TANet 臺南區域網路中心管理會

會　議　紀　錄

時間：114 年 6 月 10 日（星期二）11:00 至 12:10
地點：國立成功大學計算機與網路中心 4 樓會議室
出席：TANet 臺南區網各連線單位代表
主席：國立成功大學計算機與網路中心　李南逸代理主任
紀錄：朱敏清技士

壹、主席致詞（略）

貳、臺南區網中心報告事項(內容詳附件投影片)

一、IOT 設備暴露在外掃測清單宣導事項。
二、臺灣學術網路管理規範修正及宣導。
三、骨幹網路介接及互連作業要點修正及宣導。
四、新版 TANet 網路品質量測網站說明。
五、TANet CDN 介紹。
六、TANet CDN DNS 介紹。
七、新版 TANet NOC 網頁介紹。
八、TANet 400G 專案說明。
九、成大計網中心大樓高壓變電設備汰換說明。
其他、DNS 運作原理及相關宣導。

參、議案：

案由：下列連線單位申請提升頻寬，業經審查通過，敬請同意備查。
(1)113 年：曾文農工(1G)、德光中學(500M)、慈幼工商(300M)、瀛海中學(300M)、聖功女中(300M)、成大南工(300M)、新豐高中(300M)、光華高中(300M)。
(2)114 年：長榮女中(300M)、臺南大學(2G)、六信高中(300M)、新營高中(300M)。
說明：連線單位應遵守「臺灣學術網路骨幹網路介接及互連作業要點」，須具備內部網路使用規範、網路之整體使用流量統計、每日 IP Address 使用流量排序分析及資安相關處理機制等。
決議：同意。

肆、臨時動議：本次無臨時動議。

伍、教育訓練

題目：常見資安威脅與防護
講師：國立中山大學圖書與資訊處軟體工程組 王聖全組長
時間：13:00～16:00

國立成功大學
National Cheng Kung University

114年臺南區網管理會報告事項

國立成功大學
計算機與網路中心
朱敏清技士

TANet 臺南區域網路中心 Taiwan Academic Network

一、IoT設備暴露在外掃測清單

- 掃測單位：TANet ASOC
- 工具：SHODAN(https://www.shodan.io/)
- IoT設備：網路印表機、網路分享器、網路監視器。
- 頻率：每月
- 建議措施
  - 避免讓外部可存取
  - 非必要之服務或程式建議移除或關閉

一、IoT設備暴露在外掃測清單(範例)

建議貴校貴單位盡速檢視防火牆Policy，限制僅為校內網段存取或使用VPN連線進行存取，避免直接對外曝險等致遭受攻擊或被當作跳
另建議貴校貴單位檢視IOT設備避免使用預設帳密，如已有收到開單預設帳密，請盡速修改，謝謝

	IP	區網	學校	Port	Timestamp	Data	Hostnames	Organizatio
88	140. 74	成大區網中心	國立 學	443	2025-04-27T22:24:01.93996	HTTP/1.1 200 OK_x000D_ Date: Sun, 27 Apr 20		Ministry of E
107	140. 35	成大區網中心	國立 學	443	2025-04-27T07:13:53.66732	HTTP/1.1 200 OK_x000D_ Server: nginx_x000I		Ministry of E
146	140. 1	成大區網中心	國立 學	443	2025-04-25T05:18:57.23749	HTTP/1.1 200 OK_x000D_ Server: nginx_x000I		Ministry of E
156	140. 0	成大區網中心	國立 學	21	2025-04-24T19:39:12.26462	220 SHARP	pc-61-010.hosp.ncku.edu.tw	Ministry of E
188	140. 150	成大區網中心	國立 學	80	2025-04-22T13:41:46.39796	HTTP/1.1 200 OK_x000D_ Content-Length: 517		Ministry of E
213	140. 27	成大區網中心	國立 學	443	2025-04-21T00:31:08.17441	HTTP/1.1 200 OK_x000D_ Content-Length: 516		Ministry of E
235	203.	成大區網中心	國立 業學	80	2025-04-19T06:55:06.26780	HTTP/1.1 200 OK_x000D_ CONTENT-TYPE: t		Ministry of E
254	120. 11	成大區網中心	私立 技大學	443	2025-04-18T16:56:33.00883	HTTP/1.1 20	120-114-113-11.ksu.edu.tw,NPIB9	Ministry of E
261	140. 0	成大區網中心	國立 學	443	2025-04-18T04:18:37.63235	HTTP/1.1 200 OK_x000D_ Server: HP_Compac		Ministry of E
286	203. 41	成大區網中心	財團 大學	443	2025-04-16T01:16:24.65203	HTTP/1.1 200 OK_x000D_ CACHE-CONTROL		Ministry of E
353	140. 20	成大區網中心	國立 學	443	2025-04-09T06:57:19.98926	HTTP/1.1 20	pc-58-220.hosp.ncku.edu.tw	Ministry of E
360	140. 104	成大區網中心	國立 學	443	2025-04-09T00:26:19.06814	HTTP/1.1 200 OK_x000D_ Date: Wed, 09 Apr 2		Ministry of E

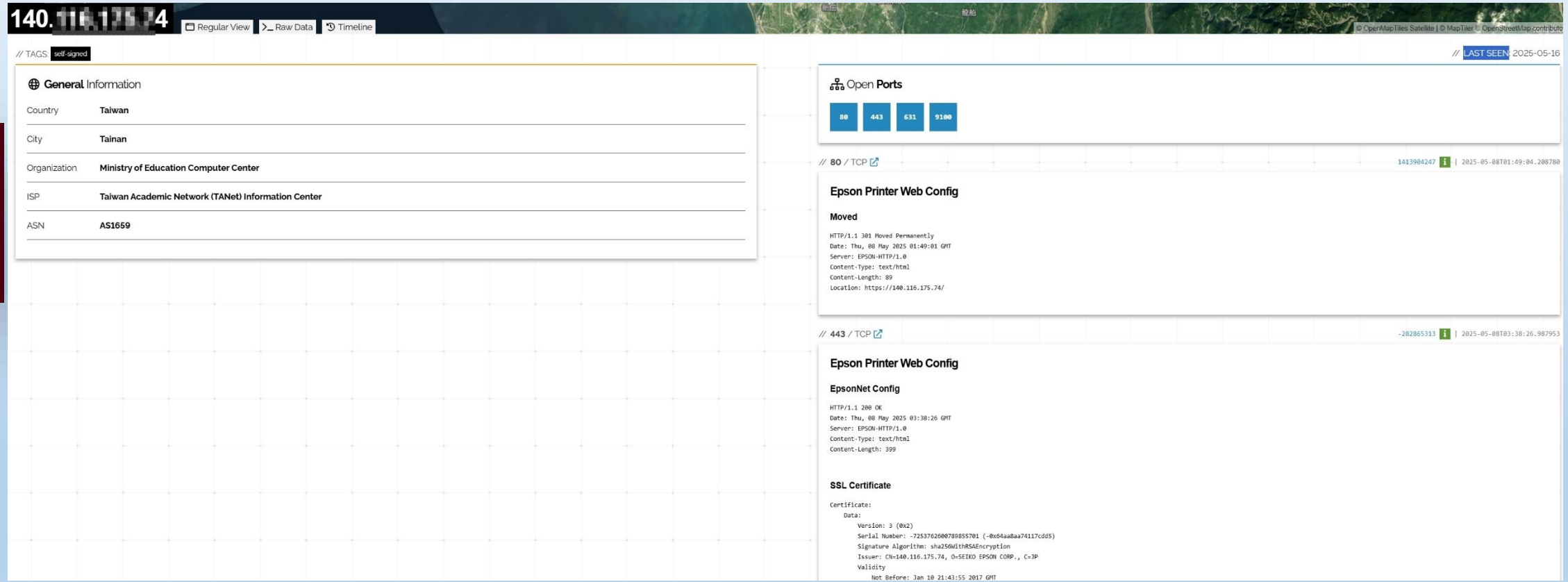
網路印表機 | 網路分享器 | 網路監視器

一、IoT設備暴露在外掃測清單(範例)

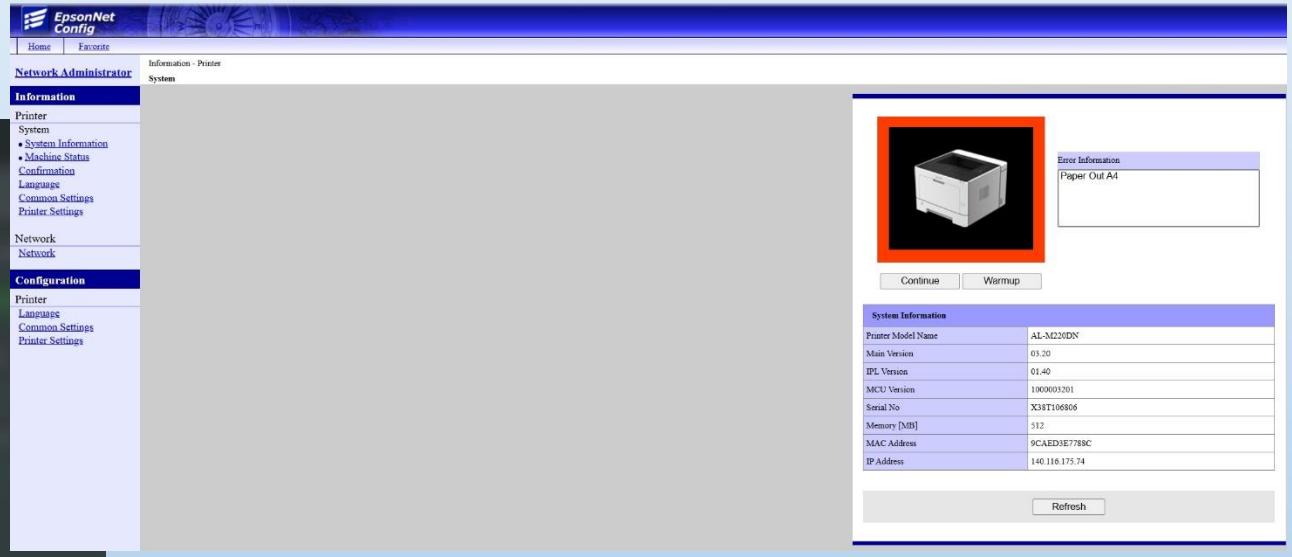
板進行攻擊，也可避免每月持續被Shodan掃描列入曝險清單

ISP	Country	ntry ISO C	City	OS	ASN	Transport	Product	Version	Web Server	Website Title
Taiwan Acad	Taiwan	TW	Tainan		AS1659	tcp	Epson Printer Web Config	Epson Printer Web Config		EPSON-HTTP/1.0
Taiwan Acad	Taiwan	TW	Tainan		AS1659	tcp	HP Printer Embedded Web Server	HP Printer Embedded Web Server		nginx
Taiwan Acad	Taiwan	TW	Tainan		AS1659	tcp	HP Printer Embedded Web Server	HP Printer Embedded Web Server		nginx
Taiwan Acad	Taiwan	TW	Tainan		AS1659	tcp	SHARP MX-M356N printer ftpd	SHARP MX-M356N	01.05.00.0s.13	
Taiwan Acad	Taiwan	TW	Tainan		AS1659	tcp	Kyocera Printer Panel	Kyocera Printer Pane	2Y3_S000.003.302	KM-MFP-http/V0.0.1
Taiwan Acad	Taiwan	TW	Tainan		AS1659	tcp	Kyocera Printer Panel	Kyocera Printer Pane	C0T_S000.004.651	KM-MFP-http/V0.0.1
Taiwan Acad	Taiwan	TW	Taichung	Linux	AS1659	tcp	Epson Printer Web Config	Epson Printer Web Config		EPSON_Linux UPnP/
Taiwan Acad	Taiwan	TW	Tainan		AS1659	tcp	HP Printer Embedded Web Server	HP Printer Embedded Web Server		HP_Compact_Server
Taiwan Acad	Taiwan	TW	Tainan		AS1659	tcp	HP Printer Embedded Web Server	HP Printer Embedded Web Server		HP_Compact_Server
Taiwan Acad	Taiwan	TW	Tainan	Linux	AS1659	tcp	Epson Printer Web Config	Epson Printer Web Config		EPSON_Linux UPnP/
Taiwan Acad	Taiwan	TW	Tainan		AS1659	tcp	HP Printer Embedded Web Server	HP Printer Embedded Web Server		nginx
Taiwan Acad	Taiwan	TW	Tainan		AS1659	tcp	Epson Printer Web Config	Epson Printer Web Config		EPSON-HTTP/1.0

一、IoT設備暴露在外掃測清單(SHODAN)



一、IoT設備暴露在外掃測清單(管理頁面)



二、臺灣學術網路管理規範

- 修正日期：112年12月20日。
- 修正第七條第六款：
  - 訂定單位所提供各式網路應用服務之相關管理辦法，且對外提供服務之資通系統應採加密機制，並使用公開、國際機構驗證且未遭破解之演算法。另對內提供服務之資通系統如未使用加密傳輸機制，應採實體隔離措施。

三、骨幹網路介接及互連作業要點更新

- 修正日期：114年4月15日。
- 新增七之一條：
  - 連線單位如有停辦、停止營運、改隸或其他不適合繼續介接者，本部、區域網路中心、縣市教育網路中心得終止其介接。連線單位為直轄市、縣（市）政府所屬機關學校者，其終止介接作業程序由各縣市教育網路中心自行訂定，並通知本部更新連線單位資訊。
  - 其他連線單位之終止介接，其介接之區域網路中心或縣市教育網路中心應於預定終止日三十日前，以書面通知該連線單位終止介接，並通知本部收回配發網段及網域名稱。但該連線單位因已停辦或停止營運而無正式聯繫管道者，不在此限。

三、骨幹網路介接及互連作業要點宣導

- 第七條：
  - 連線單位應確保所提之介接計畫書所列事項正常運作，區域網路中心或縣市教育網路中心每年應至少一次，以書面或實地訪查方式，檢核與其介接頻寬達一Gbps以上連線單位之執行情形。
  - 連線單位如未依計畫書確實執行，經通知限期改善，屆期仍未改善者，區域網路中心或縣市教育網路中心得限制或暫停連線單位必要範圍之網路連線服務。

三、骨幹網路介接及互連作業要點宣導

- 第六條：介接計畫書應包括下列項目：
  1. 所屬網路及應用系統相關伺服主機之現況與架構說明。
  2. 內部網路使用規範：應參照臺灣學術網路管理規範之相關規定，納入於各該連線單位之網路使用相關規範，並經行政程序核定及公告於學校或機關（構）之對外網站首頁。
  3. 所屬網路之整體使用流量統計：應建置與骨幹網路介接之網路使用流量情形統計資訊網頁（包括以日、週、月為單位之即時及歷史流量）。
  4. 所屬IP之每日使用流量排序分析：就服務範圍使用之IP位址，統計分析其對骨幹網路之個別IP使用流量排名最高前三十名並紀錄，紀錄內容包括流入、流出及總量等之使用流量資訊。紀錄至少應保留一個月。

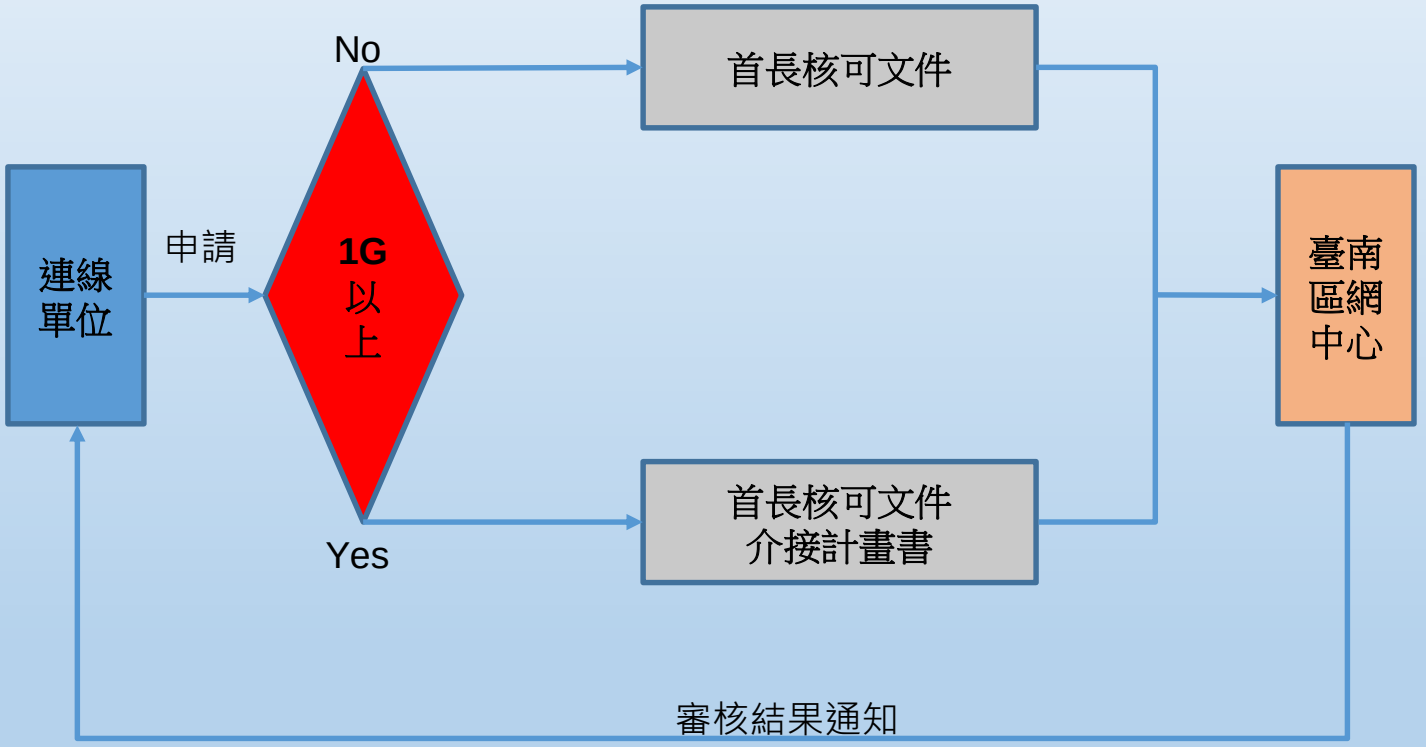
三、骨幹網路介接及互連作業要點宣導

- 第六條：介接計畫書應包括下列項目：
  5. 建立連線單位處理網路管理、資通安全之聯繫機制：至少建立abuse及security等公務電子郵件帳號（abuse主要作為spam或攻擊等不當使用之反應帳號；security用為資通安全通報使用），並指派專人管理該帳號及負責相關事宜之訊息處理。
  6. 建立IP位址管理機制：包括IP位址分配之主機用途及管理人之相關資料，登記資料如涉及個人資料，應依個人資料保護法及其相關法規規定辦理。
  7. 建立對廣告信或網路攻擊等資安事件之處理機制：包括來自單位內部或外部之異常事件，並提出具體之管理規定及改善措施。
  8. 高級中等以下學校應建立不適合存取網站內容（如色情、賭博、暴力等）之過濾防護機制：說明所建立之過濾防護機制相關軟硬體設施架構

三、骨幹網路介接及互連作業要點(開源軟體)

- 流量統計開源軟體介紹：
  - Cacti： https://www.cacti.net/
  - LibreNMS： https://www.librenms.org/
  - Zabbix： https://www.zabbix.com/
  - The dude： https://mikrotik.com/thedude

三、頻寬提升申請流程



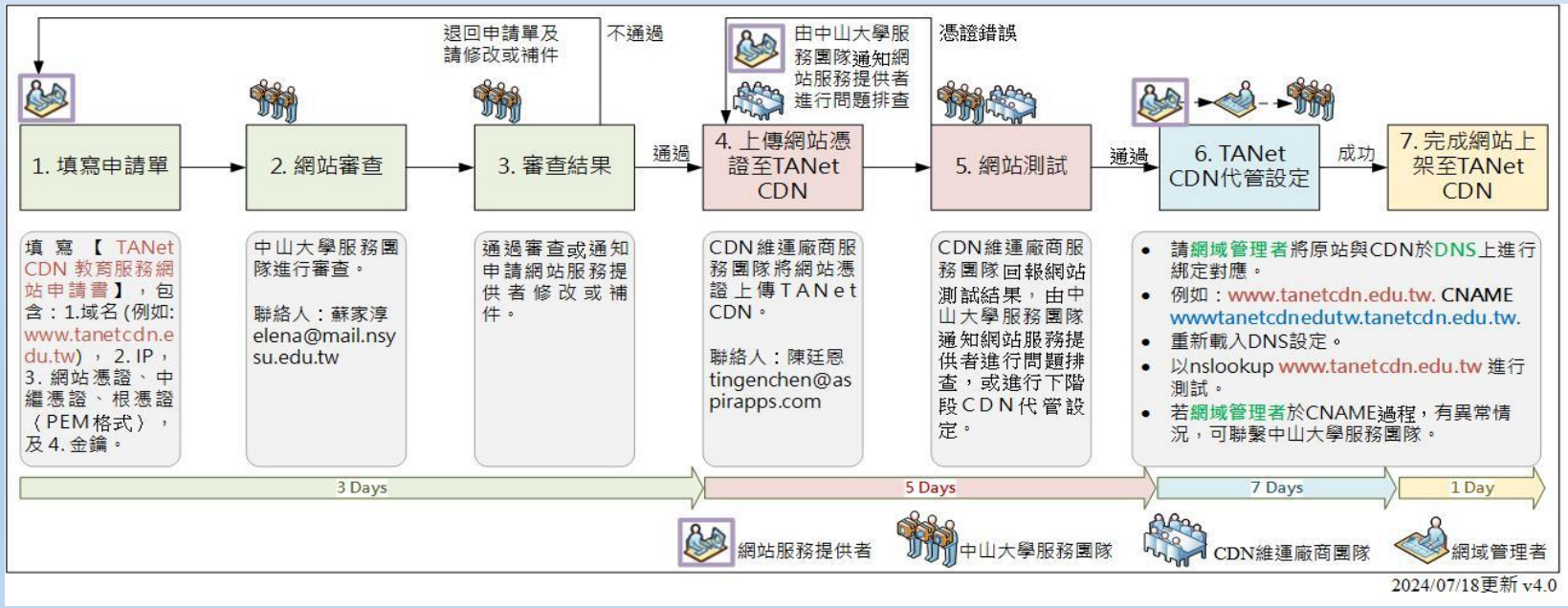
四、TANet 網路品質量測網站

- 新版： https://sp.tanet.edu.tw/

- 舊版(預計6月下線)： https://nts.tanet.edu.tw/

五、TANet CDN

- 官網資訊： https://www.tanetcdn.edu.tw/
- 申請流程



五、TANet CDN

- 使用者需知：
  - 主機IP位址或NAT IP位址：需為臺灣學術網路IP位址。
  - 主機DNS設定： DNS Resolver需支援ECS(EDNS Clinet Subnet)

```
C:\Users\Chu>dig o-o.myaddr.google.com TXT @8.8.8.8 Google DNS

; <<>> DiG 9.16.32 <<>> o-o.myaddr.google.com TXT @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5689
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;o-o.myaddr.google.com.         IN      TXT

;; ANSWER SECTION:
o-o.myaddr.google.com.  60      IN      TXT     "172.217.42.26"
o-o.myaddr.google.com.  60      IN      TXT     "edns0-client-subnet 140.116.2.0/24"
                                                ECS

;; Query time: 11 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Mon Jun 09 10:36:14 ;; MSG SIZE  rcvd: 123
```

```
C:\Users\Chu>dig o-o.myaddr.google.com TXT @168.95.1.1 HiNet DNS

; <<>> DiG 9.16.32 <<>> o-o.myaddr.google.com TXT @168.95.1.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34716
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 3fa69f4d62d4132c0100000068464901a3cef1af64af5311 (good)
;; QUESTION SECTION:
;o-o.myaddr.google.com.         IN      TXT

;; ANSWER SECTION:
o-o.myaddr.google.com.  60      IN      TXT     "2001:b000:1e0:8002:0:2:0:17"

;; Query time: 20 msec
;; SERVER: 168.95.1.1#53(168.95.1.1)
;; WHEN: Mon Jun 09 10:37:53 ;; MSG SIZE  rcvd: 118
```

六、TANet CDN DNS(測試中)

- 教育部臺南區網CDN DNS
  - IPv4：163.28.114.97、163.28.114.97
  - IPv6：2001:288:7101:1::9、2001:288:7101:1::A
- 支援ECS
- RPZ：TWNIC RPZ、MOE RPZ、 TANWP RPZ

七、新版TANet NOC網頁

- 啟用日期：114年6月2日
- 網址：https://noc.tanet.edu.tw

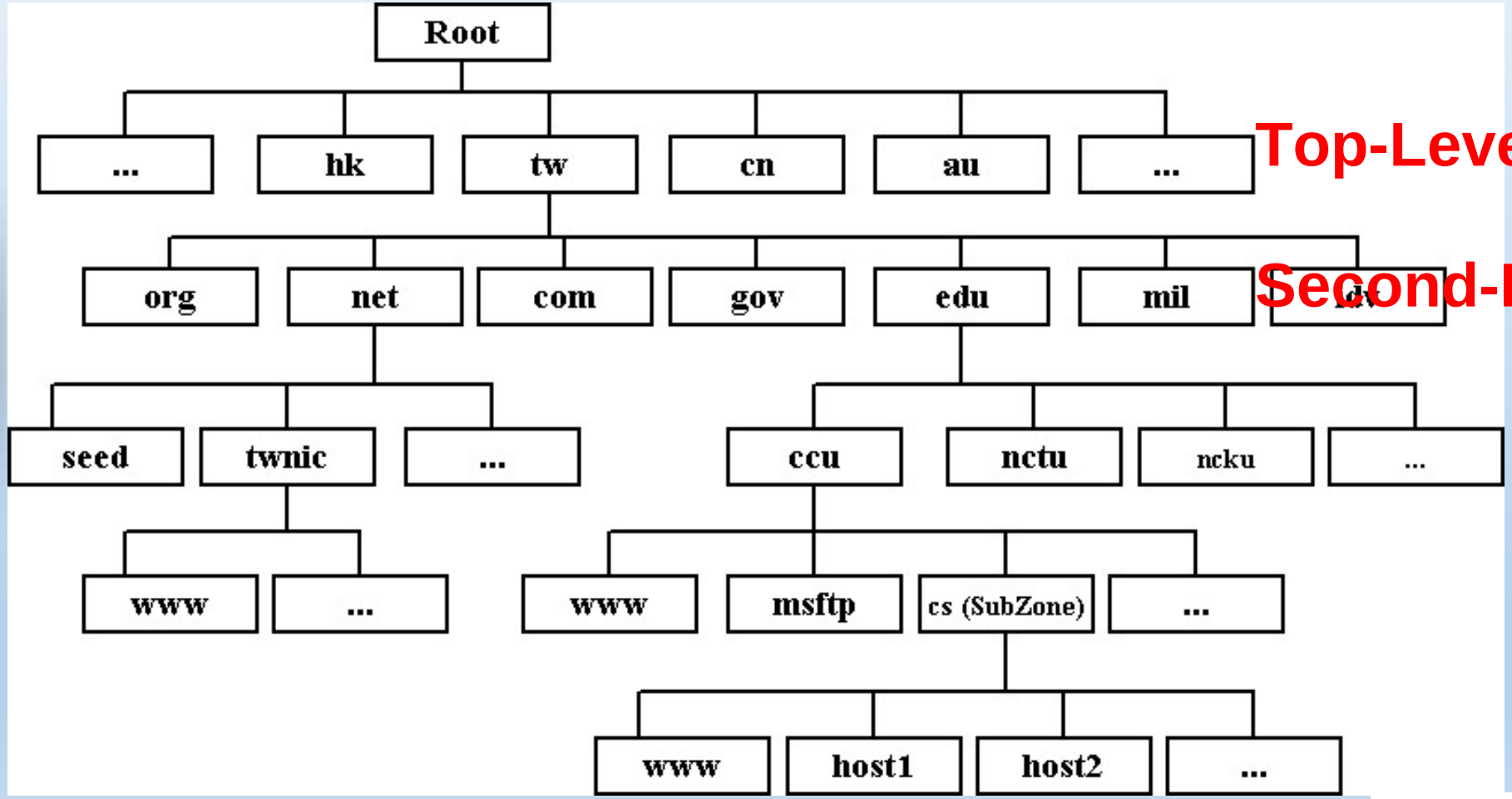
八、TANet 400G專案說明

- 臺灣學術網路 100G 骨幹網路汰換案已於113 年 10 月由遠傳電信得標，同年12月開始進行臺南區網機房場勘作業。
- 114年4月21日起進場施作。
- 目的：從原 100G主骨幹網路切換至 400G，以提升網路傳輸能力與效能。
- 臺灣學術網路架構：https://traffic.tanet.edu.tw

九、成大計網中心大樓高壓變電設備汰換說明

- 起因：現有變站設備建置已逾20年。
- 汰換流程及電力狀況：
  - 高壓變電站設備設置及切換：
    - 電力中斷一天，臺南區網網路服務暫停服務。
  - 變電站其他設備汰換之一：
    - 電力中斷三天，由發電機供電。
  - 變電站其他設備汰換之二：
    - 電力中斷三天，由發電機供電。

科普-DNS架構

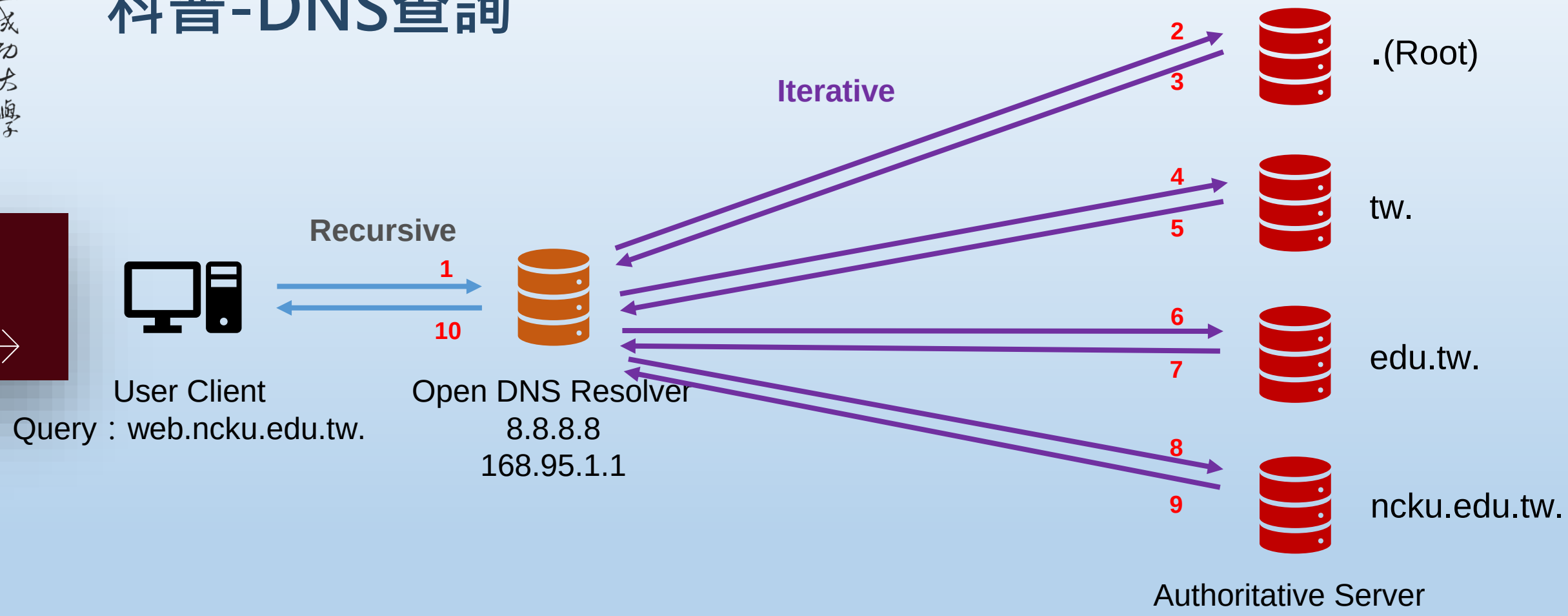


Top-Level Domain

Second-Level Domain

圖片來源：TWNIC (https://dns-learning.twnic.tw/dns/02ArchDNS.html)

科普-DNS查詢


Iterative
Recursive
1
10
2
3
4
5
6
7
8
9
.(Root)
tw.
edu.tw.
ncku.edu.tw.
User Client
Query：web.ncku.edu.tw.
Open DNS Resolver
8.8.8.8
168.95.1.1
Authoritative Server

科普- DNS查詢範例

```
C:\Users\Chu>dig +trace web.ncku.edu.tw @168.95.1.1

; <<>> DiG 9.16.32 <<>> +trace web.ncku.edu.tw @168.95.1.1
;; global options: +cmd
.                       50303   IN      NS      c.root-servers.net.
.                       50303   IN      NS      d.root-servers.net.
.                       50303   IN      NS      e.root-servers.net.
.                       50303   IN      NS      f.root-servers.net.
.                       50303   IN      NS      g.root-servers.net.
.                       50303   IN      NS      h.root-servers.net.
.                       50303   IN      NS      i.root-servers.net.
.                       50303   IN      NS      j.root-servers.net.
.                       50303   IN      NS      k.root-servers.net.
.                       50303   IN      NS      l.root-servers.net.
.                       50303   IN      NS      m.root-servers.net.
.                       50303   IN      NS      a.root-servers.net.
.                       50303   IN      NS      b.root-servers.net.
.                       50303   IN      RRSIG   NS 8 0 518400 202506
D8fSxsdcuGQF0lC/A1ebRfUd2miM8d3Chy+9 6MuFsXjFH4DK+mwX69T05Iqd6Btlvkv
I63Uo+f3THNSbfBn+eqOnZTfMw3VzE Kck1towWYtqywGD7br89KPjs+YYdKw3u7/9Rj
/8j/3yqpFSfBmtzhLgeQyxJy YlgF2wK+XVmXiVrhJ0SjL9OUwHraiksNUvtZj30HA3
;; Received 1097 bytes from 168.95.1.1#53(168.95.1.1) in 3 ms

tw.                     172800  IN      NS      a.dns.tw.
tw.                     172800  IN      NS      b.dns.tw.
tw.                     172800  IN      NS      c.dns.tw.
tw.                     172800  IN      NS      d.dns.tw.
tw.                     172800  IN      NS      e.dns.tw.
tw.                     172800  IN      NS      f.dns.tw.
tw.                     172800  IN      NS      g.dns.tw.
tw.                     172800  IN      NS      h.dns.tw.
tw.                     172800  IN      NS      anytld.apnic.net.
tw.                     86400   IN      DS      51277 8 2 462DA9AF5
BCD
tw.                     86400   IN      RRSIG   DS 8 1 86400 2025062
```

```
edu.tw.                 3600    IN      NS      edudns-a4.edu.tw.
edu.tw.                 3600    IN      NS      edudns-a3.edu.tw.
edu.tw.                 3600    IN      NS      edudns-c1.edu.tw.
edu.tw.                 3600    IN      NS      d.twnic.net.tw.
edu.tw.                 3600    IN      NS      edudns-a2.edu.tw.
edu.tw.                 3600    IN      NS      b.twnic.net.tw.
edu.tw.                 3600    IN      NS      a.twnic.net.tw.
edu.tw.                 3600    IN      NS      c.twnic.net.tw.
edu.tw.                 3600    IN      NS      edudns-c2.edu.tw.
edu.tw.                 300     IN      DS      19894 8 2 E0C877567408
F06
edu.tw.                 300     IN      DS      24025 8 2 7DFE1D2793B0
847
edu.tw.                 300     IN      DS      41570 8 2 DC750DA0EADF
3FF
edu.tw.                 300     IN      RRSIG   DS 8 2 300 20250709050
gpaHHpPC/ojnuLwet9zA1ExD8H13dxVlqpt z93vbhqohWcv9tyE+qdvFvwt2+R+4OCbpi
PyxAVV+RboansoSYRdnEtyhCA1PLG 1OE=
;; Received 996 bytes from 202.12.31.53#53(anytld.apnic.net) in 163 ms

ncku.edu.tw.            300     IN      NS      name.ncku.edu.tw.
ncku.edu.tw.            300     IN      NS      apple.ncku.edu.tw
NMBUIE5TVE44T6SNKGDH8NBE2OFPDTQC.edu.tw. 300 IN NSEC3 1 0 10 D0D7C1F3A
 NS
NMBUIE5TVE44T6SNKGDH8NBE2OFPDTQC.edu.tw. 300 IN RRSIG NSEC3 8 3 300 20
uBCpXi8otCsL1qqV6y2V49pVsgAt6LHRdGH0+9PrvtXVpg1N QdP4PCuqAot1jrQaxxLVD
l1UwI8zNnx+NjJvKa2wlocw7l3cj3i0vdVuowMZrFf iqQ=
;; Received 458 bytes from 140.111.34.133#53(edudns-a2.edu.tw) in 8 ms

web.ncku.edu.tw.        86400   IN      A       140.116.241.66
ncku.edu.tw.            86400   IN      NS      apple.ncku.edu.tw.
ncku.edu.tw.            86400   IN      NS      name.ncku.edu.tw.
;; Received 215 bytes from 163.28.112.1#53(name.ncku.edu.tw) in 2 ms
```

科普-DNS查詢-ECS範例

```
> pads.moe.edu.tw
伺服器:  dns.hinet.net
Address:  168.95.1.1

未經授權的回答:
名稱:    padsmoeedutw.tanetcdn.edu.tw
Address:  163.28.11.56
Aliases:  pads.moe.edu.tw
```

HiNet DNS
不支援ECS

原站位址

```
> pads.moe.edu.tw
伺服器:  [163.28.114.97]
Address:  163.28.114.97

未經授權的回答:
名稱:    pads.moe.edu.tw
Addresses:  2001:288:7101:1::a
          2001:288:7101:1::9
          163.28.114.97
          163.28.114.98
```

區網DNS
支援ECS

CDN位址

```
> pads.moe.edu.tw
伺服器:  dns.google
Address:  8.8.8.8

未經授權的回答:
名稱:    padsmoeedutw.tanetcdn.edu.tw
Address:  163.28.11.56
Aliases:  pads.moe.edu.tw
```

Google DNS
支援ECS

還是原站位址？

目前TANet CDN現階段僅允許TANet IP位址可存取，其他使用者IP位址則仍訪問原站。

科普-Open DNS Resolver-資訊安全

主旨	A-ISAC 210 [redacted] 用戶資訊設備疑似存在DNS Open Resolver弱點
說明	國家資通安全研究院接獲外部情資，發現 A-ISAC 210.[redacted] 用戶資訊設備疑似存在DNS Open Resolver弱點，可供外部人士查詢任意網址，由於DNS遞迴查詢功能可被有心人士用做DDoS用途，此外，曝露網域內使用之DNS查詢伺服器，亦會增加被DNS快取污染攻擊的機率，為降低網路攻擊風險，建議評估服務開放外部存取之必要性，適時調整為內部網路存取或存取控管。
手法研判	
應變措施	1. 檢視系統上有無不明帳號。2. 請使用外部網路，於終端機中輸入nslookup指令確認附件IP的DNS服務是否開啟DNS Open Resolver。 範例: 欲確認168.x.x.x是否開啟DNS Open Resolver，可用指令 nslookup www.google.com.tw 168.x.x.x，如果查詢有回答網路位址，表示有開啟。3. 系統上DNS服務若非必要，建議關閉，或是調整服務設定，限制遞迴查詢功能僅提供本地網域使用者。

原因：開啟遞迴(Recursive)查詢且未限制網段
影響：易遭受放大攻擊
建議：關閉遞迴查詢或限制網段

以BIND9為例：修改name.conf

```
Options {
        …
        recursion no;     //關閉遞迴查詢
        …
};

Options {
        …
        allow-recursion { //允許部分網段可遞迴查詢
                IP網段;
                192.168.1.0/24;
        };
…
};
```

THANKS

TANet 臺南區域網路中心
Taiwan Academic Network