

## 內網安全新境界(一)

---

### 『簡化 IP 管控』與『端點安檢防護』方案

#### 前言

IT 管理人員平日在執行 IP 管控時，常會遇到管理上的困難。這些困難大半來自於端點使用者不了解 IP 網路，或為了使用上的方便或是意圖要達成非法目的，這些使用者會變更端點的網路設定，但卻有意無意造成整體網路的問題，像是影響其他使用者網路無法連通等，因而降低整體生產力。更麻煩的是這些問題在現有的網路設備下很不容易快速查修。

#### 問題在哪裡

IT 管理人員可能需要花上半天到一整天的工作時間來處理下列其中任一項問題，例如某一使用者有下列其中一個問題回報狀況，IT 人員在沒有任何提示下，通常得對使用者網路連接線、資訊插座、連接的網路交換器、網路流量使用率、電腦主機軟硬體狀況等逐一查察，在一般人力資源不足的 IT 部門而言，無異雪上加霜。

常見的 IP 問題如下列所述：

- IP 位址衝突或冒用
- 現有固定 IP 機制不易管理
- Gateway IP 位址被誤用或冒用
- 私設 DHCP Server
- 使用者認證執行困難

## 解決之道

新一代的網路交換器針對前述這些問題應該要能提供具備完整的解決方案的 IP-Security，儘可能從異常來源端直接避免其發生，以期使 IT 管理人員能花費最少的時間及人力來解決這些日常管理面上時常發生、但又不易快速解決的惱人問題，而把資源放在更重的工作上。在今日 IT 人員日益精簡的狀況下，具備這類 IP 控管能力的網路便相對愈發重要。

針對各項 IT 人員常見的惱人問題，若在交換器上直接提供了完整的 IP-Security 解決方案，IT 人員便不需要再大費周章布建其他外加的管理系統。外加系統通常需要與特定的設備供應商搭配，無形中也造成日後擴充的限制性。若能利用廣為一般各型企業網路使用的架構，而且是業界的標準協定來達成 IP 管控能力，如此將解決方案實際導入內部網路所造成的影響便能降至最低、日後擴充亦無虞被單一供應商限制。

對常見的 IP 管控問題，分項說明如下

### 1). IP 位址衝突或冒用

問題來源通常可分為下列兩方面：

- 使用者會自行修改 IP 導致 IP 衝突
- 惡意程式(如網路蠕蟲或病毒)冒用他人 IP 位址攻擊

不論是有心或無意發生上述狀況，IT 人員接到使用者網路無法連通的申告，都難以追查實際到底是哪位使用者造成的。

早期 DHCP 開發的目的便是為了降低管 IP 位址的負荷，但 DHCP 不具備強制性，若使用者意欲自行更改 IP 位址，管理人員毫無辦法。故一般 IT 管理者的解決方式不外乎就是使用固定 IP 與 MAC 位址的方式，並手動在交換器中鎖定其 IP/MAC 的資料，使端點使用者自行變更 IP 後無法連通。但這需要大量 IT 人力介入，或是搭配專屬系統處理，使用彈性大大降低。在第 2 點問題中對此再詳述。

此時考慮採用具備自動配發端點 IP 位址後**自動鎖定** (DHCP Enforcement) 功能的交換器，則可強制端點必須使用自動配發的 IP 位址方可連通網路。除發揮 DHCP 的 IP 集中管理的特性，亦達成如同固定 IP 位址般的 IP 管控鎖定。若使用者仍意欲強行自行更改 IP 位址，則交換器將使其完全無法連

通網路，以達 IP 管控的基本要求。同時 IT 管理者可集中在 DHCP Server 管理與設定，無需在每部交換器上手動鎖定固定 IP/MAC。對日後 IP 位址的追蹤甚至稽核，皆易如反掌。

## 2). 現有固定 IP 機制不易管理：

前述問題 1 提及使用固定 IP 是現行部份 IT 人員管控使用者使用 IP 位址的方式，但確仍有下列問題：

- Switch 固定 IP 位址表數量有限，無法涵蓋全部端點數量
- 每部 switch 均需設定固定 IP 位址表，費時費工
- 限制端點只能連接固定的 port 或區域，缺乏端點移動機能

在現行企業愈來愈多提供筆記型電腦與無線網路存取的今日，固定 IP 的方式顯得完全跟不上對移動上網需求的腳步。具備 DHCP Enforcement 解決方案的交換器將移動上網與 IP 管控完美的結合，不論使用者從何處連通網路，皆可自動取得 IP 而交換器亦同時鎖定其 IP 位址，讓 IT 人員更能輕鬆導入其他移動上網的解決方案，同時做好 IP 管理。

## 3). Gateway IP 位址被誤用或冒用：

問題來源類似 IP 相衝突，但若使用者自行更改 IP 位置與 Gateway 的 IP 相同時，影響的範圍更大，並且更危險，因為

- 錯設端點 IP 與 gateway IP 相同，造成該網段全部無法連通
- 中間人(Man-in-the-middle)可側錄竊取其他同網段端點訊務資料，包括金融帳號、密碼及其他機密或敏感性資料等

交換器若是具備自動偵測及通報功能，則能全時監控是否有此類狀況發生，IT 人員可在第一時間被通知且交換器會主動嘗試修復異常狀況使網路回復正常狀況。最佳的狀況，交換器應有下列功能

- 自動偵測此一狀況並主動通知管理者
- 自動發送正確資料(ARP)覆蓋攻擊者的誤導資料
- 將攻擊者列入黑名單，阻絕其連通網路

#### 4). 私設 DHCP server

另外常見的 IP 位址配發問題則來自於網路設備的大眾化，今日使用者很容易在商場買到 IP 分享器或無線 AP 而自行連接進企業網路，有心或無意讓其內建 DHCP Server 配發非企業內部使用的 IP 造成其他使用者無法連通網路。

在導入自動配發 IP (DHCP) 的網路環境內，交換器亦需供自動化機制解決此一問題發生，以確保網路連通的順暢。除了自動偵測使用者私設之 DHCP Server 及即時通知管理者此一事件的發生外，能自動隔離該私設 DHCP Server 的網路連結，使其不再干擾其他使用者則更佳。

#### 5). 使用者認證執行困難

現行乙太網路的標準中，對內部網路使用者認證的做法只有一種，即 IEEE 802.1x port based 認證。此認證方式需要所有網路端點及交換器皆具備此一功能才可執行，對大部份年限未到的老舊設備，在無法汰換又升級無門的情況下，實難以導入。

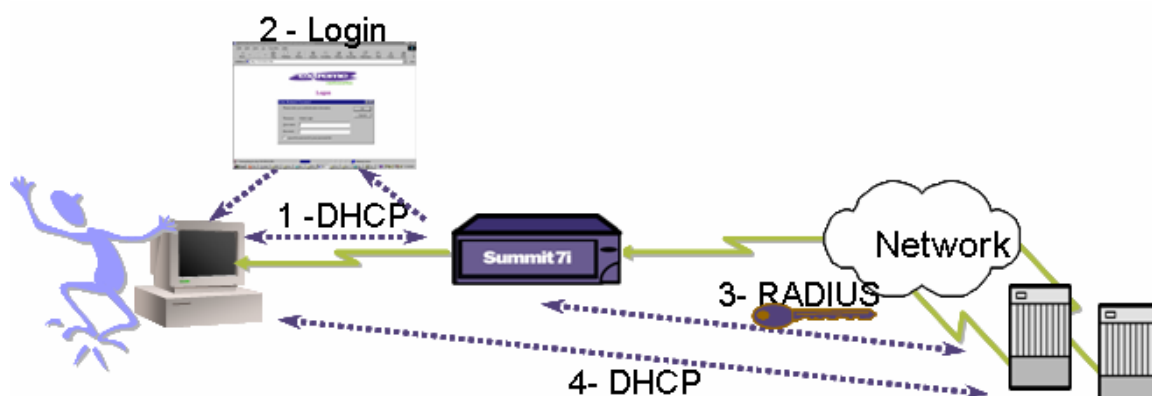
另外此認證方式以交換器實體連接介面埠為單位，若有一個使用者認證通過，則連接介面完全打通。當該介面下接一般舊型交換器或無線 AP 時，則無法驗證多個使用者，因為一人通過，其餘使用者皆可上線。更甚者，對 IT 人力吃緊的企業，主機端需要整合憑證作業，大規模的網路變動，造成管理者額外負擔。

而網頁瀏覽器(Web Browser)則幾乎是大部份端點作業系統都具備的工具，且已廣為無線網路認證機制所採用。若交換器也具有此一功能，則不論端點設備是否具備 802.1x，皆可利用 Web 介面提供認證能力。所以在導入使用者認證機制時 IT 人員應該注意下列幾件事：

- 支援 802.1x 的交換器要能對接入的使用者個別認證：所以不論其下接傳統交換器或是無線基地台，仍可對個別使用者分別認證，不再有企業全部交換器或無線 AP 都需支援 .1x 的限制，原有的設備仍可延用。
- 採用 Web 介面的認證方式：此法可突破不能安裝 802.1x 的電腦端點的問題，而以 Web Browser 作認證。今日無線網路以瀏覽器認證的方式已

頗為風行，故無需再教育使用者，縮短學習曲線。

- 對於如網路印表機或是網路攝影機等不能安裝 802.1x 及無瀏覽器的設備，另需以網路硬體位置認證 (MAC RADIUS) 的功能讓這類設備以 MAC address 做為認證依據使其連通網路。



## 展望

當自動發放 IP 又具備 IP 管控的方案是可行的時候，除了 IT 人員不再煩惱追蹤不到 IP 的窘境外，亦可以在此一平台上發展更深入的內部網路安全管控能力，例如掃瞄網路端點安全狀況的方案 (NAC)，協助 NAC 隔離不安全的使用者。在下一期的文章中對此有更進一步的說明。

## 進階學習

### 1. DHCP Enforcement

Extreme Networks 交換器提供 DHCP Snooping 的功能，在使用者自動取得 IP 位址的同時，記錄下該 DHCP 資訊內使用者所使用的 IP 位址、MAC 硬體位址、及使用的連接埠，並全自動的記錄在交換器內的表格中。當使用者嘗試使用不是系統自動配發的 IP 時，該使用者則完全接收不到資訊，形同網路斷線。但對惡意使用者而言，該使用者仍能往網路上倒垃圾癱瘓網路連通或散發單向病毒。

### 2. Source IP Guard & ARP Validation

當使用者嘗試使用不是系統自動配發的 IP 位址時，Source IP Guard 及 ARP Validation 會更進一步將該封包丟棄，讓該使用者的資料完全無法送進網路或往網路上倒任何資訊。ARP Validation 並會偵測到此一行為而告警管理者。

### **3. Trusted DHCP Server**

Extreme Networks 交換器能全時偵測是否有非 IT 部門管控的 DHCP Server 在內部網路上啟動，若偵測到此一狀況則通知 IT 人員。交換器亦提供自動隔離功能，若管理者啟動此功能，交換器將自動隔離該端點於網路之外。

### **4. Gratuitous ARP Protection**

Extreme Networks 交換器具備偵測使用者誤設或冒用 Gateway IP 位址的功能，並可將正確的 Gateway 連通資訊重新發送給每一網路端點，以嘗試修復網路連線。同時告警 IT 人員。管理者亦可啟動自動化隔離功能，將該使用者端隔離於網路之外。

各位企業管理者，你們的行動呢？