『推動 IPv4/IPv6 雙軌普行方案』

附錄七
『ICP IPv4/IPv6 平台架構雙協定升級之網路安全防護差異解析及升級實際測試』

108 年委託研究報告

108 年度「ICP IPv4/IPv6 平台架構雙協定升級之網路安全防護差異解析及升級實際測試」
期末報告

計畫委託機關：台灣網路資訊中心

中華民國 108 年 10 月

108 年委託研究報告

108 年度「ICP IPv4/IPv6 平台架構雙協定升級之網路安全防護差異解析及升級實際測試」

受委託單位

奇加互動股份有限公司

計畫主持人

林韋廷

研究人員

曾榮信、郭愷瀚、鄧丕文、金沅禹、張智崴、童冠瑜、吳奎億

研究期程：中華民國 108 年 4 月至 108 年 12 月

研究經費：新臺幣 77 萬元

中華民國 108 年 10 月

目　　次

表　次

圖　　次

提　　要

關鍵詞：網際網路、IPv4、IPv6、雙軌(Dual stack)

一、　研究緣起

數位經濟為我國目前政策之關鍵重點，為有效推動我國數位經濟發展，行政院公布「數位國家·創新經濟發展方案」政策，因應數位創新帶來之超寬頻基礎建設與資通科技發展，帶來新型態數位經濟之崛起，並從國家角度預作規劃與整備。

「數位國家·創新經濟發展方案」的發展重點之一為「數位創新基礎環境行動計畫」。本項政策目標是希望推動我國基礎建設發展，提升國家競爭力。其中，推動我國 IPv4/IPv6 雙軌普行使用是當前數位時代基礎建設中很重要的一個環節。

全球提供 IPv6 連網服務趨勢近年來轉趨明顯，導入 IPv6 服務有其必要性，其原因說明如下：

1. 全球 IPv4 位址已經發放完畢，網際網路接取服務經營者（Internet Access Service Provider；IASP）難以取得新的 IPv4 位址，為維持既有服務，導入 IPv6 是必然的選擇。
2. 導入 IPv6 可減少網路位址轉譯（Network Address Translation，縮寫 NAT）設備的投資，及減少使用 NAT 技術所產生的效能及維運障礙問題。

3. 行動電信業者對 IP 位址需求大增。

4. 開拓物聯網(IoT)創新業務需求。

5. 內容網站透過 IPv6 遞送比例逐年增加，反應出支援 IPv6 已經是世界潮流。

6. 網際網路工程任務組（Internet Engineering Task Force，縮寫：IETF）已經達成未來之新標準（RFC）皆以 IPv6 為適用平台之共識，IPv6 已經成為未來技術主流與網路的根基。

因應國際 IPv6 發展潮流，世界各國皆在推動及發展 IPv6，將藉由推動及完善國內 IPv6 網路環境及使用，建設台灣成為優質網路化社會的典範國家，並因應未來各項通訊傳播網路匯流科技發展之趨勢，創造台灣在國際資通訊科技競爭局勢中繼續領先之優勢。

本計畫希望透過分析 IPv4 及 IPv6 網路雙協定平台在安全架構設計上的差異，幫助 ICP 業者建立 IPv4/IPv6 平台架構雙協定網路安全防護檢查項目清單，使業者能快速完成基礎檢測項目，降低 ICP 業者支援 IPv6 的阻力。除此之外本計畫將輔導 ICP 業者進行升級規劃、實際測試和導入，並記錄導入過程以及解決的問題，做成升級實際案例供相關業者參考。

本案執行範圍包括：

1. 研析 ICP IPv4/IPv6 升級及網路安全防護差異

2. 建立 ICP IPv4/IPv6 平台架構雙協定網路安全防護檢查項目清單

3. 輔導 2 家 ICP 業者升級 IPv4/IPv6 雙軌網路服務

二、 研究方法及過程

國內 ICP 業者在支援 IPv6 上，因缺乏相關技術及人才，因此投入意願不高。為推展 ICP 業者提供 IPv6 網路服務，本計劃透過 ICP IPv4/IPv6 平台架構雙協定網路安全防護差異解析及升級測試，解析 ICP 升級支援 IPv4/IPv6 軟硬體設定防護資訊，並以實際輔導 ICP 業者做網站升級驗證案例。

三、 重要發現

（一）台灣固網的 IaaS 基礎設施即服務（Infrastructure as a Service，簡稱 IaaS）的第一代跟第二代都不支援 IPv6，導致將網站放置在台灣固網 IaaS 的網站都無法支援 IPv6。由於網站從現有的 IaaS 轉移到其他電信業 IaaS 的困難度跟作業成本太高，轉移期間也會導致服務中斷，因此這類需要轉移 IaaS 的 ICP 業者不願意轉移，造成網站也無法支援 IPv6。

（二）SHOPLINE 是目前國內大多數 ICP 背後使用的購物平台，不過 SHOPLINE 本身並不支援 IPv6，因此 ICP 若使用 SHOPLINE 提供購物服務者，將無法支援 IPv6。變成 ICP 的官網有支援

IPv6，但是當使用者點擊購物時，會被帶到 SHOPLINE 平台(網址已經變更)，此時卻不支援 IPv6。這種大型電子商務平台未來如果可以導入 IPv6，將讓所有使用 SHOPLINE 的 ICP 業者受益。

（三）ICP 業者導入的複雜度與其使用的機房是否有足夠的 IPv6 知識有關，若機房人員無 IPv6 知識甚至沒聽過 IPv6，則實際準備導入時，會因為 IT 人員對 IPv6 的反對，導致 IPv6 導入失敗。

四、 主要建議事項

觀察國際 IPv6 發展趨勢，從去年開始亞洲區除了我國之外，越南、馬來西亞及泰國等國家也積極努力推廣，讓 IPv6 連網比例大幅成長，可見支援 IPv6 已經是國際共識。國內部分則經多年的努力，近年來成長驚人，以此基礎持續推動 IPv6 普及，並且讓更多網站支援 IPv6 變得相當重要，根據目前計畫執行狀況的建議如下：

（一） 立即可行之建議

1. 推動 IASP 各種服務支援

根據輔導經驗，許多網站為節省硬體採購成本、解決技術人才難找與降低人力與設備維護成本，許多 ICP 選擇使用 IASP 提供的 IaaS 架構下建立網站。因此 IASP 業者是否支援

IPv6 也決定了 ICP 業者是否能使用 IPv6。持續積極推動 IASP 業者各項服務支援 IPv6，對提升國內 ICP 業者支援 IPv6 使用率有相當助益。

2. 手機預設開啟支援 IPv6

ICP 業者會擔心投入資源升級網站支援 IPv6，但使用率卻不高的問題。因此如果國內行動網路服務業者都能全部支援 IPv6，在此基礎上推動手機業者能開啟預設支援 IPv6，以提高 IPv6 使用率。

3. 獎勵積極參與 IPv6 升級的 ICP 業者

ICP 業者目前對於 IPv6 的導入大都處於觀望階段，但是如果能夠有新聞曝光，也是吸引 ICP 業者投入 IPv6 的誘因。因此建議發布新聞稿，並公布每年有哪些台灣 ICP 業者導入 IPv6，獎勵 ICP 主動升級 IPv6。

（二） 中長期性建議

1. 固網業者支援 IPv6

對台灣 ISP 業者現有機房內設備全面進行 IPv6 檢測，對於不支援 IPv6 的設備，應要求期限內汰換升級。要求所有在台灣提供雲端主機服務的電信業者都須支援 IPv4/IPv6 雙軌並行服務，並自動配發 IPv6 位址給網站業者。對台灣 ISP 業

者現有機房內設備全面進行 IPv6 檢測，對於不支援 IPv6 的設備，應要求期限內汰換升級。

2. 人員認證

要求台灣 IASP 機房的 IT 人員都需要通過 IPv6 考試認證。

3. 推動 ICP 支援 IPv4/IPv6 雙軌服務

ICP 業者願意配合輔導做 IPv4/IPv6 雙軌服務升級，大多希望有媒體曝光機會，建議提供媒體曝光機會。另外也可考慮建立 ICP IPv4/IPv6 認證標章，對於有支援的台灣 ICP 業者，給予認證標章。

4. 政府公開招標要求符合 IPv6

建議政府公開招標的網站或 APP 將支援 IPv6 列為驗收的必要項目。而投標的廠商的自己的網站也需要支援 IPv6 才可以投標，用以推動 IPv6 的發展。

5. ICP IPv4/IPv6 升級及網路安全防護差異

台灣缺乏 IPv6 推廣文章，應該撰寫 IPv6 推廣及介紹文章，從概念、實作、創意、安全等各種角度切入，教育更多的網路用戶，有助於日後 IPv6 的應用普及與發展。建議可以成立一個 IPv6 推廣網站，將國外授權的 IPv6 文章翻譯成中文之後推廣。

6. 建立 ICP IPv4/IPv6 平台架構雙協定網路安全防護檢查項目清單

建議將檢查清單放置在網站上，並提供 Wiki 方式供各家廠商增添修改檢查清單的項目，保持資料的正確性。或者直接在 Wiki 維基百科上申請中文項目的 ICP IPv4/IPv6 檢查清單，確保資料可保持更新。

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

台灣政府單位大都已經完成 IPv6 導入,但台灣民眾日常使用的一般網站尚未積極支援 IPv6,原因可能是人力不足、資訊不足、環境不支援等因素。

ICP 業者導入 IPv6 會衍生的問題包括架構上的差異、新衍生的資訊安全問題、新衍生的管理問題。藉由本計畫，將整理相關資料，供 ICP 業者在導入過程的參考資訊。

二、　計畫動機與主題

以 Alexa 台灣的流量分佈，主要網路流量是民間公司成立的網站，包括新聞媒體網站、社群網路、部落格網站、遊戲網站、電子商務網站等，這些佔台灣最多使用流量的網站，如果可以導入 IPv6，將有助於 IPv6 在台灣的推廣成果並加速產生各種基於 IPv6 而衍生的新服務與技術，從而誕生新的商業模式、產業升級。本計畫希望透過分析 IPv4 及 IPv6 網路雙協定平台在安全架構設計上的差異，幫助 ICP 業者建立 IPv4/IPv6 平台架構雙協定網路安全防護檢查項目清單，使

業者能快速完成基礎檢測項目，降低 ICP 業者支援 IPv6 的阻力。除此之外本計畫將實際輔導兩家 ICP 業者支援 IPv6。

三、　工作架構與施行方法

在「升級及網路安全防護差異」及「平台架構雙協定網路安全防護檢查項目清單」部分皆以收集資料、整理、分析、歸納跟驗證等方式進行。對於「輔導 ICP 業者升級 IPv4/IPv6 雙軌網路服務」部分，則須綜合盤點包括以下項目：

1. 機房支援程度
2. 網路環境支援程度
3. 技術人員能力與支援度
4. ICP 業者決策者對於導入 IPv6 的支持度與利益考量
5. 設備汰舊換新
6. 支援 IPv6 而導致的網路安全變化。

盤點之後與 ICP 業者共同討論解決方法。

四、　預期成果

（一）研析 ICP IPv4/IPv6 升級及網路安全防護差異

說明當網站導入 IPv6 時，如何避免因使用 IPv6 而衍生出新的安全跟隱私漏洞問題，本報告將針對 IPv4 與 IPv6 在網路安全

防護的差異進行說明，並針對網站因導入 IPv6 所衍生新問題進行歸納與整理。

（二） 建立 ICP IPv4/IPv6 平台架構雙協定網路安全防護檢查項目清單，範圍包括：

1. ICP 業者的 IPv6 設定檢測表
2. ICP 業者的網路安全檢查表

（三） 輔導 2 家 ICP 業者升級 IPv4/IPv6 雙軌網路服務

1. 提供輔導手冊供 ICP 業者參考

第二節 與計畫符合情形

一、 目標達成狀況

依照計畫內容將工作項目涵蓋以下項目：

1. 研析 ICP IPv4/IPv6 升級及網路安全防護差異
2. 建立 ICP IPv4/IPv6 平台架構雙協定網路安全防護檢查項目清單
3. 輔導 2 家 ICP 業者升級 IPv4/IPv6 雙軌網路服務

各項工作執行進度如下表所示：

研析 ICP IPv4/IPv6 升級及網路安全防護差異各項工作執行進度

	工作項目	開始日期	完成日期	進度
研析 ICP IPv4/IPv6 升級及網路安全防護差異				
1.1	通訊協定資料收集	2019/4/26	2019/5/31	100%
1.2	網路環境資訊收集	2019/5/8	2019/6/11	100%
1.3	網站資訊收集	2019/5/22	2019/6/21	100%
1.4	資安軟硬體資訊收集	2019/6/4	2019/7/11	100%
1.5	安全策略資訊收集	2019/6/17	2019/7/29	100%
1.6	資訊整理/歸納/分析/彙整/驗證	2019/6/7	2019/7/29	100%
1.7	網路環境(包括網路架構、網管、軟體升級、硬體升級)差異化比較	2019/6/4	2019/7/3	100%

1.8	伺服器(包括作業系統、網站伺服器、程式、資料庫、硬體升級)差異化比較	2019/6/6	2019/7/16	100%
1.9	資安設備(包括資安策略、資安規劃、防火牆、IDS 或者其他與資安有關之軟體或硬體的升級步驟)差異化比較	2019/6/18	2019/7/29	100%
1.10	資安防護(包括實作上的差異、內部控管、外部控管、策略)差異化比較	2019/7/4	2019/8/13	100%

建立 ICP IPv4/IPv6 平台架構雙協定網路安全防護檢查項目清單各項工作執行進度

	工作項目	開始日期	完成日期	進度
建立 ICP IPv4/IPv6 平台架構雙協定網路安全防護檢查項目清單				
2.1	資料收集/分析/歸納/整理	2019/4/26	2019/5/29	100%
2.2	網路環境升級檢查清單表	2019/5/16	2019/6/20	100%
2.3	作業系統及網站伺服器檢查清單表	2019/5/29	2019/7/8	100%
2.4	資訊安全設備(包括防火牆、入侵偵測系統、稽核系統)的檢查清單表	2019/6/18	2019/7/25	100%
2.5	檢查清單建立	2019/5/17	2019/7/2	100%

輔導 2 家 ICP 業者升級 IPv4/IPv6 雙軌網路服務項目清單各項工作執行進度

	工作項目	開始日期	完成日期	進度

輔導 2 家 ICP 業者升級 IPv4/IPv6 雙軌網路服務				
3.1	輔導手冊	2019/4/26	2019/6/12	100%
3.2	輔導手冊更新	2019/6/11	2019/10/22	100%
3.3	整理網站業者環境架構(包括網路環境,設備,主機,系統,資料庫,程式碼等)	2019/4/26	2019/5/30	100%
3.4	網路環境調整(Firewall, Router, Load Balance, DNS)	2019/5/29	2019/7/30	100%
3.5	網站環境調整(作業系統, 資料庫, 程式碼)	2019/7/30	2019/8/30	100%
3.6	安全策略跟規範調整	2019/5/31	2019/10/3	100%
3.7	測試	2019/5/29	2019/10/9	100%
3.8	測試後調整	2019/6/6	2019/10/17	100%
3.9	官網通過 IPv4/IPv6 檢查清單	2019/10/7	2019/10/22	100%
3.10	交付官網 IPv4/IPv6 檢測報告	2019/10/7	2019/10/22	100%

二、 進度符合情形

各項工作的查核點進度如下表所示：

表 1 各項查核進度表

		執行進度			
分類	工作項目	超前	符合	落後	補充說明
研析 ICP IPv4/IPv6 升級及網路安全防護差異					
1.1	通訊協定資料收集		V		技術手冊(第二章/第 1,2,3 節)
1.2	網路環境資訊收集		V		技術手冊(第二章/第 4,5,6 節)

1.3	網站資訊收集		V		技術手冊(第二章/第 7 節)
1.4	資安軟硬體資訊收集		V		輔導手冊(第三章/第 3 節)
1.5	安全策略資訊收集		V		輔導手冊(第二章/第 2,3 節)
1.6	資訊整理/歸納/分析/彙整/驗證		V		輔導手冊(第二章/第 2,3,4 節)
1.7	網路環境(包括網路架構、網管、軟體升級、硬體升級等)等差異化比較		V		技術手冊(第二章/第 8,9 節)
1.8	伺服器(包括作業系統、網站伺服器、程式、資料庫、硬體升級等)等差異化比較		V		期末報告(第二章/第 1 節)
1.9	資安設備(包括資安策略、資安規劃、防火牆、IDS 或者其他與資安有關之軟體或硬體的升級步驟)等差異化比較		V		期末報告(第二章/第 1 節)
1.10	資安防護(包括實作上的差異、內部控管、外部控管、策略等)等差異化比較		V		期末報告(第二章/第 1,2 節)
1.11	資訊更新		V		
建立 ICP IPv4/IPv6 平台架構雙協定網路安全防護檢查項目清單					
2.1	資料收集/分析/歸納/整理		V		技術手冊(第三章/第 1,2 節)
2.2	網路環境升級檢查清單表		V		技術手冊(第三章/第 3,4 節)
2.3	作業系統及網站伺服		V		技術手冊(第四章/第 1

	器檢查清單表				節)
2.4	資訊安全設備(包括防火牆、入侵偵測系統、稽核系統等等)的檢查清單表		V		技術手冊(第四章/第 1,2 節)
2.5	檢查清單建立		V		技術手冊(第四章/第 1,2 節)
2.6	檢查清單更新		V		技術手冊(第四章/第 1,2 節)
輔導 2 家 ICP 業者升級 IPv4/IPv6 雙軌網路服務					
3.1	輔導手冊		V		輔導手冊
3.2	輔導手冊更新		V		輔導手冊
3.3	整理網站業者環境架構(包括網路環境,設備,主機,系統,資料庫,程式碼等)		V		期末報告(第二章/第 3 節)
3.4	網路環境調整 (Firewall, Router, Load Balance, DNS)		V		期末報告(第二章/第 3 節)
3.5	網站環境調整(作業系統, 資料庫, 程式碼)		V		期末報告(第二章/第 3 節)
3.6	安全策略跟規範調整		V		期末報告(第二章/第 3 節)
3.7	測試		V		期末報告(第二章/第 3 節)
3.8	測試後調整		V		期末報告(第二章/第 3 節)
3.9	官網通過 IPv4/IPv6 檢查清單		V		期末報告(第二章/第 3 節)
3.10	交付官網 IPv4/IPv6 檢測報告		V		期末報告(第二章/第 3 節)

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 7 人，包含專職人員 3 人，及兼職人員 4 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 2 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	林韋廷	技術主管	碩士	負責本專案之統籌、規劃，與 ICP 業者的合作及人力調配與資源配置
助理研究員	曾榮信	技術主管	碩士	本專案共同研究人員
助理研究員	鄧丕文	專案主管	碩士	本專案共同研究人員
研究助理	吳奎億	工程師	學士	協助網站業者處理 IPv6 導入過程中的網路與系統故障排除
研究助理	童冠瑜	工程師	學士	手冊編輯、校稿及與本專案相關的主管交代事項
研究助理	金沅禹	工程師	碩士	協助網站業者處理 IPv6 導入過程中的資訊安全檢測與故障排除
研究助理	張智崴	工程師	學士	協助網站業者處理 IPv6 導入過程中網站程式碼的障礙排除

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 3　合計總經費運用情形統計表

項　目	預算金額	使用金額	使用率
人事費用	647976	647976	100%
業務費	60000	60000	100%
旅運費	24000	24000	100%
行政管理費	38024	38024	100%
合　計	770000	770000	100%

第二章　成果說明

第一節 研析 ICP IPv4/IPv6 升級及網路安全防護差異

一、 IPv6 的封包

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

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

在 IPv6 被移除的 IPv4 項目中，Identification、Flags 及 Fragment Offset 欄位都是用在 IPv4 的封包切割。用途是在當大型封包必須在僅支援較小封包的網路上傳送時產生 Fragment 問題。這種情況下，IPv4 路由器會將封包切割成較小的片段，再傳送多個封包。目的地會收集

封包並進行重組，如果重組過程中發現有遺失一個封包或封包內容有錯，則整個傳輸就需要重來。

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

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

下表是 IPv6 會用到的檔頭，延伸檔頭有順序性，如果有多個延伸標頭同時出現，需要依照順序擺放。延伸檔頭如果之後有更新，都會發佈在 RFC 6564[24]。

表 4　IPv6 延伸檔頭類型

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

IPv4 header

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

IPv6 header

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

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

圖 1　IPv4/IPv6 檔頭欄位比較

IPv4 與 IPv6 在封包檔頭(header)的比較說明如下：

表 5　IPv4/IPv6 header 說明

欄位	IPv4	IPv6	IPv4	IPv6
首部長度 (Internet Header Length)	Y	N	IPv4 有一個 IHL(Internet Header Length, IHL,首部長度)欄位，此欄位用來說明 header 長度(單位為 32 bits)，此欄位也可以用來確定資料的偏移量(offset)。這個欄位的最小值是 5 (5x32-bit words=160 bits 或者 20 bytes)，最大值是 15。	此欄位在 IPv6 已經被移除，原因是 IPv6 的 header 長度是固定的 40 bytes，這樣處理時會更有效率。
片段共用識別碼 (Identification)、標誌(Flags)及位移 (Fragment Offset)	Y	N	又稱為片段共用的唯一識別碼。共 16 位元，這個欄位主要是用來標示一個唯一值，只要封包有被切片，這些被切片的封包都會擁有同一個識別碼 (Identification)，原因是分片不一定會依照順序到達，所以在重組時需要知道分片所屬的封包。	IPv6 作法是讓主機透過 RFC 1981[5] 裡面定義的 Path MTU Discovery 處理程序，得知 Path Maximum Transmission Unit (MTU)大小。如果路由器因為封包太大不能傳送，會透過 ICMP 回傳一個「Packet Too Big」給來源主機，當來源主機收到「Packet Too Big」時，就可以決定是否利用 IPv6 的 Extension

				header 來處理，因此 IPv6 不需要 Identification、Flags 及 Fragment Offset 欄位。
檢查碼 (Checksum)	Y	N	IPv4 利用 header checksum 對首部進行檢查，如果不一致，封包就會被丟棄。重新計算的重要性是因為在傳遞過程中，可能發生 TTL (Time To Live)、Flag、Offset 變更的情況，來避免 header 錯誤。至於資料(payload)的錯誤，則交給 TCP/UDP 層來處理。	因為 IPv4 開發之初，上一層對於媒體傳輸層做 checksum 不普遍，因此 IPv4 需要 checksum。但是現在這種狀況已經不需要，因為上一層會確保資料的正確性，因此 IPv6 把這個欄位跟檢查動作拿掉，可以大幅提升傳遞速度，減少路由器檢查封包的時間。
流量標籤 (Flow Label)	N	Y	IPv4 有 QoS(Quality of Service)，表示在網路環境中，送出封包的品質，所謂的品質越好，表示有越低的延遲、較少掉包和抖動等，並且搭配更高的吞吐量和可靠性。實際作法是利用封包內容的特定欄位的高低，告訴交換器/路由器等如何處理封包。 IPv4 是在 payload	此為新欄位，用來當從來源傳送到一個或者多個目的地時，對一串或者一組 IPv6 封包 payload 訂標籤。被標籤化的封包在經過 IPv6 路由器時，可以被特別處理，例如高優先權傳送。關於 Flow Label 可以參考 RFC 1883[3]、2460[9] 跟 6437[22]。

			內做這個判斷，但是在 header 是沒有這個欄位的。	

IPv6 header 的位元格式：

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

圖 2　IPv6 header

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

二、　IPv4/IPv6 的位址格式

IPv4 位址長度為 32 位元，型態為 x.x.x.x (其中 x 皆數字，每一個數字最小為 0 最大為 255)，例如 140.130.120.110。而 IPv6 出現的目的就是為了解決 IPv4 位址不夠使用的問題，IPv6 位址的長度為 128 位元,其中 64 位元代表網路號碼,而另外 64 位元代表電腦號碼。IPv6

可以提供 2 的 128 次方個 IP 位址。而一個 IPv6 的位址格式為 xxxx: xxxx: xxxx: xxxx: xxxx: xxxx: xxxx: xxxx (其中每一個 x 都是 16 進位，數字 0~9 加字母 a~f）。例如：2001:b011:6a00:18ff:d87a:8712:dh8b:f718 就是一個 IPv6 的位址。

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

三、 IPv6 位址的分配方式

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

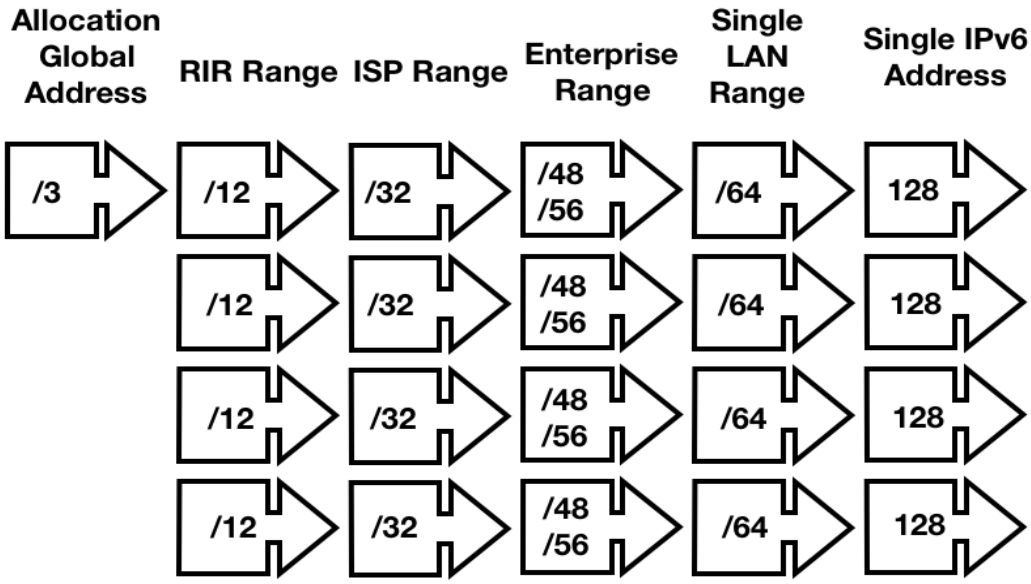

圖 3　IPv6 配置規則

四、　IPv6 對 Multicast 協定的調整

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

表 6　unicast, multicast 與 broadcast 比較

傳遞方式	說明
Unicast（單播）	唯一區域位址（unique local address，簡稱 ULA，保留區塊為 fc00::/7）類似 IPv4 的私有 IP 位址（Private IP address）的可用位址空間，即同一路由內的區域網路（或稱內網）可用位址的集

	合。 連結本地位址（link local address，保留區塊為 fe80::/64）類似 IPv4 啟用時本機自動產生的本地位址，而此本地位址只存在本機中無法跨過路由器。
Multicast（群播）	IPv4 使用 224.0.0.0/4 作為 multicast 封包使用，而 IPv6 則使用 ff00:::/8。在 IPv6 中以 multicast 取代 IPv4 的 broadcast。 在 IPv4 使用 Internet Group Management Protocol（IGMP）協定來管理 multicast group membership，而 IPv6 則不使用 IGMP，改以 Multicast Listener Discovery（MLD） messages。簡單來說，MLDv1 跟 IGMPv2 很接近，MLDv2 跟 IGMPv3 很接近。 scope 欄位是用在 multicast 時，決定哪些路由器可以轉送這些 multicast 封包。 scope 欄位共有 4-bit，其值可以是 0 - reserved 1 - Interface-Local scope 2 - Link-Local scope 3 - Reserved 4 - Admin-Local scope 5 - Site-Local scope 6 - Unassigned 7 - Unassigned 8 - Organization-Local scope 9 - Thru D Unassigned E - Global scope F - Reserved 在 scope 欄位之後有 112 bits 用來表示 multicast group ID。
Anycast（任播）	任播用來送給一群主機中的任何一台。 所謂的 anycast 是指該 IPv6 位址可以被指定到多個介面上（通常是多台不同設備）。換句話說，多台機器可以共用同一個 IPv6 位址。當有一個封包被要求傳送到一個 anycast IPv6 位址時，路由器會依據 routing table 決定送給最近的一台設備。關於 anycast 可以參考 RFC 1546[1]。

五、 IPv4/IPv6 對 IP 設定組態的差異

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

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

在 IPv6 中，除了 DHCPv6 之外，還有 Stateless Address Auto-configuration 的方式(無狀態位址自動設定)，Stateless Address Auto-configuration 又簡稱為 SLAAC，在網路設備設定上常看的都是寫成 SLAAC 的簡稱，定義在 RFC 2462[10]跟 RFC 4862[16]。所謂的無狀態機制運作機制為當一部主機啟動 IPv6 時，送出多點傳送的路

由器請求、路由器回應以路由器公告訊息(Router Advertisement; 簡稱 RA)來讓主機從路由器(Router)取得路由器的 prefix 再加上自己的介面識別碼，來自動配置 IPv6 位址。

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

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

1. 全狀態位址自動配置(Stateful Address Auto-configuration)是透過 DHCPv6 伺服器自動取得 128 位元的 IP 位址跟相關組態。
2. 無狀態位址自動配置(SLAAC，Stateless Address Auto-configuration; SLAAC)依據 RFC 2462[10]、RFC 4862[16]，可以依據自己可用資訊(介面識別碼)和從路由器公告取得的訊息(首碼)來產生自己的位址。SLAAC 作法上，主機先送出多點傳送路由器請求(Router Solicitation)，路由器則回應路由器公告(Router Advertisement)訊息來完成。

IPv6 自動組態功能啟動順序如下：

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

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

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

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

1. Stateless Auto-configuration：適用於沒有 DHCPv6 的環境，主機利用路由器的 RA 封包的首碼自動產生 IP 位址，而 DNS 則得手動輸入。(M=0，O=0)
2. Stateful DHCPv6：適用於 DHCPv6 環境下，主機直接由 DHCPv6 伺服器取得 IP 位址和其他參數如 DNS 位址。(M=0，O=1)
3. Stateless DHCPv6：使用路由器的 RA 封包取得首碼自動產生 IP 位址，至於 DNS 則由 DHCPv6 伺服器取得。(M=1，O=0)
4. 其他：由 DHCPv6 提供 IP 位址，但 DNS 或者其他參數卻不跟 DHCP 索取。(M=1，O=1)

表 7　IPv4/IPv6 設定差異

	IPv4	IPv6
設定方式	由網路服務商提供 IP 網址或者 subnet，將 IP 位址或者 subnet 設定在設備上，以啟用服務。 或者使用 DHCP 機制，從 DHCP Server 取得配置的 IP 位址。	IPv6 引入一個簡化版本的 stateless auto configuration 作法，此作法可以只要依據節點本身的資訊就可以設定，不需要去詢問任何設備。 1. 全狀態位址自動配置 (Stateful Address Auto-configuration) 2. 無狀態位址自動配置 (SLAAC，Stateless Address Autoconfiguration; SLAAC)
流量品質	以檔頭的 TOS(Type of Service)欄位來區分	1. 對路由器而言，檢查檔頭中的 Traffic Class 欄位來達成

		2. 未來可以由設備對封包 header 設定流量 Flow Label 欄位，用來支援更進階的應用

對於 IPv6 的配置我們給出以下建議：

表 8 IPv6 配置建議

作法	適合場景	補充說明
人工配置位址	適合網路設備及網頁伺服器	1. 建議關閉 RA(Router Advertisement)的發送。 2. 每一台主機都手動設定 IP(包括 gateway、DNS、防火牆)。 適合網站使用。
SLAAC+ RDNSS	適合物聯網	1. 物聯網設備通常不需要主動連網，因此網路環境越單純越好，SLAAC 有助於物聯網的發展。 2. 作法是定期經由 Multicast 發出 Router Advertisement(RA)的封包，從 RA 封包取得 IPv6 Prefix 及 Default Gateway 的資訊。 3. 主機利用收到 Prefix 跟自動產生的 Host ID(主機識別碼)即可變成主機的 IPv6 位址，位址發放之後就不再管理。 4. SLAAC 不支援發送 DNS 伺服器位址，不過新增訂 SLAAC RDNSS 已經解決此問題，只是作業系統不見得有支援。 5. 適合物聯網使用。
SLAAC+ Stateless DHCPv6	適合不需要嚴格進行資安查核管理的場所	1. 利用 SLAAC 及 DHCPv6 進行位址配置。 2. RA 負責 IPv6 位址及 Default Gateway 的指派，DHCPv6 則提供 DNS 伺服

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

表 9　IPv6 優點

分類	說明
增加 IP 位址的擴充性	IPv6 的位址從 32 bits 變為 128 bits，可以支援更多的 IP、位址自動設定。藉由增加一個「scope」欄位讓 multicasting(群播)路由延伸性增加，還有新增 anycast。
封包 header 簡化	部分 IPv4 欄位被捨棄，可以減少封包處理的頻寬消耗。
增加擴充性跟更多選項	Extension header 允許更有效率的轉送、更有彈性的選項長度及新增選項。
流量標籤能力	Flow Label 是一個新的機制用來幫封包貼上標籤，讓封包屬於某個特定的「flows」，這種機制用於即時的服務。每一個封包提供一個流量標籤，同一筆資料串列給予相同的標籤號碼，因此可以做流量控制及統計。用來支援像視訊、語音這類即時服務的需求，以提高 QoS 的品質。
授權及隱私的擴充性	在 IPv6 內增加了認證、資料完整性、資料保密的能力。(後面會說明)

六、 IPv4/IPv6(Dual Stack)雙軌服務說明

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

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

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

表 10 Ether Type 定義

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

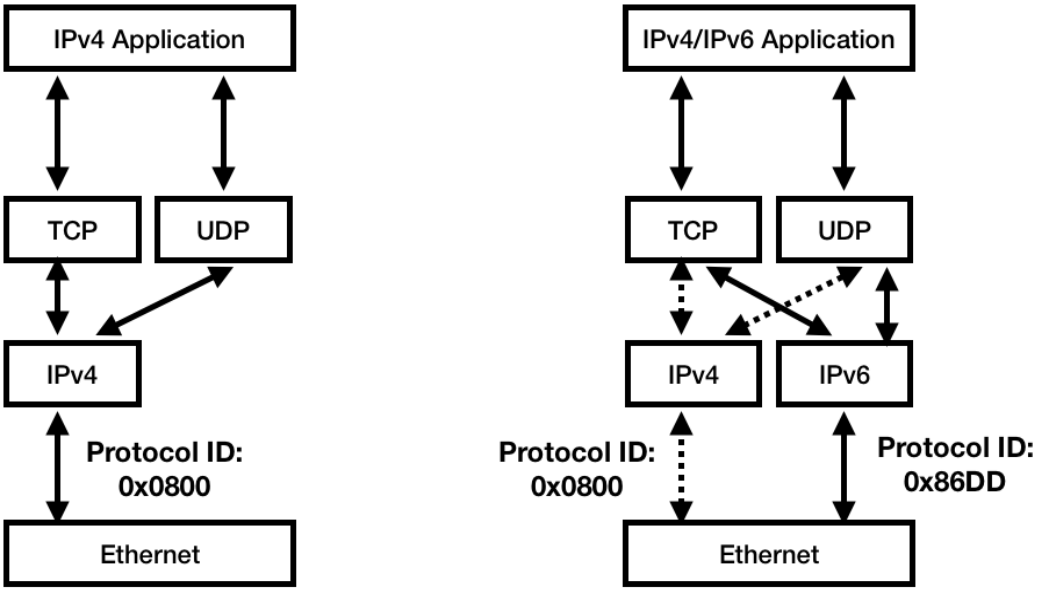

圖 4　IPv4/IPv6 傳輸差異

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

對於 IPv6 的支援，在作業系統層面，包括 Windows、Mac OS 跟 Linux(例如 Ubuntu、Centos、Fedora、SUSE 等都是 Linux 作業系統)，

早就已經支援。而硬體設備如 Cisco，也早在 2000 年宣布在 Cisco IOS Release 12.2(2)T 版本中開始支援 IPv6。

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

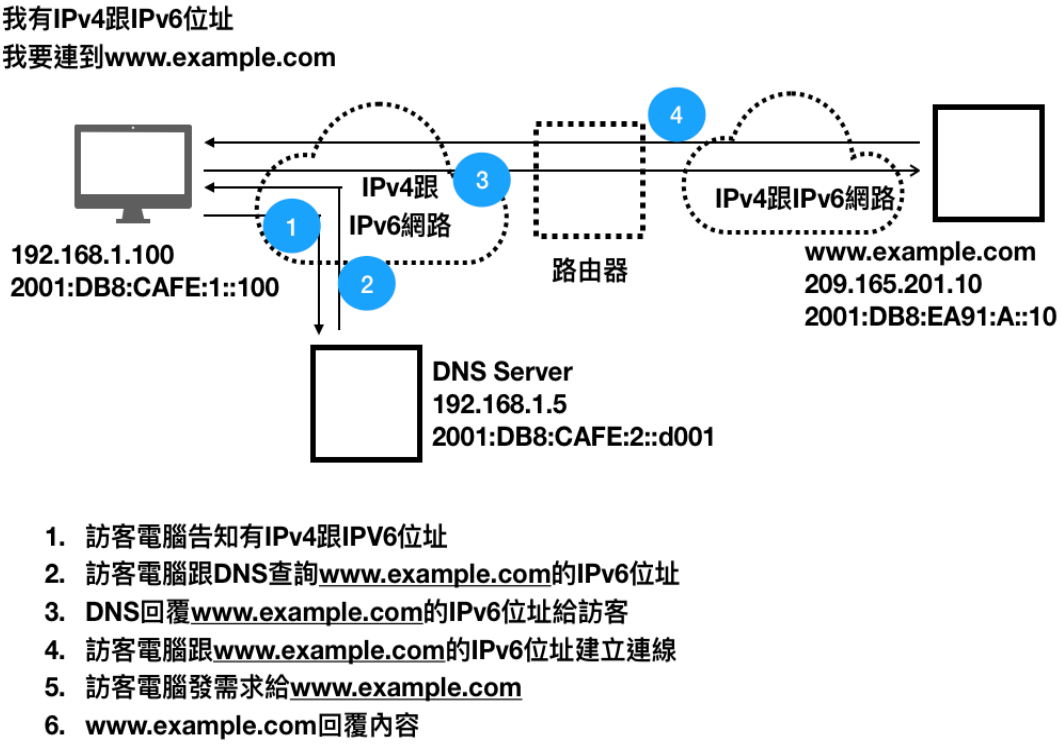

圖 5　IPv4/IPv6 連線範例

七、　ICP 機房環境比較

（一） ICP 業者機房類型

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

表 11　ICP 業者機房選擇方案

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

以上四種可以歸納成三類，這三類的優點跟缺點比較以下表整理。

表 12　ICP 選擇網路架構優缺點比較

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

（二） 網際網路服務供應商支援 IPv6 調查

我們對市場主要的網路服務商進行 IPv6 支援度的調查，用來了解當 ICP 業者是否可以繼續使用現有的網路服務商進行升級為 IPv4/IPv6 雙軌服務，對於無法支援 IPv6 的網路服務商業者，則希望

這些業者盡快支援 IPv6，提升 ICP 業者使用 IPv6 的比率。(資料日期：108 年 8 月)

表 13　網路服務商支援 IPv6 表

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

八、　IPv4/IPv6 對 ICP 作業系統、網頁伺服器的網路安全防護差異

（一）作業系統

IPv6 在目前市面上的作業系統都已經支援。最早從 1996 年開始，就有作業系統開始支援 IPv6，只是早期的 IPv6 功能屬於實

驗性質。(資料來源：Wiki)

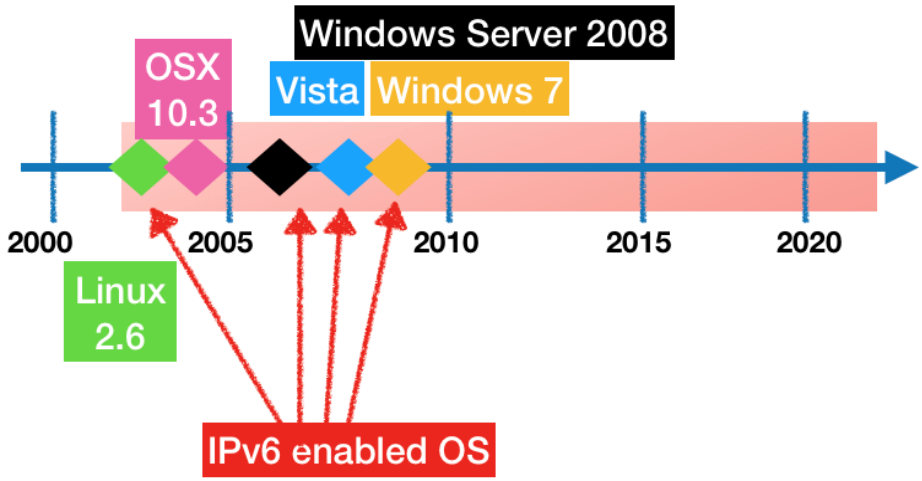

圖 6　支援 IPv6 的作業系統

表 14　作業系統支援 IPv6 年份表

年份	作業系統支援
1996	Linux Kernel 2.1.8 開始支援 IPv6
1997	IBM AIX 4.3 開始支援 IPv6
2000	FreeBSD、openBSD、NetBSD 開始支援 IPv6
2000	Windows 2000 開始支援 IPv6
2000	Sun Solaris 開始支援 IPv6
2001	Compaq OpenVMS 開始支援 IPv6
2001	Cisco IOS 路由器及 L3 交換機開始支援 IPv6
2001	HP HP-UX 11i v1 開始支援 IPv6
2002	Microsoft Windows NT 4.0 開始支援 IPv6
2003	Apple Mac OS v10.3 開始支援 IPv6
2007	Microsoft Windows Vista 開始支援 IPv6

（二） 網頁伺服器

網頁伺服器(Web Server)是指可以提供網站服務的軟體。在早期，以 IIS 跟 Apache 兩套為主，使用者多且文件豐富。近幾年，Nginx 的高效能讓它變成許多大流量的網站的首選。跟 Apache 相比較，Nginx 優異的處理速度，讓許多技術人員放棄 Apache 改用 Nginx。

IIS 內建支援 IPv6，在 Windows 主機建立 IPv6 連線後，網站即可設定 IPv6 位址以提供 IPv6 服務。開啟 Windows Server 主機 Server Manager 的畫面後，選擇 Internet Information Services（IIS）Manager 選項進行 IIS 的設定。

Apache 是 Linux 系統上最廣泛用來架設網站的軟體，Apache 在 2.0 版本之後都有支援 IPv6，在作業系統啟用 IPv6 後，Apache 只要在設定檔加入 IPv6 的位址，並允許外部連線可以連到 IPv6 位址，即可服務 IPv6 客戶。

Nginx 從 0.7.36 的版本後開始支援 IPv6， 如果要驗證現行的 nginx 版本是否已經啟用 ipv6，可以執行 nginx -V 的指令，如結果有出現「--with-ipv6」即表示有支援 IPv6。

以上軟體的設定方式可以參考輔導手冊第六章的詳細說明。

（三） 作業系統跟網頁伺服器對於網路攻擊的防禦方式比較

表 15 作業系統跟網頁伺服器對於網路攻擊的防禦方式比較

項目	IPv4 的防禦方式	IPv6 的防禦
連線及封包控制	Linux 預設使用 iptables 控制。	Linux 預設使用 ip6tables 控制。
主機跟主機之間的安全連線	安裝 IPSec 軟體，建立端點到端點的連線加密。	啟用 IPv6 的 IPsec 機制，建立端點到端點的安全加密。
黑名單與白名單主機連線控制	在/etc/hosts.deny 設定。	跟 IPv4 一樣，在 /etc/hosts.deny 設定。
Brute Force Attacks(暴力式攻擊)	DenyHosts 僅對使用 IPv4 的連接有效。它在 IPv6 下不起作用。	在 IPv6 下可以改用 Fail2ban，這套軟體可以跟 iptables(給 IPv4 使用)跟 ip6tables(給 IPv6 使用)搭配，直接將 IP 阻擋下來。
封包過濾規則	如果不使用 multicast，可以直接阻擋 multicast 封包。	如果支援在 IPv4 網路上傳送 IPv6 封包(包括以 tunnel 方式在 IPv4 網路上傳遞 IPv6 封包)，則建議以特定網卡服務此類封包，並套用過濾規則，阻擋所有的 IPv4 封包(protocol 欄位=41 的封包)且目的為 239.0.0.0/8 的封包。
阻擋保留位址	在作業系統或者 Web Server 上禁止保留位	在作業系統或者 Web Server 上禁止保留位址，

	址，因為這些位址不應該從外部連線到主機。例如 192.88.99.0/24 是 6to4 anycast(任播)的保留網址。	因為這些位址不應該從外部連線到主機。如果是在純 IPv6 環境，應該阻擋 64:ff9b::/96。
Teredo 隧道	Teredo 是一個 IPv6 轉換機制，它可為執行在 IPv4 網際網路但沒有 IPv6 網路原生連接的支援 IPv6 的主機提供完全的連通性。與其他的類似協定不同，它可以在網路位址轉換（NAT）裝置（例如家庭路由器）後完成功能(*資料來源 Wiki)。Windows 作業系統預設會啟用。在純 IPv4 環境中，需要濾掉 UDP port 3544 避免有未授權的 Teredo 連線。	Teredo 是一種臨時措施。在長遠的未來，所有 IPv6 主機都應該使用原生的 IPv6 連接。Teredo 應在原生 IPv6 連接可用時被停用(*資料來源 Wiki)。Teredo 伺服器監聽 UDP 埠 3544。 在純 IPv6 環境下，應該濾掉 Teredo 封包。
禁止爬蟲	透過 nginx 或者 apache 模組可以設定訪客連線的速度，避免爬蟲大量抓取資料，造成主機負荷過高，無法正常運作。 Nginx 的 rate limit 是透過 limit_req_zone 模組，支援 IPv4 跟 IPv6。 Apache 的 rate limit 是透過 mod_ratelimit 模組。 IIS 是透過 denyByRequestRate 或 requestLimits 或 limits 方式來達成 rate limit 效果。	Nginx 的 rate limit 是透過 limit_req_zone 模組，支援 IPv4 跟 IPv6。 Apache 的 rate limit 模組可透過 mod_limitipconn ，此模組支援 IPv6。 IIS 則是使用 Dynamic IP Restrictions (DIPR)模組來達成 rate limit。

九、 IPv4/IPv6 對 ICP 防火牆、入侵偵測系統的網路安全防護差異

（一） IPSec 在 IPv4/IPv6 上的比較

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

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

表 16 IPSec 組成說明

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

	5. 保護 IP payload 跟所有的 header 欄位 6. 定義在 RFC 2402[7]	
Encapsulating Security Payload (ESP)	1. 提供來源認證 2. 利用 hash 確保資料完整性 3. 對封包加密確保資料安全 4. Transport mode(傳送模式)ESP 不提供整個封包的完整性跟驗證 5. Tunnel mode(隧道模式)是對整個封包加密後封裝，並添加一個新的 header 6. 定義在 RFC 2406[8]	1. 在 Transport mode，ESP 預留原本的 IPv6 header，但是新增一個 ESP extension header 及一個 optional ESP trailer 2. 增加一個 optional ESP authentication trailer，利用 HMAC(Keyed-Hash Message Authentication Code; 又稱為 keyed hash)驗證封包 3. 定義在 RFC 2406[8]
Security Associations (SA)	1. 用來交換建立安全連線之間所需的資訊，包括演算法、金鑰用來加密封包。 2. 用途包括連線、驗證。 3. IPv4 使用 IKEv1 作為金鑰管理	1. 使用 IKEv2 作為金鑰管理的方式，定義於 RFC 4301[15]

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

IPSec 是 Internet Layer 的安全通道，提供設備或者網段之間的安全連線。在 RFC 規範的早期版本，IPv6 實作 IPSec 是建議使用 IKE (Internet Key Exchange，IKE Internet Key Exchange)的金鑰管理，並要求所有的 IPv6 設備都需要支援 IPSec 架構，並同時支援手動及自動設定。現在，新版的規範是建議自動設定改用 IKEv2(第二版)，此需求定義在 RFC 5996[21]。

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

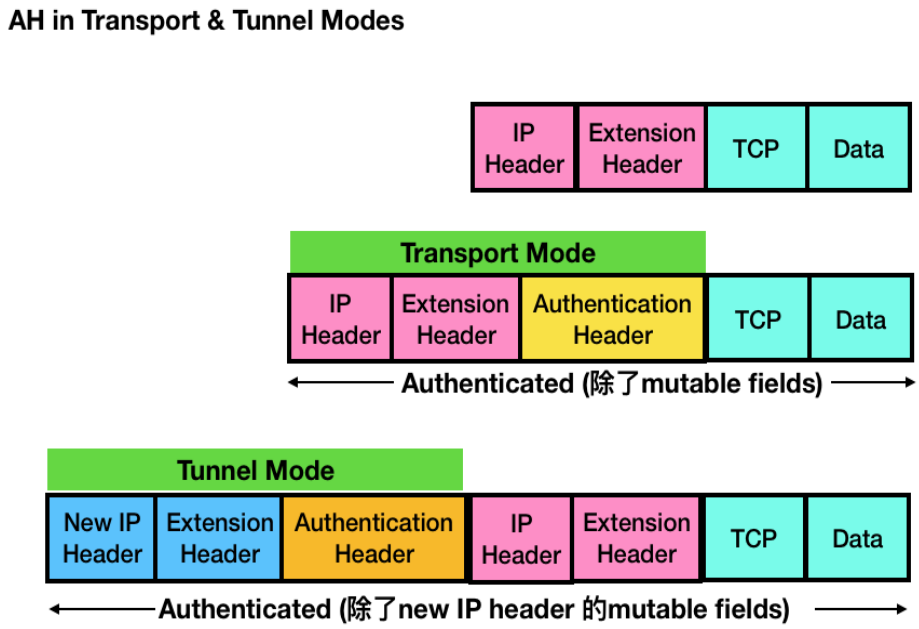

圖 7　AH in Transport & Tunnel Modes

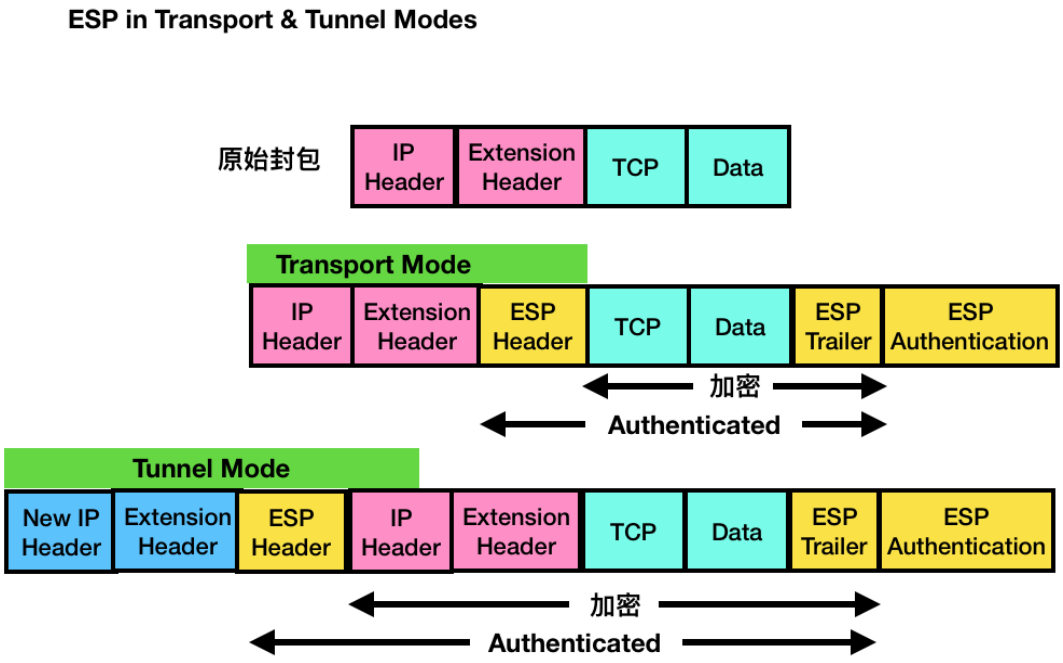

圖 8　ESP in Transport & Tunnel Modes

關於 IPv6 的安全設計，可以參考 RFC 2401[6]。在 IPv4 中最重要的端點到端點的加密 IPSec 已經直接加到 IPv6 內，關於 IPv6 IPsec 有關的討論，可以參考 RFC 4301[15]及 RFC 5996[21]。

（二） NAT 在 IPv4 與 IPv6 上的探討

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

網際網路架構委員會(Internet Architecture Board，簡稱 IAB)在 RFC 5902[20]描述關於 IPv6 環境下使用 NAT 機制的情境。會有 IPv6

是否需要 NAT 的討論起因於原本在 IPv4 下使用 NAT 的廠商，他們覺得也需要類似的機制可以在 IPv6 下使用。不過依據 IETF(Internet Engineering Task Force，網際網路工程任務組)討論結果，不需要在 IPv6 提供 NAT 機制。更多關於 IPv6 是否需要 NAT 的討論可以參考 RFC 4864[17]。

IPv6 NAT 的討論主要可以整理如下：

表 17　NAT 問題討論

問題	討論	IPv6 解決方式
Avoid Renumbering(避免重新編號)	在 RFC 4864[17]第 2.5 節討論的，許多業者希望能夠盡量減少網路維運的負責度跟工作量。對家庭用戶而言，重新編號不是一個嚴重的問題，但對企業用戶卻是。影響範圍包括需要重新配置 IP 跟 prefix 的設備，包括 DNS、DHCP、防火牆、IPSec 策略、入侵偵測系統、庫存管理系統、程式碼修正管理系統內部系統。 許多大企業使用提供商無關地址空間（Provider-independent address space，又稱 PI 地址空間）是由區域網際網路註冊管理機構（RIR）直接分配給最終用戶的一段 IP 位址，主要優點是方便設	RFC 2462[10]提供 IPv6 Stateless Address Autoconfiguration(無狀態地址自動配置)，提供自動配置跟重新編號。IPv6 的 Stateless Autoconfiguration 是 IPv6 的新功能，包括 link-local 位址、multicasting(群播)、the Neighbor Discovery(ND)通訊協定、從底層數據鏈路層地址生成地址的接口標識符的能力。

	定路由(Wiki 維基百科說明)。	
Site Multihoming(網站多宿主)	站點多宿主提供了網際網路所需的可靠性跟負載平衡。內送流量備援容錯機制(Multihoming)，亦作多重主目錄，是網際網路連線的一種容錯機制，用以提高 IP 網路上對網際網路連線的可靠度。這個機制一般只用在客戶端，而不會用在網際網路供應商(ISP)，透過為客戶端提供多於一條網際網路連線，使當中其中一條連線中斷時，系統可以自動切換使用另一條連線。(Wiki 維基百科說明)	在 RFC 3852[13]此篇 RFC 描繪了新的 IPv6 site-multihoming 架構下所欲達成的理想目標，這些理想包括提供有高效率的備援功能(redundancy)、優質的負載分享(load sharing)、高效能(performance)、支援客戶所要求的管理政策需求(policy)等優於 IPv4 目前 site-multihoming 所能提供的功能。 如何在不影響目前 site-multihoming 運作環境下(包括對營運者的維運、路由器、用戶主機等)，仍然可以優於 IPv4 目前 site-multihoming 所能提供的功能。(參考中華電信研究所 NICI IPv6 標準測試分組電子報)
Homogenous Edge Network Configurations (同質邊緣網路配置)	對家庭用戶而言，這是電信業者最常提供給家庭用戶的方案。一個家庭內即使有多台機器，對外也是只使用同一個 IP 位址。	參考 RFC 5902[20]，在 IPv6，link-local 位址可以被用來確保所有的家用 gateway 使用相同的 IP 位址，並提供 homogenous addresses 供支援的設備使用。
Network Obfuscation(網路混淆)	大多數的網路管理人員都希望隱藏主機的詳細資	可以參考 RFC 4941[19]，利用專用介

	訊，包括網路架構跟通訊內容。這樣的考量是基於這些主機都是他們公司的私有資產，由於某些主機可能需要機密性，特別是很重要的主機更是希望能夠完全保密，因此網路管理在考量網路安全時，總是認為以 NAT 來保護這些設備是最恰當的方式。	面識別元搭配亂數產生一個全球都可以識別的位址，並不定時更新資料，避免資料被收集，降低被主機資訊洩漏的風險。
Hiding Hosts(隱藏主機)	對於網路管理人員來說，隱藏跟保護內部網路內的主機資訊是重要的。這些主機可能包括工作站、筆記型電腦、伺服器、特定的終端設備(印表機、掃瞄器、IP 電話、POS 系統、門禁系統)等。 由於這些設備不需要對外服務，因此他們希望外部無法探知這些設備及資訊。 對駭客而言，對於要攻擊 NAT 內的主機，難度是較高的。而且駭客要知道一個 NAT 內有多少主機也是困難的，即使他們可以藉由收集不同的封包內容去猜測跟收集不同主機的指紋資訊，但透過這些資訊要組合成可被攻擊的目標，仍舊是一件困難的事情。	對於駭客而言，他們已經設計出透過特洛伊木馬病毒來穿透 NAT 的攻擊方式。另外有一點是 NAT 不是防火牆，不少管理者把 NAT 作為一種安全防護手段，這樣已經把防火牆跟 NAT 搞混了。安全防護應該透過防火牆來執行，而非以為 NAT 可以做到防火牆相同的效果。參考 RFC 3041[12]的作法隨機在 IPv6 中將主機隱私資訊依據需要產生，而且僅限於有限期間內才有效。由於 IPv6 位址很多，因此有許多自由隨機化子網分配，透過這種方式，讓意圖記錄跟追蹤主機資訊的人，無法推敲出真正的主機資訊。
Topology Hiding(隱藏拓	隱藏網路架構圖(拓墣圖)對於網路管理人員也是很	參考 RFC 4864[17]，作法在 RFC 3014[11]內

墣)	重要的，包括隱藏內部路由器及內部連接狀況。	有描述，主要是透過有期限限制的 IPv6 資訊，避免網路拓墣被收集跟窺探。
Simple Security(簡單安全)	因為外部主機無法直接連接到 NAT 內的主機，因為 NAT 通常是為一種安全機制。 但是不應該將 NAT 跟防火牆混淆，兩者是不同的。NAT 是把幫忙建立內部機器與外部連線，而防火牆則是控管網路安全。	透過防火牆過濾跟阻擋不安全的連線是主要解決方案，而不是誤以為用了 NAT 就可以做到簡單安全。

（三） Intrusion Detection Systems（IDS）入侵偵測系統

針對三個開源入侵檢測系統 Snort，Suricata 和 Bro 介紹對 IPv6 的支援概況。

1. Snort

於 2014 年發布的 Snort 1.6 版本後就支援檢測 IPv6 的功能，總共有 64 種與 IPv6 相關的 VRT+ET 規則，VRT rules 為 snort.org 的官方 rules，由 Sourcefire Vulnerability Research Team (VRT) 提供，每一條 rules 均經 VRT 嚴格測試，ET rules 則為 Emerging Threats rule。

表 18 Snort 規則 IPv6 特徵值統整

特徵值說明	規則數量
ICMPv6 protocol alerts	24

IPv6 protocol decode messages	24
Metasploit meterpreter binding	8
Other	8

2. Suricata

這是一套開源的入侵偵測跟入侵防禦系統。跟 Snort 使用相同的規則庫，一樣有 64 種，另外還有一項 decoder-events.rules 的檔案再提供 32 種規則，因此 Suricata 總共提供了共 96 種關於 IPv6 的規則。

3. Bro(Zeek)

是一套免費的開源軟體網路分析軟體。它可以用在網路入侵偵測系統，也可以對網路事件進行額外的即時分析。於 2012 年發布的 0.17-8 開始支援檢測 IPv6 的功能。

十、 ICP IPv4/IPv6 管理策略及安全政策

RFC 4890[18]主要建議在防火牆中過濾 ICMPv6 消息，為 IPv6 安全提供了最基本的防護。在設有防火牆的 IPv4 網路中，通常會阻斷大多數 ICMP 訊息的傳送，最主要原因是駭客可利用 ICMP 協定獲取網路異常原因等相關訊息，調整網路探測及攻擊方式。但是在 IPv6 的環境，Neighbor Discovery(ND)協定須依據 ICMPv6 回應訊息，判斷路由器或主機是否存在，因此防火牆須允許 ICMPv6 封包通過。 為防止 ICMPv6 訊息洩漏可能造成的

影響，RFC 4980 針對防火牆可能需要開放的規則提出建議，這個建議就是在實際設定時，應秉持最小化原則，針對防火牆規則的來源與目的端設定限制，盡可能設定明確的 IP 範圍，不應貪圖方便而設定為 Any，介接網際網路的防火牆如有 Echo Request 及 Echo Reply 連線需求，則須進一步確認其必要性，以下是依據 RFC 4890 整理的表格。

表 19　RFC 4890 防火牆對 ICMPv6 建議設定

建議處理	ICMP 類型
必須開放	1,2,3,4,12,129,130,131,123,143,148,149,151,152,153,133,134,135,136,141,142
通常開放	3-Code 1,4-Code 0
必須過濾丟棄	138,144,145,146,147
視需要制定是否過濾丟棄	137,139,140,5-99,102,126

RFC 7359[26]討論了雙協定下第 3 層 Virtual Private Network（VPN）tunnel 流量洩漏，並討論了可能的解決措施。由於此問題是基於路由第 3 層流量的 VPN 解決方案，因此它適用於基於 IPSec 的 VPN 隧道及 SSL / TLS VPN 隧道的解決方案。當一台主機是雙協定主機(同時啟用 IPv4 及 IPv6)，並在這台主機上安裝的 VPN 軟體不支援 IPv6 的 VPN 隧道，並且該主機連接到雙協定網路時，如果客戶端上的某些應用程序打算與目標進行通信，則客

戶端通常將查詢 A 和 AAAA DNS 資源記錄(A 是對應到 IPv4 位址，AAAA 是對應到 IPv6 位址)。由於主機同時具有 IPv4 和 IPv6 連接能力，並且預期的目的地將同時具有 A 和 AAAA DNS 資源記錄，因此可能發生主機使用 IPv6 與預期的目的地進行通信。如果此時 VPN 軟體不支援 IPv6，因此 IPv6 流量將不會使用 VPN 隧道；因此，從來源主機到目的主機，它既沒有完整性也沒有機密性保護，因此有以下兩個注意事項。

1. 如果 VPN 軟體不支援 IPv6，請在所有網路接口中禁用支援 IPv6。
2. 如果 VPN 軟體支援 IPv6，請確保所有 IPv6 流量也通過 VPN 發送。

第二節 建立 ICP IPv4/IPv6 平台架構雙協定網路安全防護檢查項目清單

一、 IPv4 與 IPv6 網路攻擊方式

RFC7123[25]詳細介紹了在 IPv4 網路上的 IPv6 網路攻擊，並討論了可能的緩解技術。而 IPv6 與 IPv4 最大的不同在 IP 層，而 IP 層的上層(HTTPS、SSH)或下層(交換器、實體機器)的實作方式並無不同，因此 IPv6 繼承了 IPv4 的安全漏洞。在 IPv6 中名稱與 IPv4 不同，但應用方式類似，面臨的漏洞相似，說明如下：

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

以下我們以常見的網路攻擊，來探討 IPv4 與 IPv6 的網路攻擊方式。

表 20　IPv4 與 IPv6 的網路攻擊方式

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

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

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

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

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

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

二、 IPv4 與 IPv6 網路攻擊的防禦措施

表 21 網路攻擊的防禦措施

攻擊名稱	IPv6	IPv4
網路竊聽	利用 IPv6 內建的 IPSec	1. 利用 IPSec protocol 進

(Sniffing)	protocol 進行 Layer 3 的資料傳遞加密	行 Layer 3 的資料傳遞加密 2. 添購 IPSec 硬體設備建立重要主機之間的連線
應用層的威脅(Application)	應用層的攻擊跟網路層的攻擊屬於不同層的攻擊，主要要注意的 IP 存取或者授權。	應用層的攻擊跟網路層的攻擊屬於不同層的攻擊，主要要注意的 IP 存取或者授權。
未經驗證或者偽照的裝置(Rogue Devices)	1. 關閉 RA，每一台重要主機都手動設定 IP、DNS 2. 針對 IPv6 設定 ACL 3. 防火牆過濾 IPv6 封包，且可以檢查 IPv4 tunnel 內的 IPv6 封包 4. 在交換機啟用 RA Guard 或 ND Detection，對於每一個 Router Advertisement 檢查是否正確，不正確的就丟棄。(注意：RA Guard 或 ND Detection 只是一個保護方法的統稱)	1. 利用防火牆管理 IP 2. 確保機器 IP 跟 MAC address 是有被驗證的 3. 使用 ACL 避免非法的 IP 入侵 4. 使用白名單限制連線
中間人攻擊(Man-in-the middle attack, MITM)	1. 利用 IPSec protocol 進行 Layer 3 的資料傳遞加密 2. 在 Layer 2 進行安全控管 3. 依據 RFC 3971[14]跟 6494[23]，使用 SEcure Neighbor Discovery(SEND)，使用獨立的 IPSec 以加密方法保護 NDP	1. 利用 IPSec protocol 進行 Layer 3 的資料傳遞加密 2. 手動設定 DHCP Server 跟 DNS Server 及 default gateway

網路掃描(Scan)	困難,因為網段內 IP 數量太多	以防火牆阻擋網段掃描
蠕蟲感染跟傳播(Worm)	因為 IPv6 的位址完全是階層式，所以可以利用此特性，做入口/出口過濾。	以防火牆及防毒軟體來阻擋 Worm 的感染及散佈。
Broadcast Amplification Attack	Broadcast 已經在 IPv6 移除。	1. 在路由器跟防火牆上禁止使用 IP broadcasting 位址。 2. 禁止 ICMP 封包。
DDoS 攻擊(洪水攻擊(Flood Attack)	1. 啟用 SEcure Neighbor Discovery (SEND) protocol 2. 啟用 Bogon route services,例如由 Team Cymru 所維護的 bogon prefix 用來處理不應該出現在網路上的 prefix。 3. 使用防火牆阻擋 4. 使用 Content Delivery Networks(CDN) 5. 啟用 IPS 或 IDS 6. 啟用 Application Delivery Controller(ADC)	1. 使用防火牆阻擋 2. 使用 Content Delivery Networks(CDN) 3. 啟用 IPS 或 IDS 4. 啟用 Application Delivery Controller(ADC)
IPv6 Latent Threats	使用具備 IPv6 能力的設備來過濾跟防護 Hosts 對 IPv6 攻擊與漏洞威脅。例如使用支援 IPv6 的 NIPS(網路型入侵防禦)、HIPS(主機入侵預防系統)或者 Firewall。	此為因為使用 IPv6 而衍生的議題。
新增的 Extension header	1. 啟用 RA-Guard 2. 升級到最新的作業系統，因為新的系統通常會	此為因為使用 IPv6 而衍生的議題。

injection 攻擊	增加對較新 RFC 的支援	
Dual-stack 引起的風險		此為因為使用 IPv6 而衍生的議題。
Tunnel Injection 及 Sniffing	1. 利用支援 IPv6 的設備來檢查來源跟目的地的 IPv6 位址並進行過濾。 2. 使用 IPSec 建立安全通道	1. 使用 IPSec 建立重要主機之間的安全通道 2. 使用白名單限制 Tunnel 的存取

三、 建立 ICP IPv4/IPv6 平台架構雙協定網路安全防護檢查項目清單

表 22 ICP 業者的 IPv6 設定檢測表

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

		位址				
CT-3	DNS	網站是否有正確設定 IPv6 位址	是	顯示 IPv6 位址	dig aaaa 根網域 @8.8.8.8 +short	dig
CT-4	DNS	網站使用的所有 DNS Server 本身要有 IPv6 位址	是	顯示 IPv6 位址	for i in `dig @8.8.8.8 +short NS 根網域`; do echo -n "$i => [ipv6] "; dig aaaa $i @8.8.8.8 +short; done	dig
CT-5	DNS	網站使用的 DNS 的 IPv6 都可以 PING 通過	是	成功顯示 PING 到的 IPv6 位址	ping6 根網域	ping6
CT-6	DNS	網站使用的 DNS 要設定網站根網域的 IPv6 位址	是	顯示 IPv6 位址	for i in `dig @8.8.8.8 +short NS 根網域`; do echo -n "$i => [ipv6] "; dig aaaa 根網域 @$i +short; done	dig
CT-7	Mail	網站使	是	顯示 IPv6 位	for i in `dig	dig

	Server	用的 Mail Server 都要有 IPv6 位址，且可以連得上		址	@8.8.8.8 +short MX 根網域 | awk '{print $2}'`; do echo -n "$i => [ipv6] "; dig aaaa $i @8.8.8.8 +short; done;	

表 23　ICP 業者的網路安全檢查表

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

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

ST-12	路由器	DDoS 攻擊（MLD reports）	是	redir6 interface victim-ip target-ip original-router new-router [new-router-mac] [hop-limit]	redir6
ST-13	路由器	DDoS 攻擊（MLDv2 reports）	是	dos-new-ip6 interface	dos-new-ip6
ST-14	路由器	中間人攻擊	是	fake_mipv6 interface home-address home-agent-address care-of-address	fake_mipv6
ST-15	路由器	DDoS 攻擊（unknown options）	是	fake_advertise6 [-DHF] [-Ors] [-n count] [-w seconds] interface ip-address-advertised [target-address [mac-address-advertised [source-ip-address]]]	fake_advertiser6
ST-16	網站主機	DDoS 攻擊（Smurf 攻擊）	是	implementation6d interface	implementation6d
ST-17	DNS	滲透測試	是	flood_dhcpc6 [-n|-N] [-1] [-d] interface [domain-name]	flood_dhcpc6
ST-18	DNS	未經驗證或者偽照的裝置	是	toobig6 [-u] interface target-ip existing-ip mtu [hop-limit]	toobig6
ST-19	DNS	未經驗證或者偽照的裝置	是	fake_dns6d interface ipv6-address [fake-ipv6-address	fake_dns6d

				[fake-mac]]	
ST-20	DNS	未經驗證或者偽照的裝置	是	fake_dnsupdate6 dns-server full-qualified-host-dns-name ipv6address	fake_dnsupdate6
ST-21	作業系統	CVE-2003-0429 Ethereal OSI 解析緩衝區溢位漏洞	是	mitm6.py [-h] [-i INTERFACE] [-l LOCALDOMAIN] [-4 ADDRESS] [-6 ADDRESS] [-m ADDRESS] [-a] [-v] [--debug] [-d DOMAIN] [-b DOMAIN] [-hw DOMAIN] [-hb DOMAIN] [--ignore-nofqdn]	mitm6
ST-22	作業系統	CVE-2004-0257 OpenBSD ICMPv6 處理遠程 DDoS 攻擊漏洞	是	fake_mld6 [-l] interface add|delete|query [multicast-address [target-address [ttl [own-ip [own-mac-address [destination-mac-address]]]]]]	fake_mld6
ST-23	防火牆	DDoS 攻擊（TCP-SYN）	是	fake_mld26 [-l] interface add|delete|query [multicast-address [target-address [ttl [own-ip [own-mac-address [destination-mac-address]]]]]]	fake_mld26
ST-24	防火牆	網路掃描	是	fake_mldrouter6 [-l] interface	fake_mldrouter6

				advertise|solicitate|terminate [own-ip [own-mac-address]]	
ST-25	防火牆	基本設定	是	fake_router6 [-HFD] interface network-address/prefix-length [dns-server [router-ip-link-local [mtu [mac-address]]]]	fake_router6
ST-26	防火牆	基本設定	是	flood_router6 [-HFD] interface	flood_router6
ST-27	其他	DDoS 攻擊	是	flood_advertise6 [-k | -m mac] interface [target]	flood_advertise6
ST-28	其他	未經驗證或者偽照的裝置	是	ndpexhaust26 [-acpPTUrR] [-s sourceip6] interface target-network	ndpexhaust26
ST-29	其他	未經驗證或者偽照的裝置	是	parasite6 [-lRFHD] interface [fake-mac]	parasite6
ST-30	其他	安全評估工具（flow label）	是	smurf6 interface victim-ip [multicast-network-address]	smurf6
ST-31	其他	掃描工具	是	rsmurf6 interface victim-ip	rsmurf6
以下為 IPv4 測試使用					
ST-32	路由器	中間人攻擊	是	arpspoof -i [Network Interface Name] -t [Victim IP] [Router IP]	Arpspoof
ST-33	防火牆	DDoS 攻	是	hping3 --traceroute	hping3

		擊		-V -1 網站	
ST-34	防火牆	中間人攻擊	是	圖形化介面操作	ettercap
ST-35	防火牆	DDoS 攻擊，中間人攻擊	是	圖形化介面操作	Evil FOCA

第三節 輔導 2 家 ICP 業者升級 IPv4/IPv6 雙軌網路服務

一、 輔導廠商記錄

（一） 旅遊咖

旅遊咖網站伺服器以 Nginx 為主，程式語言以 PHP 為主。Javascript library 使用了 Modernizr，前端也同時使用 Nginx 作為 reverse proxy 以提升網站的反應速度。

旅遊咖在 DNS 增加 AAAA record 及 DNS 反解，防火牆開啟 IPv6 封包，允許 IPv6 連線可以從外部連到主機，Load Balance 設定所有 Web Server 都可以透過 IPv6 連線。

旅遊咖使用 Nginx 作為 Web server，並在 port 443 跟 port 80 開啟 IPv6 listen，允許使用者以 IPv6 連線進入，資料庫部分調整儲存 client ip 的欄位大小，程式碼增加對於 IPv6 位址的判斷，作業系統為 Linux，也設定將 IPv6 在 Kernel 的部分打開。

旅遊咖在防火牆及主機存取控管部分，比照 IPv4 的設定規則，設定相同的 IPv6 存取控管規範，在安全策略部分比照 IPv4 的設定，複製一份作為 IPv6 的安全策略。使用作為嚴謹的安全規範，故辦公室內只有限定主機可以連到機房。辦公室網路分網

段，工程師使用的網段可以使用 IPv6，非工程師使用的網段不能使用。

旅遊咖會議記錄

日期	108 年 4 月 24 日(三)
出席	曾榮信、郭愷瀚、林韋廷
地點	台北市松山區長安東路二段 225 號 A 棟 1 樓之一
主旨	ICP IPv4/IPv6 導入
會議內容： 1.旅遊咖參與 IPv4/IPv6 輔導合作可行性評估 2.合作模式 3.輔導項目協助	

日期	108 年 4 月 26 日(五)
出席	曾榮信、郭愷瀚、林韋廷
地點	台北市松山區長安東路二段 225 號 A 棟 1 樓之一
主旨	ICP IPv4/IPv6 導入
會議內容： 1.網址調整討論 www.tripesso.com 跟 www.tripsaas.com 2. IPv6 檢測工具提供	

依第二章第二節內表 22 ICP 業者的 IPv6 設定檢測表進行旅遊咖 IPv6 設定檢驗測試，其 IPv6 確實設定成功，測試結果與畫面請參考下列的圖片。

1. CT-1：網站的 IPv6 位址可以連上(http 或 https)：通過

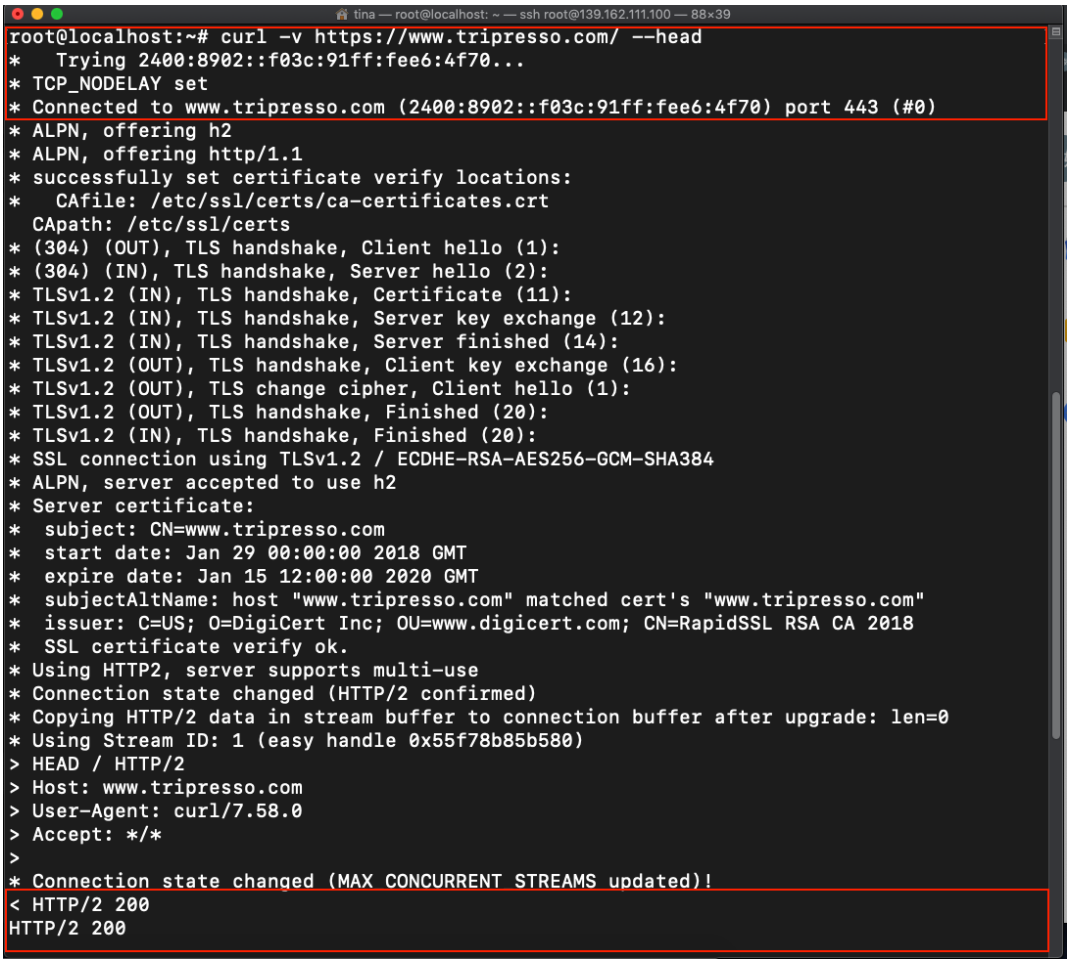

圖 9　旅遊咖 CT-1 測試結果畫面之一

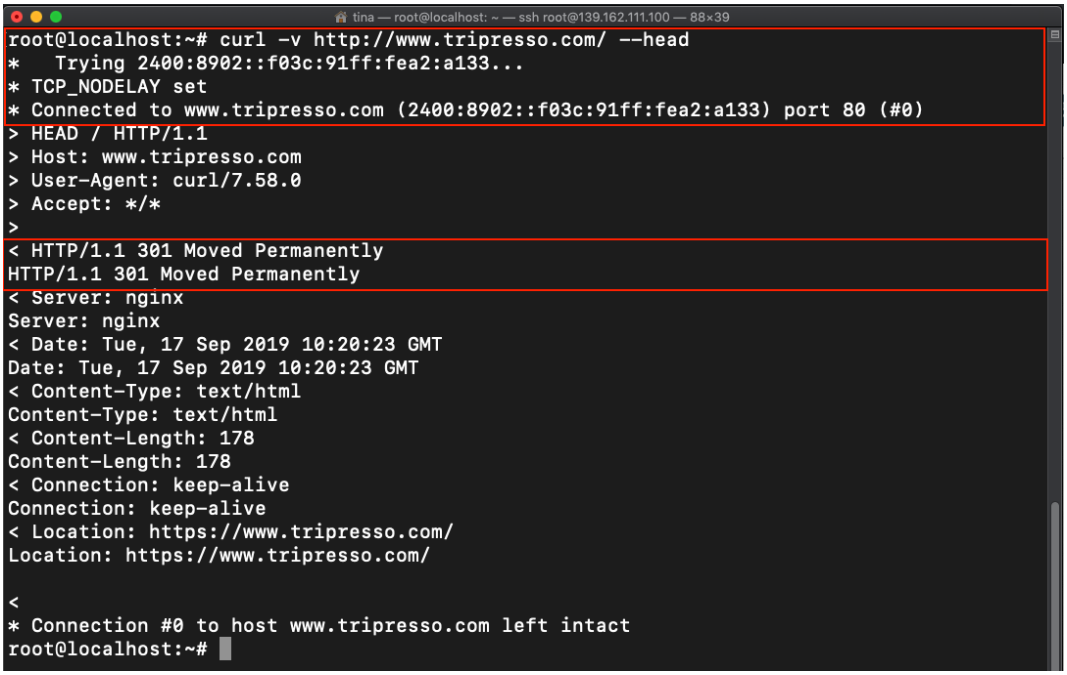

圖 10　旅遊咖 CT-1 測試結果畫面之二

2. CT-2：沿途路由器都有 IPv6 位址：通過

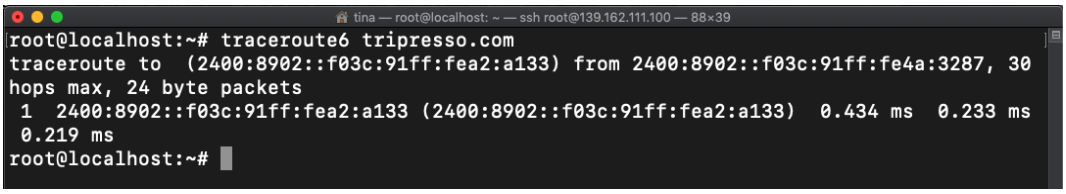

圖 11　旅遊咖 CT-2 測試結果畫面

3. CT-3：網站是否有正確設定 IPv6 位址：通過

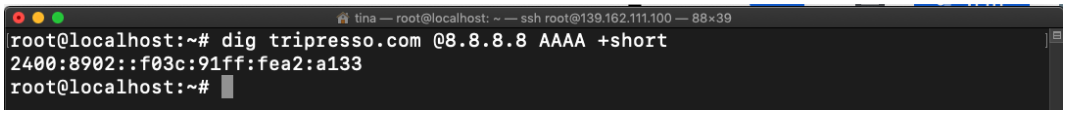

圖 12　旅遊咖 CT-3 測試結果畫面

4. CT-4：網站使用的所有 DNS Server 本身要有 IPv6 位址：通過

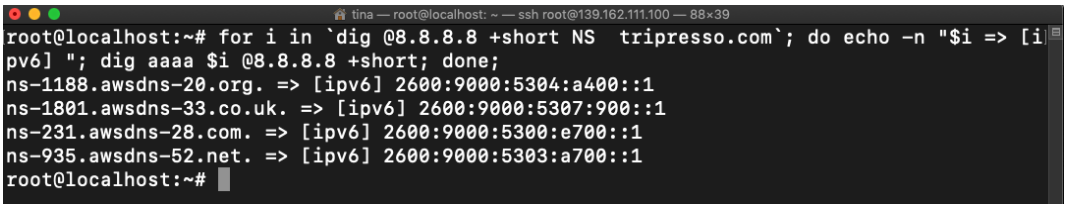

圖 13　旅遊咖 CT-4 測試結果畫面

5. CT-5：網站使用的 DNS 的 IPv6 都可以 PING 通過：通過

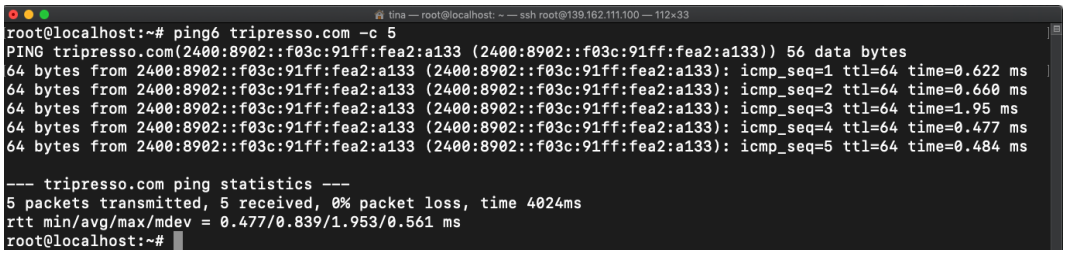

圖 14　旅遊咖 CT-5 測試結果畫面

6. CT-6：網站使用的 DNS 要設定網站根網域的 IPv6 位址：通過

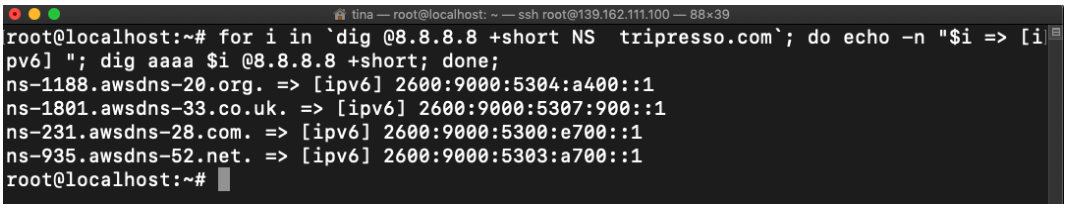

圖 15　旅遊咖 CT-6 測試結果畫面

7. CT-7：網站使用的 Mail Server 都要有 IPv6 位址，且可以連得上：

通過

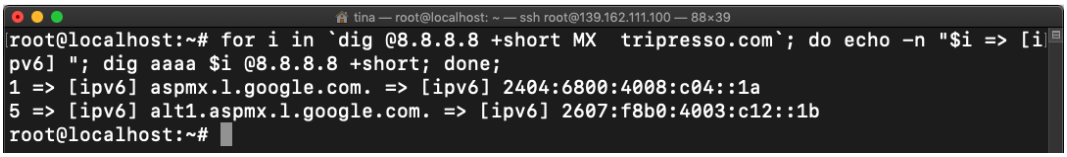

圖 16　旅遊咖 CT-7 測試結果畫面

點選網站主要功能頁面，確認其連線的 IP 確實皆為 IPv6，詳細測試結果與畫面請參考下表與畫面。

表 24　旅遊咖網站測試 IPv6 畫面列表

編號	網站頁面	是否符合 IPv6
WT-1	首頁	是
WT-2	搜尋頁面	是
WT-3	註冊頁面	是
WT-4	登入頁面	是
WT-5	會員頁面	是
WT-6	加入訂單頁面	是
WT-7	最新消息頁面	是
WT-8	旅行社評價頁面	是

圖 17　旅遊咖 WT-1 測試結果畫面

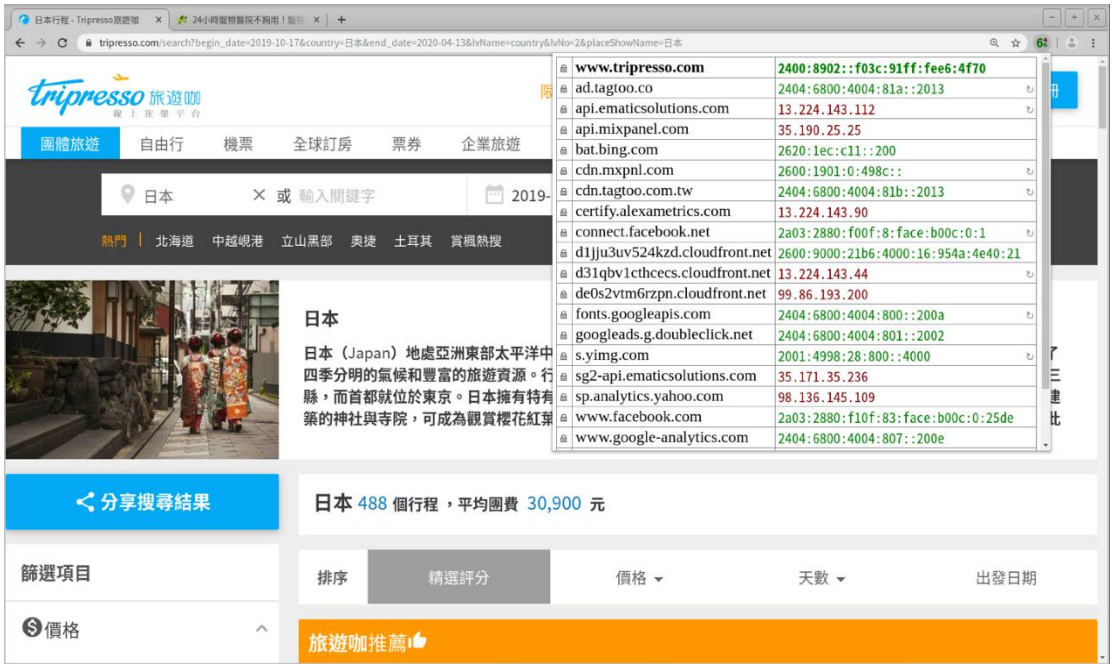

圖 18　旅遊咖 WT-2 測試結果畫面

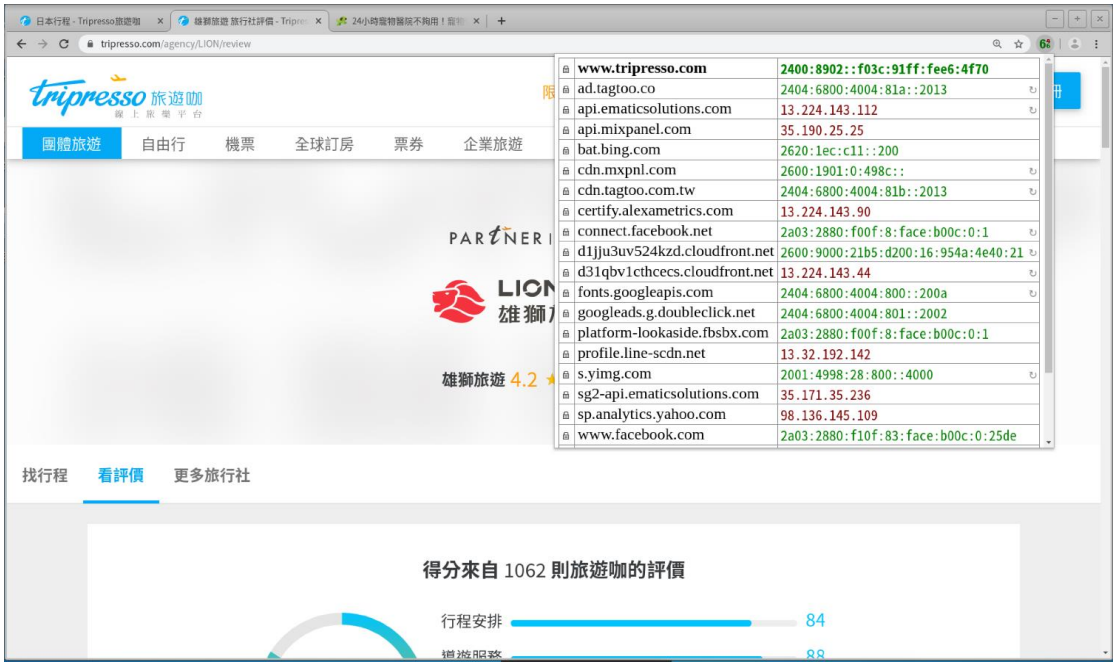

圖 19　旅遊咖 WT-3 測試結果畫面

圖 20　旅遊咖 WT-4 測試結果畫面

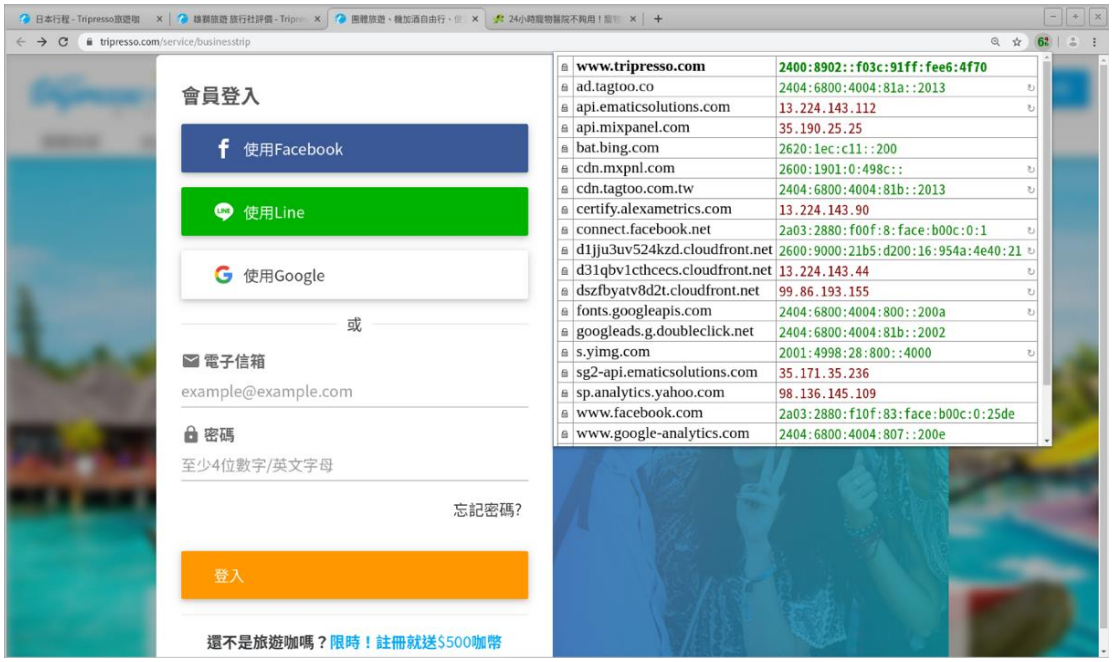

圖 21　旅遊咖 WT-5 測試結果畫面

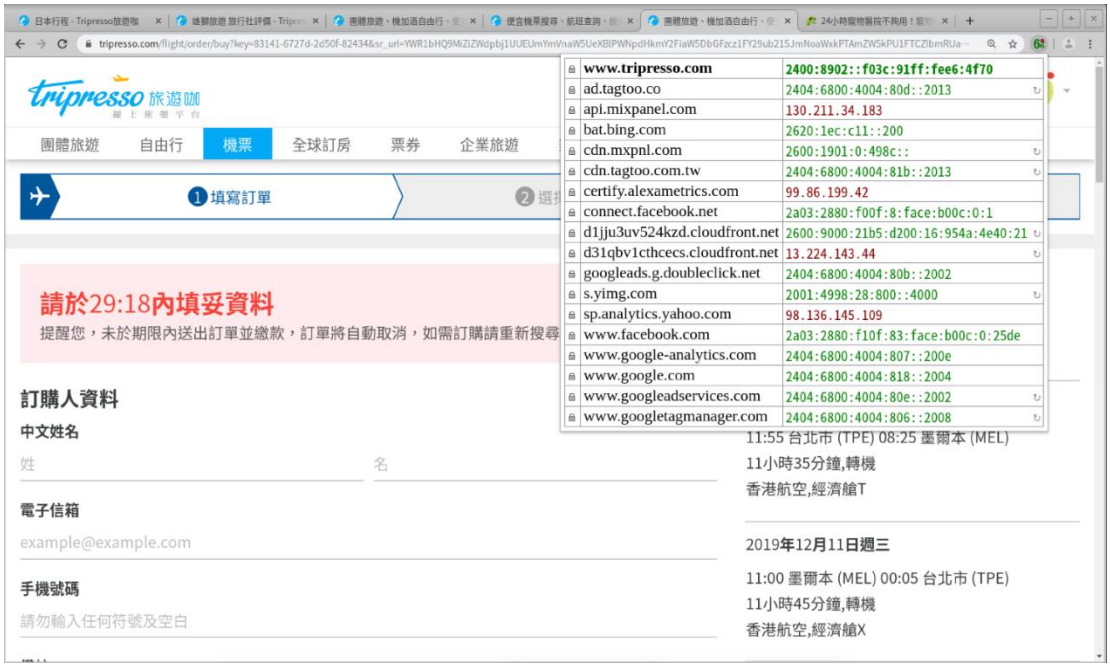

圖 22　旅遊咖 WT-6 測試結果畫面

圖 23　旅遊咖 WT-7 測試結果畫面

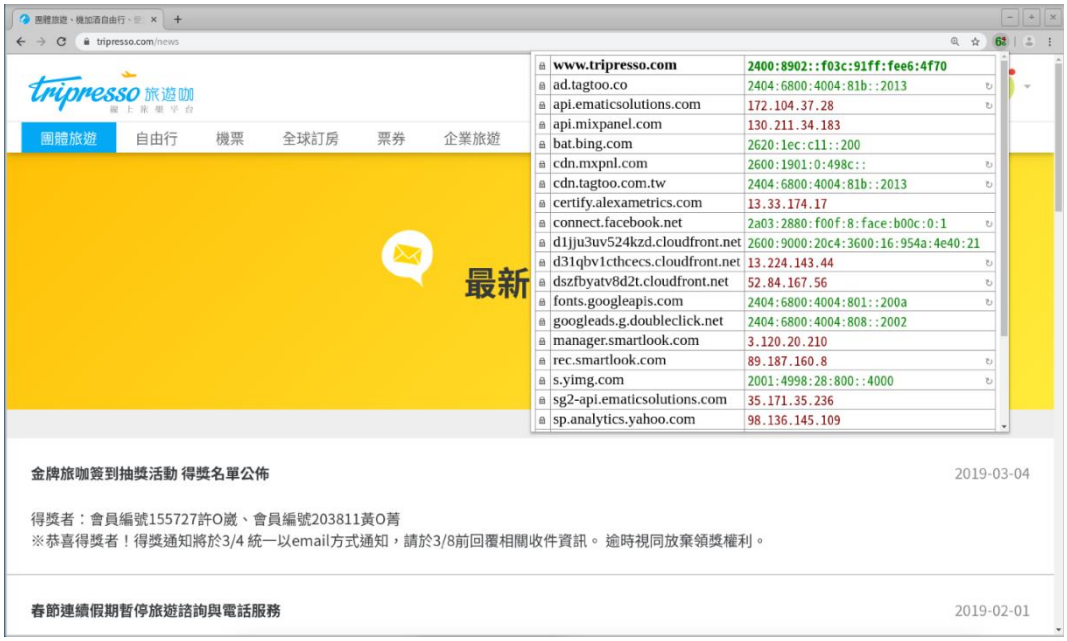

圖 24　旅遊咖 WT-8 測試結果畫面

依第二章第二節內表 23 ICP 業者的網路安全檢查表進行旅遊咖 IPv6 網路安全檢驗測試，測試結果請參考下表。

表 25　旅遊咖 IPv6 網路安全檢查表

編號	測試工具	輸入指令	測試結果
ST-1	thcsyn6	thcsyn6 eth0 2400:8902::f03c:91ff:fea2:a133 443	通過
		thcsyn6 eth0 2400:8902::f03c:91ff:fea2:a133 80	通過
ST-2	exploit6	exploit6 eth0 2400:8902::f03c:91ff:fea2:a133	通過
ST-3	fuzz_ip6	fuzz_ip6 -xIFSDHRJ eth0 2400:8902::f03c:91ff:fea2:a133	通過
ST-4	frag6	frag6 --frag-type atomic -d 2400:8902::f03c:91ff:fea2:a133 -v	通過
		frag6 --frag-reass-policy -d 2400:8902::f03c:91ff:fea2:a133 -v	通過
ST-5	flow6	flow6 -d 2400:8902::f03c:91ff:fea2:a133 -i eth0 -W	通過
ST-6	implementation6	implementation6 eth0 -s sourceip6 2400:8902::f03c:91ff:fea2:a133	通過
ST-7	flood_mld6	flood_mld6 eth0 2400:8902::f03c:91ff:fea2:a133	通過
ST-8	flood_mld26	flood_mld26 eth0 2400:8902::f03c:91ff:fea2:a133	通過
ST-9	denial6	denial6 eth0 2400:8902::f03c:91ff:fea2:a133 1	通過
		denial6 eth0 2400:8902::f03c:91ff:fea2:a133 2	通過
		denial6 eth0 2400:8902::f03c:91ff:fea2:a133 3	通過
		denial6 eth0 2400:8902::f03c:91ff:fea2:a133 4	通過
		denial6 eth0	通過

		2400:8902::f03c:91ff:fea2:a133 5	
		denial6 eth0 2400:8902::f03c:91ff:fea2:a133 6	通過
		denial6 eth0 2400:8902::f03c:91ff:fea2:a133 7	通過
ST-10~ST-35 因測試內容牽涉到公司營業機密及安全考量而沒有進行測試			

經過檢視上表的測試結果可以發現，旅遊咖的資安項目測試皆有通過。

（二） 寵物迷

寵物迷網站使用 WordPress 建置，程式語言為 PHP，資料庫使用 MySQL，Javascript library 使用了 jQuery。網站主機為 Linux based 的作業系統。

寵物迷在 DNS 增加 AAAA record，設定對應的 IPv6 位址，並設定 DNS 反解，確保 DNS 運作正常，設定 Mail Server，可以透過 Mail Server 傳遞及接收信件，調整 Firewall，允許 TCP 的 IPv6 連線封包可以進出。

寵物迷使用 WordPress 為主要平台，調整了 WordPress 對於 IPv6 的支援，升級相關套件(plugin)以支援 IPv6，升級 WordPress

以支援 IPv6 位址的儲存。

寵物迷使用 Nginx 作為 Web Server，調整了 Nginx 的 port 443 跟 port 80 的設定。寵物迷的主機是由第三方公司代管，故主機限制只能由代管公司的特定 IP 位址可以連線進入，並做授權管理。在 IPv6 的設定上，採取最嚴格的存取限制，主機只有開 port 80 跟 443 作為訪客瀏覽使用，而 port 22 則使用 public key/private key 的 key 驗證方式，避免遭到密碼字典暴力破解。

寵物迷會議記錄

日期	108 年 4 月 1 日(一)
出席	鄧丕文、林韋廷
地點	台北市松山區敦化南路一段 2 號
主旨	ICP IPv4/IPv6 導入
會議內容： 1.寵物迷現有系統架構討論 2.寵物迷參與 IPv4/IPv6 專案	

日期	108 年 5 月 27 日(一)
出席	鄧丕文、林韋廷
地點	台北市松山區敦化南路一段 2 號
主旨	網站設定
會議內容： 1.寵物迷 WordPress 網站架構調整 2.網路環境支援 IPv6 設定	

依第二章第二節內表 22 ICP 業者的 IPv6 設定檢測表進行寵物迷 IPv6 設定檢驗測試，其 IPv6 確實設定成功，測試結果與畫面請參考下列的圖片。

1. CT-1：網站的 IPv6 位址可以連上(http 或 https)：通過

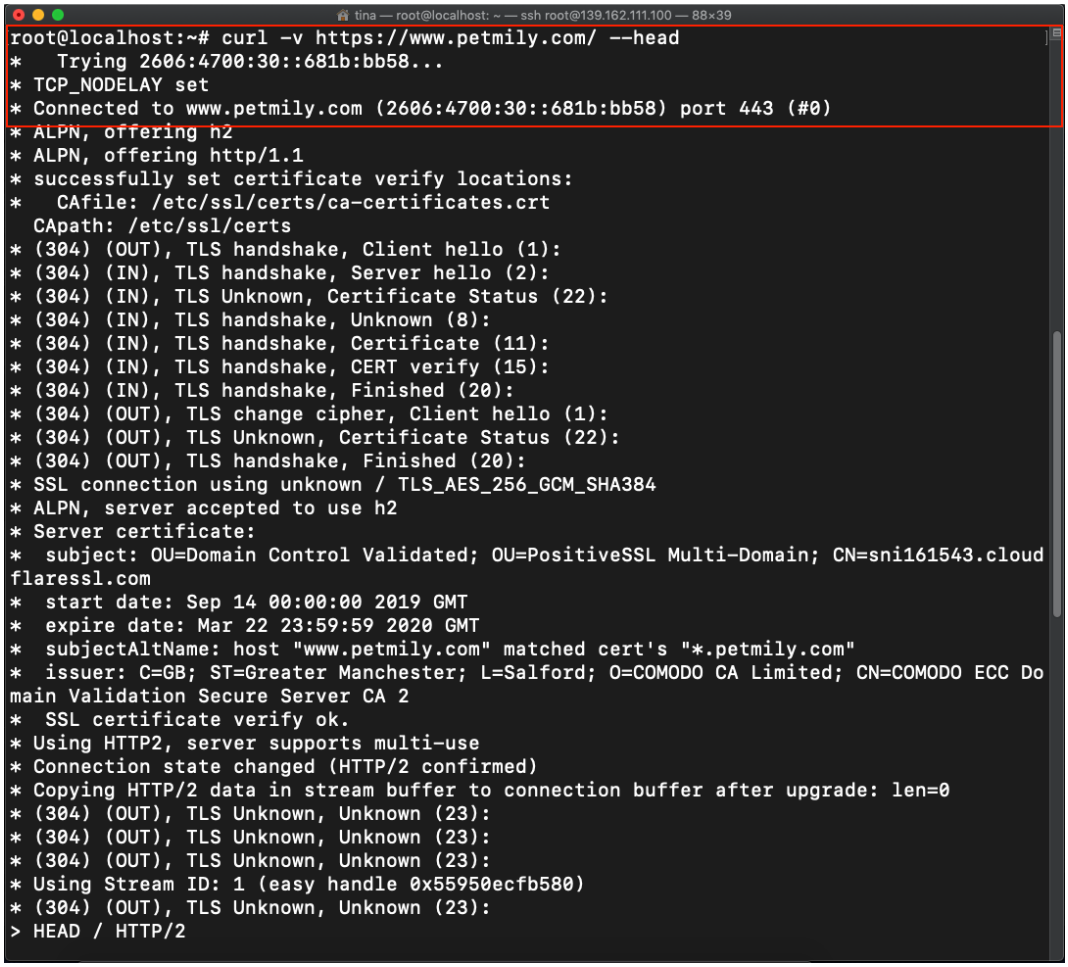

圖 25　寵物迷 CT-1 測試結果畫面之一

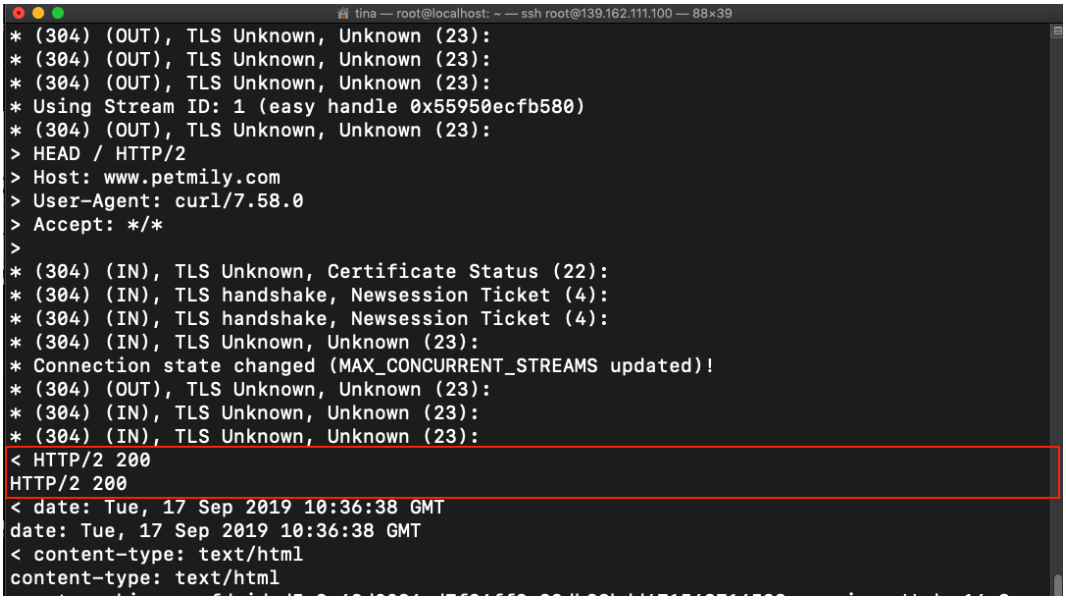

圖 26　寵物迷 CT-1 測試結果畫面之二

圖 27　寵物迷 CT-1 測試結果畫面之三

2. CT-2：沿途路由器都有 IPv6 位址：通過

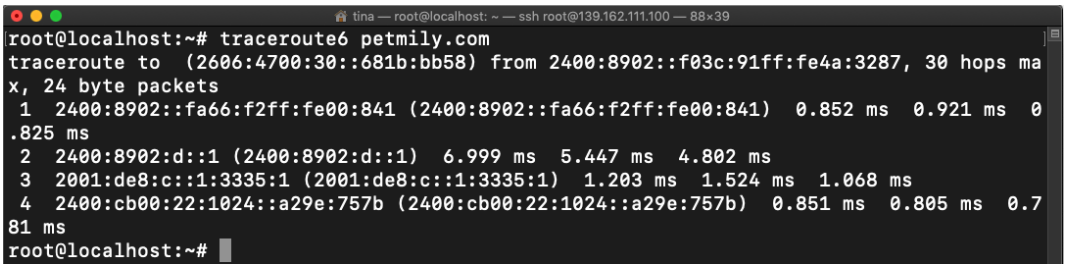

圖 28　寵物迷 CT-2 測試結果畫面

3. CT-3：網站是否有正確設定 IPv6 位址：通過

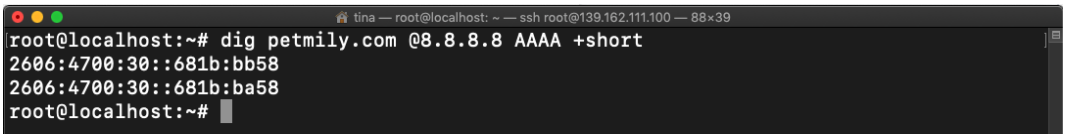

圖 29　寵物迷 CT-3 測試結果畫面

4. CT-4：網站使用的所有 DNS Server 本身要有 IPv6 位址：通過

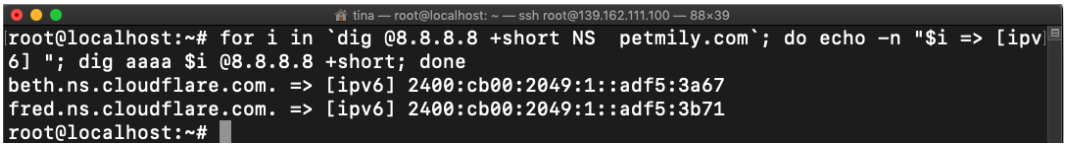

圖 30　寵物迷 CT-4 測試結果畫面

5. CT-5：網站使用的 DNS 的 IPv6 都可以 PING 通過：通過

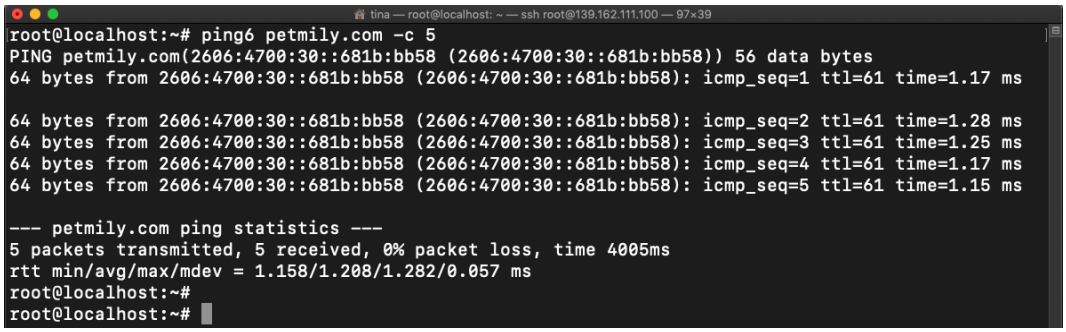

圖 31　寵物迷 CT-5 測試結果畫面

6. CT-6：網站使用的 DNS 要設定網站根網域的 IPv6 位址：通過

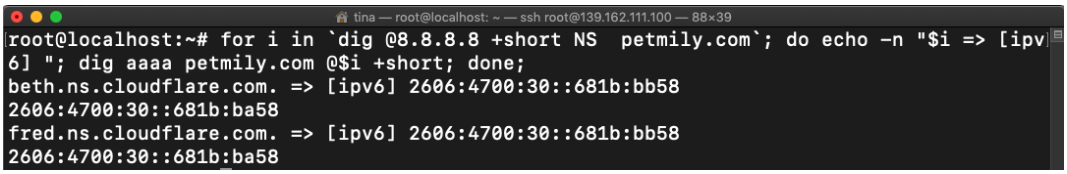

圖 32　寵物迷 CT-6 測試結果畫面

7. CT-7：網站使用的 Mail Server 都要有 IPv6 位址，且可以連得上：通過

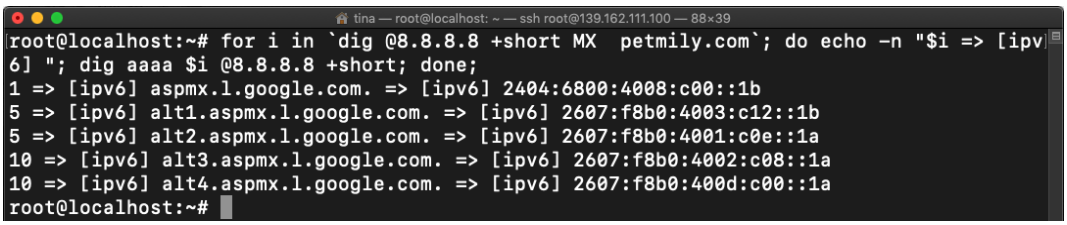

圖 33　寵物迷 CT-7 測試結果畫面

點選網站主要功能頁面，確認其連線的 IP 確實皆為 IPv6，詳細測試結果與畫面請參考下表與畫面。

表 26　寵物迷網站測試 IPv6 畫面列表

編號	網站頁面	是否符合 IPv6
WT-1	首頁	是
WT-2	搜尋頁面	是
WT-3	文章頁面	是

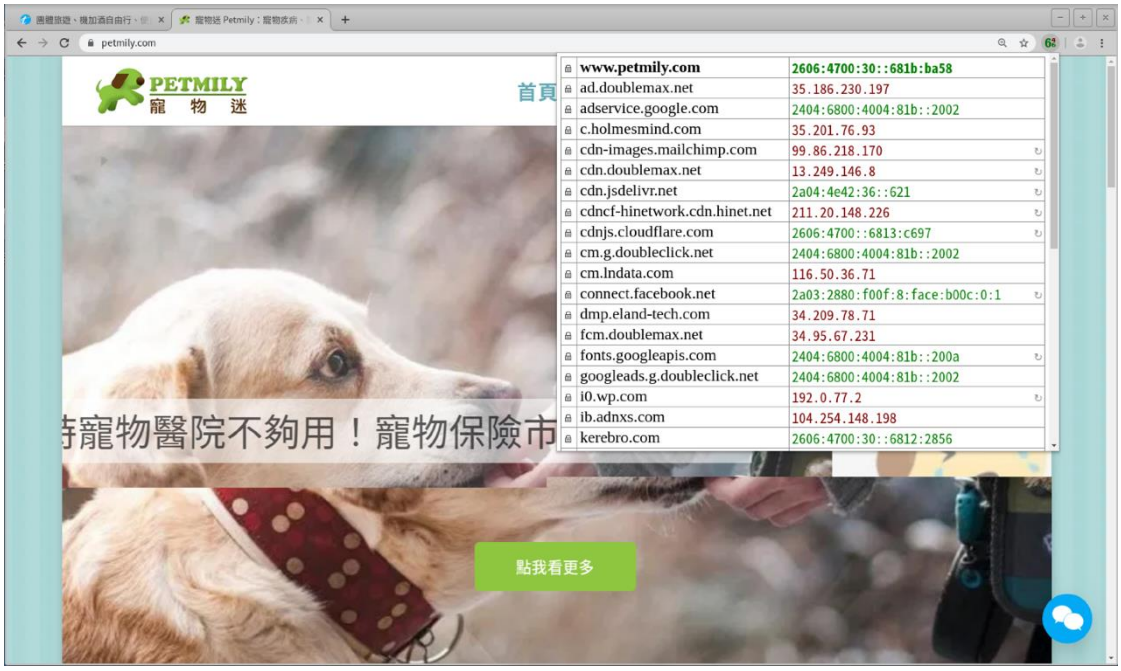

圖 34　寵物迷 WT-1 測試結果畫面

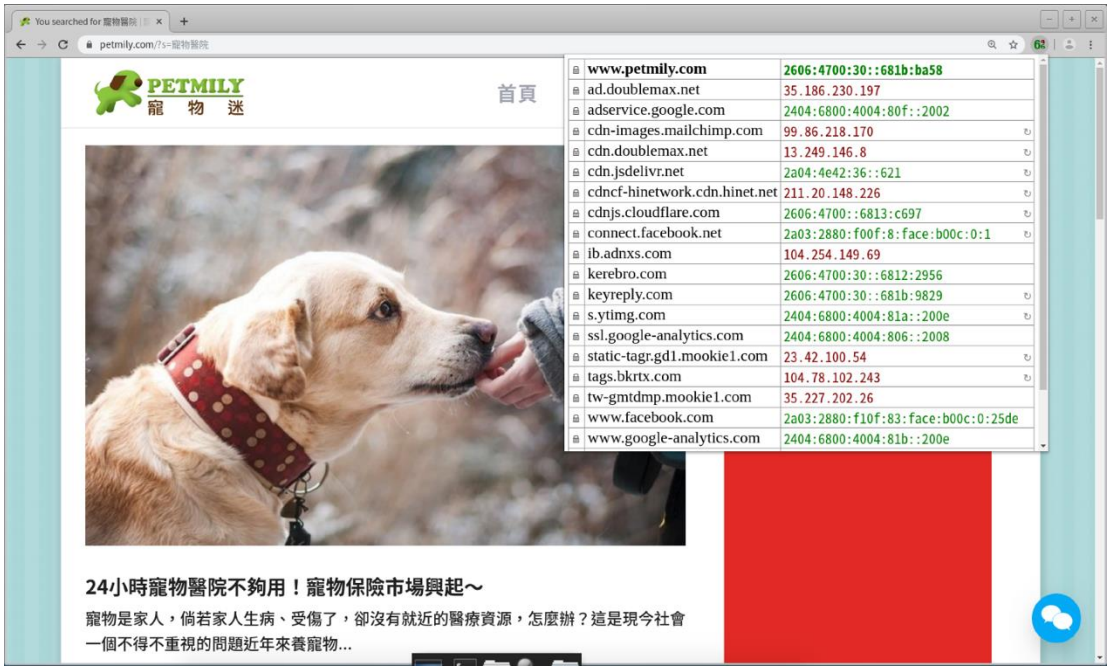

圖 35　寵物迷 WT-2 測試結果畫面

圖 36　寵物迷 WT-3 測試結果畫面

依第二章第二節內表 23 ICP 業者的網路安全檢查表進行寵物迷 IPv6 網路安全檢驗測試，測試結果請參考下表。

表 27　寵物迷 IPv6 網路安全檢查表

編號	測試工具	輸入指令	測試結果
ST-1	thcsyn6	thcsyn6 eth0 2606:4700:30::681b:ba58 80	通過
		thcsyn6 eth0 2606:4700:30::681b:bb58 80	通過
		thcsyn6 eth0 2606:4700:30::681b:ba58 443	通過
		thcsyn6 eth0 2606:4700:30::681b:bb58 443	通過
ST-2	exploit6	exploit6 eth0 2606:4700:30::681b:ba58	通過
		exploit6 eth0 2606:4700:30::681b:bb58	通過
ST-3	fuzz_ip6	fuzz_ip6 -xIFSDHRJ eth0 2606:4700:30::681b:ba58	通過
		fuzz_ip6 -xIFSDHRJ eth0 2606:4700:30::681b:bb58	通過
ST-4	frag6	frag6 --frag-type atomic -d 2606:4700:30::681b:ba58 -v	通過
		frag6 --frag-type atomic -d 2606:4700:30::681b:bb58 -v	通過
ST-5	flow6	flow6 -d 2606:4700:30::681b:ba58 -i eth0 -W	通過
		flow6 -d 2606:4700:30::681b:bb58 -i eth0 -W	通過
ST-6	implementation6	implementation6 eth0 -s sourceip6 2606:4700:30::681b:ba58	通過
		implementation6 eth0 -s sourceip6 2606:4700:30::681b:bb58	通過
ST-7	flood_mld6	flood_mld6 eth0 2606:4700:30::681b:ba58	通過
		flood_mld6 eth0 2606:4700:30::681b:bb58	通過
ST-8	flood_mld	flood_mld26 eth0	通過

	26	2606:4700:30::681b:bb58	
		flood_mld26 eth0 2606:4700:30::681b:ba58	通過
ST-9	denial6	denial6 eth0 2606:4700:30::681b:ba58 1	通過
		denial6 eth0 2606:4700:30::681b:ba58 2	通過
		denial6 eth0 2606:4700:30::681b:ba58 3	通過
		denial6 eth0 2606:4700:30::681b:ba58 4	通過
		denial6 eth0 2606:4700:30::681b:ba58 5	通過
		denial6 eth0 2606:4700:30::681b:ba58 6	通過
		denial6 eth0 2606:4700:30::681b:ba58 7	通過
		denial6 eth0 2606:4700:30::681b:bb58 1	通過
		denial6 eth0 2606:4700:30::681b:bb58 2	通過
		denial6 eth0 2606:4700:30::681b:bb58 3	通過
		denial6 eth0 2606:4700:30::681b:bb58 4	通過
		denial6 eth0 2606:4700:30::681b:bb58 5	通過
		denial6 eth0 2606:4700:30::681b:bb58 6	通過
		denial6 eth0 2606:4700:30::681b:bb58 7	通過
ST-10~ST-35 因測試內容牽涉到公司營業機密及安全考量而沒有進行測試			

經過檢視上表的測試結果可以發現，寵物迷的資安項目測試皆有通過。

（三） 運動筆記

運動筆記的網頁伺服器為 Apache，程式語言使用了 Node.js，Javascript 的框架使用了 Socket.io 及 TweenMax，資料庫使用 Firebase，Javascript 的 library 使用了 jQuery。

運動筆記在 DNS 增加 AAAA record，設定對應的 IPv6 位址，並設定 Mail Server，允許 IPv6 的信件發送及接受。

運動筆記採取最嚴格的安全控管措施，Web server 僅開放 port 80 跟 443，其他 port 全數關閉，管理人員進行主機管理時，也是透過 Web 連線進入，且設定防火牆的 ACL 政策，限制只有公司內部特定 IP 才可以存取。

運動筆記因為人力被調度到其他專案，故支援 IPv6 的專案被暫停，目前尚未有繼續 IPv6 支援的時程表。因此運動筆記的 IPv6 升級輔導先終止。

運動筆記會議記錄

日期	108 年 5 月 7 日(二)
出席	張義、吳奎億、林韋廷
地點	台北市大安區和平東路一段 216 號 7 樓
主旨	ICP IPv4/IPv6 導入
會議內容： 1.運動筆記現有系統及網路架構討論	

（四） 滔客 talk.tw 生活傳媒

滔客後台使用 Microsoft IIS 7 作為作業系統，資料庫使用 Microsoft SQL Server，程式語言使用 ASP.NET，前端使用 jQuery Javascript library 及 Bootstrap。滔客在 Alexa 全台灣排名為 714 名，擁有超大流量及眾多的訪客。滔客的網頁伺服器放在台灣固網 IaaS 第一代雲端主機上。

滔客會議記錄

日期	108 年 4 月 10 日(三)
出席	江奇峰、林韋廷
地點	台北市大安區金山南路二段 222 號 3 樓
主旨	ICP IPv4/IPv6 導入
會議內容： 1.拜訪滔客邀請加入 ICP IPv4/IPv6 輔導計畫 2.滔客提供現有架構 3.提供 IPv6 檢測工具	

日期	108 年 4 月 25 日(四)
出席	江奇峰、林韋廷
地點	台北市大安區金山南路二段 222 號 3 樓
主旨	IPv6 申請作業
會議內容： 1.向台灣固網申請 IPv6 IP，但台灣固網告知無法提供 IPv6 (第一代	

跟二代都不提供) 2.使用台灣固網雲服務第一代(IaaS, VM)

日期	108 年 5 月 2 日(四)
出席	江奇峰、林韋廷
地點	台北市大安區金山南路二段 222 號 3 樓
主旨	台灣固網 IaaS 不支援 IPv6
會議內容： 1.台灣固網不論是第一代 IaaS 還是第二代 IaaS 都不支援 IPv6 2.由於滔客網站架設在台灣固網 IaaS 第一代上，因為台灣固網 IaaS 不支援 IPv6，故與滔客的合作計畫中止	

（五） 買動漫

買動漫為台灣最大的動漫網站，在 Alexa 台灣排名 548。底層以 PHP 開發，前端使用 jQuery Javascript library，網頁伺服器為 nginx 。

買動漫會議記錄

日期	108 年 4 月 26 日(二)
出席	詹強、李益興、林韋廷
地點	台北市復興南路一段 390 號 4 樓之 3
主旨	ICP IPv4/IPv6 輔導計畫
會議內容： 1.買動漫網站有意願加入 IPv4/IPv6 計畫，不過由於負責機房管理的人力無法支援，故討論後，決定放棄。	

第三章　結論與建議

第一節 結論說明

一、 研析 ICP IPv4/IPv6 升級及網路安全防護差異

某些原本的 IPv4 漏洞，在 IPv6 可能沒有，但大部分 Pv4 的漏洞在 IPv6 都持續存在，而有些新的安全問題是因為 IPv6 才有，在 IPv4 是沒有的。當網站導入 IPv6 時，如何避免因使用 IPv6 而衍生出新的安全跟隱私漏洞問題，本報告針對 IPv4 與 IPv6 在網路安全防護的差異進行說明，並針對網站因導入 IPv6 所衍生新問題進行歸納與整理。

二、 建立 ICP IPv4/IPv6 平台架構雙協定網路安全防護檢查項目清單

清單的建立會因為不同軟硬體設備、不同版本而不同，須常調整。

三、 輔導 2 家 ICP 業者升級 IPv4/IPv6 雙軌網路服務

輔導的 ICP 廠商暫定或者無法繼續合作的原因包括：

1. 提供機房服務的固網業者(例如：台灣固網 IaaS)的軟硬體無法支援 IPv6

2. 使用的平台(例如：SHOPLINE)不支援 IPv6

第二節 建議事項

一、 研析 ICP IPv4/IPv6 升級及網路安全防護差異

台灣缺乏 IPv6 推廣文章，應該撰寫 IPv6 推廣及介紹文章，從概念、實作、創意、安全等各種角度切入，教育更多的網路用戶，有助於日後 IPv6 的應用普及與發展。建議可以成立一個 IPv6 推廣網站，將國外的 IPv6 文章翻譯成中文文章並推廣。

二、 建立 ICP IPv4/IPv6 平台架構雙協定網路安全防護檢查項目清單

建議將檢查清單放置在網站上，並提供 Wiki 方式供各家廠商增添修改檢查清單的項目，保持資料的正確性。或者直接在 Wiki 維基百科上申請中文項目的 ICP IPv6 檢查清單，確保資料可保持更新。

輔導 2 家 ICP 業者升級 IPv4/IPv6 雙軌網路服務

1. ICP 業者願意配合輔導大都希望有媒體曝光機會，建議提供媒體曝光機會。
2. 有 ICP 業者原本有意願參加，但因為台灣固網 IaaS 不支援而停止，建議能盡快要求所有在台灣提供雲端機房的業者，能全面升級支援 IPv6，這樣才可以讓更多有意願的

ICP 業者可以執行。

3. 建議由政府提供 IPv6 工程師認證，並提供補助費用，讓 IT 人員可以進修，學習 IPv6 知識，落實 IPv6 的技術推廣。

參考資料

[1] RFC 1546 Host Anycasting Service
https://tools.ietf.org/html/rfc1546
[2] RFC 1576 TN3270 Current Practices
https://tools.ietf.org/html/rfc1576
[3] RFC 1883 Internet Protocol, Version 6 (IPv6) Specification
https://tools.ietf.org/html/rfc1883
[4] RFC 1918 Address Allocation for Private Internets
https://tools.ietf.org/html/rfc1918
[5] RFC 1981 Path MTU Discovery for IP version 6
https://tools.ietf.org/html/rfc1981
[6] RFC 2401 Security Architecture for the Internet Protocol
https://tools.ietf.org/html/rfc2401
[7] RFC 2402 IP Authentication Header
https://tools.ietf.org/html/rfc2402
[8] RFC 2406 IP Encapsulating Security Payload (ESP)
https://tools.ietf.org/html/rfc2406
[9] RFC 2460 Internet Protocol, Version 6 (IPv6) Specification
https://tools.ietf.org/html/rfc2460
[10]RFC 2462 IPv6 Stateless Address Autoconfiguration
https://tools.ietf.org/html/rfc2462
[11]RFC 3014 IPv6 Stateless Address Autoconfiguration
https://tools.ietf.org/html/rfc3014
[12]RFC 3041 Privacy Extensions for Stateless Address Autoconfiguration in IPv6
https://tools.ietf.org/html/rfc3041
[13]RFC 3852 Cryptographic Message Syntax (CMS)
https://tools.ietf.org/html/rfc3852
[14]RFC 3971 SEcure Neighbor Discovery (SEND)
https://tools.ietf.org/html/rfc3971
[15]RFC 4301 Security Architecture for the Internet Protocol
https://tools.ietf.org/html/rfc4301
[16]RFC 4862 IPv6 Stateless Address Autoconfiguration
https://tools.ietf.org/html/rfc4862
[17]RFC 4864 Local Network Protection for IPv6
https://tools.ietf.org/html/rfc4864
[18]RFC 4890 Recommendations for Filtering ICMPv6 Messages in

Firewalls
https://tools.ietf.org/html/rfc4890
[19]RFC 4941 Privacy Extensions for Stateless Address Autoconfiguration in IPv6
https://tools.ietf.org/html/rfc4941
[20]RFC 5902 IAB Thoughts on IPv6 Network Address Translation
https://tools.ietf.org/html/rfc5902
[21]RFC 5996 Internet Key Exchange Protocol Version 2 (IKEv2)
https://tools.ietf.org/html/rfc5996
[22]RFC 6437 IPv6 Flow Label Specification
https://tools.ietf.org/html/rfc6437
[23]RFC 6494 Certificate Profile and Certificate Management for SEcure Neighbor Discovery (SEND)
https://tools.ietf.org/html/rfc6494
[24]RFC 6564 A Uniform Format for IPv6 Extension Headers
https://tools.ietf.org/html/rfc6564
[25]RFC 7123 Security Implications of IPv6 on IPv4 Networks
https://tools.ietf.org/html/rfc7123
[26]RFC 7359 Layer 3 Virtual Private Network (VPN) Tunnel Traffic Leakages in Dual-Stack Hosts/Networks
https://tools.ietf.org/html/rfc7359
[27]A Glance through the VPN Looking Glass: IPv6 Leakage and DNS Hijacking in Commercial VPN clients
https://petsymposium.org/2015/papers/02_Perta.pdf
[28]Understanding IPv6 And DNS Leaking, by Jay H Simmons
https://www.vpncrew.com/understanding-ipv6-and-dns-leaking/
[29]IPv6 Address Representation and Address Types, by Rick Graziani., 03 Oct 2017
http://www.ciscopress.com/articles/article.asp?p=2803866&seqNum=5
[30]The Difference Between IPv6 and IPv4 IP Addresses
https://www.coursehero.com/file/15205432/The-Difference-Between-IPv6-and-IPv4-IP-Addresses/
[31]IPV6 MULTICAST - MULTICAST LISTENER DISCOVERY (MLD), by INE
https://blog.ine.com/2009/12/26/ipv6-multicast-multicast-listener-discovery-mld
[32]Internet Protocols: Versions 4 and 6 Analysis and Comparison of

IPv4 and IPv6, by Wushi09, 21 Sep 2015
https://www.cybrary.it/0p3n/internet-protocols-versions-4-and-6-analysis-and-comparison-of-ipv4-and-ipv6/

[33]為何值得為 IPv6 的建置努力的三大理由，台網中心電子報

2019/02
https://blog.twnic.net.tw/2019/01/31/2361/

[34]What is IPv6 stateless address auto-configuration?
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=2ahUKEwiBpeiroq3kAhXMGKYKHWMhAbYQFjACegQIDBAG&url=https%3A%2F%2Fmysupport.netapp.com%2FNOW%2Fpublic%2Feseries%2Fsam%2FGUID-8538272A-B802-49D9-9EA2-96C82DAD26A2%2FGUID-06C52868-5C1F-4E76-86D5-4815C2E9EBC6.html&usg=AOvVaw2Bil-09MU4QCW5earvN8lT

[35]中華電信公司 HiNet IPv6 用戶連線參考手冊

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

[36]中華電信 HiNet IPv6 固定制服務說明

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

[37]QoS — 未來行動網路的服務品質保證

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

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

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

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

[40]IPv6/IPv4 IPv6/IPv4 轉換技術

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

[41]IPv6 Fundamentals: A Straightforward Approach to Understanding IPv6
https://books.google.com.tw/books?id=FbYjJjZNA5gC&pg=PA335&lpg=PA335&dq=ipv6+0x0800+0x86DD&source=bl&ots=5mIjGIw

W_E&sig=ACfU3U34zzWevIUhxbY4H7HL3ofpwDgKpg&hl=zh-TW&sa=X&ved=2ahUKEwjbxp3A167kAhXjGKYKHYrSCbIQ6AEwEnoECAcQAQ#v=onepage&q=ipv6%200x0800%200x86DD&f=false

[42]IPv6 跟現階段 IP 位址配發差異與發展技術介紹

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

[43]剖析 IPv6 的安全風險問題

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

[44]IPv6 Security
https://books.google.com.tw/books?id=kwOv0Aw2lIUC&pg=PT360&lpg=PT360&dq=ipv6+esp&source=bl&ots=Qmr93IAZ4f&sig=ACfU3U171Cq1dpyz0vyy1eSsYSmXg8hB7g&hl=zh-TW&sa=X&ved=2ahUKEwjSoJSL36_kAhUNCqYKHRuuCGM4ChDoATADegQIBhAB#v=onepage&q=ipv6%20esp&f=false

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

[46]剖析 IPv6 的安全風險問題

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

[47]IPv6 作業系統與應用服務建置實習(Linux)

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

[48]中華電信 IPv6 通訊協定與特性介紹

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

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

[50]IPv6 Fundamentals: A Straightforward Approach to Understanding IPv6
https://books.google.com.tw/books?id=AMkmDwAAQBAJ&pg=PT

111&lpg=PT111&dq=why+ipv6+doesn%27t+need+ihl&source=bl&ots=dpjoVgYmmv&sig=ACfU3U0XBRFNlOAC8zLPTf9zs5k1rp-rHw&hl=zh-TW&sa=X&ved=2ahUKEwj1l_7y06rkAhUiy4sBHTweC5QQ6AEwCnoECAgQAQ#v=snippet&q=security&f=false
[51]An integrated testing system for IPv6 and DNSSEC
https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/s13638-016-0675-4
[52]IPv6 Security: Attacks and Countermeasures in a Nutshell
https://www.sba-research.org/wp-content/uploads/publications/Johanna%20IPv6.pd
[53]IPv6-ready system check
http://tldp.org/HOWTO/Linux+IPv6-HOWTO/ch04s01.html
[54]ROGUE ROUTER ADVERTISEMENT ATTACK
http://6lab.cz/rogue-router-advertisement-attack/
[55]How To Detect & Prevent Rogue Devices on Your Network with UDT
https://www.youtube.com/watch?v=EZBaiEDTrfQ
[56]Attackers Can Use IPv6 to Launch Man-in-the-Middle Attacks
https://www.eweek.com/security/attackers-can-use-ipv6-to-launch-man-in-the-middle-attacks
[57]IPv6 MITM via fake router advertisements
https://isc.sans.edu/forums/diary/IPv6+MITM+via+fake+router+advertisements/10660/
[58]35 Types of DDoS Attacks Explained
https://javapipe.com/blog/ddos-types/
[59]Could IPv6 Result in More DDoS Attacks?
https://www.allot.com/blog/ipv6_ddos_attack_vulnerability/
[60]How to Prepare for IPv6 DDoS attack
https://medium.com/@CybriantMSSP/how-to-prepare-for-ipv6-ddos-attack-4620cba369fc
[61]IPv6 DDoS and Protection Measures
https://community.infoblox.com/t5/IPv6-CoE-Blog/IPv6-DDoS-and-Protection-Measures/ba-p/12830
[62]IPv6 extension headers and security: Analyzing the risk
https://searchsecurity.techtarget.com/tip/IPv6-extension-headers-and-security-Analyzing-the-risk
[63]IPv6 Extension Headers Review and Considerations
https://www.cisco.com/en/US/technologies/tk648/tk872/technologies

_white_paper0900aecd8054d37d.html
[64]Recommendations on the Filtering of IPv6 Packets Containing IPv6 Extension Headers
https://tools.ietf.org/html/draft-ietf-opsec-ipv6-eh-filtering-04
[65]Security implication and detection of threats due to manipulating IPv6 extension headers
https://ieeexplore.ieee.org/document/6726061
[66]Security Impacts of Abusing IPv6 Extension Headers
https://media.blackhat.com/ad-12/Atlasis/bh-ad-12-security-impacts-atlasis-wp.pdf
[67]thc-ipv6 工具包
https://www.mankier.com/package/thc-ipv6
[68]Get your site ready for IPv6: a step-by-step guide
https://blog.mythic-beasts.com/2014/09/15/get-your-site-ready-for-ipv6-a-step-by-step-guide/
[69]How To Configure Tools to Use IPv6 on a Linux VPS, by Justin Ellingwood, 01 Apr 2014
https://www.digitalocean.com/community/tutorials/how-to-configure-tools-to-use-ipv6-on-a-linux-vps#checking-ipv6-dns-informatio
[70]ICANNWiki
https://icannwiki.org/IPv6
[71]IPv6 Multicast Address Space Registry
https://www.iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xhtml
[72]IPv6 multicast addresses
https://study-ccna.com/ipv6-multicast-addresses/
[73]MRTG with RRDtool and Routers2 – Installation from Scratch
https://blog.webernetz.net/mrtg-with-rrdtool-and-routers2-installation-from-scratch/
[74]IPv6 Security 7 : RFC6092 and RFC4890 with full details
http://computer-outlines.over-blog.com/article-ipv6-security-7-rfc6092-and-rfc4890-with-full-details-120085093.html
[75]Network Security IPv6 Security for IPv4 Engineers
https://www.internetsociety.org/wp-content/uploads/2019/03/deploy360-ipv6-security-v1.0.pdf
[76]Waters, A., "The SLAAC Attack - using IPv6 as a weapon against IPv4", April 2011,

https://wirewatcher.wordpress.com/2011/04/04/the-slaac-attack-using-ipv6-as-a-weapon-against-ipv4/

[77]IPv6 and Open Source IDS
https://www.sans.org/reading-room/whitepapers/logging/ipv6-open-source-ids-35957

[78]維基百科 Fail2ban

https://zh.wikipedia.org/wiki/Fail2ban

中英專有名詞對照

A

ACL 存取控制列表(Access Control List)

ARP 位址解析協定(Address Resolution Protocol)

D

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

DNS 網域名稱伺服器(Domain Name System)

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

Dual Stack IPv4/ IPv6 雙協定 (Dual Stack)

E

Email 電子郵件(Electronic mail)

F

Firewall 防火牆

FTP 檔案傳輸協定(File Transfer Protocol)

I

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

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

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

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

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

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

IDC 資訊機房(Internet Data Center)

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

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

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

IPv6 Day IPv6 日(IPv6 Day)

IPv6 Ready Logo 網際網路通訊協定第六版認證獎章

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

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

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

IT 資訊技術(Information Technology)

L

L3 Switch 第三層交換器(Layer 3 Switch)

Load Balancers 負載平衡器

M

Mobile Internet 行動上網(Mobile Internet)

N

NAT 網路位址轉譯(Network Address Translation)

Network Layer 網路層(Network Layer)

P

Proxy 代理伺服器

Q

QoS 服務品質(Quality of Service)

R

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

RFC 網際網路協定規範(Request For Comments)

Router 路由器

T

TCP 傳輸控制協定(Transmission Control Protocol)

TWNIC 財團法人台灣網路資訊中心(Taiwan Network Information Center)

W

WWW 全球資訊網(World Wide Web)

WiFi AP 無線基地台(WiFi AP)