『前瞻及完整之 IPv6 生態系推動方案』

附錄八
『蒐集並整理 ISP 之 IPv6 網路安全防護準則』

109 年委託研究報告

109 年度「物聯網服務與應用研析及網際網路技術標準研析」計畫

蒐集並整理 ISP 之
IPv6 網路安全防護準則

期末報告

計畫委託機關：台灣網路資訊中心

中華民國 109 年 10 月

109 年委託研究報告

蒐集並整理 ISP 之 IPv6 網路安全防護準則

期末報告

受委託單位

東海大學資訊管理學系

計畫主持人

林正偉

指導老師

蘇暉凱

研究人員

賴囿嘉、陳晏羚

研究期程：中華民國 109 年 4 月至 109 年 12 月

研究經費：新臺幣 70 萬元

中華民國 109 年 10 月

目錄

圖目錄

表目錄

第一章 簡介

全球 IPv6 的使用率逐年攀升，提供 IPv6 網路服務的 ISP 也逐漸增加，且根據 APNIC IPv6 統計資料，台灣 IPv6 普及率已超過 50%，全世界排名第七，近年網路攻擊及如何提供安全連網議題受到相當的重視，IPv6 連網比例提升也逐漸吸引駭客進行攻擊的可能性，尤其國內 ISP 主要以支援 IPv4/IPv6 雙協定網路服務，更增加網路的複雜性。本工作項目將蒐集與彙整 ISP IPv6 網路安全防護之相關文獻，並且提出 ISP IPv6 網路安全基本防護要項與 ISP IPv6 網路連線服務安全防護建議，可供國內 ISP IPv6 建置與營運參考，也藉此提升 ISP 對 IPv6 網路安全議題能更為重視。

第二章 蒐集並整理 ISP 之 IPv6 網路安全防護準則

第一節 研析 ISP IPv6 網路安全基本防護要項

一. 簡介

本報告蒐集與彙整 ISP IPv6 網路安全防護之相關文獻，並且提出 ISP IPv6 網路安全基本防護要項，供國內 ISP IPv6 建置與營運參考。

一般網際網路服務提供者(ISP; Internet Service Provider)服務架構如圖 1 所示，包含網際網路存取服務(Internet Access Service)、網際網路互連(Internet Interworking)連結網際網路與網際網路應用服務(Internet Service)三大類，且網際網路應用服務是 ISP 提供用戶使用網際網路相關之應用服務，例如：DNS、Web…等。

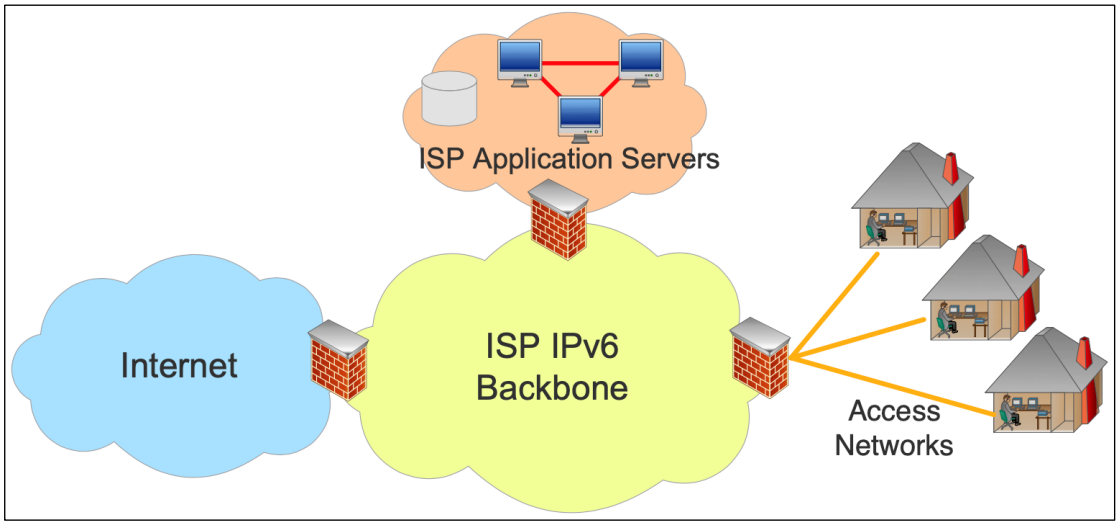

圖 1 ISP 服務架構示意圖

IETF 與 ISP IPv6 網路安全防護之相關文獻，依網際網路互連、網際網路應用服務、網際網路存取服務三個類別，本報告蒐集之文獻如表 1。

表 1 ISP IPv6 網路安全防護相關文獻

類別	IETF 相關文獻
網際網路互連 [1][2]	1. E. Vyncke, Ed., K. Chittimaneni, M. Kaeo, E. Rey, "Operational Security Considerations for IPv6 Networks," IETF Internet-Draft, draft-ietf-opsec-v6-21, November 3, 2019. 2. E. Davies, S. Krishnan, P. Savola, "IPv6 Transition/Coexistence Security Considerations," RFC 4942, September 2007.
網際網路存取服務 [3][4][5]	1. S. Asadullah, A. Ahmed, C. Popoviciu, P. Savola, J. Palet, "ISP IPv6 Deployment Scenarios in Broadband Access Networks", RFC 4779, January 2007. 2. G. Van de Velde, T. Hain, R. Droms, B. Carpenter, E. Klein, "Local Network Protection for IPv6," RFC 4864, May 2007. 3. J. Woodyatt, Ed., "Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service", RFC 6092, January 2011.
網際網路應用服務 [6]	1. B. Carpenter, S. Jiang, "IPv6 Guidance for Internet Content Providers and Application Service Providers," RFC 6883, March 2013.

二. 網際網路互連

(一) IPv6 定址安全考量

1. 位址架構

IPv6 位址分配和整體結構是安全性 IPv6 的重要部分。在最初的設計，縱使以臨時 IPv6 位址增加使用者的私密性，但其持續時間卻比預期的要長得多。儘管最初讓 IPv6 位址可以簡單地重新編號，但實際上如果沒有適當的 IP 位址管理系統(IPAM)，則重新編號可能會非常困難。

成功部署 IPv6 的關鍵任務是要準備好一個定址規劃；由於有足夠的可用的位址空間，具有服務和地理位置特性之 IPv6 位址規劃，將使位址空間成為更結構化安全策略的基礎，以允許或拒絕地理區域之間的服務。

一個常見的問題是公司是否應該使用提供商獨立(Provider Independent, PI)空間與提供商分配(Provider Allocated, PA)空間[RFC7381]，但是從安全角度來看，兩者之間幾乎沒有區別。然而，要關注的是誰擁有 IPv6 位址空間的管理所有權，以及如果當需要進行 IPv6 位址空間路由強制限制，誰具有技術上的責任，例如：源自特定位址空間的惡意犯罪活動，誰該進行強制限制。

在[RFC7934]中，建議 IPv6 網路部署從每個 Prefix 提供多個 IPv6 位址給一般主機，並且特別不建議限制主機對每個 Prefix 僅提供一個 IPv6 位址。它也建議網路使主機具有使用新 IPv6 位址的能力，而不需要明確的請求(例如：使用 SLAAC)。與每個介面設定唯一 IPv4 位址相比，每個介面具有多個 IPv6 位址是一個重大的變化。

表 2 RFC7381、RFC7934 參考文獻

編號	RFC 編號	RFC 相關訊息	
		類別	時間
1.	7381	Informational	2014/10
		標題：Enterprise IPv6 Deployment Guidelines	
2.	7934	Informational	2016/07
		標題：Host Address Availability Recommendations	

(1) 使用單一區域位址(ULA)

單一區域位址(Unique Local Addresses, ULAs)[RFC4193]，如：fc00::/8 與 fd00::/8；IPv6 單一區域位址特性相似於 IPv4 私有位址。單一區域位址適用於網路介面不需要連結得到網際網路的使用情境，如：使用於內部網路連線。單一區域位址具有網際網路全域連線範圍，但是[RFC4193]指定必須在域邊界將其過濾掉。單一區域位址與[RFC1918] IPv4 私有位址不同，並且具有不同的使用案例，[RFC4864]中描述了 ULA 的一種用法。

表 3 RFC4193、RFC1918、RFC 4864 參考文獻

編號	RFC 編號	RFC 相關訊息	
		類別	時間
1.	4193	Proposed Standard	2014/10
		標題：Unique Local IPv6 Unicast Addresses	
2.	1918	Best Current Practice	2016/07
		標題：Address Allocation for Private Internets	
3.	4864	Informational	2005/10
		標題：Local Network Protection for IPv6	

(2) 點對點鏈接(Point-to-Point Links)

[RFC6164]指定將/127 用於路由器間點對點鏈接；/127 可以防止

未正確實施[RFC4443]的路由器之間進行乒乓攻擊，還可以防止對鄰居快取記憶體的 DoS 攻擊。

某些環境還可以將鏈結本地位址使用於點對點鏈接。儘管這種做法可以進一步減少對基礎設施的攻擊，但操作上的缺點也需要仔細考慮；另請參閱[RFC7404]。

表 4 RFC6164、RFC4443、RFC7404 參考文獻

編號	RFC 編號	RFC 相關訊息	
		類別	時間
1.	6164	Proposed Standard	2011/04
		標題：Using 127-Bit IPv6 Prefixes on Inter-Router Links	
2.	4443	Internet Standard	2006/5
		標題：Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	
3.	7404	Informational	2014/11
		標題：Using Only Link-Local Addressing inside an IPv6 Network	

(3) 回送位址(Loopback Address)

許多運營商為其基礎架構中的所有 Loopback Address 保留一塊/64 區域，並為每個回送介面(Loopback Interface)從這保留的/64 Prefix 中分配一個/128。這種做法允許簡單地設定存取控制列表(ACL)，以實施那些相關回送位址的安全策略。

(4) 靜態配置位址(Statically Configured Addresses)

在考慮如何分配靜態配置位址時，考慮給定環境中外圍安全的有效性是有必要的。在操作簡便性(可以簡單地識別 IPv6 位址以進行操作調試和故障排除)與使用於偵察的不重要網路掃描風險之間是需要進行權衡選擇的。[SCANNING]介紹一些基於科學的掃描方法，這些方法讓掃描可連線到的 IPv6 節點比預期的更可行；另可參考[RFC7707]。使用已知的 IPv6 位址(例如所有鏈接本地節點的 ff02::1)或使用常見的重複位址，可以很容易地確定哪些設備是名稱服務伺服器、路由器或其他關鍵設備。即使是簡單的 traceroute，也會暴露路徑上的大多數路由器。掃描技術有很多種可能，操作人員不應該認為「亂

數隨機分配位址是不可能被掃描到的」，即使一般做法會將靜態配置的位址隨機分佈在/64 子網中，並且使用 DNS 進行名稱與位址對應，也是一樣具有安全性風險。

儘管在某些環境中，容易令人混淆的位址可能被認為可以增加額外的好處，但這並無法排除被有效執行的外圍規則，以及靜態配置的位址可能使用某些邏輯方法進行位址計算以簡化操作(因為簡單性總是有助於提高安全性)。因此，典型的部署可以將靜態和非靜態位址混合使用。

表 5 RFC7707 參考文獻

編號	RFC 編號	RFC 相關訊息	
		類別	時間
1.	7707	Informational	2016/05
		標題：Network Reconnaissance in IPv6 Networks	

(5) 臨時位址(Temporary Addresses) - SLAAC 的隱私延伸

無狀態位址自動配置(SLAAC)是基於 EUI-64 MAC 位址自動生成的 64 位元介面標識碼(IID)，該標識碼與/64 Prefix 一起構成了網際網路全域唯一的 IPv6 位址；其中 EUI-64 位址是從 48 位元的 MAC 位址生成的。[RFC8064]建議不要使用 EUI-64 位址，並且必須注意，因此大多數主機作業系統不再使用 EUI-64 位址，而是採用[RFC4941]或[RFC8064]。

如[RFC4941]中描述，隨機生成介面 ID 是 SLAAC 的一部分，具有所謂的隱私延伸位址(Privacy Extension Addresses)，用於解決一些使用者上網隱私問題。隱私延伸位址又稱為臨時位址，可以幫助減少

同一網路內節點活動的相關性，並且也可以減少暴露成為被攻擊之風險。

使用[RFC4941]隱私延伸位址可能可以避免操作員建構主機特定的存取控制列表(ACL)；[RFC4941]隱私延伸位址也可以使用於掩蓋某些惡意活動，並且應實施特定的用戶歸屬/責任程序。

[RFC8064]指定了另一種生成位址的方式，同時仍為每個網路 Prefix 保留相同的 ID；這使 SLAAC 節點在特定網路上始終具有相同的穩定 IPv6 位址，而在不同網路上具有不同的 IPv6 位址。

在某些特定的使用案例中，用戶的責任比用戶的隱私更為重要，網路運營商可能會考慮禁用 SLAAC 並僅採用 DHCPv6。但是，並非所有作業系統都支援 DHCPv6，因此一些主機將無法使用 IPv6 連線。對於大多數作業系統，可以通過以下方式來禁用 SLAAC 和隱私延伸位址：設置 M 位元來發送 RA 訊息，以提示透過 DHCPv6 獲取 IPv6 位址，但也可以透過在所有 Prefix 選項中重設所有 A 位元來禁止使用 SLAAC。然而，如果沒有在交換機/路由器強制實施，攻擊者仍然可能可以找到繞過此機制的方法。

但對於強烈要求匿名的情況下(保護用戶隱私比用戶責任更重要)，應使用隱私延伸位址。當[RFC8064]可用時，穩定的隱私位址可能是隱私(在不同網路之間)和安全/用戶責任(在網路內)之間的良好平衡。

表 6 RFC8064、RFC4941 參考文獻

編號	RFC 編號	RFC 相關訊息	
		類別	時間
2.	8064	Proposed Standard	2014/10
		標題：Recommendation on Stable IPv6 Interface	

編號	RFC 編號	RFC 相關訊息	
		類別	時間
		Identifiers	
3.	4941	Draft Standard	2016/07
		標題：Privacy Extensions for Stateless Address Autoconfiguration in IPv6	

(6) DHCP/DNS 注意事項

許多環境使用 DHCPv6 來提供位址和其他參數，以確保審核能力和可追溯性(如：Stateful DHCPv6)。一個主要的安全考量是檢測和抵制惡意 DHCP 服務器的能力。與 DHCPv4 相比，必須注意 DHCPv6 可以為每個客戶端租用多個 IPv6 位址，並且該租用不綁定到客戶端的鏈結層位址(MAC Address)，而是綁定到客戶端的 DHCP Unique ID (DUID)。

儘管 DNS 的 IPv4 和 IPv6 安全考量沒有不同，但是在 DNS64 [RFC6147]環境中需要特別考慮。具體來說，需要了解與 DNSSEC 實施的相互作用和潛在干擾。

表 7 RFC6147 參考文獻

編號	RFC 編號	RFC 相關訊息	
		類別	時間
3.	6147	Proposed Standard	2011/04
		標題：DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers	

(7) 每個主機使用/64

一種有趣的方法是按[RFC8273]的建議，在每個主機上使用/64。

由於主機的應用程序可以在/64 內更改其 IPv6 位址，因此它的/64 Prefix 是穩定的，因此可以簡化用戶歸屬(通常基於主機 MAC 位址)。

表 8 RFC8273 參考文獻

編號	RFC 編號	RFC 相關訊息	
		類別	時間
1.	8273	Informational	2017/12
		標題：Unique IPv6 Prefix per Host	

(8) 位址的隱私考慮

除了 IPv6 位址的安全性方面，還有一些隱私方面的考慮：主要是因為 IPv6 位址具有網際網路全域範圍並且在網際網路全域範圍內可見。[RFC7721]透過手動配置的 DHCPv6 或 SLAAC，詳細介紹了 IPv6 位址的隱私注意事項。

表 9 7721 參考文獻

編號	RFC 編號	RFC 相關訊息	
		類別	時間
1.	7721	Informational	2016/05
		標題：Security and Privacy Considerations for IPv6 Address Generation Mechanisms	

2. 延伸標頭

延伸標頭是 IPv4 和 IPv6 之間的重要區別。在 IPv4 的封包中，查找上層協議類型和協議標頭很簡單，然而在 IPv6 中，由於必須完全解析延伸標頭，因此更為複雜。IANA 已關閉現有「Next Header Types」，並根據[RFC7045]改採用新的「IPv6 Extension Header Types」。

由於已知丟棄包含延伸標頭封包的轉發節點會導致連接失敗和部署問題，因此這也已成為引起爭議的主題[RFC7872]。了解可變延伸標頭的作用很重要，本節列舉了需要仔細考慮的延伸標頭。

在[RFC7045]中可以找到有關中間節點應如何處理具有現有或未來延伸標頭封包的說明，[RFC6564]中描述了使用於定義未來延伸標頭的統一TLV 格式。

此外還必須注意，在封包中沒有指示「Next Protocol」欄位指向延伸標頭或指向傳輸層標頭，這可能會混淆某些過濾規則。

表 10 RFC7045、RFC7872、RFC6564 參考文獻

編號	RFC 編號	RFC 相關訊息	
		類別	時間
1	7045	Proposed Standard	2013/12
		標題：Transmission and Processing of IPv6 Extension Headers	
2	7872	Informational	2016/06
		標題：Observations on the Dropping of Packets with IPv6 Extension Headers in the Real World	
3	6564	Proposed Standard	2012/04
		標題：A Uniform Format for IPv6 Extension Headers	

(1) 延伸標頭的順序和重複

儘管[RFC8200]推薦了延伸標頭的順序和最大重複次數，但在IPv6 實作上，依然可能支援非推薦順序(例如路由之前的 ESP)或非法重複(例如多個路由標題)，延伸標頭中包含的選項也是如此(請參閱[I-D.kampanakis-6man-ipv6-eh-parsing])。在某些情況下，它導致節點在接收或轉發格式錯誤的封包時，造成崩潰。*因此，應該使用防火牆或邊緣設備來強制執行延伸標頭的建議順序和出現次數。*

表 11 RFC8200 參考文獻

編號	RFC 編號	RFC 相關訊息	
		類別	時間
1	8200	Internet Standard	2017/07
		標題：Internet Protocol, Version 6 (IPv6) Specification	

(2) 逐跳選項標頭(Hop-by-Hop Options Header)

當 IPv6 封包中存在逐跳選項標頭時，逐跳選項標頭會強制路徑中的所有節點檢查原始 IPv6 規範[RFC2460]中的此標頭。因為並不是所有路由器都可以透過硬體處理此類封包，當硬體無法處理此類封包，該封包以進行軟體處理，因此大量逐跳選項標頭可能造成服務阻斷(Denial of Service)攻擊。目前 IPv6 標準[RFC8200]的考慮了此攻擊方式，並讓中間路由器可選擇是否對逐跳選項標頭進行處理。

表 12 RFC2460、RFC8200 參考文獻

編號	RFC 編號	RFC 相關訊息	
		類別	時間
1	2460	Draft Standard	1998/12
		標題：Internet Protocol, Version 6 (IPv6) Specification	
2	8200	Internet Standard	2017/07
		標題：Internet Protocol, Version 6 (IPv6) Specification	

(3) 分段標頭(Fragment Header)

當必須分段封包時，分段標頭必須在來源端(傳送端)被使用。[RFC7112]和[RFC8200]解釋了為什麼重要：

- 防火牆和安全設備應丟棄不包含整個 IPv6 標頭鏈(含傳輸層標頭)的第一個片段。
- 目的節點應丟棄不包含整個 IPv6 標頭鏈(含傳輸層標頭)的第一片段。

如果設備無法滿足這些要求，則攻擊方可能會繞過無狀態過濾。[RFC6980]透過強制丟棄分段的 NDP 封包，將更嚴格的規則應用於 NDP。[RFC7113]描述[RFC6105]提及之 RA-guard 功能，在分段 RA 封包存在時的處理行為。

表 13 RFC7112、RFC8200…等參考文獻

編號	RFC 編號	RFC 相關訊息	
		類別	時間
1	7112	Proposed Standard	2014/01
		標題：Implications of Oversized IPv6 Header Chains	
2	8200	Internet Standard	2017/07
		標題：Internet Protocol, Version 6 (IPv6) Specification	
3	6980	Proposed Standard	2013/08
		標題：Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery	
4	7113	Informational	2014/02
		標題：Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)	
5	6105	Informational	2011/02
		標題：IPv6 Router Advertisement Guard	

(4) IP 安全延伸標頭

如果要使用 IPsec 網路級安全功能，則 IPsec [RFC4301] [RFC4301] 延伸標頭(AH [RFC4302]和 ESP [RFC4303])是需要的。

表 14 RFC4301、RFC4302、RFC4303 參考文獻

編號	RFC 編號	RFC 相關訊息	
		類別	時間
1	4301	Proposed Standard	2005/12
		標題：Security Architecture for the Internet Protocol	
2	4302	Proposed Standard	2005/12
		標題：IP Authentication Header	
3	4303	Proposed Standard	2005/12
		標題：IP Encapsulating Security Payload (ESP)	

(二) 鏈結層安全考量

IPv6 非常依賴於鄰居發現協議(NDP)[RFC4861]來執行各種鏈接操作，例如發現鏈接上的其他節點(discovering other nodes)，解析其鏈接層位址以及在鏈接上找到路由器。如果不安全，NDP 是脆弱的，且容易受到各種攻擊，例如路由器/鄰

居訊息欺騙、重定向攻擊、重複位址檢測(Duplicate Address Detection, DAD)、DoS 攻擊…等。許多對 NDP 的安全威脅，已在[RFC3756]和[RFC6583]文件說明 IPv6 ND 信任模型與威脅。

表 15 RFC4861，RFC3756、RFC6583 參考文獻

編號	RFC 編號	RFC 相關訊息	
		類別	時間
1	4861	Draft Standard	2007/09
		標題：Neighbor Discovery for IP version 6 (IPv6)	
2	3756	Informational	2004/05
		標題：IPv6 Neighbor Discovery (ND) Trust Models and Threats	
3	6583	Informational	2012/05
		標題：Operational Neighbor Discovery Problems	

(三) 路由安全考量

1. 控制層面安全

[RFC6192]定義了路由器控制平面。現代路由器結構設計將轉發(Forwarding)和路由器控制平面硬體及軟體嚴格分開，路由器控制平面支援路由和管理功能，控制平面通常被描述為路由器結構的硬體和軟體元件，使用於處理設備本身的封包，以及發送設備本地產生的封包。

轉發平面通常被描述為路由器結構的硬體和軟體元件，這些組件負責在傳入介面上接收封包，執行查找以識別封包的 IP 下一轉送節點，並確定往目的地的最佳傳出介面轉發封包。

表 16 RFC6192 參考文獻

編號	RFC 編號	RFC 相關訊息	
		類別	時間
1	6192	Informational	2011/05
		標題：Protecting the Router Control Plane	

雖然轉發平面通常是在高速硬體中實現的，但是控制平面是由通用處理

器(稱為路由器處理器 RP)實現的，因此無法高速處理封包。因此，可以透過向輸入佇列(Input Queue)填充比其處理數量更多的封包來攻擊此處理器。這樣，控制平面處理器將無法處理有效的控制封包，並且路由器可能會丟失 OSPF 或 BGP 鄰接關係，從而導致路由問題與嚴重的網路中斷。

以下方法可以降低此狀況發生：

- 在進入 RP 處理的佇列前，先丟棄不合法的控制封包。
- 限制進入封包的速度，降低 RP 的負載。

以下針對控制協定、管理協定與例外封包進行說明：

(1) 控制協定

- 丟棄從非 link-local address 收到的 OSPFv3(Next-Header 89)與 RIPng(UDP port 521)控制封包。
- 允許從所有 BGP 鄰居節點收到的 BGP 封包(TCP port 179)，其他則丟棄。
- 允許所有 ICMP 封包。

(2) 管理協定

- 丟棄發往路由器的封包，但屬於所使用協議的封包除外(例如允許 TCP 22，僅使用 SSH 時，丟棄其他所有封包)。
- 丟棄來源與安全策略不匹配的封包，例如如果 SSH 連線僅允許來自 NOC，則 ACL 應僅允許來自 NOC Prefix 的 TCP 22 封包。

(3) 例外封包

以下情況必須處理，因此當硬體無法處理，可以交給路由器 CPU 處理。

- 當資料平面轉送封包過大，產生封包過大(packet-too-big)之 ICMP 訊息。
- 當資料平面封包因其跳數限制已達到 0 而無法轉送時，產生

ICMP 跳數限制已過期(hop-limit-expired)訊息。

- 由於某種原因無法轉送資料平面封包時，產生 ICMP 目標不可達(destination-unreachable)訊息。
- 逐跳選項標頭(hop-by-hop options header)的處理，根據[RFC8200]的說明，該處理是可選擇的處理或不處理。
- 更特定於某些路由器實現：超大延伸標頭鏈，造成硬體無法處理，而必須轉到路由器 CPU 處理。

表 17 RFC8200 參考文獻

編號	RFC 編號	RFC 相關訊息	
		類別	時間
1	8200	Internet Standard	2017/07
		標題：Internet Protocol, Version 6 (IPv6) Specification	

2. 路由安全(Routing Security)

路由安全一般需要考量以下幾點：

(1) 鄰居節點之認證。

(2) 節點(Peer)間安全路由之更新。

(3) 路由過濾。

(四) 記錄與監視

為了進行網路鑑識研究，在發生安全事件或偵測到異常行為時，網路運營商應記錄多條資訊。

此日誌記錄應包括：

- 當服務可使用時(例如 Web 伺服器)，紀錄所有應用程序使用網路的日誌(包括 User Space 和 Kernel Space)。
- 來自 IP 連線流資訊匯出(IP Flow Information Export)[RFC7011]的資料，也稱為 IPfix。

- 來自各種 SNMP MIB [RFC4293]的資料。
- 鄰居暫存(Neighbor Cache)的歷史資料。
- 有狀態 DHCPv6 [RFC8415]租用暫存，尤其是當使用中繼代理[RFC6221]時。
- 來源位址驗證改善(Source Address Validation Improvement, SAVI)[RFC7039]事件，尤其是 IPv6 位址與 MAC 位址以及特定交換機或路由器介面的綁定。
- RADIUS [RFC2866] 統計記錄。

表 18 RFC7011、RFC4293…等參考文獻

編號	RFC 編號	RFC 相關訊息	
		類別	時間
1.	7011	Internet Standard	2013/09
		標題：Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information	
2.	4293	Proposed Standard	2006/04
		標題：Management Information Base for the Internet Protocol (IP)	
3.	8415	Proposed Standard	2018/11
		標題：Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	
4.	6221	Proposed Standard	2011/05
		標題：Lightweight DHCPv6 Relay Agent	
5.	7039	Informational	2013/10
		標題：Source Address Validation Improvement (SAVI) Framework	
6.	2866	Informational	2000/07
		標題：RADIUS Accounting	

請注意，有關如何收集、保存和安全丟棄這些日誌的隱私問題或法規，敦促運營商檢查其國家法律(例如歐盟的 GDPR)。

所有這些信息都可以被使用於：

- 網路鑑識：誰在哪時候，做了什麼事。
- 相關性：特定節點使用了哪個 IP 位址(假設使用隱私延伸位址[RFC4941])
- 清單：我的網路上有哪些 IPv6 節點？
- 異常行為檢測：異常流量模式通常是異常行為的症狀，而異常行為又可能構成潛在的攻擊(阻斷服務、網路掃描、節點成為殭屍網路的一部分…等)。

三. 網際網路存取服務

(一) IPv6 存取網路安全考量

1. 寬頻電纜網路

DOCSIS 電纜網路中的安全性是使用 Baseline Privacy Plus(BPI +)提供的，依賴 IP 位址的唯一部分是加密群播(Encrypted Multicast)。從語義上講，群播加密在 IPv6 環境中的工作方式與在 IPv4 網路中的工作方式相同；但是，DOCSIS 規範中需要適當的強化以支援加密的 IPv6 群播。

為了增強安全性，必須對主機進行有限的更改。主機應使用用於自動配置(auto-configuration)的隱私延伸[RFC3041]，如果主機或 GWR 上可用，則可以啟用 IPv6 防火牆功能。

ISP 提供了針對來自其自己用戶的攻擊的安全性，但是它也可以實施安全服務，以保護其用戶免受來自其網路外部的攻擊。此類服務不適用於此處討論的網路存取級別。

CMTS/ER 應該保護 ISP 網路和其他用戶免受其自己客戶之一的攻擊。因此，應在面對用戶的所有介面上使用單播反向路徑轉發(uRPF)[RFC3704]和存取控制列表(ACL)。應當根據 IPv6 的操作要求進行過濾[IPv6-Security]。

CMTS/ER 應該保護其處理資源免受大量有效客戶控制流量的侵擾，例如：路由器和鄰居請求以及 MLD 請求。

與 IPv4 服務一起使用的所有其他安全功能也應類似地應用於 IPv6。

2. 寬頻 DSL 網路

為了增強安全性，CPE 必須進行有限的更改。主機應使用自動配置的隱私延伸[RFC3041]。ISP 可以相對輕鬆地跟踪它分配給用戶的 Prefix。但是，如果法規要求 ISP 在/128 位址級別跟蹤其用戶，則可以與可提供主機可追溯性的網路管理工具並行實施隱私延伸。如果存在，則應在主機或 CPR 上啟用 IPv6 防火牆功能。

ISP 提供了針對來自其自己用戶的攻擊的安全性，但它也可以實施安全服務，以保護其用戶免受來自其網路外部的攻擊。此類服務不適用於此處

討論的網路存取級別。

作為用戶(BRAS 或邊緣路由器)的第 3 層下一跳的設備應保護網路和其他用戶免受提供者客戶之一的攻擊。因此，應在面對用戶的所有介面上使用 uRPF 和 ACL。應當根據 IPv6 的操作要求進行過濾[IPv6-Security]。

BRAS 和邊緣路由器應保護其處理資源，以防止有效的客戶控制流量氾濫，例如：路由器和鄰居請求以及 MLD 請求。速率限制應在所有面對用戶的介面上實施。應該將重點放在群播類型的流量上，因為 IPv6 控制平面最常使用它。

與 IPv4 服務一起使用的所有其他安全功能也應類似地應用於 IPv6。

3. 寬頻乙太網路

為了增強安全性，CPE 必須進行有限的更改。主機應使用用於自動配置的隱私延伸[RFC3041]，並主機可追溯性。如果存在，則應在主機或客戶前提路由器上啟用 IPv6 防火牆功能。

ISP 提供了針對來自其自己用戶的攻擊的安全性，但它也可以實施安全服務，以保護其用戶免受來自其網路外部的攻擊。此類服務不適用於此處討論的網路存取級別。

如果有用於乙太網類型的任何第二層過濾器，則 NAP 必須允許 IPv6 乙太網類型(0X86DD)。

作為用戶的第 3 層下一跳的設備(BRAS 邊緣路由器)應保護網路和其他用戶免受提供者客戶之一的攻擊。因此，應在面對用戶的所有介面上使用 uRPF 和 ACL，應當根據 IPv6 的操作要求進行過濾[IPv6-Security]。

BRAS 和邊緣路由器應保護其處理資源，以防止有效的客戶控制流量氾濫，例如：路由器和鄰居請求以及 MLD 請求。速率限制應在所有面對用戶的介面上實施。應該將重點放在群播類型的流量上，因為 IPv6 控制平面最常使用它。

與 IPv4 服務一起使用的所有其他安全功能也應類似地應用於 IPv6。

4. 無線區域網路

為了增強安全性，必須對 WLAN 主機或路由器進行有限的更改。主機應使用用於自動配置的隱私延伸[RFC3041]，並主機可追溯性。如果存在，則應在 WLAN 主機或路由器上啟用 IPv6 防火牆功能。

ISP 提供了針對來自其自己用戶的攻擊的安全性，但它也可以實施安全服務，以保護其用戶免受來自其網路外部的攻擊。此類服務不適用於此處討論的網路存取級別。

如果使用基於 Web 的身份驗證系統完成熱點上的主機身份驗證，則安全級別將取決於特定的實現。**用戶憑證絕不能通過 HTTP 以明文形式發送，Web 瀏覽器和身份驗證服務器之間應使用安全 HTTP(HTTPS)**。身份驗證服務器可以在後端使用 RADIUS 和 LDAP 服務。

身份驗證是在實施第 3 層安全策略之前確保 WLAN 網路安全的重要方面。例如，這將有助於避免對 ND 或無狀態自動配置過程的威脅。802.1x [IEEE8021X]提供了確保網路存取安全的方法。但是，多種類型的 EAP(PEAP，EAP-TLS，EAP-TTLS，EAP-FAST 和 LEAP)以及主機支援某些功能的能力可能使實施全面一致的策略變得困難。

802.11i [IEEE80211i]修訂版包含許多組件，其中最明顯的是兩個新的數據保密協議：臨時密鑰完整性協議(TKIP)和計數器模式/CBC-MAC 協議(CCMP)。802.11i 還使用 802.1X 的密鑰分發系統來控制對網路的存取。由於 802.11 處理單播和廣播流量的方式不同，因此每種流量類型都有不同的安全問題。借助幾種數據保密協議和密鑰分發，802.11i 包括一個協商過程，用於為每種流量類型選擇正確的保密協議和密鑰系統。引入的其他功能包括密鑰緩存和預身份驗證。

802.11i 修正案是無線安全性的一大進步。該修正案增加了更強大的加

密，身份驗證和密鑰管理策略，可以使無線數據和系統更安全。

如果有用於乙太網類型的任何第二層過濾器，則 NAP 必須允許 IPv6 乙太網類型(0X86DD)。

作為用戶(存取或邊緣路由器)的第 3 層下一跳的設備應保護網路和其他用戶免受提供者客戶之一的攻擊。因此，應在面對用戶的所有介面上使用 uRPF 和 ACL。應當根據 IPv6 的操作要求進行過濾[IPv6-Security]。

Access 和邊緣路由器應保護其處理資源，以防止有效的客戶控制流量(例如 RS、NS 和 MLD 請求)氾濫。速率限制應在所有面對用戶的介面上實施。應該將重點放在群播類型的流量上，因為 IPv6 控制平面最常使用它。

5. 寬頻電力線通信(PLC)

與乙太網相比，在安全性考慮方面沒有差異。

表 19 RFC3041、RFC3704 參考文獻

編號	RFC 編號	RFC 相關訊息	
		類別	時間
1	3041	Proposed Standard	2001/01
		標題：Privacy Extensions for Stateless Address Autoconfiguration in IPv6	
2	3704	Best Current Practice	2004/05
		標題：Ingress Filtering for Multihomed Networks	

(二) CPE 簡易安全功能建議

CPE 應該內建封包過濾器功能，建議過濾器應用於家用網路通過 Internet 閘道器的所有流量，而與轉發的方向無關。如果封包起源於位於內部網路中用於外部目標的節點，則稱為「出站，Outbound」；如果封包來自具有內部目標的外部來源，則稱為「入站，Inbound」。過濾器建議說明下節。

1. 非狀態式過濾器(Stateless Filters)

   (1) 在其外部 IPv6 標頭中帶有群播源地址的封包不得在任何接口上轉發或傳輸。

   (2) 在其外部 IPv6 標頭中具有等於或小於範圍的已配置範圍邊界級別(請參閱“ IPv6 範圍地址體系結構” [RFC4007])的外部群播目的地 IPv6 封包，絕不能在任何方向上轉發。 內定區域邊界級別應該是僅限內部區域，並且應該由網路管理員配置。

   (3) 禁止將帶有來源地址和/或目標地址的封包顯示在通過公共 Internet 傳輸的封包外部標頭中。 特別是，[RFC3879]棄用了 site-local 地址，[RFC5156]明確禁止使用 IPv4 對應(IPv4-Mapped)的地址，兼容 IPv4 的地址，Document Prefix 與 Overlay Routable Cryptographic Hash IDentifiers (ORCHID)。

表 20 RFC4007、RFC3879、RFC5156 參考文獻

編號	RFC 編號	RFC 相關訊息	
		類別	時間
1	4007	Proposed Standard	2005/05
		標題：IPv6 Scoped Address Architecture	
2	3879	Proposed Standard	2004/09
		標題：Deprecating Site Local Addresses	
3	5156	Informational	2008/04
		標題：Special-Use IPv6 Addresses	

2. 免連接過濾器(Connection-Free Filters)

(1) IPv6 閘道器不應該轉發包含與上層傳輸狀態記錄不匹配的 IP 標頭之 ICMPv6“目標不可達”和“數據包太大”訊息。

(2) 如果應用程序透明性最重要，則對於通用上層傳輸協議，狀態封包過濾器應具有“端點無關的過濾”行為。 如果更嚴格的過濾行為是最重要的，則過濾器應具有“地址相關過濾”行為。 過濾行為可以是網路管理員可配置的選項，並且可以獨立於其他協議的過濾行為。 過濾行為應由 DEFAULT 在端點中獨立於端點，該端點打算在沒有服務提供商管理的情況下進行供應。

3. 連線導向過濾器(Connection-Oriented Filters)

(1) 必須為出站流和明確允許的入站流，轉發所有有效的 TCP 封包序列(在[RFC0793]中定義)。 特別是，必須同時支援正常的 TCP 三向握手操作模式和同時打開操作模式。

(2) 當過濾器在 TCP 3 方交握或同時打開時，未偵測到窗口縮放選項(window-scale option)(請參閱[RFC1323])，TCP window 不改變不可以被強致執行。

表 21 RFC0793、RFC1323 參考文獻

編號	RFC 編號	RFC 相關訊息	
		類別	時間
1	0793	Internet Standard	1981/09
		標題：Transmission Control Protocol	
2	1323	Proposed Standard	1992/05
		標題：TCP Extensions for High Performance	

四. 網際網路應用服務

(一) IPv6 架構

1. 位址與子網路分配

網路內容供應商(ICP)必須先決定是否採用自己供應商無關(PI)IPv6 位址 Prefix，可從 ISP 擔任區域網路註冊機構或直接從相關的區域網際網路註冊機構(RIR)獲得此選項；另一種方法是從 ISP 獲取供應商聚合(PA)Prefix，兩種解決方案在 IPv6 中都可行。

然而廣域路由系統(BGP-4)的縮放屬性意味著應該限制 PI 位址的數量，只有大型供應商可以合法獲得 PIPrefix，並說服 ISPs 對其進行路由，數以百萬計的企業網路(包括較小的內容供應商)將使用 PAPrefix，在這種情況下，使用[RFC4192]中概述的過程，更改 ISP 將需要更改相應的 PAPrefix。

表 22 RFC4192 參考文獻

編號	RFC 編號	RFC 相關訊息	
		類別	時間
1	4192	Informational	2005/09
		標題：Procedures for Renumbering an IPv6 Network without a Flag Day	

2. 路由

在雙協定網路中，大多數 IPv4 和 IPv6 內部路由協定相當獨立且併行。

通用路由協定，例如 OSPFv3 [RFC5340]，IS-IS [RFC5308]，甚至下一代路由資訊協定(RIPng)[RFC2080] [RFC2081]，都支援 IPv6，值得注意的是，儘管 OSPF 和 RIP 在 IPv4 和 IPv6 之間存在顯著差異，但 IS-IS 的優勢在於可以在協定的單個實例中處理它們，且可能在長期內簡化操作，某些版本的 OSPFv3 也可能具有此優勢[RFC5838]，無論如何，對於訓練有素的人員，在不干擾 IPv4 服務的情況下部署 IPv6 路由應該沒有特別的困難。

在某些情況下，某些網路設備上可能需要韌體升級、需要評估雙協定路

由的效能影響，特別是，路由器供應商要求 IPv6 具有什麼傳輸效能？如果傳輸效能明顯不如 IPv4，這會是操作上的問題嗎？是否需要額外的記憶體或三態內容可定址記憶體(TCAM)空間來容納 IPv4 和 IPv6 資訊？

為了回答這些問題，ICP 將需要一個針對最初預計的 IPv6 流量及可能增長率的預測模型，如果所在位置具有多個 PAPrefix，則會顯示路由配置的複雜性，特別是要基於來源路由規則，以確保將傳出數據封包路由到適當的邊界路由器和 ISP 連接，通常不應通過 ISP Y 發送由 ISP X 分配的位址來源的數據封包，以避免通過 Y [RFC2827] [RFC3704]進行輸入過濾。

其他注意事項可以在[MULTIHOMING-WITHOUT-NAT]中找到，請注意，[RFC6296]中討論的 Prefix 轉換技術並未描述，提供公開內容伺服器的企業解決方案，每個 IPv6 子網路通支援終端機常都有一個 64Prefix，剩下的 64 位用於各個主機的介面 ID。

對照之下，典型的 IPv4 子網路的主機 ID 不得超過 8 位，於是將子網路限制為 256 個或更少的主機，雙協定設計通常對 IPv4 和 IPv6 使用相同的實體或 VLAN 子網路拓撲，因此也將使用相同的路由器拓撲，換句話說，IPv4 和 IPv6 拓撲是一致的，這意味著即使 IPv6Prefix 將允許更多的主機，IPv4 的有限子網路大小(例如 256 個主機)也將被強加給 IPv6，從理論上描述，可通過為 IPv6 實現不同的實體或 VLAN 子網路拓撲來避免此限制，這是不適當的，當出現問題時，它將導致極其複雜的故障診斷。

3. DNS

必須瞭解，一旦在 DNS 中發布了知名名稱的 AAAA 記錄，對應的伺服器將開始接收 IPv6 流量，因此將 IPv6 的 AAAA 記錄添加到 DNS 之前，須徹底的進行 ICP 測試以確保 IPv6 在伺服器，負載平衡器等正常工作，這一點非常重要。

在推出期間，通過 IPv6 配置不正確的伺服器的返回 AAAA 記錄，ICP 破壞了很多 IPv6 用戶的站點，一旦測試成功，每個 IPv4 位址具有 A 記錄

的外部可見主機(或虛擬機)都需要 IPv6 位址具有 AAAA 記錄[RFC3596]，如果適用，還需要一個迴轉分錄(在 ip6.arpa 中)，請注意，如果正在使用 CNAME 記錄，必須在 CNAME 鏈最後面的 A 記錄旁邊添加 AAAA 記錄。

根據[RFC1912]，不可能使 AAAA 記錄的名稱與用於 CNAME 記錄的名稱相同，重要的細節是，某些客戶端(尤其是 Windows XP)只能通過 IPv4 解析 DNS 名稱，即使它們可以將 IPv6 用於應用程序流量。

此外，雙協定分解器可能會嘗試通過 IPv6 解析對 A 記錄的查詢，或者通過 IPv4 解析對 AAAA 記錄的查詢，因此，建議所有 DNS 服務器都通過 IPv4 和 IPv6 應對查詢。

表 23 RFC5340、RFC5308…等參考文獻

編號	RFC 編號	RFC 相關訊息	
		類別	時間
1	5340	Proposed Standard	2008/07
		標題：OSPF for IPv6	
2	5308	Proposed Standard	2008/10
		標題：Routing IPv6 with IS-IS	
3	2080	Proposed Standard	1997/01
		標題：RIPng for IPv6	
4	2081	Informational	1997/01
		標題：RIPng Protocol Applicability Statement	
5	5838	Proposed Standard	2010/04
		標題：Support of Address Families in OSPFv3	
6	2827	Best Current Practice	2000/05
		標題：Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing	
7	3704	Best Current Practice	2004/05
		標題：Ingress Filtering for Multihomed Networks	
8	6296	Experimental	2011/06
		標題：IPv6-to-IPv6 Network Prefix Translation	
9	3596	Internet Standard	2003/10
		標題：DNS Extensions to Support IP Version 6	
10	1912	Informational	1996/02
		標題：Common DNS Operational and Configuration	

編號	RFC 編號	RFC 相關訊息	
		類別	時間
		Errors	

(二) 伺服器

1. 網路堆疊

目前受歡迎系統中，TCP/IP 網路堆疊已經支援 IPv6 多年，多數情況下，啟用 IPv6 和可能的 DHCPv6 就足夠了，其餘的將隨之而來，ICP 網路內部的伺服器，除了簡單的雙協定外，將不需要支援任何過渡技術，由於某些作業系統針對 IPv4 和 IPv6 具有單獨的防火牆規則，因此 ICP 還應評估這些規則，並確保為 IPv6 配置了適當的防火牆規則。

2. 應用層

基本的 HTTP 伺服器能夠處理啟用 IPv6 的網路堆疊，因此有必要更新到更新的軟體版本，如電子郵件協定之類的通用應用程序也是如此。

關於其他應用程序，尤其是專有應用程序，無法做出一般性聲明，因此每個 ASP 將需要做出自己的判定，由於對網路層進行更改以引入 IPv6 位址會在應用程序中引起漣漪效應，因此，在將生產環境進行雙協定之前，應在僅 IPv4，IPv6-Only 和雙協定環境中，對客戶端和伺服器應用程序進行測試，這裡的一項重要建議是，所有應用程序都應使用與 IP 版本無關的域名，而不是 IP 位址。

基於中介平台應用程序具有對 IPv4 和 IPv6 的共同支援，例如 Java，理所當然可同時支援 IPv4 和 IPv6，而無需進行其他工作，安全憑證還應包含域名而不是位址。

基於 HTTP 伺服器的特定問題是，基於 IP 位址的 cookie 身份驗證方案將需要處理雙協定客戶端，伺服器可能會為 IPv4 連接或 IPv6 連接創建 cookie，具體取決於客戶端位置上的設置以及客戶端作業系統的奇想，不保

證給定的客戶端將始終使用相同的位址系列，尤其是在存取網站的集合而不是單個網站時，例如在將 cookie 用於聯合身份驗證時，如果客戶端使用隱私位址[RFC4941]，則 IPv6 位址(但通常不是其/64Prefix)可能會非常頻繁地更改。

任何基於 32-bit IPv4 位址的 cookie 機制都需要進行重大的重構，在[RFC4038]中討論了有關應用程序轉換的一般注意事項，但其中許多不適用於雙協定 ICP 方案，創建和維護自己應用程序的 ICP，需要檢查它們是否依賴於 IPv4。

表 24 RFC4941、RFC4038 參考文獻

編號	RFC 編號	RFC 相關訊息	
		類別	時間
1	4941	Draft Standard	2007/09
		標題：Privacy Extensions for Stateless Address Autoconfiguration in IPv6	
2	4038	Informational	2005/05
		標題：Application Aspects of IPv6 Transition	

3. 紀錄

引入 IPv6 客戶端通常會導致 IPv6 位址出現在伺服器紀錄檔的“客戶端 ip”欄位中，使用相同的紀錄檔欄位保存客戶端的 IP 位址(無論是 IPv4 還是 IPv6)會是方便的，查看記錄檔和客戶端 IP 位址的下游系統也可能需要進行測試，以確保它們可以正確處理 IPv6 位址，這包括 ICP 記錄客戶端 IP 位址的任何資料庫，例如用於記錄在線購買和註解標語的 IP 位址的資料庫。

值得注意的是，從紀錄檔到個人客戶的準確回溯，需要端到端位址透通性，這是 ICP 支援本機 IPv6 連接的另一個動機，否則 IPv6-Only 的客戶將不可避免地通過某種形式的轉換機制進行連接，從而乾擾回溯。

4. 地理位置

最初，ICP 可能會發現 IPv6 客戶端的地理位存在一些弱點，隨著時間的流逝，可以假設地理定位方法和資料庫將被更新以完全支援 IPv6Prefix。

從長期觀看，沒有理由比 IPv4 的精度更高，然而隨著時間流逝，我們可以預期會有更多的行動客戶端，因此在任何情況下，僅基於 IP 位址進行地理位置定位都會成為問題，可以考慮使用更強大的技術，例如啟用 HTTP 的位置傳遞(HELD)[RFC5985]。

表 25 RFC5985 參考文獻

編號	RFC 編號	RFC 相關訊息	
		類別	時間
1	5985	Proposed Standard	2010/09
		標題：HTTP-Enabled Location Delivery (HELD)	

(三) 操作與管理

毫無疑問，最初 IPv6 有效運用將對操作產生影響，並且還將需要教育和訓練，人員將不斷更新路由器等網路元件、更新配置，最終向用戶提供資訊以及診斷新問題。

然而對於企業網路而言，例如，在許多大學校園中都有豐富的經驗，這表明在穩定狀態下，雙協定操作並不比 IPv4 難，還需要對 IPv4 執行任何管理，監視和紀錄檔記錄，因此必須更新用於這些目的的所有產品和工具，以完全支援 IPv6 管理數據，重要的是要驗證工具是否已完全更新以支援以十六進制格式輸入和顯示的 128bit 位址[RFC5952]。

由於 IPv6 網路可以使用一個以上的 IPv6Prefix 操作，因此每台主機可以使用一個以上的位址，因此這些工具必須在正常情況下進行處理。這包括使用中的任何位址管理工具以及用於創建 DHCP 和 DNS 配置的工具，這裡站點重新編號[RFC6879]中涉及的工具有很多重疊。

在 IPv6 部署的早期階段，很可能主要透過 IPv4 傳輸來管理 IPv6，這使網路管理系統可以測試 IPv4 和 IPv6 管理數據之間的依賴性，例如，是否會正確顯示混合顯示 IPv4 和 IPv6 位址的報告？在第二階段，應使用 IPv6 傳輸來管理網路，請注意，即使在遠端工作時，ICP 也有必要為其操作和支援人員提供 IPv6 連接，對於管理數據和傳輸，都應盡可能避免 IPv4 和 IPv6 之間的相互依賴性，一個失敗不應導致另一個失敗。

避免這種情況的一種預防措施是將網路管理系統雙堆疊，這樣就可以使用 IPv4 連接來修復 IPv6 配置，反之亦然雙堆疊是有必要的，但確實具有

管理擴展性和開銷方面的考慮。

如前所述，長期目標是在網路及其客戶可支援的情況下，轉向單疊 IPv6，這是在管理系統中應避免位址家族間相互依賴的另一個原因；多年以來被遺忘對 IPv4 的隱藏依賴將非常不便，特別是管理 IPv6 但本身僅在 IPv4 上運行的管理工具在 IPv4 關閉的那一天會造成災難的後果，ICP 應確保更新任何端到端可用性監視系統，以通過 IPv4 和 IPv6 監視雙堆疊伺服器。

這裡的特殊挑戰可能是監視憑藉 DNS 名稱的系統，這可能導致僅監視 IPv4 或 IPv6 中的一個，無法透過任一位址家族查看網路連接故障，如上所述，即使在遠端工作時，ICP 也有必要為其操作和支援人員提供 IPv6 連接。

表 26 RFC5952、RFC6879 參考文獻

編號	RFC 編號	RFC 相關訊息	
		類別	時間
1	5952	Proposed Standard	2010/08
		標題：A Recommendation for IPv6 Address Text Representation	
2	6879	Informational	2013/02
		標題：IPv6 Enterprise Network Renumbering Scenarios, Considerations, and Methods	

(四) 應用服務安全考量

儘管許多 ICP 可能仍在試驗和配置 IPv6 的過程中，但猖獗的成長惡意軟體將對 IPv6 發起攻擊，例如：為主機名添加了 AAAA DNS 記錄，則使用客戶端操作資料庫系統的惡意軟體，可能會自動通過 IPv4 攻擊該主機名轉變為通過 IPv6 攻擊該主機名。因此保護伺服器防火牆和其他網路安全設備支援 IPv6 並測試和配置規則十分重要。

應該將 IPv4 的安全經驗作為引導，以瞭解 IPv6 中可能存在的威脅，但不應認為它們具有相同的可能性，也不應該將其視為 IPv6 中可能存在的唯一威脅，然而實際上，或多或少地存在於 IPv4 的每種威脅或將存在於 IPv6，

必須更新防火牆、入侵檢測系統、拒絕服務預防措施和安全審核技術，以完全支援 IPv6，不用說，打開眾所周知的安全機制(例如 DNS 安全性和 DHCPv6 身份驗證)也很重要，否則 IPv6 將成為攻擊者的誘人目標。

當使用多個 PAPrefix 時，防火牆規則必須允許所有有效 Prefix，並且必須設置作為按預期工作，即使數據封包是通過一個 ISP 發送，但返回數據封包則是通過另一個 ISP 到達的，必須考慮雙堆疊防火牆的效能和記憶體大小方面。

在雙堆疊操作中，兩種協議之間可能存在交叉感染的風險。例如，成功的基於 IPv4 的拒絕服務攻擊，反之亦然也可能耗盡 IPv6 服務所需的資源，這種風險強化的論點，即 IPv6 安全性必須達到與 IPv4 相同的級別，雙堆疊虛擬私人網路(VPN)解決方案[VPN-LEAKAGES]也可能發生風險。

[RFC4864]中概述了保護 IPv6 網路不受外部攻擊的技術，假設 ICP 具有本地 IPv6 連接，建議使用 IPv4 協定類型 41 阻止傳入的 IPv6-in-IPv4 通道流量，除[RFC6343]應阻止此類傳出流量，僅應根據[RFC4890]阻止 ICMPv6 通訊；特別是對路徑 MTU 發現 Packet Too Big 訊息一定不能阻止。

與 IPv4 相比，蠻力掃描攻擊發現主機存在於 IPv6 較低，然而這不應使 ICP 陷入錯誤的安全性，因為各種命名或尋址，可能會導致 IPv6 位址空間可預測或可猜測。

在極端情況下，IPv6 主機可能配置有非常容易猜測的介面 ID。例如從“ 1”開始的連續介面 ID 手動編號的主機或子網將更容易猜測，應避免這種做法，[RFC6583]中討論了其他有用的預防措施，同樣的攻擊者可能會在紀錄檔、數據封包追、DNS 記錄(包括反向記錄)或其他地方找到 IPv6 位址，還應考慮防止惡意路由器廣告(RA Guard)[RFC6105]。

傳輸層安全性版本 1.2 [RFC5246]及其以前的版本可與 IPv6 上的 TCP 正確配合使用，這意味著基於 HTTPS 的安全性解決方案可立即應用，這同

樣適用於任何其他傳輸層或應用層安全技術。

如果 ASP 以任何方式使用 IPsec [RFC4301]和網路金鑰交換(IKE)協定[RFC5996]來保護與客戶端的連接，它們也完全適用於 IPv6，但前提是兩端的軟體堆疊已正確更新。

表 27 RFC4864、RFC6343…等參考文獻

編號	RFC 編號	RFC 相關訊息	
		類別	時間
1	4864	Informational	2007/05
		標題：Local Network Protection for IPv6	
2	6343	Informational	2011/08
		標題：Advisory Guidelines for 6to4 Deployment	
3	4890	Informational	2007/05
		標題：Recommendations for Filtering ICMPv6 Messages in Firewalls	
4	6583	Informational	2012/05
		標題：Operational Neighbor Discovery Problems	
5	6105	Informational	2011/02
		標題：IPv6 Router Advertisement Guard	
6	5246	Proposed Standard	2008/08
		標題：The Transport Layer Security (TLS) Protocol Version 1.2	
7	4301	Proposed Standard	2005/12
		標題：Security Architecture for the Internet Protocol	
8	5996	Proposed Standard	2010/09
		標題：Internet Key Exchange Protocol Version 2 (IKEv2)	

第二節 ISP IPv6 網路連線服務安全防護建議

一. 固接網路連線服務安全防護建議

本報告提供 ISP IPv6 固接網路連線服務之安全防護建議，包含有電纜寬頻網路(Cable Network)、DSL(Digital Subscriber Line)寬頻網路與寬頻乙太網路，並且根據不同網路存取服務特性，提供網路安全防護建議。

(一) 電纜寬頻網路

本節描述家用電纜寬頻網路(Cable Network)現有的基礎設施，以及電纜網路中的 IPv6 配置選項與安全防護建議。

1. 電纜寬頻網路元件

電纜寬頻網路能夠向用戶提供 IP 網路傳輸服務，以提供高速 Internet 存取和 IP 語音(VoIP, Voice over IP)服務。電纜數據服務介面規範(DOCSIS (Data Over Cable Service Interface Specification)規範)[RF-Interface]中概述了透過電纜網路傳輸 IP 流量的機制，以及定義如何透過電纜網路承載數據的標準。

以下是有線網路的一些關鍵元件：

混合光纖同軸(HFC, Hybrid fiber-coaxial)：混合光纖同軸電纜，用作基礎運輸。

CMTS(Cable modem termination system)：電纜數據機終端系統(可以是第 2 層橋接或第 3 層 CMTS 路由)。

- GWR(Gateway Router)：住宅閘道路由器(向主機提供第 3 層服務)。
- 主機：PC，筆記本電腦等，已連接到 CM(Cable Modem)或 GWR。
- CM(Cable Modem)：電纜數據機。
- ER(Edge Router)：邊緣路由器。

- MSO(Multiple-System Operator)：多服務營運商。

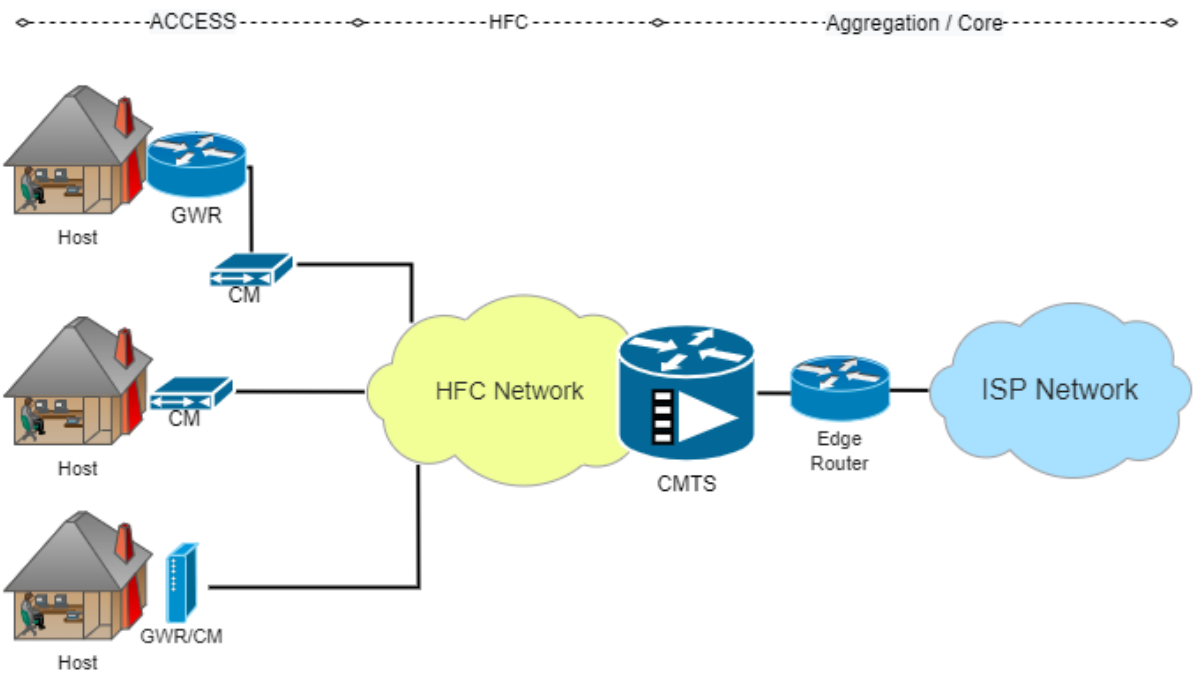

圖 2 電纜寬頻網路的關鍵元件

2. 於電纜寬頻網路部署 IPv6

(1) 在電纜網路中配置 IPv6

MSO(Multiple-System Operator)在其電纜網路上配置 IPv6 的動機之一是減輕管理負擔。出於管理目的，可以在 CM、CMTS 和 ER 上啟用 IPv6。目前電纜基礎設施的某些部分使用 IPv4 地址空間[RFC1918]，但是這些數量是有限的。因此，IPv6 最初可在管理平面上實現的電纜空間中具有實用性，之後可將其重點放在數據平面上以用於最終用戶服務。

表 28 RFC1918 參考文獻

編號	RFC 編號	RFC 相關訊息	
		類別	時間
1	1918	Best Current Practice	1996/02
		標題：Address Allocation for Private Internets	

目前的電纜網路中有兩種不同的配置模式：CMTS 橋接環境和 CMTS 路由環境，IPv6 可以配置在這兩種環境中。

- CMTS 橋接網路

  在這種情況下，CM 和 CMTS 橋接所有數據流量，來自主機設備的流量透過電纜網路轉發到 ER，然後 ER 透過 ISP 網路將流量路由至 Internet。然而，出於管理目的，CM 和 CMTS 應該需要支援一定程度的第 3 層功能。

- CMTS 路由網路

  在路由網路中，CMTS 使用 IP 路由機制，將封包路由至 ER 與 ISP 網路。CM 作為轉發數據流量的第 2 層橋接器，並出於管理目的支援某些第 3 層功能。

(2) IPv6 QoS

IPv6 不會更改或添加 DOCSIS 規範中已經存在的任何排隊/調度功能。但是 CMTS 和 CM 上的 QoS 機制需要具有 IPv6 功能。這包括對 IPv6 分類器的支援，因此可以將往返於主機設備的數據流量適當地分類為不同的服務流程，並為其分配適當的優先級(權)。對於單點傳播和多點傳播流量，需要實施適當的分類標準。

為了支援各種類型的服務，應在 CM 上針對上游流量進行流量分類和標記，並在 CMTS/ER 上針對下游流量進行流量分類和標記：數據、語音和影片。相同的 IPv4 QoS 概念和方法也應適用於 IPv6。

重要的是要注意，當對通訊進行端到端加密時，遍歷的網路設備

將無法存取許多用於分類目的的封包欄位。在這些情況下，路由器很可能會將封包放入預設類中。QoS 設計應考慮這種情況，並嘗試主要使用 IP 表頭欄位進行分類。

(3) IPv6 安全防護建議

DOCSIS 電纜網路中的安全性是使用 BaselinePrivacyPlus(BPI+)提供的，唯一依賴於 IP 地址是加密多點傳播。從語義上講，多點傳播加密在 IPv6 環境中的工作方式與在 IPv4 網路中的工作方式相同。然而，DOCSIS 規範中需要適當的增強，以支援加密的 IPv6 多點傳播。

為了增強安全性，必須對主機進行有限的更改。主機應使用於自動配置的隱私延伸[RFC3041]。如果主機或 GWR(Gateway Router)上可用，則可以啟用 IPv6 防火牆功能。

CMTS/ER 應該保護 ISP 網路和用戶免受其他用戶的攻擊。因此應在面對用戶的所有介面上使用單點傳播反向路徑轉發(uRPF)[RFC3704]和存取控制列表(ACL)。應該根據 IPv6 的操作要求進行過濾[IPv6-Security]。

CMTS/ER 應該保護其處理資源免受大量用戶控制流量的侵擾，例如：路由器和鄰居請求以及 MLD(Multicast Listener Discovery)請求。

與 IPv4 服務一起使用的所有其他安全功能也應類似地應用於 IPv6。

表 29 RFC3041、RFC3704 參考文獻

編號	RFC 編號	RFC 相關訊息	
		類別	時間
1	3041	Proposed Standard	2001/01
		標題：Privacy Extensions for Stateless Address Autoconfiguration in IPv6	
2	3704	Best Current Practice	2004/05
		標題：Ingress Filtering for Multihomed Networks	

(二) DSL 寬頻網路

本節描述了當今高速 DSL 網路中的 IPv6 配置選項與安全防護建議。

1. DSL 寬頻網路元件

數位用戶線路(DSL)寬頻服務透過本地迴路現有雙絞電話線為用戶提供 IP 連接。根據線路的品質以及用戶終端設備與數位用戶線路存取多工器(DSLAM)之間的距離，可以提供各種頻寬產品。

以下網路元件是 DSL 網路的典型代表：

- DSL 數據機：是獨立設備、合併到主機中，亦可合併路由器功能，作為 CPE 路由器。
- 用戶終端路由器(CPR)：為用戶終端網路提供第 3 層服務。通常用於為小型企業提供防火牆功能和分段廣播區域。
- 數位用戶線路存取多工器(DSLAM)：終止多條雙絞電話線，並向 BRAS 提供聚合。
- 寬頻遠端存取伺服器(BRAS, Broadband remote access server)：聚集或終止與用戶 DSL 電路相對應的多個永久虛擬電路(PVC)。
- 邊緣路由器(ER)：提供到 ISP 網路的第 3 層介面。

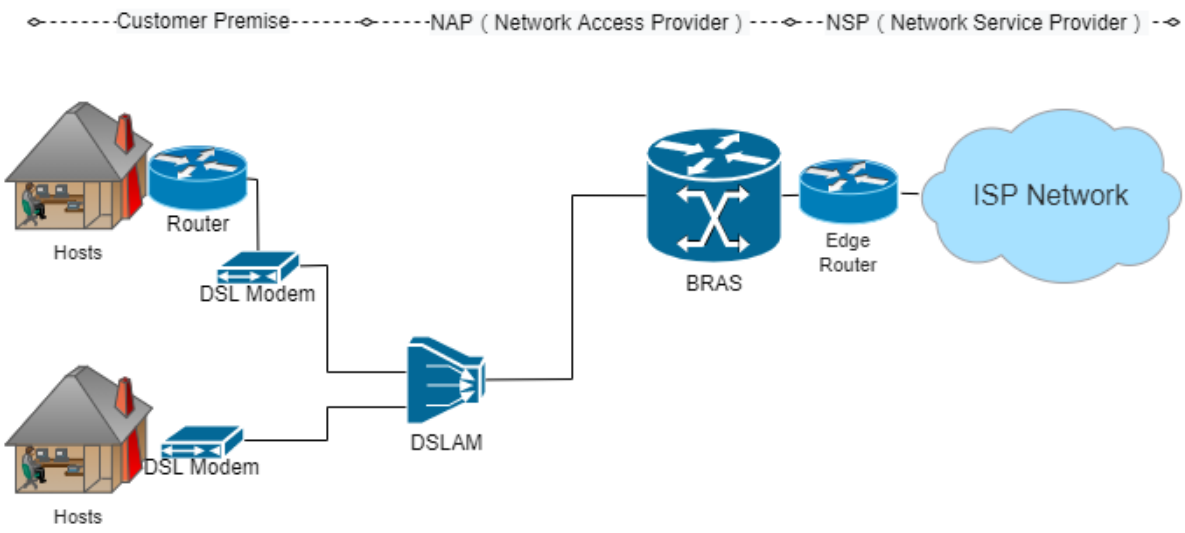

圖 3 DSL 寬頻網路的關鍵元件

2. 於 DSL 寬頻網路部署 IPv6

(1) 在 IPv4 DSL 網路中配置 IPv6

在聚合模型中，BRAS 在提供對 ISP 存取前，終止用戶 PVC 並聚合其連接。為了維持已被現有收益產生的 IPv4 服務證明和使用的配置概念和商業模型，IPv6 配置將與 IPv4 配對。描述了目前基於 DSL 寬頻存取的 IPv4 配置，在某些情況下，如果需要新的服務類型或服務，則 IPv4 和 IPv6 網路邏輯架構可能會有所不同。

透過 DSL 基礎結構提供 IPv4 連接的主要設計方法有三種：

- 點對點模型

每個用戶都透過雙絞線連接到 DSLAM，並配有一個唯一的 PVC，將其連接到服務網路服務提供者，PVC 可以在 BRAS 或邊緣路由器處終止。在這種情況下，必須在網路維護大量的第 2 層電路。

第 2 層領域可透過三種方式在 ER 處終止：

a. 在具有虛擬介面的通用網路橋接組中，該介面可將流量路由輸出。

b. 透過啟用路由橋接封裝功能，所有用戶都可以屬於同一子網。這是 IPv4 在 DSL 上最常見的配置方法，但在地址可用性問題的 IPv6 不是最佳選擇。

c. 透過在第 3 層終止 PVC，每個 PVC 都有自己的位址前綴，更適合 IPv6。

這些方法都不要求升級 CPE(DSL 數據機)。在這種情況下，來自主機或客戶前提路由器乙太網路幀橋接在分配給用戶 PVC 上。

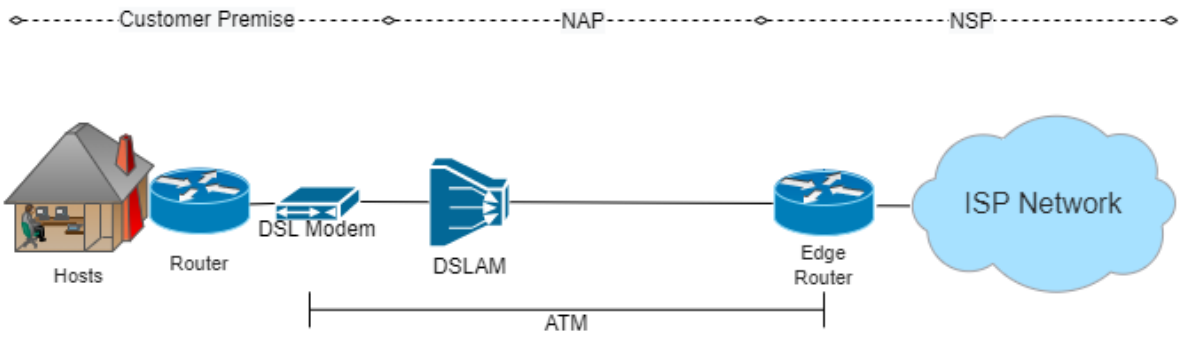

圖 4 點對點模型協定體系結構

a. IPv6 相關基礎架構更改

在這種情況下，DSL 數據機和整個 NAP 皆不知第 3 層，因此不需要更改即可支援 IPv6。必須將以下設備升級到雙協定：主機，客戶路由器(如果有)和邊緣路由器。

b. 定址

主機或客戶路由器將邊緣路由器作為其第 3 層逐跳。如果沒有客戶路由器，則訂閱者站點上的所有主機都屬於在邊緣路由器上為該訂閱者 PVC 靜態配置的同一/64 子網。主機可以使用無狀態自動配置，或基於狀態的 DHCPv6 配置透過邊緣路由器獲取地址。

由於為每個客戶手動配置是個難題，因此鼓勵實施者開發一種機制，將 PVC(或其他一些特定於客戶的訊息)自動反應到 IPv6 子網位址前綴，並將最少配置的特定位址前綴廣播給所有客戶。

如果存在客戶路由器：

- 自身與邊緣路由器之間的/64 子網上靜態配置的地址，並且在連接客戶站點的主機介面上靜態地配置/64 位址前綴，為非期望供應方法、昂貴且難以管理。

可使用本地連接地址與 ER 通訊，還可以透過無狀態自動配置動態獲取自身與 ER 之間的連接位址前綴。如需要後面的選項允許它與遠程 DHCPv6 伺服器聯繫，此步驟後，透過 DHCP-PD 請求位址前綴小於/64 位址前綴，該位址前綴又分為/64s，並分配給其下游介面。

邊緣路由器具有為每個用戶 PVC 配置的/64 位址前綴。應啟用每個 PVC，將用戶 DHCPv6 請求中繼到 ISP 網路中的 DHCPv6 伺服器，還必須啟用為使用 DHCP-PD 用戶提供存取權限的 PVC，以支援該功能，到 ISP 網路的上行連線也配置有/64 位址前綴。

用於用戶連接的位址前綴和透過 DHCP-PD 委派的位址前綴，應允許在邊緣路由器上盡可能匯集的方式進行規劃。

主機關心其他訊息(例如 DNS)是透過有狀態 DHCPv6[RFC3315]和無狀態 DHCPv6[RFC3736]提供。

表 30 RFC3315、RFC3736 參考文獻

編號	RFC 編號	RFC 相關訊息	
		類別	時間
1	3315	Proposed Standard	2003/07
		標題：Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	
2	3736	Proposed Standard	2004/04

編號	RFC 編號	RFC 相關訊息	
		類別	時間
		標題：Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6	

c. 路由

CPE 設備配置有指向邊緣路由器的預設路由，這些設備通常不需要資源、路由協定。

邊緣路由器運行 NSP 中使用的 IPv6IGP：OSPFv3 或 IS-IS 連接的位址前綴必須重新分配；使用 DHCP-PD，則邊緣路由器為每個委派位址前綴安裝一條靜態路由，必須重新分配靜態路由，位址前綴摘要應在邊緣路由器上進行。

- PPP 終止聚合(PTA)模型

在每個用戶和 BRAS 間打開 PPP 會談，BRAS 終止 PPP 會談，並在用戶和 ISP 間提供第 3 層連接。

PTA 結構依賴於 PPP 協定 (PPPoA[RFC23/64] 和 PPPoE[RFC2516])，PPP 會談由客戶前提設備發起，並在 BRAS 處終止，BRAS 授權會談對用戶進行身份驗證，並代表 ISP 提供 IP 地址、將用戶流量的第 3 層路由選擇到 NSP 邊緣路由器。

當 NSP 也是 NAP 時，BRAS 和 NSP 邊緣路由器可以是同一台設備，並提供上述功能。

此模型可以利用兩種類型的 PPP 封裝：

- 使用 PPPoA 進行連接

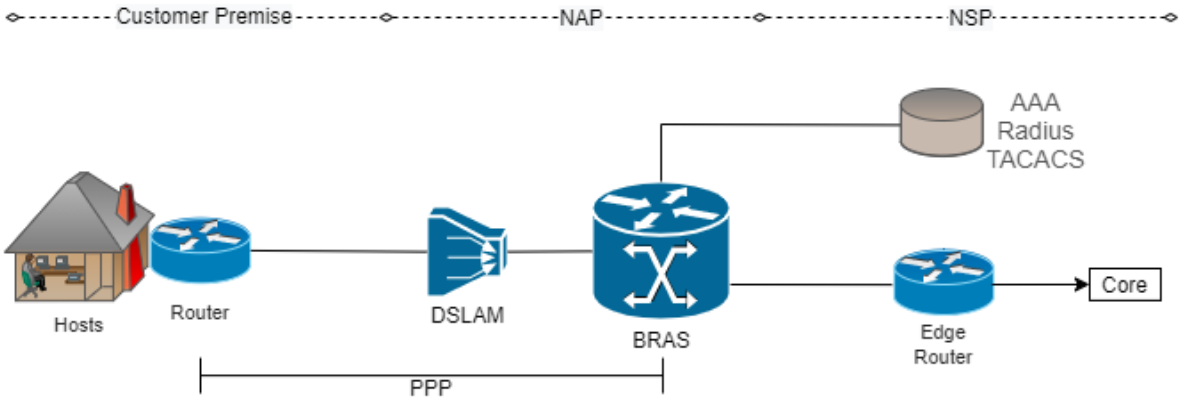

圖 5 使用 PPPoA 進行連接

PPP 會談由客戶前提設備開始；BRAS 根據本地或遠端資料庫對用戶進行身份驗證。建立會談後，BRAS 會為用戶提供地址，甚至是 DNS 伺服器，此訊息是從用戶配置文件或 DHCP 伺服器獲取。

解決方案延伸性比點對點更好，但每個 ATMPVC 只有一個 PPP 會談，因此用戶可以一次選擇一個 ISP 服務。

■ 使用 PPPoE 進行連接

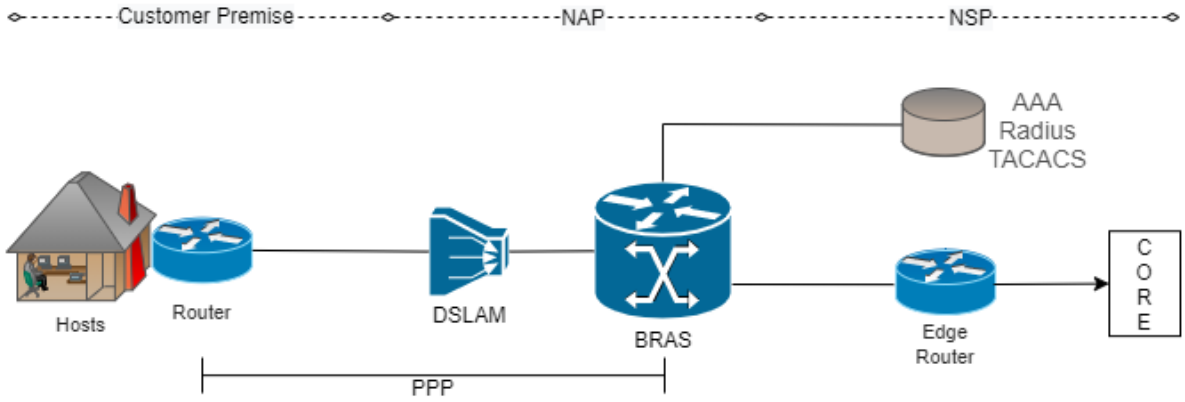

圖 6 使用 PPPoE 進行連接

PPPoE 的操作與 PPPoA 相似，不同之處在於 PPPoE 可以在同一 PVC 上支援多個會談(主機也可開始 PPPoE 會談)，允許用戶同時連接多個服務。重要的是附加的表頭，PPPoE 封裝會減少可用於

客戶流量 IPMTU。

不管使用哪種 PPP 封裝類型，PTA 模型的網路設計和操作皆相同。

a. IPv6 相關基礎架構更改

BRAS 支援第 3 層，必須對其進行升級以支援 IPv6，由於它終止 PPP 會談，須支援使用 IPv6 以實施這些 PPP 協定、將主機、客戶路由器(如果有)、BRAS 和邊緣路由器設備升級為雙協定。

b. 定址

BRAS 終止 PPP 會談，並配置文件為用戶提供 IPv6 地址。用於授權和身份驗證的用戶配置文件可以位於 BRAS 或“身份驗證、授權和計費(AAA)”伺服器。主機或客戶路由器將 BRAS 作為第 3 層逐跳。

PPP 會談可由主機或客戶路由器發起。於後者情況下，一旦與 BRAS 建立了會談並且協商了指向 BRAS 的上行連接地址，則 DHCP-PD 可用於獲取客戶路由器其他介面位址前綴。

必須啟用 BRAS，以支援 DHCP-PD 併中繼用戶站點主機 DHCPv6 請求。BRAS 與邊緣路由器連接配置/64 位址前綴。邊緣路由器連接提供與 ISP 網路其餘部分連接。用戶位址前綴和透過 DHCP-PD 委派的位址前綴應允許在 BRAS 進行最大匯集進行規劃。

c. 路由

BRAS 運行 IGP 到邊緣路由器：OSPFv3 或 IS-IS，分配給 PPP 會談地址為已連接主機路由，必須重新分配已連接位址前綴；使用 DHCP-PD，邊緣路由器為每個委派位址前綴安裝一條靜態路由、重新分配靜態路由。

邊緣路由器正在運行 ISP 網路中使用的 IGP：OSPFv3 或 IS-IS。如果單獨管理 ISP 和存取提供程序路由領域(建議分開)，在存取提供程序 IGP 和 ISPIGP 間需要受控的重新分配。

- L2TPv2 存取聚合(LAA)模型

每個用戶和 ISP 邊緣路由器間開 PPP 會談。BRAS 透過將用戶 PPP 會談封裝到 L2TPv2[RFC2661]隧道中，將用戶 PPP 會談隧道傳輸到 ISP。

在 LAA 模型中，BRAS 透過在 BRAS 與邊緣路由器間建立的 L2TPv2 隧道將 CPE 發起的會談轉發給 ISP，身份驗證、授權和用戶配置由 ISP 本身執行。

表 31 RFC2661 參考文獻

編號	RFC 編號	RFC 相關訊息	
		類別	時間
1	2661	Proposed Standard	1999/08
		標題：Layer Two Tunneling Protocol "L2TP"	

此模型可以利用兩種類型的 PPP 封裝：

- 透過 PPPoA 連接

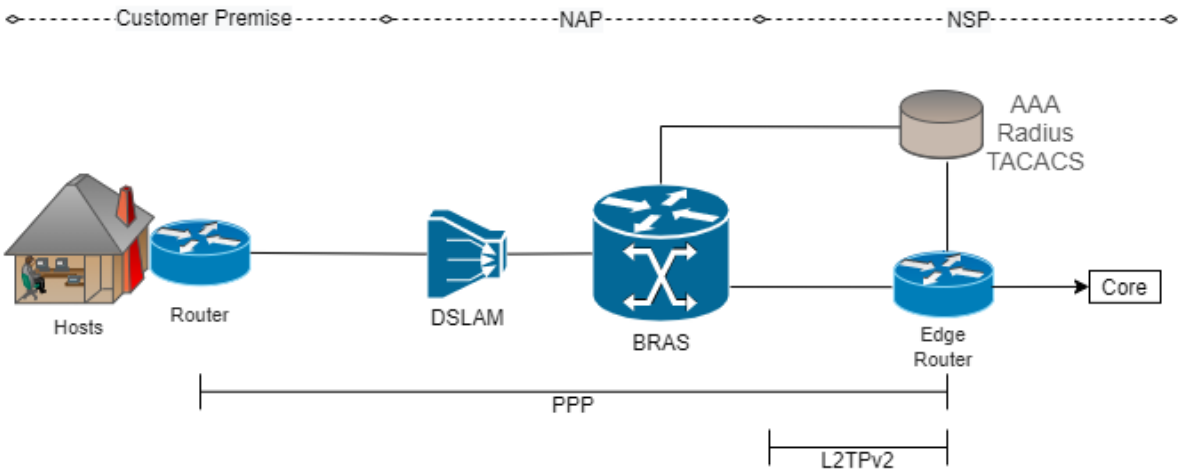

圖 7 L2TPv2 存取聚合(LAA)模型透過 PPPoA 連接

- 透過 PPPoE 連接

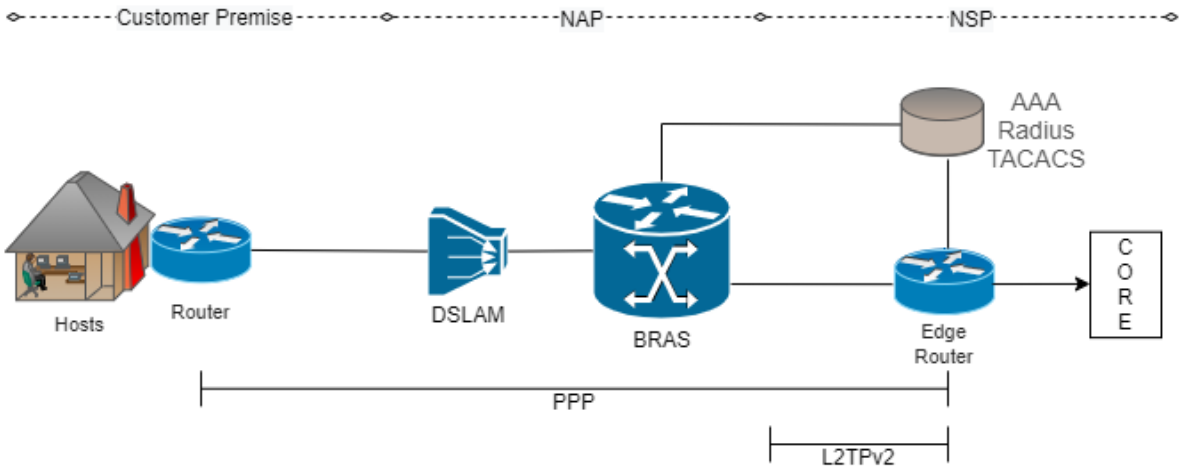

圖 8 L2TPv2 存取聚合(LAA)模型透過 PPPoE 連接

不管使用哪種 PPP 封裝類型，PTA 模型的網路設計和操作皆相同。

a. IPv6 相關基礎架構更改

BRAS 將透過用戶發起的 PPP 會談透過建立的 L2TPv2 隧道轉發到 ISP 網路中的聚合點 L2TP 網路伺服器(LNS)。L2TP 存取集中器(LAC)和 LNS 之間的 L2TPv2 隧道可以在 IPv6 或 IPv4 上運行。如果在 IPv6 上建立了隧道，必須將 BRAS 升級到雙協定。

b. 定址

用於授權和身份驗證的用戶配置文件可位於邊緣路由器或 AAA 伺服器上，主機或客戶路由器將邊緣路由器第 3 層逐跳。

PPP 會談可由主機或客戶路由器發起。在後者情況下，與邊緣路由器建立會談，DHCP-PD 即可用於獲取客戶路由器介面位址前綴，必須啟用邊緣路由器以支援 DHCP-PD 併中繼由用戶站點上的主機生成的 DHCPv6 存取。

注意 IPv6 配置與 IPv4 配置間存在顯著差異。IPv4 客戶路由器或 CPE 可終止於任何邊緣路由器(作為 LNS)，前提是假定至少有兩個出於冗餘目的，身份驗證後，將向客戶提供與其連接的

ER(LNS)的 IP 地址。這允許 ER(LNS)匯集分發給客戶地址。

IPv6 無論連接到哪個 ER(LNS)，客戶都應保留自己的地址。這可能會大大降低 ER(LNS)位址前綴聚合功能。目前的 IPv4 配置是動態的，同一用戶可根據最終連接到的 LNS 獲得不同地址。

解決方案是確保給定的 BRAS 始終連接到相同的 ER(LNS)，除非 LNS 關閉，來自位址前綴範圍的客戶將始終連接到相同的 ER,每個 ER(LNS)都可以在路由協定配置中作為主要 ER(LNS)位址前綴和次要位址前綴。在 ER(LNS)上變為“活動”狀態，便會進行匯集。

c. 路由

BRAS 運行 IPv6IGP 到邊緣路由器：OSPFv3 或 IS-IS，如果 NAP 和 NSP 由不同的組織管理，應在兩個領域間重新分配。

邊緣路由器正在運行 ISP 網路中使用的 IPv6IGP：OSPFv3 或 IS-IS。

- IPv4 和 IPv6 服務的混合模型

a. LAA 模型中的 IPv4 和 PTA 模型中的 IPv6

兩種基於 PPP 的模型 PTA 和 LAA 的共存相對簡單。LAA 模型中配置現有 IPv4 服務的 PPP 會談在邊緣路由器上終止；PTA 模型中配置新 IPv6 服務的 PPP 會談在 BRAS 上終止。

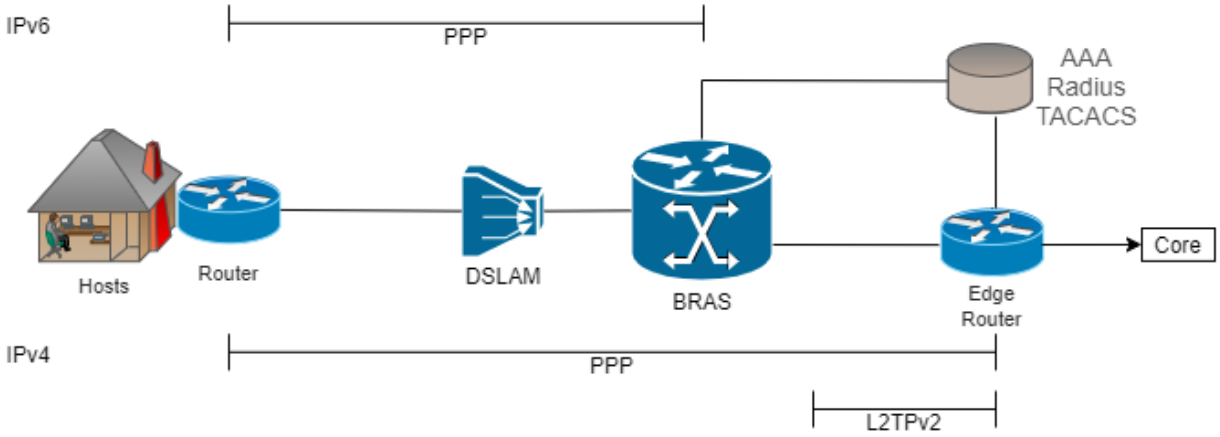

圖 9 LAA 模型中 IPv4 和 PTA 模型中 IPv6 的邏輯設計

b. LAA 模型中的 IPv4 和修改後的點對點模型中的 IPv6

對於 LAA 模型中的 IPv4 服務 PVC 在 BRAS 上終止，而 PPP 會談在邊緣路由器(LNS)上終止。對於點對點模型中的 IPv6 服務，如圖 3.1 中所述，PVC 在邊緣路由器處終止。在此混合模型中，可以在 NAP 擁有的設備 BRAS 上終止點對點連接，將 IPv6 流量透過 NAP 網路路由到 NSP。為了擁有這種混合模型，必須將 BRAS 升級為雙協定路由器，邊緣路由器的功能現已在 BRAS 上實現。

此配置模型的另一方面是，BRAS 必須能夠區分必須跨 L2TPv2 隧道橋接的 IPv4PPP 流量和必須路由至 NSP 的 IPv6 封包。在此混合設計中，必須在所有具有支援 IPv4 和 IPv6 服務的 PVC 的介面上啟用 IPv6 路由和橋接封裝(RBE)。

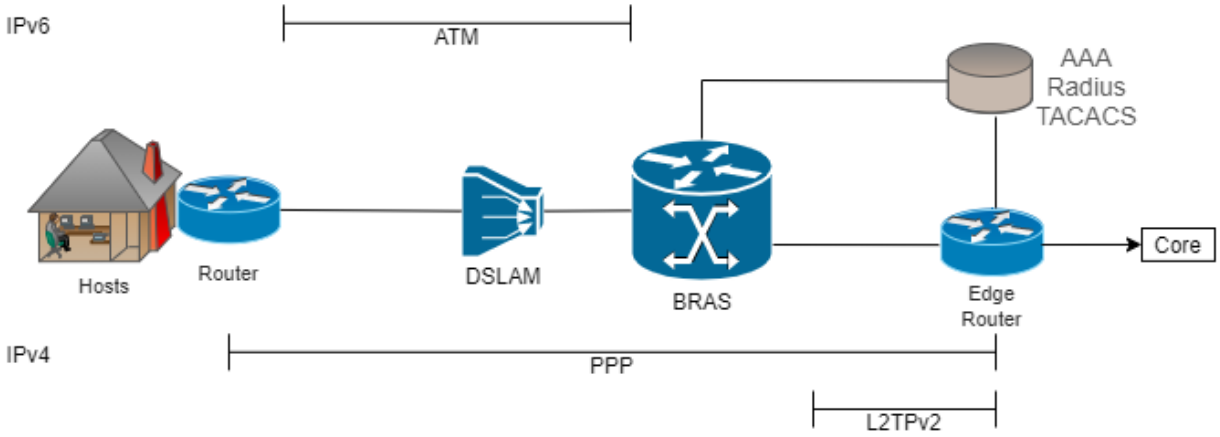

圖 10 LAA 模型中 IPv4 和修改後的點對點模型中 IPv6 的邏輯設計

(2) IPv6 QoS

QoS 配置與代表用戶的第 3 層逐跳路由器(PTA 模型中的 BRAS 或 LAA 和點對點模型中的邊緣路由器)特別相關，以便管理多個用戶間共享的資源，可能帶有各種服務級別協定。

在 DSL 基礎結構中，預期已經為 IPv4 連接實現了一定程度的流量監管。這是在整個 NAP 中實施的，超出了本文檔的範圍。

在 BRAS 或邊緣路由器上，必須配置面對用戶的介面以管理入站的客戶流量，並根據服務水平協定(SLA)調整出站到客戶的流量。

為了支援各種類型的客戶流量(數據，語音和影片)並最優化地使用基礎結構資源，流量分類和標記也應該在距離用戶最近(第 3 層)的路由器上進行。每個網路服務提供者(NAP，NSP)可以實施自己的 QoS 策略和服務，以便可以在 NAP 和 NSP 之間的邊界執行重新分類和標記，以確保 ISP 可以正確處理流量。相同的 IPv4QoS 概念和方法也應與 IPv6 一起使用。

重要的是要注意，當對通訊進行端到端加密時，遍歷的網路設備將無法存取許多用於分類目的的封包欄位。在這些情況下，路由器很可能會將封包放入預設類中。QoS 設計應考慮這種情況，並嘗試主要

使用 IP 表頭欄位進行分類。

(3) IPv6 安全防護建議

為了增強安全性，CPE 必須進行有限的更改。主機應使用自動配置的隱私延伸[RFC3041]。ISP 相對容易地追蹤它分配給用戶的位址前綴。但法規要求 ISP 在/128 地址級別追蹤其用戶，則可以與可提供主機可追溯性的網路管理工具並行實施隱私延伸。如果存在，則應在主機或 CPR 上啟用 IPv6 防火牆功能。

ISP 提供了針對來自其自身用戶的攻擊的安全性，但它也可以實施安全服務，以保護其用戶免受來自其網路外部的攻擊。此類服務不適用於此處討論的網路存取級別。

為用戶(BRAS 或邊緣路由器)的第 3 層逐跳的設備應保護網路和用戶免受其他用戶的攻擊。因此應在面對用戶的所有介面上使用 uRPF 和 ACL。應當根據 IPv6 的操作要求進行過濾[IPv6-Security]。

BRAS 和邊緣路由器應保護其處理資源，以防止有效的客戶控制流量氾濫，例如：路由器和鄰居請求以及 MLD 請求。速率限制應在所有面對用戶的介面上實施。應該將重點放在多點傳播類型的流量上，因為 IPv6 控制平面最常使用它。

與 IPv4 服務一起使用的所有其他安全功能也應類似地應用於 IPv6。

表 32 RFC3041 參考文獻

編號	RFC 編號	RFC 相關訊息	
		類別	時間
1	3041	Proposed Standard	2001/01
		標題：Privacy Extensions for Stateless Address Autoconfiguration in IPv6	

(三) 寬頻乙太網路

本節描述目前寬頻乙太網路存取中的 IPv6 配置選項與安全防護建議。

1. 乙太存取網路元件

支援 RJ-45 或光纖(光纖到府(FTTH)服務)配置到用戶的基礎結構環境中，提供 10/100Mbps 乙太網路寬頻服務，在多用戶的大城市區域中，該區域能以划算的方式配置，以及都會網路服務可向網路服務提供者提供聚合和上行服務。

以下是乙太網網路元件的典型代表：

- 存取交換機：作為訂閱者的第 2 層存取裝置。
- 客戶前提路由器：作為客戶前提網路，提供第 3 層服務。
- 聚合乙太網交換機：聚集多個用戶。
- 寬頻遠端存取伺服器(BRAS)、邊緣路由器(ER)。

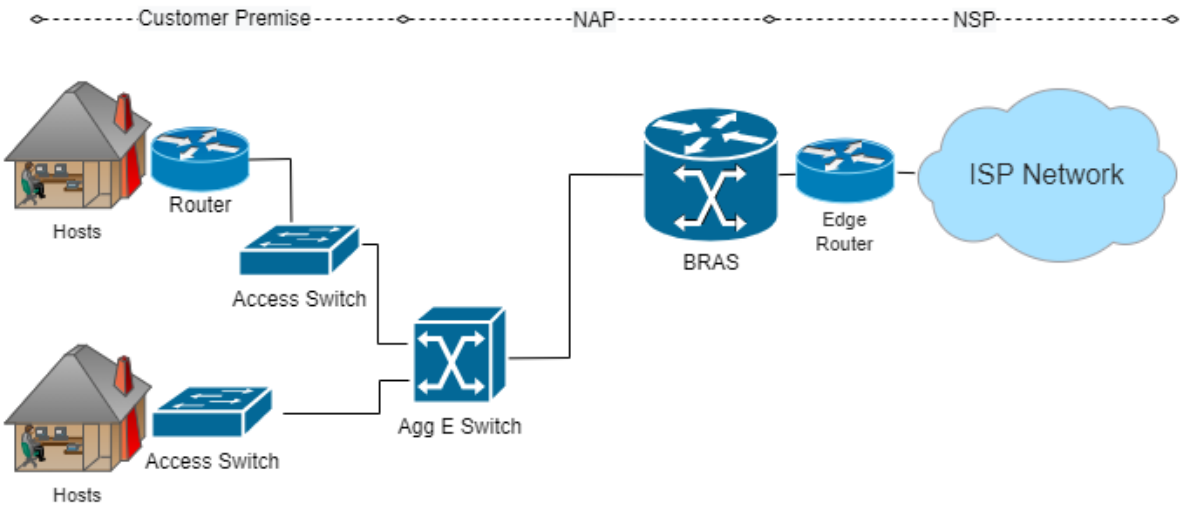

圖 11 乙太存取網路的關鍵元件

寬頻乙太網的邏輯拓撲和設計與第 3 節中討論的 DSL 寬頻網路非常相似，值得注意的是，本節中描述的一般操作，概念和建議類似地適用於基於 HomePNA 網路環境。在此環境中，某些網路元件可能使用不同的名稱。

2. 於寬頻乙太網路部署 IPv6

(1) 在 IPv4 寬頻乙太網路中配置 IPv6

透過乙太網基礎結構提供 IPv4 連接的主要設計方法有三種：

- 點對點模型

每個用戶都透過 RJ-45 或光纖連接到網路存取交換機，在存取交換機上分配一個 VLAN(可以在 BRAS 或邊緣路由器上終止)，透過 802.1Q 中繼到第 3 層設備(BRAS 或邊緣路由器)。

透過 VLAN 橋接，主機或客戶前提路由器乙太網路分配給用戶。

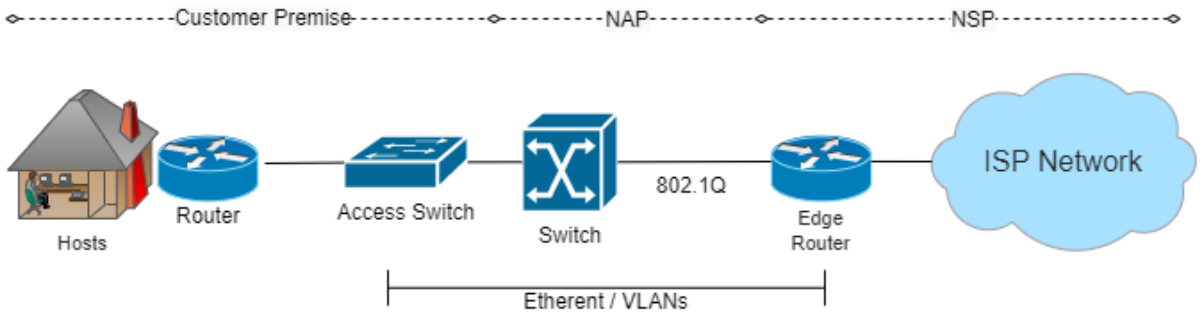

圖 12 點對點模型協定體系結構

- L2TPv2 存取聚合(LAA)模型

每個用戶和 BRAS 間打開 PPP 會談，BRAS 終止 PPP 會談，並在用戶和 ISP 間提供第 3 層連接。

在 LAA 模型中，BRAS 透過在 BRAS 與邊緣路由器之間建立的 L2TPv2 隧道將 CPE 發起的會談轉發給 ISP。在這種情況下，身份驗證、授權和用戶配置由 ISP 本身執行。

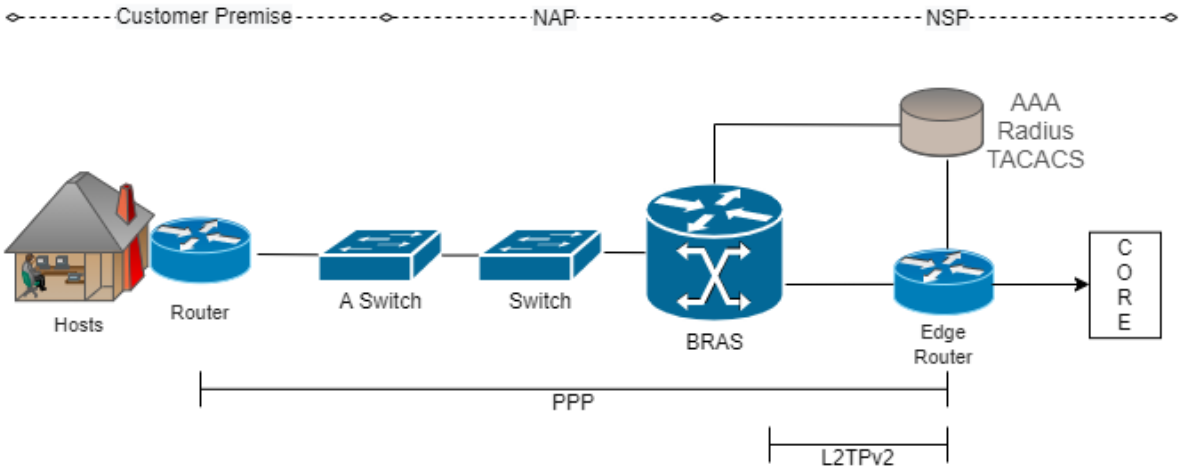

圖 13 L2TPv2 存取聚合(LAA)模型

- IPv4 和 IPv6 服務的混合模型

在每個用戶和 ISP 終端設備間打開 PPP 會談。BRAS 透過將用戶 PPP 封裝到 L2TPv2 隧道中，將它們傳輸到 ISP。

建議 IPv6 服務實現反應現有的 IPv4，簡化可管理性，並最小化了操作網路人員所需培訓。如果網路設計(用於 IPv4 的服務)支援此新服務，將不同的設計於 IPv6。

這種情況是網路服務提供者在整個 NAP 基礎結構中捆綁使用 LAA 並在其上建立隧道，該基礎設施由多個 BRAS 路由器、匯集路由器等組成，終點是 ISP 邊緣路由器。如果 SP 決定透過這種設計提供多點傳播服務，它將面臨 NAP 資源過度利用問題。邊緣路由器只能在隧道的末端複製多點傳播流量，所有用戶的副本都在整個 NAP 上進行。

修改後的點對點或 PTA 模型更適合支援多點傳播服務，在靠近 BRAS 目的地進行封包複製，拓撲節省了 NAP 資源。

IPv6 配置可以構建更好地支援服務擴展的基礎架構。將 LAA 設計用於其 IPv4 服務的 SP 會選擇針對 IPv6 修改後的點對點或 PTA 設計。

(2) IPv6 QoS

QoS 配置與用戶第 3 層逐跳路由器(PTA 模型中的 BRAS 或 LAA 和點對點模型中邊緣路由器)相關，以便管理多用戶間共享資源、帶有各種服務級別協定。

在 BRAS 或邊緣路由器上，必須配置面對用戶的介面以管理入站流量，並根據 SLA 調整出站流量。流量分類和標記也應該在最接近用戶(第 3 層)進行，以支援各類型客戶流量：數據、語音、影視。

該基礎架構提供了很好的機會來利用第 2 層設備的 QoS 功能。用於 IPv4 的基於區分服務的 QoS 應該擴展到 IPv6。

每個網路服務提供者(NAP，NSP)都可實施自己的 QoS 策略，以便在 NAP 和 NSP 間的邊界執行重新分類和標記，確保 ISP 可以正確處理流量，也應適用於 IPv6。

注意當對通訊進行端到端加密時，網路設備將無法存取許多用於分類目的封包欄位，路由器很可能會將封包放入預設類。

QoS 設計應考慮這種情況，並嘗試主要使用 IP 表頭欄位進行分類。

(3) IPv6 安全防護建議

為增強安全性，CPE 必須進行有限修改。主機應使用於自動配置隱私擴展[RFC3041]與可追溯性，並且應在主機或客戶前提路由器上啟用 IPv6 防火牆功能。

ISP 提供用戶攻擊安全性，也可以實施安全服務，以保護其用戶免受外部網路攻擊，不適用於此處討論的網路存取。

乙太網路的任何第二層過濾器，NAP 必須允許 IPv6 乙太網路類型(0X86DD)。

作為用戶第 3 層逐跳設備(BRAS 邊緣路由器)應保護網路和其他用戶免受網路服務提供者客戶攻擊，應在面對用戶的所有介面上使用

uRPF 和 ACL，根據 IPv6 的操作要求進行過濾[IPv6-Security]。

BRAS 和邊緣路由器應保護處理資源，以防止流量氾濫，例如：路由器和鄰居請求以及 MLD 請求，在 IPv6 控制平面最常用的多點傳播類型流量上，與 IPv4 所有安全功能也應應用於 IPv6。

表 33 RFC3041 參考文獻

編號	RFC 編號	RFC 相關訊息	
		類別	時間
1	3041	Proposed Standard	2001/01
		標題：Privacy Extensions for Stateless Address Autoconfiguration in IPv6	

(四) 小結論

IPv6 安全防護建議：

- 主機應使用自動配置的隱私延伸。
- 應在主機或用戶端網路存取設備上啟用 IPv6 防火牆功能。
- ISP 應保護其用戶免受來自其他用戶與其網路外部的攻擊。
- 乙太網路設備的第二層過濾器須允許 IPv6 乙太網路類型(0X86DD)。
- ISP 在 CMTS、BRAS 或 ER 應保護其處理資源，以防止有效的客戶控制流量氾濫。

二. 行動網路連線服務安全防護建議

(一) 參考架構和術語

以下圖 14 是行動網路的參考架構。

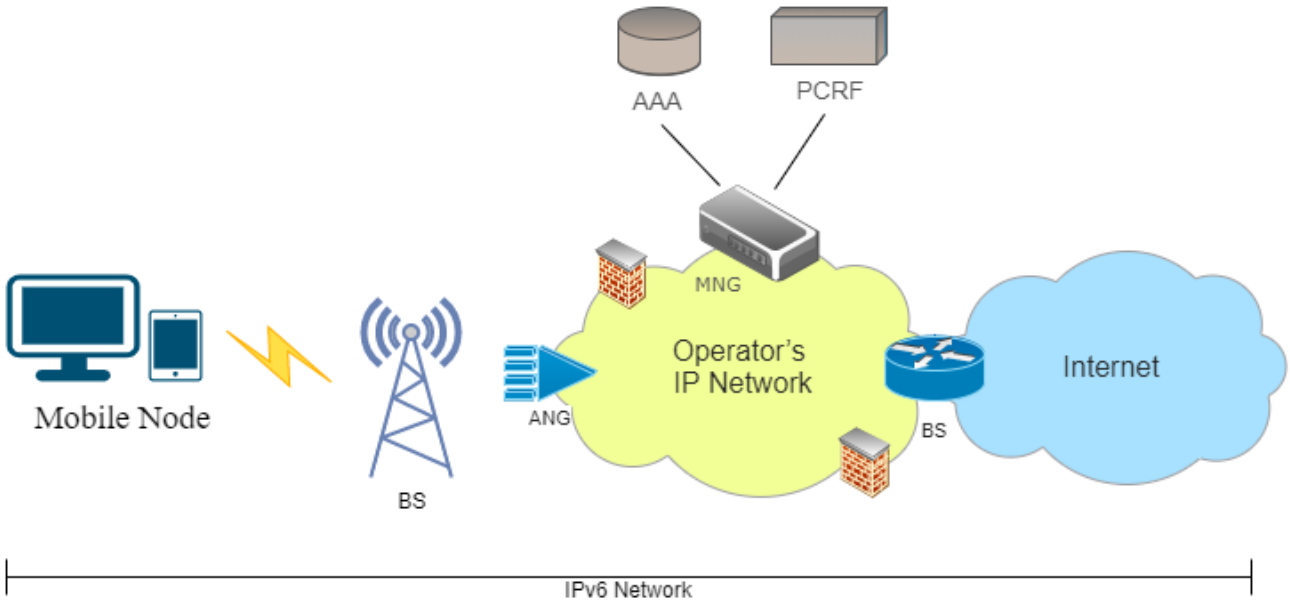

圖 14 行動網路架構

當用戶漫游到本地網路時，行動節點(MN, Mobile Node)可透過本地網路或存取網路連接到行動網路。在 3GPP(Third Generation Partnership Project)網路結構中，MN 透過連接到行動閘道器存取點(APN, Access Point Name)存取網路。APN 類似於無線區域網的服務集標識符(SSID)，可用於指定 MN 的服務類型，例如網際網路存取、高清晰度視訊、內容豐富的遊戲...等。每個可在該特定 APN 上啟用不同 IP 連接類型(即 IPv4、IPv6、IPv4v6)。

當 APN 將 MN 導向閘道器時，MN 需要到閘道器的端到端"連接"。長期演進技術(LTE)網路中，此連接透過演進分封系統(EPS, Evolved Packet System)實現。3G 普遍行動電信系統(UMTS, Universal Mobile Telecommunications System)網路中，這種連接透過封包協定(PDP, Packet Data Protocol)前後關係實現。終端到終端(end-to-end)連接透過以下定義多個節點：

- 基地台(BS, Base Station)：無線電基地台提供到 MN 無線連接。
- 存取網路閘道器(ANG, Access Network Gateway)：ANG 向 MN 轉發 IP 封包。不是 MN 預設路由器，並且 ANG 不會為行動節點執行 IP 位址分配

和管理，位於本地網路或拜訪網路中。

- 行動網路閘道器(MNG, Mobile Network Gateway)：MNG 是 MN 預設路由器，提供 IP 位址管理。MNG 提供服務品質(QoS, Quality of Service)，應用於用戶策略以及啟用計費和帳單等功能；這些功能統稱為“用戶管理”操作。如圖 14 所示，行動網路結構定義所需協定介面以管理用戶操作，通常位於本地網路。
- 邊界路由器(BR, Border Router)：顧名思義，BR 與行動網路的網際網路交界。BR 不為行動網路執行用戶管理。
- 身份驗證，授權和計費(AAA,Authentication, Authorization, and Accounting)：AAA 一般功能用於用戶身份驗證、授權以及生成帳單和計費訊息。3GPP 網路環境中，使用“歸屬位置暫存器”(HLR, Home Location Register)/“歸屬用戶伺服器”(HSS, Home Subscriber Server)功能提供用戶身份驗證以及對連接和服務的後續授權。
- 策略和計費規則功能(PCRF, Policy and Charging Rule Function)：PCRF 允許在 MNG 上應用策略和計費規則。

(二) 使用 IPv6 的考量

1. IPv4 地址耗盡

人們普遍認為，公共 IPv4 地址空間即將耗盡。該 IANA 已經耗盡了可用的 '/8' 區塊分配給區域網際網路註冊管理機構(RIR)，預計在不久的將來會耗盡。這導致了服務提供者必須了解與考慮引進新技術，以維持網際網路運行。對於網路服務提供者，有兩種方法同時解決用盡的問題：

- 延遲 IPv4 地址耗盡(即保護現有可用位址)
- 在運行的網路引入 IPv6

延遲公共 IPv4 地址耗盡的網路服務提供者包括為終端用戶分配私有

IPv4 地址或使用介面範圍延伸 IPv4 地址，這需要隧道和額外的訊號。如網路地址轉換(NAT, Network Address Translator)是在網路服務提供者處所使用(而不是客戶端)的機制來管理私有 IP 地址分配和存取網際網路。在下文中，我們主要集中在基於平移的機制，如 NAT44(即公共 IPv4、私有 IPv4)和 NAT64(即公共 IPv6 到公共 IPv4)。我們這樣做是因為 3GPP 架構已經確定了與通用分組無線業務(GPRS)隧道協議(GTP)的隧道基礎設施，和架構允許雙協定和支援配置 IPv6。

不斷增長的需求，行動網路尋址以支援私有 IPv4 中由於公共 IPv4 地址用盡的問題。相應地，存在對私人-公共 IPv4 的轉換在行動網路有更大的需求。其次在 3G 和 4G LTE 網路已在 PDP 內容和 PDN 連接的形式，對 IPv6 的支援。首先行動網路營運商可以為自己的應用程序和服務引入 IPv6。換一種說法，IETF 的推薦雙協定 IPv6 和 IPv4 網路的模型是容易適用於與不同的 APN 的支援和承載 IPv6 流量的能力，於 PDP/PDN 連接行動網路。IETF 的雙協定模型可以使用 Release-8 及以後被應用的單一 IPv4v6 PDN 連接，但需要在早期版本中單獨的 PDP 內容。最後，行動網路營運商可以使 IPv6 的預設使用，無論是 IPv4v6 PDN 或 IPv6 的 PDN 和使用 IPv4 PDN 的行動連接是必要的。

2. NAT 在行動網路中的位置

NAT44 功能需要，以節省可用的位址空間和延緩公共 IPv4 地址耗盡。然而現有大型網路的私有 IPv4 空間本身就不充裕，如行動網路。

在他們的行動網路配置 IP 地址空間的分配有所不同。一些網路配置中使用，其中“空間“是由一個共同的節點管理的“集中模式”，如 PDN 的 BR，並且由多個 MNG 共享空間中的所有連接到相同的 BR。這種模式在前期 3G 配置中，用戶存取行動網際網路在任何特定時間的數量不超過可用的地址空間已服務不周到。然而，隨著 3G 網路的出現和用戶數量的急劇後續增長

的行動網際網路上，服務網路服務提供者正越來越多地被迫考慮他們現有的網路設計和選擇。具體來說網路服務提供者不得不解決私有 IPv4 空間耗盡以及可擴展的解決方案。

為了解決私有 IPv4 耗盡的集中模式，將有必要支援在公共 NAT 功能，以及在每個閘道器的重疊私有 IPv4 地址。換言之，使用由兩個或更多的 MN(其可以被連接到相同的 MNG)很可能重疊在集中 NAT 的 IP 地址，這需要能夠區分流量。

考慮到增加的行動網際網路用戶可用的私有 IPv4 空間的管理已經成為非常重要的。使重用的可以使用空間的機制是必需的。其次在私有 IPv4 空間管理的背景下，NAT 功能的放置具有網路配置和業務的影響。與常見的 NAT 集中的模型有繼續其傳統的配置和私有 IPv4 地址的重複使用的優點。然而他們需要額外的功能，使交通分化，並與用戶 NAT，狀態相關在 MNG 狀態管理。分佈式模型也實現私有 IPv4 地址重複使用，避免行動網路營運商的核心重疊私有 IPv4 流量，但沒有需要額外的機制。由於 MNG 執行的 IPv4 地址分配並具有標準介面為 AAA 和 PCRF，分佈式模型還能夠為用戶和 NAT 狀態報告，以及策略應用的單點。總之，網路服務提供者有意容易整合 NAT 與其他用戶管理功能，以及保護和重複使用他們的私有 IPv4 空間，可以發現分佈式模型引人注目。在另一方面，那些熱衷於 NAT 的共同管理網路服務提供者可能會發現集中式模型更加引人注目。

3. IPv6-Only 部署注意事項

網路 NAT 功能提出多個原本不存在問題。在 IPv6 廣泛使用前，應將 NAT 視為臨時解決方案。網路服務提供者的 NAT 減緩公共 IPv4 位址耗盡，為保持“不斷發展”，必須迅速且同時引入 IPv6，重要的是理解部署純 IPv6 注意事項。

IPv6-Only 部署具有三個維度：網路本身、行動節點和應用程序，以{nw，

mn，ap}表示。目標是從{IPv4，IPv4，IPv4}達到{IPv6，IPv6，IPv6}。經典雙協定模型將遍歷坐標{IPv4v6，IPv4v6，IPv4v6}，每個維度都支援 IPv4 和 IPv6 共存。儘管面臨支援大規模 NAT 隱患，以及現有 3G UMTS 網路支援單獨 PDP 前後關係也存在代價。

另一個關心中間坐標是{IPv6，IPv6，IPv4}，網路和 MN 僅是 IPv6，並且網際網路應用程序主要被識別為 IPv4。最諷刺的是，為了取消 NAT(針對 IPv4-IPv4)，需引入另一種形式 NAT(即 IPv6-IPv4)以加快 IPv6 採用。

行動網路中 IPv6-Only 部署需要考慮以下注意事項。首先網路和 MN 都必須具有 IPv6 能力。加速網路升級以及使用 IPv6 MN 推出將極大地便利。用於 LTE 的 3GPP 網路設計已經要求網路行動節點支援 IPv6。即使不要求傳輸網路為 IPv6，也可以在僅 IPv4 中使用適當的現有隧道來部署可操作的 IPv6 連接。網路服務提供者可選擇在家庭網路中為用戶強制實施 IPv6-Only 的 PDN 和位址分配(請參見圖 14)。當行動網路能為網際網路存取提供 IPv6-Only 的 PDN 支援和 IPv6-IPv4 交互工作時，對於較新 MN 是可行的。但對於現有 MN，網路服務提供者仍然需要能夠支援僅 IPv4 的 PDP / PDN 連接。

使用 IPv6-Only PDN 連接將應用程序遷移到 MN 中 IPv6 帶來挑戰。提供者提供的應用程序和服務需具有 IPv6 功能。但 MN 可託管其他應用程序，在 IPv6-Only 的部署中，也需要具有 IPv6 功能。這可能是“長尾”現象；但當一些傑出應用程序開始提供 IPv6 時，會強烈地鼓勵提供應用程序層(例如網路插座介面 socket interface)升級到 IPv6。

LTE 語音(VoLTE)也帶來獨特挑戰。通常期望語音發訊號是免費的，本身是持續時間收費。發訊號和有效負載間分離是語音所獨有，無需特別考慮應用程序發訊號和有效負載流量即可解決連接問題。網際網路使用取決於用戶喜好和漫遊協定(網路服務提供者可控制網路設計，但不能控制漫遊

所依賴的對等網，也希望用戶體驗均一)。

僅對 IPv6 部署關心網路服務提供者施加強約束，使(出站)用戶漫遊到不提供 IPv6 時也支援 IPv4 尋址。有跡象表明 3GPP 結構中已部署網路節點提供了對 IPv6 PDP 前後關係支援。有必要擴大對(非常)大量行動用戶的支援，並無所不在服務。

應該鼓勵 IPv6-Only 部署及雙協定模型，推薦 IETF 方法。網路服務提供者服務和應用程序而言，是相對簡單的，透過適當 APN 和相應的 IPv6-Only PDP 或 EPS 承載提供。一些網路服務提供者會考慮 IPv6-Only 部署來進行存取，將需要 IPv6-IPv4 互通。在 IPv6-Only 部署中使用 IPv6-IPv4 轉換機制時，將適用[RFC6146]和[RFC6145]中指定的協定和相關注意事項。最終可將此類 IPv6-Only 的部署逐步引入到新的行動節點中，而現有的行動節點繼續要求僅 IPv4 的連接性。

透過主動地僅為較新的 MN 引入 IPv6，可大大減少對專用 IPv4 位址需求。

表 34 RFC6146、RFC6145 參考文獻

編號	RFC 編號	RFC 相關訊息	
		類別	時間
1	6146	Proposed Standard	2011/04
		標題：Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers	
2	6145	Proposed Standard	2011/04
		標題： IP/ICMP Translation Algorithm	

4. 固定與行動網路融合

許多網路服務提供者同時擁有固定寬頻和行動網路。存取網通常完全不同，具共同特徵，但有足夠差異，難以實現“聚集”。例如固定存取網路中不考慮漫遊。需全 IP 行動網路服務網路服務提供者提供語音服務，而固定網路網路服務提供者則不需要。

固定網路中“連接”通常能夠承載 IPv6 和 IPv4 流量，而並非所有行動網路都具有能夠支援 IPv6 和 IPv4 的“連接”(即 PDP / PDN 連接)。

在同網路服務提供者範圍內，需考慮些共同注意事項，例如 IPv4 位址管理是兩個存取網共同關心的問題。相同機制(延遲 IPv4 位址耗盡並將 IPv6 引入運行網路)也適用。由於各種原因，每個存取網路部署確切解決方案會有所不同，例如：

端點通常是電纜或 DSL 數據機固定網路中，IPv6 內對專用 IPv4 封包進行隧道傳輸是可行。端點本身是 MN 行動網路中，情況並非如此。

當網路服務提供者無法提供本機或直接 IPv6 連接且住戶閘道器可提供此服務隧道端點時，基於封裝機制(例如 6rd [RFC5969])非常有用。行動網路中，網路服務提供者可使用現有的行動網路隧道機制提供 IPv6 連接，而無需引入額外隧道層。

表 35 RFC5969 參考文獻

編號	RFC 編號	RFC 相關訊息	
		類別	時間
1	5969	Proposed Standard	2010/08
		標題：IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) -- Protocol Specification	

行動網路網路服務提供者可在網路中，具要求專用 IPv4 位址以進行 MN 識別的應用伺服器(例如電子郵件伺服器)，而固定網路網路服務提供者沒有此類要求或服務。

說明存取網使用實際解決方案取決於該特定要求。在存取網路和核心網路間有些共享。例如固定網路不需 NAT 用戶感知功能時，可在核心路由器提供該功能，而行動存取網繼續在行動閘道器提供 NAT 功能。

如果網路服務提供者選擇在 MNG 上為固定和無線網路提供通用用戶管理，則 MNG 本身將成為一個聚合節點，需同時支援固定和無線存取網

路適用過渡機制。

網路服務提供者的不更可能共享一個公共核心網路。因此通用解決方案更容易地應用於核心網路。例如，行動和固定網路閘道器的已配置隧道或 MPLS VPN 可將流量傳送到核心路由器，直到整個核心網路都啟用了 IPv6。

由於在存取網路使用 NAT，也可能需要考慮一些因素。如 Femto 網路的解決方案依賴於 Femto 基地台，可透過 IPsec 隧道與 Fpeto 基地台對等進行通訊的固定網際網路連接。

當 Femto 基地台需使用專用 IPv4 位址時，透過 Femto 基地台進行行動網路存取將受到 NAT 策略管理約束，包括定期清除和清除 NAT 狀態。策略稍微影響網路可用性，並會對行動網路網路服務提供者產生影響。如果 IPv6 通訊可以繞過 NAT，則將 Femto(或任何其他存取技術)使用 IPv6 可緩解一些擔憂。

至少在某些網路服務提供者中，人們關心固定行動聚集。在較高的服務層上，例如，為服務和應用程序提供統一的用戶體驗，也許更大的協調是可行的。跨存取網到核心網某些功能協調可能是可行的。網路服務提供者的核心網路似乎是最可行的聚合目的。

(三) IPv6 網路安全防護建議

在 3GPP 接入網路時，UE(User Equipment)和網路在網路連接[TS.33102][TS.33401]期間始終執行相互身份驗證。此外，每次創建 PDP 內容/ PDN 連接時，都可以針對 PCC(Policy and Charging Control)基礎結構[TS.23203]授權新連接，對現有連接的修改以及對 IPv6 Prefix 或 IP 地址的分配，和/或 PDN 的 AAA 服務器。

根據區域法規和行動網路營運商的部署策略，可以保護 UE 與(e)NodeB 之間 3GPP 連結的無線部分，以及 UE 與 MME / SGSN 之間的控制信令訊息，使用者流量可以受到機密性保護。控制平面始終至少受到完整性(integrity)和重放(replay)

保護，並且還可能受到機密性保護。網路傳輸部分內的保護取決於行動網路營運商的部署策略[TS.33401]。

由於 3GPP 點對點連結模型的性質以及 UE 和第一下一節點路由器(PDN-GW / GGSN 或 SGW)，UE 是連接上的唯一節點，因此可以緩解一些與連結發現和鄰居發現相關的攻擊。對於離線 IPv6 攻擊，3GPP EPS 與任何 IPv6 系統一樣容易受到攻擊。

此外，還存在 UE IP 堆疊可能使用永久訂戶身份的擔憂，如國際行動用戶身份(IMSI, International Mobile Subscriber Identity)，以 IPv6 地址識別作為永久用戶身份的來源。但這將是隱私威脅，並將允許追蹤用戶。因此，禁止將 IMSI(或[TS.23003]定義的任何身份)用作識別的來源[TS.23401]，但是沒有標準化方法去阻止，如異常行為的 UE。

(四) 小結論

IPv6 安全防護建議

- 應注意行動電話用戶使用 IPv6 地址識別用戶身份之隱私問題。
- ISP 應保護其用戶免受來自自己用戶與其網路外部的攻擊。
- ISP 在 BR 應保護其處理資源，以防止有效的客戶控制流量氾濫。

三. 公眾無線網路連線服務安全防護建議

本節提供了在當前部署的無線區域網(WLAN)基礎設施 IPv6 部署和整合方法說明，以及目前無線區域網路(WLAN)配置基礎結構的 IPv6 配置、合併方式，WLAN 使用戶可以從各個位置連接到網路，而不需待在室內。

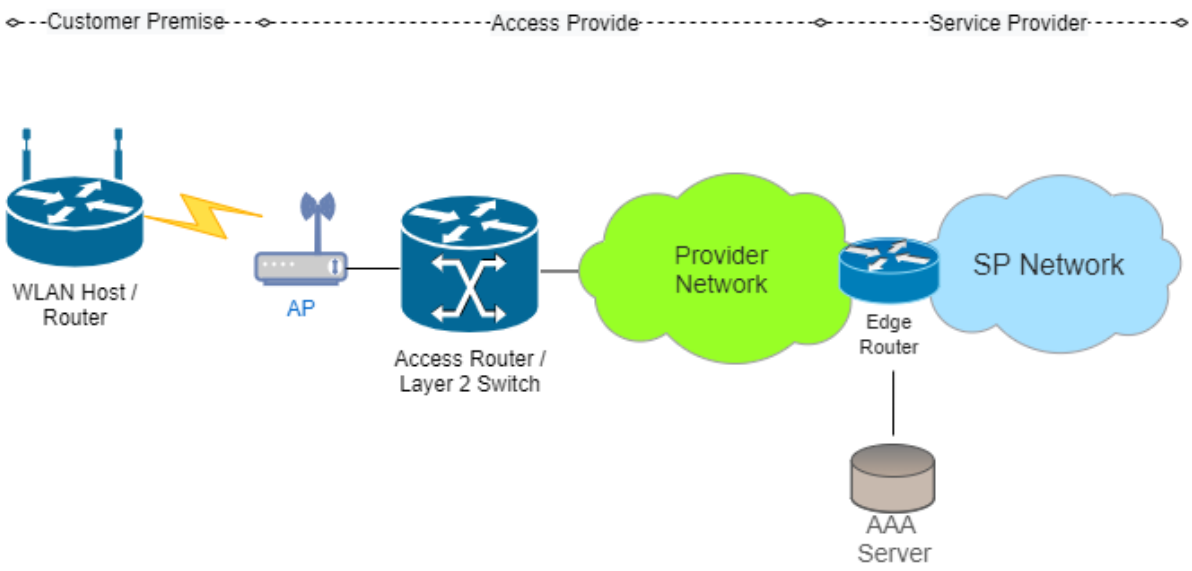

圖 15 WLAN 的關鍵元件

如圖 15 為 WLAN 的關鍵元件，主機應具無線網路介面卡(NIC, Network Interface Controller)，才能連接到無線區域網路(WLAN 為廣播網路，工作方式與乙太網路類似)。

主機開始連接時，將由 SP(Service Provider)網路的 AAA(Authentication, Authorization, and Accounting)伺服器進行身份驗證，存取點(AP, Access Point)將所有驗證參數(用戶名、密碼等)轉發到 AAA 伺服器。

AAA 伺服器對主機進行驗證，透過驗證即發送封包。AP 位於主機附近並作為橋接器，將所有來置主機的封包發送到邊緣路由器。AP 和邊緣路由器之間的底層連接可以基於任何存取層的技術，如 HFC /電纜、FTTH、xDSL 的等。

WLAN 在 WiFi 熱點有限區域內運作，當用戶位於 WLAN 覆蓋區域中，只要具有 NIC 並在設備(筆記型電腦、PC、PDA 等)中具相關設置，即可連接到網路。

用戶開始連接後，SP 將使用 DHCPv4 分配 IP 位址。多數情況下，SP 會為其客戶分配有限的公共 IP 位址。當用戶斷開連接並移動到新的 WiFi 熱點時，將重複上述驗證、位址分配和存取網路過程。

(一) 無線網路配置情境

1. 第 2 層網路存取提供者於網路服務提供者邊緣路由器進行第三層終結 (Layer 2 NAP with Layer 3 termination at NSP Edge Router)

AP 和邊緣路由器間存在第 2 層交換機時，AP 和第 2 層交換機繼續作為橋接器，將 WLAN 主機或路由器的 IPv4 和 IPv6 封包發送到邊緣路由器。

開始連接時，WLAN 主機由 SP 網路的 AAA 伺服器進行驗證。AP 將所有驗證相關參數(用戶名、密碼等)轉發到 AAA 伺服器。AAA 伺服器對 WLAN 主機進行驗證，驗證成功與 WLAN AP 相關，即獲取 IPv6 位址。此處，開始和認證過程與 IPv4 中使用的過程相同。

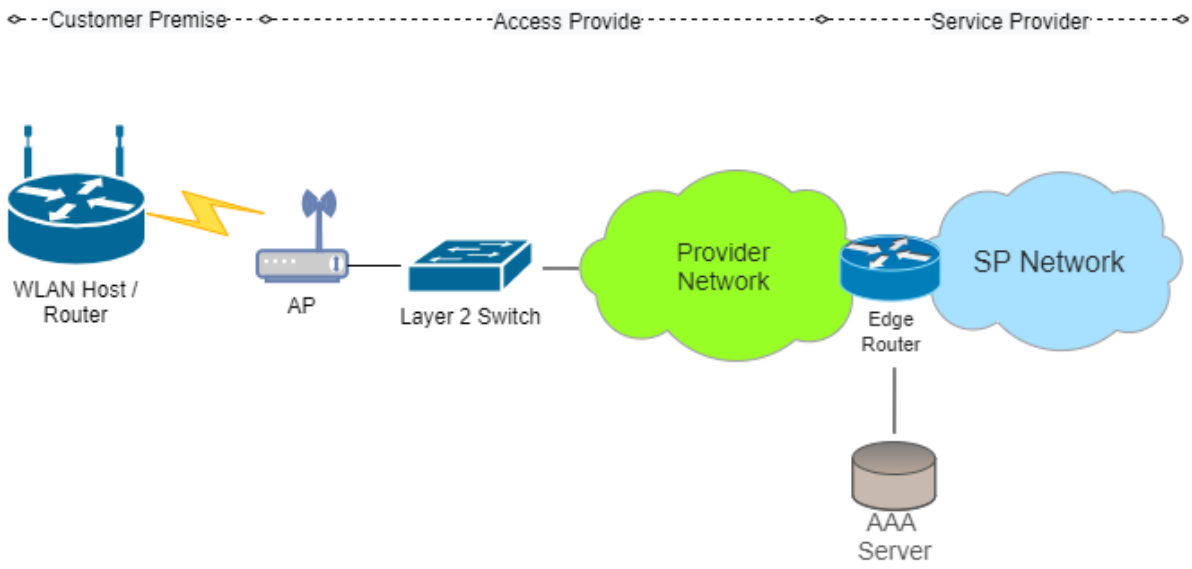

圖 16 當第 2 層交換機位於 AP 和邊緣路由器間的 WLAN 結構

(1) 更改 IPv6 相關基礎架構

透過將以下設備升級到雙協定，配置 IPv6：WLAN 主機，WLAN 路由器(如果有)和邊緣路由器。

(2) 定址

客戶 WLAN 路由器不存在時，WLAN 主機有兩個選項，可透過邊緣路由器獲取 IPv6 位址。

a. LAN 主機使用無狀態自動配置[RFC2462]從邊緣路由器獲取 IPv6

位址。WLAN 上所有主機都屬於邊緣路由器上靜態配置的同一/64 子網。IPv6 WLAN 主機可用**無狀態 DHCPv6** 來獲取相關訊息，例如 DNS 等。

b. IPv6 WLAN 主機可使用 DHCPv6 [RFC3315]，從伺服器獲取 IPv6 位址。DHCPv6 伺服器將位於 SP 核心網路中，而邊緣路由器僅作為 DHCP 中繼代理。此選項類似於 DHCPv4 下執行操作。重要的是自動配置的主機相當有限，選擇此位址分配選項，則應考慮這一點。

表 36 RFC2462、RFC3315 參考文獻

編號	RFC 編號	RFC 相關訊息	
		類別	時間
1	2462	Draft Standard	2013/12
		標題：IPv6 Stateless Address Autoconfiguration	
2	3315	Proposed Standard	2003/07
		標題：Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	

當客戶 WLAN 路由器存在時，WLAN 主機有兩個選項獲取 IPv6 位址。

a. 根據 SP 政策和客戶要求，可以在/48 和/64 [RFC3177]間為 WLAN 路由器分配位址前綴。如果 WLAN 路由器介面連接多個網路，則網路管理員將必須為連接客戶站點上 WLAN 主機的路由器介面配置/64 位址前綴。連接到這些介面的 WLAN 主機可用無狀態自動配置進行自身配置。

b. WLAN 路由器可以使用本地連接位址與 ER 通訊。還可透過無狀態自動配置動態獲取自身與 ER 間連接位址。此步驟後是透過 DHCP-PD(Prefix Delegation)請求小於/ 64 的位址前綴，並分配給其連接客戶站點上主機介面。

表 37 RFC3177 參考文獻

編號	RFC 編號	RFC 相關訊息	
		類別	時間
1	3177	Informational	2001/09
		標題：IAB/IESG Recommendations on IPv6 Address Allocations to Sites	

在此選項中，WLAN 路由器將作為請求路由器，而邊緣路由器將作為委派路由器。WLAN 路由器接收到位址前綴後，便連接客戶站點上 WLAN 主機的每個介面分配/64 位址前綴。連接到這些介面的 WLAN 主機可以使用無狀態自動配置自動進行自身配置。上行到 ISP 網路的也配置有/64 位址前綴。

SP 可更輕鬆地使用 DHCP-PD 和無狀態自動配置模型，並將客戶端指向伺服器中心以獲取 DNS /域訊息、代理配置等。使用此模型，SP 可以隨時更改位址前綴，並且 WLAN 路由器將僅基於有效/首選生命週期提取最新的位址前綴。

用戶連接的位址前綴和透過 DHCP-PD 委派的位址前綴，應允許在邊緣路由器上進行最大整理的方式進行規劃。

主機關心其他訊息(例如 DNS)，透過有狀態[RFC3315]和無狀態[RFC3736] DHCPv6 提供。

WLAN 主機或路由器配置有指向邊緣路由器的預設路由。這些設備通常不需要資源，因此不需要路由協定。

邊緣路由器運行 SP 網路中使用的 IGP，例如 OSPFv3 或用於 IPv6 的 IS-IS。連接的位址前綴必須重新分配。位址前綴概要應在邊緣路由器上進行。使用 DHCP-PD 時，IGP 必須重新分配在位址前綴委派過程中安裝的靜態路由。

2. 第三層已知網路存取提供者於存取路由器進行第三層終結(Layer 3 Aware NAP with Layer 3 Termination at Access Router)

當 AP 與邊緣路由器間存在存取路由器時，AP 繼續作為橋接器，將 IPv4 和 IPv6 封包從 WLAN 主機或路由器橋接到存取路由器。存取路由器是 SP 網路的一部分，也可以由單獨的存取網路服務提供者所擁有。

當 WLAN 主機開始連接時，與 WLAN AP 的 AAA 驗證和相關過程將類似，如第 2 層 NAP 和第 3 層在 NSP 邊緣路由器終止所述。

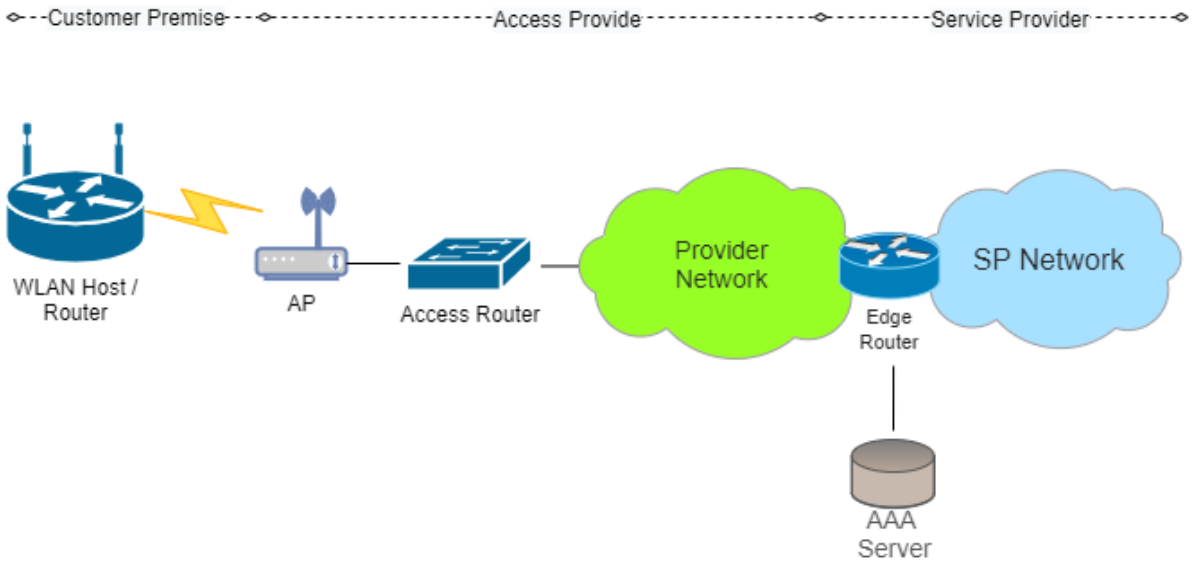

圖 17 存取路由器位於 AP 與邊緣路由器之間時的 WLAN 結構

(1) 更改 IPv6 相關基礎架構

在這種情況下，透過將以下設備升級到雙協定來配置 IPv6：WLAN 主機，WLAN 路由器(如果有)，存取路由器和邊緣路由器。

(2) 定址

在這種情況下，可以使用三個選項來分配 IPv6 位址：

a. 向存取路由器的邊緣路由器介面靜態配置為/ 64 位址前綴。存取路由器透過無狀態自動配置在邊緣路由器的介面上接收/配置/ 64 位址前綴。網路管理員必須配置/ 64 位址前綴，存取路由器界面對用戶端的問題。連接到該介面的 WLAN 主機或路由器可以使

用無狀態自動配置自動進行自身配置。

b. 此選項使用 DHCPv6 [RFC3315]為 WLAN 主機或路由器分配 IPv6 位址前綴。此選項中不使用 DHCP PD 或無狀態自動配置。DHCPv6 伺服器可以位於存取路由器，邊緣路由器或 SP 網路中的某個位置。在這種情況下，根據 DHCPv6 伺服器的位置，存取路由器或邊緣路由器將中繼的 DHCPv6 請求。

表 38 RFC3315 參考文獻

編號	RFC 編號	RFC 相關訊息	
		類別	時間
1	3315	Proposed Standard	2003/07
		標題：Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	

c. 它可以使用其本地連接位址與 ER 通訊。它還可以透過無狀態自動配置動態獲取自身與 ER 之間的連接位址。此步驟之後是透過 DHCP-PD 請求的位址前綴小於/64 的位址前綴，並分配給其連接客戶站點上主機的介面。

存取路由器將作為請求路由器，而邊緣路由器將作為委派路由器。存取路由器接收到位址前綴後，便會為其連接客戶站點上 WLAN 主機或路由器的每個介面分配/64 位址前綴。連接到這些介面的 WLAN 主機或路由器可以使用無狀態自動配置進行自身配置。到 ISP 網路的向上傳訊也配置有/64 位址前綴。

SP 可以更輕鬆地使用 DHCP PD 和無狀態自動配置模型，並將客戶端指向伺服器中央以獲取 DNS /域訊息、代理配置等。使用此模型，提供程序可以隨時更改位址前綴，而存取路由器則可以根據有效/首選生命週期簡單地提取最新的位址前綴。

如前所述，用於用戶連接的位址前綴和透過 DHCP-PD 委派的位

址前綴應該以允許在邊緣路由器進行最大整理的方式進行規劃。主機關心的其他訊息(例如 DNS)透過有狀態[RFC3315]和無狀態[RFC3736] DHCPv6 提供。

(3) 路由

WLAN 主機或路由器配置有指向存取路由器的預設路由。這些設備通常不需要資源，因此不需要路由協定。

如果存取路由器由存取提供者所有，則存取路由器可以具有指向 SP 邊緣路由器的預設路由。邊緣路由器運行 SP 網路中使用的 IGP，例如 OSPFv3 或用於 IPv6 的 IS-IS。連接的位址前綴必須重新分配。如果使用 DHCP-PD，則邊緣路由器會為每個委派的位址前綴安裝一條靜態路由。因此，必須重新分配靜態路由。位址前綴概要應在邊緣路由器上進行。

如果存取路由器由 SP 擁有，則存取路由器還將運行 IPv6 IGP，並將成為 SP IPv6 路由域(OSPFv3 或 IS-IS)的一部分。連接的位址前綴必須重新分配。如果使用 DHCP-PD，則存取路由器會為每個委派的位址前綴安裝一條靜態路由。因此，必須重新分配靜態路由。位址前綴概要應在存取路由器上進行。

3. PPP-Based 模型

PPP 終止聚合(PTA)和 L2TPv2 存取聚合(LAA)模型也可以配置在 IPv6 WLAN 環境中。

(1) IPv6 WLAN 環境中的 PTA 模型

配置 PTA 模型時，存取路由器具有第 3 層感知能力，必須對其進行升級以支援 IPv6。由於存取路由器會終止由 WLAN 主機或路由器發起的 PPP 會話，因此它必須支援 IPv6 的 PPPoE。

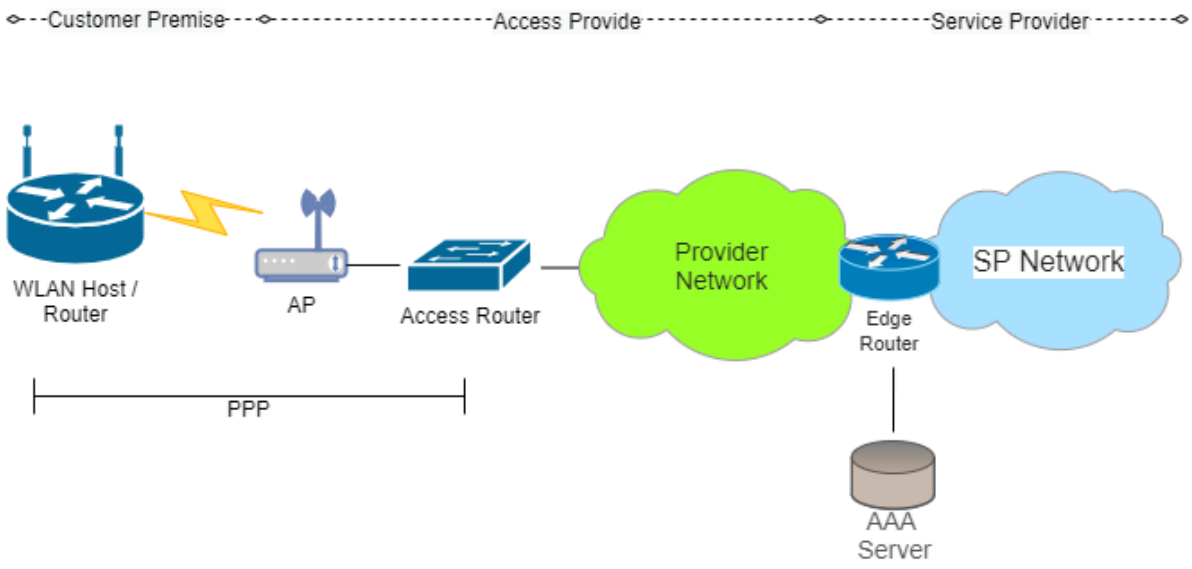

圖 18 IPv6 WLAN 環境中的 PTA 模型

a. 更改 IPv6 相關基礎架構

在這種情況下，透過將以下設備升級到雙協定來配置 IPv6：WLAN 主機、WLAN 路由器(如果有)，存取路由器和邊緣路由器。

b. 定址

DSL 寬頻網路章節描述的尋址技術也適用於 IPv6 WLAN PTA 場景。

c. 路由

DSL 寬頻網路章節中描述的路由技術也適用於 IPv6 WLAN PTA 場景。

(2) IPv6 WLAN 環境中的 LAA 模型

配置 LAA 模型時，存取路由器具有第 3 層感知能力，必須進行升級以支援 IPv6。由 WLAN 主機或路由器發起的 PPP 會話透過 L2TPv2 隧道轉發到 SP 網路中的聚合點。存取路由器必須具有為 IPv6 支援 L2TPv2 的能力。

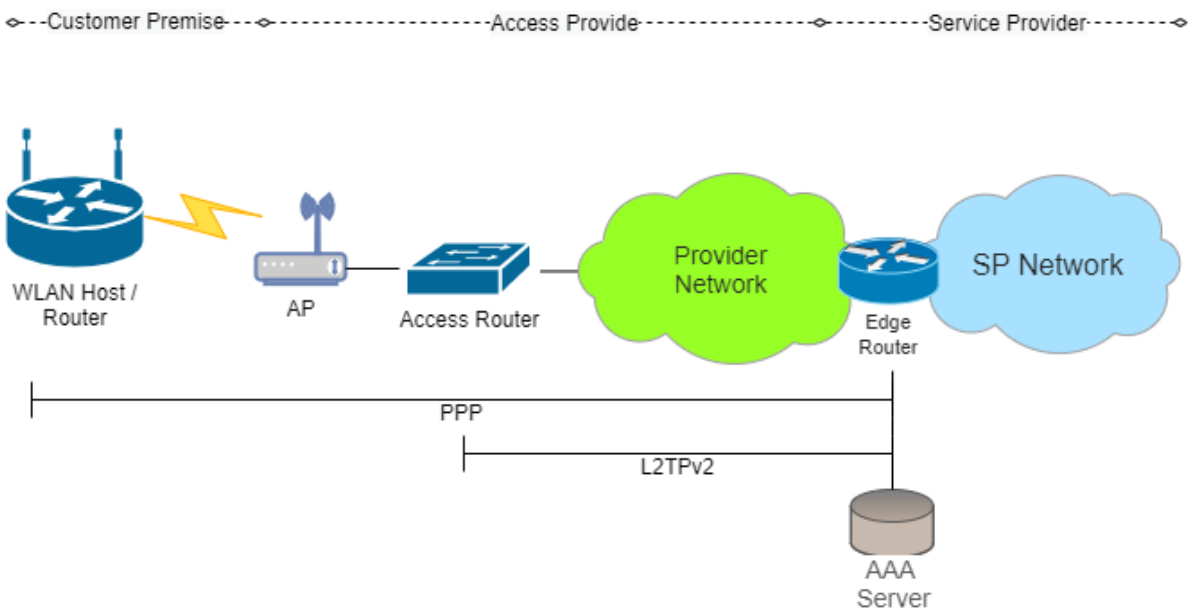

圖 19 IPv6 WLAN 環境中的 LAA 模型

a. 更改 IPv6 相關基礎架構

在這種情況下，透過將以下設備升級到雙協定來配置 IPv6：WLAN 主機、WLAN 路由器(如果有)，存取路由器和邊緣路由器。

b. 定址

DSL 寬頻網路章節中描述的尋址技術也適用於 IPv6 WLAN LAA 場景。

c. 路由

DSL 寬頻網路章節中描述的路由技術也適用於 IPv6 WLAN LAA 場景。

(二) IPv6 QoS

現在 QoS 是在 WiFi 區域以外進行，但它的整體配置還是非常重要的。QoS 的配置在邊緣路由器特別的關聯，以便管理在多個用戶與各種服務級別協議(SLA)的共享可能的資源。然而，WLAN 主機或路由器和 Access 路由器也可構成對 QoS。這包括適當的分類標準支援，將需要為 IPv6 單點傳播和多點傳播業務中實現。

在邊緣路由器上，必須將面對用戶的介面配置為管理入站客戶流量，並根據 SLA 調整向客戶出站的流量。還應該在邊緣路由器上進行流量分類和標記，以支援各種類型的客戶流量：數據、語音、影片。相同的 IPv4 QoS 概念和方法也應適用於 IPv6。

重要的是要注意，當通訊進行端到端加密時，網路設備將無法存取用於分類目的的許多數據包字段。在這些情況下，路由器很可能會將數據包放入默認的分類中。QoS 設計應考慮這種情況，並嘗試使用主要 IP 表頭欄位進行分類。

(三) IPv6 安全防護建議

為了增強安全性，必須對 WLAN 主機或路由器進行有限的更改。主機應該使用自動配置的隱私擴充，並在 WLAN 主機或路由器上啟用 IPv6 防火牆功能。

ISP 提供了針對來自自己的用戶的攻擊安全性，實施安全服務，以保護其用戶免受外部網路的攻擊。此類服務不適用於此處討論的網路訪問級別。

如果使用基於 Web 的身份驗證系統完成熱點處的主機身份驗證，則安全級別將取決於特定的實現。用戶憑證絕不能透過 HTTP 以明文形式發送。Web 瀏覽器和身份驗證服務器之間應使用安全 HTTP(HTTPS)。身份驗證服務器可以在後端使用 RADIUS 和 LDAP 服務。

身份驗證是在實施第 3 層安全策略之前確保 WLAN 網路安全的重要方面。這將有助於避免對 ND 或無狀態自動配置過程的威脅。802.1x [IEEE8021X]提供了確保網路訪問安全的方法。但是，多種類型的 EAP(PEAP、EAP-TLS、EAPTTLS、EAP-FAST 和 LEAP)以及主機支援某些功能的能力可能使實施全面一致的策略變得困難。

802.11i [IEEE80211i]修訂版包含許多組件，其中最明顯的是兩個新的數據保密協議，即臨時密鑰完整性協議(TKIP)和計數器模式/ CBC-MAC 協議(CCMP)。802.11i 還使用 802.1X 的密鑰分發系統來控制對網路的訪問。由於 802.11 處理單點傳播和廣播流量的方式不同，因此每種流量類型都有不同的安全問題。透過幾

種數據保密協議和密鑰分發，802.11i 包括一個協商過程，用於為每種流量類型選擇正確的保密協議和密鑰系統。引入的其他功能包括密鑰緩存和預身份驗證。

802.11i 修正案是無線安全性的一大進步。該修正案增加了更強大的加密，身份驗證和密鑰管理策略，可以使無線數據和系統更安全。

如果有用於乙太網類型的任何第二層過濾器，則 NAP 必須允許 IPv6 乙太網類型(0X86DD)。

作為用戶(存取邊緣路由器)的第 3 層下一節點(next hop)的設備應保護網路和其他用戶免受提供者客戶之一的攻擊。因此，應在面對用戶的所有介面上使用 uRPF(Unicast Reverse Path Forwarding)和 ACL(Access Control Lists)。應當根據 IPv6 的操作要求進行過濾[IPv6-Security]。

存取邊緣路由器應保護其處理資源，以防止有效的客戶控制流量的氾濫(例如 RS，NS 和 MLD 請求)。速率限制應在所有面對用戶的接口上實施。重點應放在 IPv6 控制平面最常使用的多點傳播類型流量上。

(四) 小結論

IPv6 安全防護建議

- 身份驗證是在實施第 3 層安全策略之前確保 WLAN 網路安全的重要工作。
- Web 瀏覽器和身份驗證服務器之間應使用安全 HTTP(HTTPS)。
- 主機應使用自動配置的隱私延伸。
- 應在主機或用戶端網路存取設備上啟用 IPv6 防火牆功能。
- ISP 應保護其用戶免受來自自己用戶與其網路外部的攻擊。
- ISP 在 Service Provider Network 應保護其處理資源，以防止有效的客戶控制流量氾濫。

第三章 結論

本計畫已完成 ISP 網際網路存取服務與 ISP IPv6 網路連線服務安全防護建議，並且針對 ISP 網際網路存取服務之固接網路、行動網路與公眾無線網路連線服務安全防護提供建議。

網際網路服務提供者(ISP，Internet Service Provider)為關鍵基礎設施提供者，根據「資通安全管理法」，關鍵基礎設施提供者應符合其所屬資通安全責任等級之要求；且根據電信管理法第 15 條第 2 項第 5 款其他主管機關指定有助於資通安全之管理措施，以及第 38 條第 3 項第 8 款之經主管機關指定與網路設置相關項目，建議 ISP 網際網路存取服務與 ISP IPv6 網路連線服務安全防護建議可納入資通安全之特定非公務機關應辦事項，以強化資通安全防護，彙整資料如表 39。

相信本報告對 ISP 導入 IPv6 連線服務，提供 IPv6 網路安全防護建議，可以讓 ISP 了解到 IPv6 網路安全防護之重要性，以及 IPv6 網路安全防護之注意項目。

表 39 特定非公務機關應辦事項與 ISP IPv6 網路安全防護建議對應表

辦理項目	辦理項目細項	ISP IPv6 網路安全防護建議
資通安全防護	網路防火牆	1. 有關 IPv6 延伸標頭的順序和重複，應該使用防火牆或邊緣設備來強制執行延伸標頭的建議順序和出現次數，詳細說明請參考本文件第 12 頁(1) 延伸標頭的順序和重複。 2. 有關 IPv6 分段標頭(Fragment Header)，防火牆和安全設備應丟棄不包含整個 IPv6 標頭鏈(含傳輸層標頭)的第一個片段，詳細說明請參考本文件第 14 頁(3) 分段標頭(Fragment Header)。 3. 有關應用服務防火牆，建議將 IPv4 的安全經驗作為引導，以瞭解 IPv6 中可能存在的威脅，更新防火牆、拒絕服務預防措施和安全審核技術，以完全支援 IPv6，詳細說明請參考本文件第 35 頁(四) 應用服務安全考量。 4. 有關 ISP IPv6 網路連線服務，無論是固接網路、行動網路或無線公眾網路，建議用戶主機或用戶終端路由器(CPR)必須啟用 IPv6 防火牆功能，詳細說明請參考本文件第二章第二節 ISP IPv6 網路連線服務安

		全防護建議之固接網路、行動網路或無線公眾網路連線服務安全防護建議。
	入侵偵測及防禦機制	有關入侵偵測及防禦機制，建議將 IPv4 的安全經驗作為引導，以瞭解 IPv6 中可能存在的威脅，更新入侵檢測系統，以完全支援 IPv6，詳細說明請參考本文件第 35 頁(四) 應用服務安全考量。
	具有對外服務之核心資通系統者，應備應用程式防火牆	有關應用服務防火牆，建議將 IPv4 的安全經驗作為引導，以瞭解 IPv6 中可能存在的威脅，更新防火牆、拒絕服務預防措施和安全審核技術，以完全支援 IPv6，詳細說明請參考本文件第 35 頁(四) 應用服務安全考量。

參考文獻

[1] E. Vyncke, Ed., K. Chittimaneni, M. Kaeo, E. Rey, "Operational Security Considerations for IPv6 Networks," IETF Internet-Draft, draft-ietf-opsec-v6-21, November 3, 2019.

[2] E. Davies, S. Krishnan, P. Savola, "IPv6 Transition/Coexistence Security Considerations," RFC 4942, September 2007.

[3] S. Asadullah, A. Ahmed, C. Popoviciu, P. Savola, J. Palet, "ISP IPv6 Deployment Scenarios in Broadband Access Networks", RFC 4779, January 2007.

[4] G. Van de Velde, T. Hain, R. Droms, B. Carpenter, E. Klein, "Local Network Protection for IPv6," RFC 4864, May 2007.

[5] J. Woodyatt, Ed., "Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service", RFC 6092, January 2011.

[6] B. Carpenter, S. Jiang, "IPv6 Guidance for Internet Content Providers and Application Service Providers," RFC 6883, March 2013.

[7] S. Asadullah, A. Ahmed, C. Popoviciu, P. Savola, J. Palet, “ISP IPv6 Deployment Scenarios in Broadband Access Networks”, RFC 4779, January 2007.

[8] R. Koodli, “Mobile Networks Considerations for IPv6 Deployment,” RFC 6212, July 2011.

[9] J. Korhonen, J. Soininen, B. Patil, T. Savolainen, G. Bajko, K. Iisakkila, “IPv6 in 3rd Generation Partnership Project (3GPP) Evolved Packet System (EPS),” RFC 6459, January 2012.