農田水利署

推動管理處三個虛擬區域網路管控
杜絕不明或未經授權設備入侵風險

尹國正

一、計畫背景與目的

為了強化管理處的資訊安全，農業部農田水利署在今(113)年度的資安計畫中，將推動對管理處內三個虛擬區域網路（VLAN）的嚴格管控。計畫重點在於杜絕外來設備隨意連接內部網路並直接上網的情況。具體而言，無論是管理處同仁或外部廠商，均不得逕自使用筆記型電腦等設備直接接入管理處的網路進行上網操作。這項措施的核心目標是提升內部網路的資安水準，避免不明或未經授權的設備帶來潛在的安全風險。

二、為何禁止不認識的設備隨意連接網路？

(一) 設備安全無法確認： 當不明設備直接接入內部網路時，且無法確定該設備是否存在安全隱憂。例如，外來設備可能缺乏防毒軟體保護、使用過時的作業系統，或存在尚未修補的安全漏洞，這些因素都可能對內部網路構成潛在威脅。

(二) 可能遭受惡意程式感染： 若外來設備已感染病毒或惡意程式，在接入內部網路後，這些威脅可能迅速傳播，導致內部系統遭受攻擊，進一步破壞網路安全環境。

(三) 內部網路資安問題： 任意設備連線可能引發一系列資安問題，包括資 料外洩風險和內部網路遭受攻擊的可能性。未經授權的連線可能被利用作為攻擊跳板，直接威脅機密資料的完整性與安全性。

三、如何防止外來設備接入網路？

為了防止外來設備接入網路，臺中管理處將採用ARP Spoofing技術來加強對內部網路的管控。

四、網路中的三個關鍵名詞

在解釋ARP Spoofing之前，先介紹網路中的三種名詞—Domain Name、IP 位址 和 MAC 位址。

(一) Domain Name（域名）： 是用來識別網路上設備的名稱，通常對應於人類容易理解的文字，如：tw.yahoo.com。域名是建立在DNS（域名系統）之上的，將人類可讀的名稱轉換為IP位址。

(二) IP 位址： 每個連接到網路的設備都有一個唯一的IP位址，用來識別設備並進行網路通信。IP位址有兩種版本：

IPv4（如192.168.1.10）和IPv6（如fe80::a00:27ff:fe62:75bd）。

(三) MAC 位址： 每個網路設備都有一個唯一的硬體位址，稱為MAC位址(如00:1A:2B:3C:4D:5E）。這是網路設備在區域網中進行通信時的物理識別碼。

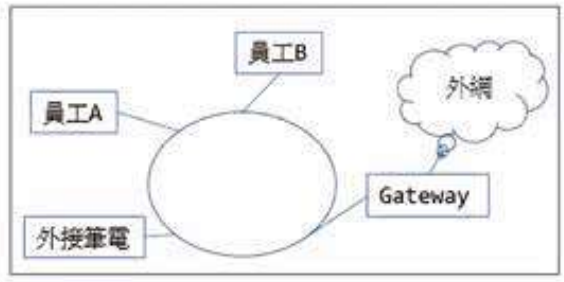
五、ARP Spoofing 原理解析

ARP（Address Resolution Protocol） 是一種用於將網路層的 IP 位址解析為數據鏈路層的 MAC 位址的協定。在正常情況下，當設備需要通訊時，它會通過ARP請求對方的MAC位址。這是一個簡單且高效的協定，但它也有安全隱患，容易被利用來進行攻擊。

圖一是臺中管理處的測試網路環境，各設備的IP和MAC位址如圖二。

各設備接上網路後，運行一段時間便會建立出各自的 arp table，如圖三。每位使用者也可以在電腦命令提示下，輸入 arp -a，顯示該電腦目前的 arp table。

圖一：網路架構圖



圖二：各設備之 IP及MAC位址

編號	設備名稱	IP	MAC
1	員工A	192.168.1.10	AA:AA:AA:AA:AA:AA
2	員工B	192.168.1.20	BB:BB:BB:BB:BB:BB
3	外來筆電	192.168.1.30	CC:CC:CC:CC:CC:CC
4	Gateway	192.168.1.254	DD:DD:DD:DD:DD:DD

圖三：各設備之arp table

員工A arp table

網際網路網址	實體位址
192.168.1.20	BB:BB:BB:BB:BB:BB
192.168.1.30	CC:CC:CC:CC:CC:CC
192.168.1.254	DD:DD:DD:DD:DD:DD

員工B arp table

網際網路網址	實體位址
192.168.1.10	AA:AA:AA:AA:AA:AA
192.168.1.30	CC:CC:CC:CC:CC:CC
192.168.1.254	DD:DD:DD:DD:DD:DD

外來筆電 arp table

網際網路網址	實體位址
192.168.1.10	AA:AA:AA:AA:AA:AA
192.168.1.20	BB:BB:BB:BB:BB:BB
192.168.1.254	DD:DD:DD:DD:DD:DD

Gateway arp table

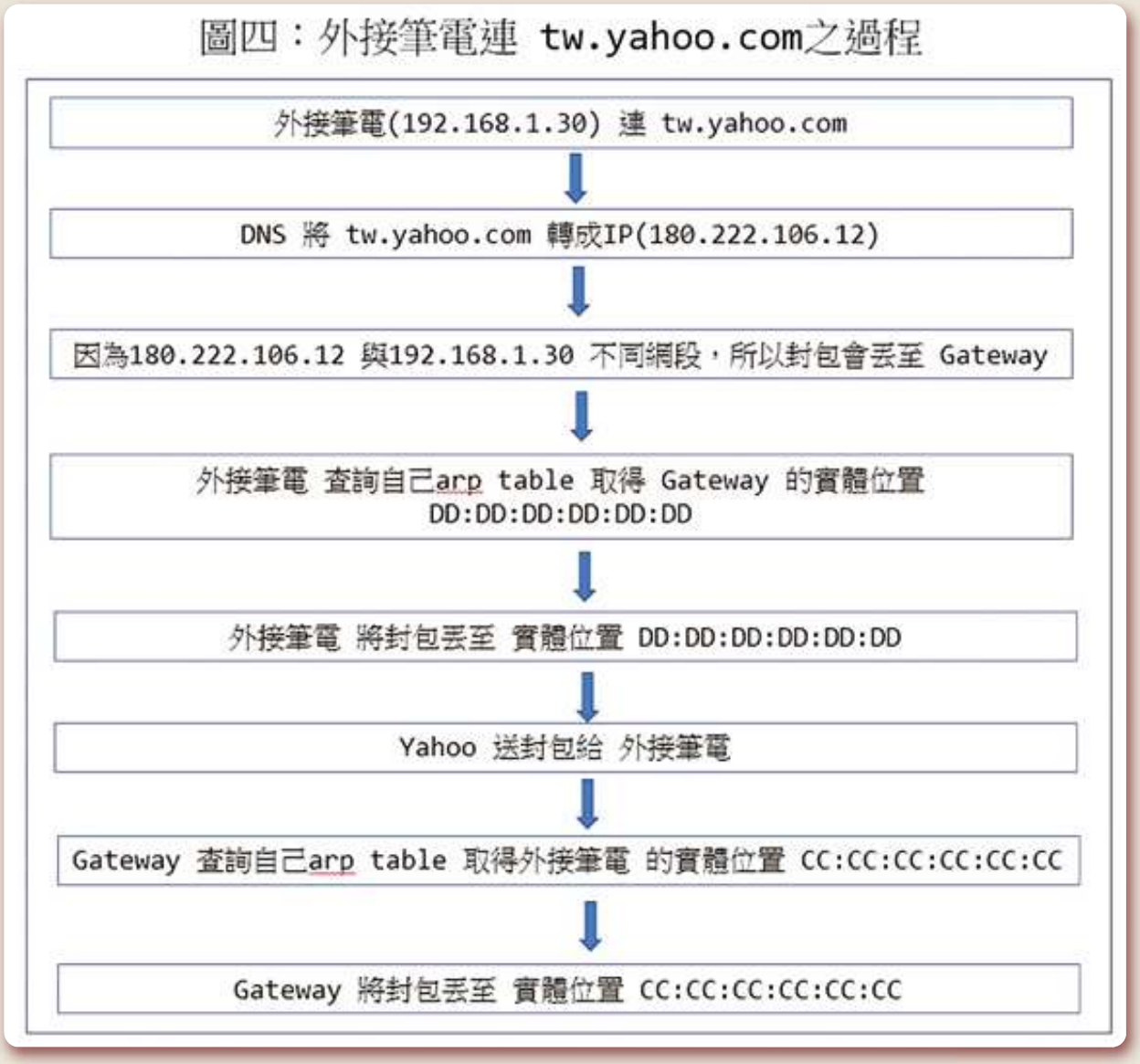
網際網路網址	實體位址
192.168.1.10	AA:AA:AA:AA:AA:AA
192.168.1.20	BB:BB:BB:BB:BB:BB
192.168.1.30	CC:CC:CC:CC:CC:CC

如果外接筆電要連上奇摩網站，它的運行過程如圖四，首先DNS server會先將tw.yahoo.com這個domain name 轉換成 IP (180.222.106.12)。再來，因為外接筆電IP 192.168.1.30 與180.222.106.12 分屬不同網段，所以封包會往Gateway丟。因為要往Gateway 丟，所以要先查詢自身arp table，取得 Gateway 的mac 位置。當奇摩網站回傳資料給外接筆電，Gateway必須先查詢自身arp table，取得外接筆電的mac位址，再將資料往外接筆電丟。

ARP Spoofing 是一種攻擊技術，攻擊者偽造ARP回應，將自己的MAC位址綁定到目標IP位址上，從而使得網路流量被重定向。具體操作步驟如下：

(一) 攻擊者在網路中發送偽造的ARP回應，宣稱自己的MAC位址對應某個合法設備的IP位址。

(二) 內部網路的其他設備會接受這個假ARP回應，將攻擊者的MAC位址作為目標設備的MAC位址，從而將所有發往該



圖五：遭攻擊後各設備之arp table

員工A arp table

網際網路網址	實體位址
192.168.1.20	BB:BB:BB:BB:BB:BB
192.168.1.30	CC:CC:CC:CC:CC:CC
192.168.1.254	DD:DD:DD:DD:DD:DD

員工B arp table

網際網路網址	實體位址
192.168.1.10	AA:AA:AA:AA:AA:AA
192.168.1.30	CC:CC:CC:CC:CC:CC
192.168.1.254	DD:DD:DD:DD:DD:DD

外來筆電 arp table

網際網路網址	實體位址
192.168.1.10	AA:AA:AA:AA:AA:AA
192.168.1.20	BB:BB:BB:BB:BB:BB
192.168.1.254	BB:BB:BB:BB:BB:BB

Gateway arp table

網際網路網址	實體位址
192.168.1.10	AA:AA:AA:AA:AA:AA
192.168.1.20	BB:BB:BB:BB:BB:BB
192.168.1.30	BB:BB:BB:BB:BB:BB

設備的網路流量誤導到攻擊者手中。

(三) 攻擊者可以進行中間人攻擊，監控、修改或攔截這些網路流量，對內部網路進行各種攻擊。

實例：在測試的網路中，員工B的IP位址為192.168.1.20，MAC位址為BB:BB:BB:BBBB:BB，而外接筆電的IP位址為192.168.1.30，MAC位址為CC:CC:CC:CC:CC:CC，Gatway的IP位址為192.168.1.254，MAC位址為DD:DD:DD:DD:DD:DD。如果將員工B當成攻擊者，發送一個ARP Spoofing的回應給外接筆電，宣稱其MAC位址為BB:BB:BB:BB:BB:BB，並將這個MAC位址與192.168.1.254綁定。接下來，員工B又發送一個ARP Spoofing的訊息給Gateway，宣稱其MAC位址為BB:BB:BB:BB:BB:BB，並將這個MAC位址與192.168.1.30綁定，最後，所有的設備的arp table就如圖五所示，紅色部分是遭竄改的mac位置。這樣一來，外接筆電丟向Gateway的封包將會改成丟向員工B，而Gateway丟向外接筆電的封包也會改成丟向員工B，造成外接筆電不能正常上網。

那為什麼員工B電腦可以當成攻擊者呢?這是因為目前管處理的每一台電腦都有安裝一個代理程式(Agent)，代理程式的主要功能是蒐集電腦上的資產資訊，但它也可以當成Arp spoofing的攻擊者，當有不明設備連上網時，代理程式便會定時的發動攻擊，讓不明設備無法正常上網。

六、結論

透過ARP Spoofing 技術，可以有效阻止不明設備隨意接入管理處網路，從源頭減少內部網路遭受攻擊的風險。在當前資安威脅日益增長的環境下，推動VLAN 管控並結合先進的資安技術，已成為保障內部網路安全的關鍵策略。

未來，臺中管理處將持續強化內部網路的資安防護，包括：

(一) 引入更多高效的安全技術。

(二) 定期檢視網路環境的安全性。

(三) 提升人員資安意識與應對能力。

期望透過這些措施，來維護資通安全，並維持業務運行的穩定性與高效性。

(作者服務於農田水利署臺中管理處) ■