『前瞻及完整之 IPv6 生態系推動方案』

附錄五
『Native IPv6 連網環境建置及 IPv6 用戶安全防護研析』

109 年委託研究報告

『Native IPv6 連網環境建置及 IPv6 用戶安全防護研析』 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

Native IPv6 連網環境建置及 IPv6 用戶安全防護研析

受委託單位

國立中央大學

資訊工程學系

計畫主持人

周立德

研究人員

劉建昌、古承晏、蔣昀劭、謝明諺、彭筱茵、賴映岑、陳宗琪、簡維德、吳晨緯、張祐綸、張晁誌

研究期程：中華民國 109 年 04 月至 109 年 12 月

研究經費：新臺幣 80 萬元

中華民國 109 年 10 月

目　　次

表　次

圖　次

提　要

關鍵詞：Native IPv6、NAT64、464XLAT、IPv6 資通安全

一、 研究緣起

未來 IPv6 網路的發展方向將朝向 Native IPv6 方面演進，因此如何在 IPv4 與 IPv6 共存下連線成為一門重要課題。雙協定模式可能無法解決所有新興網路營運商的問題，也因此產生了對於 IPv6 移轉機制的需求。NAT64 與 464XLAT 是解決 IPv4 與 IPv6 不相容網路之間互通性問題的關鍵技術。此外，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。鑑於未來 Native IPv6 的發展需求，本計畫將建立 Native IPv6 連網試驗環境及進行 Native IPv6 網路環境測試，同時並研析用戶 IPv6 資通安全防護相關議題與防禦機制，以提供我國 ISP 與企業/家庭用戶 IPv6 部署參考。

二、 研究方法及過程

由於 IPv6 協定的封包格式與 IPv4 不同，因此為了讓原 IPv4 的應用能夠在 IPv6 上使用，必須經過轉換機制，將 IPv4 的模式及 IPv6 的模式相互轉換，才可能讓 IPv6 與 IPv4 能夠互通。NAT64 與 464XLAT 是解決 IPv4 與 IPv6 不相容網路之間互通性問題的關鍵技術，本計畫將建立 Native IPv6 連網試驗環境及進行 Native IPv6 網路環境測試。同時，本計畫也針對家庭/企業 IPv6 資通安全防護相關議題進行研析，期能強化 IPv6 網路安全。主要議題如下:

(一) Native IPv6 連網網路環境建置：建置 Native IPv6 連網環境，包含 NAT64 暨 464XLAT 功能之硬體或 Freeware 建置。

(二) Native IPv6 網路環境測試：測試以有線裝置或行動裝置連接至熱門應用服務之連通性。

(三) IPv6 資通安全防護研析：進行家用/企業網路 IPv6 資通安全防護研究。

為有效達成本計畫規劃之工作項目任務，Native IPv6 連網環境建置與測試的方法主要是開源軟體工具為主，藉由校園接取網路建置 NAT64/DNS64 暨 464XLAT 的轉換服務，並針對網站以及應用服務部分規畫連線/測試以及應用服務測

項，相關建置規畫之經驗以及測試方法，可作為國內業者/廠商部署 Native IPv6 之參考。另針對 IPv6 資安防護部分，本計畫除參考 IETF IPv6 相關資通安全 RFC 標準外，也會針對 IPv6 家用/企業用戶資通安全防護相關議題研析，探討設備 IPv6 網路安全防護機制與功能，並針對企業/用戶網路 IPv6 網路安全管理提出建議。

三、 重要發現

(一) 部署 IPv6 是否採用 NAT 技術端視網路管理者設計網路架構的需求來取決，例如不考慮 E2E 服務透通性、有 multihoming 或 address independence 的需求或特殊情境的連線需求。

(二) NAT64/DNS64 可提供 **IPv6 -> NAT64 -> IPv4** 的應用情境，解決 Native IPv6 用戶連線 IPv4 服務的問題。

- 主流設備廠商如 Cisco 與 Juniper 部分產品已支援 NAT64，唯較高效能及 NAT64 功能必須有 license，且商用設備價格高昂。
  - CISCO 設備型號如 ASR1k/CSR1k/ISR4k；JUNIPER 設備如 ACX 系列已可支援。
- 如單以功能面考量，中小型網路可評估採用開源軟體專案如 Jool 搭配虛擬化技術透過 x86 主機實現 IPv6 NAT 的轉換服務。

(三) 464XLAT 可提供 **IPv4 -> CLAT -> IPv6 -> PLAT -> IPv4** 的應用情境，可使裝置及應用程式的運作維持透通性。

- 接取網路不需要使用 IPv4 位址，但亦可提供私有 IPv4 位址給使用者 (以 CLAT 的方式)，較符合未來 Native IPv6 網路演進之需求。

(四) 演進至 Native IPv6 非一蹴可及，IPv6 與 IPv4 網路將會長期共存，網路也必然會同時存在兩者的安全問題，或由此產生新的安全漏洞。

(五) 家用網路 CPE IPv6 資安防護功能設定主要以 ACL 為主，RFC 規範之 IPv6 資安建議仍須視個別廠商是否實作。

(六) 多數企業及 ISP 都以現有設備進行 IPv6 網路安全防護,功能或效能可能不足以應付駭客利用 IPv6 進行之惡意攻擊。

(七) IPv6 網路管理或可借鏡 IPv4 之思維，但企業網路的網管設備和網管軟體可支援 IPv6 仍然有限，亦缺乏對大範圍的 IPv6 網路故障定位和性能分析的機制。

(八) IPv6 資安設備產品或功能仍不如 IPv4 普及及完整，特別是防火牆辨識和處理 IPv6 封包的能力仍有待加強。

(九) 支援或啟動 IPv6 之設備或網站越來越多，但市場上仍缺乏 IPv6 相關網路安全的檢測機制或方法，IPv6 潛藏的漏洞可能增加安全風險。

(十) 目前多數網路攻擊和威脅大都來自應用層而非 IP 層，因此，保護 IPv6 網路安全與資訊安全，只靠一兩項技術並不夠，還需配合多種手段或機制(例如認證、IPsec、防火牆、訊務分流等)方可竟全功。

四、 主要建議事項

隨著 IPv4 位址的耗竭，為了確保網路服務的持續發展，各大電信營運商均致力推動 IPv6 的部署，並朝向 IPv6 only 的方向演進，唯選擇適合的 Native IPv6 部署方案，仍需結合營運商 IPv6 網路實際情況、用戶接受度、終端支援能力、技術標準成熟度、網路架構升級成本、服務需求部署及安全防護等因素綜合考慮後才能確定。針對未來 Native IPv6 網路部署方案建議如下。

(一) 考慮 IPv6 -> IPv4 上網服務的應用情境之需求，例如 IPv4 only 的網路內容服務業者，建議可採 NAT64/DNS64 方案部署，利用閘道器維護 IPv6 到 IPv4 的位址對映，提供 Native IPv6 的用戶端存取 IPv4 only 的服務的伺服器。

(二) 同時考慮 IPv6->IPv4 以及 IPv4->IPv6->IPv4 之應用情境，例如新興業者或 IPv4 不足之網路營運商，其核心網路以 IPv6 single stack 為基礎的網路架構，建議可採 464XLAT 方案部署，用戶端應用 APP 無須升級 IPv6，可使裝置及應用程式的運作維持透通性。

在家庭/企業網路 IPv6 安全部分，本報告主要針對企業網路安全議題，安全防護以及防護架構機進行研析，期可作為企業網路發展與部署企業內部 IPv6 網路安全與用戶連線的參考。相關建議如下:

(一) 網通廠商新上市之家用寬頻分享器 CPE 設備出廠即預設啟動 IPv4/IPv6 雙協定服務模式，並建議預設阻斷應限制之 IPv6 位址。

(二) 企業網路導入 IPv6 建議應準備具體的 IPv6 資安服務行動方案，包含制定 IPv6 安全策略、盤點設備/系統 IPv6 安全防護功能、建立 IPv6 安全管理制度以及加強 IPv6 網路安全教育訓練等。

(三) 有關 IPv6 網路安全部署與規劃，建議可參考 RFC 4942 與 Cisco B.C.P 文件制訂整體 IPv6 網路安全防護策略（IPv6 ACL 的原則）。

(四) IPv6 的安全佈署基本上除了防火牆必須能完整支援 IPv6 外，網路設備也需要能有效過濾與稽核 IPv6 位址，可預防未經授權的 IPv6 用戶存取企業網路的內部資源，此外，對於用戶網路終端設備的管理

則建議透過 Static 或 DHCPv6 用戶定址技術來有效管理企業網路內部主機或設備。

(五) 建議企業應及早進行 IPv6 資安防護規劃及在商用網路大規模實際演練，加強實戰經驗，方可徹底保障 IPv6 上網安全需求。

(六) 建議應針對企業網路相關資訊系統與設備建立 IPv6 相關網路安全檢測機制或方法，透過檢核機制有效提昇企業佈署 IPv6 的安全性。

Abstract

The future development direction of IPv6 networks will evolve towards Native IPv6, so how to connect under the coexistence of IPv4 and IPv6 has become an important topic. The dual-stack model may not be able to solve the problems of all emerging network operators, which has created a demand for IPv6 transition mechanisms. NAT64 and 464XLAT are the key technologies to solve the interoperability problem between IPv4 and IPv6 incompatible networks. In addition, with the development of IPv6, IPv6 security risks begin to emerge, and challenge IPv6 network protection capabilities. How to construct a secure network protection mechanism to ensure the security of IPv6 users is also an indispensable key to the deployment of IPv6. In view of the future development needs of Native IPv6, this project will establish a Native IPv6 networking test environment and conduct a test of the Native IPv6 network environment. At the same time, it also analyzes the relevant

issues and defense mechanisms of IPv6 information security protection to provide IPv6 deployment references for ISPs and enterprise/home users.

第一章 計畫執行狀況與檢討

第一節 計畫執行內容說明

一、 背景分析

鑑於 IPv4 位址資源逐漸耗盡，網路演進至 IPv6 已是國際共識，根據 Google 的統計與預測[1]，如圖 1 所示，在全球網路用戶中，可使用 IPv6 連線 Google 的比例為約 30.96%，較去年同期 22.62 成長約 8.3 個百分點，預計 2021 年將超過 40%。主要國家連線 Google 使用 IPv6 的比例，比利時 56.88%排名第一，德國 50.16 排第二，希臘 48.88%排第三[2]。

圖 1 全球 Google IPv6 Enabled User 比例與預測

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動 IPv6 商用運轉。然而，雖然 IPv6 成長快速，但仍存在一些議題須持續關注，特別是在 IPv6 與 IPv4 互通以及 IPv6 網路安全的問題急需解決。在 IPv4 向 IPv6 網路演進的過程中，一直存在以下兩個矛盾: （1） IPv4 位址短缺但 IPv4 應用仍是網路主流；(2） IPv6 位址空間充足，但支援 IPv6 應用卻仍然匱乏。在 IPv4 方面，透過 NAT A+P 方式似乎緩解了 IPv4 位址快速消耗的壓力，但是 NAT 設備長期投資成本以及端對端通訊的應用需求也受到質疑。在 IPv6 發展方面，用戶、ICP 以及 ISP 業者對 IPv4 位址枯竭的因應準備不一，使得 IPv6 推動發展不平衡，限制了 IPv6 的發展。這種矛盾又制約的情況也是讓 IPv6 發展這麼長時間的關鍵因素。儘管電信營運商網路和終端設備支援 IPv6 能力大幅提升，但由於支援 IPv6 的網站與應用服務較少，以致於 IPv6 訊務流量仍與 IPv4 有很大的差距；此外，雖然目前有部分網站及應用的首頁已宣稱可支援 IPv6/IPv4 雙協定，但其支援 IPv6 的程度大多仍只侷限於 IPv6 首頁可達，更多網站中內容仍然須透過 IPv4 存取，更深層次的網頁連結還未完整支援 IPv6，真正產生網路流量的圖片、影音等檔案支援 IPv6 的能力還有待提升。具體來說，如 Google、 Facebook 等指標性的入口網站或應

用支援 IPv6，並未能有效帶動其他網站與應用跟進部署 IPv6 的意願，IPv6 的用戶規模和網路流量仍有相當大的成長空間。為了解決這個問題，IETF [3]早期設計 NAT-PT 的解決方案 RFC2766 [4]，也就是 NAT-PT 協定轉換的技術，實現了 IPv6 網路與 IPv4 網路的雙向互通。但 NAT-PT 在實際網路應用中面臨各種缺陷，讓 IETF 建議不再使用，現已被 RFC4966 所廢除。然而為解決 NAT-PT 技術的缺陷，同時滿足 IPv6 連線 IPv4 的需求， IETF 提出新的解決方案： NAT64/DNS64 [5][6]及 464XLAT [7]。

二、 Native IPv6 發展及前景

Native IPv6 亦可寫作 「IPv6-only」的網路，其代表意義為 IPv6 是該網路中唯一運行的 IP 協定。可視作以前 Native IPv4 網路的 IP 升級版。Native IPv6 網路之所以作為 Native IPv4 以及 Dual-Stack 環境的最終目標，主要原因在於運行 Dual-Stack 網路的維運和建置成本過高，且不同網路之間存在不少差異，加之 IPv4 位址用罄，因此建議大部分網路提供商完全關閉 IPv4，改以採納 Native IPv6 做為唯一 IP 協定，以符合國際發展趨勢。然而，雖然 IPv6 的佈署能滿足大部分應用程式的業務需求，但是，在短期內要從 Native IPv4 的環境遷移到 Native IPv6 環境，最大的

挑戰在於服務對網路的支援性，並非所有服務提供商皆參與其中。其次面臨的挑戰包括對 Native IPv6 網路環境的安全性、管理方式及傳輸模式不了解。然而，隨著時代的發展，已經有許多大型企業建構了專有的應用程式支援 IPv6，但仍有許多服務提供商尚未完整支援，服務對 Native IPv6 網路的支援存在差異，又隨著 IPv6-only 的佈署不斷擴大，使得面向 Native IPv6 的過渡方式及營運面臨更大的挑戰。而 NAT64 及 464XLAT 被視為 Native IPv6 的過渡方案，乃因其提供支援用戶端不同的連線情境，即使服務尚無支援 IPv6 服務，亦可升級用戶端及營運商設備至 IPv6 環境，可優先做為 ISP 佈署 Native IPv6 的方案，以符合未來網路發展趨勢。

目前已有部分國外業者實際採用 Native IPv6 環境，如，T-Mobile，即是以 464XLAT 技術作為過渡到 Native IPv6 網路的技術[8]。此外，美國政府於今（2020）年 11 月 19 日發布《完成向 IPv6 過渡》備忘錄[9]，內容更新了有關聯邦政府營運部署和使用 IPv6 指南，希望加速遷移到 IPv6-only 的網路環境，也加強了 Native IPv6 的推行力道。

三、 工作項目

本計畫的目的主要是建置一套 Native IPv6 連網試驗環境及進行 Native IPv6 網路環境測試，推進我國 Native IPv6 網路環境佈署技術，工作項目說明如下：

(一) Native IPv6 連網網路環境建置

建置 Native IPv6 連網試驗環境一套：

- 包含 464XLAT CLAT（For NAT46 功能），以開源軟體建置
- 包含 464XLAT PLAT（For NAT64 功能），以開源軟體建置
- 包含 DNS64 Server（搭配 PLAT NAT64 使用），須用 BIND DNS Server 軟體建置

(二) Native IPv6 網路環境測試

進行 NAT64/DNS64 及 Native IPv6 網路環境測試，重點如下：

- 有線裝置-Windows 8.x 及 Windows 10.x
- 行動裝置-Android 10.x，iOS 13.x
- 測試應用服務如下，須在上述有線裝置及行動裝置環境下測試
  - Google Search

- Youtube
- Facebook
- Twitter
- Yahoo Search
- Skype
- Netflix
- FTP
- SFTP
- Windows Outlook
- Gmail

(三) IPv6 用戶資通安全防護研析

1. 進行 IPv6 家用資通安全防護研究並整理交付技術手冊一份。

   i. 研析 IPv6 網路安全的基本知識與技術，針對家庭/企業網路 IPv6 網路安全功能需求，制定用戶網路 IPv6 安全防護規範，提供 IPv6 家庭/企業網路安全管理參考建議，提出家用 IPv6 與企業用戶資通安全防護手冊各一份。內容須包含

   - IPv6 網路安全議題與解決方案
   - 路由器、交換器、防火牆與主機 IPv6 安全防護規範與建議

ii. 擬參考下列 RFC

- RFC 7381 Enterprise IPv6 Deployment Guidelines [7]
- RFC 4057 IPv6 Enterprise Network Scenarios [10]
- RFC 6092 Recommended Simple Security Capabilities in Customer Premises Equipment （CPE） for Providing Residential IPv6 Internet Service [11]

2. 進行 IPv6 企業用戶資通安全防護研究並整理交付技術手冊一份：建置 IPv6 網路安全測試環境，研擬測試項目與情境規劃（如 IPv6 ACL、MAC Filter、RA Guard 等），驗證 IPv6 網路防禦機制，並撰寫測試報告。

圖 2 為本案規劃之 IPv6 用戶資通安全防護研究範疇。

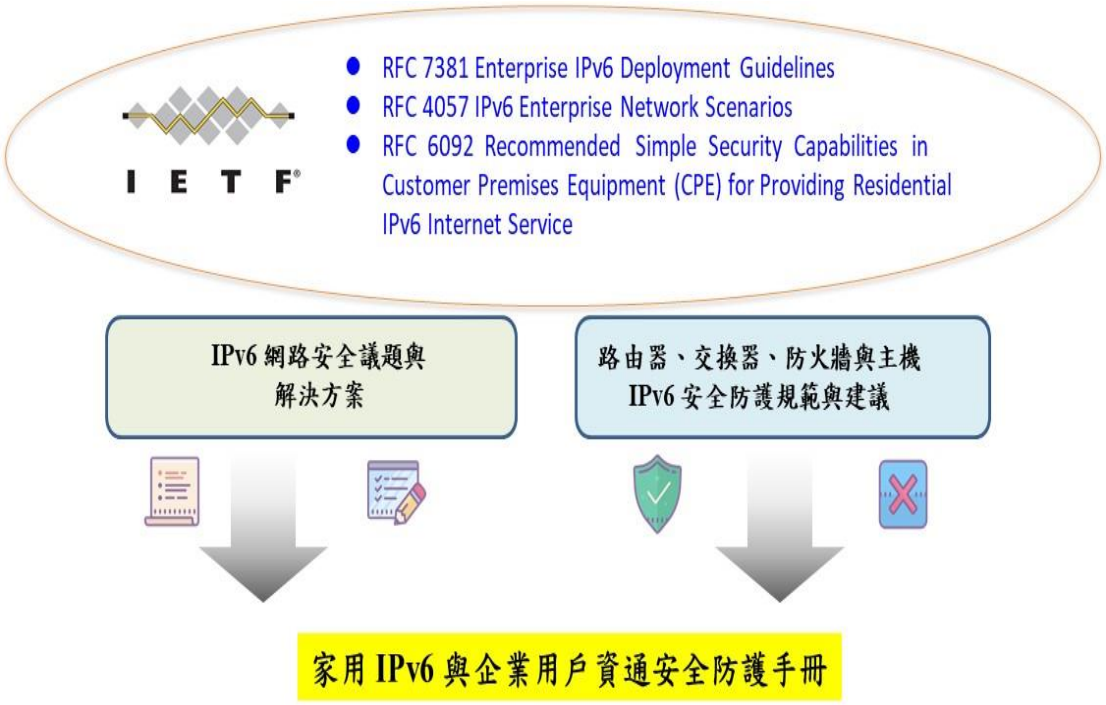


圖 2 資通安全手冊研究範疇

四、預期成果

本計畫主要建置一套 Native IPv6 連網試驗環境及進行 Native IPv6 網路環境測試，並且進行 IPv6 用戶資通安全防護研析。本計畫之執行將提供適合未來 Native IPv6 環境的轉移技術，實際驗證與測試有線裝置與行動裝置連線公眾網路服務的能力，可提供台灣 ISP 業者部署 Native IPv6 之參考；此外，為提升 IPv6 資通安全防護能力，本計畫亦針對 IPv6 網路安全技術進行研析，期能藉由本計畫研究之成果，推進我國 IPv6 技術能力，以因應未來 IPv6 資通安全防護及 Native IPv6 網路演進需求。本計畫預期成果或效益如下：

(一)建置 Native IPv6 網路環境，可提供國內業者實際建置 464XLAT 移轉服務之參考。

(二)測試 Native IPv6 網路環境，可提供國內業者部署 IPv6-only 連線 IPv4-only 服務應用情境，優化與改善網路品質的參考依據。

(三)完成家用 IPv6 與企業用戶資通安全防護手冊，可作為我國企業與家庭用戶 IPv6 安全防護之參考。

(四)完成 IPv6 網路安全測試環境建置，可作為我國各級網路測試與檢驗 IPv6 網路防禦與測試情境之參考。

五、研究方法

本計畫之執行架構圖 3 所示，主要可分為 Native IPv6 網路環境的建置/測試以及 IPv6 用戶資通安全防護研析兩大主軸。Native IPv6 網路環境的建置/測試方面，將以 JOOL [12]開源軟體搭配 BIND 9[13]工具建置 NAT64/DNS64 及 464XLAT 環境（包含 CLAT 及 PLAT 功能） [14]，並以有線裝置及無線裝置分別進行連網測試，測試其連通性。

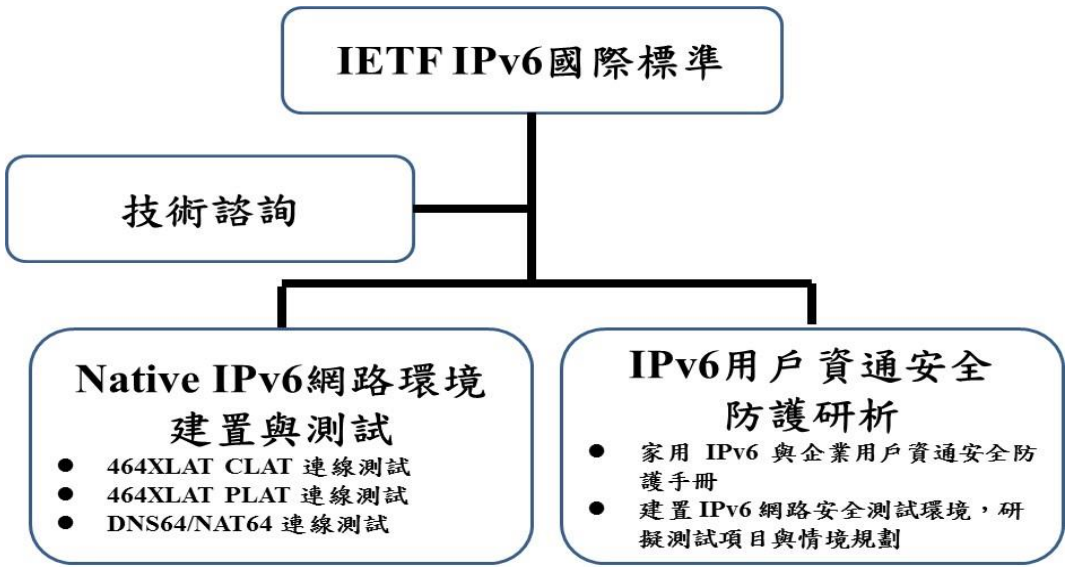


圖 3 計畫執行架構

IPv6 用戶資通安全防護研析方面，將研析 IPv6 網路安全的基本知識與技術，針對家庭/企業網路 IPv6 網路安全功能需求，制定用戶網路 IPv6 安全防護規範，提供 IPv6 家庭/企業網路安全管理參考建議。

六、施行方式與進行步驟

(一) NAT64/DNS64 連網測試

NAT64/DNS64 連網架構如圖 4 所示。NAT64 為 IPv4–to–IPv6 過渡時期的解決機制之一，配合 DNS64 就可提供 IPv6-only Client 與 IPv4-only Server 之互連，也可提供 IPv6-only 主機與 IPv4-only 主機之點對點傳輸服務，而且當中不需要對 IPv6 或 IPv4 設備做任何變動。DNS64 則主要是配合 NAT64 工作，主要是將 DNS 查詢訊息中的 A 記錄 （IPv4 位址） 合成到 AAAA 記錄 （IPv6 位址） 中，返回合成的 AAAA 記錄用戶給 IPv6 側用戶。DNS64 也解決了 NAT-PT 中的 DNS-ALG 存在的缺陷。

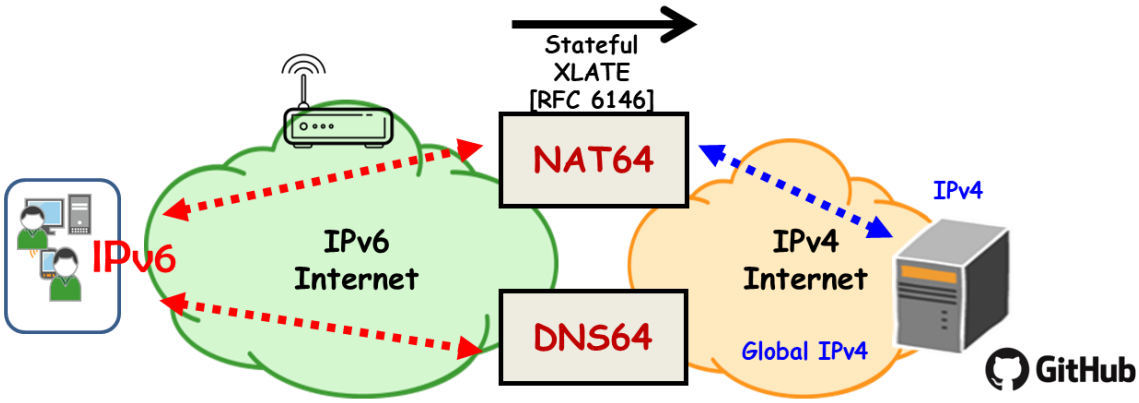


圖 4 NAT64/DNS64 測試架構

NAT64 主要針對位址以及協定在做轉譯，其中位址轉譯包含 Address 和 Port 兩部分，而協定轉譯部分主要是根據 SIIT（Stateless IP/ICMP Translation） [15]，為了讓 IPv4 位址與 IPv6 位址能夠對應，

NAT64 擁有 IPv4 Address pool 與 IPv6 Address pool，如果需要讓 IPv4 位址對應到 IPv6 位址，NAT64 將從 IPv6 Address pool 挑出一 IPv6 Prefix 並結合 32 位元之 IPv4 位址，成為分配給 IPv4 主機的 128 位元 IPv6 位址。由於 IPv4 Address pool 位址數量相對較為不足，所以在分配位址給 IPv6 主機時通常採用動態分配，即分配暫時性的位址，而非永久性的。

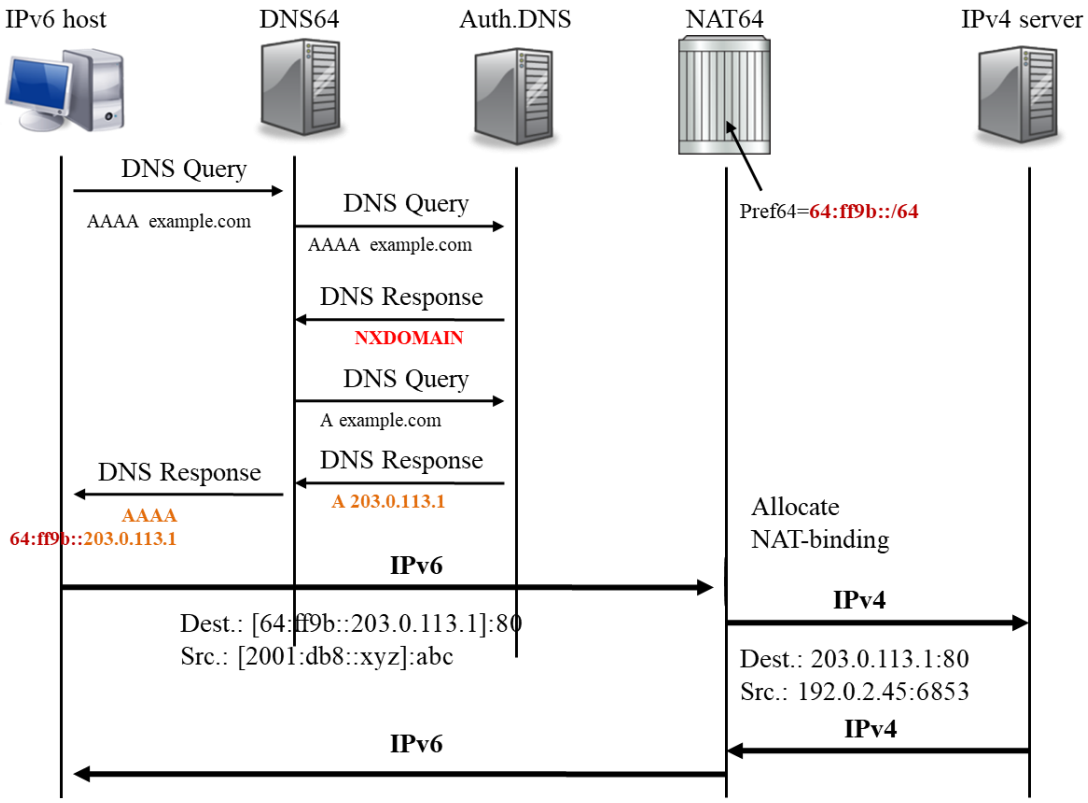


圖 5 NAT64/DNS64 Message Flow

圖 5 為 NAT64/DNS64 運作流程。主要的原理是讓 DNS64 可同時查 IPv6 和 IPv4 的位址，如有 IPv6 記錄時以 IPv6 優先，若沒有就

轉換 IPv4 為 IPv6，prefix 配合 NAT64 的設定，讓 client 連往該 IP 的封包會先經過 NAT64 router，然後 NAT64 會再轉換 IPv6 的封包成 IPv4 出去，無縫接上 IPv4 server。如 client 收到 DNS64 回應的正常 IPv6 位址，就透過一般 router 直接出去，不用再經過 NAT 64 處理。

(二) 464XLAT 連網測試

464XLAT 是一種無狀態和有狀態結合、用於 IPv4 與 IPv6 通訊轉換[16]，一般是在 CLAT 和 PLAT 上執行，讓私有網路上的 IPv4 主機可以透過 IPv6 網路跟位於 IPv4 網路上的 IPv4 伺服器或主機聯繫。CLAT 上執行無狀態地址 IPv4-IPv6 轉換 （1:1），主要是參考 RFC6052 內嵌 IPv4 位址格式；PALT 是執行有狀態地址 IPv4-IPv6 轉換，集中處理、維護私有網路 IPv4 到公眾網路 IPv4 的 NAT44。NAT64 透過使用 CGN 實現 IPv6 網路連線 IPv4 的網路，464XLAT 擴展了這種功能，允許 IPv4-Only 應用在 IPv6-Only 的網路上進行通訊，使用主機設備上不需要 IPv4 位址。464XLAT 測試架構如圖 6。

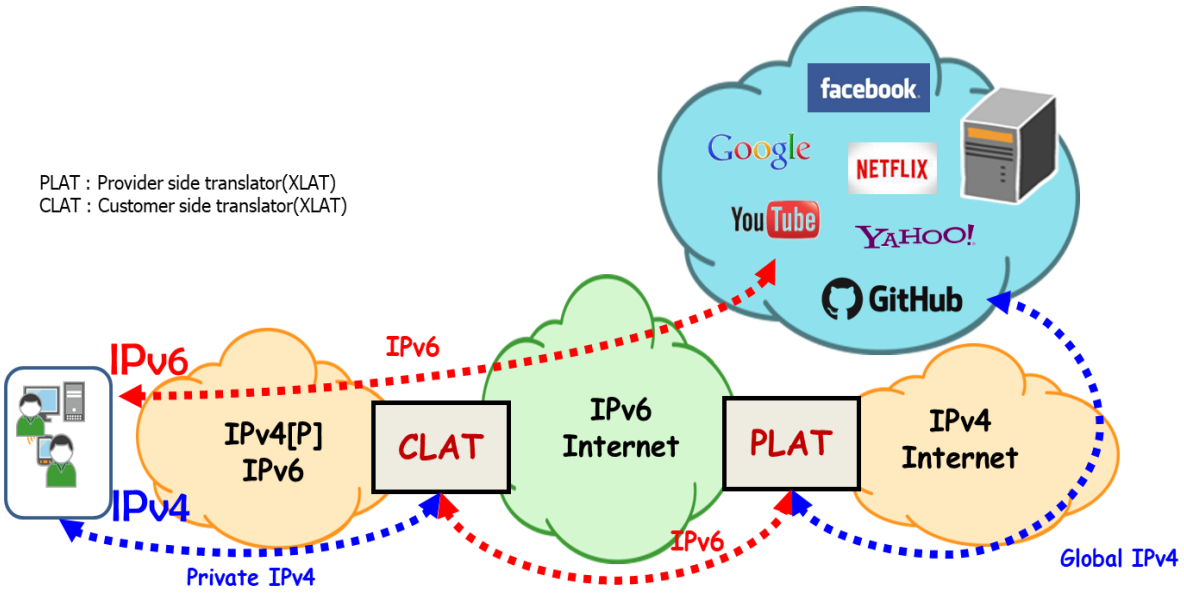


圖 6 464XLAT 測試架構

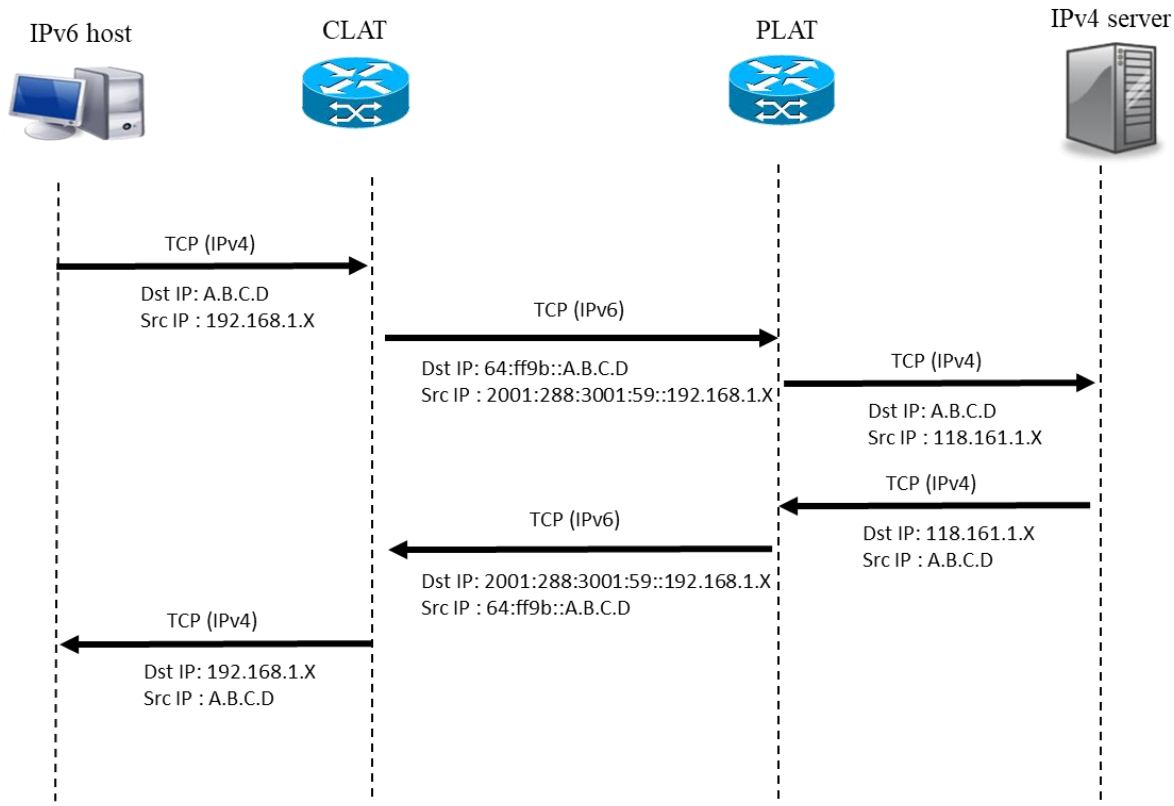


圖 7 464XLAT Message Flow

圖 7 為 464XLAT 的運作流程。464XLAT 採用 Translation 方式進行 IPv4 轉換 IPv6，在 IPv4-IPv6 網路邊界利用 CLAT 進行 NAT 轉換，將 IPv4 嵌入到 IPv6 的 Src 與 Dst 中直接進行轉換，在 IPv6 網路 PLAT 中則是以 IPv4 pool 去取一個 global IPv4 跟 private IP mapping Src 與 Dst 直接轉換，回程 PLAT 再將 global 轉成 prvate Dst ，然後再由 CLAT 直接從 IPv6 取出 IPv4 送回。

第二節　與計畫符合情形

一、目標達成狀況

依照本研究計畫工作項目時程規劃進度如下表所示：

表 1 各項工作執行進度

工作項目	月份											
	1	2	3	4	5	6	7	8	9	10	11	12
1. Native IPv6 網路環境規劃					▲							
2. Native IPv6 網路環境建置與測試										▲		
3. 期中報告						▲						
4. IPv6 家用資通安全防護研究並整理交付技術手冊						▲						
5. IPv6 企業用戶資通安全防護研究並整理交付技術手冊										▲		
6. 期末報告										▲		

▲：為各階段之工作查核點。

註 1：期中報告為 6 月 20 日前交付

註 2：期末報告為 10 月 20 日前交付

二、進度符合情形

各項工作的查核點進度，符合原計畫申請書之規劃，工作進度如下表所示：

表 2 各項查核進度表

工作項目	執行進度			原因說明
	超前	符合	落後	
Native IPv6 網路環境規劃		V		
Native IPv6 網路環境建置與測試		V		
期中報告		V		
IPv6 家用資通安全防護研究並整理交付技術手冊		V		
IPv6 企業用戶資通安全防護研究並整理交付技術手冊		V		
期末報告		V		

第三節 資源運用檢討

一、人力運用情形

本研究計畫共投入總執行人力 5 人，與原計畫申請書之規劃相符，各人力擔任之工作如下表所示：

表 3 執行人力表

類別	姓名	職位	最高學歷	在本計畫中擔任之工作
主持人	周立德	計畫主持人	博士	督導與協調計畫各項工作，進度管理，成果報告總校閱
協同研究人員	劉建昌	研究助理	博士生	規劃設計 Native IPv6 網路實驗環境與研析資通安全防護技術與方法
協同研究人員	古承晏	研究助理	碩班生	NAT64/DNS64 以及 464XLAT 功能建置與終端測試
協同研究人員	謝明諺	研究助理	碩班生	建置 IPv6 網路安全測試環境，研擬測試項目與情境規劃
協同研究人員	蔣昀劭	研究助理	碩班生	研析用戶網路 IPv6 網路安全議題與防禦機制，撰寫家用 IPv6 與企業用戶資通安全防護手冊
協同研究人員	賴映岑	研究助理	碩班生	NAT64/DNS64 以及 464XLAT 功能建置與終端測試
協同研究人員	彭筱茵	研究助理	碩班生	NAT64/DNS64 以及 464XLAT 功能建置與終端測試

類別	姓名	職位	最高學歷	在本計畫中擔任之工作
協同研究人員	陳宗琪	研究助理	碩班生	NAT64/DNS64 以及 464XLAT 功能建置與終端測試
協同研究人員	吳晨緯	研究助理	碩班生	協助撰寫家用 IPv6 與企業用戶資通安全防護手冊
協同研究人員	簡維德	研究助理	碩班生	研讀並整理 IPv6 相關 RFC 文獻
協同研究人員	張晁誌	研究助理	碩班生	NAT64/DNS64 以及 464XLAT 功能建置與終端測試
協同研究人員	張祐綸	研究助理	碩班生	協助撰寫家用 IPv6 與企業用戶資通安全防護手冊

二、經費運用情形

依照目前本研究計畫進度，依據工作規畫執行各項經費，經費運用情形與進度相當，各項經費使用如下表所示：

表 4 總經費運用情形統計表

項　目	預算金額	使用金額	使用率	備　註
人事費用	564,557	302,312	53.55%	流入數: 0 流出數: 0
儀器設備費用	0	0	0	
消耗性器材及藥品費用	0	0	0	
業務費	121,835	57,165	46.92%	流入數: 0 流出數: 0
旅運費	40,881	0	0	流入數: 0 流出數: 0
行政管理費	72,727	0	0	流入數: 0 流出數: 0
合　計	800,000	359,477	44.93%	

第二章 成果說明

第一節 Native IPv6 網路環境規劃

一、 NAT64/DNS64 暨 464XLAT 環境規劃

本計畫將分別針對 NAT64/DNS64 及 464XLAT 連網架構，以校園網路作為 IPv4 與 IPv6 接取環境，並於實驗室自行架設 NAT64/DNS64 暨 464XLAT 轉換服務，提供 IPv6 ->PLAT -> IPv4 以及 IPv4 -> CLAT -> IPv6 -> PLAT -> IPv4 兩種連線情境。圖 8 為中央大學校園網路 IPv6 位址分配。

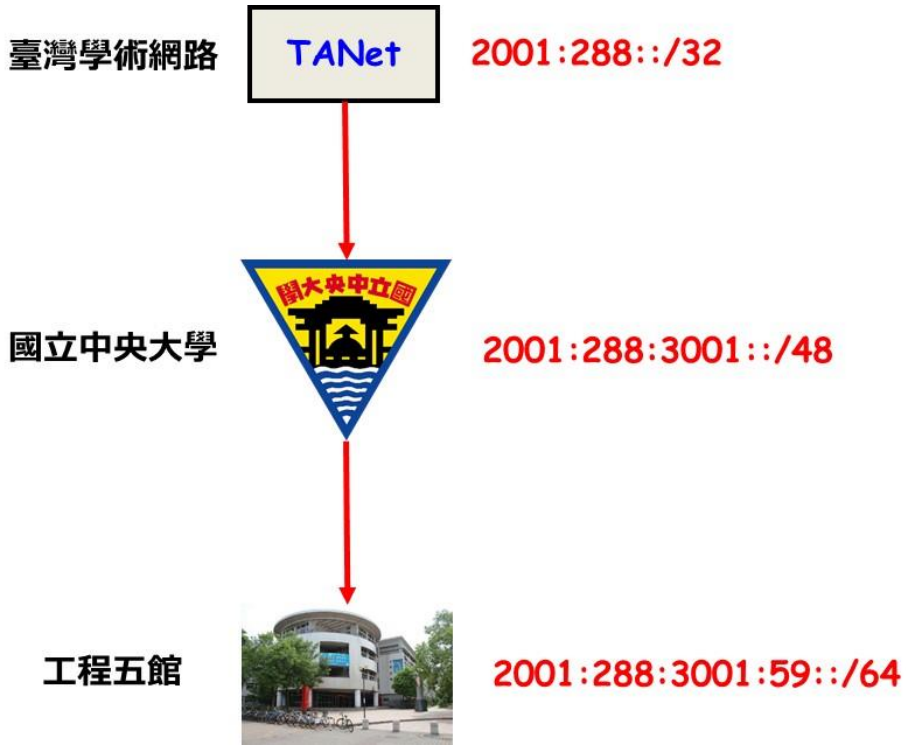


圖 8 中央大學校園網路 IPv6 位址分配

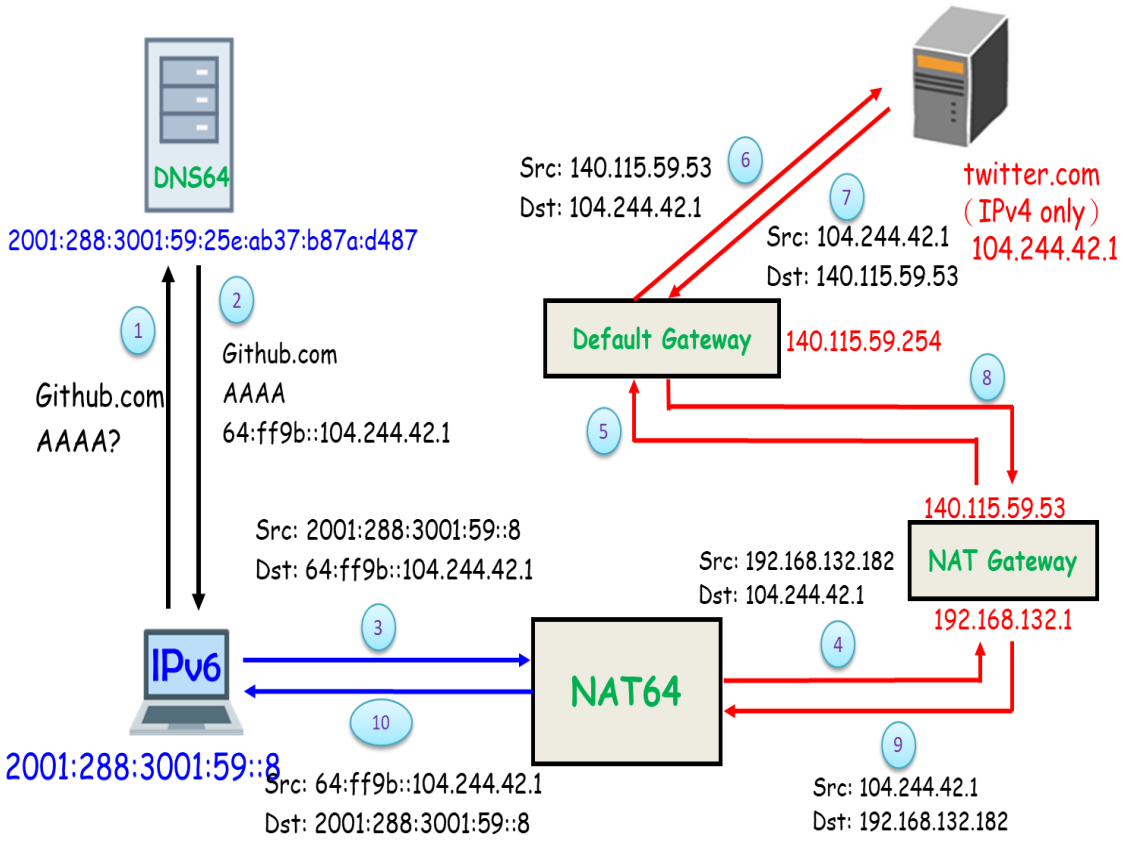


圖 9 NAT64/DNS64 實驗架構規劃與 IP 配置

NAT64/DNS64 轉換服務架構與 IP 配置如圖 9 所示。圖中左方為以 IPv6-only 連接方式連接實驗室網路之用戶，所到達網段或網域僅限於 IPv6 Internet。客戶端如預請求 IPv4 only 的網站服務（如，github.com），亟需透過 DNS64 的幫助。DNS64 架設於學校內網與外部網路之間，在收到來自客戶端有關某個域名 AAAA（IPv6 位址）紀錄的查詢時，它會像平常一般找尋答案，若該域名有 IPv6 的位址，則直接將該紀錄直接回覆給客戶端。相

反地,若找不到任何此類的紀錄,即目的地域名不提供IPv6位址,則會嘗試查找相同域名的 A 紀錄（IPv4 位址）。DNS64 會將查詢到的 A 記錄中”合成”相等數量的 AAAA 紀錄，將 32 位元的 IPv4 位址嵌入到 128 位元的 IPv6 位址中,並加上 IPv6 的前綴(此處為 64:ff9b::/96)。DNS64 即將此 IPv6 位址回覆給用戶，自此，用戶會認為該域名網站有支援 IPv6 的服務,並且可以直接與其通信。而後,用戶將此域名(新的 IPv6 位址)傳送至 NAT64。NAT64 則通過 JOOL 中之 JOOL instance 將 IPv6 位址中之前綴位址取出，留下後綴位址（原 IPv4 位址)，依此後綴即可到達該網站之 IPv4 位址，以存取該服務。

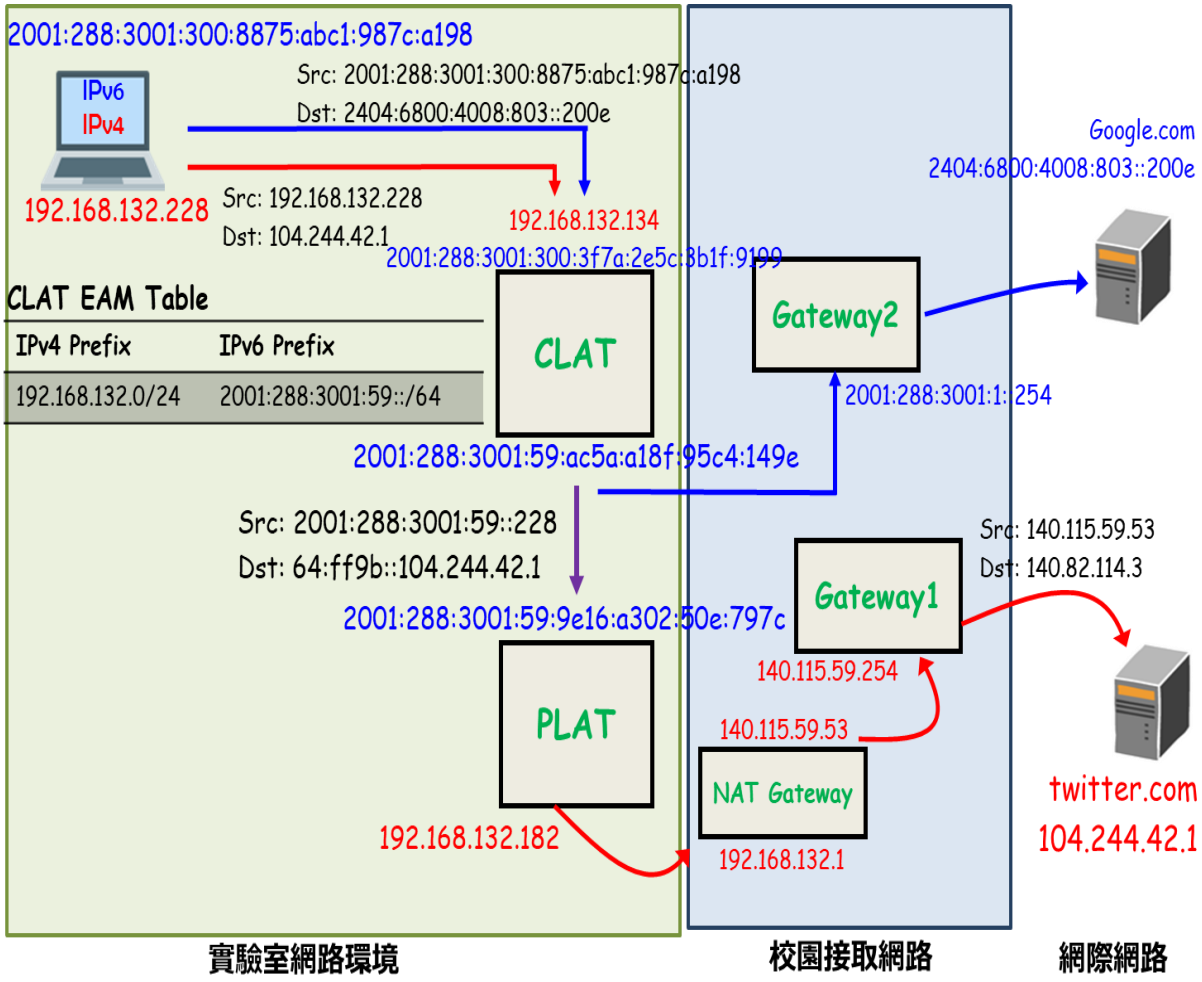


圖 10 464XLAT 實驗架構規劃與 IP 配置

464XLAT 轉換服務架構與 IP 配置如圖 10 所示。464XLAT 為具有私有位址的 IPv4 客戶端通過 IPv6 網絡連接到 IPv4 主機提供了一種簡單且可擴展的技術。我們於實驗室環境中架設一台 CLAT 及一台 PLAT 伺服器，並搭配 JOOL 開源軟體建置。CLAT 通過 JOOL instance 將 IPv4 來源地址和目標地址嵌入 IPv6 前綴中，再通過 EAMT（Explicit Address Mappings Table）方式將 IPv4

位址轉換為 IPv6，然後以 Native IPv6 方式將網路封包發送到 PLAT。 PLAT 透過 pool4 方式轉換，將 IPv6 位址轉換為 IPv4，然後通過 Native IPv4 將網路封包發送到 IPv4 主機。其中若目的地位址有支援 IPv6 服務（如，google.com），則封包可經過 CLAT 後中途下站，不須再經過 PLAT 將位址轉為 IPv4 送出，可直接由 IPv6 方式存取該服務。而 CLAT 亦可以嵌入於 IPv6-only 的移動網路中的最終用戶移動設備上[8]，從而允許移動網路提供商為其用戶推出 IPv6 服務，並在移動設備上支援 IPv4-only 的應用程式。

二、 測試項目規劃

本計畫將針對前述所建置之 NAT64/DNS64 及 464XLAT 環境進行網路連線測試。依照測試項目及測試方案可將測試規劃成三個部分—連網測試、連線測試及應用測試，如下圖所示。

圖 11 NAT64/464XLAT 測試規劃

底下針對三個測試部分做說明：

(一) 連網測試

以終端設備操作介面或應用程式為基礎，檢測 WEB 目標網站連線狀態，主要測試使用者介面配置 IPv6 參數與瀏覽器 IPv6 連網測試。測試方式係以 ICMP 及瀏覽器測試網站連線，測試網站包含：

- Google Search
- Youtube
- Yahoo Search
- Facebook
- Twitter

(二) 連線測試

以測試與比較端對端連線有無經過 NAT64/464XLAT 轉移機制的差異，須測試 IPv6 Connectivity 連通性及 IPv4 與 IPv6 之連線差異。

(三) 應用測試

以終端設備操作介面或應用程式為基礎，檢測應用服務使用狀態，從使用者角度與觀點來檢測操作或使用上是否會發生錯誤中斷情況。此項測試會針對以下應用程式做連線狀態之測試：

- Skype
- Netflix
- FTP
- SFTP
- Windows Outlook
- Gmail

第二節 Native IPv6 網路環境建置與測試

本計畫目的為建置 NAT64/DNS64 暨 464XLAT 試驗環境提供 Native IPv6 的連網環境，本章主要說明 Native IPv6 網路環境建置與測試結果。

一、 Native IPv6 環境建置

NAT64、CLAT 及 PLAT Server 建置規劃以 JOOL 開源軟體在實驗室環境中建置；DNS64 Server 則採用 BIND9 開源軟體實現。以下分別介紹及說明兩者功能：

(一) JOOL

JOOL 作為在 Linux 作業系統中實現 SIIT（Stateless IP / ICMP Translation）、IPv4/IPv6 Translation、Stateful NAT64 及 Stateless NAT64 的位址轉換功能之方案，是最廣泛被使用作為 NAT64 及 464xlat 環境建置的開源軟體之一，由 NIC Mexico 與蒙特雷科技大學開發。JOOL 以 JOOL instance 的方式來實現 IPv4/IPv6 的轉換。JOOL instance 中記錄著 IPv4/IPv6 轉換的規則，使用者可根據需求將客製化的轉發規則添加至 JOOL instance 中。而 JOOL instance 可被附加至兩種不同的 Linux 框架中—Netfilter 與 iptables，藉此可達到訊務攔截（traffic intercepting）的效果，訊務攔截後即

透過 JOOL instance 中的轉換規則，將 IPv4/IPv6 的位址進行轉換，再發送至其目的地[12]。

(二) BIND

BIND 為 Berkeley Internet Name Domain 之縮寫，最初的時候是由加州大學柏克萊分校所發展出來的 BSD UNIX 中的一部份，目前則由網際網路系統協會（Internet Systems Consortium, ISC）來負責維護與發展。BIND 是用來解決網域名稱與 IP 位址對應的軟體，且是個被廣泛使用的 DNS 伺服器軟體，它提供了強大及穩定的名稱服務，因此有近九成的 DNS 伺服器主機都是使用 BIND。目前最新的版本到 BIND 9。BIND 9.8.0 以上的版本透過 dns64 的 options statement 以達到支援 DNS64 的功能。DNS64 通過添加 IPv6 前綴到原 IPv4 位址中以完成 128 位址的 IPv6 位址轉換[13]。

針對 NAT64/DNS64 轉換服務測試環境，本計畫是以 BIND9 搭配 JOOL 開源軟體實現。IPv6-only 的用戶可透過 DNS64 獲取到目的地的 IPv6 位址，再透過 NAT64 的幫忙存取到 IPv4-only 的網站或應用程式服務。表 5 為 NAT64/DNS64 軟硬體配置，圖 12 為開源軟體設定範例。

表 5 NAT64/DNS64 資源配置配置

資源配置			
	項目	DNS64	NAT64
硬體資源配置	CPU(cores)	Intel(R) Xeon(R) CPU E5620 @ 2.40GHz 各配置2核心	
	Memory(GB)	4	4
	Disk(GB)	60	60
軟體配置	Distribution	Ubuntu 18.04	Ubuntu 18.04
	Kernel Version	5.3.0-62-generic	5.3.0-62-generic
	Implement	BIND9	JOOL
	Source Version	9.10.3-P4-Ubuntu	4.1.1.0

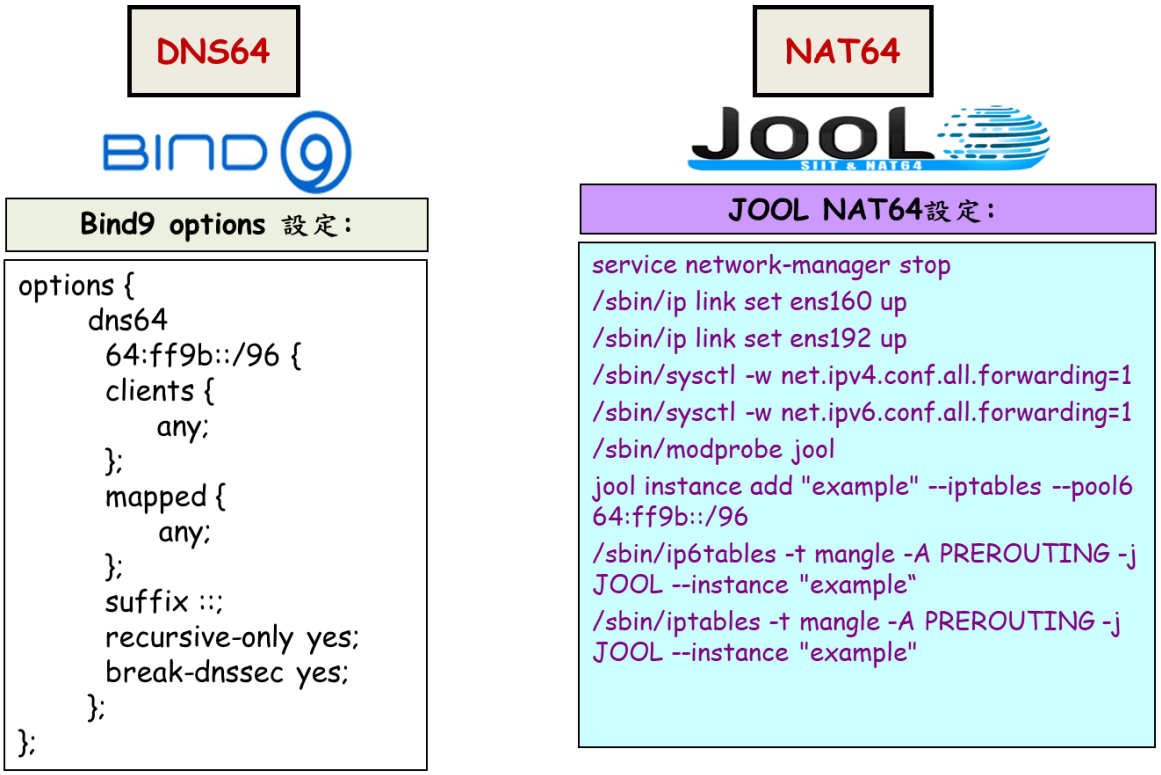


圖 12 NAT64/DNS64 設定範例

表 6 464XLAT 資源配置

資源配置			
	項目	CLAT	PLAT
硬體資源配置	CPU	Intel(R) Xeon(R) CPU E5620 @ 2.40GHz 各配置2核心	
	Memory(GB)	4	4
	Disk(GB)	60	60
軟體配置	Distribution	Ubuntu 18.04	Ubuntu 18.04
	Kernel Version	5.3.0-62-generic	5.3.0-62-generic
	Implement	JOOL	JOOL
	Source Version	4.1.1.0	4.1.1.0

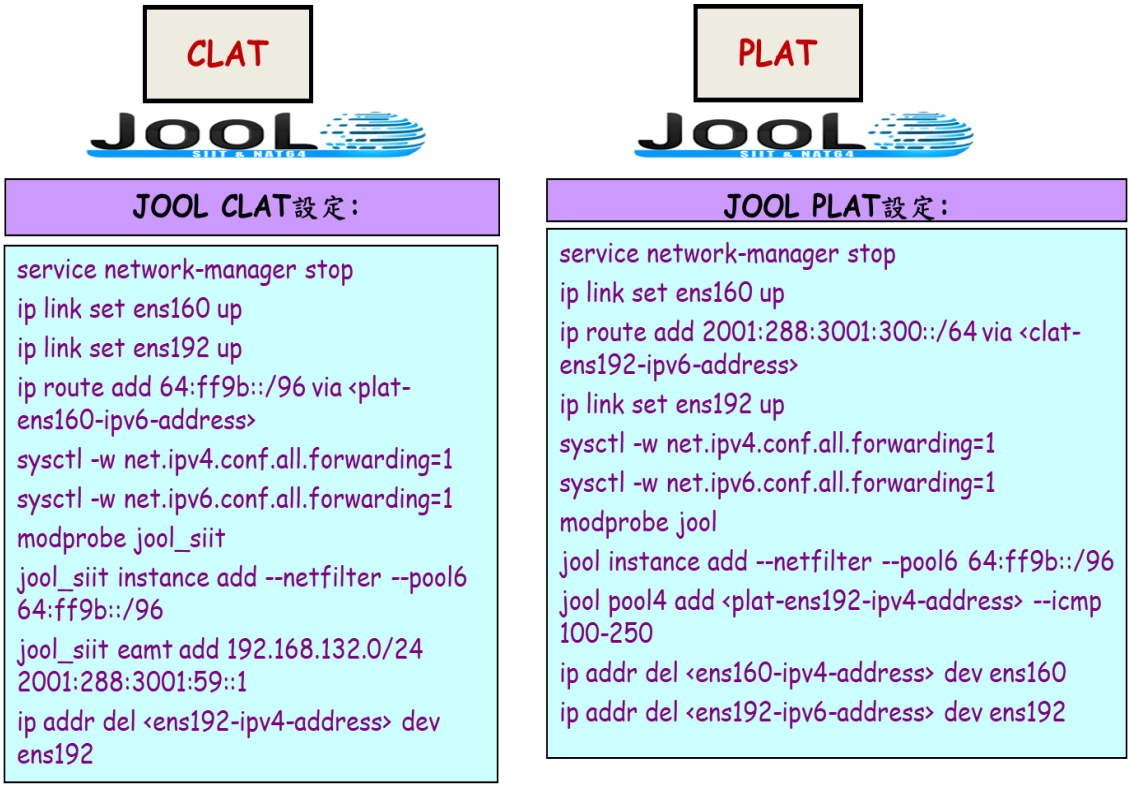


圖 13 464XLAT 設定範例

464XLAT 之 CLAT 與 PLAT 位址轉換功能同樣以 JOOL 開源軟體建置，無論為 IPv4-only、IPv6-only 或 dual-stack 的用戶，皆可透過 464XLAT 的環境存取服務，若存取服務支援 IPv6，則用戶可走 Native IPv6 環境，若存取服務僅支援 IPv4，用戶亦可透過 CLAT 及 PLAT 位址轉換功能，達到存取服務的目的。表 6 為 464XLAT 軟硬體配置，圖 13 為 JOOL 開源軟體設定範例。

二、 Native IPv6 測試結果摘要

(一) NAT64/DNS64 測試結果

NAT64/DNS64 測試結果摘要如表 7 所示。分為基本測試、連線測試及應用測試，測試結果如下說明：

表 7 NAT64 測試摘要

項次	網站名稱	網站類型	有線裝置		無線裝置	
			Win8	Win10	Android	iOS
1	Google	入口網站	v	v	v	v
2	Youtube	影音網站	v	v	v	v
3	Facebook	社群網站	v	v	v	v
4	Yahoo	入口網站	v	v	v	v
5	Netflix	影音網站	v	v	v	v
6	Twitter	社群網站	v	v	v	v

項次	服務	名稱	有線裝置		無線裝置	
			Win8	Win10	Android	iOS
7	SKYPE	通訊服務	v	v	v	v
8	FTP	下載服務	v	v	v	v
9	SFTP	傳輸服務	v	v	v	v
10	Outlook	郵件服務	v	v	v	v
11	Gmail	郵件服務	v	v	v	v

項次	網站名稱	網站支援	訊務是否會經過NAT64	Response Time	Ping	Web
1	Google	DualStack	否	4ms	v	v
2	Youtube	DualStack	否	3ms	v	v
3	Facebook	DualStack	否	3ms	v	v
4	Yahoo	DualStack	否	140ms	v	v
5	Netflix	DualStack	否	163ms	v	v
6	Twitter	IPv4 only	是	56ms	v	v

基本測試是檢測 WEB 目標網站連線狀態，使用 ICMP 及瀏覽器測試網站連線。目標網站包含 google.com、youtube.com、facebook.com、yahoo.com、netflix.com 及 twitter.com，測試結果顯示，所有網站皆通過測試。唯 twitter.com 無支援 IPv6 服務，須經由 NAT64 的轉換後方可存取網站。

連線測試是以測試端對端連現有無經過 NAT64/464XLAT 轉換機制的差異，測試基本測項中六個網站，並和 Native IPv6 環境比較，主要驗證其經過 NAT64 轉換後是否會對其 response time 造成影響。而包含 Google、Youtube、Facebook、Yahoo 及 Netflix 在內的 5 個測試網站皆為 DualStack，無論 IPv4 或 IPv6 連線方式皆可存取網站服務。而 twitter.com 因無支援 IPv6 方式連線，故無法經由 Native IPv6 環境存取服務。

應用測試是以終端設備操作介面或 APP 為基礎檢測應用服務使用狀態。測試目標為 SKYPE、FTP、SFTP、Outlook、Gmail。結果顯示所有應用測項皆通過測試。

(二) 464XLAT 測試結果

464XLAT 測試結果摘要如表 8 所示。同樣分為基本測試、連線測試及應用測試，測試結果如下說明：

表 8 464XLAT 測試摘要

項次	網站名稱	網站類型	有線裝置		無線裝置	
			Win8	Win10	Android	iOS
1	Google	入口網站	v	v	v	v
2	Youtube	影音網站	v	v	v	v
3	Facebook	社群網站	v	v	v	v
4	Yahoo	入口網站	v	v	v	v
5	Netflix	影音網站	v	v	v	v
6	Twitter	社群網站	v	v	v	v
項次	服務	名稱	有線裝置		無線裝置	
			Win8	Win10	Android	iOS
7	SKYPE	通訊服務	v	v	v	v
8	FTP	下載服務	v	v	v	v
9	SFTP	傳輸服務	v	v	v	v
10	Outlook	郵件服務	v	v	v	v
11	Gmail	郵件服務	v	v	v	v

網站支援	網站名稱	訊務是否經過CLAT	訊務是否經過PLAT	464XLAT			Native IPv4		
				Response time	Ping	Web	Response time	Ping	Web
DS	Google	是	否	3ms	v	v	4ms	v	v
DS	Youtube	是	否	4ms	v	v	4ms	v	v
DS	Facebook	是	否	3ms	v	v	28ms	v	v
DS	Yahoo	是	否	167ms	v	v	165ms	v	v
DS	Netflix	是	否	165ms	v	v	X	X	v
IPv4 only	Twitter	是	是	66.3ms	v	v	65ms	v	v

結果顯示，464XLAT 基本測試所有測項皆可透過 464XLAT 連網環境存取。其中 twitter.com 須經由 4-to-6-to-4 的轉換，而其他網站則是 6-to-6 的方式。

連線測試的部分，6 個目標網站皆可透過 464XLAT 環境存取。從表中 twitter.com 測項結果可看出經由 464XLAT 轉換和 Native IPv4 的連線方式之差異，response time 只差距 1.3ms，轉換影響甚小。

應用測試的部分，Windows10、Windows8、Android 及 iOS 四種作業系統皆皆可通過所有應用測試。

(三) 交叉測試成果

此部分測試之比較對象為兩組，一組為 Windows10 主機，需經過 Native IPv6 環境才存取目的網站，另一組同樣為

Windows10 主機，但須透過 Native IPv4 的連接方式連接外網。測試過程由 10 位實驗室成員分別操作兩台主機各 10 分鐘，期間可隨意瀏覽網站、上傳及下載檔案，事前不告知哪台主機為 Native IPv4 環境，哪台為 Native IPv6 環境。此測試主要以使用者觀點進行操作測試，比較 IPv4 和 IPv6 連線品質的差異。

實驗結果顯示，有 5 位同學準確猜出哪台電腦為 Native IPv4 環境，哪台為 Native IPv6 環境；有 4 位同學回答錯誤，將 Native IPv4 電腦誤認為 Native IPv6 環境；將 Native IPv6 電腦誤認為是 Native IPv4 環境；還有 1 位同學無法分辨。事後對受測同學進行調查，無論猜對或猜錯的同學，均表示兩者差異甚小，幾乎感受不到差別。此實驗結果證明 464XLAT 轉換機制在主觀的使用者體驗上影響很小，幾乎可以省略。而客觀的數據，如 response time 也顯示有無經過轉換機制的差異並不大，可見以 JOOL 等 open source 搭建 464XLAT 轉換環境之方案可行。

第三節 家庭 IPv6 資通安全防護研究

針對家庭 IPv6 網路安全防護，寬頻分享器是面向 IPv6 終端用戶的第一線設備，也是家庭網路環境常見的網路設備，故本節針對家庭 IPv6 資通安全防護的討論主要以 CPE 寬頻分享器為主。探討議題如下圖 14 所示。

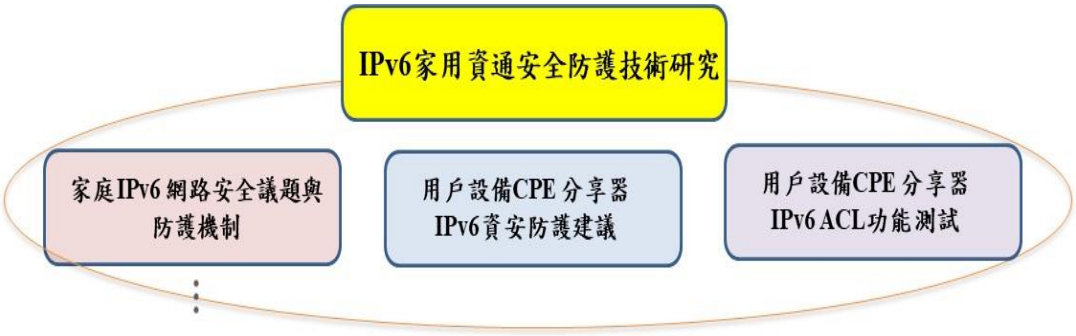


圖 14 家庭用戶 IPv6 資通安全技術研究範疇

一、 家庭 IPv6 網路安全議題與防護機制

針對家庭網路相關 IPv6 攻擊與防護議題摘要如下表 9 所示。

表 9 家庭網路 IPv6 攻擊分類

類別	說明	攻擊類型	防護機制
Neighbor Discovery 攻擊	Neighbor Discovery 協定為 IPv6 基本必要之功能無法關閉，IPv6 的 ND 攻擊方式類似 IPv4 的 ARP 攻擊	竊聽、偽冒 Spoofing、Flooding 攻擊、攻擊重導攻擊等	1.SeND (RFC 3971) 2.IPv6 ACL
Router Advertisement 攻擊	每個 IPv6 節點都可以發送 Router Advertisements，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	中間人 MITM 等、RA Flooding 阻斷服務 DoS	1.IPv6 ACL 2.RA Guard (RFC 6105)
ICMPv6 攻擊	ICMP 的主要功用為錯誤報告與診斷，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	掃描與偵查、阻斷服務 DoS 等	IPv6 ACL (RFC 4890)

二、 家用寬頻分享器 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。為此本章以 RFC 6092 為基礎，重點摘要家用寬頻分享器 IPv6 防護建議如下：

(一) IPv6 基本防護功能建議符合下列性質之封包皆丟棄，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 功能建議

- 防火牆 ICMPv6 錯誤訊息套用 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
- Connection-Free Filters ICMPv6 功能建議
- 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

(三) Mobile IPv6 Filters 功能

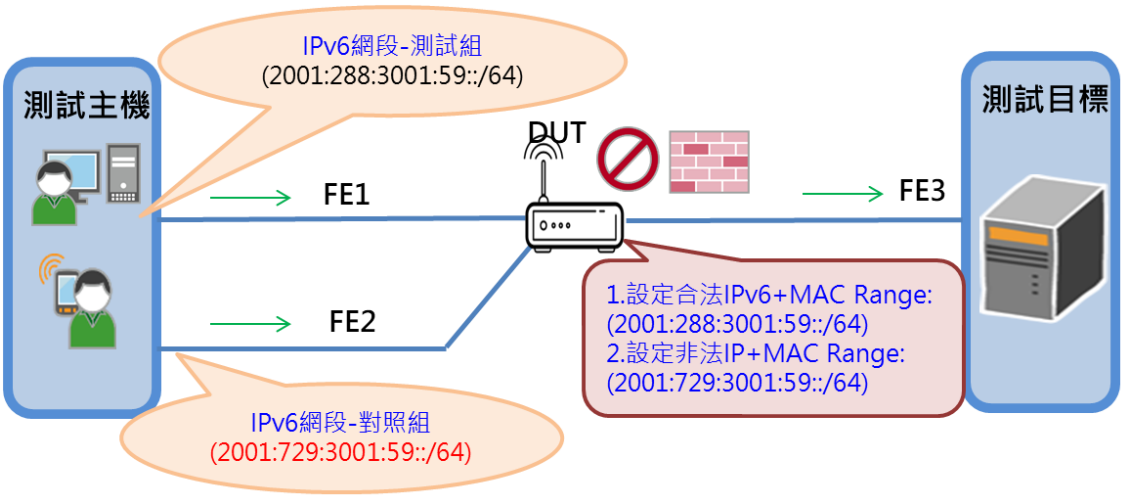
- 預設允許 Mobile IPv6
- Inbound Unsolicited Mobility Header 不符合 IPSec

security policy 需丟棄

- 預設允許與目前 Mobility Header 相關狀態記錄之 Flow

三、 家用寬頻分享器 CPE IPv6 ACL 功能測試

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。以 ACL 為例，針對 IPv6 的阻斷攻擊如 ICMP、RA flooding、IPv6 Extension Header 等攻擊情境，測試架構可參考圖 15，透過以下表範例流程針對家用 CPE 進行 IPv6 ACL 設定。



DUT : Device Under Test
FE : Fast Ethernet

圖 15 CPE IPv6 ACL 測試架構範例

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

表 10 CPE IPv6 ACL 網路安全防禦機制測試範例

步驟	測試內容
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

以 DLink 為例，針對 CPE IPv6 ACL 測試結果如圖 16 及圖

17 所示。原先 IPv6 用戶可透過寬頻分享器正常上網，啟用 ACL 功能後，驗證 ACL 是否能限制用戶終端 IPv6 連線，以 test-ipv6.com 網站為例，證明當 ACL 功能啟用後，被設定阻擋的主機確實無法取得 IPv6 位址，無法存取網站服務，ACL 功能正常。ACL 功能驗證如圖 17 所示。

圖 16 確認用戶 IPv6 上網正常（test-ipv6.com）

圖 17 IPv6 ACL 功能啟用與 test-ipv6.com 網站驗證

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)

四、 家用網路 IPv6 安全防護 Check List

家庭 IPv6 網路安全防護主要以 CPE 寬頻分享器為主。為建立 IPv6 資通安全防護之參考標準，可參考本計畫所制定的檢核清單如表 11 所示。

表 11 家用網路 IPv6 安全防護 Check List

項次	說明	備註
1	選擇具備 IPv6 防護功能(如 3-2 所描述之功能)之用戶設備 CPE	
2	使用安全的遠端存取 SSH(Secure Shell)機制和確保通信介面不使用預設密碼	
3	確認用戶設備 CPE IPv6 網路連線環境，檢測終端 IPv6 連線能力 ➢ http://ipv6-test.com/validate.php ➢ https://test-ipv6.com/	
4	確認用戶設備 CPE IPv6 位址分配規劃/配置方式，不使用 IPv6 之主機或用戶設備 CPE，可考慮關閉 IPv6 功能	
5	不使用 IPv6 之主機或網路設備，若不能關閉 IPv6 協定，須確實停用 SLAAC 機制	
6	用戶設備 CPE 必須能夠根據 IPv6 來源及目的位址來進行過濾(如 3-3)	
7	建議用戶設備 CPE 預設 ACL 需阻斷之特殊用途位址之 IPv6 訊務	
8	用戶設備 CPE 需過濾非合法用戶 IPv6 位址，限制可存取網段	
9	建議禁止使用 Tunnel 技術，(例如 IP Protocol 41、UDP 3544 teredo 等)	
10	強化個人端主機或網路設備 IPv6 資安防護(定期更新修補檔案及使用防毒軟體)	

第四節 企業 IPv6 資通安全防護研究

針對企業網路 IPv6 網路安全防護，本章主要分為企業網路安全議題與防護機制、企業網路 IPv6 資安防護建議以及基礎 IPv6 防護功能測試三個部分進行研討，如下圖 18 所示。

圖 18 企業用戶 IPv6 資通安全防護技術研究範疇

一、 企業網路 IPv6 安全議題與解決方案

(一) 引入 IPv6 可能引發的安全問題

針對 IPv6 可能引發的安全問題摘要說明如下：

- IPv4 與 IPv6 共存的架構可能存在新資安風險：由於 IPv6 與 IPv4 網路將會長期共存，網路必然會同時存在兩者的安全問題，或由此產生新的安全漏洞。目前已經發現從 IPv4 向 IPv6 轉移時出現的一些安全漏洞，例如駭客可以利用 IPv6 對同時具備 IPv4 和 IPv6 兩種協定的 LAN 網路進行非法接取，而惡意攻擊者亦可以通過安裝了雙

堆疊的 IPv6 主機，建立由 IPv6 到 IPv4 的隧道，繞過防火牆對 IPv4 網路進行攻擊。向 IPv6 協定轉移與採用其他任何一種新的網路協定一樣，其安全措施必須重新經過慎重的考慮和測試。

- IPv6 的網管設備和網管軟體仍待加強：IP 網路中許多不安全問題主要是管理造成的。IPv6 網路管理可借鏡 IPv4 的思維，但對於一些網管技術，如 SNMP 等，不管是移植還是另起爐灶，其安全性都必須從本質上有所提高。此外，企業網路的網管設備和網管軟體可支援 IPv6 仍然有限，亦缺乏對大範圍的 IPv6 網路故障定位和性能分析的機制。
- IPv6 的資安產品尚未成熟：IPv6 網路同樣需要防火牆、VPN、IDS、漏洞掃描、網路過濾、防止病毒閘道器等網路安全設備。事實上 IPv6 環境下的病毒已經出現，但這方面的安全技術研發還尚需時日。IPv6 防火牆需面對以下的一些挑戰： (A) 封包表頭的差異：在 IPv4 中並沒有擴充表頭，因此在設計 IPv6 防火牆時，需特別注意到擴充表頭，在做封包過濾時，要能辨識出含擴充表頭的封包。(B) End-to-End：網際網路最初的概念就是 End-to-End，

由於 IPv4 位址不足，因而破壞了這個架構， IPv6 解決了這個問題，而回歸到 End-to-End 的概念。但是防火牆需要做封包過濾與執行安全政策，又似乎必須剪斷 End-to-End，因此在設計 IPv6 防火牆時，就需要找出解決方法。(C) Mobility：在 IPv6 的行動能力應用上，一個外地的主機看起來都會是本地的，因此在做封包過濾時，需解決面對一個移動節點而不能把它當成外地主機的問題。(D)相對於 IPv4，IPSec 在 IPv6 是必須的功能。IPSec 是一個加密的通道，它允許任何使用者跳過安全性政策的檢查。因此在 IPv6 的環境中要使用 IPSec，就必須解決如何過濾在加密的通道中傳遞資訊的問題。 (E) Path MTU：IPv6 封包只在來源主機進行封包分割，它利用 ICMPv6 協定來找出 Path MTU，因此 IPv6 防火牆需要具備辨識和處理 ICMPv6 封包的能力。

- 其他新的安全挑戰：IPv6 協定仍需在實踐中持續做改進的動作，例如 IPv6 群播功能僅規定了簡單的認證功能，所以還難以實現嚴格的用戶限制功能，而移動 IPv6 亦存在很多新的安全挑戰。

IPv6 雖在網路保密性、完整性方面改進了 IPv4 的缺點，但

IPv6 不可能徹底解決所有安全問題，同時還會伴隨而產生新的安全問題。目前多數網路攻擊和威脅大都來自應用層而非 IP 層，因此，保護網路安全與資訊安全，只靠一兩項技術並不夠，還需配合多種手段，例如認證、IPsec、防火牆、訊務分流等方法可竟全功。

(二) IPv6 面對資安弱點的解決方案

針對 IPv6 可能引發的安全議題，以下就從 IPv6 的角度，摘要說明如何利用 IPv6 來解決上述的各種攻擊。

- 偵查：網路偵查在 IPv4 中很簡單，駭客可以使用 Ping sweep、Port scan、Application and vulnerability scan 輕易達到目的，但在 IPv6 的環境不同，由於一個 IPv6 子網的 IPv6 位址很多，通常為 2 的 64 次方，掃描起來相當費力，因而降低了被掃瞄的機會與意願。
- 非法接取：在 IPv4 網路環境下，通常會執行以下的動作來避免非法的存取:ACL on Border FW 以及 ACL on host FW。在 IPv6 網路環境下，基本上亦是利用相同的動作來避免非法的存取，在引進 IPv6 網路環境後，可進一步啟動 IPSec，對於 ACL 存取控制將有所助益。

- 表頭的篡改與數據封包的分片：在 IPv4 網路環境下，可能存在以下資安危機：(A)利用 fragmentation 來困惑或是 bypass router or FW 的 access control，(B)利用 overlapping data/header 來 bypass router or FW 的 access control，(C)利用 fragmentation 來癱瘓 IDS 等 security tools。引進 IPv6 網路環境後，RFC 標準規範在 IPv6 網路中 fragmentation 只能在終端執行，任何中間經過 fragmentation 的 packet 均可被視為攻擊發生而直接 drop，而 Overlapping fragments 在 IPv6 中是不被允許的。
- 第三層和四層資訊的欺騙：在 IPv4 網路環境下，可能存在以下資安危機: DOS、DDOS、spam、worm、virus attacks 等等。在 RFC 2827 規範建議應實現 ingress filtering 的功能，將欺騙的 L3 traffic 擋在它的源頭，但若駭客使用 subnet 內的 IP 位址，則仍有風險。此外，RFC 2827 對於 Layer 4 spoofing 的幫助並不大。引進 IPv6 網路環境後，由於 IPv6 位址具有 globally aggregated 的特性，此特性可讓 ISP 更容易實現 RFC 2827 filtering 的功能，使得整個欺騙的 L3 traffic 停留在客戶端而不會無限制的擴散。
- ARP 和 DHCP 攻擊：在 IPv4 網路環境下，可能存在以下

資安危機: (A) 駭客竄改 IP-MAC 之間的對應，使無辜的使用者與駭客對話，進而啟動 man-in-the-middle attack，(B) 駭客假冒 DHCP server，進而啟動 man-in-the-middle attack，(C) 駭客利用 flooding 攻擊，癱瘓合法的 DHCP server。引進 IPv6 網路環境後，由於 ARP 已被 ICMPv6 的 ND 所取代，所以 IPv4 網路環境下的 ARP 資安問題自然消失，但是 IPv6 的 ND 仍繼承了既有的 ARP 資安問題。IPSec 是一個可能的解決辦法，或是實現 RFC 3971 的 SEND (SEcuring Neighbor Discovery)亦可解決。

- 廣播放大攻擊：在 IPv4 網路環境下，可能存在以下資安危機：駭客利用 ICMP Echo 訊息、一個 subnet 的 broadcast destination 位址、一個假冒的 source 位址即可執行”smurf”攻擊。引進 IPv6 網路環境後， IP-directed broadcast 的動作已被移除，而若 IPv6 終端用戶實際實現 RFC2463，則”smurf”攻擊或其他類似的 Attacks 可被有效減緩。
- 路由攻擊：在 IPv4 網路環境下，一般使用 MD5 來保護 router 之間的 routing announcement information，引進 IPv6 網路環境後，可啟動 IPSec，對於預防 routing attack 有所助益。

- 偵聽：可以使用 IPSec 降低被竊取資料的機會。
- 應用層攻擊：Virus and Worm 均屬於此類，使用 IPSec 之後，相關的安全檢查與防護將落到 host 身上，因為 FW 看到的是加密過的資料。
- 中間人攻擊：可以使用 IPSec 降低被攻擊的機會，建議使用 IKE main mode。
- 泛洪：針對 Flooding，IPv6 並無新增之防護方法，建議沿用 IPv4 既有方法予以防範。

二、 設備 IPv6 安全防護建議

本節係針對資安設備，網路設備與主機摘要 IPv6 建議，期能作為企業網路部署與建置 IPv6 的參考。

(一) 資安設備

資安設備如防火牆，IDS，IPS 等均屬此類。茲摘要 IPv6 安全防護建議如下：

- 清查既有防火牆是否支援 IPv6，透過汰舊換新過程逐步更換。
- 取得支援 IPv6 的能力如以韌體升級方式支援 IPv6，須

注意檢查 CPU 負載及記憶體的消耗狀況，避免效能不足防火牆。

- 支援 IPv6 後可參考 IPv4 規則設定 IPv6 的過濾方式(ACL)，再依據觀測的 IPv6 流量資訊，逐步完善 IPv6 的防禦規則。過濾政策 Checklist 可參考附錄。

另針對流量與紀錄 Log 部分:

- 可依服務類別/個人使用統計流量：Inbound、Outbound、FTP 連線、SSH 連線、網路芳鄰、遠端桌面連線、遠端程序呼叫、Proxy、Mail、ICMP 等進行統計。
- OS 如本身可正常支援 IPv6，則 System Log 一般均可正常顯示；AP Log 則需視 AP 對 IPv6 支援度而定，建議先行測試。

(二) 網路設備

網路設備係以路由器與交換器為主，在路由器部分，IPv6 防護建議如下：

- 對外建議使用/127 點對點連線。
- 僅允許正面表列的訊務流量通過，其餘禁止。
- 關閉發送 RA。

- 過濾非必要之 ICMPv6 訊息，只處理合法網段訊務轉送。
- 依據 scope 範圍過濾群播封包。
- 禁止 Routing Header Type 0(RH0)與未知 IPv6 延伸表頭。
- 啟動 unicast Reverse Path Forwarding (uRPF) 。
- 啟動 Secure Neighbor Discovery (SEND) 。
- 停用 IPv6 轉移機制，如 6to4, ISATAP, Configured Tunnel 等。

針對交換器部分，建議是以 IPv6 First Hop Security 為主，設備本身須可支援 RA guard，DHCP guard，IPv6 Snooping，Source/Prefix Guard 以及 Destination Guard 等基本 IPv6 防護功能。

(三) 伺服器與終端設備

在伺服器部分，IPv6 安全防護建議如下：

- 部署入侵偵測系統來監督 Link-local 的流量，監督一些可疑流量型態的門檻值(threshold)。
- 強化主機系統及應用程式本身之安全。
- 定期做作業系統之 patch、安裝主機型/網路型的入侵偵測系統、主機型防火牆及防毒軟體等。

- 停用 IPv6 轉移機制，如 6to4, ISATAP, Configured Tunnel 等。
- 主動監測 IPv6 資安防護狀態，偵測到異常攻擊儘快通報

針對 IPv6 終端主機部分，建議如下：

- 避免將每個用戶的 IP 位址指定成連續的 IP 位址，應該儘量分散其 IP 的指定，及使用隨機產生的位址前綴。
- 使用私有擴展位址（Privacy extensions），來達到防禦外部對內進行偵蒐攻擊的目的。
- 使用代理伺服器，如 HTTP Proxy，以避免 Web 客戶端的 IP 被 Cache，或使用暫時的 Privacy Address。
- 所有電腦支援 IPv6 與 host-based 防火牆。
- 強化主機系統及應用程式本身之安全，如定期做作業系統之 patch、安裝主機型的入侵偵測系統、主機型防火牆及防毒軟體等。
- 建議使用 IPSec AH 來作為兩端連線的相互認證。
- 停用 IPv6 轉移機制，如 6to4, ISATAP, Configured Tunnel 等。
- 主動監測資安防護狀態，偵測到異常攻擊儘快通報。

- 定期做作業系統之 patch、安裝主機型/網路型的入侵偵測系統、主機型防火牆及防毒軟體等。
- 停用 IPv6 轉移機制，如 6to4, ISATAP, Configured Tunnel 等。

三、 企業網路設備基礎 IPv6 防護機制測試

針對企業網路基礎 IPv6 測試結果摘要如下 ：

(一) 企業網路 IPv6 測試架構

企業用戶經由企業內架設的交換機、防火牆、路由器再透過 ISP(Internet Service Provider)所提供的 Hinet 光世代網路連接至外部網路。

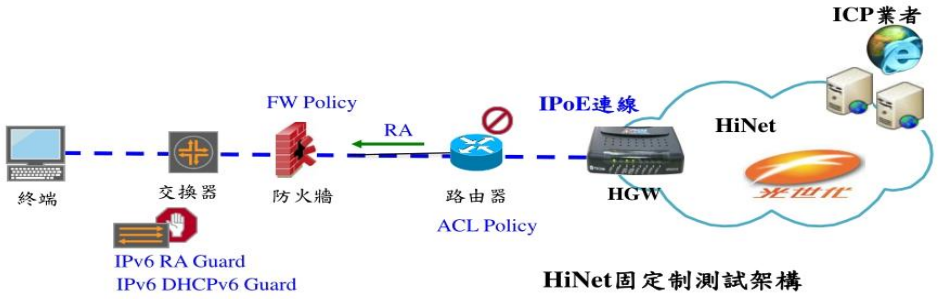


圖 19 企業網路測試架構

(二) 企業網路 IPv6 設備安全防護功能測試

甲、 交換機

(1) IPv6 Router Advertisement Guard

為了避免 IPv6 host 收到偽造的 RA 訊息，設定非正確的 default gateway 等，或攻擊者發出大量 RA 訊息使 Client 無法處理合法的訊息，Switch 設定 IPv6 RA Guard 將從非信任的來源收到的 RA Message 丟棄。

- 上方的圖為測試架構，下方的左右兩張圖皆為被攻擊的 host 的網路資訊。
- 左下的圖為尚未使用 RA Guard，使用紅色表示受害

主機收到 3333:3333:3333:3333 作為前綴，作為攻擊者主機所送出的偽造 RA。使用綠色表示受害主機實際上收到的正確 RA，設有正確的前綴。

- 右下方的圖為已使用 RA Guard，受害主機的網路資訊為正確的，並且於圖的下方附上交換機 log 的資訊，顯示交換機 FastEthernet 2 port 的 Message 被 RA Guard 丟棄。

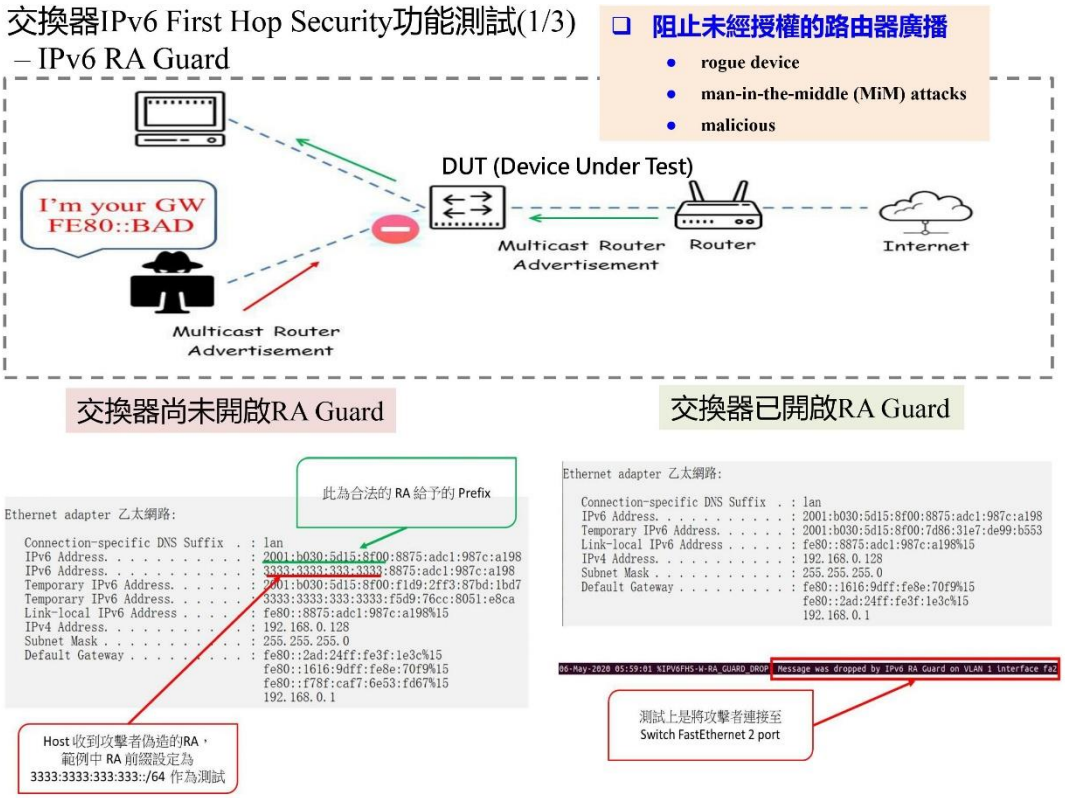


圖 20 交換機 IPv6 RA Guard 測試

(2) IPv6 DHCPv6 Guard

Switch 啟用 DHCPv6 Guard 避免 Rogue DHCP Server 向 Client 發送偽造的 DHCP Offer，使 Client 設定非正確的網路參數。

- 上方的圖為測試架構，下方的圖為交換機 log 資訊的截圖，圖中內容為攻擊者所連接至的 FastEthernet 2 port 的訊息被交換機的 IPv6 DHCP Guard 丟棄。

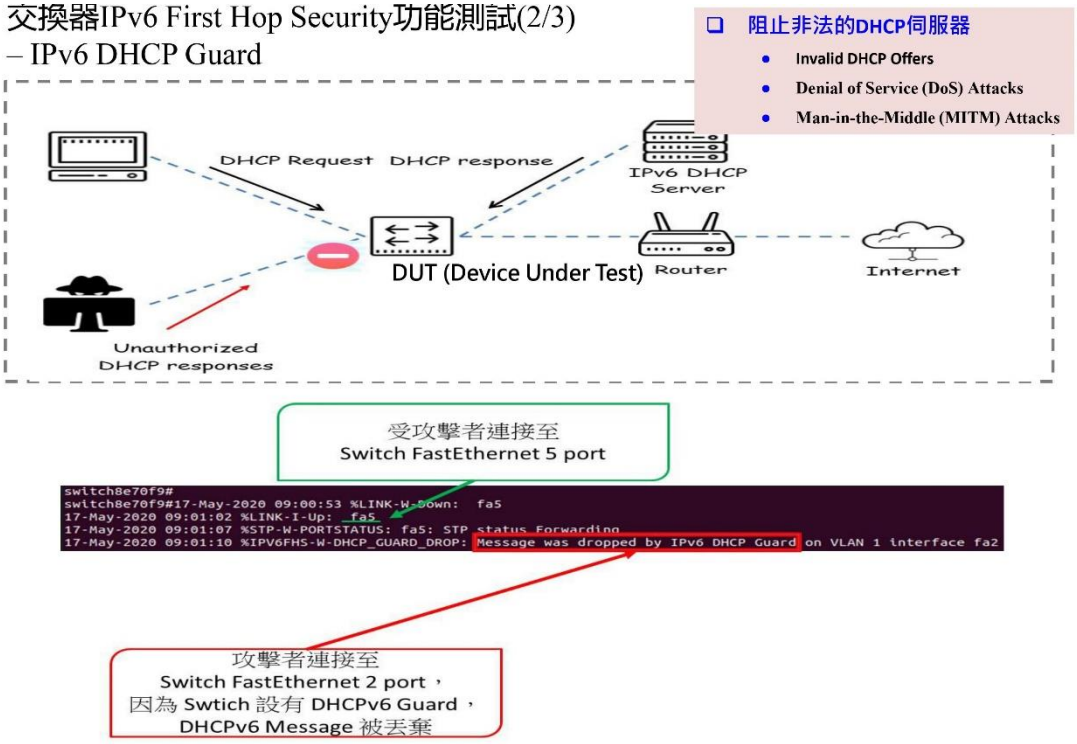


圖 21 交換機 IPv6 DHCP Guard 測試

(3) IPv6 Source Guard

Switch 設定 IPv6 Source Guard，避免惡意使用者偽造某個 host 的 IPv6 位址，Swtich 會比對 binding table 來檢查是否已經有別的 port 已經跟該 IPv6 地址綁定了。

- 上方的圖為測試架構，下方的圖為交換機 log 資訊的截圖，圖中內容為交換機 binding table 的資訊，綠色的部分表示為受害者已經連接至 FastEthertnet 2 Port，並且紅色為攻擊者因為偽造受害者的 IPv6 地址，因為 Switch 中的 binding table 攻擊者想偽造的 IPv6 地址已經綁定在其他 port 上，使得攻擊者的訊息被交換機 Source Guard 丟棄。

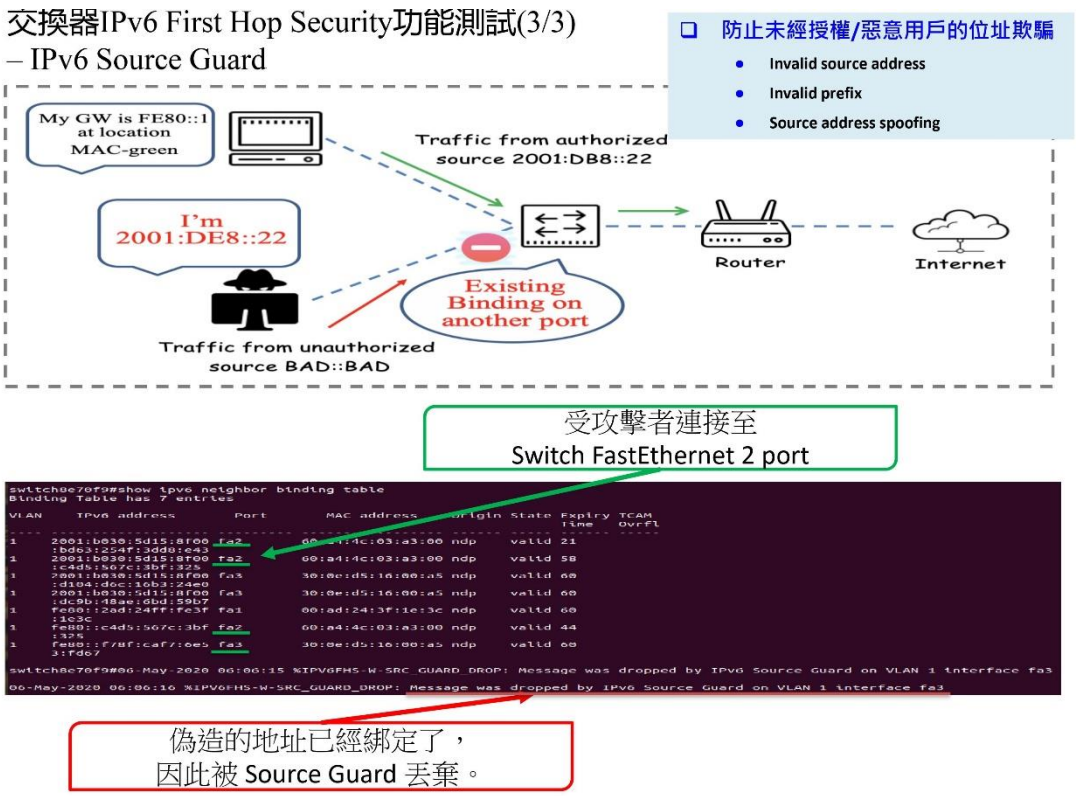


圖 22 交換機 IPv6 Source Guard

乙、 防火牆

防火牆 SSG5 IPv6 功能測試如下圖所示。

- Juniper Networks® SSG5 安全服務閘道器為高效能安全平台，適用於小型分支機構與獨立企業

測試項目	結果說明
IPv6 Address Scope	可阻擋IPv6 invalid source address
Extension Header	不管封包正確性，一率forward
Rogue RA	無法測試Rogue RA
Application	無法指定TCP/UDP port，只能使用預設port的application

	SSG5 Base/Extended
最高效能與容量 (2)	
已測試之 ScreenOS 版本	ScreenOS 6.2
防火牆效能 (大型封包)	160 Mbps
防火牆效能 (IMIX)(3)	90 Mbps
每秒防火牆封包 (64 byte)	30,000 PPS
AES256+SHA-1 VPN 效能	40 Mbps
3DES+SHA-1 VPN 效能	40 Mbps
同時連線數	8,000/16,000
每秒新連線數	2,800
最大政策數	200
最大用戶數	無限制

- RFC標準、FW支援能力及防護設定之間仍可能存在差異，網管者需了解此差異，以評估是否需採取額外措施

圖 23 Junipter SSG5 測試項目

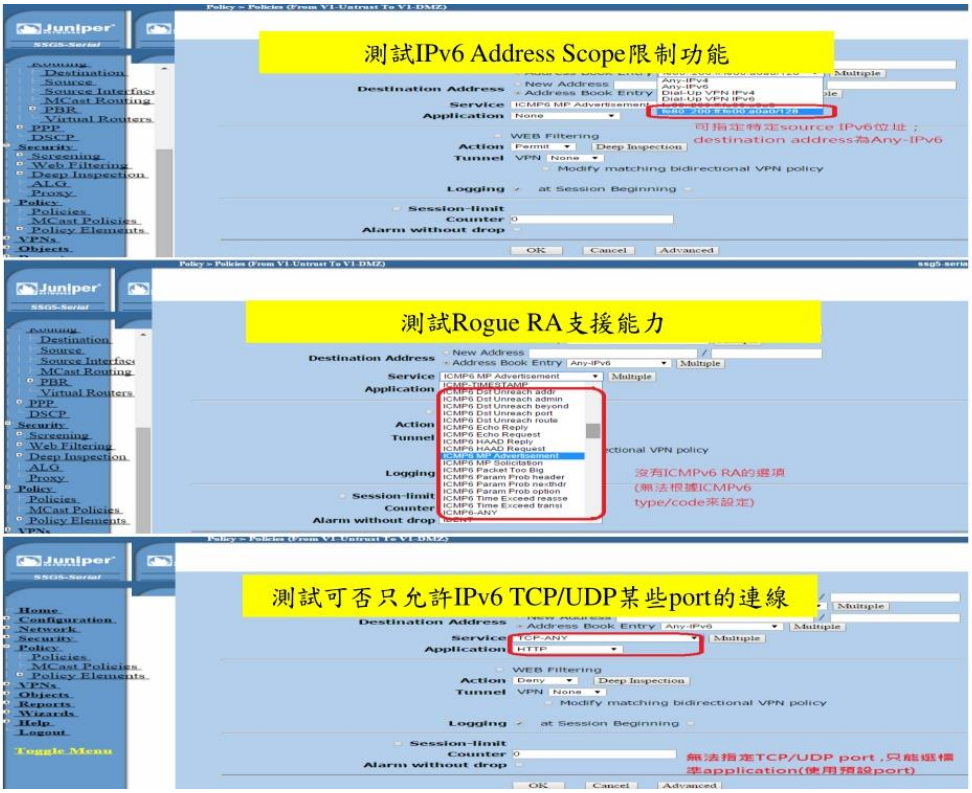


圖 24 Juniper SSG5 設定圖

丙、　路由器

路由器 ACL (Access Control List) 測試如下。首先，路由器尚未設定 ACL，測試的目標主機為 Public Google DNS 位址，可以 ping 到目標主機（圖 25）。

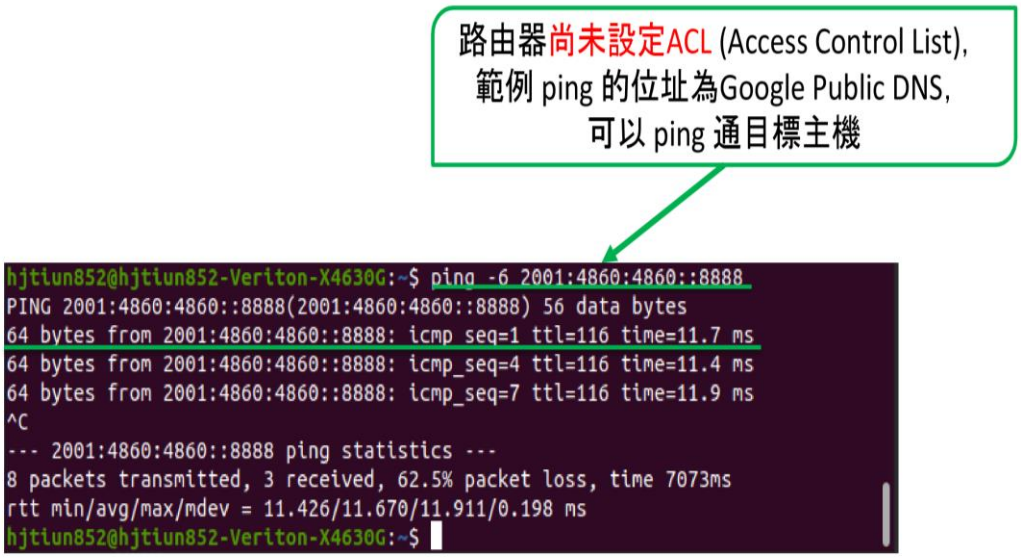


圖 25　路由器尚未設定 ACL 畫面

而圖 26 則為路由器已設定 ACL 畫面，測試的目標主機一樣為 Public Google DNS 位址，無法 ping 到目標主機。

圖 26 路由器已設定 ACL 畫面

四、 企業網路導入 IPv6 安全防護 Check List

有關 IPv6 網路安全部署與規劃，建議可參考 RFC 4942[17]與 Cisco B.C.P 文件[18]制訂整體 IPv6 網路安全防護策略（IPv6 ACL 的原則）。以下提供企業網路對外啟動 IPv6 連線基本的檢核清單，期能提供企業網路 IPv6 安全佈署之指引參考。

表 12 企業網路 IPv6 安全防護 Check List

項次	說明	備註
1	研擬企業網路 IPv6 資安工作計畫。制定 IPv6 安全策略、盤點設備/系統 IPv6 支援能力、建立 IPv6 安全管理制度以及加強 IPv6 網路安全教育訓練等	
2	避免企業外部電腦設備直接存取企業內部的網路主機或設備	
3	防火牆設備必須能完整支援 IPv6	
4	重要資訊系統建議採用固定 IPv6 位址並考慮使用加密認證機制(IPsec 或是其他類似機制)	
5	管理者需使用安全的遠端存取 SSH(Secure Shell)機制和確保本通信介面不使用預設密碼	
6	強制使用 FQDN 與 DNS 定址，本地端使用者建議使用固定 IPv6 位址或採 DHCPv6 方式	
7	決定有效的 ICMP 封包過濾執行及 RFC 4890 所建議之封包篩選規定	
8	採用 IPv6 unicast reverse path forwarding 來拒絕所有不明來源位址的封包	

項次	說明	備註
9	阻止一切來自於不安全 IPv6 網路來源位址的訊務流量	
10	檢查 Outbound traffic 以及目的位址回應的匹配條件，檢測用戶是否有無意間夾帶任何殭屍網路流量或者惡意訊務	
11	攔截所有 Inbound SSL/TLS IPv6 訊務流量，並進行必要的檢查	
12	通過 IPS 的訊務需進行網路傳輸速率的限制，以避免網路設備流量超載	
13	路由協定如 OSPFv3、RIPng、BGP and IS-IS 應使用加密認證機制加強保護	
14	建議禁止使用 Tunnel 技術，(例如 IP Protocol 41、UDP 3544 teredo 等)	
15	建議啟動 First Hop Security 機制確保 IPv6 用戶接取網路安全	

第三章 結論與建議

第一節 結論說明

未來 IPv6 網路的發展方向將朝向 Native IPv6 方面演進，因此如何在 IPv4 與 IPv6 共存下連線成為一門重要課題。本計畫主要建置一套 Native IPv6 連網試驗環境及進行 Native IPv6 網路環境測試，同時並研析 IPv6 資通安全防護相關議題與防禦機制，提供我國 ISP 與企業/家庭用戶 IPv6 部署參考。報告結論摘要重點如下：

一、 Native IPv6 連網試驗環境規劃

完成 NAT64/DNS64 暨 464XLAT IPv6 連網環境規劃，以校園網路作為 IPv4 與 IPv6 接取環境，規劃利用 JOOL 及 BIND 9 開源軟體建置 NAT64/DNS64 及 464XLAT 轉換服務連線架構，可提供 IPv6 -> NAT64 -> IPv4 以及 IPv4 -> CLAT -> IPv6 -> PLAT -> IPv44 兩種連線情境。另針對測試規劃部分，針對網站與應用服務規劃連網、連線以及應用三種測試項目，可作為營運商評估 NAT64/DNS64 及 464XLAT 轉換服務實用性的參考依據。

二、 Native IPv6 連網環境建置與測試

完成 NAT64 / 464XLAT 連網環境建置與功能測試，可作為實際驗證 IPv6 用戶連線網站與應用服務的測試場域。

三、 IPv6 家用資通安全防護技術研究

完成家用網路 IPv6 資通安全防護技術手冊，探討家庭 IPv6 網路常見 IPv6 安全議題與解決方案，依據 RFC6092 標準針對家用寬頻分享器 IPv6 資安防護提出摘要建議。此外，為驗證家用分享器 IPv6 基本防護功能，本計劃亦針對市售 DLink 寬頻分享器進行 IPv6 ACL 功能實測，可提供家用 IPv6 基礎安全防護的參考。

四、 企業網路 IPv6 資通安全防護技術研究

完成企業網路 IPv6 資通安全防護技術手冊，探討企業網路導入 IPv6 安全議題與解決方案，並針對網路設備與主機 IPv6 資安防護提出摘要建議並針對企業網路設備基礎 IPv6 防護機制進行測試。此外，為強化企業網路 IPv6 安全，本計劃亦針對企業網路導入 IPv6 安全防護需求提出檢核清單，可作為企業網路部署 IPv6 安全管理之參考。

第二節 建議事項

兼顧實務、保障品質、降低成本、網路演進是 IPv6 網路部署的四大基本原則。發展基於 IPv6 的網際網路，不僅是網際網路演進升級 IPv6 的必然趨勢，更是助力物聯網與 ICT 產業經濟融合發展、支撐 IPv6 網路創新應用的基礎，對於提升國家競爭力、加快網路 IPv6 部署演進具有重要意義。然而，IPv6 是屬於長期演進的技術，其 IPv6/IPv4 雙協定網路過渡共存期間，將無可避免引發安全議題。企業或 ISP 在佈署 IPv6 的同時也應思考，IPv6 對於既有企業網路或 ISP 網路管理的影響，如何即時因應 IPv6 網路安全攻擊事件，應該是未來 IPv6 網路安全管理的主軸。本研究主要探討 IPv6 網路安全相關問題與影響，並研究家用/企業 IPv6 網路資通安全防護技術，並能依據 IPv6 網路安全防護檢核清單建議進行家用/企業網路導入 IPv6 的安全性佈署。

相關建議事項如下：

一、針對 Native IPv6 演進部署，建議 IPv4 only 的網路內容服務業者可採 NAT64/DNS64 方案部署，解決 Native IPv6 用戶連網的問題；新興業者或 IPv4 不足之網路營運商則建議可採 464XLAT 方

案部署，使裝置及應用程式的運作維持透通性，用戶端應用 APP 無須升級 IPv6，可降低對用戶可能的影響。

二、應建立資訊系統導入 Native IPv6 標準作業流程與規範，提供 ISP/ASP 以及企業網路新建資訊系統導入 IPv6 的參考依據，使得建構在 Native IPv6 網路環境上的資訊系統得以具備更完備的 IPv6 參考規範。

三、網通廠商新上市之家用寬頻分享器 CPE 設備出廠即預設啟動 IPv4/IPv6 雙協定服務模式，並建議預設阻斷應限制之 IPv6 位址。

四、建議企業應及早進行 IPv6 資安防護規劃及在商用網路大規模實際演練，加強實戰經驗，確保 IPv6 上網安全。

五、建議應針對企業網路相關資訊系統與設備建立 IPv6 相關網路安全檢測機制或方法，透過檢核機制有效提昇企業佈署 IPv6 的安全性。

六、建議應持續推動 Native IPv6 網路發展與技術演進，簡化網路維運管理，強化 IPv6 網路安全，奠定未來 5G 和物聯網 Native IPv6 網路應用發展基礎。

第四章 參考資料來源

[1] Google IPv6 成長預測網站, Available: https://www.vyncke.org/ipv6status/project.php

[2] Google IPv6 國家排名網站, Available: https://www.aelius.com/njh/google-ipv6/

[3] The Internet Engineering Task Force Website, http://www.ietf.org/

[4] IETF RFC 2766, Network Address Translation - Protocol Translation （NAT-PT）, Available: https://tools.ietf.org/html/rfc2766

[5] IETF RFC 6416, Stateful NAT64: Network Address and Protocol Translationfrom IPv6 Clients to IPv4 Servers, Available: https://tools.ietf.org/html/rfc6416

[6] IETF RFC 6174, DNS64: DNS Extensions for Network Address Translationfrom IPv6 Clients to IPv4 Servers, Available: https://tools.ietf.org/html/rfc6174

[7] IETF RFC 7381, Enterprise IPv6 Deployment Guidelines, Available: https://tools.ietf.org/html/rfc7381

[8] 美國網際網路服務供應商（ISP）之 IPv6 發展現況(T-mobile), Available: https://www.facebook.com/notes/ip-dns-%E8%AB%96%E5%A3%87/%E7%BE%8E%E5%9C%8B%E7%B6%B2%E9%9A%9B%E7%B6%B2%E8%B7%AF%E6%9C%8D%E5%8B%99%E4%BE%9B%E6%87%89%E5%95%86isp%E4%B9%8Bipv6%E7%99%BC%E5%B1%95%E7%8F%BE%E6%B3%81t-mobile/1539560302731185/

[9]《完成向IPv6過渡》備忘錄，Available:https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-07.pdf

[10] IETF RFC 4057, IPv6 Enterprise Network Scenarios, Available: https://tools.ietf.org/html/rfc4057

[11] IETF RFC 6092, Recommended Simple Security Capabilities in Customer Premises Equipment （CPE） for Providing Residential IPv6 Internet Service, Available: https://tools.ietf.org/html/rfc6092

[12] JOOL, https://www.jool.mx/en/index.html

[13] BIND9, https://www.isc.org/bind/

[14] JOOL Wiki, https://zh.wikipedia.org/wiki/NAT64

[15] IETF RFC 2765, Stateless IP/ICMP Translation Algorithm （SIIT）, Available: https://tools.ietf.org/html/rfc2765

[16] IETF RFC 6877, 464XLAT: Combination of Stateful and Stateless Translation, Available: https://tools.ietf.org/html/rfc6877

[17] IETF RFC 4942, IPv6 Transition/Coexistence Security Considerations, Available: https://tools.ietf.org/html/rfc4942

[18] Cisco IPv6 Access Control Lists, Available: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration/xe-3s/sec-data-acl-xe-3s-book/ip6-acls-xe.html