      Demilitarized Zone？照字面直翻的話就是指非軍事區域，而電腦網絡中 DMZ (Demilitarized Zone) 區域可以解析為一個既不屬於內部網域同時也不屬於外部網域的一個特殊區域，其目的就是了為防止外來入侵者直接存取內部機密資料，針對不同資源而提供不同安全級別的保護區域，因此在建立 DMZ 時原則上就是要跟內部使用 LAN的廣播網域獨立分開的區域網路。一般企業網站大多會建置 DMZ 供外界來查詢及使用，但並不包括內部的機密資料，如此一來如過不幸被外來入侵者侵入到 DMZ 並且癱瘓網路時，重要的資料仍不至於外泄。

     簡而言之，DMZ (Demilitarized Zone) 就是一個放至於內部網域及網際網域之間作為緩衝區域的小型網域。 就實際來說說 DMZ 也是需要進行 port 的存取管控，並加上有各層防火牆的 port mapping 管制，因此大多數DMZ主機還是只有開放指定的服務的，而並不是說放在 DMZ 的 Server 就是直接對外，設定時還是要開 port 還是要應對 IP，因此基本的安全性還是有的。 這樣說起來 DMZ 應該也算是安全的，但為何我確一直告訴大家非必要不要使用IP分享器的 DMZ 功能呢？道理很簡單，就因為它是IP分享器的DMZ功能！ 試想，一台一、二仟元的簡易IP分享器內含的DMZ功能，如果等同於數十萬硬體防火牆內建的DMZ功能的話？那為什麼還要花那麼多錢去購買幾十萬的硬碟防護設備？就因為IP分享器分內的 DMZ 功能並無法完全建立一個獨立的網域空間，而且為了使用者簡便操作原則為前提，只要一設定之後就預設將所有的 Port 對應到使用者對應的 IP，這樣的設定使用者來說真的很簡便，但設好之後跟電腦直接連到對外的實際路路有何不同呢？如果您的撥接帳戶的話，那還算是無所謂的，但如果是高頻寬的用戶，或是固定IP的用戶的話那幾乎是門戶大開，因為您所接的電腦是Server，而不是PC。 既然是 Server，那一定是有提供相對的 Service 功能的電腦才會叫做 Server，如果不加以管控的話，那侵入者一旦入侵之後，只要利用這部 Server 不須要破壞就可以達到它的目的，例如：假設 Server 本身有建置 Mail Server 的功能，那我入侵之後只要用它做跳板就可以不斷的亂發信件。

     電腦很多東西不是不能用，而是要瞭解如何去應用，就像我在先前回覆同學時所寫的內容： 檢查 Domain Name 設定的步驟沒有先檢查您的 http://domain 是否正確可以使用，檢查步驟如下： 1.先確認電腦可以正常上網(不一定是限Web Server，其它的電腦也可以) 2.執行 開始→所有程式集→附屬應用程式→命令提示字元 3.在 命令提示字元 視窗內輸入 ping www.xxx.xxx (www.xxx.xxx指的是您所設定的 Domain Name) 4.確認 pinging www.xxx.xxx [nnn.nnn.nnn.nnn] with 32 btyes of data: 此串字中是否確定有回應，且[nnn.nnn.nnn.nnn]內的IP數字確定是當初設定的實體IP 單純來說這樣檢查對嗎？ 如果對的話，我告訴大家，http://webgo.tw 的 IP是[60.249.57.82] 請大家依照上述所說的方式檢查 webgo.tw 是否可用？ 結果不用說，一定都是 Request timed out. 那是不是代表 webgo.tw 沒通？當然不是，如果是的話，那您現在不就是在看幽靈網站？所以我才會在上述的檢查條件下附註說明： 若出現 Request timed out. 訊息，那表示您的 Domain Name 根本就不通，有可能是Domain設定正確，但您電腦Server端的NOIP程式未開啟，或是電腦的防火牆擋住了，或是您的電腦根本就沒有實體IP，而是通過IP分享器上網的，這些基本資訊要提供完整才能判斷，但目前最少可以確認的是您的 Domain Name http://domain 跟您的 Server 沒有連上線。

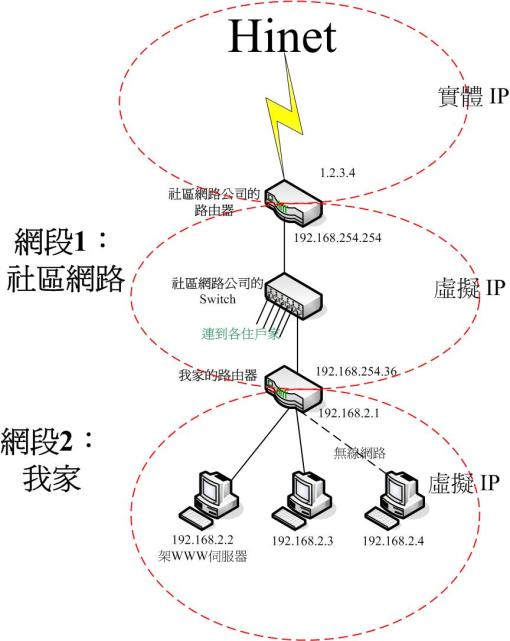
**如何在社區網路中分享多台電腦使用**

社區網路公司只給你一個虛擬 IP，如果家裡很多台電腦 (包含手機等) 要上網，一定要用 NAT，就是俗稱的 IP 分享器。IP 分享器不是只能分享實體 IP，虛擬 IP 也是可以分享的。 如圖，網段 1 是社區網路公司管理的部分，他們分配 192.168.254.36 給我用，我再根據這個 IP 分享出另外一個網段 2，就可以給我家其他電腦用。

因為社區網路公司一開始來你家裝，應該是接到你家某台電腦，所以路由器會把那台電腦的 MAC Address 記住，只認那台供上網使用。而當你換裝 NAT 之後，他們的路由器不認識 NAT 的 MAC Address，會不給你連上網，雖然顯示有連線，也是你的 NAT 和他們的路由器有連線，可是他們的路由器不給這個陌生的 NAT 連網。

所以換裝 NAT 並設定完記得要打電話給社區網路公司客服，說你有換裝 NAT，叫他們解除鎖卡號 (正確應稱為 MAC Address)，他們說解除鎖卡號之後約半小 時到一小時，等整個迴路內的 cache 全更新了就可以完全正常使用了。

我家的社區網路架構：(點擊看放大圖)

[](https://joechuang.files.wordpress.com/2010/03/e7b9aae59c9621.jpg)

**NAT 詳細設定**

社區網路公司提供的網路線插在 NAT 的 WAN 插口；你家的電腦插在 NAT 的 LAN  插口或是用無線連結。接下來登入到 NAT 的管理介面，設定如下：

**NAT 的 WAN 項目設定**

* Static IP (固定 IP)
* IP: 192.168.254.36 (社區網路公司給你的 IP)
* SubnetMask: 255.255.255.0 (社區網路公司給你的設定參數)
* Gateway: 192.168.254.254 (社區網路公司給你的設定參數，也是他們路由器在內部的 IP 位址)
* DNS: 168.95.192.1, 168.95.1.1 (這兩個都是中華電信的 DNS)

**NAT 的 LAN 項目設定**

* DHCP Range: 192.168.2.3~192.168.2.254 (動態發放的 IP 範圍)
* SubnetMask: 255.255.255.0
* Gateway: 192.168.2.1 (NAT 的 IP)
* DNS: 192.168.2.1 (NAT 的 IP)
* 之後 LAN 端的電腦就用自動取得 IP (DHCP) 即可。

**如果要架站**

1. 向社區網路要求開啟 port，但他們不會給你 well known port，我家的是給 10000 號以上的埠。
2. 在 NAT 設定 Port Mapping (Port Forwarding，此功能其實叫做 NAPT)，將社區網路公司給你的 port 轉到你架的伺服器 IP及Port。以上圖為例，如果社區網路公司給我 10000號埠，我要把它轉到我家的WWW伺服器，要如下設定：  
   Ext Port：10000  
   Int Port：80  
   Int IP：192.168.2.2  
   意即：把外面10000號埠接收到的訊息，轉發到 192.168.2.2 的 80 號埠  
   這樣就可以從外面使用 <http://122.117.51.243:10000/> 連到我家的 WWW伺服器。
3. 你電腦的 Windows 防火牆記得要打開該 Port 號。

**如果把伺服器那台放到 DMZ 中**

如此就不必設定 Port Forwarding 了，但是不會幫你轉 Port，所以如果社區網路導入了一個10000號的連線，你的伺服器也只能從 10000號接收，這時就只能修改伺服器軟體的監聽埠號，改成10000號了。