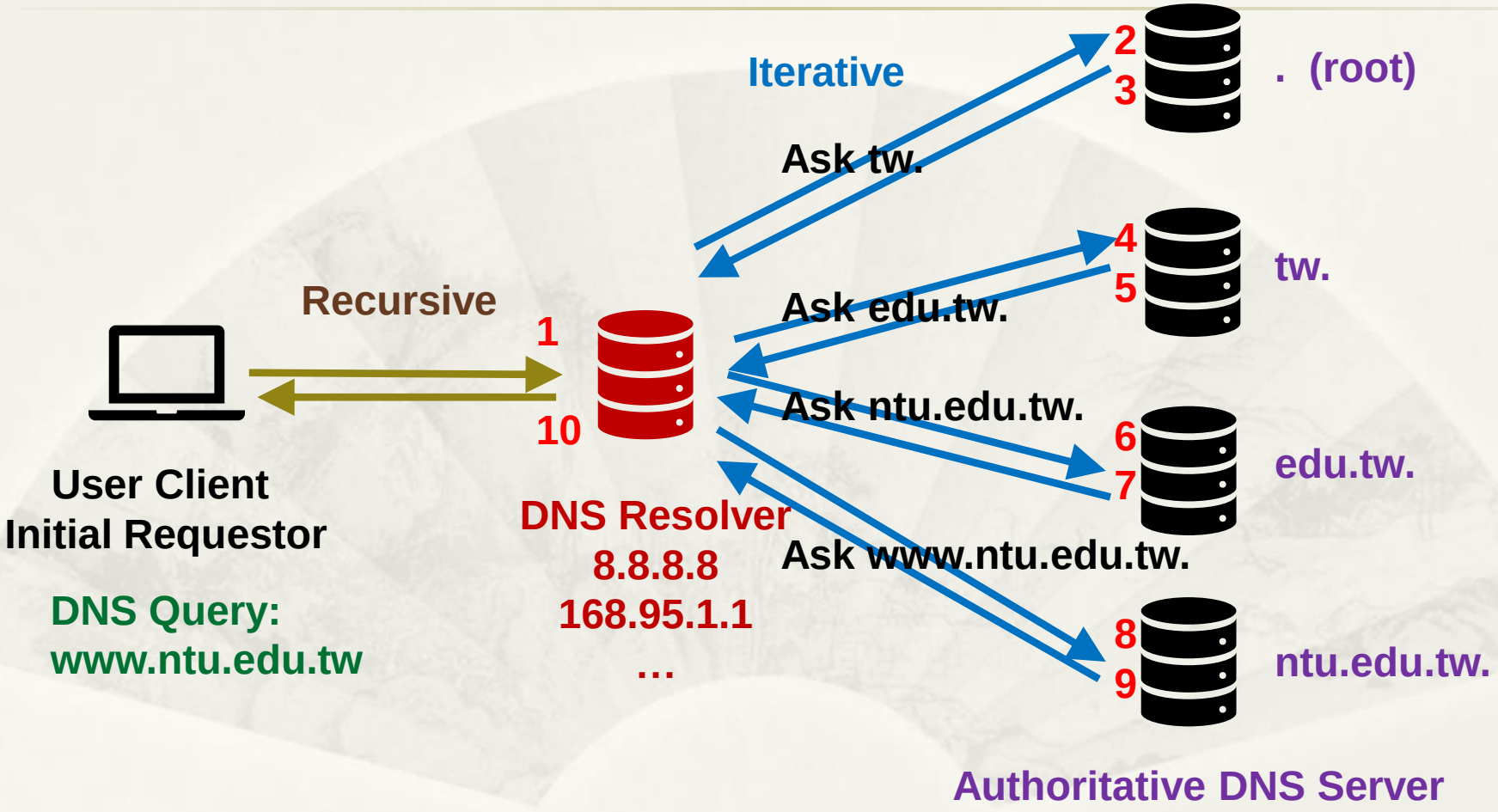
DNS
EDNS Client Subnet (ECS)

台大計中網路組
游子興
davisyou@ntu.edu.tw
02-33665008

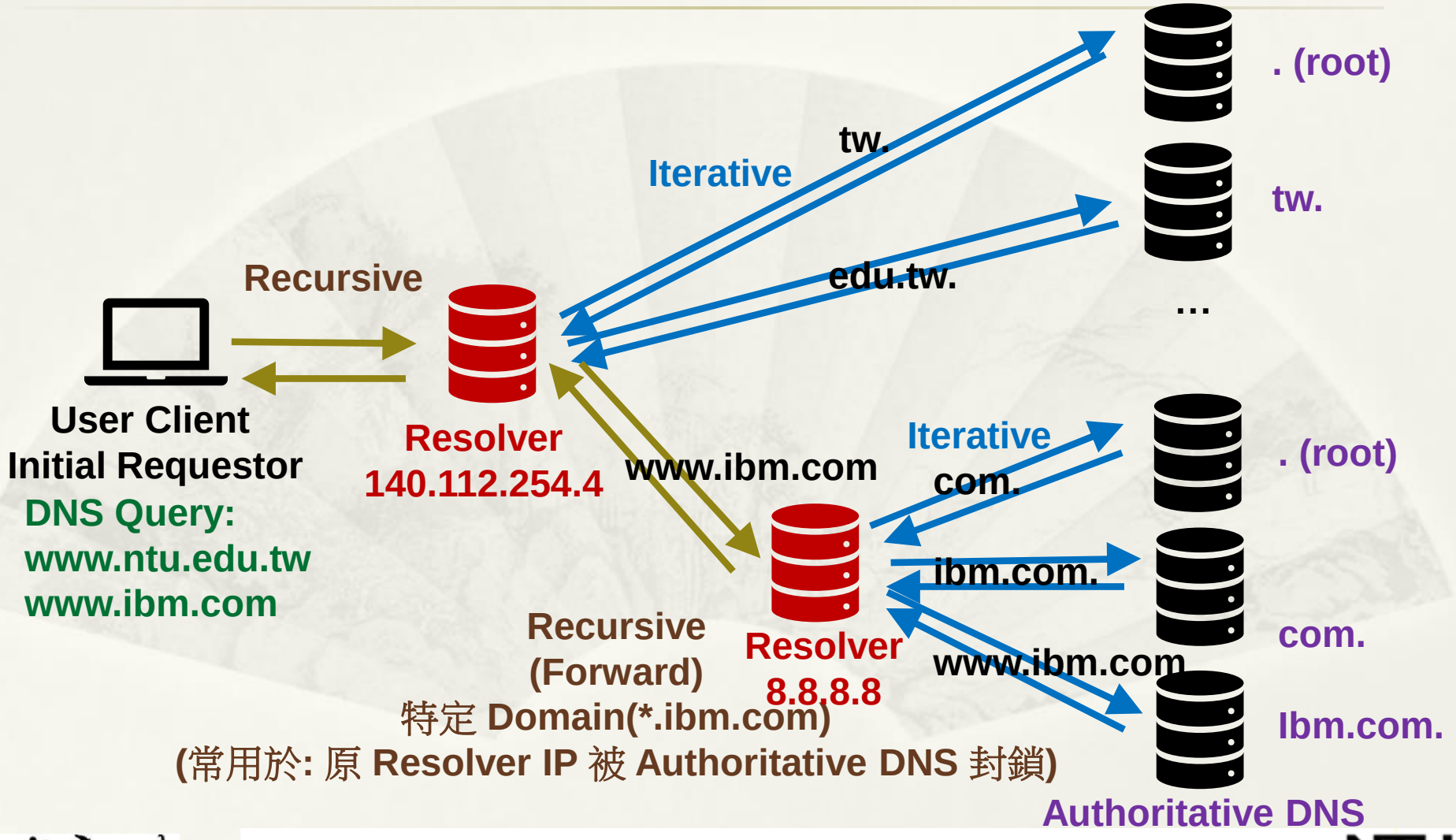
DNS 運作架構


Iterative
2
3
. (root)
Ask tw.
4
5
tw.
Recursive
Ask edu.tw.
1
10
Ask ntu.edu.tw.
6
7
edu.tw.
User Client
Initial Requestor
DNS Resolver
8.8.8.8
168.95.1.1
…
Ask www.ntu.edu.tw.
8
9
ntu.edu.tw.
DNS Query:
www.ntu.edu.tw
Authoritative DNS Server

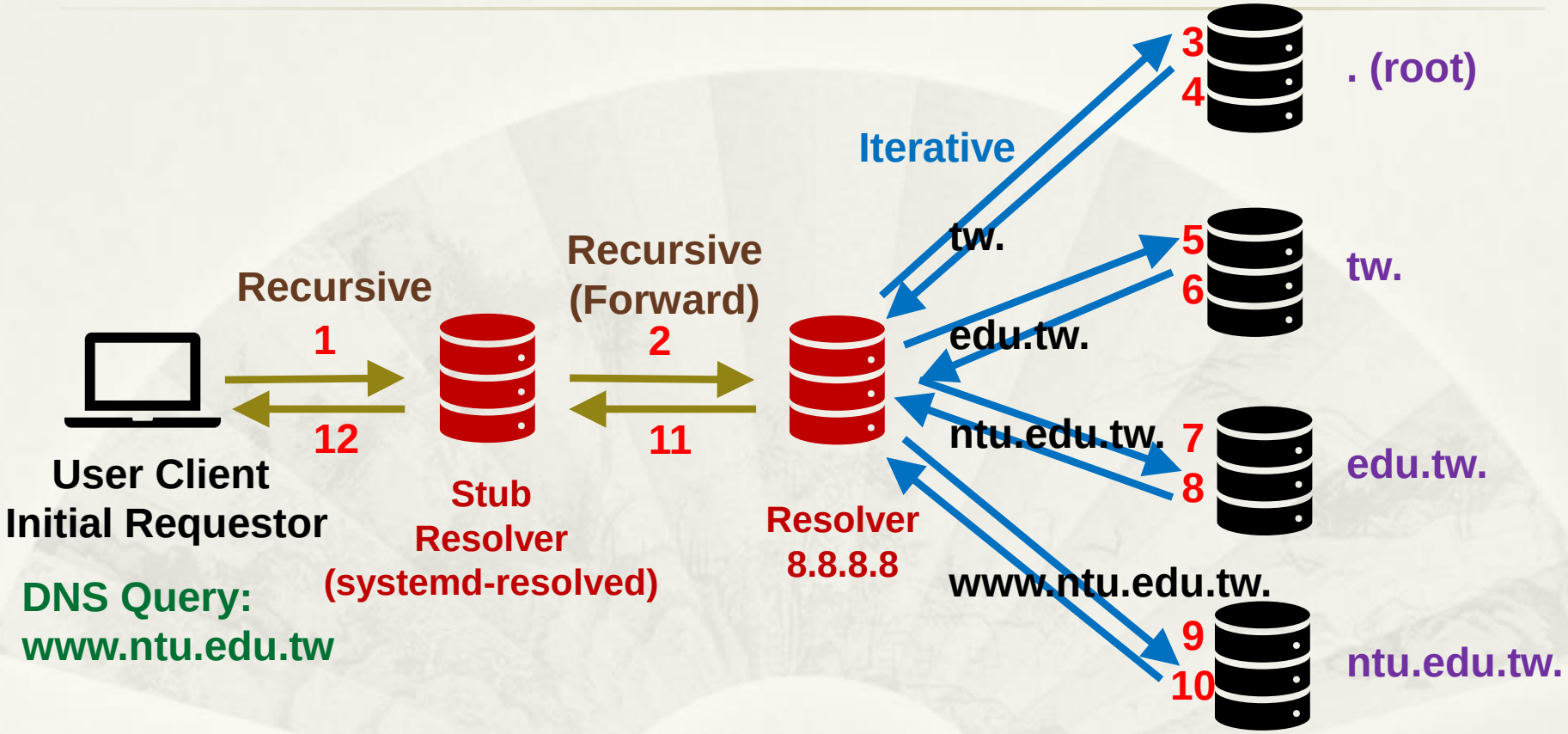
DNS 連線 @新世代 Firewall (需可分辨 Iterative/Recursive Query)

- 外對內 Port 53
  - Iterative Query 詢問校內 Authoritative DNS Server (*.ntu.edu.tw)
    - 僅允許特定 IP(官方 Authoritative Server)，可禁止私架 Authoritative DNS Server
  - Recursive Query 詢問校內 DNS Resolver
    - 應全面禁止
- 內對外 Port 53
  - Iterative Query 詢問校外 Authoritative DNS Server (*.)
    - 僅允許特定 IP(官方 DNS Resolver)，可禁止私架 DNS Resolver
  - Recursive Query 詢問校外 DNS Resolver
    - 若全面禁止，可限制使用者僅能使用校內 DNS Resolver
- ※僅觀察發起方連線

Partial Forward



Stub Resolver (All Forward)



※新版 Linux 幾乎預設皆有 Stub Resolver
目的: 提供 DNS Cache 功能

Ubuntu OS
預設值

* ~# netstat -lnptu

```
root@ubuntu2204:~# netstat -lnptu
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      906/systemd-resolve
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      995/sshd: /usr/sbin
udp        0      0 127.0.0.53:53           0.0.0.0:*                           906/systemd-resolve
```

* Resolver 設定
  /etc/resolv.conf
  nameserver 127.0.0.53

* Daemon: systemd-resolved
  ~# systemctl status systemd-resolved

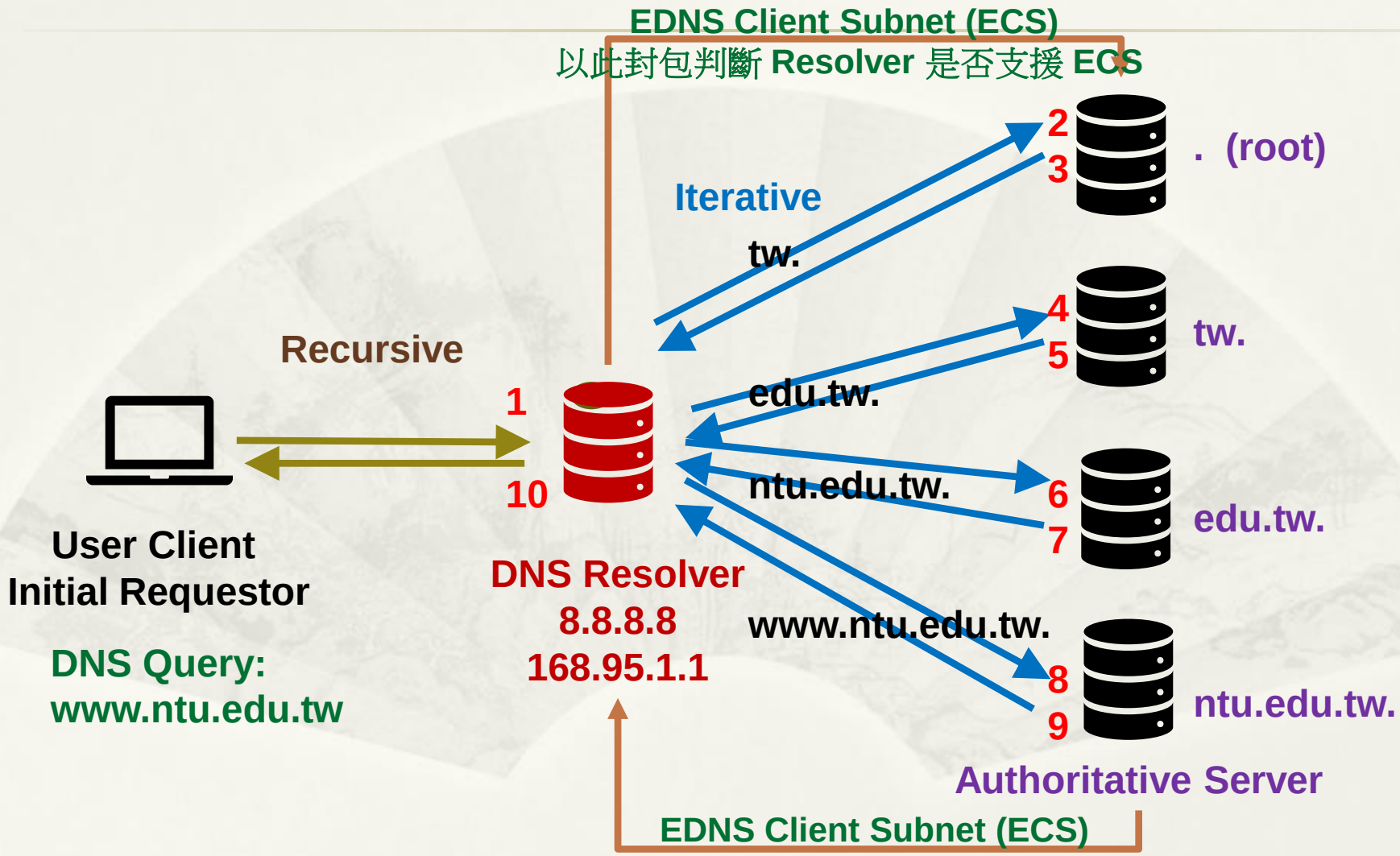
* By 網卡設定 Forward DNS
  /etc/netplan/50-cloud-init.yaml

```
network:
  ethernets:
    ens160:
      addresses:
      ....
      nameservers:
        addresses: [8.8.8.8]
```

Ubuntu OS
Stub Resolver(DNS Cache) Test

* 測試案例 1.
  * 測試解析 www.abc.com
    ~# dig a www.abc.com
  * 開啟另一個視窗觀察 DNS Query 封包，重複執行上述 dig 指令
    ~# tcpdump -n port 53
  * 預期結果:
    * 因有 Stub Resolver(systemd-resolved) DNS Cache，僅有第一次有封包向外詢問
* 測試案例 2.
  * 更改 resolv.conf 檔案
    ~# nano /etc/resolv.conf
    nameserver ~~127.0.0.53~~ 8.8.8.8
  * 重複執行 測試案例 1 步驟
  * 預期結果:
    * 因 Linux 預設無 OS-level DNS Cache ，每次 dig 皆有封包向外詢問
  * 重啟 systemd-resolved
    systemctl restart systemd-resolved
  * 觀察 /etc/resolv.conf 還原成初始值
    ~# cat /etc/resolv.conf

ECS 運作架構


EDNS Client Subnet (ECS)
以此封包判斷 Resolver 是否支援 ECS
Iterative
Recursive
tw.
edu.tw.
ntu.edu.tw.
www.ntu.edu.tw.
1
2
3
4
5
6
7
8
9
10
. (root)
tw.
edu.tw.
ntu.edu.tw.
Authoritative Server
User Client
Initial Requestor
DNS Query:
www.ntu.edu.tw
DNS Resolver
8.8.8.8
168.95.1.1
EDNS Client Subnet (ECS)
※ Authoritative Server 僅需支援 EDNS
就可回應 EDNS Client Subnet，但不代表支援 ECS

EDNS (Extension Mechanisms for DNS)

- 1999年第一個DNS 延伸安全協定發布，稱作 EDNS
- 應用
  - DNSSEC
  - EDNS Client Subnet (ECS)
  - DNS Cookie
- 支援
  - Win 2008R2 DNS 不支援

EDNS Client Subnet (ECS)

- RFC 7871
  - https://developers.google.com/speed/public-dns/docs/ecs
- Use EDNSo option to convey Client IP Subnet to Authoritative DNS Servers.
- Authoritative DNS Servers can return differing answers based on Client's Geo IP Location.
  - 支援不同地理位置解析的權威 DNS 伺服器
  - Used For Content Delivery Networks(CDN)
- Can be safely ignored.

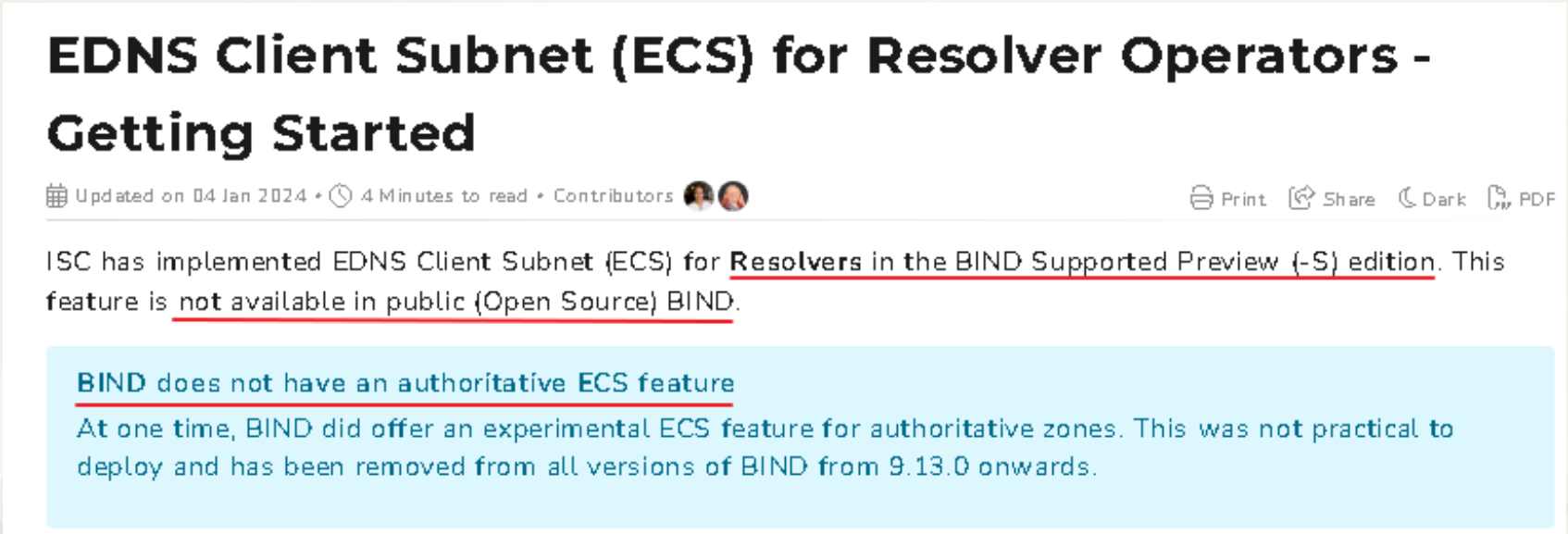
EDNS Client-Subnet Extension
支援條件

- DNS Resolver
  - Pass Client IP to Authoritative DNS Server
- Authoritative Server
  - Based on Client IP，依據地理位置解析不同 IP
  - If DNS Resolver not Support ECS, Authoritative Server will use DNS Resolver IP instead.

EDNS Client-Subnet Extension
尚未被廣泛支援原因

- Privacy and Security Issue
  - Because ECS provides User Client network information to upstream Resolver, it will reveal Client's location.
  - Cloudflare CEO Matthew Prince cited privacy concerns as reason for 1.1.1.1 to not support ECS.
    - Ref. https://en.wikipedia.org/wiki/EDNS_Client_Subnet
- BIND 最新版仍不支援 ECS
  - HiNet DNS 168.95.1.1 不支援

BIND Don't Support ECS



EDNS Client Subnet (ECS) for Resolver Operators - Getting Started

Updated on 04 Jan 2024 • 4 Minutes to read • Contributors

Print Share Dark PDF

ISC has implemented EDNS Client Subnet (ECS) for **Resolvers** in the BIND Supported Preview (-S) edition. This feature is not available in public (Open Source) BIND.

BIND does not have an authoritative ECS feature

At one time, BIND did offer an experimental ECS feature for authoritative zones. This was not practical to deploy and has been removed from all versions of BIND from 9.13.0 onwards.

* https://kb.isc.org/docs/edns-client-subnet-ecs-for-resolver-operators-getting-started

BIND Don't Support ECS

* BIND 9 Significant Features Matrix
  * https://kb.isc.org/docs/aa-01310

Feature	9.20 new stable	9.18 current stable	9.18-S current stable	9.16 EoL	9.16-S EoL
EDNS buffer size changed from 4096 to 1232 bytes (DNS Flag Day 2020)		all	all	9.16.8	9.16.8
EDNS Client-Subnet (ECS) for resolver		---	all	---	all, updated 9.16.10-S
EDNS Client-Subnet (ECS) option support for authoritative servers		---	---	removed	removed
EDNS EXPIRE option now includes AXFR and IXFR	new	---	---	---	---

補充: BIND Zone File View (Split Horizon)

- 用途: Authoritative DNS Server 支援依據不同來源 IP，解析出不同結果.
- 限制: 來源 IP 僅支援使用 Resolver IP 判斷，不支援 EDNS Client Subnet.

BIND Zone File View (Split Horizon)

```
acl intranet { 192.168.100.0/24; };
acl internet { ! 192.168.100.0/24; any; };

view "lan" {
        match-clients { "intranet"; };

        zone "centos.davis"  {
                type master;
                file “named.centos.davis.lan”; <==使用不同 Zone File
        };
};

view "wan" {
        match-clients { "internet"; };

        zone "centos.davis"  {
                type master;
                file "named.centos.davis.wan";  <==使用不同 Zone File
        };
};
```

BIND Zone File View (Split Horizon)

/var/named/named.centos.davis.lan 內容:

```
@       IN    SOA    ns.centos.davis. root.ns.centos.davis.
( 811209091 3600 3600 3600 300 )
        IN    NS     ns.centos.davis.
ns      IN    A      192.168.100.200
www     IN    A      192.168.100.252
```

/var/named/named.centos.davis.wan 內容:

```
@       IN    SOA    ns.centos.davis. root.ns.centos.davis.
( 811209091 3600 3600 3600 300 )
        IN    NS     ns.centos.davis.
ns      IN    A      140.112.2.200
www     IN    A      140.112.2.252
```

DNS Open Resolver
Public DNS Resolver

Open/Public DNS Resolver

- HiNet
  - IPv4: 168.95.1.1
  - IPv6: 2001:b000:168::1 、2001:b000:168::2
- TANet
  - IPv4: 140.111.233.5, 163.28.6.1
  - IPv6: 2001:288:0:233::5, 2001:288:1:1006:163:28:6:1
- Cloudflare
  - 1.1.1.1
- Yandex (https://dns.yandex.com/)
  - IPv4: 77.88.8.8, 77.88.8.1
  - IPv6: 2a02:6b8::feed:off, 2a02:6b8:0:1::feed:off

Google

- IPv4
  - 8.8.8.8 (google-public-dns-a.google.com)
  - 8.8.4.4 (google-public-dns-b.google.com)
- IPv6
  - 2001:4860:4860::8888
  - 2001:4860:4860::8844
- https://developers.google.com/speed/public-dns?hl=zh-tw
- https://developers.google.com/speed/public-dns/faq?hl=zh-tw#locations

Quad9

- Malware Blocking, DNSSEC Validation (this is the most typical configuration)
  - IPv4: 9.9.9.9, 149.112.112.112
  - IPv6: 2620:fe::fe, 2620:fe::9
  - HTTPS: https://dns.quad9.net/dns-query
  - TLS: tls://dns.quad9.net
- Secured w/ECS: Malware blocking, DNSSEC Validation, ECS enabled
  - IPv4: 9.9.9.11, 149.112.112.11
  - IPv6: 2620:fe::11, 2620:fe::fe:11
  - HTTPS: https://dns11.quad9.net/dns-query
  - TLS: tls://dns11.quad9.net
- Unsecured: No Malware blocking, no DNSSEC validation (for experts only!)
  - IPv4: 9.9.9.10, 149.112.112.10
  - IPv6: 2620:fe::10,2620:fe::fe:10
  - HTTPS: https://dns10.quad9.net/dns-query
  - TLS: tls://dns10.quad9.net

https://www.quad9.net/service/service-addresses-and-features/

OpenDNS

- OpenDNS（https://www.opendns.com/）
  - 208.67.220.220（Resolver2.OpenDNS.com）
  - 208.67.220.222（Resolver4.OpenDNS.com）
  - 208.67.222.220（Resolver3.OpenDNS.com）
  - 208.67.222.222（Resolver1.OpenDNS.com）
  - Family Shield Servers: 阻擋成人、惡意軟體網站
  - 208.67.222.123（resolver1-fs.opendns.com）
  - 208.67.220.123（resolver2-fs.opendns.com）
  - IPv6 實驗性質：2620:0:ccc::2, 2620:0:ccd::2

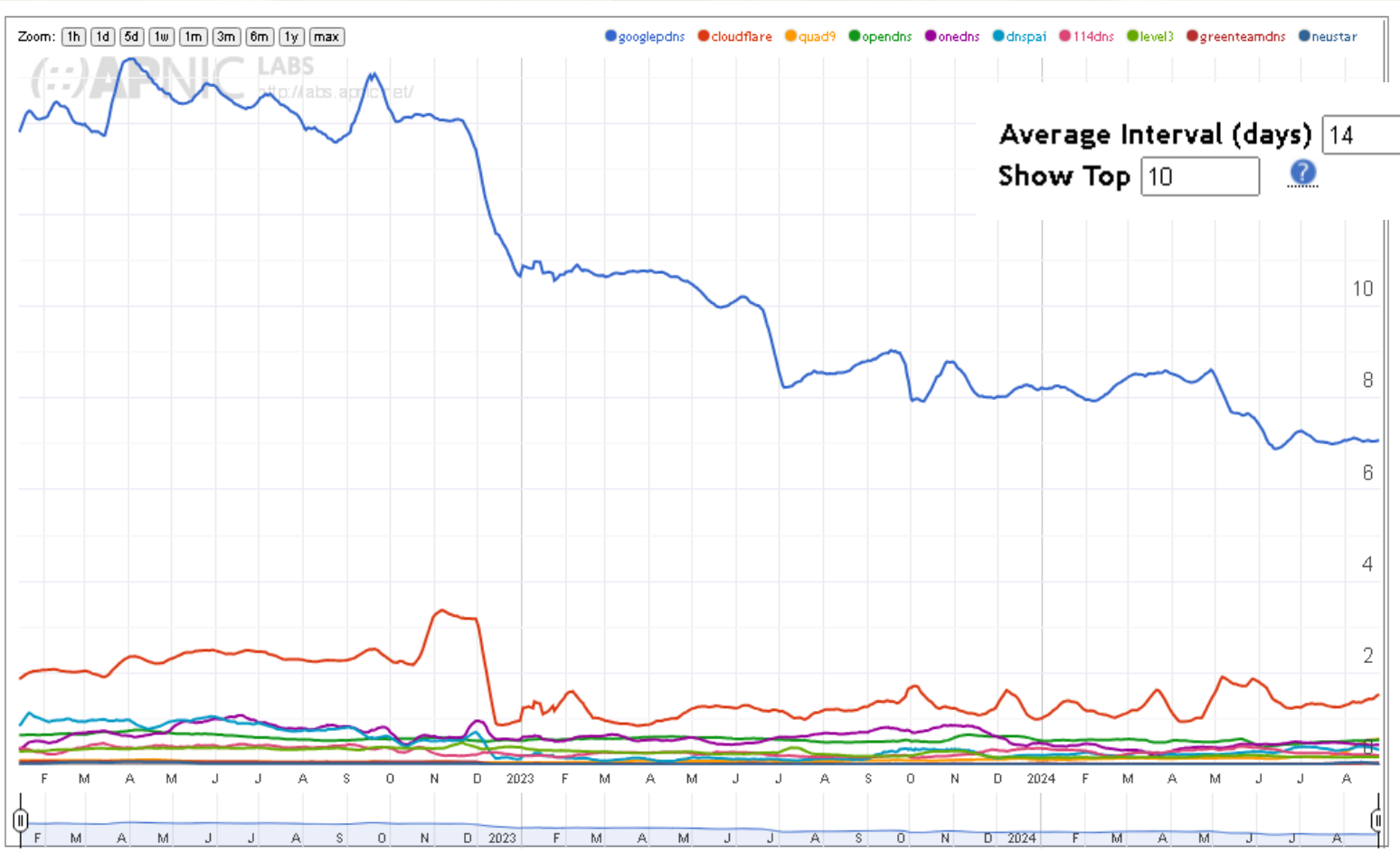
Open/Public DNS Resolver

- Public DNS Server List
  - https://dnschecker.org/public-dns
  - https://dnschecker.org/public-dns/tw

IP Address	Location	ASN Number	Software / Version	DNSSEC	Reliability
101.101.101.101 *twnic-public-dns.twnic.tw*	Taipei, Taipei	AS131621 *Taiwan Network Information Center*	101	Yes	99 %
101.102.103.104 *twnic-public-dns.twnic.tw*	Taipei, Taipei	AS131621 *Taiwan Network Information Center*	101	Yes	100 %
113.196.55.130 *113.196.55.130.ll.static.sparqnet.net*	Taipei, Taipei	AS9919 *New Century InfoComm Tech Co., Ltd.*	dnsmasq-2.45	Yes	86 %
168.95.1.1 *dns.hinet.net*	Taipei, Taipei	AS3462 *Data Communication Business Group*	—	Yes	73 %
168.95.192.1 *hntp1.hinet.net*	Taipei, Taipei	AS3462 *Data Communication Business Group*	—	Yes	75 %
220.128.231.90 *220-128-231-90.hinet-ip.hinet.net*	Taipei, Taipei	AS3462 *Data Communication Business Group*	—	No	8 %
59.124.72.210 *59-124-72-210.hinet-ip.hinet.net*	Taipei, Taipei	AS3462 *Data Communication Business Group*	—	No	62 %
113.61.224.13 *113-61-224-13.veetime.com*	Taichung, Taichung	AS17809 *VEE TIME CORP.*	—	Yes	59 %
203.71.0.1	Taipei, Taipei	AS1659 *Taiwan Academic Network (TANet)*	—	No	3 %

Open/Public DNS Resolver

* Use of DNS Resolvers for World(使用統計)
  * https://stats.labs.apnic.net/rvrs



如何選擇最佳 Open DNS Resolver ?

nslookup download.microsoft.com

```
> download.microsoft.com
伺服器:  dns.ntu.edu.tw
Address:  140.112.254.4

未經授權的回答:
名稱:    e12671.dscd.akamaiedge.net
Addresses:  2001:288:6:8b::317f
          2001:288:6:a9::317f
          163.28.224.206
Aliases:  download.microsoft.com
          dlc-shim.trafficmanager.net
          main.dl.ms.akadns.net
          download.microsoft.com.edgekey.net
```

NTU

```
> download.microsoft.com
伺服器:  resolver2.opendns.com
Address:  208.67.220.220

未經授權的回答:
名稱:    e12671.dscd.akamaiedge.net
Addresses:  2001:288:6:8b::317f
          2001:288:6:a9::317f
          163.28.224.206
Aliases:  download.microsoft.com
          dlc-shim.trafficmanager.net
          main.dl.ms.akadns.net
          download.microsoft.com.edgekey.net
```

OpenDNS

Resolver 支援 ECS

```
> download.microsoft.com
伺服器:  dns.google
Address:  8.8.8.8

未經授權的回答:
名稱:    e12671.dscd.akamaiedge.net
Addresses:  2001:288:6:8b::317f
          2001:288:6:a9::317f
          163.28.224.206
Aliases:  download.microsoft.com
          dlc-shim.trafficmanager.net
          main.dl.ms.akadns.net
          download.microsoft.com.edgekey.net
```

Google

Resolver 支援 ECS

```
> download.microsoft.com
伺服器:  [140.111.233.5]
Address:  140.111.233.5

未經授權的回答:
名稱:    e12671.dscd.akamaiedge.net
Addresses:  2001:288:6:a9::317f
          2001:288:6:8b::317f
          163.28.224.206
Aliases:  download.microsoft.com
          dlc-shim.trafficmanager.net
          main.dl.ms.akadns.net
          download.microsoft.com.edgekey.net
```

TANet 教育部

Resolver 支援 ECS

nslookup download.microsoft.com

```
> download.microsoft.com
伺服器:  one.one.one.one
Address:  1.1.1.1

未經授權的回答:
DNS request timed out.
    timeout was 2 seconds.
名稱:    e12671.dscd.akamaiedge.net
Address:  23.47.5.194
Aliases:  download.microsoft.com
          dlc-shim.trafficmanager.net
          main.dl.ms.akadns.net
          download.microsoft.com.edgekey.net
```

Cloudflare

```
> download.microsoft.com
伺服器:  dns9.quad9.net
Address:  9.9.9.9

未經授權的回答:
名稱:    e12671.dscd.akamaiedge.net
Addresses:  2600:1417:76:585::317f
          2600:1417:76:581::317f
          23.47.5.194
Aliases:  download.microsoft.com
          dlc-shim.trafficmanager.net
          main.dl.ms.akadns.net
          download.microsoft.com.edgekey.net
```

Quad9

```
> download.microsoft.com
伺服器:  dns.hinet.net
Address:  168.95.1.1

未經授權的回答:
名稱:    e12671.dscd.akamaiedge.net
Addresses:  2600:1417:1b:182::317f
          2600:1417:1b:18f::317f
          23.220.197.211
Aliases:  download.microsoft.com
          dlc-shim.trafficmanager.net
          main.dl.ms.akadns.net
          download.microsoft.com.edgekey.net
```

HiNet

Resolver 不支援 ECS

Where is Akamai CDN Server 163.28.224.206 @教育部

* Tracert

```
C:\Users\user>tracert 163.28.224.206

在上限 30 個躍點上追蹤 163.28.224.206 的路由

  1    <1 ms    <1 ms    <1 ms  172.16.0.1
  2    <1 ms    <1 ms    <1 ms  ntuccgw.cc.ntu.edu.tw [140.112.3.126]
  3    <1 ms    <1 ms    <1 ms  core_serv_0210.cc.ntu.edu.tw [140.112.0.210]
  4     1 ms     1 ms     1 ms  wan0206.cc.ntu.edu.tw [140.112.0.206]
  5     2 ms     2 ms     1 ms  wan_tanet_0070.cc.ntu.edu.tw [140.112.0.70]
  6     4 ms     3 ms     3 ms  192.192.61.82
  7     4 ms     2 ms     3 ms  192.192.61.48
  8     *        *        6 ms  192.192.61.58
  9     4 ms     3 ms     3 ms  163.28.224.206
```

* IP Whois

https://www.whois365.com/tw/ip/163.28.224.206

```
inetnum: 163.28.0.0 - 163.28.255.255
netname: T-EDU.TW-NET
descr: Ministry of Education Computer Center
descr: 12F, No 106, Sec.2,Hoping E. Rd.,
```

* Shodan

https://www.shodan.io/host/163.28.224.206

Hostnames	download.**microsoft.com** akamai.download.**microsoft.com**
Domains	MICROSOFT.COM
Country	**Taiwan**
City	**Taipei**
Organization	**Ministry of Education Computer Center**
ISP	**Taiwan Academic Network (TANet) Information Center**
ASN	**AS1659**

Where is Akamai CDN Server 23.47.5.194 @HiNet

* Tracert

```
C:\Users\user>tracert 23.47.5.194

在上限 30 個躍點上
追蹤 a23-47-5-194.deploy.static.akamaitechnologies.com [23.47.5.194] 的路由:

  1    <1 ms    <1 ms    <1 ms  172.16.0.1
  2     1 ms    <1 ms    <1 ms  ntuccgw.cc.ntu.edu.tw [140.112.3.126]
  3    <1 ms    <1 ms    <1 ms  core_serv_0170.cc.ntu.edu.tw [140.112.0.170]
  4     1 ms     1 ms     1 ms  wan0206.cc.ntu.edu.tw [140.112.0.206]
  5     2 ms     1 ms     1 ms  211-22-226-202.tpdt-3307.hinet.net [211.22.226.202]
  6     5 ms     4 ms     4 ms  220-128-26-14.tpdb-3031.hinet.net [220.128.26.14]
  7     *        *        *     要求等候逾時。
  8     4 ms     6 ms     4 ms  220-128-16-113.tcwh-3331.hinet.net [220.128.16.113]
  9    15 ms    31 ms    17 ms  211-22-226-221.hinet-ip.hinet.net [211.22.226.221]
 10    35 ms    13 ms     4 ms  a23-47-5-194.deploy.static.akamaitechnologies.com [23.47.5.194]
```

* IP Whois

  https://www.whois365.com/tw/ip/23.47.5.194

```
Akamai Technologies, Inc. AKAMAI (NET-23-32-0-0-1) 23.32.0.0 - 23.67.255.255
Akamai International, BV AIBV (NET-23-47-0-0-1) 23.47.0.0 - 23.47.7.255
```

* Shodan

  https://www.shodan.io/host/23.47.5.194

Hostnames	a23-47-5-194.deploy.static.**akamaitechnologies.com** download.**microsoft.com** akamai.download.**microsoft.com**
Domains	AKAMAITECHNOLOGIES.COM　MICROSOFT.COM
Country	**Taiwan**
City	**Yuanlin**
Organization	**Akamai International, BV**
ISP	**Akamai Technologies, Inc.**
ASN	**AS16625**

Where is Akamai CDN Server 23.220.197.211 @HiNet

* Tracert

```
C:\Users\user>tracert 23.220.197.211

在上限 30 個躍點上
追蹤 a23-220-197-211.deploy.static.akamaitechnologies.com [23.220.197.211] 的路由:

  1    <1 ms    <1 ms    <1 ms  172.16.0.1
  2    <1 ms    <1 ms    <1 ms  ntuccgw.cc.ntu.edu.tw [140.112.3.126]
  3    <1 ms    <1 ms    <1 ms  core_serv_0210.cc.ntu.edu.tw [140.112.0.210]
  4     1 ms     1 ms     1 ms  wan0206.cc.ntu.edu.tw [140.112.0.206]
  5     1 ms     1 ms     1 ms  211-22-226-202.tpdt-3307.hinet.net [211.22.226.202]
  6     2 ms     3 ms    11 ms  220-128-27-26.tpdt-3032.hinet.net [220.128.27.26]
  7     2 ms     2 ms     2 ms  220-128-9-117.tylc-3032.hinet.net [220.128.9.117]
  8     3 ms     2 ms     2 ms  220-128-9-149.tyfo-3332.hinet.net [220.128.9.149]
  9     5 ms     8 ms     7 ms  203-69-140-21.hinet-ip.hinet.net [203.69.140.21]
 10     2 ms     1 ms     1 ms  a23-220-197-211.deploy.static.akamaitechnologies.com [23.220.197.211]
```

* IP Whois

  https://www.whois365.com/tw/ip/23.220.197.211

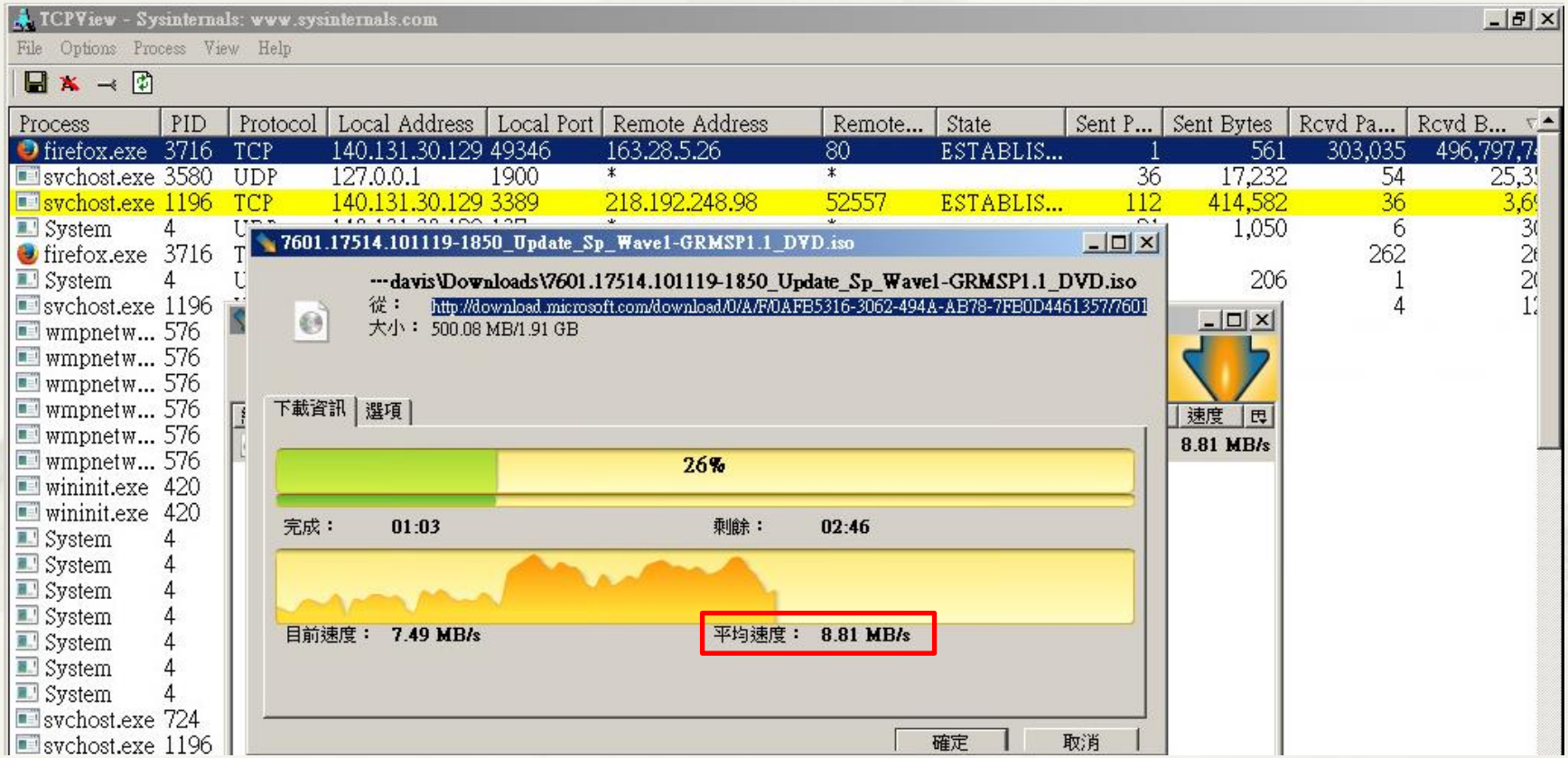
```
NetRange: 23.192.0.0 - 23.223.255.255
CIDR: 23.192.0.0/11
NetName: AKAMAI
NetHandle: NET-23-192-0-0-1
Parent: NET23 (NET-23-0-0-0-0)
NetType: Direct Allocation
OriginAS:
Organization: Akamai Technologies, Inc. (AKAMAI)
```

* Shodan

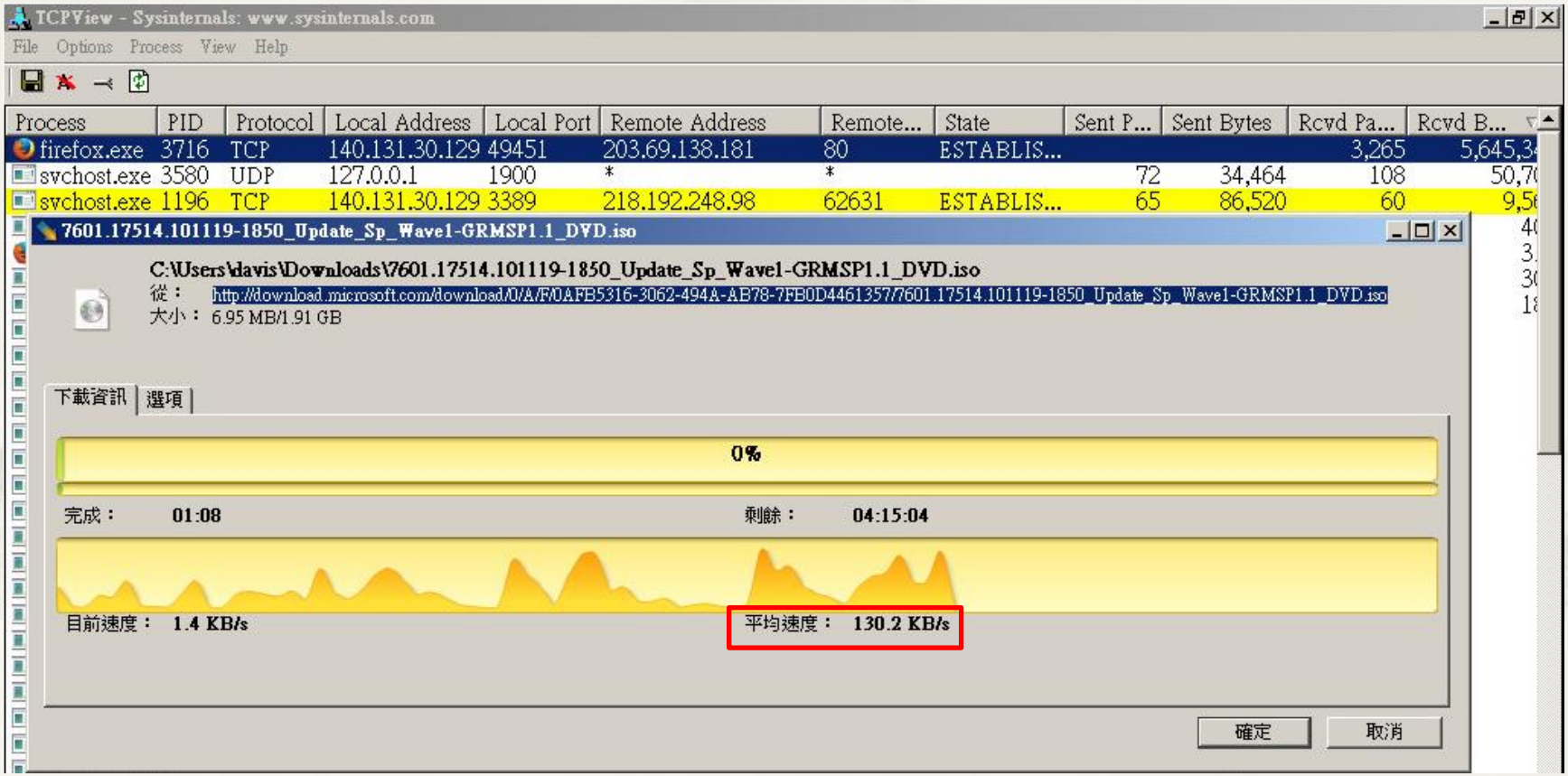
  https://www.shodan.io/host/23.220.197.211

Hostnames	a23-220-197-211.deploy.static.**akamaitechnologies.com** download.**microsoft.com** akamai.download.**microsoft.com**
Domains	AKAMAITECHNOLOGIES.COM MICROSOFT.COM
Country	**Taiwan**
City	**Taipei**
Organization	**Akamai Technologies, Inc.**
ISP	**Akamai Technologies, Inc.**
ASN	**AS16625**

Akamai CDN @教育部
下載速度正常



Akamai CDN @HiNet
下載速度偏慢



下載測試

* 使用不同 IP 網段, Gateway 在區網 Router，DNS Server 168.95.1.1
  * 下載 Win7 SP1 http://download.microsoft.com/download/0/A/F/0AFB5316-3062-494A-AB78-7FB0D4461357/7601.17514.101119-1850_Update_Sp_Wave1-GRMSP1.1_DVD.iso

單位	IP	DNS	Akamai@HiNet	下載速度
台大區網	163.28.16.44	168.95.1.1	203.69.138.171	7.59 MB/秒
亞東	120.96.32.21	168.95.1.1	203.69.138.181	31 KB/秒
德霖	210.60.141.173	168.95.1.1	203.69.138.171	90 KB/秒
台藝大	140.131.30.129	168.95.1.1	203.69.138.171	130 KB/秒

* 結論: Akamai CDN @HiNet 疑似有 QoS 設定，若來源 IP 非 HiNet 用戶，可能會被限速.

Open DNS Resolvers Compare

廠商	Resolver IP	EDNS Client Subnet	DNSSEC Validate
Google	8.8.8.8	V	V
Cloudflare	1.1.1.1	X	V
HiNet	168.95.1.1	X	X
TANet	140.111.233.5 163.28.6.1	V	V
Quad9	9.9.9.9	X	V
OpenDNS	208.67.220.220 208.67.220.222 208.67.222.220 208.67.222.222	V	V
NTU DNS	140.112.254.4	X	X

結論: DNS Resolver 設定建議

* 使用 支援 DNS EDNS Client Subnet + DNSSEC Validate 之 Open DNS Resolver

* 使用"單位內 IP 網段"自行架設之 DNS Resolver
  * 特別注意是否有 Partial/All Forward to 其他不支援 ECS 之 Resolver (例如 168.95.1.1)
    * 待測試: Forward 之後 ECS 仍可正常運作 .....

* 除非是 HiNet光世代用戶，否則不建議設定使用 168.95.1.1

如何測試 DNS Resolver 是否支援 EDNS Client Subnet

DNS Resolver
是否支援 EDNS Client Subnet

- 查詢使用 Akamai CDN 之 FQDN，利用回覆 IP 位址判斷 (如上述測試結果)
- 使用支援查詢特殊 FQDN 之 Authoritative Server 來顯示 EDNS Client Subnet
- 自行架設 Authoritative DNS Server + 封包側錄

提供查詢特殊 FQDN 之 Authoritative Server

Google 提供

Check DNS Resolver IP and EDNS Client Subnet

- FQDN

  o-o.myaddr.google.com

  or

  o-o.myaddr.l.google.com

- Query
  - TXT record type

Check DNS Resolver IP and EDNS Client Subnet

- dig o-o.myaddr.google.com TXT @8.8.8.8

```
root@ubuntu2204:~# dig o-o.myaddr.l.google.com TXT @8.8.8.8

; <<>> DiG 9.18.18-0ubuntu0.22.04.1-Ubuntu <<>> o-o.myaddr.l.google.com TXT @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24607
;; 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.l.google.com.       IN      TXT

;; ANSWER SECTION:
o-o.myaddr.l.google.com. 60     IN      TXT     "173.194.93.12"
o-o.myaddr.l.google.com. 60     IN      TXT     "edns0-client-subnet 140.112.3.0/24"
```

Google DNS

DNS Resolver IP

EDNS Client Subnet

- dig o-o.myaddr.google.com TXT @168.95.1.1

```
root@ubuntu2204:~# dig o-o.myaddr.l.google.com TXT @168.95.1.1

; <<>> DiG 9.18.18-0ubuntu0.22.04.1-Ubuntu <<>> o-o.myaddr.l.google.com TXT @168.95.1.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35189
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: e005e9abd99b2cba0f767e8f657819ef9546d1605376b9dc (good)
;; QUESTION SECTION:
;o-o.myaddr.l.google.com.       IN      TXT

;; ANSWER SECTION:
o-o.myaddr.l.google.com. 60     IN      TXT     "2001:b000:180:8002:0:2:8:58"
```

HiNet DNS

DNS Resolver IP

Check DNS Resolver IP and EDNS Client Subnet

* dig o-o.myaddr.google.com TXT @1.1.1.1

```
root@ubuntu2204:~# dig o-o.myaddr.l.google.com TXT @1.1.1.1

; <<>> DiG 9.18.18-0ubuntu0.22.04.1-Ubuntu <<>> o-o.myaddr.l.google.com TXT @1.1.1.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30461
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;o-o.myaddr.l.google.com.       IN      TXT

;; ANSWER SECTION:
o-o.myaddr.l.google.com. 52     IN      TXT     "2400:cb00:80:1024::a29e:f1c8"
```

Cloudflare DNS

DNS Resolver IP

* dig o-o.myaddr.google.com TXT @140.111.233.5

```
root@ubuntu2204:~# dig o-o.myaddr.l.google.com TXT @140.111.233.5

; <<>> DiG 9.18.18-0ubuntu0.22.04.1-Ubuntu <<>> o-o.myaddr.l.google.com TXT @140.111.233.5
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36558
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: b928cd92681cc1b65ce6f4e2658555fa2cff39cb7f3499be (good)
;; QUESTION SECTION:
;o-o.myaddr.l.google.com.       IN      TXT

;; ANSWER SECTION:
o-o.myaddr.l.google.com. 60     IN      TXT     "140.111.34.135"
o-o.myaddr.l.google.com. 60     IN      TXT     "edns0-client-subnet 140.112.3.0/24"
```

TANet DNS

DNS Resolver IP

EDNS Client Subnet

Check DNS Resolver IP and EDNS Client Subnet

* dig o-o.myaddr.google.com TXT @9.9.9.9

```
root@ubuntu2204:~# dig o-o.myaddr.l.google.com TXT @9.9.9.9

; <<>> DiG 9.18.18-0ubuntu0.22.04.1-Ubuntu <<>> o-o.myaddr.l.google.com TXT @9.9.9.9
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15290
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
o-o.myaddr.l.google.com. 60     IN      TXT     "119.31.179.35"
```

Quad9

DNS Resolver IP

* dig o-o.myaddr.google.com txt @208.67.220.220

```
root@ubuntu24:~# dig o-o.myaddr.google.com txt @208.67.220.220

; <<>> DiG 9.18.28-0ubuntu0.24.04.1-Ubuntu <<>> o-o.myaddr.google.com txt @208.67.220.220
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47797
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1410
;; QUESTION SECTION:
;o-o.myaddr.google.com.         IN      TXT

;; ANSWER SECTION:
o-o.myaddr.google.com.  60      IN      TXT     "2a04:e4c0:63::64"
o-o.myaddr.google.com.  60      IN      TXT     "edns0-client-subnet 140.112.3.0/24"
```

OpenDNS

DNS Resolver IP

EDNS Client Subnet

Check DNS Resolver IP and EDNS Client Subnet

* dig o-o.myaddr.google.com TXT @140.112.254.4

```
root@ubuntu2204:~# dig o-o.myaddr.l.google.com TXT @140.112.254.4

; <<>> DiG 9.18.18-0ubuntu0.22.04.1-Ubuntu <<>> o-o.myaddr.l.google.com TXT @140.112.254.4
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52886
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 282c03468084634901000000657810lcae5a239b389c3c37 (good)
;; QUESTION SECTION:
;o-o.myaddr.l.google.com.       IN      TXT

;; ANSWER SECTION:
o-o.myaddr.l.google.com. 60     IN      TXT     "140.112.254.71"
```

NTU DNS

DNS Resolver IP

* dig o-o.myaddr.google.com TXT @172.16.0.1

```
root@ubuntu2204:~# dig o-o.myaddr.l.google.com TXT @172.16.0.1

; <<>> DiG 9.18.18-0ubuntu0.22.04.1-Ubuntu <<>> o-o.myaddr.l.google.com TXT @172.16.0.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4516
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;o-o.myaddr.l.google.com.       IN      TXT

;; ANSWER SECTION:
o-o.myaddr.l.google.com. 60     IN      TXT     "140.112.3.82"
```

Pfsense DNS

DNS Resolver IP

提供查詢特殊 FQDN 之 Authoritative Server

TANet CDN 提供

Check DNS Resolver IP、Authoritative DNS Server、EDNS Client Subnet

* https://www.tanetcdn.edu.tw/
  * FAQ

如何取得DNS Resolver伺服器有支援EDNS Client Subnet協定的？

請依照下述操作：

1. 開啟 https://www.whatismyip.com.tw/tw/確認自己電腦出去網站的 IP 為何 (EX: 212.50.60.218)
2. 於終端機 (命令提示字元)輸入指令"dig whoami.tanetcdn.edu.tw TXT"
3. 確認DNS回應結果中有一項 "ecs"欄位，若為 212.50.60.0/24(以項目1之IP範例為例) 則為有支援；若為空值，則不支援。

Check DNS Resolver IP、Authoritative DNS Server、EDNS Client Subnet

* dig whoami.tanetcdn.edu.tw TXT @8.8.8.8

```
root@ubuntu2204:~# dig whoami.tanetcdn.edu.tw TXT @8.8.8.8

; <<>> DiG 9.18.18-0ubuntu0.22.04.1-Ubuntu <<>> whoami.tanetcdn.edu.tw TXT @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54413
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;whoami.tanetcdn.edu.tw.                IN      TXT

;; ANSWER SECTION:
whoami.tanetcdn.edu.tw. 20      IN      TXT     "ip" "192.178.36.133"
whoami.tanetcdn.edu.tw. 20      IN      TXT     "ns" "cdn-niu-cdrs02"
whoami.tanetcdn.edu.tw. 20      IN      TXT     "ecs" "140.112.3.0/24"
```

Google DNS

DNS Resolver IP

Authoritative DNS Serve

EDNS Client Subnet

Check DNS Resolver IP、Authoritative DNS Server、EDNS Client Subnet

* 有時 EDNS Client Subnet 無法正常顯示

```
root@ubuntu2204:~# dig whoami.tanetcdn.edu.tw TXT @8.8.8.8

; <<>> DiG 9.18.18-0ubuntu0.22.04.1-Ubuntu <<>> whoami.tanetcdn.edu.tw TXT @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36600
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;whoami.tanetcdn.edu.tw.                IN      TXT

;; ANSWER SECTION:
whoami.tanetcdn.edu.tw. 20      IN      TXT     "ip" "74.125.41.67"
whoami.tanetcdn.edu.tw. 20      IN      TXT     "ns" "cdn-niu-cdrs04"
whoami.tanetcdn.edu.tw. 20      IN      TXT     "ecs" ""
```

Check DNS Resolver IP、Authoritative DNS Server、EDNS Client Subnet

* dig whoami.tanetcdn.edu.tw TXT @1.1.1.1

```
root@ubuntu2204:~# dig whoami.tanetcdn.edu.tw TXT @1.1.1.1

; <<>> DiG 9.18.18-0ubuntu0.22.04.1-Ubuntu <<>> whoami.tanetcdn.edu.tw TXT @1.1.1.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39933
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;whoami.tanetcdn.edu.tw.                IN      TXT

;; ANSWER SECTION:
whoami.tanetcdn.edu.tw. 20      IN      TXT     "ip" "162.158.241.54"
whoami.tanetcdn.edu.tw. 20      IN      TXT     "ns" "cdn-niu-cdrs02"
whoami.tanetcdn.edu.tw. 20      IN      TXT     "ecs" ""
```

Cloudflare DNS

DNS Resolver IP
Authoritative DNS Serve
EDNS Client Subnet

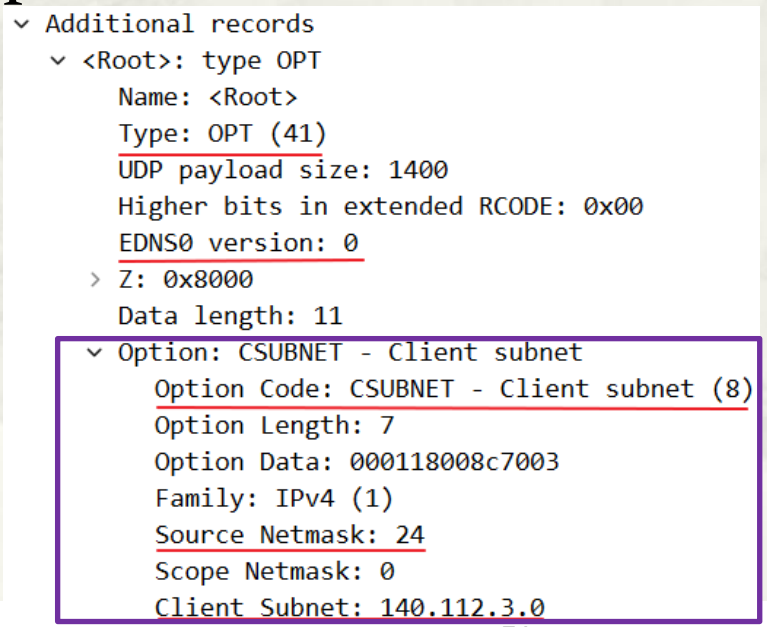
Open DNS Resolver EDNS Client Subnet Support

廠商	Resolver IP	EDNS Client Subnet
Google	8.8.8.8	V
Cloudflare	1.1.1.1	X
Hinet	168.95.1.1	X
TANet	140.111.233.5 163.28.6.1	V
Quad9	9.9.9.9	X
OpenDNS	208.67.220.220 208.67.220.222 208.67.222.220 208.67.222.222	V
NTU DNS	140.112.254.4	X

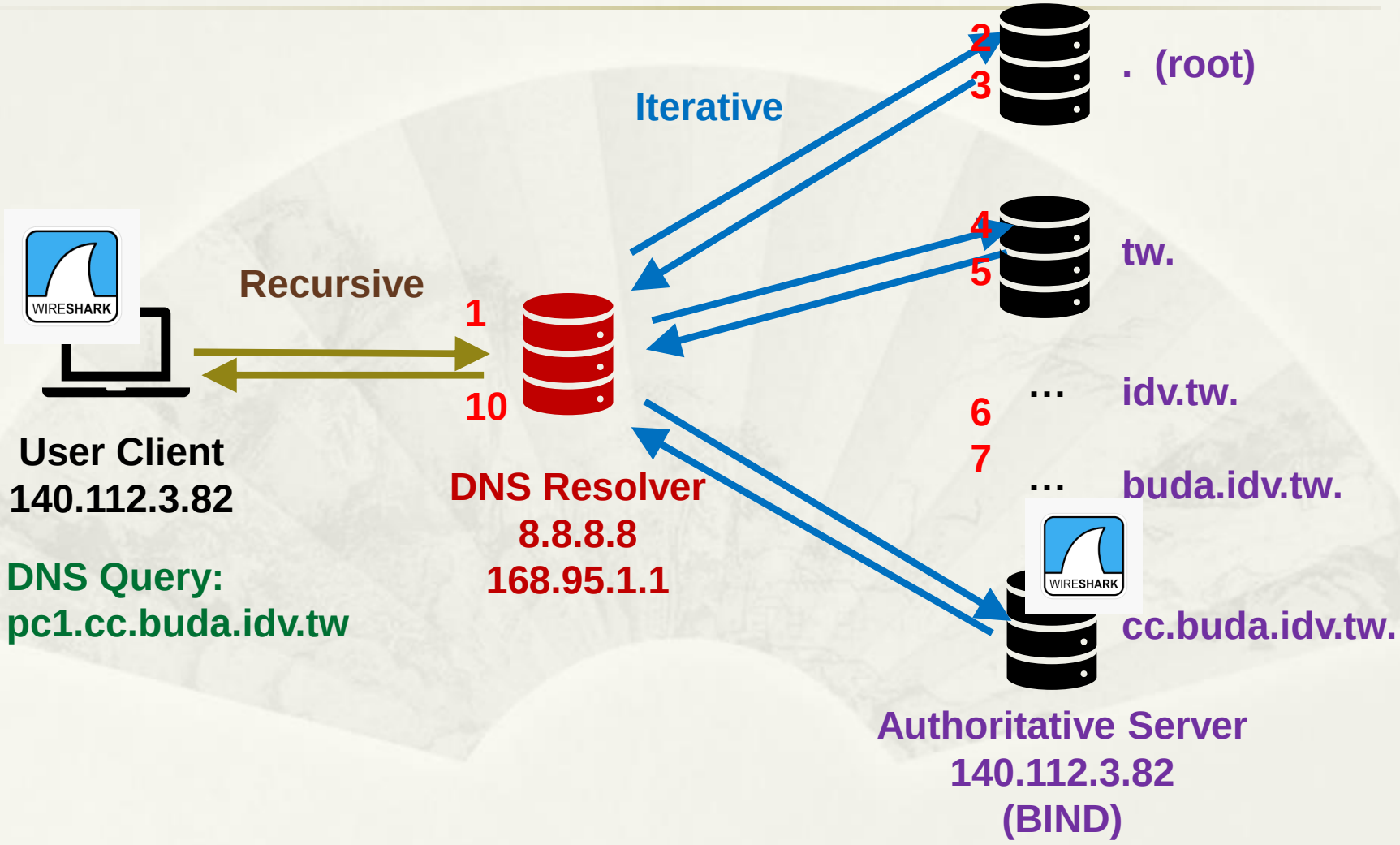
自行架設 Authoritative DNS Server + 封包側錄

偵測原理

- Authoritative Server 收到來自 DNS Resolver 之 Iterative Query
- 觀察封包內容是否含有
  - dns.opt.code == 8



測試架構


Iterative
Recursive
2
3
. (root)
4
5
tw.
1
10
…
idv.tw.
6
7
…
buda.idv.tw.
cc.buda.idv.tw.
WIRESHARK
WIRESHARK
User Client
140.112.3.82
DNS Query:
pc1.cc.buda.idv.tw
DNS Resolver
8.8.8.8
168.95.1.1
Authoritative Server
140.112.3.82
(BIND)

DNS Resolver
8.8.8.8

```
S:\Tools\Nmap7.94>nslookup
預設伺服器:  dns.google
Address:  8.8.8.8

> pc1.cc.buda.idv.tw
伺服器:  dns.google
Address:  8.8.8.8

未經授權的回答:
名稱:    pc1.cc.buda.idv.tw
Address:  140.112.3.82
```

No.	Time	udp.stream	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
1	0.000000	0	140.112.3.82	35179	8.8.8.8	53	DNS	78	Standard query 0x0002 A pc1.cc.buda.idv.tw
2	0.019571	1	173.194.93.4	61962	140.112.3.82	53	DNS	100	Standard query 0xe36b A pC1.cc.bUDa.iDV.Tw OPT
3	0.067625	1	140.112.3.82	53	173.194.93.4	61962	DNS	168	Standard query response 0xe36b A pC1.cc.bUDa.iDV.Tw A 140.112.3.
4	0.072917	0	8.8.8.8	53	140.112.3.82	35179	DNS	94	Standard query response 0x0002 A pc1.cc.buda.idv.tw A 140.112.3.

Recursive_Interative_1_8.8.8.8.pcap

Iterative DNS Query

* No 2. 以此封包判斷 Resolver 是否支援 ECS

```
Domain Name System (query)
    Transaction ID: 0xe36b
  Flags: 0x0010 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...0 .... .... = Recursion desired: Don't do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...1 .... = Non-authenticated data: Acceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  Queries
    > pC1.cc.bUDa.iDV.Tw: type A, class IN
```

```
  Additional records
    <Root>: type OPT
      Name: <Root>
      Type: OPT (41)
      UDP payload size: 1400
      Higher bits in extended RCODE: 0x00
      EDNS0 version: 0
    > Z: 0x8000
      Data length: 11
    Option: CSUBNET - Client subnet
      Option Code: CSUBNET - Client subnet (8)
      Option Length: 7
      Option Data: 000118008c7003
      Family: IPv4 (1)
      Source Netmask: 24
      Scope Netmask: 0
      Client Subnet: 140.112.3.0
```

支援 EDNS Client Subnet

Iterative DNS Reply

* No 3

```
Domain Name System (response)
    Transaction ID: 0xe36b
  Flags: 0x8410 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .1.. .... .... = Authoritative: Server is an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...0 .... .... = Recursion desired: Don't do query recursively
      .... .... 0... .... = Recursion available: Server can't do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/autho
      .... .... ...1 .... = Non-authenticated data: Acceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 1
    Additional RRs: 2
  Queries
    > pC1.cc.bUDa.iDV.Tw: type A, class IN
  Answers
    > pc1.cc.buda.idv.tw: type A, class IN, addr 140.112.3.82
  Authoritative nameservers
    > cc.buda.idv.tw: type NS, class IN, ns ns1.cc.buda.idv.tw
  Additional records
    > ns1.cc.buda.idv.tw: type A, class IN, addr 140.112.3.82
    <Root>: type OPT
        Name: <Root>
        Type: OPT (41)
        UDP payload size: 1232
        Higher bits in extended RCODE: 0x00
        EDNS0 version: 0
      > Z: 0x8000
        Data length: 11
      Option: CSUBNET - Client subnet
          Option Code: CSUBNET - Client subnet (8)
          Option Length: 7
          Option Data: 000118008c7003
          Family: IPv4 (1)
          Source Netmask: 24
          Scope Netmask: 0
          Client Subnet: 140.112.3.0
```

Authoritative Server 僅需支援 EDNS 就可回應 EDNS Client Subnet 但不代表支援 ECS

DNS Resolver 168.95.1.1

```
> server 168.95.1.1
預設伺服器:  dns.hinet.net
Address:  168.95.1.1

> pc1.cc.buda.idv.tw
伺服器:  dns.hinet.net
Address:  168.95.1.1

未經授權的回答:
名稱:    pc1.cc.buda.idv.tw
Address:  140.112.3.82
```

No.	Time	udp.stream	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
1	0.000000	0	140.112.3.82	48628	168.95.1.1	53	DNS	78	Standard query 0x0005 A pc1.cc.buda.idv.tw
2	0.007197	1	61.220.8.21	46188	140.112.3.82	53	DNS	89	Standard query 0x4dca A pc1.cc.buda.idv.tw OPT
3	0.007415	1	140.112.3.82	53	61.220.8.21	46188	DNS	105	Standard query response 0x4dca A pc1.cc.buda.idv.tw A 140.112.3.82 OPT
4	0.008440	0	168.95.1.1	53	140.112.3.82	48628	DNS	94	Standard query response 0x0005 A pc1.cc.buda.idv.tw A 140.112.3.82

* Recursive_Interative_1_168.95.1.1.pcap

Iterative DNS Query/Reply

No 2.

```
▾ Domain Name System (query)
    Transaction ID: 0x4dca
  › Flags: 0x0010 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▾ Queries
    › pc1.cc.buda.idv.tw: type A, class IN
  ▾ Additional records
    ▾ <Root>: type OPT
        Name: <Root>
        Type: OPT (41)
        UDP payload size: 512
        Higher bits in extended RCODE: 0x00
        EDNS0 version: 0
      › Z: 0x8000
        Data length: 0
```

支援 **EDNS**
但不支援 **EDNS Client Subnet**

No3.

```
▾ Domain Name System (response)
    Transaction ID: 0x4dca
  › Flags: 0x8410 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 1
  ▾ Queries
    › pc1.cc.buda.idv.tw: type A, class IN
  ▾ Answers
    › pc1.cc.buda.idv.tw: type A, class IN, addr 140.112.3.82
  ▾ Additional records
    ▾ <Root>: type OPT
        Name: <Root>
        Type: OPT (41)
        UDP payload size: 1232
        Higher bits in extended RCODE: 0x00
        EDNS0 version: 0
      › Z: 0x8000
        Data length: 0
```

DNS Cache TTL(Time To Live)

DNS 記錄異動何時生效

DNS Cache TTL 依據 Authoritative DNS Server

* Record 有指定

  <name> [ttl] IN <type> <data>

  pc1 1800 IN A 140.112.2.200

* Record 無指定

  pc1 IN A 140.112.2.200

  * Priority 1: 依據 Zone File 設定

    $TTL 3600

  * Priority 2: 依據 SOA 設定

    @ IN SOA dns.fido.net. admin.fido.net. (2024102701 360000 3600 360000 3600)

補充: TTL 很短之 FQDN

~# dig resolver-identity.cloudfront.net

```
;; ANSWER SECTION:
resolver-identity.cloudfront.net. 10 IN A       140.112.3.82
```

DNS Cache TTL @User Client(Windows)

- Display cached DNS records
  - ipconfig /displaydns
- Clear cached DNS records
  - ipconfig /flushdns
- 有 Cache 作用
  - 指令: ping pc1.buda.idv.tw
- 無 Cache 作用
  - 指令: nslookup pc1.buda.idv.tw

DNS Cache TTL @User Client(Linux)

- no OS-level DNS caching on Linux
  - Ref. https://www.makeuseof.com/view-and-flush-dns-cache-on-linux/
- systemd-resolved: for Ubuntu

  ~# resolvectl show-cache

  ~# resolvectl flush-caches

  ~# resolvectl statistics
- nscd (name service caching daemon)

  ~# strings /var/cache/nscd/hosts | uniq

  ~# /etc/init.d/nscd restart
- dnsmasq

  ~# journalctl -u dnsmasq

  ~# systemctl restart dnsmasq

DNS Cache TTL @User Client(Linux)

* 有 Cache 作用
  * ping pc1.buda.idv.tw
  * dig a pc1.buda.idv.tw
  * dig a pc1.buda.idv.tw @127.0.0.54

```
root@ubuntu24-desktop:~# netstat -lnptu
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      792/systemd-resolve
tcp        0      0 127.0.0.54:53           0.0.0.0:*               LISTEN      792/systemd-resolve
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      120699/cupsd
tcp6       0      0 ::1:631                 :::*                    LISTEN      120699/cupsd
tcp6       0      0 :::22                   :::*                    LISTEN      1/init
udp        0      0 127.0.0.54:53           0.0.0.0:*                           792/systemd-resolve
udp        0      0 127.0.0.53:53           0.0.0.0:*                           792/systemd-resolve
udp        0      0 0.0.0.0:5353            0.0.0.0:*                           1033/avahi-daemon:
udp        0      0 0.0.0.0:42257           0.0.0.0:*                           1033/avahi-daemon:
udp6       0      0 :::37984                :::*                                1033/avahi-daemon:
udp6       0      0 :::5353                 :::*                                1033/avahi-daemon:
```

* 無 Cache 作用
  * dig a pc1.buda.idv.tw @8.8.8.8

DNS Cache TTL @DNS Resolver

- Linux

  ~# dig a pc1.buda.idv.tw @140.112.254.4

```
;; ANSWER SECTION:
pc1.buda.idv.tw.        1800    IN      A       140.112.2.200
```

```
;; ANSWER SECTION:
pc1.buda.idv.tw.        1794    IN      A       140.112.2.200
```

```
;; ANSWER SECTION:
pc1.buda.idv.tw.        1669    IN      A       140.112.2.200
```

- Windows

  nslookup -debug pc1.buda.idv.tw 140.112.254.4

```
------------
伺服器:  dns.ntu.edu.tw
Address:  140.112.254.4

------------
Got answer:
    HEADER:
        opcode = QUERY, id = 2, rcode = NOERROR
        header flags:  response, want recursion, recursion avail.
        questions = 1,  answers = 1,  authority records = 0,  additional = 0

    QUESTIONS:
        pc1.buda.idv.tw, type = A, class = IN
    ANSWERS:
    ->  pc1.buda.idv.tw
        internet address = 140.112.2.200
        ttl = 1800 (30 mins)
```

DNS Cache TTL
DNS 異動生效時間

* 最長生效時間: TTL 設定時間
  * 無任何清除 Cache 動作
* 最短生效時間: 立即
  * When DNS Resolver , User Client 之前都未有此筆記錄之查詢記錄(無 Cache)
* Best Practice for DNS 記錄異動
  * 異動前建議先縮短 TTL (例. 60秒)

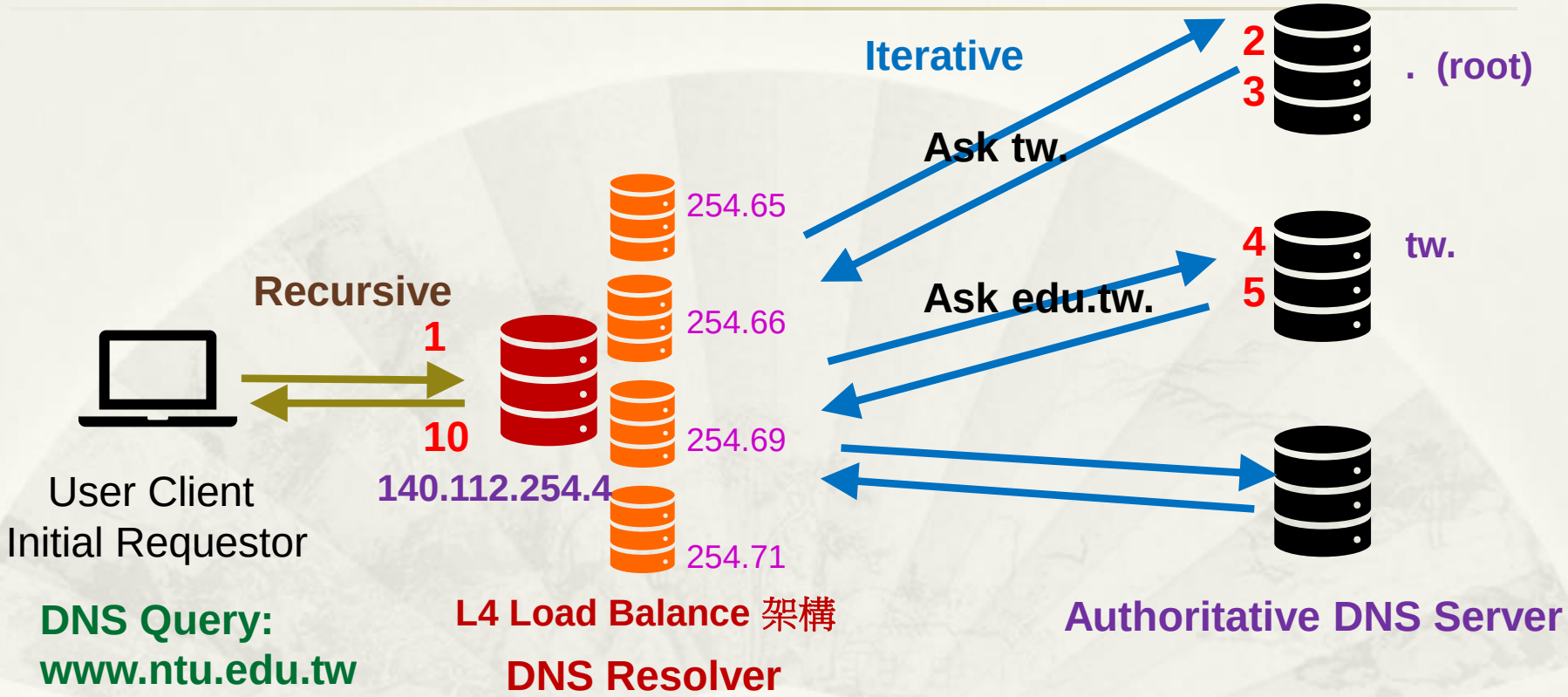
pc1 60 IN A 140.112.2.200

如何測試 DNS Resolver 實際有幾台 Servers？

168.95.1.1

8.8.8.8

台大 DNS Resolver IP 架構



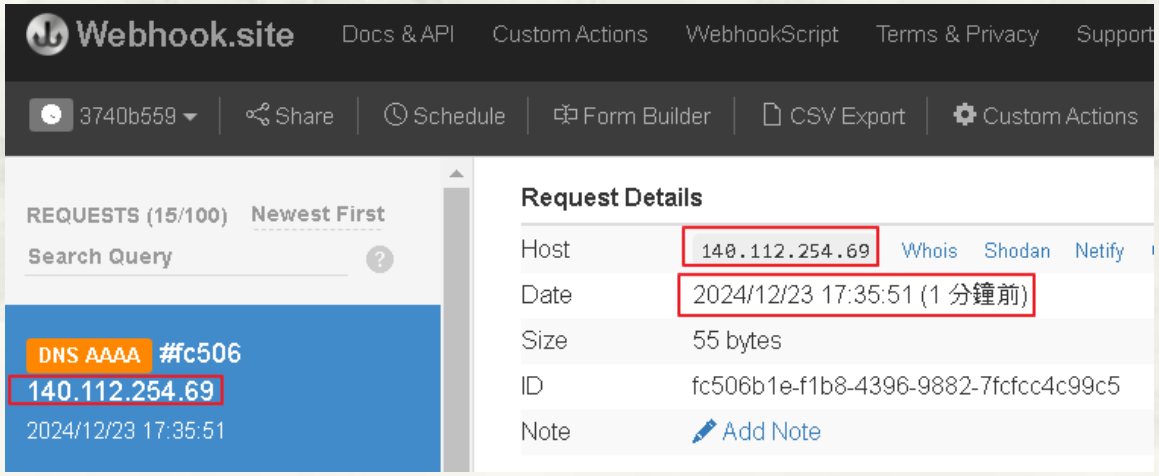
HiNet 168.95.1.1
Google 8.8.8.8
架構同上

如何測試 DNS Resolver 實際有幾台 Server？

- 方法1: 利用 dns callback online, dnslog platform 服務
  - 使用新註冊之 A record 來觀察詢問之 Resolver IP
- 方法2: DNS Authoritative Server 提供查詢特定 Domain，可顯示 Resolver IP
  - Amazon CloudFront 提供 resolver-identity.cloudfront.net
- 方法3: 觀察 DNS Record Cache TTL
  - 依據 DNS Cache TTL 規範，第一次詢問後就會 Cache 直到時間結束，才會刪除該筆記錄
  - 觀察共有幾種不同的 Cache TTL 時間，即表示有幾台 Server

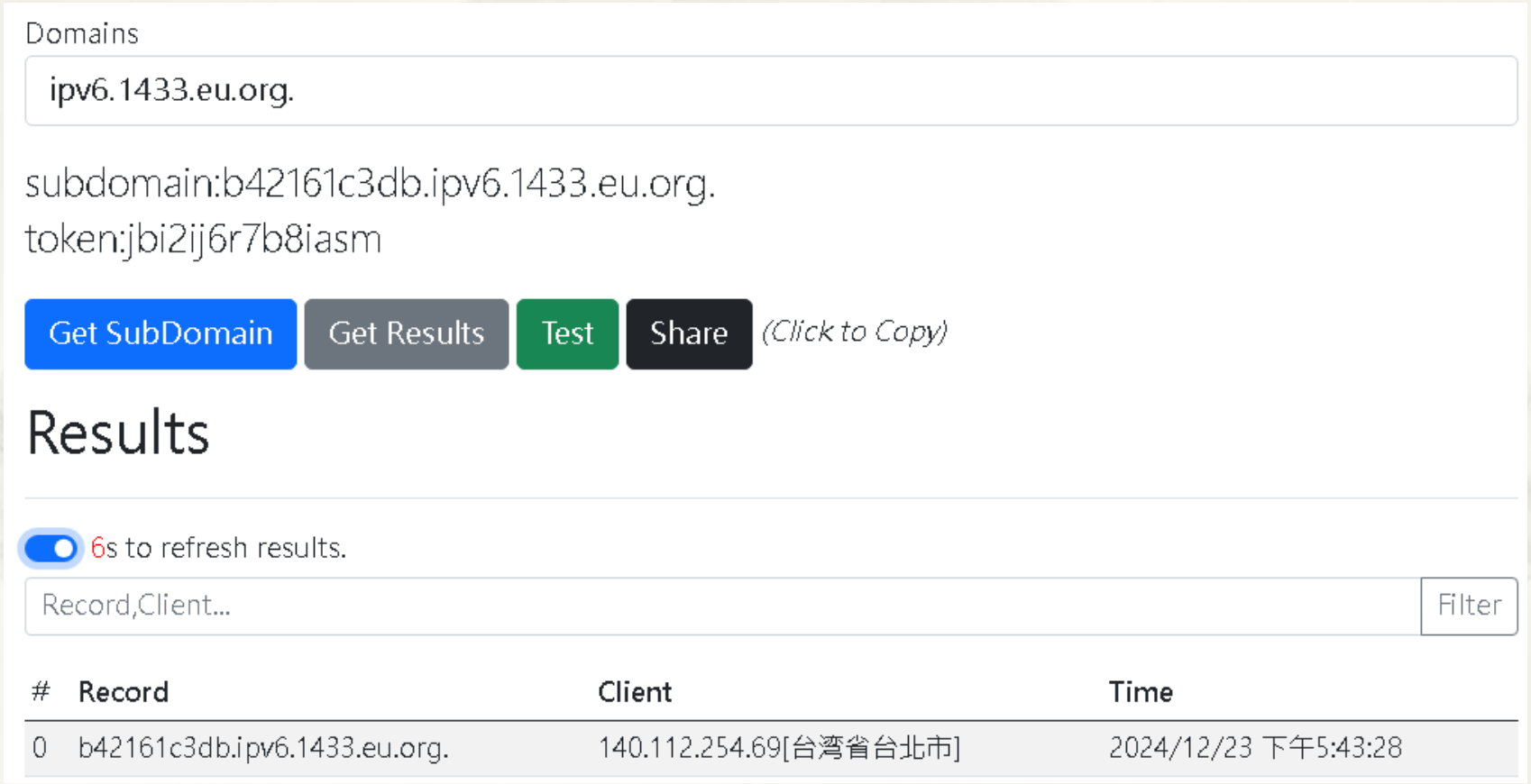
方法1: dns callback online, dnslog platform

* Google 搜尋 “dns callback online” or “dnslog platform”
* https://webhook.site/
  * nslookup 3740b559-92c4-4fa3-9a59-b0d709e63334.dnshook.site 140.112.254.4
  * 缺點: 8.8.8.8 不支援



方法1: dns callback online, dnslog platform

* https://dig.pm/



方法2: DNS Authoritative Server 提供查詢特定 Domain，可顯示 Resolver IP

* dig a resolver-identity.cloudfront.net @140.112.254.4

```
root@ubuntu24-desktop:~# dig a resolver-identity.cloudfront.net @140.112.254.4

; <<>> DiG 9.18.28-0ubuntu0.24.04.1-Ubuntu <<>> a resolver-identity.cloudfront.net @140.112.254.4
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55876
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 18c4a8528d4f9310010000006769305fc2972e63f7b55995 (good)
;; QUESTION SECTION:
;resolver-identity.cloudfront.net. IN   A

;; ANSWER SECTION:
resolver-identity.cloudfront.net. 5 IN  A       140.112.254.71
```

```
;; ANSWER SECTION:
resolver-identity.cloudfront.net. 10 IN A       140.112.254.65
```

```
;; ANSWER SECTION:
resolver-identity.cloudfront.net. 10 IN A       140.112.254.66
```

```
;; ANSWER SECTION:
resolver-identity.cloudfront.net. 6 IN  A       140.112.254.69
```

方法2: DNS Authoritative Server 提供查詢特定 Domain，可顯示 Resolver IP

* dig a resolver-identity.cloudfront.net @8.8.8.8
* dig a resolver-identity.cloudfront.net @168.95.1.1

* 缺點
  * 8.8.8.8、168.95.1.1 偶而不回應

方法3: Record Cache TTL

- Linux
  - ~# dig a pc1.buda.idv.tw @140.112.254.4

```
;; ANSWER SECTION:
pc1.buda.idv.tw.        1800    IN      A       140.112.2.200
```

- Windows
  - nslookup -debug pc1.buda.idv.tw 140.112.254.4

```
------------
伺服器:  dns.ntu.edu.tw
Address:  140.112.254.4

------------
Got answer:
    HEADER:
        opcode = QUERY, id = 2, rcode = NOERROR
        header flags:  response, want recursion, recursion avail.
        questions = 1,  answers = 1,  authority records = 0,  additional = 0

    QUESTIONS:
        pc1.buda.idv.tw, type = A, class = IN
    ANSWERS:
    ->  pc1.buda.idv.tw
        internet address = 140.112.2.200
        ttl = 1800 (30 mins)
```

簡報完畢
謝謝