NTUPA 網管交接

7th器材 蔡承佑

Outline

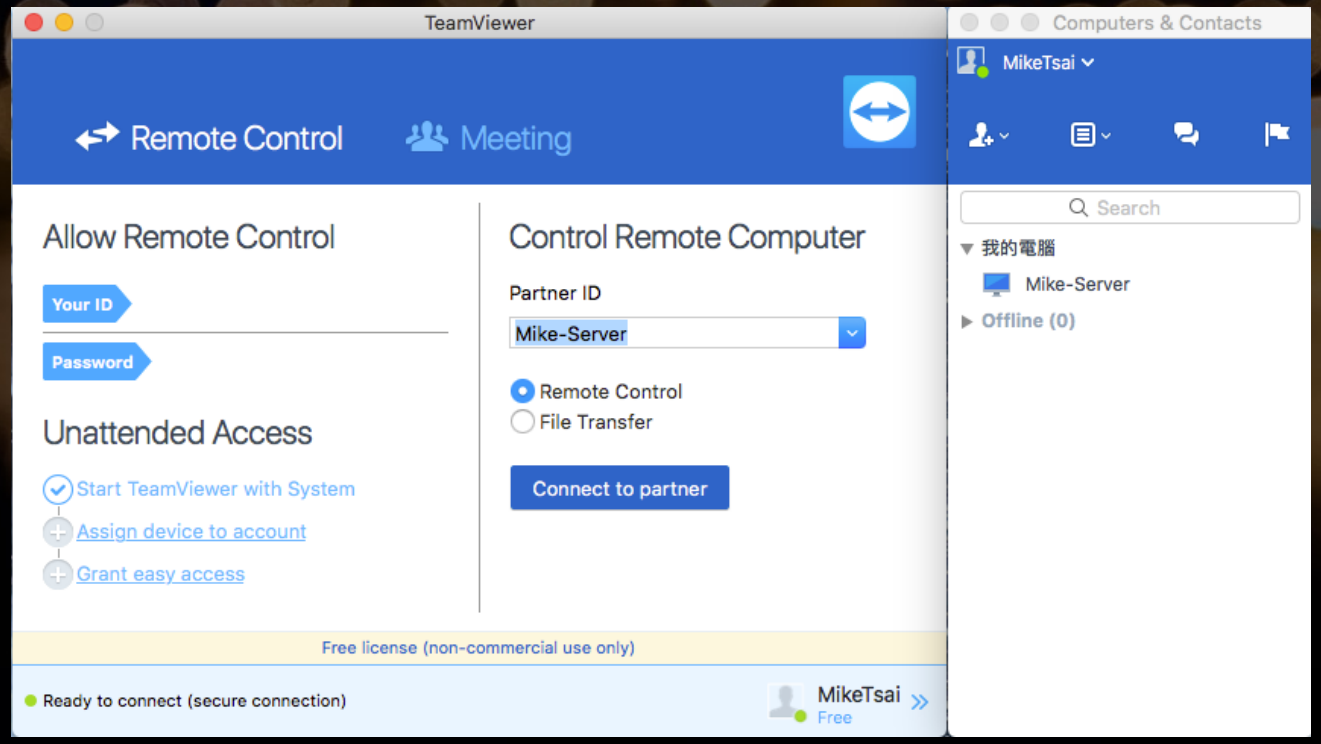
- Server (Windows)
- Server (CentOS)
- Router
- AP
- Network System Topology

Server (Windows)

- Windows 10 Enterprise (From NTU CINC)
- 1 power cable and 2 network cable
- 2 NICs
- No peripheral devices connected, controlled by TeamViewer

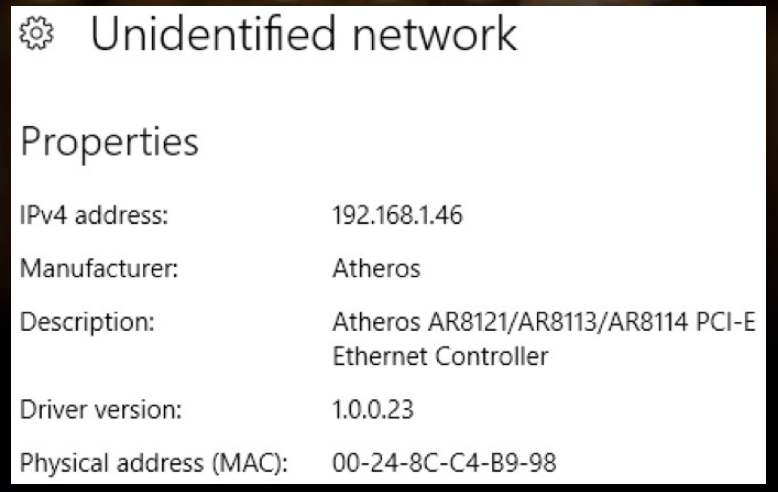
TeamViewer

- Remote Desktop Access Software
- Connect either through WAN or LAN



Server (Windows) Network Setting

- Eth1 (192.168.1.46)
  - LAN only, connected to mirroring port to listen the flow from router
- Eth2 (192.168.1.45)
  - For WAN access and daily use



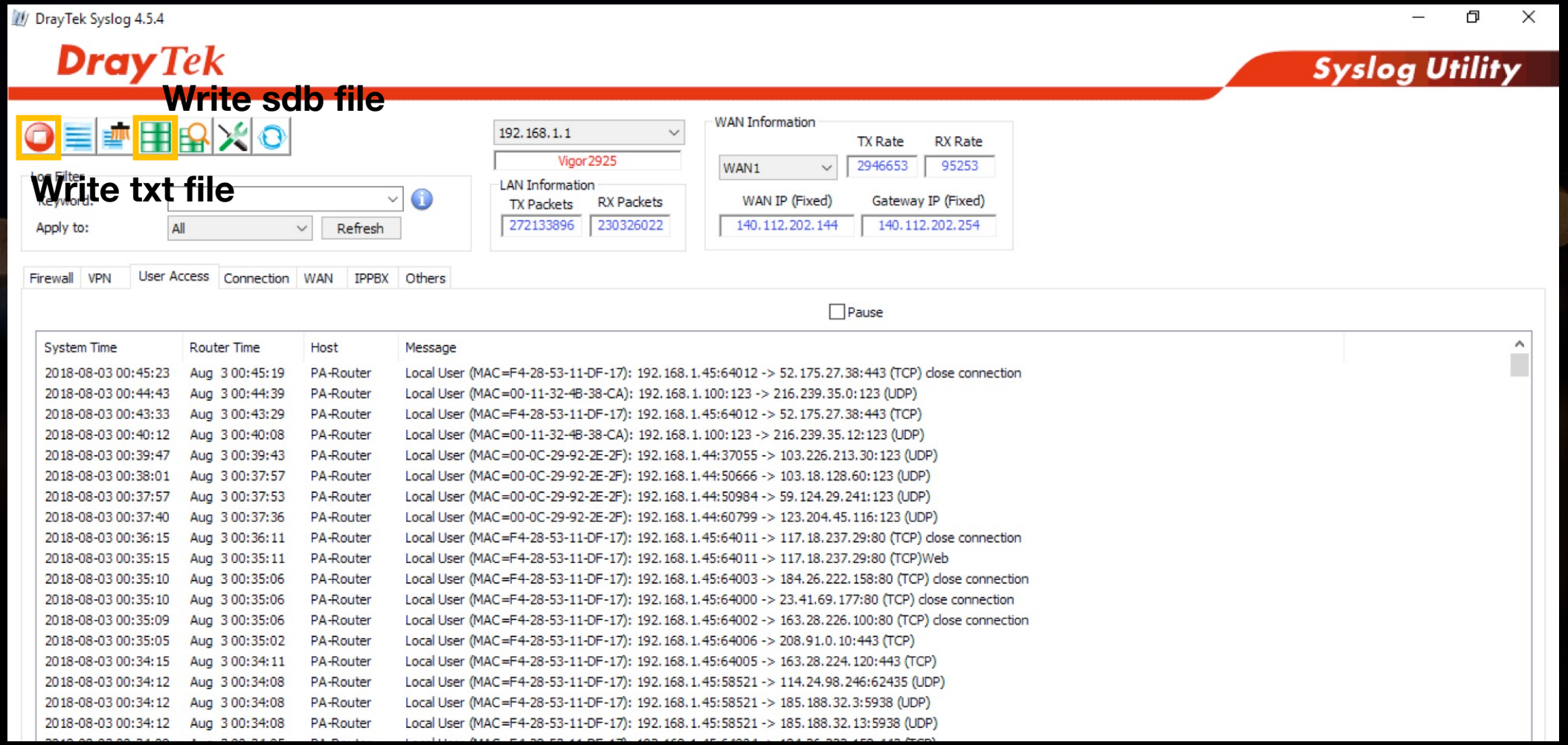
Always Active Jobs

- Syslog
  - Receive log from router through LAN
- Wireshark
  - Using mirroring port to listen the network of the whole network

Syslog

- Write txt file continuously
- Write sdb file each day

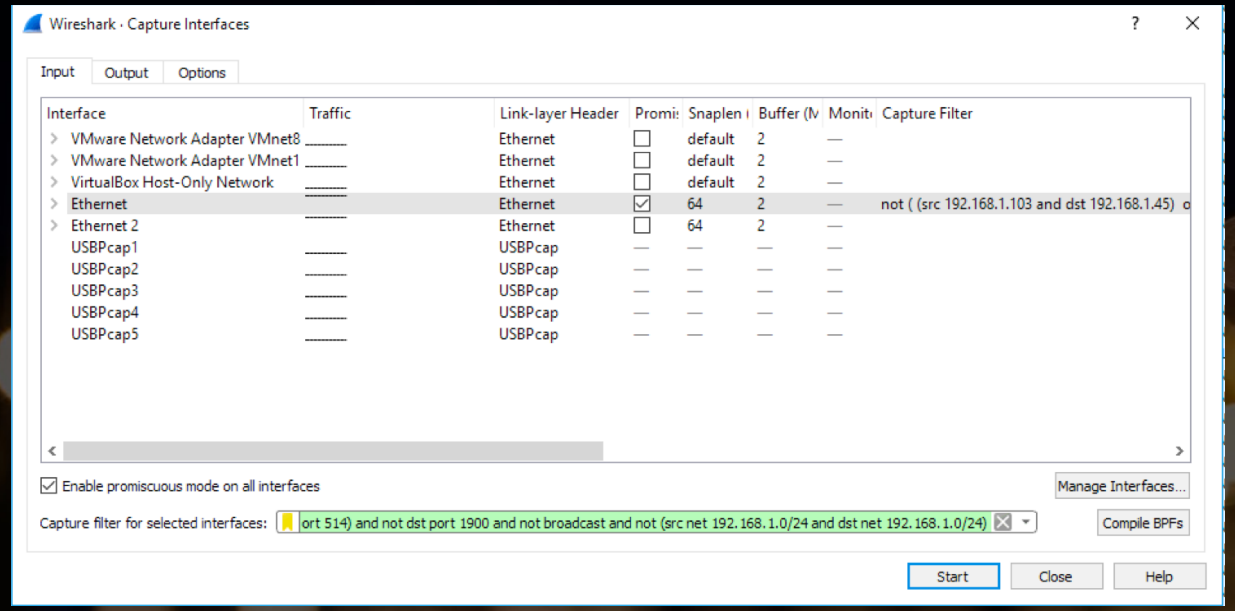
Syslog

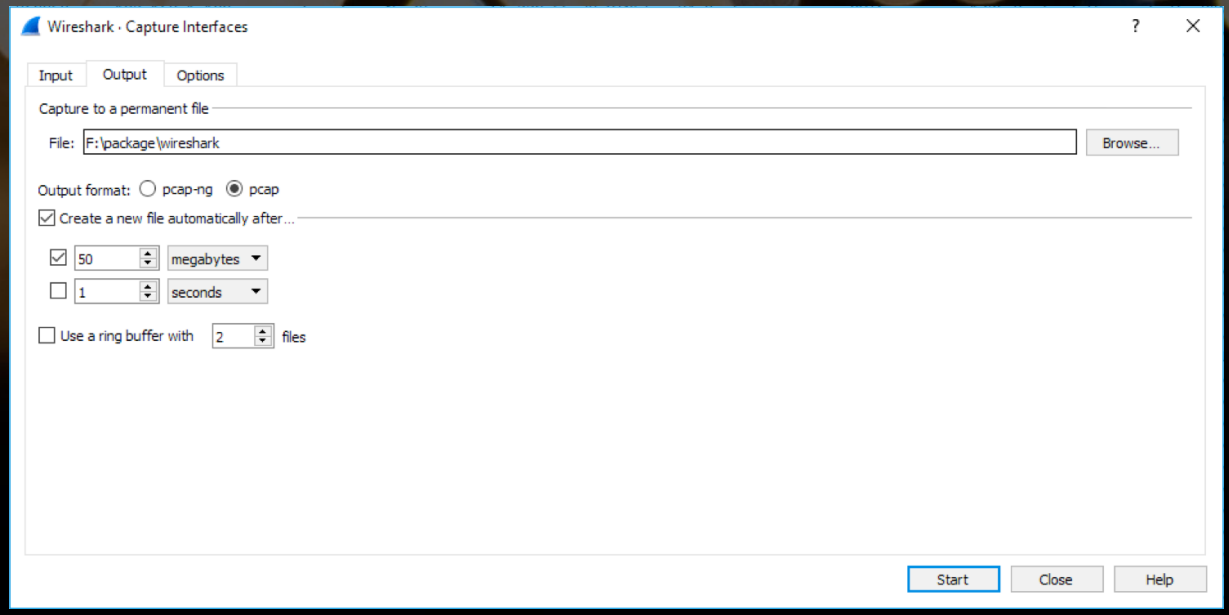

DrayTek Syslog 4.5.4
DrayTek
Syslog Utility
Write sdb file
Write txt file
192.168.1.1
Vigor2925
WAN Information
TX Rate
RX Rate
WAN1
2946653
95253
LAN Information
TX Packets
RX Packets
272133896
230326022
WAN IP (Fixed)
Gateway IP (Fixed)
140.112.202.144
140.112.202.254
Apply to:
All
Refresh
Firewall
VPN
User Access
Connection
WAN
IPPBX
Others
Pause
System Time
Router Time
Host
Message
2018-08-03 00:45:23 Aug 3 00:45:19 PA-Router Local User (MAC=F4-28-53-11-DF-17): 192.168.1.45:64012 -> 52.175.27.38:443 (TCP) close connection
2018-08-03 00:44:43 Aug 3 00:44:39 PA-Router Local User (MAC=00-11-32-4B-38-CA): 192.168.1.100:123 -> 216.239.35.0:123 (UDP)
2018-08-03 00:43:33 Aug 3 00:43:29 PA-Router Local User (MAC=F4-28-53-11-DF-17): 192.168.1.45:64012 -> 52.175.27.38:443 (TCP)
2018-08-03 00:40:12 Aug 3 00:40:08 PA-Router Local User (MAC=00-11-32-4B-38-CA): 192.168.1.100:123 -> 216.239.35.12:123 (UDP)
2018-08-03 00:39:47 Aug 3 00:39:43 PA-Router Local User (MAC=00-0C-29-92-2E-2F): 192.168.1.44:37055 -> 103.226.213.30:123 (UDP)
2018-08-03 00:38:01 Aug 3 00:37:57 PA-Router Local User (MAC=00-0C-29-92-2E-2F): 192.168.1.44:50666 -> 103.18.128.60:123 (UDP)
2018-08-03 00:37:57 Aug 3 00:37:53 PA-Router Local User (MAC=00-0C-29-92-2E-2F): 192.168.1.44:50984 -> 59.124.29.241:123 (UDP)
2018-08-03 00:37:40 Aug 3 00:37:36 PA-Router Local User (MAC=00-0C-29-92-2E-2F): 192.168.1.44:60799 -> 123.204.45.116:123 (UDP)
2018-08-03 00:36:15 Aug 3 00:36:11 PA-Router Local User (MAC=F4-28-53-11-DF-17): 192.168.1.45:64011 -> 117.18.237.29:80 (TCP) close connection
2018-08-03 00:35:15 Aug 3 00:35:11 PA-Router Local User (MAC=F4-28-53-11-DF-17): 192.168.1.45:64011 -> 117.18.237.29:80 (TCP)Web
2018-08-03 00:35:10 Aug 3 00:35:06 PA-Router Local User (MAC=F4-28-53-11-DF-17): 192.168.1.45:64003 -> 184.26.222.158:80 (TCP) close connection
2018-08-03 00:35:10 Aug 3 00:35:06 PA-Router Local User (MAC=F4-28-53-11-DF-17): 192.168.1.45:64000 -> 23.41.69.177:80 (TCP) close connection
2018-08-03 00:35:09 Aug 3 00:35:06 PA-Router Local User (MAC=F4-28-53-11-DF-17): 192.168.1.45:64002 -> 163.28.226.100:80 (TCP) close connection
2018-08-03 00:35:05 Aug 3 00:35:02 PA-Router Local User (MAC=F4-28-53-11-DF-17): 192.168.1.45:64006 -> 208.91.0.10:443 (TCP)
2018-08-03 00:34:15 Aug 3 00:34:11 PA-Router Local User (MAC=F4-28-53-11-DF-17): 192.168.1.45:64005 -> 163.28.224.120:443 (TCP)
2018-08-03 00:34:12 Aug 3 00:34:08 PA-Router Local User (MAC=F4-28-53-11-DF-17): 192.168.1.45:58521 -> 114.24.98.246:62435 (UDP)
2018-08-03 00:34:12 Aug 3 00:34:08 PA-Router Local User (MAC=F4-28-53-11-DF-17): 192.168.1.45:58521 -> 185.188.32.3:5938 (UDP)
2018-08-03 00:34:12 Aug 3 00:34:08 PA-Router Local User (MAC=F4-28-53-11-DF-17): 192.168.1.45:58521 -> 185.188.32.13:5938 (UDP)

Wireshark

- Filter – filter out unimportant information
- Output setting – output the pcap file periodically
- Zip – compress the pcap files

Wireshark

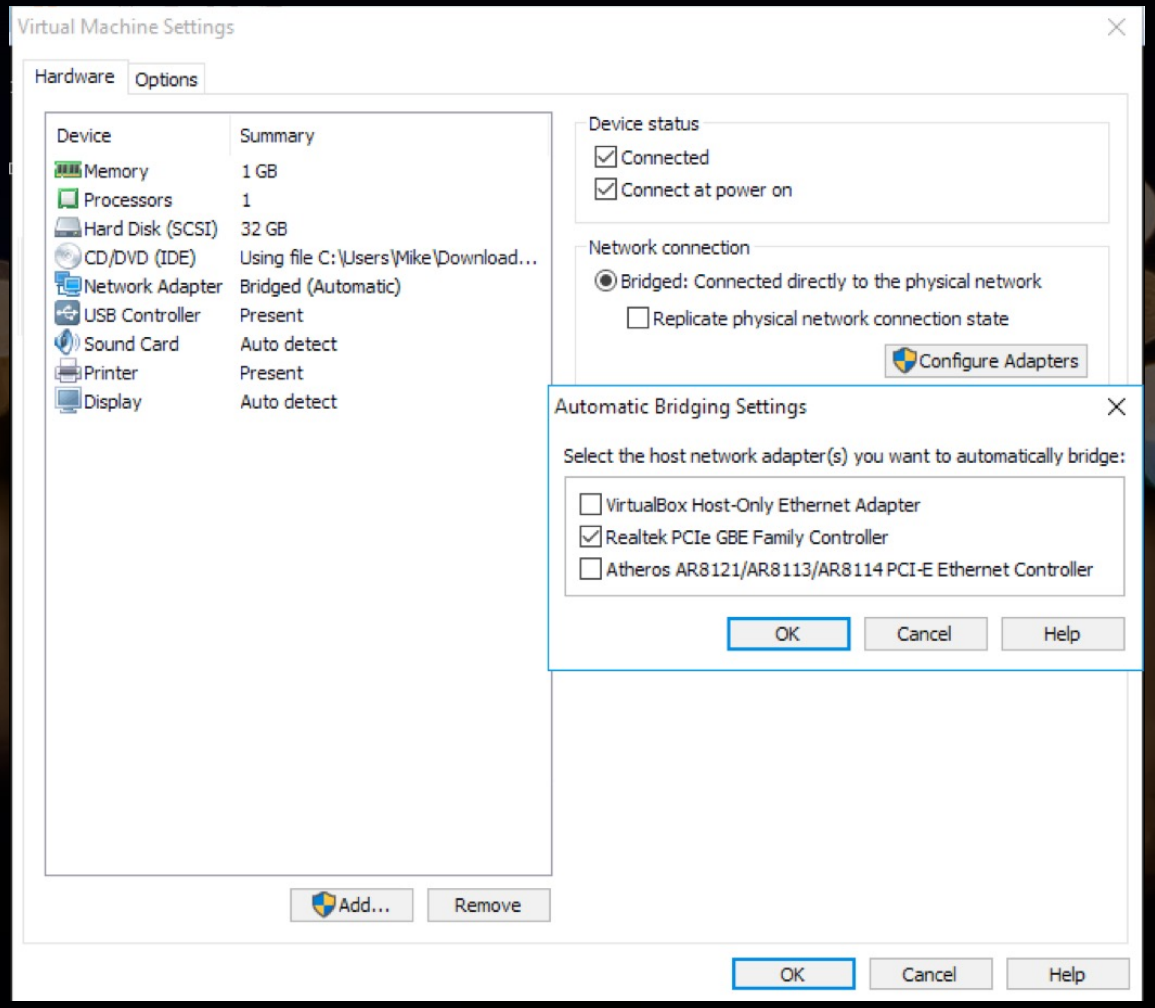

Wireshark · Capture Interfaces
Input
Output
Options
Interface
Traffic
Link-layer Header
Promi
Snaplen
Buffer (M
Monit
Capture Filter
VMware Network Adapter VMnet8
VMware Network Adapter VMnet1
VirtualBox Host-Only Network
Ethernet
Ethernet 2
USBPcap1
USBPcap2
USBPcap3
USBPcap4
USBPcap5
Ethernet
default
64
2
not ((src 192.168.1.103 and dst 192.168.1.45)
USBPcap
Enable promiscuous mode on all interfaces
Manage Interfaces...
Capture filter for selected interfaces:
ort 514) and not dst port 1900 and not broadcast and not (src net 192.168.1.0/24 and dst net 192.168.1.0/24)
Compile BPFs
Start
Close
Help


Wireshark · Capture Interfaces
Input
Output
Options
Capture to a permanent file
File:
F:\package\wireshark
Browse...
Output format:
pcap-ng
pcap
Create a new file automatically after...
50
megabytes
1
seconds
Use a ring buffer with
2
files
Start
Close
Help

Server (CentOS)

- 32-bit CentOS on VMWare on Windows
- Connected through ssh, either from LAN or WAN
- Bridged NIC on Eth2
- Radius server

Server (CentOS)



ssh

- No password access allowed (for safety issue)
- Must use key file to login
- Setup port forwarding to connect through WAN

Radius

- A protocol to work with WPA2 enterprise
- All AP query this server for user access control
- Current version on server: freeradius 3.0.16
- Multiple ports occupied currently as authentication ports
- Located at `/usr/local/etc/raddb`
- Log at `/usr/local/var/log/radius/radius.log`, or `$radlog`

Radius ports

- Port 1812: PA-Cloud-2.4G
- Port 5555: PA-Cloud-5G
- Port 5551: PA-Ground-2.4G
- Port 5553: PA-Ground-5G
- Port 5557: PA-Sky01 + PA-Sky02

- Config files at `/usr/local/etc/raddb/sites-enabled`
- Note: Dual-Band AP must set two different authentication port for each SSID

Useful tools

- `fcron`
  - Executes scheduled tasks
  - Calibrates the clock periodically
  - Output heartbeats to a tmp file
- `lsof`
  - Shows opened files by a process
  - Shows the process occupying a specific port (e.g. `lsof -i:1812`)
- `nmap`
  - IP scan (e.g. `nmap -sn 192.168.1.0/24`)
- More at `/root/Documents/IT/Notes`

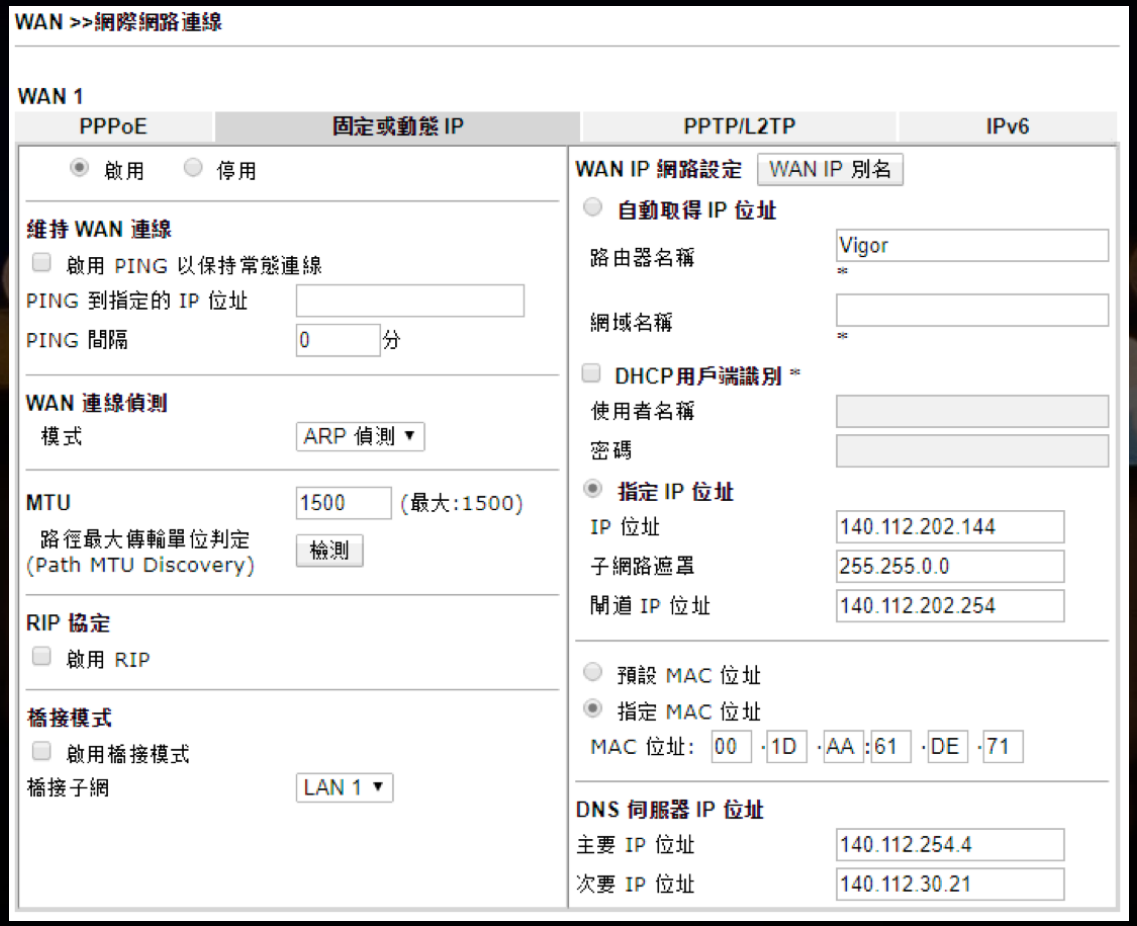
Router

- Model: DrayTek Vigor 2925
- Location: Iron cabinet in the office
- DHCP Server
- Firewall
- Syslog
- The one and only machine that uses WAN port

WAN Setting

- Fixed IP
- IP: 140.112.202.144
- Mask: 255.255.0.0
- Gateway: 140.112.202.254
- DNS1: 140.112.254.4 (CINC)
- DNS2: 140.112.30.21 (CSIE)

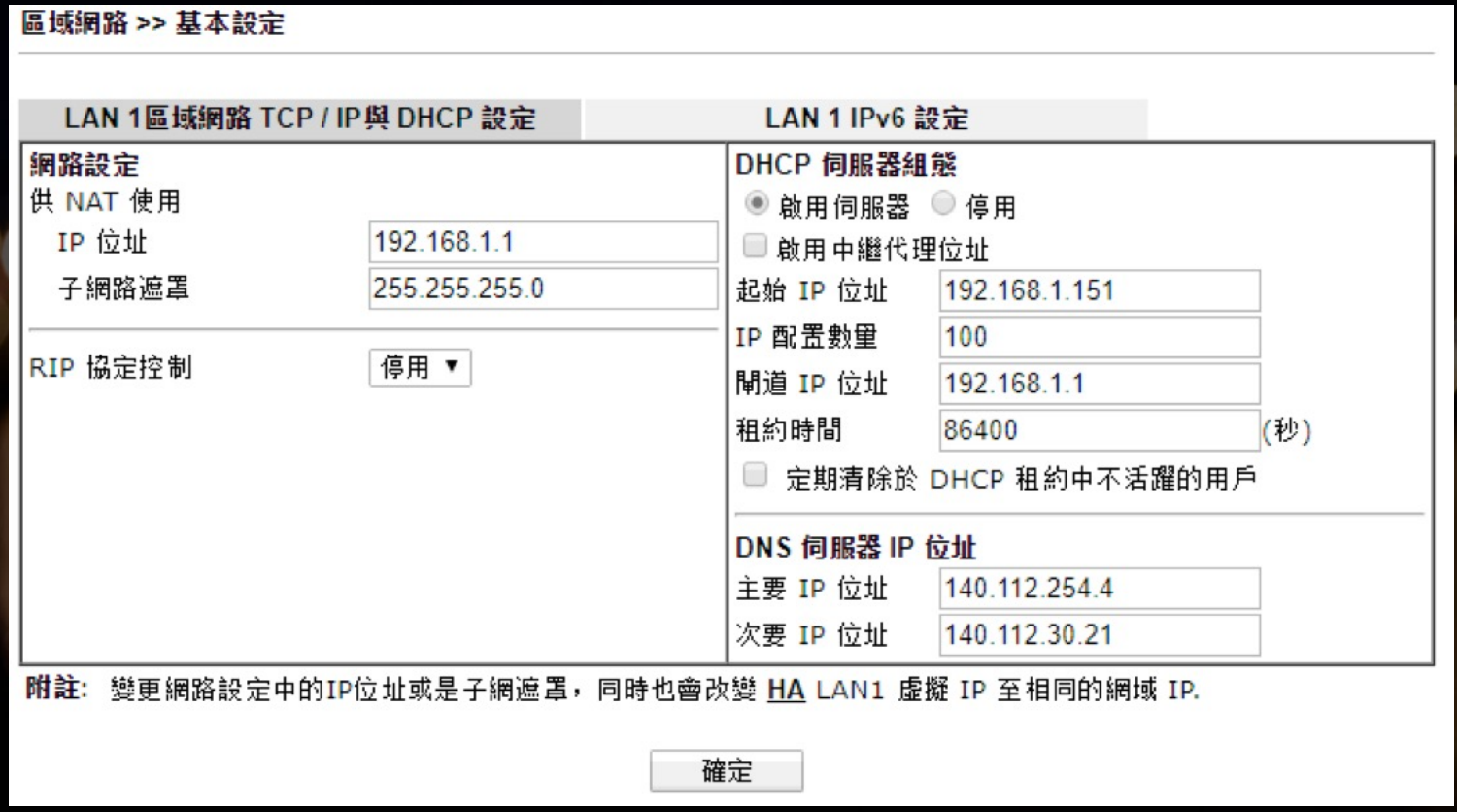
WAN Setting


WAN >>網際網路連線
WAN 1
PPPoE
固定或動態 IP
PPTP/L2TP
IPv6
啟用
停用
維持 WAN 連線
啟用 PING 以保持常態連線
PING 到指定的 IP 位址
PING 間隔
0
分
WAN 連線偵測
模式
ARP 偵測
MTU
1500
(最大:1500)
路徑最大傳輸單位判定 (Path MTU Discovery)
檢測
RIP 協定
啟用 RIP
橋接模式
啟用橋接模式
橋接子網
LAN 1
WAN IP 網路設定
WAN IP 別名
自動取得 IP 位址
路由器名稱
Vigor
網域名稱
DHCP用戶端識別
使用者名稱
密碼
指定 IP 位址
IP 位址
140.112.202.144
子網路遮罩
255.255.0.0
閘道 IP 位址
140.112.202.254
預設 MAC 位址
指定 MAC 位址
MAC 位址:
00
1D
AA
61
DE
71
DNS 伺服器 IP 位址
主要 IP 位址
140.112.254.4
次要 IP 位址
140.112.30.21

LAN Setting

- Router IP: 192.168.1.1
- Mask: 255.255.255.0
- DHCP: on

LAN Setting


區域網路 >> 基本設定
LAN 1區域網路 TCP / IP與 DHCP 設定
LAN 1 IPv6 設定
網路設定
供 NAT 使用
IP 位址
192.168.1.1
子網路遮罩
255.255.255.0
RIP 協定控制
停用
DHCP 伺服器組態
啟用伺服器
停用
啟用中繼代理位址
起始 IP 位址
192.168.1.151
IP 配置數量
100
閘道 IP 位址
192.168.1.1
租約時間
86400
(秒)
定期清除於 DHCP 租約中不活躍的用戶
DNS 伺服器 IP 位址
主要 IP 位址
140.112.254.4
次要 IP 位址
140.112.30.21
附註: 變更網路設定中的IP位址或是子網遮罩，同時也會改變 HA LAN1 虛擬 IP 至相同的網域 IP.
確定

ARP Table

- ARP (Address Resolution Protocol) maps given device (MAC) to a specific fixed IP
- Useful for network manager to identify unauthenticated devices
- To assure a device (e.g. X32) obtains a given IP even with DHCP

ARP Table

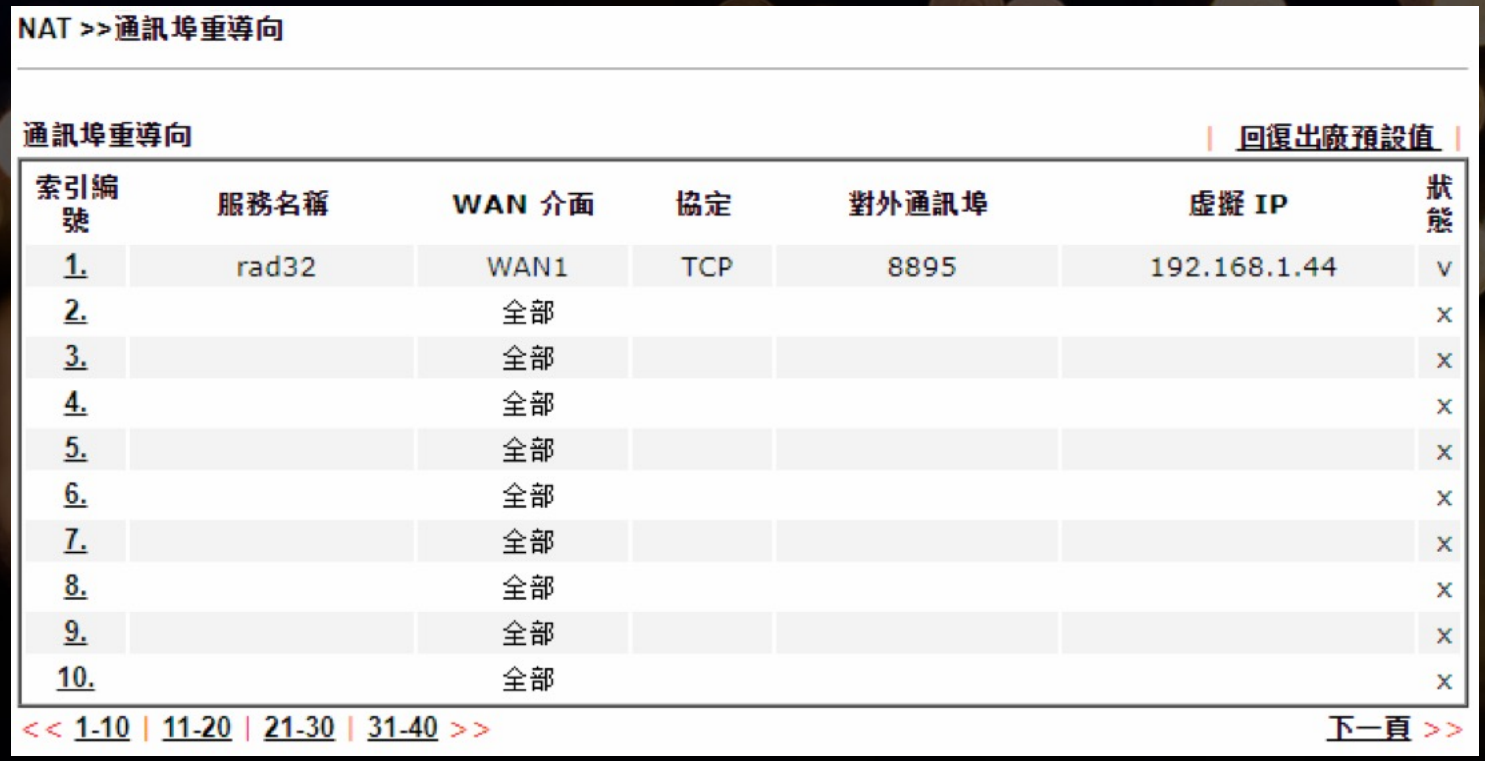

區域網路 >> 綁定 IP 與 MAC 位址
綁定 IP 與 MAC 位址
啟用
停用
限制綁定
ARP 表
全選 | 排序 | 更新頁面
IP 位址 MAC 位址
192.168.1.199 70-8B-CD-7E-A0-8E
192.168.1.200 1C-9E-46-30-AB-34
192.168.1.201 14-20-5E-F0-73-16
192.168.1.202 40-98-AD-14-37-49
192.168.1.203 94-E9-6A-46-A8-42
192.168.1.204 B4-52-7E-8F-8C-7F
192.168.1.205 32-52-97-11-F0-6A
192.168.1.206 6C-4D-73-F2-0D-DD
IP綁定清單 (限制: 300 輸入項)
全選 | 排序
索引編號 IP 位址 MAC 位址
1 192.168.1.5 18-D6-C7-FC-86-B8
2 192.168.1.6 38-D5-47-42-1F-F4
3 192.168.1.7 38-D5-47-42-22-50
4 192.168.1.8 34-97-F6-3E-63-00
5 192.168.1.44 00-0C-29-92-2E-2F
6 192.168.1.45 F4-28-53-11-DF-17
7 192.168.1.46 00-24-8C-C4-B9-98
8 192.168.1.54 78-BA-D0-0A-06-7E
9 192.168.1.55 00-0C-D0-01-06-FD
10 192.168.1.60 78-E7-D1-A5-C5-29
11 192.168.1.62 00-15-64-00-BF-68
12 192.168.1.68 00-1E-C0-27-5C-D6
13 192.168.1.70 90-1B-0E-88-7E-8D
14 192.168.1.101 DC-56-E7-05-4F-2A
新增或是更新
IP 位址
MAC 位址
說明
顯示說明
新增
更新
刪除
附註: IP-MAC 綁定後， DHCP的配發，將依該清單分配。
如果選擇了限制綁定項目，任何一個未與MAC綁定的IP即無法存取網際網路。
確定

Port Mirroring

- Mirroring flows of the whole network to a port on router

Port Forwarding

- Forwarding a port of WAN to the specified port in LAN



NAT >>通訊埠重導向

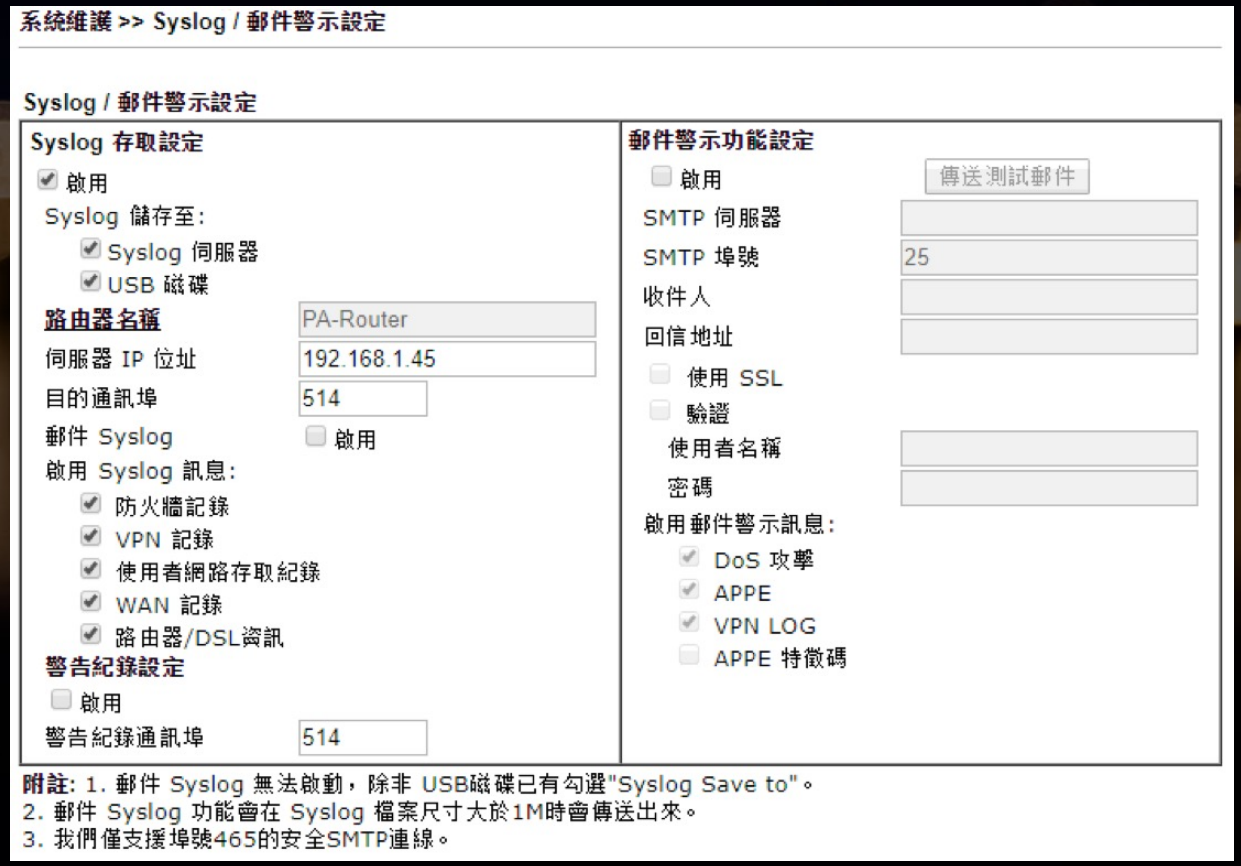
通訊埠重導向 | 回復出廠預設值 |

索引編號	服務名稱	WAN 介面	協定	對外通訊埠	虛擬 IP	狀態
1.	rad32	WAN1	TCP	8895	192.168.1.44	v
2.		全部				x
3.		全部				x
4.		全部				x
5.		全部				x
6.		全部				x
7.		全部				x
8.		全部				x
9.		全部				x
10.		全部				x

<< 1-10 | 11-20 | 21-30 | 31-40 >> 下一頁 >>

Syslog

- Saved on server and USB disk concurrently



Firewall

- Block consoles to WAN

AP

- WPA2 enterprise
- Location
- Topology

WPA2 Enterprise

- Individual account/password for each person, rather than a public password shared by a group of people.
- Needs a Radius server to manage the authentication.
- The account/password is totally the same no matter connected to which AP.
- More on radius

WPA2 Enterprise

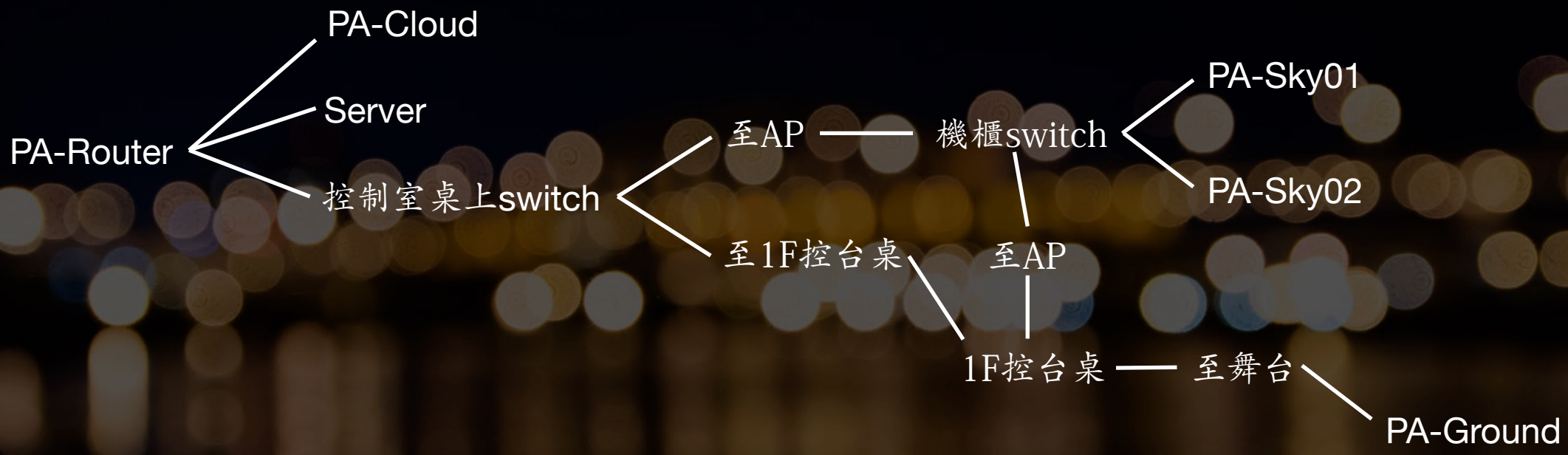
Location of APs

- PA-Cloud: 組辦
- PA-Sky01: 禮堂天上近控台側
- PA-Sky02: 禮堂天上近舞台側
- PA-Ground: 非常駐AP，通常架在禮堂1F

Location of APs

- PA-Cloud: In the office
- PA-Sky01: In the auditorium, on the console side
- PA-Sky02: In the auditorium, on the stage side
- PA-Ground: Not a permanent AP, often lies at 1F of the auditorium when it appears

Topology


PA-Cloud
Server
PA-Router
控制室桌上switch
至AP
機櫃switch
PA-Sky01
PA-Sky02
至1F控台桌
至AP
1F控台桌
至舞台
PA-Ground