嘉義縣政府「電腦網路連線安全認證系統」介紹

壹、前言

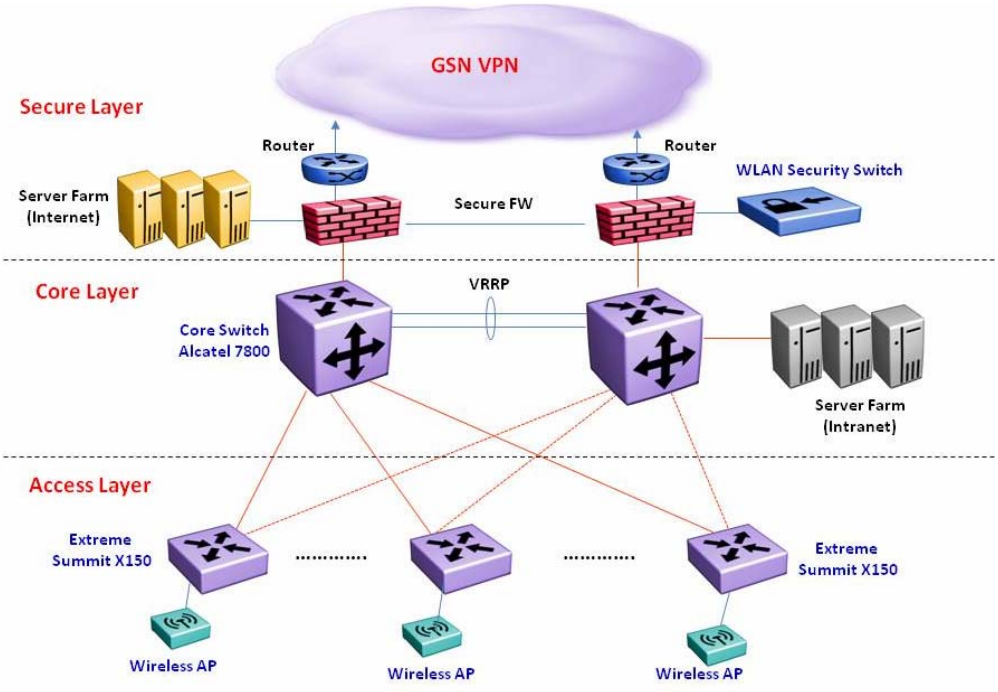
政府機關資訊數位化與寬頻化是一股無法阻擋的潮流，從近年來資訊軟、硬體及網路的蓬勃發展，我們可以充分了解到 21 世紀必有一股無法抵擋的數位化與寬頻化熱潮。為達成『人人用電腦，處處上網路』的目標，嘉義縣政府(以下簡稱本府)積極打造全新整體 e 化環境，使高度的資訊化及數位化進入到每一個同仁的工作環境。

本府現有的骨幹網路建設，早已將原有主幹傳輸容量提昇至 Gigabits 之速度，並充分提供本府資訊數位化，加上全府無線網路的輔助，突破時間、空間、距離等的限制，達到處處是辦公室、時時可上網的理念，讓全府內的數位資訊隨手可得。

當本府積極地將一項項重要的組織流程與相關資訊電子化、網路化之際，資訊安全的控管便成為非常重要的工作，面對盤根錯節的組織架構以及複雜的內外部作業關係，此時對存取系統以執行組織流程或擷取資訊的人來說，其身份的確認、權限的控管、與作業流程的記錄就成為維繫本府自動化體系正常運作不致崩解的必要條件，而這些身份確認、權限控管、系統記錄都必須在不影響既有流程順暢運作的前提下進行。內部網路身分認證的建置過程同時整合本府多項已經上線使用的資訊系統，以期使本府同仁能使用一組帳號密碼即可安全通行本府內部網路及各項資訊管理系統。

貳、系統簡介

本府電腦網路區分成有線網路與無線網路兩大區塊。有線網路部份又區分為內部骨幹網路及對外防火牆二部份，內部網路採用雙層式網路架構設計，第一層為骨幹交換器（Core Switch），第二層為邊際交換器(Edge switch)，架構概圖如下圖：



為提供一個府內高穩定性的運作環境，骨幹交換器由二部 Alcatel OmniSwitch 7800 Layer 2/3/4 Switch 組成高可用性(HA)架構，運用 VRRP(Virtual Router Redundancy Protocol)技術，使彼此除互做為備援外也做資料分流使用，以減輕骨幹交換器上資料流的承載。

每個辦公室群組對骨幹網路的邊際交換器均由 Extreme Summit X150-24T Layer 2 Switch 負責有線網路安全認證(802.1X)的驗證工作，每部邊際交換器並由二對光纖線路 UP Link 分別接至雙核心交換器，用以確保垂直骨幹傳輸的穩定性，並能提供高達 2GBPS 頻寬(IP Trunk)。

有關系統安全性的部份，骨幹交換器與邊際交換器均可提供 Mac Address 過濾功能，用以防止非法使用者入侵內部網路；並結合提供使用者認證機制功能(802.1x)，以加強網路上安全控管，使用者需經認證後方得進入內部網路，使用網路資源。骨幹交換器提供 ACL（Access Control List）指令列權限設定功能，加強安全管理機制。

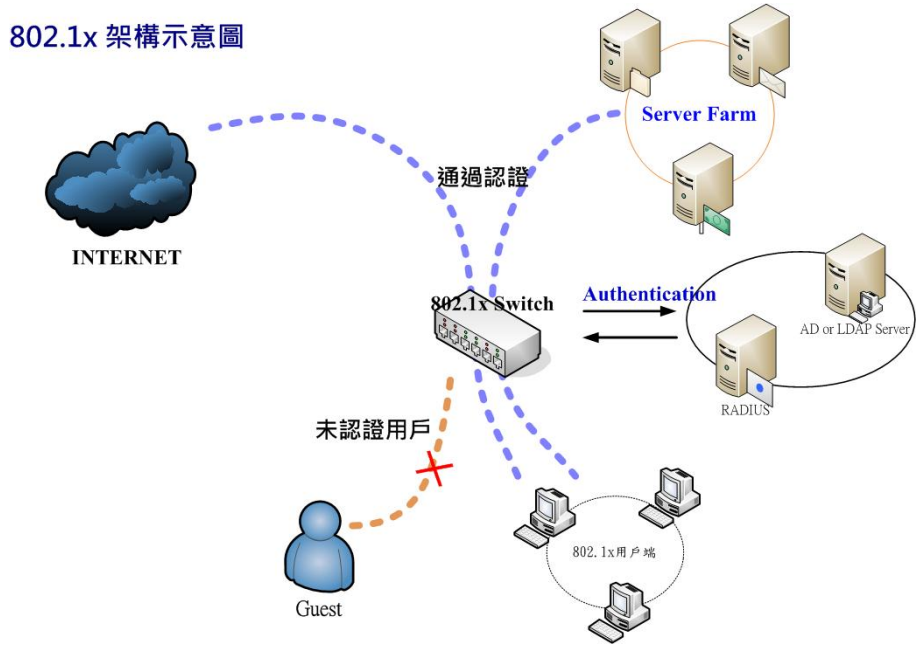
網路管理的部份有整合式的網管平台，包括 What's up Gold 監控、OmniVista 2000 交換器設備管理軟體、MRTG 網路流量分析軟體、網路認證軟體及 Identity Manager 角色區分網路存取控制機制..等，使網管人員擁有一個主動、積極的網路管理解決方案。

參、網路系統管制機制

本府網路系統安全管制機制採用使用者認證方式（User Authentication）作為網路安全的保護。所謂的使用者認證，亦即是當所有使用者要連上內部網路時，都必須要先輸入一組經過申請並授權的"使用者名稱"及"密碼"，在經過認證伺服器認證核可後，始可連上網路。若是未通過認證，則系統會認定您是一個非法使用者而拒絕連接網路。

本府網路系統安全管制機制採用 L2 Switch 內建的 802.1X 使用者認證管理機制，作為使用者連上本府骨幹網路認證使用，並利用相關網路認證軟體(RADIUS 認證伺服器)以提供使用者認證時與目錄伺服器(AD Server)的完全整合溝通。

以下為 802.1X 使用者認證系統架構及運作流程說明：



在用戶端電腦初開機時與邊際交換器之連結係處於未認證階段，在此階段用戶端電腦僅能執行認證程序無法進行其它網路資源的存取，故未經認證的用戶是處於完全

隔離的狀態，以此確保府內實體網路安全管控。其認證程序如下：

一、當用戶端開機完成，系統會自動發出“開始認證程序”的封包給邊際交換器以啓動認證程序。

二、因爲 802.1x 能夠與網域環境整合做到單一簽入，所以在用戶端於系統登入頁面輸入網域使用者帳號及密碼後，即開始進行網路認證與網域登入程序。

三、邊際交換器在接收到“使用者帳號”與“使用者密碼”後，遂與 Radius Server 進行相關身份及密碼的驗證比對程序。

四、若 Radius Server 確認驗證資料合法，即會將認證結果回覆給邊際交換器，告知該用戶端可進行網路存取，並將該帳號所屬 VLAN 等相關訊息送出。

五、用戶端在允許網路存取後，依序自 DHCP 取得 IP Address 及登入網域。

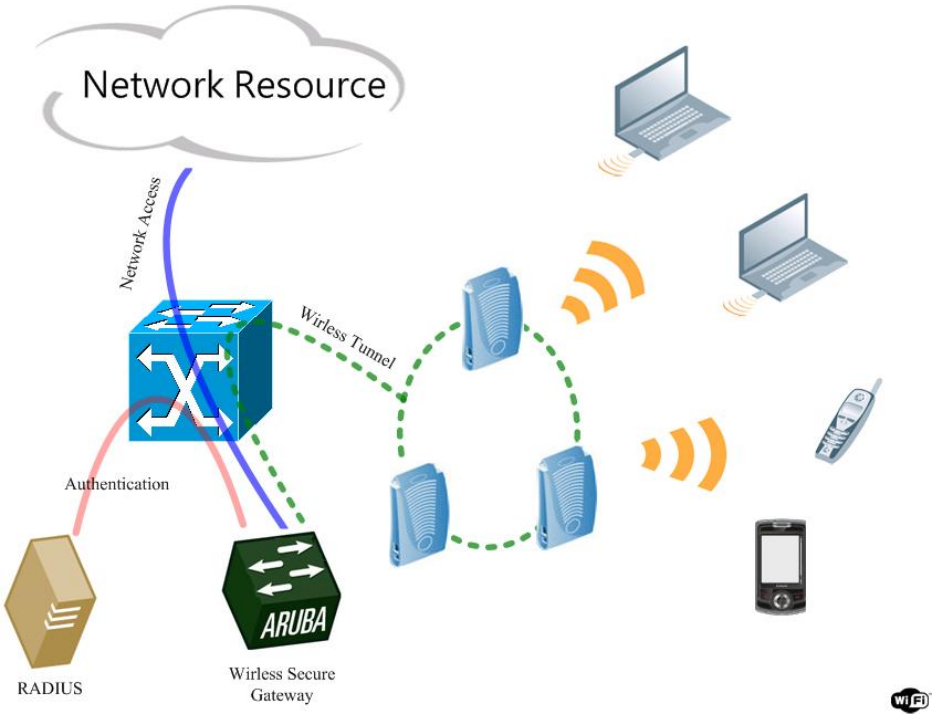
六、邊際交換器會在用戶端完成網路連結後，將用戶帳號、連結埠號、MAC Address、IP Address 等相關資訊傳送至網管系統進行帳戶存取的記錄。

肆、無線網路管控機制

由於無線網路（Wireless Network）近年來逐漸普及，政府單位及企業爲方便行動工作者（Mobile User）存取網路資源，莫不架設無線網路環境，但亦由於無線通訊的便利卻也構成對網路及資訊安全管控上的一大挑戰。

無線網路亦有其相關安全機制，一般常見的安全機制有 WEP、WPA、RC4-128bit 加密、MAC Address Access Filter 等，惟這幾種方法若非安全管控偏寬鬆就是管理不易，在大範圍佈建的環境中尚非屬理想之方式。

本府無線網路系統管控採用 ARUBA Wireless Secure Gateway 無線網路安全閘道器作爲使用者連上無線網路認證使用。



運作流程說明：

用戶端啓動無線網路後即可透過無線網路基地台(Access Point)連接到 ARUBA

Wireless Secure Gateway，並透過 Wireless Secure Gateway 的 DHCP Service 配置用戶端 IP Address，此時用戶端在認證通過前是無法存取任何網路資源。

一、當使用者打開瀏覽器後會先導向 Wireless Secure Gateway 的管控頁面以供使用者輸入“使用者名稱”及“密碼”。

二、Wireless Secure Gateway 在接收到“使用者名稱”及“密碼”資料後，連接至認證伺服器(RADIUS Server)進行驗證程序。

三、RADIUS Server 並將核覆結果回覆給 Wireless Secure Gateway。

四、如果是合法使用者，Wireless Secure Gateway 將依用戶端的權限配置對應策略(Policy)以開放使用網路資源，並記錄 Account、Mac Address、登入及登出時間等相關資訊。

伍、結語：人因網路新概念

如果從使用者使用網路的型態來看，傳統的網路使用方式幾乎都以設備爲導向，而不是以人爲導向。也就是說，若一個使用者可以存取網路，完全是因爲其所使用的設備(如：PC) 與設定可以存取網路；今天若換成另一使用者使用相同的設備，則其會有相同的權限，而對網路與網路管理者而言，會把他們視爲同一使用者。人因網路(Human Oriented Network) 正在改變大家對網路的認知：使用者可以存取網路是因爲你這個使用者，而不是因爲使用了某台 PC。因此！人因網路中所重視的是人而非設備，另言之，即對同一使用者而言，不論其所使用的 PC 爲何人所有、其所在地點爲何，其使用的網路環境都是一樣的。

網路內涵既然是以人爲導向，又如何能將其實作完成呢？簡言之，就是利用虛擬網路(VLAN) 的特性，讓使用者不論使用何 PC 與在何處都可加入同一 VLAN 之中，以取得相同的網路環境。而人因網路的另一個重點在於如何辨別使用者。現階段

本府是採用單一組“使用者帳號”與“密碼”的方式及設備，在其交換器上設計了認證式網路機制(802.1X)，透過 802.1X 中的認證機制，每個群組會有各自的網路屬性，如 IP Range(合法或非法 IP)、QoS、使用時間等，因此網路不再是一視同仁，而是不同群組或個人擁有屬於自己的特性。

（本文由嘉義縣政府研究考核處資訊管理科 提供）