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

I□□□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

NOTCE 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[]Thu Feb 01 07:00:00 2024 Asia/Taipei

序號 單位 IP 位址 偵測時間 備註 總計摘0 筆記錄

総計摘り車記録

即時檢測服務

■■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 . . . 0000 000

• 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: gr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4,
ADDITIONAL: 2
DIG:
DIG: ;; QUESTION SECTION:
DIG: ;isc.org.
                        IN
                              Α
DIG:
DIG: ;; ANSWER SECTION:
DIG: isc.org.
                                     149.20.64.69
                    60
                          IΝ
                               Α
DIG:
DIG: ;; AUTHORITY SECTION:
DIG: isc.org.
                            IN
                                  NS
                                        sfba.sns-pb.isc.org.
                    1814
DIG: isc.org.
                    1814
                            IΝ
                                  NS
                                        ns.isc.afilias-nst.info.
                            IN
                                  NS
                                        ams.sns-pb.isc.org.
DIG: isc.org.
                    1814
                            IΝ
                                        ord.sns-pb.isc.org.
DIG: isc.org.
                    1814
                                  NS
DIG:
DIG: ;; ADDITIONAL SECTION:
DIG: ns.isc.afilias-nst.info. 54300 IN
                                              199.254.63.254
                                          Α
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 А 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∏

- 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」。

2 🖬 🛛				
観智理員 (TC2)	DNS (CIRE 28			
Active Directory 钢线服装 之 DMA 何應翻 初胞 診斷 設定 方称	提供 TCP/	17 網路的名稱解析。		
12103	③ ④ 事件: 在送	去 24 小蚌 內: 1 個演訊		高 核至事件被視錄
	▼ 1個事件			E, 1838##
				内容
	3420	● ● 仲間/明朝 日期時回時間 3 2013/12/20 トモ 09:41	東源 ①3 DNS-Server-Service	() (2) (2) (2) (2) (2) (2) (2) (2) (2) (
	· · · · · · · · · · · · · · · · · · ·	1 個已等止		Q, U至購務
	 ○ ※ 先該服務: ■元名第 	1個已等止 服務名職 計算	6. 私勤時益 · 監視	42, 移至陳務 131 事好技定
	 · · · · · · · · · · · · · · ·	1 個已停止 開路名編 林島 dan 已A	8	 4. 新至陳務 1. 重要的設定 ● 中止
	 金 急銃爆器:	1 個已停止	8 計動構型 整視 止 停用 是 5法。解析 D003 名稱 - 如果此服務停止 · D003 更新 5款動 ·	 45 年度課務 25 年月12年 25 年月12年 25 年月12年 25 年月12年 25 年月12年 25 年月12日 26 年月12日 27 年月12日
	 ◇ 灸放服器: ● ◇ 灸放服器: ● DMS Server ● DMS Server ● MR 中国総営 ● 全・知果北陽行 ◇ 資源発支援 	1 個已存止	5 <u>新動機型 数視</u> P止 停用 是 5法・解析 Dol3 名編 - 如果此服務停止・Dol3 更新 5款動 -	 ○ 都至陳務 ○ 事好設定 ○ 停止 > 形動 ▶ 形動 ▶ 面前
	 ● ● 金数服務: ● 回該 Server ● 回該 Server ● 回東中国 ● 定調的設定、3 	1 個已停止	8	 ○ 報告課務 ○ 報告記 ○ 第告記 ○ 第告記 ○ 第告記 ○ 第告記 ○ 面前形動
	 ○ ② 免鉄服務: ○ DOS Server ○ DOS Server ○ DOS Server ○ 意思発支援 ○ 意思発支援 ○ 意思発支援 ○ 地話的設定、3 ○ 建活的設定、3 	1 個已停止	8	 ○ 報至陳符 ○ 報好拉定 ○ 第好拉定 ○ 第分拉定 ○ 第分社 ○ 第分社 ○ 第一次 ○ 第二次 ○ 第二次

- 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」。



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

程式 (1) -		
Cmd	開啟(O)	
	掃抽病霉 釘選到工作列(K) 釘選到 [開始] 功能表(U) 還原舊版(V)	
	傳送到(N) 剪下(T) 複製(C) 刪除(D)	•
	開設檔案位置(I) 內容(R)	
₽ 查看更多約	结果	
cmd	×	🕐 關機 →
چ 🌜	3 🚞 🖸 🝯	8 🦻

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]
. . .
        0.0.0:53
                               * *
 UDP
 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。

▲ 未託管理員: C:\Windows\system32	\cmd.exe	-0	
[AvastSvc.exe]			· ·
TCP [::1]:12119	user-PC:0	LISTENING	
[AvastSvc.exe]			
TCP [::1]:12143	user-PC:8	LISTENING	
[AvastSvc.exe]			
TCP [::1]:12465	user-PC:0	LISTENING	
[AvastSvc.exe]			
TCP [::1]:12563	user-PC:0	LISTENING	
[AvastSvc.exe]			
TCP [::1]:12993	user-PC:0	LISTENING	
[AvastSvc.exe]			
TCP [::1]:12995	user-PC:0	LISTENING	
[AvastSvc.exe]			
TCP [::1]:27275	user-PC:0	LISTENING	
[AvastSvc.exe]			
UDP 0.0.0.0:53	*:*		
SharedAccess			
[svchost.exe]			
UDP 0.0.0:500	*:*		
IREEXT			=
Isvchost.exel			
006.0.0.0.0:1069	*1*		
UDF 0.0.0.0:1500	*:*		
Incent out)			
Deceache	-1-		
Feuchast avel			
IIDP 0.0.0.0:17697	***		
[PPSAP.exe]			
IIDP 8.8.8.8:49154			
[mDNS Regmonder, eve]			
UDP 8.0.0.0:49158			
SharedAccess			
[sychost.exe]			

網路設備

№ 11 (19) (如:無線網路閘道器]|P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□

luesock	et 🛜				Sign.out, network H
atus Use	r.Authenti	cation Use	er Role	VPN Voice	
					5 Case.
Ser.	ICES CAR	190.013 2	CALCOLD.	as Locations	
ements	Groups				
					next > Page 1 Rows per page 10 -
Actions	Name	Protocol	Part	CoS Enabled	un-sort customize
	THE .	700000		AI [.	un-filter
1.	HTTP	TOPUDP	33	No	
18	HTTPS	TCP	443	No	
18	POP-3	TOP	110	No	
18	SMTP	TOP	25	No	
/ 8	TELNET	TOP	23	No	
/ 8	55H	TOP	22	No	
/ W	FTP	TCP	21	No	
1.4	POP-2	TOP	109	No	
× w	IMAP	TOP	143	No	
neck.All	Clear All	Gelete			
0 rows or	page				
8 total re-	ws downlo	ba			next > Page 1 Rows per page 10 R
t size e					2814-01-0612-23-39 C Administrative user: network Model: RRC-1
ck on the pr	encli Icon to I	dit on item.	Citck on	the trashcan loss	



D-Link 網路設備

• IEW 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

D-Link Building Networks for People	AirPlus KTREM Wireless 108G Storag	e Router
DI-624S	主頁 進階功能 工具 狀態	影影
設定蓄量	■減頻路設定 本功能為設定 DI-624S 的區域網路端 (LAN端) IP 位址。 IP 位址	
	子網路這單 255.255.255.0 本概網域名稱 (可省略)	(optional)
	DNS Relay ○ 啟用 ^⑥ 停用	
DHCP伺服器 檔案分字		
FTP向服器		
WEB伺服器		

- IN■ 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

dd-wr	t.com	cont	trol par			F Time: 08:34:37	Firmware: DD-WRT v24-sp2 (03/25) 7 up 20:51, load average: 0.06, 0.0 WAN IP: 140.114
基本設定 無言	滚網路 伺服器	杂 鏡安全	連線限制	NAT / QoS	条统管理	機器状態	
基本設定 動	BDNS (DDNS)	MAC位址被制	北陸路由	網路	EoIP 通道		
WAN 設定							幫助 更:
WAN 連接類型							自動設定 - DHCP:
連接類型		靜態 IP	•				Cablelen en Amarg.
WAN IP位址		140.	114 . 309	15			主機名: 活動入您的 TSP 提供的主様名。
子網路遠罩		255 .	255. 210	0			
制道		140.	114.309	254			劉城名稱:
STP		● 啟用 ◎	開開				
							- 配預先設定的靜態位址
網路設定							時間設定:
路由器 IP							議選擇您所在的時區和夏今時(D 期間 本給由器可以使用本地時間。
本地IP位址		192 .	168.0.	1			UTO時間.
子網路遠罩		255 .	255.255.	0			
附道		0.	0.0.	0			
Local DNS		8.	8.8.	8			
網路位址伺服器設定	E (DHCP)						
DHCP 類型		DHCP 伺服器	•				
DHCP 伺服器		● 啟用	開閉				
IP 開始位址		192.168.0.	100				
最大 DHCP 用戶數	t.	100					
用戶端租用時間		1440 分	缝				
WINS		0.	0.0.	0			
Use DNSMasq for	DHCP		石主ル	E.E	み 垂 わ	41	
Use DNSMasq for	DNS		归议	. 正后	以到川	1 Y	
DHCP-Authoritati	ve						
時間設定							
(TRIA days)							

PCI 網路設備

- N= 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。

× D M2	K-W04Ni	J	× 📃																					- 0
¢⇒¢ µnnen																								\$2 =
♥ 応用盤 Google Chrome 儲存器	2 48 16 7	保存管	34																			_	_	2
MZK-WO4NU																			Chines		OK.	4	€,	oct.
状態 管理	(A)	朝史定	進用	袋定		防火	滑		線網	络股定		USB			紀維									
設定精業											1	9636												
本地站何服器	No.	和作	****		,	: XOPA	2 1 / 191	a 80.5	1	_	113	121012		_	HØ	ALP	14/14	a 10.2	1		ня	***	3.16	1 1
P通道	1	1518 ×	UDP .	0	0 0	0	/0	0	0	0	D	- 65535	140	114			/ 255	255	255	255	53	- 53	R	
Firewall Settings	2	£16 ×	TCP .	0)	0 0	.0	/ 0	0	.0	.0	0	- 0	0	.0	.0	.0	10	0	.0	.0	0	- 0	8	, 1
	3	£8 ×	TCP .	٥.)	0 0	0	/0	0	0	0	D	- D	0	0	0	D	/ D	0	D	0	0	- 0		1
	4	£18 ×	TCP .	0)	0 0	0	/0	0	0	0	0	· 0	0	0	0	0	10	0	0	.0	0	- 0	8	
	5	188 -	TOP .	٥.)	0 0	0	/0	0	0	0	D	- D	0	0	D	D	/ D	D	D	D	0	- 0		
	6	£98 ×	TCP .	0)	0 0	0	/0	0	.0	0	0	- 0	0	0	.0	0	10	0	0	.0	0	- 0	8	
	7	198 -	TCP .	0)	0 0	0	/0	0	0	0	D	- D	0	0	0	D	10	0	D	D	0	- 0		
	8	£98 ×	TCP 💌	0)	0 0	0	/0	0	.0	.0	0	· 0	0	0	0	0	10	0	0	.0	0	- 0	8	
	9	超線:	TCP .	0	0 0	0	/0	0	0	0	D	- D	0	0	0	D	/ O	0	D	D	0	- 0		
	10	1948 💌	TCP 💌	0)	0 0	0	/0	0	0	0	0	- 0	0	0	0	0	I O	0	0	0	0	- 0	8	
	11	£8 ×	TCP .	0	0 0	0	/0	0	0	0	D	- 0	0	0	0	0	I O	0	0	.0	0	- 0	8	
	12	1948 •	TCP 💌	0	0 0	0	/0	0	0	0	0	- 0	0	0	0	0	10	0	0	0	0	- 0	8	
	13	× 88	TCP .	0	0 0	0	/0	0	0	0	D	- 0	0	0	0	0	I O	0	0	0	0	- 0		
	14	£88 •	TCP 💌	0	0 0	0	/ 0	0	0	0	0	- 0	0	0	0	0	10	0	0	0	0	- 0	8	
	46	1012	TCR IN	0		0	10	- 0	â	0	0	0	n	n	n	0	10	10		0.0				14+ 1057

PQI 網路設備

● № 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)。

	Local Area Network (LAN) Settings
Configuration	You may enable/disable networking functions and configure their parameters as your wish.
Advanced Settings	IP Address
Internet Setting	Subnet Mask
Operation Mode	LAN 2 Enable ODisable
WAN	LAN2 IP Address
DHCP clients	LAN2 Subnet Mask
VPN passthrough	MAC Address
Routing Wireless Settion	DHCP Type Server B
Basic	Start IP Address
Advanced	End IP Address
Wds	Subnet Mask
Wps Station List	Primary DNS Server
Statistics	Secondary DNS Server
Firewall	Default Gateway
	Lessa Time
V1.0.0	HIC.
Memory in the air	Statically Assigned
	Statically Assigned
	Statically Assigned
	802.1d Spanning Tree Disable 1
	LLTD (Erable :) 主畫面—>Advanced Settings—>
	IGMP Proxy Deable : DNS Proxy 改成Disable(預設是Enable)
	UPNP Trable : 即可以修正open DNS problem
	PPPoE Relay Disable :
	DNS Proxy Disable :
	Apply Cancel

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。

← → C D 140.114.	L U/home.asp	☆ =
高效能無線分享器		
Contractions Router - Million - Million	But	

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 Rout: ×			
← → C f C 101.1.1			요습 😇 🗐
TOTO			The Separteet Natwork Devicer
	NK		The smartest Network Devices
Model no.iPuppy III			
供達設定	備份/遺原		
50.50.00.00 細時20.50			
	將目前設定值匯出至電腦	將目前設定值課出至電腦	
NAT	Choose File No file chosen	使用财存的调音描述原始定	
系版工具	這序設工調 快復原繳預設值	传递厚珊珊胞值 請投此投稿	
刺體升級			
VPN用戶端			
DDNS			
系統記録権			
谱 107篇/译 一 很入密碼/请 請 管理			
重新開展			
-			
1111/confightre	- Networks	Copyright (C) 2012 TOTOLINK Ltd., All Rights Reserved	
the Edit Search Yew Encoding	Language Settings Macro Bun Window I		x
	B 2 C 8 % 3 3 5 3 5 3		
332 FN_SYNF_RATE=150			
333 FN_EN=1 334 UFP_AD_TIME=30			
335 UFP_EN=1 336 UFP_PORT=1780			
337 UPP_SUB_TIMEOUT=1800 338 LOS RM EN=0			
339 LOS_EM_TYPE=0 340 LOS_SYS_IP=0.0.0.0			
141 LOS MAIL IP=0.0.0.0			
343 LOG NODE=5			
345 L2T_IDLET=300			
347 L2T_HP=0.0.0.0 347 L2T_MSR=255.255.255.0			
348 L2T_HTD=1400 349 L2T_PASS=pass			
350 L2T_SVR=0.0.0.0 351 L2T_U3E8=12Tp_user			
352 L2T_SVRDN= 353 L2T_SVRD_SEL=0			
354 L2T_WANIF=0 355 L2T_CLONE_MAC=00:00:00	0:00:00:00		
354 L2T DHCP_MAC_EN=0 357 L2T_GN=0.0.0.0			
355 DH5 EN=0 355 DH5 58V1=140.114.63.1			
360 DNS_SRV2=140.114.64.1 361 DNS_FIX=1			
362 DNS_DEF=0.0.0.0			1
364			
lormal text file		length+6527 lines+364 Ln+358 Col+9 Sel+0	0 UNEX UTF-8 w/e BOM INS
TOTOLINK Wireless Route ×			
			ur 🖕 =
TOTO L	NK		The Smartest Network Devices
Model no iPunny III			
使建設定			
五輪封節	一 備份/還原		
細胞認定			
無線網路設定	將目前設定值匯出至電腦	約日前設定值匯出至電腦	
NAT.	Choose File profile.bin	使用财存的俱计指還原設定	
系版工具	(法序款定置) 快復原即預設值	快速厚暖预购值 捕捉此投稿	
朝禮升級			
VPN用戶端			
DDNS			
系统記錄檔			
備份/環境 思)、安全/法律学校			
重新開展			
		Appropriet 2012 TOTOLOG, All Highlic Reserved	
🛓 profile (1).bin *			Show all downloads ×

Lipsh = 0 = X

10	10	OUN	K. With	CRC30	Moute	~	
~	÷	C	ń.	ß	10.1	1.1	

TOTO L	INK		The Smartest Network Devices
Model no.iPuppy III			
速設定			
施武能	備份/遺原		
時設定			
參網路設定	將目前設定值匯出至電腦	將目前設定值匯出至電腦	
AT	Choose File profile.bin	使用财存的调计描述原設定	
施工具	恢復原職預設值	快復厚竈預設備,請您此按鈕	
體升級			
N用戶端			
ONS			
統記録描			
00/18月8 入密碼/请捕管理			
新聞相			
	2		
		Copyright (C) 2012 TOTOLINK Ltd., All Rights Reserved	
file (1).bin *			Show all downloads
	_		
TOLINK Wireless Route ×			
C & P 10.1.1.1 TOLINK Wireless Route ×			
C A D 101.1.1 C A D 101.1.1 TOLINK Wireless Route × C A D 101.1.1			(1996) 이 (1996) 이 (1996)
TOLINK Wireless Rout: *		The page at 10.1.1.1 says: ×	
TOUINK Wireless Rout: × C A h 10.1.1.1 TOUINK Wireless Rout: × C A h 10.1.1.1		The page at 10.11.11 says: ×	The Smartest Network Devices
TOLINK Wireless Rout: × C fi 101111 TOLINK Wireless Rout: × C fi 1011.1	INK	The page at 10.11.1 says: × 使用程序订编句编述要说注	지 않는 것 이 가 가 가 가 가 가 가 가 가 가 가 가 가 가 가 가 가 가
TOLINK Wretes Rout: × C fill C fill TOLINK Wretes Rout: × C fill IOLINK Wretes Rout: × C fill IOLINK Wretes Rout: × C fill IOLINK Wretes Rout: × Wodel no.iPuppy III >10.5	INK	The page at 10.1.1.1 says: × 使用编符初编句编述重整论定 OK Cancel	(1999) (고영) (1999) (고영) (1999) (고영) (1999) (고영) (1999) (1
TOLINK Weekes Rout: × で 希 10.11.1 で 希 10.11.1 で 希 10.1.1.1 て 希 10.1.1.1 私odel no.JPuppy III 連載主 総19第	INK	The page at 10.11.1 says: 本 使用编件的编句编述意思这定 OK Cencel	지가 아이지 않는 것이 않 않는 것이 않는 않는 것이 않는 것이 않는 것이 않는 것이 않는 않는 않는 것이 않는 않는 것이 않는
IOUINK Wireles Rout: × C 希 ∩ 10.1.1. TOUNK Wireles Rout: × C 希 □ 10.1.1.1 TOTOLIK Model no.1Puppy III 連股定 発起語	INK	The page at 10.11.11 says: 本 使用程序印度计编集集团定 OK Cancel	지 않는 것이 아파 가 있다. 이 아파 가 가 가 가 가 가 가 가 가 가 가 가 가 가 가 가 가 가
IOUINK Wireles Rout: × C 希 ○ 10.1.1.1 TOUNK Wireles Rout: × C 希 ○ 10.1.1.1 Rodel no.iPuppy III 漆設定 集設定 集設定	■ 備份/違原 ※目前前次体展出平常報	The page at 10.1.1.1 says: × 使用编件的编计编编集版定 OK Cancel 的日前和字信语中中文字曲	지 않는 것이 아이지 않는 것이 않 것이 않는 것이 않는 않는 것이 않는 것이 않는 것이 않는 것이 않는 것이 않이 않는 것이 않이 않는 않는 것이 않는 것이 않는 것이 않는 것이 않이 않는 않는 것이 않는
IOUNK Weekes Rout: × C 希 ○ 10.1.1.1 TOUNK Weekes Rout: × C 希 ○ 10.1.1.1 TOTOL Viekes Rout: × C 希 ○ 10.1.1.1 Rodel no.1Puppy III 漆銀定 蜂親院 蜂親院 整理定	INK 学 催份/還原 所目前設定値医出至電幅 Choose File profile bin	The page at 10.1.1.1 says: × 使用器件的操作维重整路定 OK Cancel 所目前設定值碼出空電船 在田时在的供給制度定即完	The Smartest Network Devices
IOUNK Weekes Rout: × C 希 ∩ 10.1.1.1 TOUNK Weekes Rout: × C 希 ∩ 10.1.3.1 TOUNK Weekes Rout: × C 希 ∩ 10.1.3.1 Rodel no.1Puppy III 漆設定 蜂網院設定 KT	一 催份/還原 所目前設定後国出王電船 Choose File profie.bin 運算感正面 生活ののです。	The page at 10.1.1.1 says: × 使用程序的模仿维重要说定 OK Cancel 新日前設定值逐出正型電磁 使用财存的模计指述序识定	지 않는 지 않는 것이 있다. 지 않는 것이 있는 것이 있다. The Smartest Network Devices
10UNK Weekes Rout: × C 希 ∩ 10.1.1 TOUNK Weekes Rout: × C 希 ∩ 10.1.3 TOUNK Weekes Rout: × C 希 ∩ 10.1.3 TOUNK Weekes Rout: × C 希 ∩ 10.1.3 TOUNK Weekes Rout: × C 希 ∩ 10.1.1 TOUNK Weekes Rout: × C 希 ∩ 10.1.1 C A A A A A A A A A A A A A A A A A A A	一 借日前股立後医出王電船 Choose File profile bin 道原設立面 依須原廠頂設施	The page at 10.1.1.1 says: × 使用操作的编句编编集要放定 0K Cancel 外目前放走值逐出正電腦 使用解存的调台情源原設定 依用解存的调台情源原設定 估值厚聪频数值,請投此投班	(1990) - の (1990) - の のかい のかい のかい のかい のかい のかい のかい の のかい の のかい の のかい の のかい の のかい の のかい の のかい の のかい の のかい の のかい の のかい の のかい の のかい の の かい の の かい の の かい の の かい の の かい の の つ の の の の い の
TOLINK Weekes Rout: × で 希 101.1.1 TOLINK Weekes Rout: × で 新 101.1.1 TOLINK Weekes Rout: × 101.1 * * * * * * * * * * * * *		The page at 10.11.1 says: 本 使用操作的编句编述编纂题注 	
TOLINK Weekes Rout: × で 希 101.1.1 TOLINK Weekes Rout: × で 新 101.1.1 TOLINK Weekes Rout: × で 新 101.1.1 TOLINK Weekes Rout: × 101.1 * * * * * * * * * * * * *	INK 「 借母/違原 所目前設立値国出王電報 Choose File profile bin 道原設正面 依復原順預設値	The page at 10.11.1 says: 本 使用程序的描述本基型缺乏 OK Cencel 所目前設定值碼出至電腦 使用程序的描述情愿限型 快速序唱频取值,請按此按述	
TOLINK Wretes Root: × C 香 P 10.1.1.1 TOLINK Wretes Root: × C 香 P 10.1.1.1 C 香 P 10.1.1.1 C 香 P 10.1.1.1 Undel no.iPuppy III 注意定 集初記 推設定 集初記 推設定 加加回知 第一 和 和 和 和 和 和 和 和 和 和 和 和 和	一 着 御 御 御 御 御 御 御 御 御 御 御 御 御	The page at 10.11.1 says: 本 使用程序订编印第基里段注 	The Smartest Network Devices
TOLINK Wretes Root: × C 香 10.1.1.1 TOLINK Wretes Root: × C 香 10.1.1.1 UNK Wretes Root: × C 香 10.1.1.1 Wodel no.iPuppy III 漆設定 築設整 整設定 塗鋼路設定 和 和 和 和 和 5 次 10.1.1.1 () () () () () () () () () ()	INK 「 備份/遺尿 所目前設定値度出至電価 Choose File profile bin 違序設定面 依復用御賀般値	The page at 10.11.1 says: × 使用器符切编件集重整定 0K Cencel 第日期設定值區出至電腦 使用儲存的機合指還原設定 依便厚頭預設值,請按此按照	The Smartest Network Devices
TOLINK Wretes Root: × C 香 TOLINK Wretes Root: × C 香 10.1.1 TOLINK Wretes Root: × C 香 10.1.1.1 TOLINK Wretes Root: × C 香 10.1.1.1 TOLINK Wretes Root: × C 香 10.1.1.1 TOLINK Wretes Root: × Volton K Wretes Root: × Wodel no.JPuppy III 凍設定 臭類酸設定 外国防設定 AT 換工具 電子/S 小田戶論 DNS 洗記述信 分/濃原 入密画/通貨管環	一 常 御 御 御 御 御 御 御 御 御 御 御 御 御	The page at 10.11.1 says: × 使用操存的描述 0K 如日前設室值區出至電腦 使用儲存的描述情愿限型 依使厚瘤预設值,請按此按照	The Smartest Network Devices
TOLINK Wretes Root: × C 香 TOLINK Wretes Root: × C 香 10.1.1 TOLINK Wretes Root: × C 香 10.1.1.1 TOLINK Wretes Root: × C 香 10.1.1.1 TOLINK Wretes Root: × C 香 10.1.1.1 TOLINK Wretes Root: × Wodel no. Puppy III 速設定 集設記 地設定 参加路設定 地設定	一 働 御 御 御 御 御 御 御 御 御 御 御 御 御	The page at 10.11.1 says: × 使用操作的操作维重要定 0K Cancel 新日前設定值區出至電腦 使用操作的操行措置原設定 依使厚端预設值,請按此按照	The Smartest Network Devices
TOLINK Weekes Rout: × で、作、10.1.1. TOLINK Weekes Rout: × で、作、10.1.1. TOLINK Weekes Rout: × で、作、10.1.1.1 TOLINK Weekes Rout: × たいまた、10.1.1.1 TOLINK Weekes Rout: × たいまた、10.1.1.1.1 TOLINK Weekes Rout: × たいまた、10.1.1.1.	一 備份/遺原 所日前設定値區出至電船 Choose File profile bin 道序反正面 依視界廠預設値	The page at 10.11.1 says: X 使用窗符印编印编集集算算文 0K Cancel 新日前設定值區出空電器 使用窗存的编台错圆束股宝 依他原喃频設值,請按此投程	The Smartest Network Devices

ZyXEL 網路設備

• Imm 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)。

ZYAEL		
	> 管理 > 遠報管理 > DNS	
S 80	WWW Telnet FT	TP. DNS
334W	DNS	
211 19	服務4	53
移忌 跳由	LAN	🕙 None 🛛 💩 👘 💮 Single IP 💿 IP Range 🔘 Netmask
8222	WAN	🖲 None 🗇 🚖 👘 Single IP 🕤 IP Range 🖱 Netmask
這些管理		
触捕印用		
HACE .		all the block
	松主日	まあーン海田>波波海部田->
	DNS選	單中,將WAN port53圖開
		to bulk of 48 mercificate recently to bat

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:
                                 ΙN
                                         А
;google.com.
;; ANSWER SECTION:
google.com.
                        116
                                 IΝ
                                         А
                                                 173.194.72.101
```

2024/02/01 16:25	1	7/17		Open DNS resolver 的問題			
	116	TN	٨	172 104 72 100			
google.com.	110		A	1/3.194./2.100			
google.com.	116	IN	А	173.194.72.113			
google.com.	116	IN	А	173.194.72.102			
google.com.	116	IN	А	173.194.72.138			
google.com.	116	IN	А	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	А	216.239.32.10			
ns2.google.com.	156702	IN	Α	216.239.34.10			
ns3.google.com.	156703	IN	Α	216.239.36.10			
ns4.google.com.	156702	IN	А	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
- ■ 用放性 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