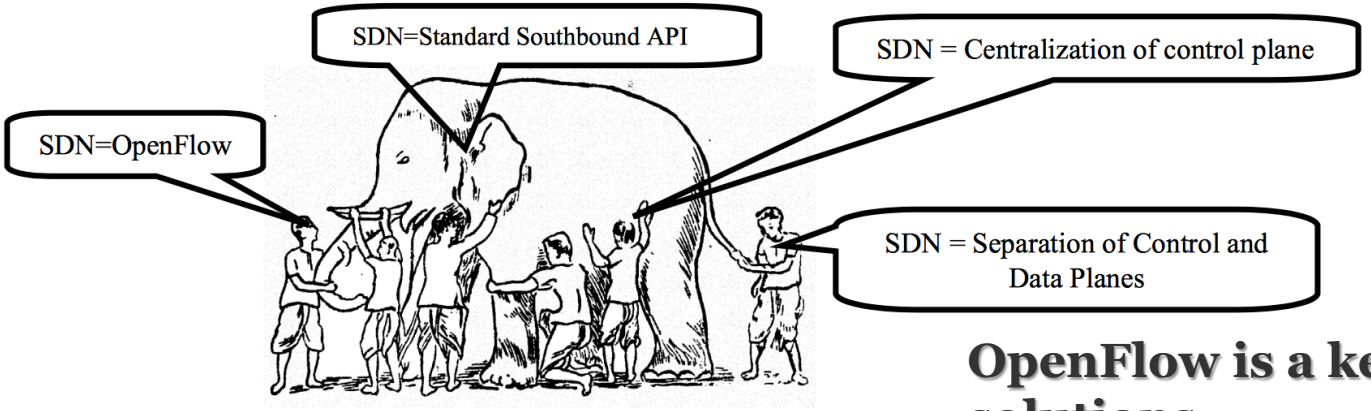
中華系統整合 CHUNGHWA SYSTEM INTEGRATION

SDN開創網路新趨勢

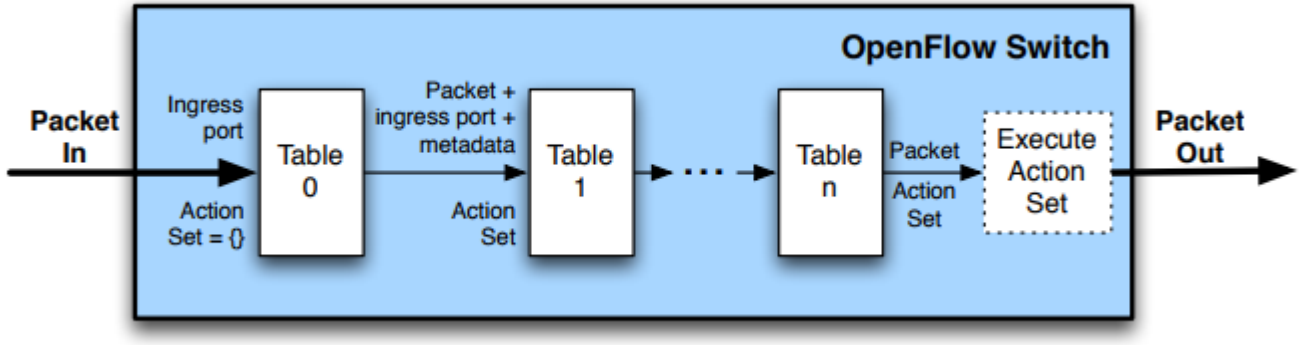
中華系統整合

楊智翔

What is SDN.....



OpenFlow is a key protocol in many SDN solutions.

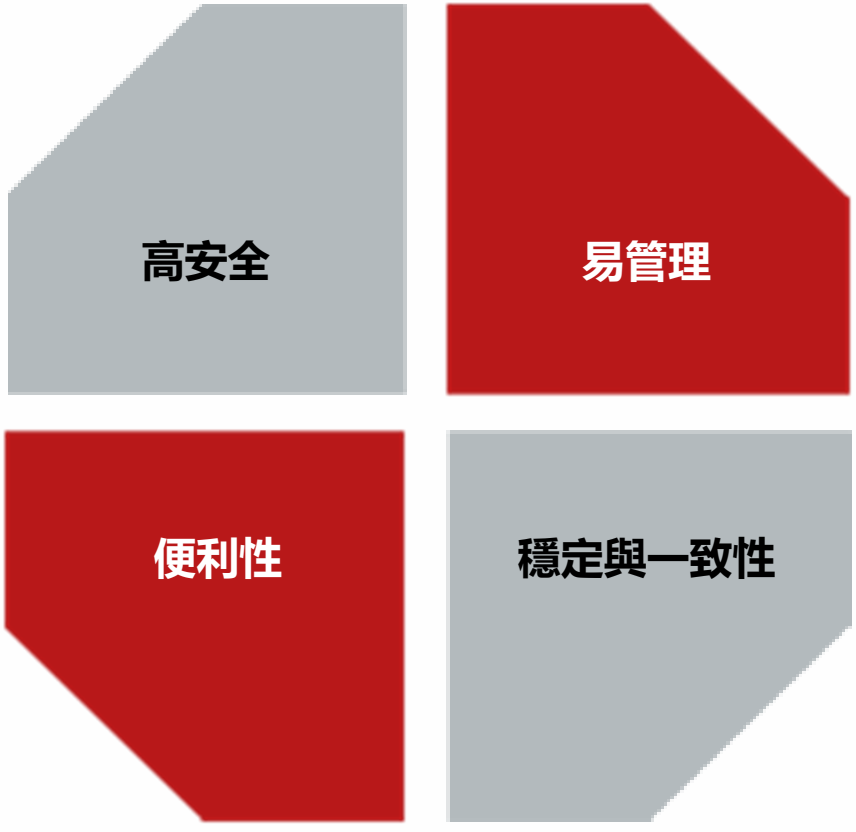


https://www.youtube.com/watch?v=Z5Gi2Bpd82M&ab_channel=IDGTECHtalk

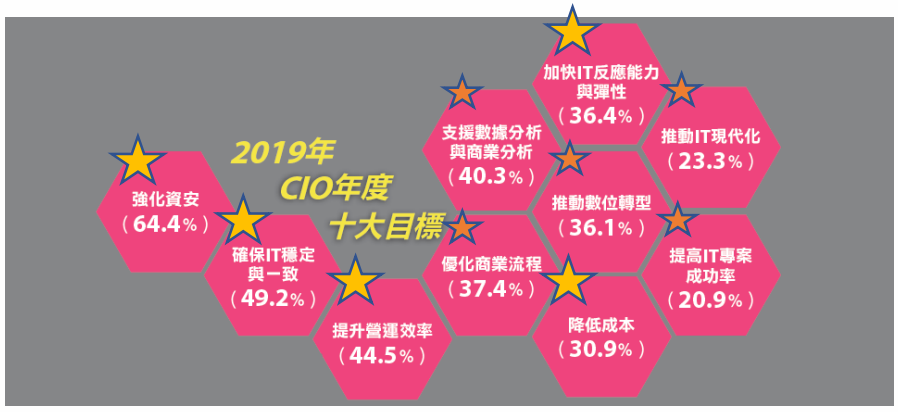
現況環境面臨問題

在「物聯網中自由、便利與安全的恐怖三角關係，您選擇了誰？」

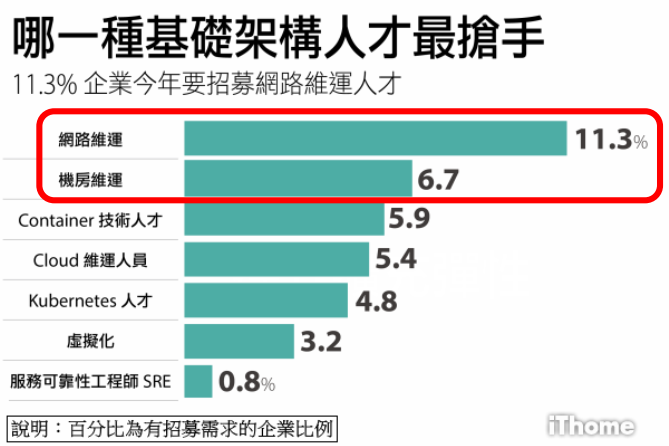
SDN導入預計效益

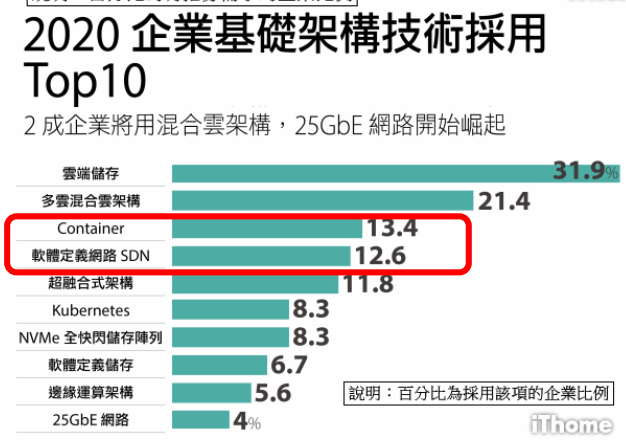


IT轉型目標



基本型IT戰略是以**維護、強化和提供IT系統運作或IT基礎功用為主的策略目標**，包括了確保**IT穩定與一致**、**強化資訊安全**、**加快IT反應能力與彈性**、**推動IT現代化**、提升業績、**降低成本**、**提升營運效率**、優化商業流程等8項。

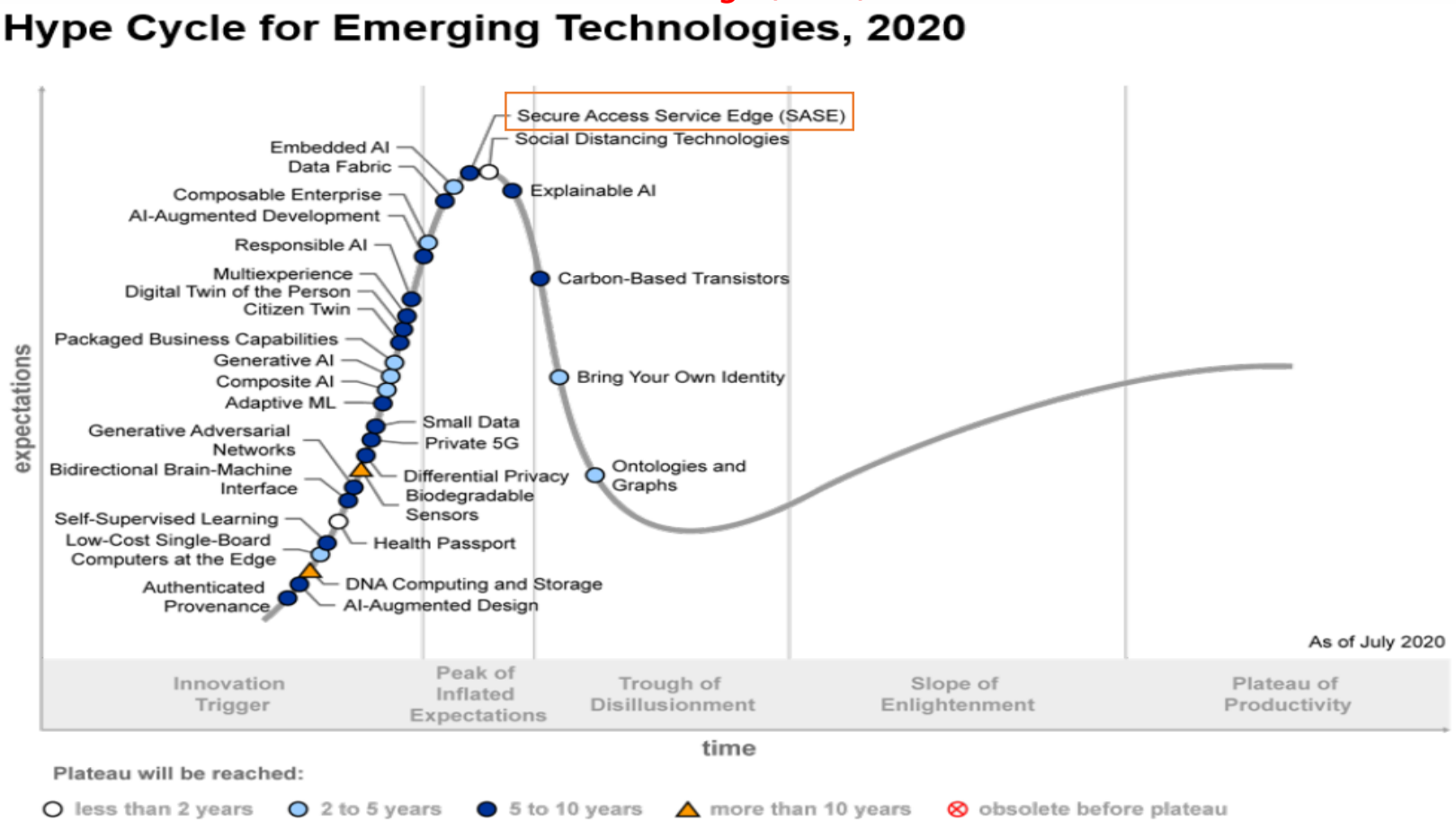




https://www.ithome.com.tw/article/129338

Hype Cycle for Emerging Technologies, 2020

Secure Access Service Edge (SASE)未來5~10年



Source: Gartner
ID: 450415

Secure Access Service Edge (SASE)

- Definition: Secure access service edge (SASE) delivers multiple capabilities，such as SD-WAN, Secure web gateway (SWG) , Cloud Access Security Brokers (CASB), NGFW and Zero Trust Network Access (ZTNA)
- 「零信任網路」(Zero Trust Network Access, ZTNA) 也稱為軟件定義邊界(SDP)，依Forrester的定義：企業不應自動信任內部或外部的任何人、事、物，應在授權存取前對任何試圖接入企業系統的人、事、物進行驗證
- SASE支持分支機構和遠端工作者訪問。SASE作為服務交付，並且基於根據設備/實體的身份，結合實時上下文和安全性/合規性政策。 身份可以與人員，設備，物聯網或邊緣計算位置相關聯

企業不應自動信任內部任何人、事、物

- Secure web gateway (SWG)
- Next-generation firewall (NGFW)
- Software Defined Perimeter (SDP)
- Cloud Access Security Brokers (CASB)

SASE, pronounced “sassy”

新一代網路管理訴求

隨著網路應用越來越多元，網路管理與安全也備受挑戰

What — **能作什麼應用**
管理使用者連網內容
管理設備使用量

When — **何時能使用網路**
管理設備使用時間

How — **紀錄使用狀況**
集中管理頁面
網路隔離/差異化管理

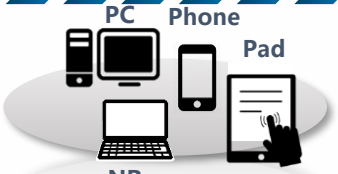
Where — **在那裡用網路**
管理設備使用位置

Who — **誰能用網路**
管理連入設備
限制使用範圍

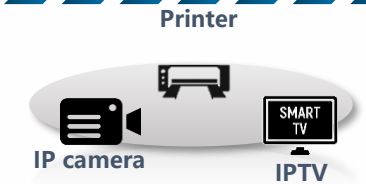
五 大 面 向

終端設備連網管理

01



個人終端設備



IoT設備

資安設備聯防

02

訊務分析設備

訊務過濾設備

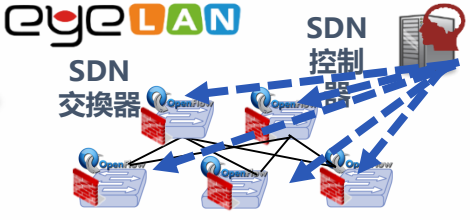
機房網路管理

03

資料中心端

集中化網路管理

04



第三方管理系統聯動

05

EyeSee

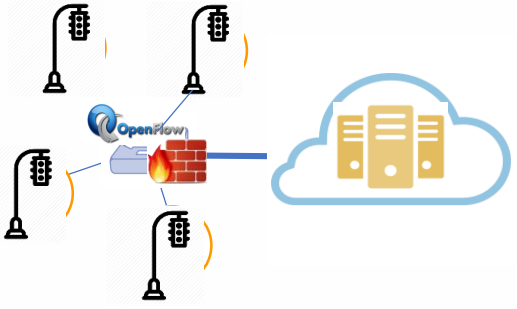
SOC平台

產品場域-適用於不同應用場域(2/2)

- 適用客戶場域：**企業網路**
- 效益：單一入口網頁集中管理、網路隔離、實名制管理、使用者流量監控、智慧障礙查測

- 適用客戶場域：**Data Center環境、雲端網路**
- 效益：網路隔離、網路服務鏈、簡化網路架構、容易擴充

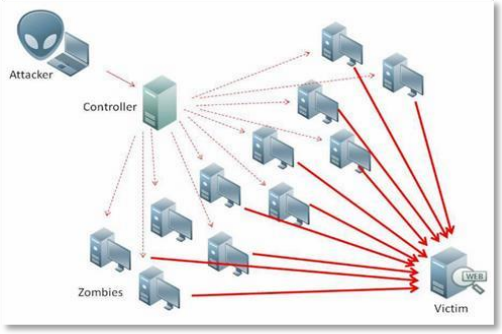
- 適用客戶場域：**教育網路、WiFi網路環境**
- 效益：節降WiFi設備成本、網路隔離、智慧路由、資安聯防、終端連網管理



- 適用客戶場域：**智慧城市環境、IoT應用環境**
- 效益：IoT設備網路管理、降低IoT網路風險

IoT設備遭駭，當成攻擊武器

IoT設備DDoS攻擊



- **萬物皆聯網導致萬物皆可駭**
  - ✓ 2016年10月21日知名網路服務 Dyn 遭受殭屍網路發動三波巨大規模 DDoS 攻擊，世界各大網站服務皆因為此攻擊而中斷，包括 Amazon、Twitter、Github、PayPal 等大型網站都因此受到影響。
  - ✓ **利用 IPCAM、CCTV、DVR、IoT 裝置等系統進行 DDoS 攻擊**
- **網路安控系統使用者關鍵問題**
  - 資安管控 ✓ IoT設備使用弱密碼
  - 網路隔離 ✓ **未進行適當的權限劃分與管理**
  - 資安管控 ✓ 容易開啓攻擊者寄送的惡意連結，導致被 XSS、CSRF 等手法攻擊
  - 使用管理 ✓ **未限制連入 IP 位址，導致安控系統可從外網任意存取**

各國均有網路攻擊事件

資料來源: iThome 2016/07

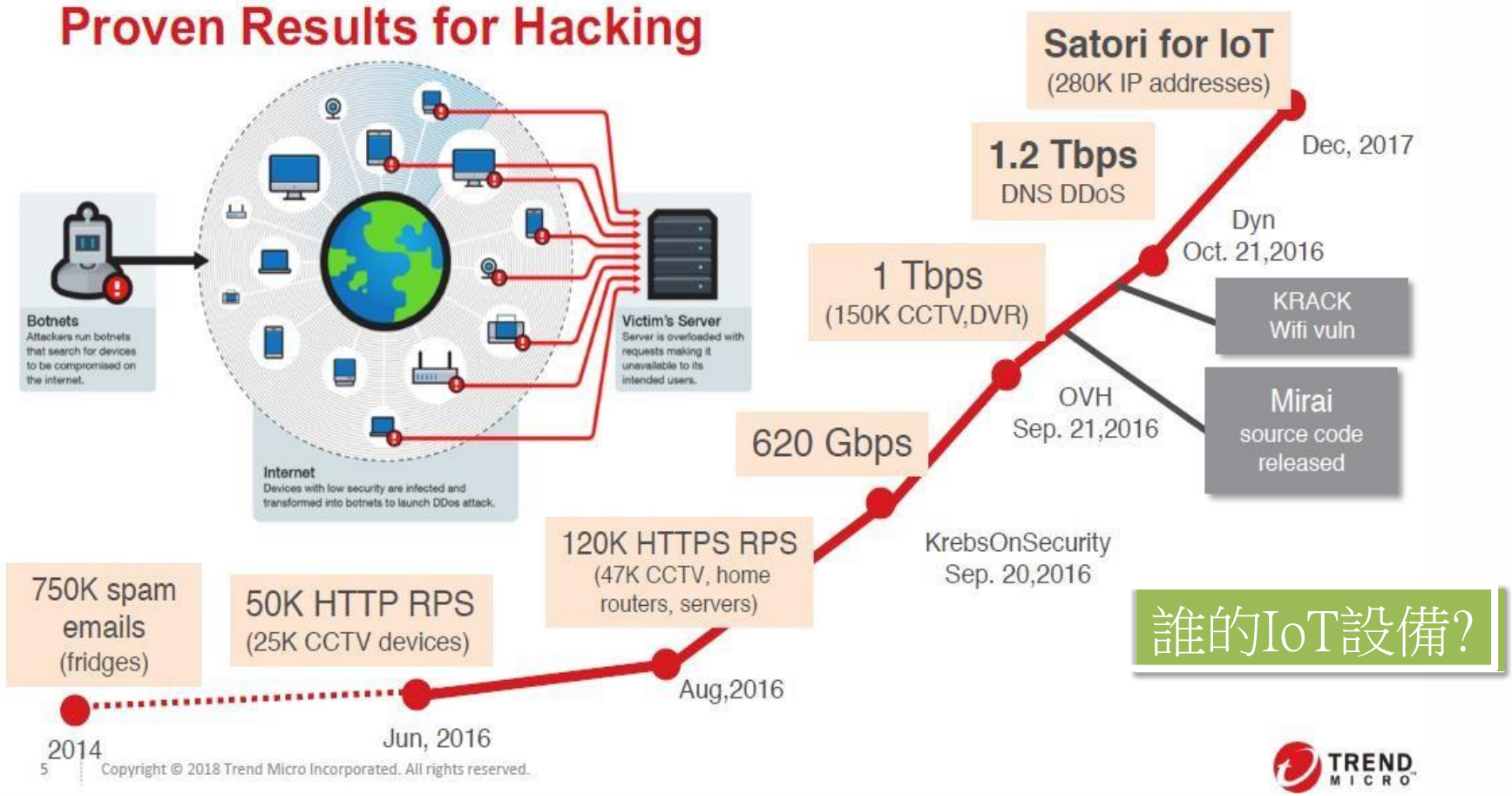
企業沒有建設資安防護嗎?
資安設備為何無效?

攻擊手法:

外對內 =>DDoS攻擊 (購買防火牆無效)

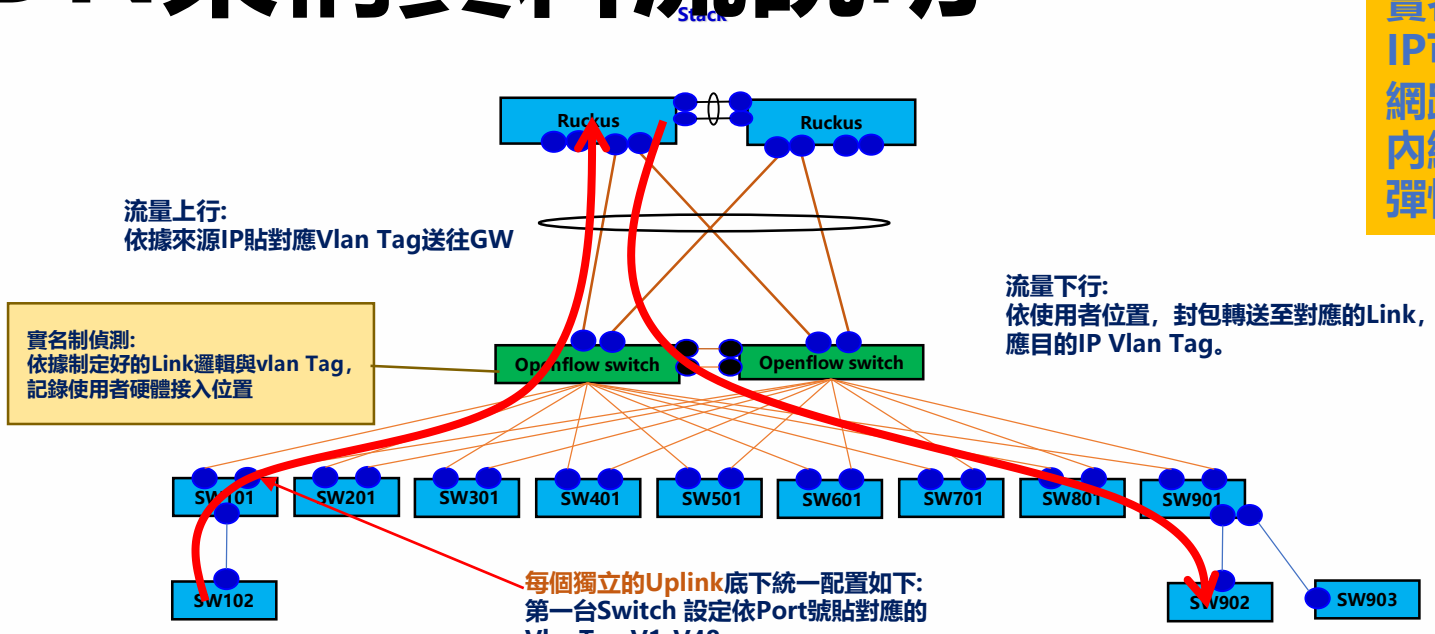
內對內 =>外部遙控內對內攻擊 (透過Ethernet網路)

IoT 攻擊逐年激增



SDN架構資料流說明

實名制管理
IP可攜性
網路隔離
內網資安聯防
彈性擴充架構



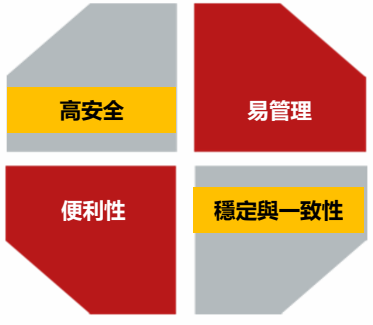
每個獨立的Uplink底下統一配置如下:
第一台Switch 設定依Port號貼對應的
VlanTag V1-V48

第二台Switch 設定依Port號貼對應的
VlanTag V49-V96

第三台Switch 設定依Port號貼對應的
VlanTag V97-V144

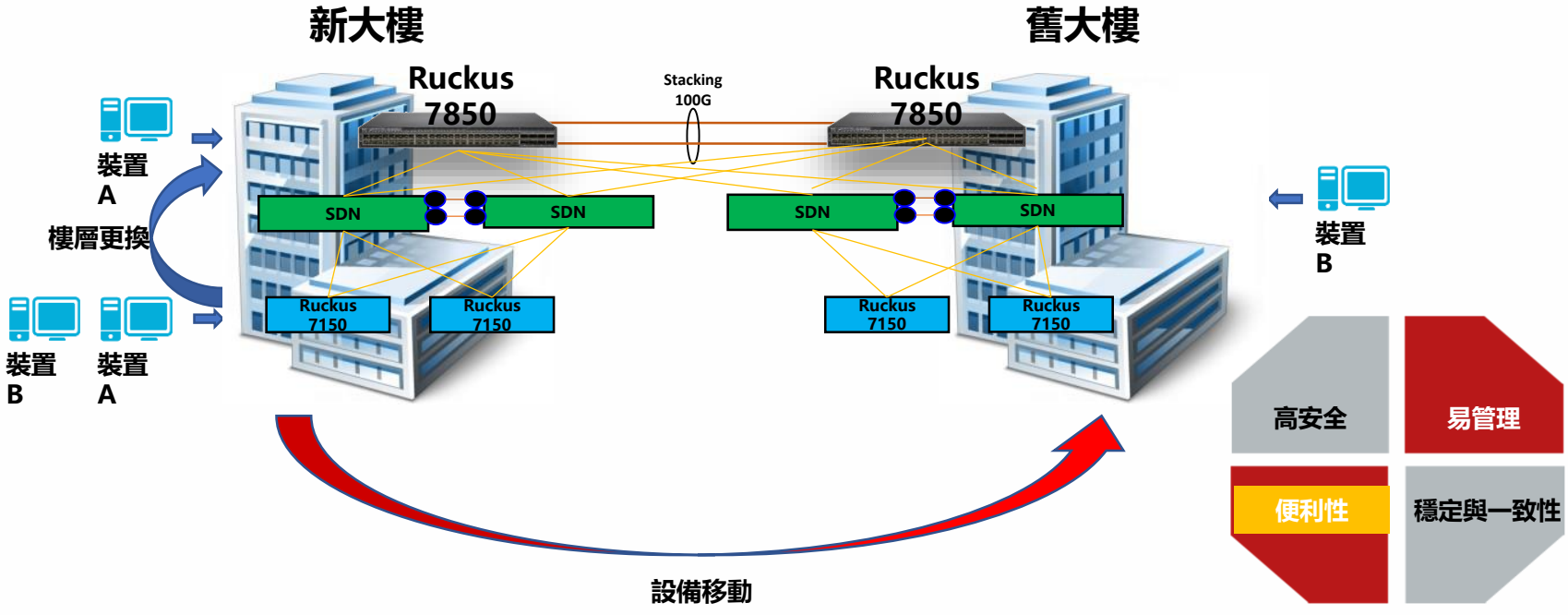
第四台以後的交換器依此邏輯設定

以每個Uplink底下可收容4096個IP裝置



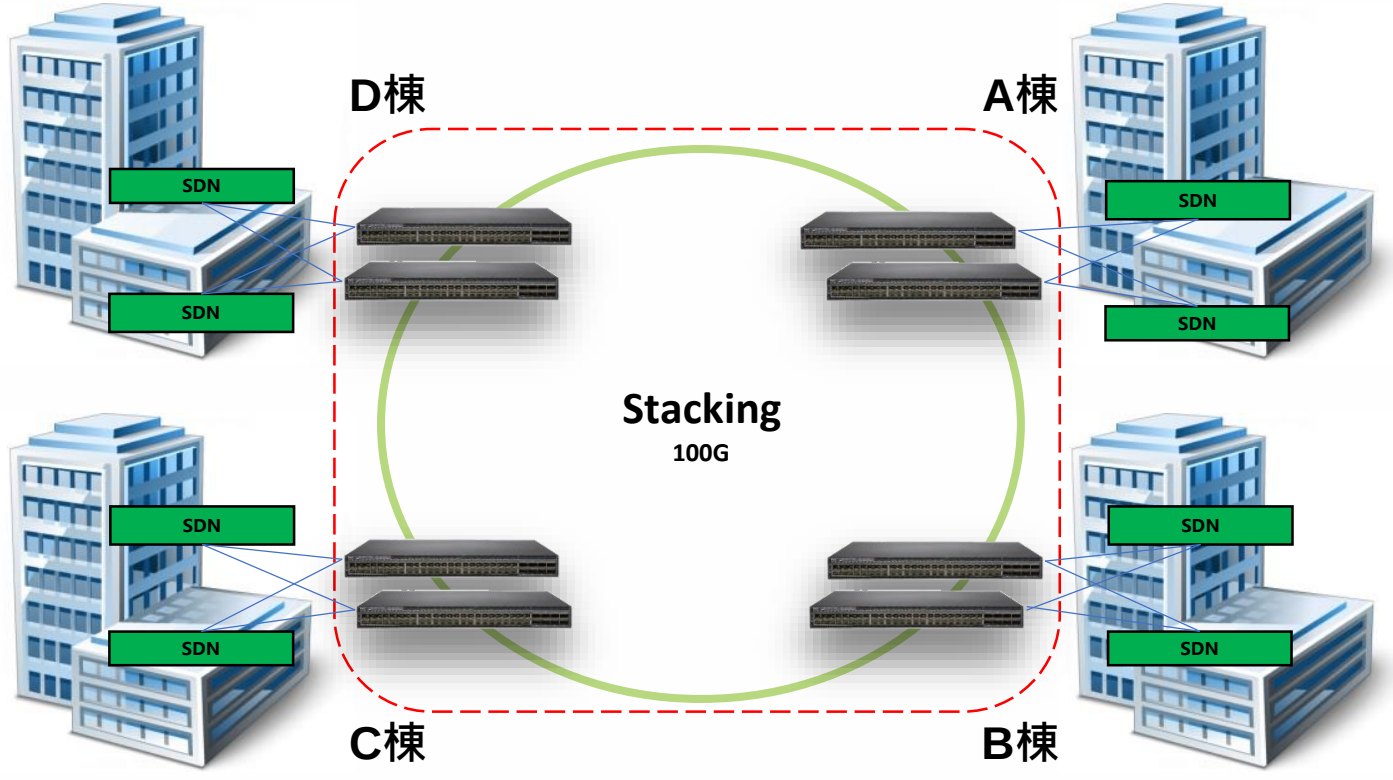
導入功能說明-IP可攜性服務

無須改變任何設定



多棟大樓光纖骨幹網路應用

Stacking形成一部全備援虛擬機箱大幅降低故障風險



1. 最高可將12台融合成一個虛擬機箱
2. 客戶只需管理單一IP
3. 提供單一環或環中環串連方式，提供建置高度彈性，並可支援跨機櫃、跨樓層、跨棟堆疊
4. 韌體更新，不需要中斷服務
5. IP可攜性服務
6. 終端位置隨時更新資訊

導入功能說明-實名制管理

直接搜尋終端

合法終端裝置列表

綁定可選擇MAC or IP+MAC

高安全 | 易管理 | 便利性 | 穩定與一致性

偵測到終端裝置（非法）

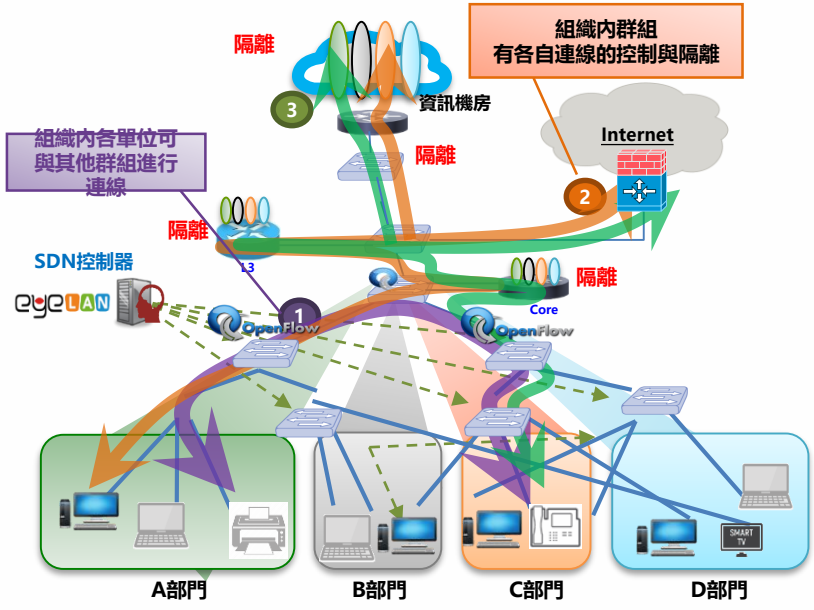
84:ef:18:13:9d:d6_169.254.72.14 169.254.72.14 169.254.72.14 84:ef:18:13:9d:d6 Unknown

84:ef:18:13:9d:d6_172.20.10.13 172.20.10.13 172.20.10.13 84:ef:18:13:9d:d6 Unknown

可預設阻擋、預設自動開通、預設自動隔離

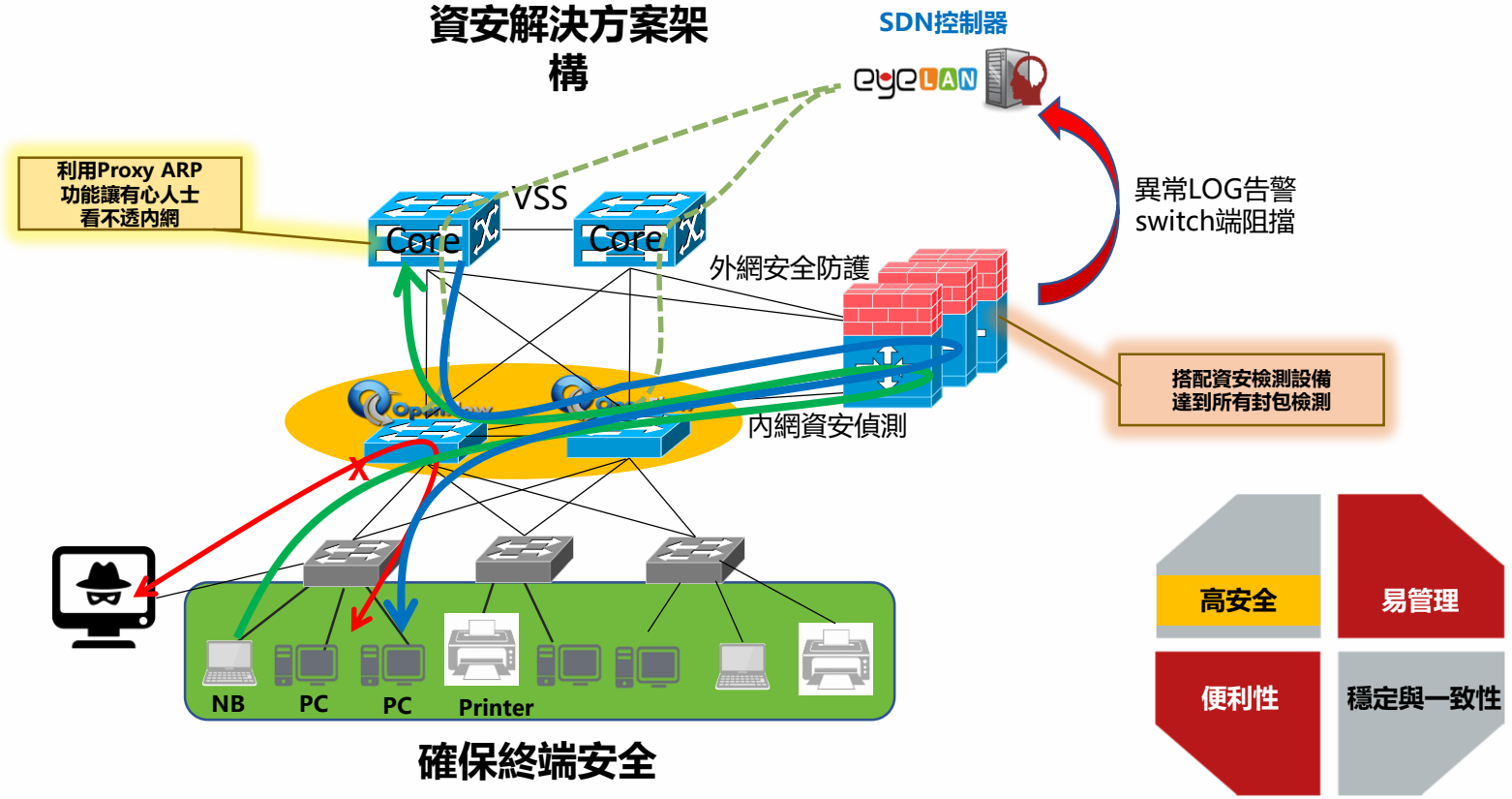
導入功能說明-網路隔離

降低資安風險之適當網路隔離

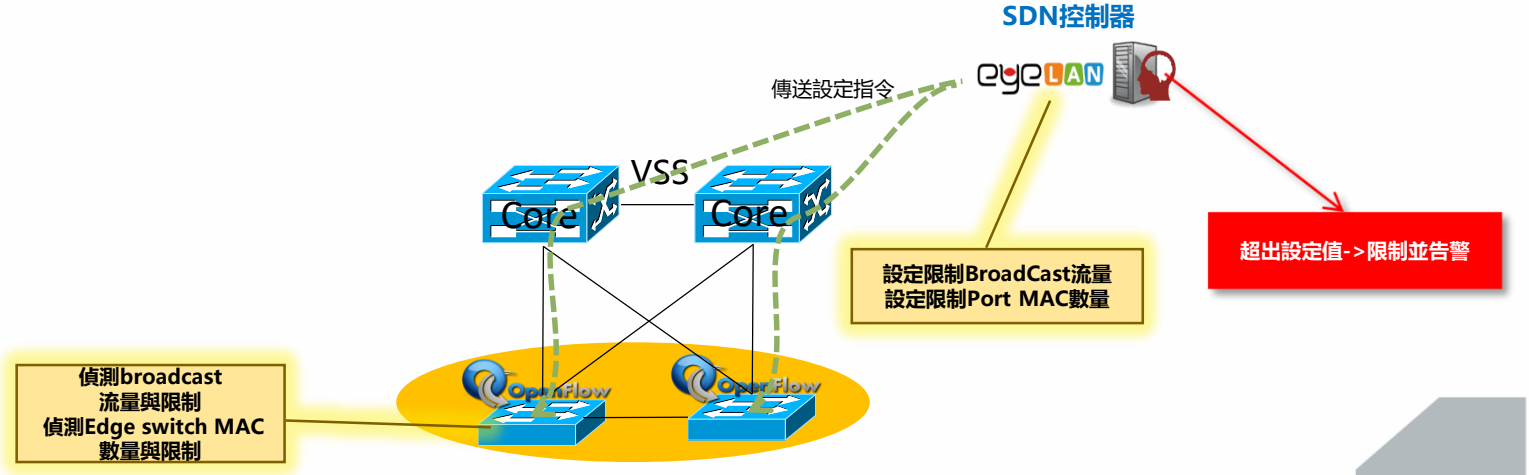


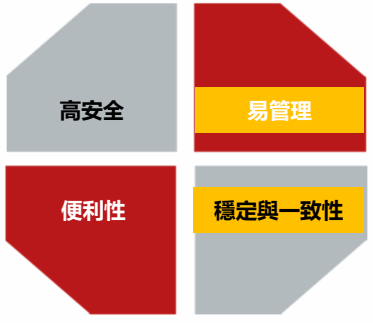
依照不同權限劃分，取得不同隔離與連網行為

導入功能說明-內網資安聯防/ARP遮蔽



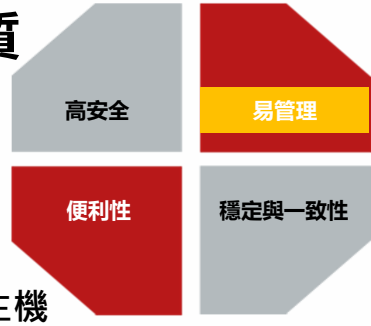
導入功能說明-Loop偵測/Hub偵測





SD-QoE功能

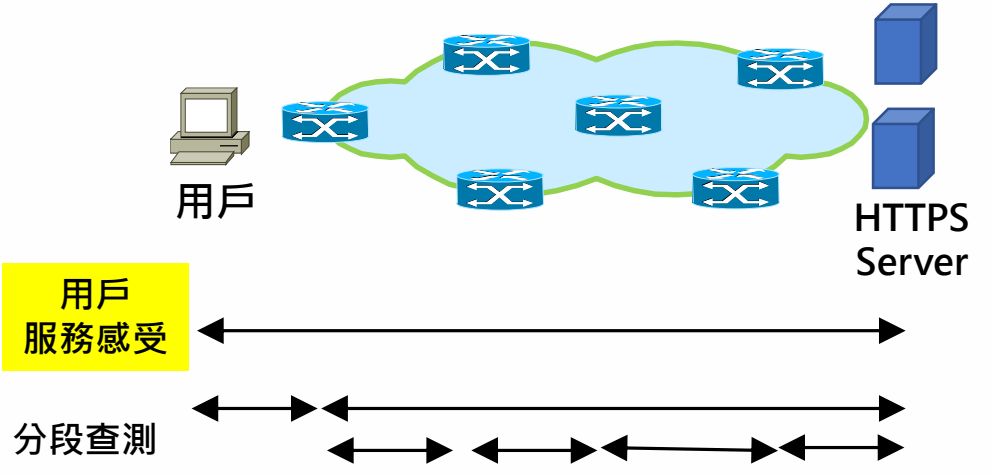
- 維運現況：當終端連線品質不佳時，維運人員須到場障礙排除
- SD-QoE：能掌握用戶使用服務感受、掌握E2E或區段間網路品質
  - 障礙時釐清障礙點(被動查測)
  - 平時定期監控網路品質(主動性)，兩種常用查測方式：Ping、GTP



障礙查測現況

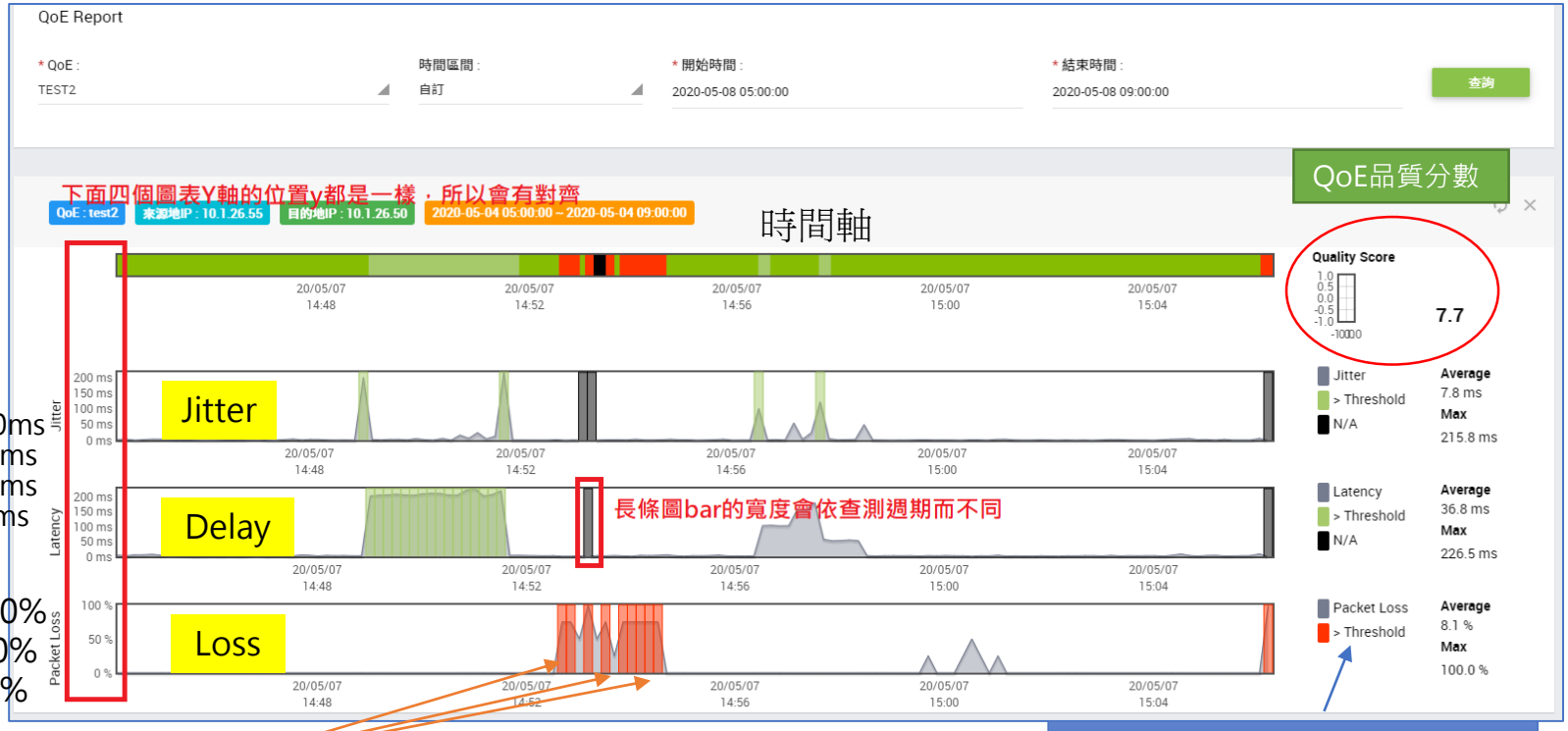
維運人員到現場手動查測
(Ping, Traceroute)

SD-QoE



導入功能說明-SD-QoE

- 視覺畫圖示，方便維運人員判斷障礙



Packet Loss 發生

若量測品質低於標準(可自行定義)
系統可以即時發送告警(e-mail, sms)

- QoE品質分數 (0~10分)
  - ✓ QoE 品質計算方式 = 狀態為 GOOD 的筆數 / 總筆數 * 10
  - ✓ 「狀態為 GOOD 的筆數」定義: Jitter, Latency, Packet Loss 沒有超過 threshold 的資料筆數

案例分享-網路自動化

需求

- 網路設備實名制管理
- 網路自動化
- 多點管理

導入前

- 人員依照員工資料建檔、登入資訊
- 依據員工上班地點，查詢該區域網路設備相關設定
- 設定新進員工網路設備相關設備配置
- 設定新進員工資安相關設備紀錄

導入後

- 人員依照員工資料建檔、登入資訊 ❶
- 自動化作業完成 ❷ ❸ ❺

案例分享- IoT管理應用

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

傳統網路問題	SDN網路方案
IoT與網路設備設定費時、各網路設備QoS設定複雜、人工判別IoT設備運作狀態	單一介面操控全網設定配置、QoS設定簡單與彈性、主動偵測IoT設備是否存活
訊務流量異常不易判斷	訊務監控 IoT設備流量，流量告警機制
訊務複製功能受限制	可依需求彈性訊務複製
無實名制管理	IoT設備可視化(實名制)管理
無內對內資安防護	降低資安風險

資安設備聯防

資安設備聯防

- EyeLAN 2000控制器、OpenFlow 交換器
- 與Palo Alto進行聯防
- 資安服務鍊

➢ 簡化維運與障礙查測流程

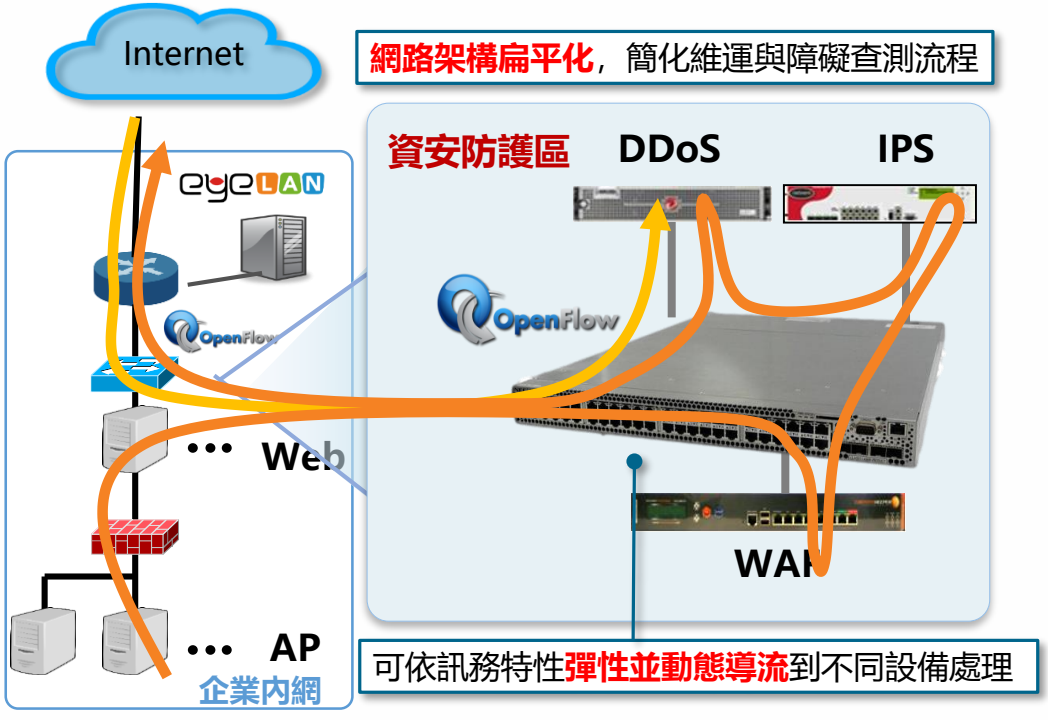
- 導入新產品或新功能應用容易
- 設備故障查測加快，更換設備容易

➢ 減輕資安設備負載

- 動態網路流量過濾及轉導，將特定網路流量導入特定資安設備

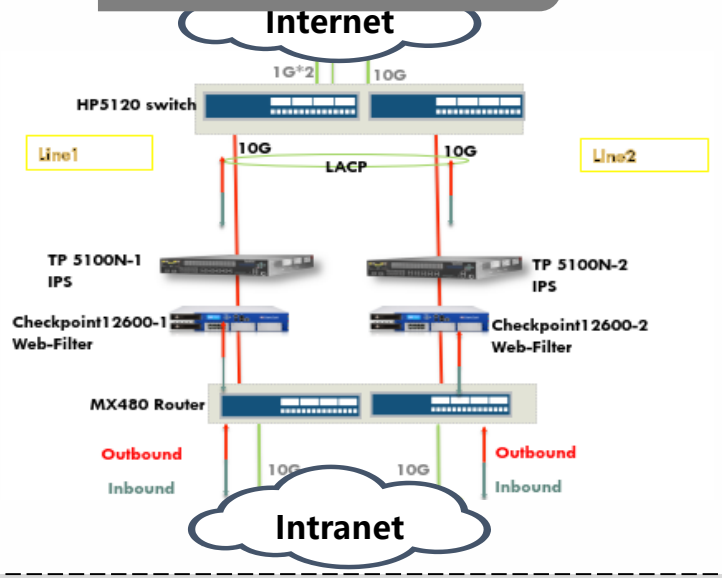
➢ 即時阻擋

- 提供API供資安設備進行訊務阻擋、Mirror、轉導



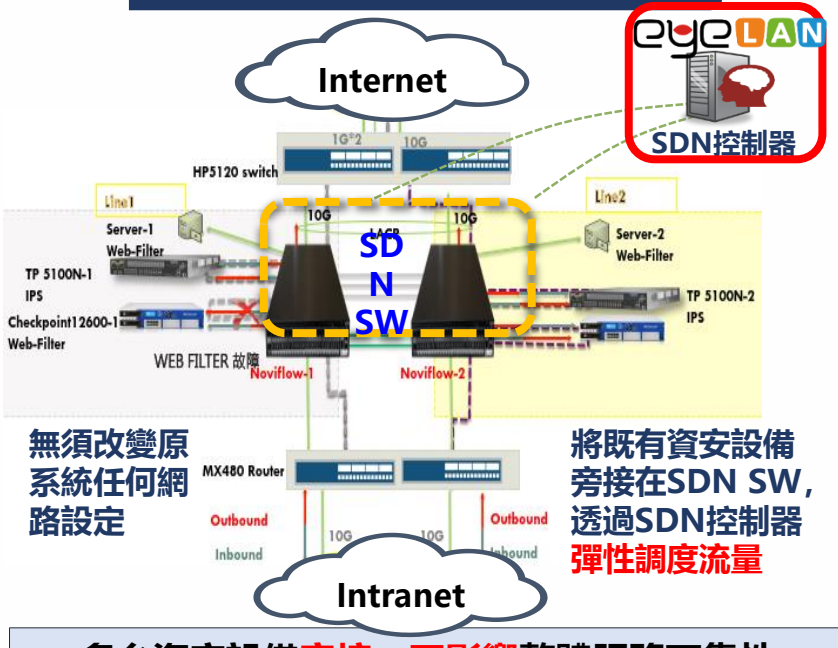
案例分享-資安導流與架構優化調整

過往的安全服務鏈架構



- 多台資安設備串接，**影響整體服務可靠性**
- 流量經過多次轉發，**產生高延遲**
- 疊加過多設備，造成**性能瓶頸**與**資安成本提升**
- 導入新產品或新功能應用，對**整體網路有影響風險**
- 設備故障**查測複雜**，**更換設備不易**
- 流量管理**分散**在各設備，**資安聯防不易**

SDN控制系統安全服務鏈架構



無須改變原系統任何網路設定

將既有資安設備旁接在SDN SW，透過SDN控制器**彈性調度流量**

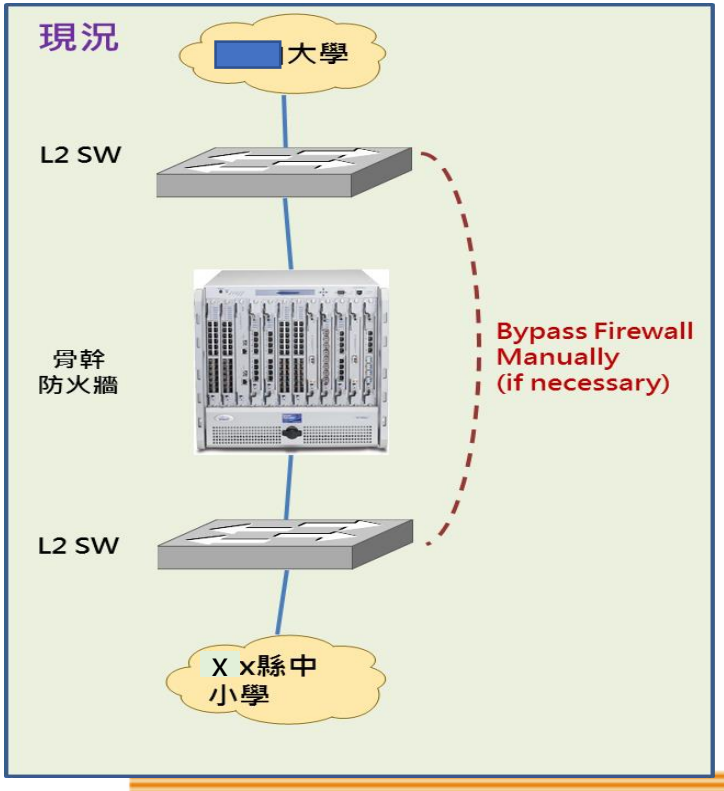
- 多台資安設備**旁接**，**不影響**整體服務可靠性
- 流量經需求導流轉發，**不產生**高延遲
- 性能彈性疊加**不造成**瓶頸
- 導入新產品或新功能應用**無任何影響風險**
- 設備故障**查測加快**，**更換設備容易**
- 兼具**流量管控功能**與**資安聯防機制**

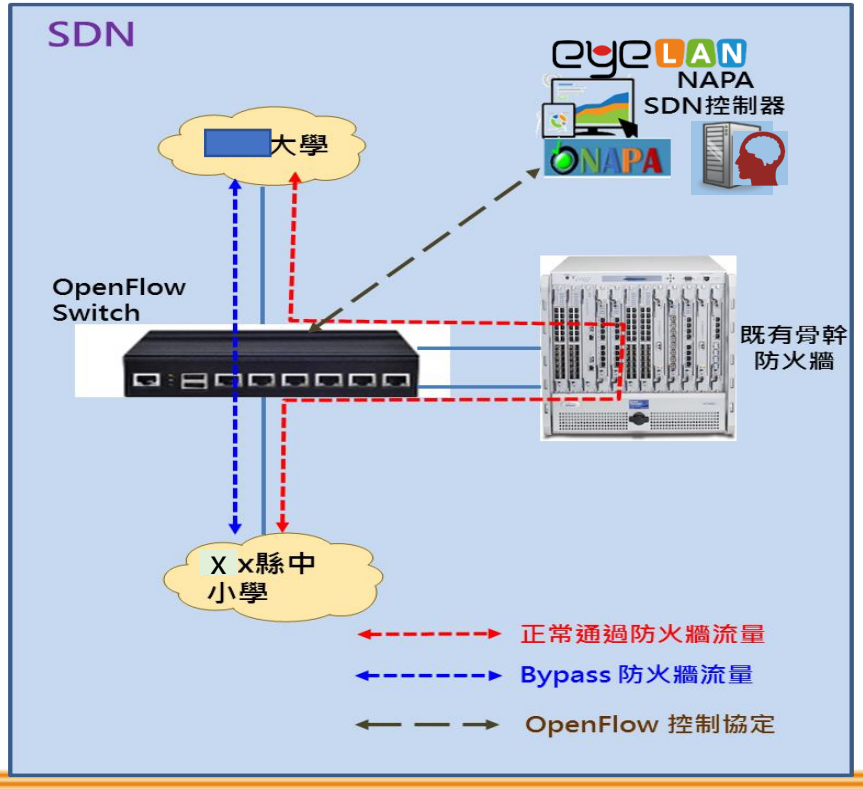
案例分享-Bypass

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

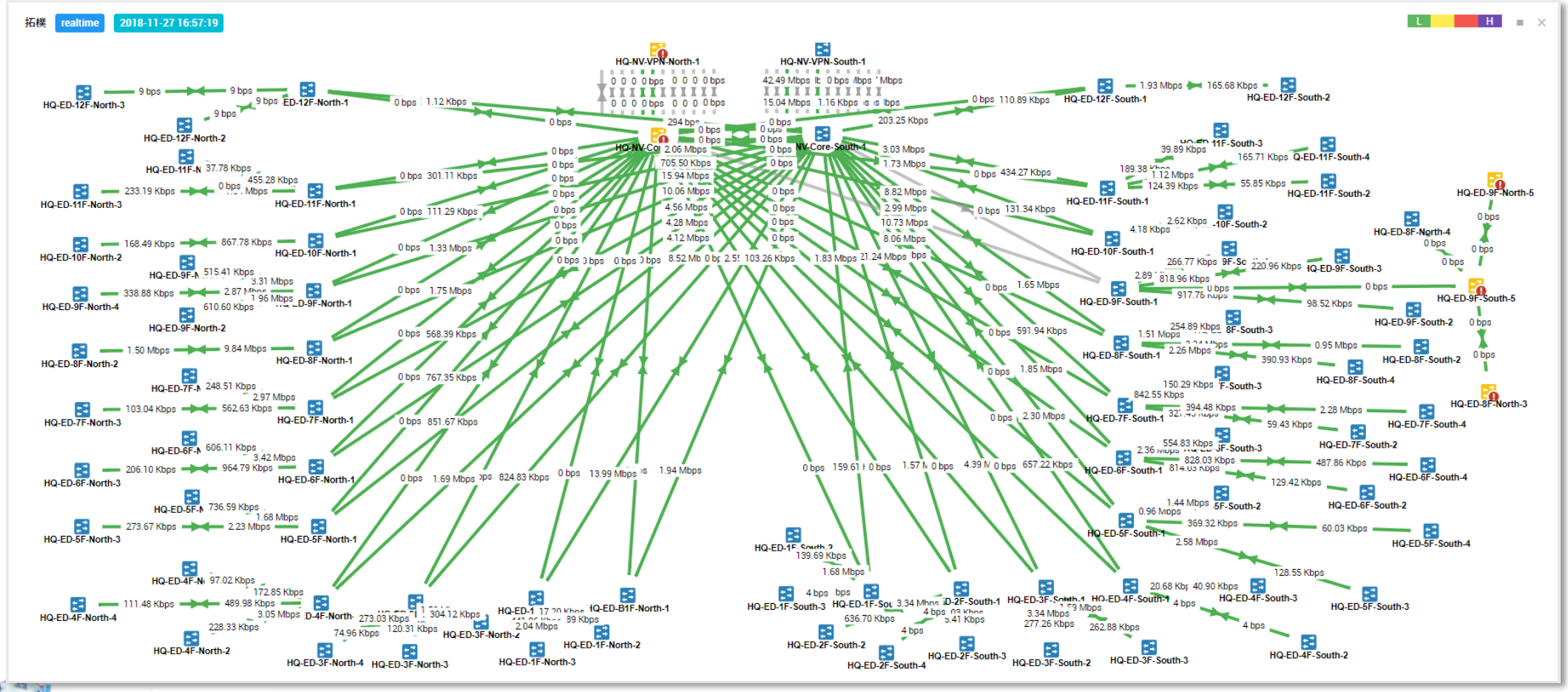
需求

- 設備故障Bypass
- 降低防火牆負載





EyeLAN網路架構拓樸圖



維運分享-中華電信總公司大樓

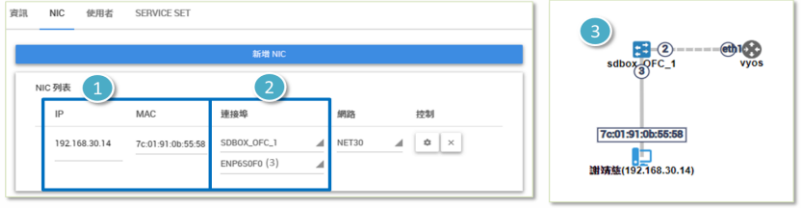
障礙查測步驟

終端設備連網管理　步驟一

- 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

終端位置 (自動偵測)　步驟二

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　步驟三

- 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

流量監控　步驟四

- 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

成功案例

中華電信 Chunghwa Telecom

中華民國國家安全局 National Security Bureau, R.O.C.

TAIPEI 臺北市政府

高雄市政府 Kaohsiung City Government

國家發展委員會 NATIONAL DEVELOPMENT COUNCIL

臺中市政府 TAICHUNG CITY GOVERNMENT

新竹市政府 HSINCHU CITY GOVERNMENT

高雄市政府教育局 EDUCATION BUREAU, KAOHSIUNG CITY GOVERNMENT

明新學校財團法人 明新科技大學 Minghsin University of Science and Technology

國立交通大學 National Chiao Tung University

中山大學 SUN YAT-SEN UNIVERSITY

國立中央大學 National Central University

中央研究院 ACADEMIA SINICA


Thank you
Q&A