智慧網管之原理與實做方法

顯赫資訊 鄭鈞文
kaiser@gentrice.net

關於我

- VoIP
- 緣起
    - 網通廠代工(課製化) Dx, Ex, Cx, Fx..
    - 網管專案
- 前瞻計畫
    - 縣市教網-智慧網管

主題

一、傳統網管與智慧網管的差異

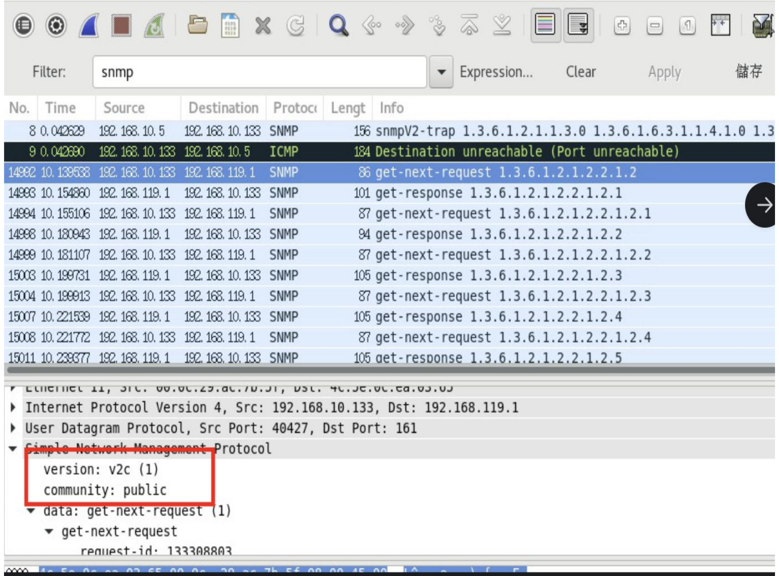
二、IoT智慧網管架構與實做

三、未來展望

一、傳統網管與智慧網管的差異

傳統網管

- 集中蒐集
  - SNMP
  - Syslog
  - Netflow
- 優點
- 缺點
- 網管的範圍
  - 大型
    - 集中、分散架構
  - 小型



傳統上：網管五大面向

國際標準FCAPS	
Fault Management 障礙管理	辨別可能的故障原因 並免日後同樣問題重複發生
Configuration Management 設置管理	妥善設備相關設定 網路拓樸偵測
Accounting Management 訊務管理	使用者及使用稽核 讓資源公平、有效利用
Performance Management 效能管理	避免瓶頸 發揮系統網路應有效能
Security Management 安全管理	確保資訊安全，強化資安

FAB

ITU - business process framework

Fulfillment

Assurance

Billing

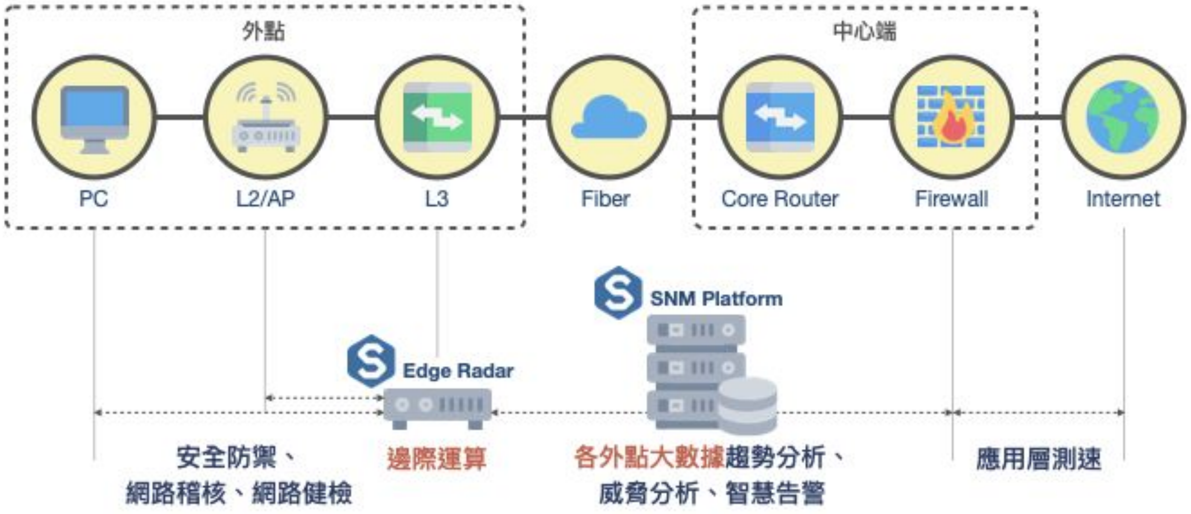
工具的演變

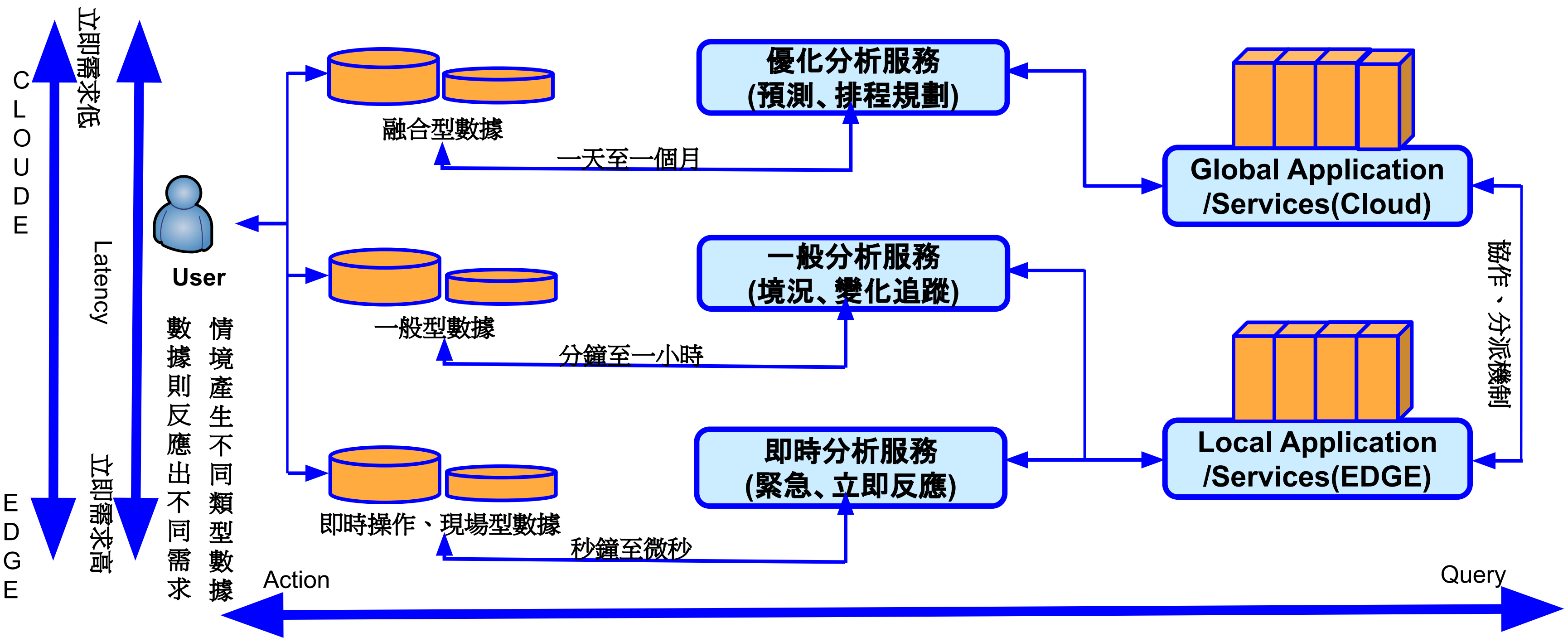
智慧網管的目的

- 降低學習門檻
  - 沒事不用看系統
  - 處理事件流程化
  - 不用學操作／不用記憶系統選單
- 減少網路斷線／故障時間
- 智慧化
  - 結合單位行事曆
  - 多點診斷
  - 交談式

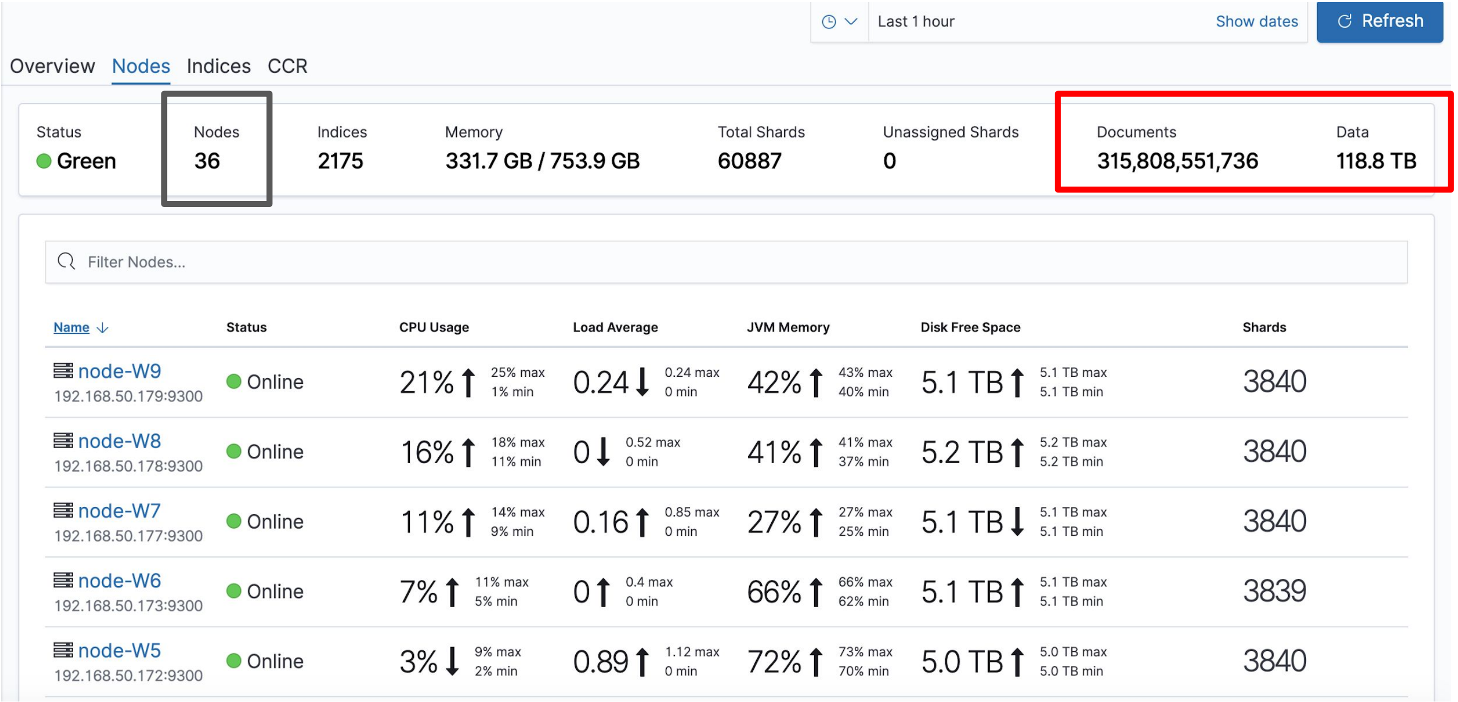
二、IoT智慧網管架構與實做

IOT edge computing

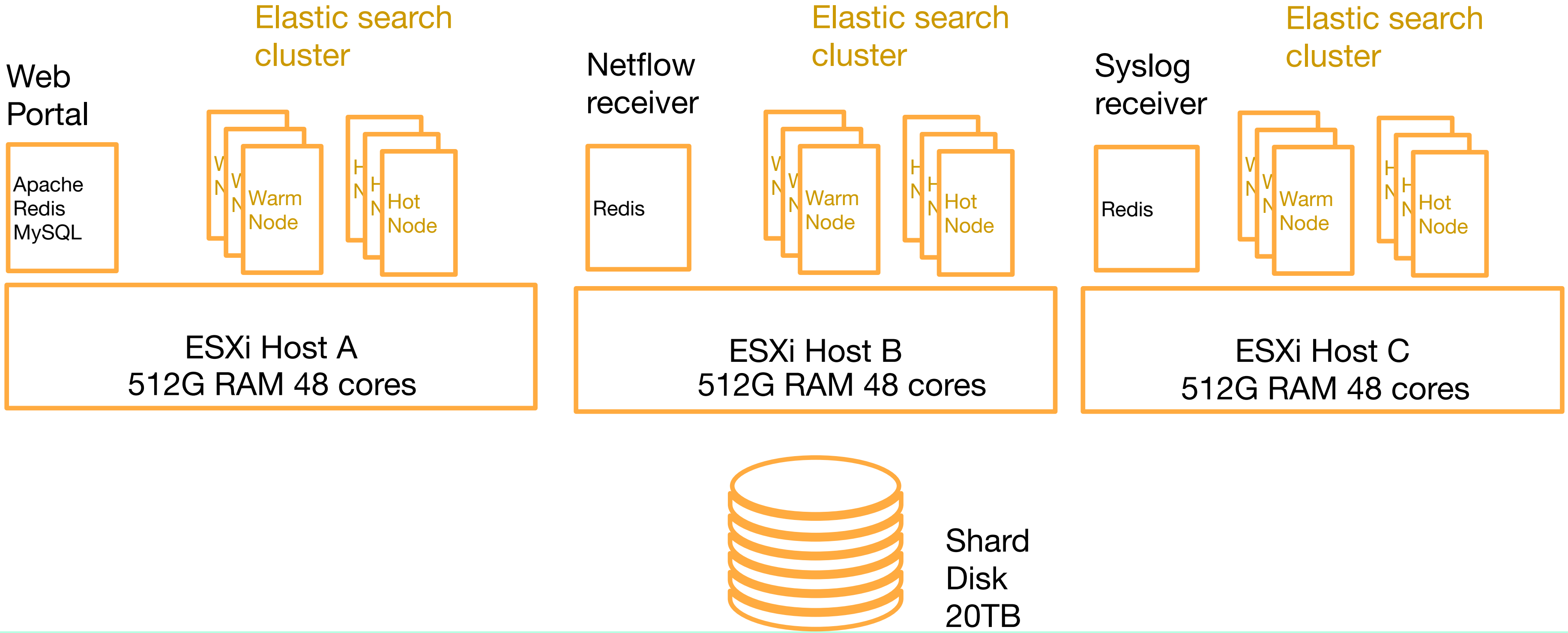



CLOUDE
立即需求低
Latency
立即需求高
EDGE
User
情境產生不同類型數據
數據則反應出不同需求
融合型數據
一天至一個月
一般型數據
分鐘至一小時
即時操作、現場型數據
秒鐘至微秒
優化分析服務
(預測、排程規劃)
一般分析服務
(境況、變化追蹤)
即時分析服務
(緊急、立即反應)
Global Application
/Services(Cloud)
Local Application
/Services(EDGE)
協作、分派機制
Action
Query

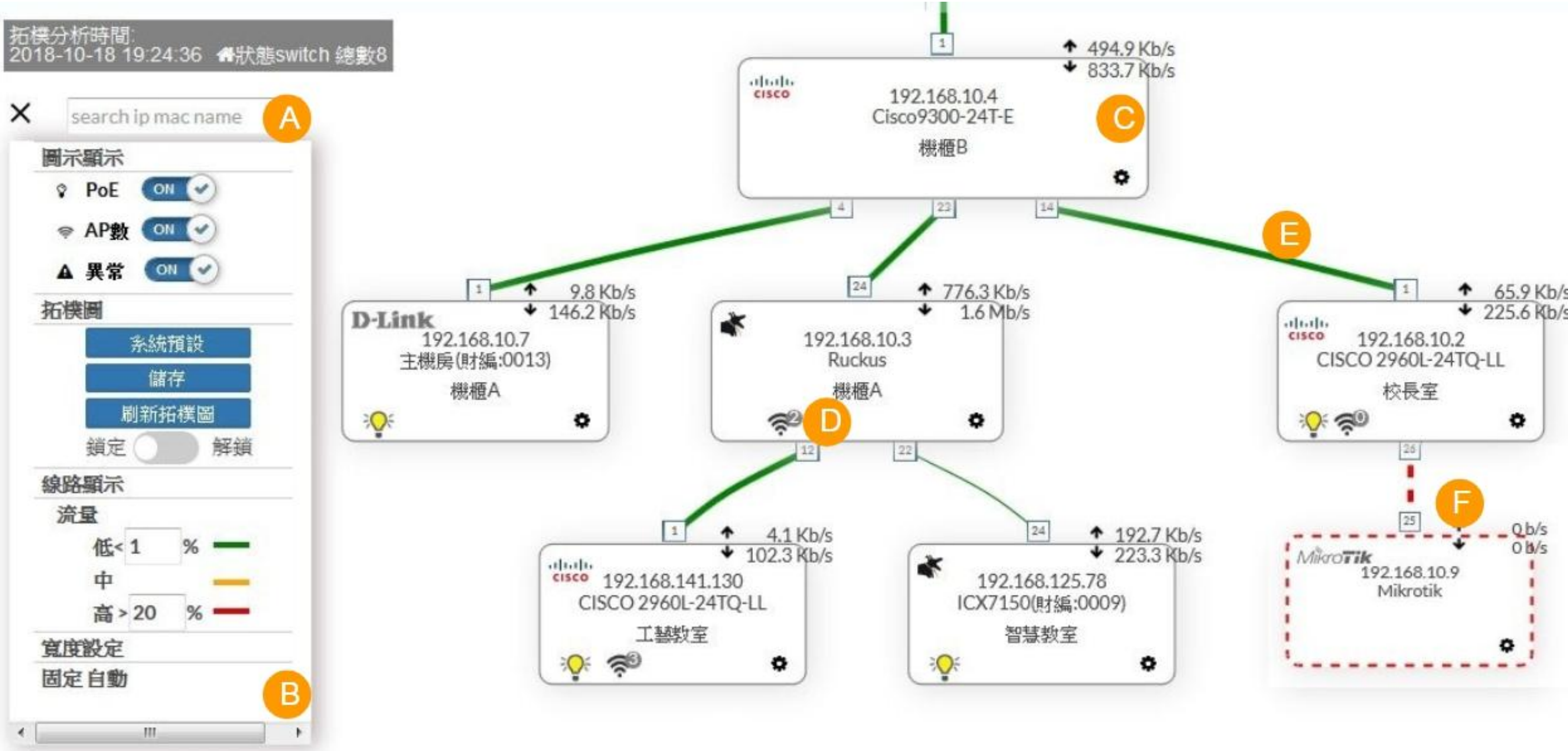
Huge volume of data



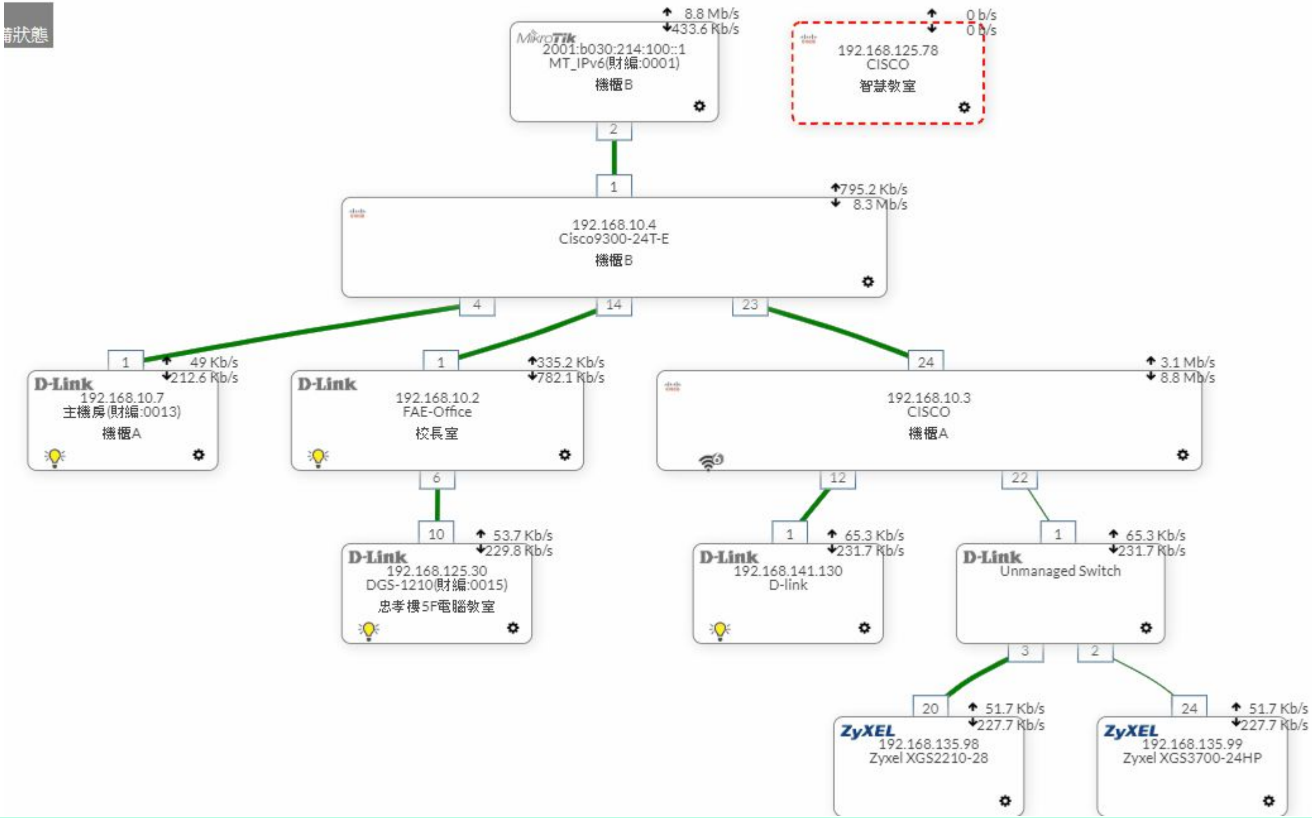
VMWARE PLAN


Web Portal
Apache
Redis
MySQL
Elastic search cluster
Warm Node
Hot Node
ESXi Host A
512G RAM 48 cores
Netflow receiver
Redis
Elastic search cluster
Warm Node
Hot Node
ESXi Host B
512G RAM 48 cores
Syslog receiver
Redis
Elastic search cluster
Warm Node
Hot Node
ESXi Host C
512G RAM 48 cores
Shard Disk 20TB

拓樸圖


拓樸分析時間:
2018-10-18 19:24:36 狀態switch 總數8
search ip mac name
A
圖示顯示
PoE ON
AP數 ON
異常 ON
拓樸圖
系統預設
儲存
刷新拓樸圖
鎖定 解鎖
線路顯示
流量
低< 1 %
中
高 > 20 %
寬度設定
固定 自動
B
494.9 Kb/s
833.7 Kb/s
192.168.10.4
Cisco9300-24T-E
機櫃B
C
9.8 Kb/s
146.2 Kb/s
D-Link
192.168.10.7
主機房(財編:0013)
機櫃A
776.3 Kb/s
1.6 Mb/s
192.168.10.3
Ruckus
機櫃A
D
E
65.9 Kb/s
225.6 Kb/s
192.168.10.2
CISCO 2960L-24TQ-LL
校長室
F
4.1 Kb/s
102.3 Kb/s
192.168.141.130
CISCO 2960L-24TQ-LL
工藝教室
192.7 Kb/s
223.3 Kb/s
192.168.125.78
ICX7150(財編:0009)
智慧教室
0 b/s
0 b/s
MikroTik
192.168.10.9
Mikrotik

VALN管理



狀態
8.8 Mb/s
433.6 Kb/s
MikroTik
2001:b030:214:100::1
MT_IPv6(財編:0001)
機櫃B
0 b/s
0 b/s
192.168.125.78
CISCO
智慧教室
2
1
795.2 Kb/s
8.3 Mb/s
192.168.10.4
Cisco9300-24T-E
機櫃B
4
14
23
1
49 Kb/s
212.6 Kb/s
D-Link
192.168.10.7
主機房(財編:0013)
機櫃A
1
335.2 Kb/s
782.1 Kb/s
D-Link
192.168.10.2
FAE-Office
校長室
24
3.1 Mb/s
8.8 Mb/s
192.168.10.3
CISCO
機櫃A
6
10
53.7 Kb/s
229.8 Kb/s
D-Link
192.168.125.30
DGS-1210(財編:0015)
忠孝樓5F電腦教室
12
22
1
65.3 Kb/s
231.7 Kb/s
D-Link
192.168.141.130
D-link
1
65.3 Kb/s
231.7 Kb/s
D-Link
Unmanaged Switch
3
2
20
51.7 Kb/s
227.7 Kb/s
ZyXEL
192.168.135.98
Zyxel XGS2210-28
24
51.7 Kb/s
227.7 Kb/s
ZyXEL
192.168.135.99
Zyxel XGS3700-24HP

拓樸執行比較

時間複雜度O(nlogn)

中南部 200所中小學

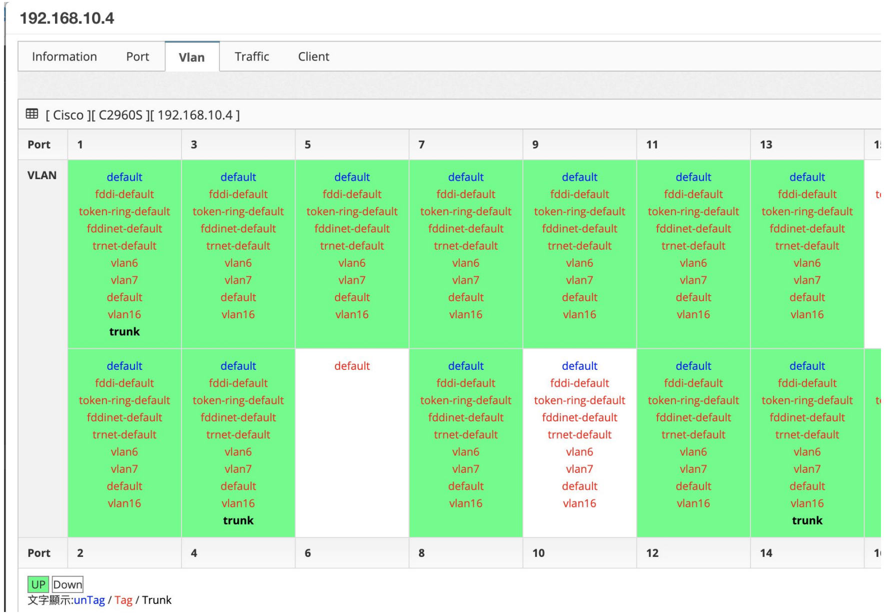
	雲端版	IoT版
執行時間	131分鐘	2分鐘
網路資料量	120MB	4MB
CPU	40%	90%

拓樸圖

- algorithm
- 更新方式
  - 拓樸的穩定度
- 非tree 架構
- stacking,redundant…
- topology comparison

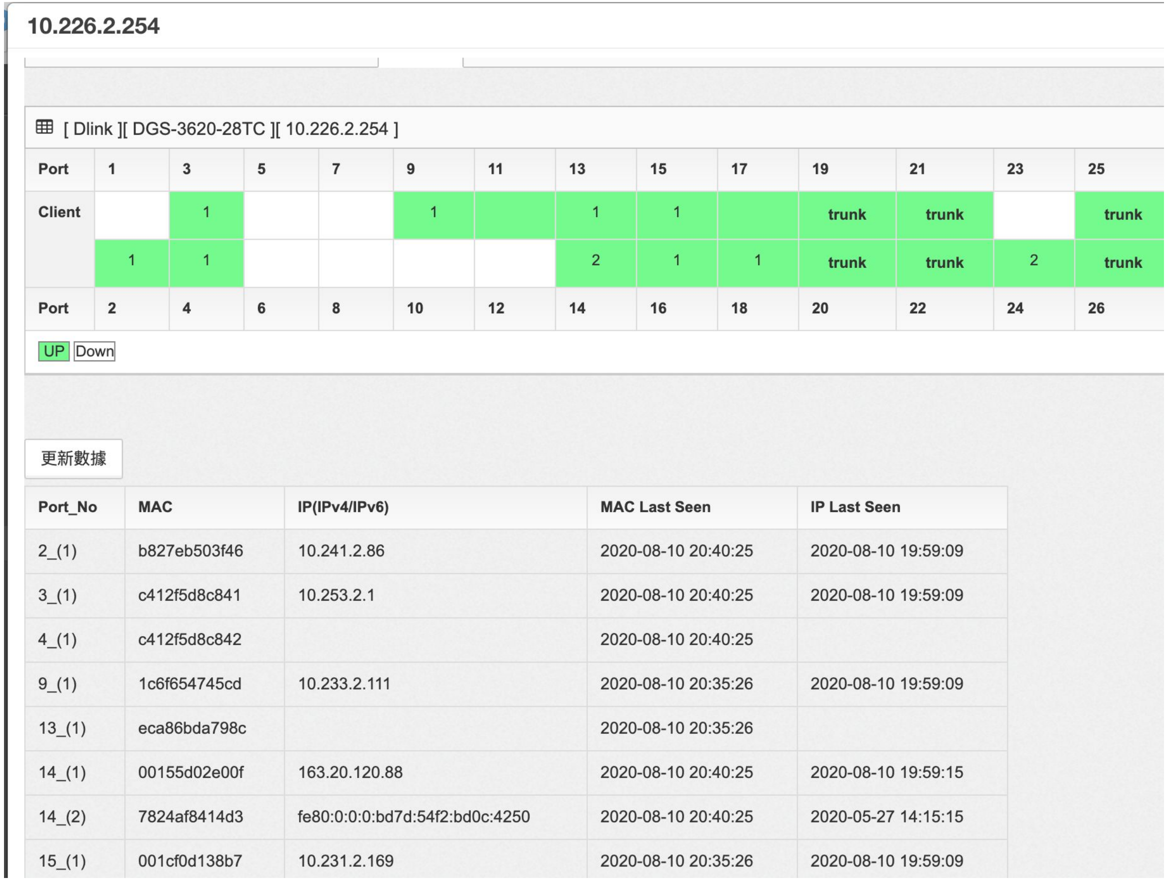
拓樸圖的重要性

- 抽象層
- IP-MAC-Port 對應資料



IP-MAC

- Switch
- Broadcast
  - ARP
  - NDP



10.226.2.254

[Dlink][DGS-3620-28TC][10.226.2.254]

Port	1	3	5	7	9	11	13	15	17	19	21	23	25
Client		1			1		1	1		trunk	trunk		trunk
	1	1					2	1	1	trunk	trunk	2	trunk
Port	2	4	6	8	10	12	14	16	18	20	22	24	26

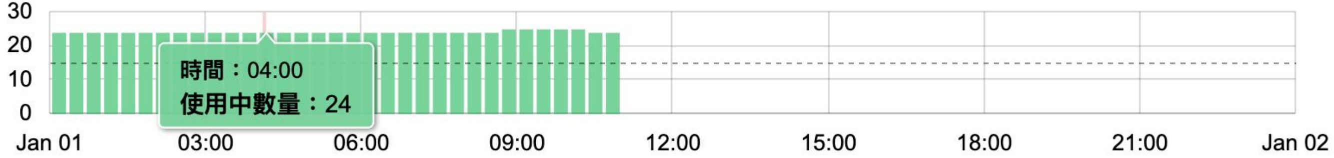
UP Down

更新數據

Port_No	MAC	IP(IPv4/IPv6)	MAC Last Seen	IP Last Seen
2_(1)	b827eb503f46	10.241.2.86	2020-08-10 20:40:25	2020-08-10 19:59:09
3_(1)	c412f5d8c841	10.253.2.1	2020-08-10 20:40:25	2020-08-10 19:59:09
4_(1)	c412f5d8c842		2020-08-10 20:40:25	
9_(1)	1c6f654745cd	10.233.2.111	2020-08-10 20:35:26	2020-08-10 19:59:09
13_(1)	eca86bda798c		2020-08-10 20:35:26	
14_(1)	00155d02e00f	163.20.120.88	2020-08-10 20:40:25	2020-08-10 19:59:15
14_(2)	7824af8414d3	fe80:0:0:0:bd7d:54f2:bd0c:4250	2020-08-10 20:40:25	2020-05-27 14:15:15
15_(1)	001cf0d138b7	10.231.2.169	2020-08-10 20:35:26	2020-08-10 19:59:09

本日 IP 活動

更新時間：10:44:19

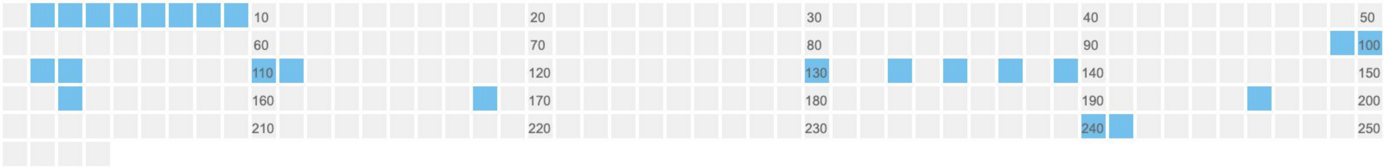


請移動上方捲軸，查看各時間 IP 活動資訊。

時間 04:00 使用中數量 24

使用中 未使用

網段：192.168.10.1 ～ 192.168.10.254




更新時間：10:45:23
使用中 IP 數量
10
5
0
Jan 01
03:00
06:00
09:00
12:00
15:00
18:00
21:00
Jan 02
時間：04:00
使用中數量：1
請移動上方捲軸，查看各時間 IP 活動資訊。
時間 04:00
使用中數量 1
使用中
未使用
網段：192.168.5.0 ～ 192.168.5.255
0
10
20
30
40
50
60
70
80
90
100
110
120
130
140
150
160
170
180
190
200
210
220
230
240
250

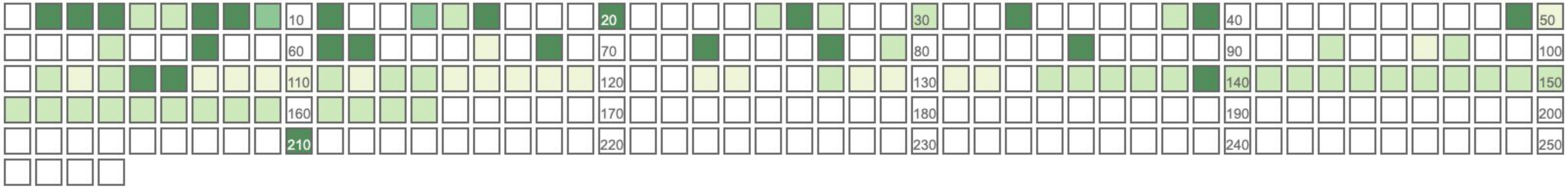
本日 IP 使用度

×

更新時間：10:46:22

☐ 30天以上無使用 ☐ 30天內使用 ☐ 15天內使用 ☐ 1天內使用 ■ 20分鐘內使用

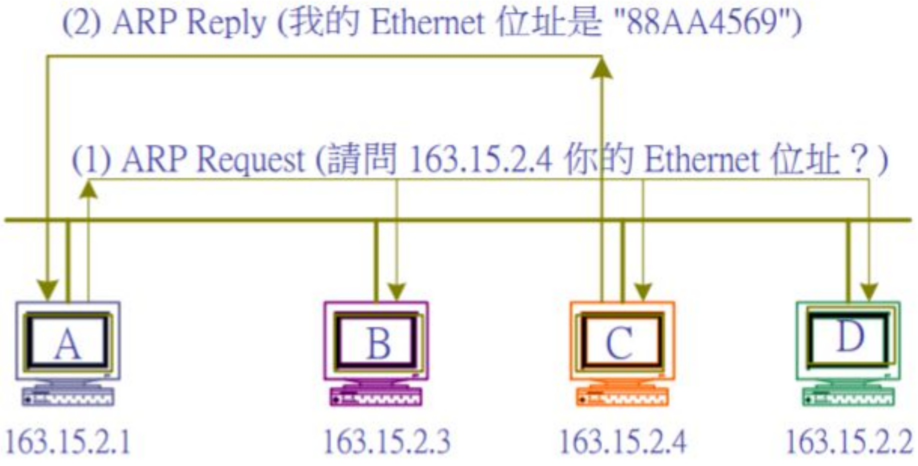
網段：192.168.3.1 ～ 192.168.3.254



ARP

- Listen
- Query
  - IP 衝突
- Buffer time, Time to Live

```
ARPING 10.241.31.69
60 bytes from 98:ee:cb:b4:8c:a5
(10.241.31.69): index=0 time=8.589 msec
60 bytes from 00:c0:ee:86:65:45
(10.241.31.69): index=1 time=8.729 msec
```



NDP (Neighbor Discovery Protocol)

- NDP 協定透過ICMPv6完成以下功能:
  - 1.無狀態的網路介面自動設定 -- 使設備不需要DHCP Server就能自動取得IP
  - 2. 位址解析: IP對應成MAC
  - 3. 鄰居偵測: 鄰近設備是否無法連結 (NUD,)
  - 4. **重複位址偵測**: 先檢查IP是否已被取用(DAD).

Router Solicitation (Type 133)

Hosts inquire with Router Solicitation messages
generate Router Advertisements immediately u

Router Advertisement (Type 134)

Routers advertise their presence together with
message.

Neighbor Solicitation (Type 135)

Neighbor solicitations are used by nodes to det
cached link layer address.

Neighbor Advertisement (Type 136)

Neighbor advertisements are used by nodes to

Redirect (Type 137)

mac: 38f9d373afa6 × + Add filter

mac_info_event-*

elected fields

_source

vailable fields

pular

type

_id

_index

_score

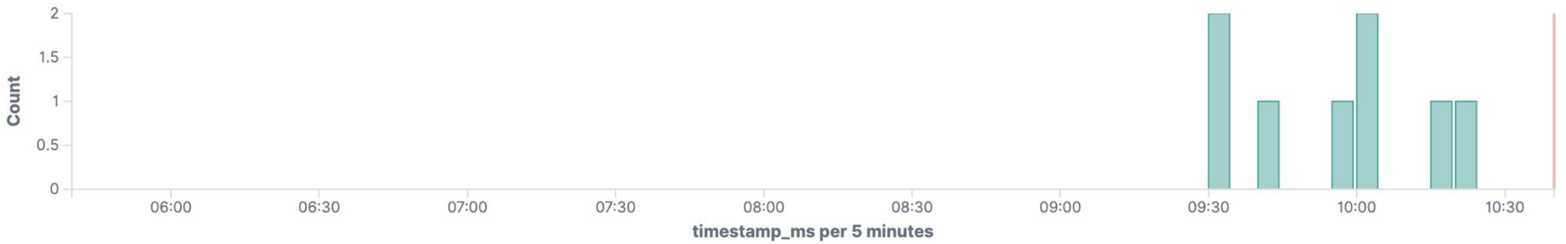
_type

dhcp_fingerprint_last_see...

final_dhcp_fingerprint

final_hostname

Aug 24, 2020 @ 05:39:56.290 - Aug 24, 2020 @ 10:39:56.290 — Auto

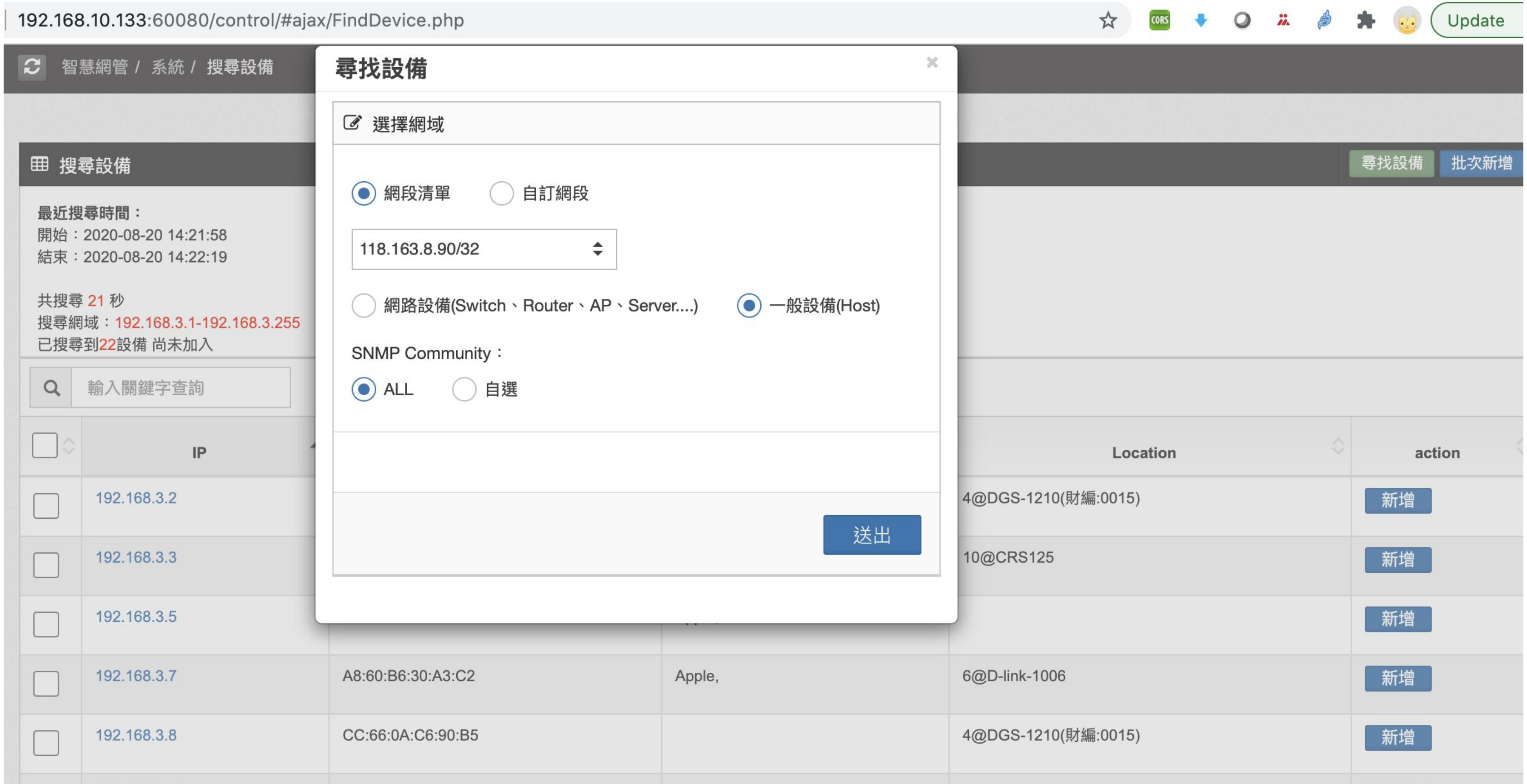


Time	_source
Aug 24, 2020 @ 10:20:07.410	mac: 38f9d373afa6 radar_mac: 0060e06e67a0 location_last_seen_ms: Aug 24, 2020 @ 10:00:22.096 dhcp_fingerprint_last_seen_ms: Aug 24, 2020 @ 09:54:22.762 final_hostname: MACBOOKPRO-AFA6 final_ipv6_list: fe80:0:0:0:14b8:c36a:49b5:30a6 final_location_sw_port: 4 timestamp_ms: Aug 24, 2020 @ 10:20:07.410 type: snapshot final_location_sw_ip: 192.168.125.30 final_dhcp_fingerprint: 1,121,3,6,15,119,252,95,44,46 ipv4_list_last_seen_ms: Aug 24, 2020 @ 10:17:10.469 final_ipv4_list: 192.168.3.11 final_location_sw_id: 170

Table JSON

_id	mG5AHnQB6mEwg0IxUOxk
_index	mac_info_event-2020.08.24
_score	-
_type	_doc
dhcp_fingerprint_last_seen_ms	Aug 24, 2020 @ 09:54:22.762
final_dhcp_fingerprint	1,121,3,6,15,119,252,95,44,46
final_hostname	MACBOOKPRO-AFA6
final_ipv4_list	192.168.3.11
final_ipv6_list	fe80:0:0:0:14b8:c36a:49b5:30a6
final_location_sw_id	170
final_location_sw_ip	192.168.125.30
final_location_sw_port	4
hostname_last_seen_ms	Aug 24, 2020 @ 10:15:13.022
ipv4_list_last_seen_ms	Aug 24, 2020 @ 10:15:13.014
ipv6_list_last_seen_ms	Aug 24, 2020 @ 10:13:50.143
location_last_seen_ms	Aug 24, 2020 @ 10:00:22.096
mac	38f9d373afa6
radar_mac	0060e06e67a0
timestamp_ms	Aug 24, 2020 @ 10:15:13.023
type	update_hostname_by_nbns
unit_id	66

網路週邊設備偵測



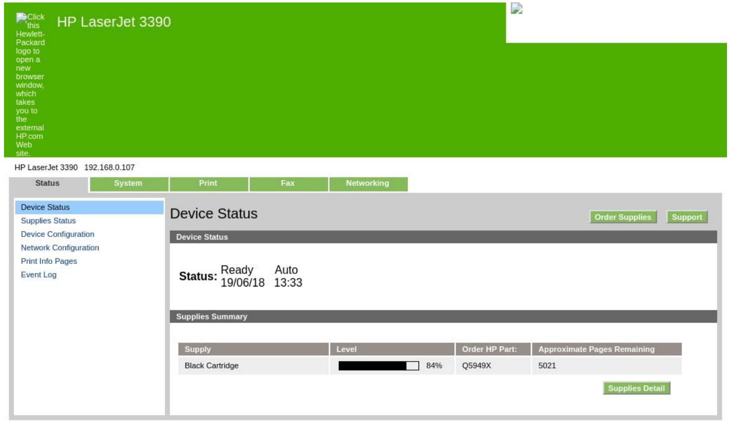
192.168.10.133:60080/control/#ajax/FindDevice.php
Update
智慧網管 / 系統 / 搜尋設備
搜尋設備
最近搜尋時間：
開始：2020-08-20 14:21:58
結束：2020-08-20 14:22:19
共搜尋 21 秒
搜尋網域：192.168.3.1-192.168.3.255
已搜尋到22設備 尚未加入
輸入關鍵字查詢
IP
Location
action
192.168.3.2
4@DGS-1210(財編:0015)
新增
192.168.3.3
10@CRS125
新增
192.168.3.5
新增
192.168.3.7
A8:60:B6:30:A3:C2
Apple,
6@D-link-1006
新增
192.168.3.8
CC:66:0A:C6:90:B5
4@DGS-1210(財編:0015)
新增
尋找設備
批次新增
尋找設備
選擇網域
網段清單
自訂網段
118.163.8.90/32
網路設備(Switch、Router、AP、Server....)
一般設備(Host)
SNMP Community：
ALL
自選
送出

網路週邊設備偵測

```
[20190618-01:06:44] ["Retrieving model from title"]
[20190618-01:06:44] ["Model=HP LaserJet 3390   192.168.0.107"]
[20190618-01:06:44] ["Login form not found"]
[20190618-01:06:44] ["Checking if unauthorized..."]
[20190618-01:06:44] ["All good, continue"]
[20190618-01:06:44] ["Status=BAD"]
[20190618-01:06:49] ["Screenshot start..."]
Taking screenshot as 192.168.0.107 00-1a-4b-21-ae-b9 BAD.jpg
[20190618-01:06:50] ["Screenshot end!"]

RESULTS
=======
IP......... 192.168.0.107
MAC........ 00:1a:4b:21:ae:b9
Vendor..... HewlettP    Hewlett Packard
Model...... HP LaserJet 3390   192.168.0.107
Security... BAD
============================================
DEVICE PROBE FINISH
============================================

Process finished
[moulder@radar v2]$
```



Speedtest

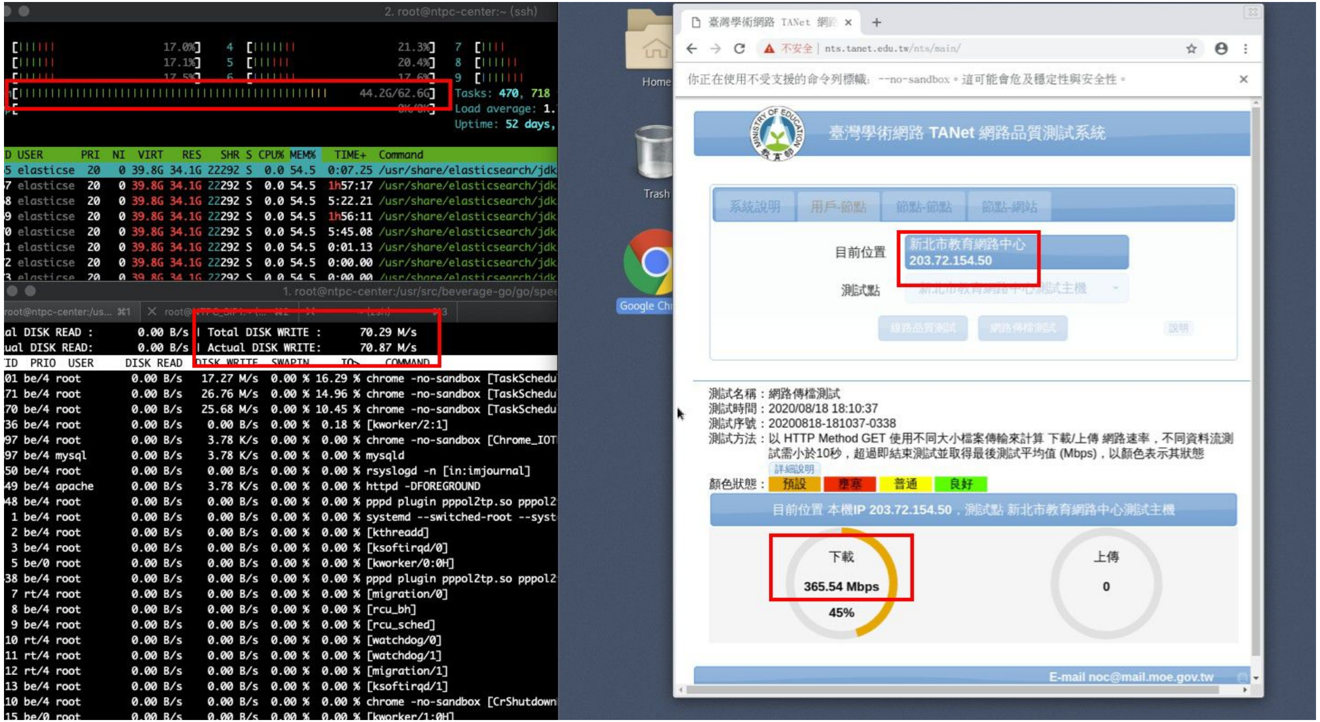
http://nts.tanet.edu.tw/nts/main/

```
Servers:
        Id  ip                  Name
        2   192.192.63.2        台北主節點測試主機
        3   192.192.63.18       新竹主節點測試主機
        4   192.192.63.26       台中主節點測試主機
        5   192.192.63.34       台南主節點測試主機
        6   192.192.63.189      中研院測試主機
        7   192.192.63.197      科技大樓測試主機
        8   192.192.63.85       臺北區網1(臺灣大學)測試主機
        9   192.192.63.93       臺北區網2(政治大學)測試主機
        10  192.192.63.101      桃園區網(中央大學)測試主機
        11  192.192.63.109      新竹區網(清華大學)測試主機
        12  192.192.63.117      竹苗區網(交通大學)測試主機
        13  192.192.63.125      臺中區網(中興大學)測試主機
        14  192.192.63.133      南投區網(暨南國際大學)測試主機
        15  192.192.63.141      雲嘉區網(中正大學)測試主機
        16  192.192.63.149      臺南區網(成功大學)測試主機
        17  192.192.63.157      高屏澎區網(中山大學)測試主機
        18  192.192.63.181      臺東區網(臺東大學)測試主機
        19  192.192.63.165      花蓮區網(東華大學)測試主機
        20  192.192.63.173      宜蘭區網(宜蘭大學)測試主機
        21  163.19.150.75       新竹市教育網路中心測試主機
        22  163.17.38.37        臺中市教育網路中心測試主機
        23  163.24.239.150      屏東縣教育網路中心測試主機
        24  163.25.121.203      金門縣教育網路中心測試主機
        25  203.68.253.225      澎湖縣教育網路中心測試主機
        26  210.240.1.210       基隆市教育網路中心測試主機
        27  163.19.163.141      苗栗縣教育網路中心測試主機
        28  163.22.49.34        南投縣教育網路中心測試主機
        29  163.19.4.27         新竹縣教育網路中心測試主機
        30  210.240.39.10       花蓮縣教育網路中心測試主機
        31  210.240.125.144     臺東縣教育網路中心測試主機
        32  163.27.230.46       雲林縣教育網路中心測試主機
        33  163.27.67.201       嘉義縣教育網路中心測試主機
        34  163.27.1.241        嘉義市教育網路中心測試主機
        35  192.83.190.236      臺南市教育網路中心測試主機
        36  140.111.64.154      宜蘭縣教育網路中心測試主機
        37  163.25.24.19        連江縣教育網路中心測試主機
        38  163.21.249.170      臺北市教育網路中心測試主機
        39  203.72.153.73       新北市教育網路中心測試主機
        40  163.28.136.35       高雄市教育網路中心測試主機
        41  163.23.200.90       彰化縣教育網路中心測試主機
        42  163.30.0.156        桃園市教育網路中心測試主機
```


MINISTRY OF EDUCATION
教育部
臺灣學術網路 TANet 網路品質測試系統
系統說明
用戶-節點
節點-節點
節點-網站
目前位置
IP位址
101.11.9.197
測試
請輸入驗證碼
WSMWH
說明
確認
關閉
測試名稱：網路傳檔測試
測試方法：以 HTTP Method G
上傳 網路速率，不同資料流測
試需小於10秒，超
ps)，以顏色表示其狀態
詳細說明
顏色狀態：
預設
壅塞
普通
良好
目前位置 本機IP 101.11.9.197，測試點 台北主節點測試主機
下載
0
上傳
0

Web based speedtest

I/O



系統說明 | 用戶-節點 | 節點-節點 | 節點-網站

起點　台北主節點測試主機

終點　新竹主節點測試主機

線路品質測試　網路傳檔測試　說明

測試名稱：網路傳檔測試
測試時間：2020/08/22 12:29:08
測試序號：20200822-122908-9070
測試方法：以 HTTP Method HEAD 連續測試 10 次，求回應時間(ms)均值，再以 HTTP Method GET 使用固定大小檔案傳輸計算 下載/上傳 網路速率，資料流測試需小於10秒，超過即結束測試並取得最後測試平均值 (Mbps)，以顏色表示其狀態 詳細說明
顏色狀態：預設　壅塞　普通　良好

測試起點 台北主節點測試主機，測試終點 新竹主節點測試主機

延遲時間	下載	上傳
2.22 ms	982.49 Mbps	980.04 Mbps

延遲時間 2.22 ms　下載 982.49 Mbps　上傳 980.04 Mbps

```
[root@10-133-radar beverage]# ./speedtest_tanet 5
```
{"DownloadSpeedAvg":"72.15Mbit","UploadSpeedAvg":"86.36Mbit","ServerName":"台南

```
root@10-133-radar beverage]# ./speedtest_tanet 5 detail
```
{"DownloadSpeedAvg":"75.24Mbit","UploadSpeedAvg":"91.86Mbit","Downloads":[{"FullUrl":"http://192.192.63.34/perl/NTS/bin1M.pl","LenBytes":1048576,"TimeMillis":245,"SpeedMbit":34.23},{"FullUrl":"http://192.192.63.34/perl/NTS/bin2M.pl","LenBytes":2097152,"TimeMillis":308,"SpeedMbit":54.47},{"FullUrl":"http://192.192.63.34/perl/NTS/bin4M.pl","LenBytes":4194304,"TimeMillis":293,"SpeedMbit":114.52},{"FullUrl":"http://192.192.63.34/perl/NTS/bin8M.pl","LenBytes":8388608,"TimeMillis":557,"SpeedMbit":120.48},{"FullUrl":"http://192.192.63.34/perl/NTS/bin16M.pl","LenBytes":16777216,"TimeMillis":1554,"SpeedMbit":86.36},{"FullUrl":"http://192.192.63.34/perl/NTS/bin32M.pl","LenBytes":33554432,"TimeMillis":4260,"SpeedMbit":63.01},{"FullUrl":"http://192.192.63.34/perl/NTS/bin64M.pl","LenBytes":67108864,"TimeMillis":6927,"SpeedMbit":77.5},{"FullUrl":"http://192.192.63.34/perl/NTS/bin128M.pl","LenBytes":213,"TimeMillis":7,"SpeedMbit":0.24},{"FullUrl":"http://192.192.63.34/perl/NTS/bin200M.pl","LenBytes":213,"TimeMillis":7,"SpeedMbit":0.24}],"Uploads":[{"FullUrl":"http://192.192.63.34/perl/NTS/upload.pl?sessId=e5cac86b1b2f40d72e36d5a2a4343490","LenBytes":1048777,"TimeMillis":168,"SpeedMbit":49.94},{"FullUrl":"http://192.192.63.34/perl/NTS/upload.pl?sessId=e5cac86b1b2f40d72e36d5a2a4343490","LenBytes":2097353,"TimeMillis":250,"SpeedMbit":67.11},{"FullUrl":"http://192.192.63.34/p

結論

1. 資料處理與生成位置
2. SNMP 安全性
3. 資料的即時性、正確性
4. L2 to L7 分析

應用情境	資料類型	資料處理位置
網路設備存活	即時資料	Cloud／Edge
對外頻寬偵測	即時資料	Cloud／Edge
網路拓樸產生	即時資料	Cloud／Edge
網路設備偵測	即時資料	Cloud／Edge
IP/MAC對應資料蒐集	即時資料	Cloud／Edge
PC所在交換器Port偵測	即時資料	Cloud／Edge
IP、MAC衝突偵測	即時資料	Edge
測速(speedtest)	即時資料	Edge
wifi 服務偵測	即時資料	Edge
Switch Loop 偵測	即時資料	Cloud／Edge
Netflow 統計	歷史巨量資料	Cloud
Syslog 查詢	歷史巨量資料	Cloud
當日流量TOPN IP	歷史資料	Cloud

敬請指教