『推動 IPv4/IPv6 雙軌普行方案』

附錄八
『ICP IPv4/IPv6 網路安全防護架構技術手冊』

108 年委託研究報告

ICP IPv4/IPv6 網路安全防護架構技術手冊

計畫委託機關：台灣網路資訊中心

中華民國 108 年

108 年委託研究報告

ICP IPv4/IPv6 網路安全防護架構技術手冊

受委託單位

奇加互動股份有限公司

計畫主持人

林韋廷

研究人員

曾榮信、郭愷瀚、鄧丕文、金沅禹、張智崴、童冠瑜、吳奎億

研究期程：中華民國 108 年 4 月至 108 年 12 月

中華民國 108 年

目　　次

表　次

圖　　次

前　言

IP（Internet Protocol）位址即網際網路協定位址，如同門牌地址，主要提供客戶於網際網路上接收與傳送資訊。因應全球 IPv4 位址用罄，啟用 IPv6 更符合未來多元行動終端及萬物聯網發展需求，尤其是物聯網、智慧家庭、車聯網/自駕車、智慧城市及醫療健康照護等應用。

網際網路版本 6 （IPv6, Internet Protocol version 6） 是下一代網際網路協定，它被設計用來替代當前網際網路 IPv4，位址長度由 32 位元提升至 128 位元，IPv6 位址空間多達 2 的 128 次方個位址。

隨著 IPv6 的部署，許多網站跟應用服務業者也提供 IPv6 的位址供用戶存取，例如 Facebook、Google 跟 Yahoo!。而 IPv6 的需求，讓設備商、雲端業者、ICP 業者、作業系統業者、軟體開發商、服務供應商也都提供 IPv6 的服務。目前大型的雲端服務業者如 Amazon AWS、Google Cloud Platform 跟 Microsoft Azure 都已經提供 IPv6 供 ICP 業者使用。

IPv6 已經逐步取代 IPv4 為各種服務的主要協定，加上 5G、物聯網的各種應用，未來將會有更多基於 IPv6 優點而產生的新應用，並

提升人類的生活品質。

第一章　IPv6 現況

根據亞太網路資訊中心（APNIC）的統計，IPv4 的網路位址已經發放完畢，為避免網路發展因為 IP 位址不足造成發展瓶頸，IPv6 規格變應運而生。IPv4 可以提供 2 的 32 次方個網路位址，而 IPv6 則可以提供 2 的 128 次方的網路位址，可以有效解決 IP 位址不夠用的問題。

依據 APNIC IPv6 量測網站資料指出，2018 年 1 月台灣 IPv6 比例僅 0.46％，排名全球第 65。但自國內中華電信 2018 年年初 4G 行動上網 IPv6 開始商用服務，5 月 HiNet 光世代及公眾 Wi-Fi 逐步啟用 IPv6，遠傳電信及台灣大哥大 4G 行動上網亦逐步啟用 IPv6，使台灣 IPv6 比例快速竄升，至 12 月達到 32.02％，全球排名躍升至第 4 名，成長速度於 2018 年創世界第一。根據 APNIC 在 2019 年 9 月 10 日統計數據，台灣已經超過 37%。

NCC 除了持續推動臺灣的 IPv6 普及之外，另外也針對用戶設備製造商、內容與應用服務網站等環節提出推動使用 IPv6 措施，以確實建立我國 IPv6 生態環境。感謝 NCC、TWNIC 及各大電信業者的支援，讓台灣在如此短暫的時間內快速部署，大幅提升國家的整體競

爭力。

第二章　ICP IPv4/IPv6 雙軌服務基礎環境介紹

第一節 IPv6 的封包

IPv6 簡化了 IPv4 的檔頭（header）結構，這樣可以減少 header 在網路傳輸過程中消耗的頻寬。IPv6 移除了 IPv4 的五個欄位：

1. Header Length（首部長度）
2. Identification（識別碼，或稱為分片共用的唯一識別碼）
3. Flags（標誌，是用來控制跟辨識分片）
4. Fragment Offset（分片偏移，指明每一個分片相對於原始封包開頭的偏移量）
5. Header Checksum（首部檢驗總和，長度為 16 位元，用來對首部進行驗證跟查錯，但不包括資料 Payload 部分）

在 IPv6 被移除的 IPv4 項目中，Identification、Flags 及 Fragment Offset 欄位都是用在 IPv4 的封包切割。用途是在當大型封包必須在僅支援較小封包的網路上傳送時產生 Fragment 問題。這種情況下，IPv4 路由器會將封包切割成較小的片段，再傳送多個封包。目的地會收集封包並進行重組，如果重組過程中發現有遺失一個封包或封包內容有錯，則整個傳輸就需要重來。

那 IPv6 為何不需要 Identification、Flags 及 Fragment Offset 欄位來處理大封包傳輸的問題呢？IPv6 作法是讓主機透過 RFC 1981[5]裡面定義的 Path MTU Discovery 處理程序得知 Path Maximum Transmission Unit（MTU）大小。如果路由器因為封包太大不能傳送，會透過 ICMP 回傳一個「Packet Too Big」給來源主機，當來源主機收到「Packet Too Big」時，就可以決定是否利用 IPv6 的延伸檔頭（Extension header）來處理，因此 IPv6 不需要前述提到的 Identification、Flags 及 Fragment Offset 欄位。

Extension header 定義在 RFC 2460[9]內。在 IPv6 中將 IPv4 Option 移除，也移除了封包分割，並把這些功能都放到延伸檔頭內，這樣就可以保持 IPv6 檔頭大小固定，提升處理速度。而想要增加功能時，以類似模組化的方式，利用延伸檔頭來達成。例如下表中的 MIPv6 (Mobility) 就是一個例子，因此 Next Header 欄位就變得重要。

下表是 IPv6 會用到的檔頭，延伸檔頭有順序性，如果有多個延伸標頭同時出現，需要依照順序擺放。延伸檔頭如果之後有更新，都會發佈在 RFC 6564[21]。

表 1　IPv6 延伸檔頭類型

檔頭類型	順序	Next Header 欄位
IPv6 Header	1	41
Hop-By-Hop (HOPOPT)	2	0
Destination	3,8	60
Routing	4	43
Fragment	5	44
Authentication (AH)	6	51
ESP	7	50
Mobility (MIPv6)	9	135
No Next Header	Last	59
ICMPv6	Last	58
TCP	Last	6
UDP	Last	17

IPv4 header

版本＊	首部長度＃	傳輸類型◎	封包總長度◎	
片段共用的唯一識別碼＃			片段標誌＃	片段位移＃
存活時間◎		IP協定◎	header檢查碼＃	
來源位址＊				
目的地位址＊				
擴充選項＃				補空白＃

IPv6 header

版本＊	流量分類◎	流量標籤◇
Payload 長度◎	下一個header◎	可傳送最大連結數◎
來源位址＊		
目的地位址＊		

＊代表欄位名稱在IPv4及IPv6相同　　◎代表名稱與位置有變動
＃代表IPv4有，但在IPv6被移除　　◇代表IPv6才出現的新欄位

圖 1　IPv4/IPv6 檔頭欄位比較

IPv4 與 IPv6 在檔頭的比較說明如下

表 2　IPv4/IPv6 header 說明

欄位	IPv4	IPv6	IPv4	IPv6
首部長度 (Internet Header Length)	Y	N	IPv4 有一個 IHL(Internet Header Length, IHL,首部長度)欄位，此欄位用來說明 header 長度(單位為 32 bits)，此欄位也可以用來確定資料的偏移量(offset)。這個欄位的最小值是 5 (5x32-bit words=160 bits 或者 20 bytes)，最大值是 15。	此欄位在 IPv6 已經被移除，原因是 IPv6 的 header 長度是固定的 40 bytes，這樣處理時會更有效率。
片段共用識別碼 (Identification)、標誌 (Flags)及位移 (Fragment Offset)	Y	N	又稱為片段共用的唯一識別碼。共 16 位元，這個欄位主要是用來標誌一個唯一值，只要封包有被切片，這些被切片的封包都會擁有同一個識別碼 (Identification)，原因是分片不一定會依照順序到達，所以在重組時需要知道分片所屬的封包。	IPv6 作法是讓主機透過 RFC 1981[5] 裡面定義的 Path MTU Discovery 處理程序，得知 Path Maximum Transmission Unit (MTU)大小。如果路由器因為封包太大不能傳送，會透過 ICMP 回傳一個「Packet Too Big」給來源主機，當來源主機收到「Packet Too Big」時，就可以決定是否利用

				IPv6 的 Extension header 來處理，因此 IPv6 不需要 Identification、Flags 及 Fragment Offset 欄位。
檢查碼 (Checksum)	Y	N	IPv4 利用 header checksum 對首部進行檢查，如果不一致，封包就會被丟棄。重新計算的重要性是因為在傳遞過程中，可能發生 TTL (Time To Live)、Flag、Offset 變更的情況，來避免 header 錯誤。至於資料(payload)的錯誤，則交給 TCP/UDP 層來處理。	因為 IPv4 開發之初，上一層對於媒體傳輸層做 checksum 不普遍，因此 IPv4 需要 checksum。但是現在這種狀況已經不需要，因為上一層會確保資料的正確性，因此 IPv6 把這個欄位跟檢查動作拿掉，可以大幅提升傳遞速度，減少路由器檢查封包的時間。
流量標籤 (Flow Label)	N	Y	IPv4 有 QoS(Quality of Service)，表示在網路環境中，送出封包的品質，所謂的品質越好，表示有越低的延遲、掉包和抖動等，並且搭配更高的吞吐量和可靠性。實際作法是利用封包內容的特定欄位的高低，告訴交換器/路由器等如何處理封包。	此為新欄位，用來當從來源傳送到一個或者多個目的地時，對一串或者一組 IPv6 封包 payload 訂標籤。被標籤化的封包在經過 IPv6 路由器時，可以被特別處理，例如高優先權傳送。關於 Flow Label 可以參考 RFC 1883[3]、2460[9] 跟 6437[20]。

			IPv4 是在 payload 內做這個判斷，但是在 header 是沒有這個欄位的。	

IPv6 header 的位元格式：

版本 (4 bits)	流量分類 (8 bits)	流量標籤 (20 bits)
Payload 長度 (16 bits)	下一個header (8 bits)	可傳送最大連結數 (8 bits)
來源位址(128 bits)		
目的地位址(128 bits)		

圖 2　IPv6 header

在 MTU（Maximum transmission unit，最大傳輸單位）部分，IPv4 最小值是 576 個位元組，而 IPv6 最小值是 1280 個位元組。IPv4 網路中，若傳出的封包大於接收路由裝置的 MTU 限制時，一般會進行封包分段成小於 MTU 的封包；在 IPv6 網路中，則是透過 IPv6 Path MTU Discovery （PMD）機制得到封包傳送路徑上的 MTU（PMTU），將封包在網路源頭進行分段

第二節 IPv4/IPv6 的位址格式

IPv4 位址長度為 32 位元，型態為 x.x.x.x （其中 x 皆數字，每一個數字最小為 0 最大為 255)，例如 140.130.120.110。而 IPv6 出現的目的就是為了解決 IPv4 位址不夠使用的問題，IPv6 位址的長度為 128 位元，其中 64 位元代表網路號碼，而另外 64 位元代表電腦號碼。IPv6 可以提供 2 的 128 次方個 IP 位址。而一個 IPv6 的位址格式為 xxxx: xxxx: xxxx: xxxx: xxxx: xxxx: xxxx: xxxx （其中每一個 x 都是 16 進位，數字 0~9 加字母 a~f)。例如：
2001:b011:6a00:18ff:d87a:8712:dh8b:f718 就是一個 IPv6 的位址。

對於 private IP 的定義，在 IPv4 中，特別定義出 10.0.0.0/8、172.16.0.0/12 跟 192.168.0.0/16 作為 Private IP 使用，在 IPv6 也另外定義了屬於 IPv6 專用的 Private IP 位址為 fc00::/7。IPv6 將位址分為公用或者暫時用 IP，在 RFC 3041[12]內有定義 IPv6 對於 Private IP 為 fd00::/8，最特別的一點是，IPv6 的暫時 IP 可以全域遞送，IPv6 的暫時位址生命週期有限，且不包括 MAC 位址的介面 ID。

第三節 IPv6 位址的分配方式

現有的 IPv6 位址發放方式是一個階層式的架構，可參考下圖的 IPv6 配置規則架構圖，以一個 IPv6 地址位址來說明 2001:0db8:130f:0000:0000:7000:0000:140b，以 16 位元為一組，每組以冒號「:」隔開，可以分為 8 組，每一個 16 位組都代表一個 IPv6 的發放規則，例如第一個 16 位元組是 Allocation Global Address，這樣的架構可以確保 IPv6 位址的發放有公平性，另外在網路安全的控管上也會有其對應的好處（下面章節將會說明）。

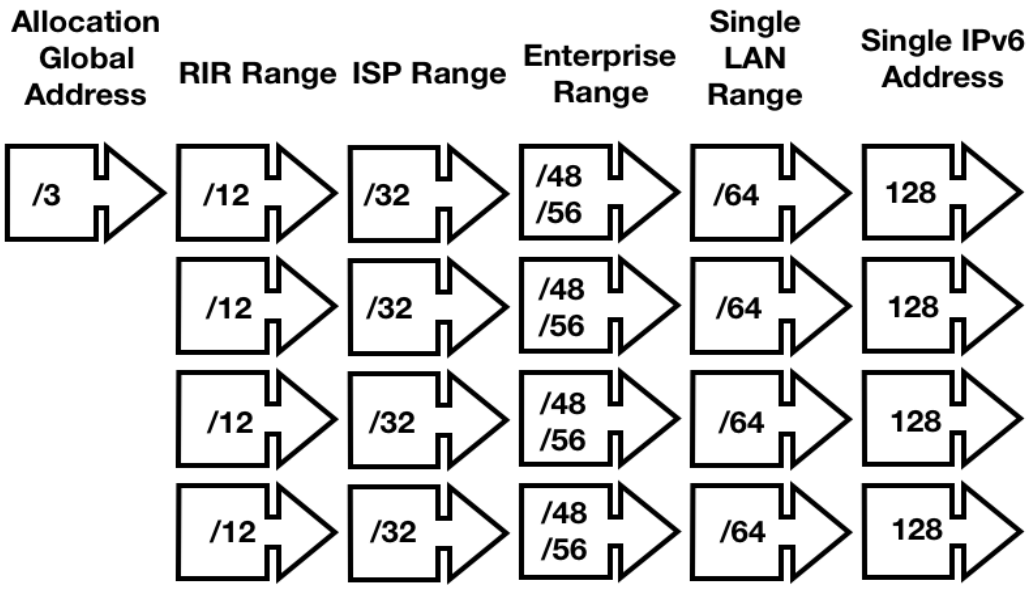

圖 3　IPv6 配置規則架構圖

第四節 IPv6 對 Multicast 協定的調整

IPv6 不支援 Broadcast，不過 IPv6 改以 Multicast（群播）來取代 IPv4 的 Broadcast（廣播），而 IPv6 新增的 Anycast（任播）則可以視為群播的一種變形。群播是將訊息傳遞給同一個群播群組內的設備或主機，而任播則是將訊息傳遞給群播群組內的單一設備或主機。IPv6 也保留了 ff00::/8 給 Multicast 使用。

表 3　unicast, multicast 與 broadcast 比較

傳遞方式	說明
Unicast（單播）	唯一區域位址（unique local address，簡稱 ULA，保留區塊為 fc00::/7）類似 IPv4 的私有 IP 位址（Private IP address）的可用位址空間，即同一路由內的區域網路（或稱內網）可用位址的集合。 連結本地位址（link local address，保留區塊為 fe80::/64）類似 IPv4 啟用時本機自動產生的本地位址，而此本地位址只存在本機中無法跨過路由器。
Multicast（群播）	IPv4 使用 224.0.0.0/4 作為 multicast 封包使用，而 IPv6 則使用 ff00:::/8。在 IPv6 中以 multicast 取代 IPv4 的 broadcast。 在 IPv4 使用 Internet Group Management Protocol（IGMP）協定來管理 multicast group membership，而 IPv6 則不使用 IGMP，改以 Multicast Listener Discovery（MLD） messages。簡單來說，MLDv1 跟 IGMPv2 很接近，MLDv2 跟 IGMPv3 很接近。 scope 欄位是用在 multicast 時，決定哪些路由器可以轉送這些 multicast 封包。

	scope 欄位共有 4-bit，其值可以是 0 - reserved 1 - Interface-Local scope 2 - Link-Local scope 3 - Reserved 4 - Admin-Local scope 5 - Site-Local scope 6 - Unassigned 7 - Unassigned 8 - Organization-Local scope 9 - Thru D Unassigned E - Global scope F – Reserved 在 scope 欄位之後有 112 bits 用來表示 multicast group ID。
Anycast（任播）	任播用來送給一群主機中的任何一台。 所謂的任播是指該 IPv6 位址可以被指定到多個介面上（通常是多台不同設備）。 換句話說，多台機器可以共用同一個 IPv6 位址。當有一個封包被要求傳送到一個 anycast IPv6 位址時，路由器會依據 routing table 決定送給最近的一台設備。關於 anycast 可以參考 RFC 1546[1]。

第五節 IPv4/IPv6 對 IP 設定組態的差異

在 IPv4 利用 DHCP 來動態配置 IP，DHCP 可以使用在許多場合，例如辦公室、家裡或者工廠。原因在於 IPv4 的 IP 位址都需要費用且數量有限，不可能每一台電腦或者主機都可以配置一個 IP，此時這些場所都會使用 NAT 搭配 DHCP 來動態配置設備的 IP，也是就是假 IP。所謂假的 IP 是指無法透過 Internet 傳遞的 IP 位址，對於這些假 IP 我們也稱為 Private IP （私有 IP），在 RFC 1918[4]內有完整的定義。Private IP 的可使用範圍包括 10.0.0.0/8、172.16.0.0/12 跟 192.168.0.0/16。

在 IPv6 內使用 DHCPv6 的作法達成類似的效果，這種方法又稱為 Stateful Address Auto-configuration（全狀態位址自動配置）。DHCPv6 協定使用 UDP port 546 跟 547 作為溝通用的 port，用戶端使用 546，另一個 547 則是給伺服器端使用。

在 IPv6 中，除了 DHCPv6 之外，還有 Stateless Address Auto-configuration 的方式（無狀態位址自動設定），Stateless Address Auto-configuration 又簡稱為 SLAAC，在網路設備設定上常看的的都是寫成 SLAAC 的簡稱，定義在 RFC 2462[10]跟 RFC 4862[15]。所謂

的無狀態機制運作機制為當一部主機啟動 IPv6 時，送出多點傳送的路由器請求、路由器回應以路由器公告訊息(Router Advertisement; 簡稱 RA）來讓主機從路由器（Router）取得路由器的 prefix 再加上自己的介面識別碼，來自動配置 IPv6 位址。

使用 SLAAC 有一個管理上的便利性，這個便利性是當更換了上網的 ISP 單位，也就是更換了電信業者之後，機器會從新的 ISP 單位得到一個全球性位址首碼，ISP 的路由器（Router）會將這個位址首碼傳給企業的 Router，而企業內的主機則透過 Router 的公告訊息（Router Advertisement; 簡稱 RA)，自動取得新的 IP 位址並覆蓋掉舊的 IPv6 位址。

IPv6 的自動定址（Auto-configuration）機制包括了以下兩種：

1. 全狀態位址自動配置（Stateful Address Auto-configuration）是透過 DHCPv6 伺服器自動取得 128 位元的 IP 位址跟相關組態。
2. 無狀態位址自動配置（SLAAC，Stateless Address Auto-configuration; SLAAC）依據 RFC 2462[10]、RFC 4862[15]，可以依據自己可用資訊（介面識別碼）和從路由器公告取得的訊息（首碼）來產生自己的位址。SLAAC 作法上，

主機先送出多點傳送路由器請求（Router Solicitation），路由器則回應路由器公告（Router Advertisement）訊息來完成。

IPv6 自動組態功能啟動順序如下：

1. 芳鄰探索（Neighbor Discovery; ND）協定
2. 位址解析（Address Resolution）
3. 重複位址偵測（Duplicate Address Detection; DAD）
4. 無狀態自動位址配置（Stateless Address Autoconfiguration）
5. 發現路由器（Router Discovery）
6. 發現首碼（Prefix Discovery）
7. DNS 發現（DNS Discovery）
8. 路由重導

IPv6 雖然是透過芳鄰探索（Neighbor Discovery; ND）來執行自動組態配置，但因為路由器公告訊息內的 M 及 O 旗標，造成四種不同的設定方式。

1. 所謂的 M 旗標是 Managed Address Configuration，如果為 1 代表要向 DHCPv6 取得 IPv6 prefix。
2. 所謂的 O 旗標是 Other Configuration，如果為 1，代表主機需要向 DNS 取得其他組態資料。

因為路由公告內的 M 及 O 可以分別為 1 或者 0，故 IPv6 的自動組態配置有四種選項：

1. Stateless Auto-configuration：適用於沒有 DHCPv6 的環境，主機利用路由器的 RA 封包的首碼自動產生 IP 位址，而 DNS 則得手動輸入。
2. Stateful DHCPv6：適用於 DHCPv6 環境下，主機直接由 DHCPv6 伺服器取得 IP 位址和其他參數如 DNS 位址。
3. Stateless DHCPv6：使用路由器的 RA 封包取得首碼自動產生 IP 位址，至於 DNS 則由 DHCPv6 伺服器取得。
4. 其他：由 DHCPv6 提供 IP 位址，但 DNS 或者其他參數卻不跟 DHCP 索取。

表 4　IPv4/IPv6 設定差異

	IPv4	IPv6
設定方式	由網路服務商提供 IP 網址或者 subnet，將 IP 位址或者 subnet 設定在設備上，以啟用服務。 或者使用 DHCP 機制，從 DHCP Server 取得配置的 IP 位址。	IPv6 引入一個簡化版本的 stateless auto configuration 作法，此作法可以只要依據節點本身的資訊就可以設定，不需要去詢問任何設備。 1. 全狀態位址自動配置 (Stateful Address Auto-configuration) 2. 無狀態位址自動配置 (SLAAC，Stateless Address

		Autoconfiguration; SLAAC)
流量品質	以檔頭的 TOS(Type of Service)欄位來區分	1. 對路由器而言，檢查檔頭中的 Traffic Class 欄位來達成 2. 未來可以由設備對封包 header 設定 Flow Label 欄位，用來支援更進階的應用

對於 IPv6 的配置我們給出以下建議：

表 5　IPv6 配置建議

作法	適合場景	補充說明
人工配置位址	適合網路設備及網頁伺服器	1. 建議關閉 RA(Router Advertisement)的發送。 2. 每一台主機都手動設定 IP(包括 gateway、DNS、防火牆)。 3. 適合網站使用。
SLAAC+ RDNSS	適合物聯網	1. 物聯網設備通常不需要主動連網，因此網路環境越單純越好，SLAAC 有助於物聯網的發展。 2. 作法是定期經由 Multicast 發出 Router Advertisement(RA)的封包，從 RA 封包取得 IPv6 Prefix 及 Default Gateway 的資訊。 3. 主機利用收到 Prefix 跟自動產生的 Host ID(主機識別碼)即可變成主機的 IPv6 位址，位址發放之後就不再管理。 4. SLAAC 不支援發送 DNS 伺服器位址，不過新增 SLAAC RDNSS 已經解決此問題，只是作業系統不見得有支援。

		5. 適合物聯網使用。
SLAAC+ Stateless DHCPv6	適合不需要嚴格進行資安查核管理的場所	1. 利用 SLAAC 及 DHCPv6 進行位址配置。 2. RA 負責 IPv6 位址及 Default Gateway 的指派，DHCPv6 則提供 DNS 伺服器位址。SLAAC 機制不會進行 IPv6 位址的更新跟維護。 3. 適合用在家裡。
Stateful DHCPv6	適合需要嚴格進行資安查核管理的場所	1. RA(Router Advertisement)負責提供 Default Gateway 2. DHCPv6 伺服器負責 IPv6 位址分配(包括 Prefix、Host ID)及 DNS 伺服器位址。 3. DHCPv6 會記錄 IPv6 位址與 MAC 位址的對應表，並經由定期位址更新維護記錄。 4. DHCPv6 不提供 Default Gateway 資訊，因此 DHCPv6 需要跟 RA 配合。 5. 適合企業內部使用。

表 6　IPv6 優點

分類	說明
增加 IP 位址的擴充性	IPv6 的位址從 32 bits 變為 128 bits，可以支援更多的 IP、位址自動設定。藉由增加一個「scope」欄位讓 multicast 路由延伸性增加，還有新增 anycast。
封包 header 簡化	部分 IPv4 欄位被捨棄，可以減少封包處理的頻寬消耗。
增加擴充性跟更多選項	Extension header 允許更有效率的轉送、更有彈性的選項長度及新增選項。
流量標籤能力	Flow Label 是一個新的機制用來幫封包貼上標籤，讓封包屬於某個特定的「flows」，這種機制用於即時的服務。每一個封包提供一個流量標籤，同一筆資料串列給予相同的標籤號碼，因此可以做流

	量控制及統計。用來支援像視訊、語音這類即時服務的需求，以提高 QoS 的品質。
授權及隱私的擴充性	在 IPv6 內增加了認證、資料完整性、資料保密的能力。(後面會說明)

第六節 IPv4/IPv6（Dual Stack）雙軌服務說明

所謂的雙軌服務，是指 ICP 網站可以讓訪客以 IPv4 或者 IPv6 連線，也代表網站同時支援兩種不同 IP 位址的連線方式。IPv6 的推廣在世界各國都正積極進行中，提供 IPv4 與 IPv6 同時支援是因應現實網路的使用狀況，原因是目前網路上仍舊以 IPv4 為主要的連線方式，但 IPv6 是一個趨勢且成長快速。

網站要支援 IPv4/IPv6 雙軌運作，我們先從網路基礎開始說起。對所有的網路設備而言，整個封包傳輸過程是以網卡為出發點，之後分為 IPv4 或 IPv6 封包，接著再以 TCP（保證傳遞）或者 UDP（不保證傳遞）往應用程式傳遞，最後完成任務。

在以太類型（Ether Type）中定義了多種協定，與 IPv4 及 IPv6 有關的整理如下表。

表 7　Ether Type 定義

以太類型編號	代表協定
0x0800	Internet Protocol version 4 (IPv4)
0x86DD	Internet Protocol version 6 (IPv6)

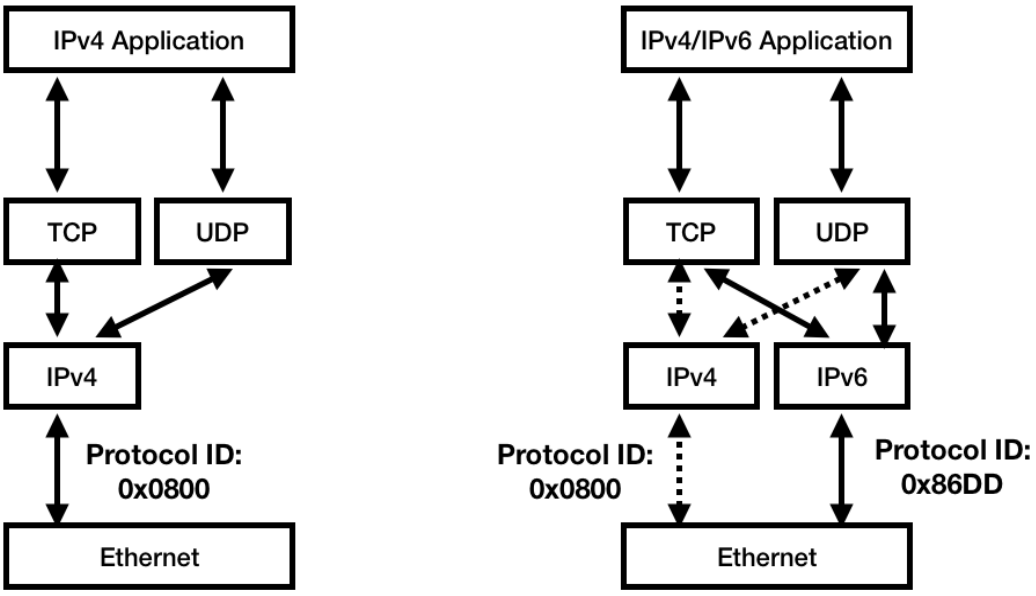

圖 4　IPv4/IPv6 傳輸差異

從上圖可以看出，IPv4 的 Ethernet frame 的 Ethernet Type 為 0x0800，而 IPv6 的 Ethernet frame 的 Ethernet Type 為 0x86DD。雖然在 Ethernet frame 內，IPv4 跟 IPv6 在 Ethernet Type 帶的值不同，但 Ethernet 是 Layer 2，因此對於 Layer 2 的設備如 Switch（交換器），並不需要去判斷 Ethernet Type，所以並沒有所謂的不支援 IPv6 的 Switch 交換器，對於所有的 IPv6 封包，仍舊可以順利的從現有的 Switch 傳遞到下一個節點。

對於 IPv6 的支援，在作業系統層面，包括 Windows、Mac OS 跟 Linux（例如 Ubuntu、Centos、Fedora、SUSE 等都是 Linux 作業系統），早就已經支援。而硬體設備如 Cisco，也早在 2000 年宣布在 Cisco IOS

Release 12.2（2）T 版本中開始支援 IPv6。

我們以圖片說明一個同時具備 IPv4 與 IPv6 的設備（可能是一台電腦、手機或平板)連到一個同時支援 IPv4 跟 IPv6 的網站的示意圖。

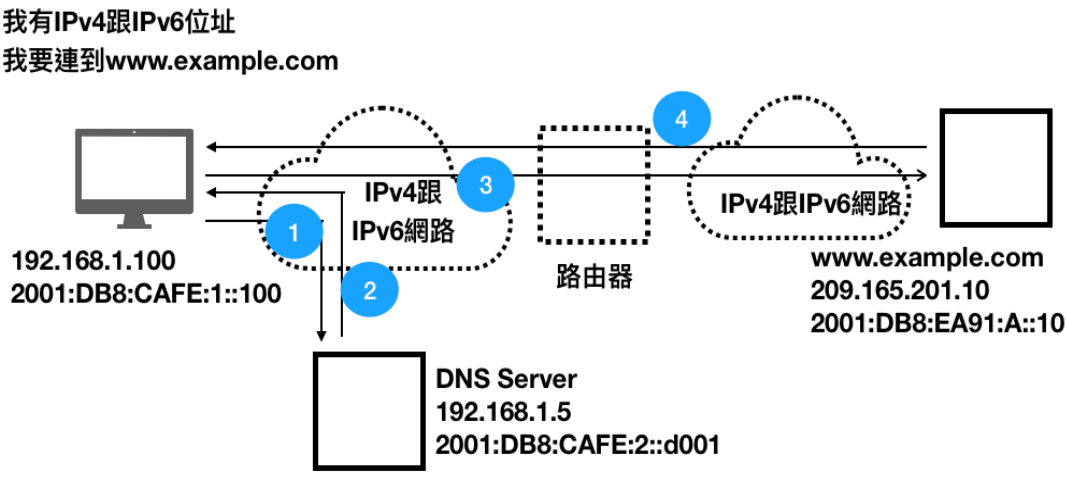

圖 5　IPv4/IPv6 連線範例

第七節 作業系統對 IPv6 的支援

IPv6 在現存的大多數作業系統都已經啟用，參考下圖可以知道在 2003 年 12 月 17 日發布 Linux 內核（Kernel）2.6.0 之後就已經完整具備 IPv6 功能。在更早之前，Linux Kernel 在 2.1.8 就加入了 IPv6 的部分功能。

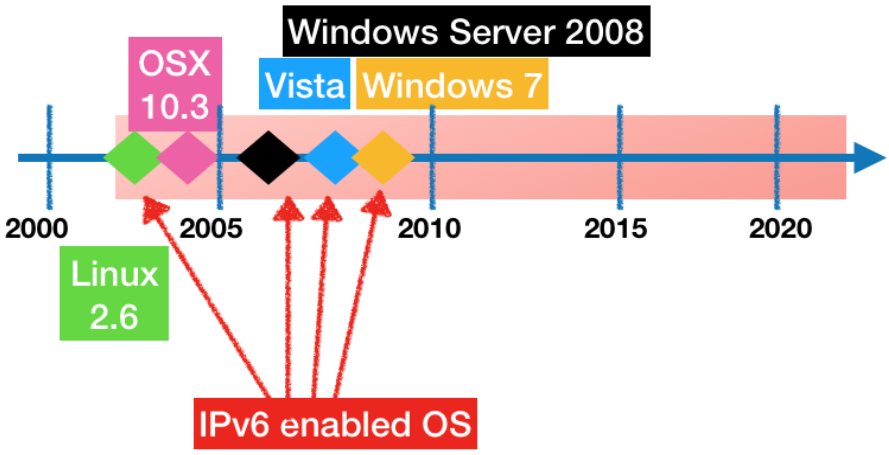

圖 6　支援 IPv6 的作業系統

第八節 ICP 機房環境比較

ICP 業者的機房設施建置環境分成多種，以下以表格整理（資料日期：108 年 8 月）。

表 8　ICP 業者機房選擇方案

作法	描述	提供業者(108 年 9 月整理)
自建	所有設備都由 ICP 業者自行採購、安裝、維護及部署。	依據需求，跟硬體廠商購買
租賃	設備由設備廠商提供給 ICP 業者租賃，有固定租期，在租用期滿之後，可以用低價購買。	遠振資訊 探集數位科技
IaaS	基礎設施即服務(Infrastructure as a Service，簡稱 IaaS）是提供消費者處理、儲存、網路以及各種基礎運算資源，以部署與執行作業系統或應用程式等各種軟體。(資料來源：Wiki 維基百科)	中華電信 台灣固網 遠傳電信 Amazon Web Services Google Cloud Platform Microsoft Azure IBM Cloud Linode DigitalOcean
PaaS	平台即服務（Platform as a Service，簡稱 PaaS）是一種雲端運算服務，提供運算平台與解決方案服務。 在雲端運算的典型層級中，PaaS 層介於軟體即服務與基礎設施即服務之間。 PaaS 提供使用者將雲端基礎設施部署與建立至用戶端，或者藉此獲得使用程式語言、程式庫與服務。(資料來	Amazon Web Services Google Cloud Platform Microsoft Azure Heroku DreamHost Oracle Cloud IBM App Connect Salesforce Platform LiquidWeb rackspace cloud Cloudways

	源：Wiki 維基百科)	

以上四種可以歸納成三類，這三類的優點跟缺點比較如下表整理。

表 9　ICP 選擇網路架構優缺點比較

	優點	缺點
自建/租用機房設備	自行架構及部署所需設備，網路拓墣及設備等級，完全自主掌控，可隨時增加或減少硬體設備。	投資成本高，人員數量倍增，須 24 小時支援，硬體定期淘汰及升級成本，技術人員能力要求高，人員不好找。
IaaS	依據需求選擇 CPU 數量及等級、記憶體大小、硬碟種類及空間大小、IP 數量，作業系統型態跟版本、資料庫種類跟版本等，無須管理硬體設備，不需 24 小時有人員定期維護設備。	對自建機房而言，硬體等採購都不需要，但技術人員需要熟悉 IaaS 的管理跟設定方式，而且作業系統得自己安裝跟管理。
PaaS	只要專注於軟體應用的部署即可，無須管理作業系統、資料庫的安裝。	如果遇到系統效能瓶頸時，相對於 IaaS 可以藉由優化作業系統或者資料庫設定就可以提升效能，但在 PaaS 卻只能藉由租用更高級的服務來達成。

第九節 網際網路服務供應商支援 IPv6 調查

我們對市場主要的網路服務商進行 IPv6 支援度的調查，用來了解當 ICP 業者是否可以繼續使用現有的網路服務商進行升級為 IPv4/IPv6 雙軌服務，對於無法支援 IPv6 的網路服務商業者，則希望這些業者盡快支援 IPv6，提升 ICP 業者使用 IPv6 的比率。（資料日期：108 年 8 月）

表 10　網路服務商支援 IPv6 表

服務類型	支援 IPv6	不支援 IPv6
IDC 機房	中華電信 台灣固網 速博 sparq 亞太線上 數位聯合 台灣電訊	
IaaS 服務	中華電信 遠傳電信 Amazon Web Services Google Cloud Platform Microsoft Azure Linode DigitalOcean	台灣固網 IBM Cloud
PaaS 服務	Amazon Web Services Google Cloud Platform Microsoft Azure DreamHost LiquidWeb rackspace cloud	Heroku Oracle Cloud IBM App Connect Salesforce Platform Cloudways

第三章　IPv4/IPv6 雙軌服務的網路安全

第一節 IPSec 在 IPv4/IPv6 上的比較

IPSec （Internet Protocol Security）是一個協定框架，透過對 IP 協定的封包進行加密和認證來保護 IP 協定的網路傳輸協定，但 IPSec 並未定義加密和金鑰交換等機制。

IPSec 是 IPv4 組成的一部分，但是 IPSec 是網路層協定，它只負責其下層的網路安全，並不負責其上層的安全。也就是說，像網頁傳遞仍舊需要 SSL，檔案傳輸需要 SFTP，郵件傳遞需要 TLS，連線傳輸需要 SSH。IPSec 的協定組成說明如下表。

表 11　IPSec 組成說明

協定	IPv4	IPv6
Authentication Header (AH)	1. 利用 hash 及一個安全共享金鑰確保連線的完整性 2. 對來源封包認證 3. 利用一個序號來防止 replay 攻擊 4. 防止 options 欄位被	1. 防止 header 注入攻擊 2. 防止 option 注入攻擊 3. 保護 IPv6 基本 header、AH 欄位、AH 之後固定的欄位、IP Payload 定義在 RFC 2402[7]

	注入攻擊 5. 保護 IP payload 跟所有的 header 欄位 6. 定義在 RFC 2402[7]	
Encapsulating Security Payload (ESP)	1. 提供來源認證 2. 利用 hash 確保資料完整性 3. 對封包加密確保資料安全 4. Transport mode(傳送模式)ESP 不提供整個封包的完整性跟驗證 5. Tunnel mode(隧道模式)是對整個封包加密後封裝，並添加一個新的 header 6. 定義在 RFC 2406[8]	1. 在 Transport mode，ESP 預留原本的 IPv6 header，但是新增一個 ESP extension header 及一個 optional ESP trailer 2. 增加一個 optional ESP authentication trailer，利用 HMAC(Keyed-Hash Message Authentication Code; 又稱為 keyed hash)驗證封包 3. 定義在 RFC 2406[8]
Security Associations (SA)	1. 用來交換建立安全連線之間所需的資訊，包括演算法、金鑰用來加密封包。 2. 用途包括連線、驗證。 3. IPv4 使用 IKEv1 作為金鑰管理	1. 使用 IKEv2 作為金鑰管理的方式，定義於 RFC 4301[14]

IPSec 的安全特性有以下幾點：

1. 不可否認性

可以證實消息發送方是唯一可能的發送者，發送者不能否認

發送過消息，當使用公鑰技術時，發送方用私鑰產生一個數字簽名隨消息一起發送，接收方用發送者的公鑰來驗證數字簽名。由於在理論上只有發送者才唯一擁有私鑰，也只有發送者才可能產生該數字簽名，所以只要數字簽名通過驗證，發送者就不能否認曾發送過該消息。但"不可否認性"不是基於認證的共享密鑰技術的特徵，因為在基於認證的共享密鑰技術中，發送方和接收方掌握相同的密鑰。

2. 反重播性

確保每個 IP 包的唯一性，保證信息萬一被截取複製後，不能再被重新利用、重新傳輸回目的地址。該特性可以防止攻擊者截取破譯信息後，再用相同的信息包冒取非法訪問權。

3. 資料完整性

防止傳輸過程中數據被篡改，確保發出數據和接收數據的一致性。 IPSec 利用 Hash 函數為每個數據包產生一個加密檢查和，接收方在打開包前先計算檢查，若包遭篡改導致檢查和不相符，數據包即被丟棄。

4. 資料可靠性

在傳輸前，對數據進行加密，可以保證在傳輸過程中，即使數據包遭截取，信息也無法被讀。該特性在 IPSec 中為可選

項，與 IPSec 策略的具體設置相關。

IPv6 的 IPSec 架構跟 IPv4 很類似，只是在 IPv4，AH 跟 ESP 是 IP protocol headers，而 IPv6 則是使用 extension header 的作法。而 IPv6 這樣作法優點是將 IPSec 作為 IPv6 protocol 的基本，而不是像 IPv4 需要額外考量的。

IPSec 是 Internet Layer 的安全通道，提供設備或者網段之間的安全連線。在 RFC 規範的早期版本，IPv6 實作 IPSec 是建議使用 IKE（Internet Key Exchange，IKE Internet Key Exchange）的金鑰管理。新版的規範是建議自動設定改用 IKEv2(第二版)，此需求定義在 RFC 5996 [19]。

IPSec 有兩種模式，分別為 Transport Mode （host-to-host） 跟 Tunnel Mode （gateway-to-gateway or gateway-to-host），以下說明 IPSec 兩種模式下對於封包的欄位變更、加密範圍及驗證範圍。

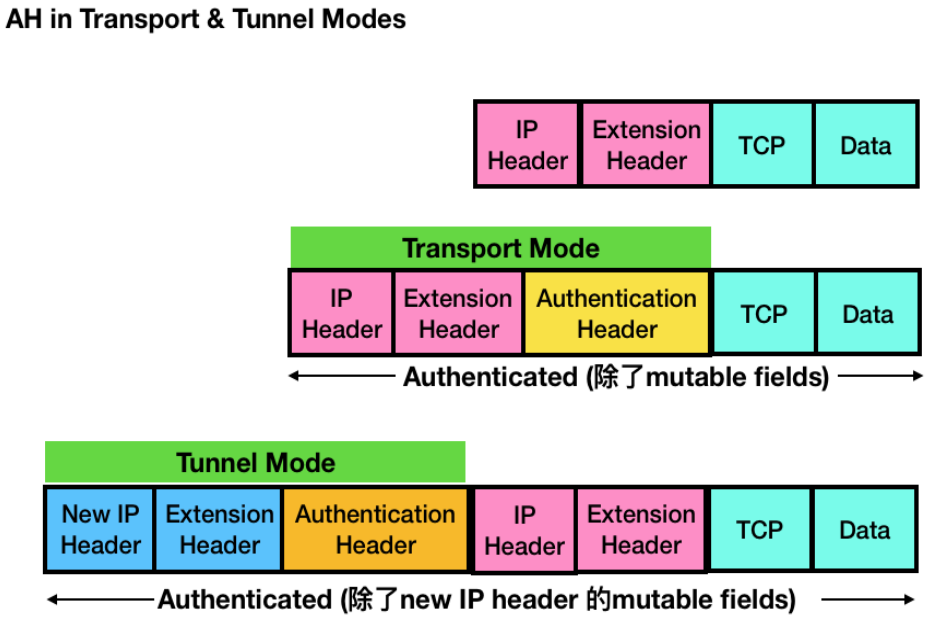

圖 7　AH in Transport & Tunnel Modes

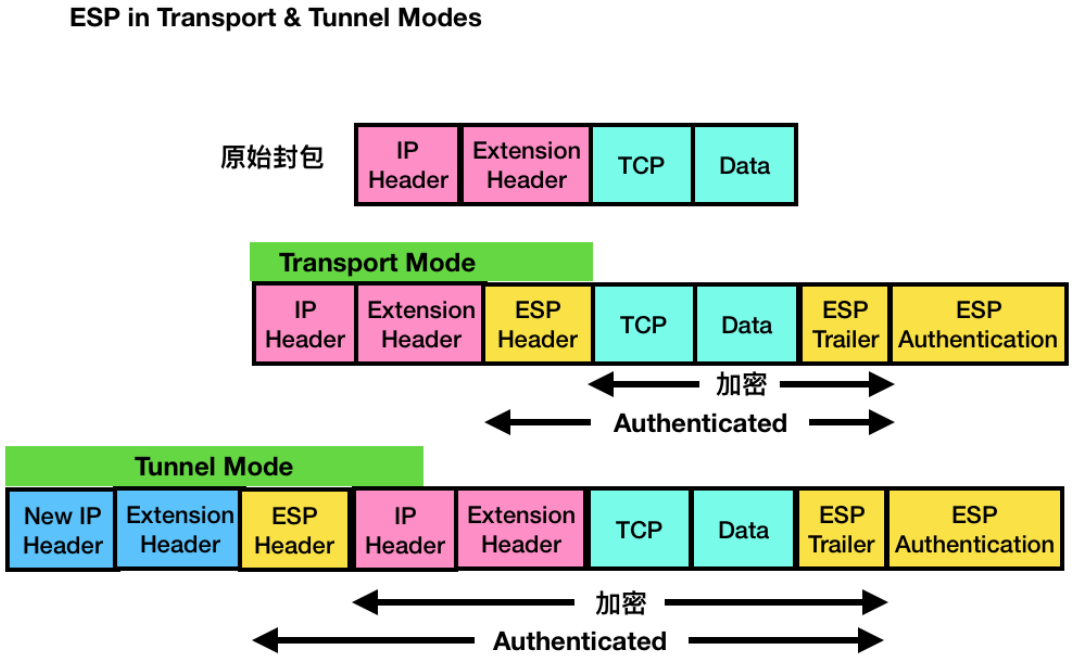

圖 8　ESP in Transport & Tunnel Modes

第二節 NAT 在 IPv4 與 IPv6 上的探討

在 IPv4，如果不需要幫每一個設備都配置一個公開實體 IP 時，此時會使用 NAT 去配置私有 IP。在 IPv6 網路環境下，由於 IPv6 數量夠多，因此不需要使用 NAT 機制來解決 IP 不足的問題。

網際網路架構委員會（Internet Architecture Board，簡稱 IAB）在 RFC 5902[18]描述關於 IPv6 環境下使用 NAT 機制的情境。會有 IPv6 是否需要 NAT 的討論起因於原本在 IPv4 下使用 NAT 的廠商，他們覺得也需要類似的機制可以在 IPv6 下使用。不過依據 IETF（Internet Engineering Task Force，網際網路工程任務組）討論結果，不需要在 IPv6 提供 NAT 機制。更多關於 IPv6 是否需要 NAT 的討論可以參考 RFC 4864[16]整理如下：

表 12　NAT 問題討論

問題	討論	IPv6 解決方式
Avoid Renumbering(避免重新編號)	在 RFC 4864[16]第 2.5 節討論的，許多業者希望能夠盡量減少網路維運的負責度跟工作量。對家庭用戶而言，重新編號不是一個嚴重的問題，但對企業用戶卻是。影響範圍包括需要重新配置 IP 跟 prefix 的設備，包括 DNS、DHCP、	RFC 2462[10]提供 IPv6 Stateless Address Autoconfiguration(無狀態地址自動配置)，提供自動配置跟重新編號。IPv6 的 Stateless Autoconfiguration 是 IPv6 的新功能，包括 link-local 位址、

	防火牆、IPSec 策略、入侵偵測系統、庫存管理系統、程式碼修正管理系統內部系統。 許多大企業使用提供商無關地址空間（Provider-independent address space，又稱 PI 地址空間）是由區域網際網路註冊管理機構（RIR）直接分配給最終用戶的一段 IP 位址，主要優點是方便設定路由(Wiki 維基百科說明)。	multicast、the Neighbor Discovery(ND)通訊協定、從底層數據鏈路層地址生成地址的接口標識符的能力。
Site Multihoming(網站多宿主)	站點多宿主提供了網際網路所需的可靠性跟負載平衡。內送流量備援容錯機制(Multihoming)，亦作多重主目錄，是網際網路連線的一種容錯機制，用以提高 IP 網路上對網際網路連線的可靠度。這個機制一般只用在客戶端，而不會用在網際網路供應商(ISP)，透過為客戶端提供多於一條網際網路連線，使當中其中一條連線中斷時，系統可以自動切換使用另一條連線。(Wiki 維基百科說明)	在 RFC 3852[13]此篇 RFC 描繪了新的 IPv6 site-multihoming 架構下所欲達成的理想目標，這些理想包括提供有高效率的備援功能(redundancy)、優質的負載分享(load sharing)、高效能(performance)、支援客戶所要求的管理政策需求(policy)等優於 IPv4 目前 site-multihoming 所能提供的功能。 如何在不影響目前 site-multihoming 運作環境下(包括對營運者的維運、路由器、用戶主機等)，仍然可以優於 IPv4 目前 site-multihoming 所能提供的功能。(參考中華

		電信研究所 NICI IPv6 標準測試分組電子報)
Homogenous Edge Network Configurations (同質邊緣網路配置)	對家庭用戶而言，這是電信業者最常提供給家庭用戶的方案。一個家庭內即使有多台機器，對外也是只使用同一個 IP 位址。	參考 RFC 5902[18]，在 IPv6，link-local 位址可以被用來確保所有的家用 gateway 使用相同的 IP 位址，並提供 homogenous addresses 供支援的設備使用。
Network Obfuscation(網路混淆)	大多數的網路管理人員都希望隱藏主機的詳細資訊，包括網路架構跟通訊內容。這樣的考量是基於這些主機都是他們公司的私有資產，由於某些主機可能需要機密性，特別是很重要的主機更是希望能夠完全保密，因此網路管理在考量網路安全時，總是認為以 NAT 來保護這些設備是最恰當的方式。	可以參考 RFC 4941[17]，利用專用介面識別元搭配亂數產生一個全球都可以識別的位址，並不定時更新資料，避免資料被收集，降低被主機資訊洩漏的風險。
Hiding Hosts(隱藏主機)	對於網路管理人員來說，隱藏跟保護內部網路內的主機資訊是重要的。這些主機可能包括工作站、筆記型電腦、伺服器、特定的終端設備(印表機、掃瞄器、IP 電話、POS 系統、門禁系統)等。 由於這些設備不需要對外服務，因此他們希望外部無法探知這些設備及資訊。 對駭客而言，對於要攻擊 NAT 內的主機，難度是較	對於駭客而言，他們已經設計出透過特洛伊木馬病毒來穿透 NAT 的攻擊方式。另外有一點是 NAT 不是防火牆，不少管理者把 NAT 作為一種安全防護手段，這樣已經把防火牆跟 NAT 搞混了。安全防護應該透過防火牆來執行，而非以為 NAT 可以做到防火牆相同的效果。參考 RFC 3041[12]的作法隨機在

	高的。而且駭客要知道一個 NAT 內有多少主機也是困難的，即使他們可以藉由收集不同的封包內容去猜測跟收集不同主機的指紋資訊，但透過這些資訊要組合成可被攻擊的目標，仍舊是一件困難的事情。	IPv6 中將主機隱私資訊依據需要產生，而且僅限於有限期間內才有效。由於 IPv6 位址很多，因此有許多自由隨機化子網分配，透過這種方式，讓意圖記錄跟追蹤主機資訊的人，無法推敲出真正的主機資訊。
Topology Hiding(隱藏拓撲)	隱藏網路架構圖(拓撲圖)對於網路管理人員也是很重要的，包括隱藏內部路由器及內部連接狀況。	參考 RFC 4864[16]，作法在 RFC 3014[11]內有描述，主要是透過有期限限制的 IPv6 資訊，避免網路拓撲被收集跟窺探。
Simple Security(簡單安全)	因為外部主機無法直接連接到 NAT 內的主機，因為 NAT 通常是為一種安全機制。 但是不應該將 NAT 跟防火牆混淆，兩者是不同的。NAT 是把幫忙建立內部機器與外部連線，而防火牆則是控管網路安全。	透過防火牆過濾跟阻擋不安全的連線是主要解決方案，而不是誤以為用了 NAT 就可以做到簡單安全。

第三節 IPv4 與 IPv6 網路攻擊方式

IPv6 與 IPv4 最大的不同在 IP 層，而 IP 層的上層（HTTPS、SSH）或下層（交換器、實體機器）的實作方式並無不同，因此 IPv6 繼承了 IPv4 的安全漏洞。在 IPv6 中名稱與 IPv4 不同，但應用方式類似的，面臨的漏洞的很像，說明如下：

1. 應用層的漏洞：應用層的漏洞與 IP 層無關。
2. NDP 協定的漏洞：IPv6 的 NDP 協定繼承了很多 IPv4 的 ARP 相關漏洞，例如惡意節點可藉由 NDP 進行如阻斷服務攻擊（DoS）及中間人攻擊（Man in the middle）。
3. DHCP 的漏洞：DHCPv6 預設沒有支援認證機制，所以也會有跟 DHCPv4 一樣的偽造 DHCP 回應的安全問題。
4. DDoS 的威脅：IPv6 雖然不支援 Broadcast，可以避免在 IPv4 的 Traffic Amplification 攻擊問題，例如 Smurf 攻擊。但是對於 DDoS 也是沒有防禦能力。
5. Main-in-the-Middle 攻擊問題：IPv6 的 IPSec 並無強制使用，只是規定要實作在 IPv6 的 Framework 中，因此 Main-in-the-Middle 問題一樣存在。

以下我們以常見的網路攻擊，來探討 IPv4 與 IPv6 的網路攻擊方

式。

表 13　IPv4 與 IPv6 的網路攻擊方式

攻擊名稱	IPv6	IPv4
網路竊聽 (Sniffing)	攻擊方式同 IPv4。	駭客擷取網路上傳遞的封包，例如把設備接在 hub 或者機房上。
應用層的威脅 (Application)	應用層的攻擊跟網路層的攻擊屬於不同層的攻擊，主要要注意的 IP 存取或者授權。	應用層的攻擊跟網路層的攻擊屬於不同層的攻擊，主要要注意的 IP 存取或者授權。
未經驗證或者偽冒的裝置(Rogue Devices)	1. 駭客已經存取網路，但是尚未取的機密資料，如果網路此時是用 IPv6 Stateless Address Autoconfiguration，駭客可以在網路上發布 IPv6 Router Advertisement。收到這個 Router Advertisement 的 IPv6 主機將會設定 IPv6 Route，造成第一個連結點為駭客設備。 2. 如果在上述情境中，資料主機有設定 IPv4 ACL 卻沒有設定 IPv6 ACL，駭客可以利用 IPv6 位址來攻擊漏洞。 3. 如果防火牆無法辨	駭客利用偽冒的 DHCP Sever，發布訊息給 DHCP Clients，造成第一個連結點為駭客設備。

	識在一條 IPv4 建立的 tunnel 內的 IPv6 封包，駭客就有機會入侵。	
中間人攻擊(Man-in-the middle attack; MITM)	1. 駭客利用假冒的 Router Advertisement 來設定網路，並影響路由。 2. 駭客再利用 NAT-PT(Network Address Translation - Port Translation)或 NAT64 建置一條 tunnel 來將 IPv6 位址轉為 IPv4 位址，此時駭客就可以藉由觀察封包，看到全部封包內容。	駭客偽冒一台 DHCP server，發布偽造的 DNS 及 gateway 資訊，造成 DHCP client 以駭客主機為第一個連結節點。
洪水攻擊(Flood Attack)	1. 駭客修改 extension headers 可以導致連結的兩個節點之間發生 denial of service 攻擊。 2. Hop-by-Hop header 及 Router Alert option 當很多封包在傳輸時，可能會造成路由器效能下降。 3. 駭客藉由變更 TCP SYN flag 導致 Fragmentation 問題。 4. 駭客修改 flow label，並提供大量不同的 flow label 來降低路由效能。	1. Zero Day(0day) DDoS 2. Ping Flood 利用一堆偽造的 Ping 封包攻擊。 3. IP Null Attack 駭客封包 header 設為 zero 通過安全檢查。 4. CharGEN Flood 傳送大量攜帶偽造 IP 的小型 UDP 封包給啟用 CharGEN 的設備(例如印表機)。 5. SNMP Flood 傳送大量攜帶偽造 IP 的

	5. Neighbor Discovery 讓駭客可以提供偽造的重複位址以癱瘓其他主機。 6. 駭客可以透過ND協定，發布偽造的 Router Advertisement，並不斷的變更 prefix，造成接收端癱瘓。 駭客可以利用偽造的受害主機 IP 發送 Multicast 造成主機癱瘓。	小型 UDP 封包給啟用 SNMP 的設備。 6. NTP Flood 傳送大量攜帶偽造IP的小型 UDP 封包給啟用 NTP 的設備。 7. SSDP(Simple Service Discovery Protocol;簡單服務發現協定) Flood 傳送大量攜帶偽造 IP 的小型 UDP 封包給啟用通用隨插即用(UPnP)的設備。 8. Fragmented HTTP Flood 駭客利用跟 web server 建立 HTTP 連線，但是將 HTTP 封包切割成很多小的 fragment，然後緩慢的送給 web server，直到 server timeout。 9. HTTP Flood 駭客發送大量的 GET、POST 或者其他 HTTP requests 以消耗 web server 資源。 10. Single Session HTTP Flood 駭客傳送大量的難以判斷的 session request。 11. Single Request HTTP Flood 駭客

		利用一個 HTTP session 內發出多個 HTTP requests。 12. Recursive HTTP GET Flood 駭客藉由重複抓去大量的資料如圖片、檔案以消耗主機資源 13. Random Recursive GET Flood 駭客以 bot 抓取有換頁功能的頁面，不斷以隨機方式的執行換頁並讀取。 14. Multi-Vector Attacks 駭客將多種攻擊方式混合一起攻擊目標網站。 15. SYN Flood 駭客偽造並傳送大量 SYN 封包給目標主機，因為一個新的封包表示是初始化一個新的 session，造成主機癱瘓。
網路掃描(Scan)	1. 困難，因為網段內 IP 數量太多 2. 但在 Dual-stack 下，駭客可以掃描 IPv4 的 Hosts 也可以攻擊主機。	直接以如 nmap 的工具對目標主機的 class C 進行掃描便可快速獲得網段內的主機 IP 及開放的 Port。
蠕蟲感染跟傳播(Worm)	2002 年第一隻 IPv6 蠕蟲 Slapper 被發現，主要是攻擊 Apache Server 並利用大部分設備具有 Dual-stack 的特性來找	IPv4 蠕蟲問題一直都很嚴重，也沒有比較好的解決方案。

	出 IPv4 的節點，然後利用這些節點來發動 IPv6 的 Flooding 攻擊。	
Broadcast Amplification Attack	IPv6 使用 Multicast 來達成 Broadcast 功能，使用 Multicast Listener Discovery 簡稱 MDL，它是從 IGMPv2(Internet Group Management Protocol version2)衍生而來，而 MLD 是 ICMPv6 的子協議，也就是說 MLD 是整個 ICMPv6 信息的子集合。而與 ICMPv6 有關的包括 NS、NA、RS、RA 及 DHCPv6 都是用 Multicast 來達成，因此偽冒與欺騙的攻擊也會存在。	駭客產生假的 Echo request，內容為受害者 IP。該封包被傳送到 Broadcast 網路。所有該網路上的主機都收到該偽造的封包。每台主機回應一個 ICMP 封包給受害主機，造成該主機被癱瘓。
DDoS 攻擊	對 FF02::1 發送 ICMPv6 Echo 迫使同網段的所有 Nodes 發送 ICMPv6 Reply 來對目標節點做 Flood 攻擊。	因為有 Broadcast，駭客利用 ICMP Echo 使網段內所有 Hosts 回應 ICMP Reply 造成大量封包。
IPv6 Latent Threats(潛伏攻擊)	駭客因為 IPv6 大量的佈建與使用而讓 IPv6 的安全問題與漏洞浮出檯面。例如現有的安全政策大都是以 IPv4 為主，對 IPv6 卻缺乏。	此部分是探討 IPv6 協定使用普及之後可能衍生的問題。
新增的 Extension header injection 攻擊	1. Next headers 的掛載順序攻擊 2. Hop-by-Hop Option Header 攻擊的	此部分是探討 IPv6 因為 header 變更而衍生的新問題。

	Padding 攻擊 3. Destination Option Header 的 Padding 攻擊 4. Routing Header 的 RH0 攻擊 5. Fragmentation Header 的攻擊 6. Upper Layer Header 的攻擊	
Dual-stack 引起的風險	在 Dual-stack 架構中，IPv4 與 IPv6 是共存於 Layer 2 之上，只是各自使用不同的 Ethernet Type，對於 TCP/UDP 是不受影響，對最上層的應用層也是不受影響的，對應用層有影響的地方只有應用程式的部分，例如記錄 IP 位址或者使用 IP 位址作為驗證。	此問題為啟用 IPv4/IPv6 才有的新問題。
Tunnel Injection 及 Sniffing	駭客如果知道 Configured Tunnel 的 IPv4 位址，可以把偽照的封包注入到 IPv6 的網路中，並且竊聽到 IPv6 封包的傳送。	駭客在進入被攻擊者網路之後，偽冒身份建立 tunnel，導致被害主機的資料遭受竊取。

第四節 IPv4 與 IPv6 網路攻擊的防禦措施

表 14　網路攻擊的防禦措施

攻擊名稱	IPv6	IPv4
網路竊聽(Sniffing)	利用 IPv6 內建的 IPSec protocol 進行 Layer 3 的資料傳遞加密	1. 利用 IPSec protocol 進行 Layer 3 的資料傳遞加密 2. 添購 IPSec 硬體設備建立重要主機之間的連線
應用層的威脅(Application)	應用層的攻擊跟網路層的攻擊屬於不同層的攻擊，主要要注意的 IP 存取或者授權。	應用層的攻擊跟網路層的攻擊屬於不同層的攻擊，主要要注意的 IP 存取或者授權。
未經驗證或者偽照的裝置(Rogue Devices)	1. 關閉 RA，每一台重要主機都手動設定 IP、DNS 2. 針對 IPv6 設定 ACL 3. 防火牆過濾 IPv6 封包，且可以檢查 IPv4 tunnel 內的 IPv6 封包 4. 在交換機啟用 RA Guard 或 ND Detection，對於每一個 Router Advertisement 檢查是否正確，不正確的就丟棄。(注意：RA Guard 或 ND Detection 只是一個保護方法的統稱)	1. 利用防火牆管理 IP 2. 確保機器 IP 跟 MAC address 是有被驗證的 3. 使用 ACL 避免非法的 IP 入侵 4. 使用白名單限制連線
中間人攻擊(Man-in-the middle attack,	1. 利用 IPSec protocol 進行 Layer 3 的資料傳遞加密	1. 利用 IPSec protocol 進行 Layer 3 的資料傳遞加密

MITM)	2. 在 Layer 2 進行安全控管 3. 依據 RFC 3971 跟 6494，使用 SEcure Neighbor Discovery(SEND)，使用獨立的 IPSec 以加密方法保護 NDP	2. 手動設定 DHCP Server 跟 DNS Server 及 default gateway
網路掃描 (Scan)	困難，因為網段內 IP 數量太多	以防火牆阻擋網段掃描
蠕蟲感染跟傳播(Worm)	因為 IPv6 的位址完全是階層式，所以可以利用此特性，做入口/出口過濾。	以防火牆及防毒軟體來阻擋 Worm 的感染及散步。
Broadcast Amplification Attack	Broadcast 已經在 IPv6 移除。	1. 在路由器跟防火牆上禁止使用 IP broadcasting 位址。 2. 禁止 ICMP 封包。
DDoS 攻擊 (洪水攻擊 (Flood Attack)	1. 啟用 SEcure Neighbor Discovery (SEND) protocol 2. 啟用 Bogon route services，例如由 Team Cymru 所維護的 bogon prefix 用來處理不應該出現在網路上的 prefix。 3. 使用防火牆阻擋 4. 使用 Content Delivery Networks(CDN) 5. 啟用 IPS 或 IDS 6. 啟用 Application Delivery Controller(ADC)	1. 使用防火牆阻擋 2. 使用 Content Delivery Networks(CDN) 3. 啟用 IPS 或 IDS 4. 啟用 Application Delivery Controller(ADC)
IPv6 Latent Threats	使用具備 IPv6 能力的設	此為因為使用 IPv6 而衍

	備來過濾跟防護 Hosts 對 IPv6 攻擊與漏洞威脅。例如使用支援 IPv6 的 NIPS(網路型入侵防禦)、HIPS(主機入侵預防系統)或者 Firewall。	生的議題。
新增的 Extension header injection 攻擊	1. 啟用 RA-Guard 2. 升級到最新的作業系統，因為新的系統通常會增加對較新 RFC 的支援	此為因為使用 IPv6 而衍生的議題。
Dual-stack 引起的風險		此為因為使用 IPv6 而衍生的議題。
Tunnel Injection 及 Sniffing	1. 利用支援 IPv6 的設備來檢查來源跟目的地的 IPv6 位址並進行過濾。 2. 使用 IPSec 建立安全通道	1. 使用 IPSec 建立重要主機之間的安全通道 2. 使用白名單限制 Tunnel 的存取

第四章　ICP IPv6 設定及 IPv6 網路安全檢測

第一節 IPv6 設定檢測

針對 IPv6 之設定是否已成功完成,將其必要的統整項目整理至下表中，可透過表格中敘述的測試工具與測試方式，判斷網路設備是否已支援 IPv6。

表 15　ICP 業者的 IPv6 設定檢測表

編號	分類	設定測試	必測與否	通過條件	測試方式	測試工具
CT-1	主機	網站的 IPv6 位址可以連上 (http 或 https)	是	Trying 顯示 IPv6 位址、出現 TCP_NODELAY set、Connected to Connected to 網址(IPv6 位址) port 443 、並顯示 successfully set certificate verify locations 出現 HTTP/2 200	curl -v 網址 --head	curl
CT-2	路由器	沿途路由器都有 IPv6 位址	是	顯示沿途路由器 IPv6 位址	traceroute6 根網域	traceroute6
CT-3	DNS	網站是否	是	顯示 IPv6 位	dig aaaa 根	dig

		有正確設定 IPv6 位址		址	網域 @8.8.8.8 +short	
CT-4	DNS	網站使用的所有 DNS Server 本身要有 IPv6 位址	是	顯示 IPv6 位址	for i in `dig @8.8.8.8 +short NS 根網域`; do echo -n "$i => [ipv6] "; dig aaaa $i @8.8.8.8 +short; done	dig
CT-5	DNS	網站使用的 DNS 的 IPv6 都可以 PING 通過	是	成功顯示 PING 到的 IPv6 位址	ping6 根網域	ping6
CT-6	DNS	網站使用的 DNS 要設定網站根網域的 IPv6 位址	是	顯示 IPv6 位址	for i in `dig @8.8.8.8 +short NS 根網域`; do echo -n "$i => [ipv6] "; dig aaaa 根網域 @$i +short; done	dig
CT-7	Mail Server	網站使用的 Mail Server 都要有 IPv6 位址，且可以連得上	是	顯示 IPv6 位址	for i in `dig @8.8.8.8 +short MX 根網域`; do echo -n "$i => [ipv6] ";	dig

					dig aaaa $i @8.8.8.8 +short; done;	

以 TWNIC 財團法人台灣網路資訊中心(www.twnic.net.tw)為例，分別針對上表 ICP 業者的 IPv6 設定檢測表的測試項目進行測試。

1. 網站的 IPv6 位址可以連上（http 或 https）

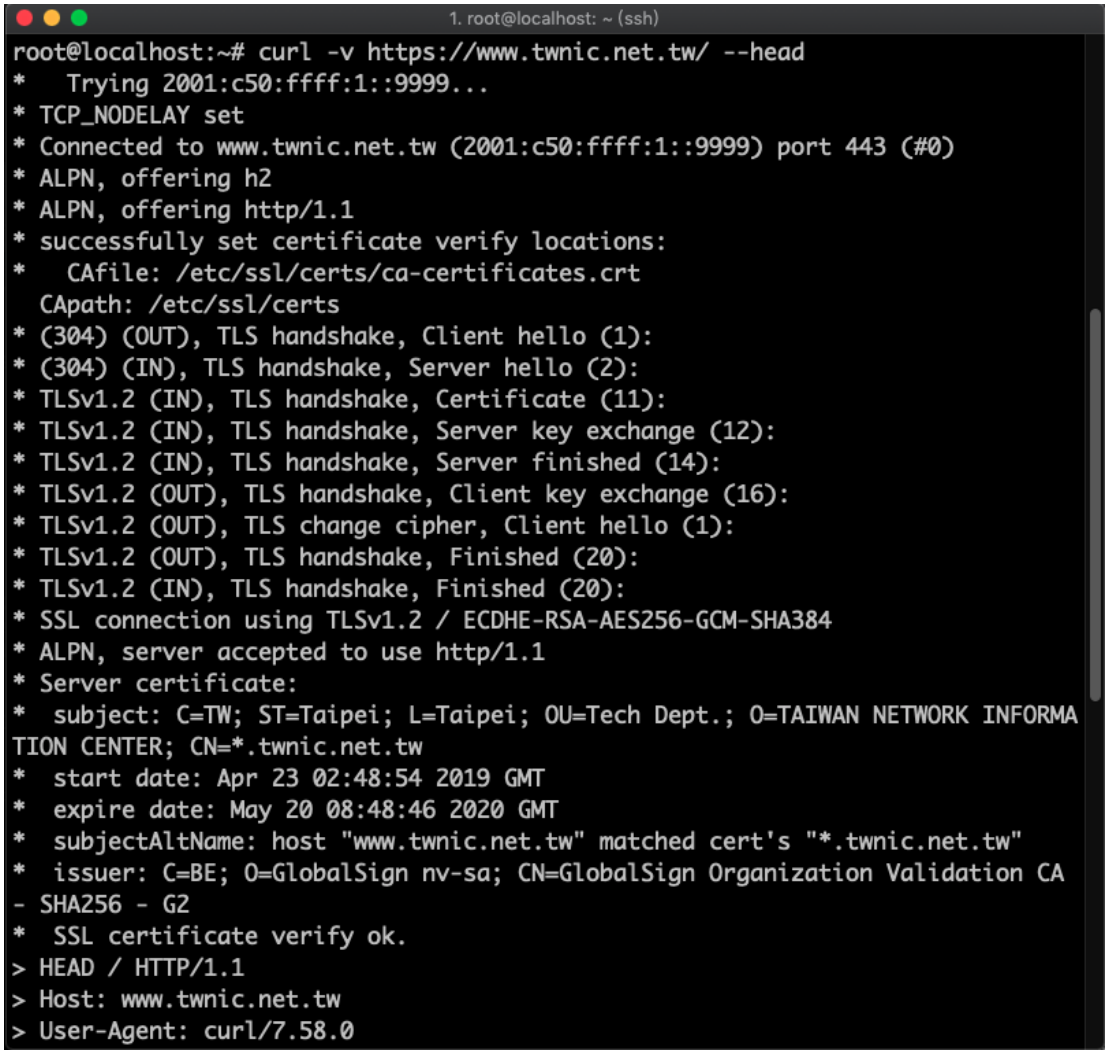

圖 9　TWNIC CT-1 測試結果畫面之一

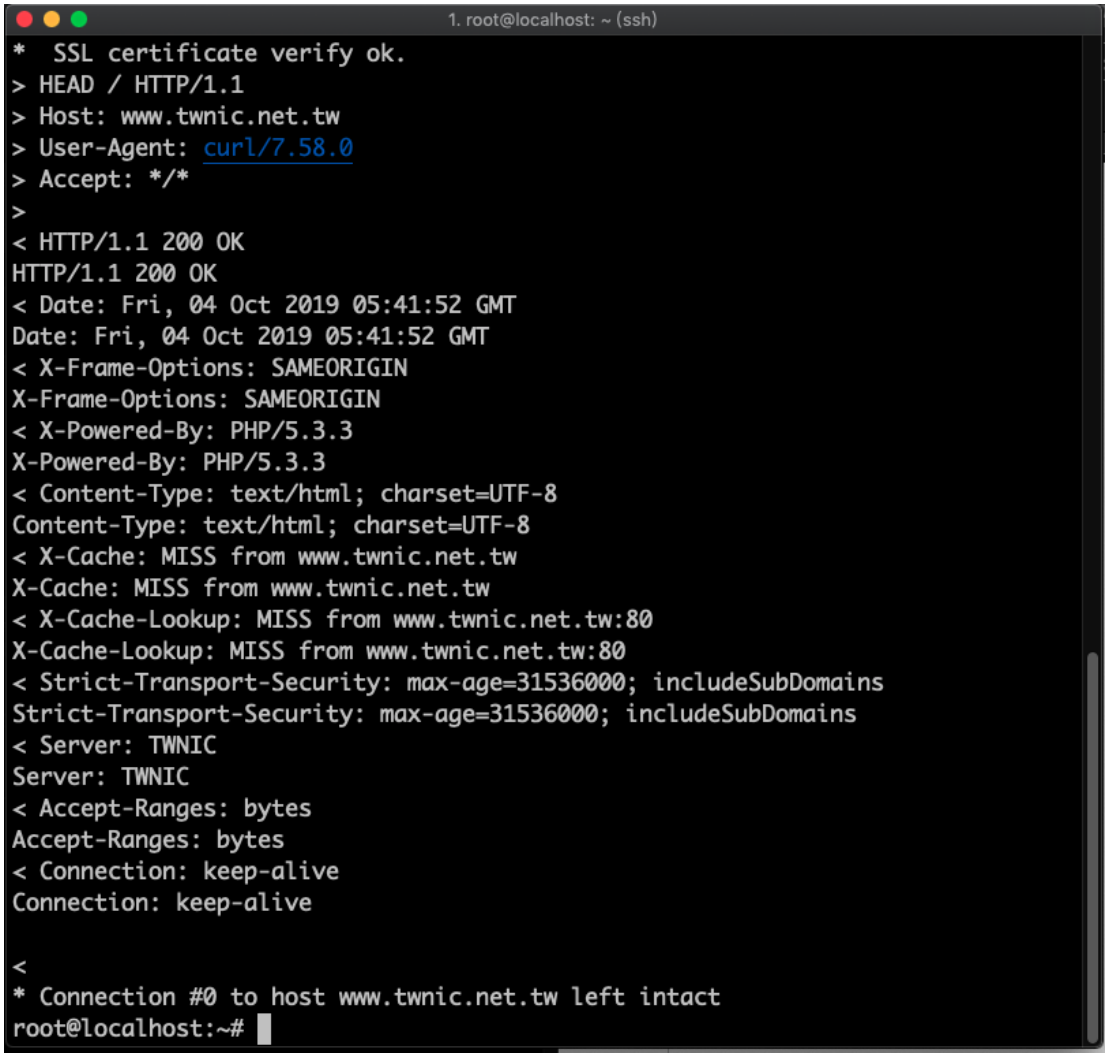

圖 10　TWNIC CT-1 測試結果畫面之二

2.　沿途路由器都有 IPv6 位址

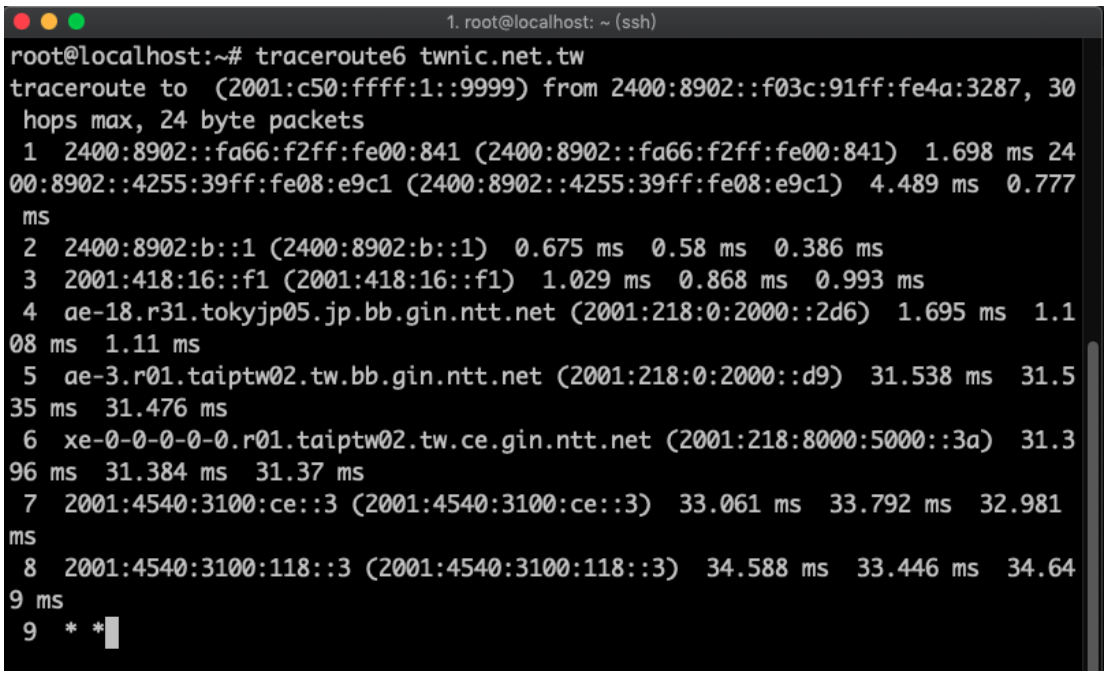

圖 11　TWNIC CT-2 測試結果畫面

3. 網站是否有正確設定 IPv6 位址

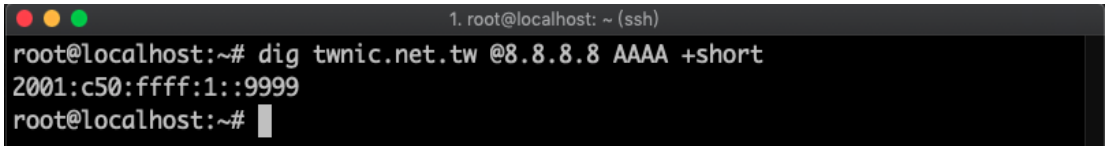

圖 12　TWNIC CT-3 測試結果畫面

4. 網站使用的所有 DNS　Server 本身要有 IPv6 位址

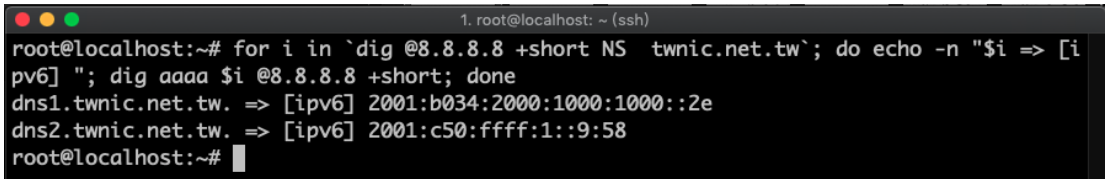

圖 13　TWNIC CT-4 測試結果畫面

5. 網站使用的 DNS 的 IPv6 都可以 PING 通過

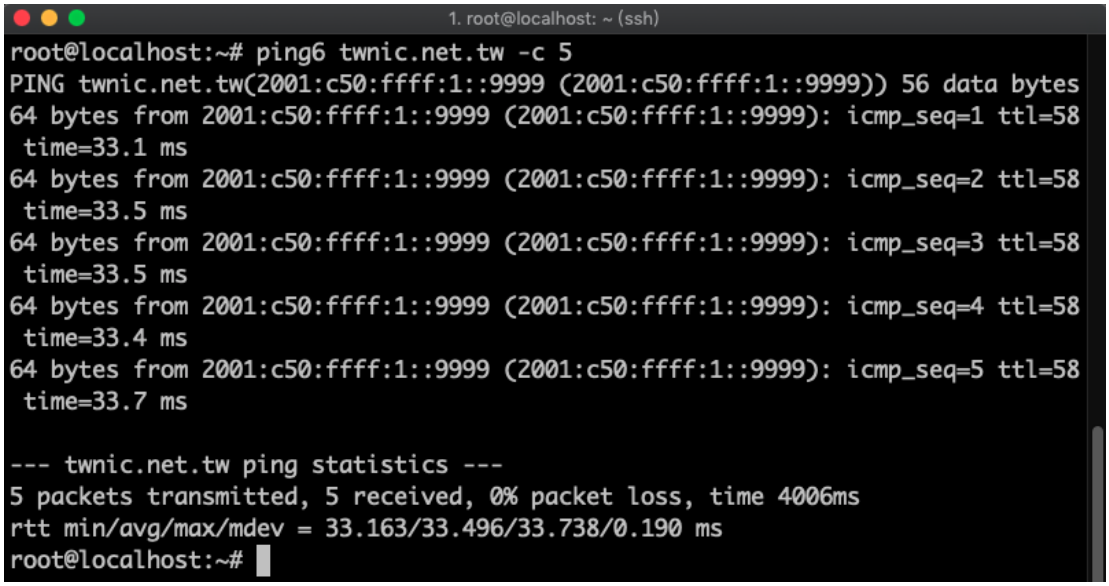

圖 14　TWNIC CT-5 測試結果畫面

6. 網站使用的 DNS 要設定網站根網域的 IPv6 位址

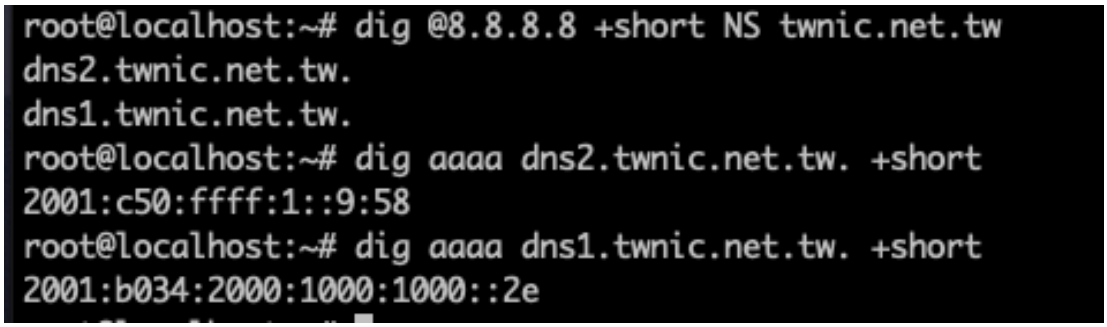

圖 15　TWNIC CT-6 測試結果畫面

7. 網站使用的 Mail Server 都要有 IPv6 位址，且可以連得上(TWNIC 的 MX 沒有設定 IPv6）

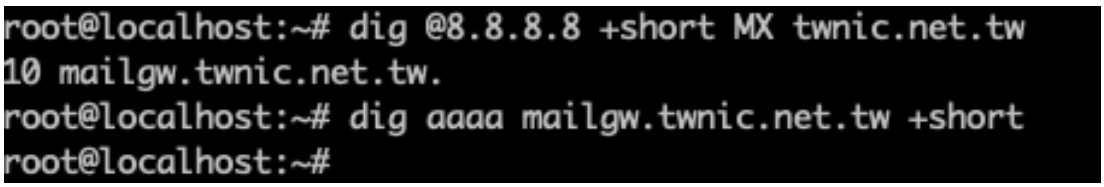

圖 16　TWNIC CT-7 測試結果畫面

第二節 網路安全檢查檢測

下表列出雙協定網路下可以檢測的安全項目與工具，透過測試工具可以模擬外界常見的網路攻擊，並檢視其結果是否通過，惟並非所有工具皆可已從外網進行測試，故於表格後僅提供可以從外網進行的測試結果範例，其餘工具還要自行於內網中進行測試並檢測其結果。

表 16　雙協定網路安全檢測項目

編號	分類	網路安全測試項目	必測與否	測試方式	測試工具
以下為 IPv6 測試使用(可於外網進行測試)					
ST-1	路由器	未經驗證或者偽照的裝置	是	thcsyn6 [-AcDrRS] [-p port] [-s sourceip6] interface target port	thcsyn6
ST-2	路由器	未經驗證或者偽照的裝置	是	exploit6 interface destination [test-case-number]	exploit6
ST-3	路由器	DDoS 攻擊（ICMPv6）	是	fuzz_ip6 [-x] [-t number | -T number] [-p number] [-IFSDHRJ] [-X|-1|-2|-3|-4|-5|-6|-7|-8|-9|-0 port] interface unicast-or-multicast-address [address-in-data-pkt]	fuzz_ip6

ST-4	路由器	Ping of Death（PoD）	是	frag6 -i [interface] --frag-id-policy -d [destination]	frag6
ST-5	路由器	網路掃描	是	flow6 -i [interface] --flow-label-policy -d [destination] -v	flow6
ST-6	網站主機	DDoS 攻擊（Smurf 攻擊）	是	implementation6 [-p] [-s sourceip6] interface destination [test-case-number]	implementation6
ST-7	其他	DDos 攻擊（Duplicate Address Detection）	是	flood_mld6 interface	flood_mld6
ST-8	其他	Upper Layer Header 的攻擊	是	flood_mld26 interface	flood_mld26
ST-9	其他	Atomic Fragment 攻擊	是	denial6 interface destination test-case-number	denial6
以下為 IPv6 測試使用(需於內網進行測試)					
ST-10	路由器	DDoS 攻擊(Router Advertisement）	是	inject_alive6 [-ap] interface	alive6
ST-11	路由器	DDoS 攻擊（neighbor advertise	是	inject_alive6 [-ap] interface	alive6

		ments）			
ST-12	路由器	DDoS 攻擊（MLD reports）	是	redir6 interface victim-ip target-ip original-router new-router [new-router-mac] [hop-limit]	redir6
ST-13	路由器	DDoS 攻擊（MLDv2 reports）	是	dos-new-ip6 interface	dos-new-ip6
ST-14	路由器	中間人攻擊	是	fake_mipv6 interface home-address home-agent-address care-of-address	fake_mipv6
ST-15	路由器	DDoS 攻擊（unknown options）	是	fake_advertise6 [-DHF] [-Ors] [-n count] [-w seconds] interface ip-address-advertised [target-address [mac-address-advertised [source-ip-address]]]	fake_advertiser6
ST-16	網站主機	DDoS 攻擊（Smurf 攻擊）	是	implementation6d interface	implementation6d
ST-17	DNS	滲透測試	是	flood_dhcpc6 [-n|-N] [-1] [-d] interface [domain-name]	flood_dhcpc6
ST-18	DNS	未經驗證或者偽照的裝置	是	toobig6 [-u] interface target-ip existing-ip mtu [hop-limit]	toobig6
ST-19	DNS	未經驗證	是	fake_dns6d interface	fake_dns6

		或者偽照的裝置		ipv6-address [fake-ipv6-address [fake-mac]]	d
ST-20	DNS	未經驗證或者偽照的裝置	是	fake_dnsupdate6 dns-server full-qualified-host-dns-name ipv6address	fake_dnsupdate6
ST-21	作業系統	CVE-2003-0429 Ethereal OSI 解析緩衝區溢位漏洞	是	mitm6.py [-h] [-i INTERFACE] [-l LOCALDOMAIN] [-4 ADDRESS] [-6 ADDRESS] [-m ADDRESS] [-a] [-v] [--debug] [-d DOMAIN] [-b DOMAIN] [-hw DOMAIN] [-hb DOMAIN] [--ignore-nofqdn]	mitm6
ST-22	作業系統	CVE-2004-0257 OpenBSD ICMPv6 處理遠程 DDoS 攻擊漏洞	是	fake_mld6 [-l] interface add|delete|query [multicast-address [target-address [ttl [own-ip [own-mac-address [destination-mac-address]]]]]]	fake_mld6
ST-23	防火牆	DDoS 攻擊（TCP-SYN）	是	fake_mld26 [-l] interface add|delete|query [multicast-address [target-address [ttl [own-ip [own-mac-address [destination-mac-address]]]]]]	fake_mld26

ST-24	防火牆	網路掃描	是	fake_mldrouter6 [-l] interface advertise|solicitate|terminate [own-ip [own-mac-address]]	fake_mldrouter6
ST-25	防火牆	基本設定	是	fake_router6 [-HFD] interface network-address/prefix-length [dns-server [router-ip-link-local [mtu [mac-address]]]]	fake_router6
ST-26	防火牆	基本設定	是	flood_router6 [-HFD] interface	flood_router6
ST-27	其他	DDoS 攻擊	是	flood_advertise6 [-k | -m mac] interface [target]	flood_advertise6
ST-28	其他	未經驗證或者偽照的裝置	是	ndpexhaust26 [-acpPTUrR] [-s sourceip6] interface target-network	ndpexhaust26
ST-29	其他	未經驗證或者偽照的裝置	是	parasite6 [-lRFHD] interface [fake-mac]	parasite6
ST-30	其他	安全評估工具（flow label）	是	smurf6 interface victim-ip [multicast-network-address]	smurf6
ST-31	其他	掃描工具	是	rsmurf6 interface victim-ip	rsmurf6
以下為 IPv4 測試使用					
ST-32	路由器	中間人攻擊	是	arpspoof -i [Network Interface Name] -t [Victim IP]	Arpspoof

				[Router IP]	
ST-33	防火牆	DDoS 攻擊	是	hping3 --traceroute -V -1 網站	hping3
ST-34	防火牆	中間人攻擊	是	圖形化介面操作	ettercap
ST-35	防火牆	DDoS 攻擊，中間人攻擊	是	圖形化介面操作	Evil FOCA

以 TWNIC 財團法人台灣網路資訊中心（www.twnic.net.tw）為例，分別針對上表 ICP 業者的 IPv6 設定檢測表的可於外網進行測試的項目進行測試。

1. 使用 thcsyn6 測試工具

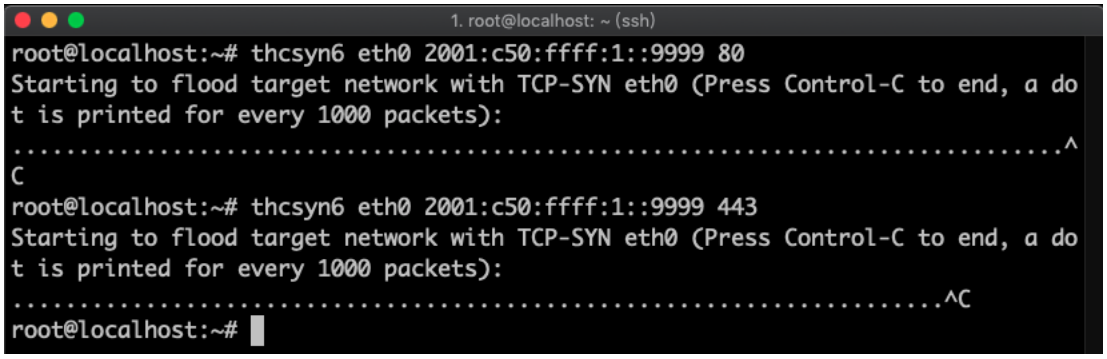

圖 17　TWNIC ST-1 測試結果畫面

2. 使用 exploit6 測試工具

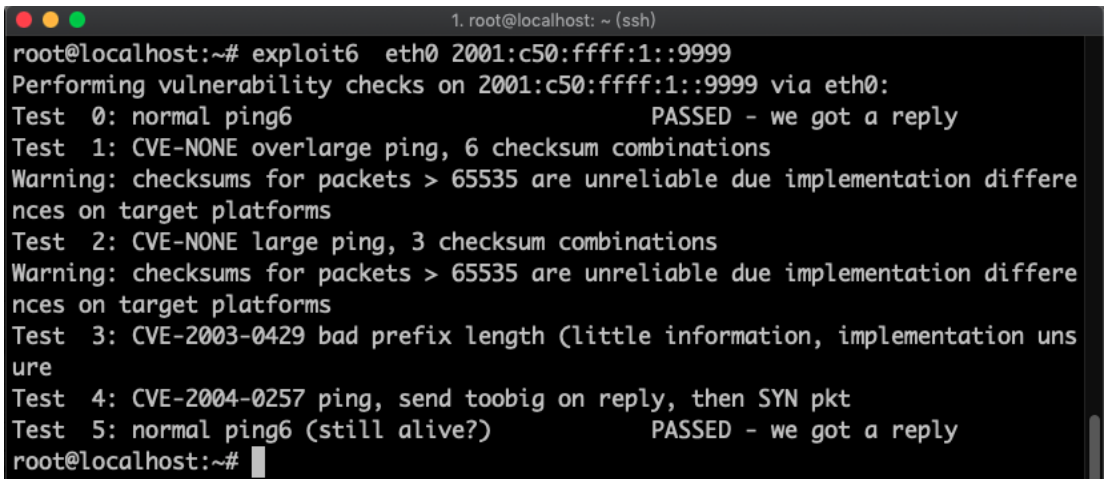

圖 18　TWNIC ST-2 測試結果畫面

3.　使用 fuzz_ip6 測試工具

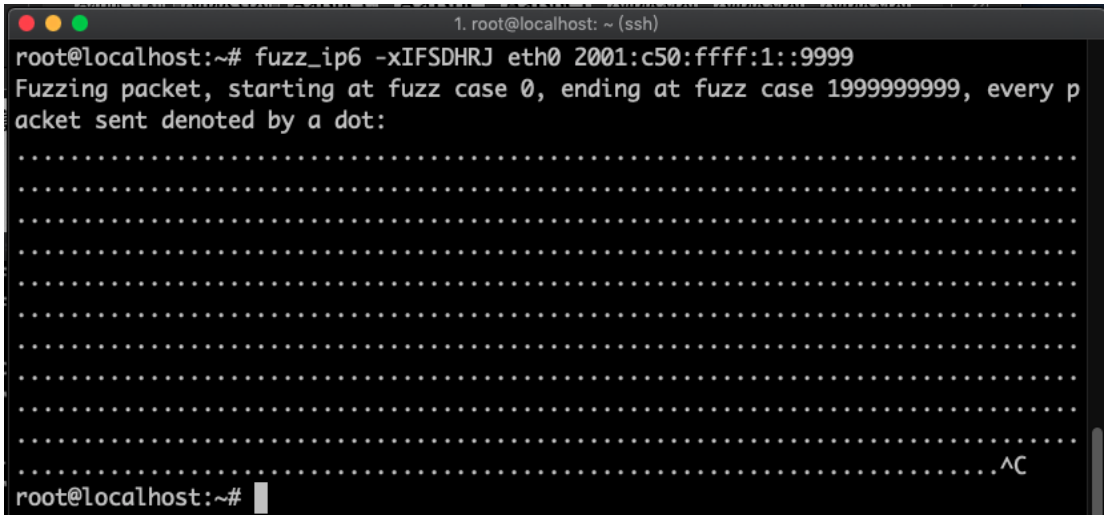

圖 19　TWNIC ST-3 測試結果畫面

4.　使用 frag6 測試工具

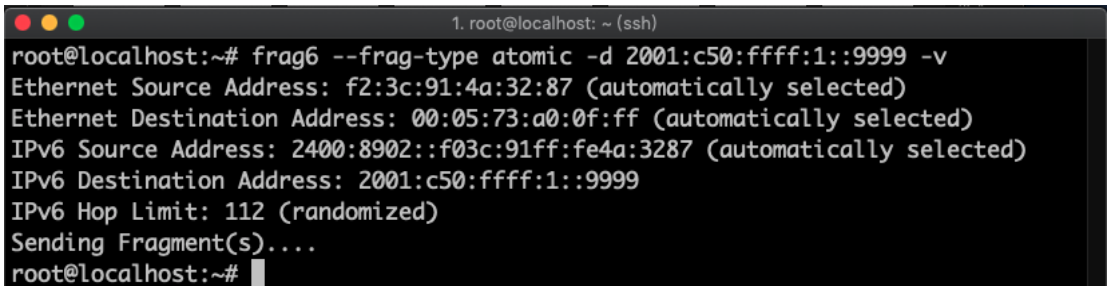

圖 20　TWNIC ST-4 測試結果畫面

5. 使用 flow6 測試工具

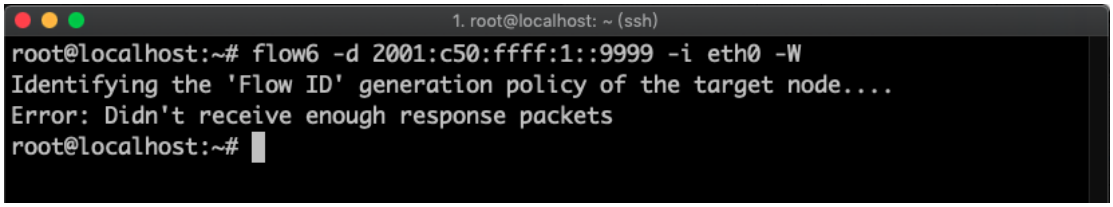

圖 21 TWNIC ST-5 測試結果畫面

6. 使用 implementation6 測試工具

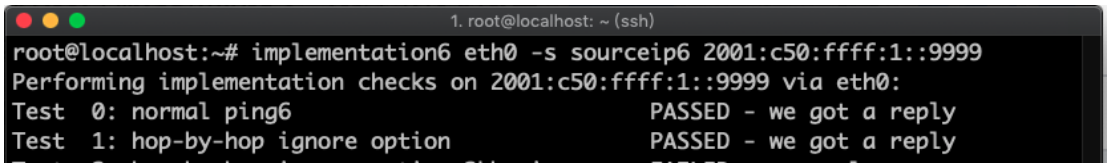

圖 22 TWNIC ST-6 測試結果畫面

7. 使用 flood_mld6 測試工具

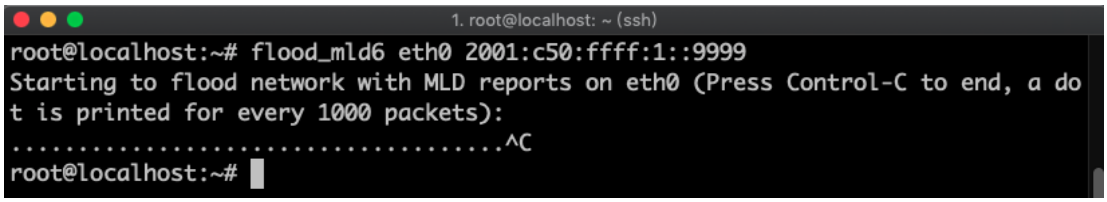

圖 23 TWNIC ST-7 測試結果畫面

8. 使用 flood_mld26 測試工具

圖 24 TWNIC ST-8 測試結果畫面

9. 使用 denial6 測試工具

圖 25　TWNIC ST-9 測試結果畫面

參考資料

[1] RFC 1546 Host Anycasting Service
https://tools.ietf.org/html/rfc1546
[2] RFC 1576 TN3270 Current Practices
https://tools.ietf.org/html/rfc1576
[3] RFC 1883 Internet Protocol, Version 6 (IPv6) Specification
https://tools.ietf.org/html/rfc1883
[4] RFC 1918 Address Allocation for Private Internets
https://tools.ietf.org/html/rfc1918
[5] RFC 1981 Path MTU Discovery for IP version 6
https://tools.ietf.org/html/rfc1981
[6] RFC 2401 Security Architecture for the Internet Protocol
https://tools.ietf.org/html/rfc2401
[7] RFC 2402 IP Authentication Header
https://tools.ietf.org/html/rfc2402
[8] RFC 2406 IP Encapsulating Security Payload (ESP)
https://tools.ietf.org/html/rfc2406
[9] RFC 2460 Internet Protocol, Version 6 (IPv6) Specification
https://tools.ietf.org/html/rfc2460
[10]RFC 2462 IPv6 Stateless Address Autoconfiguration
https://tools.ietf.org/html/rfc2462
[11]RFC 3014 IPv6 Stateless Address Autoconfiguration
https://tools.ietf.org/html/rfc3014
[12]RFC 3041 Privacy Extensions for Stateless Address Autoconfiguration in IPv6
https://tools.ietf.org/html/rfc3041
[13]RFC 3852 Cryptographic Message Syntax (CMS)
https://tools.ietf.org/html/rfc3852
[14]RFC 4301 Security Architecture for the Internet Protocol
https://tools.ietf.org/html/rfc4301
[15]RFC 4862 IPv6 Stateless Address Autoconfiguration
https://tools.ietf.org/html/rfc4862
[16]RFC 4864 Local Network Protection for IPv6
https://tools.ietf.org/html/rfc4864
[17]RFC 4941 Privacy Extensions for Stateless Address Autoconfiguration in IPv6
https://tools.ietf.org/html/rfc4941

[18]RFC 5902 IAB Thoughts on IPv6 Network Address Translation
https://tools.ietf.org/html/rfc5902
[19]RFC 5996 Internet Key Exchange Protocol Version 2 (IKEv2)
https://tools.ietf.org/html/rfc5996
[20]RFC 6437 IPv6 Flow Label Specification
https://tools.ietf.org/html/rfc6437
[21]RFC 6564 A Uniform Format for IPv6 Extension Headers
https://tools.ietf.org/html/rfc6564
[22]A Glance through the VPN Looking Glass: IPv6 Leakage and DNS Hijacking in Commercial VPN clients
https://petsymposium.org/2015/papers/02_Perta.pdf
[23]Understanding IPv6 And DNS Leaking, by Jay H Simmons
https://www.vpncrew.com/understanding-ipv6-and-dns-leaking/
[24]IPv6 Address Representation and Address Types, by Rick Graziani., 03 Oct 2017
http://www.ciscopress.com/articles/article.asp?p=2803866&seqNum=5
[25]The Difference Between IPv6 and IPv4 IP Addresses
https://www.coursehero.com/file/15205432/The-Difference-Between-IPv6-and-IPv4-IP-Addresses/
[26]IPV6 MULTICAST - MULTICAST LISTENER DISCOVERY （MLD）, by INE
https://blog.ine.com/2009/12/26/ipv6-multicast-multicast-listener-discovery-mld
[27]Internet Protocols: Versions 4 and 6 Analysis and Comparison of IPv4 and IPv6, by Wushi09, 21 Sep 2015
https://www.cybrary.it/0p3n/internet-protocols-versions-4-and-6-analysis-and-comparison-of-ipv4-and-ipv6/
[28]為何值得為 IPv6 的建置努力的三大理由，台網中心電子報 2019/02
https://blog.twnic.net.tw/2019/01/31/2361/
[29]What is IPv6 stateless address auto-configuration
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=2ahUKEwiBpeiroq3kAhXMGKYKHWMhAbYQFjACegQIDBAG&url=https%3A%2F%2Fmysupport.netapp.com%2FNOW%2Fpublic%2Feseries%2Fsam%2FGUID-85382

72A-B802-49D9-9EA2-96C82DAD26A2%2FGUID-06C52868-5C1F-4E76-86D5-4815C2E9EBC6.html&usg=AOvVaw2Bil-09MU4QCW5earvN8lT

[30]中華電信公司 HiNet IPv6 用戶連線參考手冊

http://adsl.hinet.net/download/HiNet-IPv6_User_Guide.pdf

[31]中華電信 HiNet IPv6 固定制服務說明

http://adsl.hinet.net/static_ipv6.html

[32]QoS — 未來行動網路的服務品質保證

https://www.ctimes.com.tw/DispArt/tw/-IPv4/IETF/-IEEE/-MOD/-VoIP/0404251100SZ.shtml

[33]IPv6 Routing for Mobility Environments
https://www.researchgate.net/publication/228395858_IPv6_Routing_for_Mobility_Environments

[34]台灣 2018 年 IPv6 成長速度創全球第一，台網中心電子報 2019/04

https://blog.twnic.net.tw/2019/03/29/3058/

[35]IPv6/IPv4 IPv6/IPv4 轉換技術

http://www.ipv6.org.tw/docu/elearning8_2005/1009402616b-19.pdf

[36]IPv6 Fundamentals: A Straightforward Approach to Understanding IPv6
https://books.google.com.tw/books?id=FbYjJjZNA5gC&pg=PA335&lpg=PA335&dq=ipv6+0x0800+0x86DD&source=bl&ots=5mIjGIwW_E&sig=ACfU3U34zzWevIUhxbY4H7HL3ofpwDgKpg&hl=zh-TW&sa=X&ved=2ahUKEwjbxp3A167kAhXjGKYKHYrSCbIQ6AEwEnoECAcQAQ#v=onepage&q=ipv6%200x0800%200x86DD&f=false

[37]IPv6 跟現階段 IP 位址配發差異與發展技術介紹

https://www.cadch.com/modules/news/article.php?storyid=132

[38]剖析 IPv6 的安全風險問題

http://www.rl-tech.com.tw/zh-tw/article_info.php?id=13

[39]IPv6 Security
https://books.google.com.tw/books?id=kwOv0Aw2lIUC&pg=PT360

&lpg=PT360&dq=ipv6+esp&source=bl&ots=Qmr93IAZ4f&sig=ACfU3U171Cq1dpyz0vyy1eSsYSmXg8hB7g&hl=zh-TW&sa=X&ved=2ahUKEwjSoJSL36_kAhUNCqYKHRuuCGM4ChDoATADegQIBhAB#v=onepage&q=ipv6%20esp&f=false

[40]Configuring IPv6 For Cisco IOS
https://books.google.com.tw/books?id=rj45JvYuOdIC&pg=PA275&lpg=PA275&dq=HMAC+ipv6&source=bl&ots=_jaIgiQBij&sig=ACfU3U1uuYAvFBGqK4JpBhDLJQBrPYiMuA&hl=zh-TW&sa=X&ved=2ahUKEwinmbC24a_kAhVHGaYKHTFbBTYQ6AEwB3oECAcQAQ#v=onepage&q=HMAC%20ipv6&f=false

[41]剖析 IPv6 的安全風險問題

http://www.rl-tech.com.tw/zh-tw/article_info.php?id=13

[42]IPv6 作業系統與應用服務建置實習（Linux）

http://www.wkb.idv.tw/moodle/pluginfile.php/15554/mod_page/content/7/IPv6%20Linux 講義.pdf

[43]中華電信 IPv6 通訊協定與特性介紹

http://163.28.82.8/data2/seminar99/ipv611.pdf

[44]IPv6 Packet Security
http://www.ipv6now.com.au/primers/IPv6PacketSecurity.php

[45]IPv6 Fundamentals: A Straightforward Approach to Understanding IPv6
https://books.google.com.tw/books?id=AMkmDwAAQBAJ&pg=PT111&lpg=PT111&dq=why+ipv6+doesn%27t+need+ihl&source=bl&ots=dpjoVgYmmv&sig=ACfU3U0XBRFNlOAC8zLPTf9zs5k1rp-rHw&hl=zh-TW&sa=X&ved=2ahUKEwj1l_7y06rkAhUiy4sBHTweC5QQ6AEwCnoECAgQAQ#v=snippet&q=security&f=false

[46]An integrated testing system for IPv6 and DNSSEC
https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/s13638-016-0675-4

[47]IPv6 Security: Attacks and Countermeasures in a Nutshell
https://www.sba-research.org/wp-content/uploads/publications/Johanna%20IPv6.pdf

[48]IPv6-ready system check
http://tldp.org/HOWTO/Linux+IPv6-HOWTO/ch04s01.html

[49]ROGUE ROUTER ADVERTISEMENT ATTACK
http://6lab.cz/rogue-router-advertisement-attack/
[50]How To Detect & Prevent Rogue Devices on Your Network with UDT
https://www.youtube.com/watch?v=EZBaiEDTrfQ
[51]Attackers Can Use IPv6 to Launch Man-in-the-Middle Attacks
https://www.eweek.com/security/attackers-can-use-ipv6-to-launch-man-in-the-middle-attacks
[52]IPv6 MITM via fake router advertisements
https://isc.sans.edu/forums/diary/IPv6+MITM+via+fake+router+advertisements/10660/
[53]35 Types of DDoS Attacks Explained
https://javapipe.com/blog/ddos-types/
[54]Could IPv6 Result in More DDoS Attacks?
https://www.allot.com/blog/ipv6_ddos_attack_vulnerability/
[55]How to Prepare for IPv6 DDoS attack
https://medium.com/@CybriantMSSP/how-to-prepare-for-ipv6-ddos-attack-4620cba369fc
[56]IPv6 DDoS and Protection Measures
https://community.infoblox.com/t5/IPv6-CoE-Blog/IPv6-DDoS-and-Protection-Measures/ba-p/12830
[57]IPv6 extension headers and security: Analyzing the risk
https://searchsecurity.techtarget.com/tip/IPv6-extension-headers-and-security-Analyzing-the-risk
[58]IPv6 Extension Headers Review and Considerations
https://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.html
[59]Recommendations on the Filtering of IPv6 Packets Containing IPv6 Extension Headers
https://tools.ietf.org/html/draft-ietf-opsec-ipv6-eh-filtering-04
[60]Security implication and detection of threats due to manipulating IPv6 extension headers
https://ieeexplore.ieee.org/document/6726061
[61]Security Impacts of Abusing IPv6 Extension Headers
https://media.blackhat.com/ad-12/Atlasis/bh-ad-12-security-impacts-atlasis-wp.pdf
[62]thc-ipv6 工具包

https://www.mankier.com/package/thc-ipv6
[63]Get your site ready for IPv6: a step-by-step guide
https://blog.mythic-beasts.com/2014/09/15/get-your-site-ready-for-ipv6-a-step-by-step-guide/
[64]How To Configure Tools to Use IPv6 on a Linux VPS, by Justin Ellingwood, 01 Apr 2014
https://www.digitalocean.com/community/tutorials/how-to-configure-tools-to-use-ipv6-on-a-linux-vps#checking-ipv6-dns-informatio
[65]ICANNWiki
https://icannwiki.org/IPv6
[66]IPv6 Multicast Address Space Registry
https://www.iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xhtml
[67]IPv6 multicast addresses
https://study-ccna.com/ipv6-multicast-addresses/
[68]中華電信研究所 NICI IPv6 標準測試分組電子報
http://interop.ipv6.org.tw/ENewsArchive/ENewsIPv6RFCUpdate(921001).htm
[69]維基百科 內送流量備援容錯機制
https://zh.wikipedia.org/wiki/%E5%85%A7%E9%80%81%E6%B5%81%E9%87%8F%E5%82%99%E6%8F%B4%E5%AE%B9%E9%8C%AF%E6%A9%9F%E5%88%B6
[70]Ettercap
https://www.ettercap-project.org/
[71]Evil FOCA
https://www.elevenpaths.com/labstools/evil-foca/index.html

中英專有名詞對照

A

ACL 存取控制列表（Access Control List）

ARP 位址解析協定（Address Resolution Protocol）

D

DDoS attack 阻斷服務攻擊（distributed denial-of-service attack）

DNS 網域名稱伺服器（Domain Name System）

DHCP 動態主機組態協定（Dynamic Host Configuration Protocol）

Dual Stack IPv4/ IPv6 雙協定（Dual Stack）

E

Email 電子郵件(Electronic mail）

F

Firewall 防火牆

FTP 檔案傳輸協定(File Transfer Protocol）

I

IaaS 基礎設施即服務（Infrastructure as a Service）

IAB 網際網路結構委員會（Internet Architecture Board）

ICMP 網際網路控制訊息協定（Internet Control Message Protocol）

ICMPv6 網際網路控制訊息協定第六版（Internet Control Message Protocol Version 6）

ICP 網路內容供應商（Internet Content Provider）

IETF 網際網路工程任務小組（Internet Engineering Task Force）

IDC 資訊機房（Internet Data Center）

IPsec 網際網路安全機制（Internet Protocol Security）

IPv4 網際網路通訊協定第四版（Internet Protocol version 4）

IPv6 網際網路通訊協定第六版（Internet Protocol version 6）

IPv6 Day IPv6 日（IPv6 Day）

IPv6 Ready Logo 網際網路通訊協定第六版認證獎章

IPv4/IPv6 Dual Stack 網際網路通訊協定第四版及第六版雙軌並行（IPv4/v6 Dual Stack）

ISP 網際網路服務提供者（Internet Service Provider）

IASP 網際網路服務提供者（Internet Access Service Provider）

IT 資訊技術（Information Technology）

L

L3 Switch 第三層交換器（Layer 3 Switch）

Load Balancers 負載平衡器

M

Mobile Internet 行動上網（Mobile Internet）

N

NAT 網路位址轉譯（Network Address Translation）

Network Layer 網路層（Network Layer）

P

Proxy 代理伺服器

Q

QoS 服務品質（Quality of Service）

R

RARP 逆位址解析協定（Reverse Address Resolution Protocol）

RFC 網際網路協定規範

（Request For Comments）

Router 路由器

T

TCP 傳輸控制協定

（Transmission Control Protocol）

TWNIC 財團法人台灣網路資訊

中心（Taiwan Network

Information Center）

W

WWW 全球資訊網（World Wide

Web）

WiFi AP 無線基地台（WiFi AP）