

## 自動化網路安全與管理(UPM)

---

### UPM (Universal Port Management)

#### 前言

對於 IT 管理人員而言，網路架構中 Configuration 設定變動最頻繁與連接終端設備種類最多樣的應該是 edge switch 設備，設定變動狀況譬如重新劃分 IP 網址、調整部門位置或者新增或移動 PC、IP 話機、無線 AP、網路攝影機、印表機的位置....等等。而且其連接的終端設備種類也多樣化了，包含電腦、IP 話機、無線 AP、網路印表機、攝影機等，未來更會與日俱增。

每種設備都會有不同的網路設定，若要作移動就很麻煩。針對上述的需求，管理者必須改變或新增現有 Edge 交換器的設定，譬如重新劃分或變更 VLAN 的設定、新增或變更安全性的政策 (policy)、針對網路電話及網路攝影機可能還需要做 QoS 調整設定等，這些全是耗費人力的工作，而且一直沒有一勞永逸的方法！IT 管理人員一想到就頭痛，不是嗎？

#### 問題在哪裡

在一般的狀況下，通常我們會在交換器上預設好每一埠相關的設定，我們舉個實例來看看，有一台放在 R&D 部門的交換器，有 4 個 VoIP 話機，所以會將前 4 個埠作為語音 VLAN 使用，其餘的埠屬於 RD 部門的 VLAN 以連接電腦或主機，另外還會使用 ACL 以限制重要資料的存取。管理者常會面對的需求或問題如下：

- 需要移動 IP 話機至其他座位的資訊插座
- 需要新增第五台 IP 話機到 R&D 部門
- 需要新建或新增 wireless access AP
- 其它部門的使用者使用到 R&D 部門的資訊插座，可能無法使用網路或造成 R&D 資料外洩的危機

- RD 人員到其它部門或不同辦公樓層時需要存取 RD 部門的資料

這些狀況往往讓 IT 部門管理者頭痛萬分，網路的管理性、移動性、安全性往往無法同時兼得。到底有沒有簡單又方便的方法達到上述需求呢？這將是未來網路設備功能的主要趨勢！而 Extreme Network 就首先創新開發了 UPM (Universal Port Management) 的概念來解決這些需求與問題，讓我們來介紹一下這個概念。

## 解決之道

從以往的經驗來看，上述的需求及問題每次都需要靠人力來處理及設定，或者很難解決與太麻煩而放棄修改與變動。為了滿足上述多種需求並簡化設定上的程序，Extreme Networks 提出自動化網路安全與管理方案 – UPM (Universal Port Management)，UPM 的管理非常簡單，IT 人員可在網路交換器上或透過網管系統事先建立不同類型的使用者或設備的隨身 Policy，當設備連接上線或使用者認證時將自動觸發事件並自動將隨身 Policy 設定到該設備或使用者所連接的埠上，其中過程不需任何人工的介入，以達到全自動化的安全與管理的目的，並且減少人為介入的大意誤失。我們將 UPM 所帶來的好處說明如下：

### 1). 需要移動 IP 話機至其他座位的資訊插座：

傳統上，話音連接埠皆是設定好固定住，例如每部網路交換器前 4 個埠保留給 IP 話機用。但若要變換 IP 話機的連接埠，通常不是不容易找到連接埠可用，就是 IT 人員需要大費周章調整跳線或更改 Voice VLAN 及 QoS 的相關設定，費時費工且容易出錯。

採用 UPM 之後，在設備連接上線時，不論 IP 話機連接在網路的任何一部網路交換器的任何一個連接埠，利用自動找尋設備的業界標準協定(LLDP)或其網路硬體位址(MAC OUI)來辨認 IP 話機，皆會觸發同一個事件而自動完成 IP 話機相關設定。所有網路連接埠皆可靈活運用，再不用受限於特定連接埠的情形。

### 2). 需要新增第五台 IP 話機到 R&D 部門：

此類需求除了要能達成前述自動化處理之外，在如 R&D 部門有更多網路安全性考量的地方，除了要保有 IP 話機的暢通之外，還要注意符合對 R&D 部門的安全性要求，對 IT 人員的設定常是另一大挑戰。

然 UPM 不僅提供自動化的便利性，並且可將 IP 話機同時自動切換到 Voice VLAN 而與原交換器所在的網路完全分離，話機不論連接上哪個部門的設備，依舊僅能連接話機，避免成為另外一個漏洞。

此外還有種情況一定會遇到，在 IP 話機上都有資訊插座可以再接電腦，當兩個設備都連線，兩種訊務同時在同一交換埠傳輸時，UPM 功能可以自動辨認 IP 話機的語音與一般電腦訊務而給與不同 Policy 如 VLAN、QoS、access policy 等不同設定，讓 IP 語音可以不因一般訊務的傳送干擾而降低了通話品質，並保有話機與電腦各自的安全設定。

### **3). 需要新建或新增 wireless access AP：**

UPM 可將 wireless AP 自動劃分至 Wireless VLAN，雖然現在的 wireless LAN 的解決方案已可透過 DHCP 及/或搭配 DNS 的設定自動連結至 wireless controller，但是如果可以自動將 wireless AP 劃分至 Wireless VLAN，將可以更簡化 AP 搜尋 AP 控制器的設定程序。取決於 wireless 的架構及應用，設定上可能需要提供獨立的 Wireless VLAN 以及 QoS、認證及安全性的設定

### **4). 其它部門的使用者使用到 R&D 部門的資訊插座，可能無法使用網路或造成 R&D 資料外洩的危機：**

對於員工在 R&D 部門內部開跨部門會議為例，因成員皆為員工，認證通過後便可連通，非 R&D 員工的會議成員便可連通 R&D 部門。所以部份公司的政策是全面禁止其他部門人員使用 R&D 部門網路，但這造成了使用上的不便；部份公司則被要求開放 R&D 部門的網路使用權，而喪失了 R&D 部門的安全性。

UPM 則提供一套政策跟隨的能力。不論是任何員工要到 R&D 內部使用網路，皆被限制在該員在原辦公室的權限，包括其限制及可連線到的網路資源，除了保障 R&D 部門的網路安全之外，也提供了其他部門員工的使用便利性。

### **5). RD 人員到其它部門或不同辦公樓層時需要存取 RD 部門的資料：**

若是 R&D 部門員工至其他部門開會，在配合使用者認證或鎖 MAC 位址的安全設定下，跨部門可能無法使用網路資源包括基本的上網及收發電子郵件

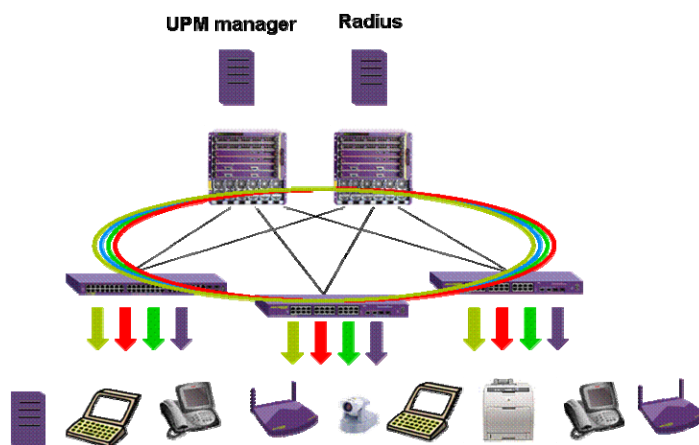
件或是無法存取 R&D 部門內的資料！或是 R&D 人員在其他部門得使用 VPN 連回 R&D 內部取得資料，甚為繁鎖且需另管理 VPN。

透過 UPM 的自動管理機制，不管 RD 或其他部門人員，連上內部網路的任何位置，該網路埠將會自動設定為 R&D 或業務部門的 VLAN，再加上自動配置的 ACL 設定，輕易的就可解決移動式內部網路存取並兼具安全控制的需求，除此之外還可以提供稽核及簡化網路存取政策的控制，因為不管該移動設備接上內部網路的任何位置，透過 DHCP 的控制一定會取得固定的 IP 位址！

## 結語

UPM 的概念無疑的將兼顧內部網路的移動性以及加強存取控制及提升網路的安全性，當然更重要的還可以透過集中式的政策性控管，簡化了設定變動頻繁及多樣化設備連接的 edge 交換器的設定工作，必可化解日益增加的網路應用所帶給 IT 管理人員的負擔。經由 UPM 的技術可以同時滿足移動性、安全性、管理性三項 IT 的需求，如此亦將成為網路設備未來功能發展的趨勢！而 Extreme Networks 正是這種創新發展的先趨。

## 技術說明



圖一：從任何地點接上網路，設定隨時跟著設備或人員移動

UPM Policy 的內容可以是網路交換器的任何指令，譬如：VLAN、QoS、ACL、傳送 802.1AB (LLDP+LLDP-MED 業界標準之自動找尋設備的協定)資料，這些

設定會跟著使用者或者設備移動，不管使用者或者設備接在內部網路任何交換埠上，以實現真正的移動性(Mobility)並兼具 QoS 及安全控管。

觸發 Policy 執行的條件包含時間、使用者名稱、MAC 或者 LLDP (Link Layer Discovery Protocol)，因此針對上述的問題 1、2 可以採用 LLDP 的方式，一但 IP 話機接上網路交換器之任一埠，透過 LLDP 的協定交換器即可辨識其為 IP 話機，進而自動將該埠設定為 Voice VLAN，除了加上 QoS 的設定外並可透過 LLDP-MED 告知 IP 話機 Call Server、File Server、ECS(E911)的位址，讓 IP 話機可以迅速連接使用。問題 3 可採取 LLDP 或者 MAC 認證的方式觸發 UPM，將 wireless AP 自動劃分至 Wireless VLAN。對於最困難的問題 4、5，透過 UPM 的自動管理機制加上使用者認證機制可知登入網路的使用者身份，因而給予個人化的差異性服務。