IT資源管理與網路安全防護系統

管理與控制 IP 位址，從困難變容易！

- **問題背景**

乙太網路 IP 與 MAC 位址之設計僅針對使用效能之改善，並未完善的考量管理與安全層面。且隨著網路資訊系統之進步與廣泛使用，直接或間接導致的資安問題更是不勝枚舉。

您平日於執行 IP 管控時，常遇到管理上困難。而困難大半來自於使用者不了解或不熟悉 IP 網路，為使用上方便或意圖達成非法目的，使用者自行變更端點之網路設定，卻造成整體網路問題，像是影響其它使用者網路無法連通等，因而降低整體生產力，而這些問題在現有的網路設備下並不容易快速查修。

為因應網路不斷增加的 IP 用戶數，網路規模一直不斷地進行擴充及迅速升級。尤其對大型企業和機構來說，幾乎無法採取中央管理的方式分配與追蹤 IP 位址。對於終端用戶 IP 的管理，不僅曠日費時，並且勞心勞神。

目前多數企業本於對資訊安全的瞭解與重視，對於應用系統、連外防火牆及病毒防範等均耗費巨資進行防護。然而，面臨網路基礎之 IP / MAC 層面，卻因無適當的解決方案，或使用複雜昂貴之管理方案、又或採用人工及暫時之處理手段，甚或視 IP / MAC 層面之問題為理所當然，使公司企業陷於網路安全控制與管理之問題根本中。

IT 資源管理與網路安全防護系統 — 為您，帶來優勢！

- **即時透視網路、解決問題**

-提供互動式，視覺化資安儀表板，讓管理者能夠快速掌握內網即時資安事件。

-提供網路資安事件日報表、月報表、季報表、年報表、圖表、IP 衝突報表、違反資安政策被阻止事件報表等，提升管理能力的最佳途徑。

IT 資源管理與網路安全防護系統— 給您的強大功能！

- **智慧存取控制**

能幫助企業掌握建立智慧存取控制方案的能力，讓您管理整個網路的中央政策並連續記錄歷史資料，如此您便足以向任何法令遵循機構或稽核機關證明自己擁有定義清楚及具有執行力的網路存取政策。

- **減少 IP 衝突**

根據 Forrester Research 的調查結果，在整體企業發生應用系統斷線的事件當中，有 15%是因網路問題而造成的，而大部份發生網路斷線的根本原因，是因為 IP 分配位址發生問題。藉由本系統減少位址衝突問題，可避免使用者遭遇令人氣沮的網路斷線事件和重要伺服器離線。

- **完整無縫整合**

以 ARP 為基礎的執行功能可控制網路邊界的存取，因此能夠充分配合 IP 網路佈署的結構原理。如此簡單而完善的架構使本系統解決方案具有操作簡易的特點，並讓它得以和其它網路元件進行無縫整合。

- **簡便低廉快速**

無須增加安裝及維護客戶軟體費用的情況下，便能取得更具重大意義的網路控制權。於此，表示使用者不須額外訓練，您也無須另外承擔更多工作。

除此之外，本系統能幫助 IT 部門整合有線與無線裝置的存取控制流程，因此能進一步減少開支。若組織將伺服器斷線和內部安全遭到入侵的成本列入考量，上述這些利益將能幫助組織快速回收投資。

- **IPv6 資訊**

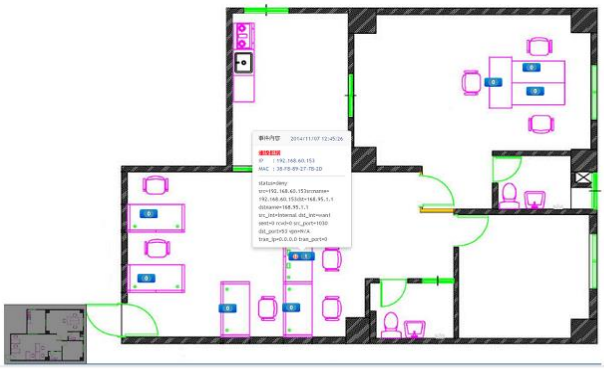
近來 IPv6 的網路環境已逐步成形，許多機關已開始推行 IPv6 的管理。而本系統也支援了 IPv6 ＆ IPv4 並行的網路架構，管理者可直接在管理介面上，進行 IPv4、IPv6、MAC 三方資訊的參照，且公司不須再為將來 IPv6 的網路管理再額外付出設備成本。

- **完善 IT 資源管理與網路安全防護**

本系統能即時執行網路的存取和控制，包括政策組態設定、網路監控、即時導入、完整的路徑稽核功能等。為 IT 組織大幅提升內部網路的控管能力，以符合沙賓法案規範及 COBIT 指導架構。

主機檢視及事件檢視中，輕鬆查詢主機在哪一樓層、哪個位置(需客製)。

平面圖檢視中，隨點隨看各位置電腦的 IP、MAC、使用者。



快速了解事件內容

透過室內平面配置圖立即得知事件
所發生的電腦位置以及對象資訊詳細內容。

• 功能規格

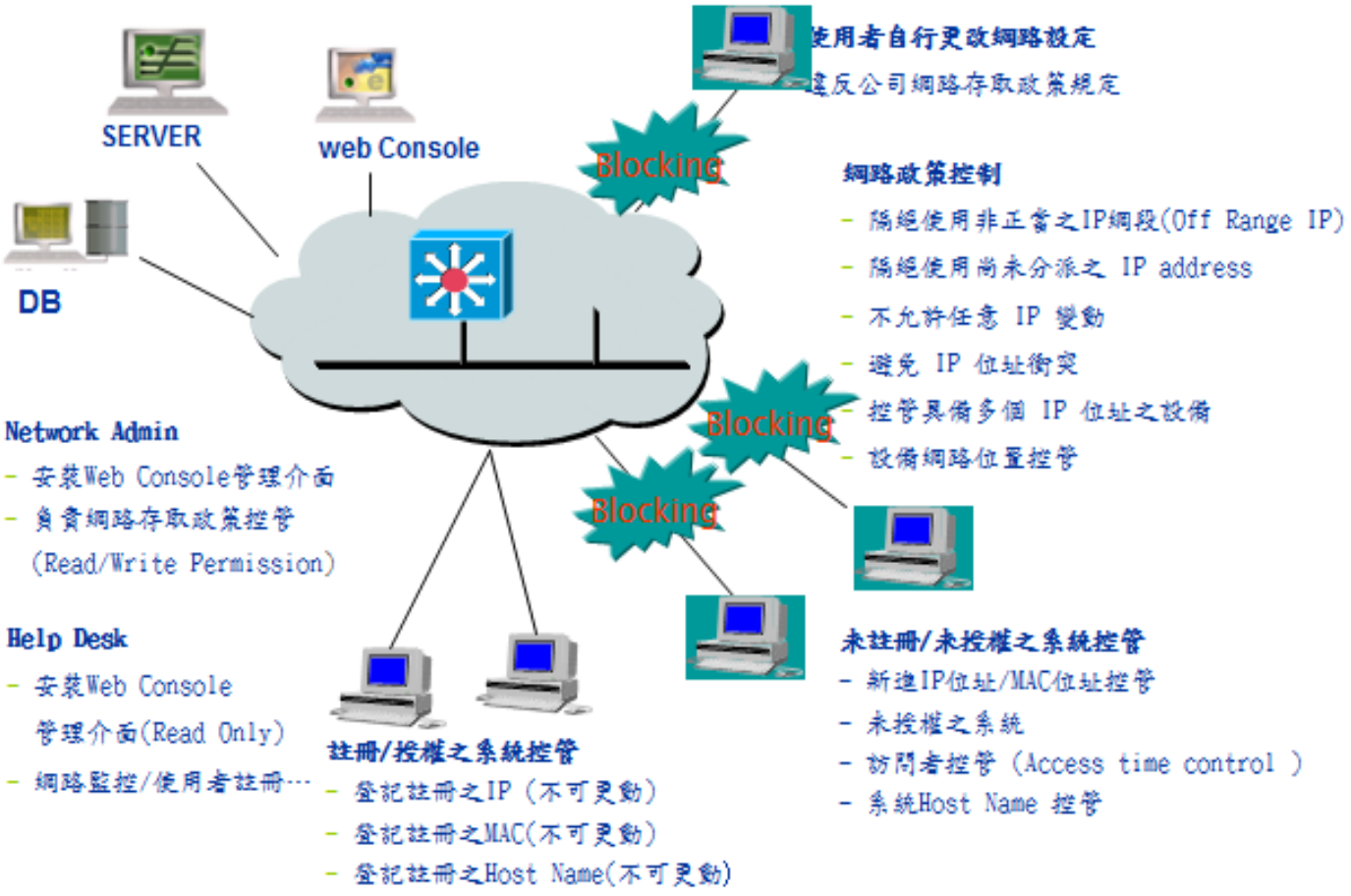
1. 完整即時 IP 資訊，可查看上線、離線、已授權、未授權、系統封鎖、衝突等主機資訊
2. 主機資訊包含 IP、IPv6、MAC、電腦名稱、網卡廠牌、連接交換器、連接埠、事件狀態、最後上線離線時間、及自定擴充欄位資料等
3. 自動偵測使用中 IPv6 Address
4. 提供授權、非授權 IP 及 MAC 相關資訊
5. 自動偵測網路中電腦網卡 NIC 廠牌
6. 即時管理及封鎖 XP、Windows 7、Windows Server、Linux、MAC OS 等電腦設備；即時管理及封鎖 Android、iOS、Windows Phone 等行動設備
7. 自動禁止使用未授權 IP / MAC 位址
8. 自動禁止超出管理範圍 IP 位址使用
9. 未授權設備同時封鎖 IPv4 及 IPv6 位址
10. 可原地即時於網路第二層封鎖 IP、MAC
11. 提供 IP 保護、禁止變更 IP、IP 封鎖、MAC 封鎖的批次設定功能
12. 封鎖未授權電腦時以網頁進行封鎖通知，管理者可編輯通知訊息之內容
13. 封鎖未授權電腦時，透過申請網頁提供使用者以 AD (Active Directory) 帳號驗證授權
14. 預先註冊 IP 或 MAC 使用
15. IP 保護，僅允許指定電腦使用被保護的 IP，非指定的電腦使用則會遭到封鎖
16. 禁止變更 IP，限制電腦僅能使用指定 IP
17. 支援管理員命令封鎖指定 IP、MAC
18. 自動偵測廣撥封包量超出使用者限制的設備，並可進行封鎖
19. 經由 SNMP 整合 Switch 資訊，可自動辨識 Link Port 並自動排除重覆無意義資料，以自動正確取得用戶接入的 Switch 及 Port
20. 可查看所管理 Switch 的 Port 列表，可查看連接在特定 Port 上的 MAC，並提示有多 MAC 連接的 Port
21. 自動偵測網路中的 DHCP 服務，警示未授權的 DHCP Server 並可進行封鎖
22. 即時事件顯示，即時監控是否發生管理者定義之重要事件
23. 完整事件記錄，包含使用者管理日誌、IP 與 MAC 狀態記錄、政策執行記錄等
24. 完整事件檢索，可依指定類型、日期區間、網段及其它指定欄位資料檢索報告，並匯出成 Excel 試算表
25. 訂閱事件自動以信件通報管理者
26. 使用者自訂擴充欄位，可依 IP 或 MAC 匯入整合相關資訊
27. 分層授權管理，開放多管理者使用。每個管理者可依各網段指派適當權限
28. 友善的 Web 管理介面，管理者無須另行安裝管理程式
29. 主機政策設定、授權 IP/MAC 等重要系統資料提供匯入、匯出功能
30. 系統健康狀態資訊，顯示系統服務及 Probe 運作狀態、管理 Switch 是否回應、及資料庫使用量。
31. 支援 802.1Q 以管理多 VLAN 網段
32. 支援 Static、DHCP 或兩種混雜的網路環境使用
33. 側接式的系統架構，無須更動既有網路環境，亦無單點脆弱的疑慮
34. 支援監看模式，有利無風險導入及利於管理者熟悉系統
35. 全面管理網段用戶，用戶端不須安裝或執行任何程式
36. 提供 Web Service API，可執行 IP 及 MAC 授權、IP/MAC 對應綁定等管理工作。
37. 系統支援安裝於虛擬機環境（VMWare）

IT 資源管理與網路安全防護系統— 完善的架構！

- **架構說明**

  系統由 Server (NAC Policy Server)及 DB 兩部份組成。組織中僅需佈署一台 Server，負責提供政策分派、資料庫連線及中央集中式 Web 主控台介面。

  其中資料庫可安裝於同一實體主機或分散架構。



飛幕科技有限公司

台北市中正區北平東路 28 號 6 樓之 1

Tel：(02)2391-2961　Fax：(02)2391-3017

Web：www.maxpower.com.tw