . . . . : Yes
IP Address. . . . . : 192.57.1.130
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.57.1.253
Primary WINS Server . . . . :192.57.1.10
Secondary WINS Server . . . :
Lease Obtained. . . . . :Jan 19 13:44:56
Lease Expires . . . . . :Jan 21 01:44:56

與 DHCP 有關的部分以紅色表示，說明如下：

DHCP Enabled. . . . . : No表示此電腦並非使用 DHCP 來指派 IP
IP Address. . . . . : 192.57.1.130
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.57.1.253
Primary WINS Server . . . . :192.57.1.10
Secondary WINS Server . . . :以上為 DHCP 指派給租用端的網路組態設定
Lease Obtained. . . . . : 為 DHCP 租約生效的時間
Lease Expires . . . . . : 為 DHCP 租約到期的時間

釋放租期

ipconfig /release 網卡編號 ->釋放某片網卡的 IP

ipconfig /release_all ->釋放所有網卡的 IP

執行此指令會使得工作站失去所有網路設定值，並取消 DHCP 提供的 IP 租期。

更新租期

ipconfig /renew 網卡編號 ->更新某片網卡的 IP

ipconfig /renew_all ->更新所有網卡的 IP

當工作站設定為使用動態 IP 時，會立刻向 DHCP 提出更新租期的請求。但是當 IP 已經發生衝突時，使用這個指令會沒有作用。這時必須先釋放租期，重新向 DHCP 提出租用請求（先 release 再 renew）。

印表機上的 DHCP server

目前有許多印表機不但可以使用動態 IP（DHCP 用戶端程式），甚至還可以當作 DHCP 伺服器來使用。如果校園網路已經有使用 DHCP，那麼這種印表機將會造成 IP 大亂，因此當 DHCP 錯誤一直無法發現原因，不妨從印表機開始查起。