

NetIRS 身份認證與存取控管案例解說

如何過濾員工或是訪客? (網管員不可不知的事)

使用者身份認證一方式不能只有一種

市面上有許多廠商皆有提供內網使用者身份驗證的方案，可是決大多數都只提供一種方法，有的網路管理員往往爲了配合該廠商的方法，甚至花大錢改變全區的網路環境，形成所謂的「買爐子，卻要拆房子」的奇怪現象。以下藉由 NetAxle 公司提供 NetIRS 身份認證管理實際案例來解說，希望能夠幫助網路管理者來正確判斷與檢視如何規劃才能符合自身需求。

案例一：完全不開放內部網路給外來者使用

某電視台員工人數 500 人，節點數約 800 個，不歡迎也不開放網路給非員工以外的人使用。

解決方案：IP-MAC 鎖定 嚴格管控

在企業要求網路環境相對嚴謹時，IP-MAC 鎖定是較爲安全且容易管理的管控機制，NetIRS 可以與多種品牌 SWITCH 互相搭配，透過搜尋 ARP Table 自動建立配對表來達到 IP-MAC 鎖定功能：一個 MAC 地址固定分配一個 IP 地址；只要不存在配對表上面的 IP 與 MAC 都無法使用網路，就算只有 IP 或 MAC 其中一種符合都無法通行。

優點：員工可以不需每次上網都要輸入使用者 ID 與密碼，就連無法輸入 ID 及密碼的設備如 PDA、IP Phone 等都能進入安全管控表列！



案例二：不固定 IP，開放員工行動辦公，跨 VLAN 存取網路

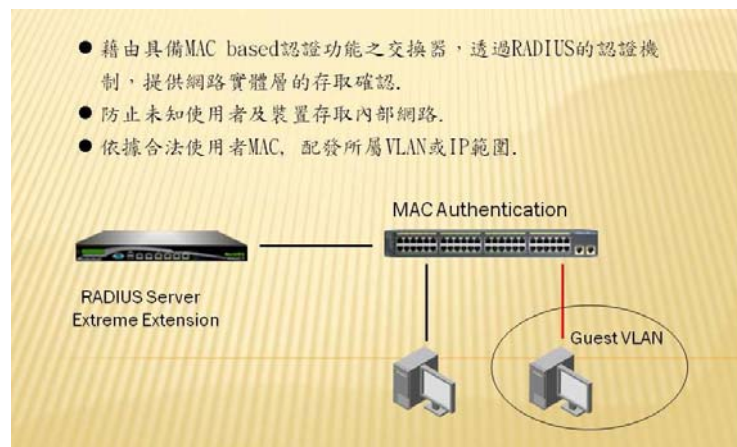
某電信公司因員工人數眾多，無法每人配給一個固定 IP；同時其網路環境在

各樓層裡又劃分不同的 VLAN，當員工帶著行動裝置從 3 樓要到 8 樓在跨 VLAN 存取網路時，IP-MAC 鎖定的方式是完全不適用。

解決方案：MAC 認證+DHCP 配給 IP

NetIRS 提供了完整的 DHCP 應用服務：當員工發出上網請求時，NetIRS 會先透過 DHCP Snooping 檢測其 MAC 地址是否合法，若合法，則 DHCP Server 便配發其專屬或臨時的 IP 供其上網。若該網路 Switch 有劃分 VLAN 時，NetIRS 亦可以與具備 MAC Based 的 Switch 搭配，提供網路實體層的存取認證，依據合法使用者的 MAC 配發所屬 VLAN 與 IP 地址，如此便可以防止未知的裝置存取內部網路。

優點：提供目前流行的行動裝置（如 iPad、iPhone、Notebook…）跨 VLAN 上網的彈性，亦兼具防止顧客假冒員工的可能。



案例三：對訪客僅開放上 Internet，員工則無限制

某大型醫院各樓層的病房管理櫃檯爲了查房與照顧住院病患，其各科主機都是用 Notebook 並使用無線上網，所以病房裡必須要開放上網以連線醫院的伺服器，然而病患與家屬每日往來變動相當大，因而使得病房成爲內網管理的一大漏洞。

解決方案：針對院內 200 台重要主機採取 IP-MAC 鎖定，其他僅開放上 Internet。

面對複合式的網路環境，NetIRS 可以採取多重認證的整合方式。根據此醫院的狀況，NetIRS 只針對院內包含伺服器 etc 200 台重要主機配給固定 IP 以採取 IP-MAC 嚴格鎖定，若有其他設備盜用此 200 台主機的 IP 時，則自動將其斷線；而針對病患與訪客攜帶行動設備要上網時，NetIRS 便啓動 DHCP 應用配給臨時的 IP 供其使用，如此便巧妙的將內部秘密網路與訪客網路做隱形的區隔，可保障醫護人員與病患家屬各別的權益！

優點：舉凡政府機構、醫院、飯店等室內公眾場所，員工與民眾混合的網路環境下，都可以暢遊在無障礙無線上網的網際空間，而無後顧之憂。

案例四：內網範圍廣大遍及縣市的身分認證管理

某縣市網路中心必須要開放給【不一定是從哪個 IP 位址】與【不固定使用哪個 MAC 設備】的行政管理者或老師可以跨各鄉鎮學校的有線或無線上網服務。

解決方案：對不受地理限制，不固定 MAC 設備的上網用戶，使用 Web 認證。

既不受 IP 或 MAC 限制，只要在 Web 使用 Browser 輸入帳號密碼，即可獲得上網權利。但是，弊端來了：在申請者要求輸入帳號密碼的同時，等於已經得到 IP 上了該內部網路了！所以 NetIRS 系統會對所有的申請者先在隔離區配發暫時的 IP 供其使用，若認證成功則另外配給真正的合法 IP 給申請者，不成功者就繼續待在隔離區囉！NetIRS 同時還支援 Windows Domain Single Sign On (SSO)，可與 Windows AD 達成一次性簽入。

1. 未授權使用者先取得隔離區 IP - 192.168.21.x

192.168.11.0 相對應之隔離區網段
192.168.21.0

2. 打開 Browser 會重導至認證網頁

3. 認證成功, 重新取得合法 IP - 192.168.11.x

- 1. 此方案在 Router 上必需使用 multi-netting 功能
- 2. 隔離區網段可使用 ACL 做控管
- 3. 隔離區網段必需可與 NetIRS 連線 (DHCP, DNS, HTTP, HTTPS)
- 4. 可配合 Switch DHCP Snooping 功能以增加安全性
- 5. 使用者已登錄 windows 系統

NetIRS之網頁認證式存取控管

優點：仿效美國機場入境般，舉凡申請入境者，都須到觀察房過濾一番，才准放行，滴水不漏，卻無人權爭議！

案例五：每次上網都要申請輸入 ID 密碼，連校長也要生氣啦！

某大學因為要開放校園網路，又顧慮到內網使用者如教授或研究生與其個人行動設備都不是長期固定在校園內，機動性又強，所以採用 Web 認證；但教授或研究生可能一天出入內網很多次，每次 Web 認證都要做一次 ID 與密碼審核，非常麻煩。

解決方案：使用 Web 認證，通過後並自動轉成 MAC 認證。

這就是 NetIRS 在複合式的網路環境的身分控管最大的優勢。由於教授或學生至多每學期才會有一次變動，所以管理者可以設定要求在開學一開始時，讓教授或研究生先以 Web 認證確定身份，在此同時 NetIRS 便紀錄該師生 Notebook 的 MAC 地址，日後這一學期內，只要該師生持相同的 Notebook 上內部網路，直接採用 MAC 認證，就不須再經過 Web 認證了。

優點：Web 認證與 MAC 認證可以同時存在而且相輔相成，原來做校園認證管理

是不需要委曲求全的！

案例六：不只回收 IP，連 Switch Port 也可以回收！

某大學實際節點數約 1 萬，但其 switch 卻超過 800 台，節點數超過 1 萬 6 仟個。根據查訪結果發現，原來其網路佈出去到各系所與教師辦公室等線路錯綜複雜，無法得知各設備與線路的使用狀況，所以當有新教授一來只好再買新 Switch 再接線至其辦公室，如此循環導致校內 Switch 越來越多，線路也越佈越複雜，使得耗費在維護閒置的 Switch 與線路等的費用與心力逐年飆高。

解決方案：回收閒置不用的 IP 與 Switch Port。

NetIRS 因採用 SNMP 網管機制，其管理的範疇可以擴散深入至每台 SNMP 設備的每個連接埠；由於

NetIRS 會紀錄每個固定 IP 的使用時間，所以當其閒置不用時，NetIRS 便會突顯出來提醒管理者以便刪除回收；同樣的，NetIRS 也監視每個 Switch Port 的使用時間與狀況，若閒置太久，管理者只需

透過 NetIRS 系統顯示畫面按【刪除】即可關閉該 Port，大大減輕管理負擔，同時更防止被偷接的弊端！

交換機 x250(192.168.11.25) Status					
序號	編碼	模式	運行中	最後使用時間	別名
1001	X250e-24p Port 1(VIP)	up(1)	down(2)	(VIP) Exceed 30 days	Internet-1
1002	X250e-24p Port 2	up(1)	down(2)	Exceed 30 days	JetFish2-E
1003	X250e-24p Port 3(VIP)	up(1)	down(2)	(VIP) 2010-09-30	Internet-2
1004	X250e-24p Port 4	up(1)	down(2)	Exceed 30 days	
1005	X250e-24p Port 5	up(1)	up(1)	運行中	
1006	X250e-24p Port 6	up(1)	up(1)	運行中	
1007	X250e-24p Port 7	up(1)	up(1)	運行中	
1008	X250e-24p Port 8	up(1)	up(1)	運行中	
1009	X250e-24p Port 9	up(1)	up(1)	運行中	
1010	X250e-24p Port 10	up(1)	up(1)	運行中	RD-Switch
1011	X250e-24p Port 11	up(1)	down(2)	Exceed 30 days	

NetIRS 系統中Switch Port回收機制畫面

優點：只要坐在資訊中心跟機房設備一起吹涼涼的冷氣，遇到【問題通報】時就【按個鍵】即可把它解決，這種特權真是比當皇帝還要快活！