

# 破解 IPv6 隱私設計 之實作管理經驗

國立暨南國際大學/南投區網中心

張瑛杰

# 為什麼要破解!?

有何必要...?

都是要從這一個故事開始



# 台灣學術網路TANet IPv6推動服務計畫

國立暨南國際大學/南投區網中心

報告人：張瑛杰

# 報告大綱

1. 難以推動的原因
2. 建議推動方式
3. 檢討數據統計的效益
4. 建議 IPv6 整合資訊方向
5. 適用於國中小的 IPv6 數據收集方式



# 專家學者 - 難以推動的原因

1. 校內各系所單位自行管理網路
2. 擔憂不可預期的問題，造成管理的困難度增加
3. RFC4941 – 難以掌握使用足跡
4. 部分舊系統龐大，修改程式仍為浩大工程
5. 基於資訊安全的考量，避免造成校園網路的風險
6. IPv6攻擊造成資訊安全設備異常紀錄
7. 校園具備 Class B，IPv4 IP address 數量充足



# 南投區網連線單位 - 難以推動的原因

1. 並非相關科系老師，對於資訊相關管理**無法掌握**
2. 學校沒有簽維護合約，**沒有廠商**協助
3. 學校配合廠商**沒有 IPv6 相關知識**
4. 增加管理上的**複雜**，造成意願低落
5. 校園僅讓**部分電腦**連上學網，因此不須推動IPv6
6. 校園**人數過少**，少於254個設備上網，不須使用 IPv6
7. 校園網路管理**規則嚴格**，減少資訊安全風險
8. 私校**未受**前瞻計畫**補助**，無相關經費更新設備



# 建議推動方式

長久以來，教育部積極推廣和宣導 IPv6  
但是依舊有許多難以推動的困難

## 建議推動方式

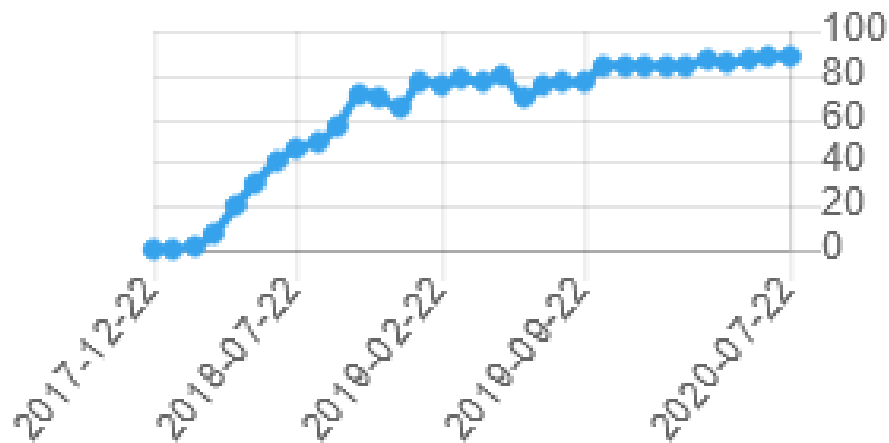
1. 軟體、硬體和資安環境皆有支援
2. 請網路管理者協助落實 IPv6 服務的啟用



# APNIC 數據統計的問題

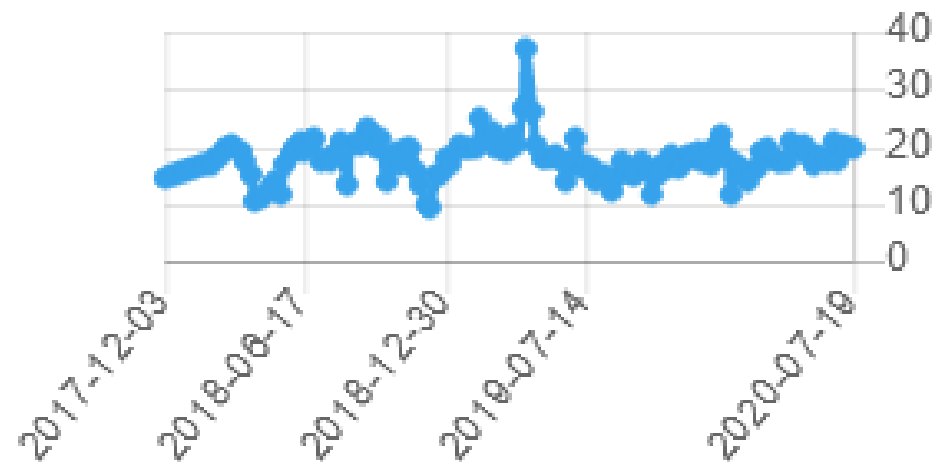
中華電信(行網) CHT Mobile

IPv6比例：87.83%



教育部 TANet

IPv6比例：19.44%



APNIC 針對全球進行IPv6 排名，雖然我國名列第8名  
但依據數據顯示台灣學術網路的 IPv6 連線比例僅為 19.44%  
相較於電信商高達 60~80% 有明顯落差





# 計算基礎 / 實務管理 的矛盾

## 計算基礎

- TWNIC 指出 APNIC 計算 IPv6 連線統計是**以一個 /64 為單位**

## 實務管理

- TANET 連線單位**不會發給每個使用者一個 /64**



# 計算基礎 / 實務管理 的矛盾

舉例：以暨南大學無線網路使用網段為例

Vlan 105

10.105.0.0/16

2001:e10:6840:105::/64

IPv6 IP address 顯示紀錄如下

2001:e10:6840:105:acd3:8129:167b:30f1

2001:e10:6840:105:b8db:6828:1f42:5ee2

...

...

06/28 共計 **2811**筆

假設這些 IP address 連線到 APNIC統計網站上，只會算成 **1** 筆



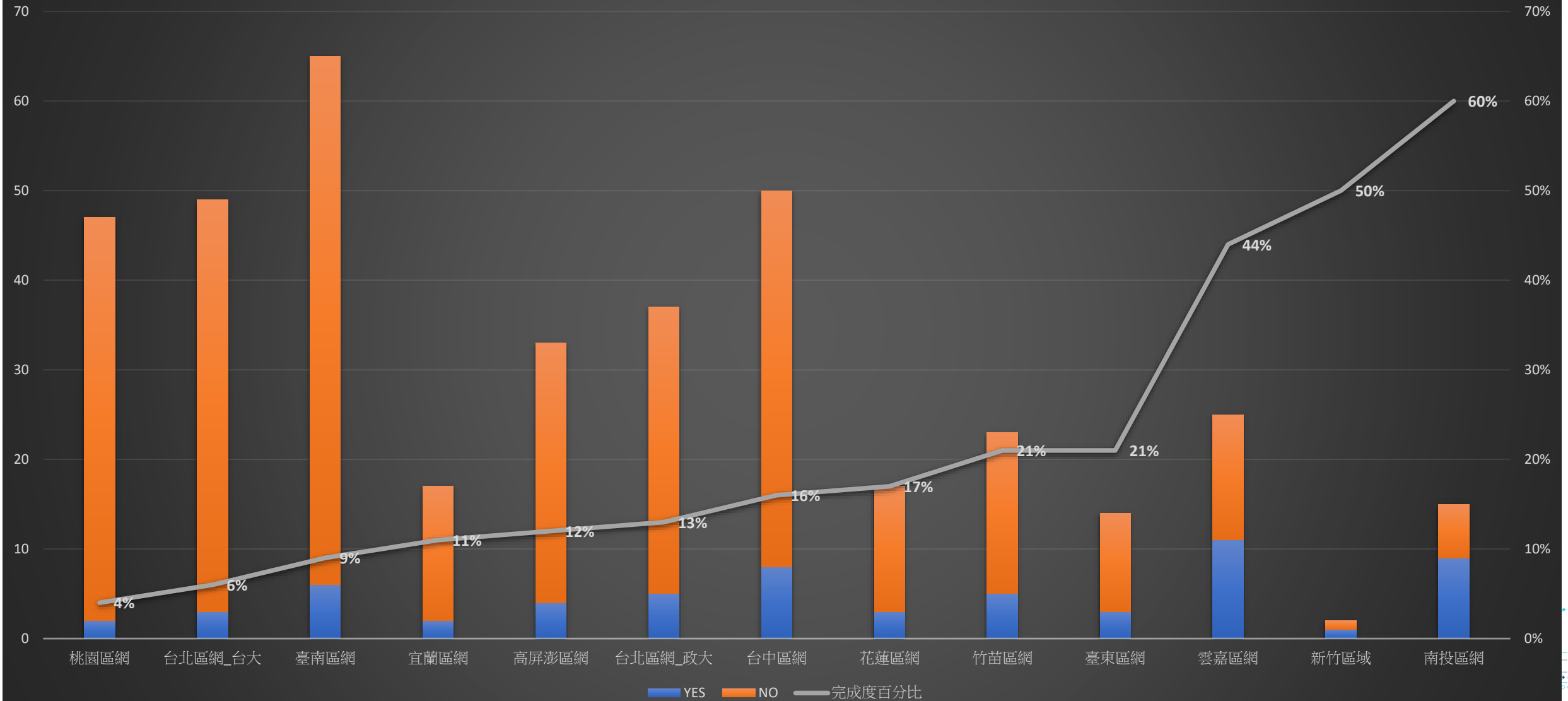
# 實測 網頁 IPv6 連線支援程度

參考 TWNIC 輔導政府單位升級IPv6 計畫

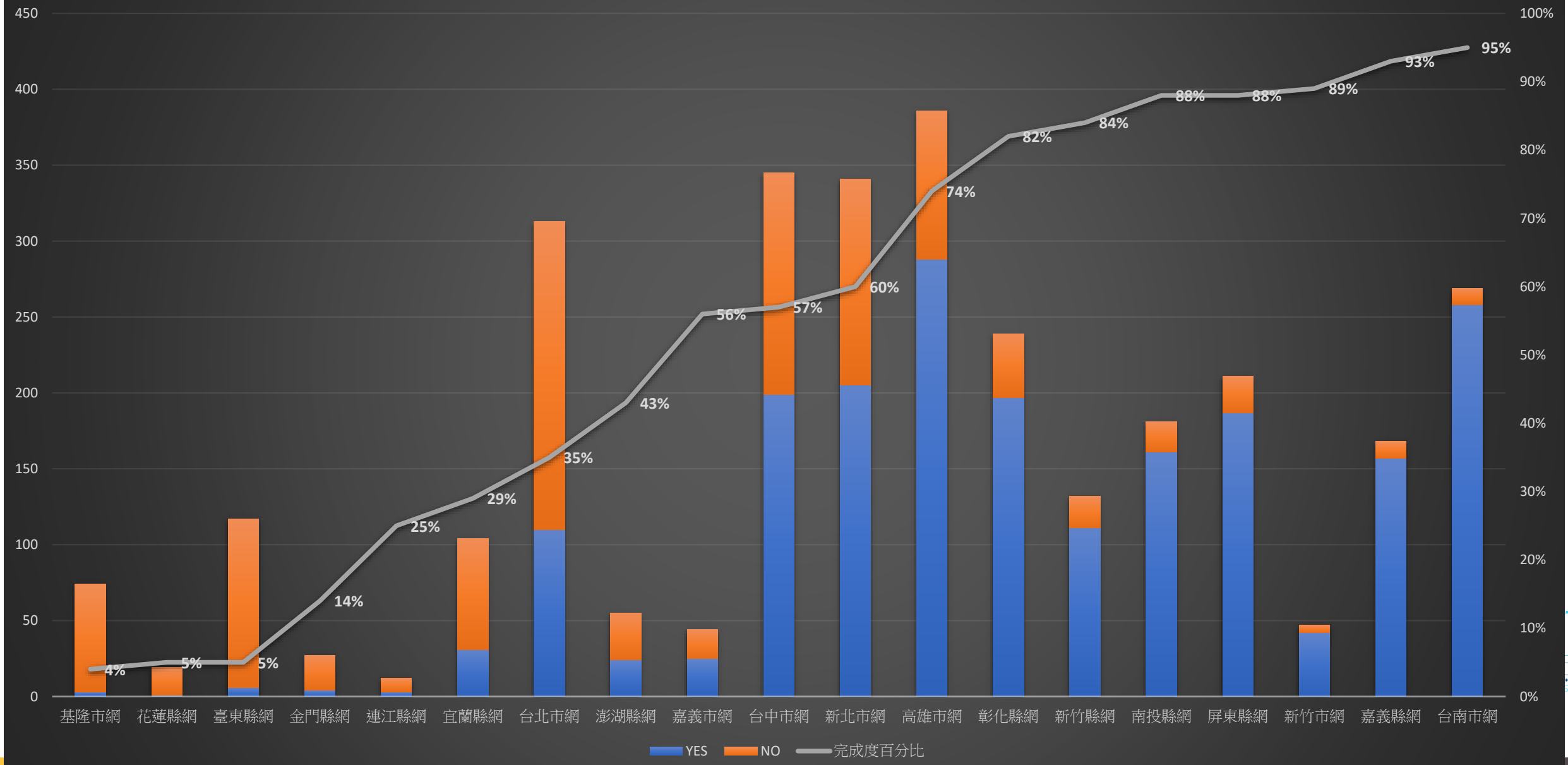
1. 區網中心連線單位 Web Server是否支援IPv6 連線
2. 縣市網路中心連線單位 Web Server是否支援IPv6 連線



### 區網中心連線單位 Web Server是否支援IPv6 連線



# 縣市網路中心連線單位 Web Server是否支援IPv6 連線



# 建議 IPv6 整合資訊方向

IPv6 是一個**技術環節**，並非一個特定服務項目

因此**需要配合TANet 各項服務進行**

包括：重要IPv6 資訊安全案例分享，有效降低不安全感  
DNS、網頁向上集中加強 IPv6 的連線服務  
鼓勵無線網路漫遊單位提供Dual-Stack 使用環境



# 連線單位的管理困擾

依據本計畫訪談經驗，要讓TANet IPv6 更加普及

各連線單位都必須收集 IPv6 IP address / MAC 的對照資訊

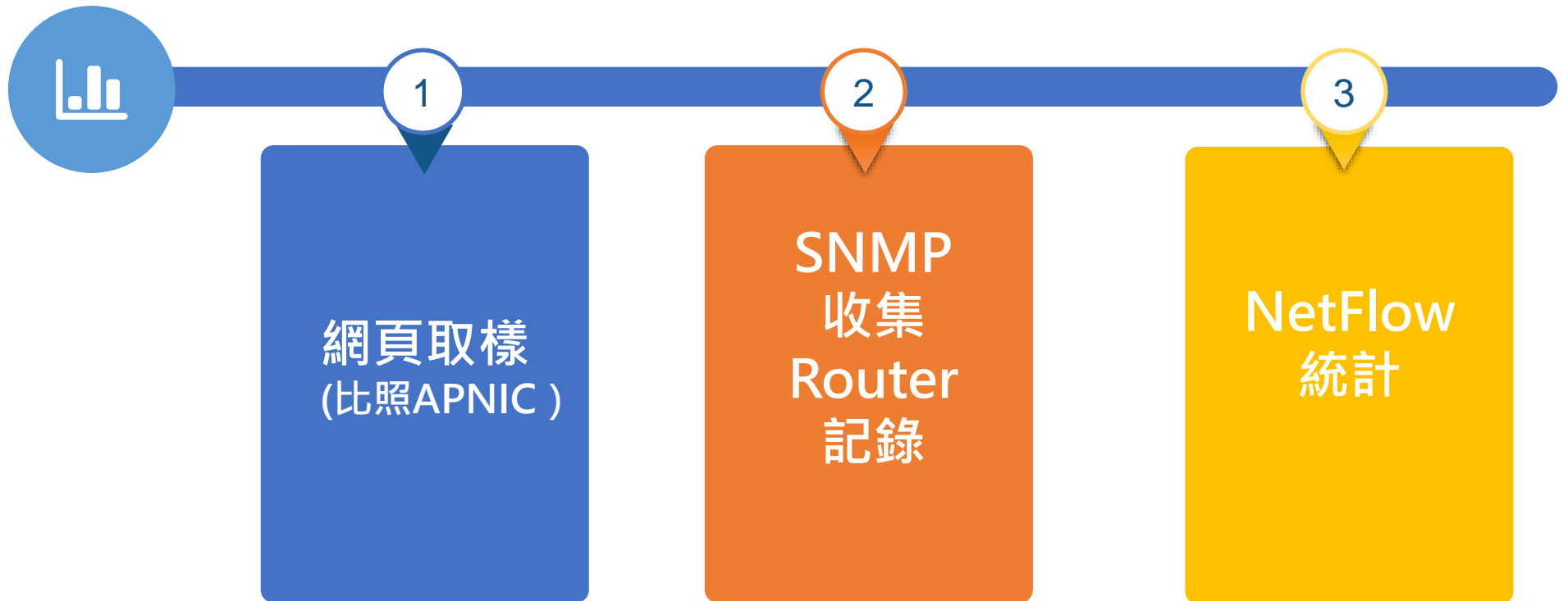
於先前計畫中提出三種方式進行不同資料收集方式



透過 SNMP 收集紀錄的方式是高度普遍的，但有其缺點

收集頻率過慢導致資料**無法全數收集**，收集頻率過快導致設備**負載過高**

**不是技術門檻較高，就是要花比較多經費達成**





# 適用於 國中小的 IPv6 數據收集方式

IPv6 並不像 IPv4 可以透過 DHCP 記錄卡號管理

管理者難以追查使用情境

常見的解決方式：SNMP 收集 Router 記錄

但會有 時間差 和 設備負載 問題

本校依據 IPv6 multicast 運作流程與機制

建置一個 低成本、低技術、低耗源 的

IPv6 IP address / MAC 的 紀錄收集與查詢 系統

已經在 國立暨南國際大學 校內完成測試和驗證

後續，完整建置和操作流程會以文件方式說明





# 委員建議 還是要想辦法解決

...該怎麼辦...

# 教育部 IPv6 分配說明

依照 TANet IPv6位址分配原則

第5點 每一連線單位或學校，核發給Prefix /48

以暨南大學來說 分配到 2001:288:C001::/48

代表校內可使用 65536 的/64網段

現況是，暨南大學校內共有 87個 Vlan，全數都有支援 Dual-stack

例如：

Vlan4	163.22.4.0/24	10.4.0.0/16	2001:288:C001:4::/64 (行政大樓)
Vlan7	163.22.7.0/24	10.7.0.0/16	2001:288:C001:7::/64 (圖書館)
Vlan9	163.22.9.0/24	10.9.0.0/16	2001:288:C001:9::/64 (行政大樓)

...

依照規劃，全校僅使用 87個 IPv6 /64 網段，仍有相當充裕的 /64 IPv6 網段可做規劃

# APNIC 判斷統計量的問題

要增加 TANET 在 APNIC 的 IPv6 使用率

唯一辦法是讓使用者使用 “前64 bit 是不相同的 IPv6 IP address” 做連線

困難點：

就算暨南大學全校都有支援 Dual-stack

高達上萬個 IPv6 IP address，但僅使用 87個 IPv6 /64 網段

因此全校 “前64 bit 是不相同的 IPv6 IP address” 只有 87組

落差太大，導致無法提升 APNIC 統計量

# 解決辦法

每一連線單位或學校，由核發Prefix /48 改為 Prefix /32

讓校內各網段由 都分配一段 /64 改為 /48

例如：以暨南大學來說 分配到 2001:288:C001::/48 -- > 改為 2001:288::/32

Vlan4 2001:288:C001:4::/64 (行政大樓) -- > 改為 2001:288:4::/48

因此同一個 Vlan 下就可能產生 65536 個 “前64 bit 是不相同的 IPv6 IP address” 的組合

例如

2001:0288:0004:1111:0000:0000:0000:000a/48

2001:0288:0004:2222:0000:0000:0000:000a/48

2001:0288:0004:3333:0000:0000:0000:000a/48

....

# 在現有資源下努力？

依照 TANet IPv6位址分配原則

第5點 每一連線單位或學校，核發給Prefix /48

一個連線單位或學校

頂多產生 65536 個 “前64 bit 是不相同的 IPv6 IP address” 的組合

**假設 Router 可以設定**

如果一個 Vlan 底下有2000~3000個設備，就要加入 3000個以上的 Prefix /64 網段 在同Vlan

還要搭配 DHCP Server 發放 IP address

**勢必會產生極大量的 ICMPv6 封包交換和複雜的設定**

**這聽起來不妥善**

# 越簡單越好

基本方案作法解說



# 資安通報

## 資安通報內容分類

1. Time
2. Source IPv4 / IPv6 address
3. Destination IPv4 / IPv6 address
4. Event

要查出校內的攻擊者

必須要有 log 可供查詢



# 紀錄 - 對照表

1. IP / MAC
2. NAT - Public / Private
3. MAC address / Switch port

# 假設有一天發生這件事情

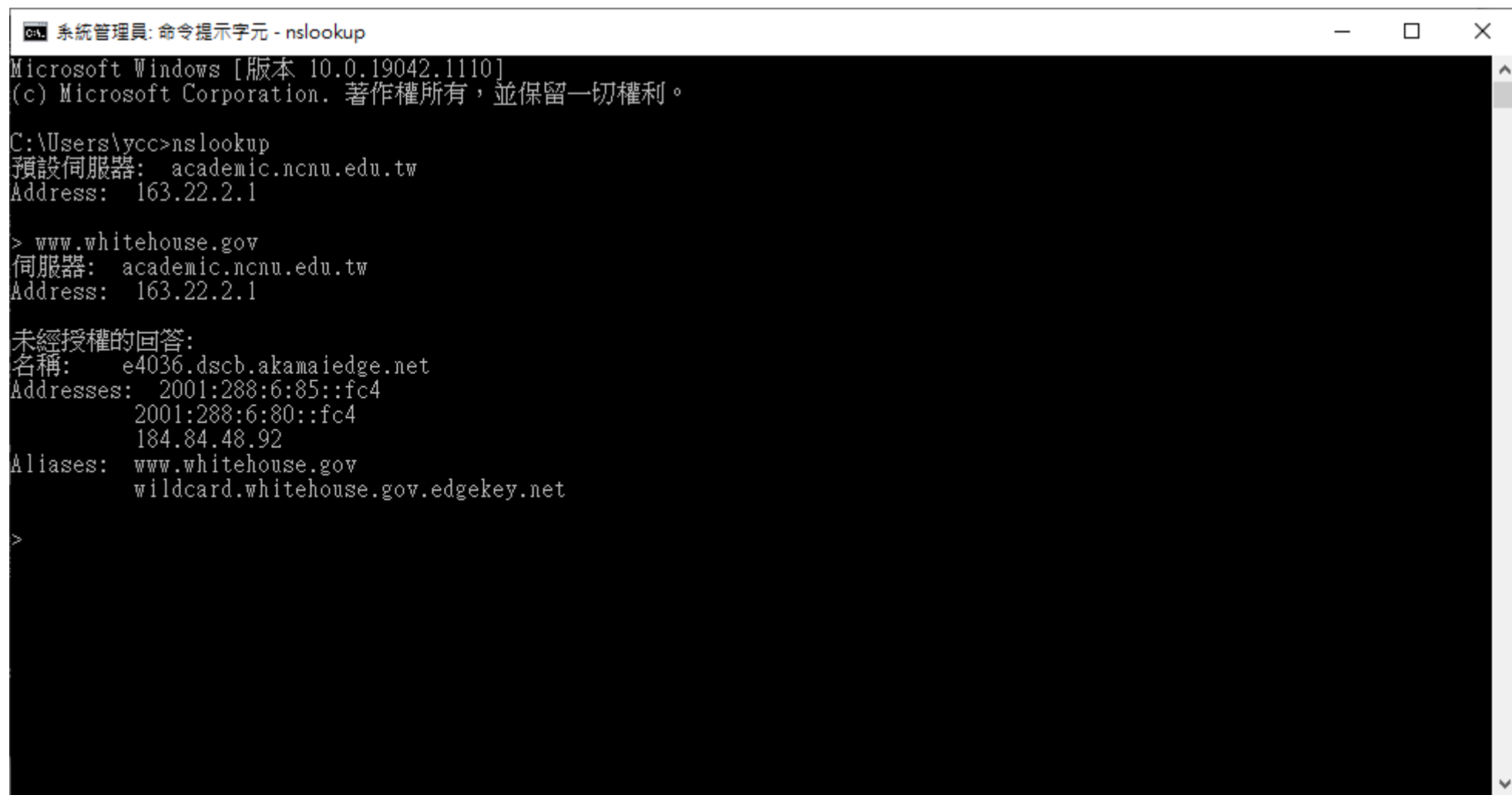
有人攻擊了美國白宮網站

# 舉例：再次強調，這是舉例

2021/08/10 14:10 由 163.22.18.4 連線至白宮網站

1. 先確定是否屬於 NAT 網段
2. 攻擊者：163.22.18.4
3. 被攻擊者：白宮網站 IP address
4. 發生時間：2021/08/10 14:10

# 步驟一：查詢 白宮網站 資訊



```
GA 系統管理員: 命令提示字元 - nslookup
Microsoft Windows [版本 10.0.19042.1110]
(c) Microsoft Corporation. 著作權所有，並保留一切權利。

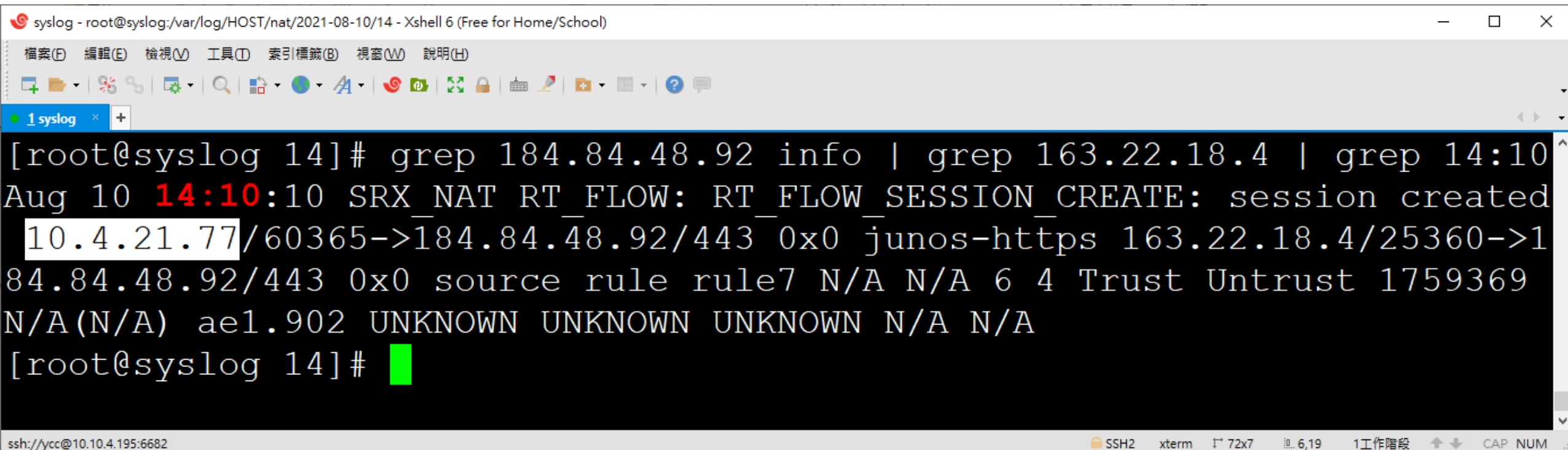
C:\Users\ycc>nslookup
預設伺服器: academic.ncnu.edu.tw
Address: 163.22.2.1

> www.whitehouse.gov
伺服器: academic.ncnu.edu.tw
Address: 163.22.2.1

未經授權的回答:
名稱: e4036.dscb.akamaiedge.net
Addresses: 2001:288:6:85::fc4
           2001:288:6:80::fc4
           184.84.48.92
Aliases: www.whitehouse.gov
         wildcard.whitehouse.gov.edgekey.net

>
```

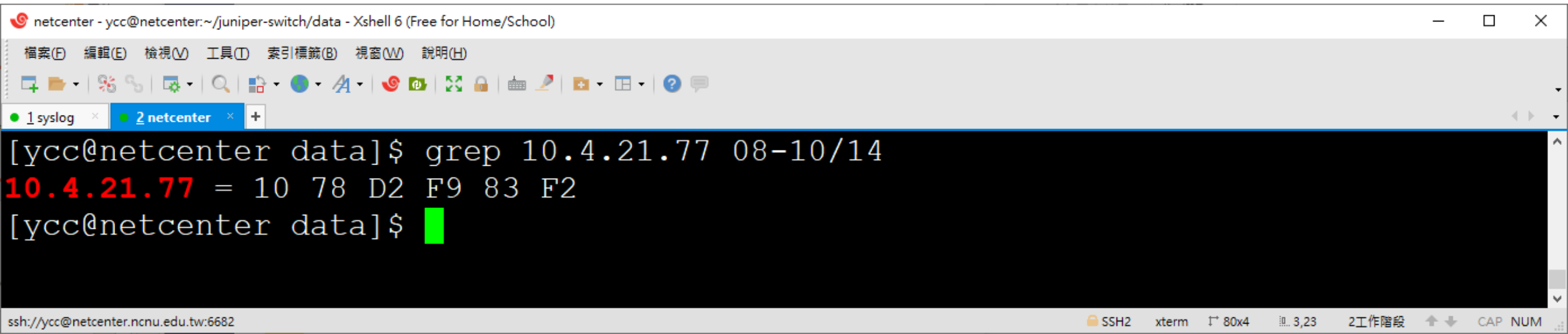
## 步驟二：NAT 對照表



```
syslog - root@syslog:/var/log/HOST/nat/2021-08-10/14 - Xshell 6 (Free for Home/School)
檔案(F) 編輯(E) 檢視(V) 工具(T) 索引標籤(B) 視窗(W) 說明(H)
1 syslog x +
[root@syslog 14]# grep 184.84.48.92 info | grep 163.22.18.4 | grep 14:10
Aug 10 14:10:10 SRX_NAT RT_FLOW: RT_FLOW_SESSION_CREATE: session created
10.4.21.77/60365->184.84.48.92/443 0x0 junos-https 163.22.18.4/25360->1
84.84.48.92/443 0x0 source rule rule7 N/A N/A 6 4 Trust Untrust 1759369
N/A(N/A) ae1.902 UNKNOWN UNKNOWN UNKNOWN N/A N/A
[root@syslog 14]#
```

ssh://ycc@10.10.4.195:6682 SSH2 xterm 72x7 6,19 1工作階段 CAP NUM

# 步驟三：SNMP LOG 查詢 IP / MAC



```
netcenter - ycc@netcenter:~/juniper-switch/data - Xshell 6 (Free for Home/School)
檔案(F) 編輯(E) 檢視(V) 工具(T) 索引標籤(B) 視窗(W) 說明(H)
1 syslog x 2 netcenter x +
[ycc@netcenter data]$ grep 10.4.21.77 08-10/14
10.4.21.77 = 10 78 D2 F9 83 F2
[ycc@netcenter data]$
```

ssh://ycc@netcenter.ncnu.edu.tw:6682 SSH2 xterm 80x4 3,23 2工作階段 CAP NUM

查出 IPv4 IP address 和 MAC 的方式

# 步驟三：DHCP LOG 查詢 IP / MAC

```
[root@dhcp2 ~]# cat /var/log/dhcpd|grep "10.4.21.77"
Aug 10 09:19:22 dhcp2 dhcpd: DHCPREQUEST for 10.4.21.77 from 10:78:d2:f9:83:f2 (DESKTOP-I8KVP72) via ens192
Aug 10 09:19:22 dhcp2 dhcpd: DHCPACK on 10.4.21.77 to 10:78:d2:f9:83:f2 (DESKTOP-I8KVP72) via ens192
Aug 10 10:56:03 dhcp2 dhcpd: DHCPREQUEST for 10.4.21.77 from 10:78:d2:f9:83:f2 (DESKTOP-I8KVP72) via 163.22.4.252
Aug 10 10:56:03 dhcp2 dhcpd: DHCPACK on 10.4.21.77 to 10:78:d2:f9:83:f2 (DESKTOP-I8KVP72) via 163.22.4.252
Aug 10 10:56:03 dhcp2 dhcpd: DHCPREQUEST for 10.4.21.77 from 10:78:d2:f9:83:f2 (DESKTOP-I8KVP72) via 163.22.4.253
Aug 10 10:56:03 dhcp2 dhcpd: DHCPACK on 10.4.21.77 to 10:78:d2:f9:83:f2 (DESKTOP-I8KVP72) via 163.22.4.253
```

```
lease 10.4.21.77 {
    starts 2 2021/08/10 02:56:03;
    ends 3 2021/08/11 02:56:03;
    cltt 2 2021/08/10 02:56:03;
    binding state active;
    next binding state free;
    hardware ethernet 10:78:d2:f9:83:f2;
    uid "\001\020x\322\371\203\362";
    client-hostname "DESKTOP-I8KVP72";
}
```

查出 IPv4 IP address 和 MAC 的方式

# DHCPv6 沒有 MAC 資訊

沒有 MAC 資訊，無法輕易查詢

**DUID - DHCP Unique Identifiers**

DHCPv6 唯一識別碼

用於客戶端從DHCPv6伺服器獲得IP位址



# 步驟四：使用者端驗證

```
GA 系統管理員: 命令提示字元
乙太網路卡 乙太網路 2:
連線特定 DNS 尾碼 . . . . . : nctu.edu.tw
描述 . . . . . : Intel(R) 82578DC Gigabit Network Connection
實體位址 . . . . . : 10-78-D2-F9-83-F2
DHCP 已啟用 . . . . . : 是
自動設定啟用 . . . . . : 是
IPv4 位址 . . . . . : 10.4.21.77(偏好選項)
子網路遮罩 . . . . . : 255.255.0.0
租用取得 . . . . . : 2021年8月10日 上午 10:56:04
租用到期 . . . . . : 2021年8月11日 上午 10:56:03
預設閘道 . . . . . : 10.4.1.254
DHCP 伺服器 . . . . . : 163.22.3.8
DNS 伺服器 . . . . . : 163.22.2.1
                           163.22.2.2
                           168.95.1.1
主要 WINS 伺服器 . . . . . : 10.6.8.31
次要 WINS 伺服器 . . . . . : 10.6.8.30
NetBIOS over Tcpip . . . . . : 啟用

乙太網路卡 乙太網路 3:
媒體狀態 . . . . . : 媒體已中斷連線
連線特定 DNS 尾碼 . . . . . :
描述 . . . . . : TAP-Windows Adapter V9
實體位址 . . . . . : 00-FF-FE-1A-1E-1E
DHCP 已啟用 . . . . . : 是
自動設定啟用 . . . . . : 是

C:\Users\ycc>
```

1. 如何收集 IPv4 arp table 和 IPv6 neighbor
2. 實作 - 使用 SNMP 記錄 IPv4 arp table
3. 實作 - 使用 SNMP 記錄 IPv6 neighbor
4. IPv6 IP address 的發放方式說明與比較
5. 挑選最適合 TANet 的 IPv6 IP address 的管理方式
6. 為什麼資安通報難以查詢 IPv6 真正的使用者
7. 回歸 IPv6 運作與設計原理
8. 如何使用 Wireshark 查看和紀錄 IPv6 封包
9. 如何使用 Tshark 查看和紀錄 IPv6 封包
10. 破解 IPv6 隱私設計的實作流程說明

# IPv4 arp table 和 IPv6 neighbor

如何收集

ycc@NCNU-EX9251-1&gt; show arp

MAC	Address	Address	Name	Interface	Flags
00		bb 10	10	irb.4 [ae17.0]	none
00		2b 10	10	irb.4 [ae17.0]	none
00		bc 10	01 10	irb.4 [ae17.0]	none
00		41 10	02 10	irb.4 [ae17.0]	none
00		e6 10	03 10	irb.4 [ae17.0]	none
00		bc 10	04 10	irb.4 [ae17.0]	none
00		c9 10	05 10	irb.4 [ae17.0]	none
00		f6 10	06 10	irb.4 [ae17.0]	none
00		98 10	07 10	irb.4 [ae17.0]	none
00		21 10	08 10	irb.4 [ae17.0]	none
00		6d 10	09 10	irb.4 [ae17.0]	none
40		ad 10	05 10	irb.4 [ae17.0]	none
40		ac 10	06 10	irb.4 [ae17.0]	none
40		55 10	07 10	irb.4 [ae17.0]	none
40		8f 10	08 10	irb.4 [ae17.0]	none
40		72 10	09 10	irb.4 [ae17.0]	none
cc		30 10	03 10	irb.4 [ae0.0]	permanent remote
1c		71 10	10	irb.4 [ae17.0]	none
3c		c3 10	10	irb.4 [ae17.0]	none
00		d2 10	10	irb.4 [ae17.0]	none
00		42 10	02 10	irb.4 [ae17.0]	none
00		19 10	03 10	irb.4 [ae17.0]	none
00		f4 10	09 10	irb.4 [ae17.0]	none
00		7f 10	01 10	irb.4 [ae17.0]	none
b8		2b 10	07 10	irb.4 [ae17.0]	none
00		16 10	09 10	irb.4 [ae17.0]	none
00		81 10	00 10	irb.4 [ae17.0]	none
00		65 10	01 10	irb.4 [ae17.0]	none
00		eb 10	02 10	irb.4 [ae17.0]	none
00		42 10	03 10	irb.4 [ae17.0]	none

ycc@NCNU-EX9251-1&gt; show ipv6 neighbors

IPv6 Address	Linklayer Address	Address	State	Exp	Rtr	Secure	Interface	
2001::e:45d2	00	a0	stale	531	no	no	irb.9 [ae12.0]	
2001:2	3	cc	30	reachable	0	no	no	irb.91 [ae0.0]
2001:e	cc	30	reachable	0	no	no	irb.2 [ae0.0]	
2001:e	00	ec	stale	931	no	no	irb.2 [ae17.0]	
2001:e	00	05	stale	583	no	no	irb.2 [ae17.0]	
2001:e	00	03	stale	1109	no	no	irb.2 [ae17.0]	
2001:e	00	ea	stale	763	yes	no	irb.2 [ae17.0]	
2001:e	00	a9	stale	682	yes	no	irb.2 [ae17.0]	
2001:e	:95ff:fe04	00	ec	stale	994	no	no	irb.2 [ae17.0]
2001:e	:56ff:fe8b	00	93	stale	23	no	no	irb.2 [ae17.0]
2001:e	:56ff:fe8b	00	f0	stale	359	no	no	irb.2 [ae17.0]
2001:e	:56ff:fe94	00	d4	stale	1188	no	no	irb.2 [ae17.0]
2001:e	:56ff:fe9c	00	ca	stale	606	no	no	irb.2 [ae17.0]
2001:e	5:52f8:22c	00	f8	stale	874	no	no	irb.2 [ae17.0]
2001:e	4:b40f:565	00	25	stale	175	no	no	irb.2 [ae17.0]
2001:e	cc	30	reachable	0	no	no	irb.3 [ae0.0]	
2001:e	00	82	stale	376	no	no	irb.3 [ae17.0]	
2001:e	:56ff:fe8b	00	26	stale	496	no	no	irb.3 [ae17.0]
2001:e	:56ff:fe9c	00	14	stale	578	no	no	irb.3 [ae17.0]
2001:e	:56ff:fe9c	00	af	stale	125	no	no	irb.3 [ae17.0]
2001:e	f:6bff:fe1	ac	cf	stale	713	no	no	irb.3 [ae17.0]
2001:e	cc	30	reachable	0	no	no	irb.4 [ae0.0]	
2001:e	00	7f	stale	774	no	no	irb.4 [ae17.0]	
2001:e	00	56	stale	940	no	no	irb.4 [ae17.0]	
2001:e	00	a4	stale	314	no	no	irb.4 [ae17.0]	
2001:e	00	5d	stale	568	no	no	irb.4 [ae17.0]	
2001:e	7	00	56	stale	673	no	no	irb.4 [ae17.0]
2001:e	01	00	7f	stale	817	no	no	irb.4 [ae17.0]
2001:e	02	00	7f	stale	224	no	no	irb.4 [ae17.0]
2001:e	03	00	7f	stale	369	no	no	irb.4 [ae17.0]

# 實作 - 使用 SNMP 記錄

如何收集

# SNMP

簡單網路管理協定

Simple Network Management Protocol

由 IETF (Internet Engineering Task Force) 所定義

用以管理網路設備之通訊協定

# SNMP 可收集資訊

1. 監控裝置正常運行時間 (sysUpTimeInstance)
2. 作業系統版本清單 (sysDescr)
3. 收集介面資訊 (ifName, ifDescr, ifSpeed, ifType, ifPhysAddr)
4. 測量網路介面吞吐量 (ifInOctets, ifOutOctets)
5. 查詢遠端ARP快取 (ipNetToMedia)



# CentOS8 - SNMP 安裝流程一

```
dnf update
```

安裝 CentOS8 系統後，執行更新

```
dnf install net-snmp net-snmp-libs net-snmp-utils
```

安裝 SNMP 相關套件

```
systemctl enable --now snmpd
```

允許開機後啟用 SNMP

# CentOS8 - SNMP安裝流程二

```
systemctl status snmpd
```

確認 SNMP 運作狀況

```
systemctl restart snmpd
```

重啟 SNMP 服務

# 實作 - 使用 SNMP 記錄 IPv4 arp table

```
snmpwalk -OX -v 2c -c public localhost ipNetToMediaPhysAddress
```

## 實際演練

### 如何編寫 shell

```
snmpwalk -OX -v 2c -c yccycc 10.4.1.252 ipNetToMediaPhysAddress
```

### 如何排程

```
crontab - e  
date '+%m-%d'
```

### 如何查詢

```
grep
```

# 實作 - 使用 SNMP 記錄 IPv6 neighbor

```
snmpwalk -OX -v 2c -c public localhost ipv6NetToMediaPhysAddress
```

## 實際演練

### 如何編寫 shell

```
snmpwalk -OX -v 2c -c public localhost ipv6NetToMediaPhysAddress
```

### 如何排程

```
crontab - e
```

```
date '+%m-%d'
```

### 如何查詢

```
grep
```

# IPv6 IP address 發放方式

說明與比較

# 兩大模式

## IPv6 手動設定

需要注意事項，停用臨時 IPv6 位址才有意義

## IPv6 自動組態配置(IPv6 Auto configuration)

分成兩大類，自動比較方便

# IPv6 自動組態配置

## IPv6 Auto configuration

全狀態位址自動配置(Stateful Address Auto-configuration)

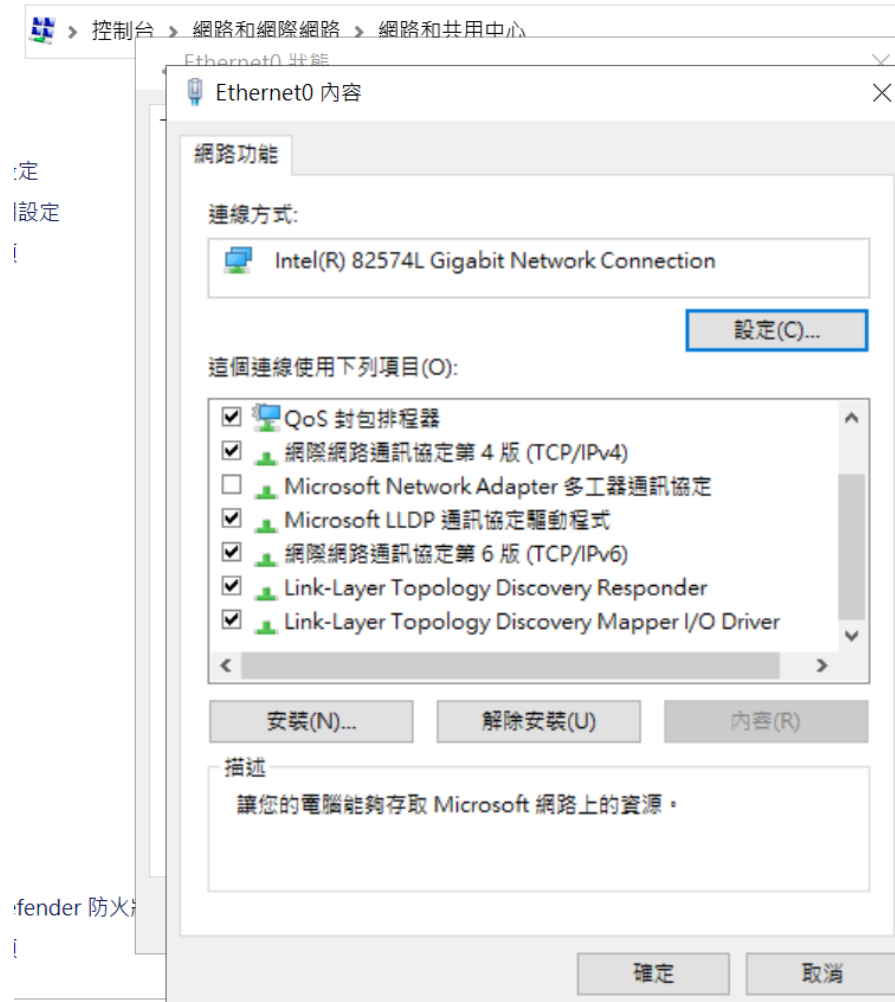
DHCPv4 相同

無狀態位址自動配置(Stateless Address Auto-configuration)

允許一部主機結合了本機可用資訊(介面識別碼)

和路由器公告取得的訊息(首碼)來產生自己的IP位址

# Windows 如何 啟用/停用 IPv6





# CentOS8 如何 啟用/停用 IPv6

```
# vi /etc/default/grub
```

在最後一行加入

```
GRUB_CMDLINE_LINUX="$GRUB_CMDLINE_LINUX ipv6.disable=1"
```

```
# grub2-mkconfig -o /boot/grub2/grub.cfg
```

```
# grub2-mkconfig -o /boot/efi/EFI/centos/grub.cfg
```

更新設定

```
# reboot
```

重新開機

# 挑選最適合 TANet

IPv6 IP address 的發放方式

# 有沒有...就是那麼簡單

最適合學界使用的 IPv6 佈建方式

無狀態位址自動配置(Stateless Address Auto-configuration)

瞬間完成的全校 IPv6 佈建方式，包括 DNS 派發

```
ycc@NCNU-EX9251-1> show configuration protocols router-advertisement interface irb.4  
dns-server-address 2001:e10:6840:2::11;  
prefix 2001:e10:6840:4::/64;
```

# 太簡單了

推廣 IPv6 不是技術問題

# 但是使用上怕怕

難以查詢 IPv6 真正的使用者

# 臨時 IPv6 位址

臨時 IPv6 位址 (Privacy Extensions for IPv6 SLAAC)

就算手動設定固定IPv6 位址

也會發生優先使用臨時IPv6 位址上網的狀況

因此在對應查詢上並不容易

# 驗證連線資訊

```
cmd 選取 命令提示字元
Microsoft Windows [版本 10.0.19042.1165]
(c) Microsoft Corporation. 著作權所有，並保留一切權利。
C:\Users\ycc>ipconfig

Windows IP 設定

乙太網路卡 Ethernet0:

    連線特定 DNS 尾碼 . . . . . :
    IPv6 位址. . . . . : 2001:e10:6840:4:c0b4:b3dd:a217:2cf2
    臨時 IPv6 位址. . . . . : 2001:e10:6840:4:682a:f58a:421a:fd4f
    連結-本機 IPv6 位址 . . . . . : fe80::c0b4:b3dd:a217:2cf2%5
    IPv4 位址 . . . . . : 163.22.4.124
    子網路遮罩 . . . . . : 255.255.255.0
    預設閘道 . . . . . : fe80::200:5eff:fe00:206%5
                          fe80::ceel:9400:464:2830%5
                          fe80::827f:f800:446:6048%5
                          163.22.4.254
```



測試你的 IPv6 連線。

總結 測試結果 分享結果 / 聯繫我們 其他 IPv6 網站 為說明台

- 你在網際網路上的IPv4位址 163.22.4.124 (ERX-TANET-ASN1 Taiwan Academic Network TANet Information Center)
- 你在網際網路上的IPv6位址 2001:e10:6840:4:682a:f58a:421a:fd4f (TWAREN-TW National Center for High-performance Computing)
- 你已經啟用 IPv6。你現在可以查看一個用來測試其他 IPv6 網站連線狀況的分頁。 [\[詳細資訊\]](#)
- 你似乎正在透過通道技術來連接 IPv4 或 IPv6。若您正在使用 VPN，那你的 VPN 只有保護一個（而非兩個）通訊協定。
- 此網站上的 HTTPS 支援位於 *Beta* 中。 [\[詳細資訊\]](#)
- 你的 DNS 伺服器（可能由你的ISP維護）似乎支援 IPv6 的網際網路通訊協定。

**你對於 IPv6 準備的分數**

10/10

當網站陸續只使用 IPv6，請提早為您的 IPv6 做準備和設定

點擊查看 [測試資料](#)

(已更新網站的 IPv6 統計)

# 回歸 IPv6 運作與設計原理

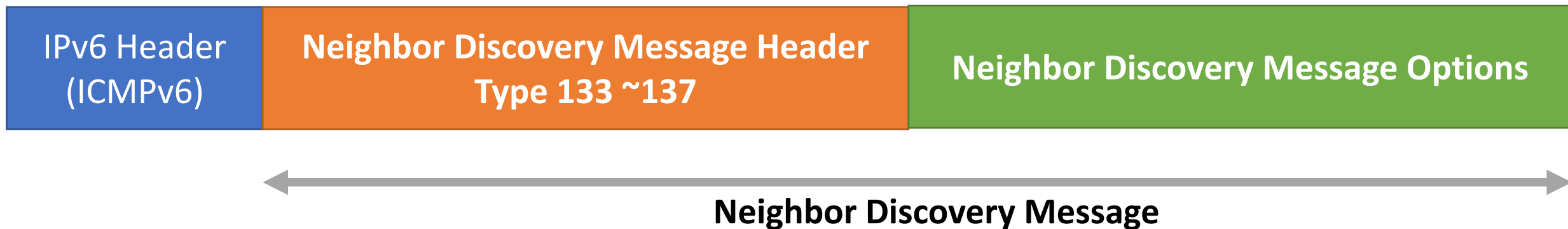


# IPv6 Neighbor Discovery

相鄰 nodes 之間的資訊交換

細分 ICMPv6 Type 133 ~ 137

再以 Option 作分類



# IPv6 Neighbor Discovery

ICMPv6 Type 133 ~ 137

133	路由器請求	Router Solicitation	( RS )
134	路由器公告	Router Advertisement	( RA )
135	鄰居請求	Neighbor Solicitation	( NS )
136	鄰居公告	Neighbor Advertisement	( NA )
137	重新導向	Redirect	



Neighbor Discovery Message

# ICMPv6 Type133

路由器請求 Router Solicitation ( RS )

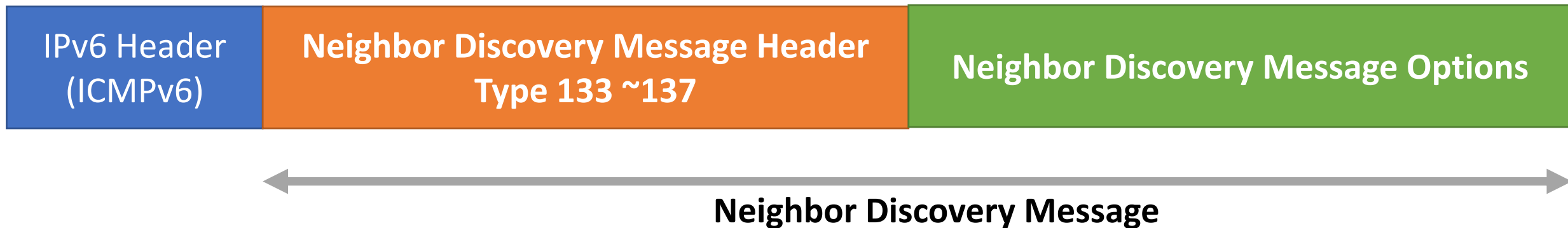
當 node 啟動 interface 時，會主動向 router 主動發出請求



# ICMPv6 Type134

路由器公告 Router Advertisement ( RA )

Router 將週期性發佈 RA message



# ICMPv6 Type135

鄰居請求                  Neighbor Solicitation ( NS )

用來解析鄰近 nodes 的 Link Layer Address

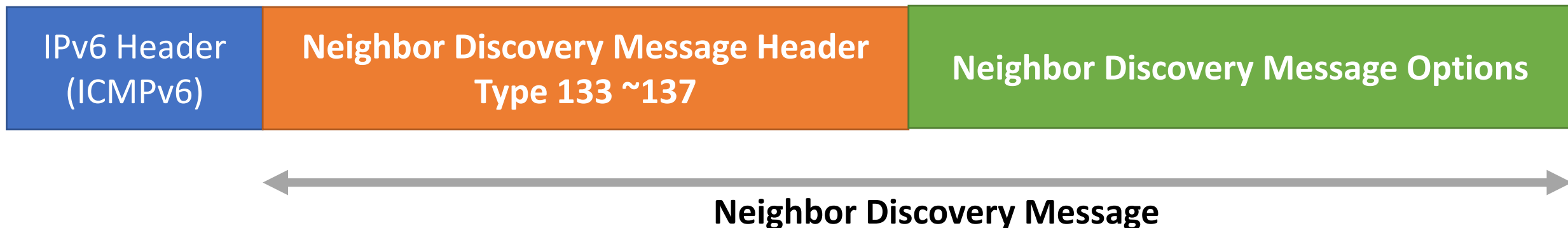


# ICMPv6 Type136

鄰居公告                  Neighbor Advertisement      ( NA )

主要包含發送者的 link layer address

用來回應 ICMPv6 Type 135 NS message

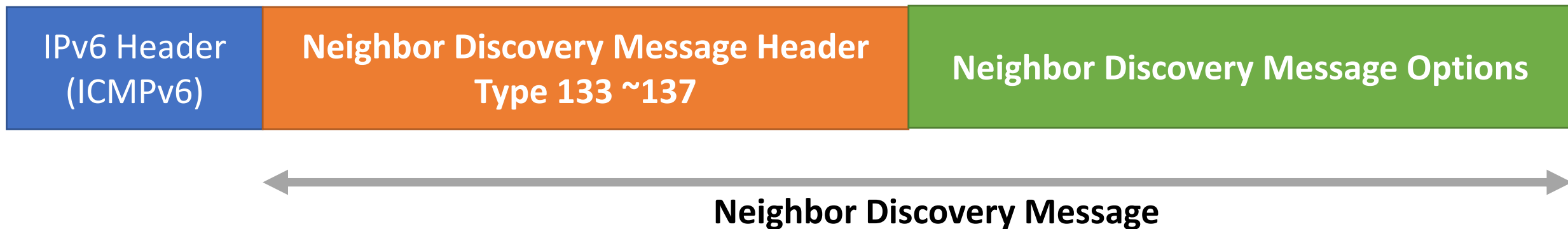


# ICMPv6 Type137

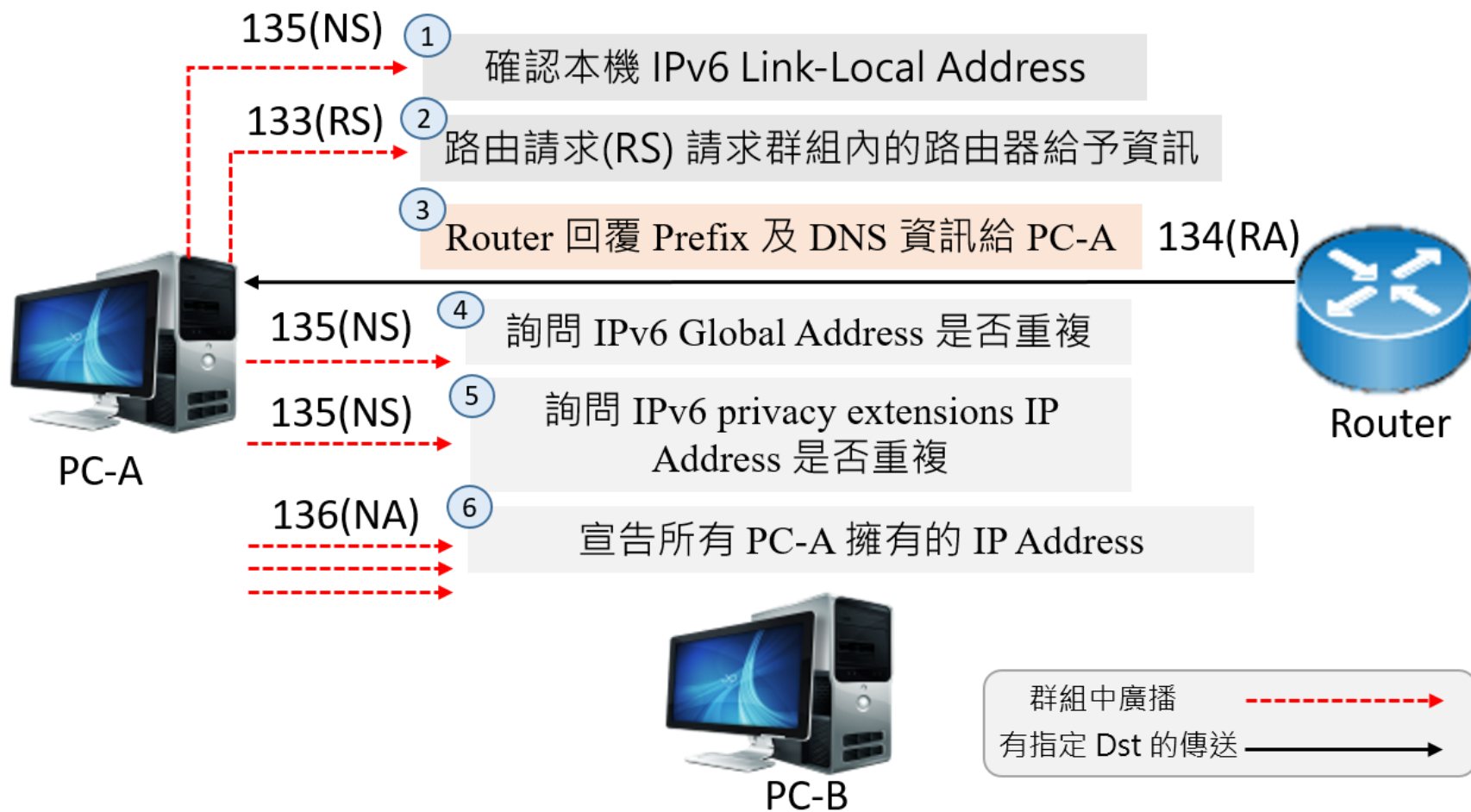
重新導向

Redirect

Router 用來告知 node 使用最佳路徑將封包送至目的位址



## Multicast 群組環境 Neighbor Discovery Protocol



取得及確認 IPv6 IP Address 過程

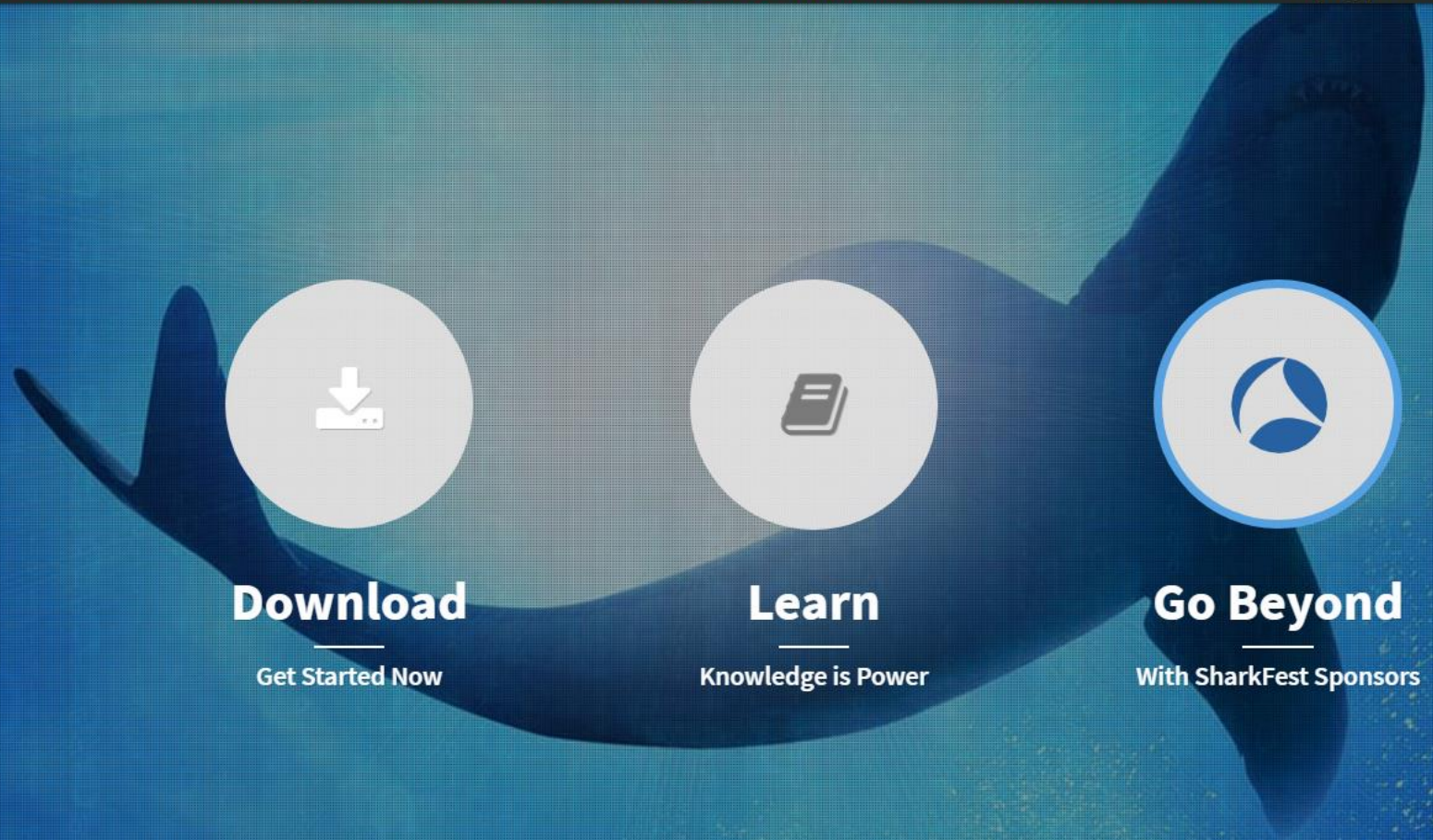


# Wireshark

安裝與基本操作



Join the Wireshark community for SharkFest'21 Virtual US, a new and online educational conference! <https://sharkfestus.wireshark.org>



**Download**  
Get Started Now



**Learn**  
Knowledge is Power



**Go Beyond**  
With SharkFest Sponsors



# Download Wireshark

The current stable release of Wireshark is 3.4.7.

Stable Release (3.4.7) • July 14, 2021

- [Windows Installer \(64-bit\)](#)
- [Windows Installer \(32-bit\)](#)
- [Windows PortableApps® \(32-bit\)](#)
- [macOS Intel 64-bit .dmg](#)
- [Source Code](#)

Old Stable Release (3.2.15) • July 14, 2021

Documentation

More downloads and documentation can be found on the [downloads page](#).

## S SharkFest Sponsors

Always-on, scalable Packet Capture that integrates with all your tools

endace.com

10G 40G 100G PACKET CAPTURE

Never Drop Packets!

100Gbps 148Mpps sustained 24/7

Line Rate Full Packet Capture Hardware System

MAXIMIZE YOUR DIGITAL PERFORMANCE

RETHINK POSSIBLE

LEARN MORE

Authorized Training Partner

Official TCP / IP Troubleshooting Course

Training & Wireshark Tools




www.scos.training

Powered by DigitalOcean

Welcome to Wireshark

### Capture

...using this filter:  All interfaces shown ▾

- 區域連線\* 10 \_\_\_\_\_
- 區域連線\* 9 \_\_\_\_\_
- 區域連線\* 8 \_\_\_\_\_
- 藍牙網路連線 \_\_\_\_\_
- Local Area Connection\* 9 \_\_\_\_\_
- 區域連線\* 1 \_\_\_\_\_
- Wi-Fi** \_\_\_\_\_ 
- 乙太網路 2 \_\_\_\_\_ 
- Adapter for loopback traffic capture \_\_\_\_\_ 
- USBPcap1 \_\_\_\_\_
- USBPcap2 \_\_\_\_\_

### Learn

[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#)  
You are running Wireshark 3.4.7 (v3.4.7-0-ge42cbf6a415f). You receive automatic updates.



Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
284	35.099710	163.22.4.124	192.168.8.104	TLSv1.2	246	[TCP Previous segment not captured
285	35.099808	192.168.8.104	163.22.4.124	TCP	66	[TCP Dup ACK 276#1] 49692 → 1924 [
286	35.099910	192.168.8.104	163.22.4.124	TCP	66	49692 → 1924 [ACK] Seq=2230 Ack=46
287	35.099968	192.168.8.104	163.22.4.124	TCP	54	49692 → 1924 [ACK] Seq=2230 Ack=46
288	35.100002	192.168.8.104	163.22.4.124	TCP	66	[TCP Dup ACK 287#1] 49692 → 1924 [
289	35.100041	192.168.8.104	163.22.4.124	TCP	54	49692 → 1924 [ACK] Seq=2230 Ack=48
290	35.100072	192.168.8.104	163.22.4.124	TCP	66	[TCP Dup ACK 289#1] 49692 → 1924 [
291	35.100218	163.22.4.124	192.168.8.104	TCP	1514	[TCP Out-Of-Order] 1924 → 49692 [A
292	35.100266	192.168.8.104	163.22.4.124	TCP	54	49692 → 1924 [ACK] Seq=2230 Ack=49
293	35.100337	192.168.8.104	163.22.4.124	TLSv1.2	107	Application Data
294	35.100722	163.22.4.124	192.168.8.104	TCP	1514	[TCP Previous segment not captured
295	35.100722	163.22.4.124	192.168.8.104	TLSv1.2	246	Application Data
296	35.100722	163.22.4.124	192.168.8.104	TCP	1514	[TCP Out-Of-Order] 1924 → 49692 [A
297	35.100765	192.168.8.104	163.22.4.124	TCP	66	[TCP Dup ACK 292#1] 49692 → 1924 [
298	35.100813	192.168.8.104	163.22.4.124	TCP	66	[TCP Dup ACK 292#2] 49692 → 1924 [
299	35.100847	192.168.8.104	163.22.4.124	TCP	66	49692 → 1924 [ACK] Seq=2283 Ack=51

> Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF\_{2EB45FB2-901B-4669-8A85-51508DD00C03}, id 0

> Ethernet II, Src: IntelCor\_cc:54:6b (98:af:65:cc:54:6b), Dst: HuaweiTe\_68:70:f4 (24:31:54:68:70:f4)

> Internet Protocol Version 4, Src: 192.168.8.104, Dst: 163.22.4.124

> Transmission Control Protocol, Src Port: 49692, Dst Port: 1924, Seq: 1, Ack: 1, Len: 0

0000 24 31 54 68 70 f4 98 af 65 cc 54 6b 08 00 45 00 \$1Thp... e·Tk...E·

# Wireshark

filter 如何下指令

ipv6

icmpv6

icmpv6.type

兩個參數

and 運算子 &&

or 運算子 ||

icmpv6.type == 134 || icmpv6.type == 135



ipv6

No.	Time	Source	Destination	Protocol	Length	Info
8938	32.669086	2404:0:802d:883d:4d44:4b0c:2043:5484	2001:4860:4860::8888	QUIC	101	Protected Payload (KP0), DCID=2994e531
8940	32.671292	2001:4860:4860::8888	2404:0:802d:883d:4d44:4b0c:2043:5484	QUIC	598	Protected Payload (KP0)
8941	32.671292	2001:4860:4860::8888	2404:0:802d:883d:4d44:4b0c:2043:5484	QUIC	88	Protected Payload (KP0)
8942	32.671677	2404:0:802d:883d:4d44:4b0c:2043:5484	2001:4860:4860::8888	QUIC	101	Protected Payload (KP0), DCID=2994e531
8944	32.676156	2001:12ff:0:4::9	2404:0:802d:883d:4d44:4b0c:2043:5484	TCP	74	443 → 64838 [ACK] Seq=5303 Ack=1115 W
8945	32.676156	2001:12ff:0:4::9	2404:0:802d:883d:4d44:4b0c:2043:5484	TLSv1.3	153	Application Data
8946	32.676156	2001:12ff:0:4::9	2404:0:802d:883d:4d44:4b0c:2043:5484	TLSv1.3	153	Application Data
8947	32.676156	2001:12ff:0:4::9	2404:0:802d:883d:4d44:4b0c:2043:5484	TLSv1.3	124	Application Data
8948	32.676251	2404:0:802d:883d:4d44:4b0c:2043:5484	2001:12ff:0:4::9	TCP	74	64838 → 443 [ACK] Seq=1115 Ack=5511 W
8950	32.678144	2001:4860:4860::8888	2404:0:802d:883d:4d44:4b0c:2043:5484	QUIC	88	Protected Payload (KP0)
8951	32.680197	2404:0:802d:883d:4d44:4b0c:2043:5484	2001:4860:4860::8888	QUIC	95	Protected Payload (KP0), DCID=2994e531
8952	32.681025	2001:12ff:0:4::9	2404:0:802d:883d:4d44:4b0c:2043:5484	TLSv1.3	120	Application Data
8953	32.681025	2001:12ff:0:4::9	2404:0:802d:883d:4d44:4b0c:2043:5484	TLSv1.3	98	Application Data
8954	32.681025	2001:12ff:0:4::9	2404:0:802d:883d:4d44:4b0c:2043:5484	TCP	74	443 → 61398 [FIN, ACK] Seq=9052 Ack=1
8955	32.681127	2404:0:802d:883d:4d44:4b0c:2043:5484	2001:12ff:0:4::9	TCP	74	61398 → 443 [ACK] Seq=1691 Ack=9053 W
8956	32.681396	2404:0:802d:883d:4d44:4b0c:2043:5484	2001:12ff:0:4::9	TCP	74	61398 → 443 [FIN, ACK] Seq=1691 Ack=90

> Frame 118: 196 bytes on wire (1568 bits), 196 bytes captured (1568 bits) on interface \Device\NPF\_{2EB45FB2-901B-4669-8A85-51508DD00C03}, id 0

> Ethernet II, Src: e6:28:66:ba:7d:0b (e6:28:66:ba:7d:0b), Dst: IntelCor\_cc:54:6b (98:af:65:cc:54:6b)

> Internet Protocol Version 6, Src: fe80::1c5c:f4bb:d6d6:20c1, Dst: ff02::fb

> User Datagram Protocol, Src Port: 5353, Dst Port: 5353

> Multicast Domain Name System (query)

0000 98 af 65 cc 54 6b e6 28 66 ba 7d 0b 86 dd 60 02 ..e.Tk.( f.}....



icmpv6

No.	Time	Source	Destination	Protocol	Length	Info
11821	38.711140	fe80::2631:54ff:fe68:70f4	fe80::88f3:9862:8df9:4ab4	ICMPv6	86	Neighbor Solicitation for fe80::88f3:9862:8df9:4ab4
11822	38.711264	fe80::88f3:9862:8df9:4ab4	fe80::2631:54ff:fe68:70f4	ICMPv6	86	Neighbor Advertisement fe80::88f3:9862:8df9:4ab4
15463	45.931460	fe80::2631:54ff:fe68:70f4	2404:0:802d:883d:4d44:4b0c:2043:5484	ICMPv6	86	Neighbor Solicitation for 2404:0:802d:883d:4d44:4b0c:2043:5484
15464	45.931533	2404:0:802d:883d:4d44:4b0c:2043:5484	fe80::2631:54ff:fe68:70f4	ICMPv6	86	Neighbor Advertisement 2404:0:802d:883d:4d44:4b0c:2043:5484
15527	46.331664	fe80::f628:53ff:fede:7054	ff02::1	ICMPv6	90	Multicast Listener Query
15537	46.352210	fe80::2631:54ff:fe68:70f4	ff02::16	ICMPv6	190	Multicast Listener Report Message v2
15576	46.634179	fe80::88f3:9862:8df9:4ab4	ff02::16	ICMPv6	170	Multicast Listener Report Message v2
15642	47.069097	fe80::7030:d8ff:fe4a:df2d	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
17596	76.006970	fe80::2631:54ff:fe68:70f4	ff02::1:fff9:4ab4	ICMPv6	86	Neighbor Solicitation for 2404:0:802d:883d:4d44:4b0c:2043:5484
17597	76.006970	fe80::2631:54ff:fe68:70f4	ff02::1:fff9:4ab4	ICMPv6	86	Neighbor Solicitation for fd24:3154:6870:f400:88f3:9862:8df9:4ab4
17598	76.006970	fe80::2631:54ff:fe68:70f4	ff02::1:ff43:5484	ICMPv6	86	Neighbor Solicitation for fd24:3154:6870:f400:88f3:9862:8df9:4ab4
17599	76.007220	2404:0:802d:883d:88f3:9862:8df9:4ab4	fe80::2631:54ff:fe68:70f4	ICMPv6	86	Neighbor Advertisement 2404:0:802d:883d:88f3:9862:8df9:4ab4
17600	76.007391	fd24:3154:6870:f400:88f3:9862:8df9:4ab4	fe80::2631:54ff:fe68:70f4	ICMPv6	86	Neighbor Advertisement fd24:3154:6870:f400:88f3:9862:8df9:4ab4
17601	76.007489	fd24:3154:6870:f400:4d44:4b0c:2043:5484	fe80::2631:54ff:fe68:70f4	ICMPv6	86	Neighbor Advertisement fd24:3154:6870:f400:4d44:4b0c:2043:5484
17791	83.851539	fe80::2631:54ff:fe68:70f4	2404:0:802d:883d:4d44:4b0c:2043:5484	ICMPv6	86	Neighbor Solicitation for 2404:0:802d:883d:4d44:4b0c:2043:5484
17792	83.851624	2404:0:802d:883d:4d44:4b0c:2043:5484	fe80::2631:54ff:fe68:70f4	ICMPv6	86	Neighbor Advertisement 2404:0:802d:883d:4d44:4b0c:2043:5484

> Frame 15527: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF\_{2EB45FB2-901B-4669-8A85-51508DD00C03}, id 0  
 > Ethernet II, Src: ZioncomE\_de:70:54 (f4:28:53:de:70:54), Dst: IntelCor\_cc:54:6b (98:af:65:cc:54:6b)  
 > Internet Protocol Version 6, Src: fe80::f628:53ff:fede:7054, Dst: ff02::1  
 > Internet Control Message Protocol v6

0000 98 af 65 cc 54 6b f4 28 53 de 70 54 86 dd 60 00 ..e.Tk.( S.pT...





icmpv6.type == 135

No.	Time	Source	Destination	Protocol	Length	Info
1120	20.641125	fe80::2631:54ff:fe68:70f4	2404:0:802d:883d:4d44:4b0c:2043:5484	ICMPv6	86	Neighbor Solicitation for 2404:0:802d:883d:4d44:4b0c:2043:5484
11821	38.711140	fe80::2631:54ff:fe68:70f4	fe80::88f3:9862:8df9:4ab4	ICMPv6	86	Neighbor Solicitation for fe80::88f3:9862:8df9:4ab4
15463	45.931460	fe80::2631:54ff:fe68:70f4	2404:0:802d:883d:4d44:4b0c:2043:5484	ICMPv6	86	Neighbor Solicitation for 2404:0:802d:883d:4d44:4b0c:2043:5484
17596	76.006970	fe80::2631:54ff:fe68:70f4	ff02::1:fff9:4ab4	ICMPv6	86	Neighbor Solicitation for 2404:0:802d:883d:4d44:4b0c:2043:5484
17597	76.006970	fe80::2631:54ff:fe68:70f4	ff02::1:fff9:4ab4	ICMPv6	86	Neighbor Solicitation for fd24:3154:6870:f4::1
17598	76.006970	fe80::2631:54ff:fe68:70f4	ff02::1:ff43:5484	ICMPv6	86	Neighbor Solicitation for fd24:3154:6870:f4::1
17791	83.851539	fe80::2631:54ff:fe68:70f4	2404:0:802d:883d:4d44:4b0c:2043:5484	ICMPv6	86	Neighbor Solicitation for 2404:0:802d:883d:4d44:4b0c:2043:5484
22900	130.992460	fe80::2631:54ff:fe68:70f4	2404:0:802d:883d:4d44:4b0c:2043:5484	ICMPv6	86	Neighbor Solicitation for 2404:0:802d:883d:4d44:4b0c:2043:5484

> Frame 15463: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF\_{2EB45FB2-901B-4669-8A85-51508DD00C03}, id 0  
> Ethernet II, Src: HuaweiTe\_68:70:f4 (24:31:54:68:70:f4), Dst: IntelCor\_cc:54:6b (98:af:65:cc:54:6b)  
> Internet Protocol Version 6, Src: fe80::2631:54ff:fe68:70f4, Dst: 2404:0:802d:883d:4d44:4b0c:2043:5484  
> Internet Control Message Protocol v6

0000 98 af 65 cc 54 6b 24 31 54 68 70 f4 86 dd 60 00 ..e.Tk\$1 Thp...`



ipv6 && icmpv6.type == 135

No.	Time	Source	Destination	Protocol	Length	Info
1120	20.641125	fe80::2631:54ff:fe68:70f4	2404:0:802d:883d:4d44:4b0c:2043:5484	ICMPv6	86	Neighbor Solicitation for 2404:0:802d:883d:4d44:4b0c:2043:5484
11821	38.711140	fe80::2631:54ff:fe68:70f4	fe80::88f3:9862:8df9:4ab4	ICMPv6	86	Neighbor Solicitation for fe80::88f3:9862:8df9:4ab4
15463	45.931460	fe80::2631:54ff:fe68:70f4	2404:0:802d:883d:4d44:4b0c:2043:5484	ICMPv6	86	Neighbor Solicitation for 2404:0:802d:883d:4d44:4b0c:2043:5484
17596	76.006970	fe80::2631:54ff:fe68:70f4	ff02::1:fff9:4ab4	ICMPv6	86	Neighbor Solicitation for 2404:0:802d:883d:4d44:4b0c:2043:5484
17597	76.006970	fe80::2631:54ff:fe68:70f4	ff02::1:fff9:4ab4	ICMPv6	86	Neighbor Solicitation for fd24:3154:6870:883d:4d44:4b0c:2043:5484
17598	76.006970	fe80::2631:54ff:fe68:70f4	ff02::1:ff43:5484	ICMPv6	86	Neighbor Solicitation for fd24:3154:6870:883d:4d44:4b0c:2043:5484
17791	83.851539	fe80::2631:54ff:fe68:70f4	2404:0:802d:883d:4d44:4b0c:2043:5484	ICMPv6	86	Neighbor Solicitation for 2404:0:802d:883d:4d44:4b0c:2043:5484
22900	130.992460	fe80::2631:54ff:fe68:70f4	2404:0:802d:883d:4d44:4b0c:2043:5484	ICMPv6	86	Neighbor Solicitation for 2404:0:802d:883d:4d44:4b0c:2043:5484
29753	194.172414	fe80::2631:54ff:fe68:70f4	2404:0:802d:883d:4d44:4b0c:2043:5484	ICMPv6	86	Neighbor Solicitation for 2404:0:802d:883d:4d44:4b0c:2043:5484
32959	214.242315	fe80::2631:54ff:fe68:70f4	ff02::1:ffd6:20c1	ICMPv6	86	Neighbor Solicitation for fe80::1c5c:f4d4:4b0c:2043:5484
37257	222.557636	fe80::2631:54ff:fe68:70f4	2404:0:802d:883d:4d44:4b0c:2043:5484	ICMPv6	86	Neighbor Solicitation for 2404:0:802d:883d:4d44:4b0c:2043:5484

> Frame 15463: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF\_{2EB45FB2-901B-4669-8A85-51508DD00C03}, id 0

> Ethernet II, Src: HuaweiTe\_68:70:f4 (24:31:54:68:70:f4), Dst: IntelCor\_cc:54:6b (98:af:65:cc:54:6b)

> Internet Protocol Version 6, Src: fe80::2631:54ff:fe68:70f4, Dst: 2404:0:802d:883d:4d44:4b0c:2043:5484

> Internet Control Message Protocol v6

0000 98 af 65 cc 54 6b 24 31 54 68 70 f4 86 dd 60 00 ..e.Tk\$1 Thp...

# 可以設定存檔方式

避免檔案過大



icmpv6.type == 134 || icmpv6.type == 135

No.	Time	Source	Destination	Protocol	Length	Info
48330	331.284173	fe80::2631:54ff:fe68:70f4	2404:0:802d:883d:4d44:4b0c:2043:5484	ICMPv6	86	Neighbor Solicitation for 2404:0:802d:883d:4d44:4b0c:2043:5484
49707	366.432385	fe80::2631:54ff:fe68:70f4	ff02::1:fff9:4ab4	ICMPv6	86	Neighbor Solicitation for 2404:0:802d:883d:4d44:4b0c:2043:5484
49708	366.432385	fe80::2631:54ff:fe68:70f4	ff02::1:fff9:4ab4	ICMPv6	86	Neighbor Solicitation for fd24:3154:6870:f400::64
49709	366.432385	fe80::2631:54ff:fe68:70f4	ff02::1:fff9:4ab4	ICMPv6	86	Neighbor Solicitation for fd24:3154:6870:f400::64

Wireshark · Capture Options

Input Output Options

Capture to a permanent file

File:  Browse...

Output format:  pcapng  pcap

Create a new file automatically...

after  packets

after  kilobytes

after  seconds

when time is a multiple of  hours

Use a ring buffer with  files

Start 關閉 說明

51532	389.677680	fe80::2631:54ff:fe68:70f4	ff02::1:fff9:4ab4	ICMPv6	86	Neighbor Solicitation for 2404:0:802d:883d:4d44:4b0c:2043:5484
53999	437.395688	fe80::2631:54ff:fe68:70f4	ff02::1:fff9:4ab4	ICMPv6	86	Neighbor Solicitation for 2404:0:802d:883d:4d44:4b0c:2043:5484
57291	500.385131	fe80::2631:54ff:fe68:70f4	ff02::1:fff9:4ab4	ICMPv6	86	Neighbor Solicitation for 2404:0:802d:883d:4d44:4b0c:2043:5484
58432	505.495453	fe80::2631:54ff:fe68:70f4	ff02::1:fff9:4ab4	ICMPv6	86	Neighbor Solicitation for 2404:0:802d:883d:4d44:4b0c:2043:5484
59598	589.977325	fe80::2631:54ff:fe68:70f4	ff02::1:fff9:4ab4	ICMPv6	86	Neighbor Solicitation for 2404:0:802d:883d:4d44:4b0c:2043:5484
59990	605.486086	fe80::2631:54ff:fe68:70f4	ff02::1:fff9:4ab4	ICMPv6	86	Neighbor Solicitation for 2404:0:802d:883d:4d44:4b0c:2043:5484
65938	618.577285	fe80::2631:54ff:fe68:70f4	ff02::1:fff9:4ab4	ICMPv6	86	Neighbor Solicitation for 2404:0:802d:883d:4d44:4b0c:2043:5484
68646	656.741345	fe80::2631:54ff:fe68:70f4	ff02::1:fff9:4ab4	ICMPv6	86	Neighbor Solicitation for 2404:0:802d:883d:4d44:4b0c:2043:5484
68647	656.741345	fe80::2631:54ff:fe68:70f4	ff02::1:fff9:4ab4	ICMPv6	86	Neighbor Solicitation for fd24:3154:6870:f400::64
68652	656.909340	fe80::2631:54ff:fe68:70f4	ff02::1:fff9:4ab4	ICMPv6	86	Neighbor Solicitation for fd24:3154:6870:f400::64
74354	796.201814	fe80::2631:54ff:fe68:70f4	ff02::1:fff9:4ab4	ICMPv6	86	Neighbor Solicitation for fe80::1c9f:3fff:fe28:5123
74517	830.107691	fe80::2631:54ff:fe68:70f4	ff02::1:fff9:4ab4	ICMPv6	86	Neighbor Solicitation for fe80::1c9f:3fff:fe28:5123

> Frame 74517: 174 bytes on wire (1392 bits) captured (1392 bits) on 0  
 > Ethernet II, Src: Huawei (08:00:00:00:00:00), Dst: Huawei (08:00:00:00:00:00)  
 > Internet Protocol Version 6, Src: 2404:0:802d:883d:4d44:4b0c:2043:5484, Dst: ff02::1:fff9:4ab4  
 > Internet Control Message Protocol, Type: Router Advertisement, Code: 0, Checksum: 0xb9f9 [correct], [Checksum Status: Good], Cur hop limit: 64  
 > Flags: 0xc8, Managed  
 Router lifetime (s): 1800  
 Reachable time (ms): 0  
 Retrans timer (ms): 0  
 > ICMPv6 Option (Prefix information : 2404:0:802d:883d::/64)  
 > ICMPv6 Option (Prefix information : fd24:3154:6870:f400::/64)  
 > ICMPv6 Option (Recursive DNS Server fe80::2631:54ff:fe68:70f4)  
 > ICMPv6 Option (MTU : 1500)  
 > ICMPv6 Option (Source link-layer address : 24:31:54:68:70:f4)

0000 98 af 65 cc 54 6b 24 31 54 68 70 f4 86 dd 60 0c ..e.Tk\$1 Thp...`

# 使用 Wireshark 缺點

1. 透過 圖形化介面 耗費大量資源
2. 建置後，遠端查詢較不容易
3. 雖然可批次存檔案，但自動整理較不易

# 該如何精簡化

Tshark

```
[root@localhost ~]# dnf search wireshark
===== Name Exactly Matched: wireshark =====
wireshark.x86_64 : Network traffic analyzer
===== Name Matched: wireshark =====
wireshark-cli.i686 : Network traffic analyzer
wireshark-cli.x86_64 : Network traffic analyzer
[root@localhost ~]# dnf wireshark.x86_64
No such command: wireshark.x86_64. Please use /usr/bin/dnf --help
It could be a DNF plugin command, try: "dnf install 'dnf-command(wireshark.x86_64)'"
[root@localhost ~]# dnf install wireshark.x86_64
CentOS Linux 8 - AppStream          623 B/s | 4.3 kB      00:07
CentOS Linux 8 - AppStream          721 kB/s | 8.8 MB      00:12
CentOS Linux 8 - BaseOS             610 B/s | 3.9 kB      00:06
CentOS Linux 8 - BaseOS            440 kB/s | 5.6 MB      00:12
CentOS Linux 8 - Extras             240 B/s | 1.5 kB      00:06
Dependencies resolved.

=====
Package                               Arch      Version                Repository             Size
=====
Installing:
wireshark                             x86_64    1:2.6.2-12.el8        appstream              3.6 M
Installing dependencies:
libatomic                             x86_64    8.4.1-1.el8           baseos                 23 k
libsmi                                 x86_64    0.4.8-23.el8         appstream              2.4 M
openal-soft                            x86_64    1.18.2-7.el8         appstream              394 k
=====
```



root@localhost:~



File Edit View Search Terminal Help

```
Verifying      : openal-soft-1.18.2-7.el8.x86_64      2/15
Verifying      : qt5-qtbase-5.12.5-8.el8.x86_64      3/15
Verifying      : qt5-qtbase-common-5.12.5-8.el8.noarch  4/15
Verifying      : qt5-qtbase-gui-5.12.5-8.el8.x86_64  5/15
Verifying      : qt5-qtdeclarative-5.12.5-1.el8.x86_64  6/15
Verifying      : qt5-qtmultimedia-5.12.5-1.el8.x86_64  7/15
Verifying      : wireshark-1:2.6.2-12.el8.x86_64      8/15
Verifying      : wireshark-cli-1:2.6.2-12.el8.x86_64   9/15
Verifying      : xcb-util-image-0.4.0-9.el8.x86_64     10/15
Verifying      : xcb-util-keysyms-0.4.0-7.el8.x86_64   11/15
Verifying      : xcb-util-renderutil-0.3.9-10.el8.x86_64 12/15
Verifying      : xcb-util-wm-0.4.1-12.el8.x86_64      13/15
Verifying      : libatomic-8.4.1-1.el8.x86_64        14/15
Verifying      : pcre2-utf16-10.32-2.el8.x86_64       15/15
```

Installed products updated.

Installed:

```
libatomic-8.4.1-1.el8.x86_64      libsmi-0.4.8-23.el8.x86_64
openal-soft-1.18.2-7.el8.x86_64   pcre2-utf16-10.32-2.el8.x86_64
qt5-qtbase-5.12.5-8.el8.x86_64    qt5-qtbase-common-5.12.5-8.el8.noarch
qt5-qtbase-gui-5.12.5-8.el8.x86_64 qt5-qtdeclarative-5.12.5-1.el8.x86_64
qt5-qtmultimedia-5.12.5-1.el8.x86_64 wireshark-1:2.6.2-12.el8.x86_64
wireshark-cli-1:2.6.2-12.el8.x86_64 xcb-util-image-0.4.0-9.el8.x86_64
xcb-util-keysyms-0.4.0-7.el8.x86_64 xcb-util-renderutil-0.3.9-10.el8.x86_64
xcb-util-wm-0.4.1-12.el8.x86_64
```

Complete!

[root@localhost ~]# tshark





root@localhost:~



File Edit View Search Terminal Help

```
349 339.668418938 fe80::e735:8bec:690c:4187 → fe80::2631:54ff:fe68:70f4 ICMPv6 78 Neighbor Advertisement fe80::e735:8bec:690c:4187 (sol)
350 339.974556355 ZyxelCom_fa:ac:29 → Broadcast 0x8899 60 Realtek Layer 2 Protocol S
351 340.487973981 fe80::1c5c:f4bb:d6d6:20c1 → ff02::16 ICMPv6 130 Multicast Listener Report Message v2
352 340.895518842 fe80::2631:54ff:fe68:70f4 → ff02::1:fff9:4ab4 ICMPv6 86 Neighbor Solicitation for fe80::88f3:9862:8df9:4ab4 from 24:31:54:68:70:f4
353 342.022090241 ZyxelCom_fa:ac:29 → Broadcast 0x8899 60 Realtek Layer 2 Protocol S
354 342.968205670 fe80::2631:54ff:fe68:70f4 → ff02::1:fff9:4ab4 ICMPv6 86 Neighbor Solicitation for 2404:0:802d:883d:88f3:9862:8df9:4ab4 from 24:31:54:68:70:f4
355 343.968480025 ZyxelCom_fa:ac:29 → Broadcast 0x8899 60 Realtek Layer 2 Protocol S
356 344.070021145 fe80::2631:54ff:fe68:70f4 → ff02::1:fff9:4ab4 ICMPv6 86 Neighbor Solicitation for fd24:3154:6870:f400:88f3:9862:8df9:4ab4 from 24:31:54:68:70:f4
357 344.070097134 fe80::2631:54ff:fe68:70f4 → ff02::1:ff43:5484 ICMPv6 86 Neighbor Solicitation for fd24:3154:6870:f400:4d44:4b0c:2043:5484 from 24:31:54:68:70:f4
358 344.070103630 fe80::2631:54ff:fe68:70f4 → ff02::1:ff0c:4187 ICMPv6 86 Neighbor Solicitation for fe80::e735:8bec:690c:4187 from 24:31:54:68:70:f4
359 344.070166279 fe80::e735:8bec:690c:4187 → fe80::2631:54ff:fe68:70f4 ICMPv6 86 Neighbor Advertisement fe80::e735:8bec:690c:4187 (sol, ovr) is at 08:00:27:bb:85:f3
360 344.070205521 fe80::2631:54ff:fe68:70f4 → ff02::1:ff97:c77b ICMPv6 86 Neighbor Solicitation for 2404:0:802d:883d:a461:d2d8:1f97:c77b from 24:31:54:68:70:f4
361 344.070232954 2404:0:802d:883d:a461:d2d8:1f97:c77b → fe80::2631:54ff:fe68:70f4 ICMPv6 86 Neighbor Advertisement 2404:0:802d:883d:a461:d2d8:1f97:c77b (sol, ovr) is at 08:00:27:bb:85:f3
```

# 會出現 MAC 的紀錄

ICMPv6 Type 135 鄰居請求 NS - Neighbor Solicitation

ICMPv6 Type 136 鄰居公告 NA - Neighbor Advertisement

# Tshark 如何下指令

Linux tshark 抓取 type135、136 指令

```
tshark -i enp0s3 -w /root/ICMP.pcap -f "icmp6[icmptype]==135 || icmp6[icmptype]==136 "
```

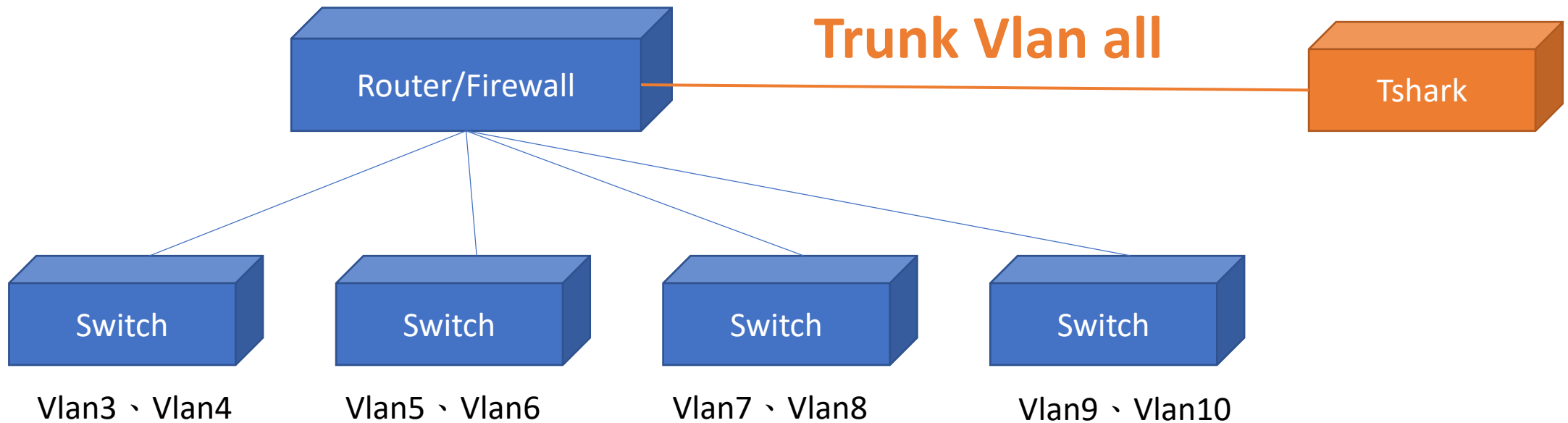
- i 指定蒐集資訊的網卡
- w 儲存名稱及副檔名
- f "過濾條件"

# 如何讀取 tshark 的檔案

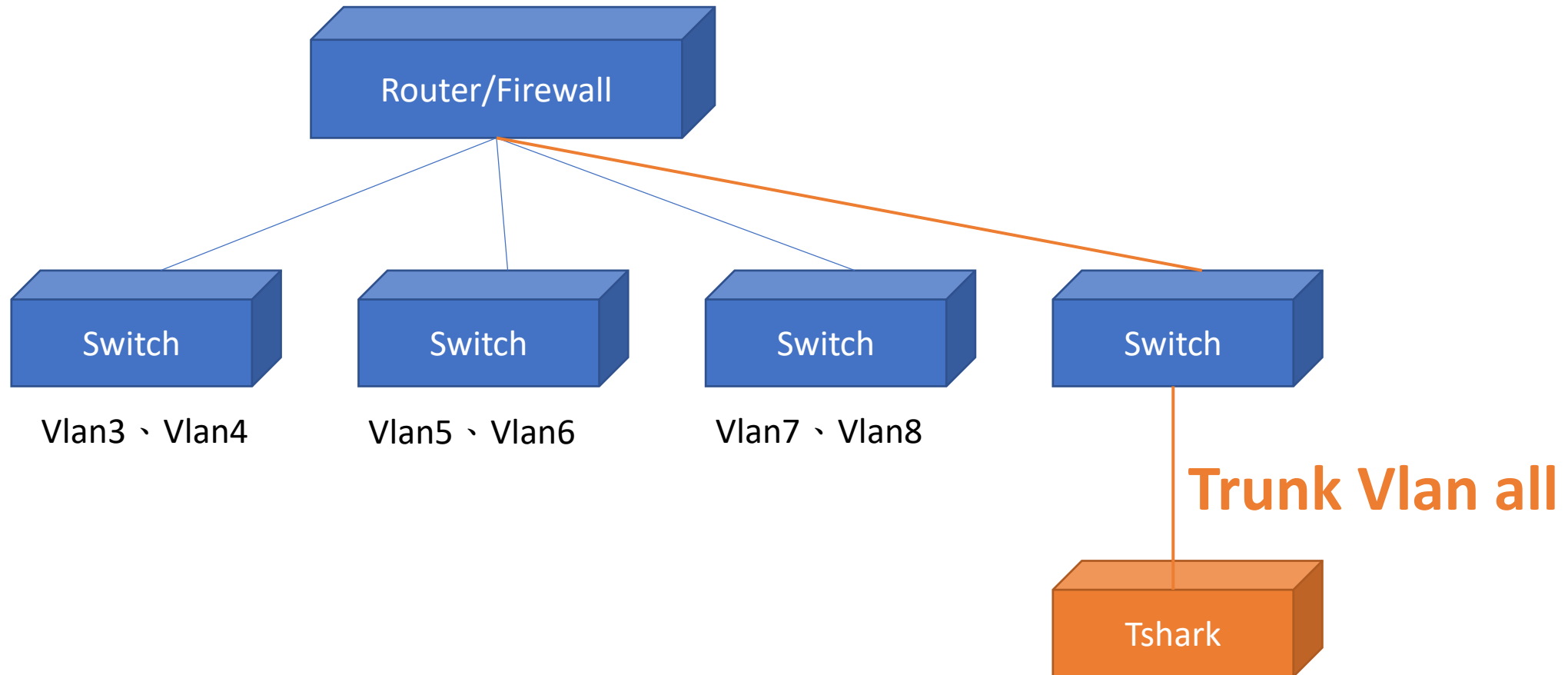
```
tshark -r ICMP.pcap -T fields -e eth.src
```

- r 讀取檔案名稱
- T fields 以欄位方式顯示
- e 選擇顯示的欄位名稱
  - e icmpv6.type
  - e eth.src
  - e icmpv6.nd.na.target\_address
  - e icmpv6.nd.ns.target\_address
  - e icmpv6.opt

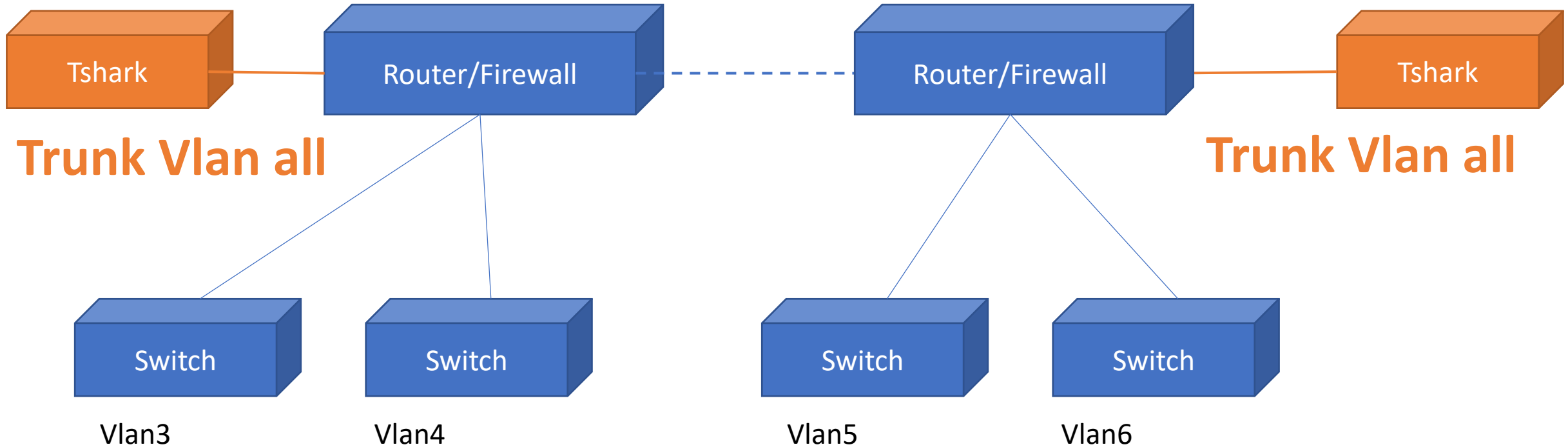
# 架構一：直接接在 Router 上



# 架構二：不一定接在 router 上

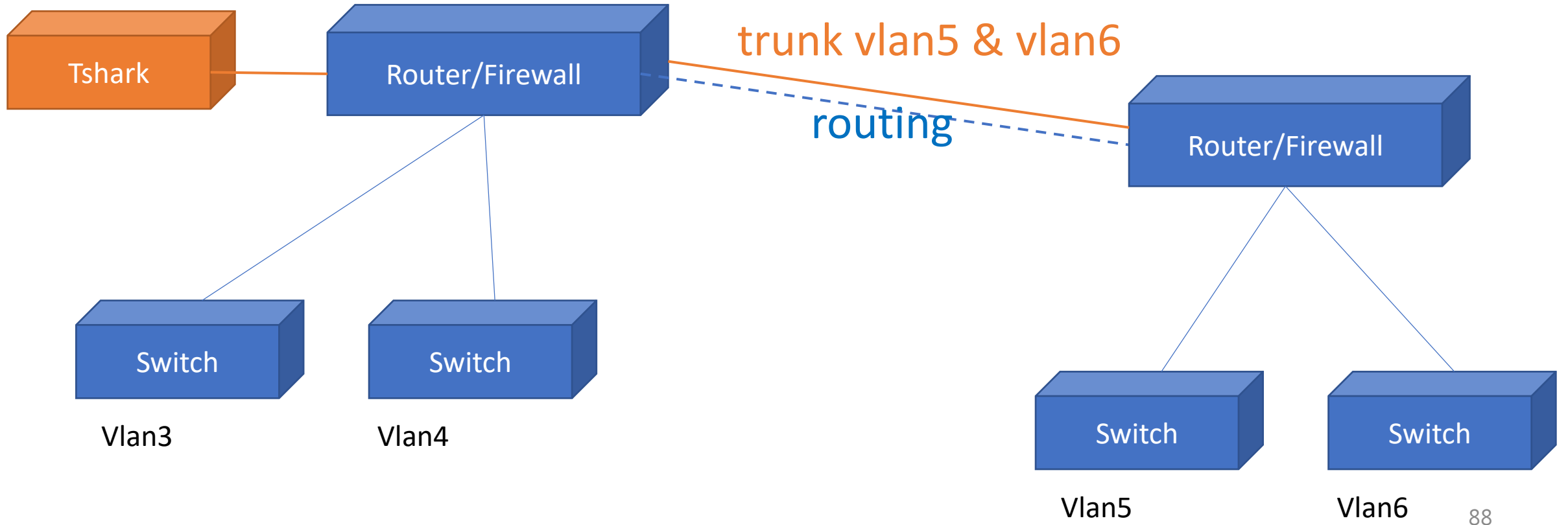


# 架構三：有兩顆以上的 Router



# 架構四：有兩顆以上的 Router

## Trunk Vlan all





# 把全校流量導向 Server 一定掛

不是 MIRROR

只要開一個 trunk vlan all 就好

沒有流量問題

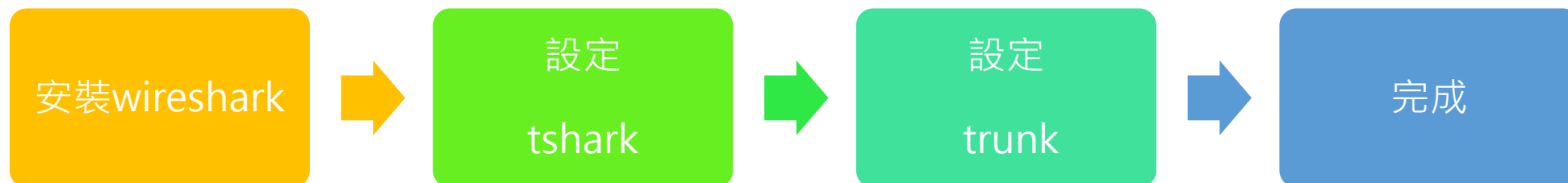
找台舊電腦



重新安裝

CentOS8

# 操作流程一



找台

Windows舊電腦

安裝

Virtual Box

安裝

CentOS 8

安裝wireshark

設定  
tshark

設定  
trunk

完成

## 操作流程二

# 如何更友善

挑戰 - 程式語言能力

# 可被優化的項目

1. 篩選特定條件進行存檔
2. 避免檔案過大的技巧
3. 文字查詢或是網頁查詢
4. 如何降低 舊電腦的 維護成本

# 有比較好嗎!?

ICMP V.S. SNMP

# 當然比較好

資料的收集完整性提升許多  
資源的消耗也降低許多

# 快了

您不用自己架設

再給我們一點時間，直接分享 安裝檔案

不用自己架設，開不開心



# Raspberry Pi – 同樣可以架設

