校園無線網路架構探討

PART 1.老松國小現行無線網路架構

PART 2.現行架構所遭遇的問題

PART 3.修改現行架構的規劃

報告人：老松國小張嘉恩

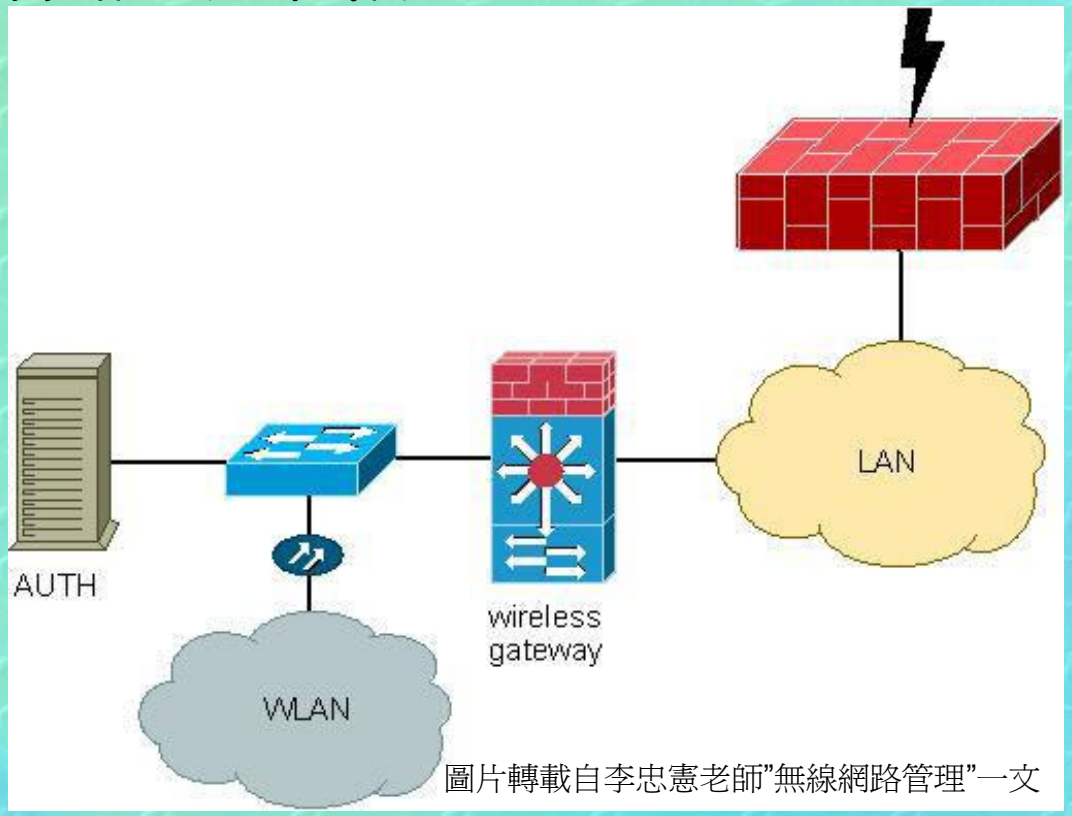
現況

- 老松國小的無線網路架設完成至今兩年多，目前的使用狀況是，本校教職同仁大部分仍習慣使用有線網路，無線網路是不得已（如沒有網路接孔的地方 ）才使用的工具。
- 本校無線網路截至目前為止，幸運地尚未遭遇重大問題，但這並不保證未來就能一直平安無事；本人無線網路方面知識淺薄，希望可藉由這次的報告，向大家請教，並討論改進的規劃。

PART 1.老松國小現行無線網路架構

- 加密:**無（WEP/WPA皆無開啓）**
- 認證採用Captive Portal機制
  m0n0Wall (DNS查詢重導向)
- 使用市網信箱帳號即可連上本校無線網路

現行無線網路架構圖



圖片轉載自李忠憲老師"無線網路管理"一文

Step1. m0n0Wall預設將認證要求導向Radius認證伺服器，再由Radius導向到市網的認證伺服器。

Step2. 認證通過後，無線網路透過m0n0Wall直接與校內有線網路連接，用同一部防火牆連線到校外。

- **IP分配**
  m0n0Wall閘道器作爲DHCP分配給用戶端**192.168.1.0/24**網段IP。
- **IP轉址**
  m0n0Wall規則設定NAT轉譯用戶端IP爲**172.16.10.0/16**與校內有線網路連接。
- **資源存取**
  可存取有線網路的資源(校務行政、網路芳鄰和網路印表機)

PART 2.現行架構所遭遇的問題

- 由於認證採用市網帳號，非本校人員只要擁有（或馬上申請）市網帳號即可透過本校無線網路上網。
- 若發生上述情形，因本校防火牆內對外採用正面表列規則，應該是無法使用點對點下載，但仍有被駭客當作攻擊跳板的疑慮。

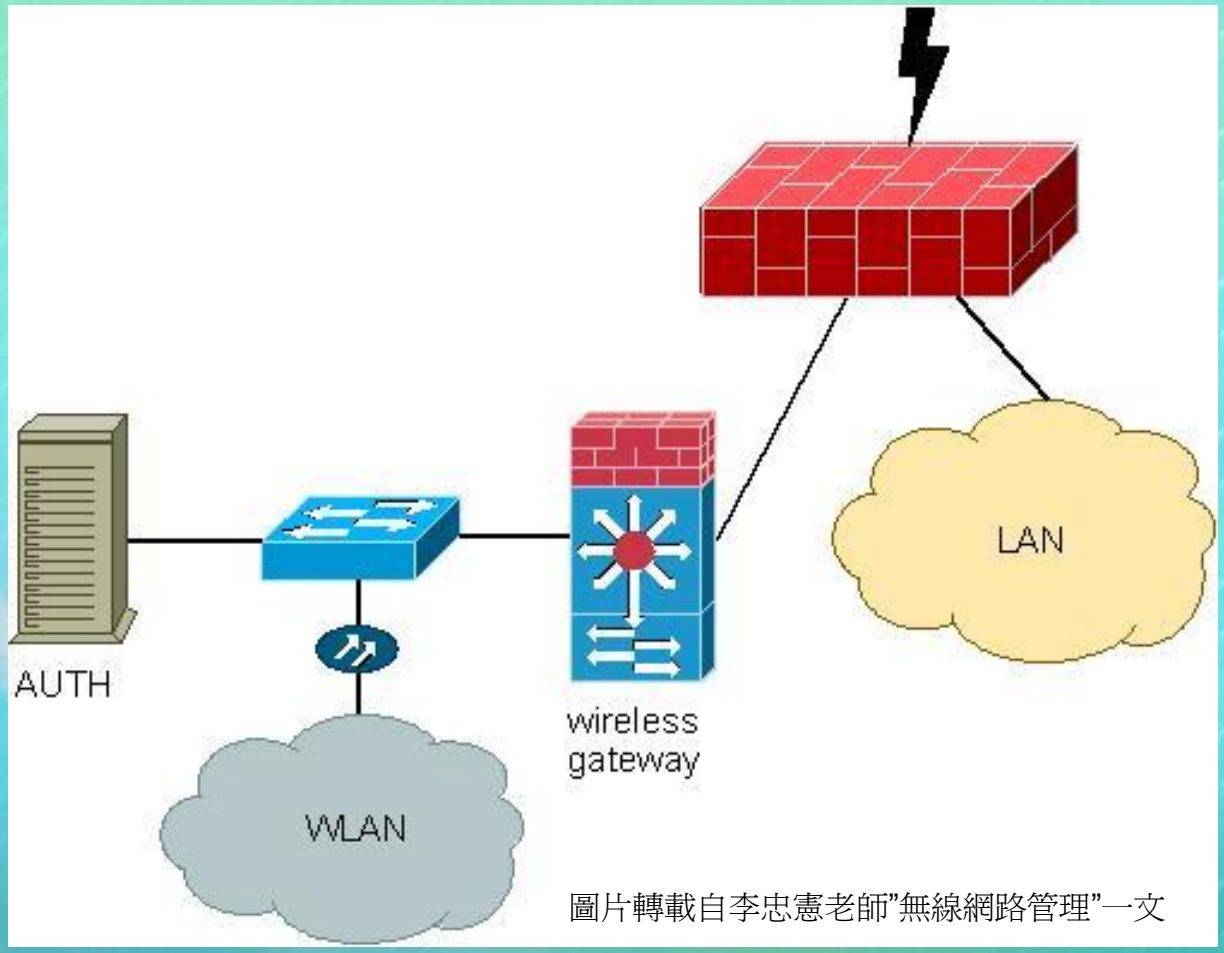
- 無線網路資料傳輸沒有加密，對於竊聽的防禦力是零，加上無線網路與有線網路直接連線，損害風險相對提高。

- 由於AP數量龐大，且架設地點多爲高處，管理上極爲不方便。

PART 3.修改現行架構的規劃

- 帳號認證部份不再採用市網信箱，由校內Radius伺服器自行認證。
- 啓用WPA加密功能。
- 校內有線網路接點足夠的情況下，無線網路將不與有線網路做連接，僅提供一般上網使用。

無線網路修改後架構圖



圖片轉載自李忠憲老師"無線網路管理"一文