Open DNS resolver 的問題

- NOTICE 自2014/01/20（一）起，**若偵測為 open DNS resolver 將自動阻斷其IP**，請使用者務必修正問題，以免屆時網路遭阻斷。**阻斷處理，詳**「不當網路資訊」
- 由於軟體及設備種類繁多，歡迎知悉某特定軟體或設備其修正方法者，能不吝提供資料，嘉惠眾人，詳：網路設備

問題概述

Open DNS resolver 指 Caching recursive DNS 伺服器對外公開（不限使用對象）提供名稱遞迴解析 (recursive name resolution)服務，可能產生以下問題：

1. 暴露於外界，容易被攻擊或平白**損耗系統及網路資源**
2. 發生**暫存中毒(cache poison)問題**
3. 容易**被外界利用，成為發動 DDoS 網路攻擊的一員**

偵測系統

NEW為防治 open DNS resolver 問題，協助處理校園內電腦因設定不慎而可能遭攻擊者利用來發動網路攻擊，故本組建置 open DNS resolver 偵測系統，**並將偵測結果提供各單位網管，以便轉知其使用者參考建議作法來修正設定及自行檢測問題是否解決**，藉以減少本校網路內 open DNS resolver 的數量。

最近七天內偵測結果

- NOTICE **若已存在本清單的 IP 地址，至少需等待至隔日系統重新偵測，通過後時才會移除**，故擬移出本清單者，請先用下方的「即時檢測服務」，檢查確認該 IP 地址已無問題後，隔日應可自清單中移除。

更新時間Wed May 28 16:45:00 2025 Asia/Taipei

序號	單位	IP 位址	偵測時間	備註
總計摘 0 筆記錄				

即時檢測服務

NEW為方便本校使用者**自行檢測其電腦或網路設備是否具有 open DNS resolver 的問題**，特建置此即時的檢測服務，**目前限由本校 IP 位址來進行檢測**。(2013/08/30上線試用)

檢測 open DNS server IP 位址: 1 . 1 . . .

- NOTICE檢測前**請先確認目標 IP 位址的電腦或設備狀態為開機且網路連線正常**，以免影響檢測結果。

檢測說明

- 類似以下輸出結果，表**具有 open DNS resolver 問題**

- **不應回覆非其所轄的 DNS 查詢**

```
Check open dns resolver for the target IP 140.114.xx.xx
Time: Wed Sep 11 09:10:11 2013

check_open_resolver: 140.114.xx.xx
DIG:
DIG: ; <<>> DiG 9.6-ESV-R7-P2 <<>> @140.114.xx.xx -t A isc.org
DIG: ; (1 server found)
DIG: ;; global options: +cmd
DIG: ;; Got answer:
DIG: ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13648
DIG: ;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4,
ADDITIONAL: 2
DIG:
DIG: ;; QUESTION SECTION:
DIG: ;isc.org.          IN    A
DIG:
DIG: ;; ANSWER SECTION:
DIG: isc.org.       60    IN    A    149.20.64.69
DIG:
DIG: ;; AUTHORITY SECTION:
DIG: isc.org.       1814    IN    NS    sfba.sns-pb.isc.org.
DIG: isc.org.       1814    IN    NS    ns.isc.afilias-nst.info.
DIG: isc.org.       1814    IN    NS    ams.sns-pb.isc.org.
DIG: isc.org.       1814    IN    NS    ord.sns-pb.isc.org.
DIG:
DIG: ;; ADDITIONAL SECTION:
DIG: ns.isc.afilias-nst.info. 54300 IN    A    199.254.63.254
DIG: ns.isc.afilias-nst.info. 54300 IN    AAAA    2001:500:2c::254
DIG:
DIG: ;; Query time: 402 msec
DIG: ;; SERVER: 140.114.xx.xx#53(140.114.xx.xx)
DIG: ;; WHEN: Wed Sep 11 09:10:11 2013
DIG: ;; MSG SIZE  rcvd: 184
DIG:

CHECK : Is 140.114.xx.xx an open resolver?
ANSWER: YES for 140.114.xx.xx
REASON: IP 140.114.xx.xx should not reply the DNS request which
does not belong to its authorized zone.
```

- 類似以下輸出結果，表**不具有 open DNS resolver 問題**
  1. **DNS 無法連線**，若電腦已開且網路已通，則此機無問題。

```
Check open dns resolver for the target IP 140.114.63.1
Time: Wed Sep 11 09:26:32 2013

check_open_resolver: 140.114.63.1
DIG:
DIG: ; <<>> DiG 9.6-ESV-R7-P2 <<>> @140.114.63.1 -t A isc.org
```

```
DIG: ; (1 server found)
DIG: ;; global options: +cmd
DIG: ;; connection timed out; no servers could be reached

CHECK : Is 140.114.63.1 an open resolver?
ANSWER: NO for 140.114.63.1
REASON: Cannot reach 140.114.63.1. If its power is off, please
turn it on and check again.
```

2. **拒絕遞迴查詢** (recursive query)

```
Check open dns resolver for the target IP 140.114.63.10
Time: Wed Sep 11 09:27:47 2013

check_open_resolver: 140.114.63.10
DIG:
DIG: ; <<>> DiG 9.6-ESV-R7-P2 <<>> @140.114.63.10 -t A isc.org
DIG: ; (1 server found)
DIG: ;; global options: +cmd
DIG: ;; Got answer:
DIG: ;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 7118
DIG: ;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0,
ADDITIONAL: 0
DIG: ;; WARNING: recursion requested but not available
DIG:
DIG: ;; QUESTION SECTION:
DIG: ;isc.org.          IN    A
DIG:
DIG: ;; Query time: 2 msec
DIG: ;; SERVER: 140.114.63.10#53(140.114.63.10)
DIG: ;; WHEN: Wed Sep 11 09:27:47 2013
DIG: ;; MSG SIZE  rcvd: 25
DIG:

CHECK : Is 140.114.63.10 an open resolver?
ANSWER: NO for 140.114.63.10
REASON: Recursion requested but not available
```

建議作法

DNS伺服器

為降低遭攻擊者利用機會，本中心提供 DNS 查詢服務，僅限本校IP位址使用。**請各系所單位伺服器管理者參酌以下建議作法，拒絕對非限定使用者(校外IP位址)提供遞迴解析(recursive resolution)的查詢服務，以避免 Open DNS resolver 問題**

1. 伺服器若**非必要提供 DNS 查詢服務，請關閉之**

2. **Caching recursive DNS 伺服器與註冊 domain name 的 Authoritative DNS 伺服器用途有別，要用不同 IP 位址來建置**，不要使用相同 IP 位址，以方便設定並提高安全性。
    1. **Caching recursive DNS 伺服器**，請限制其服務對象的來源IP位址(如：系所單位內部 IP 位址)，建議優先採用以下第一個方法：
        1. 以伺服器作業系統自身或外部的**防火牆來限制 DNS 使用者的來源IP位址(DNS 服務埠號為port UDP/53)**。
        2. 以 DNS 應用軟體（如BIND的 **ACL (access control list) 來限制來源IP位址**，如：BIND 設定的 acl 及 allow-query，詳參考資料。

```
acl nthu-nets { 140.114.0.0/16; 127.0.0.1/32; };
options {
   //(其他參數略...)
    // Recursive Name Server
    allow-query { nthu-nets; };
};
```

    2. **Authoritative DNS 伺服器**請用 DNS 應用軟體（如BIND的功能來**限制遞迴查詢權限(recursive query)**，如：BIND 設定的 recursion no，詳參考資料。

```
options {
   //(其他參數略...)
    // Authoritative-only Name Server
    recursion no;
    allow-query-cache { none; };
    allow-query { any; };
};
```

BIND

A. 限制來源 IP 位址

適用 Caching recursive DNS 伺服器，以 ACL (access control list) 限制使用者來源 IP 位址，設定方式詳：BIND 設定的 acl 及 allow-query，以下為設定檔 named.conf 相關參數。

```
acl nthu-nets { 140.114.0.0/16; 127.0.0.1/32; };
options {
   //(其他參數略...)
    // Recursive Name Server
    allow-query { nthu-nets; };
};
```

B. 限制遞迴查詢權限

適用Authoritative DNS 伺服器，設定**限制遞迴查詢權限(recursive query)**，詳：BIND 設定的 recursion no，以下為設定檔 named.conf 相關參數。

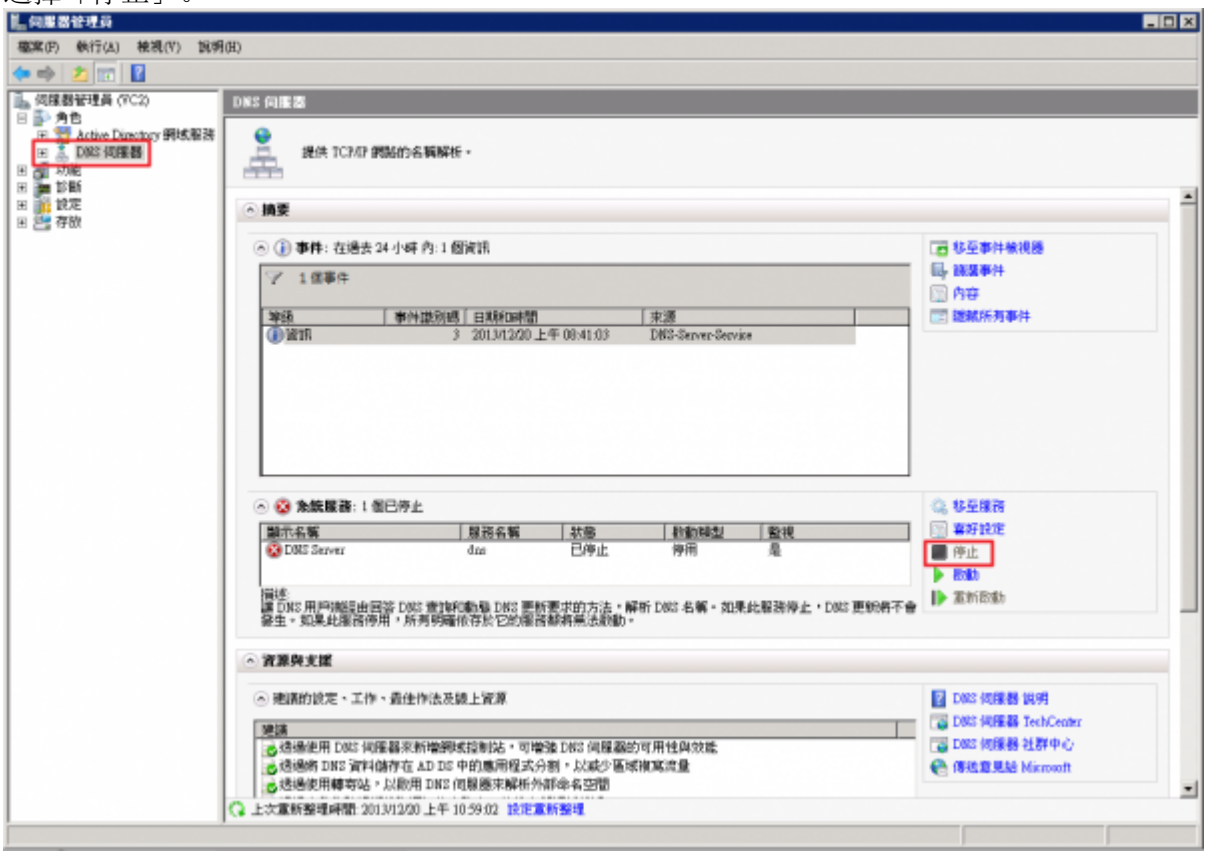
```
options {
   //(其他參數略...)
```

```
    // Authoritative-only Name Server
    recursion no;
    allow-query-cache { none; };
    allow-query { any; };
};
```

Windows 2008

A. 停止 DNS 伺服器的作法

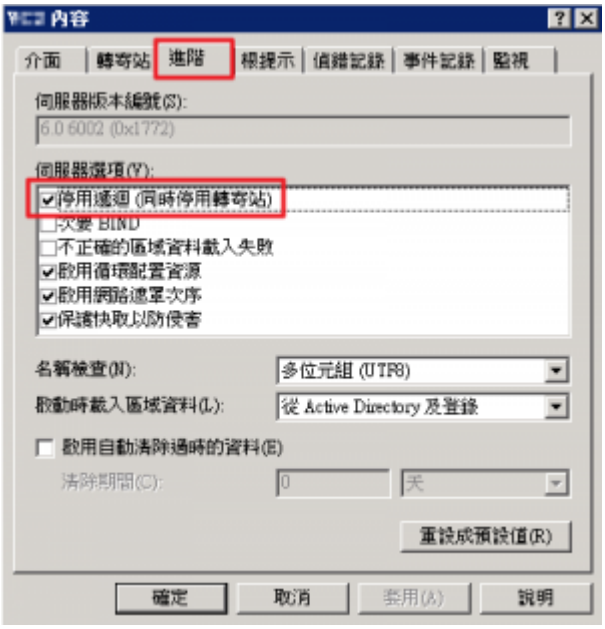
1. 由「開始」/「控制台」/「系統管理工具」/「伺服器管理員」視窗，如下圖，選擇□DNS伺服器」，選擇「停止」。



B. 僅關閉遞迴查詢權限(recursive query)的作法

1. 由「開始」/「控制台」/「系統管理工具」/「伺服器管理員」視窗，如下圖，選擇□DNS伺服器」，選擇□DNS□□主機名，選擇「內容」。

2. 由「內容」視窗，如圖，選擇「進階」，勾選「停用遞迴(同時停用轉寄站)」。



Windows 7

- 以下 A, B, C 三種方法，請視自己的情況選擇合適者。

A. 關閉Windows 7(ICS)服務，防止 DNS 服務

- 關閉Windows 7(ICS)服務，防止open DNS resolver

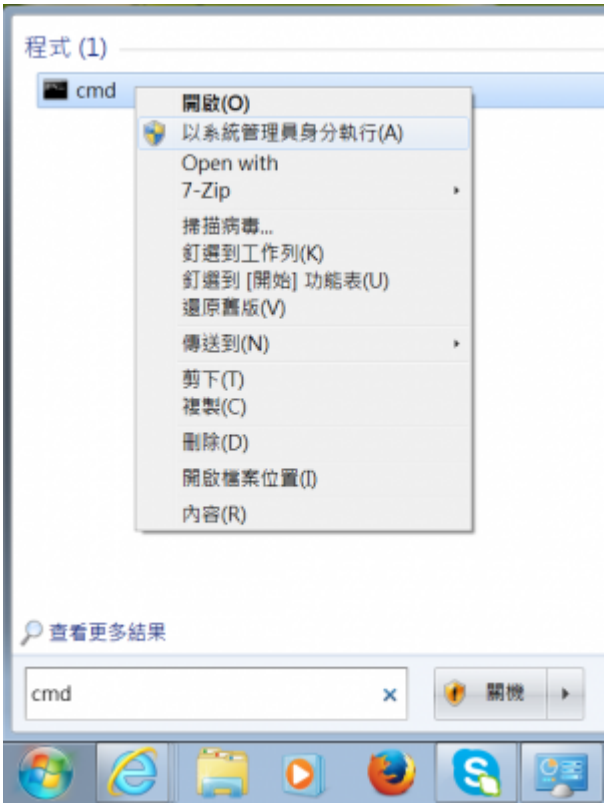
B. 以防火牆阻斷 DNS 服務

- 利用防火牆**拒絕任何 DNS 查詢封包（UDP/53）**

1. 設定Windows 7防火牆，防止open DNS resolver
2. 設定賽門鐵克防火牆，防止open DNS resolver

C. 找出 DNS 服務之對應程式並關閉之

1. **以系統管理員身份執行 cmd** 程式，如下圖



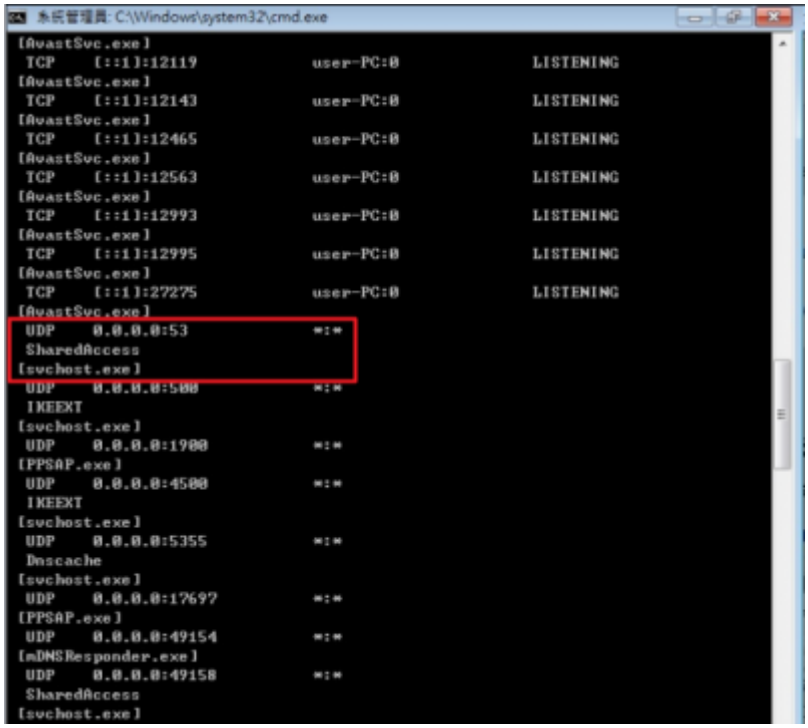
2. 執行 **netstat -ab -p UDP** 指令，以下方框為例，找出 **UDP 0.0.0.0:53 (表提供 DNS 服務)**這行資訊，則其對應的元件為 XXXXX□程式為 [yyyy.exe]□

```
C:\Windows\system32>netstat -ab -p UDP

使用中連線

  協定    本機位址               外部位址               狀態
  UDP    0.0.0.0:500            *:*
  IKEEXT
 [svchost.exe]
...
  UDP    0.0.0.0:53             *:*
  XXXXX
 [yyyyy.exe]
...
```

   - 以下圖為例，元件 SharedAccess□程式 svchosts.exe 造成 DNS 服務開啟。請使用者自行判斷是否能停止該程式及其設定方式。

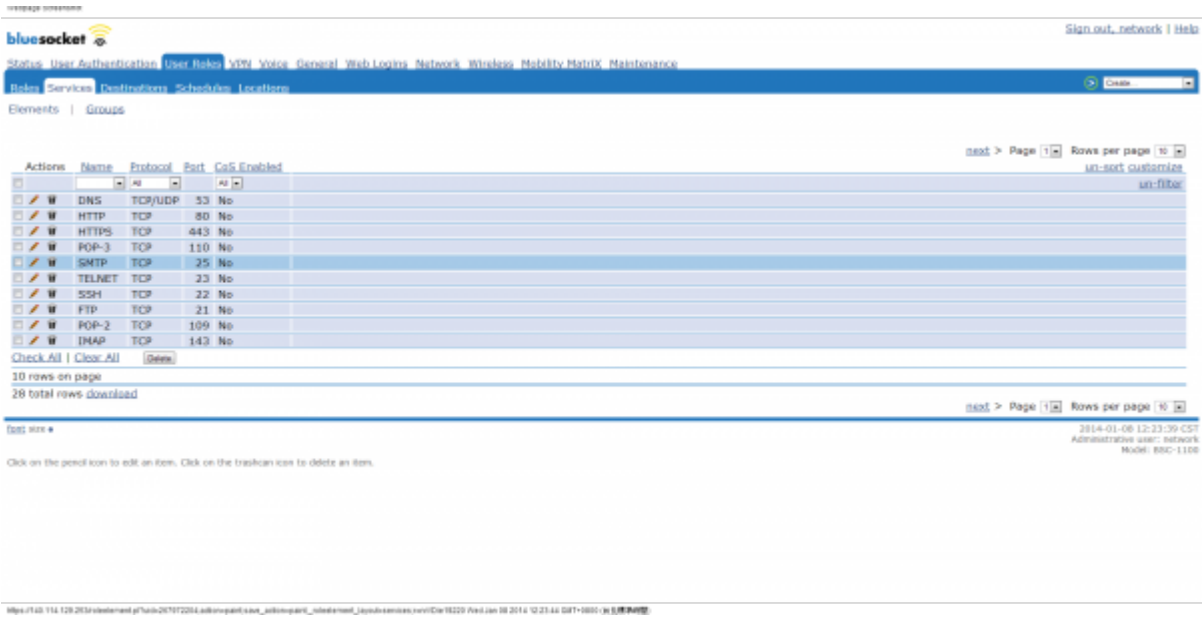


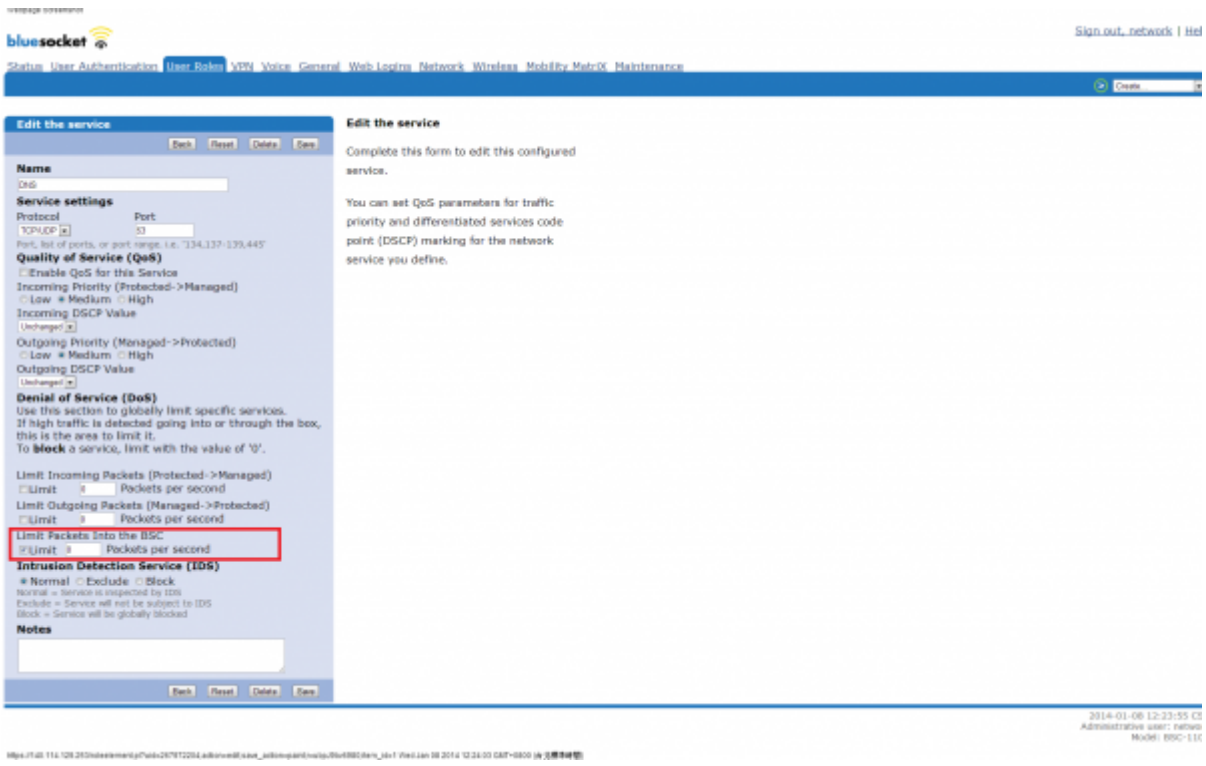
網路設備

NOTICE有些網路設備（如：無線網路閘道器IP分享器、或路由器）本身可能具有 open DNS resolver 問題，需適當調整設定或以防火牆來處理，**由於網路設備的類型繁多，若您知悉某裝置該如何處理，歡迎提供設備廠牌、型號、軟(韌)體版本、及其設定方式的畫面，寄至 mucheng @ cc.nthu.edu.tw以利製成以下網頁，嘉惠眾人，格式及文字可參考以下作法，謝謝!**

Bluesocket 網路設備

- NEW Bluesocket BSC-1100 無線網路認證閘道器：避免 open DNS resolver 問題之設定方式請參考下圖，本資料感謝化工系康嘉麟先生提供(2014/01/08)。
  - 將 **DNS** service 的 **Limit Packets Into the BSC** 選取限制流量為 **Limit 0 Packets per second**





D-Link 網路設備

- NEW D-Link DI-624S避免 open DNS resolver 問題之設定方式請參考下圖，本資料感謝物理系曾冠翔先生提供(2014/02/13)。
  - 設定 **DNS Relay 停用**

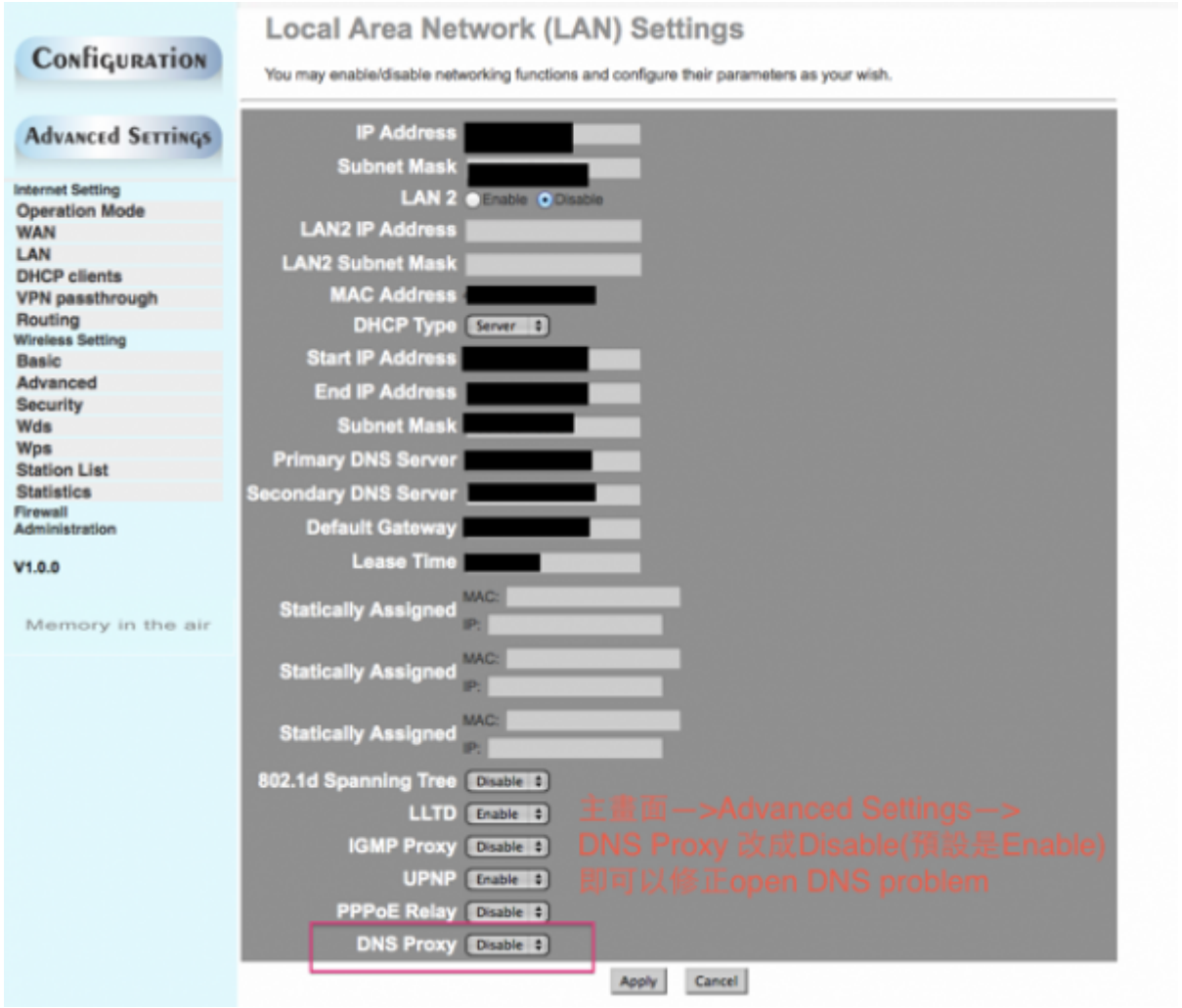
- NEW D-Link DIR-615(**使用DD-WRT韌體**)：避免 open DNS resolver 問題之設定方式請參考下圖，本資料感謝工科系何孟軒先生提供(2014/02/13)。
  - 取消 **Use DNSMasq for DHCP** 及 **Use DNSMasq for DNS**

PCI 網路設備

- NEW PCI MZK-W04NU IP 分享器：避免 open DNS resolver 問題之設定方式請參考下圖，本資料感謝工工系郭峻吉先生提供(2014/01/07)。
  - 利用防火牆**拒絕任何 DNS 查詢封包（UDP/53）**，故目的地 IP 位址填上該設備 WAN 的 IP 位址，目的地埠號為 53。

PQI 網路設備

- NEW PQI Air Pen express 迷你無線網路路由器：避免 open DNS resolver 問題之設定方式請參考下圖，本資料感謝資工系謝侑驊先生提供（2013/12/13）。



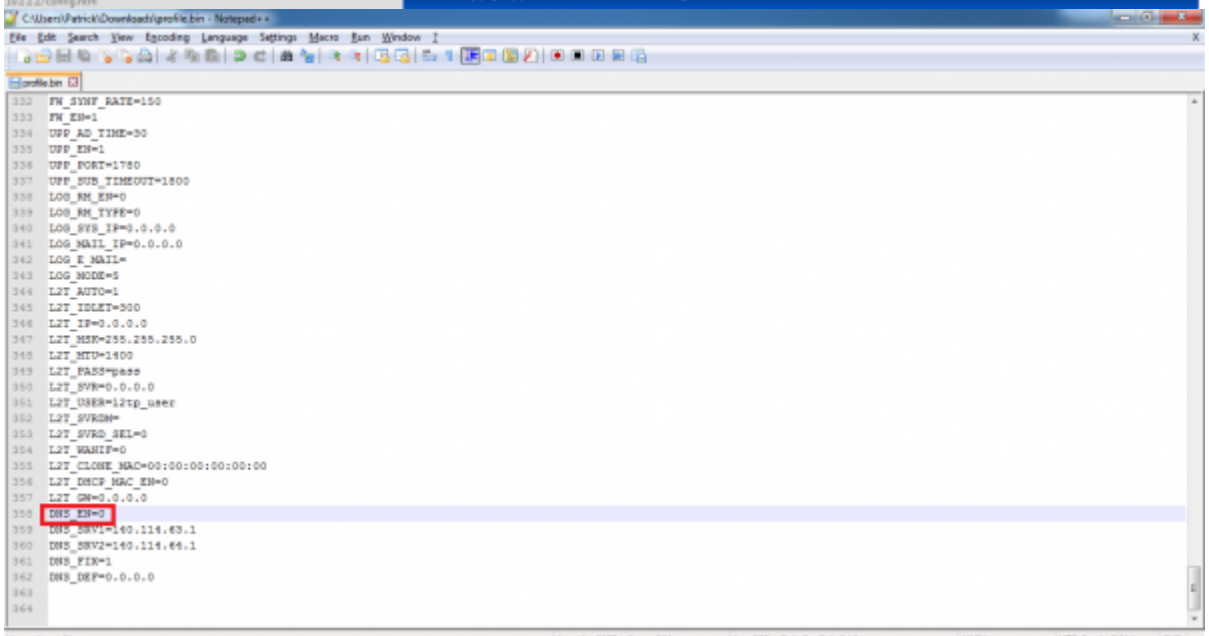
SAPIDO 網路設備

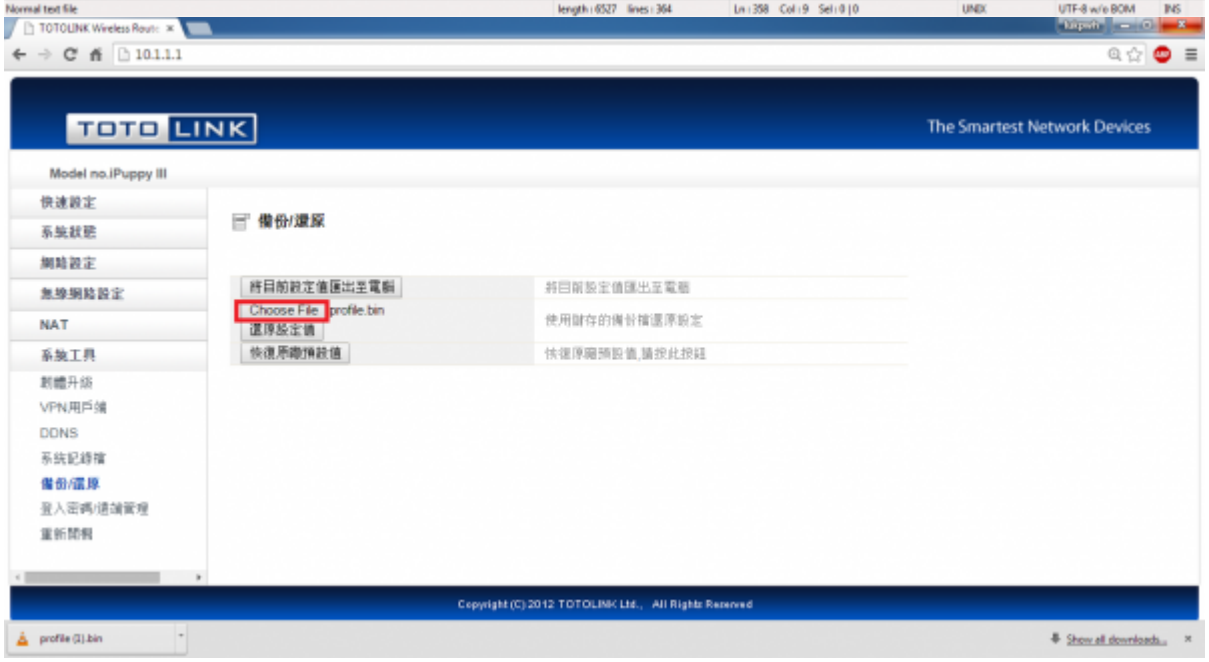
- NEW SAPIDO RB-1802 無線分享器：避免 open DNS resolver 問題之設定方式請參考下圖，本資料感謝反應器組黃昱翔先生提供（2014/01/13）。
  - 利用 NAT 將 DNS 轉給不存在的 IP 位址（本例用中 192.168.1.254），設定**啟用連接埠轉發**，同時設定位址：192.168.1.254，通訊協定：**UDP**，公用埠範圍：**53-53**，與註解□DNS□然後按下**套用變更**，即可修正open DNS resolver的問題。

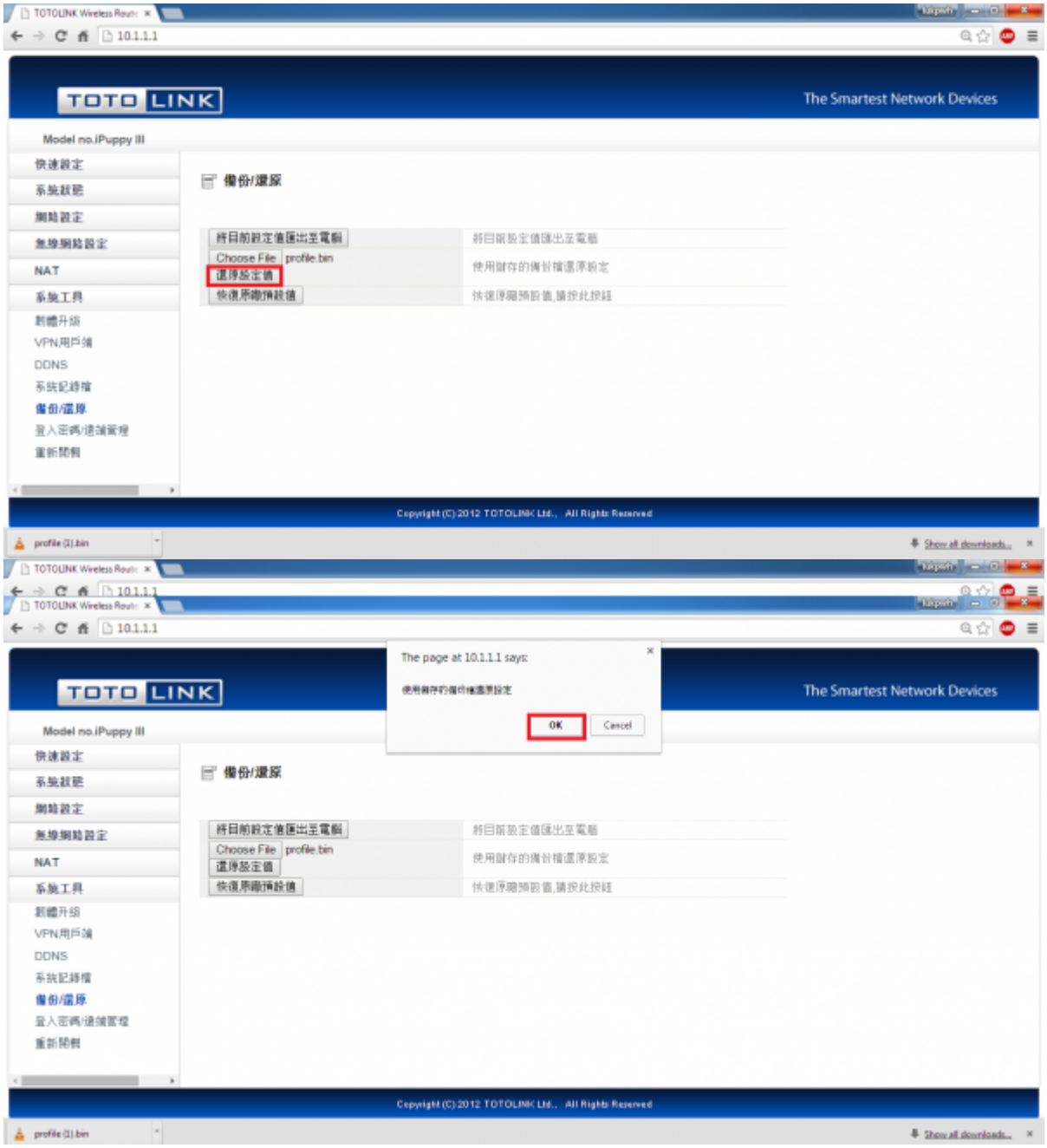
TOTOLINK 網路設備

- NEW TOTOLINK IPUPPY III 無線分享器：避免 open DNS resolver 問題之設定方式請參考下圖，本資料感謝陸同學提供（2015/03/11）。
  - 因該設備 UI 沒有關閉 DNS 服務的選項，須透過「系統工具」中「備份/還原」的功能，直接修改系統設定值來解決 open DNS resolver 的問題。

TOTOLINK Wireless Router
10.1.1.1
TOTO LINK
The Smartest Network Devices
Model no.iPuppy III
快速設定
系統狀態
網路設定
無線網路設定
NAT
系統工具
韌體升級
VPN用戶端
DDNS
系統記錄檔
備份/還原
登入密碼/遠端管理
重新開機
備份/還原
將目前設定值匯出至電腦
Choose File
No file chosen
還原設定值
恢復原廠預設值
將目前設定值匯出至電腦
使用儲存的備份檔還原設定
恢復原廠預設值,請按此按鈕
Copyright (C) 2012 TOTOLINK Ltd., All Rights Reserved

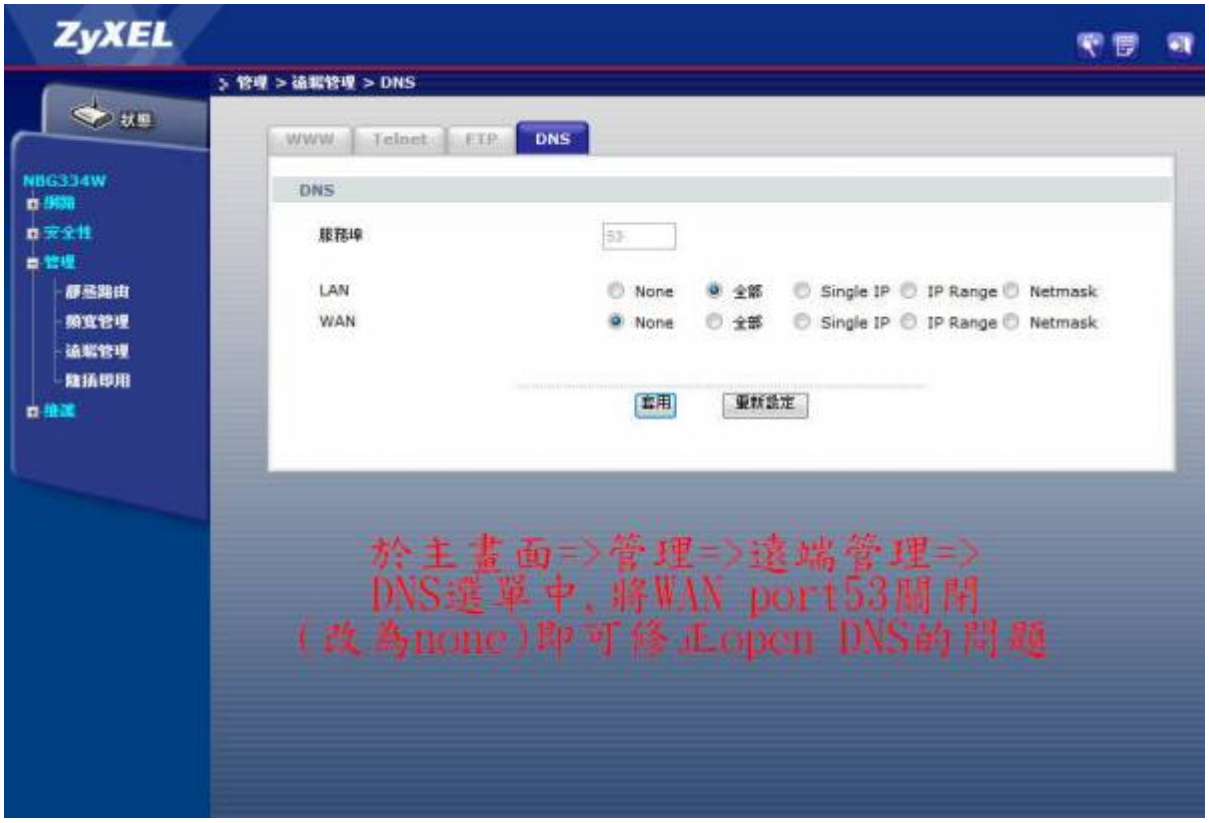

C:\Users\Patrick\Downloads\profile.bin - Notepad++
profile.bin
FW_SYNF_RATE=150
FW_EN=1
UPP_AD_TIME=30
UPP_EN=1
UPP_PORT=1750
UPP_SUB_TIMEOUT=1800
LOG_RM_EN=0
LOG_RM_TYPE=0
LOG_SYS_IP=0.0.0.0
LOG_MAIL_IP=0.0.0.0
LOG_E_MAIL=
LOG_MODE=5
L2T_AUTO=1
L2T_IDLET=300
L2T_IP=0.0.0.0
L2T_MSK=255.255.255.0
L2T_MTU=1400
L2T_PASS=pass
L2T_SVR=0.0.0.0
L2T_USER=l2tp_user
L2T_SVRDN=
L2T_SVRD_SEL=0
L2T_WANIF=0
L2T_CLONE_MAC=00:00:00:00:00:00
L2T_DHCP_MAC_EN=0
L2T_GW=0.0.0.0
DNS_EN=0
DNS_SRV1=140.114.63.1
DNS_SRV2=140.114.64.1
DNS_FIX=1
DNS_DEF=0.0.0.0
Normal text file
length : 6527 lines : 364
Ln : 358 Col : 9 Sel : 0 | 0
UNIX
UTF-8 w/o BOM
INS


TOTOLINK Wireless Router
10.1.1.1
TOTO LINK
The Smartest Network Devices
Model no.iPuppy III
快速設定
系統狀態
網路設定
無線網路設定
NAT
系統工具
韌體升級
VPN用戶端
DDNS
系統記錄檔
備份/還原
登入密碼/遠端管理
重新開機
備份/還原
將目前設定值匯出至電腦
Choose File
profile.bin
還原設定值
恢復原廠預設值
將目前設定值匯出至電腦
使用儲存的備份檔還原設定
恢復原廠預設值,請按此按鈕
Copyright (C) 2012 TOTOLINK Ltd., All Rights Reserved
profile (1).bin
Show all downloads...



ZyXEL 網路設備

- NEW 合勤 ZyXEL NBG334W 高速寬頻路由器：避免 open DNS resolver 問題之設定方式請參考下圖，本資料感謝生科院許富銘先生提供(2013/09/25)。



防火牆用法

- 本校Caching recursive DNS server (140.114.63.1) 以防火牆來限制使用者，以下為校外 IP 使用本校 140.114.63.1 來查詢非本校網域名稱 google.com 無法獲得正確回應。

```
# dig @140.114.63.1 google.com

; <<>> DiG 9.3.6-P1 <<>> @140.114.63.1 google.com
; (1 server found)
;; global options:  printcmd
;; connection timed out; no servers could be reached
```

- 但若用校內 IP□則可獲得正確回應。

```
# dig @140.114.63.1 google.com

; <<>> DiG 9.3.6-P1 <<>> @140.114.63.1 google.com
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 741
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 4, ADDITIONAL: 4

;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             116     IN      A       173.194.72.101
```

```
google.com.             116     IN      A       173.194.72.100
google.com.             116     IN      A       173.194.72.113
google.com.             116     IN      A       173.194.72.102
google.com.             116     IN      A       173.194.72.138
google.com.             116     IN      A       173.194.72.139

;; AUTHORITY SECTION:
google.com.             156701  IN      NS      ns4.google.com.
google.com.             156701  IN      NS      ns1.google.com.
google.com.             156701  IN      NS      ns2.google.com.
google.com.             156701  IN      NS      ns3.google.com.

;; ADDITIONAL SECTION:
ns1.google.com.         156702  IN      A       216.239.32.10
ns2.google.com.         156702  IN      A       216.239.34.10
ns3.google.com.         156703  IN      A       216.239.36.10
ns4.google.com.         156702  IN      A       216.239.38.10

;; Query time: 35 msec
;; SERVER: 140.114.63.1#53(140.114.63.1)
;; WHEN: Wed Apr 17 14:54:15 2013
;; MSG SIZE  rcvd: 260
```

參考資料

- DNS SURVEY: OPEN RESOLVERS
- 線上檢測是否為 Open resolver 的網站
  1. 可同時檢查10個IP位址
  2. Open DNS Resolver Project|清查 Class C (非即時的歷史資料)
- Open DNS Resolver Project
  - DNS 伺服器的設定參考資料(BIND, Microsoft)
- 認識DNS反射式攻擊
- DNS amplification attack
- NEW 開放性 DNS 解析伺服器之防治, TANET2013 臺灣網際網路研討會

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
https://net.nthu.edu.tw/netsys/dns:open_resolver

Last update: **2019/10/17 14:58**