新一代校園網路管理

朱煜煌
電信研究院
108.01.18

大綱

- 校園網路現況
- 新一代校園網路管理-EyeLAN網路解決方案
- EyeLAN應用案例
- EyeLAN管理介面

校園網路現況

- 系統眾多，各有管理系統

網路印表機勒索威脅

- 2017年2月開始，全國至少46所大院校及國中小學遭駭客入侵，以網路印表機傳送恐嚇信，勒索3個比特幣、約10萬台幣，揚言不付款，將會癱瘓網路
- 事件觀察:
  - IoT設備多使用Public IP，易於從外網連入
  - 多數設備並無管控存取連線(Access Control)，任何IP皆可連入
  - 設備多為預設管理密碼，易遭駭客破解

校園比特幣勒索災情最新統計：全臺46校遭勒索，中小學占25%

教育部統計，全臺有46所學校受駭客勒索，半數以上為大專院校，並且，受侵入印表機裡面有73%印表機是HP。教育部認為，有些縣市學校收到威脅信後，網路沒受到影響，就不會主動通報，數量恐更多。

文/ 黃泓瑜 | 2017-02-23 發表

讚 5萬 按讚加入iThome粉絲團 讚 0 分享 G+

你以為印表機很安全嗎? 全臺46所學校印表機遭駭客入侵!

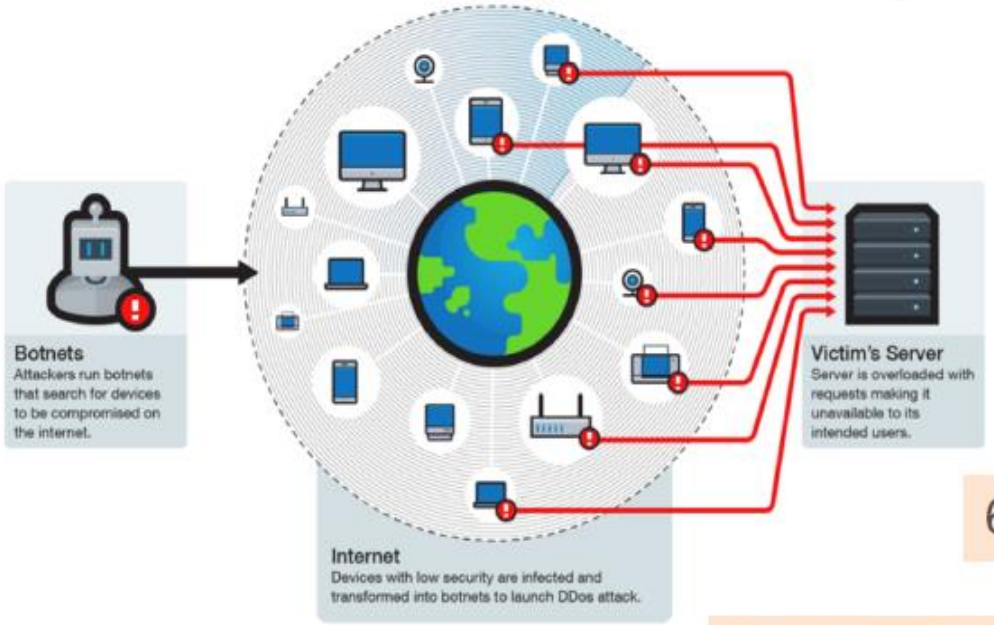
2017年03月10日 165反詐騙 165反詐騙專區

2017年資安風暴一波未平一波又起，上個月二月初臺灣證券市場才遭逢第一件大型駭客攻擊，二月底多所學校的網路印表機均收到自動列印署名為Emerson Rodrigues之恐嚇信件，要求校方指定時間前支付3個比特幣（約新臺幣10萬元），若未準時付款就會於3月1日發動網路攻擊以癱瘓學校網路。

IoT 攻擊逐年激增

誰的IoT設備?

Proven Results for Hacking



750K spam emails (fridges)

2014

50K HTTP RPS (25K CCTV devices)

Jun, 2016

120K HTTPS RPS (47K CCTV, home routers, servers)

Aug,2016

620 Gbps

KrebsOnSecurity Sep. 20,2016

1 Tbps (150K CCTV,DVR)

OVH Sep. 21,2016

1.2 Tbps DNS DDoS

Dyn Oct. 21,2016

Satori for IoT (280K IP addresses)

Dec, 2017

KRACK Wifi vuln

Mirai source code released

企業網路面對的資安威脅

2016年重大資料外洩事件年表

2016年2月9日
美國司法部：1萬名DHS與2萬名FBI員工個資遭竊
加州大學柏克萊分校：8萬名師生財務資料外洩
美國國稅局：70多萬納稅人資料遭竊
2016年3月10日
21st Century Oncology癌症醫療公司：坦言2015年遭竊220萬名患者資料
2016年4月11日
菲律賓選委會：匿名者組織侵入資料庫，5,500萬選民資料外洩
2016年5月11日
溫娣漢堡：美國300家連鎖店支付系統感染木馬，用戶支付卡資料遭竊
2016年5月17日
LinkedIn：發現2012年外洩1.17億筆資料
2016年9月22日
Yahoo：坦言2014年外洩5億筆帳戶資料
2016年10月20日
印度國家支付公司：POS機和ATM感染惡意程式，326萬張支付卡資料外洩
2016年11月13日
FriendFinder Networks成人網站：超過4.1億筆用戶資料外洩
2016年11月14日
Yahoo：揭露2013年還外洩10億用戶資料
2016年11月23日
美國海軍：外包公司員工筆電遭駭，13萬海軍個資外洩

資料來源：iThome整理，2017年1月

資料來源: iThome 2016/07

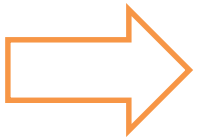
攻擊手法：

外對內 ⇒ DDoS攻擊 (購買防火牆無效)

內對內 ⇒外部遙控內對內攻擊 (透過Ethernet網路)

台積電抓出魔鬼：裝新機台未掃毒

- **蒸發78億！** 台積電抓出魔鬼：裝新機台未掃毒
- 消息人士透露，台積電是在上周五（二日）傍晚約五、六時遭電腦病毒入侵，並於當晚十時許擴散至三大廠區。依台積電昨天的公告推算，事件發生後約四十小時，已恢復八成機台生產作業，預計在關鍵的六十小時「排毒行動」後，可望全數排除電腦病毒；但比原先預期慢了約一天，受衝擊營收也比預期大
- 台積電昨天下午發布重大訊息指出，針對事件發生原因，主要是出於「新機台在安裝軟體的過程中操作失誤」，病毒在新機台連接到台積電內部電腦網路時，發生病毒擴散，但公司資料的完整性和機密資訊皆未受影響



電腦病毒會主動擴散

資料來源: https://udn.com/news/story/11311/3292432

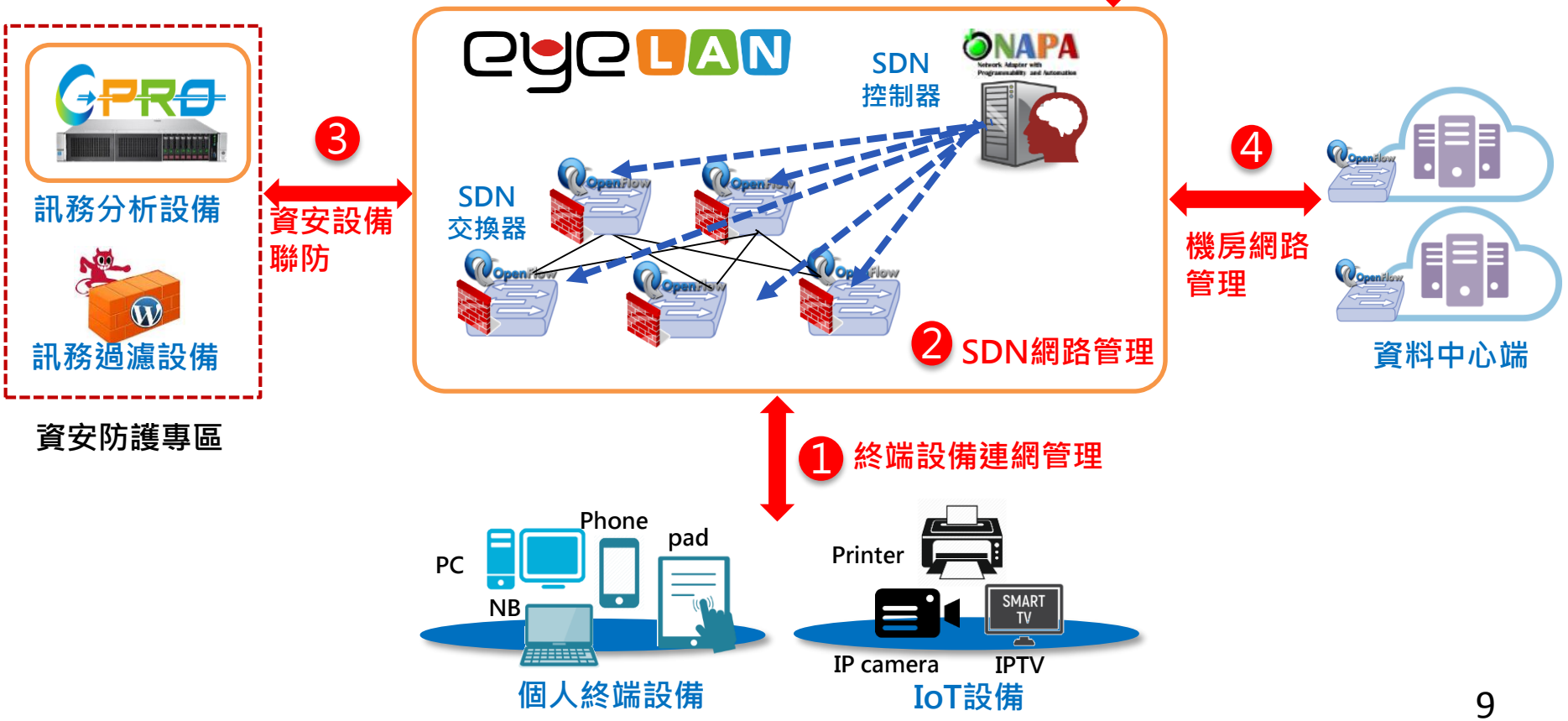
EyeLAN企業網路解決方案
(中華電信自主研發的新一代智慧網路管理系統)

EyeLAN 五大特點

1. 終端設備連網管理
2. 集中化網路管理
3. 與資安設備聯防
4. 機房網路管理
5. 第三方管理系統聯動

第三方管理系統

5



EyeLAN功能

基本功能

終端設備連網管理

核心功能

使用者/IoT設備管理

- 實名制管理
- 連網設備自動偵測
- 連線存取管控
- 網路隔離
- 連網時間管理
- 即時/歷史流量監控

SDN網路管理

核心功能

集中管理

- 集中管理頁面
- 視覺化拓樸
- OpenFlow交換器設備管理
- 網路設定備份/還原
- 系統排程工具

障礙查測

- 終端設備搜尋
- 終端線路連接查測
- 流量監控
- 日誌管理

進階功能

結合資安設備聯防

進階整合

資安強化

- 異常流量阻擋
- 封包側錄

支援機房網路

進階整合

雲網導入

- 網路拓樸與全域流量監看
- L2 Fabric 二層網路隔離
- 快速建立路徑
- 端點對端點即時障礙查測
- 端對端路徑障礙查測
- 點對點路徑建置

第三方網管系統整

進階整合

網管整合

- 全方位網路整合監控
- SDN設備與傳統網路設備納管
- 虛實設備納管
- 網路拓樸

EyeLAN 設備元件

- EyeLAN組成元件
  - NAPA控制器+ OpenFlow 交換器
  - (選配) SD-BOX, GPro, DPI.. 等
- 可與現有網路設備互運

EyeLAN產品基本組合

NAPA控制器

Open Flow交換器

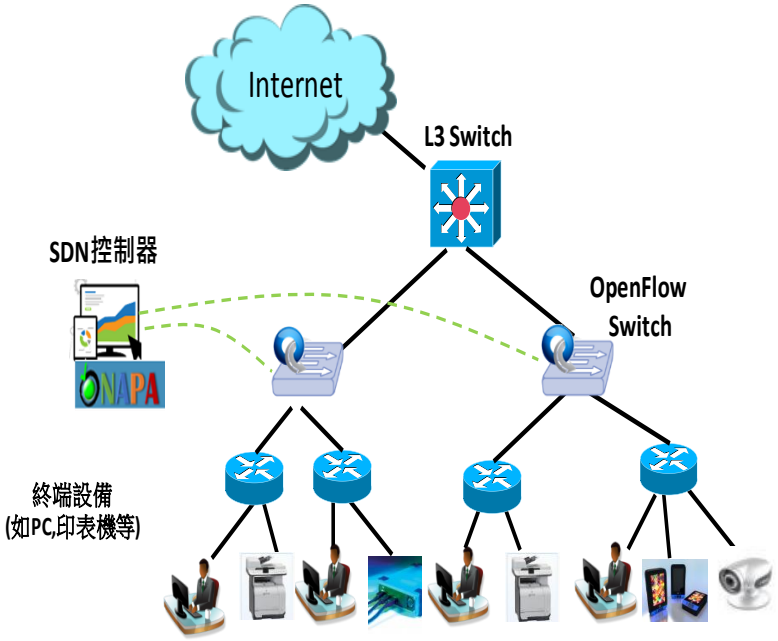
加值應用(選配)

- SD-BOX
  L3 Routing、連線加密、安全功能)
- HiGate維運管控
- GPro
  訊務側錄分析
- EyeSee
  網管企業版
- EyeQuila
  APT潛伏威脅的偵測

EyeLAN網路架構建議

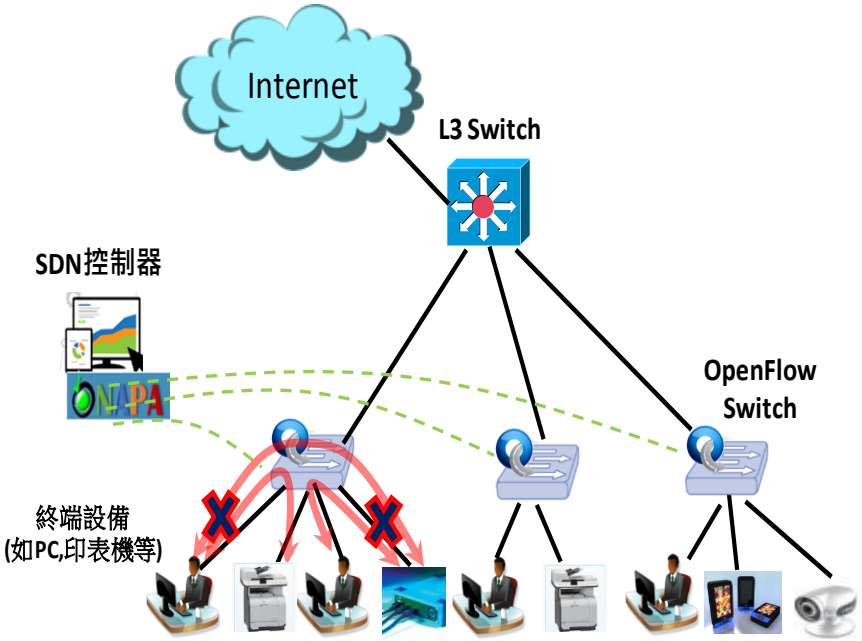
❖ 架構1

- 不改變原有網路架構
- 增加OpenFlow交換器
- 實名制可視化管理
- 無法防止ARP偵測其他設備的IP/MAC資料
- 無法防止東西向攻擊



❖ 架構2

- ✓ OpenFlow交換器取代L2交換器
- ✓ 實名制可視化管理
- ✓ 端對端隔離管理
- ✓ 可以防治ARP攻擊/偽造
- ✓ CHTNet 2.0 架構



EyeLAN (NAPA控制器) 應用案例

中華電信內部網路

- 中華電信總公司大樓
- 北分公司大樓網路
- CHT MOD Server Farm 網路
- 研究院(楊梅及大安院區)
- 電信學院(板橋、台中及高雄院區)
- 台北東門門市
- 新竹科園門市

外部客戶網路

- 高雄市政府智慧xx網路
- 經濟部工業局xx雲網路
- 台北市政府xx處網路
- 交x大學xx網路
- 台中市政府(2月導入)
- 高O市資訊OOOO (完成POC)
- 明xxx大學 (POC中)
- …

EyeLAN應用案例

案例一: 校園網路應用

架構1

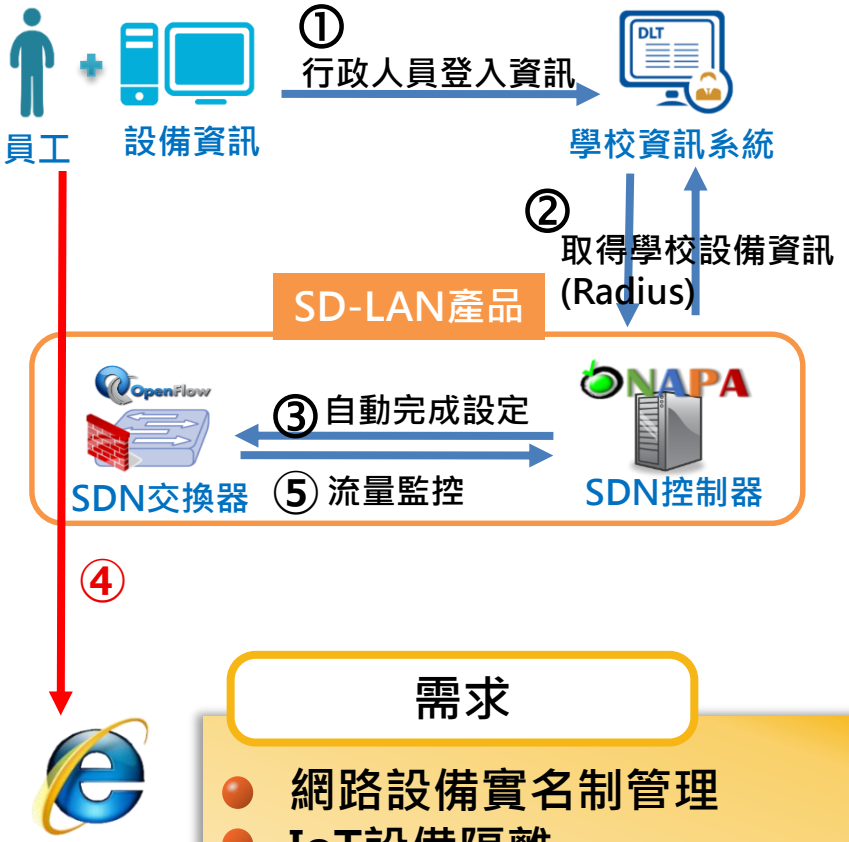
❖ 已執行

- ➢ 網路使用設備實名制管理
- ➢ 非註冊設備不可以使用網路
- ➢ 流量監控
- ➢ 管控IoT設備連網，避免被攻擊或操控 (6/4已裝機)

❖ 新需求

- ➢ 跨校園管理 (3個校區)
- ➢ 進出校園接口網路架構調整(導入SDN執行訊務工程)

情境說明



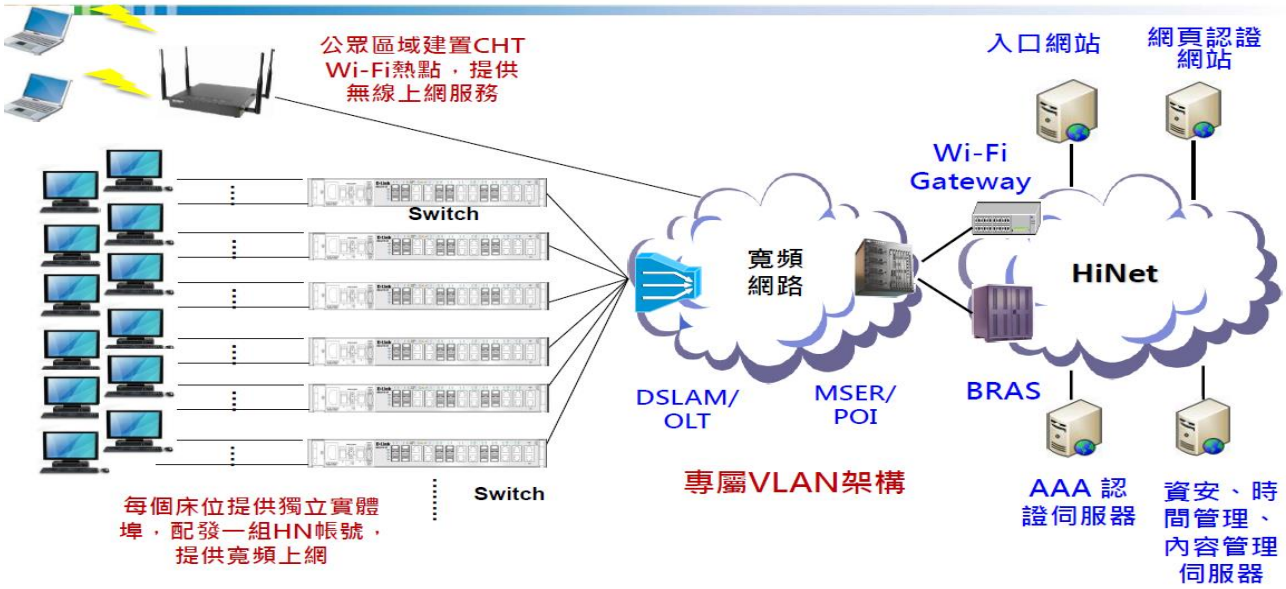
需求

- 網路設備實名制管理
- IoT設備隔離
- 多校園管理

案例二: 宿舍網路

架構1

- 可以綁定床位，可支援同學更換宿舍房間(有時幾週、有時每月)
- 可以提供使用者網路使用時數與網路流量的報表
- 可提供認證網頁，跟學校LDAP整合
- 可進行0-2點限制網速 (研究生例外)



需求

- 綁定位置
- 限時限頻寬管理
- 管理網頁Portal

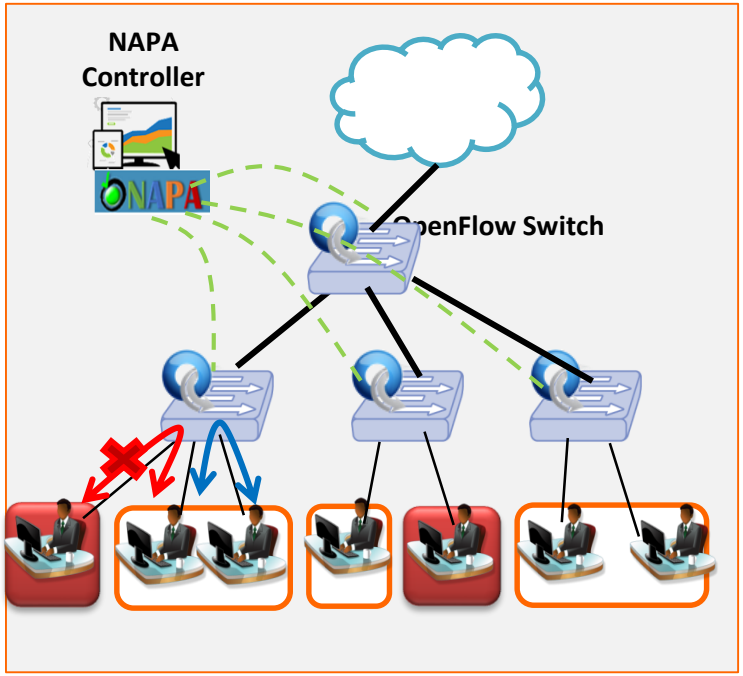
案例三: xx大學SDN建設案

架構2

- 校園網路替換成SDN網路
- 主要需求
  1. Micro-segmentation: Isolation upon infection
  2. Autoconfig of switches: 換設備自動供裝、自動偵測設備、自動訊務蒐集、自動網路拓樸
  3. Centralized management of 300+ switches

需求

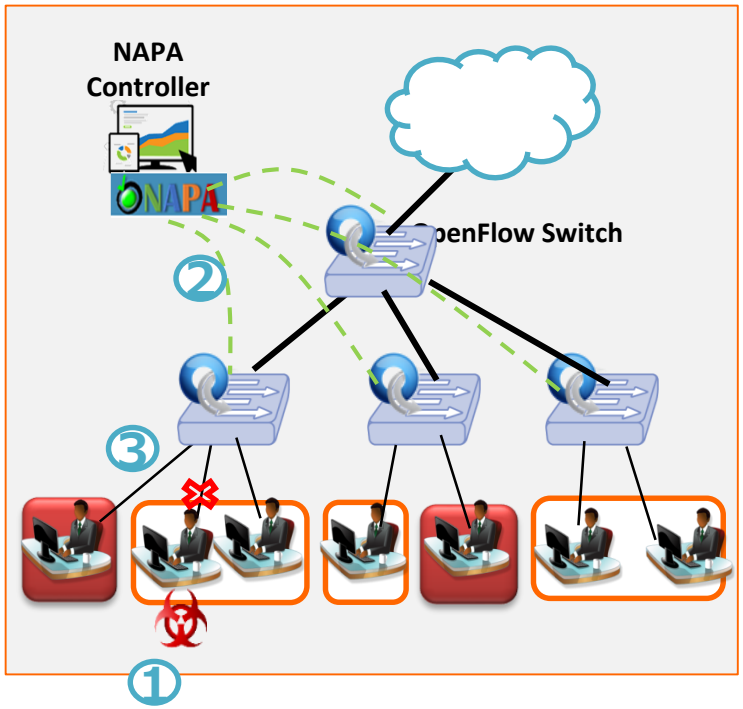
- 網路隔離
- 自動化
- 集中管理



In normal situation

Segment 1

segment 2



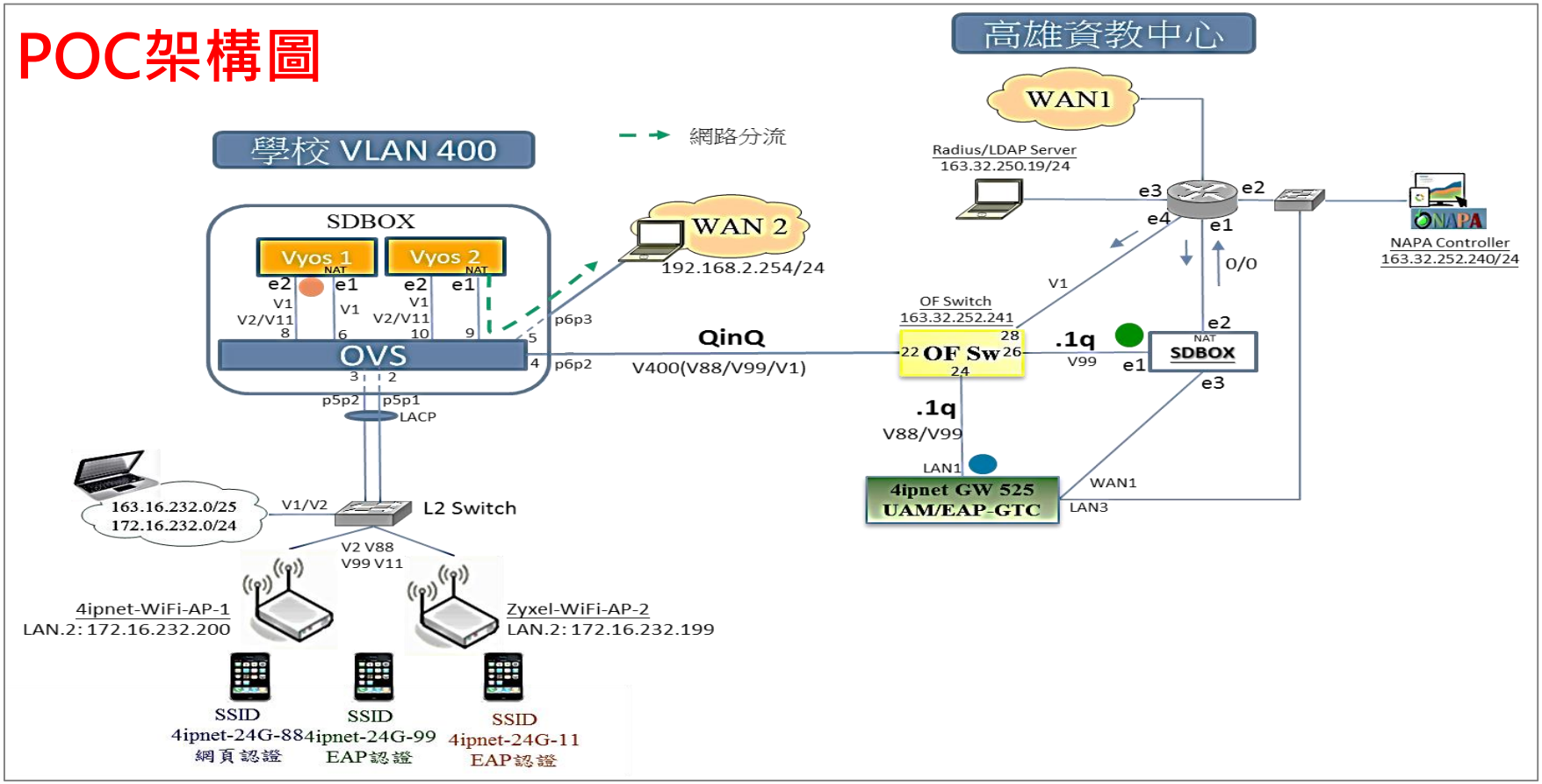
Host infected by virus

案例四: 高雄資O中心POC

- 運用SD-BOX 2.0，滿足客戶需求
  - 支援多個WAN介面，並且作分流
  - 支援Static Routing、Policy Routing
  - Thin AP改為Fat AP架構

客戶擬提出10個學校建置案(年底前決標)
108年計畫擴建到400間學校

POC架構圖

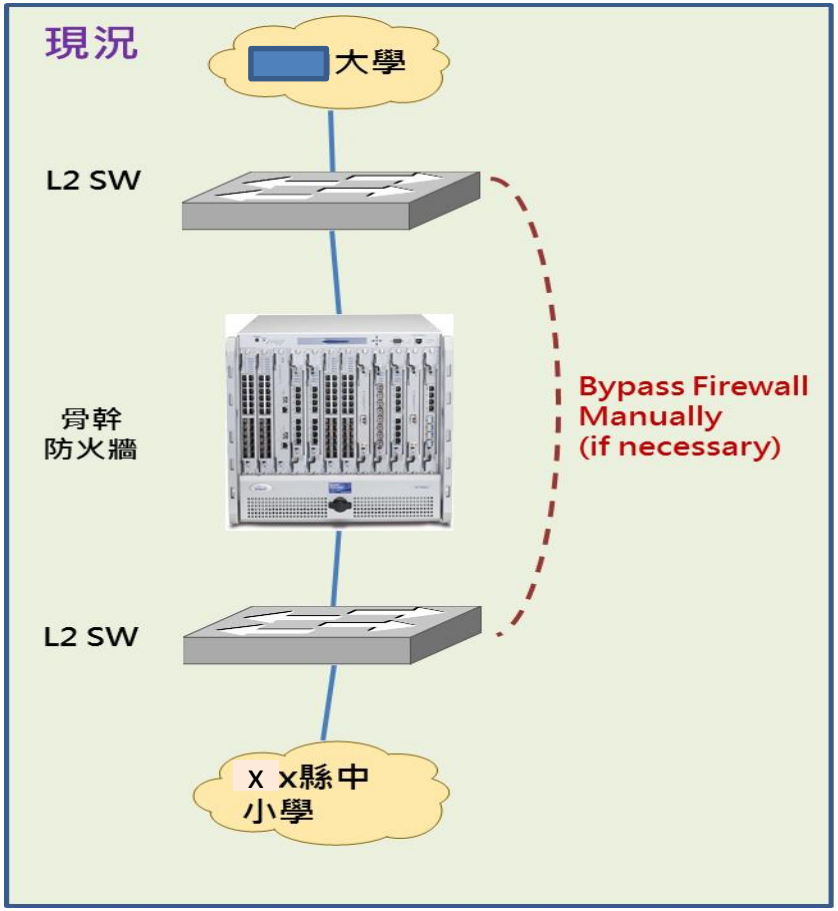


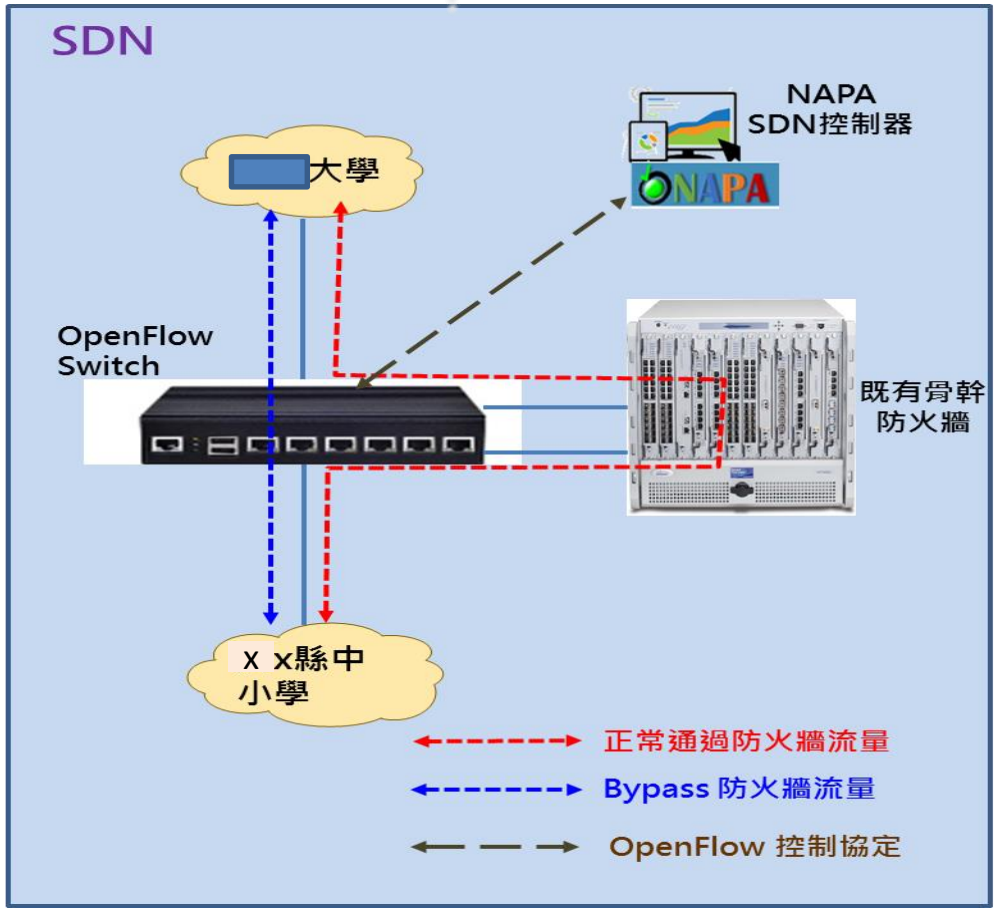
案例五: SDN輔助骨幹防火牆 架構

- OpenFlow Switch旁掛防火牆
- 進行防火牆流量offload
- 防火牆障礙時，Bypass用途

需求

- 防火牆流量offload
- 降低防火牆負載





案例六: 中華xx大樓

架構2

強化網路安全、易管理、自動化

	舊網路	新網路
設計原則	• 容易連線及使用(Default開通)，隨插隨用 • 增購防火牆進行接取管理 • 網路24小時全開通 • 單一VPN網路	• 網路嚴格管理(Default不通)，沒有申請即無法使用 • 進行設備管理(無須額外設備) • 上班時段網路開通，非上班時段需申請 • 多個VPN網路
安全	• 無內部防護機制 • 可布建防火牆進行網段隔離 • 可加購資安設備	• 無法用ARP偵測其他設備的IP/MAC資料 • 特定網段/特殊連線(業務會議)可進行隔離 • 可加購資安設備
供裝維運	• 人工操作 • 個別設定 • 人員異動須人工作業網路設定	• 資訊系統自動供裝設定 • 統一GUI集中設定/管理 • 人員異動由資訊系統自動變更
費用		• 整體費用低於舊網路

中華xx大樓網路架構

特色

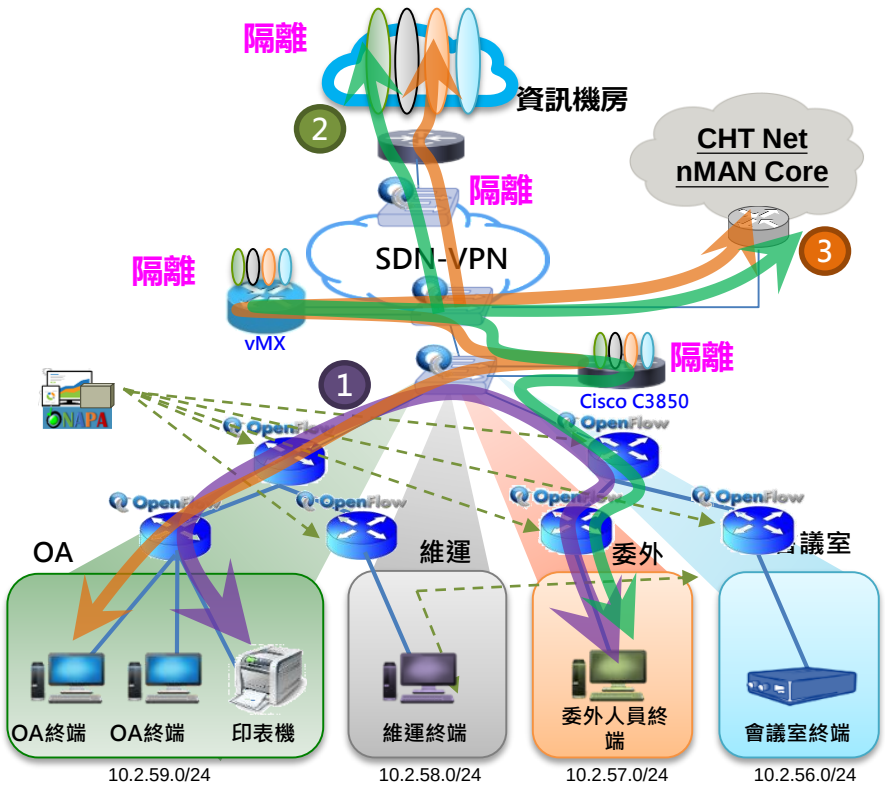
- 由資訊系統(IPAM)管理網路的使用者
- 資訊系統可動態調整設備屬性，網路接收指令自動調整設定(無人工介入)
- NAPA依據屬性將設備導到不同路徑，彼此隔離
- 網管人員透過NAPA管理網路
- 骨幹網路確實隔離(各自有路由器)

SDDC

SDN-VPN

SD-LAN

CHTNet 2.0



- 四個VPN
  - 正職
  - 專屬維運終端
  - 委外
  - 會議室終端

案例七: xx社區智慧路燈

架構2

- IoT設備可視化(實名制)管理
- 訊務監控 IoT設備設
- 主動偵測IoT設備是否存活
- QoS
- Multicasting

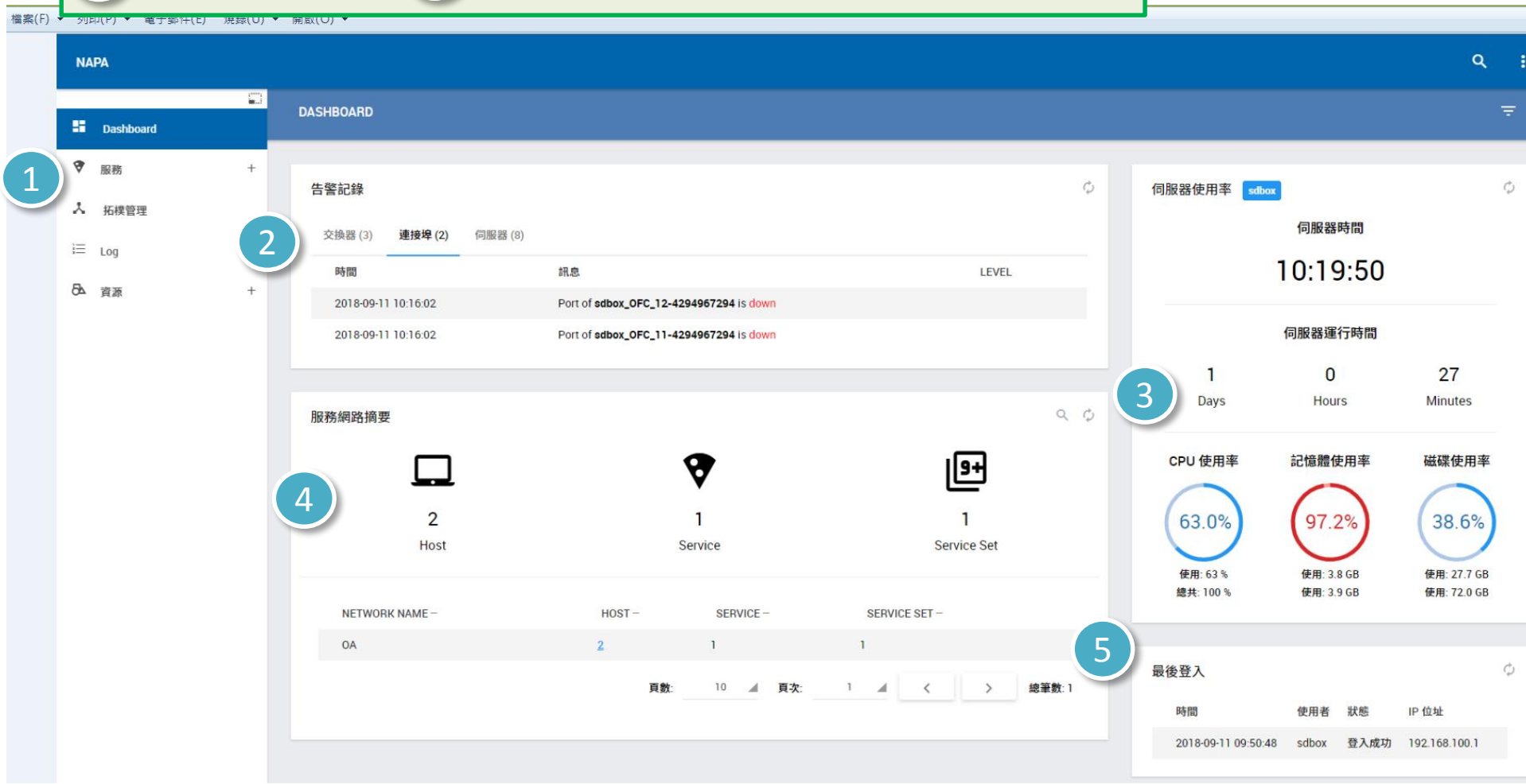
需求

- IoT設備實名制管理
- 主動偵測IoT設備狀況
- 點對多點傳送視訊
- 簡化維運負擔

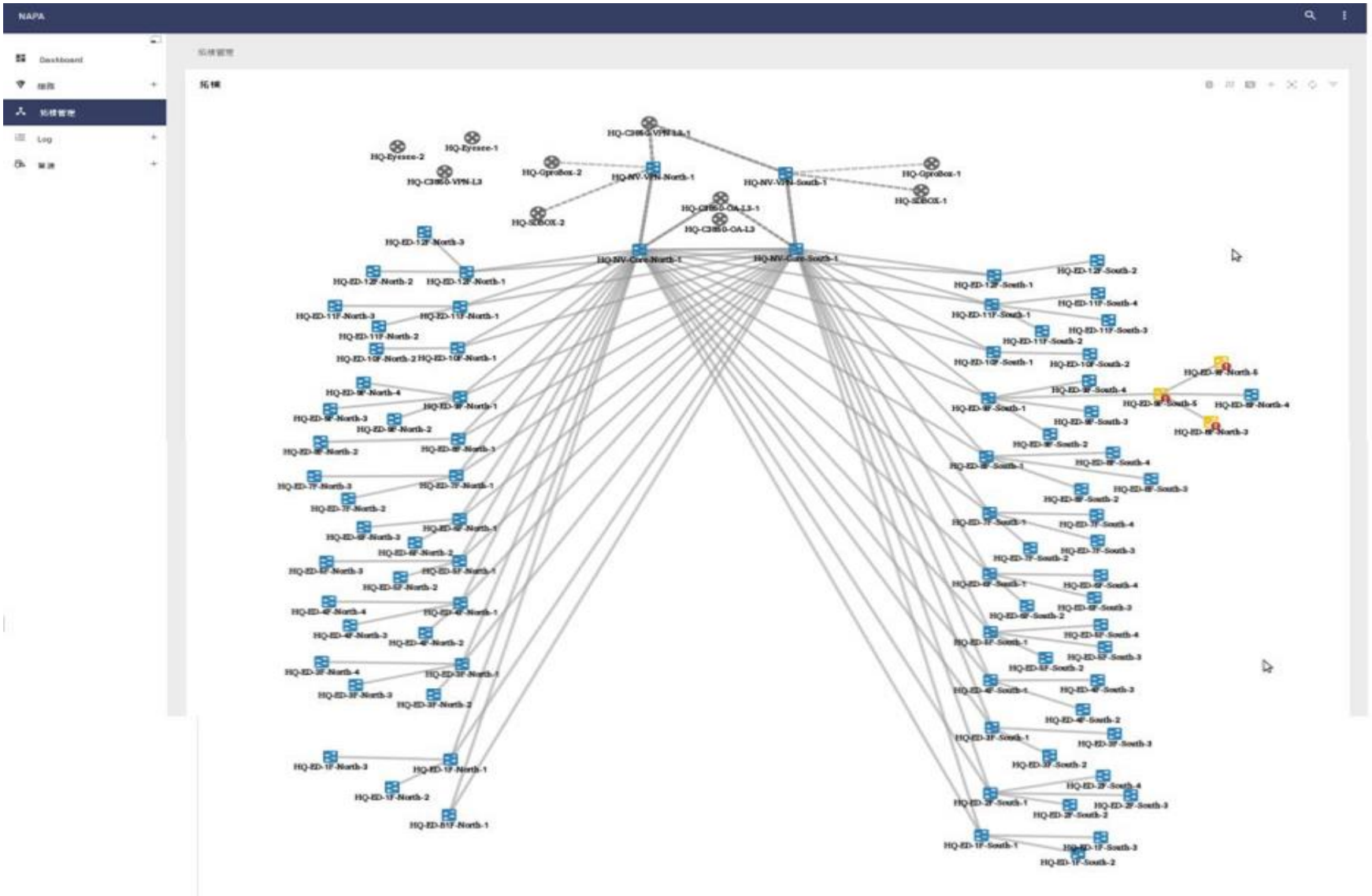
EyeLAN導入管理功能介紹

EyeLAN 介面

1. 功能列表
2. 事件告警紀錄
3. 控制器使用率
4. 服務網路
5. 最新登入列表



EyeLAN網路架構拓樸圖



終端設備連網管理

- **實名制管理**: 以使用者與身份特性管理誰可以使用網路
- **IP+MAC管控**
  - 僅允許合法IP/MAC使用網路
  - 自動禁止未授權 IP 位址 (IPv4/IPv6)或MAC位址連網
  - 避免 IP 衝突及防止 IP 、MAC 竄改

實名制管理

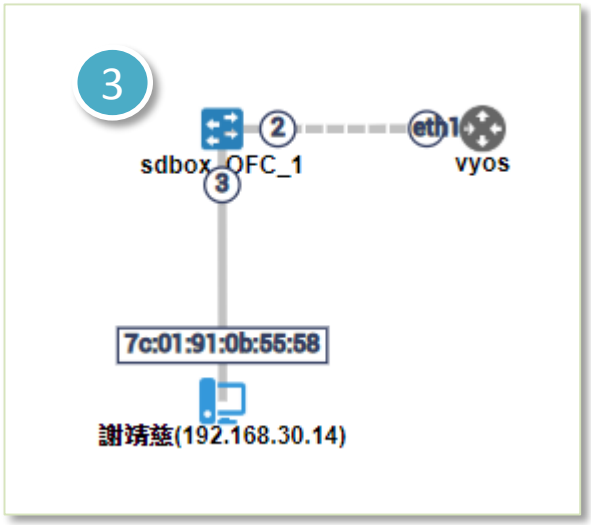
使用者	名稱	描述
王曉明	王曉明6樓辦公室PC	委外員工
謝美美	謝美美5樓辦公室PC	正職員工
謝美美	實驗室F201伺服器	

IP+MAC管控

IP	MAC	狀態
192.168.59.1	5E:16:71:AH:D9:F5	Enable
192.168.58.1	9B:16:A8:C5:D9:F7	Enable
192.168.57.1	BE:D9:F4:AF:16:71	Disable

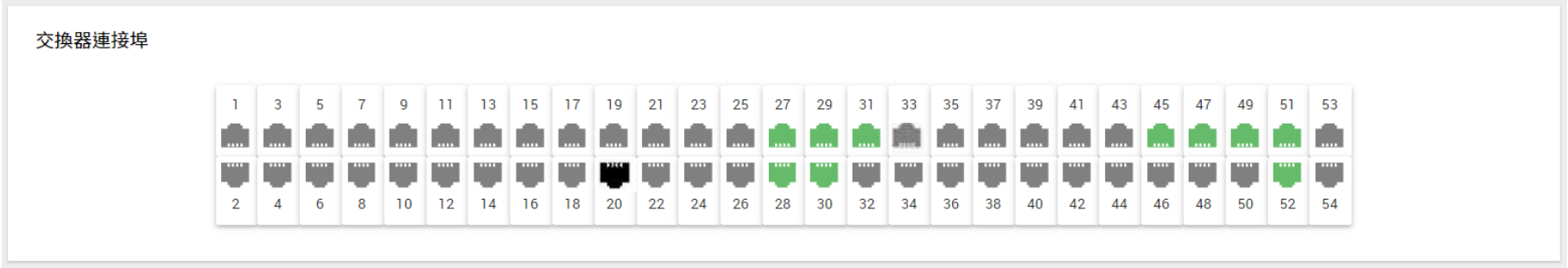
自動偵測終端位置

1. 自動偵測連網主機的IP、MAC位址資訊
2. 紀錄連網主機接入交換器及實體埠
3. 整合拓樸顯示



設備狀態顯示

- 交換器管理
  - 顯示實體埠狀態，確認線路是否鬆脫
  - 快速檢視實體埠流量



- 依實體埠數呈現
- 快速檢視實體埠流量
- 快速檢視示狀態
  - 綠色：正常
  - 灰色：無連線
  - 黑色：管理者設定為port down

連網時間管理

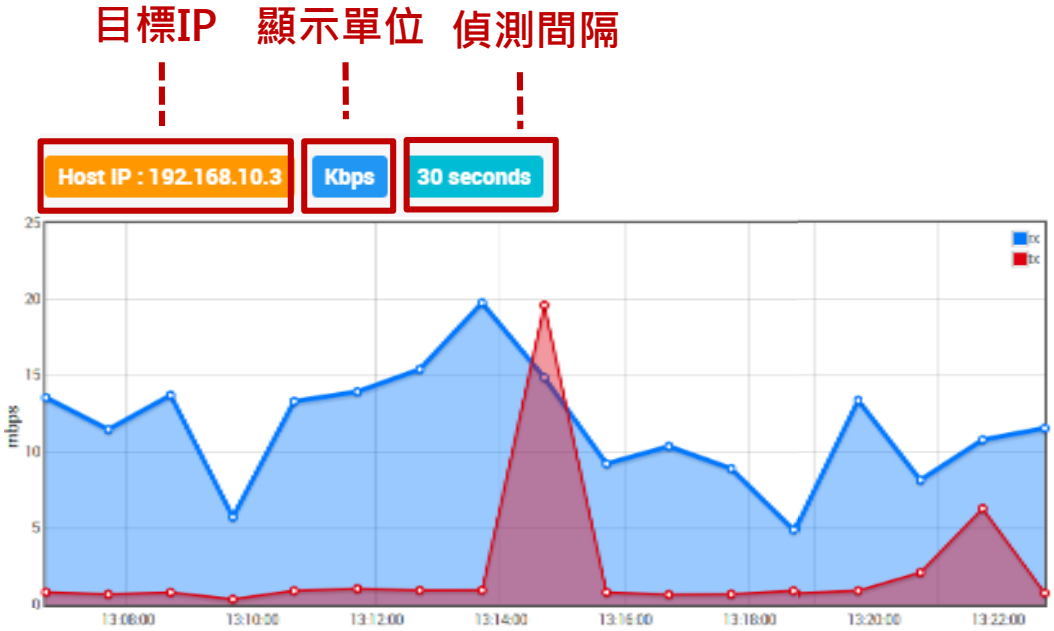
- 新增連網時間管理服務
  - 對終端設備事先設定網路啟用及終止時段
  - 允許使用網路的時間範圍內，自動開通設備連網；非允許連網的時段，當偵測設備嘗試上網則自動阻斷開通路徑

流量監控

- 實體埠或指定訊務(By MAC/ IP/ VLAN) 即時流量監控
- 實體埠或指定訊務(By MAC/ IP/ VLAN) 歷史流量監控

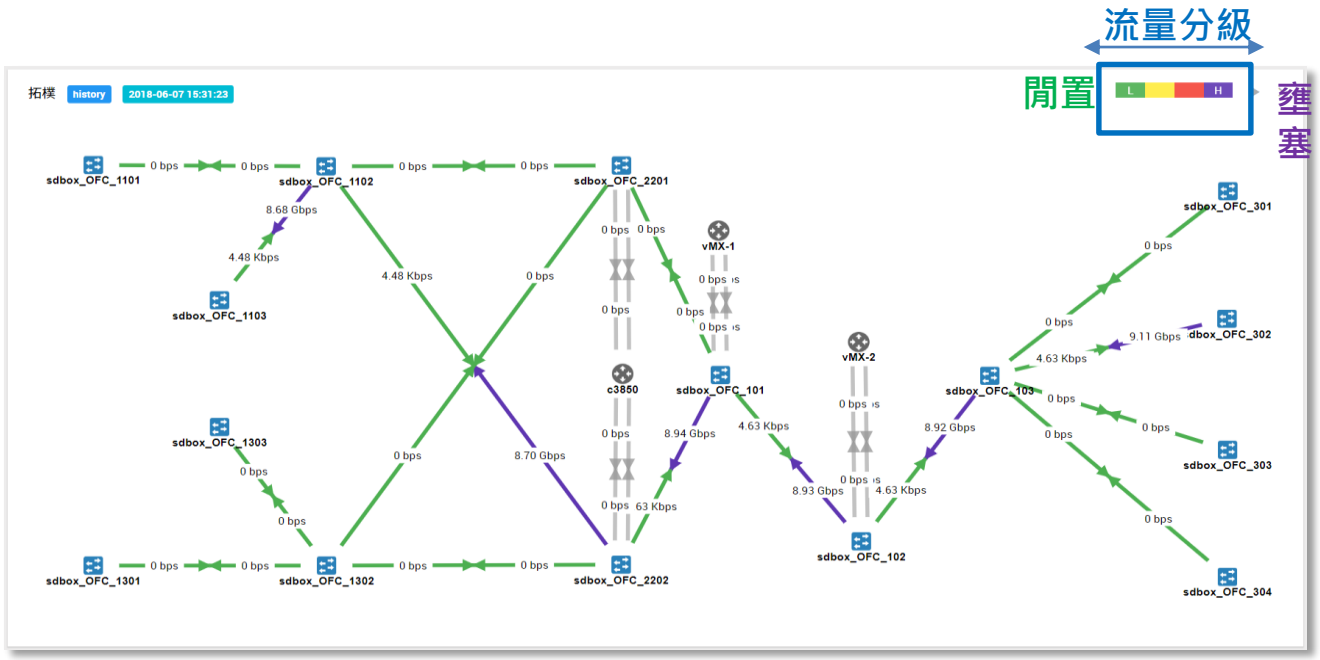
輸入監控條件

顯示查詢結果



整體網路流量監看

- 顯示整體網路拓樸, 包括OpenFlow交換器資訊, 相連的實體埠(port)及相關Flow設定等
- 提供鏈路流量監看,易於網路管理者掌握目前網路全貌



名稱	DPID	IP	硬體描述	軟體描述	製造商	OPENFLOW 版本	線上	指令
m1_OFC_100	100	127.0.0.1	Open vSwitch	2.5.2	Nicira, Inc.	1.3		
m1_OFC_101	101	127.0.0.1	Open vSwitch	2.5.2	Nicira, Inc.	1.3		

網路設定備份及還原(1/2)

- 資料庫備份
  - 提供手動/定期備份資料庫

網路設定備份及還原(2/2)

- 資料庫還原
  - 提供手動還原資料庫，當系統發生問題或人為操作不當時，可優先恢復系統數據，維持服務正常運作

中華電信
Chunghwa Telecom

感謝聆聽 敬請指教