校園網路規劃與安全

李忠憲

大綱

- 資通安全作為
- 教育體系資安責任分級
- 網路設備採購與規格識讀
- 如何改善校園網路
- 有線、無線混搭網路規劃

資通安全作為

1. 用戶端的安全性（PC、行動裝置、物聯網設備之管理）
2. 傳輸安全（DNS、零時攻擊入侵偵測、防火牆建置）
3. 伺服端的安全性（弱點掃描、資料加密、個資保護、授權驗證）
4. 應用端的安全性（制定 HSTS 規則、防範 XSS CSRF 隱碼攻擊、第三方授權）
5. 人員的安全（資安研習、資安通報演練）

網路規模越大資安需求越高！

裝置管理

1. 裝置管理通常可以做到：監看裝置、修改裝置設定、遠端鎖定、遠端重置、清除資料。
2. PC 部分可以採購資產管理系統，MAC 則可以使用 Apple Remote Desktop 管理，或納管到 MDM 中。
3. 安全等級未達 C2 的電腦，例如： windows。應安裝單機防火牆。
4. 行動裝置可使用 Jamf MDM 管理（需採購 License）。
5. 物聯網設備可使用 Spiceworks、iNet Network Scanner 或類似的開源軟體管理。

網路傳輸安全

1. DNS 需安裝 Bind 9.10 以後的版本，且應設置 RPZ。
2. 入侵偵測軟體（IPS）可以提供零時攻擊防禦。應由教育局統一採購或設置。
3. 防火牆應使用正面表列設定規則，規則應該盡量嚴謹。針對遠端登入和遠端桌面，應將發送端與接收端 IP 逐一表列。
4. 遠端登入透過 VPN 會更安全。VPN 應選用支援 IPsec 和 SSL 技術的產品，免費的 VPN 並不安全。

伺服器

1. 建置開源弱點掃描工具，例如：OpenVAS、Google 開發的 OSV-scanner。
2. 伺服器應購買具備硬體加密功能的硬碟（SED），可有效防堵勒索病毒的攻擊。
3. 中華民國資料保護學會的個資盤點工具，可以免費下載。
4. Windows 作業系統修補與強制更新，可以安裝 WSUS 服務。
5. 遠端管理，應挑選加密等級較高的產品，目前大多採用微軟發展的遠端桌面協定（RDP），安全性較高。開放原始碼軟體，例如：VNC（Virtual Network Computing），以及衍生的 TightVNC、UltraVNC，安全性較差。此外，還有TeamViewer、Splashtop、Netop 等商用軟體軟體，以及瀏覽器外掛 Chrome Remote Desktop，其安全性也不足。應先透過 VPN 連線後，再進行遠端連線，以便使用防火牆規則進行嚴格管控。

網頁應用程式的安全

1. 網頁伺服器版本要更新，應取得並安裝合法 HTTPS 金鑰，應支援 HSTS 規則設置。
2. 開發框架應該提供 XSS、CSRF、隱碼攻擊的防禦手段。
3. 如果有介接第三方登入，例如：單一身份驗證、Google、Facebook、Line...等社群帳號，應該妥善保管相關金鑰並列入移交。

資安分級

核心資通系統包含：
DNS
各校官網
存有個資的伺服器（例如：NAS、校務行政系統）
有帳號驗證功能的伺服器（例如：AD）

教育體系資安責任等級分級原則

	A級	B級	C級	D級
業務個資	■教育部 ■承接敏感業務、研究學校	■公立大專校院		
資通系統		■國家教育研究院 ■國家圖書館	■部屬機構(電台、博物館、圖書館) ■國家運動訓練中心 ■公立高級中等以下學校(有核心資通系統)	■公立高級中等以下學校(已向上集中無維運核心資通系統，無機房或僅設置通訊機房)
機關層級	■大學附設醫院(醫學中心)	■大學附設醫院(區域、地區醫院)		

*核心資通系統指依「資通安全管理法施行細則」第7條第2項：
- 支持各校「**核心業務**」持續運作必要之系統。
- 依分級辦法附表九「資通系統防護需求分級原則」，資通系統判定其防護需求等級為高者。

網路設備採購

1. 不要採購中國品牌或產地在中國的設備。

2. 骨幹光纖、L2 交換器、核心交換器、路由器...等設備近年來多由教育局統一採購。

3. 如果要自行採購交換器、無線AP、WiFi 路由器，需要熟悉業界常用的規格術語。

4. 應該依照需求採購，而非功能越多越好。功能越多，安全漏洞也越多。

5. 網路設備經常使用超過五年才會汰換，所以採購時也要考量未來的需求。

網路設備分類

Layer 1（實體層）：集線器、訊號放大器（中繼器）

Layer 2（資料鏈結層）：橋接器、交換器、無線 AP

Layer 3（網路層）：核心交換器、Edge 路由器、WiFi 路由器（分享器）

Layer 4（應用層）：應用層閘道器、防火牆、WLan 控制器

交換器分類

1. 模組化交換器：可以新增擴充模組，包含：應用程式（例如防火牆、無線或網絡分析）、額外介面、電源供應器或散熱風扇的模組。

2. 固定組態交換器：具有固定連接埠數量且無法擴充，又可分為：
    a. 無網管交換器（沒有管理介面、即插即用）
    b. 智慧型交換器（具備簡單的網頁管理介面，通常作為第 2 層交換器）
    c. 網管交換器（具備 console port 可臨機管理，具備完整的網頁管理介面，通常作為核心交換器）

交換器規格識讀

端口：GB 乙太網路、SPF（1G 光纖）、SPF+（10G 以上光纖）

供電：PoE（15W）、PoE+（30W）、PoE++（60W 或 100W）

骨幹頻寬：應為所有連接埠頻寬的 2 倍

必備功能：支援 IPv6、ARP Table 16K以上、RSTP 迴路偵錯、SNMP 或 RMON 遠端管理協定

其它常見功能：QoS、multicast、VPN、頻寬合併、DHCP、策略式路由、NAT、負載平衡、SSL 轉送代理...等

無線AP規格識讀

天線模組：至少要 2 In 2 Out（MIMO 4x4）

頻率： 2.4 + 5GHZ

通訊協定：802.11 g/n/ac/ax

加密驗證：WPA2、WPA3（WEP 和 WPA 已經不安全）

運行模式：Router、Bridge、WDS...等

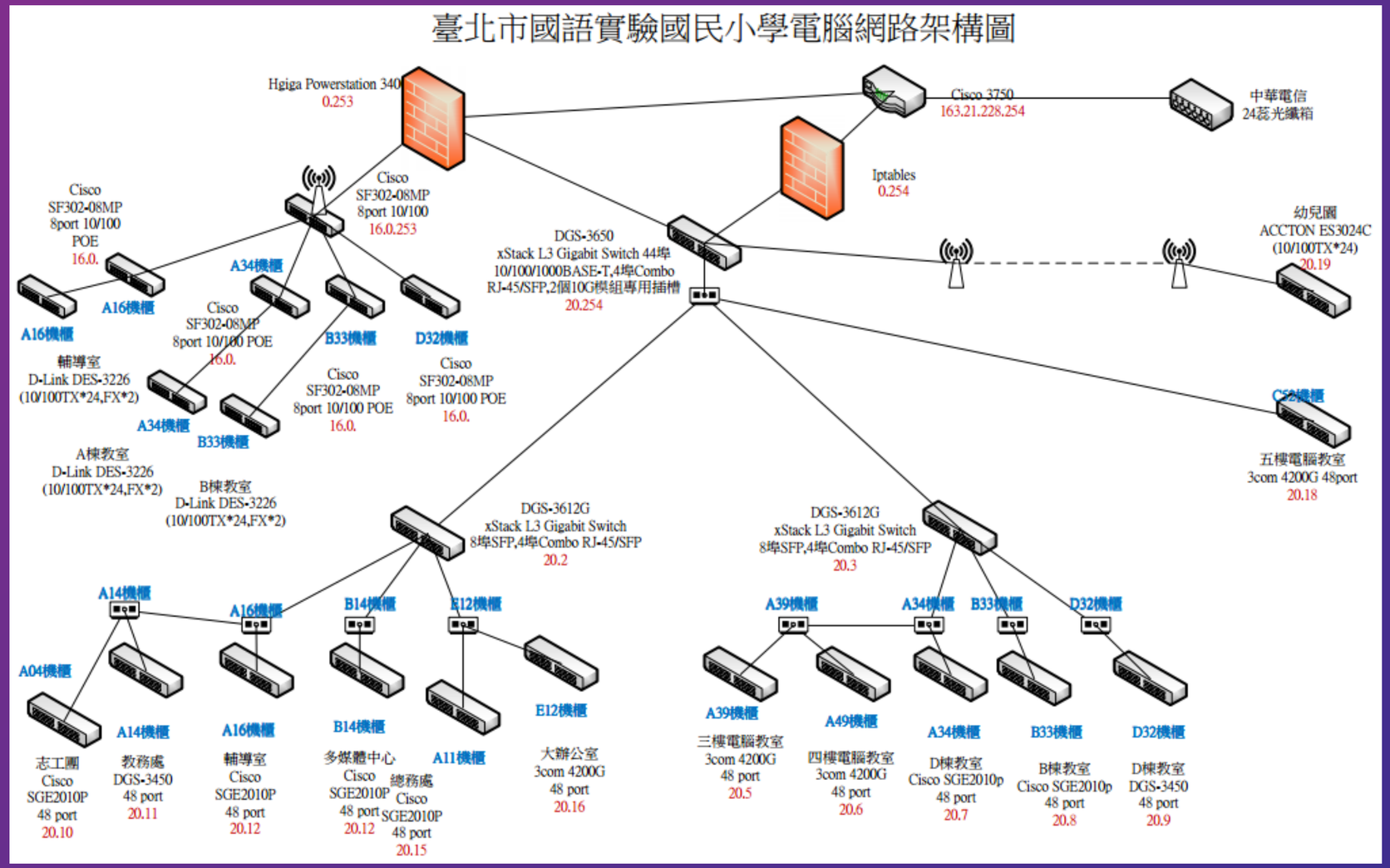
防護等級：室內型、戶外型（需防雨淋及雷擊）

網管功能：Thin AP（需採購無線控制器）、Fat AP（需有網頁管理介面）

校園網路管理工作

1. 訂定網路管理及安全政策。
2. 調查、繪製、調整及規劃校園網路架構。
3. 網路服務規劃及向上集中。
4. 災難處理與資安通報。
5. 辦理網路使用訓練以及資安研習。

繪製網路架構圖


臺北市國語實驗國民小學電腦網路架構圖
Hgiga Powerstation 340
0.253
Cisco 3750
163.21.228.254
中華電信
24芯光纖箱
Iptables
0.254
Cisco
SF302-08MP
8port 10/100
POE
16.0.
Cisco
SF302-08MP
8port 10/100
16.0.253
DGS-3650
xStack L3 Gigabit Switch 44埠
10/100/1000BASE-T,4埠Combo
RJ-45/SFP,2個10G模組專用插槽
20.254
幼兒園
ACCTON ES3024C
(10/100TX*24)
20.19
A16機櫃
A34機櫃
B33機櫃
D32機櫃
輔導室
D-Link DES-3226
(10/100TX*24,FX*2)
Cisco
SF302-08MP
8port 10/100 POE
16.0.
Cisco
SF302-08MP
8port 10/100 POE
16.0.
Cisco
SF302-08MP
8port 10/100 POE
16.0.
A34機櫃
B33機櫃
A棟教室
D-Link DES-3226
(10/100TX*24,FX*2)
B棟教室
D-Link DES-3226
(10/100TX*24,FX*2)
C52機櫃
五樓電腦教室
3com 4200G 48port
20.18
DGS-3612G
xStack L3 Gigabit Switch
8埠SFP,4埠Combo RJ-45/SFP
20.2
DGS-3612G
xStack L3 Gigabit Switch
8埠SFP,4埠Combo RJ-45/SFP
20.3
A14機櫃
A16機櫃
B14機櫃
E12機櫃
A39機櫃
A34機櫃
B33機櫃
D32機櫃
A04機櫃
A14機櫃
A16機櫃
B14機櫃
E12機櫃
A39機櫃
A49機櫃
A34機櫃
B33機櫃
D32機櫃
志工團
Cisco
SGE2010P
48 port
20.10
教務處
DGS-3450
48 port
20.11
輔導室
Cisco
SGE2010P
48 port
20.12
多媒體中心
Cisco
SGE2010P
48 port
20.12
總務處
Cisco
SGE2010P
48 port
20.15
A11機櫃
大辦公室
3com 4200G
48 port
20.16
三樓電腦教室
3com 4200G
48 port
20.5
四樓電腦教室
3com 4200G
48 port
20.6
D棟教室
Cisco SGE2010p
48 port
20.7
B棟教室
Cisco SGE2010p
48 port
20.8
D棟教室
DGS-3450
48 port
20.9

如何改善校園網路

1. 班級教室網路端點應擴增至 4 個以上，包含：PC、大屏、網路電話、無線 AP...等。
2. 找出頻寬瓶頸，已經接滿的交換器，應增加一台交換器進行分流，新交換器不應 uplink 到舊交換器。
3. 光纖分線箱中的冗餘線路可以撥給新交換器使用。
4. 將第三層設備直接接上光纖連至核心交換器，以減少網路層級。
5. 汰換老舊設備與線路，將集線器汰換成交換器，將 CAT5 汰換成 CAT6 或 CAT7，避免將 100MB 和 1000MB 線路混接於同一個交換器。
6. 線路標示（建議為「來源機櫃-目的機櫃-埠號」，例如：E54-A16-01）。
7. 逐步將所有 AP 汰換為 PoE 機種，如有餘裕可考慮部署 Thin AP（搭配軟體式 controller）。
8. 地下室、禮堂...等訊號不良的場所，可考慮使用外接延長天線。另有支援 4G LTE 的外接天線可選購。

有線、無線混搭網路規劃

為因應行動學習需要，教室內需有能取用有線網路資源（例如： airplay、nas）的無線 AP。如果沒有足夠經費擴充教室內端點，可採購具有路由功能的無線 AP，至少需提供 3 個 UTP 埠，可串接教室內的 PC 和 大屏，讓教室內所有設備位於同一個網段中。

原有佈建於走廊的無線網路 AP，仍然維持獨立運作（與內網實體區隔），以提供給 TPEfree 和 TANetRomaing 使用。

Q & A