



CureLan公司產品
IP Management System
(*IPMS*)
IP管理設備



CURELAN TECHNOLOGY

治科資訊(股)有限公司

www.CureLan.com

企業內部IP安全認證機制常見問題

- 內部IP遭合法使用者或非法使用者冒用，責任不易釐清，影響合法用戶權益、造成網管人員與企業管理負擔。
- IP認證管理機制繁複，造成使用者經常性的重複認證操作，形成使用者麻煩、管理者不勝其擾的困擾。
- IP安全認證機制與網路管理者的審查機制整合度不佳。
- 雖使用IP Spoofing技術，卻無法有效遏阻被Netcut(剪刀手)及ARP Spoof病毒攻擊(ARP Poison)竄改動態ARP Table的問題。
- 無法有效防杜L3 Switch更新動態ARP Table時的空窗時間、易使駭客趁虛而入。
- 無法有效設置DHCP管理時間，IP用戶的增刪常需重置DHCP server，影響網路作業效率。
- 實務上的IP核發管理機制與安全認證管理整合不易。(無法支援兩段式認證管理)，且無動態式的使用者自訂管理功能。

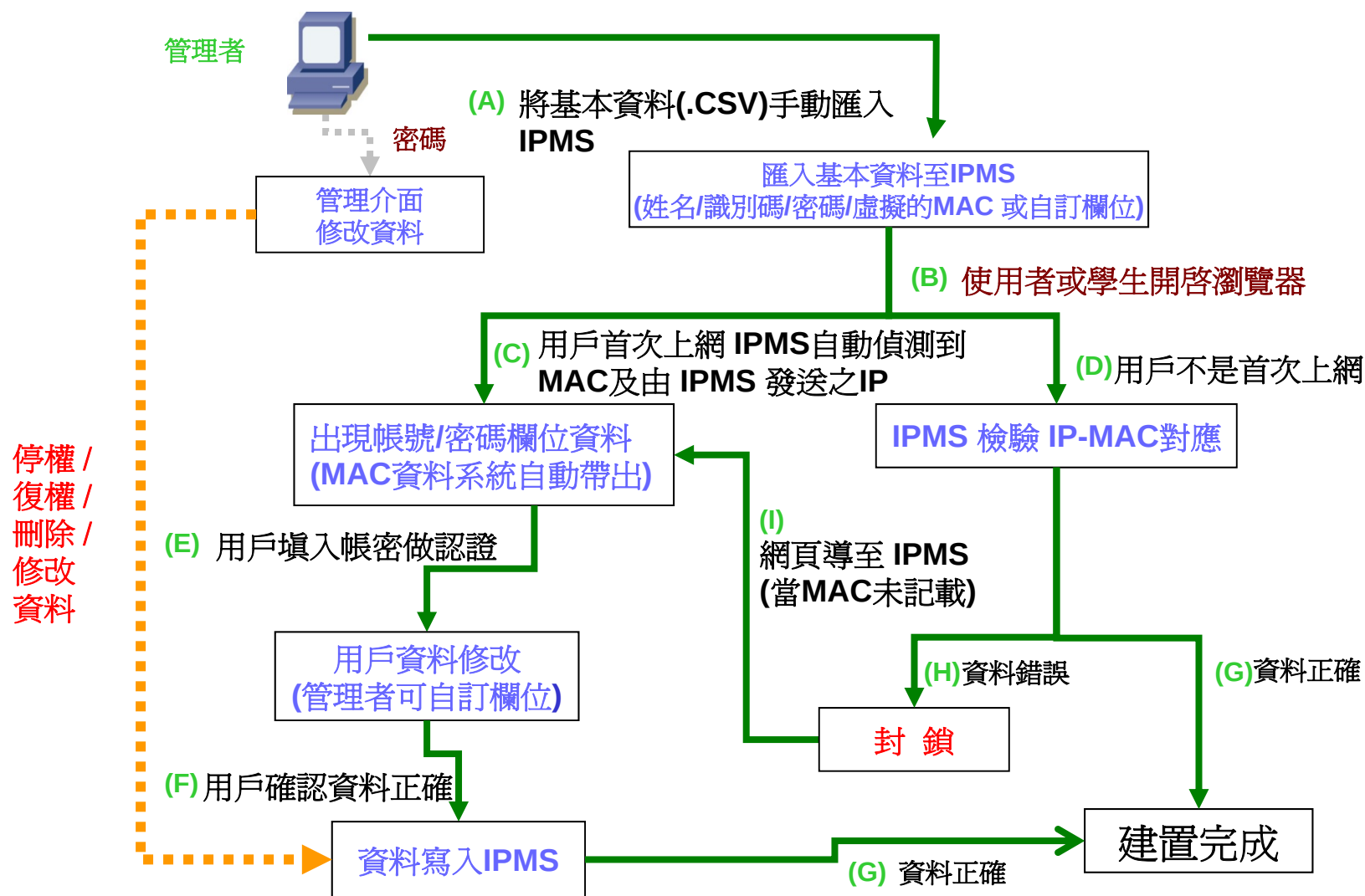
如何防範IP被別人竄改

- 使用者姓名 + IP + MAC相互綁定是最佳方式
 - ◆ 其缺點是逐筆資料鍵入會造成網管人員困擾。(IPMS提供匯入及匯出功能)
- 使用IP Spoofing技術，自動學習L3 Switch的動態ARP Table，並加以綁定IP+MAC。
 - ◆ 其缺點是每一台L3 Switch都會有5分鐘更新動態ARP Table，這5分鐘卻是IP+MAC綁定的空窗期，易被Netcut(剪刀手)及ARP Spoof病毒攻擊 (ARP Poison)竄改動態ARP Table，造成IP+MAC無效。
- 使用IPMS設備才是真正最佳解決方案
 - ◆ 以二段式認證授權方式自動取得MAC，整合使用者姓名 + IP + MAC三者的網路認證機制。
 - ◆ 與DHCP Server整合，強化企業IP核發管理機制，滿足網路安全認證需求。

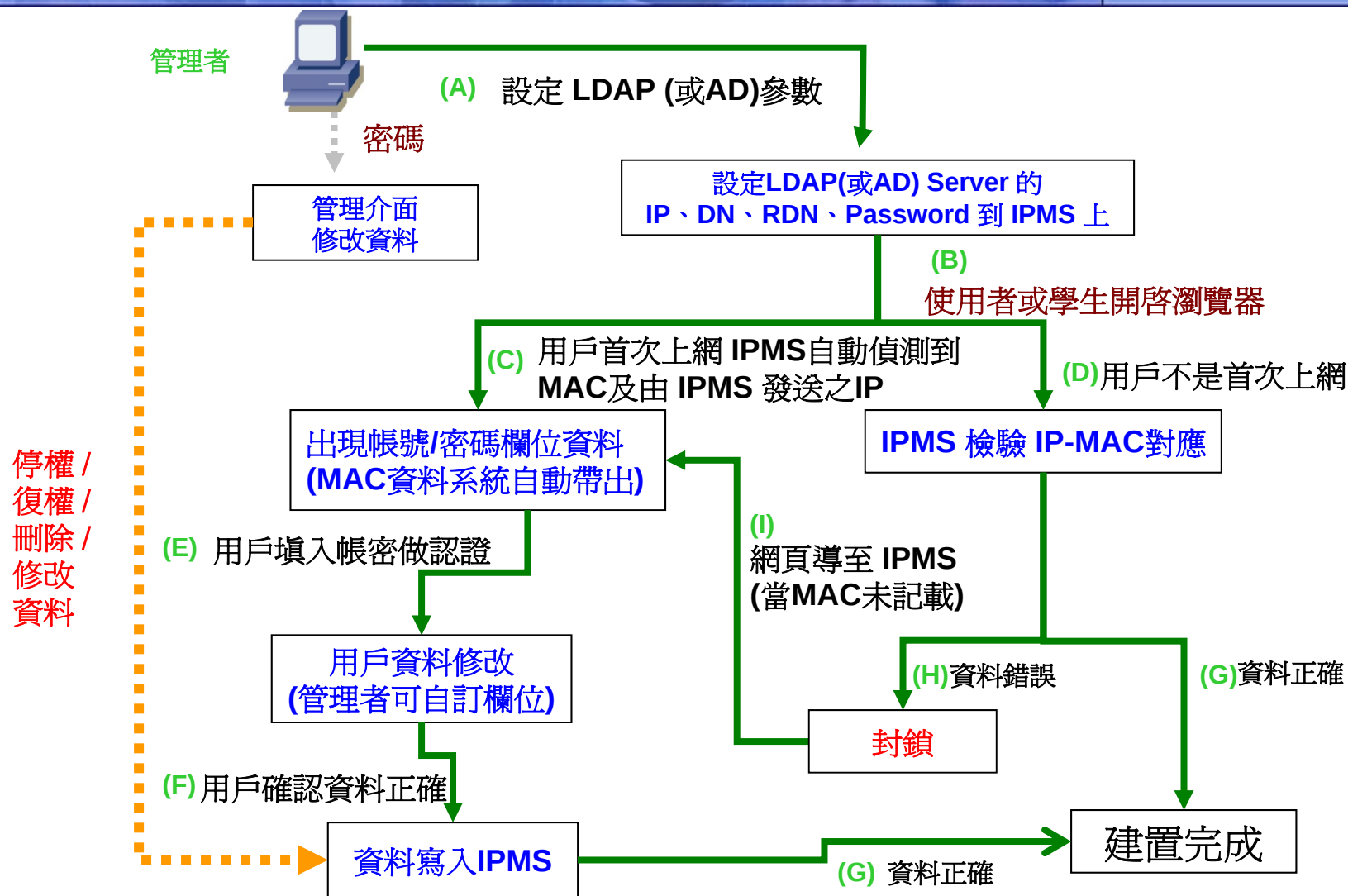
內部網路資訊安全最佳解決方案

- 運用L3 Switch (或L3 CoreSwitch)上之Arp Inspection及DHCP Snooping和DHCP Relay功能，來達成IP+MAC綁定的功能。
- 再加上IPMS設備之二段式認證授權方式，來達成 使用者姓名 + IP + MAC相互綁定功能。
- L3 Switch具備Arp Inspection及DHCP Snooping功能，廠牌有CISCO、FOUNDRY、Extreme(xos)、Alcatel。
- L3 Switch(或L3 CoreSwitch)網路設備，不支援Arp Inspection及DHCP Snooping和DHCP Relay功能，就無法來達成”使用者姓名 + IP + MAC相互綁定功能”。
- 就是L3 Switch (或L3 CoreSwitch)上，一定要有Arp Inspection及DHCP Snooping和DHCP Relay功能，而且此三種功能一定要能同時一起啟動缺一不可，才能搭配IPMS設備使用。

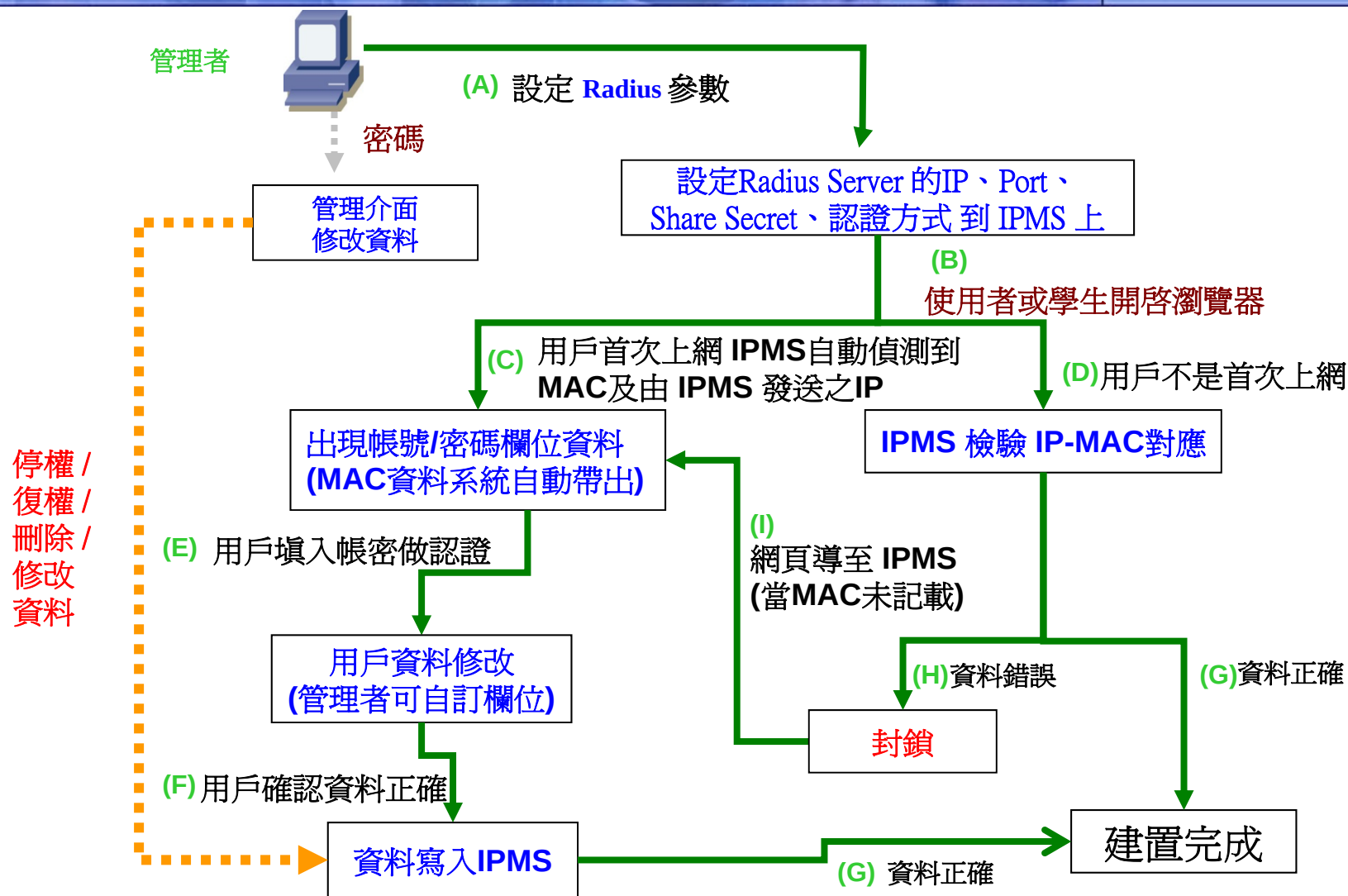
IPMS 安裝建置使用流程(1) - 匯入.CSV



IPMS安裝建置使用流程(2) - 透過LDAP(或AD)認證



IPMS安裝建置使用流程(3) - 透過Radius認證



系統參數功能解決方案-1



系統參數設定

系統架構: 單機

用戶申請完成後: 可立即上網

使用者自行更改卡號: 不可自行更改

學號/員工編號: 可重複2次

密碼寄送: 透過 SMTP 伺服器寄送密碼給使用者

寄件者: eagle@curelan.com

SMTP 伺服器: mail.curelan.com

用戶申請認證: 透過 Radius 認證

Radius Server IP: 192.83.194.253

Radius Port: 1812

Radius 密碼:

Radius 認證方式: pap

儲存 備份系統設定 還原系統設定

- 系統架構：可分為(1). 單機. (2). 雙機備援。
- 用戶申請完成後：可分為(1). 可立即上網. (2). 需經過管理者開通才可上網。
- 使用者自行更改卡號：(1). 不可自行更改. (2). 可自行更改1~10次選擇其一。
- 學號/員工編號：(1). 不限重複次數. (2). 可重複1~10次選擇其一。
- 密碼寄送：(1). 不提供忘記密碼功能. (2). 由本機直接寄送密碼給使用者. (3). 透過SMTP伺服器寄送密碼給使用者。

系統參數功能解決方案-2

二段式認證主要目的是要自動取得MAC

- 寄件者：因為有些使用單位之SMTP伺服器需要檢查一個Mail位置，有些不用，如果需要填就隨便填寫一個Mail位置即可，有些不用就不用填。
- 用戶申請認證：可分為
 - ◆ (1). 不需要認證，也就是直接使用本系統的二段式認證自動取得MAC來使用。
 - ◆ (2). 透過CSV匯入資料認證，並配合二段式認證自動取得MAC來使用。
 - ◆ (3). 透過LDAP(或AD)認證，並配合二段式認證自動取得MAC來使用。
 - LDAP認證 (或AD認證)+ 二段式認證
 - ◆ (4). 透過Radius認證，並配合二段式認證自動取得MAC來使用。
 - Radius認證 + 二段式認證
 - ◆ (5). 透過LDAP (或AD)認證，且帳號要在匯入資料中。也就是先以手動方式將使用者之CSV資料匯入在IPMS設備中，再搭配LDAP (或AD)認證，並配合二段式認證自動取得MAC來使用，此方案可防止使用者亂填”姓名及學號”。
 - 手動CSV資料匯入 + LDAP認證(或AD認證)+二段式認證
 - ◆ (6). 透過Radius認證，且帳號要在匯入資料中。也就是先以手動方式將使用者之CSV資料匯入在IPMS設備中，再搭配Radius認證，並配合二段式認證自動取得MAC來使用，此方案可防止使用者亂填”姓名及學號”。
 - 手動CSV資料匯入 + Radius認證 +二段式認證

IPMS設備之二段式認證授權方式介紹

- 二段式認證功能之優點為，當使用者不被DHCP Server認可之IP上網，本設備會將不被認可的IP自動導到”新用戶申請畫面”之畫面來申請帳號，也就是強制使用者來認證註冊。自動導到申請帳號畫面(如圖)是運用L 3 Switch的Policy Route功能。
- 採用，讓使用者自動要上網路認證填寫資料，本設備提供<http://192.168.0.68:81/apply.php>管理IP:81/apply.php頁面。
- 此頁面可連結到學校、公家機關、公司企業等的公用Web Server，讓使用者方便點選來申請認證填寫資料。
- 先填寫學號(員工編號)，此時本設備系統已自動偵測上網申請認證填寫資料的使用者之MAC(網卡卡號)00e018:6b24c2。

網址()  <http://192.168.0.68:81/apply.php>  移至  連結

新用戶申請

學號/員工編號:

網卡卡號: 00e018:6b24c2

- 填寫學號(員工編號)完後，按”送出”則會進入到另一畫面，如下圖

使用者姓名 + IP + MAC 自動相互綁定

- 使用者在”用戶資料”依欄位填寫個人資料，例；部門、宿舍(大樓名稱)、寢室門號(員工位置)即可，且本設備也自動偵測到MAC(網卡卡號) 00e018:6b24c2，顯示在”用戶資料”不用使用者來填寫。此方式本設備系統每次發現MAC(網卡卡號) 00e018:6b24c2都會發出同一個固定IP，以達到使用者姓名 + IP + MAC 相互綁定功能。

用戶資料	
學號/員工編號:	9900000
姓名:	
性別:	☒ 男 ☐ 女
密碼:	
部門:	
聯絡電話:	
電子郵件:	
宿舍(大樓):	中山樓 v
寢室門號:	
網卡卡號:	00E018:6B24C2
測測試試:	
無聊:	
test:	
儲存 清除 放棄	

IPMS提供CSV檔之匯出及匯入功能

匯出 功能介紹

- 在”用戶列表”功能中，提供”匯入”及”匯出”功能
- 讓管理者在備份（匯出）用戶資料庫時更快速更便利，而對於公家機關或公司企業過去已經存在龐大的資料庫，也可以透過匯入的功能整合到IPMS，大大降低管理者一筆一筆Key in的時間，為企業機關贏得時間優勢。

資料維護
用戶列表
未授權用戶
停權用戶
宿舍(大樓)資料
批量刪除用戶
基本用戶資料
系統功能
版面設計

選擇匯出欄位

欄位名稱	匯出欄位
系統內建欄位	
姓名	☒
性別	☒
學號/員工編號	☒
宿舍(大樓)	☒
寢室門號	☒
部門	☒
電子郵件	☐
申請日期	☒
聯絡電話	☒
網卡卡號	☒
IP位址	☒
密碼	☐
狀態	☐
類型	☐
VIP	☐
自訂欄位	
測測測式	☐
無聊	☐
test	☐

匯出
取消

IPMS提供CSV檔之匯出及匯入功能

匯入 功能介紹

- 在“用戶列表”功能中，點選“匯入”時，將欲匯入的CSV檔匯入。
- 與匯出原則相同，匯入時系統也提供選擇對應欄位界面，讓管理者確認其對應的欄位是否正確（欄位名稱 ↔ 匯入欄位），例如姓名 ↔ 姓名、性別 ↔ 性別、電子郵件 ↔ 無...等等，系統在載入的第一時間已經先各自欄位比對過一次，若完全相等則自動載入，否則請自行將“匯入欄位”下拉選取對應最合適的欄位；將各個匯入欄位選取確定後，點選“開始匯入”系統就立即處理。

選擇對應欄位

欄位名稱	匯入欄位
系統內建欄位	
姓名	姓名
性別	性別
學號/員工編號	學號/員工編號
宿舍(大樓)	宿舍(大樓)
寢室門號	無
部門	部門
電子郵件	無
申請日期	無
聯絡電話	無
網卡卡號	網卡卡號
IP位址	無
密碼	姓名
狀態	性別
類型	學號/員工編號
VIP	宿舍(大樓)
自訂欄位	部門
測測試試	網卡卡號
無聊	IP位址
test	狀態
	類型
	VIP
	無
	無

快速簡易方式建立使用者資料庫

- 透過本設備自動學習L3 CoreSwitch上之動態ARP Table表, 獲得IP及MAC對照表資料會在本設備的”基本用戶資料”建立資料庫, 但是;動態ARP Table表沒有”學號/員工編號”及”姓名”,所以管理者需要手動在本設備系統逐一輸入”學號/員工編號”及”姓名”,也可採用在本設備的”基本用戶資料”功能以手動匯入 CSV檔(使用單位原舊有使用者的資料), 但是CSV檔的欄位格式順序必須跟本設備系統欄位格式順序一致, 來建立每個使用者在本設備資料的完整性.就不需要上述比較繁瑣認證方式來建立資料庫.

Flowviewer IPMS 3000

資料維護

- 用戶列表
- 未授權用戶
- 停權用戶
- 宿舍(大樓)資料
- 批量刪除用戶
- 基本用戶資料**
- DHCP核發記錄
- IP核發統計
- 匯入學習的IP/MAC
- 刪除記錄

系統功能

版面設計

新增 匯入 匯出 清除

宿舍(大樓): 全部 搜尋: [] Go

學號/員工編號	姓名	性別	宿舍(大樓)	寢室門號	網卡卡號	IP位址	部門	聯絡電話	申請日期	動作
95000603	Steven	男	辦公室	188	0018F3:C6AE57	192.168.0.92	工程部	07-311-5186	2008/06/03	刪除 修改
95000777	eagle	男	辦公室	777	000AE4:02A2C6	192.168.0.93	研發部	07-311-7777	2008/07/01	刪除 修改
97003862	王語焉	女	天堂樓	862	001122:AABBCD	192.168.3.156	行銷部	02-39398899	2008/07/04	刪除 修改
97006893	張惠妹	女	天堂樓	893	001122:AABBCD	192.168.3.155	娛樂部	07-521-9999	2008/07/04	刪除 修改
96007001	巴菲特	男	黃鶴樓	001	338822:BADABB	192.168.2.204	財務部	07-777-9090	2008/07/17	刪除 修改
96005666	Michael Jordon	男	辦公室	666	041122:AABBCD	192.168.0.94	運動事業部	04-33995555	2008/07/17	刪除 修改
95003567	鈴木一郎	男	黃鶴樓	567	003222:AABBCD	192.168.2.202	運動事業部	07-551-8899	2008/07/17	刪除 修改
95006987	Tiger Woods	男	天堂樓	987	001122:AABACC	192.168.3.158	運動事業部	02-51518787	2008/07/17	刪除 修改
96008345	希拉蕊	女	黃鶴樓	345	001122:ACBBCC	192.168.2.203	政治部	05-337-6868	2008/07/17	刪除 修改
96008345	希拉蕊	女	天堂樓	345	001122:ACBBCC	192.168.3.179	政治部	05-337-6868	2008/07/17	刪除 修改
96008345	希拉蕊	女	辦公室	345	001122:ACBBCC	192.168.0.103	政治部	05-337-6868	2008/07/17	刪除 修改
96008345	希拉蕊	女	渤海樓	345	001122:ACBBCC	172.27.41.251	政治部	05-337-6868	2008/07/17	刪除 修改
94005687	喬峰	男	辦公室	687	001D60:1D7620	192.168.0.96	天下會	08-8986677	2008/07/22	刪除 修改
97003691	EeePC	男	辦公室	1000	002215:49B01D	192.168.0.98	敗家部	100	2008/07/24	刪除 修改
T9400	F8Va	男	辦公室	123	002215:4316A8	192.168.0.99	經濟部	123456	2008/07/29	刪除 修改

總共 26 位用戶, 第 1 位 - 第 15 位

用戶列表 功能

- 從”用戶列表”功能可得知，學號、姓名、寢室門號、網卡卡號(MAC)、IP位址、班級、連絡電話、申請日期、動作等欄位。可由IP位址查詢到使用者的資料，例；網卡卡號(MAC)、學號(員工編號)、姓名、寢室門號(員工位置)。

資料維護	新增 匯入 匯出 宿舍(大樓): 全部 搜尋:										
	學號/員工編號	姓名	性別	宿舍(大樓)	寢室門號	網卡卡號	IP位址	部門	聯絡電話	申請日期	動作
用戶列表	95000603	Steven	男	中山樓	188	0018F3:C6AE57	192.168.0.92	工程部	07-311-5186	2008/06/03	刪除 修改 開通 停權
未授權用戶	95000777	eagle	男	中山樓	777	000AE4:02A2C6	192.168.0.93	研發部	07-311-7777	2008/07/01	刪除 修改 開通 停權
停權用戶	97003862	王語焉	女	天堂樓	862	001122:AABBCD	192.168.3.156	行銷部	02-39398899	2008/07/04	刪除 修改 開通 停權
宿舍(大樓)資料	97006893	張惠妹	女	天堂樓	893	001122:AABBCD	192.168.3.155	娛樂部	07-521-9999	2008/07/04	刪除 修改 開通 停權
批量刪除用戶	96007001	巴菲特	男	黃鶴樓	001	338822:BADABB	192.168.2.204	財務部	07-777-9090	2008/07/17	刪除 修改 復權 檢查
基本用戶資料	96005666	Michael Jordan	男	中山樓	666	041122:AABBCD	192.168.0.94	運動事業部	04-33995555	2008/07/17	刪除 修改 開通 停權
系統功能	95003567	鈴木一郎	男	黃鶴樓	567	003222:AABBCD	192.168.2.202	運動事業部	07-551-8899	2008/07/17	刪除 修改 開通 停權
版面設計	95006987	Tiger Woods	男	天堂樓	987	001122:AABACC	192.168.3.158	運動事業部	02-51518787	2008/07/17	刪除 修改 開通 停權
	96008345	希拉蕊	女	黃鶴樓	345	001122:ACBBCC	192.168.2.203	政治部	05-337-6868	2008/07/17	刪除 修改 開通 停權
	96008345	希拉蕊	女	天堂樓	345	001122:ACBBCC	192.168.3.179	政治部	05-337-6868	2008/07/17	刪除 修改 開通 停權
	96008345	希拉蕊	女	中山樓	345	001122:ACBBCC	192.168.0.103	政治部	05-337-6868	2008/07/17	刪除 修改 開通 停權
	96008345	希拉蕊	女	渤海樓	345	001122:ACBBCC	172.27.41.251	政治部	05-337-6868	2008/07/17	刪除 修改 開通 停權
	94005687	喬峰	男	中山樓	687	001D60:1D7620	192.168.0.96	天下會	08-8986677	2008/07/22	刪除 修改 繳費 開通 停權
	eagle524	EeePC	男	中山樓	1000	002215:49B01D	192.168.0.98	敗家部	100	2008/07/24	刪除 修改 繳費 開通 停權
	T9400	F8Va	男	中山樓	123	002215:4316A8	192.168.0.99	經濟部	123456	2008/07/29	刪除 修改 開通 停權

總共 23 位用戶，第 1 位 - 第 15 位

藍色：未繳費用戶 紅色：停權用戶

基本用戶資料 功能(等於設備本身內建資料庫)

- 基本用戶資料與用戶列表之不同：此功能是搭配手動式匯入CSV使用者資料，與LDAP或Radius認證結合之基本用戶資料，此功能比用戶列表多了”消除”功能，當管理者發現某些匯入資料有錯誤時可整批刪除。

資料維護
用戶列表
未授權
停權用戶
宿舍(大樓)資料
批量刪除用戶
基本用戶資料
系統功能
版面設計

新增
匯入
匯出
消除

宿舍(大樓): 全部
搜尋:

學號/員工編號	姓名	性別	宿舍(大樓)	寢室門號	網卡卡號	IP位址	部門	聯絡電話	申請
95000603	Steven	男	中山樓	188	0018F3:C6AE57	192.168.0.92	工程部	07-311-5186	2008,
95000777	eagle	男	中山樓	777	000AE4:02A2C6	192.168.0.93	研發部	07-311-7777	2008,
97003862	王語焉	女	天堂樓	862	001122:AABBCD	192.168.3.156	行銷部	02-39398899	2008,
97006893	張惠妹	女	天堂樓	893	001122:AABBCC	192.168.3.155	娛樂部	07-521-9999	2008,
96007001	巴菲特	男	黃鶴樓	001	338822:BADABB	192.168.2.204	財務部	07-777-9090	2008,
96005666	Michael Jordan	男	中山樓	666	041122:AABBCC	192.168.0.94	運動事業部	04-33995555	2008,
95003567	鈴木一郎	男	黃鶴樓	567	003222:AABBCC	192.168.2.202	運動事業部	07-551-8899	2008,
95006987	Tiger Woods	男	天堂樓	987	001122:AABACC	192.168.3.158	運動事業部	02-51518787	2008,
96008345	希拉蕊	女	黃鶴樓	345	001122:ACBBCC	192.168.2.203	政治部	05-337-6868	2008,
96008345	希拉蕊	女	天堂樓	345	001122:ACBBCC	192.168.3.179	政治部	05-337-6868	2008,
96008345	希拉蕊	女	中山樓	345	001122:ACBBCC	192.168.0.103	政治部	05-337-6868	2008,
96008345	希拉蕊	女	渤海樓	345	001122:ACBBCC	172.27.41.251	政治部	05-337-6868	2008,
94005687	喬峰	男	中山樓	687	001D60:1D7620	192.168.0.96	天下會	08-8986677	2008,
97003691	EeePC	男	中山樓	1000	002215:49B01D	192.168.0.98	敗家部	100	2008,
T9400	F8Va	男	中山樓	123	002215:4316A8	192.168.0.99	經濟部	123456	2008,

總共 23 位用戶，第 1 位 - 第 15 位

未授權用戶功能(二段式認證授權功能的延伸)

- 本設備在學生開學時會開放學生來註冊填寫資料，學生在上網註冊後填寫表單，此資料會自動記錄在”未授權用戶”功能中，如果學生已繳費管理者只要按下欄位中”動作”功能之”繳費”功能，則學生的資料就會在此功能中消失表示已繳費。
- 在政府單位或公司企業，經過管理者審核通過之合法用戶直接按入欄位中”動作”功能之”開通”功能，則使用者的資料就會在此功能中消失表示已正式授權認可用戶。

資料維護
用戶列表
未授權用戶
停權用戶
宿舍(大樓)資料
批量刪除用戶
基本用戶資料
系統功能
版面設計

宿舍(大樓): 全部 搜尋: Go

學號/員工編號	姓名	性別	宿舍(大樓)	寢室門號	網卡卡號	IP位址	部門	聯絡電話	申請日期	動作
94005687	喬峰	男	中山樓	687	001D60:1D7620	192.168.0.96	天下會	08-8986677	2008/07/22	刪除 修改 繳費 開通 停權 檢查
eagle524	EeePC	男	中山樓	1000	002215:49B01D	192.168.0.98	敗家部	100	2008/07/24	刪除 修改 繳費 開通 檢查
eagle524	王明輝	女	中山樓	1234	000C29:5B8183	192.168.0.108	測試	3115186	2009/02/05	刪除 修改 繳費 開通 檢查

總共 3 位用戶，第 1 位 - 第 3 位

藍色：未繳費用戶 紅色：停權用戶

管理者 彈性輸入” 新增用戶” 資料 功能- 1

(此功能是臨時或特殊狀況才使用)

- 當管理者臨時遇到要緊急需求輸入使用者資料時，可選擇此功能。
- 此功能是在” 資料維護” 大項功能之” 用戶列表” 功能，的” 新增” 功能直接按入即可進入此畫面。
- 學校宿舍管理範例：管理者可彈性填寫” 新增用戶” 功能就表示此學生已繳費，此表單資料不會進入” 未繳費用戶功能中”。 Ps:學生上網註冊填寫表單跟此畫面是一樣。
- 政府單位及公司企業範例：管理者直接輸入使用者的資料，就不用經過二段式授權，直接進入合法授權用戶，例；學校的校長、政府單位的高級長官、公司企業的董事長等人物都是由管理者直接輸入他們的資料。
- VIP功能：本設備系統為了更嚴謹資訊安全，由本系統DHCP Server核發的IP是不能跨 L3 Switch 的Vlan，但是為了使用單位有特別需求，多了此VIP功能，只要在VIP功能” 打勾” 則本系統DHCP Server就核發可跨Vlan的IP。

管理者 彈性輸入”新增用戶”資料 功能-2

資料維護		新增		匯入		匯出		宿舍(大樓)：全部		搜尋：		
用戶列表		學號/員工編號	姓名	性別	宿舍(大樓)	寢室門號	網卡卡號	IP位址	部門	聯絡電話	申請日期	動作
未授權用戶		95000603	Steven	男	中山樓	188	0018F3:C6AE57	192.168.0.92	工程部	07-311-5186	2008/06/03	刪除 修改 開通 停權
停權用戶		95000777	eagle	男	中山樓	777	000AE4:02A2C6	192.168.0.93	研發部	07-311-7777	2008/07/01	刪除 修改 開通 停權
宿舍(大樓)資料		97003862	王語嫣	女	天堂樓	862	001122:AABBCCD	192.168.3.156	行銷部	39398899	2008/07/04	刪除 修改 開通 停權
批量刪除用戶		97006893	張惠妹	女	天堂樓	893	001122:AABBCC	192.168.3.155	娛樂部	07-521-9999	2008/07/04	刪除 修改 開通 停權
基本用戶資料		96007001	巴菲特	男	黃鶴樓	001	338822:BADABB	192.168.2.204	財務部	07-777-9090	2008/07/17	刪除 修改 復權 檢查
系統功能		96005666	Michael Jordan	男	中山樓	666	041122:AABBCC	192.168.0.94	運動事業部	04-33995555	2008/07/17	刪除 修改 開通 停權
版面設計		95003567	鈴木一郎	男	黃鶴樓	567	003222:AABBCC	192.168.2.202	運動事業部	07-551-8899	2008/07/17	刪除 修改 開通 停權
		95006987	Tiger Woods	男	天堂樓	987	001122:AABACC	192.168.3.158	運動事業部	02-51518787	2008/07/17	刪除 修改 開通 停權
		96008345	希拉蕊	女	黃鶴樓	345	001122:ACBBCC	192.168.2.203	政治部	05-337-6868	2008/07/17	刪除 修改 開通 停權
		96008345	希拉蕊	女	天堂樓	345	001122:ACBBCC	192.168.3.179	政治部	05-337-6868	2008/07/17	刪除 修改 開通 停權
		96008345	希拉蕊	女	中山樓	345	001122:ACBBCC	192.168.0.103	政治部	05-337-6868	2008/07/17	刪除 修改 開通 停權
		96008345	希拉蕊	女	渤海樓	345	001122:ACBBCC	172.27.41.251	政治部	05-337-6868	2008/07/17	刪除 修改 開通 停權
		94005687	喬峰	男	中山樓	687	001D60:1D7620	192.168.0.96	天下會	08-8986677	2008/07/22	刪除 修改 複費 開通 停權
		eagle524	EeePC	男	中山樓	1000	002215:49E51D	192.168.0.98	敗家部	100	2008/07/24	刪除 修改 複費 開通 停權
		T9400	F8Va	男	中山樓	123	002215:431673	192.168.0.99	經濟部	123456	2008/07/29	刪除 修改 開通 停權
總共 23 位用戶，第 1 位 - 第 15 位												

按下,進入此畫面

資料維護	
用戶列表	未授權用戶
停權用戶	宿舍(大樓)資料
批量刪除用戶	基本用戶資料
系統功能	版面設計

新增用戶資料

姓名: ☐ VIP

學號/員工編號:

性別: ☒ 男 ☐ 女

密碼:

部門:

聯絡電話:

電子郵件:

宿舍(大樓):

寢室門號:

網卡卡號: 卡號輸入格式: 001122:AABBCC

IP位址: ☒ 自動核發 IP ☐ 不使用 DHCP

測測試試:

無聊:

test:

儲存 消除 放棄

IPMS設備最重要特點就是具備VIP功能

- **某些廠牌**設備為了方便性所以IP在跨網段時,DHCP Server會核發不同IP,也就是IP沒有攜帶性,這會造成使用單位原有**網路流量報表的不準確性及流量配額(Quota)的設定不準**,這是**某些廠牌**設備最大漏洞,而IPMS設備也沒有IP攜帶性功能,但是IPMS設備具備IP不能跨網段功能,但是為了解決方便性問題IPMS設備具備"VIP"功能,也就是管理者在預先可將要跨網段的IP預先設定在"VIP"功能中,只有這些IP或網段的使用者才可以而且這些使用者是受到設備系統監控所以就沒有漏洞產生。

新增用戶資料

姓名:

學號/員工編號:

性別: ☒ 男 ☐ 女

密碼:

部門:

聯絡電話:

電子郵件:

宿舍(大樓):

寢室門號:

網卡卡號: 卡號輸入格式: 001122:AABBCC

IP位址: ☒ 自動核發 IP ☐ 不使用 DHCP

測測測試:

無聊:

test:

儲存 清除 放棄

DHCP 核發紀錄

- 此功能為讓管理者可以查詢DHCP Server配發IP的情況，可以確認clinet端(使用端)是否有跟DHCP Server要IP。

資料維護

用戶列表

未授權用戶

停權用戶

宿舍(大樓)資料

批量刪除用戶

基本用戶資料

DHCP核發記錄

IP核發統計

匯入學習的IP/MAC

刪除記錄

搜尋：

Go

網卡卡號	IP位址	租期開始	租期結束
00:0C:29:11:27:B8	192.168.0.80	2010/07/22 07:33:51	2010/07/22 07:43:51
00:0E:35:25:32:70	192.168.0.88	2010/07/10 06:58:41	2010/07/10 07:08:41
00:13:46:9A:63:B9	192.168.2.13	2010/01/15 21:12:16	2010/01/15 21:17:16
00:15:00:32:6E:95	192.168.0.84	2010/07/24 09:17:35	2010/07/24 09:27:35
00:1F:1F:55:E5:61	192.168.0.86	2010/07/25 01:53:37	2010/07/25 02:03:37
00:1F:D0:24:E5:01	192.168.2.100	2009/03/25 07:45:52	2009/03/25 07:50:52
00:21:91:1E:DE:39	192.168.0.87	2010/07/15 00:14:45	2010/07/15 00:24:45
00:21:91:80:B6:10	192.168.0.81	2010/07/20 00:08:51	2010/07/20 00:18:51
00:22:15:43:16:A8	192.168.3.100	2009/04/17 05:44:42	2009/04/17 05:45:44
00:23:76:B8:DF:2A	192.168.0.85	2010/07/23 12:24:31	2010/07/23 12:26:31
00:25:D3:93:5C:C2	192.168.0.83	2010/07/19 01:57:27	2010/07/19 01:57:30
00:AB:00:00:00:00	192.168.0.82	2010/03/21 08:28:00	
E0:CB:4E:1F:49:B9	192.168.0.89	2010/07/20 08:33:55	2010/07/20 08:43:55

IP核發統計

- 此功能為讓管理者可以知道, 在每個網段裡面, 總共可以允許核發IP數目, 且已核發IP數及剩餘IP數, 讓管理IP配發更為方便控管.

宿舍(大樓)	核發 IP 範圍	總共可核發 IP 數	已核發 IP 數	剩餘 IP 數
辦公室	192.168.0.90 - 192.168.0.110	21	19	2
黃鶴樓	192.168.2.200 - 192.168.2.208	9	2	7
天堂樓	192.168.3.150 - 192.168.3.250	101	3	98
渤海樓		0	0	0
易水樓	192.168.4.1 - 192.168.4.240	240	0	240
資訊處	192.168.100.1 - 192.168.100.4	4	0	4
電算中心		0	0	0
資圖中心	192.168.9.160 - 192.168.9.249 192.168.9.1 - 192.168.9.5 192.168.9.7 - 192.168.9.127	216	3	213

IP / MAC學習(屬於系統功能)

- 此功能為設定需學習的Switch IP及SNMP密碼。
- 新增:新增Route Switch IP及SNMP密碼資料。
- 啟用IP/MAC學習:當Route Switch IP都設定好了之後,把此功能啟動就可以了。

資料維護
系統功能
系統設定
管理帳號
DHCP伺服器
系統狀態
網路設定
IP/MAC學習
系統更新

新增

☒ 啟用IP/MAC學習

Route Switch IP	SNMP密碼(Community)	備註	動作
192.83.194.254	eagle	test	刪除 修改

匯入學習的IP / MAC

- 此功能為DHCP Server自動學習功能,透過SNMP協定,每隔一段時間會自動向Switch詢問已學習到的資料,再利用載入學習資料功能,把資料匯入進來。
- 載入學習資料:載入已向Switch學習到的IP及MAC,以及是在哪台switch上所學習到的,透過哪一個port連線的。
- 宿舍(大樓):可自行選擇只要匯入哪個網段的資料,或者直接匯入全部。

資料維護

- 用戶列表
- 未授權用戶
- 停權用戶
- 宿舍(大樓)資料
- 批量刪除用戶
- 基本用戶資料
- DHCP核發記錄
- IP核發統計
- 匯入學習的IP/MAC
- 刪除記錄

匯入已學習到的IP / MAC

載入學習資料

過濾條件

宿舍(大樓): 全部

IP 關鍵字:

匯入選取資料

匯入全部資料

搜尋結果

每頁顯示: 15 筆資料

☐	學號/員工編號	姓名	宿舍(大樓)	IP位址	網卡卡號	Switch	Port
☐			電算中心	192.83.194.8	001731:0714FF	192.83.194.254	8/12
☐			電算中心	192.83.194.207	001125:B79B61	192.83.194.254	8/3
☐			電算中心	192.83.194.11	00215E:DB1312	192.83.194.254	14/11
☐			電算中心	192.83.194.253	001485:2B7E50	192.83.194.254	4/4
☐			電算中心	192.83.194.177	000C6E:E34172	192.83.194.254	10/21
☐			電算中心	192.83.194.14	00112F:1A249A	192.83.194.254	8/14

刪除紀錄

- 此功能為在用戶列表刪除的資料會記錄起來,供管理者日後可做查詢使用,也可做資料復原動作.也就是說可讓管理者直接復原某一筆資料,可讓該筆資料的clinet端不用再進行”對本設備系統”註冊即可上網,以避免被刪除的資料重新登錄設備系統註冊之流程.

資料維護

- 用戶列表
- 未授權用戶
- 停權用戶
- 宿舍(大樓)資料
- 批量刪除用戶
- 基本用戶資料
- DHCP核發記錄
- IP核發統計
- 匯入學習的IP/MAC
- 刪除記錄**

宿舍(大樓): 全部

搜尋: Go

學號/員工編號	姓名	性別	宿舍(大樓)	寢室門號	網卡卡號	IP位址	部門	聯絡電話	申請日期	刪除時間	動作
96007001	巴菲特	男	黃鶴樓	001	338822:BADABB	192.168.2.204	財務部	07-777-9090	2008/07/17	1970/01/01	復原
901	test901	男	辦公室	12	0011AA:112233	192.168.0.109	研發部		2010/01/06	2010/07/21	復原
904	test904	男	資圖中心	0	00CCDD:123456	192.168.9.4			2010/01/06	2010/07/19	復原

總共 3 筆記錄, 第 1 筆 - 第 3 筆

停權用戶 功能

- 在”資料維護”大項功能之”用戶列表”功能中有一項”動作”欄位，只要按”停權”功能，設備系統會在DHCP Server將此IP列為不被認可核發的IP，使這個IP就不能上網，故此IP就會列在”停權用戶”功能中。
- 要恢復授權(復權)管理者可在”停權用戶”功能中有一項”動作”欄位，只要按”復權”功能，設備系統會在DHCP Server核發原來的IP給此使用者。

資料維護
用戶列表
未授權用戶
停權用戶
宿舍(大樓)資料
批量刪除用戶
基本用戶資料
系統功能
版面設計

宿舍(大樓): 全部
搜尋:
Go

學號/員工編號	姓名	性別	宿舍(大樓)	寢室門號	網卡卡號	IP位址	部門	聯絡電話	申請日期	動作
96007001	巴菲特	男	黃鶴樓	001	338822:BADABB	192.168.2.204	財務部	07-777-9090	2008/07/17	刪除 修改 復權 檢查

總共 1 位用戶，第 1 位 - 第 1 位

藍色：未繳費用戶 紅色：停權用戶

維修區功能

- 當有一網域不需要持續做IP+Mac綁定時（如維修區），IPMS可將此網域設定成**不需註冊**；設定完成後，此網域只使用DHCP Server之功能，因為使用單位有電腦網卡損壞維修後要測試問題，所以需要有維修區功能。



網域	核發 IP 範圍	核發 IP 給未註冊電腦	最長租期	動作
192.168.0.0	192.168.0.90 - 192.168.0.110	No	172800	NewPool 刪除 修改
-	192.168.0.80 - 192.168.0.89		600	刪除 修改
192.168.2.0	192.168.2.1 - 192.168.2.100	Yes	300	NewPool 刪除 修改
-	192.168.2.200 - 192.168.2.208	No		刪除 修改
192.168.3.0	192.168.3.1 - 192.168.3.100	Yes		
-	192.168.3.150 - 192.168.3.250	No		



DHCP Pool

子網域: 192.168.2.0

IP 範圍: -

最長租用時間: 0 天 0 時 0 分

核發 IP 給未知卡號: ☒ 是(強迫註冊) ☒ 是(不需註冊) ☐ 否

永久租用: ☐ 是 ☒ 否

儲存 清除 放棄

訊息維護

- 可針對本系統”訊息維護”之內容修改適合使用單位之標題內容，例；標題、申請成功、沒設DHCP、卡號重覆、學號/員工編號重覆、IP 位址用完、停權訊息 等功能修改為適合使用單位的內容。
- 如果訊息維護內容需要有圖案，則需要從本設備系統的”管理上傳檔案”之功能取得使用單位管理者自行製作之圖案。

資料維護

系統功能

版面設計

導覽標籤設定

資料欄位設定

訊息維護

管理上傳檔案

訊息	訊息內容	動作
標題		修改
申請成功	你的申請已經通過，重新開機後即可正常上網。 請在 2008/10/31 之前拿宿網申請單到出納組繳費，再將繳費證明拿到電算中心之後才能開通網路。 超過期限未完成繳費手續將中斷網路連線，學期內也不能再申請！	修改
沒設DHCP	系統無法偵測到你的網路卡卡號!!! 請使用自己的電腦上網申請，並將電腦的 IP 位址設定成「自動取得 IP 位址」，然後將你的電腦重新開機後再上網申請。	修改

Internet Protocol Version 4 (TCP/IPv4) 內容

一般 其他設定

如果您的網路支援這項功能，您可以取得自動指派的 IP 設定。否則，您必須詢問網路系統管理員正確的 IP 設定。

☒ 自動取得 IP 位址 (O)

☐ 使用下列的 IP 位址 (S):

IP 位址 (I):

子網路遮罩 (U):

預設閘道 (D):

管理上傳檔案

- 由使用單位管理者自行製作之圖檔，此圖檔主要是給使用者看的，目的是讓使用者了解情況，例；使用者的電腦沒有設定為”自動取得IP位置”，借由圖檔來導引使用者如何設定電腦。

資料維護
系統功能
版面設計
導覽標籤設定
資料欄位設定
訊息維護
管理上傳檔案

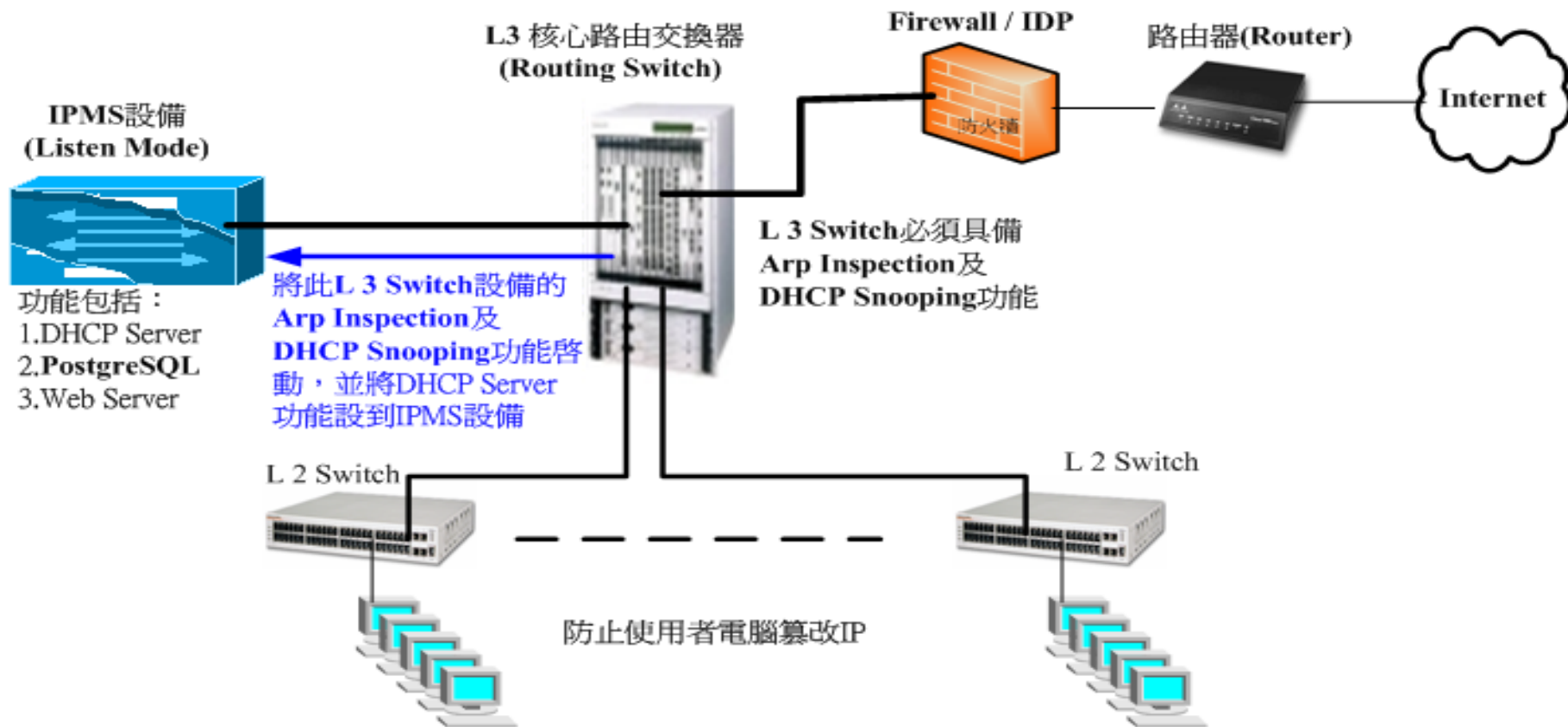
刪除選取檔案

上傳檔案

☐	檔案名稱	縮圖	檔案大小	上傳日期
☐	bill2.jpg		62079	Aug 7
☐	bill3.jpg		63148	Aug 7

此方案為最差方案, 除非” L3 核心路由交換器之DHCP Snooping功能要夠強

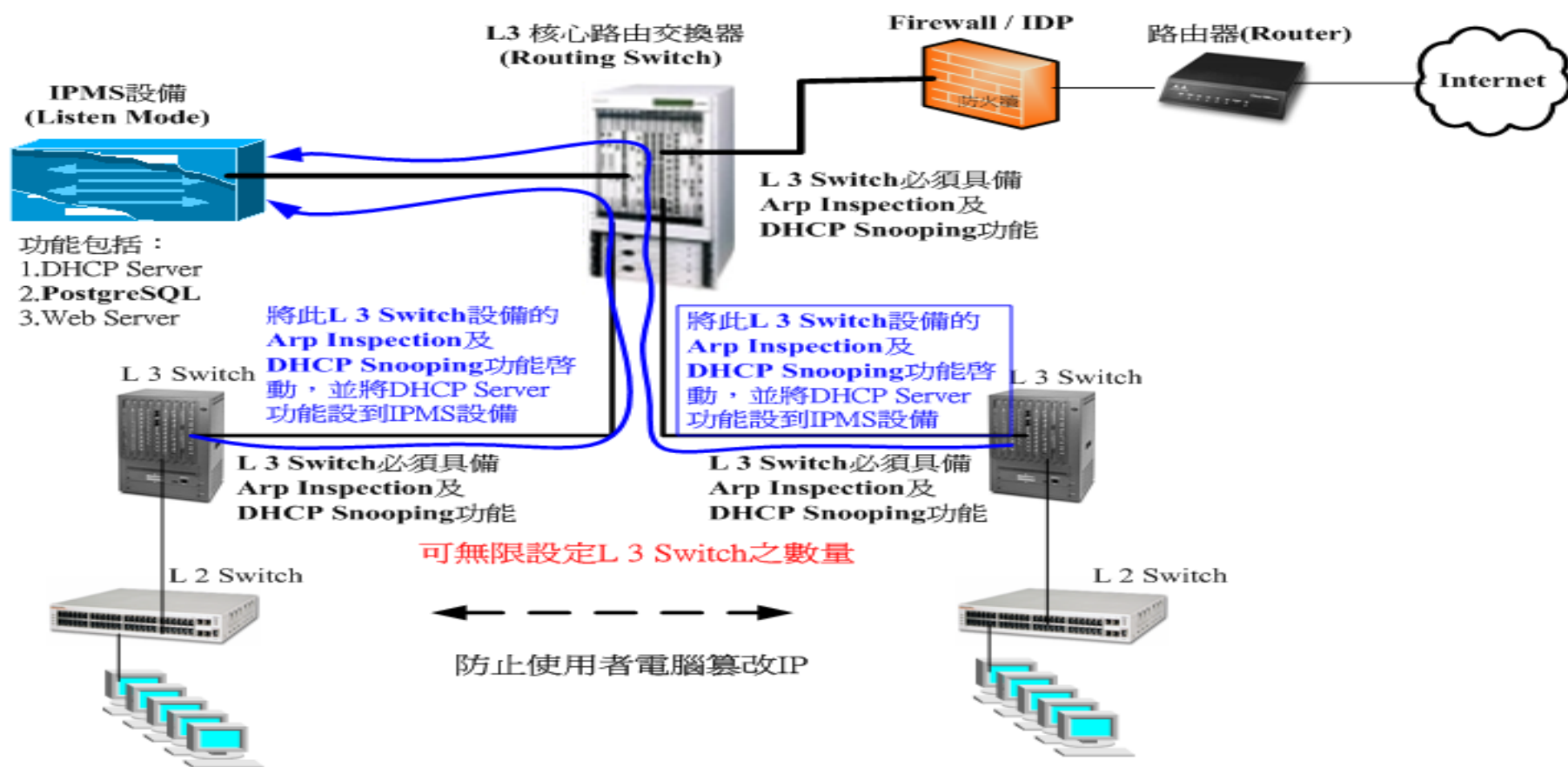
I P M S 設備之連接方式1



本設備與L 3 Switch架構 -2

此方案為最佳方案, 也就是2, 3, 3網路佈置架構

I P M S 設備之連接方式-2



IPMS 設備功能介紹

■ 本設備內建下列等主要功能

- 1. DHCP Server 。
- 2. PostgreSQL 。
- 3. Web Server 。
- Arp Inspection及DHCP Snooping和DHCP Relay功能，搭配廠牌有CISCO、FOUNDRY、Extreme(xos)、Alcatel 。

DHCP Server功能之租約(Renew)設定

- 一般DHCP Server之Renew(租約)預設值為600秒(10分鐘) ，本設備為了DHCP Server效能問題所以設計可同時設定 ” 預設租約時間” 及” 最長租約時間” ，其目的就是讓 DHCP Server之Renew(租約)時間可以延長，因為10分鐘實在太短，常常Renew會影響DHCP Server之效能，有此功能DHCP Server在管理者重新新增或刪除IP時，就不用重新Reset DHCP Server。
- 例；在高雄海洋科技大學學生宿網，在10.170.0.0之Class B 網域中設定兩組網段，一組是10.170.11.1到10.170.4.254這組網段，是不被DHCP Server所核發的IP範圍，另一組是10.170.128.1到10.170.135.254這組網段，是DHCP Server所認可核發的IP給使用者電腦的範圍，此為二段式認證授權方式。

本設備 DHCP Server功能介紹

(剛開始安裝設備時管理者先要設定之功能)

- 可先在某段網域(例；Class B)先設定兩組網段，一組網段是DHCP Server不被認可，另一組網段是被DHCP Server所認可，可以核發IP給使用者電腦，此為二段式認證授權方案。

- 資料維護
- 系統功能
 - 系統設定
 - 管理帳號
 - DHCP 伺服器**
 - 系統狀態
 - 網路設定
 - 系統更新
- 版面設計

DHCP 伺服器設定

新增領域
停用 DHCP

通用設定		動作
預設租用時間	8 天 0 時 0 分	修改
最長租用時間	16 天 0 時 0 分	修改
DNS 伺服器	168.95.1.1, 192.168.0.254	修改
WINS 伺服器		修改
Domain Name	curelan.com	修改

現有領域

網域	核發 IP 範圍	核發 IP 給未註冊電腦	最長租期	動作
172.27.41.0				NewPool 刪除 修改
-	172.27.41.251 - 172.27.41.253	No	172800	刪除 修改
192.168.0.0				NewPool 刪除 修改
-	192.168.0.80 - 192.168.0.89	Yes	600	刪除 修改
-	192.168.0.90 - 192.168.0.110	No	172800	刪除 修改
192.168.2.0				NewPool 刪除 修改
-	192.168.2.1 - 192.168.2.100	Yes	300	刪除 修改
-	192.168.2.200 - 192.168.2.208	No	172800	刪除 修改
192.168.3.0				NewPool 刪除 修改
-	192.168.3.1 - 192.168.3.100	Yes	600	刪除 修改
-	192.168.3.150 - 192.168.3.250	No	172800	刪除 修改

新增領域 功能

資料維護

系統功能

系統設定

管理帳號

DHCP 伺服器

系統狀態

DHCP 領域

子網域:

網路遮罩:

廣播位址:

Router IP:

Shared-Network:

單位:

儲存

消除

放棄

NewPool 功能

- 例：在Class B網域中在再插入一段Class C，有彈性功能之調配。

資料維護

系統功能

系統設定

管理帳號

DHCP 伺服器

系統狀態

DHCP Pool

子網域: 10.170.0.0

IP 範圍: -

最長租用時間: 0 天 0 時 0 分

核發 IP 給未知卡號: ☒ 是 ☐ 否

永久租用: ☐ 是 ☒ 否

儲存

消除

放棄

宿舍資料 功能

(剛開始安裝設備時管理者先要設定之功能)

- 管理者可將：宿舍代碼、宿舍名稱、Route Switch之管理IP填入”宿舍資料”功能中，宿舍名稱欄位才會顯示在”用戶列表”功能中的”宿舍”欄位。
- 政府單位或公司企業可將”宿舍資料”功能修改為”大樓名稱”，此功能只是要確認IP是從那一棟大樓來的IP。
- Route Switch IP所填入的IP是指L 3 Route Switch 的管理IP。
- 按下”**新增**”會進入到**下一頁**”**新增資料**”功能。指L3 Switch資料

資料維護

- 用戶列表
- 未授權用戶
- 停權用戶
- 宿舍(大樓)資料**
- 批量刪除用戶
- 基本用戶資料

系統功能

版面設計

新增

代碼	名稱	Route Switch IP	動作
1	中山樓	192.168.0.254	刪除 修改
2	黃鶴樓	192.168.0.69	刪除 修改
3	天堂樓	192.168.3.254	刪除 修改
4	渤海樓	203.64.171.28	刪除 修改
5	易水樓	192.168.0.5	刪除 修改
6	資訊處	203.64.171.28	刪除 修改

總共 6 棟，第 1 棟 - 第 6 棟

1

新增資料功能

資料維護

用戶列表

未授權用戶

停權用戶

宿舍(大樓)資料

批量刪除用戶

基本用戶資料

系統功能

版面設計

新增資料

代碼:

名稱:

Route Switch 廠牌:

Route Switch IP:

登入 Route Switch 的帳號:

登入 Route Switch 的密碼:

Route Switch 的 enable 密碼:

用戶使用之 VLAN ID:

是否使用 DHCP 分發 IP:

☐ 是 ☒ 否

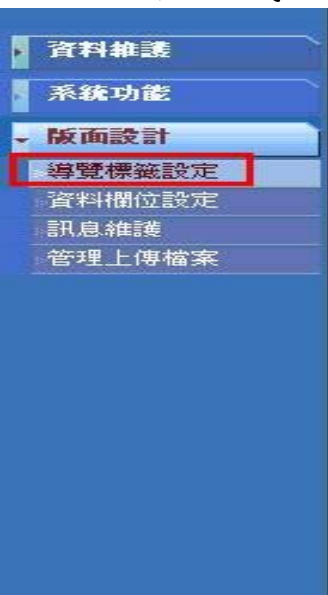
儲存

消除

放棄

版面設計 之 導覽標籤設定 功能

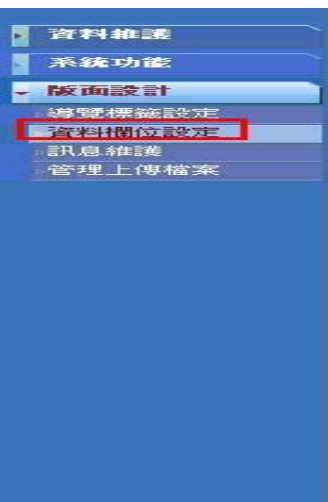
- 為了使IPMS設備更具彈性適用到公家機關及公司企業使用，MIS管理者可更改本設備**程式UI**畫面。
- 在”**版面設計**”內的”**導覽標籤設定**”選項，可編輯左邊功能選項。
- 選定”**版面設計**”底下的”**導覽標籤設定**” MIS管理者可更改本設備程式UI畫面，例；選擇”**用戶列表**”之”**修改**”功能，則可將”**用戶列表**”修改為”**用戶資料**”或由管理者自定。如圖
- 欲更改標籤名稱時，請點選動作欄內的修改（此時狀態會顯示為更新），待標籤名稱更完成時，執行更新即可。



導覽標籤設定	
標籤名稱	動作
資料維護	修改
用戶列表	更新
未授權用戶	修改 隱藏
停權用戶	修改 隱藏
宿舍(大樓)資料	修改 隱藏
批量刪除用戶	修改 隱藏
基本用戶資料	修改 隱藏
系統功能	修改
系統設定	修改 隱藏
管理帳號	修改 隱藏
DHCP 伺服器	修改 隱藏
系統狀態	修改 隱藏
網路設定	修改 隱藏
系統更新	修改 隱藏
版面設計	修改
導覽標籤設定	修改
資料欄位設定	修改 隱藏
訊息維護	修改 隱藏
管理上傳檔案	修改 隱藏

版面設計 之 資料欄位設定 功能

- “版面設計”功能底下的”資料欄位設定”其功能可讓管理者新增使用者的欄位及修改”系統內建欄位”之名稱，例；”學號”可修改為”員工編號”，”宿舍”可修改為”大樓名稱”，”寢室門號”可修改為”員工位置”（辦公室1）。
- 在版面設計”功能內的”資料欄位設定”選項，可編輯”列表顯示”（即用戶列表）及”資料輸入”（即新增用戶）內的欄位。
- “申請輸入”功能：是以搭配手動式匯入CSV使用者資料，與LDAP或Radius認證結合後，再與二段式認證自動取得MAC功能之後，要讓使用者填寫之欄位，與”資料輸入”之欄位是不一樣。



資料欄位設定				
欄位名稱	動作	資料輸入	列表顯示	申請輸入
系統內建欄位				
姓名	修改	☒	☒	☒
性別	修改	☒	☒	☒
學號/員工編號	修改	☒	☒	☒
宿舍(大樓)	修改	☒	☒	☒
寢室門號	修改	☒	☒	☒
部門	修改	☒	☒	☒
電子郵件	修改	☒	☐	☒
申請日期	修改	☐	☒	☐
聯絡電話	修改	☒	☒	☒
網卡卡號	修改	☒	☒	☒
IP位址	修改	☒	☒	☒
密碼	修改	☒	☐	☒
狀態	修改	☐	☐	☐
類型	修改	☐	☐	☐
VIP	修改	☐	☐	☐
自訂欄位				
測測測式式式	修改	☒	☐	☒
無聊	修改	☒	☐	☒
test	修改	☒	☐	☒
Add		☐	☐	☐

批量刪除用戶

- 此功能大多使用在學校單位，因為學生有畢業問題所以需要批量來刪除學生資料。

資料維護
用戶列表
未繳費用戶
停權用戶
宿舍(大樓)資料
批量刪除用戶
系統功能
版面設計

批量刪除用戶

搜尋
刪除
整批刪除

刪除條件

申請時間範圍(格式 yyyy/mm/dd，不限制請留空白):	-
學號/員工編號關鍵字:	
宿舍(大樓):	全部 ▼
IP 關鍵字:	

管理帳號

資料維護

系統功能

系統設定

管理帳號

DHCP 伺服器

系統狀態

版面設計

Add New

	Username	
	eagle	 
	cfkuo	 
	ekiss7510	 
	sense750314	 
	mingyum	 
	egbert	 
	steven	 
	Eagle	 

系統狀態

資料維護

系統功能

系統設定

管理帳號

DHCP 伺服器

系統狀態

版面設計

System Resources

	Name	Usage
	CPU	0 %
	RAM	17 %

大陸論壇對ARP攻擊新經驗

TJP5588

发表于 2008-9-2 15:31 [只看该作者](#)[小](#) [中](#) [大](#) [8楼](#)

UID 149495

帖子 3

精华 0

积分 32

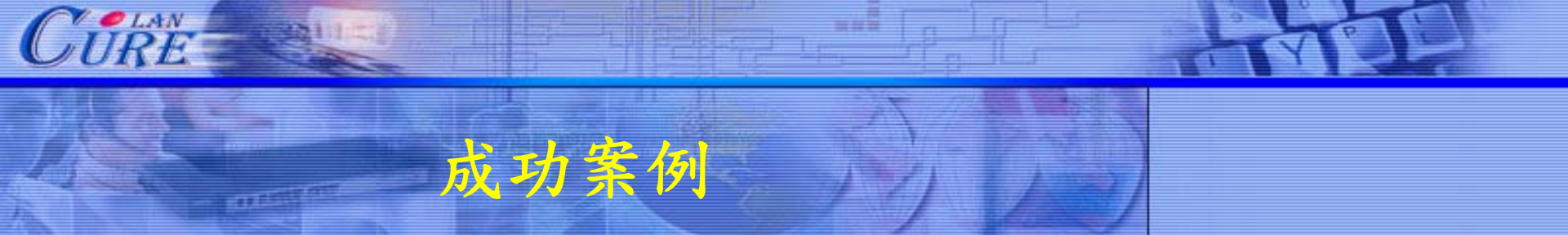
阅读权限 100

在线时间 0 小时

注册时间 2008-8-29

局域网的ARP病毒现在很猖獗，变种也很多，可防不可杀，我们一般查到都让用户直接重装系统。

[查看详细资料](#)[引用](#) [报告](#) [评分](#) [回复](#) [TOP](#)



成功案例

類型	客戶
學校	海洋科技大學
學校	嶺東科技大學
學校	長庚技術學院 嘉義分校
政府單位	屏東縣政府；海洋生物博物館
軍方單位	國防大學

98年硬體式台灣銀行第六組項次-1

共同供應契約 (LP5-980056-1) - Curelan(洽科資訊)價格(含稅)

組別	項次	品 名	廠牌	型號	產地	契約單價
六	83	網路行為安全政策管控及 隔離設備500個終端電 腦網路存取控制設備	Curelan	IPMS-550U	台灣	\$287,846
六	84	網路行為安全政策管控及 隔離設備1000個終端 電腦網路存取控制設 備	Curelan	IPMS-1050U	台灣	\$458,422

98年硬體式台灣銀行第六組項次-2

共同供應契約 (LP5-980056-1) - Curelan(治科資訊)價格(含稅)

組別	項次	品 名	廠牌	型號	產地	契約單價
六	85	網路行為安全政策管控及隔離設備2000個終端電腦網路存取控制設備	Curelan	IPMS-2000U	台灣	\$671,642
六	86	網路行為安全政策管控及隔離設備2500個終端電腦網路存取控制設備	Curelan	IPMS-3000U	台灣	\$703,625
六	87	網路行為安全政策管控及隔離設備3000個終端電腦網路存取控制設備	Curelan	IPMS-5000U	台灣	\$1,332,623

總 結

- 本設備之二段式認證授權可達成自動，使用者姓名 + IP + MAC相互綁定功能。
- 搭配 L 3 Switch的Arp Inspection及DHCP Snooping和DHCP Relay功能，才能完全做到IP + MAC功能而沒有漏洞。
- 運用IP Spoofing功能所開的系統，會受到L 3 Switch的Arp Table表Recover時間(一般都是5分鐘)的漏洞，使IP + MAC功能產品產生漏洞。
- IP Spoofing功能也會受到Netcut(剪刀手)及ARP Spoof病毒攻擊 (ARP Poison)，而產生IP + MAC功能之漏洞。