



網路現狀與經驗分享

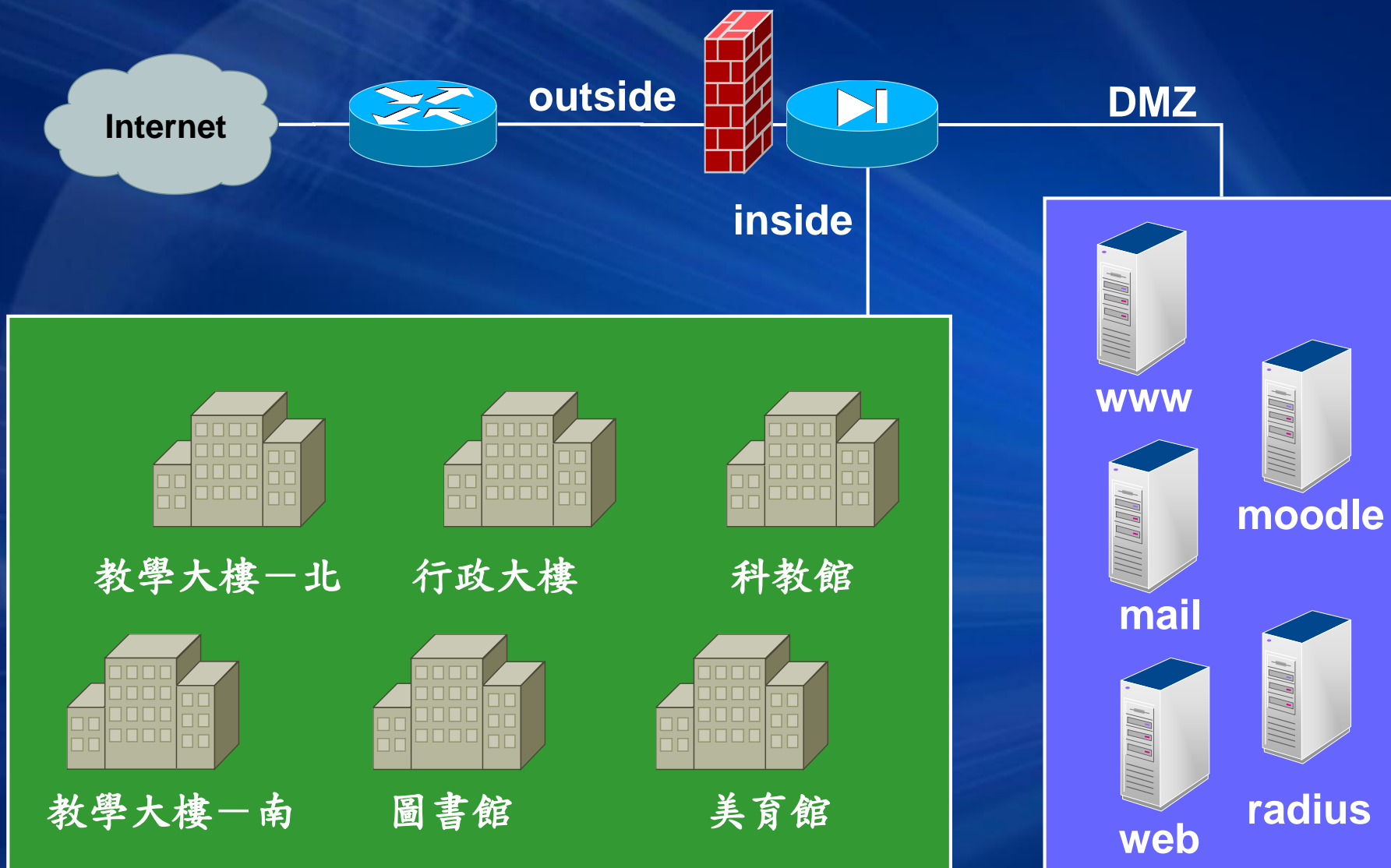
內壢高中

網路基本架構

- 使用硬體防火牆將校內網路區隔為兩界面
 - DMZ：必須提供校外服務之伺服器，位於此界面。
 - Inside：校內一般使用者及僅供校園內部使用之伺服器，位於此界面。

防火牆建置後遭遇的問題

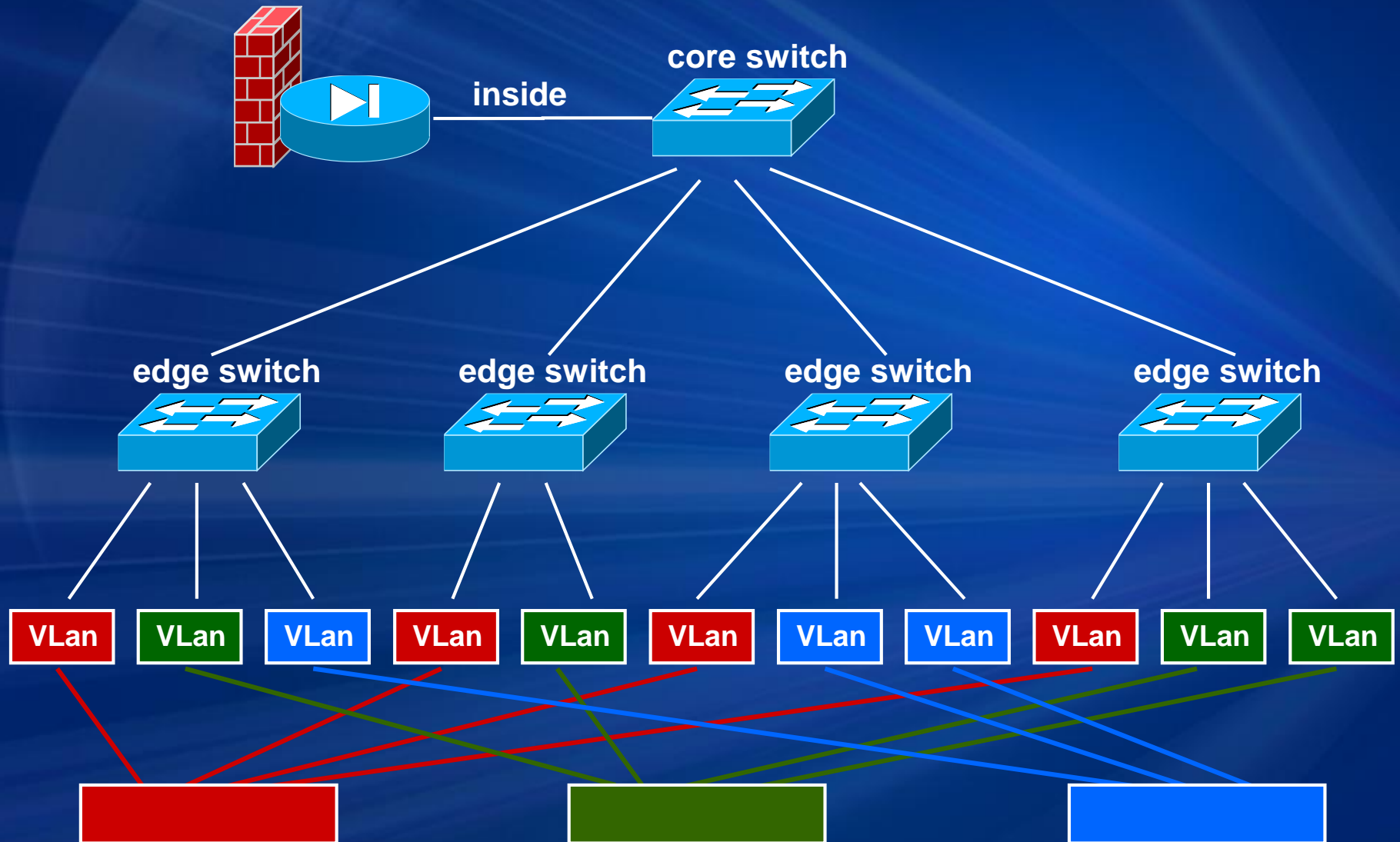
- 各單位自行採購之各系統高度依賴廠商之遠端維護。
 - 多數廠商遠端維護方式為 PC-Anywhere
 - 承辦人員要求改變防火牆規則，允許廠商可由校外直接連線進入內部網路。
 - 要求上述規則 7-24 開啟。
- 解決方式：
 - 要求廠商給定遠端 IP。
 - 限定開放時間。
 - 要求承辦人要全程監控其維護過程。



Inside

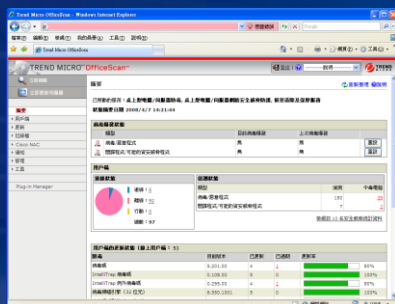
- 原來的 Inside 界面網路未劃分 Vlan，因此面臨以下問題：
 - 使用MS網路上的芳鄰等服務時，其廣播封包造成傳輸效能低落。
 - 行政及教師用電腦，因作業系統預設未關閉自動搜尋網路資料夾和印表機，導致使用者列印至非預期之印表機上。
 - 各辦公室之間位於同一區域網路中，部分具敏感性資料之單位有安全上之顧慮。
- 在更換舊有設備(Hub) 時，考量需支援 802.1q，以利彈性劃分 Vlan。

Inside (with 802.1q)



病毒防治

- 防毒軟體以 Trend OfficeScan 為主，校內使用者可自行安裝其 Client 端軟體。



Officescan
server



校內常發生的病毒相關問題

□ 目前以 USB 型病毒數量最多

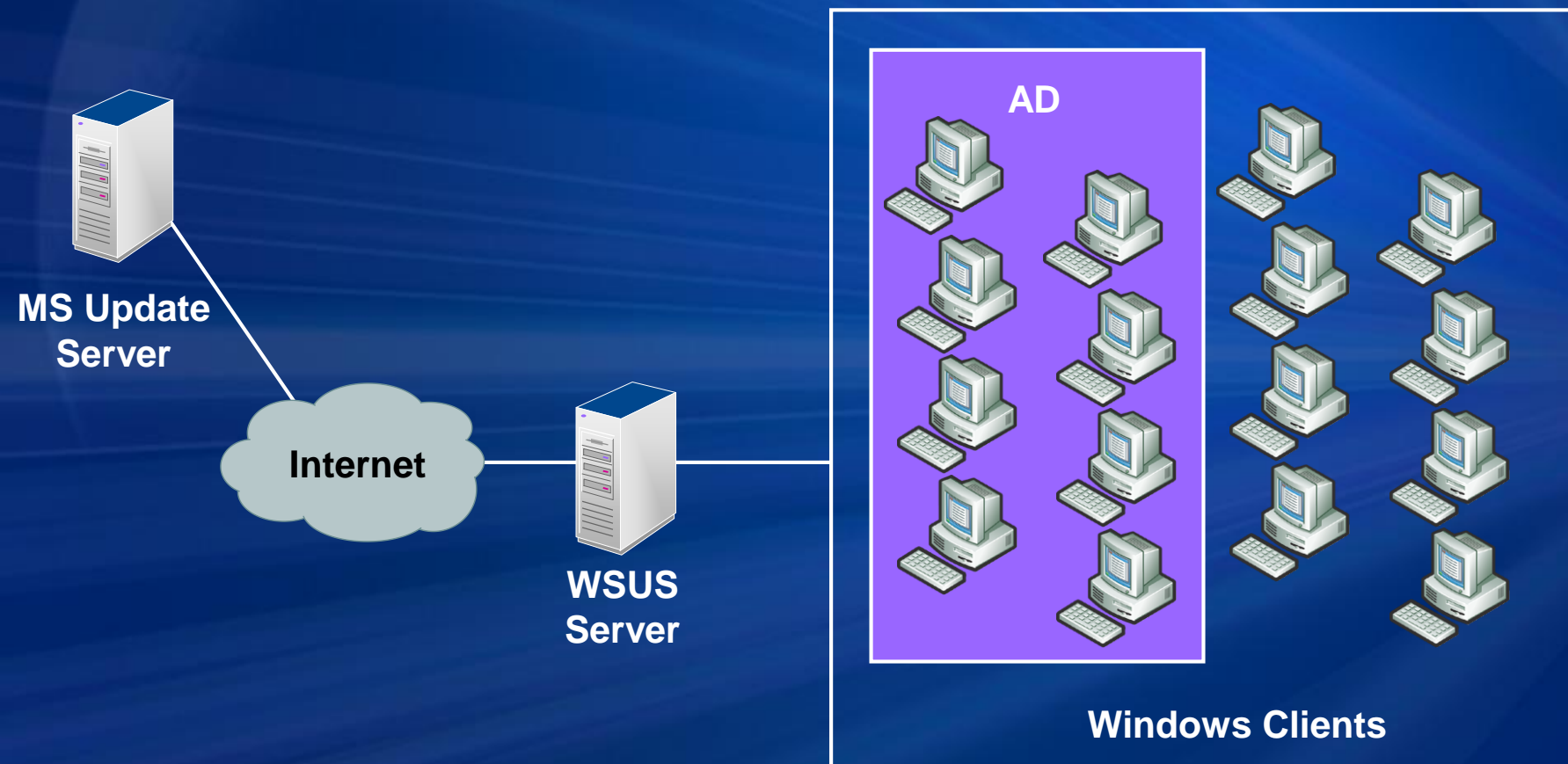
- 許多教師習慣要學生用 USB Disk 儲存作業，並帶來學校繳交。
- 教師使用學校的電腦收學生作業，並轉存於自己的 USB Disk。
- 連設備組的數位相機儲存卡都曾發現病毒。

□ 解決方式：

- Officescan 目前只要看到 autorun.inf 就一律刪除。
- 停用 autorun (含限制 mountpoint2 機碼)

Windows Update

- Windows 更新部分，架設一 WSUS 伺服器，校內各電腦可設定其為更新主機。



佈署方式

□ Active Directory 網域

- 使用群組原則設定。

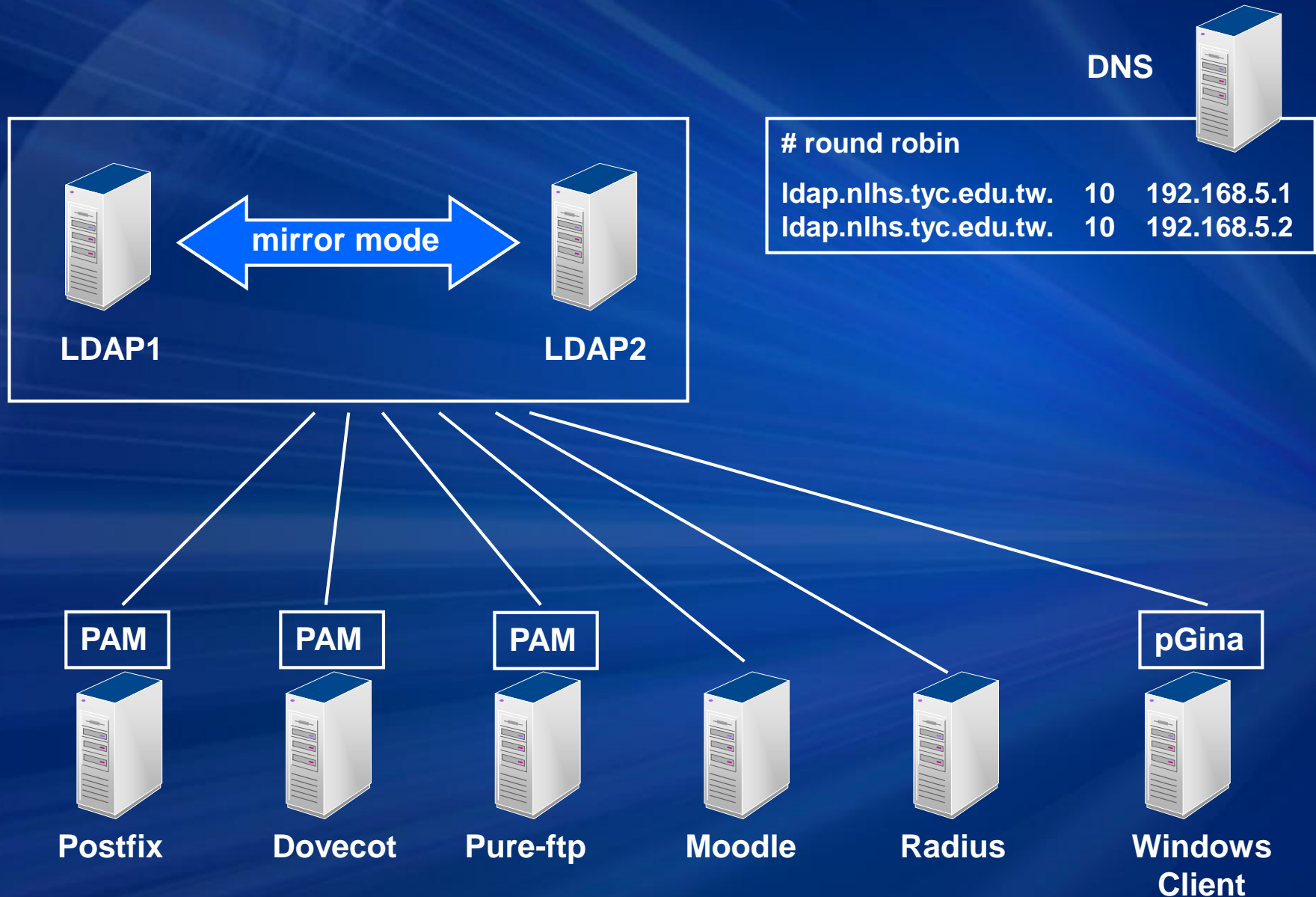
□ 非Active Directory 網域

- 使用 gpedit.msc 設定本機電腦原則。
- 將相關設定寫成一個 reg 檔，交由使用者 double click 匯入。

網路服務帳號密碼整合

- 近年隨著伺服器與網路服務之數量逐漸增加，帳號密碼管理上開始出現困擾。
 - 新進及離校教職員工必須於每一伺服器上新增或刪除帳號。
 - 雖然使用者可以自行更改各伺服器或服務上之密碼，但易發生使用者修改後，各服務上之密碼不同而常忘記的狀況。
- 目前逐漸以 LDAP 統一處理使用者身份驗證問題，使用者僅需使用單一帳號密碼。

網路服務帳號密碼整合



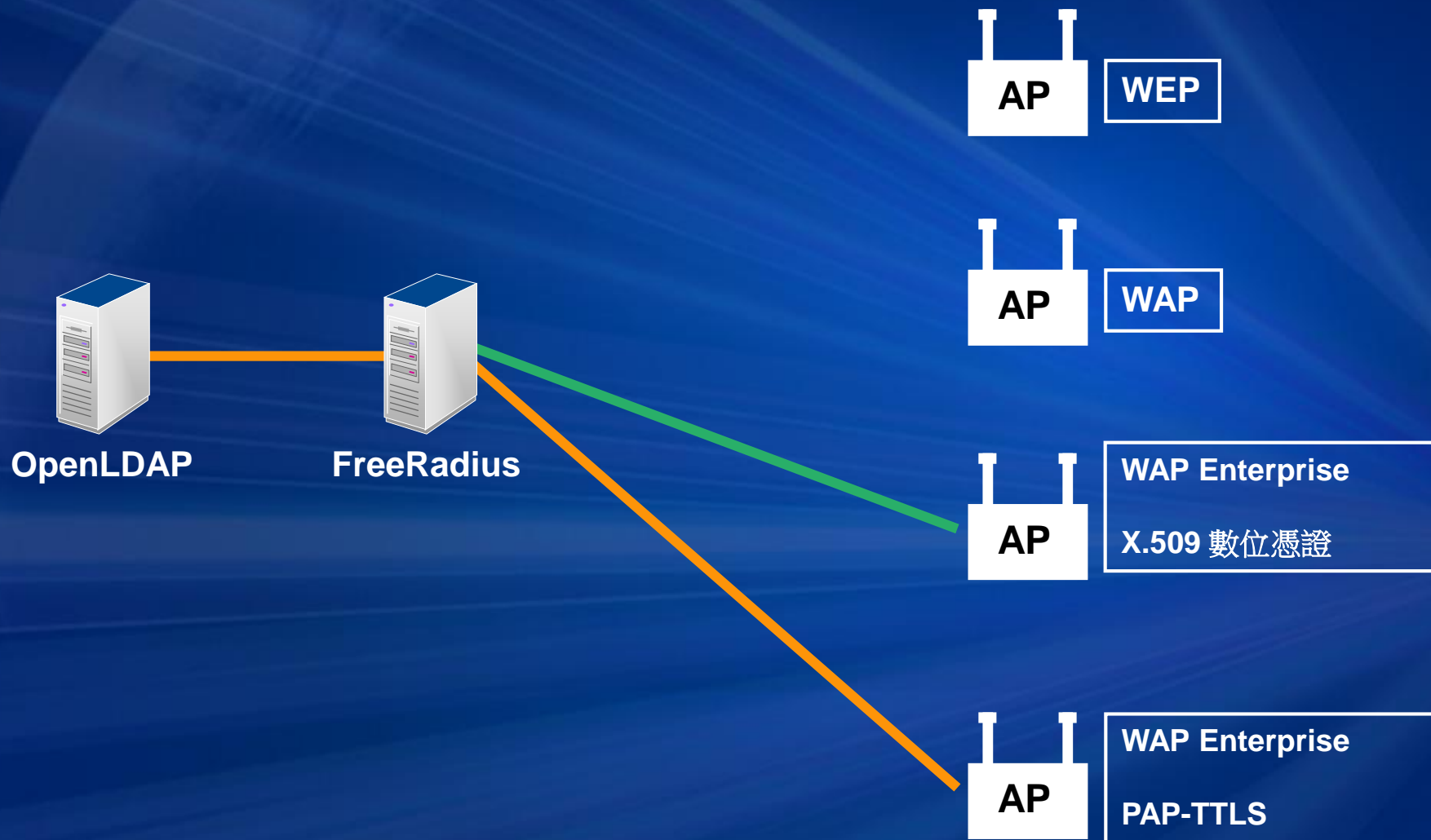
LDAP 驗證遭遇的問題

- 使用 OpenLDAP server 要記得自己設 BDB 的 index，預設 config 檔的 index 一定不適用，效能會差很多。
- 電腦教師需有幫學生修改密碼的權限，因此利用 OpenLDAP 的 ACL 給予相應權限。
- 開發相關應用程式
 - JAVA – 使用 JNDI (Java Naming and Directory Interface)
 - .Net – 使用 Novell LDAP LIBRARIES for C#
 - Web – 使用 php

無線網路身份認證

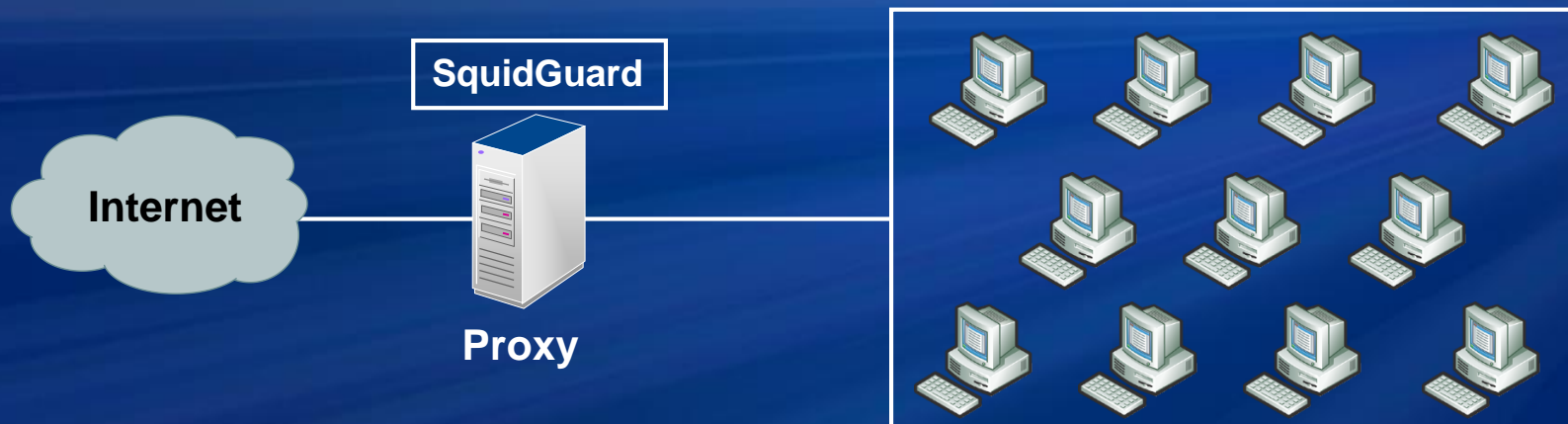
- 前幾年學校總務處及設備組在未知會校內網管單位的情形下，自行採購並安裝無線網路存取點，造成安全上極大之漏洞。
- 由於當時採購之設備對安全性協定的支援不盡相同，亦造成後續管理上的問題。

無線網路身份認證



不當資訊管理

- 目前不當資訊管理部分，使用SquidGuard過濾不當網址，黑名單來源為
 - SquidGuard
 - 教育部電算中心
 - 自行增列。



垃圾郵件過濾

- 使用 spamassassin 對電子郵件進行過濾
- 認定為垃圾郵件者，於主旨上加註一標記，由使用者於收件軟體上自行設定郵件處理規則。
- 因應部分上級單位自動發信系統有被誤判為垃圾信之狀況，另加入白名單。

線上教學平台

- 目前學校的線上教學平台使用 moodle。
- 主要以電腦科和英文科使用較多。



電腦教室 AD

- 兩間電腦教室目前以 Windows XP 為主要作業系統，其中一間安裝 XP/Ubuntu 雙系統，試著開發 Linux 與自由軟體的課程。
- 因課程上學生不需管理員權限，所以不使用還原卡，而以 Active Directory 的群組原則進行管理。

