新北市教育局

網路環境與管理介紹
經驗分享

教育研究及資訊發展科
網路諮詢輔導員 李　煒

新北市政府 Education Department, New Taipei City Government 教育局

- 學歷：
  - 國立中正大學資訊工程研究所
- 證照：
  - *ISO/IEC 27001:2022 LAC*
  - *BS10012:2017/ISO29100:2011 LAC*
  - *ISO/IEC27701:2019 LAC*
  - *資安：CHFI 、CEH 、CCNA 、NSE4 、NSPA*
  - *網路：CCNP 、JNCIA 、JNCIS*
- 工作經歷
  - **新北市教育局網路諮詢輔導員**
  - **新北市教育局網路管理輔導員**
  - **ISCB資訊安全稽核員**
  - **TACCST技術稽核檢核員**
  - **ISCB個資安全稽核觀察員**

新北市政府 教育局
Education Department, New Taipei City Government

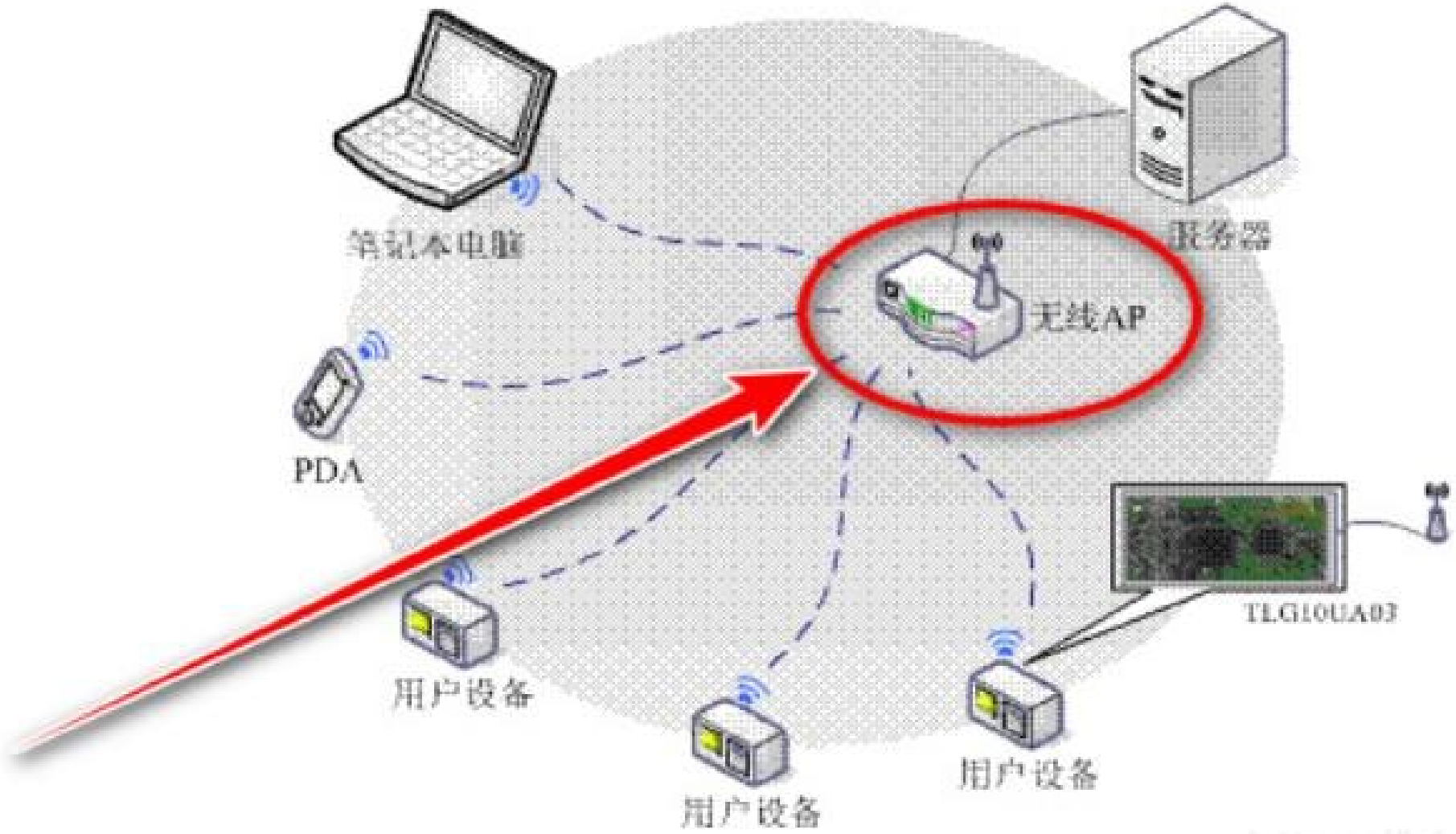
分享內容

新北市教育無線網路架設經驗分享

新北市教育網路架構分析經驗分享

資通安全技術檢核經驗分享

我們的無線網路VS WIFI Router



無線AP是甚麼
Access Point WiFi 6

這是WIFI ROUTER

OTOLINK N200RE_V5 300M...
4h.pchome.com.tw · 有庫存

路由器推薦】無線路由器(Router)、IP分享器(NAT)、交...
ofeyhong.pixnet.net

TP-Link TL-MR6400 N300 4G S...
tw.buy.yahoo.com · 有庫存

TP-Link TL-WR840N 300Mbp...
24h.pchome.com.tw · 有庫存

口袋型無線分享器】 – 網路設備...
tkec.com.tw

無線分享器| 路由器 | TOTOLINK 台灣
totolink.tw

Cisco Fortigate Dlink
Acess Point AP

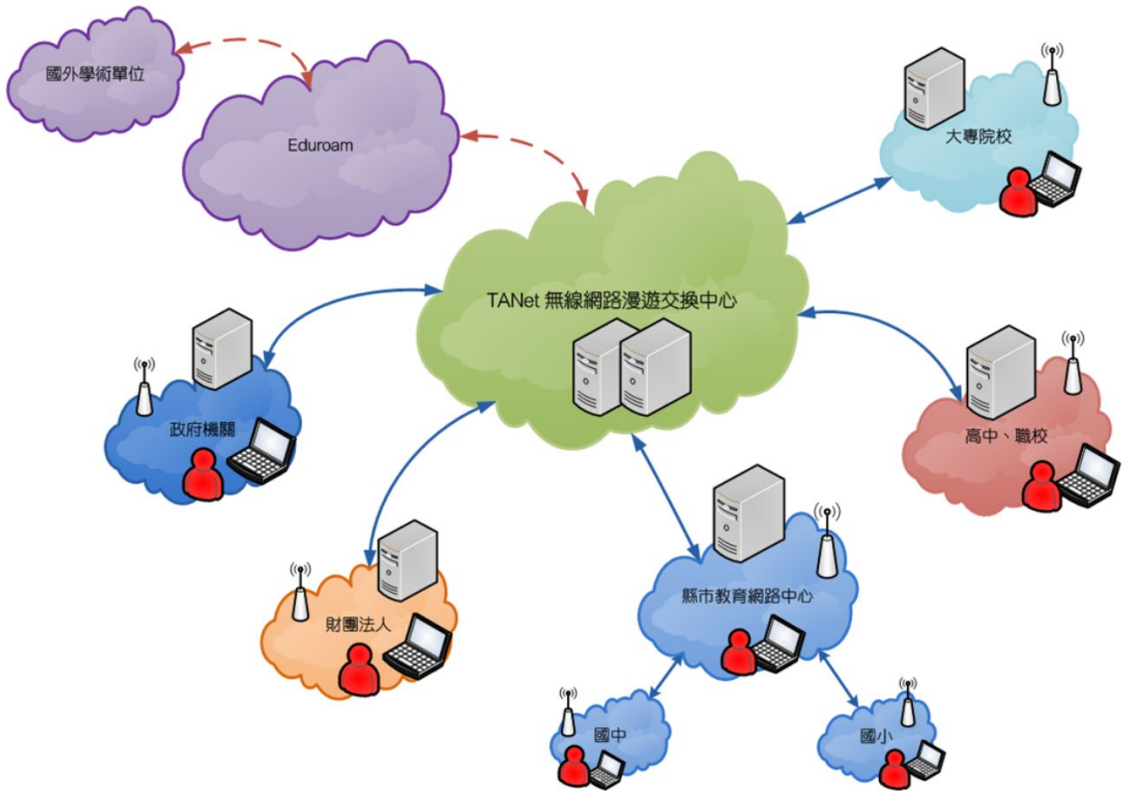
新北市政府 教育局
Education Department, New Taipei City Government

新北市WIFI行動箱第1-3代

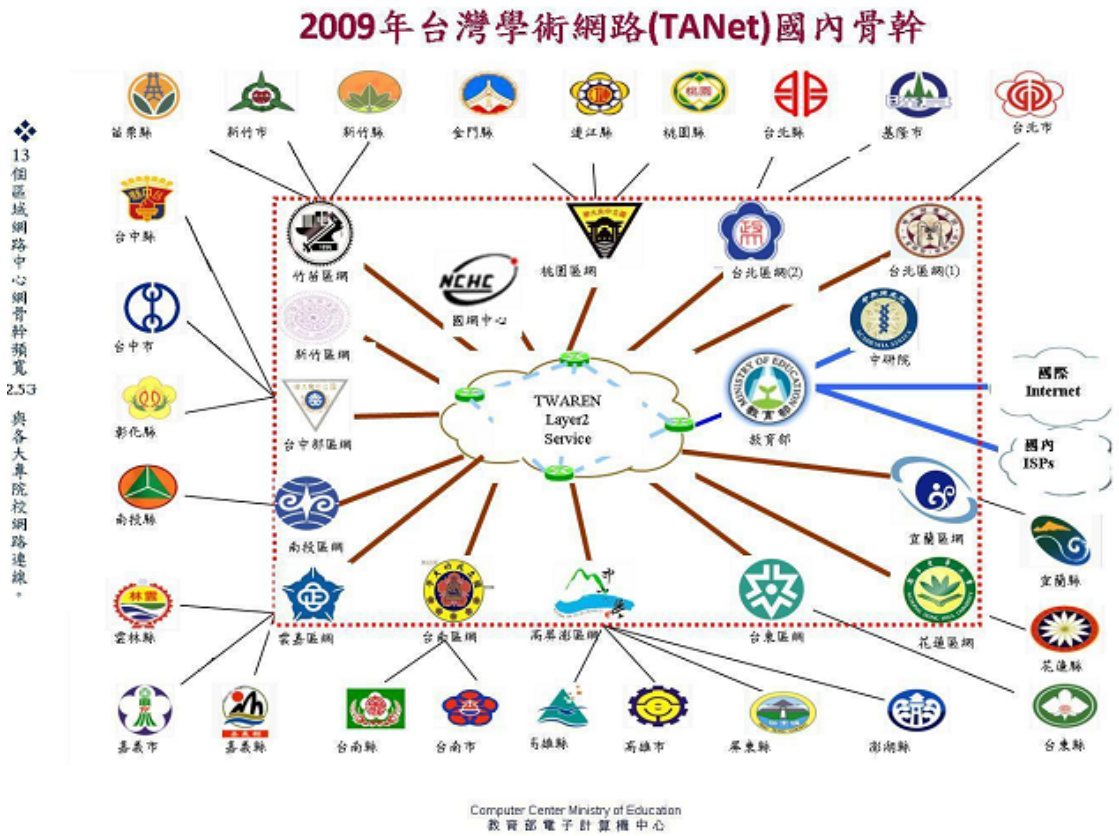
新北市政府 教育局
Education Department, New Taipei City Government

Taiwan Academic Network Roaming

TANet無線網路漫遊交換中心



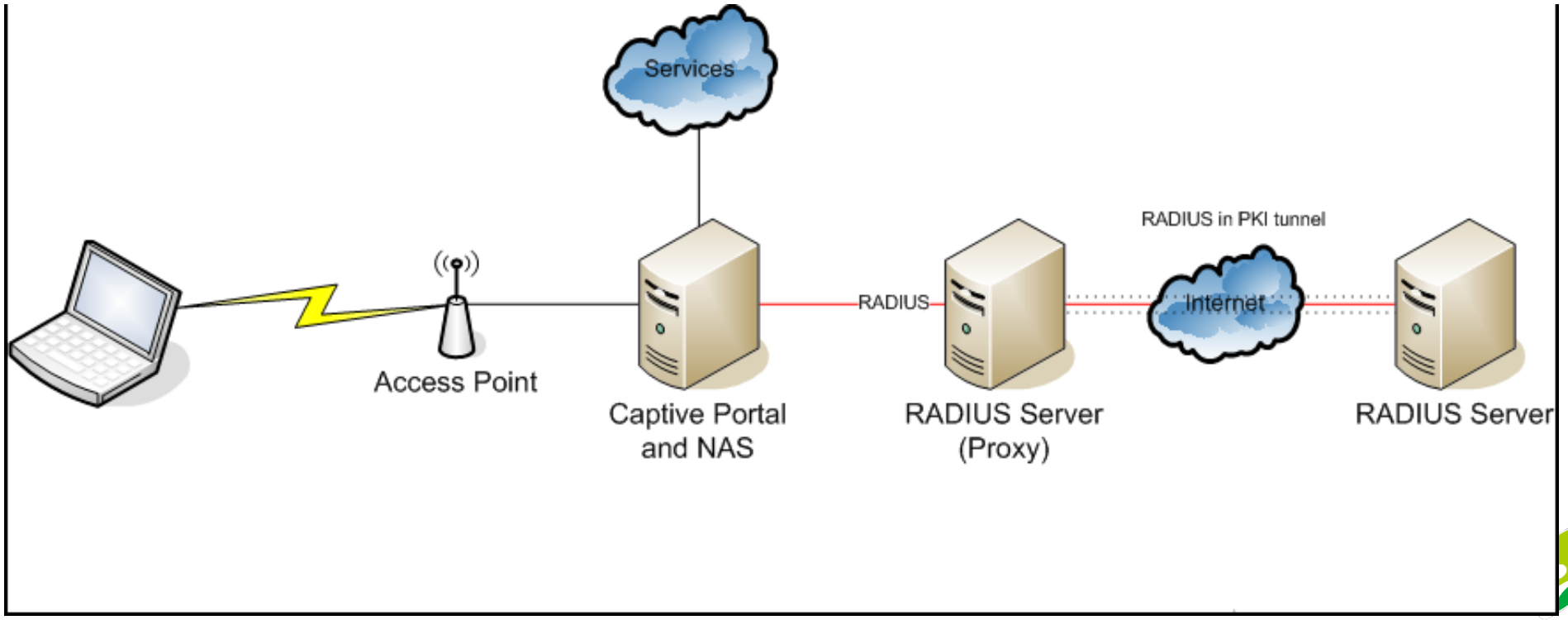
校園無線網路漫遊服務架構圖



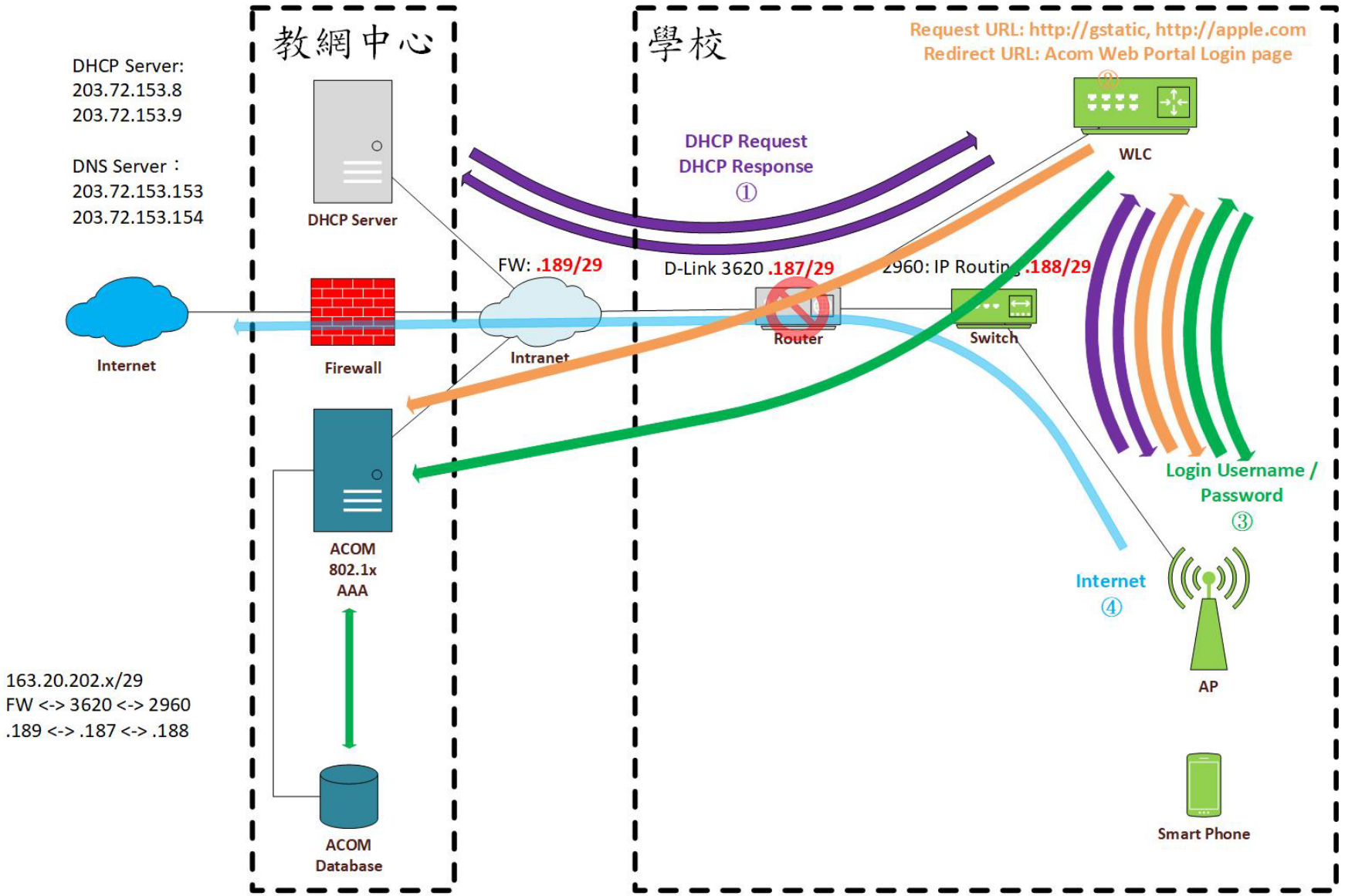
新北市政府 教育局
Education Department, New Taipei City Government

Radius Server 認證

- Authenticator(Cisco WLC 3504)帶的HOST IP
- Radius Server(ACOM)是否已經加入Authenticator ip
- Key「共享密碼」(Shared secret)　XXXXX
- Firewall udp port 1812-1813 1645-1646

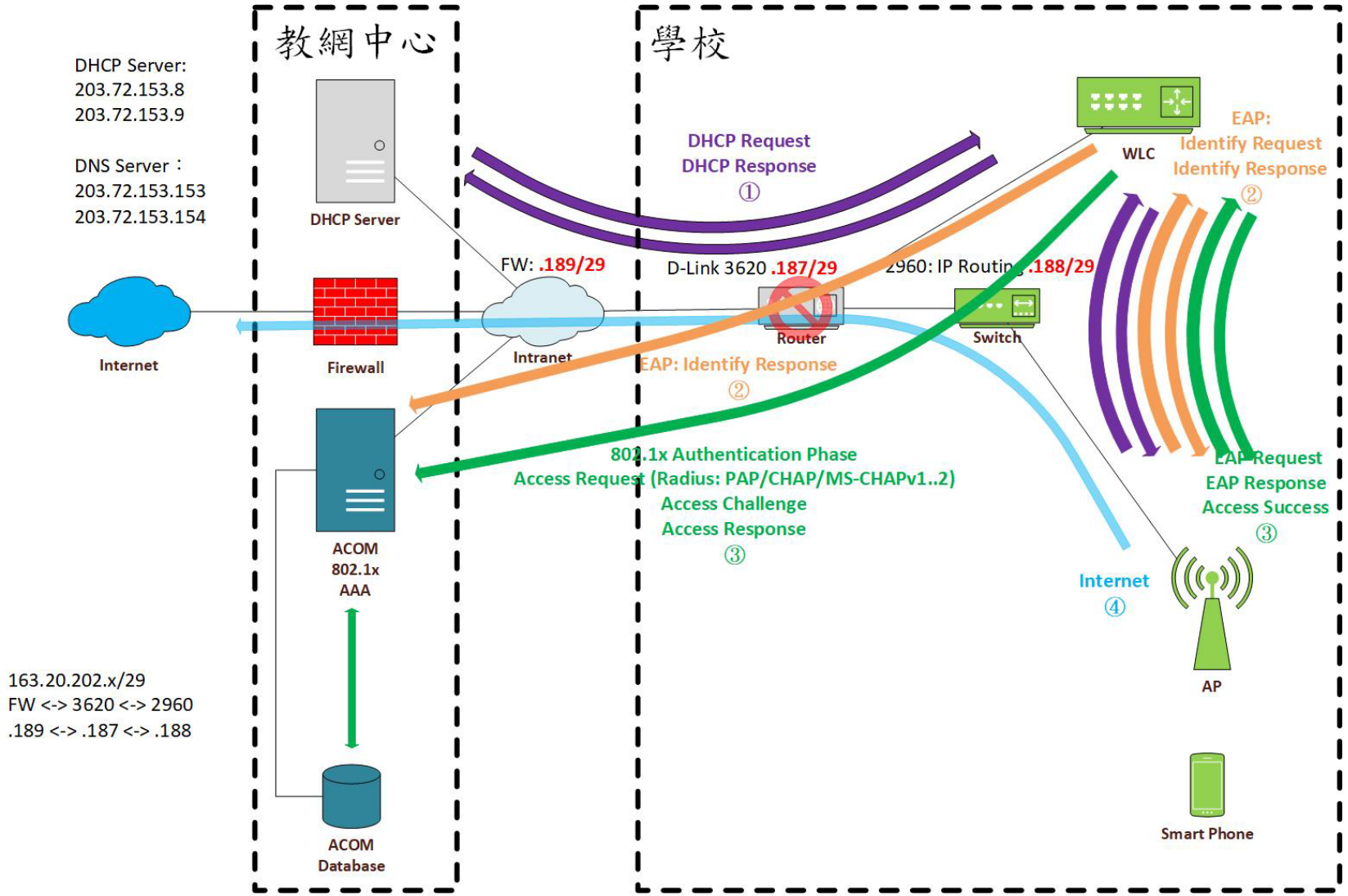


Web Portal Flow



新北市政府 教育局
Education Department, New Taipei City Government

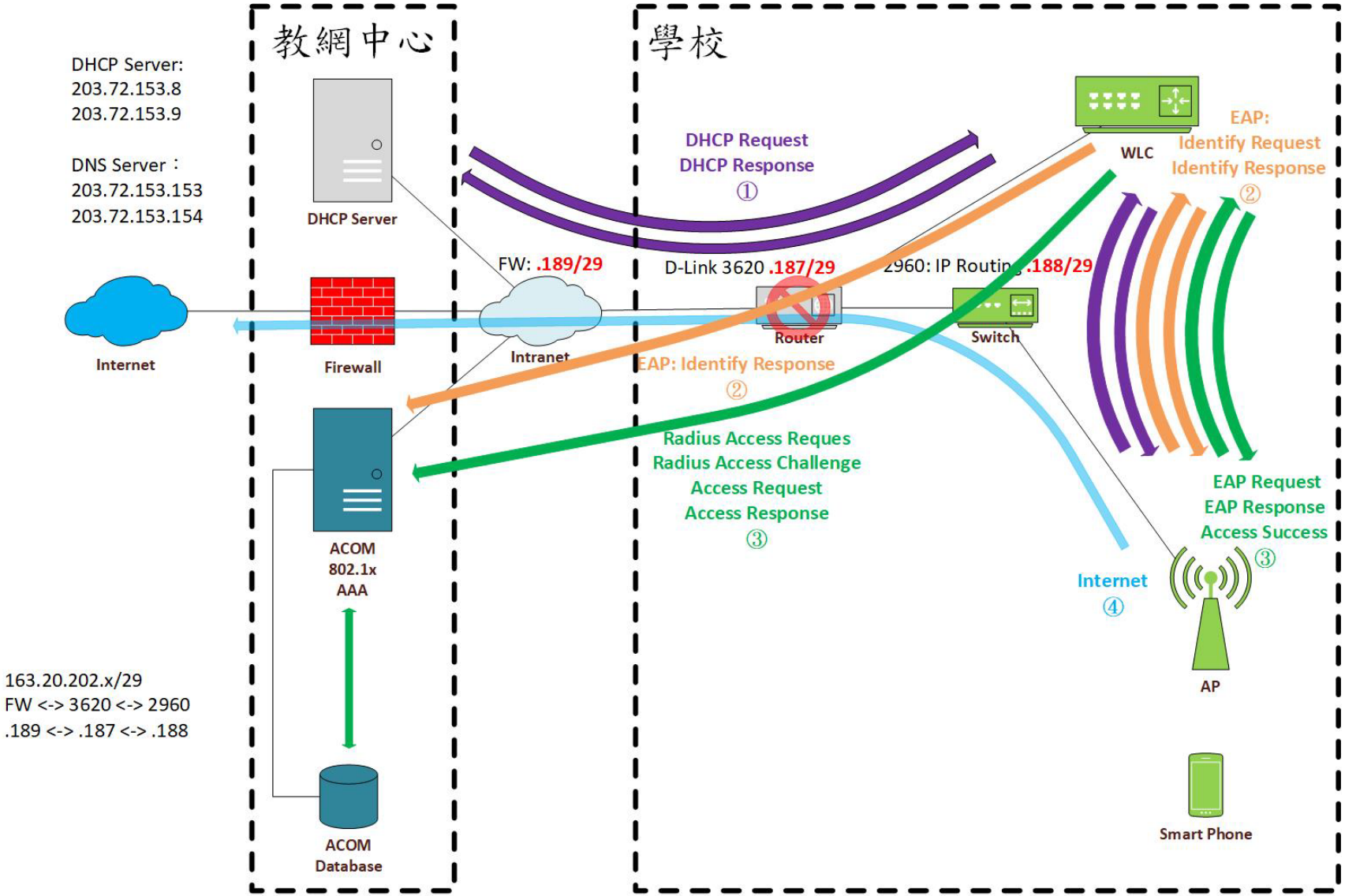
802.1X Flow



①②③④⑤⑥⑦⑧⑨⑩

新北市政府 教育局
Education Department, New Taipei City Government

MAC Filtering



新北市政府 教育局
Education Department, New Taipei City Government

外國實測


มหาวิทยาลัยเชียงใหม่
CHIANG MAI UNIVERSITY
สำนักหอสมุด
MAIN LIBRARY
17:58
Wi-Fi
eduroam
專用 Wi-Fi 位址
Wi-Fi 位址
20:69:80:D2:AB:95
使用專用位址可協助你在使用不同的 Wi-Fi 網路時，降低你的 iPhone 被追蹤的機率。
限制 IP 位址追蹤
在「郵件」和 Safari 中對已知的追蹤器隱藏你的 IP 位址來限制 IP 位址追蹤。
IPV4 位址
設定 IP
自動
IP 位址
10.81.53.6
子網路遮罩
255.255.252.0
路由器
10.81.52.1

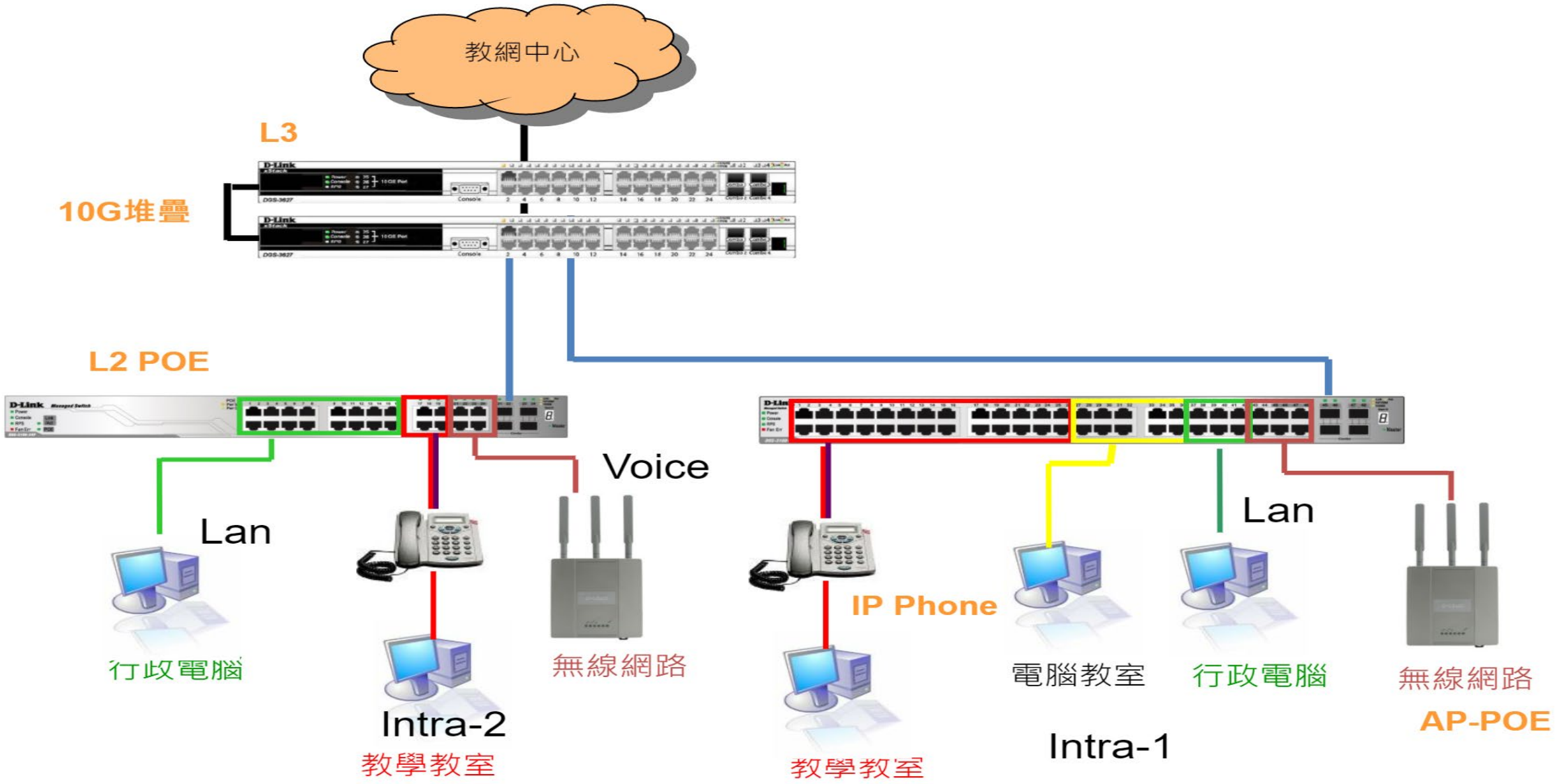

13:42
Wi-Fi
eduroam
低數據模式
專用 Wi-Fi 位址
Wi-Fi 位址
20:69:80:D2:AB:95
使用專用位址可協助你在使用不同的 Wi-Fi 網路時，降低你的 iPhone 被追蹤的機率。
限制 IP 位址追蹤
在「郵件」和 Safari 中對已知的追蹤器隱藏你的 IP 位址來限制 IP 位址追蹤。
IPV4 位址
設定 IP
自動
IP 位址
172.19.101.124
子網路遮罩
255.255.252.0
路由器
172.19.100.1


Tentoonstellingen
Exhibitions
Aziatisch Paviljoen
Asian Pavilion

如何熟習操作

- 建制實驗環境
  - 架設VM
  - 原廠申請帳號
  - 原廠下載firmware
  - 可以登入web操作
  - 可以GUI設定在ssh看config

新北市高國中小學校園網路架構



學校IP基本網段

Vlan	VID	網段	IPv6	用途
Mgt	1	10.226.56.254	2001:288:22xx:1::/64	網管用 >101 L2,>201 AP
Wan	2	163.20.202.184/29	2001:288:2201::xx/124	對外連結網段
Lan	5	163.20.66.254/24	2001:288:22xx:5::/64	行政用 保留<10 ；>250
dsa_wan	8	10.253.56.254/24	2001:288:22xx:8::/64	DSA-WAN IP (10.253.56.1)
Intra-1	10	10.231.56.254/24	2001:288:22xx:10::/64	電腦教室
Intra-2	20	10.241.56.254/24	2001:288:22xx:20::/64	教學教室
Voice	25	10.243.56.0/24	2001:288:22xx:25::/64	VoIP
Wlan	30	10.251.56.254/24	2001:288:22xx:30::/64	無線網路 (IP移至DSA-3600使用)
WPA2	35	10.245.56.0/24	2001:288:22xx:35::/64	無線WAP2用
MAC	36	10.247.56.0/24	2001:288:22xx:36::/64	無線Mobile用

ip分配規範原則及使用原理

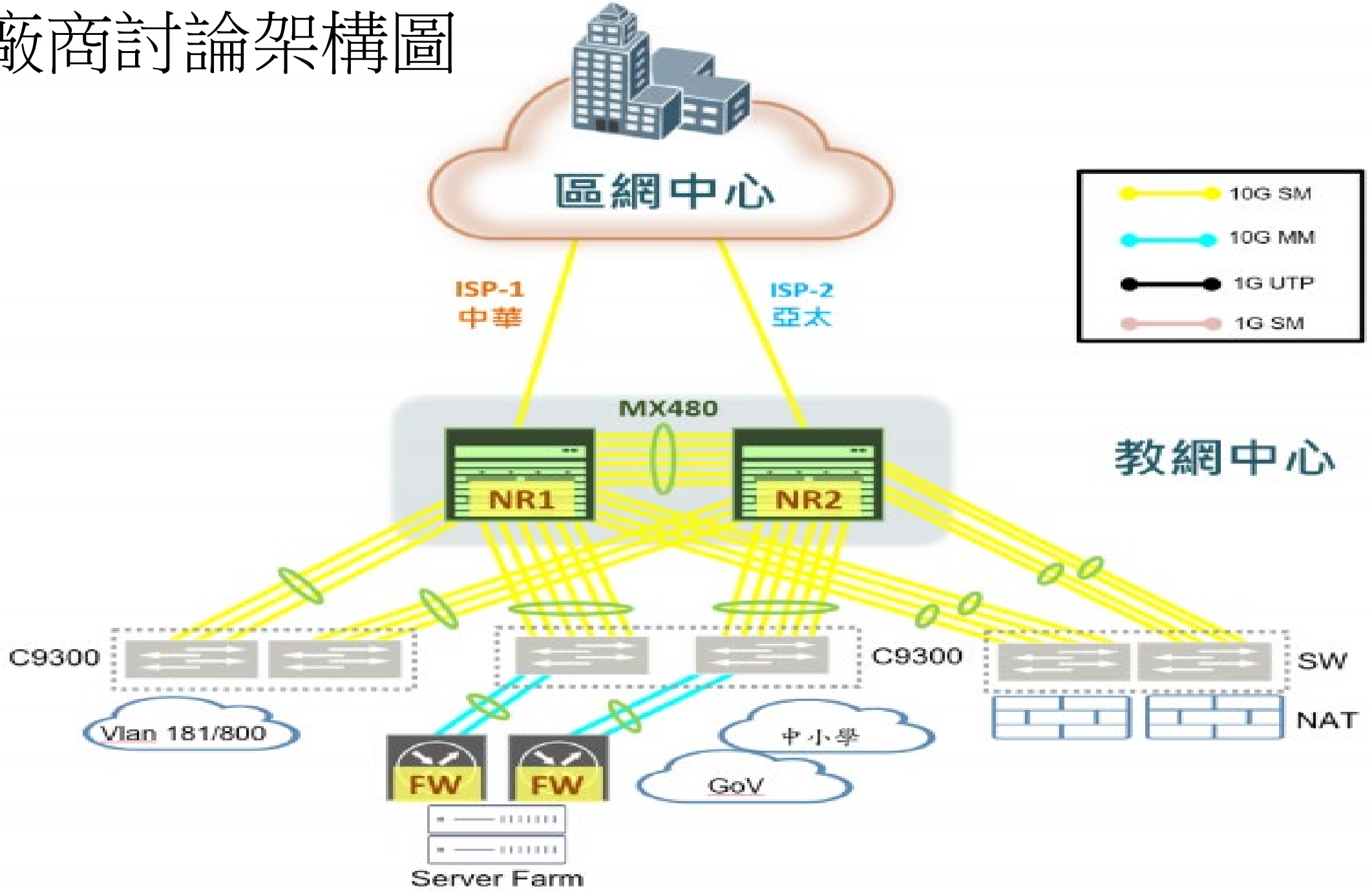
ipv4內網單一、唯一，易於log查找。

ipv4整體vlan優先於校碼，考量全市防火牆策略的運用。

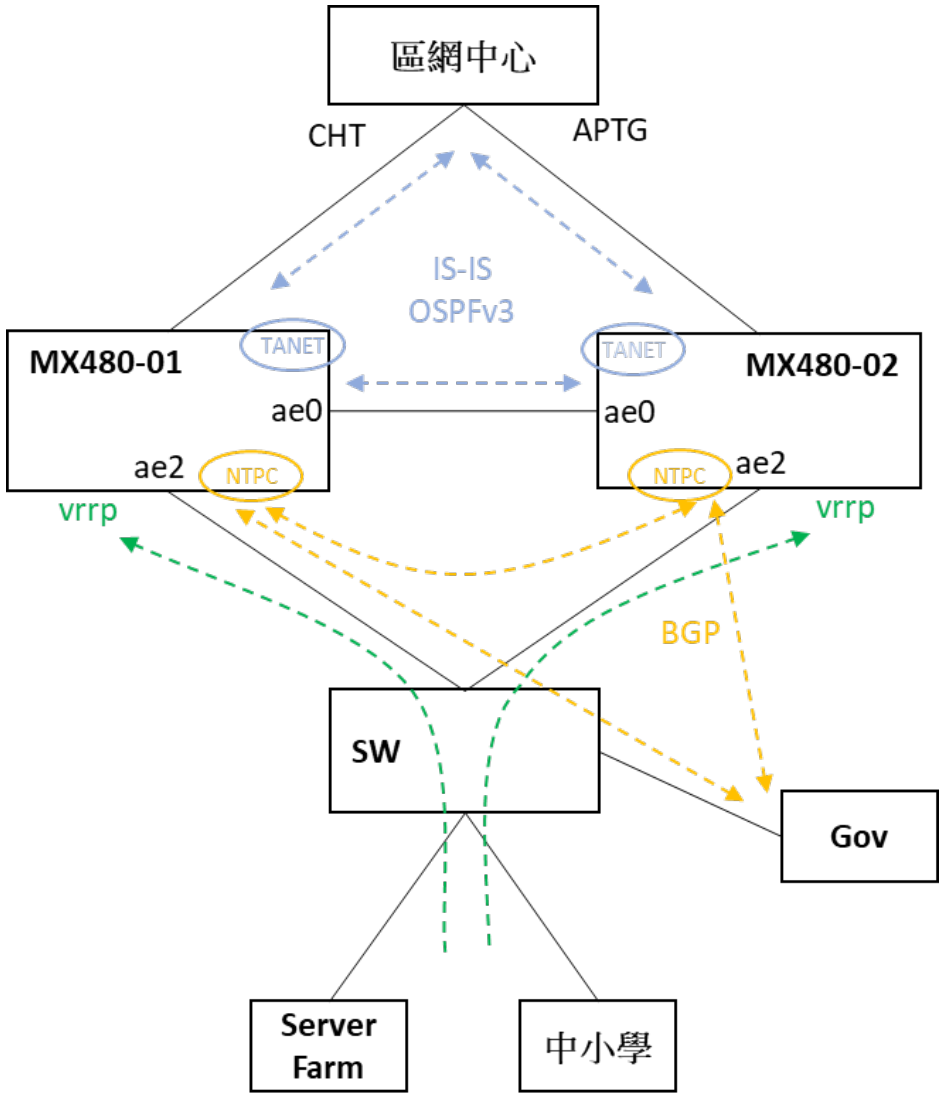
Ipv6需考量firewall policy設定。先校碼再vlan。先vlan再校碼

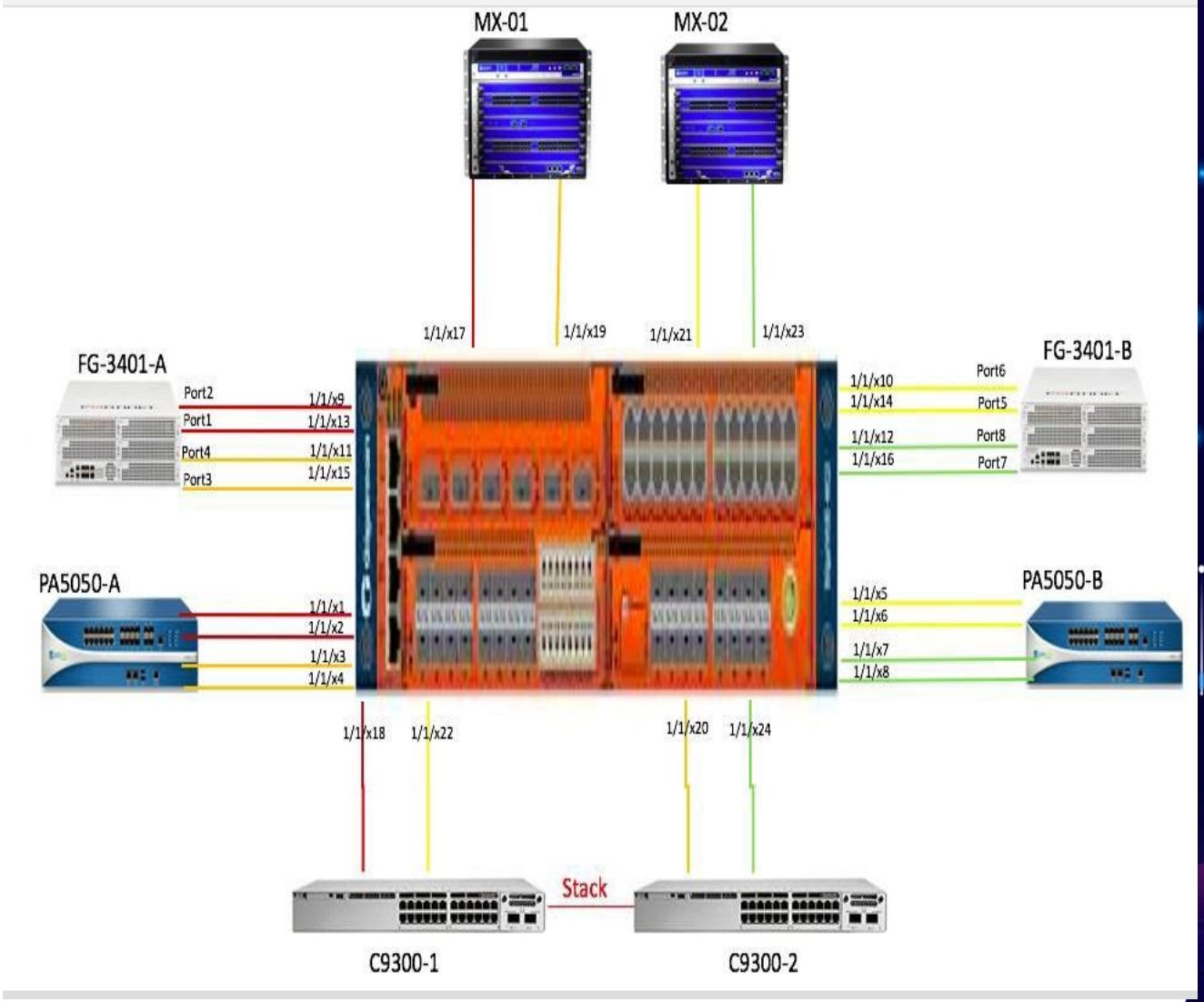
NAT pool對應設計，使用集中網段?(firewall policy考量)，使用各校實體網段?(易記)

與廠商討論架構圖

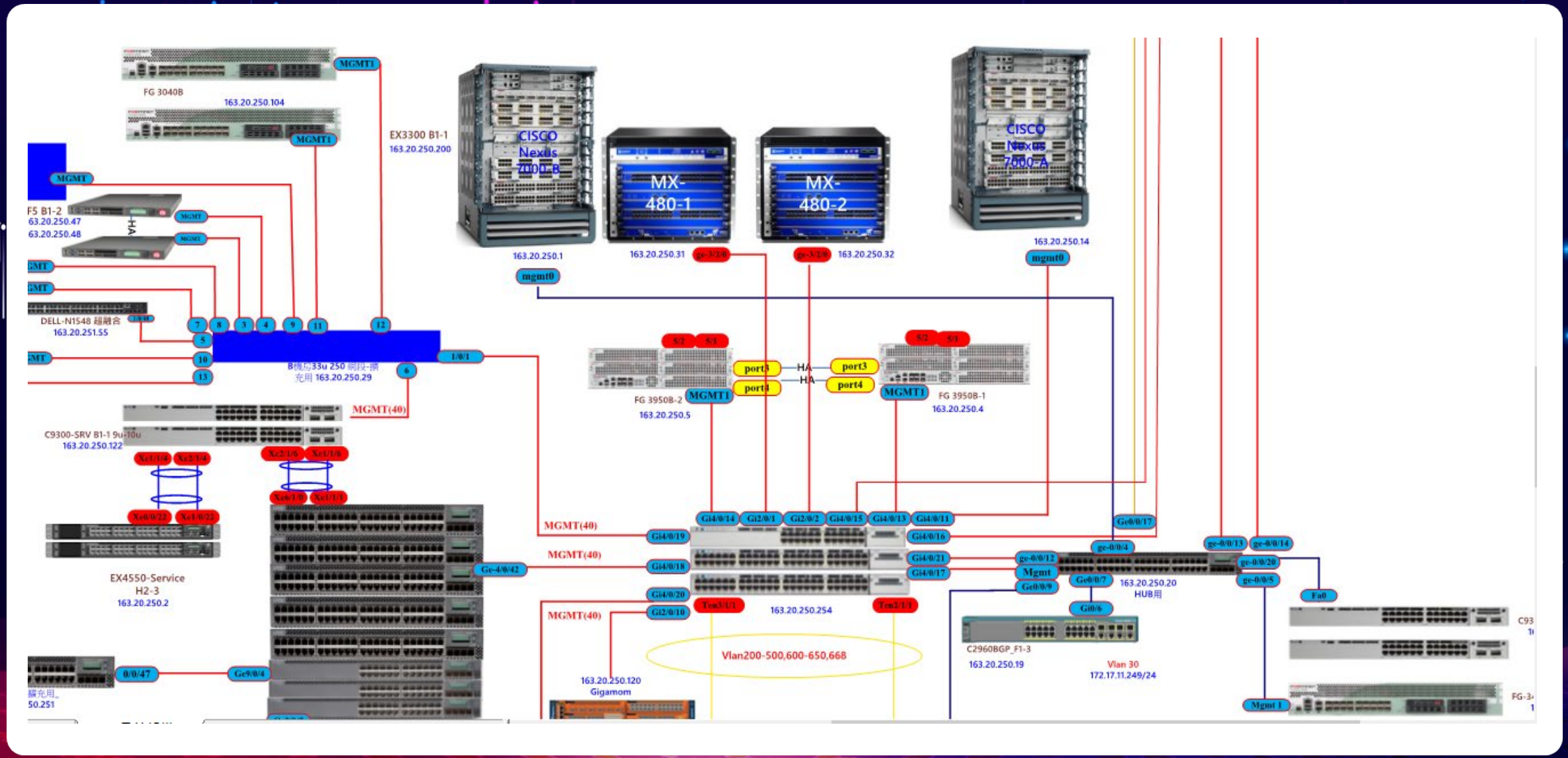

區網中心
ISP-1
中華
ISP-2
亞太
10G SM
10G MM
1G UTP
1G SM
MX480
NR1
NR2
教網中心
C9300
C9300
SW
NAT
Vlan 181/800
FW
FW
中小學
GoV
Server Farm

新北市核心骨幹交換器拓譜圖(範例)





獨立的管理線路(範例)


FG 3040B
163.20.250.104
MGMT1
EX3300 B1-1
163.20.250.200
CISCO Nexus 7000_B
MX-480-1
MX-480-2
CISCO Nexus 7000_A
163.20.250.1
163.20.250.31
163.20.250.32
163.20.250.14
mgmt0
F5 B1-2
63.20.250.47
63.20.250.48
HA
DELL-N1548 超融合
163.20.251.55
B棟5樓33u 250 網段-備用 163.20.250.29
FG 3950B-2
163.20.250.5
FG 3950B-1
163.20.250.4
port3
port4
C9300-SRV B1-1 9u-10u
163.20.250.122
MGMT(40)
EX4550-Service
H2-3
163.20.250.2
Ge-4/0/42
Ge9/0/4
163.20.250.254
Vlan200-500,600-650,668
163.20.250.120
Gigamom
C2960BGP_F1-3
163.20.250.19
Vlan 30
172.17.11.249/24
163.20.250.20
HUB用
Mgmt
Mgmt 1

資安技術檢核-A組

使用者電腦安全檢核

網路惡意活動檢測

物聯網設備檢測

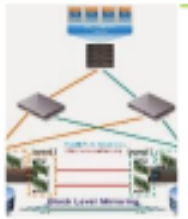
網路架構檢測

技術檢測內容

使用者電腦安全檢核

網路惡意活動檢核

核心資訊系統安全檢核



網路架構檢核

目錄伺服器安全檢核

物聯網設備檢核

組態設定安全檢核

使用者電腦安全檢核

- 使用者帳號、密碼

全單位網段端口掃描(Portscan)，透過端口(Port)掃描結果。

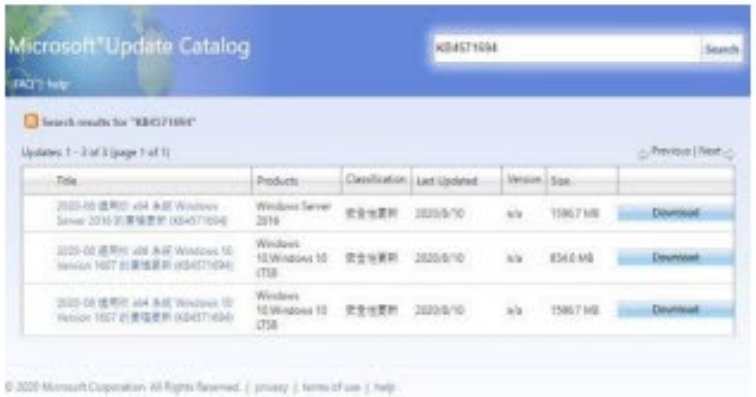
- TCPView
- shodan

- 使用者電腦進行深度檢核。
  - 惡意程式 (process explore)
  - 防毒軟體
  - JAVA軟體更新
  - ADOBEREADER軟體更新(DC)
  - ADOBEFLASHPLAYER軟體更新
  - 安裝安全性(Patch)更新情形

網域主機安全防護檢核

安全性更新

安全性修補程式(重大CVE更新???????)



防毒軟體

防毒軟體(Antivirus)安裝、更新與每日掃描情形

異常程序

利用工具與人工方式針對目錄伺服器檢核是否遭植入惡意程式
植入mimikatz????

NCCST

新北市政府 Education Department, New Taipei City Government 教育局

- 學校是否導入AD
- GPO派送情形
- 透過政府組態基準(GCB)進行掃描(遴選五台電腦)，運用盤點程式，針對瀏覽器、網通設備與應用程式進行檢測，並確認組態設定安全防護情形

NCCST

新北市政府 教育局
Education Department, New Taipei City Government

網路惡意活動檢核

- 依行政院國家資通安全會報技術服務中心最新公告之惡意中繼站C2名單(IP & DN)，針對所有使用者網段檢測惡意中繼站阻擋情形
- 伺服器異常網路活動
- 個人電腦異常網路活動
- 網路設備異常網路活動
- 惡意活動檢測→側錄6小時封包，結果進行分析

物聯網設備檢核

透過網路掃描、滲透測試或臨機操作方式執行

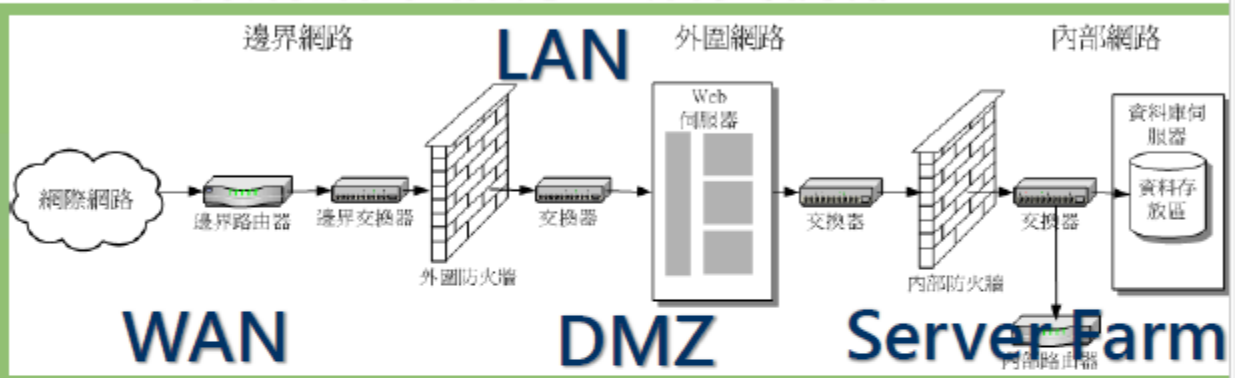
以能從外部聯網之裝置為優先

檢核方式:針對單位智慧聯網裝置進行網段端口掃描(Portscan)與漏洞掃瞄

網路印表機、網路攝影機、門禁設備、工業控制器、無線網路基地台、路由器、環控系統、或其他物聯網設備

網路架構檢核

查看網路架構分區落實情形



訪談為主(透過訪談與實際檢視方式驗證)

網路架構、網路區域間的存取、入侵偵測/防禦系統、系統本機安全機制、實體、服務備援機制

內對外連線、外對內連線、服務區域連線、防火牆規則、資料傳輸、第三方連線控制、遠端連線存取控制、網通設備存取、SNMP設定、校時設定

END