『前瞻及完整之 IPv6 生態系推動方案』

附錄六
『IPv6 用戶安全防護研析』手冊

財團法人台灣網路資訊中心

台灣網路資訊中心委託執行計畫

「Native IPv6 連網環境建置及 IPv6 用戶安全防護研析」

IPv6 家用用戶 資通安全防護技術手冊

計畫委託機關：台灣網路資訊中心

中華民國 109 年 06 月

摘要

隨著 IPv6 的發展，IPv6 安全風險開始浮現，亦挑戰 IPv6 網路防護能力，如何建構安全的網路防護機制，確保 IPv6 用戶資通安全，也是部署 IPv6 不可或缺的重要關鍵。本手冊將以 IETF IPv6 相關資通安全 RFC 標準為主，進行 IPv6 家用用戶資通安全防護相關議題研析，探討 IPv6 網路攻擊與防禦機制，並針對家用用戶網路 IPv6 網路安全管理提出建議。此外，ACL 是 IPv6 基本的 CPE 資安防護機制之一，故本手冊將以家用寬頻分享器 CPE 進行安全防護測試。手冊所得成果可提供我國 ISP 與家庭用戶 IPv6 部署參考。

目次

圖目錄

表目錄

壹、 前言

IPv4 位址逐漸耗盡，網路演進至 IPv6 已是國際共識，經過多年的發展，IPv6 在技術能力上已經逐漸成熟，各國主要電信業者均已陸續啟用 IPv6 商用運轉，隨著 IPv6 的發展，IPv6 安全風險開始浮現，亦挑戰 IPv6 網路防護能力，如何確保 IPv6 用戶資通安全，是部署 IPv6 不可或缺的重要關鍵。針對家庭 IPv6 網路安全防護，寬頻分享器 CPE 是面向 IPv6 終端用戶的第一線設備，對於家用 IPv6 網路的安全防護扮演關鍵的角色，本研究除探討家用網路 IPv6 網路攻擊與防禦機制外，亦將參考 RFC 6092 提出家用 CPE 設備的 IPv6 資安建議，並針對市售寬頻分享器 IPv6 防護功能進行基本的 IPv6 ACL 功能設計測試架構與流程。

貳、 目的及應用範圍

本報告主要針對家庭網路進行 IPv6 用戶資通安全防護相關議題研析，探討 IPv6 網路攻擊與防禦機制，並針對用戶 IPv6 網路 IPv6 網路安全管理提出建議。

參、 用戶設備 CPE IPv6 安全議題與解決方案

一、 IPv6 基本功能與協定探討

IPv6 是下一代的 Internet Protocol（IP），主要制定來解決 IPv4 位址空間的耗盡，並提供了其它的功能。RFC 4291[1]定義數種 IPv6 位址格式，大約可分為下列幾種：下表說明三種 IPv6 位址類型：單點傳送（unicast）、任意點傳送（anycast），和多點傳送（multicast）。

表 1 IPv6 位址格式分類

單點傳送	單播位址（Unicast Address）標示一個網路介面。協定會把送往位址的封包投送給其介面。 IPv6 的單播位址可以有一個代表特殊位址名字的範疇，例如: link-local 位址和唯一區域位址（ULA，unique local address）。
任意點傳送	任播位址（Anycast Address）用於指定給一群介面，通常這些介面屬於不同的節點。若封包被送到一個任播位址時，則會被轉送到成員中的其中之一。通常會根據路由協定，選擇 "最近" 的成員。任播位址通常無法輕易分別：它們擁有和正常單播位址一樣的結構，只是會在路由協定中將多個節點加入網路中。
多	多播位址（Multicast Address）也被指定到一群不同的介面，送

點 傳 送	到多播位址的封包會被傳送到所有的位址。多播位址由皆為一的位元組起始，亦即：它們的前置為 FF00::/8。其第二個位元組的最後四個位元用以標明 "範疇"。

本計畫所討論的 IPv6 位址配發機制主要以單點傳送位址為主。IPv6 的 Unicast 如同 IPv4 的 Unicast 傳送模式，用在單一節點對單一節點的資料傳送，可再分成下列型態：

(一) Global：如同 IPv4 的公開位址（Public Address），在全世界具有唯一性，其它節點不會有相同的位址。

(二) Link-Local：僅在一個特定的網路區段使用（同一個子網路中），不可被繞送到其他連結或網際網路上。功用如同 IPv4 的 APIPA 位址（169.254.X.X）。

(三) Unique-Local：位址可以在節點間繞送，但不可被繞送到網際網路。Link-Local 及 Unique-Local 位址的概念就像是 IPv4 中的私有位址，區域網路間自動建立暫時性的通訊非常有用。

一般來說，IPv6 單點傳送位址中的介面識別碼可用來識別連結上的介面，而該連結上的介面識別碼必須是獨特的，其連結則通常由子網路字首識別。單點傳送位址中的位元若全為零，則此

位址又稱為未指定位址（unspecified address），其文字表示法為「::」。單點傳送位址「::1」或「0:0:0:0:0:0:0:1」稱為回送位址（loopback address），節點會利用此位址將封包送回給自己。

網路上的終端設備要能彼此互通，除了用戶端設備 IPv6 網路位址的配發之外，首先還必須先確認用戶端設備與鄰居的關係才行。在 IPv6 的網路環境中，主要是利用 Neighbor Discovery（ND）[2]的方法來達成這個目標，描述相鄰網路節點之間關係的程序與方法，其主要的目標如下：

- 主機用它來發現相鄰路由器。
- 主機用它來發現位址、網路前置碼（Network Prefix）以及其它組態參數。
- 主機用它來解析 IPv6 封包轉寄到相鄰節點的連結層位址，並確定相鄰節點的連結層位址從何時起發生改變。
- 主機用它來確定是否仍然可以連線到相鄰節點。
- 路由器用它來通告自己的存在、主機組態參數以及網路前置碼。

在 IPv6 網路環境上，ND 主要是利用 ICMPv6 封包來傳遞並交換訊息，並使用包含 Router Solicitation （RS）、Router Advertisement （RA）、Neighbor Solicitation （NS）、Neighbor

Advertisement （NA）、Redirect 五種不同的訊息格式，其中前兩種是用來讓用戶端設備尋找路由器以及讓路由器主動廣播訊息所用，而第三與第四種是用來讓網路設備彼此交換相鄰節點訊息用，最後一種則是用來將封包轉送用的訊息。在 IPv6 的網路環境中，用戶端設備 IPv6 位址的取得必須建立在 ND 通訊協定的基礎上。

二、 家庭網路 IPv6 攻擊途徑與防護方式

本章主要探討家庭網路相關的 IPv6 攻擊與防護議題。

(一)Neighbor Discovery 攻擊與防護

芳鄰探索機制 Neighbor Discovery 為 IPv6 基本必要之功能無法關閉，ND 機制能夠正確且安全地運作，在同一連結上的各節點必須互相信任，若芳鄰探索機制在未受保護的環境中，非常容易受到惡意的攻擊。圖 1 為 IPv6 ND 攻擊示意圖。

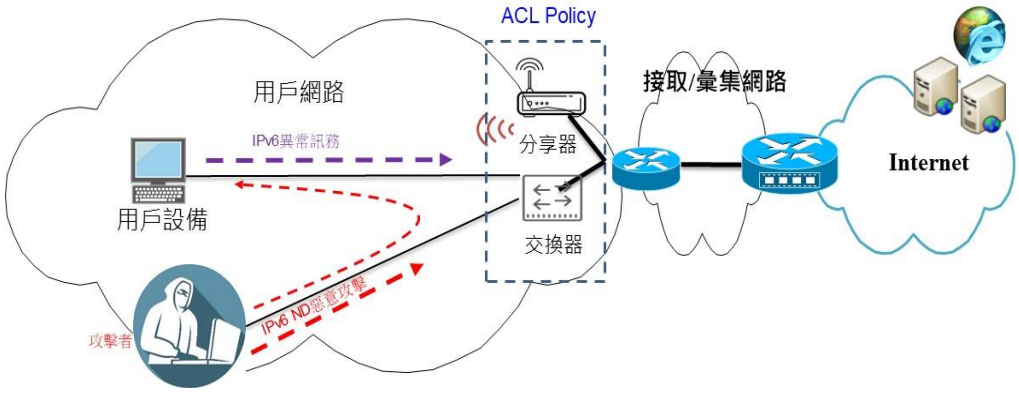

圖 1 IPv6 ND 攻擊示意圖

IPv6 的 ND 攻擊方式類似 IPv4 的 ARP 攻擊，基本上可分為三種如表 2。

表 2 IPv6 ND 資安攻擊分類

攻擊類型	說明
重導（Redirect）攻擊	攻擊者惡意將資料轉送至其他位置。
服務阻斷（Denial-of-Service）攻擊	使目標主機的網路或系統資源耗盡，使服務暫時中斷或停止，導致其正常用戶無法存取。
偽冒（Spoofing）攻擊	以假造的 IPv6 位址 於網路中進行非法攻擊行為，造成破壞。

Redirect 攻擊必須要先知道 LAN 原本路由器 IPv6 位址，將 IPv6 路由植入終端針對 Target IPv6 位址之訊務重新導向新路由器 IPv6 位址。如果新路由器 IPv6 位址不存在，將可能導致用戶 IPv6 上網的服務中斷。在 IPv6 位址配置部分，無論

SLAAC、DHCPv6、靜態 IPv6 位址設定前都必須發送 DAD NS 封包確認 LAN 環境中無 IPv6 節點使用同一個 IPv6 位址。重複位址偵測（Duplicate Address Detection）作用類似 IPv4 Gratuitous ARP，新的 IP 位址在設定前會先確認網路上是否已經有設備在使用。在 IPv6 網路中，當攻擊者監聽區域網路上所有的 NS 封包，可容易地產生具有偽造目標位址的 NS 封包來假裝重複位址偵測，或是佯裝成相同目標位址主機回應 NA 封包，讓受害節點以為發生碰撞，造成受害者無法正常取得 IP 位址的使用權，此種攻擊即稱為重複位址偵測 DoS。在偽冒攻擊部分，由於 ND 消息是不安全的，這使 ND 容易受到涉及鏈結層位址欺騙（或偽造）的攻擊。攻擊節點可以通過發送帶有欺騙性的來源 MAC 位址的鄰居請求訊息，或者通過發送帶有欺騙性目標 MAC 位址的鄰居通告位址，來將合法節點的數據包發送到其他某個鏈結層位址，然後其他節點將欺騙的 MAC 位址與合法的網路 IPv6 位址關聯在一起存起來。

在防禦機制方面，防範 ND 攻擊的最主要目標就是防止發生假冒 IP 的情形，可考慮針對 ND 通訊要求進行認證，確認是可信賴的端點後，再進行訊息交換。RFC 3971 及 RFC 6494 的 Secure Neighbor Discovery（SeND）協定對此提出三個選項

（option）：加密產生位址（Cryptographically GeneratedAddresses，簡稱 CGA）、RSA 簽 章 （RSAsignature）、時間戳記與 Nonce（Timestamp and Nonce）。SeND 機制主要實作於網路的終端節點，各節點須產生一組公鑰與私鑰，再利用 CGA 機制產生 IPv6 位址，以保證其位址擁有權；而以私鑰針對 ND 訊息所產生之 RSA 簽章係放在所有選項末端，確保訊息的機密性及完整性；至於時間戳記及 Nonce 選項則用以防止重送攻擊。

目前 SeND 機制僅主要網路設備廠商如 Cisco 支援此協定，一般用戶端 OS 尚未支援，且加解密運算可能影響設備處理效能，建置時須審慎考量其適用範圍。

(二)Router Advertisement 攻擊與防護

在 IPv6 中，路由器會週期性地群播 RA 訊息，用來通告路由器的可用性和傳遞資訊給鄰居節點，使鄰居節點在網路上可以被自動地設定。RA 訊息被 ND 用來檢測鄰居，通告 IPv6 Prefixes，協助位址的提供，以及分配鏈結參數，例如: maximum transmission unit （MTU）、hop limit、advertisement interval、lifetime 等。

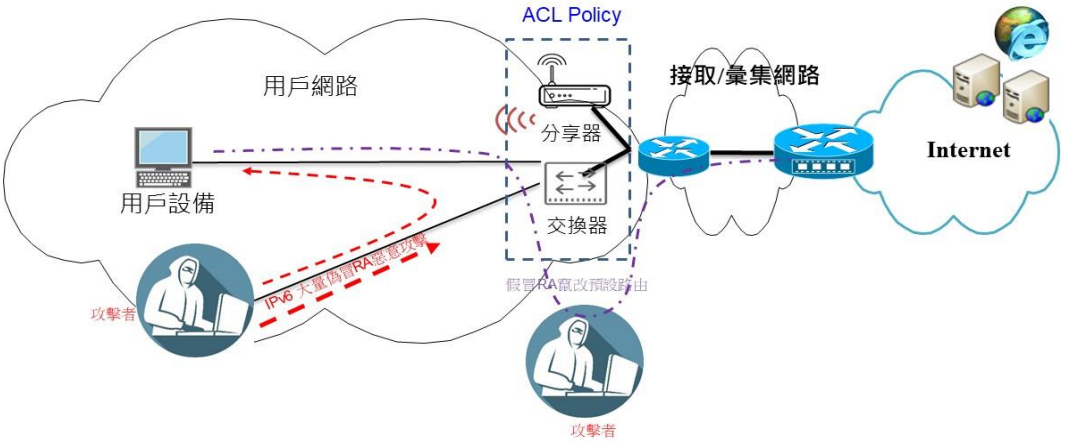

圖 2 IPv6 RA 攻擊示意圖

圖 3 為 IPv6 RA 攻擊示意圖，每個 IPv6 節點都可以發送 RA，可讓終端新增公眾 IPv6 位址、新增/刪除預設路由或廣播大量 RA 降低網路效能。假冒（Rogue）RA 攻擊以及 RA 洪水（Flooding）是兩種典型的 RA 攻擊類型，如表 1。

表 3 IPv6 RA 資安攻擊分類

攻擊類型	說明
假冒（Rogue RA）攻擊	每個 IPv6 節點都可以發送 RA，可讓終端新增公眾 IPv6 位址、新增/刪除預設路由或廣播大量 RA 降低網路效能
RA 洪水（Flooding）攻擊	發送大量 RA 夾帶 IPv6 Prefix 以消耗目標主機系統資源，影響用戶存取效率。

假冒（Rogue）攻擊，攻擊者會透過偽造 RA 封包傳送假的路由組態資訊進行攻擊，例如惡意的路由器（malicious router）、假造位址前綴（bogus prefix）、假造路由組態參數（parameters spoofing）以及假造重導訊息（spoofed redirect message）等。攻擊者可佯裝為對外的路由器（稱之為惡意的路由器），對本地連結的主機傳送群播的 RA 訊息或回應的 RA 訊息，使本地連結的主機誤認為其為對外連線的路由器，以便接收所有主機對外的連線資料，使攻擊者可以進一步發動 Man-in-the-Middle attack。除了偽冒 RA 攻擊外，IPv6 RA Flooding 則是一種嚴重的 DoS 攻擊，攻擊者發出大量偽冒的 RA，受攻擊主機資源因為處理大量 RA 被耗盡，RA flooding 可能導致整個區域網路服務阻斷，讓所有連到那個區域網路的主機系統停止運作無法回應。

IPv6 RA 攻擊防護機制可參考 RFC 6104 Rogue IPv6 Router Advertisement Problem Statement，不同服務與維運情境需要不同防護方式，有幾種不同的防護方式各有優缺點，除可透過 Port ACL 阻斷所有來自於終端（Host）發送之 ICMPv6 外，亦可以並用開源碼 NDPmon 程式以設定檔比對的方式處理。RFC 6105 也提出 RA Guard 的機制，也就是把連接在交換器的網路

裝置角色區分為 Host 或是 Router 兩種，只有連接合法 IPv6 路由器的介面套用 Router 的 Device-role，允許來自該介面 RA 訊息可以轉送到相同 VLAN 的其他所有介面；其餘介面則套用 Host 的 Device-role，來自這些介面的 RA 訊息一律阻擋下來，不可轉送到其他介面，如此一來，用戶主機只會接收到來自合法 IPv6 路由器發送的 RA 訊息，便可以有效解決 IPv6 RA 攻擊所帶來的影響。

(三)ICMPv6 攻擊與防護

Internet Control Messaging Protocol（ICMP）藉由驗證 End-to-End 的可達性，來幫助網路的故障排除，ICMP 也能回報目標主機上的錯誤，但是，由於 ICMP 的特性和缺乏內建安全機制，ICMP 很快地變成用來攻擊的手段，例如: IPv6 阻斷服務 DoS 就是最典型的 ICMPv6 攻擊。圖 7 為 ICMPv6 攻擊示意圖。

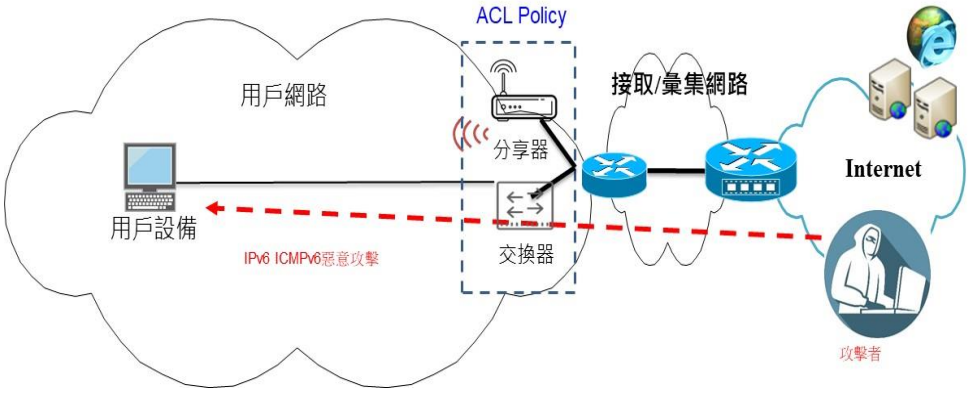

圖 3 IPv6 ICMPv6 攻擊示意圖

ICMPv6 阻斷攻擊涉及使用大量流量盡可能快地淹沒目標節點或網路，受影響節點會嘗試處理收到的請求（Request），因此會使目標無法回應其它服務，ICMPv6 包含資訊的訊息，例如: Echo Request 和 Echo Reply、RA、NS、NA，以及 Multicast Listener Discovery（MLD）皆可用於實現阻斷攻擊使目標主機或網路資源耗盡。此外，由於攻擊者可以改變來源 IPv6 位址，也使攻擊者不容易被辨識出來，使得攻擊防禦的機制更顯重要。

針對 ICMP 防禦機制方面，ICMPv6 和 ICMPv4 兩者完全不同，不同於 ICMPv4，ICMPv6 是構成 IPv6 通訊以及 IPv6 的操作有賴於 ICMPv6 的特性，基於這些原因不能單純僅僅阻檔所有 ICMPv6 message type。對 IPv4 來說，在設有防火牆的 IPv4 網路中，通常會阻斷大多數 ICMP 訊息的傳送，最主要原因是駭客可利用 ICMP 協定獲取網路異常原因等相關訊息，調整網路探測及攻擊方式，尤其介

接網際網路的防火牆必須封鎖 ICMP 的 Echo Request 及 EchoReply 訊息連線封包。但是在 IPv6 的環境中，ND 協定須依據 ICMPv6 回應訊息，判斷路由器或主機是否存在，因此防火牆須允許特定 ICMPv6 封包通過。為防止 ICMPv6 訊息洩漏可能造成的影響，RFC 4980 針對防火牆可能需要開放的規則提出建議，即於實際設定時，應秉持最小化原則，針對防火牆規則的來源與目的端設定限制，盡可能設定明確的 IP 範圍，不應貪圖方便而設定為 Any。

肆、 用戶設備 CPE IPv6 資安防護建議

隨著 IPv6 技術的日漸成熟，家庭用戶 CPE 設備廠商也已陸續支援 IPv6，然而面對駭客的威脅，基本的防禦對策是相當重要的。為此本計劃以 RFC 6092 為基礎，重點摘要家用寬頻分享器 IPv6 防護建議如下，細部的規範建議請參閱附件一，可做為設備廠商產品 IPv6 資安規格設計之參考。

(一)IPv6 基本防護功能 （不得轉送）

- 來源 IPv6 位址為群播位址之封包
- 目的 IPv6 位址為大於或等於路由器群播位址之封包
- 含有已廢除擴充標頭之封包、違反 ingress filtering 之封包
- Inbound DNS 查詢預設不能被 WAN 介面執行、Inbound DHCPv6 預設不能被 WAN 介面執行或轉送、Inbound ICMPv6 錯誤訊息 Destination Unreachable 與 Packet Too Big 不屬於由內往外通訊 Flow 狀態記錄之封包

(二)Connection-Free Filters ICMPv6 功能

- 防火牆 ICMPv6 錯訊訊息套用 RFC 4890 規範
- 預設讓由外往內 Echo Request、Time Exceeded（Type 3）、Parameter Problem（Type 4）允許通過

- Inbound 且不屬於通訊 Flow 狀態記錄之 Destination Unreachable 與 Packet Too Big 錯誤訊息皆丟棄

(三)VPN 與 IPsec Filters 功能

- 預設允許 outbound VPN，禁止 inbound VPN
- 預設允許 IPSec
- 預設允許目的埠號 500（IKE – Internet Key Exchange 專屬埠號） UDP 訊務
- 預設允許 Host Identity Protocol （HIP）
- 預設允許與目前 ESP（Encapsulating Security Payload） Flow 狀態記錄相關之 Inbound ICMPv6 錯誤訊息如 Destination Unreachable 與 Packet Too Big

(四)Mobile IPv6 Filters 功能

- 預設允許 Mobile IPv6
- Inbound Unsolicited Mobility Header 不符合 IPSec security policy 需丟棄
- 預設允許與目前 Mobility Header 相關狀態記錄之 Flow

伍、 用戶設備 CPE IPv6 ACL 規則建議

ACL（Access Control List）為存取控制列表，亦是最方便、最直接且最有效的基礎 IPv6 資安防禦方法，市售家用分享器 CPE 皆有預設支援，因此建議一般家用分享器皆可設定使用。家用用戶 CPE 分享器之 IPv6 ACL 存取控制功能，可依據設備所提供的網頁設定介面，設定需要禁止或允許通過的來源 IPv6 位址範圍、目的 IPv6 位址範圍、協定&埠的範圍等等，建議預設需阻斷的 IPv6 位址列舉如下：

- The loopback address (e.g., ::1/128)
- The unspecified address, similar to the IPv4 address 0.0.0.0 (e.g., ::/128)
- The IPv4-mapped address (e.g., ::ffff:0:0/96)
- Link-local unicast address (e.g., fe80::/10, fe90::/10, fea0::/10, feb0::/10)
- Site-local address (e.g., fc00::/7)
- The documentation address (e.g., 2001:db8::/32)
- Overlay routable cryptographic has identifiers address (e.g., 2001:10::/28)
- IPv6 Benchmarking address (e.g., 2001:2::/48)
- Discard-only prefix for remote triggered blockhole routing

address (e.g., 0100::/64)

- IANA Special Purpose address Block (e.g., 2001:0000::/29 – 2001:01f8::/29)
- Address ranges reserved by the IETF (0000::/8, 0100::/8, 0200::/7, 0400::/6, 0800::/5, 1000::/4,a000::/3, e000::/4, f800::/6, fe00::/9, fec0::/100, 3ffe::/16, etc)

陸、 用戶設備 CPE IPv6 ACL 設定流程與測試方法

針對 CPE IPv6 資安防護機制，ACL 是 IPv6 基本的防禦機制之一，家庭網路 IPv6 ACL 的安全佈署可應用於分享器/交換器或是一般家庭用戶分享器等位置，針對非經許可的 IPv6 用戶連線進行管控。

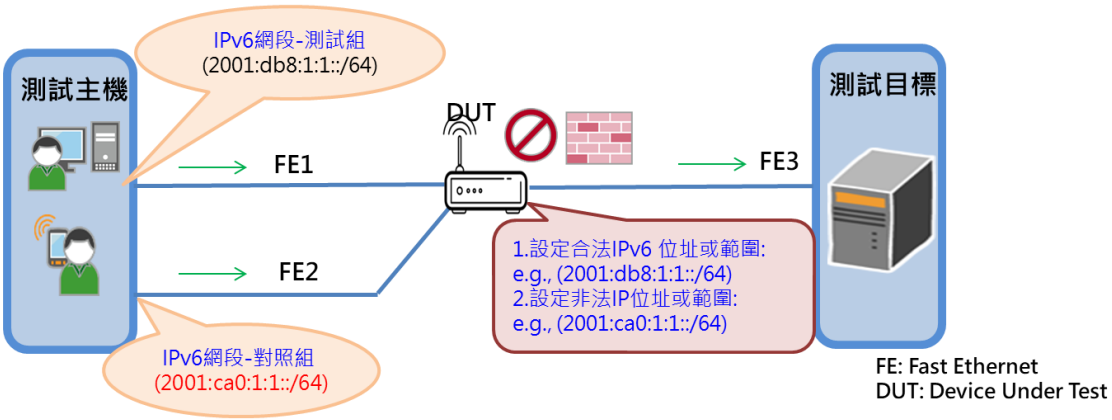

圖 4 CPE IPv6 ACL 測試架構範例

本節以 DLink 寬頻分享器為例，設計 IPv6 ACL 測試架構與流程。測試架構如圖 4 所示，測試主機可用個人終端裝置如電腦或手機等針對目標的 IPv6 網站或服務進行連線測試，中間的 DUT（Device Under Test）裝置為待測物 CPE，圖 5 為 Dlink 寬頻分享器的設定介面，測試範例流程如表 4。ACL 機制針對 IPv6 的阻斷攻擊如 ICMP、RA flooding、IPv6 Extension Header 等攻擊情境。

CPE IPv6 ACL 基本操作流程如下:

(1) 依 CPE 的產品說明書指示，以預設帳號密碼登入 CPE 的 Web 設定頁面，透過此 Web UI 方式進行相關設定

(2) 進入 IPv6 設定頁面

(3) 選擇禁止或允許下列清單進行存取

(4) 依據設定頁面，設定需要禁止或允許通過的來源 IP 位址範圍、目的 IP 位址範圍、協定&埠的範圍等等

(5) 確認新增規則，完成 IPv6 ACL 功能設定

圖 5 D-Link CPE IPv6 ACL 設定範例

表 4 IPv6 ACL 網路安全防禦機制測試範例

步驟	測試內容 (範例)
1	動作：控制介面勾選開啟 ACL 功能 檢驗：確認有無使用者介面或由指令方式控制
2	動作：加入 ACL 規則，allow Ingress ICMPv6 Packet Too Big 檢驗：確認指令正確下達
3	動作：加入 ACL 規則，deny Ingress Extension Header 檢驗：確認指令正確下達

圖 6 確認用戶 IPv6 上網正常

圖 7 啟用 ACL 功能後，被設定阻擋的主機無法取得 IPv6 位址

柒、 結論

本報告主要探討家庭 IPv6 網路安全攻擊與防護措施，研擬家庭網路設備 IPv6 網路安全功能需求建議。整理攻擊類型整理包含：

- Neighbor Discovery 攻擊與防護
- Router Advertisement 攻擊與防護
- ICMPv6 攻擊與防護

並針對家用寬頻分享器 CPE IPv6 基礎防護功能進行測試。經測試結果證實，家用寬頻分享器之 ACL 功能可確實阻擋非經許可的 IPv6 用戶連線，達到基本家用網路防護功能。藉由本計劃之研究成果期能提供我國 CPE 設備廠商與家庭用戶 IPv6 基礎安全防護之參考。

參考文獻

[1] RFC 4291 - IP Version 6 Addressing Architecture，Available:
https://tools.ietf.org/html/rfc4291

[2] RFC 4861 - Neighbor Discovery，Available:
https://tools.ietf.org/html/rfc4861

附錄一、用戶 CPE 分享器 IPv6 資安相關 RFC 規範

國立中央大學 National Central University

Mobile broadband networklab

RFC 6092
Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service

周立德

國立中央大學主任秘書

國立中央大學資訊工程學系特聘教授

Stateless Filters

Connection-Free Filters - Stateless Filters		
ID	Requirements	需求
REC-1	REC-1: Packets bearing multicast source addresses in their outer IPv6 headers MUST NOT be forwarded or transmitted on any interface.	在其外部IPv6標頭中承載multicast source addresses的封包不得在任何介面上轉送或傳輸
REC-2	REC-2: Packets bearing multicast destination addresses in their outer IPv6 headers of equal or narrower scope (see "IPv6 Scoped Address Architecture" [RFC4007]) than the configured scope boundary level of the gateway MUST NOT be forwarded in any direction. The DEFAULT scope boundary level SHOULD be organization-local scope, and it SHOULD be configurable by the network administrator.	➢ 在其外部IPv6標頭中具有相同或更窄範圍的多播目標位址的封包[RFC4007]，不可Gateway對任何方向轉送 ➢ 預設的範圍邊界級別應是organization-local scope，且其應由網路管理員配置
REC-3	REC-3: Packets bearing source and/or destination addresses forbidden to appear in the outer headers of packets transmitted over the public Internet MUST NOT be forwarded. In particular, site-local addresses are deprecated by [RFC3879], and [RFC5156] explicitly forbids the use of address blocks of types IPv4-Mapped Addresses, IPv4-Compatible Addresses, Documentation Prefix, and Overlay Routable Cryptographic Hash IDentifiers (ORCHID).	Packets bearing source和/或destination addresses的封包禁止出現在公眾網路上傳輸封包的外部標頭中 ➢ [RFC3879]不推薦使用site-local ➢ [RFC5156]明確禁止使用IPv4-Mapped位址，IPv4-Compatible位址，Documentation Prefix和Overlay Routable Cryptographic Hash Identifiers（ORCHID）

Stateless Filters

Connection-Free Filters - Stateless Filters		
ID	Requirements	需求
REC-4	REC-4: Packets bearing deprecated extension headers prior to their first upper-layer-protocol header SHOULD NOT be forwarded or transmitted on any interface. In particular, all packets with routing extension header type 0 [RFC2460] preceding the first upper- layer-protocol header MUST NOT be forwarded. See [RFC5095] for additional background.	在第一個上層協議頭之前帶有已棄用的擴展標頭的封包不應該在任何介面上轉送或傳輸。 routing extension header type 0不可轉送
REC-5	REC-5: Outbound packets MUST NOT be forwarded if the source address in their outer IPv6 header does not have a unicast prefix configured for use by globally reachable nodes on the interior network.	如外部IPv6標頭中的來源位址沒有配置為由內部網路上的globally reachable nodes使用的unicast prefix ，則不可轉送outbound封包。
REC-6	REC-6: Inbound packets MUST NOT be forwarded if the source address in their outer IPv6 header has a global unicast prefix assigned for use by globally reachable nodes on the interior network.	如外部IPv6標頭中的來源位址具有分配給內部網路上的global unicast prefix，則不可轉送inbound封包。
RFC-7	REC-7: By DEFAULT, packets with unique local source and/or destination addresses [RFC4193] SHOULD NOT be forwarded to or from the exterior network.	在預設的情況下，具有unique local source 和/或 destination addresses [RFC4193]的封包不應轉送到外部網路或從外部網路轉送
RFC-8	REC-8: By DEFAULT, inbound DNS queries received on exterior interfaces MUST NOT be processed by any integrated DNS resolving server.	在預設的情況下，外部介面上收到的inbound DNS查詢不可由任何integrated DNS 解析服務器處理。
REC-	REC-9: Inbound DHCPv6 discovery packets	在外部介面上接收的inbound DHCPv6發現封包

Connection-Free Filters

Connection-Free Filters - Internet Control and Management		
ID	Requirements	需求
REC-10	REC-10: IPv6 gateways SHOULD NOT forward ICMPv6 "Destination Unreachable" and "Packet Too Big" messages containing IP headers that do not match generic upper-layer transport state records.	IPv6 Gateway不應轉送上層傳輸狀態記錄不匹配的包含於IP標頭的ICMPv6 Destination Unreachable和Packet Too Big訊息

Connection-Free Filters

Connection-Free Filters - Upper-Layer Transport Protocols		
ID	Requirements	需求
REC-11	REC-11: If application transparency is most important, then a stateful packet filter SHOULD have "endpoint-independent filtering" behavior for generic upper-layer transport protocols. If a more stringent filtering behavior is most important, then a filter SHOULD have "address-dependent filtering" behavior. The filtering behavior MAY be an option configurable by the network administrator, and it MAY be independent of the filtering behavior for other protocols. Filtering behavior SHOULD be endpoint independent by DEFAULT in gateways intended for provisioning without service-provider management.	➢ 如果應用程序透通是最重要的，則stateful封包過濾應該對上層傳輸協議具有“endpoint-independent filtering”行為 ➢ 如果更嚴格的過濾行為是必要的，那麼過濾應該具有“address-dependent filtering”行為 ➢ 過濾行為可以是網路管理員可配置的選項，它可以獨立於其他協議的過濾行為 ➢ 在沒有服務提供商管理的情況下，過濾行為應該在Gateway設為預設be endpoint independent
REC-12	REC-12: Filter state records for generic upper-layer transport protocols MUST NOT be deleted or recycled until an idle timer not less than two minutes has expired without having forwarded a packet matching the state in some configurable amount of time. By DEFAULT, the idle timer for such state records is five minutes.	上層傳輸協議的過濾狀態記錄不得刪除或回收，直到空閒計時器不少於兩分鐘即到期且沒有在一段可配置的時間內轉送匹配狀態的封包（在預設的情況下，此類狀態記錄的空閒計時器為五分鐘）
REC-13	REC-13: Residential IPv6 gateways SHOULD provide a convenient means to update their firmware securely, for the installation of security patches and other manufacturer-recommended changes.	Residential IPv6 gateways應該提供一種方便的方法來安全地更新其韌體，安裝security patches和其他製造商建議的更新

5

Connection-Free Filters

Connection-Free Filters - UDP Filters		
ID	Requirements	需求
REC-14	REC-14: A state record for a UDP flow where both source and destination ports are outside the well-known port range (ports 0-1023) MUST NOT expire in less than two minutes of idle time. The value of the UDP state record idle timer MAY be configurable. The DEFAULT is five minutes.	UDP flows的狀態記錄，其中來源端口和目標端口都在已知的端口範圍之外（端口0-1023），到期時間不可少於兩分鐘的空閒時間。 UDP狀態記錄record idle timer的值是可配置的（ 預設是五分鐘）
REC-15	REC-15: A state record for a UDP flow where one or both of the source and destination ports are in the well-known port range (ports 0-1023) MAY expire after a period of idle time shorter than two minutes to facilitate the operation of the IANA-registered service assigned to the port in question.	UDP flows的狀態記錄，其中一個或兩個來源端口和目標端口都在已知的端口範圍內（端口0-1023）可能會在短於兩分鐘的空閒時間後到期
REC-16	REC-16: A state record for a UDP flow MUST be refreshed when a packet is forwarded from the interior to the exterior, and it MAY be refreshed when a packet is forwarded in the reverse direction.	當封包從內部轉送到外部時，必須刷新UDP flows的狀態記錄，並且當封包以反向方向轉送時，可以更新狀態記錄

Connection-Free Filters

Connection-Free Filters - UDP Filters

ID	Requirements	需求
REC-17	REC-17: If application transparency is most important, then a stateful packet filter SHOULD have "endpoint-independent filtering" behavior for UDP. If a more stringent filtering behavior is most important, then a filter SHOULD have "address-dependent filtering" behavior. The filtering behavior MAY be an option configurable by the network administrator, and it MAY be independent of the filtering behavior for TCP and other protocols. Filtering behavior SHOULD be endpoint independent by DEFAULT in gateways intended for provisioning without service-provider management.	➢ 如果應用程序透通是最重要的，那麼stateful封包過濾應該具有UDP的“endpoint-independent filtering”行為。 ➢ 如果更嚴格的過濾行為是最必要的重要的，那麼過濾應該具有“address-dependent filtering”行為。 ➢ 過濾行為可以是網路管理員可配置的選項，可以獨立於TCP和其他協議的過濾行為。
REC-18	REC-18: If a gateway forwards a UDP flow, it MUST also forward ICMPv6 "Destination Unreachable" and "Packet Too Big" messages containing UDP headers that match the flow state record.	如Gateway需轉送UDP flows，則其還必須轉送包含與flows狀態記錄匹配的UDP標頭的ICMPv6 Destination Unreachable和Packet Too Big訊息
REC-19	REC-19: Receipt of any sort of ICMPv6 message MUST NOT terminate the state record for a UDP flow.	收到任何類型的ICMPv6訊息不可中斷UDP flows的狀態記錄
REC-20	REC-20: UDP-Lite flows [RFC3828] SHOULD be handled in the same way as UDP flows, except that the upper-layer transport protocol identifier for UDP-Lite is not the same as UDP; therefore, UDP packets MUST NOT match UDP-Lite state records, and vice	UDP-Lite flows[RFC3828]應以與UDP flows相同的方式處理。

Connection-Free Filters

Connection-Free Filters - IPsec and Internet Key Exchange (IKE)

ID	Requirements	需求
REC-21	REC-21: In their DEFAULT operating mode, IPv6 gateways MUST NOT prohibit the forwarding of packets, to and from legitimate node addresses, with destination extension headers of type "Authentication Header (AH)" [RFC4302] in their outer IP extension header chain.	在預設操作模式下，IPv6 Gateway不可禁止在合法節點位址之間轉送封包，在其外部IP擴展標頭鏈中使用目標擴展標頭類型為Authentication Header（AH）”[RFC4302]
REC-22	REC-22: In their DEFAULT operating mode, IPv6 gateways MUST NOT prohibit the forwarding of packets, to and from legitimate node addresses, with an upper-layer protocol of type "Encapsulating Security Payload (ESP)" [RFC4303] in their outer IP extension header chain.	在預設操作模式下，IPv6 Gateway不可禁止在其外部IP擴展標頭鏈中使用Encapsulating Security Payload (ESP) [RFC4303]類型的上層協議來轉送與合法節點位址之間的封包
REC-23	REC-23: If a gateway forwards an ESP flow, it MUST also forward (in the reverse direction) ICMPv6 "Destination Unreachable" and "Packet Too Big" messages containing ESP headers that match the flow state record.	如Gateway需轉送ESP flows，則其必須（反向）轉送包含與flows狀態記錄匹配的ESP標頭的ICMPv6 Destination Unreachable 以及Packet Too Big 訊息
REC-24	REC-24: In their DEFAULT operating mode, IPv6 gateways MUST NOT prohibit the forwarding of any UDP packets, to and from legitimate node addresses, with a destination port of 500, i.e., the port reserved by IANA for the Internet Key Exchange (IKE) protocol [RFC5996].	在預設操作模式下，IPv6Gateway不可禁止由合法節點向目標端口500轉送的任何UDP封包

Connection-Free Filters

Connection-Free Filters- Address assignment requirements		
ID	Requirements	需求
REC-25	REC-25: In all operating modes, IPv6 gateways SHOULD use filter state records for Encapsulating Security Payload (ESP) [RFC4303] that are indexable by a 3-tuple comprising the interior node address, the exterior node address, and the ESP protocol identifier. In particular, the IPv4/NAT method of indexing state records also by the security parameters index (SPI) SHOULD NOT be used. Likewise, any mechanism that depends on detection of Internet Key Exchange (IKE) [RFC5996] initiations SHOULD NOT be used.	在所有操作模式中，IPv6 Gateway應對 Encapsulating Security Payload (ESP) [RFC4303] 使用過濾狀態記錄，這些記錄可由包含內部節點位址，外部節點位址和ESP協議標識符 特別是，也不應使用security parameters index (SPI) 索引狀態記錄的IPv4 / NAT方法。 同樣，任何依賴 Internet Key Exchange (IKE) ）[RFC5996]啟動檢測的機制都不應該被使用
REC-26	REC-26: In their DEFAULT operating mode, IPv6 gateways MUST NOT prohibit the forwarding of packets, to and from legitimate node addresses, with destination extension headers of type "Host Identity Protocol (HIP)" [RFC5201] in their outer IP extension header chain.	在預設的操作模式中，IPv6 Gateway不可禁止在合法節點之間轉送封包，並在其外部IP擴展標頭鏈中使用“Host Identity Protocol (HIP) [RFC5201]

Connection-Free Filters

Connection-Free Filters- Mobility Support in IPv6		
ID	Requirements	需求
REC-27	REC-27: The state records for flows initiated by outbound packets that bear a Home Address destination option [RFC3775] are distinguished by the addition of the home address of the flow as well as the interior care-of address. IPv6 gateways MUST NOT prohibit the forwarding of any inbound packets bearing type 2 routing headers, which otherwise match a flow state record, and where A) the address in the destination field of the IPv6 header matches the interior care-of address of the flow, and B) the Home Address field in the Type 2 Routing Header matches the home address of the flow.	➢ 帶有Home Address destination option [RFC3775]的outbound封包發起的flows的狀態記錄可由添加flow home address以及interior care-of address來區別 ➢ IPv6Gateway不可禁止轉發帶有type 2 routing headers的任何inbound封包

Connection-Free Filters

Connection-Free Filters- Mobility Support in IPv6		
ID	Requirements	需求
REC-28	REC-28: Valid sequences of Mobility Header [RFC3775] packets MUST be forwarded for all outbound and explicitly permitted inbound Mobility Header flows.	必須為所有outbound和明確允許的inbound Mobility Header flows轉送Mobility Header [RFC3775]封包的有效序列
REC-29	REC-29: If a gateway forwards a Mobility Header [RFC3775] flow, then it MUST also forward, in both directions, the IPv4 and IPv6 packets that are encapsulated in IPv6 associated with the tunnel between the home agent and the correspondent node.	如Gateway需轉送Mobility Header [RFC3775]flows，則其還必須在兩個方向上轉送封裝的IPv4和IPv6封包於於home agent以及correspondent node之間的tunnel
REC-30	REC-30: If a gateway forwards a Mobility Header [RFC3775] flow, then it MUST also forward (in the reverse direction) ICMPv6 "Destination Unreachable" and "Packet Too Big" messages containing any headers that match the associated flow state records.	如Gateway需轉送Mobility Header [RFC3775]flows，則其必須轉送（反向）ICMPv6“Destination Unreachable”和“Packet Too Big”訊息，其中包含與相關flows狀態記錄匹配的任何標頭

Connection-Oriented Filters

Connection-Oriented Filters - TCP Filters		
ID	Requirements	需求
REC-31	REC-31: All valid sequences of TCP packets (defined in [RFC0793]) MUST be forwarded for outbound flows and explicitly permitted inbound flows. In particular, both the normal TCP 3-way handshake mode of operation and the simultaneous-open mode of operation MUST be supported.	必須轉送所有有效的TCP封包序列（在[RFC0793]中定義）以用於outbound flows和明確允許的inbound flows。特別是，normal TCP 3-way handshake操作模式以及the simultaneous-open mode
REC-32	REC-32: The TCP window invariant MUST NOT be enforced on flows for which the filter did not detect whether the window-scale option (see [RFC1323]) was sent in the 3-way handshake or simultaneous-open.	TCP window invariant不可強加於flows，當過濾器未偵測到3-way handshake或simultaneous-open送出的window-scale option（參見[RFC1323]）
REC-33	REC-33: If application transparency is most important, then a stateful packet filter SHOULD have "endpoint-independent filtering" behavior for TCP. If a more stringent filtering behavior is most important, then a filter SHOULD have "address-dependent filtering“behavior. The filtering behavior MAY be an option configurable by the network administrator, and it MAY be independent of the filtering behavior for UDP and other protocols. Filtering behavior SHOULD be endpoint independent by DEFAULT in gateways intended for provisioning without service-provider management.	➢ 如應用程序透通是最重要的，那麼stateful封包過濾機制應該具備TCP endpoint-independent filtering的行為。 ➢ 如更嚴格的過濾行為是必要的，那麼過濾機制應該具備“address-dependent filtering的行為。 ➢ 過濾機制可以是網路管理員可配置的選項，可獨立於UDP和其他協議的過濾行為，在沒有服務提供者管理的情況下，過濾機制應是預設在Gateway中
12		

Connection-Oriented Filters

Connection-Oriented Filters - TCP Filters		
ID	Requirements	需求
REC-34	REC-34: By DEFAULT, a gateway MUST respond with an ICMPv6 "Destination Unreachable" error code 1 (Communication with destination administratively prohibited) to any unsolicited inbound SYN packet after waiting at least 6 seconds without first forwarding the associated outbound SYN or SYN/ACK from the interior peer.	在預設的情況下，Gateway必須回應ICMPv6 Destination Unreachable 錯誤代碼1給任何 unsolicited inbound SYN packet （等待至少6秒）
REC-35	REC-35: If a gateway cannot determine whether the endpoints of a TCP flow are active, then it MAY abandon the state record if it has been idle for some time. In such cases, the value of the "established flow idle-timeout" MUST NOT be less than two hours four minutes, as discussed in [RFC5382]. The value of the "transitory flow idle- timeout" MUST NOT be less than four minutes. The value of the idle- timeouts MAY be configurable by the network administrator.	如果Gateway無法確定TCP flow的端點是否處於活動狀態，則其可放棄該狀態記錄。 在這種情況下： ➢ established flow idle-timeout的值不得少於兩小時四分鐘 ➢ transitory flow idle- timeout的值不得少於四分鐘 ➢ idle-timeouts的值可以由網路管理員配置
REC-36	REC-36: If a gateway forwards a TCP flow, it MUST also forward ICMPv6 "Destination Unreachable" and "Packet Too Big" messages containing TCP headers that match the flow state record.	如Gateway轉送TCP flow，則其必須轉送包含與flow狀態記錄匹配的TCP標頭的ICMPv6 “Destination Unreachable”和“Packet Too Big”訊息
REC-37	REC-37: Receipt of any sort of ICMPv6 message MUST NOT terminate the state record for a TCP flow.	收到任何類型的ICMPv6訊息均不可中斷TCP flow的狀態記錄

Connection-Oriented Filters

Connection-Oriented Filters - SCTP Filters		
ID	Requirements	需求
REC-38	REC-38: All valid sequences of SCTP packets (defined in [RFC4960]) MUST be forwarded for outbound associations and explicitly permitted inbound associations. In particular, both the normal SCTP association establishment and the simultaneous-open mode of operation MUST be supported.	➢ 所有有效的SCTP封包序列（在[RFC4960]中定義）必須轉送outbound associations以及permitted inbound associations ➢ 必須支援正常的SCTP關聯建立和simultaneous-open mode。
REC-39	REC-39: By DEFAULT, a gateway MUST respond with an ICMPv6 "Destination Unreachable" error code 1 (Communication with destination administratively prohibited), to any unsolicited inbound INIT packet after waiting at least 6 seconds without first forwarding the associated outbound INIT from the interior peer.	在預設的情況下，Gateway必須回覆ICMPv6 Destination Unreachable錯誤代碼1 （等待至少6秒）
REC-40	REC-40: If a gateway cannot determine whether the endpoints of an SCTP association are active, then it MAY abandon the state record if it has been idle for some time. In such cases, the value of the "established association idle-timeout" MUST NOT be less than two hours four minutes. The value of the "transitory association idle-timeout" MUST NOT be less than four minutes. The value of the idle-timeouts MAY be configurable by the network administrator.	如Gateway無法確定SCTP關聯的端點是否處於活動狀態，若狀態記錄已空閒一段時間，則可以放棄該狀態記錄。 在這種情況下： ➢ established association idle-timeout的值不得少於兩小時四分鐘 ➢ transitory association idle-timeout的值不得少於四分鐘 ➢ idle-timeouts的值可以由網路管理員配置

Connection-Oriented Filters

Connection-Oriented Filters - SCTP Filters		
ID	Requirements	需求
REC-41	REC-41: If a gateway forwards an SCTP association, it MUST also forward ICMPv6 "Destination Unreachable" and "Packet Too Big" messages containing SCTP headers that match the association state record.	如果Gateway需轉送SCTP association，則其還必須轉送包含與關聯狀態記錄匹配的SCTP標頭的ICMPv6“Destination Unreachable”和“Packet Too Big”訊息
REC-42	REC-42: Receipt of any sort of ICMPv6 message MUST NOT terminate the state record for an SCTP association.	收到任何類型的ICMPv6訊息絕不能終止SCTP關聯的狀態記錄

Connection-Oriented Filters

Connection-Oriented Filters - DCCP Filters		
ID	Requirements	需求
REC-43	REC-43: All valid sequences of DCCP packets (defined in [RFC4340]) MUST be forwarded for all flows to exterior servers, and for any flows to interior servers that have explicitly permitted service codes.	所有有效的DCCP封包序列（在[RFC4340]中定義）必須轉送給外部服務器的所有flows，以及任何明確允許服務代碼的內部服務器flows
REC-44	REC-44: A gateway MAY abandon a DCCP state record if it has been idle for some time. In such cases, the value of the "open flow idle- timeout" MUST NOT be less than two hours four minutes. The value of the "transitory flow idle-timeout" MUST NOT be less than eight minutes. The value of the idle-timeouts MAY be configurable by the network administrator.	如果Gateway閒置一段時間，Gateway可以放棄DCCP狀態記錄，在這種情況下 ➢ open flow idle- timeout的值不得少於兩小時四分鐘。 ➢ transitory flow idle-timeout的值不得少於8分鐘 ➢ idle-timeouts的值可由網路管理員配置
REC-45	REC-45: If an Internet gateway forwards a DCCP flow, it MUST also forward ICMPv6 "Destination Unreachable" and "Packet Too Big" messages containing DCCP headers that match the flow state record.	如Internet gateways 可轉送DCCP flow，則其必須轉送包含與flow state記錄匹配的DCCP標頭的ICMPv6 “Destination Unreachable”和“Packet Too Big”訊息
REC-46	REC-46: Receipt of any sort of ICMPv6 message MUST NOT terminate the state record for a DCCP flow.	收到任何類型的ICMPv6訊息不可中斷DCCP Flow的狀態記錄

Connection-Oriented Filters

Connection-Free Filters - Level 3 Multihoming Shim Protocol for IPv6 (Shim6)		
ID	Requirements	需求
REC-47	REC-47: Valid sequences of packets bearing Shim6 payload extension headers in their outer IP extension header chains MUST be forwarded for all outbound and explicitly permitted flows. The content of the Shim6 payload extension header MAY be ignored for the purpose of state tracking.	在其外部IP擴展標頭鏈中帶有Shim6有效負載擴展標頭的封包的有效序列必須轉送給所有outbound和permitted flows

Passive Listeners

Passive Listeners		
ID	Requirements	需求
REC-48	REC-48: Internet gateways with IPv6 simple security capabilities SHOULD implement a protocol to permit applications to solicit inbound traffic without advance knowledge of the addresses of exterior nodes with which they expect to communicate.	具有IPv6簡化安全功能的Internet gateways 應允許應用程序在未預先了解其與預期外部通訊節點位址的情況下請求inbound traffic
REC-49	REC-49: Internet gateways with IPv6 simple security capabilities MUST provide an easily selected configuration option that permits a "transparent mode" of operation that forwards all unsolicited flows regardless of forwarding direction, i.e., not to use the IPv6 simple security capabilities of the gateway. The transparent mode of operation MAY be the default configuration.	➢ 具有IPv6簡化安全功能的Internet gateways 必須提供一個易於選擇的配置選項，可允許“transparent mode”操作 ➢ transparent mode模式可以預設配置

Management Applications

Management Applications		
ID	Requirements	需求
REC-50	REC-50: By DEFAULT, subscriber-managed residential gateways MUST NOT offer management application services to the exterior network.	在預設的情況下，用戶管理的residential gateways不得向外部網路提供管理應用服務。